

Cisco Wireless Phone 840 and 860 Administration Guide for Cisco Unified Communications Manager

First Published: 2021-01-08

Last Modified: 2026-11-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

About the phones 1

Cisco Wireless Phone 840 and 860 1

Ingress Protection 4

Phone model numbers 4

New and changed information 5

New and changed information for release 1.10(3) 5

New and changed information for release 1.10(0) 6

New and changed information for release 1.9(0) 6

New and changed information for release 1.8(0) 7

New and changed information for release 1.7(0) 8

New and changed information for release 1.6(0) 8

New and changed information for release 1.5(0) 9

New and changed information for release 1.4(0) 12

New and changed information for release 1.3(0) 13

Supported languages 14

Hardware, buttons, screen, and apps 15

Hardware and buttons 15

Launcher screen 19

Cisco apps 20

Care of your phone 22

Maintenance schedule 22

Maintain your phone 23

Disinfectants 25

UV disinfection 26

Dry your phone 27

Related documentation 27

Cisco Wireless Phone 840 and 860 documentation 27
Cisco Unified Communications Manager documentation 27
Cisco IP phone user support 28
Configuration and deployment workflow 28

CHAPTER 2 **Initial setup** 31
Network requirements 31
Cisco Wireless Phone 840 and 860 deployment guide 32
Cisco Unified Communications Manager requirements 32
Device enabler QED installer file 33
Phone software file 33
Phone configuration files 33
Load the COP files to Cisco Unified Communications Manager 34
Phone battery installation 35
Install the battery 36
Remove the battery 38
Hot swap the battery for Cisco Wireless Phone 860 and 860S 39
Battery contact damage prevention 40
Phone battery charging 41
Charge the battery with the AC power supply 42
Charge the battery with the USB cable and a USB port on your computer 42

CHAPTER 3 **Cisco Unified Communications Manager phone configuration** 45
Determine the MAC address of the phone 45
Install manufacturing CA certificates 45
Before you register wireless phones 46
Device pool configuration 47
Create custom SIP profile 47
Phone button template configuration 48
Phone softkey templates 48
Create a new phone security profile 49
Manual phone registration 50
Add an end user (Optional) 50
Add the phone 51

Add the phone extension 53
Phone feature configuration 55
Set up phone features for all phones 55
Set up phone features for a group of phones 56
Set up phone features for a single phone 56
Product Specific Configuration Layout fields 57
Configure visual voicemail 62
Configure Tomcat trust certificate 63
Configure the voicemail box and Web Application Password 64
Enable Visual Voicemail Access 64
Configure the voicemail server to the Cisco Unity Connection server 64
Phone services 65
Phone line configuration options 66
Problem report tool 66
Configure a customer support upload URL 67
Corporate and personal directories setup 68
Corporate directory setup 68
Personal directory setup 68
Self Care Portal overview 69
Set up user access to the Self Care Portal 69
Call pickup 70

CHAPTER 4 **Phone configuration** 71
Enterprise Mobility Management application configuration 71
Enroll the phones to the Enterprise Mobility Manager application 71
Cisco Wireless Phone Configuration Management tool 72
Cisco Wireless Phone Configuration Management tool workflow 73
Generate a QR code to initialize phones 74
Enroll phones with Cisco Wireless Phone Configuration Management tool QR code 75
Create encrypted phone configuration file 76
Preinstalled Android apps 78
Upload the phone configuration file to Cisco Unified Communications Manager 79
Update existing configuration file 80
Smart Launcher usage tips 81

Manual phone configuration 81
Wi-Fi profile configuration 82
Add the phone to a broadcasted Wi-Fi network 82
Add the phone to a nonbroadcast Wi-Fi network 83
Configure a TFTP server 84
Configure a Call server mode 85

CHAPTER 5 **Cisco app configuration 87**
Cisco app configuration overview 87
Enterprise Mobility Management application interface 87
Program the Enterprise Mobility Management application 88
Cisco Wireless Phone Configuration Management tool for Cisco app configuration 90
Access the Cisco app settings on the phone 91
Emergency app 91
Emergency app configuration 92
Send emergency event notifications 92
Motion sensor 93
Panic Button settings 95
Emergency call settings 96
Emergency tone settings 97
Emergency app and Panic Button training 98
Push to Talk app 98
User settings for Push to Talk 98
Admin settings for Push to Talk 99
Battery Life app 100
User settings for Battery Life 101
Admin settings for Battery Life 101
Buttons app 102
Programmable buttons 102
Buttons settings 104
Set a button to run an application 109
Answer and end calls using the hardware buttons 109
Set a button to answer a call 109
Set a button to end or decline a call 111

Turn ON and OFF flaslight using the hardware buttons 111
Set a button to control the flashlight 111
Set a button to toggle the flashlight 112
Cisco app package names 113
Barcode app 114
Barcode symbologies 114
General settings for the Barcode app 115
Default settings for the Barcode app 116
ScanFlex 129
ScanFlex settings 130
Actions for advanced data formatting 130
Test scan a barcode 132
Custom Settings app 133
User restrictions in Custom Settings 133
More Custom Settings 139
Call Quality Settings app 148
Wi-Fi information 148
Call Quality Settings 149
Diagnostics app 154
Sound Stage app 155
Admin Settings for Sound Stage 155
Audio profiles 156
Change the audio profile 157
Profile switch rules 158
Web API app 158
Phone state polling 159
Push settings 160
Push request notifications 161
Web application shortcuts 161
Place web application shortcuts on launcher screen 162
Device event notifications 162

CHAPTER 6 Accessories 165
Supported accessories 165

Headsets 166
Important headset safety information 166
Standard headsets 167
Bluetooth headsets 167
Desktop chargers 167
Set up the desktop chargers 168
Charge your phone and battery with desktop dual charger 169
Charge your spare 860 batteries with desktop battery charger 170
Multichargers 171
Assemble the Cisco Wireless Phone 860 Multicharger Base 172
Charge phones and batteries with multicharger 174
Charger care 175
Scanner handle for the Cisco Wireless Phone 840S 175
Install the Cisco Wireless Phone 840S in the scanner handle 176
Clips 177
Cisco accessory part numbers 177

CHAPTER 7 Maintenance 181
Reboot the phone 181
Factory default settings 181
Reset to factory default through the phone settings 182
Restore to factory default through recovery mode 182
Cisco app software updates 183

CHAPTER 8 Troubleshooting 185
General troubleshooting information 185
Details available on the phone 186
View phone information 186
Access phone status and device information 187
Access the About option for a Cisco app 187
Exit and reenter the Smart Launcher on the phone 188
Capture a screenshot on the phone 188
Problem report log bundles 189
Generate a problem report and log bundle 189

Retrieve problem report log bundles 190

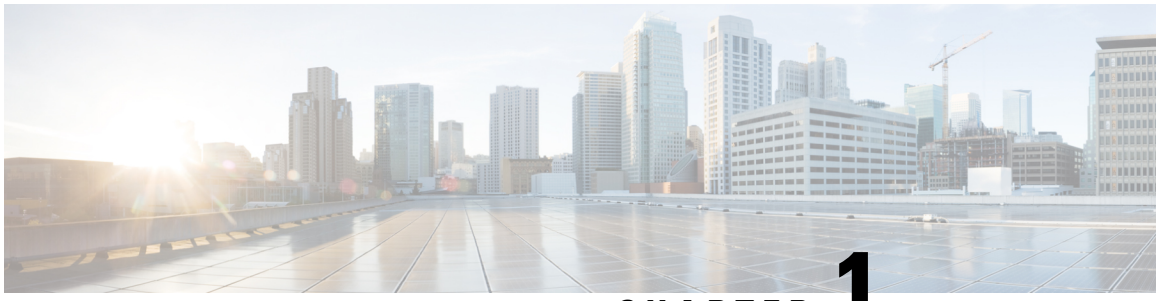
APPENDIX A

Appendix 193

InformaCast Advanced Notification Support 193

CTI-Controlled Support 195

Android 13 App Permissions 199



CHAPTER 1

About the phones

- Cisco Wireless Phone 840 and 860, on page 1
- New and changed information, on page 5
- Supported languages, on page 14
- Hardware, buttons, screen, and apps, on page 15
- Care of your phone, on page 22
- Related documentation, on page 27
- Cisco IP phone user support, on page 28
- Configuration and deployment workflow, on page 28

Cisco Wireless Phone 840 and 860

The Cisco Wireless Phone 840 and 860 are wireless smartphones. These phones provide voice communication over your organization's wireless network using Cisco Unified Communications Manager and access points (APs). They work within the Wi-Fi range set by your organization.

Like other devices powered by Android, your phone is app-driven, not menu-driven. You tap icons to open applications. Your phone may include several different Cisco apps that allow you to:

- Place and receive phone calls.
- Put calls on hold.
- Transfer calls.
- Have conference calls.
- Forward your calls.
- Monitor your phone battery life.
- Customize your phone buttons.
- If configured, provide emergency safety features such as alarms and motion monitoring.
- If configured, send group broadcasts.

Like other network devices, the administrator configures and manages these phones. Based on the needs of your organization, the administrator may limit certain apps, features, or settings that may be available on consumer-grade Android devices.

Contact your administrator for information about the configured capabilities of your phone within your organization.

The following figure shows the Cisco Wireless Phone 840 on the left and the Cisco Wireless Phone 840S on the right. The Cisco Wireless Phone 840S includes a barcode scanner.

Figure 1: Cisco Wireless Phone 840 and Cisco Wireless Phone 840S



The following figure shows the Cisco Wireless Phone 860 on the left and the Cisco Wireless Phone 860S on the right. The Cisco Wireless Phone 860S includes a barcode scanner.

Figure 2: Cisco Wireless Phone 860 and Cisco Wireless Phone 860S



The Cisco Wireless Phone 860 and Cisco Wireless Phone 860S, though larger in size than the Cisco Wireless Phone 840 and Cisco Wireless Phone 840S, are similar in appearance and functionality.

Some physical characteristics of the Cisco Wireless Phone 840 and 860 include:

- 4.0 in. (10.2 cm) touchscreen for the 840 phones
- 5.2 in. (13.2 cm) touchscreen for the 860 phones
- 8 MP rear and 5 MP front camera for the 840 phones
- 13 megapixel (MP) rear and 8 MP front camera for the 860 phones
- Damage resistant Gorilla™ glass
- Recessed display for screen protection
- Tolerance of antibacterial and alcohol-based wipes
- Latex- and lead-free
- Shockproof and vibration-proof
- USB-C interface
- USB On-the-Go (OTG) 2.0 interface for use with a desktop charger or multicharger
- Cisco Wireless Phone 840 has Ingress Protection 65 (IP65) with resistance to dust and water spray from a nozzle
- Cisco Wireless Phone 860 has Ingress Protection 68 (IP68) with resistance to dust, drops, and liquids
- Chargeable with a USB, desktop charger, or multicharger

For more details about the phones, see the product data sheet.

If configured, your phone provides enhanced productivity features that extend your call-handling capabilities, such as:

- Bluetooth® wireless headsets, including some hands-free call features
- Wireless access to your phone number and the corporate directory
- Access to network data, Android apps, and web-based services
- Online customization of the call forward feature from the Self Care portal

To prevent device damage:

- Don't intentionally submerge the phone or battery in water.
- Don't expose the phone to pressurized water or high velocity water, such as when showering, cleaning, or hand washing.
- Don't bathe or swim with the phone.
- Don't use the phone in a sauna or steam room.
- Don't use the phone in corrosive environments.
- Don't operate or store the phone, batteries, and accessories outside the suggested temperature ranges or in extremely humid, hot, or cold conditions.
- Don't intentionally drop the phone or subject it to other impacts.
- Don't disassemble the phone; don't remove any screws.
- Don't use harsh cleaning agents, like bleach and other chemicals, to clean the phone exterior.
- Don't use a broken battery.

Minimize the exposure of your phone to soap, detergent, acids or acidic foods, and any liquids; for example, salt water, soapy water, pool water, perfume, insect repellent, lotions, sun screen, oil, adhesive remover, hair dye, soft drinks, and solvents. For more information, see Care of your phone, on page 22.

Ingress Protection

The Cisco Wireless Phone 840 and 860 are tested under controlled laboratory conditions.

The Cisco Wireless Phone 840 and 840S have a rating of IP65 in ordinary locations. IP65 indicates that the phones can withstand dust and are resistant to water spray from a nozzle.

The Cisco Wireless Phone 860 and 860S have a rating of IP68 in ordinary locations. IP68 indicates that the phones can withstand dust and are resistant to brief submersion in shallow fresh water.

Due to normal wear, the resistance of the phone to dust and water may decrease. Therefore, it’s important to take care of your phone and not deliberately expose the phone to a hostile environment of dust or water.

Phone model numbers

Each phone has a model number. If you're unsure which model you have, you can locate the model number on the back of the phone after you remove the battery.

Note You can also find the model number through **Settings** > **About Phone** > **Model & hardware**.

Table 1: Cisco Wireless Phone 840 and 860 model numbers

Phone	Model number
Cisco Wireless Phone 840	CP-840
Cisco Wireless Phone 840S	CP-840S
Cisco Wireless Phone 860	CP-860
Cisco Wireless Phone 860S	CP-860S

New and changed information

The following section describes changes to this book to support new releases.

New and changed information for release 1.10(3)

The following table describes changes to this book to support release 1.10(3).

Table 2: New and changed information for release 1.10(3)

Feature	New or changed information
Answer and end calls using the hardware buttons	**New:** • Answer and end calls using the hardware buttons
Set a button to answer a call	**New:** • Set a button to answer a call
Set a button to end or decline a call	**New:** • Set a button to end or decline a call
Turn ON and OFF flashlight using the hardware buttons	**New:** • Turn ON and OFF flashlight using the hardware buttons

Feature	New or changed information
Set a button to control the flashlight	**New:** • Set a button to control the flashlight
Set a button to toggle the flashlight	**New:** • Set a button to toggle the flashlight

New and changed information for release 1.10(0)

The following table describes changes to this book to support release 1.10(0).

Table 3: New and changed information for release 1.10(0)

Feature	New or changed information
Updated Ringtone Per Line Management for Cisco Unified Communications Manager	**Updated:** • Product Specific Configuration Layout fields
Third Party Application Conflicts	**Updated:** • General issues
CTI Controlled support	**Updated:** • Add the phone
Cisco Unified IP Phone Services Application Development / XML object support (Informacast)	**New:** • InformaCast Advanced Notification Support
CTI Controlled support	**New:** • CTI-Controlled Support

New and changed information for release 1.9(0)

The following table describes changes to this book to support release 1.9(0).

Table 4: New and changed information for release 1.9(0)

Feature	New or changed information
Cisco Unified Survivable Remote Site Telephony	**Updated:** • Phone services

Feature	New or changed information
Add Configuration File Dump to Cisco Apps and Log Bundles	**Updated:** • Generate a problem report and log bundle
Call Pickup	**New:** • Call pickup
Report a Problem User Choice in Cisco Phone UI	**Updated:** • Generate a problem report and log bundle
Diagnostics Application	**New:** • Diagnostics app **Updated:** • Cisco apps package names
CAC is Disabled by Default	**Updated:** • Call Quality Settings > Wi-Fi preferences
Announced Caller ID	**Updated:** • Product Specific Configuration Layout fields
Mute SIP Registration Notifications	**Updated:** • Product Specific Configuration Layout fields
Push Custom Ringtone, Notification, Alarm, and Wallpaper	**Updated:** • More Custom Settings > Sounds • More Custom Settings > Wallpaper

New and changed information for release 1.8(0)

The following table describes changes to this book to support release 1.8(0).

Table 5: New and changed information for release 1.8(0)

Feature	New or changed information
Recording for Cisco Unified Communications Manager	**Updated:** • Phone line configuration options

Feature	New or changed information
Recording for Cisco Unified Communications Manager	**Updated:** • Add the phone extension
Ringtone Per Line Management for Cisco Unified Communications Manager	**Updated:** • Product Specific Configuration Layout fields

New and changed information for release 1.7(0)

The following table describes changes to this book to support release 1.7(0).

Table 6: New and changed information for release 1.7(0)

Feature	New or changed information
Lightweight Directory Access Protocol (LDAP) for Webex Calling	**Updated:** • Phone services
Maximum Battery Charge Cycles Notification	**Updated:** • Battery Life app
Sound Stage app	**Updated:** • Cisco apps package names
Sound Stage app	**New:** • Sound Stage app

New and changed information for release 1.6(0)

The following table describes changes to this book to support release 1.6(0).

Table 7: New and changed information for release 1.6(0)

Feature	New or changed information
Webex Calling support	**Updated:** • Phone services
Configure a Call server mode	**New:** • Configure a Call server mode

New and changed information for release 1.5(0)

The following table describes changes to this book to support release 1.5(0).

Table 8: New and changed information for release 1.5(0)

Feature	New or changed information
New Cisco Wireless Phone Configuration Management tool to quickly deploy and configure multiple Cisco Wireless Phones without an Enterprise Mobility Management (EMM) application. When you use the Cisco Wireless Phone Configuration Management tool, the phone has a new smart launcher screen with single-app or multi-app display mode.	

Feature	New or changed information
	New: • Cisco Wireless Phone Configuration Management tool , on page 72 • Cisco Wireless Phone Configuration Management tool workflow, on page 73 • Generate a QR code to initialize phones, on page 74 • Enroll phones with Cisco Wireless Phone Configuration Management tool QR code, on page 75 • Create encrypted phone configuration file, on page 76 • Preinstalled Android apps, on page 78 • Upload the phone configuration file to Cisco Unified Communications Manager, on page 79 • Update existing configuration file, on page 80 • Cisco Wireless Phone Configuration Management tool for Cisco app configuration, on page 90 • Exit and reenter the Smart Launcher on the phone, on page 188 **Updated**: • Cisco Wireless Phone 840 and 860, on page 1 • Launcher screen, on page 19 • Cisco apps, on page 20 • Configuration and deployment workflow, on page 28 • Cisco Unified Communications Manager requirements, on page 32 • Load the COP files to Cisco Unified Communications Manager, on page 34 • Create a new phone security profile, on page 49 • Product Specific Configuration Layout fields, on page 57 • Enroll the phones to the Enterprise Mobility Manager application, on page 71 • Manual phone configuration, on page 81 • Cisco app configuration overview, on page 87 • User restrictions in Custom Settings, on page 133 • Capture a screenshot on the phone, on page 188

Feature	New or changed information
Alternate Network Time Protocol (NTP) service from local network in DHCP option 42.	**Updated**: • Network requirements, on page 31 • More Custom Settings, on page 139

New and changed information for release 1.4(0)

The following table describes changes to this book to support release 1.4(0).

Table 9: New and changed information for release 1.4(0)

Feature	New or changed information
To download firmware, use HTTP on TCP 6970 only, not HTTPS on TCP 6971	**Updated**: Product Specific Configuration Layout fields, on page 57 Cisco app software updates, on page 183
Extension mobility cross cluster (EMCC)	**Updated**: Phone services, on page 65
Personal directory is available with contacts that synchronize through Cisco Unified Communications Manager	**New**: Corporate and personal directories setup, on page 68 Corporate directory setup, on page 68 Personal directory setup, on page 68 Self Care Portal overview, on page 69 Set up user access to the Self Care Portal, on page 69
New test scan is available in the Barcode app	**Updated**: Barcode app, on page 114 **New**: Test scan a barcode, on page 132
Information about the Wi-Fi access point connection displays in the Call Quality Settings app	**New**: Wi-Fi information, on page 148
Updates to the user interface with new Webex branding color and style	**Updated**: With this release, you'll notice some minor changes to user interface elements, such as button colors and icon shapes. The only icon that looks different is on the **Call Quality Settings** app.

New and changed information for release 1.3(0)

The following table describes changes to this book to support release 1.3(0).

Table 10: New and changed information for release 1.3(0)

Feature	New or changed information
Multiple lines	**Updated**: • Before you register wireless phones, on page 46 • Phone button template configuration, on page 48 • Add the phone extension, on page 53 • Configure a TFTP server, on page 84 • Access phone status and device information, on page 187 • Access the About option for a Cisco app, on page 187 • Generate a problem report and log bundle, on page 189
Shared lines	**Updated**: • Before you register wireless phones, on page 46 • Phone button template configuration, on page 48
Privacy on shared lines	**Updated**: • Before you register wireless phones, on page 46 • Phone button template configuration, on page 48
Cisco Extension Mobility	**New**: • Phone services, on page 65
Auto answer	**New**: • Phone line configuration options, on page 66
Line text label	**New**: • Phone line configuration options, on page 66
Call Admission Control and Traffic Specification	**Updated**: • Network requirements, on page 31
PTT broadcast on a locked phone	**Updated**: • Admin settings for Push to Talk , on page 99

Feature	New or changed information
Custom Settings app has **Dark theme** and **Nearby share** quick settings tiles	**Updated**: • User restrictions in Custom Settings, on page 133
Custom Settings app now includes display settings	**Updated**: • More Custom Settings, on page 139
More information about model numbers and accessories	**New**: • Phone model numbers, on page 4 • Cisco accessory part numbers, on page 177 **Updated**: • Phone battery charging, on page 41 • Charge the battery with the AC power supply, on page 42 • Charge the battery with the USB cable and a USB port on your computer, on page 42 • Supported accessories, on page 165 • Desktop chargers, on page 167 • Multichargers, on page 171 • Clips, on page 177

Supported languages

The phones currently support the following languages.

- Danish
- Dutch
- English
- Finnish
- French
- German
- Hungarian
- Italian
- Norwegian
- Portuguese

- Russian
- Slovenian
- Spanish
- Swedish

Hardware, buttons, screen, and apps

Your phone's hardware, buttons, screens, and apps are similar to that of a consumer-grade smartphone or other Android device. However, since your phone is a managed device, your organization may configure certain limitations or allowances on the phone.

Hardware and buttons

Your wireless phone has many hardware features and buttons that you use regularly.

Although the Cisco Wireless Phone 840 and Cisco Wireless Phone 860 are different sizes, the hardware and buttons perform the same actions. However, the hardware features and buttons are not in the same location on the phones. Another difference between the phones is that the Cisco Wireless Phone 840 doesn't have a fingerprint button.

Cisco Wireless Phone 840 hardware and buttons

The following figure shows the Cisco Wireless Phone 840 and 840S with a barcode scanner.

Figure 3: Cisco Wireless Phone 840 and 840S

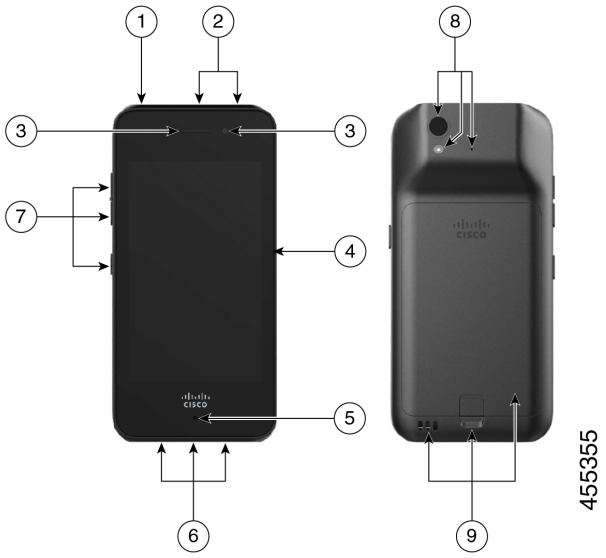


Table 11: Cisco Wireless Phone 840 and 840S hardware and buttons

Group number	Hardware or buttons in group
1	On the top left of the phone is the round **Power** button, which turns the power on and off, and locks and unlocks the screen.
2	On the top center of the Cisco Wireless Phone 840S is the barcode scanner, and on the top right is a round red **Programmable Emergency** alarm button. • Barcode scanner—If the phone is an 840S, scans a barcode. • **Programmable Emergency** button—By default this programmable button is set as an **Emergency** button. If configured, the button sends a preprogrammed emergency panic alert.
3	On the top front of the phone is the receive speaker in the middle, and the front camera on the right. • Receive speaker—Receives audio. • Front camera—Captures images.
4	On the right side of the phone is the **Programmable PTT** button. By default this programmable button is set to activate PTT. If enabled, PTT sends broadcast messages over preprogrammed channels like a walkie-talkie.
5	On the bottom front of the phone is the microphone, which captures your audio to send.
6	On the bottom of the phone is the headset jack on the left, the USB charging port in the middle, and the speaker on the right. • Headset jack—Supports a headset with a 3.5-mm audio plug. • USB charging port—Supports a USB cable to charge the phone. • Speaker—Receives audio you can hear.
7	On the left side of the phone are three programmable buttons. By default, the top and middle buttons are set as **Volume up** and **Volume down** respectively. By default, the bottom button is not set. • **Programmable Volume up** button—By default, this programmable button is set to turn up the volume. • **Programmable Volume down** button—By default, this programmable button is set to turn down the volume. • **Programmable** button—By default, this programmable button is set as the barcode scanner on the 840S phones.

Group number	Hardware or buttons in group
8	On the upper left back of the phone is the rear camera above the flash lens or torch, with the rear microphone to the right. • Rear camera—Captures images. • Flash lens or torch—Emits light for a camera flash, or torch flashlight. • Rear microphone—Cancels noise.
9	On the lower back of the phone are the charger contacts on the left, the battery latch in the middle lower edge of the battery, and the battery. • Charger contacts—Connects with the contacts on a desktop charger or multicharger to charge the battery. • Battery latch—Releases and catches the battery in the phone. • Rechargeable battery—Powers the phone.

Cisco Wireless Phone 860 hardware and buttons

The following figure shows the Cisco Wireless Phone 860 and 860S with a barcode scanner.

Figure 4: Cisco Wireless Phone 860 and 860S

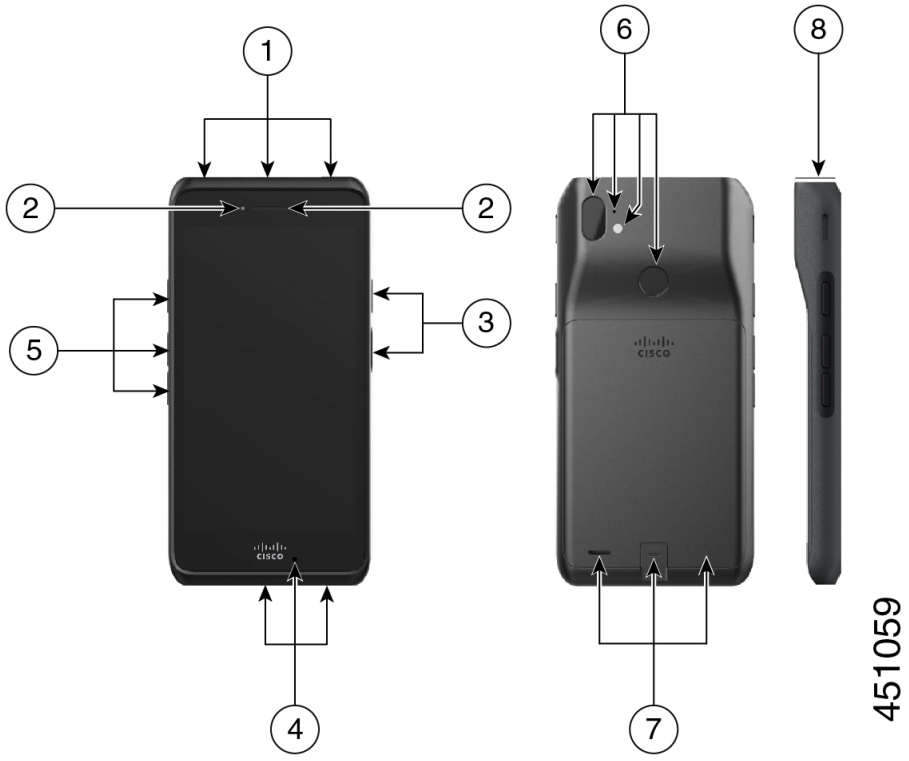


Table 12: Cisco Wireless Phone 860 and 860S hardware and buttons

Group number	Hardware or buttons in group
1	On the top of the phone is the headset jack on the left, the bar code scanner for 860S phones in the middle, and a red **Programmable Emergency** alarm button on the right. • Headset jack—Supports a headset with a 3.5-mm audio plug. • Barcode scanner—If the phone is an 860S, scans a barcode. • **Programmable Emergency** button—By default this programmable button is set as an **Emergency** button. If configured, the button sends a preprogrammed emergency panic alert.
2	On the top front left of the phone is the front camera, with the receive speaker to the right. • Front camera—Captures images. • Receive speaker—Receives audio.
3	On the right side of the phone is the **Programmable Push to Talk (PTT)** button on the top, and the **Power** button on the bottom. • **Programmable PTT** button—By default this programmable button is set to activate PTT. If enabled, PTT sends broadcast messages over preprogrammed channels like a walkie-talkie. • **Power** button—Turns the power on and off, and locks and unlocks the screen. A raised edge protects the power button, so it's not easy to press by accident.
4	On the bottom of the phone is the USB charging port on the left, the microphone in the middle, and the charger contacts on the right. • USB charging port—Supports a USB cable to charge the phone. • Microphone—Captures your audio to send. • Charger contacts—Connects with the contacts on a desktop charger to charge the battery.
5	On the left side of the phone are three programmable buttons. By default, the top button is set as the **Scanner** for 860S phones. By default, the middle and bottom buttons are set as **Volume up** and **Volume down** respectively. • **Programmable** button—By default, this programmable button is set as the barcode scanner on the 860S phones. • **Programmable Volume up** button—By default, this programmable button is set to turn up the volume. • **Programmable Volume down** button—By default, this programmable button is set to turn down the volume.

Group number	Hardware or buttons in group
6	On the top back of the phone is the rear camera on the far left, and the rear microphone above the flash lens or torch. In the upper middle of the phone is a **Programmable Fingerprint** scanner button. • Rear camera—Captures images. • Rear microphone—Cancels noise. • Flash lens or torch—Emits light for a camera flash, or torch flashlight. • **Programmable Fingerprint** scanner button—By default, this programmable button is set to act as a fingerprint scanner to unlock the phone.
7	On the lower back of the phone is the rear speaker on the left, the battery latch in the middle lower edge of the battery, and the battery. • Rear speaker—Receives audio you can hear. • Battery latch—Releases and catches the battery in the phone. • Rechargeable battery—Powers the phone.
8	This side view of the 860S highlights the barcode scanner on the top of the phone.

Note If you use an incorrect cable to connect to the phone USB port, third-party accessories such as keyboards or a mouse may not work. When buying these products, look for Benson Approved and OTG cables. Any cables or adapters must be USB certified and built to the USB-C specification.

Note If available, you can reprogram the **Programmable** buttons with the **Buttons** app.

Launcher screen

The launcher screen is the first screen that you see after you turn on or unlock the phone. It differs based on how the administrator customizes the phones, but contains the following general areas:

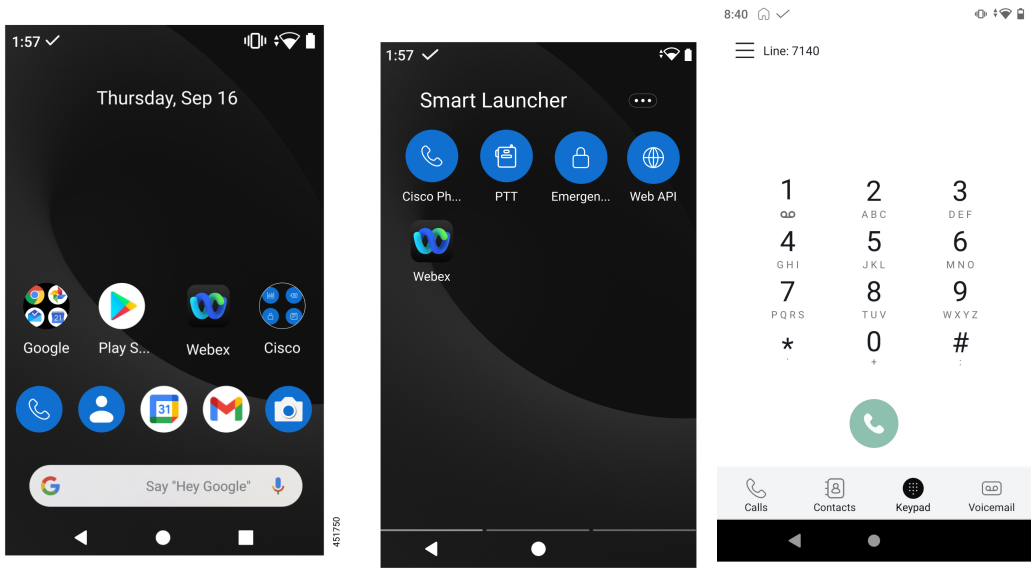
- **Top of the screen**—Contains the status bar, which displays the time and icons that give you information about the status of your phone and notifications.
- **Body of the screen**—Contains the apps and widgets that the administrator installs on the phone. The administrator may use a smart launcher to display a limited number of apps, so what you see can vary from a:
  - Launcher screen with all the factory default apps and widgets such as a phone, web browser, camera, and collection of Android and custom **Cisco** apps.
  - Smart launcher screen with multiple selected apps.

- Smart launcher screen with a single, open app.

- **Bottom of the screen**—Contains navigation controls.

Note The smart launchers in this guide show what you may see if the administrator uses the Cisco Wireless Phone Configuration Management tool to set up your phone. Your phone may not look or act exactly as described in this guide if set up with another tool, such as an Enterprise Mobility Management (EMM) application.

Figure 5: Sample launcher screens: factory default launcher, smart launcher with multiple apps, and smart launcher with a single open app



Cisco apps

These Cisco apps may be available on your phone.

Table 13: Cisco apps

Cisco app	Description
	The **Cisco Phone** app allows you to use full SIP phone call functionality.
	The **Barcode** app allows you to use the barcode scanner on your 800S phone.

Cisco app	Description
	The **Battery Life** app displays the current condition of the battery and allows you to adjust the battery alarm volume.
	The **Buttons** app allows you to program the buttons on your device.
	The **Call Quality Settings** app allows the administrator to optimize audio and video calls from Cisco dialers or other third-party dialers.
	The **Custom Settings** app allows the administrator to provide extra controls for the phone.
	The **Emergency** app allows you to use personal monitoring alarms and emergency calling. Deploy this app in lone worker environments or where you need extra security.
	The **Logging** app allows the administrator to access various debug options on the phone.
	The **PTT** app allows you to use a radio multicast app on your device.
	The **System Updater** app allows you to see the current and available firmware versions for the phone. However, the administrator manages and pushes firmware updates to the phone through the Cisco Unified Communications Manager. .
	The **Web API** app allows developers to interface with external services and provide links to frequently used websites.

Cisco app	Description
	The **Smart Launcher** app allows the administrator to specify which apps to display on the launcher screen.
	The **Device Policy Controller** app allows the administrator to specify which apps aren't allowed on the phone.
	The **Diagnostics** app allows the administrator to perform diagnostics tests quickly and efficiently to verify phone's hardware components.

Care of your phone

Your phone is rugged and made for use in tough environments. It's built out of strong and resilient plastics. All components are durable and reliable.

We've extensively tested the phones and warranty them for normal use under rigorous conditions. The Cisco Wireless Phone 840 has an IP65 rating and the Cisco Wireless Phone 860 has an IP68 rating. However, accidental, or inadvertent exposure to various substances can cause the phone to perform poorly or fail completely.

There are many substances that you can't clean off without damaging the device beyond repair. For instance, if you drop your phone into glue or paint, even if you carefully clean the phone, it may not function properly. Also, oil-based substances, such as make-up or lotion, can leave a sticky residue on the phone that attracts and binds particles. This can jam key components such as the camera, microphone, speaker, or headset jack. We don't cover damage from such conditions under warranty. You can prevent or remedy such damage through careful use and proper care and maintenance.



Warning There are no serviceable parts in the phone, batteries, or chargers. Don't open or disassemble the phone case, battery, or charger. You void your warranty if you disassemble any of these items.



Caution Don't roughly handle the battery contacts when you clean the phone, or you may bend them. If you bend the battery contacts, the phone may not turn on or it may display a battery error.

Maintenance schedule

It's important to clean your phone regularly so that it functions properly. To set an effective maintenance schedule for your phone, consider the following degrees of exposure and types of substances that may be present in your organization.

Table 14: Sample exposure levels

Exposure level	Typical work setting	Potential substances
Light exposure	Normal office settings with desks and chairs and moderately mobile workers.	• Paper and fiber lint. • Light soil, dust, and pet hair and dander • Food residue and spills. • Human residue from coughs, sneezes, makeup, lotion, or hair products.
Medium exposure	Interactive work settings with lots of human contact, such as medical outpatient facilities, restaurants, hotels, light manufacturing, schools, and retail.	• All the substances from the light exposure list, in larger quantities. • Possibly some substances from the heavy exposure list.
Heavy exposure	Highly interactive work with much more human contact and exposure to different types of substances.	• All the substances from the light and medium exposure list. • Manufacturing materials such as metal lint and other particulates, various types of fluids, glues and solutions, and waste products. • In-patient medical exposures include body fluids and waste, medical chemicals, drugs, and various residue from medical processes.

Maintain your phone

To avoid substances building up on your phone, follow these steps to maintain your phone. How frequently you follow these steps depends on your work environment and exposure to various substances.

Warning

- Never bend battery contacts.
- Never submerge your phone into any cleaning solution.
- Never allow a cleaning solution to pool on the phone or in an orifice.
- Never spray any solution directly onto the phone.
- Never mix cleaning agents. The combined effects of cleaning agents are unknown. Mixing chemical agents could seriously degrade the construction of the phone and make it susceptible to damage, even with normal use.
- Never use furniture polishes, waxes, or plasticizer-based cleaners (ArmorAll®, and so on).
- Never use lanolin, aloe, glycerin, or other skin care products.
- Never use hand sanitizers to clean your phone or handle your phone when hands are wet with sanitizer solution.
- Never apply any solvent such as acetone, mineral spirits, and so on
- Don’t exert undue pressure on the battery contacts on the bottom of the phone and inside the battery compartment. Don’t rub, scrub, or use bleach.

Procedure

Step 1 Turn off the phone and remove the clip and battery.

Step 2 Spray canned air into crevices and orifices to blow out any lint or dirt.

Always point canned air at an angle away from your face and eyes.

Warning Always wear safety goggles or glasses.

Never insert any instrument into any orifice including the microphone, earpiece, headphone jack, USB plug, reset pin hole, or battery contacts.

Step 3 Clean surface dirt with soap and water with a damp, lint-free cloth.

You may scrub stubborn spots.

Warning Don't scrub or bend battery contacts.

Don't squeeze water or any liquid into orifices, or a sticky plug can form that blocks the opening. The result may be a significant deterioration in performance.

Step 4 Wipe off soap film with a different clean damp cloth.

Step 5 Dry with yet another clean dry cloth.

Step 6 Wipe battery contacts with a cotton swab dampened with alcohol to remove any lint.

Step 7 Polish the glass screen, photo lenses, flashlight, fingerprint scanner, and barcode reader (if present) with glass cleaner towelettes.

Caution Don't exert too much pressure on the glass screen.

Step 8 Clean the clip and battery separately.

Step 9 When the phone and battery are completely dry, reinstall the battery and replace the clip.

Step 10 Use an approved disinfectant to sanitize the device.

Disinfectants

Products listed here are often used to clean and disinfect in medical environments. They are considered safe when used according to solution strength and manufacturer instructions. New products are introduced constantly and generally have similar ingredients. Always follow the manufacturer guidelines for a cleaning or disinfecting product.

Table 15: Generic liquid products

Product	Solution strength
Hydrogen peroxide	Use a 3% solution
Bleach	Use a 10% solution (Sodium Hypochlorite 0.55%) **Warning** Don't use on metal charging contacts.
Isopropyl alcohol	Up to 91% solution

Here are some brand name products that you can use:

- AZOWIPE™
- Brulin BruTab 6S® Tablets
- Clinell© Universal Wipes
- Clorox© Dispatch Hospital Cleaner Disinfectant Towels with Bleach
- Clorox© Formula 409® Glass and Surface Cleaner
- Clorox© Healthcare Bleach Germicidal Wipes
- Clorox© Healthcare Hydrogen Peroxide Wipes
- Clorox© Healthcare Multi-Surface Quat Alcohol WipesDispatch® Hospital Cleaner with Bleach
- Diversey© D10® Concentrate Detergent Sanitizer

- Diversey© Dimension 256 Neutral Disinfectant Cleaner
- Diversey© Oxivir® Tb Wipes
- Diversey© Virex II® 256 One-Step Disinfectant Cleaner
- Medipal© Alcohol Wipes
- Metrex© CaviCide®
- Metrex© CaviCide1®
- Metrex© CaviWipes™
- Metrex© CaviWipes1®
- Oxivir©
- PDI© Easy Screen® Cleaning Wipe
- PDI© Sani-Cloth AF3® Germicidal Disposable Wipe
- PDI© Sani-Cloth® Bleach Germicidal Disposable Wipe
- PDI© Sani-Cloth® HB Sani-Germicidal Disposable Wipe
- PDI© Sani-Cloth® Plus Germicidal Disposable Cloth
- PDI© Super Sani-Cloth® Germicidal Wipe
- Progressive© Products Wipes Plus
- Sani© Professional Disinfecting Multi-Surface Wipes
- Sani-Hands® Instant Hand Sanitizing Wipes
- SC Johnson© Windex® Original Glass Cleaner with Ammonia-D
- Spartan© Hepacide® Quat II
- Sterets© Alcowipe®
- Steris© Coverage Plus Germicidal Surface Wipes
- Veridien© Viraguard
- Windex© Glass Cleaner

UV disinfection

Ultraviolet (UV) light from the C spectrum has germicidal properties and is used within specially built chambers to disinfect devices. It is best to use UV-C chambers after you clean a device. In a medical environment, germicidal UV-C is employed as an extra safeguard against Healthcare-Associated Infections or Hospital Acquired Infections (HAIs). Although ultraviolet light destroys viruses, bacteria, and spores it can damage plastics.

Labs conducted extensive testing to determine the durability of Cisco Wireless Phone 840 and 860 when exposed to UV-C. The phones were tested against a UV-C chamber, the AUVS KR615, designed for disinfecting mobile devices under hospital disinfection protocols. Commonly known as **The UV Box**, the KR615 was developed and is manufactured by Advanced Ultra-Violet Systems and is available through Safety Net.

Due to its superior plastic enclosure and precision manufacturing, the phones exceeded performance expectations and retained full functionality and integrity throughout the tests. We therefore approve germicidal UV-C for disinfecting Cisco Wireless Phone 840 and 860 when used according to both Cisco and UV-C device manufacturer guidelines. For more information about **The UV Box**, visit Safety Net.

Dry your phone

If your phone is dropped into water or the interior gets wet, you need to take steps to dry your phone.

Warning Use of an oven or dryer on the phone to speed up drying can damage the phone and voids the warranty.

Note If the phone doesn't work after these steps, contact your administrator.

Procedure

Step 1 Immediately power off the phone and remove the battery.

Step 2 Shake excess liquid from the phone.

Step 3 Place the phone and battery in an area that is at room temperature and has good airflow.

Step 4 Let the phone and battery dry for 72 hours before you reconnect the battery and power on the phone.

Related documentation

Use the following sections to obtain related information.

Cisco Wireless Phone 840 and 860 documentation

You can locate publications that are specific to your language, phone model, and call control system from the product support page for the Cisco Wireless Phone.

You can also access the Cisco Wireless Phone 840 and 860 Deployment Guide from the product support page.

Cisco Unified Communications Manager documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release on the product support page.

Cisco IP phone user support

If you are an administrator, you are likely the primary source of information for Cisco IP phone users in your network or company. It is important to provide current and thorough information to end users.

To successfully use some of the features on the Cisco IP phone (including Services and voice message system options), users must receive information from you, or from your network team or must be able to contact you for assistance. Make sure to provide users with the names of people to contact for assistance and with instructions for contacting those people.

We recommend that you create a web page on your internal support site that provides end users with important information about their Cisco IP phones.

Consider including the following types of information on this site:

- User guides for all Cisco IP phone models that you support
- Information on how to access the Cisco Unified Communications Self Care Portal
- List of features supported
- User guide or quick reference for your voicemail system

Configuration and deployment workflow

Cisco Unified Communications Manager (Unified Communications Manager) provides call services through the Cisco Phone app. There are options to set up and manage these phones:

- We recommend that you use an Enterprise Mobility Management (EMM) application, such as Cisco Meraki Systems Manager, to manage the devices and Cisco apps.
- If you don't have an EMM application, we recommend that you use the Cisco Wireless Phone Configuration Management tool to set up phones with release 1.5(0) or later.
- If you don’t use an EMM application or the Cisco Wireless Phone Configuration Management tool, you can manage the devices and apps individually on each phone. However, we don't recommend this method for deployments of more than a few phones.

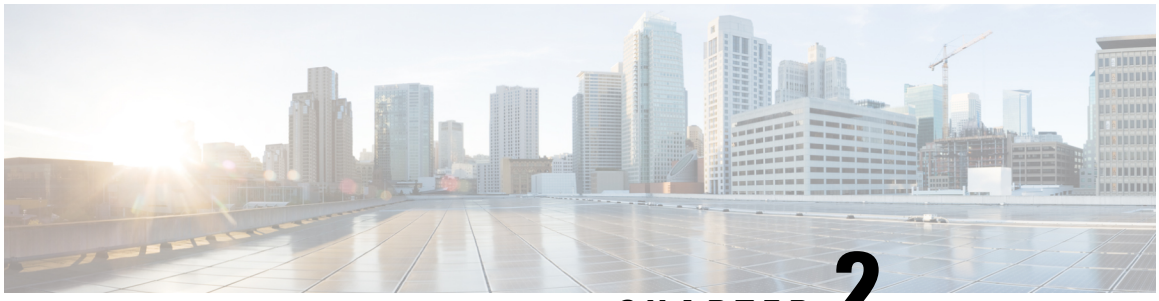
We also recommend using an EMM application or the Cisco Wireless Phone Configuration Management tool and a Quick Response (QR) code to program the phones to connect to a WPA2 PSK WLAN and, if applicable, the EMM application. Alternately, you can use a Google Wizard to manually configure the network Service Set Identifier (SSID) settings.

Procedure

	Command or Action	Purpose
Step 1	Configure the network.	See Network requirements, on page 31.
Step 2	Configure Unified Communications Manager to initialize devices.	• You can manually program Unified Communications Manager for a few devices.

	Command or Action	Purpose
		• You can also use a bulk programming method to replace several of these steps to provision many devices at once. See Cisco Unified Communications Manager phone configuration, on page 45.
Step 3	Fully charge the phones.	Use a USB, desktop charger, or multicharger to fully charge the phone. See Phone battery charging, on page 41, Desktop chargers, on page 167, or Multichargers, on page 171.
Step 4	Choose one of the following: • (Recommended, especially if you need third-party apps) Configure an EMM application console and generate a QR code to program the phones to connect to a WPA2 PSK WLAN and EMM application. • (Recommended, if you don't have an EMM application) Configure the Cisco Wireless Phone Configuration Management tool and generate a QR code to program the phones to connect to a WPA2 PSK WLAN. • (Recommended only for small deployments) If not using an EMM application or Cisco Wireless Phone Configuration Management tool, manually configure the SSID settings to program the phones to connect to the wireless network.	See Phone configuration, on page 71 and Cisco app configuration, on page 87.
Step 5	Phones contact Unified Communications Manager and, if used, the EMM application, or configuration file created in the Cisco Wireless Phone Configuration Management tool: • Each phone uses DHCP option 150 or 66 to locate its HTTP (Alt TFTP) servers. Using its Unified Communications Manager device name (based on its MAC address) the phone downloads its configuration file in the Unified Communications Manager. • Each phone connects to the WLAN. • (Optional) Each phone enrolls with the EMM application. The EMM application	See Phone configuration, on page 71 and Cisco app configuration, on page 87.

	Command or Action	Purpose
	provides the phone apps, certificates, and configuration for all non-Unified Communications Manager related functionality.	
Step 6	The phone is fully functional and downloads software updates from the server, which is administered through the Unified Communications Manager. If used, the EMM application provides app updates.	See Phone configuration, on page 71 and Cisco app configuration, on page 87.



CHAPTER 2

Initial setup

- Network requirements, on page 31
- Cisco Unified Communications Manager requirements, on page 32
- Phone battery installation, on page 35
- Battery contact damage prevention, on page 40
- Phone battery charging, on page 41

Network requirements

Network requirements for the Cisco Wireless Phone 840 and 860 include:

- Cisco Unified Communications Manager (Unified Communications Manager):
  - Minimum: 11.5(1)
  - Recommended: 12.5(1) or later
- Supported Wi-Fi access point.

  For supported access point options, see the Cisco Wireless Phone 840 and 860 Deployment Guide.

For Unified Communications Manager registration, the phone must be able to use either ICMP or TCP port 7 to check whether the TFTP node is reachable. It sends ICMP packets first. If ICMP is blocked, it tries TCP port 7. If both are blocked, the phone does not attempt to connect on TCP port 6970.

The phone uses DHCP Option 150 or 66 for Unified Communications Manager server configuration. If the network doesn't provide DHCP Option 150 or 66, or is pointing to the incorrect Unified Communications Manager server, then you must manually configure the servers in the Cisco Phone app.

Hosts on the network use DHCP to obtain initial configuration information, including IP address, subnet mask, default gateway, and HTTP server address. DHCP eases the administrative burden of manually configuring each host with an IP address and other configuration information. DHCP also provides automatic reconfiguration of network configuration when devices are moved between subnets. The configuration information is provided by a DHCP server that is located in the network, which responds to DHCP requests from DHCP-capable clients. Although the server is referred to as an HTTP server in this document, the actual communications protocol that is used is HTTP or HTTPS.

To simplify deployment of these devices, configure the phones to use DHCP. Use any Request for Comments (RFC) 2131 compliant DHCP server to provide configuration information to the phones.

Configure the phones to rely on DHCP Option 150 or 66 to identify the source of telephony configuration information, available from a Unified Communications Manager HTTP server. Option 150 or 66 should contain a single IP address in a system with one Unified Communications Manager HTTP server or two IP addresses for deployments where there are two HTTP servers within the same cluster.

The phone uses the second address if it fails to contact the primary HTTP server, thus providing redundancy. To achieve both redundancy and load sharing between the HTTP servers, you can configure Option 150 or 66 to provide the two HTTP server addresses in reverse order for half of the DHCP scopes.

The phone requires using a direct IP address (that is, not relying on a Domain Name System (DNS) service) for Option 150 or 66 because doing so eliminates dependencies on DNS service availability during the phone boot and registration process.

Note From release 1.3(0) and later, you can enable Call Admission Control (CAC) and Traffic Specification (TSPEC) for call control and voice on the WLAN Controller or Access Point. See the Cisco Wireless Phone 840 and 860 Deployment Guide for more information.

Note By default, the Cisco Wireless Phones send a Network Time Protocol (NTP) request to a server on the internet to get the date and time, or to the internal NTP server that you set in the **Custom Settings** app.

From release 1.5(0) and later, you can define a server in DHCP option 42 to provide an alternate NTP service in case the NTP server isn't available. If the NTP server isn't available, for example there's no internet, the phones get their time source from the server that you define in DHCP option 42.

Related Topics

More Custom Settings, on page 139

Cisco Wireless Phone 840 and 860 deployment guide

The Cisco Wireless Phone 840 and 860 Deployment Guide contains useful information about the wireless phone in the Wi-Fi environment.

Cisco Unified Communications Manager requirements

Cisco Unified Communications Manager (Unified Communications Manager) requirements for the Cisco Wireless Phone 840 and 860 include:

- Unified Communications Manager 11.5, 12.5, 14.0, or later
- Installation of both of these Cisco Options Package (COP) files on Unified Communications Manager:
  - Device enabler QED installer—Enables Cisco Wireless Phone 840 and 860 in Unified Communications Manager.
  - Phone software—Updates software for all Cisco apps.

Note If you want to use the Cisco Wireless Phone Configuration Management tool to configure your phones, install release 1.5(0) files or later.

Device enabler QED installer file

The Cisco Unified Communications Manager (Unified Communications Manager) device enabler QED installer Cisco Options Package (COP) file contains configuration files that register the phone and enable features on the phone. Install the latest device enabler QED installer COP file on the Unified Communications Manager so that the Cisco Wireless Phone 840 and 860 can register to the Unified Communications Manager and access the phone features. New features may be turned off by default and they have attributes or settings that you must configure.

Phone software file

The factory installs a version of the phone software on the phone during manufacturing. But that software may not be the latest version.

Your Cisco Unified Communications Manager stores the software loads. If the version of software on the phone isn't the latest version, the Cisco Unified Communications Manager sends the updated software load to the phone.

Caution You can't downgrade the phone software to an earlier version. The lowest phone software version that you can have on the phone is the factory installed version. However, when you upgrade the phone software, that version becomes the lowest possible software version. Even if you perform a factory reset, the phone software stays on the latest installed version.

Phone configuration files

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

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

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

Load the COP files to Cisco Unified Communications Manager

You must install the Cisco Wireless Phone 840 and 860 device enabler QED installer and phone software Cisco Options Package (COP) files into each Cisco Unified Communications Manager (Unified Communications Manager) in the cluster.

Note These COP files are signed with the sha512 checksum. Cisco Unified Communications Manager versions before version 14 don't automatically include support for sha512.

For the first installation, install the device enabler QED installer file first and then the software file.

For future software updates, there is not always a corresponding device enabler QED installer update. When a software update is available, check the latest version of the device enabler QED installer file to see whether you also must update it.

Note With each new software release, the Cisco apps are also updated in the Play Store. However, if you manage the phones through an Enterprise Mobility Management (EMM) application, we recommend that you update the firmware on the phones to minimize any risk of app incompatibility.

Before you begin

- Download the device enabler QED installer and phone software COP files from the Software Download site.

Note If you want to use the Cisco Wireless Phone Configuration Management tool to configure your phones, install release 1.5(0) files or later.

- If you have Unified Communications Manager version 11.5 or 12.5 and don't already have sha512 checksum support enabled, install ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn.

Caution Choose an appropriate time to perform this task. As part of this task you must restart each Unified Communications Manager in the cluster after you install a device enabler QED installer COP file, unless your version of Unified Communications Manager offers an alternate process that does not require a reboot.

See the *Manage Device Firmware* section of the *Administration Guide for Cisco Unified Communications Manager* for your Unified Communications Manager version, to see if it allows an installation process that does not require a reboot.

Procedure

Step 1 In each Unified Communications Manager in the cluster, select **Cisco Unified OS Administration** > **Software Upgrades** > **Install/Upgrade**.

Step 2 Enter the Software Location data.

Step 3 Click **Next**.

Step 4 Select the COP (.cop.sha512) file.



Note If the COP file doesn't appear in the available files list, ensure that you enable sha512 checksum support.

Step 5 Click **Next** to download the COP file to Unified Communications Manager.

Step 6 Check that the file checksum details are correct.

Step 7 Click **Next** to install the COP file on Unified Communications Manager.

Step 8 Click **Install Another** and repeat steps 2–7 to install another COP file.

Step 9 Perform the following actions based on the COP files that you installed.

a) If you installed a device enabler QED installer COP file:

- **For 11.5(1)SU4 and earlier**:
  - Reboot all Unified Communications Manager nodes through **Cisco Unified OS Administration** > **Settings** > **Version** > **Restart**.
- **For 11.5(1)SU5 and later or 12.5(1) and later**:
  - Restart the Cisco Tomcat service on all Unified Communications Manager nodes.
  - If running the Unified Communications Manager service on the publisher node, restart the service on the publisher node only. You do not need to restart the Cisco Call Manager Service on subscriber nodes.

b) If you installed a software COP file, restart the Cisco TFTP service for all nodes running the Cisco TFTP service.

Phone battery installation

You must read the information in the Product Safety and Security chapter of the User Guide, before you install or charge the battery, or use the phone.

Before you can use your phone, you must install and charge the battery. The battery may already be installed in your phone, or you may have to install it yourself.

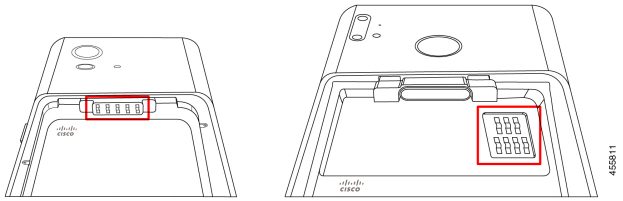
To maximize the battery storage capacity and lifespan, fully charge the battery before you turn on and set up the phone.

Install the battery

Don't install the battery in a dusty or wet environment.

The steps to install the battery are the same for both the Cisco Wireless Phone 840 and Cisco Wireless Phone 860. However, the battery contacts are in different locations on these models, as shown in the following illustration. The illustrations in the steps are of the Cisco Wireless Phone 860.

Figure 6: Battery contact location on the Cisco Wireless Phone 840 and Cisco Wireless Phone 860

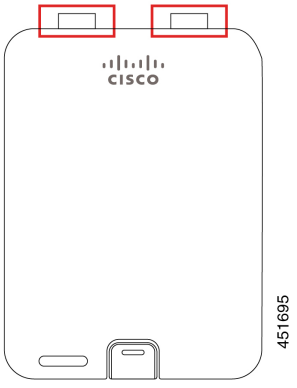


Warning Take care not to damage the battery contacts within the handset when you remove the battery from the handset. Take special care not to touch, compress, or come into contact with the battery contacts in any way or damage may occur.

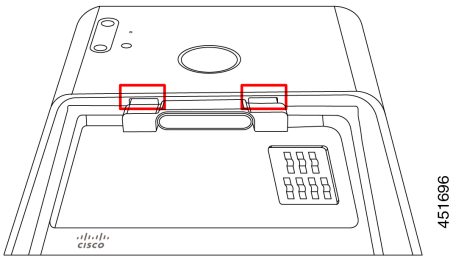
Warning Use only the Cisco-branded batteries for this phone. If you attempt to use a third-party battery, you will receive an error and the battery will not work. We don't support damage from attempting to use third-party batteries.

Procedure

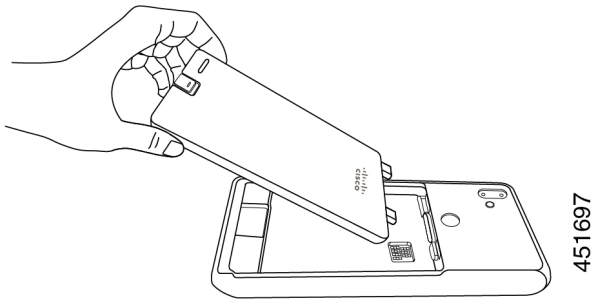
Step 1 Locate the two battery tabs on the top edge of the battery.



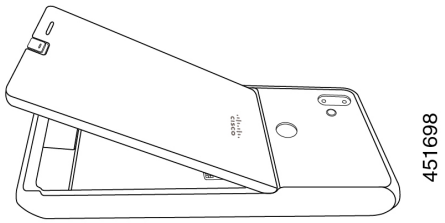
Step 2 Locate the two slots in the wall at the top of the phone battery compartment.



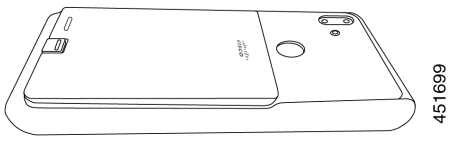
Step 3 Position the battery at an angle approximately 45–60 degrees to the phone battery compartment. Point the battery edge with the two plastic tabs toward the two slots in the battery compartment.



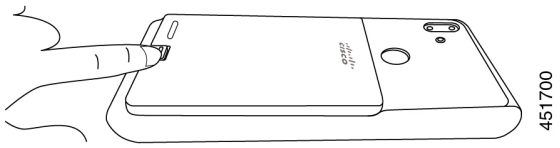
Step 4 Insert the two plastic battery tabs directly into the two battery compartment slots.



Step 5 Use the tab and slot contact point as a pivot to lower the battery into the compartment.



Step 6 Use your finger to press down until you feel and hear the battery clip snap into place.



Related Topics

Phone battery charging, on page 41

Remove the battery

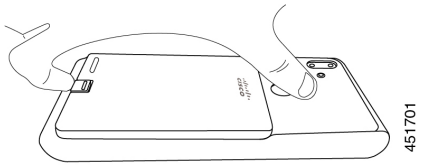
Battery removal follows a reversed but similar procedure to battery insertion.

The steps to remove the battery are the same for both the Cisco Wireless Phone 860 and Cisco Wireless Phone 840. However, the battery contacts are in different locations on these models. The illustrations in the following steps are of the Cisco Wireless Phone 860.

Procedure

Step 1 To disengage the battery clip, gently use a fingernail to depress the clip towards the top of the phone.

Caution Don’t pull up on or twist the clip. Don't use a tool, such as letter opener or screwdriver, to pry the clip open. An incorrect prying action with a tool can break the battery clip.

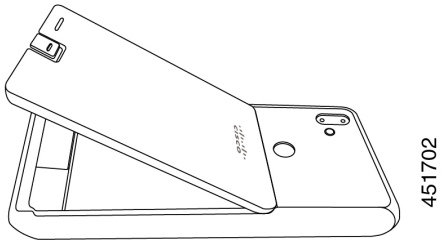


Step 2 Use your fingernail to lift the battery gently about an eighth of an inch (a few millimeters) out of the battery compartment.

Step 3 Release the battery clip and grab the battery with your fingers.

Step 4 Use the battery tabs and battery compartment slots as a pivot point to raise the battery edge out the battery compartment.

Warning Don’t slide the battery across the battery compartment because this action may damage the contacts.



Step 5 Gently withdraw the battery tabs from the battery compartment slots and lift the battery out of the battery compartment.

Warning Make sure that no part of the battery drags across the battery contacts in the phone.

Hot swap the battery for Cisco Wireless Phone 860 and 860S

The Cisco Wireless Phone 860 and 860S have a hot swap feature that allows you to continue to use your phone while you change a low battery. During a hot swap, the internal phone battery provides minimum power to allow the phone to remain on.

You can perform a battery hot swap under most normal operations, such as during a voice call or other activity on an active phone screen. Active use of the phone or anything that increases the power draw during a hot swap may, in rare situations, cause the phone to power off.

Caution If the new battery that you use during the hot swap doesn't have a proper charge, a low battery alert displays and the phone shuts down.

If the internal phone battery isn't awake and charged, the battery hot swap may fail. If the phone was in sleep mode or if you just turned on the phone, the internal battery may not be awake and charged.

Note The Cisco Wireless Phone 840 and 840S don't have an internal battery, so they don't support the hot swap feature.

Before you begin

- Make sure that the new battery that you use during the hot swap has a proper charge.
- If the phone was in sleep mode or if you just turned on the phone, wake and charge the internal battery:
  1. Choose one of the following:
     - If the phone screen was in sleep mode, unlock the phone and wait for 30 seconds.
     - If you just turned on the phone, unlock the phone and wait for 3-5 minutes.
  2. Briefly press the **Power** button to turn off the phone screen and wait for 3-5 seconds.

Procedure

Step 1 Remove the battery.

Step 2 Within 60 seconds, install the new battery.

Related Topics

Install the battery, on page 36
Remove the battery, on page 38

Battery contact damage prevention

If you slide or drag part of the battery over the battery contacts during insertion or removal, it may damage the battery contacts.

Damaged battery contacts that can't make proper contact with the contacts in the phone, may cause issues such as:

- The phone won’t power on.
- The phone shuts down randomly.
- The phone displays an **Invalid Battery Shutdown** message before it shuts down.

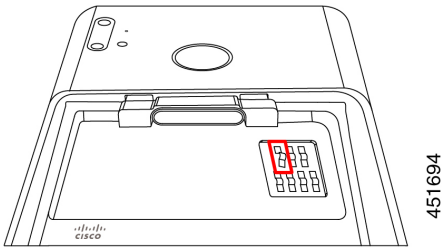
In these failure scenarios, remove the battery from the phone and examine the battery contact fingers and pads.

Note The battery contacts are in different locations on the Cisco Wireless Phone 840 and Cisco Wireless Phone 860.

- Check that the contacts aren’t dirty or covered with any substances, or it may prevent a proper electrical connection.
- Check that the contact fingers on the phone are straight relative to the contact base, with all fingers at the same height.

In the following image of the Cisco Wireless Phone 860 battery compartment, the finger on the top left illustrates damage from incorrect battery insertion.

Figure 7: Cisco Wireless Phone 860 battery contact damage



Phone battery charging

Warning Explosion hazard: Don’t charge the phone battery in a potentially explosive atmosphere. Statement 431

You can charge the battery using any of the following options:

- USB cable—You can charge the phone with an Cisco Unified Communications Manager Attendant Console power adapter or your computer.
- Desktop chargers—You can charge a phone and spare battery.
- Multicharger—You can charge several phones or batteries at the same time.

The length of time to charge a phone and battery varies depending on the charge method.

- It takes about 3 hours to charge a phone using the USB cable and AC plug.
- It takes about 8 hours to charge a phone using the USB cable and your computer.
- Under normal conditions, a discharged battery charges fully in approximately 3 hours in a desktop or multicharger.
- If both a phone and battery are in a desktop charger, the phone takes priority. So it takes longer to charge the battery.

The table shows the charging time for each phone model:

Phone Model	Configuration	Charging
840/840S	Phone with battery	3.5 hrs
840/840S	Standalone battery	3.5 hrs
860/860S	Phone with battery	3.5 hrs
	Standalone battery	3.5 hrs

Note Charge your phone batteries in an ambient temperature of 50–86°F (10–30°C) for the best results. If you charge the batteries outside of this temperature range, it results in longer charge times or incomplete charge cycles.

Store the batteries in dry conditions at approximately 65° F (20° C).

Caution Don’t let the main battery or the internal battery of your Cisco Wireless Phone 860 or 860S fully deplete for extended periods. If you must store the phone or battery for longer than one month, then we recommend that you fully charge the battery installed in the phone to 100% every six months. Never store a phone without the main battery for longer than one month.

Note Severely damaged battery contact pins are not repairable and not covered under the Cisco warranty. Minor deformation may be remediated by carefully bending the battery contact pins back to the correct position using appropriate tools. Cisco is not responsible for any damage that is caused during this action.

Related Topics

Charge the battery with the AC power supply, on page 42
Charge the battery with the USB cable and a USB port on your computer, on page 42
Desktop chargers, on page 167
Multichargers, on page 171

Charge the battery with the AC power supply

If you don't have a desktop charger or multicharger, you can charge your phone battery using the USB cable and AC power adapter.

Caution Use only the approved USB cable and power adapter for the Cisco Wireless Phone 840 and 860.

Procedure

Step 1 Plug the USB cable into the bottom of the phone with the pins aligned.

Step 2 Plug the USB cable into the power adapter.

Step 3 Plug the power adapter into the electrical outlet.

Charge the battery with the USB cable and a USB port on your computer

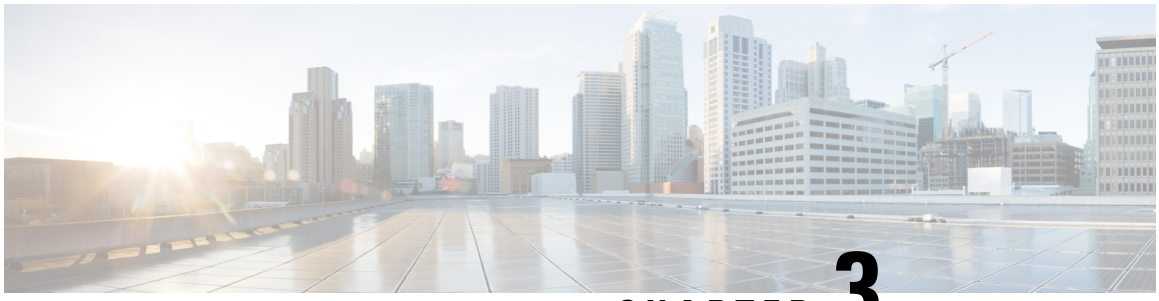
If you don't have a desktop charger, multicharger, or USB cable and AC power adapter, you can charge your phone with a USB cable and computer. However, this method takes more time to charge your phone than the other methods.

Caution Use only the approved USB cable for the Cisco Wireless Phone 840 and 860.

Procedure

Step 1 Plug the USB cable into the bottom of the phone with the pins aligned.

Step 2 Plug the USB cable into a USB port on a computer.



CHAPTER 3

Cisco Unified Communications Manager phone configuration

- Determine the MAC address of the phone, on page 45
- Install manufacturing CA certificates, on page 45
- Before you register wireless phones, on page 46
- Manual phone registration, on page 50
- Phone feature configuration, on page 55

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 16: 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.
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.

Field name	Field type or choices	Default	Description
Advertise G.722 and Opus Codecs	Use System Default Disabled Enabled	Use System Default	Indicates whether the phone advertises the G.722 and Opus codecs to the Cisco Unified Communications Manager (Unified Communications Manager). • 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. **Note** Codec negotiation involves two steps: 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			This parameter contains the address of the server for the optional second registration. **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.
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.

Field name	Field type or choices	Default	Description
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. • 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. • 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, on page 183

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:

a) On the Cisco Unity Connection server, navigate to **Cisco Unified OS Administration**.
b) Navigate to **Security** > **Certificate Management**.
c) Select the certificate labeled **tomcat-trust**.
d) Choose to download the .pem file.

Step 2 Import the certificate to each Cisco Unified Communications Manager in the cluster.

a) On the Cisco Unified Communications Manager server, navigate to **Cisco Unified OS Administration**.
b) Navigate to **Security** > **Certificate Management**.
c) Click **Upload Certificate/Certificate Chain**.
d) From the **Certificate Purpose** drop-down list, choose **tomcat-trust**.
e) Enter a **Description** for the certificate, such as **tomcat-trust**.
f) Click **Browse** to search for, and select, the certificate.
g) 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, on page 189

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.

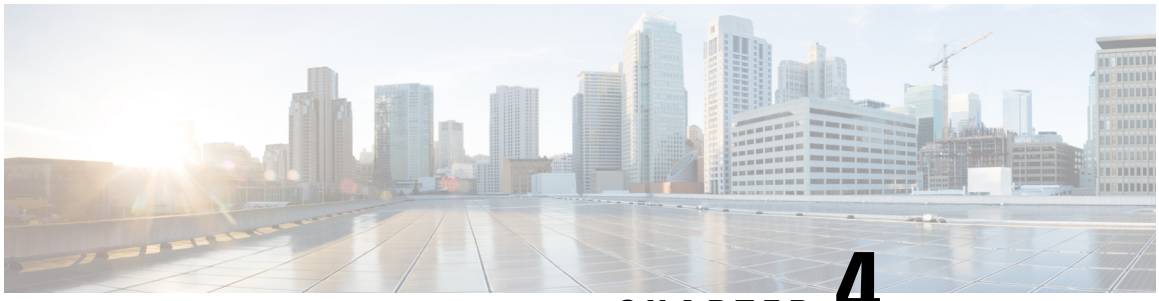
Step 5 In the Permission Information section, ensure that the Groups list includes **Standard CCM End Users**.

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.



CHAPTER 4

Phone configuration

- Enterprise Mobility Management application configuration, on page 71
- Cisco Wireless Phone Configuration Management tool , on page 72
- Manual phone configuration, on page 81

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.

Note Initial provisioning via a downloaded QR code is only supported in the light mode of the browser. If the browser is set to the dark mode, the phone may fail to detect the QR code border, preventing the scan from initiating.

Related Topics

Cisco app package names, on page 113

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 With firmware release 2.1(0) for Cisco Wireless Phone 860, the Android OS is upgraded from version 10 to 13. Since Android 13 manages permissions differently, Cisco application permissions must be granted for the CP-860 software to function properly. For more information, see Android 13 App Permissions, on page 199.

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.

Note The Cisco Wireless Phone 840 and 860 must be in range of the configured Wi-Fi network, otherwise setup will fail.

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, on page 49.
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, on page 34.

	Command or Action	Purpose
Step 4	Factory reset the phones.	See Reset to factory default through the phone settings, on page 182.
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 76.
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 79.
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 74.
Step 8	Enroll the phones with the QR code.	See Enroll phones with Cisco Wireless Phone Configuration Management tool QR code, on page 75.
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 80.

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.

Note Initial provisioning via a downloaded QR code is only supported in the light mode of the browser. If the browser is set to the dark mode, the phone may fail to detect the QR code border, preventing the scan from initiating.

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, on page 182
Generate a QR code to initialize phones, on page 74
Create encrypted phone configuration file, on page 76

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 disallowed:

- **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, on page 87.

- **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, on page 113
Preinstalled Android apps, on page 78
Update existing configuration file, on page 80
Product Specific Configuration Layout fields, on page 57
Cisco Wireless Phone Configuration Management tool for Cisco app configuration, on page 90

Preinstalled Android apps

You can set these preinstalled Android apps to be either allowed or disallowed on the phones though 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 17: 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

Default disallowed Android apps	App package name
YouTube	com.google.android.youtube

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

Table 18: More preinstalled apps

Preinstalled app	App package name
Calculator	com.google.android.calculator
Calendar	ccom.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, on page 57

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 76
Upload the phone configuration file to Cisco Unified Communications Manager, on page 79

Smart Launcher usage tips

Pay attention to the following when working with the Smart Launcher:

- In Smart Launcher, the phone has only four Quick Settings: **Display brightness**, **Flashlight**, **Volume controls**, and **Exit Launcher**. You can access the Quick Settings from the notification shade in the single-app mode, or in the **Overflow** menu in the multiple-app mode.

  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.

- You cannot capture a screenshot while the Smart Launcher is activated.
- On Cisco Wireless Phone 840 and 860, applications launched via Smart Launcher continue to run in the background. Currently, there is no direct method to terminate these background applications while Smart Launcher is active. This is because the recent apps navigation button is removed. Long pressing on an application icon to force stop the application or manage notifications or permissions is not allowed. To terminate the applications, refer to Exit and reenter the Smart Launcher on the phone and exit the Smart Launcher first.
- When Smart Launcher is activated, app notifications are not displayed while the screen is locked (display off / sleep state). Notifications do not trigger an automatic screen wake; they are displayed only after the screen is manually turned on.
- When Smart Launcher is inactive, the screen wakes automatically upon receiving app notifications.
- The administrator setting of **Lock screen display** > **Always ON for clock and notification icons / New notifications** becomes disabled while the Smart Launcher is activated.

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**.

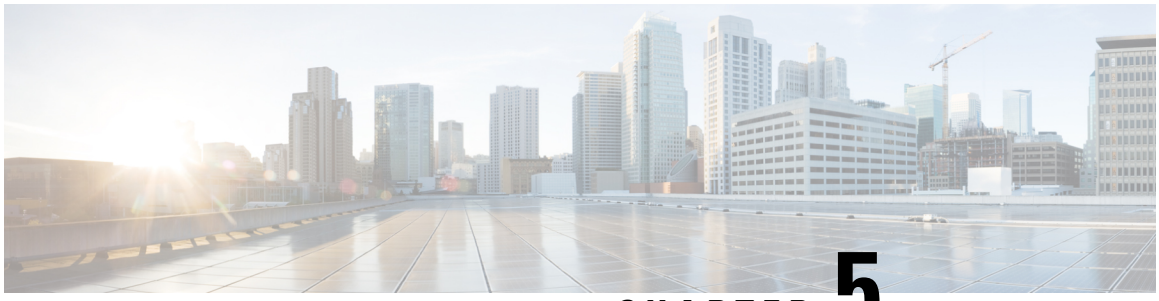
Step 4 Enter the **Local Phone Unlock Password**.

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.



CHAPTER 5

Cisco app configuration

- Cisco app configuration overview, on page 87
- Emergency app, on page 91
- Push to Talk app, on page 98
- Battery Life app, on page 100
- Buttons app, on page 102
- Barcode app, on page 114
- Custom Settings app, on page 133
- Call Quality Settings app, on page 148
- Diagnostics app, on page 154
- Sound Stage app, on page 155
- Web API app, on page 158

Cisco app configuration overview

Configure the Cisco apps and their settings as required by your organization. To configure the Cisco apps, you can:

- Use an Enterprise Mobility Management (EMM) application (Recommended for multiple phones)
- Use the Cisco Wireless Phone Configuration Management tool (Recommended for multiple phones if you don't have an EMM application)
- Use the **Settings** menu for each app directly on the phone (Recommended only for a small number of phones)

Enterprise Mobility Management application interface

The following Cisco apps are on the Google Play Store. You can configure these apps through an Enterprise Mobility Management (EMM) application.

- Emergency
- Push to Talk (PTT)
- Battery Life
- Buttons

- Barcode
- Custom Settings
- Call Quality Settings
- Web API

Note The Barcode, Buttons, Call Quality Settings, and Custom Settings apps are OEMConfig apps. To configure these apps, your EMM must support the OEMConfig enhanced schema. If necessary, consult with your EMM support for assistance.

Program the Enterprise Mobility Management application

The Cisco Wireless Phone 840 and 860 is designed for environments that deploy mobile devices using an Enterprise Mobility Management (EMM) application solution such as Cisco Meraki Systems Manager. Your EMM application allows you to group devices so that you can manage them independently.

For specific directions on how to use Cisco Meraki Systems Manager to group phones, see the technical documentation.

Before you begin

- Configure your EMM application with your domain certificate.
- Link the phones to an existing or new Android for Work account to manage access to apps in the Google Play Store, including Cisco apps.

Procedure

Step 1 Sign in to the EMM application.

Step 2 Set up an Android for Work account, which allows you to sequester the phones from external access and provide only those apps which your organization requires.

Step 3 Create a configuration profile that contains payloads for each configuration area required.

Note We recommend that you set the following minimal settings.

- **Restrictions**: Enable use of the camera and allow app installation.
- **Android Restrictions**:
  - **System settings**: Prevent Android Debug Bridge (ADB) access.
  - **System settings**: Prevent installation of apps from unknown sources.
  - **Permissions**: Auto grant all permissions. For more information on how Android 13 manages Cisco application permissions differently compared to Android 10, see Android 13 App Permissions, on page 199.
- **Android System Apps**: Specify the allowed list of Cisco apps that you download to the EMM application from Google Play Store.
- **Android Wallpaper**: If needed, lock screen message.
- **Wi-Fi Profile**: Configure Wi-Fi settings.

Step 4 Add an Android Enterprise Owner Account to identify the administrator who manages the phone profile.

Note Ensure that the account isn't a local EMM application account, but an Android Enterprise Owner Account.

Step 5 Create identifying tags so that you can separate phones into corresponding groups.

Note Set groups and tags as a payload under the Profiles console. Set the Device Configuration option as Targets. However, at this point, the device only knows that it's a certain model with a certain serial number and MAC address. After enrollment, you can assign device tags with more granularity. You can group devices by specific owners, keywords, or device types, depending on the desired groupings.

Step 6 Use the full name of the Cisco app (com.cisco.xxxx) to download the desired Cisco apps from the Google Play Store.

Note The app and the settings download to the Profile console. Each app is automatically added to the list and the app settings added as payloads.

Step 7 Configure the Cisco apps with the key-value pairs.

Note The key-value pairs should have downloaded with the app. Check the key-value pairs to be sure of accuracy and configure any settings. If any key-value pairs don't download, manually add them.

Step 8 In the EMM application console, approve the apps for distribution.

Step 9 Configure the Android Kiosk Mode to include the apps that you want.

Note Kiosk Mode is a launcher for the phone UI. Only approved apps are available to select for the opening screen.

Related Topics

Cisco app package names, on page 113

Cisco Wireless Phone Configuration Management tool for Cisco app configuration

If you are not using an Enterprise Mobility Management (EMM) application to configure the Cisco app settings, you can configure the settings for each of these Cisco apps in the Cisco Wireless Phone Configuration Management tool.

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

The settings and defaults for these apps in the Cisco Wireless Phone Configuration Management tool are the same as they are on the phones.

Note We recommend that you disallow the **Allow Notification Shade Settings Gear** in the Custom Settings app in Cisco Wireless Phone Configuration Management tool. Otherwise, users can easily open apps that aren't on the Smart Launcher.

Related Topics

Create encrypted phone configuration file, on page 76

Access the Cisco app settings on the phone

If you are not using an Enterprise Mobility Management (EMM) application or the Cisco Wireless Phone Configuration Management tool to configure the Cisco app settings, you can access the settings for each Cisco app on the phone.

Procedure

Step 1 From the phone, tap the desired Cisco app.

The **Buttons**, **Call Quality Settings**, **Custom Settings**, and **Web API** apps open directly to their settings page.

Step 2 For the **Barcode**, **Battery Life**, **Emergency**, and **PTT** apps, tap the **Overflow** ⋮ menu.

Step 3 Tap **Settings**.

Emergency app

The **Emergency** app and **Panic Button** include features to monitor and alarm for emergency situations. These features are useful in lone worker environments or where organizations require extra security. How you program these features depends on what type of situation you anticipate.

- The **Emergency** app uses an accelerometer to monitor the personal motion of the phone user. If configured, the app can alarm or send emergency calls to indicate that the user is under some type of physical duress due to lack of movement, tilt, or shaking of the phone. You can configure each type of motion monitoring with varying degrees of sensitivity and amount of time to activate the warning.
- The **Panic Button** produces a loud or silent alarm and, if programmed, instantaneously calls a preprogrammed emergency number. By default, the red button on the top of the phone is set as the **Panic Button**. There is also a soft **Panic Button** in the **Emergency** app.



Note If enabled, users may change the button actions with the **Buttons** app. If desired, you can disable a user's ability to change the default **Panic Button** in the **Buttons** app.

Caution The reliability of the **Emergency** app and **Panic Button** depends on the functionality and reliability of your organization's infrastructure. The infrastructure includes the wireless LAN, the LAN, the call server, the central provisioning server, the server hosting location services, the central security system and its servers, the correct configuration of the handsets, correct installation and configuration management server, and thorough training of personnel.

We assume no responsibility and shall not be liable for any of the above dependency factors. In addition, please be aware that the **Panic Button** and **Emergency** app should not be your sole solution to any of your safety concerns and are not a substitute for safe practices and procedures.

Emergency app configuration

You can configure the following **Emergency** app settings.

- Motion sensor
- Panic button
- Emergency call
- Emergency tone

Send emergency event notifications

If your system interfaces with a third-party security application, you can also send an emergency event notification when the alarm state triggers and cancels.

Note To identify the location of an alerting phone, the **Emergency** app must use the **Web API** app to interface with a method to locate the phone. Typically, they use a type of location services that use the SSID and AP location to identify the phone's location.

Both a trigger event and a cancel event for an Emergency or Panic Button alarm send a notification to the URL.

Procedure

Step 1 From the Web API settings, choose **Device event notifications** > **Add new notification URL**.

Step 2 Enter a descriptive notification name and URL of the security application.

Step 3 Check the box beside **Emergency events** as the type of event you are sending to this URL.

Motion sensor

When an Emergency motion alarm is triggered, the phone displays a warning screen for a configurable number of seconds. If the user does not cancel the warning, the alarm state occurs and, if configured, the phone places an emergency call.

The motion detectors function accurately only when the phone is secured to the body. The user is not able to turn off the Emergency application without turning off the phone. Configure the Snooze option to allow temporary suspension of Emergency monitoring. Emergency monitoring is also suspended when the phone is connected to the USB charger.

The three conditions of motion are:

- **No movement**—the phone remains still for a configurable number of seconds, potentially indicating that the user is not moving. A certain amount of motion is normal, even when sitting, but no motion at all can indicate that a person is unable to move due to unconsciousness or being restrained.
- **Tilt**—the phone is not vertical for a configurable number of seconds, indicating that the user has fallen or is in some other position than sitting, standing, or walking. The tilt condition may indicate that the user is leaning over to pick up something.
- **Running**—the phone detects shaking, which may indicate that the user is moving quickly or suffering a seizure.

Based on your organization's needs and environmental conditions, you can configure all phones with the same settings, or you can configure the phones in groups or individually.

The user has no control over these settings, so you must configure the settings to provide the most secure response without annoying the user with excessive warnings.

Motion sensor settings

Use the following settings to configure the motion sensor.

Table 19: Motion sensor settings

Field	Field type or choices	Default	Description
Monitoring	On Off	Off	Enables Emergency motion monitoring. Enable this setting to allow any of the motion settings to trigger an alarm.
No movement sensitivity	Disabled Level 1 (lowest) Level 2 Level 2 Level 2 Level 2 Level 2 Level 7 (highest)	Disabled	Sets the degree of motionlessness or lack of any type of movement of the phone to trigger an alarm. Level 1 is the least sensitive. An alarm triggers a warning if the user is moving some, but below the normal threshold. Level 7 is the most sensitive. An alarm triggers if the user is almost completely still.

Field	Field type or choices	Default	Description
No movement timeout (seconds)	Integer 10–300	30	Sets the length of time in seconds that the user would have to maintain the configured degree of stillness (or a more severe degree).
Tilt sensitivity	Disabled Level 1 (lowest) Level 2 Level 2 Level 2 Level 2 Level 2 Level 7 (highest)	Disabled	Sets the nonvertical position of the phone that is required to trigger an alarm. Level 1 is the least sensitive. An alarm triggers if the user is nearly prone. Level 7 is the most sensitive. An alarm triggers if the user was leaning somewhat.
Tilt timeout (seconds)	Integer 10–300	10	Sets the length of time in seconds that the user would have to maintain the configured degree of tilt (or a more severe degree).
Running sensitivity	Disabled Level 1 (lowest) Level 2 Level 2 Level 2 Level 2 Level 2 Level 7 (highest)	Disabled	Sets the amount of shaking of the phone that is required to trigger an alarm. Level 1 is the least sensitive. An alarm triggers if there is quite a bit of jostling. Level 7 is the most sensitive. An alarm triggers if the user walks quickly or runs.
Running timeout (seconds)	Integer 10–60	10	Sets the length of time in seconds that the user would have to maintain the configured degree of shaking (or a more severe degree).
Snooze timeout (seconds)	Integer 0–300	0	The Snooze feature allows the user to temporarily suspend Emergency motion monitoring. To activate this feature, set the timeout in seconds 1–300. By default, the Snooze feature is disabled (set to 0).

Field	Field type or choices	Default	Description
Warning timeout (seconds)	Integer 10–60	10	Sets the warning timeout in seconds. This is the amount of time between the trigger of the warning and the alarm state. In the alarm state, an emergency call might be placed or an alarm is sent to an external security application.

Related Topics

Access the Cisco app settings on the phone, on page 91

Panic Button settings

When the user activates an enabled Panic Button, an alarm displays on the phone until the user cancels it. By default, the Panic Button is disabled.

Use the following settings to configure the Panic Button.

Table 20: Panic Button settings

Field	Field type or choices	Default	Description
Panic button	Disabled Long press Two short presses Two short or one long press	Disabled	Defines the sequence that the user uses to trigger the **Panic Button** alarm. You can also disable the **Panic Button** alarm from this setting.
Panic button silent alarm	On Off	On	Enables the silent alarm, which disables the loud local alarm that sounds when a user triggers the **Panic Button**. If the user is under duress, a silent alarm doesn't alert the assailant.
Panic button alarm timeout	Integer 5–30	5	Sets the amount of time, in seconds, to time out the panic alarm.

Related Topics

Access the Cisco app settings on the phone, on page 91

Sample Panic Button configuration options

You can set the Panic Button to perform various actions based on the user's needs.

Table 21: Sample Panic Button configuration options

Option	Description	Settings
Local panic alarm without an emergency phone call	Allows the user to alert people nearby with a loud alarm, but does not place an emergency call. The loud alarm helps people to locate the user, or scares away any potential threats.	Set the **Panic button silent alarm** to Off. Set the **Emergency call** to Off.
Silent duress alarm with or without an emergency phone call	Allows the user to silently send an alarm signal for help. If the user also must place an emergency call, you can turn off the speakerphone option to maintain the silence. If the Panic Button automatically pushes an alert to an external security application, you do not need to set an emergency call.	Set the **Panic button silent alarm** to On. Set the **Emergency call** to either On or Off. If necessary, set the **Emergency dial force speaker** to Off.
Incapacitation panic alarm with an emergency phone call	Allows an incapacitated user to place an emergency call. An incapacitated user may not be able to hold the phone to their ear. To ensure that both parties can hear the phone call audio, set the alarm to be silent and turn on the forced speakerphone option.	Set the **Panic button silent alarm** to On. Set the **Emergency call** to On. Set the **Emergency dial force speaker** to On.

Emergency call settings

You can configure the Panic Button to place an emergency call when the user activates the Panic Button. By default, the emergency call is disabled.

Use the following settings to configure emergency calls.

Table 22: Emergency Call settings

Field	Field type or choices	Default	Description
Emergency call	On Off	Off	Enables the phone to call the emergency number configured in **Emergency dial number**, if the user triggers the Panic Button or an Emergency motion alarm.

Field	Field type or choices	Default	Description
Emergency dial force speaker	On Off	On	Enables the speakerphone when the phone places an emergency call. This setting allows the user to be in handsfree mode in case they can't hold the phone to their ear.
Emergency dial number	Any valid TN 911	911	Defines the number that the phone dials when the user triggers the Panic Button or an Emergency motion alarm. You must configure and enable the other related settings for the emergency call to occur. Follow any dial plan rules when you enter the emergency dial number.

Related Topics

Access the Cisco app settings on the phone, on page 91

Emergency tone settings

You can set the emergency warning and alarm tones from the list of available phone ringtones.

Use the following settings to configure the emergency tones.

Table 23: Emergency tone settings

Field	Field type or choices	Default	Description
Warning tone	Default notification sound None List of available warning tones	Default (Pixie Dust)	Configures the tone to play during a warning period. This tone plays at a gradually increasing volume. Tones play even if the user silences the handset. **Note** There is no warning period for the Panic Button; it goes straight to the alarm state.
Alarm tone	Default alarm sound None List of available alarm tones	Default (Cesium)	Configures the tone to play when a Panic Button press or Emergency alarm triggers. This tone plays at a high volume. Tones play even if the user silences the handset.

Related Topics

Access the Cisco app settings on the phone, on page 91

Emergency app and Panic Button training

Ensure that you train your users about how to use the **Emergency** app and **Panic Button** within your organization. Use the following list as a guide:

- Monitoring
  - Which motion detection sensors are active? What is the degree of sensitivity? What is the timeout? How long is the warning state?
  - What happens when an alarm is triggered? Is there an emergency call? Is there an external security application, and if so, what does it do?
  - Is the Snooze option configured? If so, for how long?
- Panic Button
  - How do you activate the Panic Button? With a long press, two short presses, or either?
  - If you press the Panic Button, will the phone place an emergency call?
  - If you press the Panic Button, will it sound an alarm through the speakerphone?
  - If the phone places an emergency call, does the audio come through the speakerphone?

Push to Talk app

The Push to Talk (PTT) app is a radio multicast app, where the phones can operate in a group broadcast mode, like walkie-talkies.

For the PTT functionality to work on your network, you must enable the multicast feature on your access points. For detailed information, see the Cisco Wireless Phone 840 and 860 Deployment Guide.

By default, PTT is disabled. As an administrator, you:

- Enable or disable PTT mode.
- Subscribe users to some or all the 25 available channels to receive, and optionally transmit, broadcasts.

Related Topics

Access the Cisco app settings on the phone, on page 91

User settings for Push to Talk

The user controls the following Push to Talk (PTT) settings on the phone.

Table 24: User settings for PTT

Field	Field type or choices	Default	Description
PTT volume	Integer 0–100	20	Controls the volume percentage of the PTT volume.

Field	Field type or choices	Default	Description
Default channel	Channel 1 - ALL Channels that have both **Channel can transmit** and **Channel subscription** Admin settings set to **Yes**	Channel 1 - ALL	The user sets their default channel. The default channel is the channel that broadcasts when the user presses the programmed **PTT** button or the **Talk** button in the **PTT** app. A user can set a channel as their default channel only if they are subscribed to the channel and are able to transmit on the channel.

Admin settings for Push to Talk

Use the following Admin settings to configure Push to Talk (PTT).

Table 25: Admin settings for PTT

Field	Field type or choices	Default	Description
Enable PTT	On Off	Off	PTT must be enabled for it to be activated on the selected handsets.
Allow PTT transmission when phone is locked	On Off	Off	From release 1.3(0) onward, you can set PTT to transmit even if the phone is locked.
Username	Text	Anonymous	This is the caller ID that displays on the broadcast. Usually set at Device or Group level. If nothing is entered, the default is **Anonymous**.
Multicast address	Domain name or IP address	224.0.1.116	Defines the multicast address for broadcast traffic.
Codec	G.711Mu G.726	G.726	Defines the codec.
Channel setup			You can set up to 25 PTT channels. By default, the Channel #1 label defaults to ALL, and its transmit and subscription options are set to Yes.

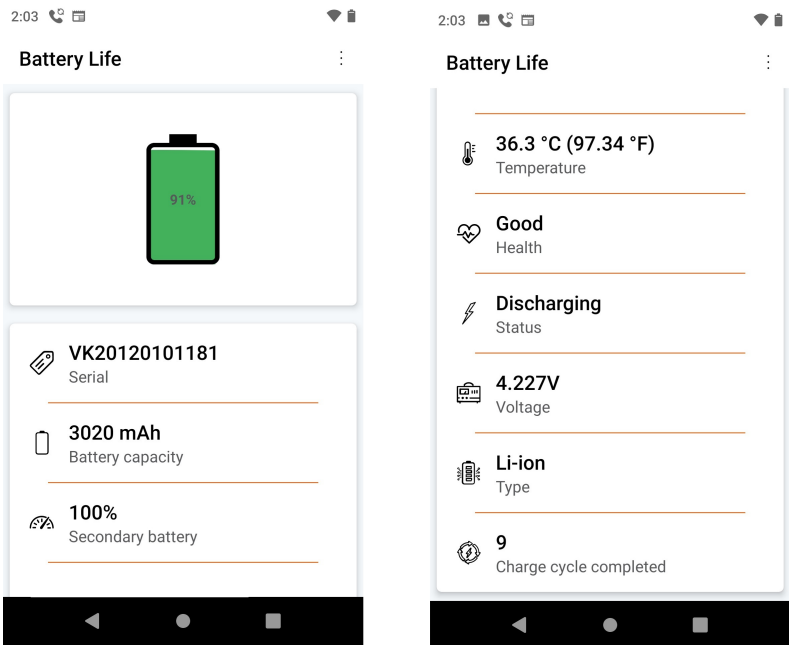
Use the following Channel setup settings to configure the desired PTT channels.

Table 26: Channel setup settings

Field	Field type or choices	Default	Description
Channel # n label	String	For Channel # 1: ALL For Channel #2-25: Blank	Allows you to enter a label for the channel. **Note** You can enter a label with more than 15 characters, but a long label truncates when it displays on the handset.
Channel can transmit	Yes No	For Channel # 1 - ALL: Yes For Channel #2-25: No	Enables a user to transmit on the channel.
Channel subscription	Yes No	For Channel # 1 - ALL: Yes For Channel #2-25: No.	Subscribes a user to the channel so that they can receive broadcasts.

Battery Life app

By default, battery monitoring is disabled. When you enable battery life monitoring, the **Battery Life** app dashboard displays the following:



- Battery serial number

- Battery capacity
- Temperature
- Health
- Charging status
- Voltage
- Battery type
- Charge cycle completed

A low battery warning notification displays on the screen if the percentage of remaining battery life is below the set **Low battery threshold**.

As administrator, you can also enable sound and vibration for the low battery alarm.



Note The Cisco Wireless Phone 860 and Cisco Wireless Phone 860S have an internal secondary battery, which operates the phone during a hot swap. The **Battery Life** app dashboard displays the general status of the internal battery. For more information about the secondary battery, you can tap **Open additional metrics and options**.

The The Cisco Wireless Phone 840 and 840S do not have an internal battery.

For 1.7(0) or later, if the number of charge cycles exceed the specified maximum count, you receive a notification to replace the battery. Make sure to replace the battery immediately after you receive a notification for better performance.

Related Topics

Access the Cisco app settings on the phone, on page 91

User settings for Battery Life

The user controls the following Battery Life settings.

Table 27: User settings for Battery Life

Field	Field type or choices	Default	Description
Alarm volume	Integer 0–100	50	Controls the volume percentage of the low battery alarm. This is a user-controlled setting.

Admin settings for Battery Life

Use the following Admin settings to configure the Battery Life app.

Table 28: Admin settings for Battery Life

Field	Field type or choices	Default	Description
Alarm volume	Integer 0–100	50	Controls the volume percentage of the low battery alarm. This is a user-controlled setting.
Enable battery monitoring	On Off	Off	Enables or disables battery monitoring. When disabled, the low battery alarm does not sound and the battery life details such as the serial number, capacity, temperature, and charging status do not display.
Vibrate	On Off	Off	Causes the phone to vibrate if the battery alarm is active and battery monitoring is enabled.
Sound	On Off	Off	Enables sound for the battery alarm, if the battery alarm is active and battery monitoring is enabled.
Alarm tone	Default alarm sound None List of available alarm tones	Default (Cesium)	Defines the battery alarm tone.
Low battery threshold	15% 20%	15%	Defines the percentage of remaining battery life to trigger the alarm.
Snooze time	1 min 2 min 3 min 4 min 5 min	2 min	Defines the number of minutes the alarm is silenced when the user snoozes the battery life alarm.

Buttons app

The **Buttons** app allows you to program the buttons on their phone. You can disable user control for all buttons or for specific buttons. For example, you can disable user control of the **Programmable Emergency** button, to ensure that users can always access that feature.

Programmable buttons

The following illustrations and table show the programmable buttons on the phone.

Note The programmable buttons for the Cisco Wireless Phone 840 and Cisco Wireless Phone 860 are not in the same location. Also, the Cisco Wireless Phone 840 and 840S don't have a Fingerprint button.

Figure 8: Programmable buttons on the Cisco Wireless Phone 840 and 840S

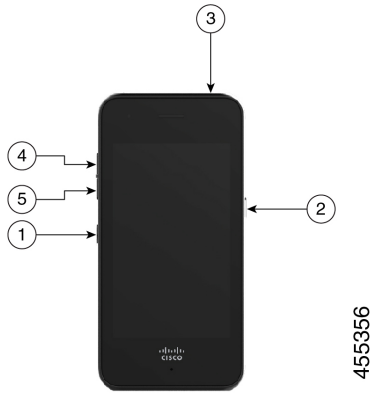


Figure 9: Programmable buttons on the Cisco Wireless Phone 860 and 860S



Table 29: Programmable buttons

Callout	Programmable button
1	Left button
2	Right button
3	Top
4	Volume up
5	Volume down

Callout	Programmable button
6	Fingerprint—For Cisco Wireless Phone 860 and 860S only.

Buttons settings

Through the Buttons app settings, you can:

- Enable or disable the user's ability to change some or all programmable buttons.
- Change the default programmable button actions.

Use the following settings to configure the buttons.

Table 30: Buttons settings

Field	Field type or choices	Default	Description
Left button user assigned	Enabled Disabled	Enabled	Enables the user to change the **Left button**.
Left button	No action Home key Back key Menu key PTT Emergency Volume up Volume down Run application Open URL Scanner (for 800S phones only) Custom 1 Custom 2 Custom 3 Custom 4	For phones with a barcode scanner: Scanner For phones without a barcode scanner: No action	Allows the user to control the button action if you enable **Left button user assigned**.
Right button user assigned	Enabled Disabled	Enabled	Enables the user to change the **Right button**.

Field	Field type or choices	Default	Description
Right button	No action Home key Back key Menu key PTT Emergency Volume up Volume down Run application Open URL Scanner (for 800S phones only) Custom 1 Custom 2 Custom 3 Custom 4	PTT	Allows the user to control the button action if you enable **Right button user assigned**.
Top button user assigned	Enabled Disabled	Enabled	Enables the user to change the **Top** button.

Field	Field type or choices	Default	Description
Top	No action Home key Back key Menu key PTT Emergency Volume up Volume down Run application Open URL Scanner (for 800S phones only) Custom 1 Custom 2 Custom 3 Custom 4	Emergency	Allows the user to control the button action if you enable **Top button user assigned**.
Fingerprint button user assigned	Enabled Disabled	Enabled	For Cisco Wireless Phone 860 and Cisco Wireless Phone 860S only. Enables the user to change the **Fingerprint** button.

Field	Field type or choices	Default	Description
Fingerprint	No action Home key Back key Menu key PTT Emergency Volume up Volume down Run application Open URL Scanner (for 800S phones only) Fingerprint Custom 1 Custom 2 Custom 3 Custom 4	Fingerprint	For Cisco Wireless Phone 860 and Cisco Wireless Phone 860S only. Allows the user to control the button action if you enable **Fingerprint button user assigned**.
Volume up button user assigned	Enabled Disabled	Enabled	Enables the user to change the **Volume up** button.

Field	Field type or choices	Default	Description
Volume up	No action Home key Back key Menu key PTT Emergency Volume up Volume down Run application Open URL Scanner (for 800S phones only) Custom 1 Custom 2 Custom 3	Volume up	Allows the user to control the button action if you enable **Volume up button user assigned**.
Volume down button user assigned	Enabled Disabled	Enabled	Enables the user to change the **Volume down** button.
Volume down	No action Home key Back key Menu key PTT Emergency Volume up Volume down Run application Open URL Scanner (for 800S phones only) Custom 1 Custom 2 Custom 3	Volume down	Allows the user to control the button action if you enable **Volume down button user assigned**.

Related Topics

Cisco app package names, on page 113
Access the Cisco app settings on the phone, on page 91

Set a button to run an application

You can configure a programmable button to open any app that is on the phone.

In the Enterprise Mobility Management (EMM) application, specify both the app package name and the app activity name in the configuration string:

```
<package name>/<package name>.<activity name>
```

When you include the app activity name, it allows you to push that configuration to the phones before you install the named app on the phones.

Note If you use only the app package name and the app is not yet on the phone, the **Buttons** app can't apply that setting. When you do install the app later, and the user presses the button, the app will not launch.

Procedure

Step 1 In the EMM application, select **Run application**.

Step 2 Enter the package name of the app and the activity name of the screen within the app.

For example, the package name for the Cisco Phone app is `com.cisco.phone`. The package name plus the dialer activity name is `com.cisco.phone/com.cisco.phone.activities.Dialer`.

Answer and end calls using the hardware buttons

For release 1.10(3) or later, you can answer and disconnect the calls by pressing the hardware buttons instead of using the on-screen controls. By default, this feature doesn't come enabled. So, you have to turn it on manually using the Buttons application.

Note You cannot use the same button to answer and end the calls.

Set a button to answer a call

To set a button to answer a call:

Procedure

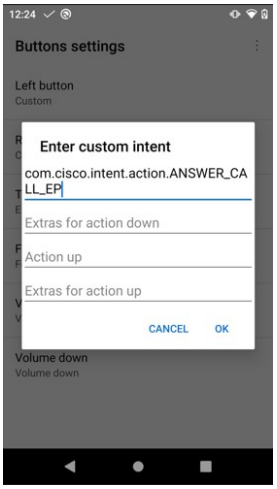
Step 1 Access the **Buttons** app.

Step 2 In the **Buttons settings** menu, select the button that you want to use to answer a call.

Step 3 Choose **Custom** in the resulting action menu.

Note Make sure not to choose Custom1 - 4.

Step 4 In the **Enter custom intent** popup window that appears enter one of the following strings in the **Action down** field (field text is case-sensitive):



- To send the audio to the phone's earpiece (shown in the screenshot above):

  `com.cisco.intent.action.ANSWER_CALL_EP`

- To use the phone as a speakerphone:

  `com.cisco.intent.action.ANSWER_CALL_SP`

- To send the audio to a wired headset:

  `com.cisco.intent.action.ANSWER_CALL_HS`

Note If the phone is connected to a Bluetooth headset the audio will automatically route to the headset regardless of which string is entered above.

Step 5 Leave the remaining fields empty.

Step 6 Tap **OK** to save your settings.

Your button can now be used to answer the incoming calls.

Set a button to end or decline a call

To set a button to end the current call or decline an incoming call:

Procedure

Step 1 Access the **Buttons** app.

Step 2 In the **Buttons settings** menu, select the button that you want to answer a call.

Step 3 Choose **Custom** in the resulting action menu.

Note Make sure not to choose Custom1 - 4.

Step 4 In the **Enter custom intent** popup window that appears enter the following string in the **Action down** field (field text is case-sensitive):

```
com.cisco.intent.action.DECLINE_CALL
```

Step 5 Leave the remaining fields empty.

Step 6 Tap **OK** to save your settings.

Your button can now be used to end a call or decline an incoming call.

Turn ON and OFF flaslight using the hardware buttons

For release 1.10(3) or later, you can turn ON and OFF the flashlight by pressing the hardware buttons.

Set a button to control the flashlight

To set a button to turn the flashlight on when the button is pressed and held, and turn the flashlight off when the button is released:

Procedure

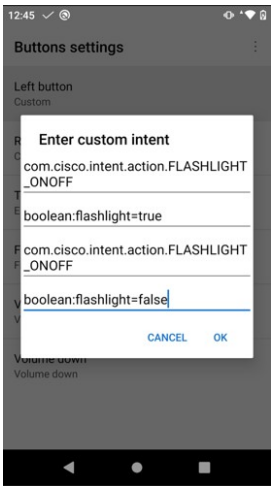
Step 1 Access the **Buttons** app.

Step 2 In the **Buttons settings** menu, select the button you that you want to control the flashlight.

Step 3 Choose **Custom** in the resulting action menu.

Note Make sure not to choose Custom1 - 4.

Step 4 In the **Enter custom intent** popup window that appears enter the following in the **Action down** and **Action up** fields (field text is case-sensitive):




```
com.cisco.intent.action.FLASHLIGHT_ONOFF
```

Step 5 In the Extras for action down field enter the following:

```
boolean:flashlight=true
```

Step 6 In the **Extras for action up** field enter the following:

```
boolean:flashlight=false
```

Step 7 Tap **OK** to save your settings.

Your button will now turn on the flashlight when pressed and held, and turn off the flashlight when released.

Set a button to toggle the flashlight

To set a button to toggle the flashlight on and off:

Procedure

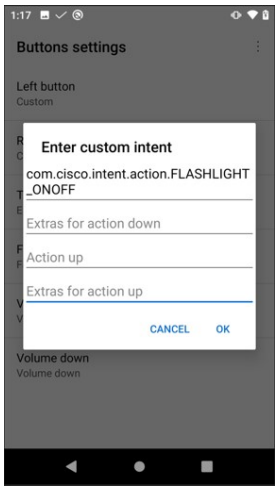
Step 1 Access the **Buttons** app.

Step 2 In the **Buttons settings** menu, select the button you that you want to control the flashlight.

Step 3 Choose **Custom** in the resulting action menu.

Note Make sure not to choose Custom1 - 4.

Step 4 In the **Enter custom intent** popup window that appears enter the following in the **Action down** and **Action up** fields (field text is case-sensitive):



`com.cisco.intent.action.FLASHLIGHT_ONOFF`

Step 5 Leave the remaining fields empty.

Step 6 Tap **OK** to save your settings.

Pressing your button will now toggle the flashlight on and off.

Cisco app package names

The following are the package names for the Cisco apps.

Table 31: Cisco app package names

Cisco app	Cisco app package name
Barcode	com.cisco.barcode.service
Battery Life	com.cisco.batterylife
Buttons	com.cisco.buttons
Call Quality Settings	com.cisco.callquality
Cisco Phone	com.cisco.phone
Custom Settings	com.cisco.customsettings
Diagnostics	com.cisco.diagnostics
Emergency	com.cisco.emergency
Logging	com.cisco.logging
PTT	com.cisco.ptt
System Updater	com.cisco.sysupdater

Cisco app	Cisco app package name
Sound Stage	com.cisco.soundstage
Web API	com.cisco.webapi

Note The Smart Launcher and Device Policy Controller apps are not on the Google store and are available only through the Cisco Wireless Phone Configuration Management tool.

Barcode app

The Cisco Wireless Phone 840S and Cisco Wireless Phone 860S have a built-in barcode scanner. The Cisco Wireless Phone 840 and Cisco Wireless Phone 860 don't have a barcode scanner.

By default, the barcode scanner is enabled along with all supported symbologies. As an administrator, you control the **General settings**, **Default settings**, and **ScanFlex** settings of the **Barcode** app.

As an administrator, you can:

- Enable and disable barcode scanning.
- Decide which symbologies to deploy.
- Set audible acknowledgments of a scan.
- Set the intensity of the scan light.
- Set the Enter key to move to the next field to be populated by scanning.
- Enable automatic enter of carriage return.
- Test scan barcodes before you give the phones to users.

Related Topics

Access the Cisco app settings on the phone, on page 91
Test scan a barcode, on page 132

Barcode symbologies

The Cisco Wireless Phone 840S and 860S barcode scanners support the following barcode symbologies.

Table 32: Supported barcode symbologies

Aztec	Codabar	Interleaved 2 of 5
CCA EAN-128	Code 11	ISBT-128
CCA EAN-13	Code 128	ISBT-128 Con
CCA EAN-8	Code 32	Macro PDF

CCA GS1 DataBar Expanded	Code 39 Full ASCII	Macro QR
CCA GS1 DataBar Limited	Code 39 Trioptic	Matrix 2 of 5
CCA GS1 DataBar-14	Code 93	Micro PDF
CCA UPC-A	DataMatrix	Micro QR
CCA UPC-E	EAN-128	MSI
CCB EAN-128	EAN-13	PDF-417
CCB EAN-13	EAN-13 + 2 Supplemental	QR Code
CCB EAN-8	EAN-13 + 5 supplemental EAN-8	UPC-A
CCB GS1 DataBar Expanded	EAN-8	UPC-A + 2 Supplemental
CCB GS1 DataBar Limited	EAN-8 + 2 Supplemental	UPC-A + 5 supplemental
CCB GS1 DataBar-14	EAN-8 + 5 supplemental	UPC-E0
CCB UPC-A	GS1 128	UPC-E0 + 2 Supplemental
CCB UPC-E	GS1 DataBar Expanded	UPC-E0 + 5 supplemental
CCC EAN-128	GS1 DataBar Limited	
	GS1 DataBar-14	
	Han Xin	

General settings for the Barcode app

Use the following settings to enable or disable the barcode scanner and configure general scan settings such as sounds and vibration.

Table 33: General settings for the Barcode app

Field	Field type or choices	Default	Description
Enable barcode scanner	On Off	On	Enables the barcode scanner.
Allow scan on screen lock **(Only for Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	Allows barcode scanning while the phone is locked.
Decode session timeout	0.5 seconds to 9.9 seconds	5	Sets the amount of time for the decode session timeout.

Field	Field type or choices	Default	Description
Vibrate on scan	On Off	On	Sets the phone to vibrate on scan.
Sound on scan	On Off	On	Sets the phone to produce a sound on scan.
Barcode tone	Low pitch single beep Low pitch double beep High pitch double beep	Low pitch single beep	Sets the barcode scan tone.
Illumination power	0–10	5	Sets the illumination power of the barcode scanner.
Allow URL redirection to browser **(Only for Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	Allows URL redirction.

Default settings for the Barcode app

You can set the following default settings for the Barcode app.

Data manipulation settings

Use the following settings to configure any rules about how to manipulate the scanned data, such as automatically adding or striping data.

Table 34: Data manipulation settings

Field	Field type or choices	Default	Description
Enable AIM codes or symbol id	Disable Enable AIM codes Enable symbol id	Disable	Prefixes AIM code or symbol id before data. The AIM code is an industry standard 3-character identifier that provides information about the symbology that is generated by the decoder of a scanner. The code is prepended to the scanned barcode and may be employed by keyboard injection and the data sent through the intent.
Automatic carriage return	On Off	Off	Adds an Enter when inject text to an input field.
Automatic Tab	On Off	Off	Adds a Tab at the end of an injected barcode value.
Trim barcode data	On Off	Off	Removes any trailing or leading whitespaces from a scanned barcode data.
Strip characters from left	Integer	0	Strips this number of characters from the left (as displayed on screen) of the barcode data. Only positive integers allowed.
Strip characters from right	Integer	0	Strips this number of characters from the right (as displayed on screen) of the barcode data. Only positive integers allowed.
Prepend String	String		Prepends a string to the scanned barcode data.
Append String	String		Appends a string to the scanned barcode data.

Custom intent settings

Use the following settings to configure any custom intent settings.

Table 35: Custom intent settings

Field	Field type or choices	Default	Description
Intent delivery method	Disable Stat activity Start service Start foreground service Send broadcast	Disable	Choose intent delivery method.
Intent action	String		Enter intent action.
Intent category	String		Enter intent category.

Symbology settings

Use the following settings to enable or disable individual barcode symbologies and their related settings. By default all supported symbologies are enabled.

The following table describes the default settings for the Aztec symbology.

Table 36: Aztec

Field	Field type or choices	Default	Description
Enable Aztec	On Off	ON	Enables or disables the symbology.
Aztec decoding	Regular Inverse Both	Regular	Sets the decoding.

The following table describes the default settings for the Codabar symbology.

Table 37: Codabar

Field	Field type or choices	Default	Description
Enable Codabar	On Off	ON	Enables or disables the symbology.
Codabar length	0–55	5	Sets the Codabar length.
Enable Codabar NOTIS editing	On Off	OFF	Strips start and stop characters.

The following table describes the default settings for the Code 11 symbology.

Table 38: Code 11

Field	Field type or choices	Default	Description
Code 11	On Off	ON	Enables or disables the symbology.
Code 11 check digit verification	Disable check digits One check digit Two check digits	Disable check digits	Enables or disables check digit verification.
Enable transmit code 11 Check Digit	On Off	OFF	Enables or disables transmit. To transmit, enable verification.

The following table describes the default settings for the Code 32 symbology.

Table 39: Code 32

Field	Field type or choices	Default	Description
Code 32	On Off	ON	Enables or disables the symbology. Enable Code 39 to enable Code 32.

The following table describes the default settings for the Code 39 symbology.

Table 40: Code 39

Field	Field type or choices	Default	Description
Enable Code 39	On Off	ON	Enables or disables the symbology. Enable Code 39 to enable Code 32.
Enable Code 39 check digit verification	On Off	OFF	Enables or disables check digit verification.
Enable transmit Code 39 check digit	On Off	OFF	Enables or disables transmit.
Enable Code 39 full ASCII conversion	On Off	OFF	Enables or disables full ASCII conversion.

The following table describes the default settings for the Code 93 symbology.

Table 41: Code 93

Field	Field type or choices	Default	Description
Enable Code 93	On Off	ON	Enables or disables the symbology.

The following table describes the default settings for the Code 128 symbology.

Table 42: Code 128

Field	Field type or choices	Default	Description
Enable Code 128	On Off	ON	Enables or disables the symbology.

The following table describes the default settings for the Data Matrix symbology.

Table 43: Data Matrix

Field	Field type or choices	Default	Description
Enable Data Matrix	On Off	ON	Enables or disables the symbology.
Data Matrix mirror images	Never Mirror Both	Never	Sets mirror images.
Data Matrix decoding	Regular Inverse Both	Regular	Sets decoding.

The following table describes the default settings for the EAN 8 symbology.

Table 44: EAN 8

Field	Field type or choices	Default	Description
Enable EAN 8	On Off	ON	Enables or disables the symbology.
Enable convert EAN 8 to EAN 13	On Off	OFF	Enables or disables conversion to EAN 13.

Field	Field type or choices	Default	Description
Enable transmit EAN 8 check digit	On Off	OFF	Enables or disables transmit.

The following table describes the default settings for the EAN 13 symbology.

Table 45: EAN13

Field	Field type or choices	Default	Description
Enable EAN 13	On Off	ON	Enables or disables the symbology.

The following table describes the default settings for the GS1 DataBar symbology.

Table 46: GS1 DataBar

Field	Field type or choices	Default	Description
Enable GS1 DataBar 14	On Off	ON	Enables or disables the symbology.
Enable GS1 DataBar composite CCA CCB, and CCC	On Off	ON	
Enable GS1 DataBar Expanded	On Off	ON	
Enable GS1 DataBar Limited	On Off	ON	

The following table describes the default settings for the GS1 128 symbology.

Table 47: GS1 128

Field	Field type or choices	Default	Description
Enable GS1-128	On Off	ON	Enables or disables the symbology.

The following table describes the default settings for the Han Xin symbology.

Table 48: Han Xin code

Field	Field type or choices	Default	Description
Enable Han Xin code	On Off	ON	Enables or disables the symbology.

The following table describes the default settings for the Interleaved 2 of 5 symbology.

Table 49: Interleaved 2 of 5

Field	Field type or choices	Default	Description
Enable Interleaved 2 of 5	On Off	ON	Enables or disables the symbology.
Enable Interleaved 2 of 5 quiet zone	On Off	OFF	Enables or disables quiet zone.
Interleaved 2 of 5 check digit verification	Disable USS OPCC	Disable	Enables or disables check digit verification.
Enable transmit Interleaved 2 of 5 check digit	On Off	OFF	Enables or disables transmit.
Interleaved 2 of 5 length type	One discrete length Two discrete lengths Length within range Any length	One discrete length	Governs the usage of the two integer fields that follow. For **Two discrete lengths** and **Length within range**, it does not matter which value is in which field.
Set Interleaved 2 of 5 length 1 (0 to 55)	0–55	14	Applicable for all scheme choices except **Any length**, which ignores it. Default value applies only to **One discrete length**.
Set Interleaved 2 of 5 length 2 (0 to 55)	0–55	0	Applicable for **Two discrete lengths** and **Length within range** only.

The following table describes the default settings for the ISBT 128 symbology.

Table 50: ISBT 128

Field	Field type or choices	Default	Description
Enable ISBT 128	On Off	ON	Enables International Society of Blood Transfusion (ISBT) 128 symbology.
Select an option for concatenating pairs of ISTB code types	Disable Enable Autodiscriminate	Disable	Disable ISBT Concatenation: The device does not concatenate pairs of ISBT codes it encounters. Enable ISBT Concatenation: There must be two ISBT codes for the device to decode and perform concatenation. The device does not decode single ISBT symbols. Autodiscriminate ISBT Concatenation: The device decodes and concatenates pairs of ISBT codes immediately. If only a single ISBT symbol is present, the device must decode the symbol the number of times set via ISBT Concatenation Redundancy before transmitting its data to confirm that there is no additional ISBT symbol.
Enable check ISBT table	On Off	ON	If you enable ISBT Concatenation, enable Check ISBT Table to concatenate only those pairs found in this table.
ISTB concatenation redundancy	2 to 20	10	With ISBT Concatenation set to Autodiscriminate, this option sets the number of times the device must decode an ISBT symbol before determining that there is no additional symbol.

The following table describes the default settings for the Matrix 2 of 5 symbology.

Table 51: Matrix 2 of 5

Field	Field type or choices	Default	Description
Enable Matrix 2 of 5	On Off	ON	Enables or disables the symbology.
Enable Matrix 2 of 5 check digit	On Off	OFF	
Enable transmit Matrix 2 of 5 check digit	On Off	OFF	Enables or disables transmit.

The following table describes the default settings for the Micro PDF symbology.

Table 52: Micro PDF

Field	Field type or choices	Default	Description
Enable Micro PDF	On Off	ON	Enables or disables the symbology.

The following table describes the default settings for the Micro QR symbology.

Table 53: Micro QR

Field	Field type or choices	Default	Description
Enable Micro QR	On Off	ON	Enables or disables the symbology.

The following table describes the default settings for the MSI Plessey symbology.

Table 54: MSI Plessey

Field	Field type or choices	Default	Description
MSI Plessey	On Off	ON	Enables or disables the symbology.
Number of MSI check digits	One Digit Two Digits	One digit	
Enable transmit MSI check digit	On Off	OFF	Enables or disables transmit.
MSI check digit algorithm	MOD 10/MOD11 MOD 10/MOD10	MOD 10/MOD10	

The following table describes the default settings for the PDF 417 symbology.

Table 55: PDF 417

Field	Field type or choices	Default	Description
Enable PDF 417	On Off	ON	Enables or disables the symbology.

The following table describes the default settings for the QR symbology.

Table 56: QR

Field	Field type or choices	Default	Description
Enable QR	On Off	ON	Enables or disables the symbology.
QR decoding	Regular Inverse Both	Regular	Sets decoding.

The following table describes the default settings for the UPC-A symbology.

Note Enable EAN/UPC supplementals per option in Administrative settings to enable supplementals for UPC-A or UPC-E or both.

Table 57: UPC-A

Field	Field type or choices	Default	Description
Enable UPC-A	On Off	ON	Enables or disables the symbology.
Enable transmit UPC-A check digit	On Off	ON	Enables or disables transmit.
Transmit UPC-A preamble	No preamble:0 System character System character and country code	System character	Sets transmit preamble.

The following table describes the default settings for the UPC-E symbology.

Note Enable EAN/UPC supplementals per option in Administrative settings to enable supplementals for UPC-A or UPC-E or both.

Table 58: UPC-E

Field	Field type or choices	Default	Description
Enable UPC-E	On Off	ON	Enables or disables the symbology.

Field	Field type or choices	Default	Description
Enable transmit UPC-E check digit	On Off	ON	Enables or disables transmit.
Transmit UPC-E preamble	No preamble System character System character and country code	System character	Sets transmit preamble.
Enable convert UPCE to UPCA	On Off	OFF	Enables or disables conversion.

The following table describes the default settings 1D barcode.

Table 59: 1D Barcode settings

Field	Field type or choices	Default	Description
Inverse 1D Decoding	Dark on light Light on dark Either	Dark on light	Sets decoding.

The following table describes supplemental symbology settings.

Table 60: Supplemental settings

Field	Field type or choices	Default	Description
Supplemental setting for UPCA, UPCE and EAN barcodes	Disable Enable	Disable	Enables or disables supplemental setting.

The following table describes more symbology settings.

Table 61: More settings

Field	Field type or choices	Default	Description
EAN/UPC supplementals	Disable Enable	Disable	Global to both EAN 8 and EAN 13.
Polarity (all 1-D barcodes)	Dark on light Either Light on dark	Dark on light	Sets polarity.

Replace control characters settings

As needed, use the following replace control character settings to replace certain ASCII0-31 control character keys in a barcode string with a space or punctuation.

Table 62: Replace control characters

Field	Field type or choices	Default	Description
Replace **n**	Use control character SPACE List of Latin punctuation or symbols	SPACE	Replaces control character [**n**] with a space or a punctuation. You can also choose to use the control character itself.

The following table lists the control characters that you can replace with a space or punctuation.

Table 63: Control characters

Control character	Control character decimal
NULL (NUL)	0
Start of Header (SOH)	1
Start of Text (STX)	2
End of Text (ETX)	3
End of Transmission (EOT)	4
Enquiry (ENQ)	5
Acknowledge (ACK)	6
Bell (BEL)	7
Backspace (BS)	8
Horizontal Tab (HT)	9
Line Feed (LF)	10
Vertical Tab (VT)	11
Form Feed (FF)	12
Carriage Return (CR)	13
Shift Out (SO)	14
Shift In (SI)	15

Control character	Control character decimal
Data Link Escape (DLE)	16
Data Control 1 (DC1)	17
Data Control 2 (DC2)	18
Data Control 3 (DC3)	19
Data Control 4 (DC4)	20
Negative ACK (NAK)	21
Synchronize (SYN)	22
End Text Block (ETB)	23
Cancel (CAN)	24
End Message (EM)	25
Substitute (SUB)	26
Escape (ESC)	27
File Separator (FS)	28
Group Separator (GS)	29
Record Separator (RS)	30
Unit Separator (US)	31

The following table lists the punction that you can use to replace control characters.

Table 64: Latin punctuation or symbols

Latin punctuation or symbol	Description
!	Exclamation point
"	Quotation mark
#	Number sign
$	Dollar sign
%	Percent sign
&	Ampersand
'	Apostrophe
(	Left parenthesis
)	Right parenthesis

Latin punctuation or symbol	Description
*	Asterisk
+	Plus sign
,	Comma
-	Hyphen-Minus
.	Full stop or period
/	Forward slash or Solidus
:	Colon
;	Semicolon
<	Less-than sign
=	Equal sign
>	Greater-than sign
?	Question mark
@	Commercial at symbol
[	Left square bracket
\	Black slash or Reverse solidus
]	Right square bracket
^	Tent, control, or Circumflex accent
_	Underline, underscore, or low line
`	Grave accent
{	Left curly bracket
|	Pipe, or Vertical line
}	Right curly bracket
~	Tilde

ScanFlex

The Barcode service uses ScanFlex, a feature that allows the Barcode service to support custom data manipulation for individual applications.

Using the barcode settings and the Enterprise Mobility Management (EMM) application interface, you can group applications using barcode service into profiles which contain the exact package names that the app developers provide. Within each profile, you can enable required symbologies and configure custom data manipulation settings. When the given app is identified in the foreground, the barcode scanner only scans the symbologies that you program for that identified app.

ScanFlex allows custom intents to provide more specificity. For custom intents to function, the third-party application must be in the foreground. Some common intent delivery methods are:

- Start activity
- Start service
- Start foreground service
- Send broadcast

Custom intents and keyboard emulation use the manipulated barcode data.

ScanFlex settings

Set the following for each ScanFlex application or activity that you add.

Table 65: ScanFlex settings

Field	Field type or choices	Default	Description
Application or activity name(s)	String		Enter a name for the application or activity. If more than one name, use a comma to separate names.
Symbology settings for application(s) entered above			Set desired symbology settings for the application or activity.
Format data			Select desired symbologies, and set their data manipulation and custom intent settings.
Advanced data formatting			Select desired symbologies, and set custom actions and parameters.

Related Topics

Default settings for the Barcode app, on page 116

Actions for advanced data formatting

In the ScanFlex **Advanced data formatting** settings, you can set the scanner to perform up to ten different actions on a scanned string. You can set the actions to happen in any order, and you may repeat an action if needed.

Each action has two parameters that are associated with it: parameter 1 and parameter 2. The parameter fields may not be necessary for some actions.

The following table describes actions that move the cursor.

Table 66: Actions that move the cursor

Action	Cursor action description	Directions for parameters
Move forward	Move the cursor forward by **n** spots.	Enter **n** in Parameter 1.
Move back	Move the cursor backward by **n** spots.	Enter **n** in Parameter 1.
Move to beginning	Move the cursor to the beginning of the string.	No parameter required.
Move to end	Move the cursor to the end of the string.	No parameter required.
Move to beginning of sub-string	Move the cursor to the beginning of a sub-string.	Enter the sub-string in Parameter 1.
Move to the end of sub-string	Move the cursor to the end of a sub-string.	Enter the sub-string in Parameter 1.

The following table describes actions that don't move the cursor.

Table 67: Actions that don't move the cursor

Action	Action description	Directions for parameters
Trim whitespace	Remove leading or trailing whitespaces.	No parameter required.
Remove all whitespace	Remove all whitespaces.	No parameter required.
Remove all leading zeros	Remove leading zeros on the left of the string.	No parameter required.
Pad zeros at beginning	Add n zeros at the beginning.	Enter n in Parameter 1.
Replace first sub-string	Replace the first encountered sub-string in the scanned string.	Enter the sub-string that you want to replace in Parameter 1, and enter the new sub-string in Parameter 2.
Replace all sub-strings	Replace all encountered sub-string in the scanned string.	Enter the sub-string that you want to replace in Parameter 1, and enter the new sub-string in Parameter 2.
Remove characters	Remove characters encountered in the string.	Enter the character in Parameter 1.
Add text	Add text	Enter the text in Parameter 1.
Add code	Add character as integer code.	Enter integer code of the desired character in Parameter 1.

Action	Action description	Directions for parameters
Add tab	Add a Tab from the current position of cursor. **Note** ScanFlex uses a built-in pause after Tab; therefore, you do not need to manually add a pause.	No parameter required.
Add enter	Add an Enter at the current position of the cursor. **Note** ScanFlex uses a built-in pause after Enter; therefore, you do not need to manually add a pause.	No parameter required.

Test scan a barcode

Before you use the barcode scanner for the first time, check that the scanner is properly configured to scan your barcode type.

Before you begin

- Use the small tab to remove the plastic cover on the barcode scanner.
- Use the **Buttons** app to program a button as the **Scanner**.

Note By default, the top-left button of the Cisco Wireless Phone 860S is set to **Scanner**.

By default, the bottom-left button of the Cisco Wireless Phone 840S is set to **Scanner**.

Procedure

Step 1 Access the **Barcode** app.

Step 2 Tap the **Overflow** ⋮ menu.

Step 3 Tap **Test scan**.

Step 4 From the Barcode screen, tap the barcode scanner button.

Step 5 Point the barcode reader 1–18 inches (2.5–46 centimeters) from the barcode that you want to scan.

Step 6 Press and hold the programmed **Scanner** button with the light shining across the entire barcode symbol until the light turns off and you hear a beep.

The **Barcode type** and the **Scanned barcode data** appear on the Barcode screen. The barcode search button is enabled.

Step 7 Tap the barcode search button to find data about the scanned barcode.
The search results appear in the default browser on your phone.

Custom Settings app

The **Custom Settings** app provides phone control settings. It includes:

- User restrictions, where you can grant or restrict access to certain phone settings for the phone user.
- General administrative phone settings, such as time, device, sleep, touch, sound, and wallpaper settings.

Related Topics

Access the Cisco app settings on the phone, on page 91

User restrictions in Custom Settings

By default, all the user restrictions are on, which means that users can control these settings on their phones. If you don't want users to control certain settings, you can change these settings to Off.

User restrictions for Wi-Fi and airplane mode

The following table describes the user restriction settings that are related to Wi-Fi and airplane mode.

Table 68: User restriction settings for Wi-Fi and airplane mode

Field	Field type or choices	Default	Description
Allow Wi-Fi toggle Allow Internet Toggle **(Only For Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can enable or disable **Wi-Fi** in the quick settings tiles. If the **Allow quick settings tiles** is disabled, all the quick settings tiles are not available.
Allow airplane mode toggle	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can enable or disable **Airplane mode** in the quick settings tiles. If the **Allow quick settings tiles** is disabled, the **Airplane mode** quick settings tile is not available.

User restrictions for quick settings tiles

The following table describes the user restriction settings that are related to the quick settings tiles.

Table 69: User restriction settings for quick settings tiles

Field	Field type or choices	Default	Description
Allow quick settings tiles	On Off	On	If enabled, all enabled quick setting tiles are accessible to the end user. If disabled, all quick setting tiles are inaccessible to the end user.
Wi-Fi Internet **(Only for Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Bluetooth	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Do not disturb	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Flashlight	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Rotation lock Auto rotate **(Only for Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.

Field	Field type or choices	Default	Description
Battery saver	On Off	On	If enabled and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Mobile data	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Airplane mode	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Cast Screen cast**(Only for Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
High touch	On Off	On	If enabled and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Hotspot	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Night light	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.

Field	Field type or choices	Default	Description
Location	On Off	On	If enabled and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Invert colors Color inversion **(Only for Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	If enabled and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Data saver	On Off	On	If enabled, and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Dark theme	On Off	On	Available from release 1.3(0) onward, the **Dark theme** setting changes the display from dark text on a light background, to light text on a dark background. If enabled and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
Nearby share Quick share **(Only for Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	Available from release 1.3(0) onward, **Nearby share** is an Android platform setting that enables phones to share files, links, and pictures with other devices within a certain range. If enabled and if the **Allow quick settings tiles** is enabled, the user can control this quick setting tile. If disabled, the quick setting tile is hidden and can't be added.
For Cisco Wireless Phone 860 Only (version 2.1(0) and later)			
Alarm	On Off	On	Opens the Google Clock app to set an alarm or access other Clock functions.

Field	Field type or choices	Default	Description
Device Control	On Off	On	Enables control of smart devices connected to the Google Home app.
Screen record	On Off	On	Opens screen recording options.
Extra dim	On Off	On	Enables users to dim the screen when working in low-light environments.
QR scan	On Off	On	Launches the Camera app to scan a QR code.
Color correction	On Off	On	Allows a user to modify how colors display on their phone and are useful for a vision impaired user or for the user who want to set their display to grayscale. To access Android Color correction, navigate to Settings > Accessibility > Color and motion > Color correction. This quick settings tile allows a user to toggle Color correction on or off.
Live caption	On Off	On	Provides real-time captions for media playback. This parameter may be unavailable even if it is enabled in the app. To make this feature available, navigate to Android Settings > Accessibility > Captions > Live Captions > Download.
Calculator	On Off	On	Launches the Google Calculator app.

User restrictions for notification shade settings gear

The following table describes the user restriction setting that is related to the settings gear in the notification shade.

Table 70: User restriction settings for notification shade settings gear

Field	Field type or choices	Default	Description
Allow notification shade settings gear	On Off	On	If enabled, the user can make Android settings changes through the gear in the notification shade. If disabled, the Android settings gear in the notification shade is not accessible to the user. **Note** If you are using a Smart Launcher to restrict user access to certain apps and settings, we recommend that you disallow this setting through the Cisco Wireless Phone Configuration Management tool. Otherwise, users can easily open apps that aren't on the Smart Launcher.
Allow manage notification settings button **(Only for Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	If enabled, manages the notification settings.

User restrictions for time

The following table describes the user restriction settings that are related to time.

Table 71: User restriction settings for time

Field	Field type or choices	Default	Description
Allow time zone configuration	On Off	On	If enabled, the user can manually change the time zone on the phone from **Settings** > **System** > **Date & Time**. If disabled, the user cannot manually change the time zone on the phone.
Allow time format configuration	On Off	On	If enabled, the user can manually change the time format on the phone from **Settings** > **System** > **Date & Time**. If disabled, the user cannot manually change the time format on the phone.

Field	Field type or choices	Default	Description
Allow automatic time zone toggle	On Off	On	Not applicable for Wi-Fi enabled phones.

User restrictions for emergency calls

The following table describes the user restriction setting that is related to emergency calls from the lock screen.

Table 72: User restriction settings for emergency calls

Field	Field type or choices	Default	Description
Allow emergency call button on lockscreen	On Off	On	If enabled, displays the **EMERGENCY** button when the phone screen is locked. **Note** Regardless of whether you enable or disable this setting, a **RETURN to CALL** button is present if the phone is in a call and locked.

User restrictions for lock screen proximity sensor

The following table describes the user restriction setting that is related to the lock screen proximity sensor.

Table 73: User restriction settings for lock screen proximity sensor

Field	Field type or choices	Default	Description
Lock screen proximity detection	On Off	On	If enabled, the phone screen automatically locks when the user covers the proximity sensor. This prevents accidental input when a user puts the phone in a pocket.

More Custom Settings

Some of the Custom Settings allow you to give users control of certain phone settings from the Android settings menu. You are also able to enable or disable certain settings, or set a specific value at the Enterprise Mobility Management (EMM) application or Cisco Wireless Phone Configuration Management tool level.

Consider the following when you configure the Custom Settings:

- If you set a value in the EMM application, users can't change it on the Custom Settings menu, but they may be able to change it on the Android settings menu. The changed value reflects in the Custom Settings menu but the EMM application could override the changed value at any time.
- If you set a value in the Cisco Wireless Phone Configuration Management tool, users can't change it on the Custom Settings menu, or on the Android settings menu.

- If you set a Custom Setting to:
  - **User controlled**, it allows the user to control the setting from the Android settings menu. In this case, the Android setting menu takes precedence over the Custom Setting.
  - **Enable**, the user could disable it in the Android menu. The changed value reflects in the Custom Settings menu but the EMM application could override the changed value at any time.
  - **Disable**, the user could enable it in the Android menu. The changed value reflects in the Custom Settings menu but the EMM application could override the changed value at any time.
- If you use a secure launcher, users can't access the Android settings menu even if you set a Custom Setting to **User controlled**.

Time

Use the following settings to configure custom time settings.

Table 74: Time settings

Field	Field type or choices	Default	Description
NTP server address	String	2.android.pool.ntp.org	The Network Time Protocol (NTP) domain name or IP address. Deploy a local time server for phones that are not connected to the internet and therefore getting their time from Google or some other cloud server. **Note** From release 1.5(0), you can also define a server in DHCP option 42 to provide NTP service in case the NTP server isn't available.
Time zone	Choice	Unset/deferred	A drop-down list of all the available time zones. Unset/deferred does not set a time zone through this configuration remotely. **Caution** The time zone settings are listed by country/region/city and also have a number setting under Etc. (Etc/GMT+/-##). However, the number values (for example, –2 or +2) are reversed from usual GMT time designations. Your setting for Etc/GMT+2 transposes into the actual setting of GMT-2). Therefore, we recommend that you use the country/region/city option whenever possible.

Field	Field type or choices	Default	Description
Time format	Unset/deferred 12 hours 24 hours	Unset/deferred	Unset/deferred does not set a time format through this configuration remotely.
Automatic time zone	On Off	On	Enables or disables automatic time zone.
Allow location to set time (**For Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	On Off	On	Enables to set time for a location.

Device info

Use the following settings to configure custom device information settings.

Table 75: Device info settings

Field	Field type or choices	Default	Description
Display device info	On Off	Off	If enabled, provides four text fields for more information about the user who is assigned this phone. This information appears in the phone notifications and on a locked screen.
Device info 1	String		First parameter for device information notification
Device info 2	String		Second parameter for device information notification
Device info 3	String		Third parameter for device information notification
Device info 4	String		Fourth parameter for device information notification

Device name

Use the following setting to configure a custom name for the device.

Table 76: Edit device name setting

Field	Field type	Default	Description
Device name	String		Allows you to set the Android device name. This is useful when you use an Enterprise Mobility Management (EMM) application to configure the phones.

Battery

Use the following settings to configure custom battery settings.

Table 77: Battery settings

Field	Field type or choices	Default	Description
Battery optimization allow list	Comma-delimited list of package names		Android Battery Saver mode curtails functionality to conserve the battery life. However, it also reduces functionality by turning off apps that you might want to remain operational. Apps that you add to this list remain operational when the user turns on the phone's Battery Saver mode. **Caution** Apps that you add to this list increase battery usage by staying awake. Ensure that users have extra batteries available.
Allow battery saver	On Off	On	If enabled, allows the user to turn battery saver mode on or off. Battery saver mode can have a significant impact on what apps are available or functioning.
Battery percentage	User controlled Enable Disable	User controlled	User controlled: makes the **Battery percentage** Android setting available for the user to show or hide the battery percentage in the phone status bar. Enable and Disable: make the **Battery percentage** Android setting unavailable to users and allow the EMM application to control the setting. • Enable displays the battery percentage on the status bar. • Disable means that the battery percentage doesn't display on the phone.

Keyboard

Use the following setting to configure the keyboard Google voice typing setting.

Table 78: Keyboard setting

Field	Field choices	Default	Description
Google™ voice typing	On Off	On	Enables or disables Google voice typing.

Sleep

Use the following setting to configure the sleep setting.

Table 79: Sleep setting

Field	Field choices	Default	Description
Time to sleep after inactivity	User controlled 15 seconds 30 seconds 1 minute 5 minutes 10 minutes 30 minutes	User controlled	Sets the amount of time before the screen times out after inactivity. **User controlled** allows users to control the sleep settings available in the Android settings menu.

Display

Allows certain display settings available in the Android settings menu to be controlled by an EMM application or by the end user.

Use the following settings to configure custom display settings.

Table 80: Display settings

Field	Field type or choices	Default	Description
Display size	User controlled Small Default Large	User controlled	Sets the display size, which includes all interface elements such as text and images. **Note** For the Cisco Wireless Phone 840 and 840S, the large display size is not currently available, so if you choose this option, the phone uses the default display size.

Field	Field type or choices	Default	Description
Font size	User controlled Small Default Large Largest	User controlled	Sets the font size.
System navigation	User controlled Gesture navigation 2-button navigation 3-button navigation	User controlled	Sets the system navigation. **Note** For the Cisco Wireless Phone 840 and 840S, 2-button navigation is not currently available, so if you choose this option, the phone uses the 3-button navigation.
Auto-rotate screen	User controlled Enable Disable	User controlled	User controlled: makes the **Auto-rotate screen** Android setting available for users to turn automatic screen rotation on or off. Enable and Disable: make the **Auto-rotate screen** Android setting unavailable to users and allow the EMM application to control the setting. • Enable turns on automatic screen rotation. • Disable means that automatic screen rotation is not available.

Touch

Allows certain touch settings available in the Android settings menu to be controlled by an EMM application or by the end user.

Use the following settings to configure custom touch settings.

Table 81: Touch settings

Field	Field type or choices	Default	Description
Dialpad tones	User controlled Enable Disable	User controlled	Tones available on the phone or custom tones that are programmed in an EMM application.

Field	Field type or choices	Default	Description
Touch sounds	User controlled Enable Disable	User controlled	Percussive sounds available on the phone or in an EMM application.
Vibrate on tap	User controlled Enable Disable	User controlled	A vibration when the user taps the phone touchscreen.

Sounds

Use the following settings to configure custom sound settings.

Table 82: Sounds settings

Field	Field type or choices	Default	Description
Ringtones	List of available ringtones	All	Select the system ringtone sounds that you want to be available.
Default ringtone	Default ringtone List of available ringtones	Default (Flutey Phone)	Must be enabled on the **Ringtones** list.
Notification sounds	List of available notification sounds	All	Select the system notification sounds that you want to be available.
Default notification sound	Default notification sound List of available notification sounds	Default (Pixie Dust)	Must be enabled on the **Notification sounds** list.
Alarm sounds	List of available alarm sounds	All	Select the system alarm sounds that you want to be available.
Default alarm sound	Default alarm sound List of available alarm sounds	Default (Cesium)	Must be enabled on the **Alarm sounds** list.

Note Using CUCM, you can download more ringtones, notification sounds, and alarm sounds. The downloaded ringtones and sounds will appear in their respective list.

Camera

Use the following setting to configure the jump to camera setting.

Table 83: Camera setting

Field	Field choices	Default	Description
Jump to camera Quickly open camera**(Only For Cisco Wireless Phone 860 only (from version 2.1(0) and later)**	User controlled Enable Disable	User controlled	Allows certain camera settings available in the Android settings menu to be controlled by an EMM application or by the end user. Permits the user to set the **Jump to camera** Android setting. User controlled implies the Android settings value takes precedence.

Wallpaper

Use the following settings to configure custom wallpaper settings.

Table 84: Wallpaper settings

Field	Field type	Default	Description
Lock screen wallpaper	String	Not configured	Enter the complete file path starting with the exact location of the image file—where is it stored on the phone. Example `/sdcard/<name_of_image_file>`.
Home screen wallpaper	String	Not configured	Enter the complete file path.

Note Using CUCM, you can download more wallpapers for Lock screen and Home screen. The downloaded wallpapers will appear in their respective list.

Admin reboot command

Use the following settings to configure custom admin reboot command settings.

Table 85: Admin reboot command settings

Field	Field type or choices	Default	Description
Reboot command ID	String		Sets reboot command ID.
Reboot schedule type	Timer When next plugged-in	Timer	Sets when to schedule reboot.

Timer reboot configuration

Use the following settings to configure custom timer reboot settings.

Table 86: Timer reboot configuration settings

Field	Field type or choices	Default	Description
Time until first automatic reboot attempt	Immediately (0 minutes) 1 minute 5 minutes 10 minutes 15 minutes 30 minutes 1 hours 2 hours 3 hours 4 hours 6 hours 8 hours 12 hours	Immediately (0 minutes)	Sets time until first automatic reboot attempt.
Number of times to allow delaying reboot attempt	None 1 2 3 4 6 8 12 Unlimited	None	Sets the number of times to allow a user to delay the reboot attempt.

Field	Field type or choices	Default	Description
Time to delay reboot attempt for	1 minute 5 minutes 10 minutes 15 minutes 30 minutes 1 hours 2 hours 3 hours 4 hours 6 hours 8 hours 12 hours	1 minute	Sets the time to delay the reboot attempt.

Call Quality Settings app

Call quality settings are automatically set in the phone. However, if your support personnel direct you to adjust a setting such as the Wi-Fi band or channels, you can do so with the **Call Quality Settings** app.

By default, all Wi-Fi band options and band channels are enabled. Make sure to enable at least one band and channel, other wise the phone loses connection and does not function.

Caution Review the bands and channels in use at the intended location before you make any changes. If you select the wrong band or channels, you can permanently disconnect phones from the network. Contact Cisco TAC if incorrect band selection disables the phones. Finally, you may need to manually reset factory defaults to the phones.

Related Topics

Access the Cisco app settings on the phone, on page 91

Wi-Fi information

The **Call Quality Settings** app displays information about the Wi-Fi access point connection to the phone. This Wi-Fi information may help you to troubleshoot call quality issues.

Table 87: Wi-Fi information

Field	Description
SSID	Service Set Identifier (SSID) is the unique name that identifies the wireless network.
AP name	Access point (AP) name displays the name of the AP.
BSSID	Basic Service Set Identifier (BSSID) is the MAC of the radio MAC + SSID.
Channel	Channel displays the AP radio channel.
RSSI	Received Signal Strength Indicator (RSSI) is the strength of the signal connecting the phone and access point.
Noise	Noise indicates the level of background noise in the environment.
CU	Channel utilization (CU) shows how busy the channel is.

Call Quality Settings

You can configure the following Call Quality Settings as required.

Wi-Fi low RSSI threshold

If Cisco TAC instructs you, use the following setting to change the threshold for the Wi-Fi low Received Signal Strength Indicator (RSSI).

Table 88: Wi-Fi low RSSI threshold

Field	Field type or choices	Default	Description
Wi-Fi Low RSSI threshold	Integer –55 to –100	–67	Voice quality can degrade if the Wi-Fi signal is too weak. The RSSI changes as the user moves closer to or away from the connected AP. The RSSI threshold value setting is the RSSI level at or below which the phone seeks a better AP. The phone uses many attributes of an AP to determine if it is a good candidate including the current load on the AP, the available bandwidth on the AP, and channel. Sometimes the best AP may have an RSSI value lower than other candidates. **Caution** Consult Cisco TAC before you change the RSSI threshold value.

Channel selection

Use the following settings to select Wi-Fi bands.

Table 89: Wi-Fi band selection options

Field	Field type or choices	Default	Description
Auto	Enabled Disabled	Enabled	When enabled: • The phone uses any available band or channel. • You can't select a specific band or channel. • The phone ignores, but does not forget, your individual channel preferences. When disabled, you can select which band to enable and select specific channels within each band. You can't disable both Wi-Fi bands at the same time.
2.4 GHz Wi-Fi band	Enabled Disabled	Enabled	If enabled: • The phone uses any available channel in the 2.4 GHz band. • You can enable or disable specific channels within 2.4 GHz band.
5 GHz Wi-Fi band	Enabled Disabled	Enabled	If enabled: • The phone uses any available channel in the 5 GHz band. • You can enable or disable specific channels within 5 GHz subbands. Each subband includes a group of channels.

Use the following settings to select 2.4 GHz channels.

Table 90: 2.4 GHz channel selection

Field	Field type or choices	Default	Description
Channel 1 (2412 MHz)	On Off	On	Enables channel.

Field	Field type or choices	Default	Description
Channel 2 (2417 MHz)	On Off	On	Enables channel.
Channel 3 (2422 MHz)	On Off	On	Enables channel.
Channel 4 (2427 MHz)	On Off	On	Enables channel.
Channel 5 (2432 MHz)	On Off	On	Enables channel.
Channel 6 (2437 MHz)	On Off	On	Enables channel.
Channel 7 (2442 MHz)	On Off	On	Enables channel.
Channel 8 (2447 MHz)	On Off	On	Enables channel.
Channel 9 (2452 MHz)	On Off	On	Enables channel.
Channel 10 (2457 MHz)	On Off	On	Enables channel.
Channel 11 (2462 MHz)	On Off	On	Enables channel.
Channel 12 (2467 MHz)	On Off	On	Enables channel.
Channel 13 (2472 MHz)	On Off	On	Enables channel.
Channel 14 (2484 MHz)	On Off	On	Enables channel.

Use the following settings to select 5.0 GHz channels.

Table 91: 5.0 GHz channel selection

Field	Field type or choices	Default	Description
Channel 36 (5180 MHz)	On Off	On	Enables channel.
Channel 40 (5200 MHz)	On Off	On	Enables channel.
Channel 44 (5220 MHz)	On Off	On	Enables channel.
Channel 48 (5140 MHz)	On Off	On	Enables channel.
Channel 52 DFS (5260 MHz)	On Off	On	Enables channel.
Channel 56 DFS (5280 MHz)	On Off	On	Enables channel.
Channel 60 DFS (5300 MHz)	On Off	On	Enables channel.
Channel 64 DFS (5320 MHz)	On Off	On	Enables channel.
Channel 100 DFS (5500 MHz)	On Off	On	Enables channel.
Channel 104 DFS (5520 MHz)	On Off	On	Enables channel.
Channel 108 DFS (5540 MHz)	On Off	On	Enables channel.
Channel 112 DFS (5560 MHz)	On Off	On	Enables channel.
Channel 116 DFS (5580 MHz)	On Off	On	Enables channel.
Channel 120 DFS (5600 MHz)	On Off	On	Enables channel.

Field	Field type or choices	Default	Description
Channel 124 DFS (5620 MHz)	On Off	On	Enables channel.
Channel 128 DFS (5640 MHz)	On Off	On	Enables channel.
Channel 132 DFS (5660 MHz)	On Off	On	Enables channel.
Channel 136 DFS (5680 MHz)	On Off	On	Enables channel.
Channel 140 DFS (5700 MHz)	On Off	On	Enables channel.
Channel 144 DFS (5720 MHz)	On Off	On	Enables channel.
Channel 149 (5745 MHz)	On Off	On	Enables channel.
Channel 153 (5765 MHz)	On Off	On	Enables channel.
Channel 157 (5785 MHz)	On Off	On	Enables channel.
Channel 161 (5805 MHz)	On Off	On	Enables channel.
Channel 165 (5825 MHz)	On Off	On	Enables channel.

Wi-Fi preferences

Use the following settings to select Wi-Fi preferences.

Table 92: Wi-Fi preferences

Field	Field type or choices	Default	Description
FT	Preferred Not preferred	Preferred	Fast Transition (FT)

Field	Field type or choices	Default	Description
CCKM **Note** This parameter is not available for Cisco Wireless Phone 860 from version 2.1(0) and later	Preferred Not preferred	Preferred	Cisco Centralized Key Management (CCKM)
CAC **Note** This parameter is not available for Cisco Wireless Phone 860 from version 2.1(0) and later	ON OFF	OFF	Call Admission Control (CAC)

Diagnostics app

Diagnostics application allows administrator to perform diagnostics tests quickly and efficiently to verify phone's hardware components.

As an administrator, you can:

- Perfom individual tests for the following features:
  - Audio
  - Battery
  - Buttons
  - Camera
  - Display
  - NFC
  - Sensor
  - Touchscreen
  - Vibration
  - Wi-Fi
- View Test Results
- Reset Test Results

- Generate QRCode
- View information such as Software Versions, Android Version, Device Serial, Wi-Fi Mac Address, Device Model, and Battery Serial.

Sound Stage app

The sound stage app prevents the users from accidentally muting the phone and missing critical phone calls or alerts. This app will override and ignore volume changes made by the user or third-party applications that conflict with the admin settings. Volume Profile configurations typically provided by EMM. It also controls volume on alerts and notifications from third-party applications.

Allows control of volume and can be set it to lower levels during night Shifts from 7PM- 7AM or any customer set time. Controls volume on Cisco applications such as WebAPI, Battery Life and PTT which have independent volume setting. Controls volume levels, low or high, based on customer needs when connected to a power charger. Allows volume control when entering or exiting Quiet zones within the hospital like Neonatal Intensive Care Unit (NICU). This can be set both manual using the phone UI or automatic by scanning a pre-programmed NFC card placed at entrance and exits. This feature has the capability to program NFC cards using Android Beam.

Admin Settings for Sound Stage

Use the following Admin settings to configure the Sound Stage app.

Table 93: Admin settings for Sound Stage

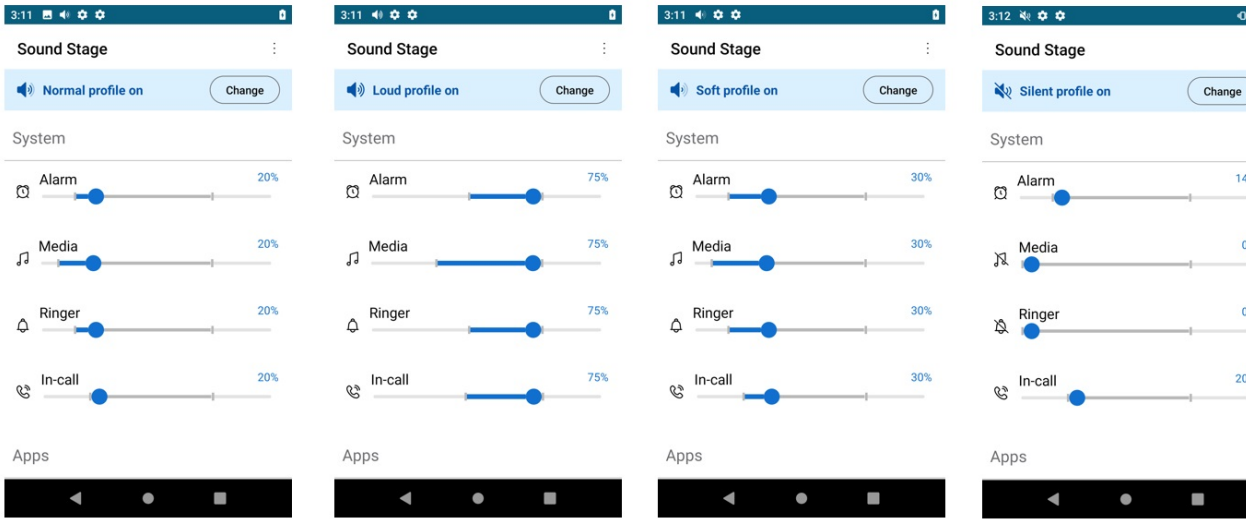
Field	Field type or choices	Default	Description
Enable Sound Stage	On Off	Off	Enables Sound Stage app. If the **Enable Sound Stage** is disabled, all the admin settings tiles are not available.
Enable sound profile switch	On Off	Off	If the **Enable Sound Stage** tile is enabled, you can enable or disable **Enable sound profile switch**.
Enable normal profile	On Off	Off	If the **Enable Sound Stage** tile is enabled, you can enable or disable **Enable normal profile**.
Enable loud profile	On Off	Off	If the **Enable Sound Stage** tile is enabled, you can enable or disable **Enable loud profile**.

Field	Field type or choices	Default	Description
Enable soft profile	On Off	Off	If the **Enable Sound Stage** tile is enabled, you can enable or disable **Enable soft profile**.
Enable silent profile	On Off	Off	If the **Enable Sound Stage** tile is enabled, you can enable or disable **Enable silent profile**.
Enable personal profile	On Off	Off	If the **Enable Sound Stage** tile is enabled, you can enable or disable **Enable personal profile**.
Persist active profile notification	On Off	Off	If the **Enable Sound Stage** tile is enabled, you can enable or disable **Persist active profile notification**.
Switch profiles silently	On Off	Off	If the **Enable Sound Stage** tile is enabled, you can enable or disable **Switch profiles silently**.

Audio profiles

You can access **Audio profiles** only if the **Enable Sound Stage** tile is enabled under **Settings** > **Admin settings**.

Sound stage app has four types of standard audio profiles, they are **Normal**, **Loud**, **Soft**, and **Silent**. Each profile contains a default a minimum and a maximum volume level that the phone can be set for that media type. However, you may use **Personal Profile**.



You can also customize any of the audio profiles as required, by changing the the volume level for alarm, media, ringer, in-call, and apps as applicable.

Change the audio profile

You can change the audio profile only if the **Enable Sound Stage** tile is enabled in **Settings** > **Admin settings**. By default normal profile will be activated.

Note The audio profile could also be changed by scanning a programmed NFC tag without the phone open.

To change the audio profile:

Procedure

Step 1 Access the **Sound Stage** app.

Step 2 Tap the **Change** button for the active audio profile.

Step 3 Choose one of the following audio profiles.

- Normal
- Loud
- Soft
- Silent
- Personal

Profile switch rules

You can set up profile switch rules based on behavior (charging) or time.

Behavior Based: Allows you to set up profile switch rule that automatically switches audio profile to desired profile when a mobile phone is charging. You can set up behavior based profile switch rule by enabling **Charging** tile in **Settings** > **Profile switch rules**.

Time Based: Allows you to set up profile switch rule that automatically switches audio profile to desired profile at a specified time. You can specify four different time based profile switch rules. You can set up the time based profile switch rule by tapping on any of the four time slots in **Settings** > **Profile switch rules** > **TIME BASED** and specify the time and desired audio profile.

Note If you have set up both behavior based and time based profile switch rules, the high priority will be behavior based.

You can set up the charging based profile switch rules, only if **Charging** tile is enabled in **Settings** > **Profile switch rules**. You can also set up the time based profile switch rules.

Note

To change the **Switch to**profile:

Procedure

Step 1 Access the **Sound Stage** app.

Step 2 Tap the **Overflow** menu.

Step 3 Select **Settings** > **Profile switch rules** .

Step 4 Tap **Charging**.

Step 5 Choose one of the following **Switch to** options .

- Normal
- Loud
- Soft
- Silent
- Personal

Web API app

Developers use the **Web API** app to interface with external services and provide links to frequently used websites. Web API allows you to configure the phones to integrate with an XML application.

The following table describes the Web API settings.

Table 94: Web API settings

Field	Field type or choices	Default	Description
Enable Web API	On Off	Off	Enables or disables Web API.
Enable Web access	On Off	Off	Enables or disables Web access.
Data format	XML JSON	XML	Sets the data format. XML is the only supported format.

Related Topics

Access the Cisco app settings on the phone, on page 91

Phone state polling

You can set the following phone state polling parameters.

Table 95: Polling parameters

Field	Field type or choices	Default	Description
Username	String		Defines the username that the phone requires to authenticate polling.
Password	String		Defines the password that the phone requires to authenticate polling.
Respond mode	Requester URL	Requester	Defines the method for sending the requested polling data. If the **Respond mode** is requester, the response is automatically sent to the HTTP server running at the address where the request was made.
URL	String		When the **Respond mode** is set as URL, this field defines the URL of a valid HTTP server that gets the response. You must enter the URL. This can be a different address than the requester.

Push settings

When you configure push settings, consider that when a phone receives a push request, it reacts differently based on the following:

- If a phone is in a call and receives a push with a priority of High, Important, or Normal, the phone accepts the push but does nothing.
- If a phone receives a push request when it is in Do Not Disturb (DND) with:
  - Total Silence—The phone does not make any sound and only displays visual notification. The phone stays in Total Silence mode after the push request.
  - Alarms Only and Priority Only—The phone changes mode to Normal, presents visual notification, and plays the notification sound. The phone stays in Normal mode after the push request.

Use the following settings to configure push settings.

Table 96: Push settings

Field	Field type or choices	Default	Description
Username	String		Defines the username for the Web API to do any kind of push.
Password	String		Defines the password for the Web API to do any kind of push.
Push alert priority	All Critical High Important Normal None	All	Sets the priority for messages from the app. Only messages with the selected priority level display. • All—Allows all priority push messages. • Critical—Allows only critical push messages. • High—Allows only high priority push messages. • Important—Allows only important push messages. • Normal—Allows only normal push messages. • None—Discards all push messages.

Field	Field type or choices	Default	Description
Server root URL			Defines the URL of the application server. This root URL is combined with the phone address and sent to the phone's browser. For example, if the application server root URL is `http://172.24.128.85:8080/sampleapps` and the relative URL is `/examples/sample.html`, the URL that is sent to the web browser on the phone is `http://172.24.128.85:8080/sampleapps/examples/sample.html`. The URL can be either HTTP or HTTPS.
Enable notification ringtone	On Off	Off	Defines whether a notification ringtone sound plays when a phone receives a push message. The notification sound that plays is set by the user in the phone **Settings** > **Sound** > **Default notification sound**.
Web API volume	0–100	50	Sets the volume for the push ringtone.

Push request notifications

Each push request alert that appears in the notification drawer includes a **View Alert** option and a triangular exclamation icon. The color of the icon varies according to the priority of the alert:

- Critical: Red
- High: Orange
- Important: Yellow
- Normal: Green

If you receive multiple push requests, the notifications in the notification drawer are grouped by priority. The groups display in descending order with Critical on top and Normal at the bottom and they indicate the number of alerts of each priority received.

If you reboot the phone, it does not automatically clear critical alerts. After you reboot a pin protected phone, if there is an uncleared critical push request, a pop-up dialog with a message **Unlock the phone to view critical alerts** appears.

Web application shortcuts

The Web API app allows you to configure the phones to integrate with an XML application. You can configure up to 12 web application shortcuts. Enter the following fields for each of the desired web application shortcuts.

Table 97: Web application shortcut settings

Field	Field type or choices	Default	Description
Shortcut title	String		Defines a title for the web application shortcut. The title displays in the widget box on the phone after you reboot the phone.
Shortcut URL	String		Defines the application URL. You can enter any URL available to the phones.

Place web application shortcuts on launcher screen

For easy access to web application shortcuts, place the shortcuts on the phone launcher screen. Once you place a shortcut on the launcher screen, you can tap the shortcut to open the web application in a browser.

Procedure

Step 1 Long press the home screen.

Step 2 Tap **Widgets**.

Step 3 Touch and hold the shortcut.

Step 4 Drag the shortcut to the desired location on a launcher screen.

Device event notifications

You can configure the phones to send notifications of the following phone events to a defined URL.

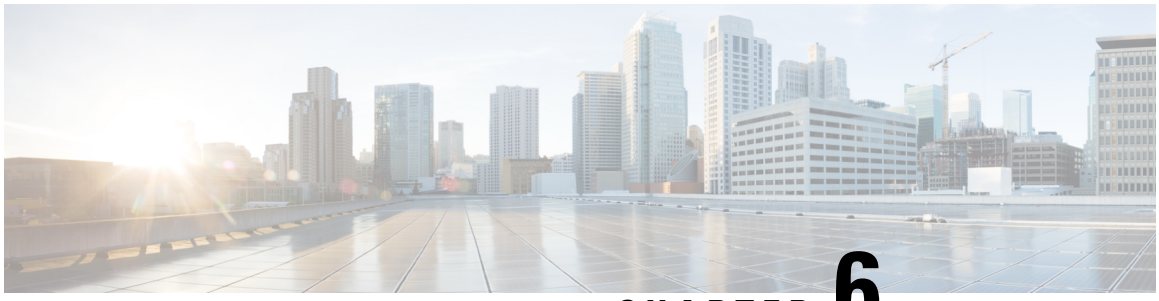
- All events
- Cisco Phone events such as phone state changes, incoming or outgoing calls, or SIP registration.
- Emergency events

Note To edit an existing event URL, delete it and reenter the information with the new URL name or address.

Use the following settings to configure event notifications.

Table 98: Device event notification settings

Field	Field type or choices	Default	Description
Notification name	String		Defines a descriptive label for the event.
Notification URL	String		Defines the URL for the event.
None	On Off	On	By default, there are no notification events.
All	On Off	Off	Sends notifications about all phone events when enabled.
Cisco Phone events: Outgoing	On Off	Off	Sends notifications about all outgoing phone events when enabled.
Cisco Phone events: Incoming	On Off	Off	Sends notifications about all incoming phone events when enabled.
Cisco Phone events: State Change	On Off	Off	Sends notifications about all phone state change events when enabled.
Cisco Phone events: Login/out	On Off	Off	Sends notifications about all phone login and logout events when enabled.
Cisco Phone events: Registration	On Off	Off	Sends notifications about all phone registration events when enabled.
Cisco Phone events: Unregistration	On Off	Off	Sends notifications about all phone unregistration events when enabled.
Emergency events	On Off	Off	Sends notifications about all Emergency events when enabled.



CHAPTER 6

Accessories

- Supported accessories, on page 165
- Headsets, on page 166
- Desktop chargers, on page 167
- Multichargers, on page 171
- Charger care, on page 175
- Scanner handle for the Cisco Wireless Phone 840S, on page 175
- Clips, on page 177
- Cisco accessory part numbers, on page 177

Supported accessories

You can use several accessories with your phone. For part numbers of the approved accessories, see Cisco accessory part numbers, on page 177.

Caution Use only the approved chargers and power supplies for your phone.

- **Headsets**—Standard headsets that use a 3.5-mm jack or Bluetooth® headsets.

Note The phones don't support Apple headsets. The phones can connect to Bluetooth headsets and speakers only. They don’t support any other type of Bluetooth device.

- **Desktop chargers**—Use the approved power supply.
  - Cisco Wireless Phone 840 Desktop Charger
  - Cisco Wireless Phone 840 Desktop Dual Charger
  - Cisco Wireless Phone 860 Desktop Dual Charger Module
  - Cisco Wireless Phone 860 Desktop Battery Charger Module

- **Multichargers**—Use the approved power supply.
  - Cisco Wireless Phone 840 Multicharger
  - Cisco Wireless Phone 840 Battery Multicharger
  - Cisco Wireless Phone 860 Multicharger Base—Holds up to four 860 Desktop Charger Modules (in any configuration: Dual or Battery).
- **USB charger**—Use the approved power supply.
- **Spare batteries**
- **Scanner handle**—For the Cisco Wireless Phone 840S only.
- **Clips**
- **Cases**—For the Cisco Wireless Phone 860 and 860S only.

Headsets

You can use wired and Bluetooth® headsets with your phone.

Although we perform some internal testing of third-party wired and Bluetooth wireless headsets for use with the Cisco Wireless Phone 840 and 860, we don't certify or support products from headset or handset vendors. Because of the inherent environmental and hardware inconsistencies in the locations where phones are deployed, there's not a single "best" solution that is optimal for all environments. We recommend that customers test the headsets that work best in their environment before deploying many units in their network.

Note The Cisco Wireless Phone 840 and 860 hasn't been tested for wired and Bluetooth headsets in hazardous locations.

We recommend the use of good quality external devices, like headsets that are screened against unwanted radio frequency (RF) and audio frequency (AF) signals. Depending on the quality of these devices and their proximity to other devices such as cell phones and two-way radios, some audio noise may still occur.

The primary reason that a particular headset would be inappropriate for the phone is the potential for an audible hum. This hum can be heard by either the remote party or by both the remote party and you, the phone user. Some potential humming or buzzing sounds can be caused by a range of outside sources, for example, electric lights, electric motors, or large PC monitors. In some instances, the mechanics or electronics of various headsets can cause remote parties to hear an echo of their own voice when they speak to phone users.

Important headset safety information

High Sound Pressure—Avoid listening to high volume levels for long periods to prevent possible hearing damage.

When you plug in your headset, lower the volume of the headset speaker before you put the headset on. If you remember to lower the volume before you take the headset off, the volume will start lower when you plug in your headset again.

Be aware of your surroundings. When you use your headset, it may block out important external sounds, particularly in emergencies or in noisy environments. Don't use the headset while driving. Don't leave your headset or headset cables in an area where people or pets can trip over them. Always supervise children who are near your headset or headset cables.

Standard headsets

You can use a wired headset with your phone. The headset requires a 3.5 mm, 3-band, 4-connector plug.

We recommend the Cisco Headset 520 Series. These headsets offer outstanding audio performance. For more information about the headset, see Cisco Headset 500 Series.

If you plug a headset into the phone during an active call, the audio path automatically changes to the headset.

Bluetooth headsets

You can use a Bluetooth® headset with your phone. When you use a Bluetooth wireless headset, the headset usually increases battery power consumption on your phone and may result in reducing battery life.

For a Bluetooth wireless headset to work, it does not need to be within direct line-of-sight of the phone, but some barriers, such as walls or doors, and interference from other electronic devices, can affect the connection.

We recommend the Cisco Headset 560 Series and Cisco Headset 730. These headsets offer outstanding audio performance. For more information about the headsets, see Cisco Headset 500 Series and Cisco Headset 700 Series.

Desktop chargers

The following desktop chargers are compatible with your phone.

However, the desktop chargers for the Cisco Wireless Phone 840 and Cisco Wireless Phone 860 are not interchangeable.

Caution Use only the approved chargers and power supplies for your phone.

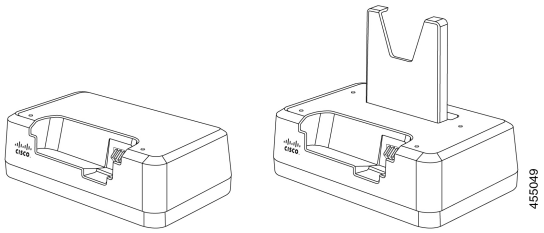
Cisco Wireless Phone 840 and 840S

The Cisco Wireless Phone 840 and 840S also have two types of desktop chargers.

Table 99: Desktop chargers

Charger name	Charger capacity
Cisco Wireless Phone 840 Desktop Charger	One 840 phone
Cisco Wireless Phone 840 Desktop Dual Charger	One 840 phone and one 840 battery

Figure 10: Cisco Wireless Phone 840 Desktop Charger and Cisco Wireless Phone 840 Desktop Dual Charger



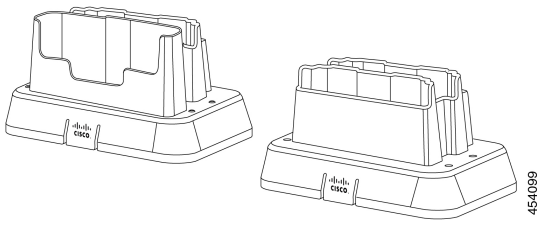
Cisco Wireless Phone 860 and 860S

The Cisco Wireless Phone 860 and 860S have two types of desktop chargers.

Table 100: Desktop chargers

Charger name	Charger capacity
Cisco Wireless Phone 860 Desktop Dual Charger Module	One 860 phone and one 860 battery
Cisco Wireless Phone 860 Desktop Battery Charger Module	Two 860 batteries

Figure 11: Cisco Wireless Phone 860 Desktop Dual Charger Module and Cisco Wireless Phone 860 Desktop Battery Charger Module



Set up the desktop chargers

Follow these steps for all Cisco Wireless Phone 840 and 860 desktop chargers.

The following illustration is of the Cisco Wireless Phone 860 Desktop Dual Charger Module.

Caution Use only the approved chargers and power supplies for your phone.

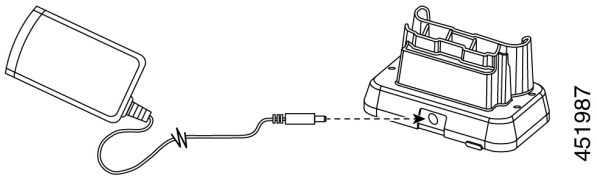
Before you begin

Ensure that the power supply has the correct plug for your area.

Procedure

Step 1 Place the module on a flat surface within reach of a power outlet.

Step 2 Plug the power supply into the module.



Step 3 Plug the other end of the power supply into a power outlet.

Charge your phone and battery with desktop dual charger

You can charge your phone and one spare battery with the desktop dual charger.

If both the phone and battery are in the charger, the phone takes priority. So it may take longer to charge the battery.

There are two LEDs: one for the phone and one for the battery. The LEDs turn on when you properly seat the phone and battery.

- A solid red LED indicates that the item is charging.
- A solid green LED indicates that the item is fully charged.
- An LED that is off indicates an empty slot or an error condition.

Note These steps are the same for both the Cisco Wireless Phone 840 Desktop Dual Charger and Cisco Wireless Phone 860 Desktop Dual Charger Module. The illustration is of the Cisco Wireless Phone 860 Desktop Dual Charger Module.

Before you begin

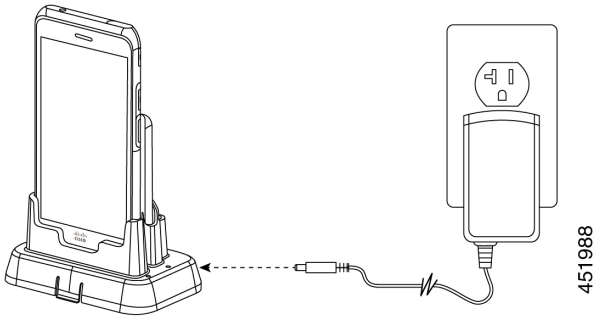
Ensure that you properly set up the desktop charger.

Caution Use only the approved chargers and power supplies for your phone.

Procedure

Step 1 With the battery charging contacts down, insert a spare battery into the dual charger rear slot.

Step 2 Insert your phone face forward into the dual charger front slot.



Charge your spare 860 batteries with desktop battery charger

You can charge up to two spare 860 batteries at a time in the Cisco Wireless Phone 860 Desktop Battery Charger Module.

Caution You can't use this charger for 840 batteries.

There are two LEDs: one for each battery. The LEDs turn on when you properly seat the batteries.

- A solid red LED indicates that the item is charging.
- A solid green LED indicates that the item is fully charged.
- An LED that is off indicates an empty slot or an error condition.

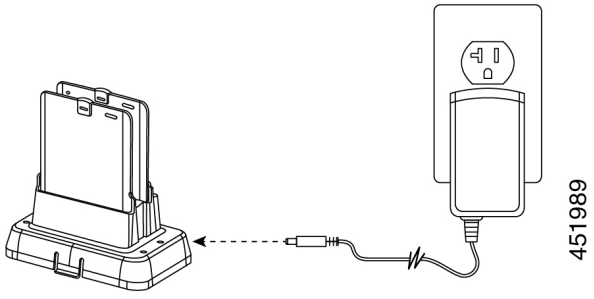
Before you begin

Ensure that you properly set up the Cisco Wireless Phone 860 Desktop Battery Charger Module.

Caution Use only the approved chargers and power supplies for your phone.

Procedure

With the battery charging contacts facing down, insert a spare battery into each charger slot.



Multichargers

The following multichargers are compatible with your phone.

However, the multichargers for the Cisco Wireless Phone 840 and Cisco Wireless Phone 860 are not interchangeable.

Caution Use only the approved chargers and power supplies for your phone.

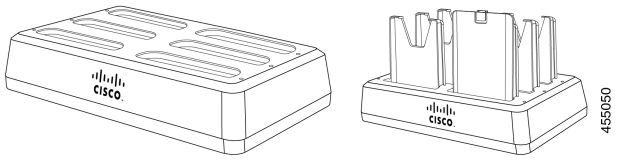
Cisco Wireless Phone 840 and 840S

The Cisco Wireless Phone 840 and 840S have two standalone multichargers:

Table 101: Multichargers

Charger name	Charger capacity
Cisco Wireless Phone 840 Multicharger	Six 840 phones
Cisco Wireless Phone 840 Battery Multicharger	Six 840 batteries

Figure 12: Cisco Wireless Phone 840 Multicharger and Cisco Wireless Phone 840 Battery Multicharger



Cisco Wireless Phone 860 and 860S

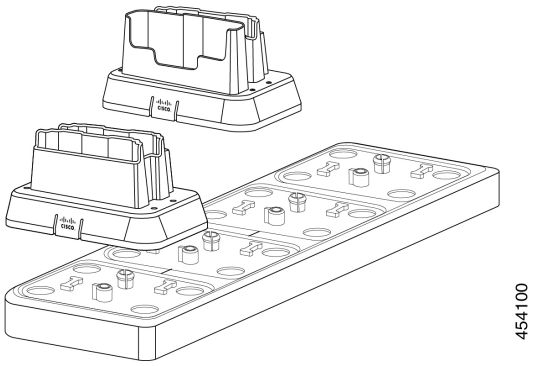
The Cisco Wireless Phone 860 and 860S multicharger includes a Cisco Wireless Phone 860 Multicharger Base that holds up to four of the following 860 desktop charger modules in any configuration:

- Cisco Wireless Phone 860 Desktop Dual Charger Module
- Cisco Wireless Phone 860 Desktop Battery Charger Module

Table 102: Sample multicharger configuration

Cisco Wireless Phone 860 Multicharger Base configuration	Charger capacity
With four Cisco Wireless Phone 860 Desktop Dual Charger Modules	Four phones and four batteries
With two Cisco Wireless Phone 860 Desktop Dual Charger Modules and two Cisco Wireless Phone 860 Desktop Battery Charger Modules	Two phones and six batteries
With four Cisco Wireless Phone 860 Desktop Battery Charger Modules	Eight batteries

Figure 13: Cisco Wireless Phone 860 Multicharger Base with 860 Desktop Charger Modules



Assemble the Cisco Wireless Phone 860 Multicharger Base

You can insert up to four desktop charger modules into the multi charger base. You can use any combination of the Cisco Wireless Phone 860 Desktop Dual Charger Modules and Cisco Wireless Phone 860 Desktop Battery Charger Modules as desired.

Caution Use only the power supply that comes with the multicharger base.

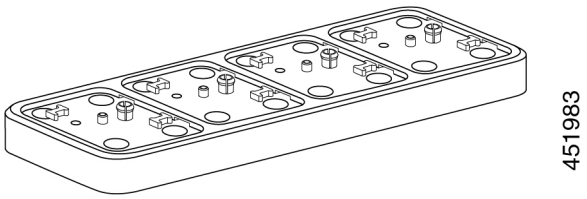
Red and green LEDs blink at powerup.

Before you begin

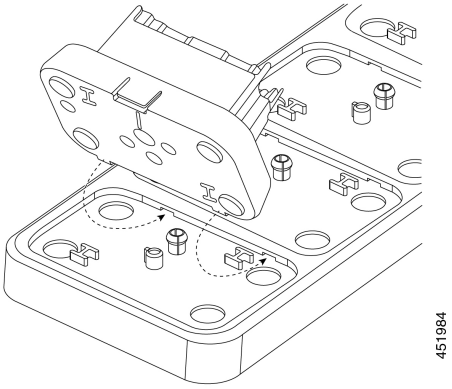
Ensure that the power supply has the correct plug for your area.

Procedure

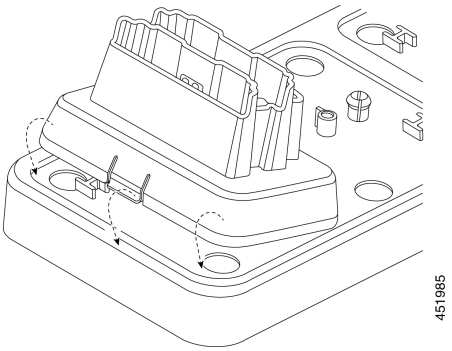
Step 1 Place the multicharger base on a flat surface within reach of power outlet.



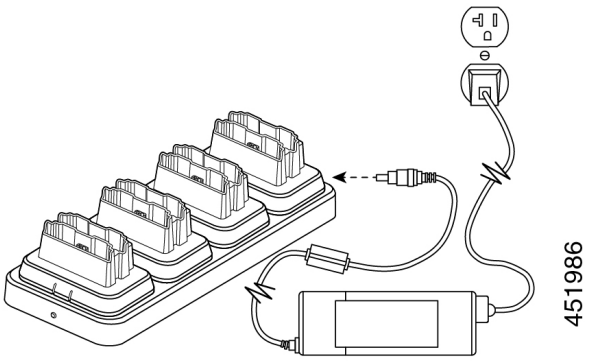
Step 2 Insert the tabs on the back of the desktop charger module into the slots on the base.



Step 3 Rock the desktop charger module forward and use the front tab to snap it into place.



Step 4 Plug the multicharger base power supply into the base and a power outlet.



Charge phones and batteries with multicharger

With the 840 multichargers, you can charge up to six phones or batteries at a time. Each slot has an LED.

With the 860 multicharger, you can charge up to eight items at a time. Each desktop module has two LEDs, one for each slot.

- Solid red LED indicates that the item is charging.
- Solid green LED indicates that the item is fully charged.
- LED that is off indicates an empty slot or an error condition.

Before you begin

For the 840 phones, ensure that you plug in the multicharger.

For the 860 phones, ensure that you properly set up the Cisco Wireless Phone 860 Multicharger Base and install up to four desktop charger modules.

Caution Use only the approved chargers and power supplies for your phone.

Procedure

Insert the phones and batteries into the slots.

Related Topics

Assemble the Cisco Wireless Phone 860 Multicharger Base, on page 172
Charge your phone and battery with desktop dual charger, on page 169

Charger care

Although you don't handle the chargers as much as the phones, they can get dirty, so it's important to periodically clean them.



Caution The plastic in the charger is different from the plastic in the phone, so it doesn't withstand rigorous disinfection.

Follow the same steps to clean the charger as you do for the phones, but pay special attention to the following:

- Remove the phone and battery from the charger. Unplug the charger.
- Never immerse the charger in liquid.
- Don't spray any solution directly onto the charger. Dampen a cloth and wipe instead. Do not allow liquid to pool on or in the plastic.
- Don't use a bleach solution on battery contacts.
- Don't to exert undue pressure on electrical contacts inside the charger compartment. Do not bend the contacts.
- For light to heavy soil—Wipe the charger surface with a water-dampened cloth or paper towel to remove most films or residue. If the soiling is too stubborn for plain water, use a mild detergent solution, Lysol®, isopropyl alcohol, or diluted bleach (10 percent or less).
- Wipe battery contacts with a cotton swab dampened with alcohol to remove any lint.
- Never use the following products to clean your charger:
  - Don't use furniture polishes, waxes, or plasticizer-based cleaners such as ArmorAll®.
  - Don't use lanolin, aloe, glycerin, or other skin care products.
  - Don't use hand sanitizers to clean chargers or handle the charger when your hands are wet with sanitizer solution.
  - Don't apply any solvent such as acetone, mineral spirits, and so on.
- Allow the charger to air dry. You may wipe the charger with a soft dry cloth to hasten dry time. Be sure that electrical contacts are completely dry and lint-free. When fully dry, you may plug in the charger and reinsert the battery and phone.

Scanner handle for the Cisco Wireless Phone 840S

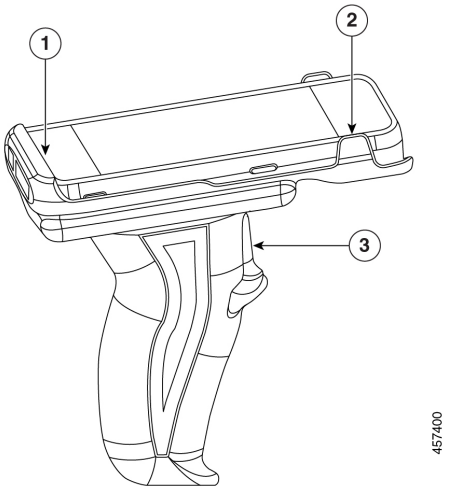
There is a scanner handle available for the Cisco Wireless Phone 840S. Use the scanner handle to easily scan multiple barcodes.

Figure 14: Cisco Wireless Phone 840S with scanner handle



Install the Cisco Wireless Phone 840S in the scanner handle

Figure 15: Cisco Wireless Phone 840S in the scanner handle



Procedure

Step 1 Insert the bottom end of the Cisco Wireless Phone 840S in the scanner handle.

Step 2 Press down on the top end of the phone to snap it in place on the scanner handle.

Step 3 Scan a barcode with the trigger on the scanner handle to test that it works.

Clips

There are clips available for the Cisco Wireless Phone 840 and 860.

The following illustration is of the rotating belt clip holsters for the Cisco Wireless Phone 840 and 840S. The belt clips for the Cisco Wireless Phone 860 and 860S don't have a holster and aren't interchangeable with the 840 clips.

Figure 16: Cisco Wireless Phone 840 and 840S and clips



Cisco accessory part numbers

The following tables provide the part numbers for the approved Cisco accessories for the Cisco Wireless Phone 840 and 860. For more information, see the Cisco Wireless Phone Data Sheet.

Caution Use only the approved chargers and power supplies for your phone.

Table 103: Desktop chargers and power supplies

Accessory	Part number	Power supply model number
Cisco Wireless Phone 840 Desktop Charger	CP-840-PH-DCHR=	—
Cisco Wireless Phone 840 Desktop Dual Charger	CP-840-DUAL-DCHR=	—
Cisco Wireless Phone 840 Desktop Charger and Cisco Wireless Phone 840 Desktop Dual Charger power supply for Australia	CP-840-DCHR-PS-AU=	SK01T8-0570260S

Accessory	Part number	Power supply model number
Cisco Wireless Phone 840 Desktop Charger and Cisco Wireless Phone 840 Desktop Dual Charger power supply for the European Union	CP-840-DCHR-PS-EU=	SK01T8-0570260V
Cisco Wireless Phone 840 Desktop Charger and Cisco Wireless Phone 840 Desktop Dual Charger power supply for North America	CP-840-DCHR-PS-NA=	SK01T8-0570260U
Cisco Wireless Phone 840 Desktop Charger and Cisco Wireless Phone 840 Desktop Dual Charger power supply for the United Kingdom	CP-840-DCHR-PS-UK=	SK01T8-0570260B
Cisco Wireless Phone 860 Desktop Dual Charger Module	CP-860-DCHR=	—
Cisco Wireless Phone 860 Desktop Battery Charger Module	CP-860-BAT-DCHR=	—
Cisco Wireless Phone 860 Desktop Dual Charger Module and Cisco Wireless Phone 860 Desktop Battery Charger Module power supply	CP-860-DCHR-PSU=	HK-AY-120A200-CP

Table 104: Multichargers and power supplies

Accessory	Part number	Power supply model number
Cisco Wireless Phone 840 Multicharger with power supply	CP-840-PH-MCHR=	KT090A1200667B3
Cisco Wireless Phone 840 Battery Multicharger with power supply	CP-840-BAT-MCHR=	KT090A1200667B3
Cisco Wireless Phone 860 Multicharger Base with power supply	CP-860-MCHR=	FSP090-ABAN3

Table 105: USB cable and power adapter

Accessory	Part number	Power adapter model number
Cisco Wireless Phone 840 and 860 USB cable and power adapter wall plug	CP-800-USBCH=	IN-CA-310Q

Table 106: Spare batteries

Accessory	Part number
Cisco Wireless Phone 840 and 840S spare battery	CP-840-BAT=

Accessory	Part number
Cisco Wireless Phone 860 and 860S spare battery	CP-860-BAT=

Table 107: Scanner handle

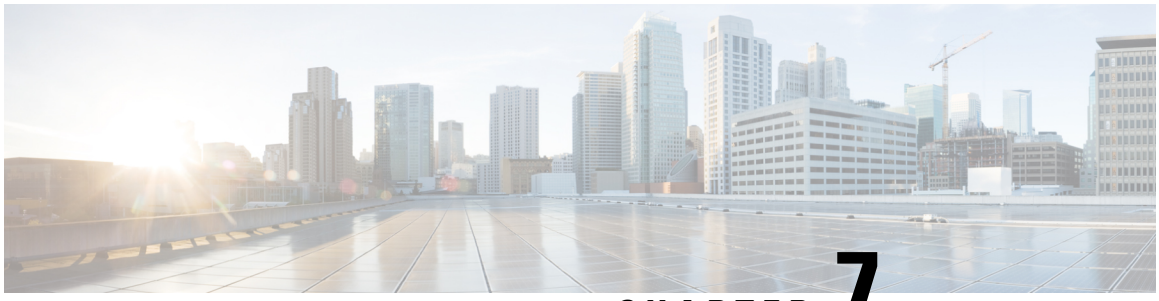
Accessory	Part number
Cisco Wireless Phone 840S scanner handle	CP-840S-HANDLE=

Table 108: Clips

Accessory	Part number
Cisco Wireless Phone 840 rotating belt clip holster	CP-840-CLIP=
Cisco Wireless Phone 840S rotating belt clip holster	CP-840S-CLIP=
Cisco Wireless Phone 860 belt clip	CP-860-CLIP=
Cisco Wireless Phone 860S belt clip	CP-860S-CLIP=

Table 109: Cases

Accessory	Part number
Cisco Wireless Phone 860 case	CP-860-CASE=
Cisco Wireless Phone 860S case	CP-860S-CASE=



CHAPTER 7

Maintenance

- Reboot the phone, on page 181
- Factory default settings, on page 181
- Cisco app software updates, on page 183

Reboot the phone

At times, you may need to manually reboot the phone.

Procedure

Step 1 Press and hold the **Power** button.

Step 2 Tap **Restart** .

Factory default settings

If necessary, you can restore the factory default settings of the phone.

Note If you perform a factory reset, the phone software stays on the latest installed version.

We recommend that you enroll your phones through an Enterprise Mobility Management (EMM) application so that you are the Device Owner and you can factory reset the phones through the EMM application.

However, if you do not enroll the phones in an EMM application, you can restore a phone to the factory defaults using the following methods:

- If you're able to boot the phone, use the phone **Settings** method.
- If you're not able to boot the phone, use the recovery mode method.

Reset to factory default through the phone settings

If the phone is not enrolled in an Enterprise Mobility Management (EMM) application, you can restore the factory default settings of the phone through the **Settings** on the phone.

Caution If the phone has a Google account or other device ownership, then it has factory wipe protection which prevents the wipe of certain account details. You must have the Google account information to access the phone after you restore factory defaults.

Procedure

Step 1 Access the **Settings** app.
Step 2 Tap **System**.
Step 3 Select **Advanced** > **Reset options**.
Step 4 Tap **Erase all data (factory reset)**.
Step 5 Tap **Erase all data**.
Step 6 Tap **Erase all data**.

Restore to factory default through recovery mode

You can restore the factory default settings of the phone through recovery mode. However, it is best to follow these steps as a last resort and only if:

- The phone is not enrolled in an Enterprise Mobility Management (EMM) application.
- You can't boot the phone to access the **Settings**.
- The phone user has not signed in to a unique Google account.

Caution If you use recovery mode to reset the factory defaults of a phone that had been signed in to a unique Google account, you will need the Google account and password. You must work with the phone user, Google account owner, and Google to reset the phone.

Procedure

Step 1 Press and hold the **Power** button.
Step 2 Tap **Power off**.
Step 3 Press and hold the red **Emergency** button and press hold the **Power** button until the phone vibrates, then release the **Power** button. Continue to hold the **Emergency** button.

Step 4 Once the bootloader screen is displayed, release the red **Emergency** button.

Step 5 Press the **Volume down** button until **Recovery mode** displays.

Step 6 Press the **Power** button to select **Recovery mode**.
The phone restarts and returns to a new screen that displays the Android icon.

Step 7 Press and hold the **Power** button, then quickly press and release the **Volume up** button to enter the **Recovery Menu** screen.

Step 8 When the **Recovery Menu** displays, release the **Power** button.

Step 9 Press the **Volume down** button to highlight **Wipe data/factory reset**.

Step 10 Press the **Power** button to select **Wipe data/factory reset**.

Step 11 Press the **Volume down** button to highlight **Factory data reset**.

Step 12 Press the **Power button** to select **Factory data reset**.

Step 13 When **Reboot system now** is highlighted, press the **Power** button.

Cisco app software updates

To upgrade the Cisco app software, use one of these methods:

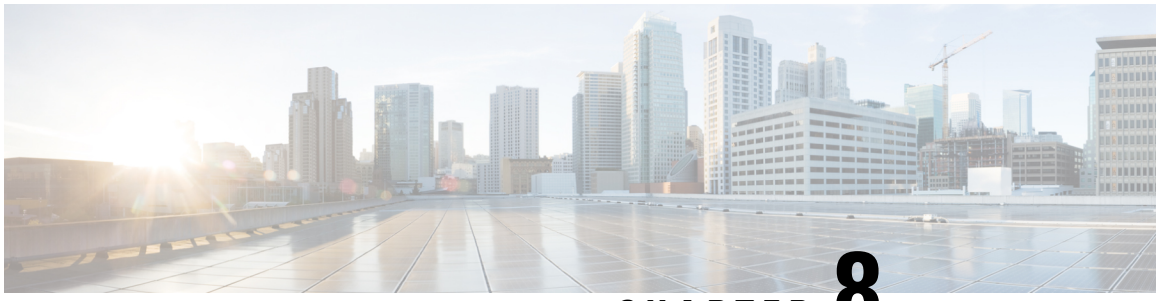
- Install the latest signed software COP file to the Cisco Unified Communications Manager.

Note After you upload the COP file, the phone prompts the user to reboot and apply the new software, unless you enabled the **Reboot immediately after downloading software updates** option in the **Product Specific Configuration Layout** pane.

- Copy the extracted firmware ZIP files contents to the HTTP (port 6970) load server defined in the **Product Specific Configuration Layout** pane. Then, update the device default or individual phone load within Cisco Unified Communications Manager, so that the phone upgrades after it is restarted.

Related Topics

Load the COP files to Cisco Unified Communications Manager, on page 34
Product Specific Configuration Layout fields, on page 57



CHAPTER 8

Troubleshooting

- General troubleshooting information, on page 185
- Details available on the phone, on page 186
- Problem report log bundles, on page 189

General troubleshooting information

General issues

The following table provides general troubleshooting information.

Table 110: General troubleshooting tips

Problem	Solution
You're not in a call and the phone goes black and displays the message: **Close proximity detected**.	Your phone has a proximity sensor at the top right. When this sensor is blocked, the phone screen is black. The sensor is normally blocked by the face when the earpiece is used to listen to a caller. If you're not in a call and you see the message: **Close proximity detected**. The sensor may be covered with a finger or paper or something else that blocks light. If there's no apparent blockage, clean the area of the sensor.
While using a standard headset, you experience a scratchy or intermittent signal.	The headset connector may be dirty. If available, blow canned air into the connector to clear debris. Always point canned air orientation at glancing angles away from your face and eyes and always wear safety goggles or glasses when performing this procedure. Do not use air compressors on the connectors, since they apply too much force.
Third Party Application Conflicts	Third party application interference can be eliminated by factory reset and reregistration of a problematic phone. For more details about the factory reset, see Restoring Factory Defaults in the Cisco Wireless Phone 840 and 860 Deployment Guide.

Visual voicemail issues

The following table provides general troubleshooting information that is related to issues with Visual Voicemail.

Table 111: Visual voicemail troubleshooting tips

Problem	Solution
`Unauthorized` message appears in the Enter Unity Web Credentials dialog box after the user enters their credentials and selects the Login option.	Validate that the: • User enters the same Username as the Alias field (including case) on the User's Mailbox in the Cisco Unity Connection voice messaging system. • User uses the Web Application password, not the Voicemail pin. • Password Settings for the User's Web Application Password don't have the User Must Change Password at Next Sign-In check box selected.
When the user navigates to the Voicemail tab of the Cisco Phone app, a brief toast notification appears, which states `Voicemail connection error. Unable to connect` along with an error message `Voicemail Authentication failed! Unable to connect to voicemail. Please contact your administrator`. Also, you know that visual voicemail is not working on other devices at the same site.	Validate that the Cisco Unity Connection server's tomcat-trust certificate has been imported into the Cisco Unified Communications Manager's trust store and the Tomcat service has been restarted since the import occurred.
`Voicemail connection error. Unable to connect.` toast notification appears on the screen when the user navigates to the Voicemail tab of the Cisco Phone app.	Visual voicemail is unable to connect to the Cisco Unity Connection server. Investigate potential connectivity issues between the user's phone and the server.
`This feature has been disabled by your administrator` appears when the user navigates to the Voicemail tab of the Cisco Phone app.	Enable visual voicemail from the Phone Configuration page in Cisco Unified Communications Manager. This error appears only if visual voicemail was enabled previously, and then disabled.

Details available on the phone

You can see some status and details about the phone in the Cisco apps.

This information helps you troubleshoot problems when you are in the same location as your user.

View phone information

The **About phone** setting displays information such as the **Device name**, **Model & hardware**, **Android version**, **Wi-Fi MAC address**, **Bluetooth address**, and **Build number**.

Note To access the **Settings** app from any screen, swipe down on the status bar at the top of the screen and tap the **Settings** gear icon.

Note You can also access the **Settings** app in the launcher screen. Swipe up to open the launcher.

Procedure

Step 1 Access the **Settings** app.

Step 2 Tap **About phone**.

Access phone status and device information

The **Cisco phone status** and **Device information** menus provide information about the device and the connections between the phone and the call control system.

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 Tap **Cisco phone status**.

Step 4 Tap **Device information**.

Access the About option for a Cisco app

The **About** menu option provides information about the app itself, including the version number. You might need to provide this information to the administrator from time to time.

Procedure

Step 1 Tap the desired 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 Tap **About**.

Exit and reenter the Smart Launcher on the phone

When troubleshooting issues on a phone with a Cisco Wireless Phone Configuration Management tool Smart Launcher, you can exit the Smart Launcher to access settings and apps outside of the Smart Launcher.

Before you begin

Get the updated **Local Phone Unlock Password**. The default password to exit the Smart Launcher is **#. Make sure to change this password so you can't exit the Smart Launcher and access more settings or apps.

Procedure

Step 1 To exit the launcher, tap the **Overflow** ••• menu, then tap **Exit Launcher**, and enter the **Local Phone Unlock Password**.

Step 2 To reenter the launcher, swipe up to access more apps, and tap the **Smart Launcher** app.

Note: You can also restart the phone to automatically open the Smart Launcher.

Capture a screenshot on the phone

When troubleshooting, it may be helpful to have a screenshot of the phone.

Note You cannot capture a screenshot while the Smart Launcher is activated.

Procedure

Do one of the following:

- Press the **Power** and **Volume down** buttons at the same time.
- (On Android 13) Swipe up to access the task manager and tap **Screenshot**.
- (On Android 10) Press and hold the **Power** button, and then tap **Screenshot**. A notification briefly pops to the foreground and then appears in the notification drawer.

  Tap the notification to **Share**, **Edit**, or **Delete** the screenshot.

Note Unless you delete a screenshot, you can also locate it in the **Files** app, if available.

Problem report log bundles

If a user experiences a problem with their phone, they may generate a problem report on the phone and send you the log bundle, or you may need to generate a problem report or retrieve the log bundle yourself.

Generate a problem report and log bundle

You generate a problem report and log bundle in the phone.

It may take several minutes to generate the problem report and log bundle. When you tap **Report Problem**, a notification pops to the foreground and then appears in the notification drawer. You know that the report is complete when the phone vibrates twice and the notification disappears.

For release 1.9(0) or later, when you tap **Report Problem**, a screen appears and allows you to report a specific issue type before a notification pops up.

Note For release 1.9(0) or later, the log bundle that is generated also includes a configuration .zip file which contains the configuration for each application in .txt file format.

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** > **Report problem**.

- For release 1.3(0), tap **Report problem**.
- For release 1.9(0), tap **Report problem**.

Step 4 For release 1.9(0), perform the following actions:

a) Select one of the following issue types:

- Telephony call (dropper, other)
- Audio quality
- Battery
- Other

b) Enter the user comment. (Optional)
c) Select the date and time of the issue ocurred.
d) Tap **Submit**.

Retrieve problem report log bundles

Log bundles include the phone's MAC address, a timestamp, and the string **LogBundle** in the filename.

Before you begin

Get a detailed description and approximate time of the issue from the phone user.

To retrieve log bundles from the phone, you must first enable **Web Access** through the Cisco Unified Communications Manager Vendor Specific Option.

To retrieve log bundles from a problem report upload URL server, you must first define the problem report upload URL in the phone's Cisco Unified Communications Manager Vendor Specific Configuration Layout fields.

Note The problem report upload URL server must support file uploads using php.

Procedure

Choose one of these options:

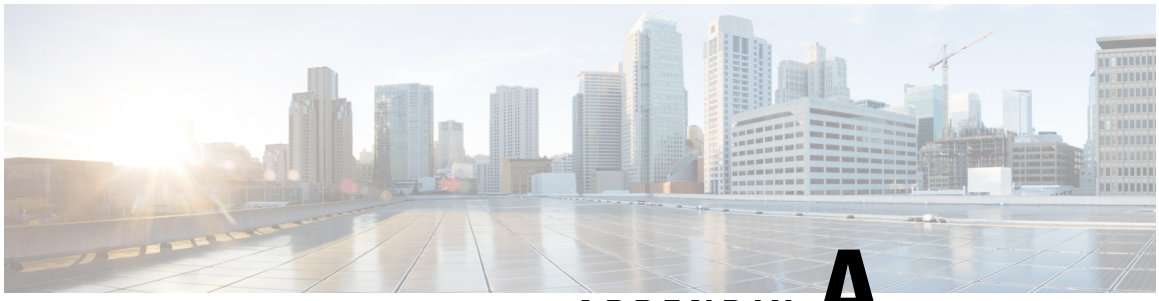
- Download, or ask the user to download the log bundle from the phone web browser **Device Logs** tab.

Note The log bundles appear at the bottom of the page.

- Locate the log bundle on the problem report upload URL server.



Note To locate the file, it may help to search by MAC address or the string **LogBundle**.



APPENDIX A

Appendix

- InformaCast Advanced Notification Support, on page 193
- CTI-Controlled Support, on page 195
- Android 13 App Permissions, on page 199

InformaCast Advanced Notification Support

Configure and Troubleshoot Informacast

In general, Cisco Wireless Phone 840 or 860 support multicast audio broadcasts, text notifications, and user feedback to the InformaCast server using the XSI APIs. InformaCast can be configured to use HTTP or Cisco Unified Communications Manager JTAPI interfaces to the Cisco Unified Communications Manager.

For more information about Configure and Troubleshoot Informacast, see Configure and Troubleshoot Informacast

Unsupported InformaCast Features

Cisco Wireless Phone 840 or 860 currentlly doesnot support Push to Talk and Quick Page services. Phones subscribed to these services will have no way to activate the service on the device. Cisco Wireless Phone 840 or 860 also does not support One Button Paging, where the QuickPage service is assigned to a Service URL button in the device's Phone Button Template. As the phone does not allow configuration of buttons in the Cisco Unified Communications Manager.

Partially Supported InformaCast Features

Call Aware

Call Aware is primarily used to detect when a 911 emergency call has been dialed, which then triggers an InformaCast broadcast. It can also be used to detect calls to numbers other than 911, monitor calls that have been detected, and record those calls. For example, you could use it to trigger an InformaCast broadcast whenever someone calls the Front Desk, and a supervisor could elect to monitor those calls for quality assurance or record them for review later. Cisco Wireless Phone 840 or 860 does not support monitoring and recording of calls.

Text and Audio Messages using Talk and Listen

InformaCast messages that contain both text and audio can be configured with the option to "Start a phone call with any phones in a recipient group and allow everyone to speak in real time (Talk and Listen)". When

Cisco Wireless Phone 840 or 860 receives one of these messages, the “talk” and “exit” softkeys are not displayed, so the Cisco Wireless Phone 840 or 860 can only listen to other phones that are transmitting audio.

Notes on InformaCast Features

Panic Button

Cisco Wireless Phone 840 or 860 have a red button which by default is configured to be the Emergency button on the device. This function can also be mapped to other device buttons using the Buttons application. Using the Emergency app, you can configure the phone to trigger an alarm or make an emergency call through the CiscoPhone app when the user does either a long press, 2 short presses, or 2 short or one long press of the configured Emergency button. By default, no actions are taken.

InformaCast’s panic button service can be used with or without the configuration of the Emergency app. In the step where the Cisco IP Phone Service is configured on the Cisco Unified Communications Manager (Create an InformaCast XML Service (singlewire.com)), the Cisco IP Phone Service created must be named **InformaCast** (this is not case-sensitive), otherwise the device will not recognize it as a service configured for the Panic button feature, and there will be no way for the user to activate it.

If the Emergency App is enabled, it continues to do what it currently does when the panic button is pressed. If both InformaCast and the Emergency App are being used, the Emergency app should be configured to trigger the alarm after one long press of the button, because if 2 presses are configured, the InformaCast service will be triggered twice. The Red circular on-screen panic button press in the Emergency app will not trigger the InformaCast panic button service.

Other Notes

If the phone is not in an active call, the Cisco Wireless Phone 840 or 860 displays a notification to the user when it receives a broadcast message from InformaCast.

The user can choose to view or ignore the message and stop the multicast audio stream by touching the corresponding button on the notification. If a broadcast contains audio only, this behavior differs from the 8821, which has no way of disabling the audio stream. If the phone is in a call, the multicast audio stream will not be played unless the user elects to play it by clicking on the button in the notification, which will place the existing call on hold.

If the phone is locked, the broadcast message is automatically displayed, and audio is played (if not in a call) without any user interaction. The user still has the ability to stop the audio through the stop button on the displayed message. If the user is in a call while the phone is locked, then ANSWER button in the notification must be clicked to hear the broadcast.

Phone vibration settings set on the InformaCast Broadcast Parameters page are ignored by Cisco Wireless Phone 840 or 860.

Cisco Wireless Phone 840 or 860 behaves as shown in the following table when multiple broadcasts are sent by InformaCast, depending on the configuration of the Enable Message Blending check box on the InformaCast Broadcast Parameters page:

Priority and Arrival Order	Blending Enabled	Blending Disabled
Lower priority broadcast (A) followed by higher priority broadcast (B).	Switches from playing broadcast A to playing broadcast B; once B is over, switches back to playing the rest of A.	Switches from playing broadcast A to playing broadcast B; once B is over, switches back to playing the rest of A.

Priority and Arrival Order	Blending Enabled	Blending Disabled
Broadcast (A) followed by broadcast (B) with the same priority.	Plays A in full, ignores broadcast B.	Plays broadcast A in full, then switches to playing the rest of B.
Higher priority broadcast (A) followed by lower priority broadcast (B).	Plays broadcast A in full, then switches to playing the rest of broadcast B.	Plays broadcast A in full, then switches to playing the rest of broadcast B.

CTI-Controlled Support

Need

InformaCast can use either HTTP or Cisco Unified Communications Manager JTAPI.

Using Cisco Unified Communications Manager JTAPI requires Cisco Unified Communications Manager to say the device supports computer telephony integration (CTI).

The one key feature that is used by InformaCast is XSI object pass thru – see page 276 of the Cisco Unified Communications Manager JTAPI developers guide:

XSI Object Pass Through Applications can pass XML objects through Cisco Unified Communications Manager JTAPI and CTI interfaces to the phone. The XML object can contain display updates, softkey update/enable/disable, and other types of updates on the phone that are available through Cisco IP Phone Services features. This allows applications to access Cisco IP Phone Service capabilities through Cisco Unified Communications Manager JTAPI and CTI interfaces without maintaining independent connections to the phones.

Authentication and Mechanism Sending an HTTP POST request to the phone web server, which requires the phone IP address, performs an object push. The web server parses the request, authorizes the request through the HTTP that is returned to the Cisco Unified Communications Manager, runs the request, and returns an XML response that indicates the success or failure of the request to the application. With XSI, the Cisco IP Phone Services object gets sent directly to the phone by the Skinny Client Control Protocol (SCCP). The phone does not authenticate the request, because the Cisco Unified Communications Manager JTAPI client is trusted and does not require the phone IP address. For more information on actual XML contents, see the Cisco IP Phone Services Application Development Notes.

Discussion

Cisco Wireless Phone 840 or 860 offers limited CTI support and customers can enable and test functionality with Third-party Software that exercises the CTI, but their results maybe limited based on what exact functionality is exercised by the Third-party Software.

SIP Signaling and CTI

The line messaging guide details the kinds of remotecc REFERs we can get from CTI.

The following requests are supported from Cisco Unified Communications Manager to the phone. Details are in the CMCM 8.0 Line Messaging guide (see table on page 78) and CUCM 12 version of the guide on page 125.

Remote cc request	Purpose	Currently supported in CiscoPhone app
initiatecallreq	Triggers endpoint to send an INVITE to Cisco Unified CM. An offhook NOTIFY may precede this INVITE	No
holdretrievereq	Used to resume a held dialog.	No
privacyreq	Used to send shared line privacy setting to the endpoint	Yes
statuslineupdatereq	Used to display a status message on a phone UI	Yes (although we do not display the message passed in this by the CUCM – we use our own logic). Looks like this was put in when we did CUCM conferencing and is used for call pickup Our code is feature state specific and this could come with no context.
playtonereq	Used to play a tone at the device.	Yes – for call pickup. Initially we also would get this with CUCM conferencing, but we changed the implementation method. Our code is feature state specific and this could come with no context.
cfwdallupdate	Used to send call forward all settings to the endpoint for a particular line	Yes, this is how devices learn whether CFA is active when they first register.
datapassthroughreq	Cisco Unified CM uses Data PassThrough Request to pass subelements to features and CTI applications	Yes (new in 1.10 for supporting XSI over JTAPI)
holdreversionreq	The Cisco Unified CM hold reversion feature uses this request to trigger the endpoint to invoke hold reversion on the specified call	No
monitorcallreq	CTI applications use this to request that a phone begin monitoring a call on another phone.	No – but will if we implement silent monitoring
dndrequest	CTI applications use this to request that a phone simulate the user pressing the DND softkey. This toggles the phone DND state from enabled to disabled or from disabled to endabled	No

Remote cc request	Purpose	Currently supported in CiscoPhone app
dndupdate	Cisco Unified CM uses this request to convey DND status and DND option settings when either setting is modified by using the Cisco Unified CM web administrative interface	No
Linekeyupdate	CTI uses this to request the phone to update the Intercom speeddial setting.	No
talkbackreq	CTI applications use this request to initiate Intercom talkback for establishing two-way media.	No
dialdtmfreq	Requests phone to dial the DTMF digit	No. This is only in the 12.5 document

Even if we do not support a particular request, we should still send an appropriate SIP response and a terminating NOTIFY, if necessary.

Part of supporting CTI is also that the phone informs CUCM of various events via remotecc REFER messages. See the table on page 120 of the 12.5 version of the document:

Remotecc request	Feature	Description	Currently supported in CiscoPhone app
softkeyeventmsg	conference	Create a conference	Yes, for CUCM conferencing
softkeyeventmsg	park	Park a call	Yes – note we use parkmonitor, not park. Parkmonitor is not listed in the document.
softkeyeventmsg	conflist	List participants in a conference	No. We use the NOTIFY sent from CUCM. We don’t support the phone pressing the softkey to get it.
softkeyeventmsg	rmlastconf	Remove last participant added to a conference	No
softkeyeventmsg	idivert	Activate immediate diversion feature	Yes

Remotecc request	Feature	Description	Currently supported in CiscoPhone app
softkeyeventmsg	callback	The CallBack feature allows you to receive notification when a busy extension is available to receive calls. You can activate Call Back for a destination phone that is within the same Unified Communications Manager cluster as your phone or on a remote Private Integrated Network Exchange (PINX) over QSIG trunks or QSIG-enabled intercluster trunks.	No
Softkeyeventmsg	Qrt	Quality Reporting Tool	No
Softkeyeventmsg	Select	Allows a call to be locked such that remote devices can't remotely resume a held call.	Yes
Softkeyeventmsg	Unselect	Opposite of Select	Yes
Softkeyeventmsg	Privacy	Toggle privacy status for all lines on the phone	Yes
Linekeyeventmsg		This is how the phone sends line key presses to the CUCM for features that don't have an associated standard SIP primitive in this release. Document mentions privacy, but we support that through softkey press.	No
Datapassthrureq		Send XSI XML key presses to CUCM features and CTI applications	No

For more information, see

jtapi - Cisco Developer

Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager, Release 14 and SUs (upload-large-file.s3.us-east-2.amazonaws.com)

Android 13 App Permissions

With firmware release 2.1(0) for Cisco Wireless Phone 860, the Android OS is upgraded from version 10 to 13. Since Android 13 manages permissions differently, Cisco application permissions must be granted for the CP-860 software to function properly.

If the phone is managed by a Cisco Wireless Phone Configuration Management Utility configuration file, permissions are granted automatically. If the phone is managed by an EMM (Enterprise Mobility Management) solution, you must configure the EMM to grant all necessary permissions in the configuration profile or within the specific application settings. Additionally, location services must be enabled on the Android device.

The table below lists the app and the respective permission.

Application	Permission
Barcode	android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.CALL_PHONE android.permission.POST_NOTIFICATIONS android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE
Battery Life	android.permission.POST_NOTIFICATIONS
Cisco Phone	android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG android.permission.CAMERA android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.RECORD_AUDIO android.permission.CALL_PHONE android.permission.READ_PHONE_STATE android.permission.POST_NOTIFICATIONS android.permission.USE_SIP android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_BACKGROUND_LOCATION Additionally, Android must be configured to allow the use of location services by turning on the Use location setting in Android settings > Location.
Custom Settings	android.permission.BLUETOOTH_CONNECT android.permission.POST_NOTIFICATIONS android.permission.READ_PHONE_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_EXTERNAL_STORAGE
Diagnostics	android.permission.CAMERA android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.BLUETOOTH_SCAN android.permission.BLUETOOTH_CONNECT

Application	Permission
	android.permission.RECORD_AUDIO android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE
Logging	android.permission.READ_PHONE_STATE android.permission.POST_NOTIFICATIONS
Emergency	android.permission.POST_NOTIFICATIONS
Sound Stage	android.permission.POST_NOTIFICATIONS
System Updater	android.permission.READ_PHONE_STATE android.permission.POST_NOTIFICATIONS
Web API	android.permission.ACCESS_FINE_LOCATION android.permission.READ_PHONE_STATE android.permission.POST_NOTIFICATIONS android.permission.ACCESS_COARSE_LOCATION android.permission.CALL_PHONE
AppUrl Buttons PIT Call Quality	(No permission requested)