Phone Features and Setup

Phone Features and Setup Overview

After you install Cisco IP Phones in your network, configure their network settings, and add them to Third-Party Call Control System, you must use the Third-Party Call Control System to configure telephony features, optionally modify phone templates, set up services, and assign users.

You can modify additional settings for the Cisco IP Phone from Third-Party Call Control Configuration Utility. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks.

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

Telephony Features

After you add Cisco IP Phones to Third-Party Call Control system, 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 Third-Party Call Control system.

Note   The Third-Party Call Control system also provides several service parameters that you can use to configure various telephony functions.

Feature	Description and More Information
AES 256 Encryption Support for Phones	Enhances security by supporting TLS 1.2 and new ciphers.
Alphanumeric Dialing	Allows users to place a call with alphanumeric characters. You can use these characters for alphanumeric dialing: a-z, A-Z, 0-9, -, _, ., and +.
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.
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.
Audio Settings	Configures audio settings for the phone speaker, the handset, and the headsets that are connected to the phone.
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with the speakerphone.
Busy Lamp Field (BLF)	Allows user to monitor call state of a directory number.
Busy Lamp Field (BLF) Pickup	Allows user to pick up incoming calls to the directory number monitored through BLF.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.
Call Display Restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call. RPID and PAID caller id handling are supported.
Call Forward	Allows users to redirect incoming calls to another number. Call Forward services include Call Forward All, Call Forward Busy, Call Forward No Answer.
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.

Feature	Description and More Information
Call Forward Notification	Allows you to configure the information that the user sees when receiving a forwarded call.
Call History for Shared Line	Allows you to view shared line activity in the phone Call History. This feature: • Logs missed calls for a shared line. • Logs all answered and placed calls for a shared line.
Call Park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone.
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 Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Incoming call information appears on the phone display.
Caller ID	Caller identification such as a phone number, name, or other descriptive text appear on the phone display.
Caller ID Blocking	Allows a user to block their phone number or name from phones that have caller identification enabled.
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.
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 WebDialer	Allows users to make calls from web and desktop applications.
Classic Ringtone	Supports narrowband and wideband ringtones. The feature makes the available ringtones common with other Cisco IP Phones.
Client Matter Code (CMC)	Enables a user to specify that a call relates to a specific client matter.

Feature	Description and More Information
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually.
	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.
	Note Be sure to inform your users whether these features are activated.
Configurable RTP/sRTP Port Range	Provides a configurable port range (Port Min to Port Max) for Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP).
	The value range for the Port Min and Port Max is 2048 to 49151.
	The default RTP and sRTP port range is 16384 to 16482.
	Note If the value range (Port Max - Port Min) is less than 16 or you use an incorrect port range, the port range (16382 to 32766) is used instead.
	You configure the RTP and sRTP port range in the SIP Profile.
Contacts Management of the BroadSoft Personal Directory on the Phone	Provides the user with the ability to add, edit, and delete in the BroadSoft Personal directory. Allows the user to add contacts from recent calls or any types of directories (if enabled).
	In addition administrator can set the BroadSoft Personal directory as the target directory to store new contacts.
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.
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.
Directed Call Pickup	Allows a user to pick up a ringing call on a DN directly by pressing the GPickUp softkey and entering the directory number of the device that is ringing.
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.

Feature	Description and More Information
DND and Call Forward Indication on Non-selected Line Key	Displays the DND and call forward icons next the to the line key label. The line key should be enabled with feature key sync. The line key should also be enabled with DND or call forward.
Emergency Calls	Enables users to make emergency calls. The emergency services receive the phone's location and a call-back number, to use when the emergency call unexpectedly disconnects.
EnergyWise	Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings.
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).
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.
Forced Authorization Code (FAC)	Controls the types of calls that certain users can place.
Feature Activation Code	Allows a user to enable, disable, or configure the Call Forward All service.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group.
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 configurations are required unless you want to use Music On Hold. See "Music On Hold" in this table. • 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.
HTTP Proxy	Allows you to set up a proxy server for the phone.
HTTPS for Phone Services	Increases security by requiring communication using HTTPS. **Note** When the web is in HTTPS mode, the phone is an HTTPS server.
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`.
IPv6 Support	Provides support for expanded IP addressing on Cisco IP Phones. IPv6 support is provided in standalone or in dual-stack configurations. In dual-stack mode, the phone is able to communicate using IPv4 and IPv6 simultaneously, independent of the content.

Feature	Description and More Information
Jitter Buffer	The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for both audio and video streams.
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.
Join	Allows users to combine two calls that are on one line to create a conference call and remain on thecall.
Line Display Enhancement	Improves Call Display by removing the central dividing line when it is not required. This feature applies to the Cisco IP Phone 7841 only.
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.
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.
Message Waiting Indicator	When you have a message, a message displays on the phone screen. Your phone also provides an audible message waiting indicator.
Minimum Ring Volume	Sets a minimum ringer volume level for an IP phone.
Missed Call Logging	Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance.
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.
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.

Feature	Description and More Information
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.
Multicasting Paging	Enables users to page some or all phones. If the phone is on an active call while a group page starts, the incoming page is ignored.
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 ten 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 10/6. Any configuration more than 10/6 is not officially supported.
Music On Hold	Plays music while callers are on hold.
Mute	Mutes the phone microphone.
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.
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.
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 PIN) 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.

Feature	Description and More Information
Peer Firmware Sharing (PFS)	Allows IP Phones located at remote sites to share the firmware files amongst them, which saves bandwidth when the upgrade process takes place. This feature uses Cisco Peer-to-Peer-Distribution Protocol (CPPDP) which is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. CPPDP is also used to copy firmware or other files from peer devices to the neighbouring devices. PFS aids in firmware upgrades in branch/remote office deployment scenarios that run over bandwidth-limited WAN links. Provides the following advantages over the traditional upgrade method: • 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 The more the number of IP phones, the better it's performance compared to the traditional firmware upgrade method.
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.
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.
Power Negotiation over LLDP	Allows the phone to negotiate power using Link Level Endpoint Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP).
Problem Reporting Tool	Submits phone logs or reports problems to an administrator.
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.
Redial	Allows users to call the most recently dialed phone number by pressing a button or the Redial softkey.
Remote Customization (RC)	Allows a service provider to customize the phone remotely. There is no need for either the service provider to physically touch the phone or a user to configure the phone. The service provider can work with a sales engineer at the time of ordering to set this up.
Ringtone Setting	Identifies ring type used for a line when a phone has another active call.
Reverse Name Lookup	Identifies the caller name using the incoming or outgoing call number. You must configure either the LDAP Directory or the XML directory. You can enable or disable the reverse name lookup using the phone administration web page.

Feature	Description and More Information
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.
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.
Show Caller Name and Caller Number	The phones can display both the caller name and caller number for incoming calls. The phone screen size limits the length of the caller name and the caller number that display.
	If boxes are displayed in the caller name, follow the procedure in Display Caller Number Instead of Unresolved Caller Name, on page 83.
	This feature applies to the incoming call alert only and doesn't change the Call Forward and Hunt Group features.
	See "Caller ID" in this table.
Show Product Configuration Version	Allows you to customize the product configuration version that shows on the phone screen **Product information**.
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.
Silence Incoming Call	Allows you to silence an incoming call by pressing **Ignore** softkey or by pressing the volume button down.
Speed Dial	Dials a specified number that has been previously stored.
Synchronization of Call Waiting and Anonymous Call Rejection	Allows you to enable or disable synchronization of the Call Waiting and Anonymous Call Rejection functions between a specific line and a BroadSoft XSI server.
Time Zone Update	Updates the Cisco IP Phone with time zone changes.

Feature	Description and More Information
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.
Voice Message System	Enables callers to leave messages if calls are unanswered.
Web Access Enable by Default	Web services are enabled by default.
XSI call logs display	Allows you to configure a phone to display recent call logs from either the BroadWorks server or the local phone. After you enable the feature, the **Recents** screen has a **Display recents from** menu and the user can choose the XSI call logs or the local call logs.

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 the web interface or in the configuration file (cfg.xml).

Note   The Cisco IP Conference Phone 7832 Multiplatform Phones doesn't have programmable feature buttons.

Table 1: Features with Corresponding Buttons and Softkeys

Feature Name	Dedicated Feature Button	Softkey
Answer	Not supported	Supported
Call Forward All	Not supported	Supported
Call Forward Busy	Not supported	Supported
Call Forward No Answer	Not supported	Supported
Call Park	Not supported	Supported
Call Pickup (Pick Up)	Not supported	Supported
Category	Not supported	Supported
Conference	Not supported	Supported (only displayed during connected call conference scenario)
Divert	Not supported	Supported

Feature Name	Dedicated Feature Button	Softkey
Do Not Disturb	Not supported	Supported
Hold	Not supported	Supported
Mute	Supported	Not supported
Redial	Not supported	Supported
Speed Dial	Not supported	Supported
Transfer	Not supported	Supported (only displayed during connected call transfer scenario)

Assign a Speed Dial Number

You can configure speed dials on the phone with the web interface. The user can see the configured speed dials on the phone and can use the speed dial number to call the corresponding contact.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **User**.

Step 2   In the **Speed Dial** section, enter a name in **Speed Dial (n) Name** and the number in **Speed Dial (n) Number** that corresponds to the speed dial entry.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. The speed dial parameters are line-specific. Enter a string in the format

```
<Speed_Dial_1_Name ua="rw">John Wood</Speed_Dial_1_Name>
<Speed_Dial_1_Number ua="rw">12345678</Speed_Dial_1_Number>
```

Step 3   Click **Submit All Changes**.

DTMF Wait and Pause Parameters

Speed dial, directory, extended function, and other strings configured in the phone can include *wait* (**X**) and *pause* (**,**) characters. These characters that allow manual and automatic DTMF (Dual-Tone Multi-Frequency) signal transmission.

You can add the wait and pause character with speed-dial, extended function, or directory strings in the format:

```
{Dial_String}[ ][,|X][DTMF_string][,|X][DTMF_string]
```

where:

- Dial_String —is the number that the user is trying to reach. For example, 8537777 or 14088537777.

- [ ](space)—is a dial termination character that defines or delimits the end of the dial string. The space is mandatory. If the phone encounters an X or a comma (,) before the space, the characters are treated as part of dial string.

- , (comma)—is a 2-second pause that is inserted for each comma in the string.

- X (wait)—indicates that the phone is waits for user input and acknowledgement.

  When the user manually enters the DTMF signal with the key pad, the user sees a message to acknowledge that the transmission of the manual entry is complete. On confirmation, the phone sends any DTMF signals defined by the *DTMF_string*. The phone executes the next parameter. If there are no more parameters in the dial string to execute, the phone exits to the main screen.

  The wait prompt window does not disappear until the user confirms the wait prompt or the call is ended either by the user or ended by the remote device.

- DTMF_string—is the DTMF signals that a user sends to a remote device after the call is connected. The phone cannot send signals other than valid DTMF signals.

Example:

18887225555,,5552X2222

A speed dial entry triggers the phone to dial 18887225555. The space indicates the end of the dial string. The phone waits 4 seconds (2 commas), and then sends the DTMF signals 5552.

A message is displayed, prompting the user to manually enter digits. When the user finishes dialing the digits, the user presses **OK** to confirm the manual input is complete. The phone sends the DTMF signals 2222.

Usage Guidelines

A user can transmit digits any time, as long as the call is connected.

The maximum length of the string, including the Xs or commas (,), is limited to the length of a speed-dial entry, dial screen entry, directory entry, and other dialed strings.

When a wait is initiated, the phone displays the home screen and prompts the user to input more digits with the key pad. If this action occurs while the user is editing an entry, the edits might be lost.

If only the first part of a dial string matches a dial plan when the call is dialed, the portion of the dial string that does not match the dial string is ignored. For example:

85377776666,,1,23

If 8537777 matches a dial plan, the characters 6666 are ignored. The phone waits 4 seconds before sending DTMF 1. It then wait 2 seconds and sends DTMF 23.

When logging the call, the phone only logs the dial string; the DTMF strings are not logged.

Valid DTMF signals are 0-9, *, or #. All other characters are ignored.

Limitations

When the call is connected and immediately transferred, the phone might not be able to process the DTMF signals. This depends on the length of time that the call is connected before it is transferred.

Enable Conference Button with a Star Code

You can add a star code to the Conference button so that your user can press the button only once to add many active calls to a conference. You can enable this feature from the phone web page.

Before you begin

- The phone server must suppport this feature.

- Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Ext(n)**, where n is an extension number.

Step 2   In the **Call Features Settings** section, configure the **Conference Single Hardkey** and **Conference Bridge URL** fields as defined in Conference Button Parameters, on page 14.

You can also enable the conference button with a xml file. Enter a string in this format:

```
<Conference_Bridge_URL_1_ ua="na">*55</Conference_Bridge_URL_1_>
<Conference_Single_Hardkey_1_ ua="na">Yes</Conference_Single_Hardkey_1_>
```

Step 3   Click **Submit All Changes**.

Conference Button Parameters

The following table defines the function and usage of the conference button parameters in the **Call Features Settings** section under the **Voice** > **Ext (n)** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 2: Conference Button Parameters

Parameter	Description and default value
Conference Single Hardkey	You can use this field to specify whether to use only the Conferenc button on the key to initiate a conference call. When set to **Yes**, the user can use only the Conference button to initiate a conference call. The **Conf** softkey is deactivated. When set to **No**, the user can use both the Conference button and the **Conf** softkey. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Conference_Single_Hardkey_1 ua="na">Yes</Conference_Single_Hardkey_1_>` • In the phone web interface, set this field to **Yes** or **No** to enable or disable this feature. Allowed values: Yes|No Default: No
Conference Bridge URL	URL used to join a conference call, generally in the form of a dialable number or a URI in this format `user@IPaddress:port`. • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Conference_Bridge_URL_1_ ua="na">*55</Conference_Bridge_URL_1_>` • in the phone web interface, specify the URI or a number as the conference bridge. Default: Empty

Configure Alphanumeric Dialing

You can configure a phone so that the user of the phone can make a call by dialing alphanumeric characters instead of dialing only digits. In the phone web page, you can configure alphanumeric dialing with speed-dial, blf, and call pickup.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Ext (n)**.

Step 2   In the **Dial Plan** section, set **Enable URI Dialing** to **Yes** to enable alphanumeric dialing.

You can also configure the parameter in the configuration file (cfg.xml). The parameter is line-specific.

`<Enable_URI_Dialing_1_ ua="na">Yes</Enable_URI_Dialing_1_>`

Step 3   Select **Voice** > **Phone**, you can add a string on a line key in this format to enable speed dial with alphanumeric dialing capability:

```
fnc=sd;ext=xxxx.yyyy@$PROXY;nme=yyyy,xxxx
```

For example:

```
fnc=sd;ext=first.last@$PROXY;nme=Last,First
```

The above example will enable the user to dial "first.last" to make a call.

Note   The supported characters that you can use for alphanumeric dialing are a-z, A-Z, 0-9, -, _, ., and +.

Step 4   Click **Submit All Changes**.

Set the Optional Network Configuration

Optional network servers provide resources such as DNS lookup, network time, logging, and device discovery.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in Parameters for Optional Network Configuration, on page 16.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **System**.

Step 2   In the **Optional Network Configuration** section, set up the fields as described in Parameters for Optional Network Configuration, on page 16.

Step 3   Click **Submit All Changes**.

Parameters for Optional Network Configuration

The following table defines the function and usage of the access control parameters in the **Optional Network Configuration** section under the **Voice** > **System** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 3: Parameters for Optional Network Configuration

Parameter	Description and Default Value
Host Name	The hostname of the server that the phone uses. • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Host_Name ua="rw">serverhost.com</Host_Name>` • On the phone web interface, enter the host name of the server to use. Default: Empty
Domain	The network domain of the Phone. If you're using LDAP, see LDAP Configuration. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Domain ua="rw">domainexample.com</Domain>` • In the phone web interface, enter the domain of the phone. Default: Empty
DNS Server Order	Specifies the sequence for selecting the DNS server. Perform one of the following: • Manual, DHCP • Manual • DHCP, Manual • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<DNS_Server_Order ua="na">Manual,DHCP</DNS_Server_Order>` • In the phone web interface, specify the order that the phone follows to select the DNS server. Allowed values: Manual,DHCP|Manual|DHCP,Manual Default: Manual, DHCP
DNS Query Mode	Specifies the mode of DNS query. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<DNS_Query_Mode ua="na">Parallel</DNS_Query_Mode>` • In the phone web interface, select the mode of DNS query. Allowed values: Parallel|Sequential Default: Parallel

Parameter	Description and Default Value
DNS Caching Enable	Enables or disables DNS caching. When enabled, the DNS query results are cached. The phone retrieves the local DNS cache until the local cache is expired. When disabled, the phone always performs DNS queries. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<DNS_Caching_Enable ua="na">Yes</DNS_Caching_Enable>` • In the phone web interface, set this field to **Yes** or **No** to enable or disable DNS caching. Allowed values: Yes|No Default: Yes
Switch Port Config	Allows you to select speed and duplex of the network port. Values are: • Auto • 10 HALF • 10 FULL • 100 HALF • 100 FULL Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Switch_Port_Config ua="na">AUTO</Switch_Port_Config>` • On the phone web interface, select the speed for the port or select **Auto** to allow the system to select the speed. Default: Auto
Enable PC Port Mirror	Enables or disables PC Port mirroring on the phone. When set to **Yes**, you can see the packets on the phone. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Enable_PC_Port_Mirror ua="na">No</Enable_PC_Port_Mirror>` • In the phone web interface, set this field to **Yes** or **No** to enable or disable PC port mirroring on the phone. Allowed values: Yes|No Default: No
Syslog Server	See System Log Parameters.
Syslog identifier	See System Log Parameters.

Parameter	Description and Default Value
Primary NTP Server	IP address or name of the primary NTP server used to synchronize its time. You can set primary NTP server for both IPv4 and IPv6. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Primary_NTP_Server ua="rw">192.168.1.10</Primary_NTP_Server>` • In the phone web interface, specify the IP address or host name of the NTP server. Default: Blank
Secondary NTP Server	IP address or name of the secondary NTP server used to synchronize its time. You can set primary NTP server for both IPv4 and IPv6. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Secondary_NTP_Server ua="rw">192.168.1.11</Secondary_NTP_Server>` • In the phone web interface, specify the IP address or host name of the NTP server. Default: Blank
Use Config TOS	This field controls whether the phone uses the Time of Service (TOS) parameters on the **Ext (n)** tab. Set this field to **Yes** when you want the phones to use the TOS configuration specified on the **Ext (n)** tab. Otherwise, set this field to **No**. • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Use_Config_TOS ua="na">No</Use_Config_TOS>` • In the phone web interface, select Yes or No as needed. Allowed values: Yes|No Default: No

XML Services

The phones provide support for XML services, such as an XML Directory Service or other XML applications. For XML services, only HTTP and HTTPS support is available.

The following Cisco XML objects are supported:

- CiscoIPPhoneMenu
- CiscoIPPhoneText
- CiscoIPPhoneInput
- CiscoIPPhoneDirectory

- CiscoIPPhoneIconMenu

- CiscoIPPhoneStatus

- CiscoIPPhoneExecute

- CiscoIPPhoneImage

- CiscoIPPhoneImageFile

- CiscoIPPhoneGraphicMenu

- CiscoIPPhoneFileMenu

- CiscoIPPhoneStatusFile

- CiscoIPPhoneResponse

- CiscoIPPhoneError

- CiscoIPPhoneGraphicFileMenu

- Init:CallHistory

- EditDial:n

The full list of supported URIs is contained in *Cisco Unified IP Phone Services Application Development Notes for Cisco Unified Communications Manager and Multiplatform Phones*, located here:

XML Directory Service

When an XML URL requires authentication, use the parameters **XML UserName** and **XML Password**.

The parameter **XML UserName** in XML URL is replaced by $XML UserName.

For example:

The parameter XML UserName is **cisco**. The XML Directory Service URL is **http://www.sipurash.compath?username=$XML_User_Name**.

This results in the request URL: `http://www.sipurash.com/path?username=cisco.`

Configure a Phone to Connect to an XML Application

You can also configure the parameters in the configuration file (cfg.xml) as defined in

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 In the **XML Service** section, configure the **XML Application Service Name** and **XML Application Service URL** fields as defined in Parameters for XML Applications, on page 21.

Step 3 (Optional) Specify the username and password to authenticate XML service in the **XML User Name** and **XML Password** fields as defined in Parameters for XML Applications, on page 21.

Step 4 (Optional) Enable and configure authentication for CGI/Execute URL via Post from an external application (for example, a web application) to the phones.

Configure the **CISCO XML EXE Enable** and **CISCO XML EXE Auth Mode** fields as defined in Parameters for XML Applications, on page 21.

Step 5 Click **Submit All Changes**.

Parameters for XML Applications

The following table defines the function and usage of the XML application parameters in the **XML Service** section under the **Voice** > **Phone** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 4: Parameters for XML Applications

Parameter	Description
XML Application Service Name	Name of the XML application. The name displays on the phone as a web application choice. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<XML_Application_Service_Name ua="na">XML_APP</XML_Application_Service_Name>` • In the phone web interface, enter a name for the XML application. Default: Empty
XML Application Service URL	The URL where the XML application is located. Macro variables are supported in XML URLs. For the valid macro variables, see Macro Variables, on page 23. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<XML_Application_Service_URL ua="na">XML_APP</XML_Application_Service_URL>` • In the phone web interface, enter the URL for the XML application. Default: Empty

Parameter	Description
XML User Name	XML service username for authentication purposes. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<XML_User_Name ua="na">username</XML_User_Name>` • In the phone web interface, enter the usename used for authenticating XML service. Default: Empty

XML Password	XML service password for the specified XML User Name. The password you entered in this field shows in the configuration file (cfg.xml) as
	
	`<!--`
	`<XML_Password ua="na">*************</XML_Password>`
	`-->`
	
	Default: Empty

CISCO XML EXE Enable	Specifies whether authentication is required to access the XML application server. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<CISCO_XML_EXE_Enable ua="na">Yes</CISCO_XML_EXE_Enable>` • In the phone web interface, set it to **Yes** or **No** to enable or disable authentication. Allowed values: No Default: No
CISCO XML EXE Auth Mode	Specifies the authentication mode for Cisco XML EXE. The available options are: • Trusted—No authentication is performed regardless of the local credential. • Local Credential—Authentication is based on the digest authentication using the local credential, if set. If the local credential is not set, then no authentication is performed. • Remote Credential—Authentication is based on the digest authentication using the remote credential as set in the XML application on the web page (to access an XML application server). Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<CISCO_XML_EXE_Auth_Mode ua="na">Local Credential</CISCO_XML_EXE_Auth_Mode>` • In the phone web interface, select an authentication mode. Allowed values: Trusted|Local Credential|Remote Credential Default: Local Credential

Macro Variables

You can use macro variables in XML URLs. The following macro variables are supported:

- User ID—UID1, UID2 to UIDn

- Display name—DISPLAYNAME1, DISPLAYNAME2 to DISPLAYNAMEn

- Auth ID—AUTHID1, AUTHID2 to AUTHIDn

- Proxy—PROXY1, PROXY2 to PROXYn

- MAC Address using lowercase hex digits—MA

- Product Name—PN

- Product Series Number—PSN

- Serial Number—SERIAL_NUMBER

The following table shows the list of macros supported on the phones:

Macro Name	Macro Expansion
$	The form $$ expands to a single $ character.
A through P	Replaced by general-purpose parameters GPP_A through GPP_P.
SA through SD	Replaced by special purpose parameters GPP_SA through GPP_SD. These parameters hold keys or passwords used in provisioning. **Note** $SA through $SD are recognized as arguments to the optional resync URL qualifier, --key.
MA	MAC address using lowercase hex digits (000e08aabbcc).
MAU	MAC address using uppercase hex digits (000E08AABBCC).
MAC	MAC address using lowercase hex digits with a colon to separate hex digit pairs (00:0e:08:aa:bb:cc).
PN	Product Name; for example, IP Phone 7832.
PSN	Product Series Number; for example, 7832.
SN	Serial Number string; for example, 88012BA01234.
CCERT	SSL Client Certificate status, installed or not installed.
IP	IP address of the phone within its local subnet; for example, 192.168.1.100.
EXTIP	External IP of the phone, as seen on the internet; for example, 66.43.16.52.

Macro Name	Macro Expansion
SWVER	Software version string. Use the software version string to compare against the current phone's firmware load. Follow the format below: • For Firmware Release 11.3(1)SR1 and previous: sip*yyyy*.*11-0-1*MPP-*376* where *yyyy* indicates the phone model or phone series; *11* is the major version; *0* is the minor version; *1MPP* is the micro version; and *376* is the build number. • For Firmware Release 11.3(2) and later: sip*yyyy*.*11-3-2*MPP*0001-609* where *yyyy* indicates the phone model or phone series; *11* is the major version; *3* is the minor version; *2MPP0001* is the micro version; and *609* is the build number. There are two methods to compare firmware loads: • **With quotes, "$SWVER"**–Variable acts as a string in firmware load name comparisons. For `"$SWVER" eq "sipyyyy.11-2-1MPP-312.loads"` or `"$SWVER" eq "sipyyyy.11-3-2MPP0001-609.loads"`, the phone model number and the version numbers in the load name are part of the comparison. • **Without quotes, $SWVER**–Variable is parsed to determine a build number, plus major, minor, and micro revision numbers. For example, when the `sip88xx.11-3-2MPP0001-598.loads` and `sip8845_65.11-3-2MMP0001-598.loads` firmware names are parsed, the result ignores the model number and load number. The result for both firmware names yields a major revision=`11`, minor revision=`3`, micro revision=`2MPP0001`, and build number=`598`. See more information about firmware version comparison, see Macro Expansion Variables.
HWVER	Hardware version string; for example, 1.88.1.
PRVST	Provisioning State (a numeric string): • -1 = explicit resync request • 0 = power-up resync • 1 = periodic resync • 2 = resync failed, retry attempted
UPGST	Upgrade State (a numeric string): • 1 = first upgrade attempt • 2 = upgrade failed, retry attempt
UPGERR	Result message (ERR) of previous upgrade attempt; for example, http_get failed.

Macro Name	Macro Expansion
PRVTMR	Seconds since last resync attempt.
UPGTMR	Seconds since last upgrade attempt.
REGTMR1	Seconds since Line 1 lost registration with SIP server.
REGTMR2	Seconds since Line 2 lost registration with SIP server.
UPGCOND	Legacy macro name.
SCHEME	File access scheme (TFTP, HTTP, or HTTPS, obtained after parsing resync or upgrade URL).
METH	Deprecated alias for SCHEME, do not use.
SERV	Request target server hostname.
SERVIP	Request target server IP address (following DNS lookup).
PORT	Request target UDP/TCP port.
PATH	Request target file path.
ERR	Result message of resync or upgrade attempt.
UIDn	The contents of the Line n UserID configuration parameter.
ISCUST	If unit is customized, value=1, otherwise 0. **Note** Customization status viewable on Web UI Info page.
INCOMINGNAME	Name associated with first connected, ringing, or inbound call.
REMOTENUMBER	Phone number of first connected, ringing, or inbound call. If there are multiple calls, the data associated with the first call found is provided.
DISPLAYNAMEn	The contents of the Line N Display Name configuration parameter.
AUTHIDn	The contents of the Line N auth ID configuration parameter.

Shared Lines

A shared line is a directory number that appears on more than one phone. You can create a shared line by assigning the same directory number to various phones.

Incoming calls display on all phones that share a line, and anyone can answer the call. Only one call remains active at a time on a phone.

Call information displays on all phones that are sharing a line. If somebody turns on the privacy feature, you do not see the outbound calls made from the phone. However, you see inbound calls to the shared line.

All phones with a shared line ring when a call is made to the line. If you place the shared call on hold, anyone shared with the line can resume the call by pressing ▮▮ or the **Resume** softkey.

The following shared line features are supported:

- Line Seizure
- Public Hold
- Private Hold
- Silent Barge (only through enabled programmable softkey)

The following features are supported as for a private line

- Transfer
- Conference
- Call Park / Call Retrieve
- Call Pickup
- Do Not Disturb
- Call Forward

You can configure each phone independently. Account information is usually the same for all IP phones, but settings such as the dial plan or preferred codec information can vary.

Configure a Shared Line

You can create a shared line by assigning the same directory number to more than one phone on the phone web page.

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code. To configure each parameter, see the syntax of the string in Parameters for Configuring a Shared Line, on page 27.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Ext(n)**, where **(n)** is the number of an extension to share.

Step 2   In the **General** section, set the **Line Enable** parameter as described in the Parameters for Configuring a Shared Line, on page 27 table.

Step 3   In the **Share Line Appearance** section, set **Share Ext**, **Shared User ID field**, **Subscription Expires**, and **Restrict MWI** parameters as described in the Parameters for Configuring a Shared Line, on page 27 table.

Step 4   In the **Proxy and Registration** section, enter the IP address of the proxy server in the **Proxy** field.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Proxy_1_ ua="na">as1bsoft.sipurash.com</Proxy_1_>
```

Example for proxy server address: as1bsoft.sipurash.com

Step 5 In the **Subscriber Information** section, enter the **Display Name** and **User ID** (extension number) for the shared extension.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Display_Name_1_ ua="na">name</Display_Name_1_>
<User_ID_1_ ua="na">4085273251</User_ID_1_>
```

Step 6 In the **Miscellaneous Line Key Settings** section, set **SCA Barge-In Enable** parameter as described in the table.

Step 7 Click **Submit All Changes.**

Parameters for Configuring a Shared Line

The following table describes the parameters in the **Voice** > **Ext(n)** tab of the phone web page.

The following table defines the function and usage of Shared Line parameters in the General and Share Line Appearance sections under the Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

Table 5: Parameters for Shared Lines

Parameter	Description

Line Enable	Enables a line for the service.
	
	Perform one of the following:
	
	    • In the phone web interface, select **yes** to enable. Otherwise, select **No**.
	
	    • In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	```<Line_Enable_1_ ua="na">Yes</Line_Enable_1_>```
	
	Valid values: Yes|No
	
	Default: Yes

Share Ext	Indicates whether other Cisco IP phones share this extension is, or the extension is private.
	
	Perform one of the following:
	
	    • In the phone web interface, select **yes** to enable. Otherwise, select **No**.
	
	    • In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	```<Share_Ext_1_ ua="na">No</Share_Ext_1_>```
	
	If you set **Share Ext** to **No**, this extension is private and doesn't share calls, regardless of the **Share Line Appearance** setting. If you set this extension to **Yes**, calls follow the **Share Line Appearance** setting.
	
	Valid values: Yes|No
	
	Default: Yes

Parameter	Description

Shared User ID	The user identified assigned to the shared line appearance.
	
	Perform one of the following:
	
	    • In the phone web interface, enter the user ID.
	
	    • In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	    `<Shared_User_ID_1_ ua="na">Shared UserID</Shared_User_ID_1`>

Subscription Expires	Number of seconds before the SIP subscription expires. Before the subscription expiration, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension.
	
	Perform one of the following:
	
	    • In the phone web interface, enter the value in seconds.
	
	    • In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	    `<Subscription_Expires_1_ ua="na">3600</Subscription_Expires_1_>`
	
	Valid values: An integer from 10 through 65535
	
	Default: 3600 seconds

Restrict MWI (Message Waiting Indicator)	Indicates the message waiting indicator lights only for messages on private.
	
	Perform one of the following:
	
	    • In the phone web interface, select **Yes** to enable. When enabled the message waiting indicator lights only for messages on private. Otherwise, select **No**.
	
	    • In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	    `<Restrict_MWI_1_ ua="na">No</Restrict_MWI_1_>`
	
	Valid values: Yes|No
	
	Default: No

The following table describes the parameters in the **Voice** > **Phone** tab of the phone web page.

Table 6: Miscellaneous Line Key Settings

Parameter	Description

SCA Barge-In Enable	Enables the SCA Barge-In. Perform one of the following: • In the phone web interface, select **Yes** to enable. Otherwise, select **No**. • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<SCA_Barge-In-Enable ua="na">No</SCA_Barge-In-Enable>` Valid values: Yes|No Default: No

Add Dialog-Based Shared Line Appearance

You can now enable dialog-based shared line, so that the phones in the shared line can subscribe to the dialog event package.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **SIP**.

Step 2   In the **SIP Parameters** section, set the **Share Line Event Package Type** parameter to **Dialog** to subscribe the phone to the dialog event package.

You can also set the parameter to **Call-Info** and the phone retains the legacy behavior.

Default value: **Call-Info**

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

`<Share_Line_Event_Package_Type ua="na">Dialog</Share_Line_Event_Package_Type>`

Step 3   Click **Submit All Changes**.

Assign a Ringtone to an Extension

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code. To configure each parameter, see the syntax of the string in .

Before you begin

Access the Phone Web Interface.

Procedure

Step 1	Select **Voice** > **Ext(n)**, where **(n)** is the number of a phone extension.
Step 2	In the **Call Feature Settings** section, select the **Default Ring** parameter from the list or select no ring.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Default_Ring_3_ ua="rw">1</Default_Ring_3_>
```

Step 3	Select **Voice** > **Phone**.
Step 4	In the **Ringtone** section, set the **Ring(n)** and **Silent Ring Duration** parameters as described in the table.
Step 5	Click **Submit All Changes**.

Parameters for Ringtone

The following table describes the parameters for **Ringtone**.

Table 7: Parameters for Ringtone

Parameter	Description

Ring1 to Ring12	Ring tone scripts for various ringtones.
	
	In the phone configuration XML file (cfg.xml), enter a string in this format:
	
	`<!-- Ringtone -->`
	`<Ring1 ua="na">n=Sunrise;w=file://Sunrise.rwb;c=1</Ring1>`
	`<Ring2 ua="na">n=Chirp 1;w=file://chirp1.raw;c=1</Ring2>`
	`<Ring3 ua="na">n=Chirp 2;w=file://chirp2.raw;c=1</Ring3>`
	`<Ring4 ua="na">n=Delight;w=file://Delight.rwb;c=1</Ring4>`
	`<Ring5 ua="na">n=Evolve;w=file://Evolve.rwb;c=1</Ring5>`
	`<Ring6 ua="na">n=Mellow;w=file://Mellow.rwb;c=1</Ring6>`
	`<Ring7 ua="na">n=Mischief;w=file://Mischief.rwb;c=1</Ring7>`
	`<Ring8 ua="na">n=Reflections;w=file://Reflections.rwb;c=1</Ring8>`
	`<Ring9 ua="na">n=Ringer;w=file://Ringer.rwb;c=1</Ring9>`
	`<Ring10 ua="na">n=Ascent;w=file://Ascent.rwb;c=1</Ring10>`
	`<Ring11 ua="na">n=Are you there;w=file://AreYouThereF.raw;c=1</Ring11>`
	`<Ring12 ua="na">n=Chime;w=file://Chime.raw;c=1</Ring12>`
	`<Silent_Ring_Duration ua="na">60</Silent_Ring_Duration>`

Parameter	Description
Silent Ring Duration	Controls the duration of the silent ring. For example, if the parameter is set to 20 seconds, the phone plays the silent ring for 20 seconds then sends 480 response to INVITE message. In the phone configuration XML file (cfg.xml), enter a string in this format: **<Ring1 ua="na">n=Sunrise;w=file://Sunrise.rwb;c=1</Ring1>** **<Silent_Ring_Duration ua="na">60</Silent_Ring_Duration>**

Add Distinctive Ringtone

You can configure the characteristics of each ring tone using a ring tone script. When the phone receives SIP Alert-INFO message and the message format is correct, then the phone plays the specified ringtone. Otherwise, the phone plays the default ringtone.

Procedure

In a ring tone script, assign a name for the ring tone and add the script to configure a distinctive ringtone in the format:

```
n=ring-tone-name;h=hint;w=waveform-id-or-path;c=cadence-id;b=break-time;t=total-time
```

where:

n = ring-tone-name that identifies this ring tone. This name appears on the Ring Tone menu of the phone. The same name can be used in a SIP Alert-Info header in an inbound INVITE request to tell the phone to play the corresponding ring tone. The name should contain the same characters allowed in a URL only.

h = hint used to SIP Alert-INFO rule.

w = waveform-id-or-path which is the index of the desired waveform to use in this ring tone. The built-in waveforms are:

- 1 = Classic phone with mechanical bell

- 2 = Typical phone ring

- 3 = Classic ring tone

- 4 = Wide-band frequency sweep signal

c = is the index of the desired cadence to play the given waveform. 8 cadences (1–8) as defined in <Cadence 1> through <Cadence 8>. Cadence-id can be 0 If w=3,4. Setting c=0 implies the on-time is the natural length of the ring tone file.

b = break-time that specifies the number of seconds to break between two bursts of ring tone, such as b=2.5.

t = total-time that specifies the total number of seconds to play the ring tone before it times out.

In the phone configuration XML file (cfg.xml), enter a string in this format:

```
<!-- Ringtone -->
<Ring1 ua="na">n=Sunrise;w=file://Sunrise.rwb;c=1</Ring1>
<Ring2 ua="na">n=Chirp 1;w=file://chirp1.raw;c=1</Ring2>
<Ring3 ua="na">n=Chirp 2;w=file://chirp2.raw;c=1</Ring3>
<Ring4 ua="na">n=Delight;w=file://Delight.rwb;c=1</Ring4>
<Ring5 ua="na">n=Evolve;w=file://Evolve.rwb;c=1</Ring5>
<Ring6 ua="na">n=Mellow;w=file://Mellow.rwb;c=1</Ring6>
<Ring7 ua="na">n=Mischief;w=file://Mischief.rwb;c=1</Ring7>
<Ring8 ua="na">n=Reflections;w=file://Reflections.rwb;c=1</Ring8>
<Ring9 ua="na">n=Ringer;w=file://Ringer.rwb;c=1</Ring9>
<Ring10 ua="na">n=Ascent;w=file://Ascent.rwb;c=1</Ring10>
<Ring11 ua="na">n=Are you there;w=file://AreYouThereF.raw;c=1</Ring11>
<Ring12 ua="na">n=Chime;w=file://Chime.raw;c=1</Ring12>
<Silent_Ring_Duration ua="na">60</Silent_Ring_Duration>
```

Enable Hoteling on a Phone

When you enable the hoteling feature of BroadSoft on the phone, the user can sign in to the phone as a guest. After the guest sign out of the phone, the user will switch back to the host user.

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Ext [n]** (where [n] is the extension number).

Step 2   In the **Call Feature Settings** section, set **Enable Broadsoft Hoteling** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Enable_Broadsoft_Hoteling_1_ua="na">Yes</Enable_Broadsoft_Hoteling_1>
```

Options: Yes and No

Default: No

Step 3   Set the amount of time (in seconds) that the user can be signed in as a guest on the phone in **Hoteling Subscription Expires**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Hoteling_Subscription_Expires_1_ua="na">3600</Hoteling_Subscription_Expires_1>
```

Valid values: An integer from 10 through 86400

Default: 3600

Step 4   Click **Submit All Changes**.

Enable Flexible Seating on a Phone

With the Flexible Seating feature of BroadSoft, the phone downloads and is reconfigured with Flexible Seating Guest's device files when the guest is associated with the host. The phone is treated as an alternate device of the guest. The call originations from guest's primary device are also allowed. The guest's primary device is also alerted on incoming calls to the guest. For more information, see the BroadSoft documentation.

In addition, with the feature enabled on the phone, the phone can cache the user credentials for the LDAP directory. If the cache contains the user credentials, the guest user can bypass the sign-in procedure to access the LDAP directory. The cache can store up to 50 user credentials. The phone removes the least-used credentials when the cache size limit is reached.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1	Select **Voice** > **Ext [n]** (where [n] is the extension number).
Step 2	In the **Call Feature Settings** section, set **Enable Broadsoft Hoteling** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Enable_Broadsoft_Hoteling_1_ua="na">Yes</Enable_Broadsoft_Hoteling_1>
```

Options: Yes and No

Default: No

Step 3	Click **Submit All Changes**.

Enable Extension Mobility on a Phone

With the Extension Mobility (EM) feature enabled on the phone, any user can sign in to the phone other than their own in the same network. In this scenario, the phone can be shared with other users. After the users sign in, they can see their own line number displayed on the phone screen, and their contacts in the personal address directory.

In addition, the phone can cache the user credentials for the LDAP directory when the user signs into the phone with the feature. If the cache contains the user credentials, the user can bypass the sign-in procedure to access the LDAP directory. The cache can store up to 50 user credentials. The phone removes the least-used credentials when the cache size limit is reached.

You can also configure the parameters in the phone configuration file with XML (cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **Extension Mobility** section, set **EM Enable** to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<EM_Enable ua="na">Yes</EM_Enable>
```

Options: Yes and No

Default: No

Step 3   Set the amount of time (in minutes) that the user can be signed in on the phone in **Session Timer(m)**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Session_Timer_m_ ua="na">480</Session_Timer_m_>
```

Default: 480

Step 4   Click **Submit All Changes**.

Set the User Password

Configure a password so the phone is protected and secured. Both administrators and users can configure a password and control access to the phone.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **System**.

Step 2   Under the section **System Configuration**, locate the parameter **User Password**, and click **Change Password** next to the parameter.

Step 3   Enter the current user password in the **Old Password** field.

If you don't have a password, keep the field empty.

Step 4   Enter a new password in the **New Password** field.

Step 5   Click **Submit**.

The message `Password has been changed successfully.` will display in the web page. The web page will refresh in several seconds.

After you set the user password, this parameter displays the following in the phone configuration XML file (cfg.xml):

```
<!--
 <User_Password ua="rw">*************</User_Password>
-->
```

Download Problem Reporting Tool Logs

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

If you are working with Cisco TAC to troubleshoot a problem, they typically require the logs from the Problem Reporting Tool to help resolve the issue.

To issue a problem report, users access the Problem Reporting Tool and provide the date and time that the problem occurred, and a description of the problem. You need to download the problem report from the Configuration Utility page.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Info** > **Debug Info** > **Device Logs**.

Step 2   In the **Problem Reports** area, click the problem report file to download.

Step 3   Save the file to your local system and open the file to access the problem reporting logs.

Configure Problem Report Tool

You must use a server with an upload script to receive the problem reports that the user sends from the phone.

- If the URL specified in the **PRT Upload Rule** field is valid, users get a notification alert on the phone UI saying that they have successfully submitted the problem report.

- If the **PRT Upload Rule** field is empty or has an invalid URL, users get a notification alert on the phone UI saying that the data upload failed.

The phone uses an HTTP/HTTPS POST mechanism, with parameters similar to an HTTP form-based upload. The following parameters are included in the upload (utilizing multipart MIME encoding):

- devicename (example: "SEP001122334455")

- serialno (example: "FCH12345ABC")

- username (The user name is either the **Station Display Name** or the **User ID** of the extension. The **Station Display Name** is first considered. If this field is empty, then the **User ID** is chosen.)

• prt_file (example: "probrep-20141021-162840.tar.gz")

You can generate PRT automatically at specific intervals and can define the PRT file name.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the Parameters for Configure Problem Report Tool, on page 37 table.

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
<?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.");
}

?>
```

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1	Select **Voice** > **Provisioning**.
Step 2	In the **Problem Report Tool** section, set the fields as described in the Parameters for Configure Problem Report Tool, on page 37 table.
Step 3	Click **Submit All Changes**.

Parameters for Configure Problem Report Tool

The following table defines the function and usage of Configure Problem Report Tool parameters in the Problem Report Tool section under the Voice > Provisioning tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

Table 8: Parameters for Configure Problem Report Tool

Parameter	Description

PRT Upload Rule	Specifies the path to the PRT upload script.
	
	If the **PRT Max Timer** and **PRT Upload Rule** fields are empty, the phone doesn't generate the problem reports automatically unless user manually performs the generation.
	
	Perform one of the following:
	
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	`<PRT_Upload_Rule ua="na">https://proxy.example.com/prt_upload.php</PRT_Upload_Rule>`
	
	• In the phone web page, enter the path in the format:
	
	`https://proxy.example.com/prt_upload.php`
	
	or
	
	`http://proxy.example.com/prt_upload.php`
	
	Default: Empty

PRT Upload Method	Determines the method used to upload PRT logs to the remote server. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<PRT_Upload_Method ua="na">POST</PRT_Upload_Method>` • In the phone web page, select **POST** or **PUT** methods to upload the logs to the remote server. Valid values: POST and PUT Default: POST

Parameter	Description
PRT Max Timer	Determines at what interval (minutes) the phone starts generating problem report automatically. If the **PRT Max Timer** and **PRT Upload Rule** fields are empty, the phone doesn't generate the problem reports automatically unless user manually performs the generation. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<PRT_Max_Timer ua="na">30</PRT_Max_Timer>` • In the phone web page, enter the interval duration in minutes. Valid value range: 15 minutes to 1440 minutes Default: Empty

PRT Name	Defines a name for the generated PRT file.
	
	Perform one of the following:
	
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	`<PRT_Name ua="na">prt-string1-$MACRO</PRT_Name>`
	
	Enter the name in the format:
	
	`prt-string1-$MACRO`
	
	• In the phone web page, enter the name in the format:
	
	`prt-string1-$MACRO`
	
	Default: Empty

PRT HTTP Header	Specifies the HTTP header for the URL in **PRT Upload Rule**.
	
	The parameter value is associated with **PRT HTTP Header Value**.
	
	Only when both parameters are configured, the HTTP header is included in the HTTP request.
	
	Perform one of the following:
	
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	`<PRT_HTTP_Header ua="na">x-cisco-spark-canary-opts</PRT_HTTP_Header>`
	
	• In the phone web page, enter the HTTP header in the format:
	
	`x-cisco-spark-canary-opts`
	
	Valid value range: a-z, A-Z, 0-9, underscore (_), and hyphen (-)
	
	Default: Empty

Parameter	Description

PRT HTTP Header Value	Sets the value of the specified HTTP header.
	
	The parameter value is associated with **PRT HTTP Header**.
	
	Only when both parameters are configured, the HTTP header is included in the HTTP request.
	
	Perform one of the following:
	
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	`<PRT_HTTP_Header_Value`
	`ua="na">always</PRT_HTTP_Header_Value>`
	
	• In the phone web page, enter the value in the format:
	
	`always`
	
	Valid value range: a-z, A-Z, 0-9, underscore (_), comma (,), semicolon (;), equal (=), and hyphen (-)
	
	Note Except for the underscore (_), the first character must not be a special character.
	
	Default: Empty

Server-Configured Paging

You can configure a paging group on a server so that users can page a group of phones. For more details, refer to your server documentation.

Configure Multicast Paging

You can set up Multicast paging to allow users to page to phones. The page can go to all phones or a group of phones in the same network. Any phone in the group can initiate a multicast paging session. The page is received only by the phones that are set to listen for the paging group.

You can add a phone to up to 10 paging groups. Each paging group has a unique multicast port and number. The phones within a paging group must subscribe to the same multicast IP address, port, and multicast number.

You configure the priority for the incoming page from a specific group. When a phone is active and an important page must be played, the user hears the page on the active audio path.

When multiple paging sessions occur, they are answered in chronological order. After the active page ends, the next page is automatically answered. When do not disturb (DND) is enabled, the phone ignores any incoming paging.

You can specify a codec for the paging to use. The supported codecs are G711a, G711u, G722, and G729. If you don't specify the codec, paging uses G711u by default.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in .

Before you begin

- Make sure that your network supports multicast so that all devices in the same paging group are able to receive paging.

- For Wi-Fi networks, enable and properly configure the access point for multicast.

- Make sure that all the phones in a paging group are in the same network.

- Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1	Select **Voice** > **Phone**.
Step 2	Go to the **Multiple Paging Group Parameters** section.
Step 3	Enter multicast paging scripts as defined in Parameters for Multiple Paging Group, on page 40.
Step 4	Click **Submit All Changes**.

Parameters for Multiple Paging Group

The following table defines the function and usage of the multiple paging group parameters in the **Voice** > **Phone** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 9: Multiple Paging Group Parameters

Feature	Description
Group 1 Paging Script – Group 10 Paging Script	

Feature	Description

	Enter a string to configure the phone to listen for and initiate multicast paging. You can add a phone to up to 10 paging groups. Enter the script in this format:
	
	`pggrp=<multicast-address>:<port>;<name=group_name>;<num=multicast_number>;`
	`<listen=boolean_value>;<pri=priority_level>;<codec=codec_name>;`
	
	Example script:
	
	`pggrp=224.168.168.168:34560;name=GroupA;num=500;listen=yes;pri=1;codec=g711a;`
	
	• Multicast IP address (multicast-address) and port (port)—Enter the multicast IP address and the port specified on your paging server. The port number must be unique for each group and an even number within 1000 and 65534.
	
	Make sure that you set the same multicast IP address and port for all the phones within a paging group. Otherwise, the phones can't receive paging.
	
	• Paging group name (name)—Optionally enter the name of the paging group. The name helps you identify the paging group the phone is in when you have multiple paging groups.
	
	• Multicast number (num)—Specify the number for the phone to listen for multicast paging and initiate a multicast paging session. Assign the same multicast number to all the phones within the group. The number must comply to the dial plan specified for the line to initiate a multicast.
	
	• Listen status (listen)—Specify whether the phone listens for paging from this group. Set this parameter to **yes** to make the phone listen for the paging. Otherwise, set it to **no**, or don't include this parameter in the script.
	
	• Priority (pri)—Specify priority between paging and phone call. If you don't specify the priority or don't include this parameter in the script, the phone uses priority **1**. The four priority levels are:
	
	  • **0**: Paging takes precedent over phone call. When the phone is on an active call, an incoming paging places the active call on hold. The call resumes when the paging ends.
	
	  • **1**: When the phone receives an incoming paging on an active call, the user hears the mix of the paging and the call.
	
	  • **2**: The user is alerted with the paging tone when receiving an incoming paging on an active line. The incoming paging isn't answered unless the active call is put on hold or ends.
	
	  • **3**: The phone ignores the incoming paging without any alert when the phone is on an active call.
	
	• Audio codec (codec)—Optionally specify the audio codec for the multicast paging to use. The supported codecs are G711a, G711u, G722, and G729. If you don't specify the codec or don't include the codec parameter in the script, the phone uses G711u codec.
	
	Perform one of the following:
	
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:

Feature	Description

	`<Group_1_Paging_Script`
	`ua="na">pggrp=224.168.168.168:34560;name=Group_1;`
	`num=800;listen=yes;pri=1;codec=g722</Group_1_Paging_Script>`
	
	• In the phone web interface, configure this field with a valid string.
	
	Default: Empty

Configure a Phone to Accept Pages Automatically

The Single Paging or Intercom feature enables a user to directly contact another user by phone. If the phone of the person being paged has been configured to accept pages automatically, the phone does not ring. Instead, a direct connection between the two phones is automatically established when paging is initiated.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **User**.

Step 2   In the **Supplementary Services** section, choose **Yes** for the **Auto Answer Page** parameter.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

`<Auto_Answer_Page ua="na">Yes</Auto_Answer_Page>`

Options: Yes and No

Default: Yes

Step 3   Click **Submit All Changes**.

Manage Phones with TR-069

You can use the protocols and standards defined in Technical Report 069 (TR-069) to manage phones. TR-069 explains the common platform for management of all phones and other customer-premises equipment (CPE) in large-scale deployments. The platform is independent of phone types and manufacturers.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the Parameters for TR-069 Configuration, on page 45 table.

As a bidirectional SOAP/HTTP-based protocol, TR-069 provides the communication between CPEs and Auto Configuration Servers (ACS).

For TR-069 Enhancements, see TR-069 Parameter Comparison.

Phone Features and Setup

View TR-069 Status

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **TR-069**.

Step 2   Set up the fields as described in Parameters for TR-069 Configuration, on page 45 table.

Step 3   Click **Submit All Changes**.

View TR-069 Status

When you enable TR-069 on a user phone, you can view status of TR-069 parameters on the phone web interface.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the Parameters for TR-069 Configuration, on page 45 table.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Select **Info** > **Status** > **TR-069 Status**.

You can view status of TR-069 parameters in Parameters for TR-069 Configuration, on page 45 table.

Phone Features and Setup

44

Parameters for TR-069 Configuration

The following table defines the function and usage of Call Center Agent Setup parameters in the ACD Settings section under the Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

Table 10: Parameters for TR-069 Configuration

Parameter	Description
Enable TR-069	Settings that enables or disables the TR-069 function. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Enable_TR-069 ua="na">No</Enable_TR-069>` • In the phone web page, select **Yes** to enable this feature and select **No** to disable it. Valid values: Yes|No Default: No
ACS URL	URL of the ACS that uses the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when it uses SSL or TLS. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<ACS_URL ua="na">https://acs.url.com</ACS_URL>` • In the phone web page, enter a valid HTTP or HTTPS URL of the ACS. Default: Blank
ACS Username	Username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<ACS_Username ua="na">acs username</ACS_Username>` • In the phone web page, enter a valid username for HTTPS-based authentication of the CPE. Default: admin

Parameter	Description
ACS Password	Password to access to the ACS for a specific user. This password is used only for HTTP-based authentication of the CPE. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<ACS_Password ua="na"/>` • In the phone web page, enter a valid password for HTTPS-based authentication of the CPE. Default: Blank
ACS URL In Use	URL of the ACS that is currently in use. This is a read-only field.
Connection Request URL	This is read-only field showing the URL of the ACS that makes the connection request to the CPE.
Connection Request Username	Username that authenticates the ACS that makes the connection request to the CPE. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Connection_Request_Password ua="na"/>` • In the phone web page, enter a valid username that authenticates the ACS.
Connection Request Password	Password used to authenticate the ACS that makes a connection request to the CPE. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Connection_Request_Password ua="na"/>` • In the phone web page, enter a valid password that authenticates the ACS. Default: Blank

Parameter	Description
Periodic Inform Interval	Duration in seconds of the interval between CPE attempts to connect to the ACS when Periodic Inform Enable is set to yes. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Periodic_Inform_Interval ua="na">20</Periodic_Inform_Interval>` • In the phone web page, enter a valid duration in seconds. Default: 20
Periodic Inform Enable	Settings that enables or disables the CPE connection requests. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Periodic_Inform_Enable ua="na">Yes</Periodic_Inform_Enable>` • In the phone web page, select **Yes** to enable this feature and select **No** to disable it. Valid values: Yes|No Default: Yes
TR-069 Traceability	Settings that enables or disables TR-069 transaction logs. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<TR-069_Traceability ua="na">Yes</TR-069_Traceability>` • In the phone web page, select **Yes** to enable this feature and select **No** to disable it. Valid values: Yes|No Default: No

Parameter	Description
CWMP V1.2 Support	Settings that enables or disables CPE WAN Management Protocol (CWMP) support. If set to disable, the phone does not send any Inform messages to the ACS nor accept any connection requests from the ACS.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	`<CWMP_V1.2_Support ua="na">Yes</CWMP_V1.2_Support>`
	• In the phone web page, select **Yes** to enable this feature and select **No** to disable it.
	Valid values: Yes|No
	Default: Yes
TR-069 VoiceObject Init	Settings to modify voice objects.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	`<TR-069_VoiceObject_Init ua="na">Yes</TR-069_VoiceObject_Init>`
	• In the phone web page, select **Yes** to initialize all voice objects to factory default values or select **No** to retain the current values.
	Valid values: Yes|No
	Default: Yes
TR-069 DHCPOption Init	Settings to modify DHCP settings.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	`<TR-069_DHCPOption_Init ua="na">Yes</TR-069_DHCPOption_Init>`
	• In the phone web page, select **Yes** to initialize the DHCP settings from the ACS or select **No** to retain the current DHCP settings.
	Valid values: Yes|No
	Default: Yes

Parameter	Description
BACKUP ACS URL	Backup URL of the ACS that uses the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACScertificate when it uses SSL or TLS.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:

	`<BACKUP_ACS_URL`
	`ua="na">https://acs.url.com</BACKUP_ACS_URL>`
	• In the phone web page, enter a valid URL that uses the CPE WAN Management Protocol.

	Default: Blank
BACKUP ACS User	Backup username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:

	`<BACKUP_ACS_User ua="na">backup`
	`username</BACKUP_ACS_User>`
	• In the phone web page, enter a valid username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol.

	Default: Blank
BACKUP ACS Password	Backup password to access to the ACS for a specific user. This password is used only for HTTP-based authentication of the CPE.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	`<BACKUP_ACS_Password ua="na"/>` • In the phone web page, enter a valid password that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol.
	Default: Blank
Note	If you do not configure the above parameters, you can also fetch them through DHCP options 60,43, and 125.

Enable Electronic Hookswitch

The Electronic Hookswitch feature enables users to use headsets that electronically connect a wireless headset to a phone. Typically, the headset requires a base that plugs into the phone and communicates with the headset. Here are the supported headsets:

- Plantronics Savi 740

- Jabra PRO920

- Jabra PRO9400

- Sennheiser DW Pro1

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **User**.

Step 2   In the **Audio Volume** section, set the **Electronic HookSwitch Control** parameter to **Yes** to enable the feature.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Ehook_Enable ua="na">Yes</Ehook_Enable>
```

Options: Yes and No

Default: No

Step 3   Click **Submit All Changes**.

Set up a Secure Extension

You can configure an extension to only accept secure calls. If the extension is configured to only accept secure calls then any calls the extension makes will be secure.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

- Make sure that **Secure Call Serv** is enabled (set to **Yes**) in the **Supplementary Services** area on the **Voice** > **Phone** tab.

  You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Secure_Call_Serv ua="na">Yes</Secure_Call_Serv>
```

- SIP transport with TLS can be set statically on the phone web page or automatically with information in the DNS NAPTR records. If the SIP transport parameter is set for the phone extension as TLS, the phone only allows SRTP. If the SIP transport parameter is set to AUTO, the phone performs a DNS query to get the transport method.

- Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Ext(n)**.

Step 2   In the **Call Feature Settings** section, in the **Secure Call Option** field, choose **Optional**, **Required**, or **Strict**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Secure_Call_Option_1_ ua="na">Optional</Secure_Call_Option_1_>
```

Options: Optional, Required, and Strict

- Optional ‐ Retains the current secure call option for the phone.

- Required ‐ Rejects nonsecure calls from other phones.

- Strict ‐ Allows SRTP only when SIP transport is set to **TLS**. Allows RTP only when SIP transport is **UDP/TCP**.

Default: Optional

Step 3   Click **Submit All Changes**.

Configure the SIP Transport

For SIP messages, you can configure each extension to use:

- a specific protocol
- the protocol automatically selected by the phone

When you set up automatic selection, the phone determines the transport protocol based on the Name Authority Pointer (NAPTR) records on the DNS server. The phone uses the protocol with the highest priority in the records.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1	Select **Voice** > **Ext(n)**, where n is an extension number.
Step 2	In the **SIP Settings** section, set the **SIP Transport** parameter to select a transport protocol for SIP messages.

You can configure this parameter in the phone configuration XML file (cfg.xml) with a string in this format:

```
<SIP_Transport_n_ ua="na">UDP</SIP_Transport_n_>
```

where n is the extension number.

Options: UDP, TCP, TLS, and Auto

AUTO allows the phone to select the appropriate protocol automatically, based on the NAPTR records on the DNS server.

Default: UDP

Step 3	Click **Submit All Changes**.

Block Non-Proxy SIP Messages to a Phone

You can disable the ability of the phone to receive incoming SIP messages from a non-proxy server. When you enable this feature, the phone only accepts SIP messages from:

- proxy server
- outbound proxy server
- alternative proxy server
- alternative outbound proxy server
- IN-Dialog message from proxy server and non-proxy server. For example: Call Session dialog and Subscribe dialog

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1	Select **Voice** > **System**.
Step 2	In the **System Configuration** section, set the **Block Nonproxy SIP** paramter to **Yes** to block any incoming non-proxy SIP messages except IN-dialog message. If you choose **No**, the phone does not block any incoming non-proxy SIP messages.

Set **Block Nonproxy SIP** to **No** for phones that use TCP or TLS to transport SIP messages. Nonproxy SIP messages transported over TCP or TLS are blocked by default.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

`<Auto_Answer_Page ua="na">Yes</Auto_Answer_Page>`

Options: Yes and No

Default: No

Step 3   Click **Submit All Changes**.

Configure a Privacy Header

A user privacy header in the SIP message sets user privacy needs from the trusted network.

You can set the user privacy header value for each line extension.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Extension**.

Step 2   In the **SIP Settings** section, set the **Privacy Header** parameter to set user privacy in the SIP message in the trusted network.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

`<Privacy_Header_2_ ua="na">header</Privacy_Header_2_>`

Options:

- Disabled (default)

- none—The user requests that a privacy service applies no privacy functions to this SIP message.

- header—The user needs a privacy service to obscure headers which cannot be purged of identifying information.

- session—The user requests that a privacy service provide anonymity for the sessions.

- user—The user requests a privacy level only by intermediaries.

- id—The user requests that the system substitute an id that doesn't reveal the IP address or host name.

Default: Disabled

Step 3   Click **Submit All Changes**.

Enable P-Early-Media Support

You can determine whether to include the P-Early-Media header in the SIP message of outgoing calls. The P-Early-Media header contains the status of the early media stream. If the status indicates that the network is blocking the early media stream, the phone plays the local ringback tone. Otherwise, the phone plays the early media while waiting for the call to be connected.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **Ext (n)**.

Step 2 In the **SIP Settings** section, set the **P-Early-Media Support** to **Yes** to control whether the P-Early-Media header is included in the SIP message for an outgoing call.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<P-Early-Media_Support_1_ ua="na">No</P-Early-Media_Support_1_>
```

Options: Yes and No

Default: No

Step 3 Click **Submit All Changes**.

Enable Peer Firmware Sharing

Peer Firmware Sharing (PFS) is a firmware distribution model which allows a Cisco IP phone to find other phones of the same model or series on the subnet and share updated firmware files when you need to upgrade multiple phones all at the same time. PFS uses Cisco Peer-to-Peer-Distribution Protocol (CPPDP) which is a Cisco proprietary protocol. With CPPDP, all the devices in the subnet form a peer-to-peer hierarchy, and then copy the firmware or the other files from peer devices to the neighboring devices. To optimize firmware upgrades, a root phone downloads the firmware image from the load server and then transfers the firmware to other phones on the subnet using TCP connections.

Peer firmware sharing:

• Limits congestion on TFTP transfers to centralized remove load servers.

• Eliminates the need to manually control firmware upgrades.

• Reduces phone downtime during upgrades when large numbers of phones are reset simultaneously.

Note
- Peer firmware sharing does not function unless multiple phones are set to upgrade at the same time. When a NOTIFY is sent with Event:resync, it initiates a resync on the phone. Example of an xml that can contain the configurations to initiate the upgrade:

  "Event:resync;profile="http://10.77.10.141/profile.xml
- When you set the Peer Firmware Sharing Log server to an IP address and port, the PFS specific logs are sent to that server as UDP messages. This setting must be done on each phone. You can then use the log messages when troubleshooting issues related to PFS.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Provisioning**.

Step 2   In the **Firmware Upgrade** section, set the parameters:

a)   Set the **Peer Firmware Sharing** parameter.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

`<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>`

Options: Yes and No

Default: Yes

b)   Set the **Peer Firmware Sharing Log Server** paramter to indicate the IP address and the port to which the UDP message is sent.

For example: 10.98.76.123:514 where, 10.98.76.123 is the IP address and 514 is the port number.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

`<Peer_Firmware_Sharing_Log_Server>192.168.5.5</ Peer_Firmware_Sharing_Log_Server>`

Peer_Firmware_Sharing_Log_Server specifies UDP Remote syslog server hostname and the port. The port defaults to the default syslog 514.

Step 3   Click **Submit All Changes**.

Specify the Profile Authentication Type

Profile Authentication allows phone users to resynchronize the provisioning profile onto the phone. Authentication information is required while the phone tries to resynchronize and download configuration

file for the first time and gets an HTTP or HTTPS 401 authentication error. When you enable this feature, the **Profile account setup** screen is displayed on the phone for the following situations:

- When the HTTP or HTTPs 401 authentication error occurs during first-time provisioning after the phone reboots

- When the profile account username and password are empty

- When there are no username and password in the Profile Rule

If the **Profile account setup** screen is missed or ignored, the user can also access the setup screen through the phone screen menu, or the **Setup** softkey, which displays only when no line on the phone is registered.

When you disable the feature, the **Profile account setup** screen doesn't display on the phone.

The username and password in the **Profile Rule** field have a higher priority than the profile account.

- When you provide a correct URL in the **Profile Rule** field without a username and password, the phone requires authentication or digest to resynchronize the profile. With the correct profile account, authentication passes. With an incorrect profile account, authentication fails.

- When you provide a correct URL in the **Profile Rule** field with a correct username and password, the phone requires authentication or digest to resynchronize the profile. The profile account is not used for phone resynchronization. Sign-in is successful.

- When you provide a correct URL in the **Profile Rule** field with an incorrect username and password, the phone requires authentication or digest to resynchronize the profile. The profile account isn't used for phone resynchronization. Sign-in always fails.

- When you provide an incorrect URL in the **Profile Rule** field, sign-in always fails.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

You can specify the profile authentication type from the phone administration web page.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **Provisioning**.

Step 2 In the **Configuration Profile** section, set the **Profile Authentication Type** parameter to specify the credentials to use for profile account authentication.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Profile_Authentication_Type ua="na">Disabled</Profile_Authentication_Type>
```

Options:

- **Disabled**: Disables the profile account feature.When this feature is disabled, the **Profile account setup** menu doesn't display on the phone screen.

- **Basic HTTP Authentication**: The HTTP login credentials are used to authenticate the profile account.

- **XSI Authentication**: XSI login credentials or XSI SIP credentials are used to authenticate the profile account. The authentication credentials depend on the XSI Authentication Type for the phone:

  When the XSI Authentication Type for the phone is set to Login Credentials, the XSI login credentials are used.

  When the XSI Authentication Type for the phone is set to SIP Credentials, the XSI SIP credentials are used.

Default: Basic HTTP Authentication

Step 3   Click **Submit All Changes**.

Control the Authentication Requirement to Access the Phone Menus

You can control if authentication is required to access phone menus.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   Set the **LCD Authentication** and **LCD Authentication Customization** sections as described in the Parameters for User Authentication Control, on page 57 table.

Parameters for User Authentication Control

The following table defines the function and usage of the parameters for user authentication control feature in the **LCD Authentication** and **LCD Authentication Customization** section under the **Voice** > **Phone** tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file (cfg.xml) with XML code to configure a parameter.

Table 11: Parameters for User Authentication Control

Parameter	Description

Require Authentication for LCD Menu Access	Controls whether the user requires authentication to access phone menus.
	
	Perform one of the following:
	
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	`<Require_Authentication_for_LCD_Menu_Access`
	`ua="na">Default</Require_Authentication_for_LCD_Menu_Access>`
	
	• On the phone web interface, select the required value.
	
	Allowed values: Default|Customized|No
	
	• **Default**—When selected, user needs to provide password and then sign in to access the phone menus that requires authentication. Phone continues to support all the functionalities that are supported in the releases prior to 11.3(2). Phone displays lock screen icon.
	
	To access any phone menus that require authentication, user needs to provide the password and press **Sign in**. The lock icon remains locked. After the user signs in, the lock icon is unlocked.
	
	• **Customized**—When selected, user requires authentication only to access **Profile rule** and **Factory reset** menus on the phone. Authenticaion control of these two menus also depends on the settings of the **Factory Reset Menu** menu and the **Profile Rule Menu** menu. User will not require any authentication to access other phone menus.
	
	• **No**—When selected, the **Sign in** menu, the **Sign out** menu, the lock icon, and the **Set password** menus are not available on the phone. User can access phone menus without any authentication.
	
	Default value: Default

Factory Reset Menu	Specifies if the user requires authentication to access **Factory reset** menu on the phone. You can customize this parameter to **Yes** or **No** only when you set the **Require Authentication for LCD Menu Access** parameter to **Customized**. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Factory_Reset_Menu ua="na">Yes</Factory_Reset_Menu>` • On the phone web interface, set this parameter to **Yes** or **No** as needed. Allowed values: Yes|No Default value: Yes

Parameter	Description
Profile Rule Menu	Specifies if the user requires authentication to access **Profile rule** menu on the phone. You can customize this parameter to **Yes** or **No** only when you set the **Require Authentication for LCD Menu Access** parameter to **Customized**. Perform one of the following: `<Profile_Rule_Menu ua="na">Yes</Profile_Rule_Menu>` • On the phone web interface, set this parameter to **Yes** or **No** as needed. Allowed values: Yes|No Default value: Yes

Silence an Incoming Call with Ignore Soft Key

You can add the **Ignore** softkey on the phone. User can press this softkey to silence an incoming call when busy and don't want to be disturbed. When the user presses the softkey, the phone stops ringing, but the user gets a visual alert, and, can answer the phone call.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.

Step 3   Enter the following values in the **Ringing Key List** field:

         answer|1;ignore|2;ignoresilent|3;

Step 4   Click **Submit All Changes**.

Move an Active Call from a Phone to Other Phones (Locations)

You can configure a phone to allow a call to seamlessly be moved from one desk phone(location) to another mobile phone or desk phone(location).

When you enable this feature, the **Anywhere** menu is added into the phone screen. The user can use this menu to add multiple phones as locations to the extension. When there is an incoming call in that extension, all the added phones will ring and the user can answer the incoming call from any location. The locations list also gets saved to the BroadWorks XSI server.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the Parameters for Moving Active Call to Other Locations, on page 61 table.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Ext(n)**.

Step 2   In the **XSI Line Service** section, set the **XSI Host Server**, **XSI Authentication Type**, **Login User ID**, **Login Password**, and **Anywhere Enable** parameters as described in the Parameters for Moving Active Call to Other Locations, on page 61 table.

If you select **SIP Credentials** for **XSI Authentication Type**, you need to enter subsriber **Auth ID** and **Password** in the **Subscriber Information** section.

Step 3   Click **Submit All Changes**.

Parameters for Moving Active Call to Other Locations

The following table defines the function and usage of Moving Active Call to Locations parameters in the XSI Line Service section under the Ext(n) tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

Table 12: Parameters for Moving Active Call to Locations

Parameter	Description

XSI Host Server	Enter the name of the server. For example:
	
	`xsi.iop1.broadworks.net`
	
	Note XSI Host Server uses http protocol by default. To enable XSI over HTTPS, you can specify https:// in the server.
	
	Perform one of the following:
	
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	
	`<XSI_Host_Server ua="na">https://xsi.iop1.broadworks.net</XSI_Host_Server>`
	• In the phone web page, enter the server.
	
	For example:
	
	`https://xsi.iop1.broadworks.net`
	
	You can also specify a port for the server. For example:
	
	`https://xsi.iop1.broadworks.net:5061`
	
	If you don't specify a port. The default port for the specified protocol is used.
	
	Default: Blank

Parameter	Description
XSI Authentication Type	Determines the XSI authentication type.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	``` <XSI_Authentication_Type ua="na">SIP Credentials</XSI_Authentication_Type> ```
	• In the phone web page, select an authentication type.
	Options:
	Login Credentials - authenticates access with Login User ID and Login Password.
	SIP Credentials - authenticates access with the register Auth ID and Password of the SIP account registered on the phone.
	If you select **SIP Credentials** for **XSI Authentication Type**, you need to enter subscriber **Auth ID** and **Password** in the **Subscriber Information** section.
	Default: Login Credentials
Login User ID	BroadSoft User ID of the phone user.
	For example:
	`johndoe@xdp.broadsoft.com.`
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	``` <Login_User_ID ua="na">4081005300@as1bsoft22.sipurash.com</Login_User_ID> ```
	• In the phone web page, enter a valid user ID.
	For any XSI Authentication Type, you must enter **Login User ID**. The BroadWorks Anywhere feature does not work without this parameter.
	Default: admin
Login Password	Alphanumeric password associated with the Login User ID.
	Enter Login Password, when you select **Login Credentials** for XSI authentication type.
	After you enter the password, this parameter shows the following in the configuration file (cfg.xml): `<ACS_Password ua="na">************</ACS_Password>`
	Default: Blank

Parameter	Description
Anywhere Enable	Enables BroadWorks Anywhere feature on an extension.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format:
	`<Anywhere_Enable_1_ ua="na">Yes</Anywhere_Enable_1_>`
	• In the phone web page, select **Yes**, Anywhere is enabled on this line, and the user can use the phone menu to add multiple locations to this specific line.
	Valid values: Yes|No
	Default: Yes

Sync the Block Caller ID Feature with the Phone and the BroadWords XSI Server

You can sync the **Block caller id** status on the phone and the **Line ID Blocking** status on the BroadWorks XSI server. When you enable the synchronization, the changes that the user makes in the **Block caller id** settings also changes the BroadWorks server settings.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **Ext(n)**.

Step 2 In the **XSI Line Service** section, set the **Block CID Enable** parameter. Choose **Yes** to enable the synchronization of blocking caller id status with the server using XSI interface. Choose **No** to use the phone's local blocking caller id settings.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

`<Block_CID_Enable_1_ ua="na">No</Block_CID_Enable_1_>`

Note
• When **Feature Key Sync** is set to **Yes**, FKS takes precedent over XSI synchronization.

• If XSI host server and credentials are not entered and the **CFWD Enable** field is set to **Yes**, the phone user can't forward calls on the phone.

Options: Yes and No

Default: No

Step 3   Click **Submit All Changes**.

Enable Viewing BroadWorks XSI Call Logs on a Line

You can configure a phone to display recent call logs from either the BroadWorks server or the local phone. After you enable the feature, the Recents screen has a **Display recents from** menu and the user can choose the XSI call logs or the local call logs.

You can set up a feature to do a reverse name lookup against local contacts for BroadWorks server call logs. For example, on server you set up a user 3280 (4085273280) with name "cx400 liu" and another user 3281(4085273281) with name "cx401 liu". User 3280 is registered on phone A and user 3281 is registered on phone B. From phone A you make a missed call, a received call, or a placed call on phone B. The display of the broadsoft call logs on phone B appears as follows:

- If the personal directory doesn't have a contact that matches with the caller name, the BroadWorks call logs on phone B displays the original name "cx400 liu" saved in the server as the caller name.

- If the personal directory has a contact with "Name" = "B3280" and "Work" = "3280" that matches with the calling number, the BroadWorks call logs on phone B displays the contact name "B3280" as the caller name.

- If the personal directory has a contact with "Name" = "C3280" and "Work" = "03280", and the user configures a caller id map rule (<3:03>x.), the BroadWorks call logs on the phone B displays "C3280" using the mapped phone number 03280. If there is a matched contact of the unmapped phone number, the mapped phone number will not be used for reverse name lookup.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code. To configure each parameter, see the syntax of the string in the Parameters for BroadWorks XSI Call Logs on a Line, on page 65 table.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

CallLog Enable field is enabled.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **XSI Phone Service** section, set the **XSI Host Server**, **XSI Authentication Type**, **Login User ID**, **Login Password**, and **Directory Enable** fields as described in Parameters for BroadWorks XSI Call Logs on a Line, on page 65.

If you select **SIP Credentials** for **XSI Authentication Type**, you need to enter **SIP Auth ID** and **SIP Password** in this section.

Step 3   Set the **CallLog Associated Line** and **Display Recents From** fields as described in Parameters for BroadWorks XSI Call Logs on a Line, on page 65.

Note   The **Display recents from** menu doesn't appear in the **Recents** phone screen when you set the value of the **CallLog Enable** field to **No**,

Step 4   Click **Submit All Changes**.

Parameters for BroadWorks XSI Call Logs on a Line

The following table defines the function and usage of XSI Call Logs on a Line parameters in the XSI Phone Service section under the Phone tab in the phone web interface. It also defines the syntax of the string that is added in the phone configuration file with XML(cfg.xml) code to configure a parameter.

Table 13: Parameters for XSI Call Logs on a Line

Parameter	Description
XSI Host Server	Enter the name of the server; for example, `xsi.iop1.broadworks.net` . **Note** XSI Host Server uses http protocol by default. To enable XSI over HTTPS, you can specify `https://` in the server. • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<XSI_Host_Server ua="na">https://xsi.iop1.broadworks.net</XSI_Host_Server>` • In the phone web interface, enter the XSI server to use. Default: Empty
XSI Authentication Type	Determines the XSI authentication type. Select **Login Credentials** to authenticate access with XSI id and password. Select **SIP Credentials** to authenticate access with the register user ID and password of the SIP account registered on the phone. • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<XSI_Authentication_Type ua="na">SIP Credentials</XSI_Authentication_Type>` • In the phone web interface, specify the authentication type for XSI service. Options: SIP Credentials and Login Credentials Default: Login Credentials

Parameter	Description
Login User ID	BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com.
	Enter SIP Auth ID when you select **Login Credentials** or **SIP Credentials** for XSI authentication type.
	When you choose SIP Auth ID as **SIP Credentials**, you must enter Login User ID. Without Login User ID, the BroadSoft directory will not appear under the phone Directory list.
	• In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Login_User_ID ua="na">username</Login_User_ID>` • In the phone web interface, enter the username used to authenticate the access to the XSI server.
	Default: Empty
Login Password	Alphanumeric password associated with the User ID.
	Enter login password, when you select **Login Credentials** for XSI authentication type.
	Default: Empty
Directory Enable	Enables BroadSoft directory for the phone user. Select **Yes** to enable the directory and select **No** to disable it.
	Perform one of the following:
	• In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Directory_Enable ua="na">Yes</Directory_Enable>` • In the phone web interface, set this field to **Yes** to enable the BroadSoft directory.
	Option: Yes and No
	Default: No

Parameter	Description
CallLog Associated Line	Allows you to select a phone line for which you want to display the recent call logs. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<CallLog_Associated_Line ua="na">1</CallLog_Associated_Line>` • In the phone web interface, Select a phone line. Valid values: 1 to 10 Default: 1
Display Recents From	Allows you to set which type of recent call logs the phone will display. Perform one of the following: • In the phone configuration file with XML(cfg.xml), enter a string in this format: `<Display_Recents_From ua="na">Phone</Display_Recents_From>` • In the phone web interface, Choose **Server** to display BroadSoft XSI recent call logs and select **Phone** to display local recent call logs. Option: Phone and Server Default: Phone **Note** The **Display recents from** is added to the **Recents** screen of the phone only when you set **CallLog Enable** to **Yes** and **Display Recents From** type to **Server**.

Enable Feature Key Sync

When you enable the Feature Key Synchronization (FKS), the settings of call forward and do not disturb (DND) on the server are synchronized to the phone. The changes in DND and call forward settings made on the phone will also be synchronized to the server.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1	Select **Voice** > **Ext [n]** (where [n] is the extension number).
Step 2	In the **Call Feature Settings** section, set the **Feature Key Sync** field to **Yes**.
Step 3	Click **Submit All Changes**.

Related Topics

DND and Call Forward Status Sync

You can configure the settings on the phone administration web page to enable status synchronization of do not disturb (DND) and call forward between the phone and the server.

There are two ways to synchronize the feature status:

- Feature Key Synchronization (FKS)

- XSI Synchronization

FKS uses SIP messages to communicate the feature status. XSI Synchronization uses HTTP messages. If both FKS and XSI synchronization are enabled, FKS takes precedent over XSI synchronization. See the table below for how FKS interacts with XSI synchronization.

Table 14: Interaction Between FKS and XSI Synchronization

Feature Key Sync	DND Enabled	CFWD Enabled	DND Sync	CFWD Sync
Yes	Yes	Yes	Yes (SIP)	Yes (SIP)
Yes	No	No	Yes (SIP)	Yes (SIP)
Yes	No	Yes	Yes (SIP)	Yes (SIP)
Yes	No	No	Yes (SIP)	Yes (SIP)
No	Yes	Yes	Yes (HTTP)	Yes (HTTP)
No	No	Yes	No	Yes (HTTP)
No	Yes	No	Yes (HTTP)	No
No	No	No	No	No

If a line key is configured with FKS or XSI synchronization and is also enabled with DND or call forward, the respective DND ⊘ icon or the call forward ⤨ icon is displayed next to the line key label. If the line key has a missed call, a voice message, or an urgent voicemail alert, the DND icon or the call forward icon is also displayed with the alert notification.

Enable Call Forward Status Sync via XSI Service

When call forward sync is enabled, the settings related to call forward on the server are synchronized to the phone. The changes in call forward settings made on the phone will also be synchronized to the server.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

- Access the phone administration web page. See Access the Phone Web Interface.

- Configure the XSI host server and the corresponding credentials on the **Voice** > **Ext (n)** tab.

  - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.

  - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.

- Disable Feature Key Sync (FKS) in **Call Feature Settings** section from **Voice** > **Ext (n)** .

Procedure

Step 1   Select **Voice** > **Ext [n]** (where [n] is the extension number).

Step 2   In the **XSI Line Service** section, set the **CFWD Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<CFWD_Enable_1_ ua="na">Yes</CFWD_Enable_1_>
```

Options: Yes and No

Default: Yes

Note   If XSI sync for call forward is enabled and the XSI host server or XSI account is not configured correctly, the phone user can't forward calls on the phone.

Step 3   Click **Submit All Changes**.

Related Topics

Enable DND Status Sync via XSI Service

When do not disturb (DND) sync is enabled, the DND setting on the server is synchronized to the phone. The changes in DND setting made on the phone will also be synchronized to the server.

You can also configure the parameters in the phone configuration file with XML(cfg.xml) code.

Before you begin

- Access the phone administration web page. See Access the Phone Web Interface.

- Configure the XSI host server and the corresponding credentials on the **Voice** > **Ext (n)** tab.

    - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.

    - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.

- Disable Feature Key Synchronization (FKS) in **Call Feature Settings** section from **Voice** > **Ext (n)**.

Procedure

Step 1   Select **Voice** > **Ext [n]** (where [n] is the extension number).

Step 2   In the **XSI Line Service** section, set the **DND Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<DND_Enable_1_ ua="na">Yes</DND_Enable_1_>
```

Options: Yes and No

Default: Yes

Step 3   Click **Submit All Changes**.

Related Topics

Enable Synchronization of Anonymous Call Rejection via XSI Service

You can enable synchronization of Anonymous Call Rejection for each line via the XSI service. The function can be used to reject calls from callers who have blocked the display of their number.

Except for the setting for each line, you can also use the **Block ANC Setting** field under the **Supplementary Services** section from **Voice** > **User** to directly enable or disable the function for all lines.

The priority of the setting: **Block Anonymous Call Enable** > **Block ANC Setting**.

For example, if you set **Block Anonymous Call Enable** to **Yes** for a specific line, the setting in the **Block ANC Setting** doesn't take effect for the line, it takes effect for other lines on which **Block Anonymous Call Enable** is **No**.

Before you begin

- Access the phone administration web page. See Access the Phone Web Interface.

- Configure the XSI host server and the corresponding credentials on the **Voice** > **Ext (n)** tab.

  - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.

  - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.

- Ensure that Anonymous Call Rejection is enabled on the line or in the XSI service. Otherwise, your user still receives anonymous calls.

Procedure

Step 1   Select **Voice** > **Ext [n]** (where [n] is the extension number).

Step 2   In the **XSI Line Service** section, set the **Block Anonymous Call Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Block_Anonymous_Call_Enable_n_ ua="na">Yes</Block_Anonymous_Call_Enable_n_>
```

Where n is the extension number.

Options: Yes and No

Default: No

Step 3   Click **Submit All Changes**.

After the change takes effect, the XSI service takes over the phone to provide the function. The function doesn't work in the following scenarios even though **Block Anonymous Call Enable** is set to **Yes**:

- The function is disabled in the XSI service.

- The function is disabled on the line.

Because the function status is synchronized between the XSI service and the line.

Set Feature Activation Code for Anonymous Call Rejection

You can set activation code to block or remove blocking of anonymous calls for all lines on which synchronization of Anonymous Call Rejection is disabled.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Regional**.

Step 2   In the **Vertical Service Activation Codes** section, ensure that the **Block ANC Act Code** field is set to the value defined by the server. The default value is *77.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<Block_ANC_Act_Code ua="na">*77</Block_ANC_Act_Code>
```

Step 3   In the **Vertical Service Activation Codes** section, ensure that the **Block ANC Deact Code** field is set to the value defined by the server. The default value is *87.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<Block_ANC_Deact_Code ua="na">*87</Block_ANC_Deact_Code>
```

Step 4   Click **Submit All Changes**.

Your user can dial *77 or *87 and press the **Call** softkey to block all anonymous calls or remove the blocking.

This operation is identical to the setting on the **Block ANC Setting** field under the **Supplementary Services** section from **Voice** > **User**. It takes effect for the lines on which the **Block Anonymous Call Enable** (under the **XSI Line Service** section from **Voice** > **Ext**) is set to **No**.

Enable Synchronization of Call Waiting via XSI Service

You can enable synchronization of Call Waiting for each line via the XSI service. The function allows the user to receive incoming calls while on another call.

Except for the setting, you can also use the **CW Setting** field under the **Supplementary Services** section from **Voice** > **User** to directly enable or disable the function for all lines.

The priority of the setting: **Call Waiting Enable** > **CW Setting**.

For example, if you set **Call Waiting Enable** to **Yes** for a specific line, the setting in the **CW Setting** doesn't take effect for the line, it only takes effect for other lines on which **Call Waiting Enable** is set to **No**.

Before you begin

- Access the phone administration web page. See Access the Phone Web Interface.

- Configure the XSI host server and the corresponding credentials on the **Voice** > **Ext (n)** tab.

  - When using **Login Credentials** for XSI server authentication, enter **XSI Host Server**, **Login User ID**, and **Login Password** in the **XSI Line Service** section.

  - When using **SIP Credentials** for XSI server authentication, enter **XSI Host Server** and **Login User ID** in the **XSI Line Service** section, and **Auth ID** and **Password** in the **Subscriber Information** section.

• Ensure that Call Waiting is enabled on the line or in the XSI service. Otherwise, your user doesn't receive any incoming calls while on a call.

Procedure

Step 1   Select **Voice** > **Ext [n]** (where [n] is the extension number).

Step 2   In the **XSI Line Service** section, set the **Call Waiting Enable** parameter to **Yes**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<Call_Waiting_Enable_n_ ua="na">Yes</Call_Waiting_Enable_n_>
```

Where *n* is the extension number.

Options: Yes and No

Default: No

Step 3   Click **Submit All Changes**.

After the change takes effect, the XSI service takes over the phone to provide the function. The function doesn't work in the following scenarios even though **Call Waiting Enable** is set to **Yes**:

• The function is disabled in the XSI service.

• The function is disabled on the line.

Because the function status is synchronized between the XSI service and the line.

Set Feature Activation Code for Call Waiting

You can set activation code (star code) that can be used to activate or deactivate Call Waiting for all lines.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **Regional**.

Step 2   In the **Vertical Service Activation Codes** section, ensure that the **CW Act Code** field is set to the value defined by the server. The default value is *56.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<CW_Act_Code ua="na">*56</CW_Act_Code>
```

Step 3   In the **Vertical Service Activation Codes** section, ensure that the **CW_Deact_Code** field is set to the value defined by the server. The default value is *57.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<CW_Deact_Code ua="na">*57</CW_Deact_Code>
```

Step 4   In the **Vertical Service Activation Codes** section, ensure that the **CW_Per_Call_Act_Code** field is set to the value defined by the server. The default value is *71.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<CW_Per_Call_Act_Code ua="na">*71</CW_Per_Call_Act_Code>
```

Step 5   In the **Vertical Service Activation Codes** section, ensure that the **CW_Per_Call_Deact_Code** field is set to the value defined by the server. The default value is *70.

In the phone configuration file with XML(cfg.xml), enter a string in this format:

```
<CW_Per_Call_Deact_Code ua="na">*70</CW_Per_Call_Deact_Code>
```

Step 6   Click **Submit All Changes**.

Your user can dial *56 or *57 and press the **Call** softkey to activate or deactivate Call Waiting for all incoming calls. This operation is identical to the setting on the **CW Setting** field under the **Supplementary Services** section from **Voice** > **User**. These activation codes don't take effect for the lines where synchronization of Call Waiting via the XSI service is enabled.

Your user can dial *71 or *70 and press the **Call** softkey to temporarily activate or deactivate Call Waiting for the next incoming call on an active call. These activation codes still take effect for the lines where synchronization of Call Waiting via the XSI service is enabled. If Call Waiting is disabled in the XSI service, the server blocks all incoming calls, therefore these activation codes don't take effect.

Enable End-of-Call Statistics Reports in SIP Messages

You can enable the phone to send end-of-call statistics in Session Initiation Protocol (SIP) messages (BYE and re-INVITE messages). The phone sends call statistics to the other party of the call when the call terminates or when the call is on hold. The statistics include:

- Real-time Transport Protocol (RTP) packets sent or received
- Total bytes sent or received
- Total number of lost packets
- Delay jitter
- Round-trip delay
- Call duration

The call statistics are sent as headers in SIP BYE messages and SIP BYE response messages (200 OK and re-INVITE during hold). For audio sessions, the headers are `RTP-RxStat` and `RTP-TxStat`.

Example of call statistics in a SIP BYE message:

```
Rtp-Rxstat: Dur=13,Pkt=408,Oct=97680,LatePkt=8,LostPkt=0,AvgJit=0,VQMetrics="CCR=0.0017;
ICR=0.0000;ICRmx=0.0077;CS=2;SCS=0;VoRxCodec=PCMU;CID=4;VoPktSizeMs=30;VoPktLost=0;
VoPktDis=1;VoOneWayDelayMs=281;maxJitter=12;MOScq=4.21;MOSlq=3.52;network=ethernet;
hwType=CP-8865;rtpBitrate=60110;rtcpBitrate=0"
```

```
Rtp-Txstat: Dur=13,Pkt=417,Oct=100080,tvqMetrics="TxCodec=PCMU;rtpbitrate=61587;rtcpbitrate=0
```

For description of the attributes in call statistics, see Attributes for Call Statistics in SIP Messages, on page 75.

You can also use the `Call_Statistics` parameter in the phone configuration file to enable this feature.

```
<Call_Statistics ua="na">Yes</Call_Statistics>
```

Before you begin

Access the phone administration web page, see Access the Phone Web Interface.

Procedure

Step 1   Select **Voice** > **SIP**.

Step 2   In the **RTP Parameters** section, set the **Call Statistics** field to **Yes** to enable the phone to send call statistics in SIP BYE and re-INVITE messages.

You can also configure this parameter in the configuration file (cfg.xml) by entering a string in this format:

```
<Call_Statistics ua="na">Yes</Call_Statistics>
```

The allowed values are Yes|No. The defaut value is No.

Step 3   Click **Submit All Changes**.

Attributes for Call Statistics in SIP Messages

Table 15: Audio: RTP-RxStat Payload

Attribute	Description	Mandatory
Dur	Duration of media session/call	Yes
Pkt	Number of RTP packets received	Yes
Oct	Number of RTP packets octets received	No
LatePkt	Number of RTP packets received and discarded as late due to outside of buffer window	Yes
LostPkt	Number of RTP packets lost	Yes
AvgJit	Average Jitter over session duration	Yes
VoRxCodec	Stream/session codec negotiated	Yes
VoPktSizeMs	Packet size in milliseconds	Yes
maxJitter	Max Jitter detected	Yes
VoOneWayDelayMs	Latency/one way delay	Yes

Attribute	Description	Mandatory
MOScq	Mean opinion score conversational quality for the session, per RFC https://tools.ietf.org/html/rfc3611	Yes
maxBurstPktLost	Maximum number of sequential packets lost	No
avgBurstPktLost	Average number of sequential packets lost in a burst. The number can be used in conjunction with overall loss to compare the impact of loss on the call quality.	No
networkType	Type of network the device is on (if possible).	Yes
hwType	Hardware client that the session/media is running on. More relevant for soft clients but still useful for hard phones. For example, Model number CP-8865.	Yes

Table 16: Audio: RTP-TxStat Payload

Attribute	Description	Mandatory
Dur	Duration of session	Yes
Pkt	Number of RTP packets transmitted	Yes
Oct	Number of RTP packets octets transmitted	Yes
TxCodec	Transmit codec	Yes
rtpBitRate	Total RTP transmit bit rate (bits/sec)	Yes
rctpBitRate	Total RCTP transmit bit rate (bits/sec)	Yes

SIP Session ID

The Multiplatform phones now support "Session Identifier". This feature helps to overcome the limitations with the existing call-identifiers and allows end-to-end tracking of a SIP session in IP-based multimedia communication systems in compliance with RFC 7989. To support session identifier, "Session-ID" header is added in the SIP request and response messages.

"Session Identifier" refers to the value of the identifier, whereas "Session-ID" refers to the header field used to convey the identifier.

- When a user initiates the call, the phone while sending SIP INVITE message, generates the local-UUID.

- When the UAS receives the SIP-INVITE, the phone picks up the local UUIDs with the incoming messages and appends it to the received Session-ID header and sends the header in reponses.

- The same UUIDs are maintained in all the SIP messages of a particular session.

- The phone maintains the same local-UUID during other features, such as conference or transfer.

- This header is implemented in REGISTER method, the local-UUID remains same for all the REGISTER messages till the phone fails to REGISTER.

The Session-ID comprises of Universally Unique Identifier (UUID) for each user agent participating in a call. Each call consists of two UUID known as local UUID and remote UUID. Local UUID is the UUID generated from the originating user agent and remote UUID is generated from the terminating user agent. The UUID values are presented as strings of lower-case hexadecimal characters, with the most significant octet of the UUID appearing first. Session Identifier comprises of 32 characters and remains same for the entire session.

Session ID format

Components will implement Session-ID which is global session ID ready.

A sample current session ID passed in http header by phones (dashes are just included for clarity) is 00000000-0000-0000-0000-5ca48a65079a.

A session-ID format: UUUUUUUUSSSS5000y000DDDDDDDDDDDD where,

UUUUUUUU - A randomly generated unique ID[0-9a-f] for the session. Examples of new session IDs generated are:

- Phone going off hook

- Entry of the activation code through to first SIP first registration (the onboarding flow)

SSSS - The source that generates the session. For example, if the source type is "Cisco MPP" the source value (SSSS) can be "0100".

Y - Any of the values of 8, 9, A, or B and should be compliant with UUID v5 RFC.

DDDDDDDDDDDD - MAC address of the phone.

SessionID Example in SIP Messages

This header is supported in the in-call dialog messages like INVITE/ACK/CANCEL/BYE/UPDATE/INFO/REFER and their responses as well as out-of-call messages essentially the REGISTER.

```
Request-Line: INVITE sip:901@10.89.107.37:5060 SIP/2.0
      Session-ID: 298da61300105000a00000ebd5cbd5c1;remote=00000000000000000000000000000000

Status-Line: SIP/2.0 100 Trying
Session-ID: fbaa810a00105000a00000ebd5cc118b;remote=298da61300105000a00000ebd5cbd5c1

Status-Line: SIP/2.0 180 Ringing
      Session-ID: fbaa810a00105000a00000ebd5cc118b;remote=298da61300105000a00000ebd5cbd5c1

Status-Line: SIP/2.0 200 OK
      Session-ID: fbaa810a00105000a00000ebd5cc118b;remote=298da61300105000a00000ebd5cbd5c1

Request-Line: ACK sip:901@10.89.107.37:5060 SIP/2.0
      Session-ID: 298da61300105000a00000ebd5cbd5c1;remote=fbaa810a00105000a00000ebd5cc118b

Request-Line: BYE sip:901@10.89.107.37:5060 SIP/2.0
      Session-ID: 298da61300105000a00000ebd5cbd5c1;remote=fbaa810a00105000a00000ebd5cc118b

Status-Line: SIP/2.0 200 OK
      Session-ID: fbaa810a00105000a00000ebd5cc118b;remote=298da61300105000a00000ebd5cbd5c1
```

Enable SIP Session ID

You can enable SIP session ID to overcome the limitations with the existing call-identifiers and to allow end-to-end tracking of a SIP session.

Before you begin

Access the Phone Web Interface

Procedure

Step 1	Select **Voice** > **Ext(n)**.
Step 2	Go to the **SIP Settings** section.
Step 3	Set the **SIP SessionID Support** field as described in the Session ID Parameters, on page 78 table.
Step 4	Click **Submit All Changes**.

Session ID Parameters

The following table defines the function and usage of each parameter in the **SIP Settings** section in the **Voice** > **Ext(n)** tab of the phone web page. It also defines the syntax of the string that is added in the phone configuration file with XML (cfg.xml) code to configure a parameter.

Parameter Name	Description and Default Value
SIP SessioID Support	Controls the SIP session ID support. Perform one of the following • In the phone configuration file with XML (cfg.xml) enter a string in this format. `<SIP_SessionID_Support_1_ ua="na">Yes</SIP_SessionID_Support_1_>` • In the phone web page select **Yes** to enable the feature. Allowed values: Yes/No Default: Yes.

Set Up a Phone for Remote SDK

You can configure remote SDK for a multiplatform phone. The remote SDK provides a WebSocket based protocol through which the phone can be controlled.

Before you begin

• Access the Phone Web Interface

• A WebSocket server must be running with an address and port reachable from the phone.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   Go to the **WebSocket API** section.

Step 3   Set the **Control Server URL** and the **Allowed APIs** fields as described in the table.

Step 4   Click **Submit All Changes**.

WebSocket API Parameters

The following table defines the function and usage of each parameter in the **WebSocket API** section in the **Voice** > **Phone** tab of the phone web page. It also defines the syntax of the string that is added in the phone configuration file with XML (cfg.xml) code to configure a parameter.

Parameter Name	Description and Default Value

Control Server URL	The URL of a WebSocket server to which the phone attempts to stay connected.
	
	• In the phone configuration file with XML (cfg.xml) enter a string in this format.
	
	`<Control_Server_URL ua="na"/>`
	
	• In the phone web page enter the URL of a WebSocket server.
	
	For example:
	
	`<Control_Server_URL>wss://my-server.com/ws-server-path</Control_Server_URL>`
	
	The URL should be in one of the following formats:
	
	• For a nonsecure HTTP connection:
	
	`ws://your-server-name/path`
	
	• For a secure HTTPS connection:
	
	`wss://your-server-name/some-path`
	
	We recommend a secure connection.
	
	Default: Empty.

Parameter Name	Description and Default Value
Allowed APIs	A regular expression that can be used to limit the API calls that are allowed from the controlling server. • In the phone configuration file with XML(cfg.xml) enter a string in this format. `<Allowed_APIs ua="na">.*</Allowed_APIs>` • In the phone web page enter an appropriate regular expression. The regular expression provided is matched with the Request-URI path provided in the API request from the controlling server. If the entire path is not matched by the given regular expression, the API call is rejected. Allowed values are: • **.***: All APIs are allowed • **/api/Call/v1/.***: All v1 **Call** interface calls are allowed. • **/api/Call/v1/(Dial|Hangup)**: Only the v1 Call interface calls **Dial** and **Hangup** are allowed. Default: .*

Hide a Menu Item from Being Displayed on the Phone Screen

By default, all the menu items on the phone screen **Information and settings** are visible to users. You can configure the phone to hide or show specific menu items. When hidden, the items don't display on the phone screen.

You can hide any of the following menu items as needed:

- Speed dials
- User preferences
- Network configuration
- Device administration
- Status
- Report problem

You can also configure the visibility of the menu items in the configuration file (cfg.xml) with strings in this format:

```
<Device_Administration ua="na">No</Device_Administration>
```

See the parameter syntax and valid values in .

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 In the **Menu Visibility** section, set the menu items that you want to hide to **No**.

Step 3 Click **Submit All Changes**.

Parameters for Menu Visibility

The following table defines the function and usage of each parameter in the **Menu Visibility** section of the **Voice** > **Phone** tab.

Table 17: Parameters for Menu Visibility

Parameter Name	Description and Default Value
Speed Dials	Controls whether to show the **Speed dials** menu on the phone screen. Set this field to **Yes** to show the menu. Otherwise, set it to **No**. Perform one of the following: • In the phone configuration file (cfg.xml) with XML, enter a string in this format: `<Speed_Dials ua="na">Yes</Speed_Dials>` • In the phone web interface, select **Yes** or **No** to show or hide the menu. Valid values: Yes and No Default: Yes
User Preferences	Controls whether to show the **User preferences** menu on the phone screen. Set this field to **Yes** to show the menu. Otherwise, set it to **No**. Perform one of the following: • In the phone configuration file (cfg.xml) with XML, enter a string in this format: `<User_Preferences ua="na">Yes</User_Preferences>` • In the phone web interface, select **Yes** or **No** to show or hide the menu. Valid values: Yes and No Default: Yes

Parameter Name	Description and Default Value
Network Configuration	Controls whether to show the **Network configuration** menu on the phone screen. Set this field to **Yes** to show the menu. Otherwise, set it to **No**. Perform one of the following: • In the phone configuration file (cfg.xml) with XML, enter a string in this format: `<Network_Configuration ua="na">Yes</Network_Configuration>` • In the phone web interface, select **Yes** or **No** to show or hide the menu. Valid values: Yes and No Default: Yes
Device Administration	Controls whether to show the **Device administration** menu on the phone screen. Set this field to **Yes** to show the menu. Otherwise, set it to **No**. Perform one of the following: • In the phone configuration file (cfg.xml) with XML, enter a string in this format: `<Device_Administration ua="na">Yes</Device_Administration>` • In the phone web interface, select **Yes** or **No** to show or hide the menu. Valid values: Yes and No Default: Yes
Status	Controls whether to show the **Status** menu on the phone screen. Set this field to **Yes** to show the menu. Otherwise, set it to **No**. Perform one of the following: • In the phone configuration file (cfg.xml) with XML, enter a string in this format: `<Status ua="na">Yes</Status>` • In the phone web interface, select **Yes** or **No** to show or hide the menu. Valid values: Yes and No Default: Yes

Parameter Name	Description and Default Value
Report Problem	Controls whether to show the **Report problem** menu under the **Status** menu on the phone screen. Set this field to **Yes** to show the menu. Otherwise, set it to **No**.
	When the **Status** menu is invisible, the **Report problem** menu is invisible as well.
	Perform one of the following:
	• In the phone configuration file (cfg.xml) with XML, enter a string in this format:
	`<Report_Problem_Menu ua="na">Yes</Report_Problem_Menu>`
	• In the phone web interface, select **Yes** or **No** to show or hide the menu.
	Valid values: Yes and No
	Default: Yes

Display Caller Number Instead of Unresolved Caller Name

By default, the phone displays both the caller name and the caller number in an incoming call alert. When the phone can't resolve the characters in caller name, the user sees boxes instead of the caller name. You can configure the phone to display only the number when any unresolved characters are detected in the caller name.

Procedure

Step 1   Select **Voice** > **Regional**.

Step 2   In the **Language** section, set the **Replace Unresolved Caller Name with Number** field to **Yes**.

You can also configure this parameter in the configuration file (cfg.xml) with a string in this format:

```
<Replace_Unresolved_Caller_Name_with_Number
ua="na">Yes</Replace_Unresolved_Caller_Name_with_Number>
```

The valid values are Yes and No. The default setting is No.

Step 3   Click **Submit All Changes**.

Phone Features and Setup

Menu Shortcuts Mapping on PSK

Menu Shortcuts Mapping on PSK

Table 18: Menu Shortcuts Mapping

Function (fnc=)	URL String (url=)	Target Menu
shortcut	settings	**Settings**
shortcut	accessibility	**Settings** > **Accessibility**
shortcut	recents	**Settings** > **Recents**
shortcut	allcalls	**Settings** > **Recents** > **All calls**
shortcut	missedcalls	**Settings** > **Recents** > **Missed calls**
shortcut	receivedcalls	**Settings** > **Recents** > **Received calls**
shortcut	placedcalls	**Settings** > **Recents** > **Placed calls**
shortcut	speeddials	**Settings** > **Speed dials**
shortcut	userpref	**Settings** > **User preferences**
shortcut	callpref	**Settings** > **User preferences** > **Call preferences**
shortcut	cfwsetting	**Settings** > **User preferences** > **Call preferences** > **Call forwarding**
shortcut	anywhere	**Settings** > **User preferences** > **Call preferences** > **Anywhere**
shortcut	audiopref	**Settings** > **User preferences** > **Audio preferences**
shortcut	screenpref	**Settings** > **User preferences** > **Screen preferences**
shortcut	screensaver	**Settings** > **User preferences** > **Screen preferences** > **Screen saver**
shortcut	attconsole	**Settings** > **User preferences** > **Attendant console preferences**
shortcut	ringtone	**Settings** > **User preferences** > **Ringtone**
shortcut	bluetooth	**Settings** > **Bluetooth**
shortcut	networkconf	**Settings** > **Network configuration**
shortcut	ethernetconf	**Settings** > **Network configuration** > **Ethernet configuration**
shortcut	ipv4setting	**Settings** > **Network configuration** > **IPv4 address settings**
shortcut	ipv6setting	**Settings** > **Network configuration** > **IPv6 address settings**
shortcut	adminsetting	**Settings** > **Device administration**

Phone Features and Setup

84

Function (fnc=)	URL String (url=)	Target Menu
shortcut	setpassword	**Settings** > **Device administration** > **Set password**
shortcut	usersignin	**Settings** > **Device administration** > **Sign in**
shortcut	usersignout	**Settings** > **Device administration** > **Sign out**
shortcut	datetime	**Settings** > **Device administration** > **Date/Time**
shortcut	language	**Settings** > **Device administration** > **Language**
shortcut	restart	**Settings** > **Device administration** > **Restart**
shortcut	factoryreset	**Settings** > **Device administration** > **Factory reset**
shortcut	profilerule	**Settings** > **Device administration** > **Profile rule**
shortcut	profileaccount	**Settings** > **Device administration** > **Profile account setup**
shortcut	status	**Settings** > **Status**
shortcut	productinfo	**Settings** > **Status** > **Product information**
shortcut	networkstatus	**Settings** > **Status** > **Network status**
shortcut	ipv4status	**Settings** > **Status** > **Network status** > **IPv4 status**
shortcut	ipv6status	**Settings** > **Status** > **Network status** > **IPv6 status**
shortcut	phonestatus	**Settings** > **Status** > **Phone status**
shortcut	phonestat	**Settings** > **Status** > **Phone status** > **Phone status**
shortcut	linestatus	**Settings** > **Status** > **Phone status** > **Line status**
shortcut	provstatus	**Settings** > **Status** > **Phone status** > **Provisioning**
shortcut	callstat	**Settings** > **Status** > **Phone status** > **Call statistics**
shortcut	reportproblem	**Settings** > **Status** > **Report problem**
shortcut	reboothistory	**Settings** > **Status** > **Reboot history**
shortcut	accessories	**Settings** > **Status** > **Accessories**
shortcut	statusmessage	**Settings** > **Status** > **Status messages**
shortcut	directories	**Directories**
shortcut	personaldir	**Directories** > **Personal address book**
shortcut	alldir	**Directories** > **All**

Function (fnc=)	URL String (url=)	Target Menu
shortcut	ldapdir	**Directories** > **Corporate directory (LDAP)** The LDAP directory name is customizable.
shortcut	broadsoftdir	**Directories** > **BroadSoft directory** The BroadSoft directory name is customizable.
shortcut	bsdirpers	**Directories** > **BroadSoft directory** > **Personal** The BroadSoft directory name is customizable.
shortcut	bsdirgrp	**Directories** > **BroadSoft directory** > **Group** The BroadSoft directory name is customizable.
shortcut	bsdirent	**Directories** > **BroadSoft directory** > **Enterprise** The BroadSoft directory name is customizable.
shortcut	bsdirgrpcom	**Directories** > **BroadSoft directory** > **Group common** The BroadSoft directory name is customizable.
shortcut	bsdirentcom	**Directories** > **BroadSoft directory** > **Enterprise common** The BroadSoft directory name is customizable.
shortcut	xmppdir	**Directories** > **IM&P contacts** The XMPP directory name is customizable.
shortcut	xmlapp	**Settings** > **Cisco XML services** The XML application name is customizable.
shortcut	xmldir	**Directories** > **Corporate directory (XML)** The XML directory name is customizable.
shortcut	webexdir	**Directories** > **Webex directory** The Webex directory name is customizable. By default, the softkey displays the directory name as `Webex Dir`.
shortcut	proxyset	**Settings** > **Network configuration** > **HTTP proxy settings**

Add a Menu Shortcut to a Programmable Softkey

You can configure a softkey as a phone menu shortcut.

Before you begin

Access the phone administration web page. See Access the Phone Web Interface.

Procedure

Step 1 Select **Voice** > **Phone**.

Step 2 In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** field to **Yes**.

You can also configure the parameter in the configuration file (cfg.xml) with a string in this format:

```
<Programmable_Softkey_Enable ua="rw">Yes</Programmable_Softkey_Enable>
```

Step 3 Configure a PSK field from PSK 1 through PSK 16 with a string in this format:

```
fnc=shortcut;url=userpref;nme=User preferences
```

where:

- fnc= shortcut means function=phone menu shortcut.

- url= userpref is the menu to open with this line key. It's the **User preferences** menu in this example. For more shortcut mapping, see Menu Shortcuts Mapping on PSK, on page 84.

- nme= XXXX is the menu shortcut name displayed on the phone. In the example, the softkey displays **User preferences**.

You can also configure this parameter in the configuration file (cfg.xml). Enter a string in this format:

```
<PSK_n ua="rw">fnc=shortcut;url=userpref;nme=User preferences</PSK_n>
```

where *n* is the PSK number.

Step 4 Add the configured PSK to the desired key list.

Example: Add the configured **PSK 2** to **Idle Key List**. Do any of these actions:

- Add psk2 to the **Idle Key List** field.

```
psk2;em_login;acd_login;acd_logout;astate;redial;cfwd;dnd;lcr;
```

- In the configuration file (cfg.xml), enter a string in this format:

```
<Idle_Key_List
ua="rw">psk2;em_login;acd_login;acd_logout;astate;redial;cfwd;dnd;lcr;</Idle_Key_List>
```

Step 5 Click **Submit All Changes**.

Enable LDAP Unified Search

You can enable the unified search in the LDAP directory. The search allows you to enter any value as filters. For example, first name, last name, extension, or phone number. The phone transfers the request as a single search request.

Before you begin

- Access the phone administration web page. See Access the Phone Web Interface.

- **Browse Mode Enable** parameter set to **Yes** or **No**.

Procedure

Step 1   Select **Voice** > **Phone**.

Step 2   In the **LDAP** section, set the parameter **Unified Search Enable** to **Yes** to enable the LDAP unified search. If the parameter is set to **Yes**, the phone transfers requests with OR filter.

If you set the value to **No**, the phone uses simple or advanced search and transfers requests with AND filter.

Default value is **No**.

You can configure this parameter in the phone configuration XML file (cfg.xml) by entering a string in this format:

```
<LDAP_Unified_Search_Enable>Yes</LDAP_Unified_Search_Enable>
```

Conditions based on **Browse Mode Enable** and **Unified Search Enable** parameter values:

- **Browse Mode Enable** parameter is **No** and **Unified Search Enable** parameter is **No** - when the user chooses the LDAP directory on the phone, the **Query LDAP server** screen displays **Simple search** and **Advanced search** menus.

- **Browse Mode Enable** parameter is **No** and **Unified Search Enable** parameter is **Yes** - when the user chooses the LDAP directory, the phone navigates to the **LDAP query form** (unified search screen) directly. If there is no value in the search box, the search displays all contacts in the directory.

- **Browse Mode Enable** parameter is **Yes** and **Unified Search Enable** parameter is **No** - when the user navigates to the LDAP directory and clicks the **Option** softkey, the phone displays the **Simple search** and the **Advanced search** menus.

- **Browse Mode Enable** parameter is **Yes** and **Unified Search Enable** parameter is **Yes** - when the user navigates to the LDAP directory and clicks the **Option** softkey, the phone displays only one **Search** menu. After clicking the **Search** menu, the unified search screen **LDAP query form** appears.

Step 3   Click **Submit All Changes**.