Phone Features and Setup

Cisco IP Phone User Support

If you are a system 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

Telephone Features

After you add Cisco IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. The following table includes a list of supported telephony features, many of which you can configure by using Cisco Unified Communications Manager Administration.

For information about using most of these features on the phone, see the *Cisco IP Phone 7800 Series User Guide*. See Feature Buttons and Softkeys, on page 17 for a list of features that can be configured as programmable buttons and dedicated softkeys and feature buttons.

When adding features to the phone line keys, you are limited by the number of line keys available. You cannot add more features than the number of line keys on your phone.

Note Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information on accessing and configuring service parameters, see the documentation for your particular Cisco Unified Communications Manager release.

For more information on the functions of a service, select the name of the parameter or the question mark (?) help button in the Product Specific Configuration window.

Feature	Description and More Information
Abbreviated Dialing	Allows users to speed dial a phone number by entering an assigned index code (1-199) on the phone keypad. **Note** You can use Abbreviated Dialing while on-hook or off-hook. Users assign index codes from the Self Care Portal.
Actionable Incoming Call Alert	Provides different options to control the incoming call alerts. You can disable or enable the call alert. You can also activate or deactivate the caller ID display. **Note** Because the Cisco IP Phone 7811 does not have line key, it enables the call alert by default but cannot disable it. See Actionable Incoming Call Alert, Product Specific Configuration, on page 21.
AES 256 Encryption Support for Phones	Enhances security by supporting TLS 1.2 and new ciphers. For more information, see Supported Security Features.
Agent Greeting	Allows an agent to create and update a prerecorded greeting that plays at the beginning of a customer call, before the agent begins the conversation with the caller. The agent can prerecord a single greeting or multiple ones as needed. See Enable Agent Greeting, on page 43.
Any Call Pickup	Allows users to pick up a call on any line in their call pickup group, regardless of how the call was routed to the phone. See call park information in the documentation for your particular Cisco Unified Communications Manager release.
Assisted Directed Call Park	Enables users to park a call by pressing only one button using the Direct Park feature. Administrators must configure a Busy Lamp Field (BLF) Assisted Directed Call Park button. When users press an idle BLF Assisted Directed Call Park button for an active call, the active call is parked at the Direct Park slot associated with the Assisted Directed Call Park button. See the call park information in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Audible Message Waiting Indicator (AMWI)	A stutter tone from the handset, headset, or speakerphone indicates that a user has one or more new voice messages on a line. **Note** The stutter tone is line-specific. You hear it only when using the line with the waiting messages.
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone or the headset. **Note** The Cisco IP Phone 7811 does not support a headset. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Automatic Port Synchronization	Enables the phone to synchronize the PC and SW ports to the same speed and to duplex. Only ports configured for auto negotiate change speeds. See Automatic Port Synchronization, Product Specific Configuration, on page 21.
Auto Pickup	Allows a user to use one-touch pickup functionality for call pickup features. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release.
Always On Mode	Always keeps the DECT connection between the headset and base even when the user is not on a call or playing music. This feature is supported on Cisco Headset 500 Series. See Headset template management in Call Manager for more information.
Barge	Enables a user to barge into a call by establishing the three-way conference call using the built-in conference bridge of the target phone. See “cBarge” in this table.
Block External to External Transfer	Prevents users from transferring an external call to another external number. See call transfer restrictions in the documentation for your particular Cisco Unified Communications Manager release.
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number associated with a speed-dial button on the phone. **Note** The Cisco IP Phone 7811 does not support the feature. See presence information in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Busy Lamp Field (BLF) Pickup	Provides enhancements to BLF speed dial. Allows you to configure a Directory Number (DN) that a user can monitor for incoming calls. When the DN receives an incoming call, the system alerts the monitoring user, who can then pick up the call. **Note** The Cisco IP Phone 7811 does not support the feature. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release..
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available. See call back information in the documentation for your particular Cisco Unified Communications Manager release.
Call Display Restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call. See routing and call display information in the documentation for your particular Cisco Unified Communications Manager release.
Call Forward	Allows users to redirect incoming calls to another number. Call Forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage. See directory number information in the documentation for your particular Cisco Unified Communications Manager release and Customize the Self Care Portal Display.
Call Forward All Loop Breakout	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through.
Call Forward All Loop Prevention	Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing Forward Maximum Hop Count service parameter allows.
Call Forward Configurable Display	Allows specifying information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Call Forward Destination Override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Call Forward Notification	Allows you to configure the information that the user sees when receiving a forwarded call. See Set Up Call Forward Notification, on page 45.

Feature	Description and More Information
Call History for Shared Line	Allows you to view shared line activity in the phone Call History. This feature will: • Log missed calls for a shared line • Log all answered and placed calls for a shared line See Call History Shared Line, Product Specific Configuration, on page 21.
Call Park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system.
Call Pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.
Call Recording	Allows a supervisor to record an active call. The user might hear a recording audible alert tone during a call when it is being recorded. When a call is secured, the security status of the call is displayed as a lock icon on Cisco IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being recorded. **Note** When an active call is being monitored or recorded, the user can receive or place intercom calls; however, if the user places an intercom call, the active call is put on hold, which causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the party whose call is being monitored must resume the call.
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Incoming call information appears on the phone display. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Call Waiting Ring	Provides Call Waiting users with the option of an audible ring instead of the standard beep. Options are Ring, Ring Once, Flash Only, and Beep Only. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Caller ID	Caller identification such as a phone number, name, or other descriptive text appear on the phone display. See routing, call display, and directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Caller ID Blocking	Allows a user to block their phone number or name from phones that have caller identification enabled. See routing and directory number information in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Calling Party Normalization	Calling party normalization presents phone calls to the user with a dialable phone number. Any escape codes are added to the number so that the user can easily connect to the caller again. The dialable number is saved in the call history and can be saved in the Personal Address Book.
CAST for SIP	Establishes communication between the Cisco Unified Video Advantage (CUVA) and the Cisco IP phones to support video on the PC even if the IP phone does not have video capability. The main software supported is Cisco Jabber.
cBarge	Allows a user to join a nonprivate call on a shared phone line. cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features . For more information, refer to the "Barge" chapter, Feature Configuration Guide for Cisco Unified Communications Manager.
Cisco Extension Mobility	Allows users to temporarily access their Cisco IP Phone configuration such as line appearances, services, and speed dials from shared Cisco IP Phone by logging into the Cisco Extension Mobility service on that phone when they log into the Cisco Extension Mobility service on that phone. Cisco Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.
Cisco Extension Mobility Cross Cluster (EMCC)	Enables a user configured in one cluster to log into a Cisco IP Phone in another cluster. Users from a home cluster log into a Cisco IP Phone at a visiting cluster. **Note** Configure Cisco Extension Mobility on Cisco IP Phones before you configure EMCC.
Cisco IP Phone 7811 Support	Provides support for the Cisco IP Phone 7811. The phone does not support headset, display backlight, intercom, AUX Port, programmable feature button, and line keys.
Cisco Sans 2.0 Latin Font Support	Introduces the Cisco Sans 2.0 font for all Latin characters in the Call Display.
Cisco Unified Communications Manager Express (Unified CME) Version Negotiation	The Cisco Unified Communication Manager Express uses a special tag in the information sent to the phone to identify itself. This tag enables the phone to provide services to the user that the switch supports. See: • *Cisco Unified Communications Manager Express System Administrator Guide* • *Cisco Unified Communications Manager Express Interaction*.
Cisco Unified Video Advantage (CUVA)	Allows users to make video calls by using a Cisco IP Phone, a personal computer, and an external video camera. **Note** Configure the Video Capabilities parameter in the Product Specific Configuration Layout section in Phone Configuration. See the Cisco Unified Video Advantage documentation.
Cisco WebDialer	Allows users to make calls from web and desktop applications.

Feature	Description and More Information
Classic Ringtone	Supports narrowband and wideband ringtones. The feature makes the available ringtones common with other Cisco IP Phones. See Custom Phone Ringtones.
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference and Meet Me. Allows a noninitiator in a standard (adhoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line. The Advance Adhoc Conference service parameter, disabled by default in Cisco Unified Communications Manager Administration, allows you to enable these features. **Note** Be sure to inform your users whether these features are activated.
Confidential Access Level (CAL)	Controls whether a call can be completed based on the CAL configuration in the Cisco Unified Communications Manager. When CAL is enabled, the user sees information about the call in a CAL message. The phone displays the CAL message for the duration of the call. If a call fails due to an incompatible CAL, the phone displays a failure message. You set up the failure message that the user sees.
Configurable Energy Efficient Ethernet (EEE) for Port and Switch	Provides a method to control EEE functions on personal computer port and switch port by enabling or disabling EEE. The feature controls both type of ports individually. The default value is Enabled. See Energy Efficient Ethernet for Port and Switch, Product Specific Configuration, on page 21.
Configurable RTP/sRTP Port Range	Provides a configurable port range (2048 to 65535) for Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP). The default RTP and sRTP port range is 16384 to 32764. You configure the RTP and sRTP port range in the SIP Profile. See Set Up RTP/sRTP Port Range, on page 49.
CTI Applications	A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.
Device Invoked Recording	Provides end users with the ability to record their telephone calls via a softkey. In addition administrators may continue to record telephone calls via the CTI User Interface. See Device Invoked Recording, Product Specific Configuration, on page 21.

Feature	Description and More Information
Directed Call Park	Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number. **Note** If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features. See call park information in the documentation for your particular Cisco Unified Communications Manager release.
Disable Line Key Barge	The softkeys are controlled by configuration in the Cisco Unified Communications Manager. The Line Key Barge parameter in the Administration window has the following options: • Default: Press Line Key can conference into the call. • Off: Press Line Key Barge a new call. • Turn on softkey: Press Line Key turns on softkeys configured in remote-in-use and user can conference into the call through cBarge. **Note** The Cisco IP Phone 7811 does not support the feature.
Distinctive Ring	Allows users to hear different ring types depending on whether the call was originated from an internal station or external call coming from a trunk. Internal calls generate one ring, while external calls generate two rings with a very short pause between the rings. No configuration is required. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release.
Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system. When a call is diverted, the line becomes available to make or receive new calls.
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur. When enabled, the user sees the DND icon on their phone screen. If multilevel precedence and preemption (MLPP) is configured and the user receives a precedence call, the phone will ring with a special ringtone. See Set Up Do Not Disturb, on page 43.
EnergyWise	Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings. **Note** The Cisco IP Phone 7811 does not support this feature. See Power Save Plus (EnergyWise), Product Specific Configuration, on page 21 .
Enhanced Secure Extension Mobility Cross Cluster (EMCC)	Improves the Secure Extension Mobility Cross Cluster (EMCC) feature by preserving the network and security configurations on the login phone. By so doing, security policies are maintained, network bandwidth is preserved and network failure is avoided within the visiting cluster (VC).

Feature	Description and More Information
Extension Mobility Size Safe and Feature Safe	With Feature Safe, your phone can use any phone button template that has the same number of line buttons that the phone model supports. Size Safe allows your phone to use any phone button template that is configured on the system.
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. See “Services” in this table.
Headset Sidetone Control	Allows an administrator to set the sidetone level of a wired headset. **Note** The Cisco IP Phone 7811 does not support a headset.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release.
Hold Reversion	Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user. Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if not resumed. A call that triggers Hold Reversion also displays an animated icon in the call bubble. You can configure call focus priority to favor incoming or reverting calls.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.
Hold/Resume	Allows the user to move a connected call from an active state to a held state. • No configuration required unless you want to use Music On Hold. See “Music On Hold” in this table for information. • See “Hold Reversion” in this table.
HTTP Download	Enhances the file download process to the phone to use HTTP by default. If the HTTP download fails, the phone reverts to using the TFTP download.
HTTPS for Phone Services	Increases security by requiring communication using HTTPS. **Note** IP Phones can be HTTPS clients; they cannot be HTTPS servers. See HTTPS for Phone Services, Product Specific Configuration, on page 21.
Hunt Group	Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When the first directory number in the hunt group is busy, the system hunts in a predetermined sequence for the next available directory number in the group and directs the call to that phone. You can have either the hunt group name or the pilot number display on the Incoming Call Alert. See hunt groups and routing plans in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Improve Caller Name and Number Display	Improves the display of caller names and numbers. If the Caller Name is known then the Caller Number is displayed instead of unknown.
Incoming Call Toast Timer	Allows you to set the length of time that an incoming call toast (notification) appears on the phone screen. See Incoming Call Toast Timer, Product Specific Configuration, on page 21 .
Intercom	Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to: • Directly dial a specific intercom extension. • Initiate an intercom call and then prompt the user to enter a valid intercom number. **Note** If your user logs into the same phone on a daily basis using their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile, and assign the phone as the default intercom device for the intercom line. The Cisco IP Phone 7811 does not support this feature.
IPv6-only Support	IPv6-only support is provided in standalone or in configuration with IPv4-only. See Configure Network Settings. For more details about IPv6 deployment, see the IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0.
Jitter Buffer	The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for both audio and video streams.
Join	Allows users to combine two calls that are on one line to create a conference call and remain on thecall. **Note** Because Cisco IP Phone 7811 has only one line, the phone uses the Calls softkey to join two calls in the same line. See Join and Direct Transfer Policy, Product Specific Configuration, on page 21 .
Join Across Lines	Allows users to combine calls that are on multiple phone lines to create a conference call. Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. **Note** Because Cisco IP Phone 7811 has only one line, it does not support this feature. See Join and Direct Transfer Policy, Product Specific Configuration, on page 21 .
Line Display Enhancement	Improves the call display by removing the central dividing line when it is not required. This feature applies to the Cisco IP Phone 7841 only.

Feature	Description and More Information
Line Status for Call Lists	Allows the user to see the Line Status availability status of monitored line numbers in the Call History list. The Line Status states are • Unknown • Idle • Busy • DND See Enable BLF for Call Lists, on page 46.
Line Text Label	Sets a text label for a phone line instead of the directory number. See Set the Label for a Line, on page 55.
Log out of hunt groups	Allows users to log out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent nonhunt group calls from ringing their phone. See hunt group information in the documentation for your particular Cisco Unified Communications Manager release and Set Up Softkey Template, on page 57.
Malicious Caller Identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.
Meet Me Conference	Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time.
Message Waiting	Defines directory numbers for message waiting on and off indicators. A directly-connected voice-message system uses the specified directory number to set or to clear a message waiting indication for a particular Cisco IP Phone. See message waiting and voicemail information in the documentation for your particular Cisco Unified Communications Manager release.
Message Waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages. See message waiting and voicemail information in the documentation for your particular Cisco Unified Communications Manager release.
Minimum Ring Volume	Sets a minimum ringer volume level for an IP phone. See Minimum Ring Volume, Product Specific Configuration, on page 21 .
Missed Call Logging	Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance. See directory information in the documentation for your particular Cisco Unified Communications Manager release.
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desk phone and a remote device such as a mobile phone. Users can restrict the group of callers according to phone number and time of day.

Feature	Description and More Information
Mobile and Remote Access Through Expressway	Allows remote workers to easily and securely connect into the corporate network without using a virtual private network (VPN) client tunnel. See Mobile and Remote Access Through Expressway, on page 50.
Mobile Voice Access	Extends Mobile Connect capabilities by allowing users to access an interactive voice response (IVR) system to originate a call from a remote device such as a cellular phone.
Monitoring and Recording	Allows a supervisor to silently monitor an active call. The supervisor cannot be heard by either party on the call. The user might hear a monitoring audible alert tone during a call when it is being monitored. When a call is secured, the security status of the call is displayed as a lock icon on Cisco IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being monitored. **Note** When an active call is being monitored or recorded, the use can receive or place intercom calls; however, if the user place an intercom call, the active call will be put on hold, which causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the party whose call is being monitored must resume the call. See Set Up Monitoring and Recording, on page 44.
Multilevel Precedence and Preemption	Enables the user to make and receive urgent or critical calls in some specialized environments, such as military or government offices. See Multilevel Precedence and Preemption, on page 57.
Multiple Calls Per Line Appearance	Each line can support multiple calls. By default, the phone supports two active calls per line, and a maximum of six active calls per line. Only one call can be connected at any time; other calls are automatically placed on hold. The system allows you to configure maximum calls/busy trigger not more than 6/6. Any configuration more than 6/6 is not officially supported. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Music On Hold	Plays music while callers are on hold.
Mute	Mutes the handset or headset microphone.
New Phone Hardware	Provides updated hardware versions of the Cisco IP Phone 7821, 7841, and 7861. The new phones do not support firmware releases prior to 10.3(1).
No Alert Name	Makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The call appears as an Alert Call followed by the caller's telephone number.
Onhook Dialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset or press Dial.

Feature	Description and More Information
Other Group Pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group. See call pickup information in the documentation for your particular Cisco Unified Communications Manager release.
Outbound Roll Over	Allows users to make a call when the number of calls for a line exceeds the maximum number of calls (MNC). This feature is configured on Cisco Unified Communication Manager by navigating **Device > Phone**. It is disabled by default. **Note** The Cisco IP Phone 7811 does not support this feature.
Pause in Speed Dial	Users can set up the speed-dial feature to reach destinations that require Forced Authorization Code (FAC) or Client Matter Code (CMC), dialing pauses, and additional digits (such as a user extension, a meeting access code, or a voicemail password) without manual intervention. When the user presses the speed dial, the phone establishes the call to the specified DN and sends the specified FAC, CMC, and DTMF digits to the destination and inserts the necessary dialing pauses.
Peer Firmware Sharing	Provides the following advantages in high-speed campus LAN settings: • Limits congestion on TFTP transfers to centralized remote TFTP servers • Eliminates the need to manually control firmware upgrades • Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously Peer Firmware Sharing may also aid in firmware upgrades in branch/remote office deployment scenarios that run over bandwidth-limited WAN links. See Peer Firmware Sharing, Product Specific Configuration, on page 21 .
Phone Display Message for Extension Mobility Users	This feature enhances the phone interface for the Extension Mobility user by providing friendly messages.
PLK Support for Queue Statistics	The PLK Support for Queue Statistics feature enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen. **Note** The Cisco IP Phone 7811 does not support this feature. See Set Up Softkey Template, on page 57.
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a plus (+) sign. To dial the + sign, the user needs to press and hold the star (*) key for at least 1 second. This applies to dialing the first digit for an on-hook (including edit mode) or off-hook call.

Feature	Description and More Information
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone display about the call of the other user. **Note** The Cisco IP Phone 7811 does not support privacy. See barge information in the documentation for your particular Cisco Unified Communications Manager release.
Private Line Automated Ringdown (PLAR)	The Cisco Unified Communications Manager administrator can configure a phone number that the Cisco IP Phone dials as soon as the handset goes off hook. This can be useful for phones that are designated for calling emergency or “hotline” numbers. The administrator can configure a delay of up to 15-seconds. This allows the user time to place a call before the phone defaults to the hotline number. The timer is configurable through the parameter **Off Hook To First Digit Timer** under **Device** > **Device Settings** > **SIP Profile**. For more information, refer to *Feature Configuration Guide for Cisco Unified Communications Manager*. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.
Problem Report Tool (PRT)	Submit phone logs or report problems to an administrator. See Problem Report Tool, on page 54.
Programmable Feature Buttons	You can assign features, such as New Call, Call Back, and Forward All to line buttons. **Note** The Cisco IP Phone 7811 does not support this feature. See phone button templates in the documentation for your particular Cisco Unified Communications Manager release.
Quality Reporting Tool (QRT)	Allows users to submit information about problem phone calls by pressing a button. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.
Recents	Allows you to enable/disable the Recents softkey on a phone.
Redial	Allows users to call the most recently dialed phone number by pressing a button or the Redial softkey.
Reroute Direct Calls to Remote Destination to Enterprise Number	Reroutes a direct call to a user's mobile phone to the enterprise number (desk phone). For an incoming call to remote destination (mobile phone), only remote destination rings; desk phone does not ring. When the call is answered on their mobile phone, the desk phone displays a Remote In Use message. During these calls, users can make use of various features of their mobile phone. See Cisco Unified Mobility information in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Remote Port Configuration	Allows you to configure the speed and duplex function of the phone Ethernet ports remotely by using Cisco Unified Communications Manager Administration. This enhances the performance for large deployments with specific port settings. **Note** If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed on the phone. See Remote Port Configuration, Product Specific Configuration, on page 21 .
Ringtone Setting	Identifies ring type used for a line when a phone has another active call. See directory number information in the documentation for your particular Cisco Unified Communications Manager release and Custom Phone Ringtones.
RTCP Hold For SIP	Ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.
Secure Conference	Allows secure phones to place conference calls using a secured conference bridge. As new participants are added by using Confrn, Join, cBarge softkeys or MeetMe conferencing, the secure call icon displays as long as all participants use secure phones. The Conference List displays the security level of each conference participant. Initiators can remove nonsecure participants from the Conference List. Noninitiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set. See conference information in the documentation for your particular Cisco Unified Communications Manager release and Supported Security Features
Secure EMCC	Improves the EMCC feature by providing enhanced security for a user logging into their phone from a remote office.
Services	Allows you to use the Cisco IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe.
Services URL button	Allows users to access services from a programmable button rather than by using the Services menu on a phone. **Note** The Cisco IP Phone 7811 does not support this feature.
Serviceability for SIP Endpoints	Enables administrators to quickly and easily gather debug information from phones. This feature uses SSH to remotely access each IP phone. SSH must be enabled on each phone for this feature to function.
Shared Line	Allows a user with multiple phones to share the same phone number or allows a user to share a phone number with a coworker. See directory number information in the documentation for your particular Cisco Unified Communications Manager release.

Feature	Description and More Information
Show Calling ID and Calling Number	The phones can display both the calling ID and calling number for incoming calls. The IP phone LCD display size limits the length of the calling ID and the calling number that display. The Show Calling ID and Calling Number feature applies to the incoming call alert only and does not change the function of the Call Forward and Hunt Group features. See “Caller ID” in this table.
Show Duration for Call History	Displays the time duration of placed and received calls in the Call History details. If the duration is greater than or equal to one hour, the time is displayed in the Hour, Minute, Second (HH:MM:SS) format. If the duration is less than one hour, the time is displayed in the Minute, Second (MM:SS) format. If the duration is less than one minute, the time is displayed in the Second (SS) format.
Simplify Extension Mobility Login with Cisco Headsets	Enables users to sign into Extension Mobility with their Cisco headsets. When the phone is in Mobile and Remote Access through Expressway (MRA) mode, the user can use the headset to sign into the phone Headset login with MRA requires Cisco Unified Communications Manager(UCM) Release 11.5(1)SU8,11.5(1)SU.9, 12.5(1)SU3 or later.
Speed Dial	Dials a specified number that has been previously stored.
SSH Access	Allows you to enable or disable the SSH Access setting using Cisco Unified Communications Manager Administration. Enabling the SSH server allows the phone to accept the SSH connections. Disabling the SSH server functionality of the phone blocks the SSH access to the phone. See SSH Access, Product Specific Configuration, on page 21 .
Time-of-Day Routing	Restricts access to specified telephony features by time period. See time and date information in the documentation for your particular Cisco Unified Communications Manager release.
Time Zone Update	Updates the Cisco IP Phone with time zone changes. See time and date information in the documentation for your particular Cisco Unified Communications Manager release..
Transfer	Allows users to redirect connected calls from their phones to another number. Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. See Join and Direct Transfer Policy, Product Specific Configuration, on page 21 .

Feature	Description and More Information
TVS	Trust Verification Services (TVS) enables phones to authenticate signed configurations and authenticate other servers or peers without increasing the size of the Certificate Trust List (CTL) or requiring the downloading of an updated CTL file to the phone. TVS is enabled by default. The Security Setting menu on the phone displays the TVS information.
UCR 2008	The Cisco IP Phones support Unified Capabilities Requirements (UCR) 2008 by providing the following functions: • Support for Federal Information Processing Standard(FIPS) • Support for 80-bit SRTCP Tagging As an IP Phone administrator, you must set up specific parameters in Cisco Unified Communications Manager Administration. See UCR 2008 Setup, on page 46.
Voice Message System	Enables callers to leave messages if calls are unanswered.
Web Access Disabled by Default	Enhances security by disabling access to all web services, such as HTTP. Users can only access web services if you enable web access. See UCR 2008 Setup, on page 46.
Whisper Announcement	Plays a brief, prerecorded message to an agent just before the agent connects with each caller. The announcement plays only to the agent; the caller hears ringing (based on existing ring tone patterns) while the announcement plays. The content of the announcement can contain information about the caller that helps prepare the agent to handle the call. The information can include caller language preference, choices the caller made from a menu (Sales, Service), customer status (Platinum, Gold, Regular), and so on.
Whisper Coaching	An enhancement to silent call monitoring feature that allows supervisors to talk to agents during a monitoring session. This feature provides applications the ability to change the current monitoring mode of a monitoring call from Silent Monitoring to Whisper Coaching and vice versa.

Related Topics

Cisco Unified Communications Manager Documentation

Feature Buttons and Softkeys

The following table provides information about features that are available on softkeys, features that are available on dedicated feature buttons, and features that you need to configure as programmable feature buttons. A “Supported” entry in the table indicates that the feature is supported for the corresponding button type or softkey. Of the two button types and softkeys, only programmable feature buttons require configuration in Cisco IP Phone administration.

Note The Cisco IP Phone 7811 does not have programmable feature buttons.

For information about configuring programmable feature buttons, see Phone Button Templates, on page 59.

Table 1: Features with Corresponding Buttons and Softkeys

Feature Name	Dedicated Feature Button	Programmable Feature Button	Softkey
Answer		Supported	Supported
Barge			Supported
Call Back		Supported	Supported
Call Forward All		Supported	Supported
Call Park		Supported	Supported
Call Park Line Status		Supported	
Call Pickup (Pick Up)		Supported	Supported
Call Pickup Line Status		Supported	
Conference	Supported		Supported (only displayed during connected call conference scenario)
Divert			Supported
Do Not Disturb		Supported	Supported
Executive - Access to **Settings** > **Assistant** menu		Supported	
Executive Assistant - Access to **Settings** > **Executive** menu		Supported	
Group Pickup (Group Pick Up)		Supported	Supported
Hold	Supported		Supported
Hunt Groups		Supported	Supported
Intercom		Supported	
Malicious Call Identification (MCID)		Supported	Supported
Meet Me		Supported	Supported
Mobile Connect (Mobility)		Supported	Supported

Feature Name	Dedicated Feature Button	Programmable Feature Button	Softkey
Mute	Supported		
Other Pickup		Supported	Supported
Privacy		Supported	
Queue Status		Supported	
Quality Reporting Tool (QRT)		Supported	Supported
Record	Not supported	Not supported	Supported
Redial		Supported	Supported
Speed Dial		Supported	Supported
Speed Dial Line Status		Supported	
Transfer	Supported		Supported (only displayed during connected call transfer scenario)

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

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

Table 2: Product Specific Configuration Fields

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Disable Speakerphone	Checkbox	Unchecked	Turns off the speakerphone capability of the phone.
Disable Speakerphone and Headset	Checkbox	Unchecked	Turns off the speakerphone and headset capability of the phone.
Disable Handset	Checkbox	Unchecked	Turns off the handset capability of the phone.
PC Port	Disabled Enabled	Enabled	Controls the ability to use the PC port to connect a computer into the LAN.
Settings Access	Disabled Enabled Restricted	Enabled	Enables, disables, or restricts access to local phone configuration settings in the Settings app. • Disabled—The Settings menu does not display any options. • Enabled—All entries in the Settings menu are accessible. • Restricted—Only the Phone settings menu is accessible.
Gratuitous ARP	Disabled Enabled	Disabled	Enables or disables the ability for the phone to learn MAC addresses from Gratuitous ARP. This capability is required to monitor or record voice streams.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
PC Voice VLAN Access	Disabled Enabled	Enabled	Indicates whether the phone will allow a device attached to the PC (access) port to access the Voice VLAN. • Disabled—The computer can't send and receive data on the Voice VLAN or from the phone. • Enabled—The computer can send and receive data from the Voice VLAN or from the phone. Set this field to Enabled if an application is being run on the computer that to monitor phone traffic. These applications could include monitoring and recording applications, and the use of network monitoring software for analysis purposes.
Video Capabilities	Disabled Enabled	Disabled	Allows users to make video calls by using a Cisco IP Phone, a personal computer, and a video camera.
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.
Disable TLS 1.0 and TLS 1.1 for Web Access	Disabled Enabled	Disabled	Controls the use of TLS 1.2 for a web server connection. • Disabled—A phone configured for TLS1.0, TLS 1.1, or TLS1.2 can function as a HTTPs server. • Enabled—Only a phone configured for TLS1.2 can function as a HTTPs server.
Enbloc Dialing	Disabled Enabled	Disabled	Controls the dialing method. • Disabled—The Cisco Unified Communications Manager waits for the interdigit timer to expire when there is a dial plan or route pattern overlap. • Enabled—The entire dialed string is sent to Cisco Unified Communications Manager once the dialing is complete. To avoid the T.302 timer timeout, we recommend that you enable Enbloc Dialing whenever there is a dialplan or route pattern overlap. Forced Authorization Codes (FAC) or Client Matter Codes (CMC) do not support the Enbloc Dialing. If you use FAC or CMC to manage call access and accounting, then you cannot use this feature.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Days Backlight Not Active	Days of the week		Defines the days that the backlight does not turn on automatically at the time specified in the Backlight On Time field. Choose the day or days from the drop-down list. To choose more than one day, **Ctrl+click** each day that you want.
Backlight On Time	hh:mm		Defines the time each day that the backlight turns on automatically (except on the days specified in the Backlight Display Not Active field). Enter the time in this field in 24 hour format, where 0:00 is midnight. For example, to automatically turn the backlight on at 07:00 a.m. (0700), enter 07:00. To turn the backlight on at 02:00 p.m. (1400), enter 14:00. If this field is blank, the backlight automatically turns on at 0:00.
Backlight On Duration	hh:mm		Defines the length of time that the backlight remains on after turning on at the time specified in the Backlight On Time field. For example, to keep the backlight on for 4 hours and 30 minutes after it turns on automatically, enter 04:30. If this field is blank, the phone turns off at the end of the day (0:00). If Backlight On Time is 0:00 and the backlight on duration is blank (or 24:00), the backlight does not turn off.
Backlight Idle Timeout	hh:mm		Defines the length of time that the phone is idle before the backlight turns off. Applies only when the backlight was off as scheduled and was turned on by a user (by pressing a button on the phone or lifting the handset). For example, to turn the backlight off when the phone is idle for 1 hour and 30 minutes after a user turns the backlight on, enter 01:30.
Backlight On When Incoming Call	Disabled Enabled	Enabled	Turns the backlight on when there is an incoming call.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Enable Power Save Plus	Days of the week		Defines the schedule of days for which the phone powers off. Choose the day or days from the drop-down list. To choose more than one day, **Ctrl+click** each day that you want. When Enable Power Save Plus is turned on, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.
Phone On Time	hh:mm		Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 07:00 a.m. (0700), enter 07:00. To power up the phone at 02:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 07:00, the Phone On Time must be no earlier than 07:20.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Phone Off Time	hh:mm		Defines the time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20. For more information, see Set Up Idle Display.
Phone Off Idle Timeout	hh:mm		Indicates the length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the Select key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use.
Enable Audible Alert	Checkbox	Unchecked	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. This check box applies only if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	Up to 127 characters		Identifies the EnergyWise domain that the phone is in.
EnergyWise Secret	Up to 127 characters		Identifies the security secret password that is used to communicate with the endpoints in the EnergyWise domain.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Allow EnergyWise Overrides	Check box	Unchecked	Determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply: • One or more days must be selected in the Enable Power Save Plus field. • The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override. For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected. • If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Cisco Unified Communications Manager Administration. • To change the power level on the phone again, EnergyWise must reissue a new power level change command. To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.
Join and Direct Transfer Policy	Same line, across line enable Same line enable only Same line, across line disable	Same line, across line enable	Controls the ability of a user to join and transfer calls. • Same line, across line enable—Users can directly transfer or join a call on current line to another call on another line. • Same line enable only—Users can only directly transfer or join the calls when both calls are on same line. • Same line, across line disable— Users can't join or transfer calls on the same line. The join and transfer features are disabled and the user can't do the direct transfer or join function.
Span to PC Port	Disabled Enabled	Disabled	Indicates whether the phone forwards packets that are transmitted and received on the network port to the access port.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Logging Display	Disabled Enabled PC Controlled	Disabled	Selects what type of console logging is allowed. This option does not control the generation of logs—just whether the logs display. • Disabled—Indicates that logging doesn't display to the console, nor to the connected downstream port. • Enabled—Indicates that logs are always sent to the console and to the downstream port. Use Enabled to force logs on, so they can be captured with a packet sniffer. • PC Controlled—Indicates that the workstation attached to the PC port controls whether logging is enabled.
Recording Tone	Disabled Enabled	Disabled	Controls the playing of the tone when a user is recording a call.
Recording Tone Local Volume	Integer 0–100	100	Controls the volume of the recording tone to the local user.
Recording Tone Remote Volume	Integer 0–100	50	Controls the volume of the recording tone to the remote user.
Recording Tone Duration	Integer 1–3000 milliseconds		Controls the duration of the recording tone.
"more" Soft Key Timer	Integer 0, 5–30 seconds	5	Controls the duration that a row of secondary softkeys is displayed before the phone displays the initial set of softkeys. 0 disables the timer.
Log Server	String of up to 256 characters		Identifies the IPv4 syslog server for phone debug output. The format for the address is: **`address:<port>@@base=<0-7>;pfs=<0-1>`**
Remote Log	Disabled Enabled	Disabled	Controls the ability to send logs to the syslog server.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Log Profile	Default Preset Telephony SIP UI Network Media Upgrade Accessory Security Wi-Fi VPN Energywise MobileRemoteAc	Preset	Specifies the predefined logging profile. • Default—Default debug logging level • Preset—Does not overwrite the phone local debug logging setting • Telephony—Logs information about Telephony or call features • SIP—Logs information about SIP signaling • UI—Logs information about the phone user interface • Network—Logs network information • Media—Logs media information • Upgrade—Logs upgrade information • Accessory—Logs accessory information • Security—Logs security information • Wi-Fi—Logs Wi-Fi information • VPN—Logs virtual private network information • Energywise—Logs energy-savings information • MobileRemoteAC—Logs Mobile and Remote Access through Expressway information
IPv6 Log Server	String of up to 256 characters		Identifies the IPv6 syslog server for phone debug output. The format for the address is: `[address]:<port>@@base=<0-7>;pfs=<0-1>`
Outbound Rollover	Disabled Enabled	Disabled	Allows users to make a call when the number of calls for a line exceeds the maximum number of calls (MNC). The Cisco IP Phone 7811 does not support this field.
Cisco Discovery Protocol (CDP): Switch Port	Disabled Enabled	Enabled	Controls Cisco Discovery Protocol on the SW port of the phone.
Cisco Discovery Protocol (CDP): PC Port	Disabled Enabled	Enabled	Controls Cisco Discovery Protocol on the PC port of the phone.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP_MED): Switch Port	Disabled Enabled	Enabled	Enables LLDP-MED on the SW port.
Link Layer Discovery Protocol (LLDP): PC Port	Disabled Enabled	Enabled	Enables LLDP on the PC port.
LLDP Asset ID	String, up to 32 characters		Identifies the asset ID that is assigned to the phone for inventory management.
LLDP Power Priority	Unknown Low High Critical	Unknown	Assigns a phone power priority to the switch, thus enabling the switch to appropriately provide power to the phones.
802.1x Authentication	User Controlled Disabled Enabled	User Controlled	Specifies the 802.1x authentication feature status. • User Controlled—The user can configure the 802.1x on the phone. • Disabled—802.1x authentication is not used. • Enabled—802.1x authentication is used, and you configure the authentication for the phones.
Automatic Port Synchronization	Disabled Enabled	Disabled	Synchronizes ports to the lowest speed between ports of a phone to eliminate packet loss.
Switch Port Remote Configuration	Disabled Enabled	Disabled	Allows you to configure the speed and duplex function of the phone SW port remotely. This enhances the performance for large deployments with specific port settings. If the SW ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed on the phone.
PC Port Remote Configuration	Disabled Enabled	Disabled	Allows you to configure the speed and duplex function of the phone PC port remotely. This enhances the performance for large deployments with specific port settings. If the ports are configured for Remote Port Configuration in Cisco Unified Communications Manager, the data cannot be changed on the phone.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
SSH Access	Disabled Enabled	Disabled	Controls the access to the SSH daemon through port 22. Leaving port 22 open leaves the phone vulnerable to Denial of Service (DoS) attacks.
Incoming Call Toast Timer	Integer 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60 seconds	5	Gives the time, in seconds, that the toast displays. The time includes the fade-in and fade-out times for the window.
Line Key Barge	cBarge Turn on Softkey Barge Off	cBarge	Controls the ability for a user to join a nonprivate call on a shared phone line. • cBarge—Enables a user to add another person to a call. The call automatically converts to a conference, allowing the user and other parties to access conference features. • Turn on Softkey—Enables a user to conference into a call on a shared line using cBarge. • Barge—Enables a user to add another user to a call but does not convert the call into a conference. • Off—Disables barge. A new call initiates when the user presses the line key.
Ring Locale	Default Japan	Default	Controls the ringing pattern.
TLS Resumption Timer	Integer 0–3600 seconds	3600	Controls the ability to resume a TLS session without repeating the entire TLS authentication process. If the field is set to 0, then the TLS session resumption is disabled.
FIPS Mode	Disabled Enabled	Disabled	Enables or disables the Federal Information Processing Standards (FIPS) mode on the phone.
HOLD/RESUME Key	HOLD/RESUME Key HOLD Key	HOLD/RESUME Key	Controls the text for the **Hold** softkey. • HOLD/RESUME Key—The softkey displays **Hold/Resume**. • HOLD Key—The softkey displays **Hold**.
Record Call Log from Shared Line	Disabled Enabled	Disabled	Specifies whether to record a shared line call in the call log.
Minimum Ring Volume	0-Silent Volume level 1–15	0-Silent	Controls the minimum ring volume for the phone. You can set a phone so that the ringer cannot be turned off.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Peer Firmware Sharing	Disabled Enabled	Enabled	Allows the phone to find other phones of the same model on the subnet and share updated firmware files. If the phone has a new firmware load, it can share that load with the other phones. If one of the other phones has a new firmware load, the phone can download the firmware from the other phone, instead of from the TFTP server. Peer firmware sharing: • Limits congestion on TFTP transfers to centralized remove TFTP servers. • Eliminates the need to manually control firmware upgrades. • Reduces phone downtime during upgrades when large numbers of phones are reset simultaneously. • Helps with firmware upgrades in branch or remote office deployment scenarios that run over bandwidth-limited WAN links.
Load Server	String of up to 256 characters		Identifies the alternate IPv4 server that the phone uses to obtain firmware loads and upgrades. The format for the address is: **address:<port>@@base=<0-7>;pfs=<0-1>**
IPv6 Load Server	String of up to 256 characters		Identifies the alternate IPv6-only server that the phone uses to obtain firmware loads and upgrades. The format for the address is: **[address]:<port>@@base=<0-7>;pfs=<0-1>**
Wideband Headset UI Control	Disabled Enabled	Enabled	Allows the user to use the wideband codec for an analog headset.
Wideband Headset	Disabled Enabled	Enabled	Enables or disables the use of a Wideband Headset on the phone. Used in conjunction with User Control Wideband Headset. For more information, see Set Up Wideband Codec

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
Detect Unified CM Connection Failure	Normal Delayed	Normal	Determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM), which is the first step before device failover to a backup Unified CM/SRST occurs. • Normal—Detection of a Unified CM connection failure occurs at the standard system rate. Choose this value for faster recognition of a Unified CM connection failure. • Delayed—Detection of a Unified CM connection failover occurs approximately four times slower than Normal. Choose this value if you prefer failover to be delayed slightly to give the connection the opportunity to reestablish The precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing.
Special Requirement ID	String		Controls custom features from Engineering Special (ES) loads.
Console Access	Disabled Enabled	Disabled	Specifies whether the serial console is enabled or disabled.
Actionable Incoming Call Alert	Disabled Show for all Incoming Call Show for Invisible Incoming Call	Show for all Incoming Call	Controls the type of incoming call alert that displays on the phone screen. • Disabled—The actionable incoming call alert is disabled and the user sees the traditional incoming call pop-up alert. • Show for all Incoming Call—The actionable incoming call alert displays for all calls regardless of visibility. • Show for Invisible Incoming Call—The actionable incoming call alert displays for calls not shown on the phone. This parameter behaves similarly to the incoming call alert pop-up notification.
Energy Efficient Ethernet(EEE): PC Port	Disabled Enabled	Disabled	Controls EEE on the PC port.
Energy Efficient Ethernet(EEE): SW Port	Disabled Enabled	Disabled	Controls EEE on the SW port.

Field Name	Field Type or Choices	Default	Description and Usage Guidelines
User Credentials Persist for Expressway Sign in	Disabled Enabled	Disabled	Controls if the phone stores the user's sign-in credentials. When disabled, the user always sees the prompt to sign into the Expressway server for Mobile and Remote Access (MRA). If you would like to make it easier for users to log in, you enable this field so that the Expressway login credentials are persistent. The user then only has to enter their login credentials the first time. Any time after that (when the phone is powered on off-premise), the login information is prepopulated on the Sign-in screen. For more information, see the Mobile and Remote Access Through Expressway, on page 50.
HTPS Server	HTTP and HTTPS enabled HTTPS only	HTTP and HTTPS enabled	Controls the type of communication to the phone. If you select HTTPS only, phone communication is more secure.
Customer support upload URL	String, up to 256 characters		Provides the URL for the Problem Report Tool (PRT). If you deploy devices with Mobile and Remote Access through Expressway, you must also add the PRT server address to the HTTP Server Allow list on the Expressway server. For more information, see the Mobile and Remote Access Through Expressway, on page 50.
Recents Softkey	Disabled Enabled	Enabled	Controls the display of the Recents softkey on the phone.
Admin Configurable Ringer	Disabled Chirp1 Chirp2	Disabled	Controls the ringtone and the ability for users to set the ringtone. • When set to **`Disabled`**, users can configure the default ringtone on their phones. • For all other values, users cannot change the ringtone. The **Set** softkey does not display in the **Ringtone** menu.
Customer Support Use			Reserved for Cisco TAC.
Disable TLS Ciphers	See Disable Transport Layer Security Ciphers, on page 35.	None	Disables the selected TLS cipher. Disable more than one cipher suite by selecting and holding the **Ctrl** key on your computer keyboard.

Note Codec negotiation involves two steps:

1. The phone advertises the supported codec to the Cisco Unified Communications Manager. Not all endpoints support the same set of codecs.
2. When the Cisco Unified Communications Manager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly supported codec based on various factors, including the region pair setting.

Feature Configuration Best Practices

You can set up the phone features to suit your users' needs. But we have some recommendations for certain situations and deployments that might help you.

High Call Volume Environments

In a high call volume environment, we recommend that you set up some features in a specific way.

Field	Administration Area	Recommended Setting
Always Use Prime Line	Device Information	Off or On For more information, see Field: Always Use Prime Line, on page 35.
Actionable Incoming Call Alert	Product Specific Configuration Layout	Show for all Incoming Call
Show All Calls on Primary Line	Product Specific Configuration Layout	Enabled
Revert to All Calls	Product Specific Configuration Layout	Enabled

Multiline Environments

In a multiline environment, we recommend that you set up some features in a specific way.

Field	Administration Area	Recommended Setting
Always Use Prime Line	Device Information	Off For more information, see Field: Always Use Prime Line, on page 35.
Actionable Incoming Call Alert	Product Specific Configuration Layout	Show for all Incoming Call

Field	Administration Area	Recommended Setting
Show All Calls on Primary Line	Product Specific Configuration Layout	Enabled
Revert to All Calls	Product Specific Configuration Layout	Enabled

Field: Always Use Prime Line

This field specifies whether the primary line on an IP phone is chosen when a user goes off-hook. If this parameter is set to True, when a phone goes off-hook, the primary line is chosen and becomes the active line. Even if a call rings on the second line of the user, when the phone goes off-hook, it makes only the first line active. It does not answer the inbound call on the second line. In this case, the user must choose the second line to answer the call. The default value is set to False.

The purpose of the Always Use Prime Line field is very similar to the combination of Show All Calls on the Primary Line and Revert to All Calls when both of those two features are enabled. However, the main difference is that when Always Use Prime Line is enabled, inbound calls are not answered on the second line. Only dial tone is heard on the prime line. There are certain high call volume environments where this is the desired user experience. In general, it is best to leave this field disabled except for high call volume environments that require this feature.

Disable Transport Layer Security Ciphers

You can disable Transport Layer Security (TLS) ciphers with the **Disable TLS Ciphers** parameter. This allows you to tailor your security for known vulnerabilities, and to align your network with your company's policies for ciphers.

None is the default setting.

Disable more than one cipher suite by selecting and holding the **Ctrl** key on your computer keyboard. If you select all of the phone ciphers, then phone TLS service is impacted. Your choices are:

- None
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

For more information about phone security, see *Cisco IP Phone 7800 and 8800 Series Security Overview White Paper* (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html).

Enable Call History for Shared Line

Allows you to view your shared line activity in the Call History. This feature:

- Logs missed calls for a shared line.
- Logs all answered and placed calls for a shared line.

Before you begin

Disable Privacy before you enable Call History for Shared Line. Otherwise Call History doesn't display the calls other users answer.

Procedure

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

Step 2 Locate the phone to be configured.

Step 3 Navigate to the Record Call Log from Shared Line drop-down in the Product Specific Configuration area.

Step 4 Select **Enabled** from the drop-down list.

Step 5 Select **Save**.

Schedule Power Save for Cisco IP Phone

To conserve power and ensure the longevity of the phone screen display, you can set the display to turn off when it is not needed.

You can configure settings in Cisco Unified Communications Manager Administration to turn off the display at a designated time on some days and all day on other days. For example, you may choose to turn off the display after business hours on weekdays and all day on Saturdays and Sundays.

Note The Cisco IP Phone 7811 does not support Power Save.

You can take any of these actions to turn on the display any time it is off:

- Press any button on the phone.

  The phone takes the action designated by that button in addition to turning on the display.
- Lift the handset.

When you turn the display on, it remains on until the phone has remained idle for a designated length of time, then it turns off automatically.

For more information, see Product Specific Configuration, on page 21

Procedure

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

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

Step 3 Navigate to the Product Specific Configuration area and set the following fields:

- Days Display Not Active
- Display On Time
- Display On Duration
- Display Idle Timeout

Table 3: PowerSave Configuration Fields

Field	Description
Days Display Not Active	Days that the display does not turn on automatically at the time specified in the Display On Time field. Choose the day or days from the drop-down list. To choose more than one day, Ctrl-click each day that you want.
Display On Time	Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field). Enter the time in this field in 24-hour format, where 0:00 is midnight. For example, to automatically turn the display on at 07:00a.m., (0700), enter **07:00**. To turn the display on at 02:00p.m. (1400), enter **14:00**. If this field is blank, the display will automatically turn on at 0:00.
Display On Duration	Length of time that the display remains on after turning on at the time specified in the Display On Time field. Enter the value in this field in the format *hours:minutes*. For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter **04:30**. If this field is blank, the phone will turn off at the end of the day (0:00). **Note** If Display On Time is 0:00 and the display on duration is blank (or 24:00), the display will remain on continuously.
Display Idle Timeout	Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by a user (by pressing a button on the phone or lifting the handset). Enter the value in this field in the format *hours:minutes*. For example, to turn the display off when the phone is idle for 1 hour and 30 minutes after a user turns the display on, enter **01:30**. The default value is 01:00.

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

Schedule EnergyWise on Cisco IP Phone

To reduce power consumption, configure the phone to sleep (power down) and wake (power up) if your system includes an EnergyWise controller.

Note The Cisco IP Phone 7811 does not support Power Save Plus.

You configure settings in Cisco Unified Communications Manager Administration to enable EnergyWise and configure sleep and wake times. These parameters are closely tied to the phone display configuration parameters.

When EnergyWise is enabled and a sleep time is set, the phone sends a request to the switch to wake it up at the configured time. The switch returns either an acceptance or a rejection of the request. If the switch rejects the request or if the switch does not reply, the phone does not power down. If the switch accepts the request, the idle phone goes to sleep, thus reducing the power consumption to a predetermined level. A phone that is not idle sets an idle timer and goes to sleep after the idle timer expires.

To wake up the phone, press Select. At the scheduled wake time, the system restores power to the phone, waking it up.

For more information, see Product Specific Configuration, on page 21

Procedure

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

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

Step 3 Navigate to the Product Specific Configuration area and set the following fields.

- Enable Power Save Plus
- Phone On Time
- Phone Off Time
- Phone Off Idle Timeout
- Enable Audible Alert
- EnergyWise Domain
- EnergyWise Secret
- Allow EnergyWise Overrides

Table 4: EnergyWise Configuration Fields

Field	Description
Enable Power Save Plus	Selects the schedule of days for which the phone powers off. Select multiple days by pressing and holding the Control key while clicking on the days for the schedule. By default, no days are selected. When Enable Power Save Plus is checked, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.
Phone On Time	Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 07:00 a.m. (0700), enter 07:00. To power up the phone at 02:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00.
Phone Off Time	The time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20.

Field	Description
Phone Off Idle Timeout	The length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the **Select** key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use. The range of the field is 20 to 1440 minutes. The default value is 60 minutes.
Enable Audible Alert	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. The audible alert uses the phone ringtone, which briefly plays at specific times during the 10-minute alerting period. The alerting ringtone plays at the user-designated volume level. The audible alert schedule is: • At 10 minutes before power down, play the ringtone four times. • At 7 minutes before power down, play the ringtone four times. • At 4 minutes before power down, play the ringtone four times. • At 30 seconds before power down, play the ringtone 15 times or until the phone powers off. This check box applies only if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	The EnergyWise domain that the phone is in. The maximum length of this field is 127 characters.
EnergyWise Secret	The security secret password that is used to communicate with the endpoints in the EnergyWise domain. The maximum length of this field is 127 characters.

Field	Description
Allow EnergyWise Overrides	This check box determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply: • One or more days must be selected in the Enable Power Save Plus field. • The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override. For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected. • If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Unified Communications Manager Administration. • To change the power level on the phone again, EnergyWise must reissue a new power level change command. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. If the Allow EnergyWise Overrides remains checked but no days are selected in the Enable Power Save Plus field, Power Save Plus is not disabled.

Step 4 Select **Save**.

Step 5 Select **Apply Config**.

Step 6 Restart the phone.

Set up AS-SIP

Depending on how you have configured your phone system, you may be able to make priority calls using the Assured Services for SIP Lines (AS-SIP) feature.

With this feature, routine calls are placed normally. However, during an emergency, you can select a priority level that helps ensure the delivery of critical calls. Depending upon how your phone is configured, you may have to sign-in also.

When you receives a priority call, a precedence level icon displays next to the caller's name on your phone.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Select a profile.

Step 3 Set the Is Assured SIP Service Enabled check box.

This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Step 4 Enable MLPP Authorization for a device by checking the MLPP User Authorization check box.

When the MLPP User Authorization check box is enabled, the system challenges the AS-SIP phone for the user's credentials when a precedence call is made.

Step 5 Set the Resource Priority namespace.

An AS-SIP phone is associated with a single Resource Priority namespace.

If <*None*> is left as the namespace in the SIP profile, then the default namespace is used.

All devices using this profile must be restarted.

Step 6 Select **Apply**.

Step 7 Choose **Device** > **Phone**.

Step 8 Locate the phone that you are setting up.

Step 9 Navigate to the MLPP section and set the following fields:

- MLPP Indication:
  - Set the MLPP Indication to **On** to enable MLPP regardless of the enterprise or common config settings.
  - Set the MLPP Indication to **Default** and MLPP is enabled for a device at the common device config or enterprise parameter levels.
  - When MLPP Indication is set to **Off**, MLPP is disabled for the device regardless of the common device or enterprise parameter configuration.
- MLPP Preemption: Determines whether preemption for reuse can be performed on the device. This type of preemption is used to remove an existing call and offer a higher precedence call to the user of the device.
  - When set to **Disabled**, only preemption 'not for reuse' can be performed on the device. This type of preemption occurs when the user is not the called party but is in a call with the called party or is using a preempted network resource. For example, a trunk channel or reserved bandwidth allocation.
  - When set to **Forceful**, preempt for reuse is enabled. Existing calls may be preempted to offer a higher precedence call to the user.
  - When set to **Default**, the setting from the common configuration or enterprise level is used.

Step 10 Choose **User Management** > **End User** and select a user.

Step 11 Navigate to the MLPP Authorization section and configure MLPP Authorization for a user.

The MLPP User Identification number must be composed of 6 to 20 numeric characters.

The MLPP Password must be composed of 4 to 20 numeric (0-9) characters

The Precedence Authorization level can be set to any standard precedence level from Routine to Executive Override

Step 12 Select **Save**.

Step 13 Set up the MLPP DSCP for an End User.

The DSCP values for video streams can be configured for each precedence level in the QoS section of the Service Parameters. All DSCP values include the decimal value in the setting.

Step 14 To add a third-party AS-SIP phone, choose **Device** > **Phone** > **Add New**

The phone Add list displays the third-party AS-SIP phone as an available choice.

The device configuration fields are the same as those for Cisco phones.

Set Up Do Not Disturb

When Do Not Disturb (DND) is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur.

You can configure the phone with a phone-button template with DND as one of the selected features.

For more information, see the Do Not Disturb information in the documentation for your particular Cisco Unified Communications Manager release.

Procedure

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

Step 2 Locate the phone to be configured.

Step 3 Set the following parameters.

- Do Not Disturb: This check box allows you to enable DND on the phone.
- DND Option: Ring Off, Call Reject, or Use Common Phone Profile Setting.

  Do not choose Call Reject if you want priority (MLPP) calls to ring this phone when DND is turned on.
- DND Incoming Call Alert: Choose the type of alert, if any, to play on a phone for incoming calls when DND is active.

  Note This parameter is located on in the Common Phone Profile window and the Phone Configuration window. The Phone Configuration window value takes precedence.

Step 4 Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation

Enable Agent Greeting

The Agent Greeting feature allows an agent to create and update a prerecorded greeting that plays at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. The agent can prerecord a single greeting or multiple greetings, as needed, and create and update the greetings.

When a customer calls, the agent and the caller hear the prerecorded greeting. The agent can remain on mute until the greeting ends or the agent can answer the call over the greeting.

All codecs supported for the phone are supported for Agent Greeting calls.

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

Procedure

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

Step 2 Locate the IP phone that you want to configure.

Step 3 Scroll to the Device Information Layout pane and set **Built In Bridge** to On or Default.

Step 4 Select **Save**.

Step 5 Check the setting of the bridge:

a) Choose **System** > **Service Parameters**.
b) Select the appropriate Server and Service.
c) Scroll to the Clusterwide Parameters (Device - Phone) pane and set **Builtin Bridge Enable** to On.
d) Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation

Set Up Monitoring and Recording

The Monitoring and Recording feature allows a supervisor to monitor an active call silently. Neither party on the call can hear the supervisor. The user may receive an audible alert during a call when it is being monitored.

When a call is secure, a lock icon displays. Callers may also receive an audible alert to indicate that the call is being monitored. The connected parties may also receive an audible alert that indicates that the call is secure and is being monitored.

When an active call is being monitored or recorded, the user can receive or place intercom calls; however, if the user places an intercom call, the active call is put on hold. This action causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the person being monitored must resume the call.

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

The following procedure adds a user to the standard monitoring user groups.

Before you begin

The Cisco Unified Communications Manager must be configured to support Monitoring and Recording.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **User Management** > **Application User**.

Step 2 Check the Standard CTI Allow Call Monitoring user group and the Standard CTI Allow Call Recording user groups.

Step 3 Click **Add Selected**.

Step 4 Click **Add to User Group**.

Step 5 Add the user phones to the list of Application Users controlled devices.

Step 6 Select **Save**.

Related Topics

Cisco Unified Communications Manager Documentation

Set Up Call Forward Notification

You can control the call forward settings.

Procedure

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

Step 2 Locate the phone to be set up.

Step 3 Configure the Call Forward Notification fields.

Field	Description
Caller Name	When this check box is checked, the caller name displays in the notification window. By default, this check box is checked.
Caller Number	When this check box is checked, the caller number displays in the notification window. By default, this check box is not checked.
Redirected Number	When this check box is checked, the information about the caller who last forwarded the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, the notification box that D sees contains the phone information for caller C. By default, this check box is not checked.
Dialed Number	When this check box is checked, the information about the original recipient of the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, then the notification box that D sees contains the phone information for caller B. By default, this check box is checked.

Step 4 Select **Save**.

Enable BLF for Call Lists

Procedure

Step 1 In the Cisco Unified Communications Manager Administration, select **System** > **Enterprise Parameters**.

Step 2 From the BLF for Call Lists drop-down list box, choose the applicable profile.

By default, the feature is disabled.

Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:

a. Device Configuration window settings

b. Common Phone Profile window settings

c. Enterprise Phone Configuration window settings

Step 3 Select **Save**.

Enable Device Invoked Recording

Configure the Device Invoked Recording feature from Cisco Unified Communications Manager Administration. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Procedure

Step 1 Set the IP Phone Built In Bridge parameter to **On**.

Step 2 In the Line Configuration page, set Recording Option to **Selective Call Recording Enabled** and select the appropriate Recording profile.

Related Topics

Cisco Unified Communications Manager Documentation

UCR 2008 Setup

The parameters that support UCR 2008 reside in Cisco Unified Communications Manager Administration. The following table describes the parameters and indicates the path to change the setting.

Table 5: UCR 2008 Parameter Location

Parameter	Administration Path
FIPS Mode	**Device** > **Device Settings** > **Common Phone Profile**
	System > **Enterprise Phone Configuration**
	Device > **Phones**
SSH Access	**Device** > **Phone**
	Device > **Device Settings** > **Common Phone Profile**
Web Access	**Device** > **Phone**
	System > **Enterprise Phone Configuration**
	Device > **Device Settings** > **Common Phone Profile**
80-bit SRTCP	**Device** > **Device Settings** > **Common Phone Profile**
	System > **Enterprise Phone Configuration**
IP Addressing Mode	**Device** > **Device Settings** > **Common Device Configuration**
IP Addressing Mode Preference for Signaling	**Device** > **Device Settings** > **Common Device Configuration**

Set Up UCR 2008 in Common Device Configuration

Use this procedure to set the following UCR 2008 parameters:

- IP Addressing Mode
- IP Addressing Mode Preference for Signaling

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Set the IP Addressing Mode parameter.

Step 3 Set the IP Addressing Mode Preference for Signaling parameter.

Step 4 Select **Save**.

Set Up UCR 2008 in Common Phone Profile

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access

- 80-bit SRTCP
- Web Access

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 Set the FIPS Mode parameter to **Enabled**.

Step 3 Set the SSH Access parameter to **Disabled**.

Step 4 Set the Web Access parameter to **Disabled**.

Step 5 Set the 80-bit SRTCP parameter to **Enabled**.

Step 6 Select **Save**.

Set Up UCR 2008 in Enterprise Phone Configuration

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- 80-bit SRTCP
- Web Access

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Phone Configuration**.

Step 2 Set the FIPS Mode parameter to **Enabled**.

Step 3 Set the 80-bit SRTCP parameter to **Enabled**.

Step 4 Set the Web Access parameter to **Disabled**.

Step 5 Select **Save**.

Set Up UCR 2008 in Phone

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- Web Access

Procedure

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

Step 2 Set the SSH Access parameter to **Disabled**.

Step 3 Set the FIPS Mode parameter to **Enabled**.

Step 4 Set the Web Access parameter to **Disabled**.

Step 5 Select **Save**.

Set Up RTP/sRTP Port Range

You configure the Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP) port values in the SIP profile. RTP and sRTP port values range from 2048 to 65535, with a default range of 16384 to 32764. Some port values within the RTP and sRTP port range are designated for other phone services. You cannot configure these ports for RTP and sRTP.

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

Procedure

Step 1 Select **Device** > **Device Settings** > **SIP Profile**

Step 2 Choose the search criteria to use and click **Find**.

Step 3 Select the profile to modify.

Step 4 Set the Start Media Port and Stop Media Port to contain the start and end of the port range.

The following list identifies the UDP ports that are used for other phone services and thus not available for RTP and sRTP use:

port 4051

used for the Peer Firmware Sharing (PFS) feature

port 5060

used for SIP over UDP transport

port range 49152 to 53247

used for local ephemeral ports

port range 53248 to 65535

used for the VxC single tunnel VPN feature

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Related Topics

Cisco Unified Communications Manager Documentation

Mobile and Remote Access Through Expressway

Mobile and Remote Access Through Expressway(MRA) lets remote workers easily and securely connect into the corporate network without using a virtual private network (VPN) client tunnel. Expressway uses Transport Layer Security (TLS) to secure network traffic. For a phone to authenticate an Expressway certificate and establish a TLS session, a public Certificate Authority that the phone firmware trusts must sign the Expressway certificate. It is not possible to install or trust other CA certificates on phones for authenticating an Expressway certificate.

The list of CA certificates embedded in the phone firmware is available at http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-technical-reference-list.html.

Mobile and Remote Access Through Expressway (MRA)works with Cisco Expressway. You must be familiar with the Cisco Expressway documentation, including the *Cisco Expressway Administrator Guide* and the *Cisco Expressway Basic Configuration Deployment Guide*. Cisco Expressway documentation is available at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html.

Only the IPv4 protocol is supported for Mobile and Remote Access Through Expressway users.

For additional information about working with Mobile and Remote Access Through Expressway, see:

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Unified Communications Mobile and Remote Access via Cisco VCS Deployment Guide*
- *Cisco TelePresence Video Communication Server (VCS), Configuration Guides*
- *Mobile and Remote Access Through Cisco Expressway Deployment Guide*

During the phone registration process, the phone synchronizes the displayed date and time with the Network Time Protocol (NTP) server. With MRA, the DHCP option 42 tag is used to locate the IP addresses of the NTP servers designated for time and date synchronization. If the DHCP option 42 tag is not found in the configuration information, the phone looks for the 0.tandberg.pool.ntp.org tag to identify the NTP servers.

After registration, the phone uses information from the SIP message to synchronize the displayed date and time unless an NTP server is configured in the Cisco Unified Communications Manager phone configuration.

Note If the phone security profile for any of your phones has TFTP Encrypted Config checked, you cannot use the phone with Mobile and Remote Access. The MRA solution does not support device interaction with Certificate Authority Proxy Function (CAPF).

SIP OAuth mode is supported for MRA. This mode allows you to use OAuth access tokens for authentication in secure environments.

Note For SIP OAuth in Mobile and Remote Access (MRA) mode, use only Activation Code Onboarding with Mobile and Remote Access when you deploy the phone. Activation with a username and password is not supported.

SIP OAuth mode requires Expressway x14.0(1) and later, or Cisco Unified Communications Manager 14.0(1) and later.

For additional information on SIP OAuth mode see *Feature Configuration Guide for Cisco Unified Communications Manager*, Release 14.0(1) or later.

Deployment Scenarios

The following table shows various deployment scenarios for Mobile and Remote Access Through Expressway.

Scenario	Actions
On-premises user logs in to the enterprise network, after deploying Mobile and Remote Access Through Expressway.	The enterprise network is detected, and the phone registers with Cisco Unified Communications Manager as it would normally.
Off-premises user logs in to the enterprise network with Mobile and Remote Access Through Expressway.	The phone detects that it is in off-premises mode, the Mobile and Remote Access Through Expressway Sign-In window appears, and the user connects to the corporate network. Users must have a valid service name, username, and password to connect to the network. Users must also reset the service mode to clear the Alternate TFTP setting before they can access the company network. This clears the Alternate TFTP Server setting so the phone detects the off-premises network. If a phone is being deployed out of the box, users may skip the reset Network Settings requirement. If users have DHCP option 150 or option 66 enabled on their network router, they may not be able to sign in to the corporate network. Users should disable these DHCP settings or configure their static IP address directly.

Media Paths and Interactive Connectivity Establishment

You can deploy Interactive Connectivity Establishment (ICE) to improve the reliability of Mobile and Remote Access (MRA) calls that cross a firewall or Network Address Translation (NAT). ICE is an optional deployment that uses Serial Tunneling and Traversal Using Relays around NAT services to select the best media path for a call.

Secondary Turn Server and Turn Server Failover is not supported.

For more information about MRA and ICE, see *System Configuration Guide for Cisco Unified Communications Manager, Release 12.0(1)* or later. You can also find additional information in the Internet Engineering Task Force (IETF) Request for Comment documents:

- *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*(RFC 5766)
- *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols* (RFC 5245)

Phone Features Available for Mobile and Remote Access Through Expressway

Mobile and Remote Access Through Expressway provides secure VPN-less access to collaboration services for Cisco mobile and remote users. But to preserve network security, it limits access to some phone features.

The following list shows the phone features available with Mobile and Remote Access Through Expressway.

Table 6: Feature Support and Mobile and Remote Access Through Expressway

Phone Feature	Phone Firmware Release
Abbreviated Dialing	10.3(1) and later
Answer Oldest	11.5(1)SR1 and later
Assisted Directed Call Park	10.3(1) and later
Auto Answer	11.5(1)SR1 and later
Barge and cBarge	11.5(1)SR1 and later
Busy Lamp Field (BLF)	10.3(1) and later
Busy Lamp Field (BLF) Pickup	10.3(1) and later
Busy Lamp Field (BLF) Speed Dial	10.3(1) and later
Call Back	10.3(1) and later
Call Forward	10.3(1) and later
Call Forward Notification	10.3(1) and later
Call Park	10.3(1) and later
Call Pickup	10.3(1) and later
Cisco Unified Serviceability	11.5(1)SR1 and later
Client Access License (CAL)	11.5(1)SR1 and later
Conference	10.3(1) and later
Conference List / Remove Participant	11.5(1)SR1 and later
Corporate Directory	11.5(1)SR1 and later
CTI Applications (CTI Controlled)	11.5(1)SR1 and later
Directed Call Park	10.3(1) and later
Distinctive Ring	11.5(1)SR1 and later
Divert	10.3(1) and later
Divert	10.3(1) and later

Phone Feature	Phone Firmware Release
Forced Access Codes and Client Matter Codes	11.5(1)SR1 and later
Group Call Pickup	10.3(1) and later
Hold/Resume	10.3(1) and later
Hold Reversion	10.3(1) and later
Immediate Divert	10.3(1) and later
Join	10.3(1) and later
Malicious Caller Identification (MCID)	11.5(1)SR1 and later
Meet Me Conference	10.3(1) and later
Message Waiting Indicator	10.3(1) and later
Mobile Connect	10.3(1) and later
Mobile Voice Access	10.3(1) and later
Multilevel Precedence and Preemption (MLPP)	11.5(1)SR1 and later
Multiline	11.5(1)SR1 and later
Music On Hold	10.3(1) and later
Mute	10.3(1) and later
Network profiles (Automatic)	11.5(1)SR1 and later
Off-hook Dialing	10.3(1) and later
On-hook Dialing	10.3(1) and later
Plus Dialing	10.3(1) and later
Privacy	11.5(1)SR1 and later
Private Line Automated Ringdown (PLAR)	11.5(1)SR1 and later
Redial	10.3(1) and later
Speed Dial (does not support a pause)	10.3(1) and later
Services URL button	11.5(1)SR1 and later
Transfer	10.3(1) and later
Uniform Resource Identifier (URI) Dialing	10.3(1) and later

Problem Report Tool

Users submit problem reports to you with the Problem Report Tool.

Note The Problem Report Tool logs are required by Cisco TAC when troubleshooting problems. The logs are cleared if you restart the phone. Collect the logs before you restart the phones.

To issue a problem report, users access the Problem Report Tool and provide the date and time that the problem occurred, and a description of the problem.

If the PRT upload fails, you can access the PRT file for the phone from the URL **http://<phone-ip-address>/FS/<prt-file-name>**. This URL is displayed on the phone in the following cases:

- If the phone is in the factory default state. The URL is active for 1 hour. After 1 hour, the user should try to submit the phone logs again.
- If the phone has downloaded a configuration file and the call control system allows web access to the phone.

You must add a server address to the **Customer Support Upload URL** field on Cisco Unified Communications Manager.

If you are deploying devices with Mobile and Remote Access through Expressway, you must also add the PRT server address to the HTTP Server Allow list on the Expressway server.

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.");
}

?>
```

Note The phones only support HTTP URLs.

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.

Set the Label for a Line

You can set up a phone to display a text label instead of the directory number. Use this label to identify the line by name or function. For example, if your user shares lines on the phone, you could identify the line with the name of the person that shares the line.

When adding a label to a key expansion module, only the first 25 characters are displayed on a line.

Procedure

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

Step 2 Locate the phone to be configured.

Step 3 Locate the line instance and set the Line Text Label field.

Step 4 (Optional) If the label needs to be applied to other devices that share the line, check the Update Shared Device Settings check box and click **Propagate Selected**.

Step 5 Select **Save**.

Assured Services SIP

Assured Services SIP(AS-SIP) is a collection of features and protocols that offer a highly secure call flow for Cisco IP Phones and third-party phones. The following features are collectively known as AS-SIP:

- Multilevel Precedence and Preemption (MLPP)
- Differentiated Services Code Point (DSCP)
- Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP)
- Internet Protocol version 6 (IPv6)

AS-SIP is often used with Multilevel Precedence and Preemption (MLPP) to prioritize calls during an emergency. With MLPP, you assign a priority level to your outgoing calls, from level 1 (low) to level 5 (high). When you receive a call, a precedence level icon displays on the phone that shows the call priority.

To configure AS-SIP, complete the following tasks on Cisco Unified Communications Manager:

- Configure a Digest User—Configure the end user to use digest authentication for SIP requests.
- Configure SIP Phone Secure Port—Cisco Unified Communications Manager uses this port to listen to SIP phones for SIP line registrations over TLS.
- Restart Services—After configuring the secure port, restart the Cisco Unified Communications Manager and Cisco CTL Provider services. Configure SIP Profile for AS-SIP-Configure a SIP profile with SIP settings for your AS-SIP endpoints and for your SIP trunks. The phone-specific parameters are not downloaded to a third-party AS-SIP phone. They are used only by Cisco Unified Manager. Third-party phones must locally configure the same settings.
- Configure Phone Security Profile for AS-SIP—You can use the phone security profile to assign security settings such as TLS, SRTP, and digest authentication.
- Configure AS-SIP Endpoint—Configure a Cisco IP Phone or a third-party endpoint with AS-SIP support.
- Associate Device with End Use—Associate the endpoint with a user.
- Configure SIP Trunk Security Profile for AS-SIP—You can use the sip trunk security profile to assign security features such as TLS or digest authentication to a SIP trunk.
- Configure SIP Trunk for AS-SIP—Configure a SIP trunk with AS-SIP support.
- Configure AS-SIP Features—Configure additional AS-SIP features such as MLPP, TLS, V.150, and IPv6.

For detailed information about configuring AS-SIP, see the "Configure AS-SIP Endpoints" chapter, *System Configuration Guide for Cisco Unified Communications Manager*.

Multilevel Precedence and Preemption

Multilevel Precedence and Preemption (MLPP) allows you to prioritize calls during emergencies or other crisis situations. You assign a priority to your outgoing calls that range from 1 to 5. Incoming calls display an icon that shows the call priority. Authenticated users can preempt calls either to targeted stations or through fully subscribed TDM trunks.

This capability assures high-ranking personnel of communication to critical organizations and personnel.

MLPP is often used with Assured Services SIP(AS-SIP). For detailed information about configuring MLPP, see the "Configure Multilevel Precedence and Preemption" chapter, *System Configuration Guide for Cisco Unified Communications Manager*.

Migration of your Phone to a Multiplatform Phone Directly

You can migrate your enterprise phone to a multiplatform phone easily in one step without using transition firmware load. All you need is to obtain and authorize the migration license from the server.

For more information, see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html

Set Up Softkey Template

You can associate up to 18 softkeys with applications that are supported by the Cisco IP Phone. An application that supports softkeys can have one or more standard softkey templates associated with it.

Cisco Unified Communications Manager supports the Standard User and Standard Feature softkey template. You can modify a standard softkey template by making a copy of it, giving it a new name, and making updates to that copied softkey template. You can also modify a nonstandard softkey template.

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

The phones do not support all the softkeys that are configurable in Softkey Template Configuration on Cisco Unified Communications Manager Administration. The following table lists the features, softkeys that can be configured on a softkey template, and note whether it is supported on the Cisco IP Phone.

Table 7: Configurable Softkeys

Feature	Configurable softkeys in the Softkey Template configuration	Support status	Notes
Answer	Answer (Answer)	Yes	-
Barge	Barge (Barge)	No	Cisco IP Phone 7811, 7821, 7841, and 7861 support cBarge only.
Call Back	Call Back (CallBack)	Yes	Configure as a programmable line key or as a softkey.
Call Forward All	Forward All (cfwdAll)	Yes	Phone displays `Fwd ALL` or `Fwd Off`.

Feature	Configurable softkeys in the Softkey Template configuration	Support status	Notes
Call Park	Call Park (Park)	Yes	Configure as a programmable line key or as a softkey.
Call Pickup	Pick Up (Pickup)	Yes	Configure as a programmable line key or as a softkey.
cBarge	Conference Barge (cBarge)	Yes	Configure as a programmable line key or as a softkey.
Conference	Conference (Conf)	Yes	Configure as a softkey only.
Conference List	Details	Yes	Phone displays Details.
Divert	ImmediateDivert (iDivert)	Yes	Phone displays Divert. Starting with Firmware Release 10.3(1), the phone displays Decline for the softkey.
Do Not Disturb	Toggle Do Not Disturb (DND)	Yes	Configure as a programmable line button or softkey.
End Call	End Call (EndCall)	Yes	
Group Pickup	Group PickUp (GPickUp)	Yes	Configure as a programmable line button or softkey
Hold	Hold (Hold)	Yes	Hold is a dedicated button.
Hunt Group	HLog (HLog)	Yes	Configure as a programmable line button or softkey.
Join	Join (Join)	No	
Malicious Call Identification	Toggle Malicious Call Identification (MCID)	Yes	Configure as a programmable feature button or softkey.
Meet Me	Meet Me (MeetMe)	Yes	Configure as a programmable feature button or softkey.
Mobile Connect	Mobility (Mobility)	Yes	Configure as a programmable feature button or softkey.
New Call	New Call (NewCall)	Yes	Phone displays `New Call`.
Other Pickup	Other Pickup (oPickup)	Yes	Configure as a programmable feature button or softkey.
PLK Support for Queue Statistics	Queue Status	Yes	-
Quality Reporting Tool	Quality Reporting Tool (QRT)	Yes	Configure as a programmable feature button or softkey.

Feature	Configurable softkeys in the Softkey Template configuration	Support status	Notes
Recents	Recents	Yes	Enables/Disables the softkey.
Redial	Redial (Redial)	Yes	-
Remove Last Conference Participant	Remove Last Conference Participant (Remove)	Yes	Phone displays `Remove` when a participant is selected.
Resume	Resume (Resume)	Yes	Resume is a dedicated button.
Speed Dial	Abbreviated Dial (AbbrDial)	Yes	Phone displays `SpeedDial`.
Transfer	Direct Transfer (DirTrfr)	Yes	This feature is supported as a soft key or a dedicated button.
Video Mode Command	Video Mode Command (VidMode)	No	-

Cisco Unified Communications Manager allows you to configure any softkey in a softkey template, but unsupported softkeys do not display on the phone.

Procedure

Step 1 In Cisco Unified Communications Manager, select **Device** > **Device Settings** > **Softkey Template**.

Step 2 Locate the template that you want to change.

Step 3 Select Configure Softkey Layout from the Related Links list and click **Go**.

Step 4 Configure the softkey positions.

Step 5 Select **Save** to save the layout, template, and modification

Step 6 Select **Apply Config** to apply the template to the phones.

Related Topics

Cisco Unified Communications Manager Documentation

Phone Button Templates

Phone button templates let you assign speed dials and call-handling features to programmable buttons. Call-handling features that can be assigned to buttons include Answer, Mobility, and All Calls.

Ideally, you modify templates before you register phones on the network. In this way, you can access customized phone button template options from Cisco Unified Communications Manager during registration.

Modify Phone Button Template

For more information about IP Phone services and configuring line buttons, see the documentation for your particular Cisco Unified Communications Manager release.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find**.

Step 3 Select the phone model.

Step 4 Select **Copy**, enter a name for the new template, and then select **Save**.

The Phone Button Template Configuration window opens.

Step 5 Identify the button that you would like to assign, and select **Service URL** from the Features drop-down list that associates with the line.

Step 6 Select **Save** to create a new phone button template that uses the service URL.

Step 7 Choose **Device** > **Phone** and open the Phone Configuration window for the phone.

Step 8 Select the new phone button template from the Phone Button Template drop-down list.

Step 9 Select **Save** to store the change and then select **Apply Config** to implement the change.

The phone user can now access the Self Care Portal and associate the service with a button on the phone.

Related Topics

Cisco Unified Communications Manager Documentation

Set Up PAB or Speed Dial as IP Phone Service

You can modify a phone button template to associate a service URL with a programmable button. Doing so provides users with single-button access to the PAB and Speed Dials. Before you modify the phone button template, you must configure PAB or Speed Dials as an IP Phone service. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

To configure PAB or Speed Dial as an IP Phone service (if it is not already a service), follow these steps:

Procedure

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

The Find and List IP Phone Services window displays.

Step 2 Click **Add New**.

The IP Phone Services Configuration window displays.

Step 3 Enter the following settings:

- Service Name: Enter **Personal Address Book**.
- Service Description: Enter an optional description of the service.
- Service URL

  For PAB, enter the following URL:

  http://<Unified CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**

  For Fast Dial, enter the following URL:

  http://<Unified-CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**
- Secure Service URL

  For PAB, enter the following URL:

  https://<Unified CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab**

  For Fast Dial, enter the following URL:

  https://<Unified-CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd**
- Service Category: Select **XML Service**.
- Service Type: Select **Directories**.
- Enable: Select the check box.

  http://<IP_address> or *https://<IP_address>* (Depends on the protocol that the Cisco IP Phone supports.)

Step 4 Select **Save**.

Note If you change the service URL, remove an IP Phone service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, you must click **Update Subscriptions** to update all currently subscribed users with the changes; otherwise, users must resubscribe to the service to rebuild the correct URL.

Related Topics

Cisco Unified Communications Manager Documentation

Headset Management on Older Versions of Cisco Unified Communications Manager

If you have a version of Cisco Unified Communications Manager older than 12.5(1)SU1, you can remotely configure your Cisco headset settings for use with on-premises phones.

Remote headset configuration on Cisco Unified Communication Manager version 10.5(2), 11.0(1), 11.5(1), 12.0(1), and 12.5(1) requires you to download a file from the Cisco Software Download website, edit the file, and then upload the file on the Cisco Unified Communications Manager TFTP server. The file is a JavaScript Object Notification (JSON) file. The updated headset configuration is applied to the enterprise headsets over a 10 to 30-minute time frame to prevent a traffic backlog on the TFTP server.

Note You can manage and configure headsets through Cisco Unified Communications Manager Administration version 11.5(1)SU7.

Note the following as you work with the JSON file:

- The settings aren't applied if you are missing a bracket or brackets in the code. Use an online tool such as JSON Formatter and check the format.
- Set the **updatedTime** setting to the current epoch time or the configuration is not applied. Alternatively, you can increase the **updatedTime** value by +1 to make it larger than the previous version.
- Do not change the parameter name or the setting will not be applied.

For more information on the TFTP service, see the "Manage Device Firmware" chapter of the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*.

Upgrade your phones to the latest firmware release before you apply the `defaultheadsetconfig.json` file. The following table describes the default settings you can adjust with the JSON file.

Download the Default Headset Configuration File

Before configuring the headset parameters remotely, you must download the latest JavaScript Object Notation (JSON) sample file.

Procedure

Step 1 Go to the following URL: https://software.cisco.com/download/home/286320550.

Step 2 Choose **Headsets 500 Series**.

Step 3 Select your headset series.

Step 4 Choose a release folder and select the zip file.

Step 5 Click the **Download** or **Add to cart** button, and follow the prompts.

Step 6 Unzip the file to a directory on your PC.

What to do next

Modify the Default Headset Configuration File, on page 62

Modify the Default Headset Configuration File

Note the following as you work with the JavaScript Object Notation (JSON) file:

- The settings aren't applied if you are missing a bracket or brackets in the code. Use an online tool such as JSON Formatter and check the format.
- Set the "**updatedTime**" setting to the current epoch time or the configuration is not applied.
- Confirm that **firmwareName** is `LATEST` or the configurations will not be applied.

- Do not change a parameter name or the setting will not be applied.

Procedure

Step 1 Open the `defaultheadsetconfig.json` file with a text editor.

Step 2 Edit the **updatedTime** and the headset parameter values you wish to modify.

A sample script is shown below. This script is provided for reference only. Use it as a guide as you configure your headset parameters. Use the JSON file that was included with your firmware load.

```
{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedTime": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
            "532"
          ],
          "modelFirmware": [
            {
              "firmwareName": "LATEST",
              "latest": true,
              "firmwareParams": [
                {
                  "name": "Speaker Volume",
                  "access": "Both",
                  "usageId": 32,
                  "value": 7
                },
                {
                  "name": "Microphone Gain",
                  "access": "Both",
                  "usageId": 33,
                  "value": 2
                },
                {
                  "name": "Sidetone",
                  "access": "Both",
                  "usageId": 34,
                  "value": 1
                },
                {
                  "name": "Equalizer",
                  "access": "Both",
                  "usageId": 35,
                  "value": 3
                }
              ]
            }
          ]
        },
```

```
  {
    "modelSeries": "560",
    "models": [
      "560",
      "561",
      "562"
    ],
    "modelFirmware": [
      {
        "firmwareName": "LATEST",
        "latest": true,
        "firmwareParams": [
          {
            "name": "Speaker Volume",
            "access": "Both",
            "usageId": 32,
            "value": 7
          },
          {
            "name": "Microphone Gain",
            "access": "Both",
            "usageId": 33,
            "value": 2
          },
          {
            "name": "Sidetone",
            "access": "Both",
            "usageId": 34,
            "value": 1
          },
          {
            "name": "Equalizer",
            "access": "Both",
            "usageId": 35,
            "value": 3
          },
          {
            "name": "Audio Bandwidth",
            "access": "Admin",
            "usageId": 36,
            "value": 0
          },
          {
            "name": "Bluetooth",
            "access": "Admin",
            "usageId": 39,
            "value": 0
          },
          {
            "name": "DECT Radio Range",
            "access": "Admin",
            "usageId": 37,
            "value": 0
          }
          {
             "name": "Conference",
            "access": "Admin",
            "usageId": 41,
            "value": 0
        ]
      }
    ]
  }
]
```

```
        }
    }
}
```

Step 3 Save the `defaultheadsetconfig.json`.

What to do next

Install the default configuration file.

Install the Default Configuration File on Cisco Unified Communications Manager

After you edit the `defaultheadsetconfig.json` file, install it on Cisco Unified Communications Manager using the TFTP File Management tool.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **TFTP File Management**.

Step 2 Select **Upload File**.

Step 3 Select **Choose File** and navigate to the `defaultheadsetconfig.json` file.

Step 4 Select **Upload File**.

Step 5 Click **Close**.

Restart the Cisco TFTP Server

After you upload the `defaultheadsetconfig.json` file to the TFTP directory, restart the Cisco TFTP server and reset the phones. After about 10–15 minutes, the download process begins and the new configurations are applied to the headsets. It takes an additional 10 to 30 minutes for the settings to be applied.

Procedure

Step 1 Log in to Cisco Unified Serviceability and choose **Tools** > **Control Center - Feature Services**.

Step 2 From the **Server** drop-down list box, choose the server on which the Cisco TFTP service is running.

Step 3 Click the radio button that corresponds to the **Cisco TFTP** service.

Step 4 Click **Restart**.