POLYCOM®

Administrator's Guide for the Polycom® UC Software

3.3.0 | June 2010 | 1725-11530-330 Rev. A

Trademark Information

POLYCOM®, the Polycom “Triangles” logo and the names and marks associated with Polycom’s products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient’s personal use, without the express written permission of Polycom.

Patent Information

The accompanying product is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Disclaimer

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

Copyright Notice

Portions of the software contained in this product are:
Copyright © 1998, 1999, 2000 Thai Open Source Software Center Ltd. and Clark Cooper
Copyright © 1998 by the Massachusetts Institute of Technology
Copyright © 1998-2008 The OpenSSL Project
Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved
Copyright © 1995-2002 Jean-Loup Gailly and Mark Adler
Copyright © 1996-2008, Daniel Stenberg, <daniel@haxx.se>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Polycom, Inc.
4750 Willow Road
Pleasanton, CA 94588-2708
USA

About This Guide

The Administrator's Guide for the Polycom® UC Software is for administrators who need to configure, customize, manage, and troubleshoot Polycom® SoundPoint® IP, SoundStation® IP, and VVX® phones. This guide covers the SoundPoint IP 320, 321, 330, 331, 335, 450, 550, 560, 650, and 670 desktop phones, the SoundStation IP 5000, 6000 and 7000 conference phones, and the VVX 1500 business media phone.

The following related documents for the SoundPoint IP, SoundStation IP, and VVX phones are available:

- Quick Start Guides, which describe how to assemble the phones
- Quick User Guides, which describe the most basic features available on the phones
- User Guides, which describe the basic and advanced features available on the phones
- Web Applications Developer's Guide, which assists in the development of applications that run on the SoundPoint IP and SoundStation IP phone's Microbrowser and the VVX 1500 phone's Browser
- Technical Bulletins, which describe workarounds to existing issues and provide expanded descriptions and examples
- Release Notes, which describe the new and changed features and fixed problems in the latest version of the software

For support or service, please contact your Polycom® reseller or go to Polycom Technical Support at http://www.polycom.com/support/.

Polycom recommends that you record the phone model numbers, software (both the BootROM and UC Software), and partner platform for future reference.

SoundPoint IP, SoundStation IP, and VVX models: _____

BootROM version: _____

UC Software version: _____

Partner Platform: _____

Contents

1

Introducing the Polycom UC Software Family of Phones

This chapter introduces the family of Polycom® phones that run the Polycom® UC Software, which is described in this guide.

This family of phones provides a powerful, yet flexible IP communications solution for Ethernet TCP/IP networks, delivering excellent voice quality. The high-resolution graphic display supplies content for call information, multiple languages, directory access, and system status. These phones support advanced functionality, including multiple call and flexible line appearances, HTTPS secure provisioning, presence, custom ring tones, and local conferencing.

These phones are endpoints in the overall network topology designed to interoperate with other compatible equipment including application servers, media servers, internet-working gateways, voice bridges, and other end points.

The following models are described:

- SoundPoint IP Desktop Phones
- SoundStation IP Conference Phones
- VVX 1500 Business Media Phone

For a list of key features available on these phones running the latest software, refer to Key Features of Your Polycom Phones on page 1-6.

SoundPoint IP Desktop Phones

This section describes the current SoundPoint® IP desktop phones. For individual guides, refer to the product literature available at http://www.polycom.com/voicedocumentation/. Additional options are also available. For more information, contact your Polycom distributor.

Note Documentation for the SoundPoint IP 300, 301, 430, 500, 501, 600, and 601 desktop phones is available at http://www.polycom.com/voicedocumentation/ . These 'legacy' phones are not directly supported by the newest software, Polycom UC Software 3.3.0 .

The currently supported desktop phones are:

- SoundPoint IP 320/321/330/331/335

- SoundPoint IP 450

- SoundPoint IP 550/560

- SoundPoint IP 650

- SoundPoint IP 670

SoundStation IP Conference Phones

This section describes the current SoundStation® IP conference phones. For individual guides, refer to the product literature available at http://www.polycom.com/voicedocumentation/. Additional options are also available. For more information, contact your Polycom distributor.

Note Documentation for the SoundStation IP 4000 conference phone is available at http://www.polycom.com/voicedocumentation/ . This 'legacy' phone is not directly supported by the newest software, Polycom UC Software 3.3.0 .

The currently supported conference phones are:

- SoundStation IP 5000

- SoundStation IP 6000

- SoundStation IP 7000

VVX 1500 Business Media Phone

This section describes the current VVX® 1500 business media phone. For the individual guide, refer to the product literature available at http://www.polycom.com/voicedocumentation/. Additional options are also available. For more information, contact your Polycom distributor.

Key Features of Your Polycom Phones

The key features of the Polycom phones running Polycom UC Software are:

- Award winning sound quality and full-duplex speakerphone or conference phone
  - Permits natural, high-quality, two-way conversations
  - Uses Polycom's industry leading Acoustic Clarity Technology
  - Most phone models support Polycom's HDVoice™ technology
- Easy-to-use
  - An easy transition from traditional PBX systems into the world of IP Communications
  - Up to 18 dedicated hard keys for access to commonly used features
  - Up to four context-sensitive soft keys for further menu-driven activities
- Platform independent
  - Supports multiple protocols and platforms enabling standardization on one phone for multiple locations, systems and vendors
  - Polycom's support of the leading protocols and industry partners makes it a future-proof choice
- Field upgradeable
  - Upgrade phones as standards develop and protocols evolve
  - Extends the life of the phone to protect your investment
  - Application flexibility for call management and new telephony applications
- Large LCD
  - Easy-to-use, easily readable and intuitive interface
  - Support of rich application content, including multiple call appearances, presence and instant messaging, and XML services
  - 102 x 23 pixel graphical LCD for the SoundPoint IP 320/321/330/331/335
  - 256 x 116 pixel graphical grayscale LCD for the SoundPoint IP 450 (supports Asian characters)
  - 320 x 160 pixel graphical grayscale LCD for the SoundPoint IP 550/560/650 (supports Asian characters)
  - 320 x 160 pixel graphical color LCD for the SoundPoint IP 670 (supports Asian characters)
  - 248x 68 pixel graphical LCD for SoundStation IP 5000

  - 248 x 68 pixel graphical LCD for the SoundStation IP 6000
  - 256 x 128 pixel graphical grayscale LCD for the SoundStation IP 7000
  - 800 x 480 pixel graphical color LCD for the VVX 1500 (touch screen)
- Dual auto-sensing 10/100/1000baseT Ethernet ports
  - Leverages existing infrastructure investment
  - No re-wiring with existing CAT 5 cabling
  - Simplifies installation
  - 1000baseT is supported by the SoundPoint IP 560 and 670 and VVX 1500 only
- Power over Ethernet (PoE) port or Power pack option
  - Built-in IEEE 802.3af PoE port on the SoundPoint IP 320/321/330/331/335, 450, 550, 560, 650, and 670, the SoundStation IP 5000, 6000 and 7000, and VVX 1500 (auto-sensing)
  - Unused pairs on Ethernet port are used to deliver power to the phone via a wall adapter allowing fewer wires to desktop (for the SoundStation IP 6000 and 7000 conference phones)
- Multiple language support on most phones
  - Set on-screen language to your preference. Select from Chinese (Simplified), Danish, Dutch, English (Canada, United Kingdom, and United States), French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese (Brazilian), Russian, Slovenian, Spanish (International), and Swedish.
  - Chinese (Simplified), Japanese, and Korean are not supported on the SoundPoint IP 320/321/330/331/335 phones.
- Microbrowser
  - Supports a subset of XHTML constructs; otherwise runs like any other Web browser.
- Browser on the Polycom VVX 1500
  - Supports XHTML 1.1 constructs, HTML 4.01, JavaScript, CCS 2.1, and SVG 1.1 (partial support).
- XML status/control API
  - Ability to poll phones for call status and device information.
  - Ability to receive telephony notification events.

  For more information, refer to *Web Applications Developer's Guide*, which is available at http://www.polycom.com/voicedocumentation/

2

Overview

This chapter provides an overview of the Polycom® UC Software and how the phones fit into the network configuration.

The UC Software supports the deployment of Polycom phones in several deployment scenarios:

- As a SIP based endpoint interoperating with a SIP call server or soft-switch. For more information, review the remainder of this chapter.
- As an H.323 video endpoint (Polycom VVX® 1500). For more information, on using phones in a strict H.323 environment, refer to the *Deployment Guide for the Polycom® VVX® 1500 D Business Media Phone*, which is available from http://www.polycom.com/support/video/business_media_phones/vvx1500d.html .
- In conjunction with a Polycom HDX video system (SoundStation® IP 7000) . For more information on using phones with a Polycom HDX system, refer to *Integration Guide for the Polycom® SoundStation® IP 7000 Conference Phone Connected to a Polycom® HDX® System*, which is available from http://www.polycom.com/support/voice/soundstation_ip_series/soundstation_ip7000_hdx_series.html .

SIP is the Internet Engineering Task Force (IETF) standard for multimedia communications over IP. It is an ASCII-based, application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints. Like other voice over IP (VoIP) protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

For the Polycom phones to successfully operate as a SIP endpoint in your network, they must meet the following requirements:

- A working IP network is established.
- Routers are configured for VoIP.
- VoIP gateways are configured for SIP.

- The latest (or compatible) Polycom UC Software image is available.
- A call server is active and configured to receive and send SIP messages.

  For more information on IP PBX and softswitch vendors, go to http://www.polycom.com/techpartners1/ .

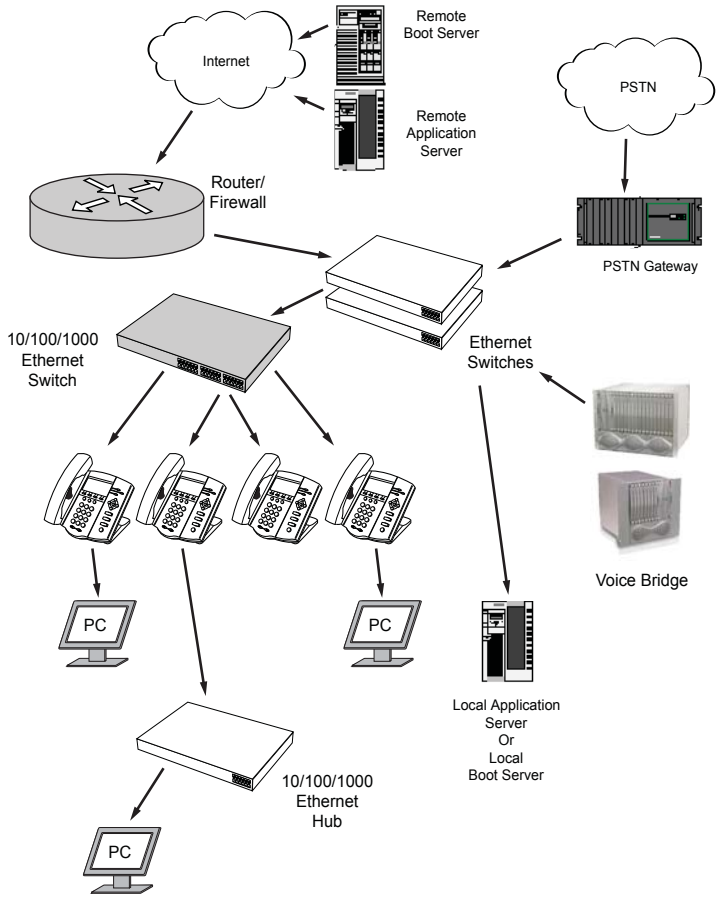
This chapter contains information on:

To set up your Polycom phones on the network, refer to Setting up Your System on page 3-1. To configure your Polycom phones with the desired features, refer to Configuring Your System on page 4-1. To troubleshoot any problems with your Polycom phones on the network, refer to Troubleshooting Your Polycom Phones on page 5-1.

Where Polycom Phones Fit

The phones connect physically to a standard office twisted-pair (IEEE 802.3) 10/100/1000 megabytes per second Ethernet LAN and send and receive all data using the same packet-based technology. Since the phone is a data terminal, digitized audio being just another type of data from its perspective, the phone is capable of vastly more than traditional business phones. As

Polycom phones run the same protocols as your office personal computer, many innovative applications can be developed without resorting to specialized technology.

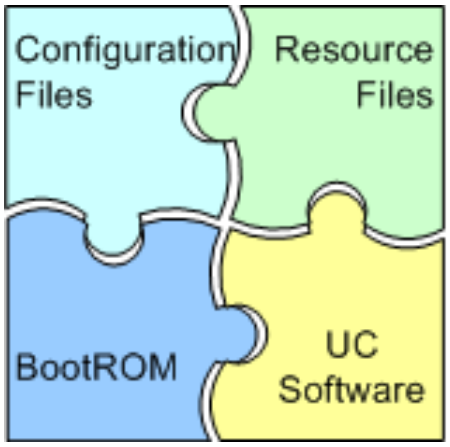


Polycom Phone Software Architecture

The architecture of the Polycom phone software is made of 4 basic components:

- BootROM—loads first when the phone is powered on
- Polycom UC Software—software that implements the phone and the related functionality of the device
- Configuration—configuration parameters stored in separate files

- Resource Files—optional, needed by some of the advanced features



BootROM

The BootROM is a small application that resides in the flash memory on the phone. All phones come from the factory with a BootROM pre-loaded.

The BootROM performs the following tasks in order:

1. Performs a power on self test (POST).
2. (Optional) Allows you to enter the setup menu where various network and provisioning options can be set.

   The BootROM software controls the user interface when the setup menu is accessed.
3. Requests IP settings and accesses the provisioning server (or boot server) to look for any updates to the BootROM application.

   If updates are found, they are downloaded and saved to flash memory, eventually overwriting itself after verifying the integrity of the download.
4. If a new BootROM is downloaded, formats the file system clearing out any application software and configuration files that may have been present.
5. Downloads the master configuration file.

   This file is either called **<MAC-address>.cfg** or **000000000000.cfg** . This file is used by the BootROM and the application for a list of other files that are needed for the operation of the phone.
6. Examines the master configuration file for the name of the application file, and then looks for this file on the provisioning server.

   If the copy on the provisioning server is different than the one stored in flash memory or there is no file stored in flash memory, the application file is downloaded.

7. Extracts the application from flash memory.
8. Installs the application into RAM, then uploads a log file with events from the boot cycle.

The BootROM will then terminate, and the application takes over.

Polycom UC Software

The Polycom UC Software manages the VoIP stack, the digital signal processor (DSP), the user interface, and the network interaction. UC Software manages everything to do with the phone's operation. UC software implements the following functions and features:

- VoIP signalling for a wide range of voice and video telephony functions using SIP signalling for call setup and control.
- H.323 signalling for video telephony.
- Industry standard security techniques for ensuring that all provisioning, signalling, and media transactions are robustly authenticated and encrypted.
- Advanced audio signal processing for handset, headset, and speakerphone communications using a wide range of audio codecs.
- Flexible provisioning methods to support single phone, small business, and large multi-site enterprise deployments.

The software is a single file binary image and contains a digital signature to prevent tampering or loading rogue software images.

There is a new image file in each release of software.

The software performs the following tasks in order:

1. Downloads system, per-phone configuration, and resource files.

   There are a number of configuration template files (for example, **sip-basic.cfg** and **reg-basic.cfg**). Customize these files for your own use. Include only those that you need. For more information, refer to Sample Template Files on page A-6.
2. Controls all aspects of the phone.
3. Uploads log files.

BootROM and Polycom UC Software Wrapper

Both the BootROM and Polycom UC Software run on multiple platforms (meaning all previously released versions of hardware that are still supported).

Current build archives have both split and combined images, so it is up to the administrator which model(s) to support. Using split files saves a lot of internal network traffic during reboots and updates.

Note As of SIP 3.2.2, the VVX 1500 BootROM and SIP software were distributed as a one package.

Configuration

The Polycom phones can be configured automatically through files stored on a central provisioning server, manually through the phone's local UI or web interface, or by using a combination of the automatic and manual methods.

The recommended method for configuring phones is automatically through a central provisioning server, but if one is not available, the manual method will allow changes to most of the key settings.

Warning Configuration files should only be modified by a knowledgeable system administrator. Applying incorrect parameters may render the phone unusable. The configuration files which accompany a specific release of UC Software must be used together with that software. Failure to do this may render the phone unusable.

Note You can make changes to the configuration files through the web interface to the phone. Using your chosen browser, enter the phone's IP address as the browser address. For more information, refer to Modifying Phone's Configuration Using the Web Interface on page C-25.

Changes made through the web interface are written to the override file (highest priority). These changes remain active and will take precedence over the configuration files stored on the provisioning server until **Reset Web Configuration** is performed.

The precedence order for configuration parameter changes is as follows (highest to lowest):

- User changes through the phone's user interface
- Web configuration through a browser
- Polycom CMA system
- Configuration files
- Default values

The phone configuration files consist of:

- Master Configuration Files
- Polycom UC Software Configuration Files
- Override Files

This section also contains information on:

- Central Provisioning
- Manual Configuration

Master Configuration Files

The master configuration files can be one of:

- Specified master configuration file
- Per-phone master configuration file
- Default master configuration file

For more information, refer to Master Configuration Files on page A-2.

Polycom UC Software Configuration Files

Configuration files can be arranged in a flexible manner and parameters may be moved around within the files and the filenames themselves can be changed as needed. These files dictate the behavior of the phone once it is running the executable specified in the master configuration file. Configuration parameters may be included in more than one configuration file. In this case, the parameter encountered first when reading the configuration files from left to right in the **<MACAddress>.cfg** file will take precedence. As of Polycom UC Software 3.3.0, the use of configuration files is optional, which means that the phone will attempt to boot up even if there are no configuration files on the provisioning server.

For more information, refer to Sample Template Files on page A-6.

Override Files

This file contains all changes that are made by a user through the their phone (for example, time/date formats, ring types, and backlight intensity). The file allows the phone to keep user preferences through reboots and upgrades (providing that the system permits the override file to be written to the provisioning server).

As of Polycom UC Software 3.3.0, separate overrides files are kept for local and web configuration changes.

- There is an option to clear the local override file available to the system administrator—press the **Menu** key, and then select **Settings > Advanced > Admin Settings > Reset to Defaults > Reset Local Configuration**. You will be prompted to enter the administrative password.
- There is an option to clear the web override file available to the system administrator—press the **Menu** key, and then select **Settings > Advanced > Admin Settings > Reset to Defaults > Reset Web Configuration**. You will be prompted to enter the administrative password.

Central Provisioning

The phones can be centrally provisioned from a provisioning server through a system of global and per-phone configuration files. The provisioning server also facilitates automated application upgrades, logging, and a measure of fault tolerance. Multiple redundant provisioning servers can be configured to improve reliability.

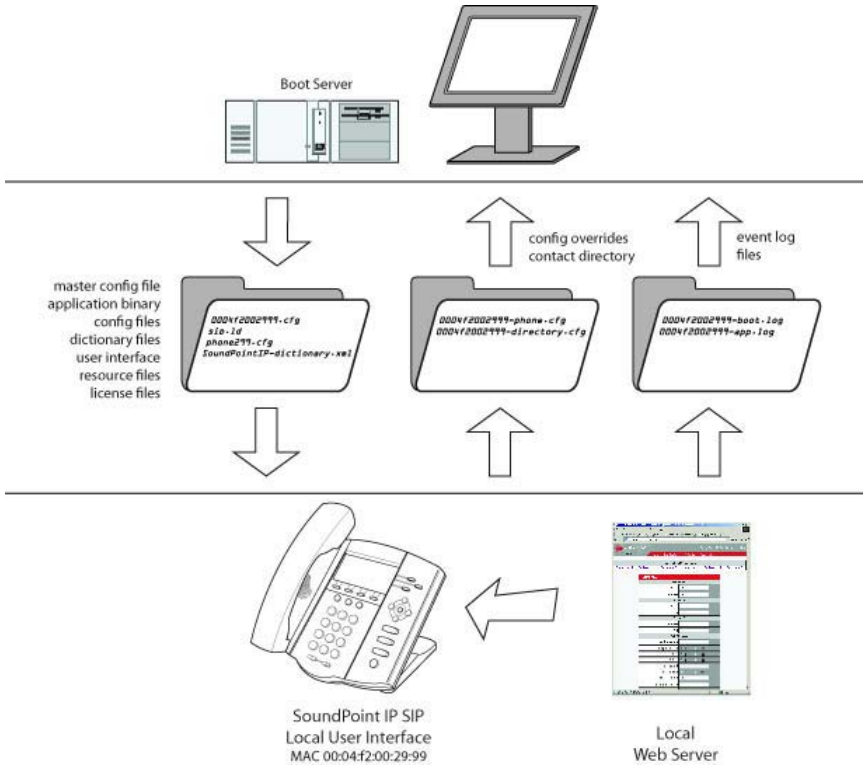
In the central provisioning method, there are two major classifications of configuration files:

- System configuration files
- Per-phone configuration files

Parameters can be stored in the files in any order and can be placed in any number of files. For example, it might be desirable to set the default CODEC for a remote user differently than for all the users who reside in the head office. By adding the CODEC settings to a particular user's per-phone file, the values in the system file are ignored.

Note Verify the order of the configuration files. Parameters in the configuration file loaded first will overwrite those in later configuration files.

The following figure shows one possible layout of the central provisioning method.



Manual Configuration

When the manual configuration method is employed (using the phone's user interface and/or the web interface), any changes made are stored in a configuration override file. This file is stored on the phone, but a copy will also be uploaded to the central provisioning server if one is being used. When the phone boots, this file is loaded by the application after any centrally provisioned files have been read, and its settings will override those in the centrally provisioned files.

This can create a lot of confusion about where parameters are being set, and so it is best to avoid using the manual method unless you have good reason to do so.

Resource Files

In addition to the application and the configuration files, the phones may require resource files that are used by some of the advanced features. These files are optional, but if the particular feature is being employed, these files are required.

Some examples of resource files include:

- Language dictionaries
- Custom fonts
- Ring tones
- Synthesized tones
- Contact directories

Note If you need to remove the resource files from a phone at some later date—for example, you are giving the phone to a new user—instructions on how to put the phone into the factory default state can be found in "Quick Tip 18298: Resetting and Rebooting Polycom Phones" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Available Features

This section provides information about the features available on the Polycom phones running Polycom UC Software:

- Basic User Features
  - Automatic Off-Hook Call Placement—Supports an optional automatic off-hook call placement feature for each registration.

- Call Forward—Provides a flexible call forwarding feature to forward calls to another destination.
- Call Hold—Pauses activity on one call so that the user may use the phone for another task, such as making or receiving another call.
- Call Log—Contains call information such as remote party identification, time and date, and call duration in three separate lists, missed calls, received calls, and placed calls on most platforms.
- Call Park/Retrieve—An active call can be parked. A parked call can be retrieved by any phone.
- Call Timer—A separate call timer, in hours, minutes, and seconds, is maintained for each distinct call in progress.
- Call Transfer—Call transfer allows the user to transfer a call in progress to some other destination.
- Call Waiting—When an incoming call arrives while the user is active on another call, the incoming call is presented to the user visually on the display and a configurable sound effect will be mixed with the active call audio.
- Called Party Identification—The phone displays and logs the identity of the party specified for outgoing calls.
- Calling Party Identification—The phone displays the caller identity, derived from the network signaling, when an incoming call is presented, if information is provided by the call server.
- Connected Party Identification—The identity of the party to which the user has connected is displayed and logged, if the name is provided by the call server.
- Message Waiting Indication—The volume of user interface sound effects, such as the ringer, and the receive volume of call audio is adjustable.
- Customizable Audio Sound Effects—Audio sound effects used for incoming call alerting and other indications are customizable.
- Directed Call Pick-Up and Group Call Pick-Up—Calls to another phone can be picked up by dialing the extension of the other phone. Calls to another phone within a pre-defined group can be picked up without dialing the extension of the other phone.
- Distinctive Call Waiting—Calls can be mapped to distinct call waiting types.
- Distinctive Incoming Call Treatment—The phone can automatically apply distinctive treatment to calls containing specific attributes.
- Distinctive Ringing—The user can select the ring type for each line and the ring type for specific callers can be assigned in the contact directory.

- Do Not Disturb—A do-not-disturb feature is available to temporarily stop all incoming call alerting.
- Graphic Display Backgrounds—A picture or design displayed on the background of the graphic display.
- Handset, Headset, and Speakerphone—SoundPoint IP phones come standard with a handset and a dedicated headset connection (headset not supplied). All SoundPoint IP, SoundStation IP, and VVX phones have full-duplex speakerphones.
- Idle Display Image Display—All phones can display a customized animation on the idle display in addition to the time and date.
- Last Call Return—The phone allows call server-based last call return.
- Local / Centralized Conferencing—The phone can conference together the local user with the remote parties of two independent calls and can support centralized conferences for which external resources are used such as a conference bridge. The advanced aspects of conferencing are part of the Productivity Suite.
- Local Contact Directory—The phone maintains a local contact directory that can be downloaded from the provisioning server and edited locally. Any edits to the Contact Directory made on the phone are saved to the provisioning server as a backup.
- Local Digit Map—The phone has a local digit map to automate the setup phase of number-only calls.
- Message Waiting Indication—The phone will flash a message-waiting indicator (MWI) LED when instant messages and voice messages are waiting.
- Microphone Mute—When the microphone mute feature is activated, visual feedback is provided.
- Missed Call Notification—The phone can display the number of calls missed since the user last looked at the Missed Calls list.
- Soft Key Activated User Interface—The user interface makes extensive use of intuitive, context-sensitive soft key menus.
- Speed Dial—The speed dial system allows calls to be placed quickly from dedicated keys as well as from a speed dial menu.
- Time and Date Display—Time and date can be displayed in certain operating modes such as when the phone is idle and during a call.

- Advanced Features
  - Access URL in SIP Message—Ability for the SoundPoint IP phones to be able to receive a URL inside a SIP message (for example, as a SIP header extension in a SIP INVITE) and subsequently access that given URL in the Microbrowser.
  - SIP-B Automatic Call Distribution—Supports ACD agent available and unavailable and allows ACD login and logout. Requires call server support.
  - Bridged Line Appearance—Calls and lines on multiple phones can be logically related to each other. Requires call server support.
  - Browser and Microbrowser—The SoundPoint IP 450, 550, 560, 600, 601, 650, and 670 desktop phones, the SoundStation IP 5000, 6000, and 7000 conference phones, and the VVX 1500 phones (pre-SIP 3.2.2) support an XHTML microbrowser. The VVX 1500 phones running SIP 3.2.2 or later support a Webkit browser.
  - Busy Lamp Field—Allows monitoring the hook status and remote party information of users through the busy lamp field (BLF) LEDs and displays on an attendant console phone. This feature may require call server support.
  - Capturing Phone's Current Screen—Allows the phone's current display to be displayed in a web browser.
  - Configurable Feature Keys—Certain key functions can be changed from the factory defaults.
  - Configurable Soft Keys—Allows users to create their own soft keys and have them displayed with or without the standard SoundPoint IP and SoundStation IP soft keys.
  - Corporate Directory—The phone can be configured to access your corporate directory if it has a standard LDAP interface. This feature is part of the Productivity Suite. Active Directory, OpenLDAP, Microsoft ADAM, and SunLDAP are currently supported.
  - Customizable Fonts—The phone's user interface can be customized by changing the fonts used on the display and the LED indicator patterns.
  - Display of Warnings from SIP Headers—Displays a "pop-up" to user that is found in the Warning Field from a SIP header.
  - Downloadable Fonts—New fonts can be loaded onto the phone.
  - Enhanced Busy Lamp Field—Allows an attendant to see a remote line that is Ringing and answer a remote ringing call using a single key-press. Also allows the attendant to view the caller-id of remote active and ringing calls. This feature may require call server support.
  - Enhanced Feature Keys (EFKs)—Allows users to redefine soft keys to suit their needs. In SIP 3.0, this feature required a license key.

- Feature Synchronized Automatic Call Distribution—Supports ACD agent available and unavailable and allows ACD sign in and sign out. Requires call server support.
- Instant Messaging—Supports sending and receiving instant text messages.
- LLDP and Supported TLVs—Support for Link Layer Discovery Protocol (LLDP) and media extensions (LLDP-MED) such as VLAN configuration. For provisioning information, refer to Ethernet Menu on page 3-12.
- Microsoft Live Communications Server 2005 Integration—SoundPoint IP and SoundStation IP phones can be used with Microsoft Live Communications Server 2005 and Microsoft Office Communicator to help improve business efficiency and increase productivity and to share ideas and information immediately with business contacts. Requires call server support.
- Multilingual User Interface—All phones have multilingual user interfaces.
- Multiple Call Appearances—The phone supports multiple concurrent calls. The hold feature can be used to pause activity on one call and switch to another call.
- Multiple Line Keys per Registration—More than one line key can be allocated to a single registration.
- Multiple Registrations—SoundPoint IP desktop phones and VVX 1500 phones support multiple registrations per phone. However, SoundStation IP conference phones support a single registration.
- Network Address Translation—The phones can work with certain types of network address translation (NAT).
- Presence—Allows the phone to monitor the status of other users/devices and allows other users to monitor it. Requires call server support.
- Quick Setup of Polycom Phones—Simplifies the process of entering provisioning server parameters.
- Real-Time Transport Protocol Ports—The phone treats all real- time transport protocol (RTP) streams as bi-directional from a control perspective and expects that both RTP end points will negotiate the respective destination IP addresses and ports.
- Recording and Playback of Audio Calls — Recording and playback allows the user to record any active conversation using the phone on a USB device. The files are date and time stamped for easy archiving and can be played back on the phone or on any computer with a media playback program that supports the **.wav** format. This feature is part of the Productivity Suite.

  - Server Redundancy—Server redundancy is often required in VoIP deployments to ensure continuity of phone service for events where the call server needs to be taken offline for maintenance, the server fails, or the connection from the phone to the server fails.
  - Shared Call Appearances—Calls and lines on multiple phones can be logically related to each other. Requires call server support.
  - Static DNS Cache—Set up a static DNS cache and provide for negative caching.
  - Synthesized Call Progress Tones—In order to emulate the familiar and efficient audible call progress feedback generated by the PSTN and traditional PBX equipment, call progress tones are synthesized during the life cycle of a call. Customizable for certain regions, for example, Europe has different tones from North America.
  - Voice Mail Integration—Compatible with voice mail servers.

- Audio Features
  - Acoustic Echo Cancellation—Employs advanced acoustic echo cancellation for hands-free operation.
  - Audio Codecs—Supports a wide range of industry standard audio codecs.
  - Automatic Gain Control—Designed for hands-free operation, boosts the transmit gain of the local user in certain circumstances.
  - Background Noise Suppression—Designed primarily for hands-free operation, reduces background noise to enhance communication in noisy environments.
  - Comfort Noise Fill—Designed to help provide a consistent noise level to the remote user of a hands-free call.
  - DTMF Event RTP Payload—Conforms to RFC 2833, which describes a standard RTP-compatible technique for conveying DTMF dialing and other telephony events over an RTP media stream.
  - DTMF Tone Generation—Generates dual tone multi-frequency (DTMF) tones in response to user dialing on the dial pad.
  - Dynamic Noise Reduction— Provides maximum microphone sensitivity, while automatically reducing background noise on SoundStation IP 7000 conference phones.
  - IEEE 802.1p/Q—The phone will tag all Ethernet packets it transmits with an 802.1Q VLAN header.
  - IP Type-of-Service—Allows for the setting of TOS settings.
  - Jitter Buffer and Packet Error Concealment—Employs a high-performance jitter buffer and packet error concealment system designed to mitigate packet inter-arrival jitter and out-of-order or lost (lost or excessively delayed by the network) packets.

  - Low-Delay Audio Packet Transmission—Designed to minimize latency for audio packet transmission.
  - Treble/Bass Controls—Equalizes the tone of the high and low frequency sound from the speakers on SoundStation IP 7000 conference phones.
  - Voice Activity Detection—Conserves network bandwidth by detecting periods of relative "silence" in the transmit data path and replacing that silence efficiently with special packets that indicate silence is occurring.
  - Voice Quality Monitoring—Generates various quality metrics including MOS and R-factor for listening and conversational quality. This feature is part of the Productivity Suite.

- Video Features
  - Video Codecs—Support the standard video codecs on the VVX 1500 phones only.
  - H.323 Protocol—Support for the H.323 protocol for the VVX 1500 phones only.
- Video Integration Features
  - For more information on how to use the SoundStation IP 7000 with Polycom HDX systems, refer to the "SoundStation IP 7000 & Polycom HDX Systems" support page at http://www.polycom.com/support/voice/soundstation_ip_series/soundstation_ip7000_hdx_series.html .
- Security Features
  - Local User and Administrator Privilege Levels—Several local settings menus are protected with two privilege levels, user and administrator, each with its own password.
  - Configuration File Encryption—Confidential information stored in configuration files must be protected (encrypted). The phone can recognize encrypted files, which it downloads from the provisioning server and it can encrypt files before uploading them to the provisioning server.
  - Custom Certificates—When trying to establish a connection to a provisioning server for application provisioning, the phone trusts certificates issued by widely recognized certificate authorities (CAs).
  - Digital Certificates— Support for digital certificates and associated private keys on certain models of Polycom phones.
  - Incoming Signaling Validation—Levels of security are provided for validating incoming network signaling.
  - Mutual TLS Authentication—Support for phone authentication of the server and server authentication of the phone.

  - Secure Real-Time Transport Protocol—Encrypting audio streams to avoid interception and eavesdropping.

For more information on each feature and its associated configuration parameters, see the appropriate section in Configuring Your System on page 4-1.

New Features in Polycom UC Software 3.3.0

Note

Certain phone models (referred to as 'legacy' phones) are not supported in the Polycom UC Software 3.3.0 release.

The SoundPoint IP 300 and 500 phones will be supported on the latest maintenance patch release of the SIP 2.1 software stream—currently SIP 2.1.4 . Any new features introduced after SIP 2.1.4 are not supported. Refer to the *SIP 2.1 Administrator Guide*, which is available at http://www.polycom.com/global/documents/support/setup_maintenance/products/voice/sip_2.1_addendum_to_sip_2.0_administrator%27s_guide.pdf .

The SoundPoint IP 301, 501, 600, and 601 and the SoundStation IP 4000 phones will be supported on the latest maintenance patch release of the SIP 3.1 software stream—currently SIP 3.1.6 . Any new features introduced after 3.1.6 are not supported. Configuration parameters related to these phones will be removed from the **sip.cfg** and **phone1.cfg** files in the next major release. To administer these phones, refer to the *SIP 3.1 Administrator's Guide*, which is available at http://www.polycom.com/voicedocumentation/ .

The SoundPoint IP 430 will be supported on the latest maintenance part release of the SIP 3.2 software stream—currently 3.2.3 . Any new features introduced after 3.2.3 are not supported. Configuration parameters related to these phones have been removed. To administer these phones, refer to the *SIP 3.2 Administrator's Guide*, which is available at http://www.polycom.com/voicedocumentation/ .

The following new features were introduced in SIP 3.2.3:

- DHCP Menu—This feature has been enhanced as follows:
  - Support for an alternate format for DHCP option 60 as well as the introduction of DHCP Vendor Identifying Options 43 and 125.

The following existing features were changed in SIP 3.2.3:

- Audible Ringer Location—Allows the user to change where incoming call ringing plays out.
- Server Redundancy—Polycom phones have a "failover" feature that enables them to re-register before diverting SIP signaling to an alternate server.
- A new loud ringer .wav file—**Warble.wav**—was introduced.

The following new features were introduced in Polycom UC Software 3.3.0:

- Support for EAPOL Logoff Message—The PC Ethernet port on the SoundPoint IP 33x, 450, 550, 560, 601, 650, and 670, and Polycom VVX 1500 phone can be used to connect a computer to the network with the phone acting as a pass-through switch.
- Locking the Phone—Protects unattended phones, but allows authorized and emergency calls to be placed.
- Configurable TLS Cipher Suites—Allow administrators to configure which cipher suites may be used for TLS connections, including support for the 'null' cipher which is useful for troubleshooting purposes.
- Calling Party Identification—These features have been enhanced as follows:
  - During the 'ringing' stage of an incoming call on the SoundPoint IP 331 and 335, the caller ID will automatically scroll. Auto-scrolling stops— the left and right arrow keys can be used to scroll—once the call is connected.

The following existing features were changed in Polycom UC Software 3.3.0:

- Configuration Parameters—Significant changes to the configuration system in this release. For a brief introduction, refer to "Technical Bulletin 56449: Polycom SoundPoint IP/SoundStation IP/VVX Software Changes". For more detailed information, refer to "Technical Bulletin 60519: Simplified Configuration Enhancements in Polycom UC Software 3.3.0". Both technical bulletins can be found at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html
- Enhanced Feature Keys—Supported on SoundStation IP 5000, 6000, and 7000 conference phones.
- Local / Centralized Conferencing—The behavior of Polycom phones when the conference host exits a conference is now configurable:
  - The remaining parties are left connected and can continue to talk. This is the previous behavior.
  - All parties are disconnected from the conference.

Documentation of the newly released SoundStation IP 5000 conference phone has also been added.

Note When SoundPoint IP 32x/33x is used in this guide, it includes the SoundPoint IP 320, 321, 330, 331, and 335 phones.

3

Setting up Your System

Your Polycom® phone is designed to be used like a regular phone on a public switched telephone network (PSTN).

This chapter provides basic instructions for setting up your Polycom phones. This chapter contains information on:

- Setting Up the Network
- Setting Up the Provisioning Server
- Deploying Phones From the Provisioning Server
- Upgrading Polycom UC Software

Because of the large number of optional installations and configurations that are available, this chapter focuses on one particular way that the Polycom® UC Software and the required external systems might initially be installed and configured in your network.

For more information on configuring your system, refer to Configuring Your System on page 4-1. For more information on the configuration files required for setting up your system, refer to Configuration Files on page A-1.

For installation and maintenance of Polycom phones, the use of a provisioning server is strongly recommended. This allows for flexibility in installing, upgrading, maintaining, and configuring the phone. Configuration, log, and directory files are normally located on this server. Allowing the phone write access to the server is encouraged.

The phone is designed such that, if it cannot locate a provisioning server when it boots up, it will operate with internally saved parameters. This is useful for occasions when the provisioning server is not available, but is not intended to be used for long-term operation of the phones.

However, if you want to register a single Polycom phone, refer to “Quick Tip 44011: Register Standalone Polycom Phones“ at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

This chapter also contains information on:

- Provisioning SoundStation IP 7000 Phones Using C-Link
- Provisioning VVX 1500 Phones Using a Polycom CMA System

Setting Up the Network

Regardless of whether or not you will be installing a centrally provisioned system, you must perform basic TCP/IP network setup, such as IP address and subnet mask configuration, to get your organization's phones up and running.

Polycom UC Software uses the network to query the provisioning server for upgrades, which is an optional process that will happen automatically when properly deployed. For more information on the basic network settings, refer to DHCP or Manual TCP/IP Setup on page 3-2.

The BootROM on the phone performs the provisioning functions of downloading the BootROM, the **<MACaddress>.cfg** file, and UC Software, and uploading log files. For more information, refer to Supported Provisioning Protocols on page 3-4.

Basic network settings can be changed during BootROM download using the BootROM's setup menu. A similar menu system is present in the application for changing the same network parameters. For more information, refer to Modifying the Network Configuration on page 3-6.

DHCP or Manual TCP/IP Setup

Basic network settings can be derived from DHCP, or entered manually using the phone's LCD-based user interface, or downloaded from configuration files.

Polycom recommends using DHCP where possible to eliminate repetitive manual data entry.

The following table shows the manually entered networking parameters that may be overridden by parameters obtained from a DHCP server, an alternate DHCP server, or configuration file:

Parameter	DHCP Option	DHCP	Alternate DHCP	Configuration File (application only)	Local FLASH
		⇨ priority when more than one source exists ⇨			
		1	2	3	4
IP address	1	•	-	-	•
subnet mask	1	•	-	-	•
IP gateway	3	•	-	-	•
boot server address	Refer to DHCP Menu on page 3-8	•	•	-	•
SIP server address	151 ***Note:*** *This value is configurable*.	•	-	-	•
SNTP server address	42 then 4	•	-	•	•
SNTP GMT offset	2	•	-	•	•
DNS server IP address	6	•	-	-	•
alternate DNS server IP address	6	•	-	-	•
DNS domain	15	•	-	-	•
VLAN ID	Refer to DHCP Menu on page 3-8	***Warning:*** *Link Layer Discovery Protocol (LLDP) overrides Cisco Discovery Protocol (CDP). CDP overrides Local FLASH which overrides DHCP VLAN Discovery.*			

For more information on DHCP options, go to http://www.ietf.org/rfc/rfc2131.txt?number=2131 or http://www.ietf.org/rfc/rfc2132.txt?number=2132.

Note

The configuration file value for ***SNTP server address*** and ***SNTP GMT offset*** can be configured to override the DHCP value. Refer to `tcpIpApp.sntp.addressoverrideDHCP` in <sntp/> on page A-113.

The CDP Compatibility value can be obtained from a connected Ethernet switch if the switch supports CDP.

In the case where you do not have control of your DHCP server or do not have the ability to set the DHCP options, an alternate method of automatically discovering the provisioning server address is required. Connecting to a secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server value is one possibility. For more information, refer to http://www.ietf.org/rfc/rfc3361.txt?number=3361 and http://www.ietf.org/rfc/rfc3925.txt?number=3925.

Supported Provisioning Protocols

The BootROM performs the provisioning functions of downloading configuration files, uploading and downloading the configuration override file and user directory, and downloading the dictionary and uploading log files.

The protocol that will be used to transfer files from the provisioning server depends on several factors including the phone model and whether the BootROM or Polycom UC Software stage of provisioning is in progress. By default, the phones are shipped with FTP enabled as the provisioning protocol. If an unsupported protocol is specified, this may result in a defined behavior (see the table below for details of which protocol the phone will use). The Specified Protocol listed in the table can be selected in the ***Server Type*** field or the ***Server Address*** can include a transfer protocol, for example http://usr:pwd@server (refer to Server Menu on page 3-11). The boot server address can be an IP address, domain string name, or URL. The boot server address can also be obtained through DHCP. Configuration file names in the **<MACaddress>.cfg** file can include a transfer protocol, for example https://usr:pwd@server/dir/file.cfg. If a user name and password are specified as part of the server address or file name, they will be used only if the server supports them.

Note

A URL should contain forward slashes instead of back slashes and should not contain spaces. Escape characters are not supported. If a user name and password are not specified, the Server User and Server Password will be used (refer to Server Menu on page 3-11).

Specified Protocol	Protocol used by BootROM		Protocol used by Polycom UC Software
	IP 32x, 33x, 450, 550, 560, 650, 670, 5000, 6000, and 7000	VVX 1500	IP 32x, 33x, 450, 550, 560, 650, 670, 5000, 6000, and 7000, VVX 1500
FTP	FTP	FTP	FTP
TFTP	TFTP	TFTP	TFTP
HTTP	HTTP	HTTP	HTTP
HTTPS	HTTP	HTTPS	HTTPS

Note There are two types of FTP methods—active and passive. UC Software is not compatible with active FTP. Secure provisioning was implemented in a previous release.

Note Setting Option 66 to tftp://192.168.9.10 has the effect of forcing a TFTP download. Using a TFTP URL (for example, tftp://provserver.polycom.com) has the same effect.

Note Both digest and basic authentication are supported when using HTTP/S for Polycom UC Software. Only digest authentication is supported when using HTTP by the BootROM. If the **Server Type** is configured as HTTPS, the BootROM will contact the same address and apply the same username and password to authentication challenges only the protocol used will be HTTP. No SSL negotiation will take place, so servers that do not allow unsecured HTTP connections will not be able to provision files.

For downloading the BootROM and application images to the phone, the secure HTTPS protocol is not available. To guarantee software integrity, the BootROM will only download cryptographically signed BootROM or application images. For HTTPS, widely recognized certificate authorities are trusted by the phone (refer to Trusted Certificate Authority List on page C-1) and custom certificates can be added to the phone (refer to “Technical Bulletin 17877: Using Custom Certificates With Polycom Phones“ at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

As of SIP 3.2, Mutual Transport Layer Security (TLS) authentication is available. For more information, refer to Mutual TLS Authentication on page 4-97.

Note

If you want to use digest authentication against the Microsoft Internet Information Services server:

- Use Microsoft Internet Information Server 6.0 or later.
- Digest authentication needs the user name and password to be saved in reversible encryption.
- The user account on the server must have administrative privileges.
- The wildcard must be set as MIME type; otherwise the phone will not download *.cfg, *.ld and other required files. This is due to the fact that the Microsoft Internet Information Server cannot recognize these extensions and will return a "File not found" error. To configure wildcard for MIME type, refer to http://support.microsoft.com/kb/326965 .

For more information, refer to http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/809552a3-3473-48a7-9683-c6df0cdfda21.mspx?mfr=true .

Modifying the Network Configuration

You can access the network configuration menu:

- **During BootROM Phase**. The network configuration menu is accessible during the auto-boot countdown of the BootROM phase of operation. Press the **Setup** soft key to launch the main menu.
- **During Polycom UC Software Phase**. The network configuration menu is accessible from the phone's main menu. Select **Menu>Settings>Advanced>Admin Settings>Network Configuration**. Advanced Settings are locked by default. Enter the administrator password to unlock. The factory default password is 456. Polycom recommends that you change the administrative password from the default value.

Phone network configuration parameters may be modified by means of:

- Main Menu
- DHCP Menu
- Server Menu
- Ethernet Menu
- Syslog Menu

Use the soft keys, the arrow keys, the **Select** and **Delete** keys to make changes.

Certain parameters are read-only due to the value of other parameters. For example, if the DHCP Client parameter is enabled, the ***Phone IP Addr*** and ***Subnet Mask*** parameters are dimmed or not visible since these are guaranteed to be supplied by the DHCP server (mandatory DHCP parameters) and the statically assigned IP address and subnet mask will never be used in this configuration.

Resetting to Factory Defaults

The basic network configuration referred to in the subsequent sections can be reset to factory defaults using a menu selection from the **Advanced Settings** menu or using a multiple key combination described in Multiple Key Combinations on page C-9.

Main Menu

The following configuration parameters can be modified on the main setup menu:

Name	Possible Values	Description
DHCP Client	Enabled, Disabled	If enabled, DHCP will be used to obtain the parameters discussed in DHCP or Manual TCP/IP Setup on page 3-2.
DHCP Menu		Refer to DHCP Menu on page 3-8. ***Note:*** *Disabled when DHCP client is disabled.*
Phone IP Address	dotted-decimal IP address	Phone's IP address. ***Note:*** *Disabled when DHCP client is enabled.*
Subnet Mask	dotted-decimal subnet mask	Phone's subnet mask. ***Note:*** *Disabled when DHCP client is enabled*.
IP Gateway	dotted-decimal IP address	Phone's default router.
Server Menu		Refer to Server Menu on page 3-11.
SNTP Address	dotted-decimal IP address OR domain name string	Simple Network Time Protocol (SNTP) server from which the phone will obtain the current time.
GMT Offset	-13 through +12	Offset of the local time zone from Greenwich Mean Time (GMT) in half hour increments.
DNS Server	dotted-decimal IP address	Primary server to which the phone directs Domain Name System (DNS) queries.
DNS Alternate Server	dotted-decimal IP address	Secondary server to which the phone directs Domain Name System queries.
DNS Domain	domain name string	Phone's DNS domain.

Name	Possible Values	Description
Ethernet		Refer to Ethernet Menu on page 3-12.
EM Power	Enabled, Disabled	This parameter is relevant if the phone gets Power over Ethernet (PoE). If enabled, the phone will set power requirements in CDP to 12W so that up to three Expansion Modules (EM) can be powered. If disabled, the phone will set power requirements in CDP to 5W which means no Expansion Modules can be powered (it will not work).
Syslog		Refer to Syslog Menu on page 3-13.

Note A parameter value of "???" indicates that the parameter has not yet been set and saved in the phone's configuration. Any such parameter should have its value set before continuing.

The ***EM Power*** parameter is only available on SoundPoint IP 650 and 670 phones.

Note To switch the text entry mode on the SoundPoint IP 32x/33x, press the #. You may want to use URL or IP address modes when entering server addresses.

DHCP Menu

The DHCP menu is accessible only when the DHCP client is enabled. The following DHCP configuration parameters can be modified on the DHCP menu:

Name	Possible Values	Description
Boot Server	0=Option 66	The phone will look for option number 66 (string type) in the response received from the DHCP server. The DHCP server should send address information in option 66 that matches one of the formats described for ***Server Address*** in the next section, Server Menu. If the DHCP server sends nothing, the following scenarios are possible: • If a boot server value is stored in flash memory and the value is not "0.0.0.0", then the value stored in flash is used. • Otherwise the phone sends out a DHCP INFORM query. - If a single alternate DHCP server responds, this is functionally equivalent to the scenario where the primary DHCP server responds with a valid boot server value. - If no alternate DHCP server responds, the INFORM query process will retry and eventually time out.

Name	Possible Values	Description
Boot Server (continued)	1=Custom	The phone will look for the option number specified by the ***Boot Server Option*** parameter (below), and the type specified by the ***Boot Server Option Type*** parameter (below) in the response received from the DHCP server. If the DHCP server sends nothing, the following scenarios are possible: • If a boot server value is stored in flash memory and the value is not “0.0.0.0”, then the value stored in flash is used. • Otherwise the phone sends out a DHCP INFORM query. - If a single alternate DHCP server responds, this is functionally equivalent to the scenario where the primary DHCP server responds with a valid boot server value. - If no alternate DHCP server responds, the INFORM query process will retry and eventually time out.
	2=Static	The phone will use the boot server configured through the Server Menu. For more information, refer to the next section, Server Menu.
	3=Custom+Option 66	The phone will first use the custom option if present or use Option 66 if the custom option is not present. If the DHCP server sends nothing, the following scenarios are possible: • If a boot server value is stored in flash memory and the value is not “0.0.0.0”, then the value stored in flash is used. • Otherwise the phone sends out a DHCP INFORM query. - If a single alternate DHCP server responds, this is functionally equivalent to the scenario where the primary DHCP server responds with a valid boot server value. The phone prefers the custom option value over the Option 66 value, but if no custom option is given, the phone will use the Option 66 value. - If no alternate DHCP server responds, the INFORM query process will retry and eventually time out.
Boot Server Option	128 through 254 (Cannot be the same as VLAN ID Option)	When the boot server parameter is set to Custom, this parameter specifies the DHCP option number in which the phone will look for its boot server.
Boot Server Option Type	0=IP Address, 1=String	When the ***Boot Server*** parameter is set to Custom, this parameter specifies the type of the DHCP option in which the phone will look for its boot server. The ***IP Address*** must specify the boot server. The String must match one of the formats described for ***Server Address*** in the next section, Server Menu.

Name	Possible Values	Description
VLAN Discovery	0=Disabled (default)	No VLAN discovery through DHCP.
	1=Fixed	Use predefined DHCP vendor-specific option values of 128, 144, 157 and 191. If this is used, the ***VLAN ID Option*** field will be ignored
	2=Custom	Use the number specified in the ***VLAN ID Option*** field as the DHCP private option value.
VLAN ID Option	128 through 254 (Cannot be the same as ***Boot Server Option***) (default is 129)	The DHCP private option value (when ***VLAN Discovery*** is set to Custom). For more information, refer to Assigning a VLAN ID Using DHCP on page C-21.
Option 60 Format	0=RFC 3925 Binary	Vendor identifying information in the format defined in RFC 3925, which can be found at http://tools.ietf.org/html/rfc3925 . For more information, refer to "Technical Bulletin 54041: Using DHCP Vendor Identifying Options With Polycom Phones" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html . ***Note**: DHCP option 125 containing the RFC 3295 formatted data will be sent whenever option 60 is sent.* ***Note**: DHCP option 43 data is ignored.*
	1=ASCII String	Vendor identifying information in ASCII. ***Note**: DHCP option 125 containing the RFC 3295 formatted data will be sent whenever option 60 is sent.* ***Note**: DHCP option 43 data is interpreted as encapsulated DHCP options and these will take precedence over options received outside of option 43.*

Note

If multiple alternate DHCP servers respond:

- The phone should gather the responses from alternate DHCP servers.
- If configured for `Custom+Option66`, the phone will select the first response that contains a valid "custom" option value.
- If none of the responses contain a "custom" option value, the phone will select the first response that contains a valid "option66" value.

Server Menu

The following server configuration parameters can be modified on the Server menu:

Name	Possible Values	Description
Server Type	0=FTP, 1=TFTP, 2=HTTP, 3=HTTPS, 4=FTPS, 5=Invalid	The protocol that the phone will use to obtain configuration and phone application files from the provisioning server. Refer to Supported Provisioning Protocols on page 3-4. ***Note**: Active FTP is not supported for BootROM version 3.0 or later. Passive FTP is still supported.* ***Note:** Only implicit FTPS is supported.*
Server Address	dotted-decimal IP address OR domain name string OR URL All addresses can be followed by an optional directory and optional file name.	The provisioning server to use if the DHCP client is disabled, the DHCP server does not send a boot server option, or the ***Boot Server*** parameter is set to Static. The phone can contact multiple IP addresses per DNS name. These redundant provisioning servers must all use the same protocol. If a URL is used it can include a user name and password. Refer to Supported Provisioning Protocols on page 3-4. A directory and the master configuration file can be specified. ***Note:** ":", "@", or "/" can be used in the user name or password these characters if they are correctly escaped using the method specified in RFC 1738.*
Server User	any string	The user name used when the phone logs into the server (if required) for the selected ***Server Type***. ***Note:** If the Server Address is a URL with a user name, this will be ignored.*
Server Password	any string	The password used when the phone logs in to the server if required for the selected ***Server Type***. ***Note:** If the Server Address is a URL with user name and password, this will be ignored.*
File Transmit Tries	1 to 10 Default 3	The number of attempts to transfer a file. (An attempt is defined as trying to download the file from all IP addresses that map to a particular domain name.)
Retry Wait	0 to 300 Default 1	The minimum amount of time that must elapse before retrying a file transfer, in seconds. The time is measured from the start of a transfer attempt which is defined as the set of upload/download transactions made with the IP addresses that map to a given provisioning server's DNS host name. If the set of transactions in an attempt is equal to or greater than the Retry Wait value, then there will be no further delay before the next attempt is started. For more information, refer toDeploying Phones From the Provisioning Server on page 3-17.

Name	Possible Values	Description
Tag SN to UA	Disabled, Enabled	If enabled, the phone's serial number (MAC address) is included in the User-Agent header of the Microbrowser. The default value is Disabled.

Note The ***Server User*** and ***Server Password*** parameters should be changed from the default values. Note that for insecure protocols the user chosen should have very few privileges on the server.

Ethernet Menu

The following Ethernet configuration parameters can be modified on the Ethernet menu:

Name	Possible Values	Description
LLDP	Enabled, Disabled	If enabled, the phone will use the LLDP protocol to communicate with the network switch for certain network parameters. Most often this will be used to set the VLAN that the phone should use for voice traffic. It also reports power management to the switch. The default value is Enabled. If the switch does not support it, VLAN Discovery is used. Refer to DHCP Menu on page 3-8. There are four ways to get VLAN on the phone and they can all be turned on, but the VLAN used is chosen by priority of each method. The priority is: 1. LLDP; 2. CDP; 3. DVD (VLAN Via DHCP); 4. Static (VLAN ID entered in config menu). For more information, refer to LLDP and Supported TLVs on page C-28.
CDP Compatibility	Enabled, Disabled	If enabled, the phone will use CDP compatible signaling to communicate with the network switch for certain network parameters. Most often this will be used to set the VLAN that the phone should use for Voice Traffic, and for the phone to communicate its PoE power requirements to the switch. The default value is Enabled.
VLAN ID	Null, 0 through 4094	Phone's 802.1Q VLAN identifier. The default value is Null. ***Note:*** *Null = no VLAN tagging*
VLAN Filtering	Enabled, Disabled	Filter received Ethernet packets so that the TCP/IP stack does not process bad data or too much data. Enable/disable the VLAN filtering state. The default value is Disabled.

Name	Possible Values	Description
Storm Filtering	Enabled, Disabled	Filter received Ethernet packets so that the TCP/IP stack does not process bad data or too much data. Enable/disable the DoS storm prevention state. The default value is Enabled.
LAN Port Mode	0 = Auto 1 = 10HD 2 = 10FD 3 = 100HD 4 = 100FD 5 = 1000FD	The network speed over the Ethernet. The default value is Auto. HD means half duplex and FD means full duplex. ***Note**: Polycom recommends that you do not change this setting.*
PC Port Mode	0 = Auto 1 = 10HD 2 = 10FD 3 = 100HD 4 = 100FD 5 = 1000FD -1 = Disabled	The network speed over the Ethernet. The default value is Auto. HD means half duplex and FD means full duplex. ***Note**: Polycom recommends that you do not change this setting unless you want to disable the PC port.*
1000BT LAN Clock	0=Auto 1=Slave 2=Master	The mode of the LAN clock. The default value is Slave (this device receives its clock timing from a master device). ***Note**: Polycom recommends that you do not change this setting unless you are having Ethernet connectivity issues. This setting was chosen to give the best results from an EMI perspective.*
1000BT PC Clock	0=Auto 1=Slave 2=Master	The mode of the PC clock. The default value is Auto. ***Note**: Polycom recommends that you do not change this setting unless you are having Ethernet connectivity issues. This setting was chosen to give the best results from an EMI perspective.*

Note

The LAN Port Mode applies to all phones supported by SIP 3.0 . The PC Port Mode parameters are only available on phones with a second Ethernet port.

Only the SoundPoint IP 560 and 670 and VVX 1500 phones supports the LAN Port Mode and PC Port Mode setting of 1000FD.

The 1000BT LAN Clock and 1000BT PC Clock parameters are only available on SoundPoint IP 560 and 670 phones.

Syslog Menu

Syslog is a standard for forwarding log messages in an IP network. The term "syslog" is often used for both the actual syslog protocol, as well as the application or library sending syslog messages.

The syslog protocol is a very simplistic protocol: the syslog sender sends a small textual message (less than 1024 bytes) to the syslog receiver. The receiver is commonly called "syslogd", "syslog daemon" or "syslog server". Syslog messages can be sent through UDP, TCP, or TLS. The data is sent in cleartext.

Syslog is supported by a wide variety of devices and receivers. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

The syslog protocol is defined in RFC 3164. For more information on syslog, go to http://www.ietf.org/rfc/rfc3164.txt?number=3164 .

The following syslog configuration parameters can be modified on the Syslog menu:

Name	Possible Values	Description
Server Address	dotted-decimal IP address OR domain name string	The syslog server IP address or host name. The default value is NULL.
Server Type	None=0, UDP=1, TCP=2, TLS=3	The protocol that the phone will use to write to the syslog server. If set to "None", transmission is turned off, but the server address is preserved.
Facility	0 to 23	A description of what generated the log message. For more information, refer to section 4.1.1 of RFC 3164. The default value is 16, which maps to "local 0".
Render Level	0 to 6	Specifies the lowest class of event that will be rendered to syslog. It is based on `log.render.level` and can be a lower value. Refer to <log/> on page D-4. ***Note:*** *Use left and right arrow keys to change values.*
Prepend MAC Address	Enabled, Disabled	If enabled, the phone's MAC address is prepended to the log message sent to the syslog server.

Setting Up the Provisioning Server

The provisioning server can be on the local LAN or anywhere on the Internet.

Multiple provisioning servers can be configured by having the provisioning server DNS name map to multiple IP addresses. The default number of provisioning servers is one and the maximum number is eight. The following protocols are supported for redundant provisioning servers: HTTPS, HTTP, and FTP. For more information on the protocol used on each platform, refer to Supported Provisioning Protocols on page 3-4.

All of the provisioning servers must be reachable by the same protocol and the content available on them must be identical. The parameters described in section Server Menu on page 3-11 can be used to configure the number of times each server will be tried for a file transfer and also how long to wait between each attempt. The maximum number of servers to be tried is configurable. For more information, contact your Certified Polycom Reseller.

Note Be aware of how logs, overrides and directories are uploaded to servers that map to multiple IP addresses. The server that these files are uploaded to may change over time.

If you want to use redundancy for uploads, synchronize the files between servers in the background.

However, you may want to disable the redundancy for uploads by specifying specific IP addresses instead of URLs for logs, overrides, and directory in the **<MAC-address>.cfg** .

To set up the provisioning server:

Note Use this procedure as a recommendation if this is your first provisioning server setup.

1. Install a provisioning server application or locate suitable existing server(s).

Polycom recommends that you use RFC-compliant servers.

2. Create an account and home directory.

Note If the provisioning protocol requires an account name and password, the server account name and password must match those configured in the phones. Defaults are: provisioning protocol: FTP, name: PlcmSpIp, password: PlcmSpIp.

   Each phone may open multiple connections to the server.

   The phone will attempt to upload log files, a configuration override file, and a directory file to the server. This requires that the phone's account has delete, write, and read permissions. The phone will still function without these permissions, but will not be able to upload files.

   The files downloaded from the server by the phone should be made read-only.

Note Typically all phones are configured with the same server account, but the server account provides a means of conveniently partitioning the configuration. Give each account an unique home directory on the server and change the configuration on an account-by-account basis.

3. Copy all files from the distribution zip file to the phone home directory.

   Maintain the same folder hierarchy.

   There are two distribution zip files. The combined image file contains:

   - **sip.ld**
   - a number of template files (for example, **sip-basic.cfg** and **reg-basic.cfg** can be found in the **Config** folder)
   - **000000000000.cfg**
   - **000000000000-directory~.xml**
   - **SoundPointIP-dictionary.xml** (one for each supported language)
   - **SoundPointIPWelcome.wav**

   The split image file contains individual **sip.ld** files for each model as well as the template files and dictionary files.

   Refer to the latest *Release Notes* for a detailed description of each file in the distribution and further information on determining which distribution to use.

Provisioning Server Security Policy

You must decide on a provisioning server security policy.

POLYCOM

Polycom recommends allowing file uploads to the provisioning server where the security environment permits. This allows event log files to be uploaded and changes made by the phone user to the configuration (through the web server and local user interface) and changes made to the directory to be backed up. This greatly eases our ability to provide customer support in diagnosing issues that may occur with the phone operation.

For organizational purposes, configuring a separate log file directory, override directory, contact directory, and license directory is recommended, but not required. The different directories can have different access permissions. For example, for LOG, CONTACTS, and OVERRIDES, allow full access (read and write) and for all others, read-only access. For more information on LOG_FILE_DIRECTORY, OVERRIDES, CONTACTS, and LICENSE, refer to Master Configuration Files on page A-2.

File permissions should give the minimum access required and the account used should have no other rights on the server.

The phone's server account needs to be able to add files to which it can write in the log file directory and the root directory. It must also be able to list files in all directories mentioned in the **<MAC-address>.cfg** file. All other files that the phone needs to read, such as the application executable and the standard configuration files, should be made read-only through file server file permissions.

Deploying Phones From the Provisioning Server

You can successfully deploy Polycom phones from one or more provisioning servers.

For all Polycom phones, follow the normal provisioning process in the next section, Provisioning Phones. If you have decided to daisy-chain two SoundStation IP 7000 conference phones together, read the information in Provisioning SoundStation IP 7000 Phones Using C-Link on page 3-24 to understand the different provisioning options available. If your organization uses the Polycom® Converged Management Application™ (CMA™) system, read the information in Provisioning VVX 1500 Phones Using a Polycom CMA System on page 3-25 to understand the different provisioning option available for your organization's VVX 1500 phones.

Provisioning Phones

As of Polycom UC Software 3.3.0, Polycom phones will start up without any configuration files; however, certain parameters will need to be changed for your phones to be usable within your organization (for example, registration address and label, and SIP server address). You can create as many configuration files as you want; you may want to put SIP server parameters in one file and enhanced feature key definitions on another file. If you want, you can put all parameters into one file.

These changes can be made through one of the following methods:

- Using configuration files hosted on a provisioning server
- Using a web browser to access the phone's web interface
- Using the phone's local user interface

For large scale deployments, the configuration file method is strongly recommended. For smaller scale deployments, the phone web interface or local interface may be used, but administrators need to be aware that settings made by these methods will take precedence over centralized configuration files.

For more information on creating configuration files, refer to the "Configuration File Management on Polycom Phones" white paper at http://www.polycom.com/global/documents/support/technical/products/voice/white_paper_configuration_file_management_on_soundpoint_ip_phones.pdf .

For more information on phone configuration and provisioning, refer to the appropriate Technical Bulletins and Quick Tips at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

For more information on encrypting configuration files, refer to Encrypting Configuration Files on page C-4.

To deploy phones from the provisioning server:

1. Create per-phone configuration file(s) by performing the following steps:
   a. Obtain a list of phone Ethernet addresses (barcoded label on underside of phone and on the outside of the box).
   b. Create per-phone **phone[MACaddress].cfg** file.

      For more information on template files included with Polycom UC software 3.3.0, refer to Sample Template Files on page A-6.

Note

Throughout this guide, the terms Ethernet address and MAC address are used interchangeable.

Do not use **[MACaddress]-phone.cfg** as the per-phone filename. This filename is used by the phone itself to store user preferences (overrides).

      For example, add phone registration parameters.

2. Create per-site configuration file(s) by performing the following steps:
   a. Create per-site **site[location].cfg** file.

      For more information on template files included with Polycom UC software 3.3.0, refer to Sample Template Files on page A-6.

      For example, add the SIP server or feature parameters.

      Most of the default settings are typically adequate, however, if SNTP settings are not available through DHCP, the SNTP GMT offset and (possibly) the SNTP server address will need to be edited for the correct local conditions. Changing the default daylight savings parameters will likely be necessary outside of North American locations. (Optional) Disable the local web (HTTP) server or change its signaling port if local security policy dictates (refer to <httpd/> on page A-63). Change the default location settings for user interface language and time and date format (refer to <lcl/> on page A-65).

3. Create a master configuration file by performing the following steps:

   a. Create per-phone or per-platform **<MACaddress>.cfg** files by using the **00000000000.cfg** and files from the distribution as templates.

      For more information, refer to Master Configuration Files on page A-2.

   b. Edit the CONFIG_FILES attribute of the **<MACaddress>.cfg** files so that it references the appropriate configuration file(s).

      For example, add a reference to **phone[MACaddress].cfg** and **sip650.cfg**.

   c. Edit the LOG_FILE_DIRECTORY attribute of the **<MACaddress>.cfg** files so that it points to the log file directory.

   d. Edit the CONTACT_DIRECTORY attribute of the **<MACaddress>.cfg** files so that it points to the organization's contact directory.

4. Reboot the phones by pressing the reboot multiple key combination.

   For more information, refer to Multiple Key Combinations on page C-9.

   The BootROM and UC Software modify the APPLICATION APP_FILE_PATH attribute of the **<MACaddress>.cfg** files so that it references the appropriate **sip.ld** files.

   For example, the reference to **sip.ld** is changed to **2345-11670-001.sip.ld** to boot the SoundPoint IP 670 image.

Note

At this point, the phone sends a DHCP Discover packet to the DHCP server. This is found in the Bootstrap Protocol/option "Vendor Class Identifier" section of the packet and includes the phone's part number and the BootROM version.

For example, a SoundPoint IP 650 might send the following information:

5EL@ DC?5cSc52*46*(9N7*<u6=pPolycomSoundPointIP-SPIP_6502345-12600-001,1B R/4.0.0.0155/23-May-07 13:35BR/4.0.0.0155/23-May-07 13:35

For more information, refer to Parsing Vendor ID Information on page C-22.

5. Ensure that the configuration process completed correctly.

   For example, on the phone, press the **Menu** key, and then select **Status > Platform > Application** to see the UC Software version and **Status > Platform > Configuration** to see the configuration files downloaded to the phone.

   Monitor the provisioning server event log and the uploaded event log files (if permitted). All configuration files used by the provisioning server are logged.

You can now instruct your users to start making calls.

Upgrading Polycom UC Software

You can upgrade the software that is running on the Polycom phones in your organization. The exact steps that you perform are dependent on the version of Polycom UC Software that is currently running on the phones and the version that you want to upgrade to.

The BootROM, application executable, and configuration files can be updated automatically through the centralized provisioning model. These files are read-only by default.

Most organization can use the instructions shown in the next section, Supporting Current SoundPoint IP, SoundStation IP, and VVX Phones. If you provisioned your VVX phones using CMA, refer to Upgrading Polycom UC Software Using Polycom CMA on page 3-27.

However, if your organization has a mixture of legacy phones—for example, SoundPoint IP 300, 301, 430, 500, 501, 600, 601 and/or SoundStation IP 4000 phones—deployed along with other models, you will need to change the phone configuration files to continue to support the SoundPoint IP 300, 301, 430, 500, 501, 600, and 601 and SoundStation IP 4000 phones when software releases UC Software 3.3.0 or later are deployed. These models were discontinued as follows:

- The SoundPoint IP 300 and 500 phones as of May 2006
- The SoundPoint IP 301, 600, and 601 phones as March 2008
- The SoundPoint IP 501 phone as of August 2009
- The SoundStation IP 4000 phone as of May 2009
- The SoundPoint IP 430 phone as of April 2010

In all cases, refer to Supporting Legacy SoundPoint IP and SoundStation IP Phones on page 3-22.

Warning

The SoundPoint IP 300 and 500 phones will be supported on the latest maintenance patch release of the SIP 2.1 software stream—currently SIP 2.1.4. Any critical issues that affect SoundPoint IP 300 and 500 phones will be addressed by a maintenance patch on this stream until the End of Life date for these products. Phones should be upgraded to BootROM 4.0.0 for these changes to be effective.

The SoundPoint IP 301, 501, 600, and 601 and the SoundStation IP 4000 phones will be supported on the latest maintenance patch release of the SIP 3.1 software stream—currently SIP 3.1.3 . Any critical issues that affect SoundPoint IP 300 and 500 phones will be addressed by a maintenance patch on this stream until the End of Life date for these products. Phones should be upgraded to BootROM 4.0.0 or later for these changes to be effective.

The SoundPoint IP 430 phone will be supported on the latest maintenance patch release of the SIP 3.2 software stream—currently SIP 3.2.3. Any critical issues that affect SoundPoint IP 430 phones will be addressed by a maintenance patch on this stream until the End of Life date for these products. Phones should be upgraded to BootROM 4.2.2 for these changes to be effective.

Supporting Current SoundPoint IP, SoundStation IP, and VVX Phones

Warning

If you need to upgrade any VVX 1500 phones running SIP 3.1.3 or earlier to SIP 3.2.2 or later, you must perform additional steps before rebooting the phone to download the software. Refer to "Technical Bulletin 53522: Upgrading the VVX 1500 Phone to SIP 3.2.2" at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

To update phones to Polycom UC Software 3.3.0:

1. Back up old application and configuration files.
2. Create new configuration files.

   Differences between old and new versions of configuration files are explained in the *Release Notes* that accompany the software. All changes are mandatory for upgrading to UC Software 3.3.0.

Warning

The configuration files listed in CONFIG_FILES attribute of the master configuration file must be updated when the software is updated. Any new configuration files must be added to the CONFIG_FILES attribute in the appropriate order.

Mandatory changes must be made or the software may not behave as expected.

For more information, refer to the "Configuration File Management on Polycom Phones" white paper at http://www.polycom.com/global/documents/support/technical/products/voice/white_paper_configuration_file_management_on_soundpoint_ip_phones.pdf .

3. Save the new configuration files and images (such as **sip.ld**) on the provisioning server.
4. Reboot the phones using automatic methods such as polling or check-sync.

   Using the reboot multiple key combination should be done as a backup option only. For more information, refer to Multiple Key Combinations on page C-9.

   Since the APPLICATION APP_FILE_PATH attribute of the **<MACaddress>.cfg** files references the individual **sip.ld** files, it is possible to verify that an update is applied to phones of a particular model.

   For example, the reference to **sip.ld** is changed to **2345-11670-001.sip.ld** to boot the SoundPoint IP 670 image.

   The phones can be rebooted remotely through the SIP signaling protocol. Refer to <specialEvent/> on page A-156.

The phones can be configured to periodically poll the provisioning server to check for changed configuration files or application executable. If a change is detected, the phone will reboot to download the change. Refer to <prov/> on page A-78.

Supporting Legacy SoundPoint IP and SoundStation IP Phones

With enhancements available since BootROM 4.0.0 and SIP 2.1.2, you can modify the **000000000000.cfg** or **<MACaddress>.cfg** configuration file to direct phones to load the software image and configuration files based on the phone model number. Refer to Master Configuration Files on page A-2.

Polycom UC Software 3.3.0 or later software distributions contain only the new distribution files for the new release. You must rename the **sip.ld**, **sip.cfg**, and **phone1.cfg** from a previous 2.1.x distribution that is compatible with SoundPoint IP 300 and 500 phones or a previous 3.1.y distribution that is compatible with SoundPoint IP 301, 501, 600, and 601 SoundStation IP 4000 phones or a previous 3.2.z distribution that is compatible with SoundPoint IP 430 phones.

The following procedure must be used for upgrading to UC Software 3.3.0 or later for installations that have SoundPoint IP 300, 301, 430, 500, 501, 600, 601 and SoundStation IP 4000 phones deployed. It is also recommended that this same approach be followed even if these phones are not part of the deployment as it will simplify management of phone systems with future software releases.

To upgrade phones to Polycom UC Software 3.3.0:

1. Do one of the following steps:
   a. Place all **bootrom.ld** files corresponding to BootROM release zip file onto the provisioning server.
   b. Ensure that all phones are running BootROM 4.0.0 or later code.
2. Copy **sip.ld** (or the appropriate individual **sip.ld** from the split image file) from the UC Software 3.3.0 or later release distribution onto the provisioning server.

   These are the relevant files for all phones except the SoundPoint IP 300, 301, 430, 500, 501, 600, 601 and SoundStation IP 4000 phones.
3. Rename **sip.ld**, **sip.cfg**, and **phone1.cfg** from the previous distribution to **sip_21x.ld**, **sip_21x.cfg**, and **phone1_21x.cfg** respectively on the provisioning server.

   These are the relevant files for supporting the SoundPoint IP 300 and 500 phones.

4. Rename **sip.ld**, **sip.cfg**, and **phone1.cfg** from the previous distribution to **sip_31y.ld**, **sip_31y.cfg**, and **phone1_31y.cfg** respectively on the provisioning server.

   These are the relevant files for supporting the SoundPoint IP 301, 501, 600, 601 and SoundStation IP 4000 phones.

5. Rename **sip.ld**, **sip.cfg**, and **phone1.cfg** from the previous distribution to **sip_323.ld**, **sip_323.cfg**, and **phone1_323.cfg** respectively on the provisioning server.

   These are the relevant files for supporting the SoundPoint IP 430 phones.

6. Modify the **000000000000.cfg** file, if required, to match your configuration file structure.

   For example:

```
    <APPLICATION
    APP_FILE_PATH="sip.ld"
    APP_FILE_PATH_SPIP500="sip_214.ld"
    APP_FILE_PATH_SPIP300="sip_214.ld"
    APP_FILE_PATH_SPIP601="sip_313.ld"
    APP_FILE_PATH_SPIP600="sip_313.ld"
    APP_FILE_PATH_SPIP501="sip_313.ld"
    APP_FILE_PATH_SPIP301="sip_313.ld"
    APP_FILE_PATH_SSIP4000="sip_313.ld"
    APP_FILE_PATH_SPIP430="sip_323.ld"
    CONFIG_FILES="[PHONE_MAC_ADDRESS]-user.cfg, phone1.cfg, sip.cfg"
    CONFIG_FILES_SPIP500="[PHONE_MAC_ADDRESS]-user.cfg,
phone1_214.cfg, sip_214.cfg"
    CONFIG_FILES_SPIP300="[PHONE_MAC_ADDRESS]-user.cfg,
phone1_214.cfg, sip_214.cfg"
    CONFIG_FILES_SPIP601="[PHONE_MAC_ADDRESS]-user.cfg,
phone1_313.cfg, sip_313.cfg"
    CONFIG_FILES_SPIP600="[PHONE_MAC_ADDRESS]-user.cfg,
phone1_313.cfg, sip_313.cfg"
    CONFIG_FILES_SPIP501="[PHONE_MAC_ADDRESS]-user.cfg,
phone1_313.cfg, sip_313.cfg"
    CONFIG_FILES_SPIP301="[PHONE_MAC_ADDRESS]-user.cfg,
phone1_313.cfg, sip_313.cfg"
    CONFIG_FILES_SSIP4000="[PHONE_MAC_ADDRESS]-user.cfg,
phone1_313.cfg, sip_313.cfg"
    CONFIG_FILES_SPIP430="[PHONE_MAC_ADDRESS]-user.cfg,
phone1_323.cfg, sip_323.cfg"
    MISC_FILES=""
    LOG_FILE_DIRECTORY=""
    OVERRIDES_DIRECTORY=""
    CONTACTS_DIRECTORY=""
    />
```

7. Remove any **<MACaddress>.cfg** files that may have been used with earlier releases from the provisioning server.

Note

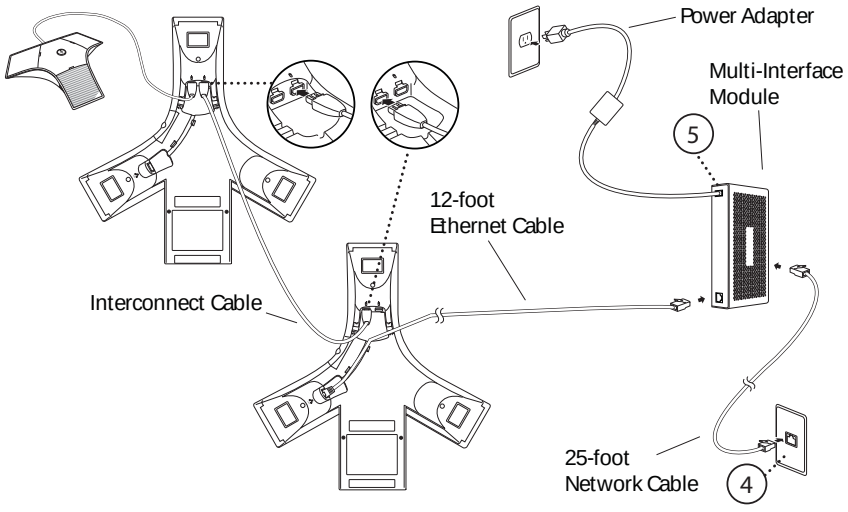
This approach takes advantage of an enhancement that was added in BootROM 3.2.1/SIP 2.0.1 that allows for the substitution of the phone specific [MACADDRESS] inside configuration files. This avoids the need to create unique **<MACaddress>.cfg** files for each phone such that the default **000000000000.cfg** file can be used for all phones in a deployment.

If this approach is not used, then changes will need to be made to all the **<MACaddress>.cfg** files for SoundPoint IP 300, 301, 430, 500, 501, 600, and 601 and SoundStation IP 4000 phones or all of the **<MACaddress>.cfg** files if it is not explicitly known which phones are SoundPoint IP 300, 301, 430, 500, 501, 600, and 601 and SoundStation IP 4000 phones.

For more information, refer to "Technical Bulletin 35311: Supporting Legacy Polycom Phones with SIP 2.2.0, SIP 3.2.0, or Polycom UC Software 3.3.0 and Later Releases" at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Provisioning SoundStation IP 7000 Phones Using C-Link

Normally the SoundStation IP 7000 conference phone is provisioned over the Ethernet by the provisioning server. However, when two SoundStation IP 7000 phones are daisy-chained together, the one that is not directly connected to the Ethernet can still be provisioned (known as the secondary).



The provisioning over C-Link feature is automatically enabled when a SoundStation IP 7000 phone is not connected to the Ethernet. Both SoundStation IP 7000 phones must be running the same version of Polycom UC Software.

The steps for provisioning the secondary SoundStation IP 7000 phone are the same as for the primary SoundStation IP 7000 phone. You can reboot the primary without rebooting the secondary. However, the primary and

secondary should be rebooted together for the primary/secondary relationship to be recognized. If you power up both SoundStation IP 7000 phones, the primary will power up first.

Currently, provisioning over C-Link is supported for the following configurations of SoundStation IP 7000 conference phones:

- Two SoundStation IP 7000 conference phone daisy-chained together
- Two SoundStation IP 7000 conference phone daisy-chained together with one external microphone, specifically designed for the SoundStation IP 7000 conference phone

The provisioning server (or proxy) for the secondary is determined by the following criteria:

- The primary phone must be powered up using Multi-Interface Module. PoE will not provide enough power for both phones.
- If the secondary is configured for DHCP, use the primary's provisioning server if the primary is configured for DHCP.
- If the secondary is not configured for DHCP, use the secondary's static provisioning server if it exists.
- If the secondary's static provisioning server does not exists, use the primary's provisioning server (ignoring the source).

For more information on daisy-chaining and setting up the SoundStation IP 7000 conference phone, refer to the *Setup Guide for the Polycom SoundStation IP 7000 Phone*, which is available at http://www.polycom.com/voicedocumentation/.

Provisioning VVX 1500 Phones Using a Polycom CMA System

Note This functionality will be available in a future patch release.

You can provision your organization's VVX 1500 phones and update the software using a Polycom CMA system. Refer to the latest *Release Notes* for Polycom UC Software and Polycom CMA for specific compatibility requirements and recommendations.

You can also provision your organization's VVX 1500 phones in a hybrid model, using both Polycom CMA and a provisioning server. In such a situation, Polycom CMA has a higher priority. When the phone reboots, it will check the Polycom CMA system first for new software, and then checks the provisioning server for configuration files and directories to upload if directed to do so (by setting the CMA mode to **Disable**, refer to Disabling Provisioning by Polycom CMA System on page 3-27).

In dynamic management mode, the Polycom CMA system can do the following:

- Configure VVX 1500 phones using an automatic provisioning service
- Register VVX 1500 phones with a standard-based presence service, so that presence states are shared with Polycom CMA contacts
- Provide VVX 1500 phones with automatic software updates

This section contains information on:

- Provisioning Using Polycom CMA
- Upgrading Polycom UC Software Using Polycom CMA
- Monitoring by Polycom CMA

Provisioning Using Polycom CMA

Note

To be provisioned by the Polycom CMA system, the VVX phones must be running at least Polycom UC Software 3.3.0 .

Polycom CMA requires that the management application be installed on the same network to which your VVX 1500 phones are connected.

To configure the provisioning service settings on VVX 1500 phones:

1. Press the **Menu** key, and then select **Settings > Advanced > Admininstration Settings > Network Configuration > CMA Menu**.

   You must enter the administrator password to access the network configuration. The factory default password is **456**.

2. Enter the following values:
   - **CMA Mode**: Select **Static** or **Auto**.
   - **Server Address**: Enter the address of the Polycom CMA system running the provisioning service. The address can be an IP address or a fully qualified domain name. For example, **123.45.67.890** .
3. Scroll to **Login Credentials** and tap the **Select** soft key. Enter the following values:
   - **CMA Domain**: Enter the domain for registering to the provisioning service. For example, **NorthAmerica** .

Note

If you are not using a Single Sign On login with Active Directory on the Polycom CMA system, the domain will be **local** using the local accounts created on the Polycom CMA server.

   - **CMA User**: Enter the username for registering to the provisioning service. For example, **bsmith** .

- **CMA Password**: Enter the password that registers the VX 1500 phone to the provisioning service (associated with the CMA user account). For example, **123456** .

4. Tap the **Back** soft key three times.
5. Select **Save Config**.

   The VVX 1500 phone reboots.

Note

Only one phone line associated with a Polycom CMA system can be provisioned on a VVX 1500 phone, but the line key associated with that line is configurable. For more information on configuration file settings, refer to <prov/> on page A-78.

The user can now search for CMA users and groups in the CMA directory, place calls to those contacts, and view their presence status. For more information, refer to the *User Guide for the Polycom VVX 1500 Phone* at http://www.polycom.com/support/vvx1500 .

For more information about provisioning by a Polycom CMA system, refer to the *Polycom CMA System Deploying Visual Communications Administration Guide* and *Polycom CMA System Operations Guide*, which are available at http://www.polycom/support/cma_4000_5000 .

Disabling Provisioning by Polycom CMA System

To disable provisioning of the VVX 1500 phones by the Polycom CMA system:

1. Press the **Menu** key, and then select **Settings > Advanced > Admininstration Settings > Network Configuration > CMA Menu**.

   You must enter the administrator password to access the network configuration. The factory default password is **456**.
2. Enter the following values:
   - **CMA Mode**: Select **Disable**.
3. Tap the **Back** soft key twice.
4. Select **Save Config**.

   The VVX 1500 phone reboots.

Upgrading Polycom UC Software Using Polycom CMA

Software upgrades of the VVX 1500 phones are triggered by the Polycom CMA system as either automatic or scheduled updates.

Note

Software update timer changes will not take effect until the next interval—after the current interval expires. For example:

- The current software update timer is set to 60 minutes.
- The provisioning by the Polycom CMA system fails.
- The software update timer is reset to five minutes (default).

The five minute timer is not fired off until the last 60 minutes timer expires.

For more information about software updates from the Polycom CMA system, refer to the *Polycom CMA System Deploying Visual Communications Administration Guide* and *Polycom CMA System Operations Guide*, which are available at http://www.polycom/support/cma_4000_5000 .

Monitoring by Polycom CMA

The following information is sent by the VVX 1500 phone to the Polycom CMA system :

- Network adapter probe—This is the first message that the VVX 1500 phone sends to the Polycom CMA system. It provides the phone's IP address.
- Software update check—This message provides the phone model, MAC address, and UC Software version currently running on the phone.
- Software update status—This message provides confirmation of the phone's software upgrade.
- Provisioning profile—This message requests configuration data for the phone so that the user can access the CMA directory, add CMA contacts to their Buddy list, and places audio and video calls to those contacts.
- Provisioning status—This message provides confirmation of the receipt of the configuration data from the Polycom CMA system.
- Call statistics—These messages are sent for all calls placed or answered by the phone's user.
- Call end—This message is sent after all calls have ended.
- Heartbeat data—This message is sent to the Polycom CMA system periodically. How often the message is sent is configured by the administrator of the Polycom CMA system.
- Events— This message provides information like gatekeeper registration events, presence registration events, and LDAP events to the Polycom CMA system.

4

Configuring Your System

After you set up your Polycom® phones on the network, you can allow users to place and answer calls using the default configuration, however, you may require some basic changes to optimize your system for best results.

This chapter provides information for making configuration changes for:

- Setting Up Basic Features
- Setting Up Advanced Features
- Setting Up Audio Features
- Setting Up Video Features
- Setting Up Security Features

This chapter also provides instructions on:

- Configuring Polycom Phones Locally

To troubleshoot any problems with your Polycom phones on the network, refer to Troubleshooting Your Polycom Phones on page 5-1. For more information on the configuration files, refer to Configuration Files on page A-1.

Setting Up Basic Features

This section provides information for making configuration changes for the following basic features:

- Call Log
- Call Timer
- Call Waiting
- Called Party Identification
- Calling Party Identification

- Missed Call Notification
- Connected Party Identification
- Message Waiting Indication
- Distinctive Incoming Call Treatment
- Distinctive Ringing
- Distinctive Call Waiting
- Do Not Disturb
- Handset, Headset, and Speakerphone
- Local Contact Directory
- Local Digit Map
- Microphone Mute
- Soft Key Activated User Interface
- Speed Dial
- Time and Date Display
- Idle Display Image Display
- Ethernet Switch
- Graphic Display Backgrounds

This section also provides information for making configuration changes for the following basic call management features:

- Automatic Off-Hook Call Placement
- Call Hold
- Call Transfer
- Local / Centralized Conferencing
- Call Forward
- Directed Call Pick-Up
- Group Call Pick-Up
- Call Park/Retrieve
- Last Call Return

Call Log

The phone maintains a call log. The log contains call information such as remote party identification, time and date, and call duration. It can be used to redial previous outgoing calls, return incoming calls, and save contact information from call log entries to the contact directory.

The call log is stored in volatile memory and is maintained automatically by the phone in three separate lists: Missed Calls, Received Calls and Placed Calls. The call lists can be cleared manually by the user and will be erased when the phone is restarted.

Note

On some SoundPoint IP platforms, missed calls and received calls appear in one list. Missed calls appear as  and received calls appear as  .

The “call list” feature can be disabled on all SoundPoint IP and SoundStation IP platforms except the SoundPoint IP 32x/33x and SoundStation IP 7000.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Enable or disable all call lists or individual call lists. • Refer to <feature/> on page A-58.

Call Timer

A call timer is provided on the display. A separate call timer is maintained for each distinct call in progress. The call duration appears in hours, minutes, and seconds.

There are no related configuration changes.

Call Waiting

When an incoming call arrives while the user is active on another call, the incoming call is presented to the user visually on the LCD display. A configurable sound effect such as the familiar call-waiting beep will be mixed with the active call audio as well.

Configuration changes can performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify the ring tone heard on an incoming call when another call is active. • Refer to <callWaiting/> on page A-30.
	Configuration template: **reg-advanced.cfg**	Disable call waiting. • Refer to <reg/> on page A-82.

For related configuration changes, refer to Customizable Audio Sound Effects on page 4-74.

Called Party Identification

The phone displays and logs the identity of the remote party specified for outgoing calls. This is the party that the user intends to connect with.

The identity displayed is based on the number of the placed call and information obtained from the network signaling.

Note The phone does not match the number of the placed call to any entries in the Local Contact Directory or Corporate Directory.

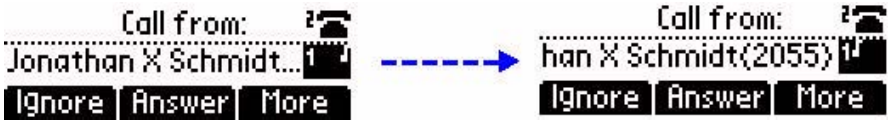
There are no related configuration changes.

Calling Party Identification

The phone displays the caller identity, derived from the network signaling, when an incoming call is presented, if the information is provided by the call server. For calls from parties for which a directory entry exists, the local name assigned to the Contact Directory entry may optionally be substituted.

Note The phone does not match the received number to any entries in the Corporate Directory.

During the 'ringing' stage of an incoming call on the SoundPoint IP 331 and 335, the caller ID will automatically scroll as of Polycom® UC Software 3.3.0. Auto-scrolling stops once the call is connected, but the left and right arrow keys can be used to scroll. For example:



Configuration changes can performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration templates: **reg-advanced.cfg**, **site.cfg**	Specify whether or not to use directory name substitution. • Refer to <up/> on page A-120.
Local	Web Server (if enabled)	Specify whether or not to use directory name substitution. Navigate to: http://<phoneIPAddress>/coreConf.htm#us Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.

Missed Call Notification

The phone can display the number of calls missed since the user last looked at the Missed Calls list. The phone can be configured to use a built-in missed call counter or to display information provided by a Session Initiation Protocol (SIP) server.

Note On some SoundPoint IP platforms, missed calls and received calls appear in one list.

Configuration changes can performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.
	Configuration template: **reg-advanced.cfg**	Specify per-registration whether all missed-call events or only remote/server-generated missed-call events will be displayed. • Refer to <serverMissedCall/> on page A-29.

Connected Party Identification

The identity of the remote party to which the user has connected is displayed and logged, if the name and ID is provided by the call server. The connected party identity is derived from the network signaling. In some cases the remote party will be different from the called party identity due to network call diversion. For example, Bob places a call to Alice, but he ends up connected to Fred. The phone does not match caller IDs against the local contact directory or corporate directory entries.

There are no related configuration changes.

Message Waiting Indication

The phone will flash a message-waiting indicator (MWI) LED when instant messages and voice messages are waiting.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify per-registration whether the MWI LED is enabled or disabled. • Refer to <mwi/> on page A-72.
	Configuration templates: **reg-advanced.cfg**, **site.cfg**	Specify whether MWI notification is displayed for registration x (pre-SIP 2.1 behavior is enabled). • Refer to <up/> on page A-120.

Distinctive Incoming Call Treatment

The phone can automatically apply distinctive treatment to calls containing specific attributes. The distinctive treatment that can be applied includes customizable alerting sound effects and automatic call diversion or rejection. Call attributes that can trigger distinctive treatment include the calling party name or SIP contact (number or URL format).

For related configuration changes, refer to Local Contact Directory on page 4-9.

Distinctive Ringing

There are three options for distinctive ringing:

1. The user can select the ring type for each line by pressing the **Menu** key, and then selecting **Settings > Basic > Ring Type**. This option has the third (lowest) priority.
2. The ring type for specific callers can be assigned in the contact directory. For more information, refer to Distinctive Incoming Call Treatment, the previous section. This option is second in priority.
3. The `voIpProt.SIP.alertInfo.x.value` and `voIpProt.SIP.alertInfo.x.class` fields can be used to map calls to specific ring types. This option requires server support and is first (highest) in priority.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify the mapping of Alert-Info strings to ring types. • Refer to <alertInfo/> on page A-155.
	Configuration template: **reg-advanced.cfg**	Specify the ring type to be used for each line. • Refer to <reg/> on page A-82.
	XML File: **<Ethernet address>-directory.xml**	This file can be created manually using an XML editor. • Refer to Local Contact Directory on page 4-9.
Local	Local Phone User Interface	The user can edit the ring types selected for each line under the Settings menu. The user can also edit the directory contents. Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Local Configuration** menu selection and the **<Ethernet address>-phone.cfg** is removed from the provisioning server.

Distinctive Call Waiting

The `voIpProt.SIP.alertInfo.x.value` and `voIpProt.SIP.alertInfo.x.class` fields can be used to map calls to distinct call waiting types, currently limited to two styles. This feature requires server support.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify the mapping of Alert-Info strings to call waiting types. • Refer to <alertInfo/> on page A-155.

Do Not Disturb

A Do Not Disturb (DND) feature is available to temporarily stop all incoming call alerting. Calls can optionally be treated as though the phone is busy while DND is enabled. DND can be configured as a per-registration feature. Incoming calls received while DND is enabled are logged as missed. For more information on forwarding calls while DND is enabled, refer to Call Forward on page 4-22.

Note A phone with a shared line that has DND enabled will show an incoming call, but the phone will not ring.

Server-based DND is active if the feature is enabled on both the phone and the server and the phone is registered. The server-based DND feature is applicable for all registrations on the phone (no per-registration mode) and it disables local Call Forward and DND features unless configured otherwise.

Server-based DND will behave the same as per-SIP 2.1 per-registration feature with the following exceptions:

- Server based DND cannot be used if the phone is configured as a shared line.
- If server-based DND is enabled, but inactive, and the user presses the DND key or selects the DND option on the Feature menu, the "Do Not Disturb" message does not appear on the user's phone (incoming call alerting will continue).

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Enable or disable server-based DND. • Refer to <SIP/> on page A-147. Enable or disable local DND behavior when server-based enabled. • Refer to <SIP/> on page A-147. Specify whether or not DND results in incoming calls being given busy treatment. • Refer to <call/> on page A-21. Specify whether DND is treated as a per-registration feature or a global feature on the phone. • Refer to <dnd/> on page A-50.
	Configuration template: **reg-advanced.cfg**	Enable or disable server-based DND as a per-registration feature. • Refer to <reg/>on page A-82.
Local	Local Phone User Interface	Enable or disable DND using the **Do Not Disturb** key on the SoundPoint IP 550, 560, 650, and 670 and the Polycom VVX 1500 or the "Do Not Disturb" option on the Features menu on the SoundPoint IP 32x/33x and 450 and SoundStation IP 5000, 6000 and 7000. ***Note:*** *The LED on the* ***Do Not Disturb*** *key on the Polycom VVX 1500 is red when pressed or when server-based DND is enabled.*

Handset, Headset, and Speakerphone

SoundPoint IP phones come standard with a handset and a dedicated connector is provided for a headset (not supplied). All Polycom phones are full-duplex speakerphones. The SoundPoint IP phones provide dedicated keys for convenient selection of either the speakerphone or headset.

All Polycom desktop phones can be configured to use the electronic hookswitch. For more information, refer to "Technical Bulletin 35150: Using an Electronic Hookswitch with SoundPoint IP and Polycom VVX 1500 Phones" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration templates: **reg-advanced.cfg**, **site.cfg**	Enable or disable persistent headset mode. • Refer to <up/> on page A-120. Enable or disable hands-free speakerphone mode. • Refer to <up/> on page A-120. Specify whether or not the electronic hookswitch is enabled and what type of headset is attached. • Refer to <up/> on page A-120. Switch audio mode from handset to headset or headset to handset. • Refer to <up/> on page A-120.
Local	Web Server (if enabled)	Enable or disable persistent headset mode. Navigate to: http://<phoneIPAddress>/coreConf.htm#us Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.
	Local Phone User Interface	Enable or disable persistent headset mode through the Settings menu (**Settings > Basic > Preferences > Headset > Headset Memory Mode**). Enable or disable hands-free speakerphone mode through the Settings menu (**Settings > Advanced > Admin Settings > Phone Settings**). Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Local Configuration** menu selection.

Local Contact Directory

The phone maintains a local contact directory. The directory can be downloaded from the provisioning server and edited locally (if configured in that way). Contact information from previous calls may be easily added to the directory for convenient future access.

The directory is the central database for several other features including speed-dial, distinctive incoming call treatment, presence, and instant messaging. The maximum number of entries in the local contact directory is phone-dependent.

Note

If a user makes a change to the local contact directory, there is a five second timeout before it is uploaded to the provisioning server as **<mac-address>-directory.xml**.

If so configured, the first and last name fields of the local contact directory entries which match incoming calls will be used for caller identification display and in the call lists (instead of the name provided through network signaling).

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **features.cfg**	Specify the maximum number of contacts allowed. • Refer to <local/> on page A-43. Specify whether or not the local contact directory is read only. • Refer to <local/> on page A-43.
	XML file**:** **000000000000-directory.xml**	A sample file named **000000000000-directory~.xml** (Note the extra "~" in the filename) is included with the application file distribution. This file can be used as a template for the per-phone ***<Ethernet address>*-directory.xml** directories (edit contents, then rename to ***<Ethernet address>*-directory.xml**). It also can be used to seed new phones with an initial directory (edit contents, then remove "~" from file name). Telephones without a local directory, such as new units from the factory, will download the **00000000000-directory.xml** directory and base their initial directory on it. These files should be edited with an XML editor. These files can be downloaded once per reflash. For information on file format, refer to the next section, Local Contact Directory File Format.
	XML file: **<Ethernet address>-directory.xml**	This file can be created manually using an XML editor. For information on file format, refer to the next section, Local Contact Directory File Format.
Local	Local Phone User Interface	The user can edit the directory contents if configured in that way. Changes will be stored in the phone's flash file system and backed up to the provisioning server copy of ***<Ethernet address>*-directory.xml** if this is configured. When the phone boots, the provisioning server copy of the directory, if present, will overwrite the local copy.

Local Contact Directory File Format

An example of a local contact directory is shown below. The subsequent table provides an explanation of each element. Elements can appear in any order.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<directory>
   <item_list>
      <item>
         <ln>Doe</ln>
```

```
            <fn>John</fn>
            <ct>1001</ct>
            <sd>1</sd>
            <lb>Mr</lb>
            <pt>H323</pt>
            <rt>1</rt>
            <dc/>
            <ad>0</ad>
            <ar>0</ar>
            <bw>0</bw>
            <bb>0</bb>
         </item>
          ...
          <item>
            <ln>Smith</ln>
            <fn>Bill</fn>
            <ct>1003</ct>
            <sd>3</sd>
            <lb>Dr</lb>
            <pt>SIP</pt>
            <rt>3</rt>
            <dc/>
            <ad>0</ad>
            <ar>0</ar>
            <bw>0</bw>
            <bb>0</bb>
         </item>
      </item_list>
   </directory>
```

Element	Permitted Values	Interpretation
fn	UTF-8 encoded string of up to 40 bytes	first name ***Note**: In some cases, this will be less than 40 characters due to UTF-8's variable length encoding.*
ln	UTF-8 encoded string of up to 40 bytes	last name ***Note**: In some cases, this will be less than 40 characters due to UTF-8's variable length encoding.*
ct	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a validSIP URL	contact Used by the phone to address a remote party in the same way that a string of digits or a SIP URL are dialed manually by the user. This element is also used to associate incoming callers with a particular directory entry. For VVX 1500 phones, the maximum field length is 128 characters; for all other phones, the maximum is 128 characters. ***Note**: This field cannot be null or duplicated.*

Element	Permitted Values	Interpretation
sd	Null, 1 to 9999	speed-dial index Associates a particular entry with a speed dial bin for one-touch dialing or dialing from the speed dial menu. ***Note**: On the SoundPoint IP 32x/33x and the SoundStation IP 7000, the maximum speed-dial index is 99.*
lb	UTF-8 encoded string of up to 40 bytes	label ***Note**: In some cases, this will be less than 40 characters due to UTF-8's variable length encoding.* ***Note**: The label of a contact directory item is by default the label attribute of the item. If the label attribute does not exist or is Null, then the concatenation of first name and last name will be used as label. A space is added between first and last names.*
pt	"SIP", "H323", or "Unspecified"	protocol The protocol to use when placing a call to this contact.
rt	Null, 1 to 21	ring type When incoming calls can be associated with a directory entry by matching the address fields, this field is used to specify ring type to be used.
dc	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a validSIP URL	divert contact The forward-to address for the autodivert feature.
ad	0,1	auto divert If set to 1, automatically diverts callers that match the directory entry to the address specified in divert contact. ***Note**: If auto-divert is enabled, it has precedence over auto-reject.*
ar	0,1	auto-reject If set to 1, automatically rejects callers that match the directory entry. ***Note**: If auto-divert is also enabled, it has precedence over auto-reject.*
bw	0,1	buddy watching If set to 1, add this contact to the list of watched phones.
bb	0,1	buddy block If set to 1, block this contact from watching this phone.

Local Digit Map

The phone has a local digit map feature to automate the setup phase of number-only calls. When properly configured, this feature eliminates the need for using the **Dial** or **Send** soft key when making outgoing calls. As soon as a digit pattern matching the digit map is found, the call setup process will complete automatically. The configuration syntax is based on recommendations in 2.1.5 of RFC 3435. The phone behavior when the user dials digits that do not match the digit map is configurable. It is possible to strip a trailing # from the digits sent or to replace certain matched digits (with the introduction of "R" to the digit map). It is also possible to direct the protocol used to place a call (with the introduction of "S" and "H" to the digit map).

For more detailed information on digit maps, refer to the next section, Digit Maps.

For more information, refer to "Technical Bulletin 11572: Changes to Local Digit Maps on Polycom Phones" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Note Digit maps do not apply to on-hook dialing. The parameter settings described in <dialplan/> on page A-34 are ignored during on-hook dialing.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **site.cfg**	Specify impossible match behavior, trailing # behavior, digit map matching strings, and time out value. • Refer to <dialplan/> on page A-34. Specify per-registration impossible match behavior, trailing # behavior, digit map matching strings, and time out values that override those per-site values. • Refer to <dialplan/> on page A-34.
Local	Web Server (if enabled)	Specify impossible match behavior, trailing # behavior, digit map matching strings, and time out value. Navigate to: http://<phoneIPAddress>/appConf.htm#ls Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the Reset Web Configuration menu selection and the **<Ethernet address>-web.cfg** is removed from the provisioning server.

Digit Maps

A digit map is defined either by a "string" or by a list of strings. Each string in the list is an alternative numbering scheme, specified either as a set of digits or timers, or as an expression over which the gateway will attempt to find a shortest possible match.

Digit map extension letter "R" indicates that certain matched strings are replaced. Digit map timer letter "T" indicates a timer expiry. Digit map protocol letters "S" and "H" indicate the protocol to use when placing a call. The following examples shows the semantics of the syntax:

- `R9RRxxxxxxx`—Remove 9 at the beginning of the dialed number
  - For example, if a customer dials 914539400, the first 9 is removed when the call is placed.
- `RR604Rxxxxxxx`—Prepend 604 to all seven digit numbers
  - For example, if a customer dials 4539400, 604 is added to the front of the number, so a call to 6044539400 is placed.
- `R9R604Rxxxxxxx`—Replaces 9 with 604
- `R999R911R`—Convert 999 to 911
- `xxR601R600Rxx`—When applied on 1160122 gives 1160022
- xR60xR600Rxxxxxxx—Any 60x will be replaced with 600 in the middle of the dialed number that matches
  - For example, if a customer dials 16092345678, a call is placed to 16002345678.
- 911xxx.T— A period (".") which matches an arbitrary number, including zero, of occurrences of the preceding construct
  - For example:
    911123 with waiting time to comply with T is a match
    9111234 with waiting time to comply with T is a match
    91112345 with waiting time to comply with T is a match
    and the number can grow indefinitely given that pressing the next digit takes less than T.
- 0xxxS|33xxH—All four digit numbers starting with a 0 are placed using the SIP protocol, whereas all four digit numbers starting with 33 are placed using the H.323 protocol.

Note

Only VVX 1500 phones will match the "H". It is ignored by all other phones and the user will need to press the **Send** soft key to complete dialing. For example, if the digit map is "33xxH", the result is as follows:

- If a VVX 1500 user dials "3302" on an H.323 or dual protocol line, the call will be placed after the user dials the last digit.
- If a SoundPoint IP 650 user dials "3307", the user must press the **Send** soft key to complete dialing.

The following guidelines should be noted:

- The letters (x, T, R, S, H) are case sensitive.
- You must use only *, #, +, or 0-9 between second and third R
- If a digit map does not comply, it is not included in the digit plan as a valid one. That is, no matching is done against it.
- There is no limitation on the number of R triplet sets in a digit map. However, a digit map that contains less than full number of triplet sets (for example, a total of 2Rs or 5Rs) is considered an invalid digit map.
- Using T in the left part of RRR syntax is not recommended. For example, R0TR322R should be avoided.

Microphone Mute

A microphone mute feature is provided. When activated, visual feedback is provided. This is a local function and cannot be overridden by the network.

There are no related configuration changes.

Soft Key Activated User Interface

The user interface makes extensive use of intuitive, context-sensitive soft key menus. The soft key function is shown above the key on the graphic display.

Using the Configurable Soft Key configuration parameters, an administrator can modify the default soft keys by removing them at different call stages and/or adding specific single or multiple functions. Refer to Enhanced Feature Keys on page 4-40 and Configurable Soft Keys on page 4-45.

Speed Dial

Entries in the local directory can be linked to the speed dial system. The speed dial system allows calls to be placed quickly from dedicated keys as well as from a speed dial menu.

For SoundPoint IP 32x/33x desktop phones and SoundStation IP 6000 and 7000 conference phones, the speed dial index range is 1 to 99. For all other SoundPoint IP and Polycom VVX phones, the range is 1 to 9999.

If Presence watching is enabled for speed dial entries, their status will be shown on the idle display (if the SIP server supports this feature). For more information, refer to Presence on page 4-60.

Configuration changes can performed centrally at the provisioning server or locally:

Central (provisioning server)	XML file: **<Ethernet address>-directory.xml**	The <sd>x</sd> element in the ***<Ethernet address>*-directory.xml** file links a directory entry to a speed dial resource within the phone. Speed dial entries are mapped automatically to unused line keys (line keys are not available on the SoundStation IP 6000 and 7000) and are available for selection within the speed dial menu. (Press the **Up** arrow key from the idle display to jump to the Speed Dial list). • Refer to Local Contact Directory on page 4-9.
Local	Local Phone User Interface	The next available Speed Dial Index is assigned to new directory entries. Key pad short cuts are available to facilitate assigning and modifying the Speed Dial Index value for entries in the directory. The Speed Dial Index field is used to link directory entries to speed dial operations. Changes will be stored in the phone's flash file system and backed up to the provisioning server copy of ***<Ethernet address>*-directory.xml** if this is configured. When the phone boots, the provisioning server copy of the directory, if present, will overwrite the local copy.

Time and Date Display

The phone maintains a local clock and calendar. Time and date can be displayed in certain operating modes such as when the phone is idle and during a call. The clock and calendar must be synchronized to a remote Simple Network Time Protocol (SNTP) timeserver. The time and date displayed on the phone will flash continuously to indicate that they are not accurate until a successful SNTP response is received. The time and date display can use one of several different formats and can be turned off. The SoundPoint IP 32x/33x and IP 450 phones have a limited selection of date formats due to a smaller display size.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration templates: **reg-advanced.cfg**, **site.cfg**	Turn time and date display on or off. • Refer to <up/> on page A-120. Set the time and date display formats. • Refer to <datetime/> on page A-68. Set the basic SNTP settings and daylight savings parameters. • Refer to <sntp/> on page A-113.
Local	Web Server (if enabled)	Set the basic SNTP and daylight savings settings. Navigate to: http://<phoneIPAddress>/coreConf.htm#ti Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection and the **<Ethernet address>-web.cfg** is removed from the provisioning server.
	Local Phone User Interface	The basic SNTP settings can be made in the Network Configuration menu. Refer to DHCP or Manual TCP/IP Setup on page 3-2. The user can edit the time and date format and enable or disable the time and date display under the Settings menu. Changes are saved to local flash and backed up to <*Ethernet address*>-phone.cfg on the provisioning server. They will permanently override global settings unless deleted through the Reset Local Config menu selection.

Idle Display Image Display

All phones can display a customized static image on the idle display in addition to the time and date. For example, a company logo could be displayed (refer to Adding a Customizable Logo on the Idle Display on page C-6).

Note As of Polycom UC Software 3.3.0, customized animations are not supported.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	To add an idle display static logo. • Refer to <bitmap/> on page A-20.

Ethernet Switch

The SoundPoint IP phones (except the SoundPoint IP 32x) and the VVX 1500 contain two Ethernet ports, labeled LAN and PC, and an embedded Ethernet switch that runs at full line-rate. The SoundStation IP phones contain only one Ethernet port, labeled LAN. The Ethernet switch allows a personal computer and other Ethernet devices to connect to the office LAN by daisy chaining through the phone, eliminating the need for a stand-alone hub. The SoundPoint IP switch gives higher transmit priority to packets originating in the phone. The phone can be powered through a local AC power adapter or can be line-powered (power supplied through the signaling or idle pairs of the LAN Ethernet cable). Line powering typically requires that the phone plugs directly into a dedicated LAN jack. Devices that do not require LAN power can then plug into the SoundPoint IP PC Ethernet port. To disable the PC Ethernet port, refer to Disabling PC Ethernet Port on page C-25.

SoundPoint IP Switch - Port Priorities

To help ensure good voice quality, the Ethernet switch embedded in the SoundPoint IP phones should be configured to give voice traffic emanating from the phone higher transmit priority than those from a device connected to the PC port. If not using a VLAN (VLAN set to blank in the setup menu), this will automatically be the case. If using a VLAN, ensure that the 802.1p priorities for both default and real-time transport protocol (RTP) packet types are set to 2 or greater. Otherwise, these packets will compete equally with those from the PC port. For more information, refer to<voice/> on page A-134 and <video/> on page A-125.

Graphic Display Backgrounds

You can set up a picture or design to be displayed on the background of the graphic display of all SoundPoint IP 450, 550, 560, 650, and 670 and Polycom VVX 1500 phones.

Note When installing a background of your choice, care needs to be taken to ensure that the background does not adversely affect the visibility of the text on the phone display. As a general rule, backgrounds should be light in shading for better usability.

For SoundPoint IP 450, 550, 560, 650, and 670 phones:

- There are a number of default backgrounds, both solid color and pictures. Both BMP and JPEG files are supported. You can also select the label color for soft key and line key labels. Users can select which background and label color appears on their phone.

  You can modify the supported solid color and pictures backgrounds. For example, you can add a gray solid color background or modify a picture to one of your choice.

For Polycom VVX 1500 phones:

- You can select the pictures or designs displayed on the background. The supported formats include JPEG, BMP, and PNG and the maximum size is 800x480. A default picture is displayed when the phone starts up the first time.

  Users can select which background appears on their individual phones. Users can also select a background from an image displayed by the digital picture frame feature (refer to Digital Picture Frame on page 4-39).

Note Support for resolutions greater than 800x480 is inconsistent. Content may be truncated or nor displayed. Progressive/multiscan JPEG images are not supported at this time.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **features.cfg**	Specify which background will be displayed. • Refer to <bg/> on page A-16.
Local	Local Phone User Interface	On the Polycom VVX 1500, the user can save one of the images as the background by selecting **Save as Background** on the touch screen.

To modify the backgrounds displayed on the supported SoundPoint IP phones:

1. Modify the **features.cfg** configuration file as follows:
   a. Open **features.cfg** in an XML editor.
   b. Locate the background parameter.
   c. For the solid backgrounds, set the name and RGB values. For example:

```
bg.hiRes.gray.pat.solid.3.name="Gray"
bg.hiRes.gray.pat.solid.3.red="128"
bg.hiRes.gray.pat.solid.3.green="128"
bg.hiRes.gray.pat.solid.3.blue="128"
```

   d. For images, select a filename. For example:

```
bg.hiRes.gray.bm.3.name="polycom.jpg"
bg.hiRes.gray.bm.3.em.name="polycomEM.jpg"
bg.hiRes.gray.bm.3.adj="0"
```

   The default size for images on a phone is 320 x 160. The default size for images on an Expansion Module is 160 x 320. Use a photo editor on a computer to adjust the image you want to display. (Edit the image so the main subject is centered in the upper right corner of the display.)

   Download the file to the provisioning server.

e Save the modified **features.cfg** configuration file.

Automatic Off-Hook Call Placement

The phone supports an optional automatic off-hook call placement feature for each registration. This feature is sometimes referred to as 'hot-dialing'.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **reg-advanced.cfg**	Specify which registrations have the feature and what contact to call when going off hook. • Refer to <autoOffHook/> on page A-28.

Call Hold

The purpose of hold is to pause activity on one call so that the user may use the phone for another task, such as to make or receive another call. Network signaling is employed to request that the remote party stop sending media and to inform them that they are being held. A configurable local hold reminder feature can be used to remind the user that they have placed calls on hold. The call hold reminder is always played through the speakerphone.

As of SIP 3.1, you can supply a Music on Hold URI if supported by the call server. For more information, refer to draft RFC *draft-worley-service-example*.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify whether RFC 2543 (c=0.0.0.0) or RFC 3264 (a=sendonly or a=inactive) outgoing hold signaling is used. • Refer to <SIP/> on page A-147. Specify local hold reminder options. • Refer to <hold/><localReminder/> on page A-27. Specify the Music on Hold URI. • Refer to <musicOnHold/> on page A-157.
Local	Web Server (if enabled)	Specify whether or not to use RFC 2543 (c=0.0.0.0) outgoing hold signaling. The alternative is RFC 3264 (a=sendonly or a=inactive). Navigate to: http://<phoneIPAddress>/appConf.htm#ls Changes are saved to local flash and backed up to **<*Ethernet address*>-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection and the **<Ethernet address>-web.cfg** is removed from the provisioning server.
	Local Phone User Interface	Use the **Call Server Configuration** menu to specify whether or not to use RFC 2543 (c=0.0.0.0) outgoing hold signaling. The alternative is RFC 3264 (a=sendonly or a=inactive).

Call Transfer

Call transfer enables the user (party A) to move an existing call (party B) into a new call between party B and another user (party C) selected by party A. The phone offers three types of transfers:

- Blind transfers—The call is transferred immediately to party C after party A has finished dialing party C's number. Party A does not hear ring-back.
- Attended transfers—Party A dials party C's number and hears ring-back and decides to complete the transfer before party C answers. This option can be disabled.
- Consultative transfers—Party A dials party C's number and talks privately with party C after the call is answered, and then completes the transfer or hangs up.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify whether to allow a transfer during the proceeding state of a consultation call. • Refer to <SIP/> on page A-147. Specify whether a transfer is blind or not. • Refer to <call/> on page A-21.

Local / Centralized Conferencing

The phone can conference together the local user with the remote parties of a configurable number of independent calls by using the phone's local audio processing resources for the audio bridging. There is no dependency on network signaling for local conferences.

All phones support three-party local conferencing. The SoundPoint IP 450, 550, 560, 650, and 670 phones may support four-way local conferencing.

Note

Four-party conferencing requires a license key for activation. For more information, refer to Manage Conferences on page 4-22.

If theconference host of a three-party local conference ends the call, the other parties of the call may still be able to communicate. If the conference host of a four-party local conference ends the call, the conference ends.

The phone also supports centralized conferences for which external resources are used such as a conference bridge. This relies on network signaling.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify the conference hold behavior (all parties on hold or only host is on hold). • Refer to <call/> on page A-21. Specify whether or not the remaining parties can communicate after the conference host exits the conference. • Refer to <call/> on page A-21. Specify whether or not all parties hear sound effects while setting up a conference. • Refer to <call/> on page A-21. Specify which type of conference to establish and the address of the centralized conference resource. • Refer to <SIP/> on page A-147.

Manage Conferences

Note

This feature is supported on the SoundPoint IP 450, 550, 560, 650, and 670 desktop phones, the SoundStation IP 7000 conference phone, and the Polycom VVX business media phone.

This feature requires a license key for activation on all phones except the SoundStation IP 7000 and the Polycom VVX 1500. Using this feature may require purchase of a license key or activation by Polycom channels. For more information, contact your Certified Polycom Reseller.

The individual parties within a conference can be managed. New parties can be added and information about the conference participants can be viewed (for example, names, phone numbers, send/receive status or media flow, receive and transmit codecs, and hold status).

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.

Call Forward

The phone provides a flexible call forwarding feature to forward calls to another destination. Call forwarding can be applied in the following cases:

- Automatically to all calls
- Calls from a specific caller (extension)
- When the phone is busy

- When Do Not Disturb is active
- After an extended period of alerting

The user can elect to manually forward calls while they are in the alerting state to a predefined or manually specified destination. The call forwarding feature works in conjunction with the distinctive incoming call treatment feature (refer to Distinctive Incoming Call Treatment on page 4-6). The user's ability to originate calls is unaffected by all call forwarding options. Each registration has its own forwarding properties.

Server-based call forwarding is active if the feature is enabled on both the phone and the server and the phone is registered. If server-based call forwarding is enabled on any of the phone's registrations, the other registrations are not affected. Server-based call forwarding disables local Call Forward and DND features unless configured otherwise.

Server-based call forwarding will behave the same as per-SIP 2.1 feature with the following exception:

- If server-based call forwarding is enabled, but inactive, and the user selects the call forward soft key, the "moving arrow" icon does not appear on the user's phone (incoming calls are not forwarded).

Note Server-based and local call forwarding are disabled if Shared Call Appearance or Bridged Line Appearance is enabled.

The Diversion field with a SIP header is often used by the call server to inform the phone of a call's history. For example, when a phone has been set to enable call forwarding, the Diversion header allows the receiving phone to indicate who the call was from, and from which phone number it was forwarded. (For more information, refer to Header Support on page B-4.) .

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Enable or disable server-based call forwarding. • Refer to <SIP/> on page A-147. Enable or disable local call forwarding behavior when server-based enabled. • Refer to <SIP/> on page A-147. Enable or disable display of Diversion header and the order in which to display the caller ID and number. • Refer to <SIP/> on page A-147. Set all call diversion settings including a global forward-to contact and individual settings for call forward all, call forward busy, call forward no-answer, and call forward do-not-disturb. • Refer to <divert/> on page A-48.
	Configuration template: **reg-advanced.cfg**	Enable or disable server-based call forwarding as a per-registration feature. • Refer to <reg/>on page A-82.
Local	Web Server (if enabled)	Set all call diversion settings. Navigate to: http://<phoneIPAddress>/reg.htm Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection and the **<Ethernet address>-web.cfg** is removed from the provisioning server.
	Local Phone User Interface	The user can set the call-forward-all setting from the idle display (enable/disable and specify the forward-to contact) as well as divert callers while the call is alerting. Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Local Configuration** menu selection and the **<Ethernet address>-phone.cfg** is removed from the provisioning server.

Directed Call Pick-Up

Calls to another phone can be picked up by dialing the extension of the other phone. This feature depends on support from a SIP server. With many SIP servers, directed call pick-up is implemented using a particular star code sequence. With some SIP servers, specific network signaling is used to implement this feature.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.
	Configuration template: **sip-interop.cfg**	Determine the type of directed call pickup. • Refer to <call/> on page A-21. Determine the type of SIP header to include. • Refer to <volpProt/> on page A-141.

Group Call Pick-Up

Calls to another phone within a pre-defined group can be picked up without dialing the extension of the other phone. This feature depends on support from a SIP server. With many SIP servers, group call pick-up is implemented using a particular star code sequence. With some SIP servers, specific network signaling is used to implement this feature.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.

Call Park/Retrieve

An active call can be parked, and the parked call can be retrieved by another phone. This feature depends on support from a SIP server. With many SIP servers, this feature is implemented using a particular star code sequence. With some SIP servers, specific network signaling is used to implement this feature.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.
	Configuration template: **sip-interop.cfg**	Determine the type of call park and retrieval string. • Refer to <call/> on page A-21.

Last Call Return

The phone allows server-based last call return. This feature depends on support from a SIP server. With many SIP servers, this feature is implemented using a particular star code sequence. With some SIP servers, specific network signaling is used to implement this feature.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.
	Configuration template: **sip-interop.cfg**	Specify the string sent to the server for last-call-return. • Refer to <call/> on page A-21.

Setting Up Advanced Features

This section provides information for making configuration changes for the following advanced features:

- Configurable Feature Keys
- Multiple Line Keys per Registration
- Multiple Call Appearances
- Customizable Fonts
- Instant Messaging
- Multilingual User Interface
- Downloadable Fonts
- Synthesized Call Progress Tones
- Browser and Microbrowser
- Real-Time Transport Protocol Ports
- Network Address Translation
- Corporate Directory
- CMA Directory
- Recording and Playback of Audio Calls
- Digital Picture Frame
- Enhanced Feature Keys

- Configurable Soft Keys
- LCD Power Saving

This section also provides information for making configuration changes for the following advanced call server features:

- Shared Call Appearances
- Bridged Line Appearance
- Busy Lamp Field
- Voice Mail Integration
- Multiple Registrations
- SIP-B Automatic Call Distribution
- Feature Synchronized Automatic Call Distribution
- Server Redundancy
- Presence
- CMA Presence
- Microsoft Live Communications Server 2005 Integration
- Access URL in SIP Message
- Static DNS Cache
- Display of Warnings from SIP Headers
- Quick Setup of Polycom Phones

Configurable Feature Keys

All key functions can be changed from the factory defaults. The scrolling timeout for specific keys can be configured.

Note

Since there is no Redial key on the SoundPoint IP 32x/33x phone, the redial function cannot be remapped.

SoundStation IP 6000 and 7000 keys cannot be remapped to behave as Speed Dial keys.

The rules for remapping of key functions are:

- The phone keys that have removable key caps can be mapped to the following:
  - Any function that is implemented as a removable key cap on any of the phones (Directories, Applications, Conference, Transfer, Redial, Menu, Messages, Do Not Disturb, Call Lists)

  - A speed-dial
  - An enhanced feature key operation
  - Null
- The phone keys without removable key caps cannot be remapped. These include:
  - Any keys on the dial pad
  - Volume control
  - Handsfree, Mute, Headset
  - Hold
  - Navigation Cluster

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration Template: **features.cfg**	Set the key scrolling timeout, key functions, and sub-pointers for each key (usually not necessary). • Refer to <key/> on page A-63.

For more information on the default feature key layouts, refer to Default Feature Key Layouts on page C-11.

Multiple Line Keys per Registration

More than one Line Key can be allocated to a single registration (phone number or line) on SoundPoint IP and Polycom VVX 1500 phones. The number of Line Keys allocated per registration is configurable.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **reg-advanced.cfg**	Specify the number of line keys to assign per registration. • Refer to <reg/> on page A-82.
Local	Web Server (if enabled)	Specify the number of line keys to assign per registration. Navigate to http://<phoneIPAddress>/reg.htm Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection and the **<Ethernet address>-phone.cfg** is removed from the provisioning server.
	Local Phone User Interface	Specify the number of line keys to assign per registration using the **Line Configuration** menu. Either the Web Server or the provisioning server configuration files or the local phone user interface should be used to configure registrations, not a mixture of these options. When the Line Configuration menu is used, it is assumed that all registrations use the same server.

Multiple Call Appearances

The phone supports multiple concurrent calls. The hold feature can be used to pause activity on one call and switch to another call. The number of concurrent calls per line key is configurable. Each registration can have more than one line key assigned to it (refer to the previous section, Multiple Line Keys per Registration).

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **reg-basic.cfg**	Specify the default number of calls that can be active or on hold per line key. • Refer to <call/> on page A-21.
	Configuration template: **reg-advanced.cfg**	Specify per-registration the number of calls that can be active or on hold per line key assigned to that registration. This will override the default value. • Refer to <reg/> on page A-82.

Local	Web Server (if enabled)	Specify the default number of calls that can be active or on hold per line key and the number of calls per registration that can be active or on hold per line key assigned to that registration. Navigate to http://<phoneIPAddress>/appConf.htm#ls and http://<phoneIPAddress>/reg.htm Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection and the **<Ethernet address>-phone.cfg** is removed from the provisioning server.
	Local Phone User Interface	Specify per-registration the number of calls that can be active or on hold per line key assigned to that registration using the **Line Configuration** menu. Either the Web Server or the provisioning server configuration files or the local phone user interface should be used to configure registrations, not a mixture of these options. When the Line Configuration menu is used, it is assumed that all registrations use the same server.

Customizable Fonts

The phone's user interface can be customized by changing the fonts used on the display and the LED indicator patterns. Pre-existing fonts embedded in the software can be overwritten or new fonts can be downloaded.

Note Customizable fonts are not supported on the Polycom VVX 1500.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration Template: **region.cfg**	Specify fonts to overwrite existing ones or specify new fonts. • Refer to <font/> on page A-61.

Instant Messaging

All phones (except the SoundPoint IP 32x/33x) support sending and receiving instant text messages. The user is alerted to incoming messages visually and audibly. The user can view the messages immediately or when it is convenient. For sending messages, the user can either select a message from a preset list of short messages or an alphanumeric text entry mode allows the typing of custom messages using the dial pad. Message sending can be initiated by replying to an incoming message or by initiating a new dialog. The destination for new dialog messages can be entered manually or selected from the contact directory, the preferred method.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.

Multilingual User Interface

The system administrator or the user can select the language. Support for major western European languages is included and additional languages can be easily added. Support for Asian languages (Chinese, Japanese, and Korean) is also included, but will display only on the higher resolution displays of the SoundPoint IP 450, 550, 560, 650, and 670, the SoundStation IP 5000, 6000, and 7000, and Polycom VVX 1500. A WGL4 character set is displayed by the SoundStation IP 7000. For more information, refer to http://www.microsoft.com/OpenType/otspec/WGL4E.HTM.

For basic character support and extended character support (available on SoundPoint IP 450, 550, 560, 650 and 670 and SoundStation IP platforms), refer to <ml/> on page A-65. (Note that within a Unicode range, some characters may not be supported due to their infrequent usage.)

The SoundPoint IP and SoundStation IP user interface is available in the following languages by default: Simplified Chinese (if displayable), Danish, Dutch, English, French, German, Italian, Japanese (if displayable), Korean (if displayable), Norwegian, Polish, Brazilian Portuguese, Russian, Slovenian, International Spanish, and Swedish.

Note The multilingual feature relies on dictionary files resident on the provisioning server. The dictionary files are downloaded from the provisioning server whenever the language is changed or at boot time when a language other than the internal US English language has been configured. If the dictionary files are inaccessible, the language will revert to the internal language.

Note Currently, the multilingual feature is only available in the Polycom UC Software. The BootROM application is available in English only.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration file: **site.cfg**	Specify the boot-up language and the selection of language choices to be made available to the user. • Refer to <ml/> on page A-65. For instructions on adding new languages, refer to To add new languages to those included with the distribution: on page A-66.
Local	Local Phone User Interface	The user can select the preferred language under the Settings menu. The languages appears in the list in the language itself. For example, German appears in the list as "Deutsch" and Swedish appears as "Svenska". For administrator convenience, the ISO representation of each language is also included in the language selection menu. Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Local Configuration** menu selection and the **<Ethernet address>-phone.cfg** is removed from the provisioning server.

Downloadable Fonts

New fonts can be loaded onto the phone. For guidelines on downloading fonts, refer to <font/> on page A-61.

Note Downloadable fonts are not supported on the SoundStation IP 6000 and 7000 and the Polycom VVX 1500.

Synthesized Call Progress Tones

In order to emulate the familiar and efficient audible call progress feedback generated by the PSTN and traditional PBX equipment, call progress tones are synthesized during the life cycle of a call. These call progress tones are configurable for compatibility with worldwide telephony standards or local preferences. The built-in call progress tones are based on North American standard tones. For other geographies, certain tones may be reconfigured by the administrator using configuration files.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **site.cfg**	Specify the basic tone frequencies, levels, and basic repetitive cadences. • Refer to <chord/> on page A-119. Specify downloaded sampled audio files for advanced call progress tones. • Refer to <saf/> on page A-93.
	Configuration template: **region.cfg**	Specify patterns. • Refer to <pat/> on page A-96.

Browser and Microbrowser

The SoundPoint IP 450, 550, 560, 650, and 670 phones, the SoundStation IP 5000, 6000, and 7000 phones support an XHTML Microbrowser. This can be launched by pressing the **Applications** key or it can be accessed through the **Menu** key by selecting Applications.

Note On some older phones, the **Applications** key is labeled **Services**.

The Polycom VVX 1500 phones running SIP 3.2.2 or later support a full browser. This can be launched by pressing the **App** key or it can accessed through the **Menu** key by selecting **Applications**.

Note If the browser uses over 30MB of memory and either the amount of free memory on the phone is below 6MB or the real time is between 1am to 5am, then the browser will restart. Once the browser has restarted, the last displayed web page is restored.

Two instances of the Microbrowser or Browser may run concurrently:

- An instance with standard interactive user interface
- An instance that does not support user input, but appears in a window on the idle display. (On the VVX 1500 phone, the idle browser allows interactivity to start up the active browser only.)

For more information, refer to the *Web Application Developer's Guide,* which can be found at http://www.polycom.com/voicedocumentation/.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **applications.cfg**	Specify the Application browser home page, a proxy to use, and size limits. • Refer to <mb/> on page A-69. Specify the telephone notification and state polling events to be recorded and location of the push server. • Refer to <apps/> on page A-10.
Local	Web Server (if enabled)	Specify the Applications browser home page and proxy to use. Navigate to http://<phoneIPAddress>/coreConf.htm#mb Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection and the **<Ethernet address>-web.cfg** is removed from the provisioning server.

Real-Time Transport Protocol Ports

The phone is compatible with RFC 1889 - RTP: A Transport Protocol for Real-Time Applications - and the updated RFCs 3550 and 3551. Consistent with RFC 1889, the phone treats all RTP streams as bi-directional from a control perspective and expects that both RTP end points will negotiate the respective destination IP addresses and ports. This allows real-time transport control protocol (RTCP) to operate correctly even with RTP media flowing in only a single direction, or not at all. It also allows greater security: packets from unauthorized sources can be rejected.

The phone can filter incoming RTP packets arriving on a particular port by IP address. Packets arriving from a non-negotiated IP address can be discarded.

The phone can also enforce symmetric port operation for RTP packets: packets arriving with the source port set to other than the negotiated remote sink port can be rejected.

The phone can also fix the destination transport port to a specified value regardless of the negotiated port. This can be useful for communicating through firewalls. When this is enabled, all RTP traffic will be sent to the specified port and will be expected to arrive on that port as well. Incoming packets are sorted by the source IP address and port, allowing multiple RTP streams to be multiplexed.

The RTP port range used by the phone can be specified. Since conferencing and multiple RTP streams are supported, several ports can be used concurrently. Consistent with RFC 1889, the next higher odd port is used to send and receive RTCP.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **site.cfg**	Specify whether to filter incoming RTP packets by IP address, whether to require symmetric port usage or whether to jam the destination port and specify the local RTP port range start. • Refer to <rtp/> on page A-80.
Local	Web Server (if enabled)	Specify whether to filter incoming RTP packets by IP address, whether to require symmetric port usage, whether to jam the destination port and specify the local RTP port range start. Navigate to: http://<phoneIPAddress>/netConf.htm#rt Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.

Network Address Translation

The phone can work with certain types of network address translation (NAT). The phone's signaling and RTP traffic use symmetric ports (the source port in transmitted packets is the same as the associated listening port used to receive packets) and the external IP address and ports used by the NAT on the phone's behalf can be configured on a per-phone basis.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify the external NAT IP address and the ports to be used for signaling and RTP traffic. • Refer to <nat/> on page A-73.
Local	Web Server (if enabled)	Specify the external NAT IP address and the ports to be used for signaling and the RTP traffic. Navigate to: http://<phoneIPAddress>/netConf.htm#na Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection and the **<Ethernet address>-web.cfg** is removed from the provisioning server.

Corporate Directory

Note This feature requires a license key for activation except on the SoundStation IP 7000 and Polycom VVX 1500. Using this feature may require purchase of a license key or activation by Polycom channels. For more information, contact your Certified Polycom Reseller.

The SoundPoint IP, SoundStation IP, and VVX phones can be configured to interface with a corporate directory server that supports the Lightweight Directory Access Protocol (LDAP) version 3. Currently the following LDAP servers are supported:

- Microsoft® Active Directory 2003 SP2
- Sun ONE Directory Server 5.2 p6
- Open LDAP Directory Server 2.4.12
- Microsoft Active Directory Application Mode (ADAM) 1.0 SP1

Both corporate directories that support server-side sorting and those that do not are supported. In the latter case, the sorting is performed on the phone.

Polycom recommends using corporate directories that have server-side sorting.

Polycom recommends that you consult your LDAP Administrator when making any configuration changes for this feature.

The corporate directory can be browsed or searched. Entries retrieved from the LDAP server can be saved to the local contact directory on the phone. Phone calls can be placed based on the phone number contained in the LDAP entry.

The corporate directory interface is read only, so that editing or deleting existing directory entries as well as adding new directory entries from the phone is not be possible. (There is no matching of first and last names in the corporate directory to incoming calls, caller identification display, and in the call lists.)

All attributes are considered to be Unicode text. Validity checking will be performed when a call is placed or the entry is saved to the local contact directory.

The corporate directory LDAP server status can be reviewed through the Status menu (**Status > CD Server Status**).

For detailed examples for all currently supported LDAP directories, refer to "Technical Bulletin 41137: Best Practices When Using Corporate Directory on Polycom Phones" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **features.cfg**	Specify the location of the corporate directory's LDAP server, the LDAP attributes, how often to refresh the local cache from the LDAP server, and other miscellaneous parameters. • Refer to <corp/> on page A-44.

Local	Local Phone User Interface	Enable or disable persistent viewing through the Settings menu (***Settings > Basic > Preferences > Corporate Directory > View Persistency***). Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Local Configuration** menu selection.

This section contains the following information:

- Corporate Directory LDAP Attributes
- Browsing the Corporate Directory

Corporate Directory LDAP Attributes

The entry attributes in the corporate directory are mapped through **features.cfg** configuration file attributes to the LDAP attributes first_name, last_name, phone_number, and others so Polycom UC Software knows how to use them for searching, dialing, or saving to the local contact directory. Multiple attributes of the same type are allowed.

Note The maximum of eight attributes can be configured.

The configuration order dictates how the attributes are displayed and sorted. The first attribute is the primary sort index and the second attribute is the secondary sort index. The other attributes are not used in sorting.

To limit the amount of data displayed in the corporate directory, filtering of the entries can be configured for all attribute types. Filtering can be configured to be retained if the phone reboots.

For more information on LDAP attributes, refer to *RFC 4510 - Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*.

Browsing the Corporate Directory

The Polycom phone will establish a session with the corporate directory and download enough entries to fill its cache:

- when the corporate directory is first accessed
- when the phone boots up if the background synchronization parameter is enabled

The requested entries are based on the configured attributes (see previous section).

If the background synchronization parameter is enabled, a timer is initiated to permit a periodic download from the corporate directory.

Entries are sorted according to the order in which the first two attributes are configured (for example, last name, then first name).

The browse position within the corporate directory as well as the attribute filters are maintained for subsequent corporate directory access can be saved (if so configured).

CMA Directory

Note This functionality will be available in a future patch release.

Note This feature is available on the VVX 1500 phone only and requires provisioning of the phone by a Polycom CMA system. This feature may require a license key for activation on the VVX 1500. Using this feature may require purchase of a license key or activation by Polycom channels. For more information, contact your Certified Polycom Reseller.

The CMA Directory can be searched. Entries retrieved from the LDAP server can be saved to the Buddies list on the phone. Phone calls can be placed based on the phone number contained in the LDAP entry. CMA Contacts can be grouped together on the CMA Server.

All attributes are considered to be Unicode text. Validity checking will be performed when a call is placed or the entry is saved to the Buddies list.

For more information, refer to the *User Guide for the Polycom VVX 1500 Phone* at http://www.polycom.com/support/vvx1500 .

Recording and Playback of Audio Calls

Note This feature requires a license key for activation except for the Polycom VVX 1500. Using this feature may require purchase of a license key or activation by Polycom channels. For more information, contact your Certified Polycom Reseller.

The SoundPoint IP 650 and 670 and the Polycom VVX 1500 phones can be configured to allow recording of audio calls on a supported USB device.

The filenames of the recorded **.wav** files will include a date/time stamp (for example, **20Apr2007_190012.wav** was created on April 20, 2007 at 19:00:12). An indication of the recording time remaining—the space available of the attached USB storage media—appears on the graphic display. The user can browse through all recorded files through the menu shown on the graphic display.

Note Notify your users that they may be required by federal, state, and/or local laws to notify some or all called parties when they are recording.

Playback of recorded files can occur on the phone as well as on other devices, such as a Windows® or Apple® based computer using an application like Windows Media Player® or iTunes®.

The user controls which calls are recorded and played back.

For a list of supported USB devices, refer to "Technical Bulletin 38084: Supported USB Devices for SoundPoint IP 650 and 670 and Polycom VVX 1500 Phones" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.

Digital Picture Frame

Note This feature is only supported on the Polycom VVX 1500.

A slide show of multiple personal images stored on a USB flash drive can be displayed on the VVX 1500 phone during the idle mode. The supported formats include JPEG, BMP, and PNG. The maximum image size is 9999x9999. A maximum of 1000 images can be displayed and these must be stored in a directory of the USB flash drive that you create.

Note Although 9999x9999 images and progressive/multiscan JPEG images are supported, the maximum image size that can be downloaded is restricted by the available memory in the phone.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.
	Configuration template: **reg-advanced.cfg**, **site.cfg**	Specify the feature appears. • Refer to <up/> on page A-120.

Note The digital picture frame can be accessed through the PicFrame:// URL.

Enhanced Feature Keys

Note The Enhanced Feature Key (EFK) feature from SIP 3.0 is compatible with Enhanced Feature Key feature from SIP 3.1 . However, improvements have been made, and Polycom recommends that existing configuration files be reviewed and updated.

Customers replacing legacy telephony PBX or key system would like to get equivalent functionality from their new VoIP telephony system. The enhanced feature key capability is designed to allow system administrators to program the speed-dials and soft keys on their phones to interact with the phone user to implement commonly used functions such as "Call Park" in an intuitive fashion.

This capability applies to the SoundPoint IP 32x/33x, 450, 550, 560, 650, and 670 desktop phones, the SoundStation IP 5000, 6000, and 7000 conference phones, and Polycom VVX 1500 business media phones. The enhanced feature key functionality is implemented using Star Code sequences and SIP messaging.

The enhanced feature key macro language was designed to follow current configuration file standards and to be extensible. It is described in more detail in <efk/> on page A-53.

The particular Star Code sequence and the associated prompts displayed on the SoundPoint IP phone for the enhanced feature are defined by macros. These macros are case sensitive.

The enhanced feature key capability can be used to provide a customized, interactive user interface by mapping functions from speed-dial keys, soft keys and re-mapped hard function keys.

This section provides detailed information on:

- Configuration File Changes
- Useful Tips
- Examples

For more examples including sample configuration files, refer to "Technical Bulletin 42250: Using Enhanced Feature Keys and Configurable Soft Keys on Polycom Phones" at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Configuration File Changes

Note

The configuration file changes and the enhanced feature key definitions can be included together in one configuration file.

A sample configuration for this feature—including the enhanced feature keys definitions shown in the following section, Examples— may be included with the SIP 3.1 release.

Create a new configuration file in order to make configuration changes. For more information on why to create another configuration file, refer to the "Configuration File Management on Polycom Phones" white paper at http://www.polycom.com/global/documents/support/technical/products/voice/white_paper_configuration_file_management_on_soundpoint_ip_phones.pdf .

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58. Add Enhanced Feature Keys. • Refer to <efk/> on page A-53.
	Configuration template: **reg-basic.cfg**	Specify two calls per line key. • Refer to <reg/> on page A-82.
	XML file: **<Ethernet address>-directory.xml**	This file holds the macro names which correspond to the `mname` fields in the configuration file where the enhanced feature keys are defined. Macro names must be embedded into the contact (`cn`) fields with the "!" prefix. You can also add labels in the first name (`fn`) fields. For information on file format, refer to Local Contact Directory File Format on page 4-10.

Useful Tips

The following information should be noted:

- Activation of the enhanced feature key will fail if configured values are invalid except where noted in previous sections.
- All failures are logged at level 4 (minor).
- If two macros have the same name, the first one will be used and the subsequent ones will be ignored.
- "'!" and "^" macro prefixes cannot be mixed in the same macro line.
- A sequence of characters prefixed with "!" are parsed as a macro name. The exception is the speed dial reference, which starts with "!" and contains digits only.
- A sequence of characters prefixed with "^" is the action string.

- The sequence of characters accessed from speed dial keys must be prefixed by either "!" or "^" so it will be processed as an enhanced feature key. All macro references and action strings added to the local directory `contact` field must be prefixed by either "!" or "^".
- Action strings used in soft key definitions do not need to be prefixed by "^". However, the "!" prefix must be used if macros or speed dials are referenced.

  For more information, refer to Configurable Soft Keys on page 4-45.
- A sequence of macro names in the same macro is supported (for example, "!m1!m2").
- A sequence of speed dial references is supported (for example, "!1!2").
- A sequence of macro names and speed dial references is supported (for example, "!m1!2!m2").
- Macro names that appear in the local contact directory must follow the format "!<macro name>" , where <macro name> must match an `<elklist> mname` entry. The maximum macro length is 100 characters.
- A sequence of macros is supported, but cannot be mixed with other action types.
- Action strings that appear in the local contact directory must follow the format "^<action string>". Action strings can reference other macros or speed dial indexes. Protection against recursive macro calls exists (the enhanced feature keys fails once 50 macro substitutions is reached).

Examples

Configuration File Changes

You must make the following changes to the `<feature/>` parameter that is defined in the **features.cfg** configuration file:

```
<feature feature.enhancedFeatureKeys.enabled="1" />
```

Action String Example

The action string "`$Changup$*444*$P1N4$$Tinvite$$Cwaitconnect$$P2N3$$Cpause2$$Tdtmf$$Changup$`" is executed as follows:

1. The user is prompted for 4 digits. For example, "1234".
2. The user is prompted for 3 digits. For example, "567".
3. The user's active call is disconnected.
4. The string "*444*1234" is sent using the INVITE method.
5. Once connected, there is a 2 second pause, and then the string "567" is sent using DTMF dialing on the active call.

6. The active call is disconnected.

Speed Dial Example

Your organization voice mail system is accessible through 7700 and your voice mail password is 2154. You could use a speed dial key to access your voice mail if you entered "7700$Cpause3$2154" as the contact number.

Enhanced Feature Key XML Files

You must ensure that the following XML code exists for the definition of "Call Park":

```
...
<efklist
...
    efk.efklist.2.mname="callpark"
    efk.efklist.2.status="1"
    efk.efklist.2.label="Call Park"
    efk.efklist.2.use.idle="1"
    efk.efklist.2.use.active="1"
    efk.efklist.2.use.alerting="1"
    efk.efklist.2.use.dialtone="1"
    efk.efklist.2.use.proceeding="1"
    efk.efklist.2.use.setup="1"
    efk.efklist.2.type="invite"
    efk.efklist.2.action.string="*68*$P1N10$"
...
/>
<efkprompt
    efk.efkprompt.1.status="1"
    efk.efkprompt.1.label="Enter Number: "
    efk.efkprompt.1.userfeedback="visible"
    efk.efkprompt.1.type="numeric"
...
/>
...
```

Contact Directory Changes

You must make the following contact directory changes for the definition of "Call Park":

```
<directory>
    <item_list>
        <item>
            <fn>Call Park</fn>
            <ct>!callpark</ct>
            <sd>2</sd>
            <rt>4</rt>
            <ad>0</ad>
            <ar>0</ar>
            <bw>0</bw>
```

```
            <bb>0</bb>
        </item>
    </item_list>
</directory>
```

Note To avoid users accidentally deleting the definitions in the contact directory, make the contact directory read only. For more information, refer to <local/> on page A-43.

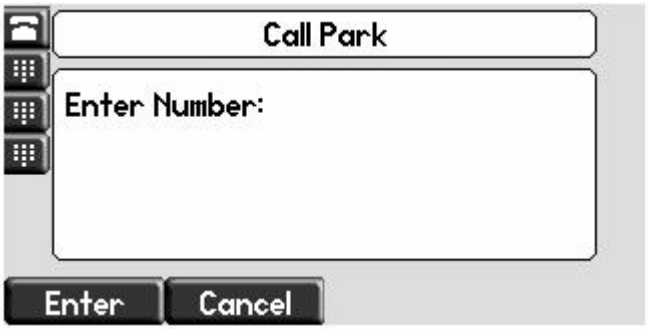
Using Call Park Key

The following figure shows the second speed dial key mapped to Call Park (as well as others mapped to Park Return and Call Pickup).

To use the Call Park key during an active call:

1. When there is an active call on line 2233:
   a. Select the **Call Park** soft key.

      The Call Park screen appears.



   b. Enter the number where you want to park the active call, then select the **Enter** soft key.

      The Call Park * code (*68) is prepended to the number you entered and the call is parked at that location by the call server. The active call is put on hold during this operation.

Configurable Soft Keys

This feature enables phone system administrators to "program" certain frequently used functions onto the soft keys at the bottom of the phone display. This programming can be controlled based on call state. For example a Call Park function can be presented to the user when in an active call state.

If certain hard keys are missing, you may want to create a soft key. For example, if there is no **Do Not Disturb** key on a phone, you could create a **Do Not Disturb** soft key.

New soft keys can be mapped into:

- An Enhanced Feature Key sequence
- A speed dial contact directory entry
- Directly into the Enhanced Feature Key macro
- Directly into a URL
- A chained list of actions

It is possible to disable the display of specific standard keys—the soft keys that are displayed on SoundStation IP, SoundStation IP, and Polycom VVX 1500 phones—to make room for other soft keys that your organization wants displayed. To ensure that the usability of features is not compromised, the disabling of certain soft keys in certain circumstances may be restricted. When a standard soft key is disabled, the space where it was remains empty. The standard keys that can be disabled include:

- **New Call**
- **End Call**
- **Split**
- **Join**
- **Forward**
- **Directories** (or **Dir** as it is called on the SoundPoint IP 32x/33x)

- **Callers** (appears on the SoundPoint IP 32x/33x)
- **MyStatus** and **Buddies**
- **Hold**, **Transfer**, and **Conference**

Note The **Hold**, **Transfer,** and **Conference** are grouped together to avoid usability issues.

Custom soft keys can be added in the following call states:

- Idle—There are no active calls.
- Active—This state starts when a call is connected. It stops when the call stops or changes to another state (like hold or dial tone).
- Alerting (or ringing or incoming proceeding)—The phone is ringing.
- Dial tone—You can hear the dial tone.
- Proceeding (or outgoing proceeding)—This state starts when the phone sends a request to the network. It stops when the call is connected.
- Setup—This state starts when the user starts keying in a phone number. This state ends when the Proceeding state starts.
- Hold—The call is put on hold locally.

Custom soft keys can be configured to precede the standard soft keys that are still displayed. The order of the custom soft keys follows the configuration order. The standard soft keys are shifted to the right and any empty spaces are removed.

If the custom soft keys are configured to not precede the standard soft keys, then the standard soft keys do not move. The order of the custom soft keys—starting from the leftmost empty space—follows the empty spaces. Any extra custom soft keys that are left after all empty spaces are used are appended at the end.

Up to 10 soft keys can be configured. Any additional soft keys are ignored. If more soft keys are defined than fit on the graphic display at one time, a **More** soft key is displayed followed by the remainder of the soft keys that you have defined.

This capability applies to the SoundPoint IP 32x/33x, 450, 550, 560, 650, and 670 desktop phones, the SoundStation IP 5000, 6000, and 7000 conference phones, and Polycom VVX 1500 phones. This capability is linked to the Enhanced Feature Key feature (refer to Enhanced Feature Keys on page 4-40.)

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn the Enhanced Feature keys feature on or off. • Refer to <feature/> on page A-58. Specify the soft key label, in what states it should be displayed, and prompt for input if required. • Refer to <softkey/> on page A-108.

Configuration File Examples

For more examples, refer to "Technical Bulletin 42250: Using Enhanced Feature Keys and Configurable Soft Keys on Polycom Phones" at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

To disable the New Call soft key:

1. Update the **features.cfg** configuration as follows:

```
softkey.feature.newcall = 0
```

2. Reboot the phone.

   The **New Call** soft key is not displayed and the space where it usually appears is empty.

To map a chained list of actions to a soft key:

1. Configure speed dial index 2 in contact directory with a regular phone number. For example, enter "2900" in the contact field.
2. Configure speed dial index 1 in contact directory with "!2" in contact field.
3. Update the **features.cfg** configuration as follows:

```
softkey.1.label = ChainAct
softkey.1.action = $S1$$Tinvite$
softkey.1.use.idle = 1
```

4. Reboot the phone.

   If you press the soft key **ChainAct**, the phone dials number 2900.

To map the Do Not Disturb Enhanced Feature Key sequence to a soft key:

1. Update **features.cfg** as follows:

```
softkey.1.label = DND
softkey.1.action = $FDoNotDisturb$
softkey.1.use.idle = 1
```

2. Reboot the phone.

   A **DND** soft key is displayed on the phone when it is in the idle state.

   When the **DND** soft key is pressed, the Do Not Disturb icon is displayed.

To map a Send to Voice Mail Enhanced Feature Key sequence to a soft key:

Note The exact star code to transfer the active call to Voice Mail depends on your call server.

1. Update **features.cfg** as follows:

```
softkey.2.label = ToVMail
softkey.2.action = ^*55$P1N10$$Tinvite$
softkey.2.use.alerting = 1
```

2. Reboot the phone.

   When another party calls, the **ToVMail** soft key is displayed. When the user presses **ToVMail** soft key, the other party is transferred to voice mail.

LCD Power Saving

Note This feature is only supported on the Polycom VVX 1500 phone.

This feature applies during configured non-working hours and when the phone is idle. Working hours are defined in the configuration files and users can change the default values through the phone's menu to accommodate their individual schedules. The Polycom VVX 1500 phone enters power-saving mode after it has been idle for a certain period of time and its camera doesn't detect motion. The phone's ability to detect the users' presence is biased for easy detection during office hours and for difficult detection during off hours.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **site.cfg**	Turn this feature on or off and configure how it works. • Refer to <powerSaving/> on page A-76.

Shared Call Appearances

Calls and lines on multiple phones can be logically related to each other. A call that is active on one phone will be presented visually to phones that share that call appearance. Mutual exclusion features emulate traditional PBX or key

system privacy for shared calls. Incoming calls can be presented to multiple phones simultaneously. Users at the different locations have the ability to interrupt remote active calls.

This feature is dependent on support from a SIP server that binds the appearances together logically and looks after the necessary state notifications and performs an access control function. For more information, refer to Shared Call Appearance Signaling on page B-10.

Note Shared call appearances and bridged line appearances are two different signaling methods of implementing a feature whereby more than one phone can share the same line or registration. These implementations are dependent on the SIP server. The methods are mutually exclusive and you should confirm with the call server vendor which (if any) method is supported.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify whether diversion should be disabled on shared lines. • Refer to <shared/> on page A-26. Specify line-seize subscription period. • Refer to <server/> on page A-142. Specify standard or non-standard behavior for processing line-seize subscription for mutual exclusion feature. • Refer to <specialEvent/> on page A-156. Specify per-registration line type (private or shared), barge-in capabilities, and line-seize subscription period if using per-registration servers. A shared line will subscribe to a server providing call state information. • Refer to <reg/> on page A-82. Specify per-registration whether diversion should be disabled on shared lines. • Refer to <divert/> on page A-48.

Local	Web Server (if enabled)	Specify line-seize subscription period. Navigate to http://<phoneIPAddress>/appConf.htm#se Specify standard or non-standard behavior for processing line-seize subscription for mutual exclusion feature. Navigate to http://<phoneIPAddress>/appConf.htm#ls Specify per-registration line type (private or shared) and line-seize subscription period if using per-registration servers, and whether diversion should be disabled on shared lines. Navigate to http://<phoneIPAddress>/reg.htm Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection and the **<Ethernet address>-phone.cfg** is removed from the provisioning server.
	Local Phone User Interface	Specify per-registration line type (private or shared) using the **Line Configuration** menu. Either the Web Server or the provisioning server configuration files or the local phone user interface should be used to configure registrations, not a mixture of these options. When the Line Configuration menu is used, it is assumed that all registrations use the same server.

Bridged Line Appearance

Calls and lines on multiple phones can be logically related to each other. A call that is active on one phone will be presented visually to phones that share that line. Incoming calls can be presented to multiple phones simultaneously. This feature is dependent on support from a SIP server that binds the appearances together logically and looks after the necessary state notifications and performs an access control function. For more information, refer to Bridged Line Appearance Signaling on page B-10.

Note

Bridged line appearances and shared call appearances are two different signaling methods of implementing a feature whereby more than one phone can share the same line or registration. These implementations are dependent on the SIP server. The methods are mutually exclusive and you should confirm with the call server vendor which (if any) method is supported.

In the configuration files, bridged lines are configured by "shared line" parameters.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify whether diversion should be disabled on shared lines. • Refer to <call/> on page A-21.
	Configuration template: **reg-advanced.cfg**	Specify per-registration line type (private or shared) and the shared line third party name. A shared line will subscribe to a server providing call state information. • Refer to <reg/> on page A-82. Specify per-registration whether diversion should be disabled on shared lines. • Refer to <divert/> on page A-48.
Local	Web Server (if enabled)	Specify per-registration line type (private or shared) and third party name, and whether diversion should be disabled on shared lines. Navigate to http://<phoneIPAddress>/reg.htm Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection and the **<Ethernet address>-phone.cfg** is removed from the provisioning server.
	Local Phone User Interface	Specify per-registration line type (private or shared) and the shared line third party name using the **Line Configuration** menu. Either the Web Server or the provisioning server configuration files or the local phone user interface should be used to configure registrations, not a mixture of these options. When the Line Configuration menu is used, it is assumed that all registrations use the same server.

Busy Lamp Field

Note

This feature is available only on SoundPoint IP 450, 550, 560, 600, 601, 650, and 670 phones. Other SoundPoint IP phone models may be monitored, but cannot be configured to monitor other phones.

Some aspects of this feature are dependent on the SIP server signaling. You should consult your SIP server partner or Polycom Channel partner for information as needed.

The Busy Lamp Field (BLF) feature enhances support for a phone-based attendant console. It allows monitoring the hook status and remote party information of users through the busy lamp fields and displays on an attendant console phone.

In the SIP 3.1 release, the BLF feature was updated for the following:

- Visual and audible indication when a remote line is in an alerting state
- Display of the caller ID of calls on remotely monitored lines

- Single button "Directed Call Pickup" on a remote line

In the SIP 3.2 release, the BLF feature was updated for the following:

- Configurable list of remote parties to a maximum of 47 with configurable line key labels
- The introduction of configurable default key press actions
- The ability to remove spontaneous call appearances from incoming calls on monitored lines

For more information, refer to "Quick Tip 37381: Enhanced BLF"at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Polycom recommends that the BLF not be used in conjunction with the Microsoft Live Communications Server 2005 feature. For more information, refer to Microsoft Live Communications Server 2005 Integration on page 4-61.

Note Use this feature with TCPpreferred transport (refer to <server/> on page A-142). You can also use UDP transport on SoundPoint IP 650 and 670 phones.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify the list SIP URI and index of the registration which will be used to send a SUBSCRIBE to the list SIP URI specified in `attendant.uri`. • Refer to <attendant/> on page A-13. Specify the list of monitored resources. • Refer to <resourceList/> on page A-14 and <behaviors/> on page A-15.

Voice Mail Integration

The phone is compatible with voice mail servers. The subscribe contact and callback mode can be configured per user/registration on the phone. The phone can be configured with a SIP URL to be called automatically by the phone when the user elects to retrieve messages. Voice mail access can be configured to be through a single key press (for example, the **Messages** key on the SoundPoint IP 450, 550, 560, 650, and 670, and the **MSG** key on the Polycom VVX 1500). A message-waiting signal from a voice mail server triggers the message-waiting indicator to flash and the call waiting audio tone is played through the active audio path.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration templates: **reg-advanced.cfg**, **site.cfg**	For one-touch voice mail access, enable the “one-touch voice mail” user preference. • Refer to <up/> on page A-120.
	Configuration templates: **sip-interop.cfg**	For one-touch voice mail access, bypass instant messages to remove the step of selecting between instant messages and voice mail after pressing the **Messages** key on the SoundPoint IP 450, 550, 560, 650, and 670 and the **MSG** key on the Polycom VVX 1500 (Instant messages are still accessible from the Main Menu). On a per-registration basis, specify a subscribe contact for solicited NOTIFY applications, a callback mode (self call-back or another contact), and the contact to call when the user accesses voice mail. • Refer to <msg/> on page A-72.
Local	Web Server (if enabled)	For one-touch voice mail access, enable the “one-touch voice mail” user preference and bypass instant messages to remove the step of selecting between instant messages and voice mail after pressing the **Messages** key on the SoundPoint IP 450, 550, 560, 650, and 670 and the **MSG** key on the Polycom VVX 1500 (Instant messages are still accessible from the Main Menu). Navigate to http://<phoneIPAddress>/coreConf.htm#us On a per-registration basis, specify a subscribe contact for solicited NOTIFY applications, a callback mode (self call-back or another contact) to call when the user accesses voice mail. Navigate to http://<phoneIPAddress>/reg.htm Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.

Multiple Registrations

The SoundPoint IP 32x/33x supports a maximum of two registrations, the SoundPoint IP 450 supports three registrations, the SoundPoint IP 550 and 560 support four, and the SoundPoint IP 650 and 670 and the Polycom VVX 1500 support 6. Up to three SoundPoint IP Expansion Modules can be added to a single host SoundPoint IP 650 and 670 phone increasing the total number of registrations to 34. The SoundStation IP 5000, 6000, and 7000 supports a single registration.

Each registration can be mapped to one or more line keys (a line key can be used for only one registration). The user can select which registration to use for outgoing calls or which to use when initiating new instant message dialogs.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify the local SIP signaling port and an array of SIP servers to register to. For each server specify the registration period and the signaling failure behavior. • Refer to <SIP/> on page A-147 and <server/> on page A-142.
	Configuration templates: **reg-basic.cfg, reg-advanced.cfg**	For up to maximum number of registrations, specify a display name, a SIP address, an optional display label, an authentication user ID and password, the number of line keys to use, and an optional array of registration servers. The authentication user ID and password are optional and for security reasons can be omitted from the configuration files. The local flash parameters will be used instead. The optional array of servers and their associated parameters will override the servers specified in `<server/>` if non-Null. • Refer to <reg/> on page A-82.
Local	Web Server (if enabled)	Specify the local SIP signaling port and an array of SIP servers to register to. Navigate to http://<phoneIPAddress>/appConf.htm#se For up to six registrations (depending on the phone model, in this case the maximum is six even for the IP 650 and 670), specify a display name, a SIP address, an optional display label, an authentication user ID and password, the number of line keys to use, and an optional array of registration servers. The authentication user ID and password are optional and for security reasons can be omitted from the configuration files. The local flash parameters will be used instead. The optional array of servers will override the servers specified in `<server/>` in non-Null. This will also override the servers on the appConf.htm web page. Navigate to http://<phoneIPAddress>/reg.htm Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.
	Local Phone User Interface	Use the **Call Server Configuration** and **Line Configuration** menu to specify the local SIP signaling port, a default SIP server to register to and registration information for up to twelve registrations (depending on the phone model). These configuration menus contains a sub-set of all the parameters available in the configuration files. Either the Web Server or the provisioning server configuration files or the local phone user interface should be used to configure registrations, not a mixture of these options. When the Line Configuration menu is used, it is assumed that all registrations use the same server. Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Local Configuration** menu selection.

SIP-B Automatic Call Distribution

Note For more information on SIP-B and supported features on Polycom phones, contact Polycom Product Management.

The phone allows Automatic Call Distribution (ACD) login and logout. This feature depends on support from a SIP server.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.
	Configuration template: **reg-advanced.cfg**	Enable this feature per registration. • Refer to <reg/> on page A-82.

The phone also supports ACD agent availability. This feature depends on support from a SIP server.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58.
	Configuration template: **reg-advanced.cfg**	Enable this feature per registration. • Refer to <reg/> on page A-82.

Feature Synchronized Automatic Call Distribution

As of SIP 3.1.2, you can use your SoundPoint IP phones in a call center agent/supervisor role on a supported call server.

When this feature is enabled, the phone will indicate the ACD Call Center Agent state as directed by the call server. The call center agent is provided with an entry method to initiate Sign In/Sign Out and other ACD states through soft keys, however, the phone state will only change once the server has acknowledged that the phone can move into that new state—in this way, the ACD state is maintained in synchronization with the call server and any ACD computer-based soft-clients. The SIP signaling used for this implementation is described in the Device Key Synchronization Requirements Document; Release R14 sp2; Document version 1.6. Contact Polycom Product Management for more information.

The Feature Synchronized ACD feature is supported on SoundPoint IP 32x/33x, 450, 550, 560, 650, and 670, and VVX 1500 phones.

Note The Feature Synchronized ACD feature is distinct from the existing SIP-B Automatic Call Distribution functionality, which was added in SIP 1.6 .

For details on how to configure SoundPoint IP, SoundStation IP, and VVX phones for Feature Synchronized ACD, refer to "Technical Bulletin 34787: Using Feature Synchronized Automatic Call Distribution with Polycom SoundPoint IP and Polycom VVX 1500 Phones" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <feature/> on page A-58. Set the registration to be used for Feature Synchronized ACD and the users sign-in state. • Refer to <acd/>on page A-10.
	Configuration template: **sip-interop.cfg**	Enable or disable Feature Synchronized ACD. • Refer to <SIP/> on page A-147.

Server Redundancy

Server redundancy is often required in VoIP deployments to ensure continuity of phone service for events where the call server needs to be taken offline for maintenance, the server fails, or the connection between the phone and the server fails.

Two types of redundancy are possible:

- **Fail-over**: In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/off-line. This mode of operation should be done using DNS mechanisms or "IP Address Moving" from the primary to the back-up server.
- **Fallback**: In this mode, a second less featured call server (router or gateway device) with SIP capability takes over call control to provide basic calling capability, but without some of the richer features offered by the primary call server (for example, shared lines, presence, and Message Waiting Indicator). Polycom phones support configuration of multiple servers per SIP registration for this purpose.

In some cases, a combination of the two may be deployed.

Note Your SIP server provider should be consulted for recommended methods of configuring phones and servers for fail-over configuration.

Warning

Prior to SIP 2.1, the `reg.x.server.y` parameters (refer to <reg/> on page A-82) could be used for fail-over configuration. The older behavior is no longer supported. Customers that are using the `reg.x.server.y`. configuration parameters where y>=2 should take care to ensure that their current deployments are not adversely affected. For example the phone will only support advanced SIP features such as shared lines, missed calls, presence with the primary server (y=1).

For more information, refer to "Technical Bulletin 5844: SIP Server Fallback Enhancements on Polycom Phones" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify global primary and fallback server configuration parameters. • Refer to <volpProt/> on page A-141.
	Configuration template: **reg-advanced.cfg**	Specify per registration primary and fallback server configuration parameters values that override those in `<voIpProt/>`. • Refer to <reg/> on page A-82.

DNS SIP Server Name Resolution

If a DNS name is given for a proxy/registrar address, the IP address(es) associated with that name will be discovered as specified in RFC 3263. If a port is given, the only lookup will be an A record. If no port is given, NAPTR and SRV records will be tried, before falling back on A records if NAPTR and SRV records return no results. If no port is given, and none is found through DNS, 5060 will be used.

Refer to http://www.ietf.org/rfc/rfc3263.txt for an example.

Note

Failure to resolve a DNS name is treated as signaling failure that will cause a failover.

Behavior When the Primary Server Connection Fails

For Outgoing Calls (INVITE Fallback)

When the user initiates a call, the phone will go through the following steps to connect the call:

1. Try to make the call using the working server.
2. If the working server does not respond correctly to the INVITE, then try and make a call using the next server in the list (even if there is no current registration with these servers). This could be the case if the Internet connection has gone down, but the registration to the working server has not yet expired.

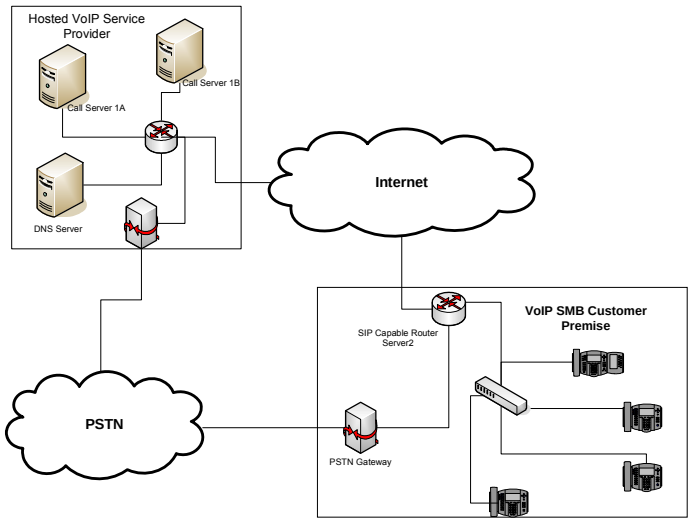
3. If the second server is also unavailable, the phone will try all possible servers (even those not currently registered) until it either succeeds in making a call or exhausts the list at which point the call will fail.

At the start of a call, server availability is determined by SIP signaling failure. SIP signaling failure depends on the SIP protocol being used as described below:

- If TCP is used, then the signaling fails if the connection fails or the Send fails.
- If UDP is used, then the signaling fails if ICMP is detected or if the signal times out. If the signaling has been attempted through all servers in the list and this is the last server, then the signaling fails after the complete UDP timeout defined in RFC 3261. If it is not the last server in the list, the maximum number of retries using the configurable retry timeout is used. For more information, refer to <server/> on page A-142 and <reg/> on page A-82.

Warning

If DNS is used to resolve the address for Servers, the DNS server is unavailable, and the TTL for the DNS records has expired, the phone will attempt to contact the DNS server to resolve the address of all servers in its list *before* initiating a call. These attempts will timeout, but the timeout mechanism can cause long delays (for example, two minutes) before the phone call proceeds "using the working server". To mitigate this issue, long TTLs should be used. It is strongly recommended that an on-site DNS server is deployed as part of the redundancy solution.



Phone Configuration

The phones at the customer site are configured as follows:

- Server 1 (the primary server) will be configured with the address of the service provider call server. The IP address of the server(s) to be used will be provided by the DNS server. For example:

  `reg.1.server.1.address="voipserver.serviceprovider.com"`

- Server 2 (the fallback server) will be configured to the address of the router/gateway that provides the fallback telephony support and is on-site. For example:

  `reg.1.server.2.address=172.23.0.1`

Note It is possible to configure the phone for more than two servers per registration, but you need to exercise caution when doing this to ensure that the phone and network load generated by registration refresh of multiple registrations do not become excessive. This would be of particularly concern if a phone had multiple registrations with multiple servers per registration and it is expected that some of these servers will be unavailable.

Phone Operation for Registration

After the phone has booted up, it will register to all the servers that are configured.

Server 1 is the primary server and supports greater SIP functionality than any of servers. For example, SUBSCRIBE/NOTIFY services (used for features such as shared lines, presence, and BLF) will only be established with Server 1.

Upon registration timer expiry of each server registration, the phone will attempt to re-register. If this is unsuccessful, normal SIP re-registration behavior (typically at intervals of 30 to 60 seconds) will proceed and continue until the registration is successful (for example, when the Internet link is once again operational). While the primary server registration is unavailable, the next highest priority server in the list will serve as the working server. As soon as the primary server registration succeeds, it will return to being the working server.

Note If `reg.x.server.y.register` is set to 0, then phone will not register to that server. However, the INVITE will fail over to that server if all higher priority servers are down.

Recommended Practices for Fallback Deployments

In situations where server redundancy for fall-back purpose is used, the following measures should be taken to optimize the effectiveness of the solution:

1. Deploy an on-site DNS server to avoid long call initiation delays that can result if the DNS server records expire.

2. Do not use OutBoundProxy configurations on the phone if the OutBoundProxy could be unreachable when the fallback occurs. SoundPoint IP phones can only be configured with one OutBoundProxy per registration and all traffic for that registration will be routed through this proxy for all servers attached to that registration. If Server 2 is not accessible through the configured proxy, call signaling with Server 2 will fail.
3. Avoid using too many servers as part of the redundancy configuration as each registration will generate more traffic.
4. Educate users as to the features that will not be available when in "fallback" operating mode.

Presence

The Presence feature allows the phone to monitor the status of other users/devices and allows other users to monitor it. The status of monitored users is displayed visually and is updated in real time in the Buddies list or, for speed dial entries, on the phone's idle display. Users can block others from monitoring their phones and are notified when a change in monitored status occurs. Phone status changes are broadcast automatically to monitoring phones when the user engages in calls or invokes do-not-disturb. The user can also manually specify a state to convey, overriding, and perhaps masking, the automatic behavior.

The presence feature works differently when Microsoft Live Communications Server 2005 is used as the call server. For more information, refer to Microsoft Live Communications Server 2005 Integration on page 4-61.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	XML file: **<Ethernet address>-directory.xml**	The <bw>0</bw> (buddy watching) and <bb>0</bb> (buddy blocking) elements in the ***<Ethernet address>*-directory.xml** file dictate the Presence aspects of directory entries. • Refer to Local Contact Directory on page 4-9.
Local	Local Phone User Interface	The user can edit the directory contents. The *Watch Buddy* and *Block Buddy* fields control the buddy behavior of contacts. Changes will be stored in the phone's flash file system and backed up to the provisioning server copy of ***<Ethernet address>*-directory.xml** if this is configured. When the phone boots, the provisioning server copy of the directory, if present, will overwrite the local copy.

CMA Presence

Note This functionality will be available in a future patch release.

Note This feature is available on the VVX 1500 phone only and requires provisioning of the phone by a Polycom CMA system. This feature may require a license key for activation on the VVX 1500. Using this feature may require purchase of a license key or activation by Polycom channels. For more information, contact your Certified Polycom Reseller.

The CMA Presence feature allows the phone to monitor the status of other CMA Contacts/devices and allows other users to monitor it. The status of monitored users is displayed visually and is updated in real time in the Buddies list or, for speed dial entries, on the phone's idle display. Users are notified when a change in monitored status occurs. Phone status changes are broadcast automatically to monitoring phones when the user engages in calls or invokes do-not-disturb. The user can also manually specify a state to convey, overriding, and perhaps masking, the automatic behavior.

For more information, refer to the *User Guide for the Polycom VVX 1500 Phone* at http://www.polycom.com/support/vvx1500 .

Microsoft Live Communications Server 2005 Integration

Polycom phones can used with Microsoft® Live Communications Server 2005 and Microsoft Office Communicator to help improve business efficiencies and increase productivity and to share ideas and information immediately with business contacts.

For instructions on changing the configuration files, refer to Configuration File Examples on page 4-62.

Note Any contacts added through the Polycom phone's buddy list will appear as a contact in Microsoft Office Communicator and Windows Messenger.

POLYCOM

Polycom recommends that the BLF not be used in conjunction with the Microsoft Live Communications Server 2005 feature. For more information, refer to Busy Lamp Field on page 4-51.

Configuration changes can performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify that support for Microsoft Live Communications Server 2005 is enabled. • Refer to <SIP/> on page A-147.
	Configuration template: **features.cfg**	Specify the line/registration number used to send SUBSCRIBE for presence. • Refer to <pres/> on page A-78. Turn the presence and messaging features on or off. • Refer to <feature/> on page A-58. Specify the line/registration number which has roaming buddies support enabled. • Refer to <roaming_buddies/> on page A-92. Specify the line/registration number which has roaming privacy support enabled. • Refer to <roaming_privacy/> on page A-93.
	Configuration template: **reg-advanced.cfg**	Specify the number of line keys to assign per registration. • Refer to <reg/> on page A-82.

Configuration File Examples

Polycom phones can be deployed in two basic methods. In the first method, Microsoft Live Communications Server 2005 serves as the call server and the phones have a single registration. In the second method, the phone has a primary registration to call server—that is not Microsoft Live Communications Server (LCS)—and a secondary registration to LCS for presence purposes.

To set up a single registration with Microsoft Live Communications Server 2005 as the call server:

1. Create a new configuration file as follows:
   a. Open an XML editor.
   b. Enable the `presence` feature by adding:

      ```
      feature.presence.enabled="1"
      ```

   c. Enable the `messaging` feature by adding:

      ```
      feature.messaging.enabled="1"
      ```

   d. Set the `voIpProt.server.x.transport` attribute to TCPpreferred or TLS by adding one of the following:

      ```
      voIpProt.server.x.transport="TCPpreferred"
      voIpProt.server.x.transport="TLS"
      ```

      Your selection depends on your LCS configuration.

e Set the `voIpProt.server.x.address` to the LCS address. For example:

`voIpProt.server.1.address="lcs2005.local"`

f Enable Microsoft Live Communications Server by adding:

`voIpProt.SIP.lcs="1"`

g (Optional) If SIP forking is desired, set `voIpProt.SIP.ms-forking` to 1.

Refer to <SIP/> on page A-147.

h Set the `reg.1.address` to the LCS address. For example:

`reg.1.address="7778"`

i Set the `reg.1.server.y.address` to the LCS server name. For example:

`reg.1.server.1.address="lcsServer.company.com"`

j (Optional) Set the `reg.1.server.y.transport` attribute to TCPpreferred or TLS. See step **d)**.

k Set `reg.1.auth.userId` to the phone's LCS username. For example:

`reg.1.auth.userId="jbloggs"`

l Set `reg.1.auth.password` to the LCS password. For example:

`reg.1.auth.password="Password2"`

m Set the `roaming_buddies.reg` to the appropriate line number: For example:

`roaming_buddies.reg="1"`

Refer to <roaming_buddies/> on page A-92.

n Set the `roaming_privacy.reg` to the appropriate line number. For example:

`roaming_privacy.reg="1"`

Refer to <roaming_privacy/> on page A-93.

o Save the new configuration file.

p Add this new configuration file to the **000000000000.cfg** or **<MACaddress>.cfg** file and reboot the appropriate phones.

To set up a dual registration with Microsoft Live Communications Server 2005 as the presence server:

1. Create a new configuration file as follows:

a Open an XML editor.

b (Optional) Enable the `presence` feature by adding:

```
feature.presence.enabled="1"
```

c (Optional) Enable the `messaging` feature by adding:

```
feature.messaging.enabled="1"
```

d (Optional) If SIP forking is desired, set `voIpProt.SIP.ms-forking` to 1.

Refer to <SIP/> on page A-147.

e Select a registration to be used for the Microsoft Live Communications Server 2005. Typically, this would be x=2.

f Set the `reg.x.address` to the LCS address. For example:

```
reg.2.address="7778"
```

g Set the `reg.x.server.y.address` to the LCS server name. For example:

```
reg.2.server.1.address="lcsServer.company.com"
```

h (Optional) Set the `reg.2.server.y.transport` attribute to TCPpreferred or TLS. See step **d)** in the previous section.

i Set `reg.x.auth.userId` to the phone's LCS username. For example:

```
reg.2.auth.userId="jbloggs"
```

j Set `reg.x.auth.password` to the LCS password. For example:

```
reg.2.auth.password="Password2"
```

k Set the `roaming_buddies.reg` to the number corresponding to the LCS registration. For example:

```
roaming_buddies.reg=2
```

Refer to <roaming_buddies/> on page A-92.

l Set the `roaming_privacy.reg` element to the number corresponding to the LCS registration. For example:

```
roaming_privacy.reg=2
```

Refer to <roaming_privacy/> on page A-93.

m Save the new configuration file.

n Add this new configuration file to the **000000000000.cfg** or **<MACaddress>.cfg** file and reboot the appropriate phones.

Access URL in SIP Message

Introduced in SIP 2.2, this feature that allows information contained in incoming SIP signaling to refer to XHTML web content that can be rendered by the SoundPoint IP and SoundStation IP phone's Microbrowser and the VVX 1500 phone's Browser.

Supporting this feature allows use of the phone's display to provide information before someone takes a call and while they are on a call (for example, a SIP re-INVITE). The information accessible at the URL can be anything that you want to have displayed.

Configuration changes can performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn this feature on or off. • Refer to <mb/> on page A-69.

This section provides detailed information on:

- Web Content Examples
- User Interface
- Signaling Changes

Web Content Examples

This feature can be used in the following circumstances:

- Call Center—Customer information

  The URL provided allows the phone to access information about a customer and display it before the agent takes the call.

- Call Center—Scripts for different call center groups

  The phone can access a script of questions for an agent to ask a caller when a call comes in. The script can be different for each agent group.

- Restaurant menu on a hotel phone

  A guest dials a number for the restaurant and a voice indicates that the menu is now available for viewing on the phone.

User Interface

There are three user interface aspects to this feature:

- Web content status indication
- Web content retrieval (spontaneous and on-demand)
- Settings menu item to control active versus passive behavior

Web Content Status Indication

When valid web content (validity is determined through a SIP header parameter) is available for a SIP call, it is indicated by an icon that appears after the call appearance status text, regardless of the call state. In the examples

shown below, a lightning bolt symbol is used to indicate that web content is available for the displayed call appearance and the user is encouraged to press the **Select** key to retrieve and display the content through the Microbrowser.

SoundPoint IP 330 Graphic Display

SoundPoint IP 550 Graphic Display

Web Content Retrieval

Web content is retrieved either spontaneously (active mode) or at the request of the user (passive mode).

- **Active Mode.** Two methods can be used to achieve spontaneous web content retrieval: static configuration parameters or parameters received as part of the SIP signaling. If parameters received in the SIP signaling conflict with the static configuration, the parameters in the SIP signaling will take precedence.

  If the phone is configured to spontaneously retrieve web content, the phone will launch the interactive Microbrowser and have it fetch the appropriate URL upon arrival of the appropriate SIP signaling, subject to some conditions described below.

  Since new web content URLs can be received at any time—as the first URL for a call or a replacement URL—rules are needed to match displayed web content with automatic phone behavior, which are valid actions from within the Microbrowser context.

  Spontaneous web content will only be retrieved and displayed for a call if that call occupies, or will occupy, the UI focus at the time of the event.

- **Passive Mode.** Web content can also be retrieved when the user chooses to do so. The fact that web content is available for viewing is shown through the call appearance-based web content icon described in Web

Content Status Indication on page 4-65. The Select key can be used to fetch the associated web content for the call that is in focus. If the web content has expired, the icon will be removed and the Select key will perform no function.

Passive mode is recommended for applications where the Microbrowser is used for other applications. In the SIP 2.2 feature, interactive microbrowser sessions will be interrupted by the arrival of active-mode web content URLs, which may cause annoyance, although the Back navigation function will work in this context.

Settings Menu

If enabled, a new SIP web content entry is added to the **Setting > Basic > Preferences** menu to allow the user to change the current content retrieval mode. Two options are provided: passive mode and active mode.

Signaling Changes

A new SIP header must be used to report web content associated with SIP phone calls (the SSAWC header follow the BNF for the standard SIP header Alert-Info):

```
Alert-Info = "Alert-Info" HCOLON alert-param *(COMMA alert-param)
alert-param = LAQUOT absoluteURI RAQUOT *( SEMI generic-param )
```

The web content must be located with an absolute URI, which begins with the scheme identifier. Currently only the HTTP scheme is supported.

So an example header might look like:

```
Access-URL: <http://server.polycom.com/content23456.xhtml>
```

This header may be placed in SIP requests and responses, as appropriate so long as the messages are part of an INVITE-initiated dialog and the phone can associate them with an existing phone call.

This feature also requires the definition of two optional parameters:

- An *expires* parameter is defined to indicate the lifespan of the URL itself, or, assuming that the URL is permanent, the time span for which the content is expected to have relevance to the call with which it is associated. If the parameter is absent or invalid, this will be interpreted to mean that the content or the URL itself will be persistent in nature. A value, if it is present, will indicate the lifespan of the content in seconds (zero has special significance—see example below). When the lifespan expires, the phone will remove both the indication of the URL and the ability of the user to retrieve it.

For example:

```
Access-URL:
<http://server.polycom.com/content23456.xhtml>;expires=60
```

If the server wishes to invalidate a previous URL, it can send a new header (through UPDATE) with expires=0. The *expires* parameter is ignored when determining whether to spontaneously retrieve the web content unless expires=0.

- A *mode* parameter is defined to indicate whether the web content should be displayed spontaneously or retrieved on-demand. Two values are allowed: active and passive. If the parameter is absent or invalid, this will be interpreted the same as passive, meaning that the web content will be retrievable on-demand but will not be spontaneously displayed. If the value is set to active, the web content will be spontaneously displayed, subject to the rules discussed under **Active Mode** in Web Content Retrieval on page 4-66.

  For example:

```
Access-URL:
<http://server.polycom.com/content23456.xhtml>;expires=60;mode
=passive
```

  In this case, the phone will indicate in the call appearance user interface that web content is available for a period of 60 seconds and will retrieve the web content at the request of the user for a period of up to 60 seconds but the phone will not spontaneously switch to the microbrowser application and download the content.

Static DNS Cache

Starting with SIP 2.1.0, failover redundancy can only be utilized when the configured IP server hostname resolves (through SRV or A record) to multiple IP addresses. Unfortunately, some customer's are unable to configure the DNS to take advantage of failover redundancy.

The solution in SIP 3.1 is to provide the ability to statically configure a set of DNS NAPTR SRV and/or A records into the phone.

When a phone is configured with a DNS server, it will behave as follows by default:

- An initial attempt to resolve a hostname that is within the static DNS cache, for example to register with its SIP registrar, results in a query to the DNS.
- If the initial DNS query returns no results for the hostname or cannot be contacted, then the values in the static cache are used for their configured time interval.

- After the configured time interval has elapsed, a resolution attempt of the hostname will again result in a query to the DNS.
- If a DNS query for a hostname that is in the static cache returns a result, the values from the DNS are used and the statically cached values are ignored.

When a phone is not configured with a DNS server, it will behave as follows

- An attempt to resolve a hostname that is within the static DNS cache will always return the results from the static cache.

Support for negative DNS caching as described in RFC 2308 is also provided to allow faster failover when prior DNS queries have returned no results from the DNS server. For more information, go to http://tools.ietf.org/html/rfc2308 .

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg (site.cfg?)**	Specify DNS NAPTR, SRV, and A records for use when the phone is not configured to use a DNS server. • Refer to <dns/> on page A-51.

Configuration File Examples

Polycom recommends that you create another file with your organization's modifications. If you must change any Polycom templates, back them up first.

For more information, refer to the "Configuration File Management on Polycom Phones" white paper at http://www.polycom.com/global/documents/support/technical/products/voice/white_paper_configuration_file_management_on_soundpoint_ip_phones.pdf .

Example 1

This example shows how to configure static DNS cache using A records IP addresses in SIP server address fields.

When the static DNS cache is not used, the **sip-interop.cfg** configuration would look as follows:

```
reg.1.address="1001"
reg.1.server.1.address="172.23.0.140"
reg.1.server.1.port="5075"
reg.1.server.1.transport="UDPOnly"
reg.1.server.2.address="172.23.0.150"
reg.1.server.2.port="5075"
reg.1.server.2.transport="UDPOnly"
```

When the static DNS cache is used, the **sip-interop.cfg** configuration would look as follows:

```
reg.1.address="1001"
reg.1.server.1.address="sipserver.example.com"
reg.1.server.1.port="5075"
reg.1.server.1.transport="UDPOnly"
reg.1.server.2.address=""
reg.1.server.2.port=""
reg.1.server.2.transport=""

dns.cache.A.1.name="sipserver.example.com"
dns.cache.A.1.ttl="3600"
dns.cache.A.1.address="172.23.0.140"
dns.cache.A.2.name="sipserver.example.com"
dns.cache.A.2.ttl="3600"
dns.cache.A.2.address="172.23.0.150"
```

Note Above addresses are presented to Polycom UC Software in order, for example, `dns.cache.A.1`, `dns.cache.A.2`, and so on.

Example 2

This example shows how to configure static DNS cache where your DNS provides A records for `server.X.address` but not SRV. In this case, the static DNS cache on the phone provides SRV records. For more information, go to http://tools.ietf.org/html/rfc3263 .

When the static DNS cache is not used, the **sip-interop.cfg** configuration would look as follows:

```
reg.1.address="1002@sipserver.example.com"
reg.1.server.1.address="primary.sipserver.example.com"
reg.1.server.1.port="5075"
reg.1.server.1.transport="UDPOnly"
reg.1.server.2.address="secondary.sipserver.example.com"
reg.1.server.2.port="5075"
reg.1.server.2.transport="UDPOnly"
```

When the static DNS cache is used, the **sip-interop.cfg** configuration would look as follows:

```
reg.1.address="1002"
reg.1.server.1.address="sipserver.example.com"
reg.1.server.1.port=""
reg.1.server.1.transport="UDPOnly"
reg.1.server.2.address=""
reg.1.server.2.port=""
reg.1.server.2.transport=""

dns.cache.SRV.1.name="_sip._udp.sipserver.example.com "
dns.cache.SRV.1.ttl= "3600"
dns.cache.SRV.1.priority="1"
dns.cache.SRV.1.weight="1"
```

```
dns.cache.SRV.1.port="5075"
dns.cache.SRV.1.target="primary.sipserver.example.com"

dns.cache.SRV.2.name="_sip._udp.sipserver.example.com "
dns.cache.SRV.2.ttl= "3600"
dns.cache.SRV.2.priority="2"
dns.cache.SRV.2.weight="1"
dns.cache.SRV.2.port="5075"
dns.cache.SRV.2.target="secondary.sipserver.example.com
```

Note The `reg.1.server.1.port` and `reg.1.server.2.port` values in this example are set to null to force SRV lookups.

Example 3

This example shows how to configure static DNS cache where your DNS provides NAPTR and SRV records for `server.X.address` .

When the static DNS cache is not used, the **sip-interop.cfg** configuration would look as follows:

```
reg.1.address="1002@sipserver.example.com
reg.1.server.1.address="172.23.0.140"
reg.1.server.1.port="5075"
reg.1.server.1.transport="UDPOnly"
reg.1.server.2.address="172.23.0.150"
reg.1.server.2.port="5075"
reg.1.server.2.transport="UDPOnly"
```

When the static DNS cache is used, the **sip-interop.cfg** configuration would look as follows:

```
reg.1.address="1002"
reg.1.server.1.address="sipserver.example.com"
reg.1.server.1.port=""
reg.1.server.1.transport=""
reg.1.server.2.address=""
reg.1.server.2.port=""
reg.1.server.2.transport=""

dns.cache.NAPTR.1.name="sipserver.example.com"
dns.cache.NAPTR.1.ttl= "3600"
dns.cache.NAPTR.1.order="1"
dns.cache.NAPTR.1.preference="1"
dns.cache.NAPTR.1.flag="s"
dns.cache.NAPTR.1.service=" SIP+D2U"
dns.cache.NAPTR.1.regexp=""
dns.cache.NAPTR.1.replacement="_sip._udp.sipserver.example.com"

dns.cache.SRV.1.name="_sip._udp.sipserver.example.com "
dns.cache.SRV.1.ttl= "3600"
```

```
dns.cache.SRV.1.priority="1"
dns.cache.SRV.1.weight="1"
dns.cache.SRV.1.port="5075"
dns.cache.SRV.1.target="primary.sipserver.example.com"

dns.cache.SRV.2.name="_sip._udp.sipserver.example.com "
dns.cache.SRV.2.ttl= "3600"
dns.cache.SRV.2.priority="2"
dns.cache.SRV.2.weight="1"
dns.cache.SRV.2.port="5075"
dns.cache.SRV.2.target="secondary.sipserver.example.com

dns.cache.A.1.name="primary.sipserver.example.com"
dns.cache.A.1.ttl="3600"
dns.cache.A.1.address="172.23.0.140"

dns.cache.A.2.name="secondary.sipserver.example.com"
dns.cache.A.2.ttl="3600"
dns.cache.A.2.address="172.23.0.150"
```

Note The `reg.1.server.1.port`, `reg.1.server.2.port`, `reg.1.server.1.transport`, and `reg.1.server.2.transport` values in this example are set to null to force NAPTR lookups.

Display of Warnings from SIP Headers

The Warning Field from a SIP header may be used to cause the phone to display a three second "pop-up" to the user. For example, this feature can be used to inform the user of information such as the reason that a call transfer action failed (bad extension entered, for example). (For more information, refer to Header Support on page B-4.)

These messages are displayed in any language supported by the phone for three seconds unless overridden by another message or action.

For example, if a user parks a call, the following message appears on their phone:

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Turn this feature on or off and specify which warnings are displayable. • Refer to <SIP/> on page A-147.

Quick Setup of Polycom Phones

In the SIP 3.1.2 release, a Quick Setup feature was added to simplify the process of entering the provisioning (boot) server parameters from the phone's user interface. This feature is designed to make it easier for on-site, "out of the box" provisioning of SoundPoint IP, SoundStation IP, and VVX phones.

When enabled, this feature will present a **QSetup** soft key to the user. When the user presses the **QSetup** soft key, a new menu will immediately appear that allows them to configure the necessary parameters for the phone to access the provisioning server for configuration. The **QSetup** soft key may be disabled using a configuration file setting such that it does not appear after it has been successfully configured.

The Quick Setup feature is supported on all SoundPoint IP 32x/33x, 450, 550, 560, 650, and 670 desktop phones, SoundStation IP 5000, 6000 and 7000 conference phones, and Polycom VVX 1500 phones.

System administrators can enable the Quick Setup feature through the use of a new parameter in **site.cfg** configuration file (or through the phone's menu).

For details on how to configure SoundPoint IP, SoundStation IP, and VVX phones for quick setup, refer to "Technical Bulletin 45460: Using Quick Setup with Polycom Phones" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **site.cfg**	Turn this feature on or off . • Refer to <prov/> on page A-78.

Setting Up Audio Features

Proprietary state-of-the-art digital signal processing (DSP) technology is used to provide an excellent audio experience.

This section provides information for making configuration changes for the following audio-related features:

- Customizable Audio Sound Effects

- Context Sensitive Volume Control
- Low-Delay Audio Packet Transmission
- Jitter Buffer and Packet Error Concealment
- Voice Activity Detection
- DTMF Tone Generation
- DTMF Event RTP Payload
- Acoustic Echo Cancellation
- Audio Codecs
- Background Noise Suppression
- Comfort Noise Fill
- Automatic Gain Control
- IP Type-of-Service
- IEEE 802.1p/Q
- Voice Quality Monitoring
- Dynamic Noise Reduction
- Treble/Bass Controls
- Audible Ringer Location

Customizable Audio Sound Effects

Audio sound effects used for incoming call alerting and other indications are customizable. Sound effects can be composed of patterns of synthesized tones or sample audio files. The default sample audio files may be replaced with alternates in **.wav** file format. Supported **.wav** formats include:

- mono G.711 (13-bit dynamic range, 8-khz sample rate)
- mono L16/16000 (16-bit dynamic range, 16-kHz sample rate)
- mono L16/32000 (16-bit dynamic range, 32-kHz sample rate)
- mono L16/48000 (16-bit dynamic range, 48-kHz sample rate)

Note L16/32000 and L16/48000 are only supported on SoundPoint IP 7000 phones.

Note The alternate sampled audio sound effect files must be present on the provisioning server or the Internet for downloading at boot time.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration templates: **site.cfg**, **region.cfg**	Specify patterns used for sound effects and the individual tones or sampled audio files used within them. • Refer to <saf/> on page A-93 or <se/> on page A-95.
Local	Web Server (if enabled)	Specify sampled audio wave files to replace the built-in defaults. Navigate to http://<phoneIPAddress>/coreConf.htm#sa Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.

Context Sensitive Volume Control

The volume of user interface sound effects, such as the ringer, and the receive volume of call audio is adjustable for speakerphone, handset, and headset separately. While transmit levels are fixed according to the TIA/EIA-810-A standard, receive volume is adjustable. For SoundPoint IP and VVX phones, if using the default configuration parameters, the receive handset/headset volume resets to nominal after each call to comply with regulatory requirements. Handsfree volume persists with subsequent calls.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **site.cfg**	Adjust receive and handset/headset volume. • Refer to <volume/> on page A-137.

Low-Delay Audio Packet Transmission

The phone is designed to minimize latency for audio packet transmission.

There are no related configuration changes.

Jitter Buffer and Packet Error Concealment

The phone employs a high-performance jitter buffer and packet error concealment system designed to mitigate packet inter-arrival jitter and out-of-order or lost (lost or excessively delayed by the network) packets. The jitter buffer is adaptive and configurable for different network environments. When packets are lost, a concealment algorithm minimizes the resulting negative audio consequences.

There are no related configuration changes.

Voice Activity Detection

The purpose of voice activity detection (VAD) is to conserve network bandwidth by detecting periods of relative "silence" in the transmit data path and replacing that silence efficiently with special packets that indicate silence is occurring. For those compression algorithms without an inherent VAD function, such as G.711, the phone is compatible with the comprehensive codec-independent comfort noise transmission algorithm specified in RFC 3389. This algorithm is derived from G.711 Appendix II, which defines a comfort noise (CN) payload format (or bit-stream) for G.711 use in packet-based, multimedia communication systems. The phone generates CN packets (also known as Silence Insertion Descriptor (SID) frames) and also decodes CN packets, efficiently regenerating a facsimile of the background noise at the remote end.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **site.cfg**	Enable or disable VAD and set the detection threshold. • Refer to <vad/> on page A-138.

DTMF Tone Generation

The phone generates dual tone multi-frequency (DTMF) tones in response to user dialing on the dial pad. These tones are transmitted in the real-time transport protocol (RTP) streams of connected calls. The phone can encode the DTMF tones using the active voice codec or using RFC 2833 compatible encoding. The coding format decision is based on the capabilities of the remote end point.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Set the DTMF tone levels, autodialing on and off times, and other parameters. • Refer to <DTMF/> on page A-118.

DTMF Event RTP Payload

The phone is compatible with RFC 2833 - *RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals*. RFC 2833 describes a standard RTP-compatible technique for conveying DTMF dialing and other telephony events over an RTP media stream. The phone generates RFC 2833 (DTMF only) events but does not regenerate, nor otherwise use, DTMF events received from the remote end of the call.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Enable or disable RFC 2833 support in SDP offers and specify the payload value to use in SDP offers. • Refer to <DTMF/> on page A-118.

Acoustic Echo Cancellation

Note Do not make changes to acoustic echo cancellation parameters without prior consultation with Polycom Customer Support.

The phone employs advanced acoustic echo cancellation (AEC) for hands-free operation. Both linear and non-linear techniques are employed to aggressively reduce echo yet provide for natural full-duplex communication patterns.

When using the handset on any SoundPoint IP phones, AEC is not normally required. In certain situations, where echo is experienced by the far-end party, when the user is on the handset, AEC may be enabled to reduce/avoid this echo. To achieve this, make the following changes in the **techsupport.cfg** configuration template (default settings for these parameters are disabled):

```
voice.aec.hs.enable = 1
voice.ns.hs.enable = 1
voice.ns.hs.signalAttn = -6
voice.ns.hs.silenceAttn = -9
```

For more information, refer to <aec/> on page D-12.

Audio Codecs

The following table shows which audio codecs are support by each of the SoundPoint IP, SoundStation IP, and Polycom VVX phones:

Phone	Supported Audio Codecs	Priority
SoundPoint IP 320, 321, 330, and 331	• G.711μ-law	• 6
	• G.711a-law	• 7
	• G.729AB	• 8
	• Lin16 (16.16ksps	• 0
	• iLBC (13.33kbps, 15.2kbps)	• 0, 0

Phone	Supported Audio Codecs	Priority
SoundPoint IP 335, 450, 550, 560, 650, and 670	• G.711μ-law	• 6
	• G.711a-law	• 7
	• G.722	• 4
	• G.729AB	• 8
	• Lin16 (16.16ksps)	• 0
	• iLBC (13.33kbps, 15.2kbps)	• 0, 0
SoundStation IP 5000	• G.711μ-law	• 6
	• G.711a-law	• 7
	• G.722	• 4
	• G.729AB	• 8
	• Lin16 (16.16ksps)	• 0
	• iLBC (13.33kbps, 15.2kbps) ***Note**: Only one of iLBC or G.729AB is supported.*	• 0, 0
SoundStation IP 6000	• G.711μ-law	• 6
	• G.711a-law	• 7
	• G.722	• 4
	• G.722.1 (16kbps, 24kbps, 32kbps)	• 0, 0, 5
	• G.722.1C (24kbps, 32kbps, 48kbps)	• 0, 0, 2
	• G.729AB	• 8
	• Siren14 (24kbps, 32kbps, 48kbps)	• 0, 0, 3
	• Lin16 (16.16ksps)	• 0
	• iLBC (13.33kbps, 15.2kbps)	• 0, 0

Phone	Supported Audio Codecs	Priority
SoundStation IP 7000	• G.711μ-law	• 6
	• G.711a-law	• 7
	• G.722	• 4
	• G.722.1 (16kbps, 24kbps, 32kbps)	• 0, 0, 5
	• G.722.1C (24kbps, 32kbps, 48kbps)	• 0, 0, 2
	• G.729AB	• 8
	• Lin16 (16.8ksps, 16.16ksps, 16.32ksps, 16.44.1ksps, 16.48ksps)	• 0, 0, 0, 0, 0
	• Siren14 (24kbps, 32kbps, 48kbps)	• 0, 0, 3
	• Siren22 (22.32kbps, 22.48kbps, 22.64kbps)	• 0, 0, 0
	• iLBC (13.33kbps, 15.2kbps)	• 0
Polycom VVX 1500	• G.711μ-law	• 6
	• G.711a-law	• 7
	• G.719 (32kbps, 48kbps, 64kbps)	• 0, 0, 0
	• G.722	• 4
	• G.722.1 (16kbps, 24kbps, 32kbps)	• 0, 0, 5
	• G.722.1C (24kbps, 32kbps, 48kbps)	• 0, 0, 2
	• G.729AB	• 8
	• Lin16 (16.8ksps, 16.16ksps, 16.32ksps, 16.44.1ksps, 16.48ksps)	• 0, 0, 0, 0, 0
	• Siren14 (24kbps, 32kbps, 48kbps)	• 0, 0, 3
	• iLBC (13.33kbps, 15.2kbps)	• 0, 0

The following table summarizes the supported audio codecs:

Algorithm	Ref.	Raw Bit Rate	IP Bit Rate	Sample Rate	Frame Size	Effective audio bandwidth
G.711μ-law	RFC 1890	64 Kbps	80 Kbps	8 Ksps	10ms - 80ms	3.5KHz
G.711a-law	RFC 1890	64 Kbps	80 Kbps	8 Ksps	10ms - 80ms	3.5KHz
G.719	RFC 5404	32 Kbps, 48 Kbps, 64 Kbps	48Kbps 64Kbps 80Kbps	48 kHz	20ms	20kHz
G.722	RFC 1890	64 Kbps	80 Kbps	16 Ksps	10ms - 80ms	7 KHz
G.722.1	RFC 3047	16 Kbps, 24 Kbps, 32 Kbps	32Kbps 40Kbps 48Kbps	16 Ksps	20ms - 80ms	7 KHz
G.722.1C	G7221C	24 Kbps 32 Kbps 48 Kbps	40Kbps 48Kbps 64Kbps	32 Ksps	20ms - 80ms	14 KHz
G.729AB	RFC 1890	8 Kbps	24Kbps	8 Ksps	10ms - 80ms	3.5KHz
SID	RFC 3389	N/A	N/A	N/A	N/A	N/A
Lin16	RFC 1890	128 Kbps 256 Kbps 512 Kbps 705.6 Kbps 768 Kbps	132Kbps 260Kbps 516Kbps 709.6Kbps 772Kbps	8 Ksps 16 Ksps 32 Ksps 44.1 Ksps 48 Ksps	10ms	3.5 KHz 7 KHz 14 KHz 20 KHz 22 KHz
Siren14	SIREN14	24 Kbps 32 Kbps 48 Kbps	40Kbps 48Kbps 64Kbps	32 Ksps	20ms - 80ms	14 KHz
Siren22	SIREN22	32 Kbps 48 Kbps 64 Kbps	48Kbps 64Kbps 80Kbps	48 Ksps	20ms - 80ms	22 KHz
RFC 2833	RFC 2833	N/A	N/A	N/A	N/A	N/A
iLBC	RFC 3951	13.33Kbps 15.2Kbps	31.2Kbps 24Kbps	8 Ksps	30ms - 60ms 20ms - 80ms	3.5KHz

Note The network bandwidth necessary to send the encoded voice is typically 5-10% higher than the encoded bit rate due to packetization overhead. For example, a G.722.1C call at 48kbps consumes about 100kbps of network bandwidth (two-way audio).

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **site.cfg**	Specify codec priority, preferred payload sizes, and jitter buffer tuning parameters. • Refer to <codecPref/> on page A-135.
Local	Web Server (if enabled)	Specify codec priority, preferred payload sizes, and jitter buffer tuning parameters. Navigate to http://<phoneIPAddress>/coreConf.htm#au Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.

Background Noise Suppression

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

There are no related configuration changes.

Comfort Noise Fill

Comfort noise fill is designed to help provide a consistent noise level to the remote user of a hands-free call. Fluctuations in perceived background noise levels are an undesirable side effect of the non-linear component of most AEC systems. This feature uses noise synthesis techniques to smooth out the noise level in the direction toward the remote user, providing a more natural call experience.

There are no related configuration changes.

Automatic Gain Control

Automatic Gain Control (AGC) is applicable to hands-free operation and is used to boost the transmit gain of the local talker in certain circumstances. This increases the effective user-phone radius and helps with the intelligibility of soft-talkers.

There are no related configuration changes.

IP Type-of-Service

The "type of service" field in an IP packet header consists of four type-of-service (TOS) bits and a 3-bit precedence field. Each TOS bit can be set to either 0 or 1. The precedence field can be set to a value from 0 through 7. The type of service can be configured specifically for RTP packets and call control packets, such as SIP signaling packets.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **site.cfg**	Specify protocol-specific IP TOS settings. • Refer to <IP/> on page A-80.
Local	Web Server (if enabled)	Specify protocol-specific IP TOS settings. Navigate to: http://<phoneIPAddress>/netConf.htm#qo Changes are saved to local flash and backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.

IEEE 802.1p/Q

The phone will tag all Ethernet packets it transmits with an 802.1Q VLAN header for one of the following reasons:

- When it has a valid VLAN ID set in its network configuration
- When it is instructed to tag packets through Cisco Discovery Protocol (CDP) running on a connected Ethernet switch
- When a VLAN ID is obtained from DHCP (refer to DHCP Menu on page 3-8)

The 802.1p/Q user_priority field can be set to a value from 0 to 7. The user_priority can be configured specifically for RTP packets and call control packets, such as SIP signaling packets, with default settings configurable for all other packets.

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **site.cfg**	Specify default and protocol-specific 802.1p/Q settings. • Refer to <ethernet/> on page A-79.
Local	Web Server (if enabled)	Specify default and protocol-specific 802.1p/Q settings. Navigate to http://<phoneIPAddress>/netConf.htm#qo Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.
	Local Phone User Interface	Specify whether CDP is to be used or manually set the VLAN ID or configure DHCP VLAN Discovery. Phase 1: BootRom - Navigate to: SETUP menu during auto-boot countdown. Phase 2: Polycom UC Software - Navigate to: ***Menu>Settings>Advanced>Admin Settings>Network Configuration*** • Refer to Setting Up the Network on page 3-2.

Voice Quality Monitoring

Note This feature requires a license key for activation except for the Polycom VVX 1500. Using this feature may require purchase of a license key or activation by Polycom channels. For more information, contact your Certified Polycom Reseller.

The SoundPoint IP phones can be configured to generate various quality metrics for listening and conversational quality. These metrics can be sent between the phones in RTCP XR packets. The metrics can also be sent as SIP PUBLISH messages to a central voice quality report collector. The collection of these metrics is supported on the SoundPoint IP 32x/33x, 450, 550, 560, 650, and 670 phones and the Polycom VVX 1500 phone.

Note Voice Quality Monitoring is not supported on the SoundStation IP 6000 and 7000 conference phones at this time. Only Voice Quality Monitoring of the audio portion is supported on the Polycom VVX 1500 at this time.

The RTCP XR packets are compliant with *RFC 3611 - RTP Control Extended Reports (RTCP XR)*. The packets are sent to a report collector as specified in draft RFC *draft-ietf_sipping_rtcp-summary-02*.

Three types of quality reports can be enabled:

- Alert—Generated when the call quality degrades below a configurable threshold.
- Periodic—Generated during a call at a configurable period.
- Session—Generated at the end of a call.

A wide range of performance metrics are generated. Some are based on current values, such as jitter buffer nominal delay and round trip delay, while others cover the time period from the beginning of the call until the report is sent, such as network packet loss. Some metrics are computed using other metrics as input, such as listening Mean Opinion Score (MOS), conversational MOS, listening R-factor, and conversational R-factor.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Specify the location of the central report collector, how often the reports are generated, and the warning and critical threshold values that will cause generation of alert reports. • Refer to <quality monitoring/> on page A-138.

Dynamic Noise Reduction

Dynamic noise reduction (DNR) provides maximum microphone sensitivity, while automatically reducing background noise— from fans, projectors, heating and air conditioning—for clearer sound and more efficient conferencing.

There are no related configuration changes.

Treble/Bass Controls

The treble and bass controls equalize the tone of the high and low frequency sound from the speakers.

The SoundStation IP 7000 phone's treble and bass controls can be modified by the user (through **Menu > Settings > Basic > Audio > Treble EQ** or **Bass EQ**).

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration templates: **reg-advanced.cfg**, **site.cfg**	Specify the user's preferences for treble and bass. • Refer to <up/> on page A-120.

Audible Ringer Location

As of Polycom UC Software 3.3.0, the user can select where the incoming call ringing plays out (through **Menu > Settings > Basic > Preferences > Audible Ringer**) on all SoundPoint IP and VVX 1500 phones. By default, the ringing is played out on the phone's speaker; however, the user can also select the handset, the headset, or the location of the active call.

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration templates: **reg-advanced.cfg**	Specify the location of the audible ringer. • Refer to <se/> on page A-95.

Setting Up Video Features

The Polycom VVX 1500 phone supports transmission and reception of high quality video images. The video is compatible with RFC 3984 - RTP Payload Format for H.264 Video, RFC 4629 - RTP Payload Format for ITU-T Rec. H.263 Video, and RFC 5168 - XML Schema for Media Control.

This section provides information for making configuration changes for the following video-related features:

- Video Transmission
- Video Codecs
- H.323 Protocol

Video Transmission

By default, at the start of a video call, the VVX 1500 phone transmits an RTP encapsulated video stream with images captured from the local camera. Users can stop and start video transmission by pressing the **Video** key, and then selecting the appropriate soft key.

You can control of the following features of the VVX 1500 phone's camera:

- Flicker avoidance
- Frame rate
- Brightness level
- Saturation level
- Contrast level
- Sharpness level

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **video.cfg**	Turn video transmission off at the near end when calls start and transmit still image if video not available. • Refer to <video/> on page A-125. Specify camera parameters. • Refer to <camera/> on page A-132. Determine how the local camera is displayed. • Refer to <localCameraView/> on page A-133.
Local	Local Phone User Interface	The user can set the individual video settings from the menu through **Settings > Basic > Video > Video Call Settings**, **Video Screen Mode**, and **Local Camera View**. The user can set the individual camera settings from the menu through **Settings > Basic > Video > Camera Settings**.

Video Codecs

The following table summarizes the VVX 1500 phone's video codec support:

Algorithm	MIME Type	Bit Rate	Frame Rate	Frame Size	Effective video bandwidth
H.261	H261/90000	64 kbps to 768 kbps	5 fps to 30 fps	Tx Frame size: CIF, QCIF RX Frame size: CIF, QCIF	Refer to Bit Rate column.
H.263	H263/90000, H263-1998/90000, H263-2000/90000			Tx Frame size:CIF, QCIF Rx Frame size:CIF, QCIF, SQCIF, QVGA, SVGA, SIF	
H.264	H264/90000				

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **video.cfg**	Specify codec priority, payload type and jitter buffer tuning parameters. • Refer to <codecPref/> on page A-127 and <profile/> on page A-127.

H.323 Protocol

Note This feature may require a license key for activation on the VVX 1500. Using this feature may require purchase of a license key or activation by Polycom channels. For more information, contact your Certified Polycom Reseller.

As of SIP 3.2.2, telephony signaling support via the H.323 family of protocols enabling direct communication with H.323 endpoints, gatekeepers, call and media servers, and signaling gateways is supported on the VVX 1500 phone.

SIP and H.323 signaling can be supported at the same time, including bridging both types of calls during multi-party conference calls. Automatic detection of the correct or optimal signaling protocol is available when dialing from the contact or corporate directories. While SIP supports server redundancy and several transport options, only a single configured H.323 gatekeeper address per phone is supported. H.323 gatekeepers are optional, but if available, they must be used. If a gatekeeper is not configured or unavailable, calls can still be made if so configured.

If the H.323 protocol is disabled, there will be no visible evidence in the user interface of the VVX 1500 phone.

Support of the SIP protocol for telephony signaling can be disabled on the VVX 1500 such that all calls would be routed via the H.323 protocol.

This section provides detailed information on:

- Supported Standards
- Supported Polycom Interoperability
- Configuration File Changes
- Useful Tips
- Examples

Supported Standards

The following standards are supported by the implementation of this feature:

Standard	Description
ITU-T Recommendation H.323 (2003)	Packet-based multimedia communications systems
ITU-T Recommendation Q.931 (1998)	ISDN user-network interface layer 3 specification for basic call control
ITU-T Recommendation H.225.0 (2003)	Call signaling protocols and media stream packetization for packet based multimedia communications systems

Standard	Description
ITU-T Recommendation H.245 (5/2003)	Control protocol for multimedia communication
ITU-T Recommendation H.235.0 - H.235.9 (2005)	Security and encryption for H Series (H.323 and other H.245 based) multimedia terminals
ITU-T Recommendation H.350.1 (8/2003)	Directory services architecture for H.323

Supported Polycom Interoperability

Video calls are supported to the following Polycom endpoints/bridges/call servers (or gatekeepers)/media servers:

Make/Model	Protocol	Software Version
Polycom CMA System	H.323	SW 5.0
Polycom HDX® 9000 series	SIP/ISDN/H.323	SW 2.6.0
Polycom HDX® 8000 series	SIP/ISDN/H.323	SW 2.6.0
Polycom HDX® 7000 series	SIP/ISDN/H.323	SW 2.6.0
Polycom HDX® 6000	SIP/ISDN/H.323	SW 2.6.0
Polycom HDX® 4000 series	SIP/ISDN/H.323	SW 2.6.0
Polycom RMX® 2000	H.323	SW 4.0.2.7
Polycom Quality Definition Experience™ (QDX™)	H.323	SW 4.0, 4.0.1
Polycom RMX® 1000	H.323	SW 1.1.1.8787
Polycom RMX® 2000	H.323	SW 5.0.1.24, 6.0
Polycom RSS™	H.323	SW 6.0
Polycom VBP™ 6400-ST series	H.323	SW 9.1.5.1
Polycom VBP™ 5300-ST series	H.323	SW 9.1.5.1
Polycom VBP™ 5300-E series	H.323	SW 9.1.5.1
Polycom VBP™ 4350 series	H.323	SW 9.1.5.1
Polycom VBP™ 200	H.323	SW 9.5.2
Polycom VSX® 8000	SIP/ISDN/H.323	SW 9.0.6
Polycom VSX® 7000s and VSX® 7000e	SIP/ISDN/H.323	SW 9.0.6
Polycom VSX® 6000 and 6000a	SIP/ISDN/H.323	SW 9.0.5.1

Make/Model	Protocol	Software Version
Polycom VSX® 5000	SIP/ISDN/H.323	SW 9.0.5.1
Polycom VSX® 3000	SIP/ISDN/H.323	SW 9.0.5.1
Polycom V700™	SIP/ISDN/H.323	SW 9.0.5.1
Polycom V500™	SIP/ISDN/H.323	SW 9.0.5.1

Note Refer to the *Release Notes* for the latest list of supported Polycom endpoints/bridges/call servers (or gatekeepers)/media servers and any supported third party products. Any issues (and possible workarounds) with any of the above-mentioned products are also documented in the *Release Notes*.

Configuration File Changes

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **reg-advanced.cfg**, **site.cfg**	Specify call routing parameters. • Refer to <up/> on page A-120 and <call/> on page A-21. Specify auto-answer parameters and auto off-hook protocol for dual-protocol lines. • Refer to <call/> on page A-21.
	Configuration template: **sip-interop.cfg**	Specify the registration protocol. • Refer to <reg/> on page A-82.
	Configuration template: **H323.cfg**	Specify H.323 protocol, server, gatekeeper, and DTMF signaling parameters. • Refer to <voIpProt/> on page A-141. Specify the registration protocol. • Refer to <reg/> on page A-82.
	Configuration template: **video.cfg**	Specify the video call rate. • Refer to <video/> on page A-125.
	Configuration template: **site.cfg**	Specify H.323 media encryption parameters. • Refer to <H235/> on page A-106.

Useful Tips

The following information should be noted:

- If the phone has only the H.323 protocol enabled, it cannot be used to answer SIP calls.
- If the phone has only the SIP protocol enabled, it cannot be used to answer H.323 calls.

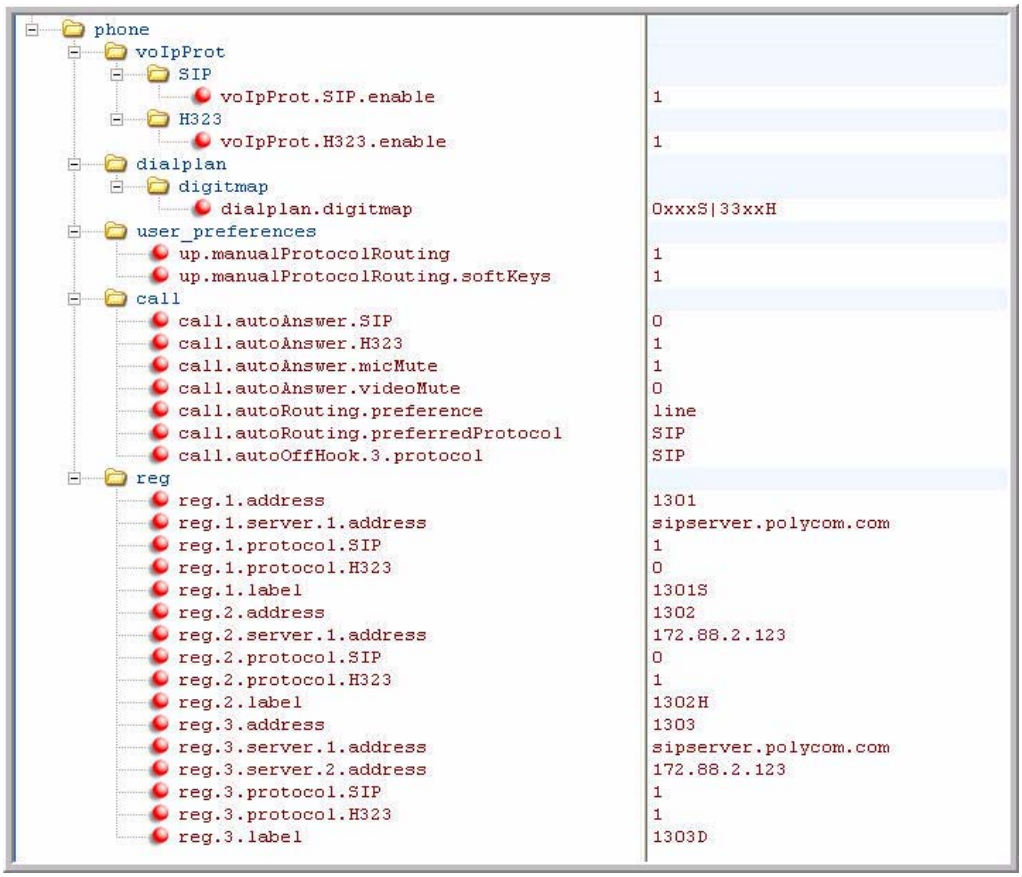
- If both SIP and H.323 protocols are disabled by mistake, the phone will continue to work as a SIP-only phone; however, the phone is not registered (you are able to send and receive SIP URL calls).
- The protocol that is used to place a call is stored in the placed call list of the user's phone.
- The protocol to be used when placing a call from the user's local contact directory is unspecified by default. The user can select SIP or H.323.
- The protocol that is used when placing a call from the user's corporate directory depends on the order of the attributes in the corporate directory. If only SIP_address is defined, then the SIP protocol is used. If only H323_address is defined, then the H.323 protocol is used. If both are defined, then the one that is defined first is used. For example, if `dir.corp.attribute.4.type` is **SIP_address** and `dir.corp.attribute.5.type` is **H323_address**, then the SIP protocol is used.
- By default, the user is presented with protocol routing choices when a call could be placed with more than one protocol from its current context. The user must choose between SIP and H.323 to place a call by pressing the appropriate soft key.
- Calls made using H.323 cannot be forwarded or transferred.
  - The **Transfer** and **Forward** soft keys are not displayed during an H.323 call on a VVX 1500 phone. The **Forward** soft key is not displayed on the idle display of a VVX 1500 phone if the primary line is an H.323 line.
  - If a VVX 1500 user presses the **Transfer** soft key during an H.323 call on a VVX 1500 phone, no action is taken.
  - The auto-divert field in the local contact directory entry is ignored when a call is placed to that contact using H.323.
  - If a conference host ends a three-way conference the call and one of the party is connected by H.323, that party is not transferred to the other party.

Examples

The following example **sip-h323.cfg** configuration file shows the relevant parameters:

- To configure both SIP and H.323 protocols
- To set up a SIP and H.323 dial plan—Numbers with the format "0xxx" are placed on a SIP line and numbers with the format "33xx" are placed on an H.323 line

- To set up manual protocol routing using soft keys—If the protocol to use to place a call cannot be determined, the **Use SIP** and **Use H.323** soft keys appear, and the user must select one for the call to be placed.
- To configure auto-answering on H.323 calls only
- To set the preferred protocol to SIP
- To set to configure one SIP line, one H.323 line, and a dual protocol line—both SIP and H.323 can be used.
- To set the preferred protocol for off-hook calls on the third (dual protocol) line to SIP



Setting Up Security Features

This section provides information for making configuration changes for the following security-related features:

- Local User and Administrator Privilege Levels
- Custom Certificates

- Incoming Signaling Validation
- Configuration File Encryption
- Digital Certificates
- Mutual TLS Authentication
- Secure Real-Time Transport Protocol
- Configurable TLS Cipher Suites
- Locking the Phone
- Support for EAPOL Logoff Message

Local User and Administrator Privilege Levels

Several local settings menus are protected with two privilege levels, user and administrator, each with its own password. The phone will prompt for either the user or administrator password before granting access to the various menu options. When the user password is requested, the administrator password will also work. The web server is protected by the administrator password (refer to Configuring Polycom Phones Locally on page 4-102).

Configuration changes can be performed centrally at the provisioning server or locally:

Central (provisioning server)	Configuration template: **site.cfg**	Specify the minimum lengths for the user and administrator passwords. • Refer to <pwd/><length/> on page A-103.
Local	Web Server (if enabled)	None.
	Local Phone User Interface	The user and administrator passwords can be changed under the Settings menu or through configuration parameters (refer to <device/> on page A-30). Passwords can consist of ASCII characters 32-127 (0x20-0x7F) only. Changes are saved to local flash but are not backed up to ***<Ethernet address>*-phone.cfg** on the provisioning server for security reasons.

Custom Certificates

The phone trusts certificates issued by widely recognized certificate authorities when trying to establish a connection to a provisioning server for application provisioning. Refer to Trusted Certificate Authority List on page C-1.

In addition, custom certificates can be added to the phone. This is done by using the SSL Security menu on the phone to provide the URL of the custom certificate then select an option to use this custom certificate.

Note For more information on using custom certificates, refer to “Technical Bulletin 17877: Using Custom Certificates With Polycom Phones” at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Configuration changes can be performed locally:

Local	Local Phone User Interface	The custom certificate can be specified and the type of certificate to trust can be set under the **Settings** menu.

Incoming Signaling Validation

The three optional levels of security for validating incoming network signaling are:

- Source IP address validation
- Digest authentication
- Source IP address validation and digest authentication

Configuration changes can be performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify the type of validation to perform on a request-by-request basis, appropriate to specific event types in some cases. • Refer to <requestValidation/> on page A-155.

Configuration File Encryption

Configuration files (excluding the master configuration file), contact directories, and configuration override files can all be encrypted.

Note Encrypted configuration files can be decrypted on the SoundPoint IP 32x, 33x, 450, 550, 560, 650, and 670, the SoundStation IP 5000, 6000, and 7000, and the Polycom VVX 1500 phones.

The master configuration file cannot be encrypted on the provisioning server. This file is downloaded by the BootROM that does not recognize encrypted files. For more information, refer to Master Configuration Files on page A-2.

For more information on encrypting configuration files including determining whether an encrypted file is the same as an unencrypted file and using the SDK to facilitate key generation, refer to Encrypting Configuration Files on page C-4.

Configuration changes can be performed centrally at the provisioning server:

Central provisioning server)	Configuration template: **site.cfg**	Specify the phone-specific contact directory and the phone-specific configuration override file. • Refer to <encryption/> on page A-102.
	Configuration template: **device.cfg**	Change the encryption key. • Refer to <device/> on page A-30.

Digital Certificates

Starting in May 2009, Polycom is installing a digital certificate on certain SoundPoint IP phone models at the manufacturing facility. Over time, other SoundPoint IP phone models as well as all SoundStation IP and VVX phone models will have a digital certificate. Refer to "Technical Bulletin 37148: Device Certificates on Polycom Phones"at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

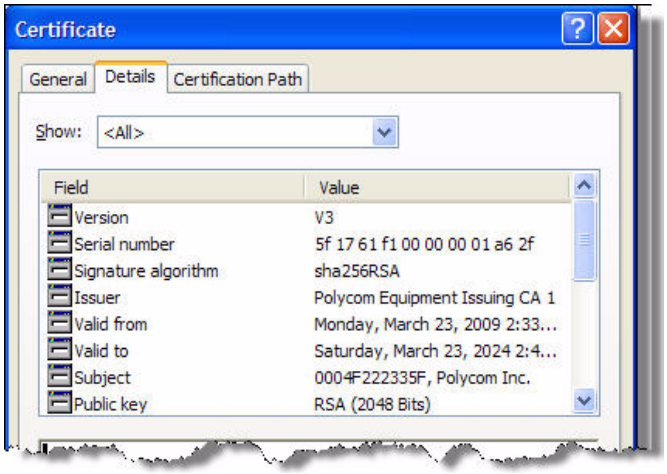
This X.509 digital certificate is 'signed' by the Polycom Root CA and may be used for a server to authenticate the phone when initiating Transport Layer Security (TLS) based communications such as those used for HTTPS provisioning and TLS SIP signaling encryption. The Polycom Root CA can be downloaded from http://pki.polycom.com/pki . The X.509 digital certificates are set to expire on March 9, 2044.

An X.509 digital certificate is a digitally signed statement. The X.509 standard defines what information can go into a certificate. All X.509 certificates have the following fields, in addition to the signature:

- **Version**. This identifies which version of the X.509 standard applies to this certificate, which affects what information can be specified in it.
- **Serial Number**. The entity that created the certificate is responsible for assigning it a serial number to distinguish it from other certificates it issues.
- **Signature Algorithm Identifier**. This identifies the algorithm used by the Certificate Authority (CA) to sign the certificate.
- **Issuer Name**. The X.500 name of the entity that signed the certificate. This is normally a CA. Using this certificate implies trusting the entity that signed this certificate.
- **Validity Period**. Each certificate is valid only for a limited amount of time. This period is described by a start date and time and an end date and time, and can be as short as a few seconds or almost as long as a century.
- **Subject Name**. The name of the entity whose public key the certificate identifies. This name uses the X.500 standard, so it is intended to be unique across the Internet.

- **Subject Public Key Information**. This is the public key of the entity being named, together with an algorithm identifier which specifies which public key cryptographic system this key belongs to and any associated key parameters.

The following is an example of a Polycom device certificate (if opened with the Microsoft Internet Explorer 7 or Firefox 3.5 browser on a computer running Microsoft XP Service Pack 3):



The device certificate and associated private key are stored on the phone in its non-volatile memory as part of the manufacturing process.

For more information on digital certificates, refer to http://www.ietf.org/html.charters/pkix-charter.html and http://www.ietf.org/rfc/rfc2459.txt .

To determine if there is a digital certificate on a Polycom phone:

1. Press the **Menu** key, and then select **Status > Platform > Phone**.
2. Scroll down to the bottom of screen.

   One of three possible strings are displayed:

   – "Device Certificate: Installed" is displayed if the certificate is available in flash memory, all the certificate fields are valid (listed above) and certificate has not expired.

   – "Device Certificate: Not Installed" is displayed if the certificate is not available in flash memory (or the flash memory location where the device certificate is to be stored is blank).

   – "Device Certificate: Invalid" is displayed if the certificate is not valid (if any of the fields listed above are not correct).

Mutual TLS Authentication

Mutual Transport Layer Security (TLS) authentication is a process in which both entities in a communications link authenticate each other. In a network environment, the phone authenticates the server and vice-versa. In this way, phone users can be assured that they are doing business exclusively with legitimate entities and servers can be certain that all would-be users are attempting to gain access for legitimate purposes.

This feature requires that the phone being used has a Polycom factory-installed device certificate. Refer to the previous section, Digital Certificates.

Prior to SIP 3.2, and in cases where the phones do not have factory-installed device certificates, the phone will authenticate to the server as part of the TLS authentication, but the server cannot cryptographically-authenticate the phone. This is sometime referred to as Server Authentication or single-sided Authentication.

Mutual TLS authentication is optional and is initiated by the server. When the phone acts as a TLS client and the server is configured to require mutual TLS, the server will request, and then validate the client certificate during the handshake. If the server is configured to require mutual TLS, a device certificate and an associated private key must be loaded on the phone.

The digital certificate, stored on the phone, is used by:

- HTTPS device configuration, if the server is configured for Mutual Authentication
- SIP signaling—when the selected transport protocol is TLS and the server is configured for Mutual Authentication
- Syslog—when the selected transport protocol is TLS and the server is configured for Mutual Authentication
- Corporate Directory—when the selected transport protocol is TLS and the server is configured for Mutual Authentication

Note At this time, the user will not be able to modify or update the digital certificate or the associated private key stored on the phone during manufacturing.

The Polycom Root CA can be downloaded from http://pki.polycom.com . The location of the Certificate Revocation List (CRL)—a list of all expired certificates signed by the Polycom Root CA—is part of the Polycom Root CA digital certificate. If Mutual TLS is enabled, the Polycom Root CA must be downloaded onto the HTTPS server.

At this time, the following operating systems/web servers combinations are supported:

- Microsoft Internet Information Services 6.0 on Microsoft Windows Server 2003

- Apache v1.3 on Microsoft Windows XP

For more information on using Mutual TLS with Microsoft® Internet Information Services (IIS) 6.0, refer to "Technical Bulletin 52609: Mutual Transport Layer Security Provisioning Using Microsoft Internet Information Services 6.0" at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Secure Real-Time Transport Protocol

Secure Real-Time Transport Protocol (SRTP) provides means of encrypting the audio stream(s) to avoid interception and eavesdropping on phone calls. Both RTP and RTCP signaling may be encrypted using an AES algorithm as described in RFC3711. When this feature is enabled on the phones, phones will negotiate with the other end-point whether and what type of encryption or authentication to utilize for the session. This negotiation process is compliant with RFC4568 (Session Description Protocol (SDP) Security Descriptions for Media Streams).

For more information, refer to http://www.ietf.org/rfc/rfc3711.txt?number=3711 .

For the procedure describing how two phones set up SRTP for a call, refer to http://www.ietf.org/rfc/rfc4568.txt?number=4568 .

Authentication proves to the phone receiving the RTP/RTCP stream that the packets are from the expected source and have not been tampered with. Encryption modifies the data in the RTP/RTCP streams so that, if the data is captured or intercepted, it cannot be understood—it sounds like noise. Only the receiver knows the key to restore the data.

A number of session parameters have been added to allow you to turn off authentication and encryption for RTP and RTCP streams. This is done mainly to reduce the CPU usage.

Note When SRTP is enabled on Polycom's older platforms (for example, the SoundPoint IP 301 and 501), they may quickly exceed their CPU capacity after one call. Local conferences on SoundPoint IP 301, IP 501, IP 600, and IP 601 phones may fall-back to unencrypted mode due to processor power limitations.

If the call is completely secure (RTP authentication and encryption and RTCP authentication and RTCP encryption are enabled), then the user sees a padlock symbol  appearing in the last frame of the connected context animation (two arrow moving towards each other) .

Configuration changes can performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **sip-interop.cfg**	Specify the parameters to enable and disable SRTP. • Refer to <sec/> on page A-101.

Configuration File Examples

In Example 1, the **sip-interop.cfg** configuration file is shown below:

```
sec.srtp.offer = "1"
sec.srtp.sessionParams.noAuth.offer = "1"
sec.srtp.sessionParams.noEncrypRTP.offer = "1"
sec.srtp.sessionParams.noEncrypRTCP.offer = "1"
sec.srtp.require = "0"
sec.srtp.sessionParams.noAuth.require = "0"
sec.srtp.sessionParams.noEncrypRTP.require = "0"
sec.srtp.sessionParams.noEncrypRTCP.require = "0"
```

This would result in an offer (SIP INVITE with SDP) with 8 crypto attributes with the following session parameters:

```
<no session parameters>
UNENCRYPTED_SRTCP
UNENCRYPTED_SRTP
UNAUTHENTICATED_SRTP
UNAUTHENTICATED_SRTP,UNENCRYPTED_SRTCP
UNENCRYPTED_SRTP,UNENCRYPTED_SRTCP
UNAUTHENTICATED_SRTP,UNENCRYPTED_SRTP
UNAUTHENTICATED_SRTP,UNENCRYPTED_SRTP,UNENCRYPTED_SRTCP
```

In the above example, the crypto attributes are ordered "most secure" to "least secure" (more security turned off). The phone receiving this call should chose the most secure crypto it can support based on the SRTP "require" settings in **sip.cfg** and reply with it in the SDP of a 200 OK SIP message.

In Example 2, the **sip-interop.cfg** configuration file is shown below:

```
sec.srtp.offer = "1"
sec.srtp.sessionParams.noAuth.offer = "1"
sec.srtp.sessionParams.noEncrypRTP.offer = "1"
sec.srtp.sessionParams.noEncrypRTCP.offer = "1"
sec.srtp.require = "1"
sec.srtp.sessionParams.noAuth.require = "0"
sec.srtp.sessionParams.noEncrypRTP.require = "1"
sec.srtp.sessionParams.noEncrypRTCP.require = "0"
```

This would result in an offer (SIP INVITE with SDP) with 4 crypto attributes with the following session parameters:

```
UNENCRYPTED_SRTP
```

```
UNENCRYPTED_SRTP,UNENCRYPTED_SRTCP
UNAUTHENTICATED_SRTP,UNENCRYPTED_SRTP
UNAUTHENTICATED_SRTP,UNENCRYPTED_SRTP,UNENCRYPTED_SRTCP
```

In the above example, every crypto includes the UNENCRYPTED_SRTP session parameter because it is required.

If nothing compatible is offered based on receiving phone's STRP "require" settings, then the call is rejected or dropped.

Configurable TLS Cipher Suites

The phone administrator can control which of cipher suites will be offered/accepted during TLS session negotiation. The phone supports the following cipher suites (see table below), and the configuration is achieved as through to <TLS/> on page A-108 . The 'Null Cipher' is a special case option which will not encrypt the signaling traffic, and is useful for troubleshooting purposes.

ADH	ADH-RC4-MD5, ADH-DES-CBC-SHA, ADH-DES-CBC3-SHA, ADH-AES128-SHA, ADH-AES256-SHA
AES128	AES128-SHA
AES256	AES256-SHA
DES	DES-CBC-SHA, DES-CBC3-SHA
DHE	DHE-DSS-AES128-SHA, DHE-DSS-AES256-SHA, DHE-RSA-AES128-SHA, DHE-RSA-AES256-SHA,
EXP	EXP-RC4-MD5, EXP-DES-CBC-SH, EXP-EDH-DSS-DES-CBC-SHA, EXP-DES-CBC-SHA, EXP-ADH-RC4-MD5, EXP-ADH-DES-CBC-SHA, EXP-EDH-RSA-DES-CBC-SHA
EDH	EDH-RSA-DES-CBC-SHA, EDH-DSS-DES-CBC3-SHA, EDH-DSS-CBC-SHA
NULL	NULL-MD5, NULL-SHA
RC4	RC4-MD5, RC4-SHA

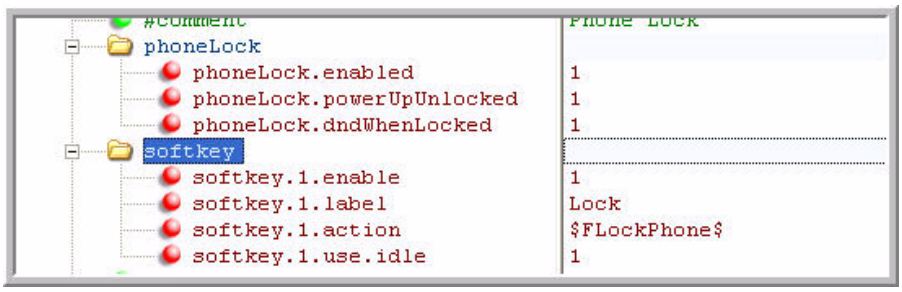
Configuration changes can performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **site.cfg**	Specify the TLS cipher suites for all and specific aspects of Polycom UC Software 3.3.0 • Refer to <TLS/> on page A-108.
Local	Web Server (if enabled)	Specify the TLS cipher suites for all and specific aspects of UC Software 3.3.0 Navigate to http://<phoneIPAddress>/netConf#sec . Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.

Locking the Phone

Note The Enhanced Feature Key feature must be enabled if you want to use the **Lock** soft key.

As of Polycom UC Software 3.3.0, the user can lock their phone by pressing the **Lock** soft key or through the menu by selecting **Menu > Settings > Basic > Lock Phone**. The following configuration file snippet shows how to create the **Lock** soft key.



Once the phone is locked, all user features and access to menus are disabled. The messages "The phone is locked." and "Authorized calls only." appear on the graphic display. Incoming calls to the phone may receive a Do Not Disturb treatment. The administrator configures the authorized numbers to which users can place calls.

Using the **New Call** soft key, the user can place calls to up to five authorized numbers only including the emergency number. If the user places a call —using the keypad— to a number that matches an authorized number, the call will proceed. This is to ensure that certain numbers such as emergency numbers can be placed from the phone.

To unlock the phone, the user presses the **Unlock** soft key and enters their password; if it is entered correctly, the phone returns to its normal idle state.

In case the user forgets their password, the system administrator can unlock their phone either by entering the administrator password or by disabling (and re-enabling) the feature using configuration parameters. The latter method facilitates remote unlocking and avoids disclosing the administrator password to the user.

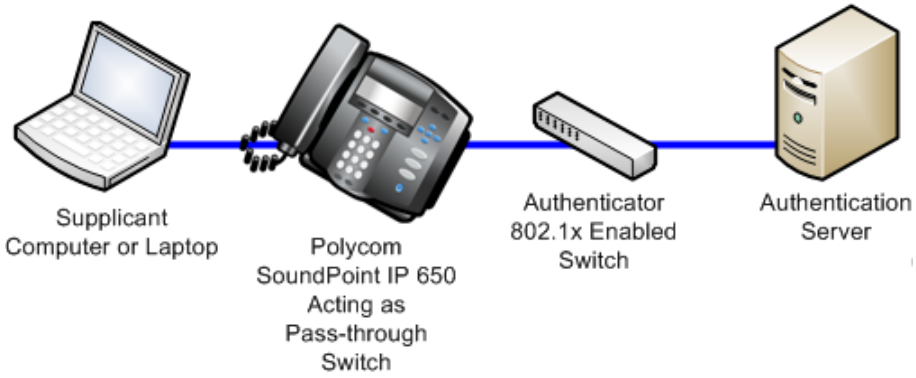
Note If a locked phone is part of a 'shared line' group, calls to the shared line will be presented visually on the locked phone and the phone's user will be able to answer the call on the 'locked' phone.

Configuration changes can performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **features.cfg**	Turn the Enhanced Feature Key feature on or off. • Refer to <feature/> on page A-58. Add Enhanced Feature Keys. • Refer to <efk/> on page A-53. Turn the phone lock feature on or off. • Refer to <phoneLock/> on page A-74.
Local	Web Server (if enabled)	Turn the phone lock feature on or off. Navigate to http://<phoneIPAddress>/phoneLockConf.htm . Changes are saved to local flash and backed up to ***<Ethernet address>*-web.cfg** on the provisioning server. Changes will permanently override global settings unless deleted through the **Reset Web Configuration** menu selection.

Support for EAPOL Logoff Message

Certain SoundPoint IP phones have a PC Ethernet port. The PC Ethernet port on the SoundPoint IP 33x, 450, 550, 560, 601, 650, and 670, and Polycom VVX 1500 phone can be used to connect a computer to the network with the phone acting as a pass-through switch. The following figure shows this configuration.



As of Polycom UC Software 3.3.0, Polycom phones will send an Extensible Authentication Protocol Over LAN (EAPOL) Logoff message on behalf of an authenticate supplicant (computer), when the supplicant is disconnected from the network.

Configuration changes can performed centrally at the provisioning server:

Central (provisioning server)	Configuration template: **site.cfg**	Turn the EAPOL Logoff message feature on or off. • Refer to <dot1x/> <eapollogoff/> on page A-107.

Configuring Polycom Phones Locally

A local phone-based configuration web server is available, unless it is disabled through a configuration file. It can be used as the only method of modifying phone configuration or as a distributed method of augmenting a centralized provisioning model. For more information, refer to <httpd/> on page A-63.

The phone's local user interface also permits many application settings to be modified, such as SIP server address, ring type, or regional settings such as time/date format and language.

Local Web Server Access	Point your web browser to http://<phoneIPAddress>/. Configuration pages are accessible from the menu along the top banner. The web server will issue an authentication challenge to all pages except for the home page. Credentials are (case sensitive): User Name: Polycom Password: The administrator password is used for this.
Local Settings Menu Access	Some items in the Settings menu are locked to prevent accidental changes. To unlock these menus, enter the user or administrator passwords. The administrator password can be used anywhere that the user password is used. (Polycom recommends that you change the administrative password from the default value.) Factory default passwords are: User password: 123 Administrator password: 456

Passwords:	
Administrator password required.	Network Configuration Line Configuration Call Server Configuration SSL Security settings Reset to Default - local configuration, device settings, and file system format
User password required.	Reboot Phone

Changes made through the web server or local user interface are stored internally as overrides. These overrides take precedence over settings contained in the configuration obtained from the provisioning server.

If the provisioning server permits uploads, these override setting will be saved in a file called **<*Ethernet address*>-phone.cfg** on the provisioning server as well as in flash memory.

Warning

Local configuration changes will continue to override the provisioning server-derived configuration until deleted through the **Reset Local Configuration** menu selection or configured using the ‘device set ‘ procedure.

For more information, refer to Modifying Phone’s Configuration Using the Web Interface on page C-25.

5

Troubleshooting Your Polycom Phones

This chapter provides you with some tools and techniques for troubleshooting Polycom® phones running Polycom® UC Software. The phone can provide feedback in the form of on-screen error messages, status indicators, and log files for troubleshooting issues.

This chapter includes information on:

- BootROM Error Messages
- Polycom UC Software Error Messages
- Status Menu
- Log Files
- Testing Phone Hardware
- Uploading Phone's Configuration

This chapter also presents phone issues, likely causes, and corrective actions. Issues are grouped as follows:

- Power and Startup
- Controls
- Access to Screens and Systems
- Calling
- Displays
- Audio
- Licensable Features
- Upgrading

Review the latest *Release Notes* for the Polycom UC Software for known problems and possible workarounds. For the latest *Release Notes* and the latest version of this Administrator's Guide, go to Polycom Technical Support at http://www.polycom.com/support/voice/.

If a problem is not listed in this chapter nor described in the latest *Release Notes*, contact your Certified Polycom Reseller for support.

Error Messages

There are several different error messages that can be displayed on the phone when it is booting. Some of these errors are fatal, meaning that the phone will not able to boot until this issue has been resolved, and some are recoverable, meaning the phone will continue booting after the error, but the configuration of the phone may not be what you were expecting.

BootROM Error Messages

Most of these errors are also logged on the phone's boot log, however, if you are having trouble connecting to the provisioning server, the phone will likely not be able to upload the boot log for you to examine.

Failed to get boot parameters via DHCP

The phone does not have an IP address and therefore cannot boot. Check that all cables are connected, the DHCP server is running and that the phone has not been put into a VLAN which is different from the DHCP server. Check the DHCP configuration.

Application <file name> is not compatible with this phone!

When the BootROM displays an error like "The application is not compatible", it means an application file was downloaded from the provisioning server, but it cannot be installed on this phone. This issue can usually be resolved by finding a software image that is compatible with the hardware or the BootROM being used and installing this on the provisioning server. There are various different hardware and software dependencies. Refer to the latest *Release Notes* for details on the version you are using.

Could not contact boot server, using existing configuration

The phone could not contact the provisioning server, but the causes may be numerous. It may be cabling issue, it may be related to DHCP configuration, or it could be a problem with the provisioning server itself. The phone can recover from this error so long as it previously downloaded a valid application BootROM image and all of the necessary configuration files.

Error, application is not present!

There is no application stored in flash memory and the phone cannot boot. Compatible Polycom UC Software must be downloaded into the phone using one of the supported provisioning protocols. You need to resolve the issue of connecting to the provisioning server. This error is typically a result of one of the above errors. This error is fatal, but recoverable. Contact your system administrator.

Not all configuration files were present on the server

Similarly, a message about configuration files not being present, means that the phone was able to reach the provisioning server, but that it was not able to find all the necessary files. So long as the files exist in flash memory, the phone can boot following this error. The probable cause of this error is a misconfiguration of the **<MACaddress>.cfg** file.

Note This error does not occur with BootROM 3.2.2 B or later.

Error loading <file name>

When the required file does not exist in flash memory and cannot be found on the provisioning server, the "Error loading" message will tell you which file could not be found. This error only remains on the screen for a few seconds so you need to watch closely. The phone reboots.

Note This error does not occur with BootROM 3.2.2 B or later.

Polycom UC Software Error Messages

Config file error: Files contain invalid params: <filename1>, <filename2>, ...
Config file error: <filename> contains invalid params.

These messages appears if any of the following pre-Polycom UC Software 3.3.0 parameters are found in the configuration files:

- `tone.chord.ringer.1.freq.1`
- `se.pat.callProg.1.name`
- `ind.anim.IP_500.1.frame.1.duration`
- `ind.pattern.1.step.1.state`
- `feature.2.name`
- `feature.9.name`

This message also appears if any configuration file contains:

- More than 100 '"unknown" parameters, or
- More than 100 "out-of-range" values, or
- More than 100 "invalid" values.

Update the configuration files to use the correct parameters. For more information, refer to Configuration Parameters on page A-8.

Network link is down

Since the Polycom phones do not have an LED indicating network LINK status like many networking devices, if a link failure is detected while the phone is running a message saying "Network link is down" will be displayed. This message will be shown on the screen whenever the phone is not in the menu system and will remain on screen until the link problem is resolved. Call related functions (for example, soft keys and feature keys) disabled when the network is down; however the menu works.

Status

When the phone is unable to register with the call control server, the icon  is shown (outline). Once the phone is registered, the icon  is shown (solid). On the SoundStation IP 7000, the icons are  and  . On the VVX 1500, the icons are  and  .

Flashing Time

If the phone has not been able to contact the SNTP server or if one has not been configured, the date/time display will flash until this is fixed. If an SNTP is not available, the data/time display can be turned off so that the flashing display is not a distraction.

CMA Presence not registered.
CMA Directory not registered.
CMA provisioning error.
CMA authentication failed.

These messages may appear if a VVX phone is having connection issues with the Polycom Converged Management Application™ (CMA™) system that provisioned it. For more information about provisioning by a Polycom CMA system, refer to the *Polycom CMA System Deploying Visual Communications Administration Guide* and *Polycom CMA System Operations Guide*, which are available at http://www.polycom/support/cma_4000_5000 .

Status Menu

Debugging of single phone may be possible through an examination of the phone's status menu. Press **Menu**, select ***Status***, and then press the **Select** soft key.

Under the ***Platform*** selection, you can get details on the phone's serial number or MAC address, the current IP address, the BootROM version, the application version, the name of the configuration files in use, and the address of the provisioning server.

In the ***Network*** menu, the phone will provide information about TCP/IP setting, Ethernet port speed, connectivity status of the PC port, and statistics on packets sent and received since last boot. This would also be a good place to look and see how long it has been since the phone rebooted. The Call Statistics screen shows packets sent and received on the last call.

The ***Lines*** menu will give you details about the status of each line that has been configured on the phone.

Finally, the ***Diagnostics*** menu offers a series of hardware tests to verify correct operation of the microphone, speaker, handset, and third party headset, if present. It will also let you test that each of the keys on the phone is working, and it will display the function that has been assigned to each of the keys in the configuration. This is also where you can test the LCD for faulty pixels.

In addition to the hardware tests, the Diagnostics menu has a series of real-time graphs for CPU, network and memory utilization that can be helpful in diagnosing performance issues.

Log Files

Polycom phones will log various events to files stored in the flash file system and will periodically upload these log files to the provisioning server. The files are stored in the phone's home directory or a user-configurable directory. You can also configure a phone to send log messages to a syslog server. If a phone was provisioned by a Polycom CMA system, log messages will be sent to the Polycom CMA system.

There is one log file for the BootROM and one for the application. When a phone uploads its log files, they are saved on the provisioning server with the MAC address of the phone prepended to the file name. For example, **0004f200360b-boot.log** and **0004f200360b-app.log** are the files associated with MAC address 00f4f200360b. The BootROM log file is uploaded to the provisioning server after every reboot. The application log file is uploaded periodically or when the local copy reaches a predetermined size. If the BootROM was updated (and the file system is cleared), the phone's current **app.log** is uploaded to the provisioning server as **MAC-appFlash.log** . For more information on log file contents, refer to <log/> on page D-4.

Both log files can be uploaded on demand using a multiple key combination described in Multiple Key Combinations on page C-9. The phone uploads four files, namely, **mac-boot.log**, **app-boot.log**, **mac-now-boot.log**, and **mac-now-app.log**. The "now_" logs are uploaded manually unless they are empty.

The amount of logging that the phone performs can be tuned for the application to provide more or less detail on specific components of the phone's software. For example, if you are troubleshooting a SIP signaling issue, you are not likely interested in DSP events. Logging levels are adjusted in the configuration files or via the web interface. You should not modify the default logging levels unless directed to by Polycom Technical Support. Inappropriate logging levels can cause performance issues on the phone.

In addition to logging events, the phone can be configured to automatically execute command-line instructions at specified intervals that output run-time information such as memory utilization, task status, or network buffer contents to the log file. These techniques should only be used in consultation with Polycom Technical Support.

Polycom UC Software Logging Options

Each of the components of the Polycom UC Software is capable of logging events of different severity. This allows you to capture lower severity events in one part of the application, while still only getting high severity event for other components.

The parameters for log level settings are found in the **techsupport.cfg** configuration file. They are `log.level.change.module_name`. Log levels range from 1 to 6 (1 for the most detailed logging, 6 for critical errors only). There are currently 27 different log types that can be adjusted to assist with the investigation of different problems.

When testing is complete, remember to return all logging levels to the default value of 4.

There are other logging parameters that you may wish to modify. Changing these parameters does not have the same impact as changing the logging levels, but you should still understand how your changes will affect the phone and the network.

- `log.render.level`—Sets the lowest level that can be logged (default=1)
- `log.render.file.size`—Maximum size before log file is uploaded (default=16 kb)
- `log.render.file.upload.period`—Frequency of log uploads (default is 172800 seconds = 48 hours)
- `log.render.file.upload.append`—Controls if log files on the provisioning server are overwritten or appended, not supported by all servers

- `log.render.file.upload.append.sizeLimit`—Controls the maximum size of log files on the provisioning server (default=512 kb)
- `log.render.file.upload.append.limitMode`—Controls action to take when server log reaches max size, actions are stop and delete

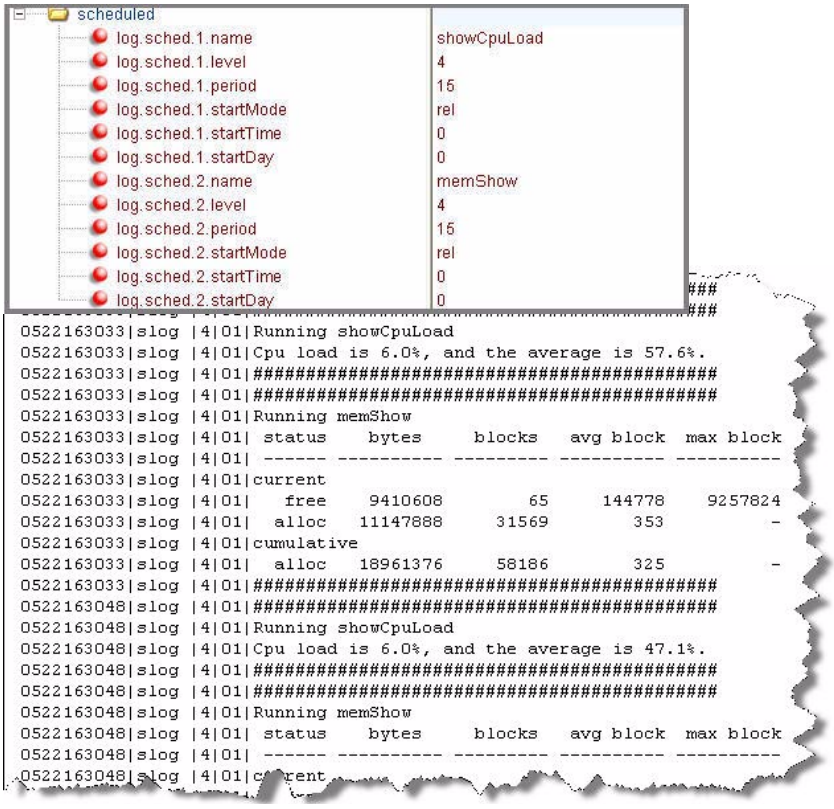
Scheduled Logging

Scheduled logging is a powerful tool for anyone who is trying to troubleshoot an issue with the phone that only occurs after some time in operation.

The output of these instructions is written to the application log, and can be examined later (for trend data).

The parameters for scheduled logging are found in the **techsupport.cfg** configuration file. They are `log.sched.module_name`.

The following figure shows an example of a configuration file and the resulting log file.



Manual Log Upload

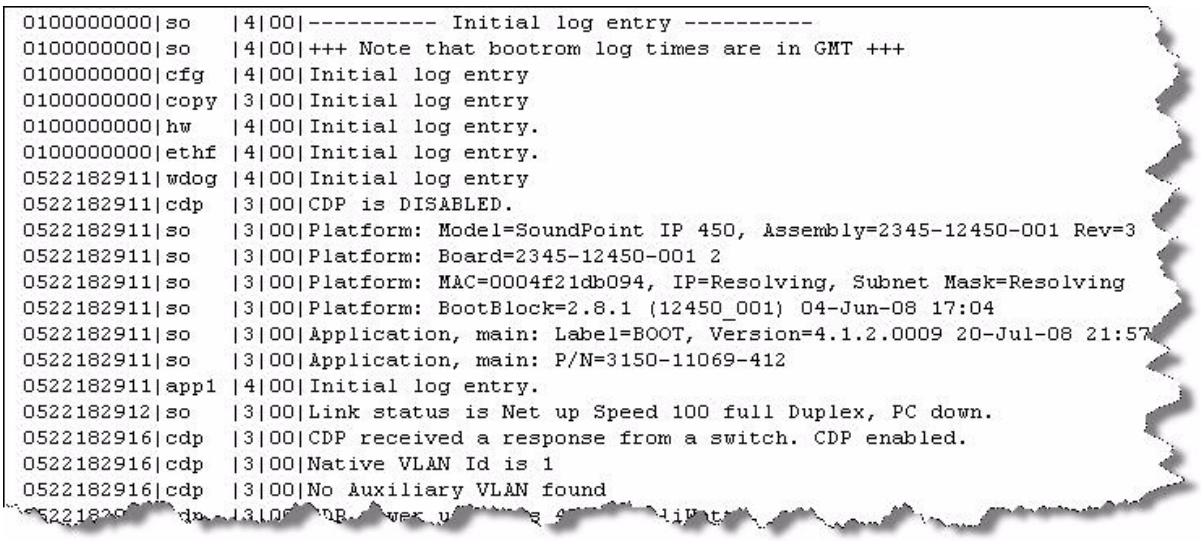
If you want to look at the log files without having to wait for the phone to upload them (which could take as long as 24 hours or more), initiate an upload by pressing correct combination of keys on the phone.

For more information, refer to Multiple Key Combinations on page C-9.

When the log files are manually uploaded, the word "now" is inserted into the name of the file, for example, 0004f200360b-now-boot.log .

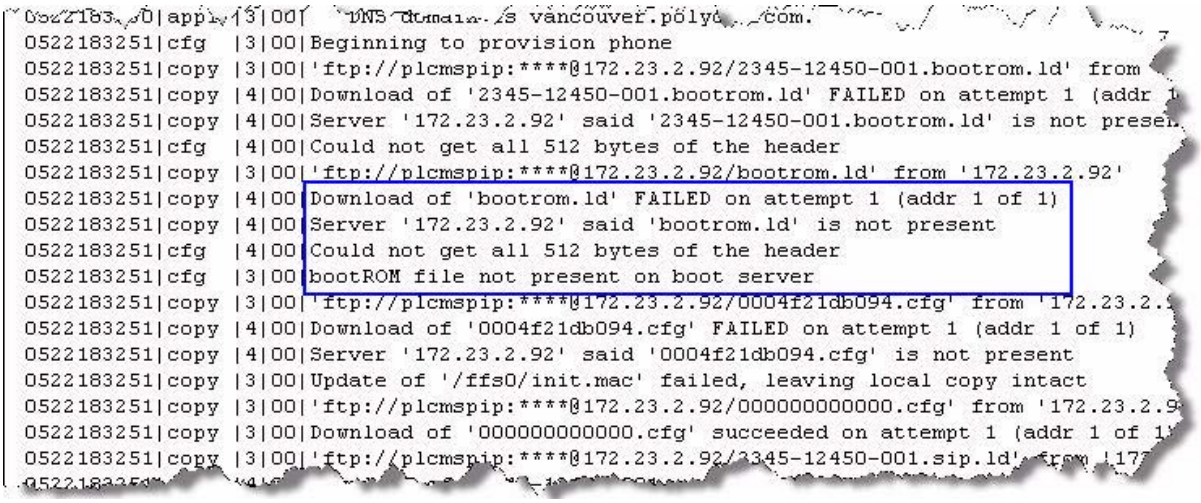
Reading a Boot Log

The following figure shows a portion of a boot log file:



Boot Failure Messages

The following figure shows a number of boot failure messages:



Reading an Application Log

The following figure shows portions of an application log file:

Reading a Syslog

The following shows a portion of a syslog log file—the messages look identical to the normal log with the addition of a timestamp and IP address:

```
Jan  0 00:00:00 172.23.7.249 0100000000|so   |4|00|---------- Initial log entry ----------
Jan  0 00:00:00 172.23.7.249 0100000000|so   |4|00|+++ Note that bootrom log times are in GMT +++
Jan  0 00:00:00 172.23.7.249 0100000000|cfg  |4|00|Initial log entry
Jan  0 00:00:00 172.23.7.249 0100000000|copy |3|00|Initial log entry
Jan  0 00:00:00 172.23.7.249 0100000000|hw   |4|00|Initial log entry.
Jan  0 00:00:00 172.23.7.249 0100000000|ethf |4|00|Initial log entry.
Feb 13 01:12:39 172.23.7.249 0213011239|wdog |4|00|Initial log entry
Feb 13 01:12:39 172.23.7.249 0213011239|cdp  |3|00|CDP is DISABLED.
Feb 13 01:12:39 172.23.7.249 0213011239|so   |3|00|Platform: Model=SoundPoint IP 650, Assembly=2345-12600-
Feb 13 01:12:39 172.23.7.249 0213011239|so   |3|00|Platform: Board=2345-12600-001 1
Feb 13 01:12:39 172.23.7.249 0213011239|so   |3|00|Platform: MAC=0004f2111511, IP=Resolving, Subnet Mask=
Feb 13 01:12:39 172.23.7.249 0213011239|so   |3|00|Platform: BootBlock=2.7.0 (12600_001) 30-May-06 15:58
Feb 13 01:12:39 172.23.7.249 0213011239|so   |3|00|Application, main: Label=BOOT, Version=4.1.0.0219 10-D
Feb 13 01:12:39 172.23.7.249 0213011239|so   |3|00|Application, main: P/N=3150-11069-410
Feb 13 01:12:39 172.23.7.249 0213011239|appl |4|00|Initial log entry.
Feb 13 01:12:40 172.23.7.249 0213011240|so   |3|00|Link status is Net down, PC down.
Feb 13 01:12:41 172.23.7.249 0213011241|so   |3|00|Link status is Net up Speed 100 half Duplex, PC down.
Feb 13 01:12:41 172.23.7.249 0213011241|cdp  |3|00|CDP is disabled.
Feb 13 01:12:45 172.23.7.249 0213011245|appl |3|00|DNS resolver servers are '172.23.0.200' '172.23.0.239'
Feb 13 01:12:45 172.23.7.249 0213011245|appl |3|00|DNS resolver search domain is 'vancouver.polycom.com'
Feb 13 01:12:45 172.23.7.249 0213011245|appl |3|00|Bootline: esw(3,0)bootHost:flash e=172.23.7.249:ffff00
Apr 15 22:32:22 172.23.7.249 0415223222|appl |3|00|Time has been set from 172.23.0.200 (172.23.0.200).
Apr 15 22:32:22 172.23.7.249 0415223222|appl |3|00|DHCP returned result 0x3E7 from server 172.23.0.232.
Apr 15 22:32:22 172.23.7.249 0415223222|appl |3|00|   Phone IP address is 172.23.7.249.
Apr 15 22:32:22 172.23.7.249 0415223222|appl |3|00|   Subnet mask is 255.255.0.0.
Apr 15 22:32:22 172.23.7.249 0415223222|appl |3|00|   Gateway address is 172.23.2.240.
Apr 15 22:32:22 172.23.7.249 0415223222|appl |3|00|   Time server is 172.23.0.200.
Apr 15 22:32:22 172.23.7.249 0415223222|appl |3|00|   GMT offset is -28800 seconds.
Apr 15 [illegible]
```

Testing Phone Hardware

To obtain more detailed troubleshooting information, you can access certain menus on the SoundPoint IP and SoundStation IP phone that test the phone hardware.

From the diagnostics menu, you can test:

- The phone's microphones, speaker, handset, and any third-party handset (if present)
- Keypad mapping—You can verify the function assign to each key.
- Graphic display—You can test the LCD for faulty pixels.

To test the phone hardware:

>> Press the **Menu** key, and then select **Status > Diagnostics > Test Hardware > Audio Diagnostics**, **Keypad Diagnostics**, or **Display Diagnostics**.

Uploading Phone's Configuration

In Polycom UC Software 3.3.0, the ability to upload the configuration files representing phone's current configuration was added. A number of files could be uploaded to the provisioning server, one for every active source along with the current non-default configuration set.

This is primarily a diagnostics tool to help find configuration errors.

To upload the phone's current configuration:

1. Press the **Menu** key, and then select **Settings > Advanced > Admin Settings > Upload Configuration** .
2. Select one of **All Sources**, **Configuration Files**, **Local**, **CMA**, and **Web**.

   The CMA option will appear on the VVX 1500 phone only.
3. Press the **Upload** soft key.

   The phone uploads the configuration file to the location that you specified in `prov.configUploadPath` (refer to <prov/> on page A-78).

   For example, if you select **ALL**, a file **[MACAddress]-update-all.cfg** is uploaded.

Power and Startup

Symptom	Problem	Corrective Action
There are power issues.	The Polycom phone has no power.	Do one of the following: • Verify that no lights appear on the unit when it is powered up. • Check if the phone is properly plugged into a functional AC outlet. • Make sure that the phone isn't plugged into a plug controlled by a light switch that is off. • If plugged into a power strip, try plugging directly into a wall outlet instead. • Try the phone in another room where the electricity is known to be working on a particular outlet. • If using PoE, the power supply voltage may be too high or too low.
The phone will not boot.	There is a corrupt or invalid firmware image or configuration on the phone.	Ensure that the provisioning server is accessible on the network and a valid software load and valid configuration files are available. Ensure that the phone is pointing to the provisioning server on the network. Reboot the phone.

Controls

Symptom	Problem	Corrective Action
The dial pad does not work.	The dial pad on the Polycom phone does not respond.	Do one of the following: • Check for a response from other feature keys or from the dial pad. • Place a call to the phone from a known working telephone. Check for display updates. • Press the **Menu** key followed by **System Status** and **Server Status** to check if the telephone is correctly registered to the server. • Press the **Menu** key followed by **System Status** and **Network Statistics**. Scroll down to see if LAN port shows active or Inactive. • Check the termination at the switch or hub end of the network LAN cable. Ensure that the switch/hub port connected to the telephone is operational (if not accessible, contact your system administrator). • Before restarting your phone, contact your system administrator, since this may allow more detailed troubleshooting to occur before losing any current status information.

Access to Screens and Systems

Symptom	Problem	Corrective Action
There is no response from feature key presses.	The Polycom phone is not in active state.	Do one of the following: • Press the keys more slowly. • Check to see whether or not the key has been mapped to a different function or disabled. • Make a call to the phone to check for inbound call display and ringing as normal. If successful, try to press feature keys within the call to access Directory or Buddy Status, for example. • Press **Menu** followed by **Status > Lines** to confirm line is actively registered to the call server. • Reboot the phone to attempt re-registration to the call server (refer to Rebooting the Phone on page C-10).
The display shows "Network Link is Down".	The LAN cable is not properly connected.	Do one of the following: • Check termination at the switch or hub (furthest end of the cable from the phone). • Check that the switch or hub is operational (flashing link/status lights) or contact your system administrator. • Press **Menu** followed by **Status > Network**. Scroll down to verify that the LAN is active. • Ping phone from another machine. • Reboot the phone to attempt re-registration to the call server (refer to Rebooting the Phone on page C-10).

Calling

Symptom	Problem	Corrective Action
There is no dial tone.	Power is not correctly applied to the Polycom phone.	Do one of the following: • Check that the display is illuminated. • Make sure the LAN cable is inserted properly at the rear of the phone (try unplugging and re-inserting the cable). • If using in-line powering, have your system administrator check that the switch is supplying power to the phone.
	Dial tone is not present on one of audio paths.	Do one of the following: • Switch between Handset, Headset (if present) or Hands-Free Speakerphone to see if dial tone is present on another paths. • If dial tone exists on another path, connect a different handset or headset to isolate the problem. • Check configuration for gain levels.
	The phone is not registered.	Contact your system administrator.
The phone does not ring.	Ring setting or volume is low.	Do one of the following: • Adjust the ringing level from the front panel using the volume up/down keys. • Check same status of handset, headset (if connected) and through the Hands-Free Speakerphone.
	Outbound or inbound calling is unsuccessful.	Do one of the following: • Place a call to the phone under investigation. Check that the display indicates incoming call information. • Lift the handset. Ensure dial tone is present and place a call to another extension or number. Check that the display changes in response.
The line icon shows an unregistered line icon.	The phone line is unregistered.	Contact your system administrator.

Displays

Symptom	Problem	Corrective Action
There is no display. The display is incorrect. The display has bad contrast.	Power is not correctly applied to the Polycom phone.	Do one of the following: • Check that the display is illuminated. • Make sure the LAN cable is inserted properly at the rear of the phone (try unplugging and re-inserting the cable). • If using in-line powering, have your system administrator check that the switch is supplying power to the phone. • Use the screen capture feature. Refer to Capturing Phone's Current Screen on page C-28.
	The contrast needs adjustment.	Do one of the following: • Refer to the appropriate Polycom phone User Guide. • Reboot the phone to obtain a default level of contrast (refer to Rebooting the Phone on page C-10). • Use the screen capture feature. Refer to Capturing Phone's Current Screen on page C-28.
	Outbound or inbound calling is unsuccessful.	Do one of the following: • Place a call to the phone under investigation. Check that the display indicates incoming call information. • Lift the handset. Ensure dial tone is present and place a call to another extension or number. Check that the display changes in response. • Use the screen capture feature. Refer to Capturing Phone's Current Screen on page C-28.
The display is flickering.	Certain type of older fluorescent lighting causes the display to appear to flicker.	Do one of the following: • Move the Polycom phone away from the lights. • Replace the lights. • Use the screen capture feature. Refer to Capturing Phone's Current Screen on page C-28.

Audio

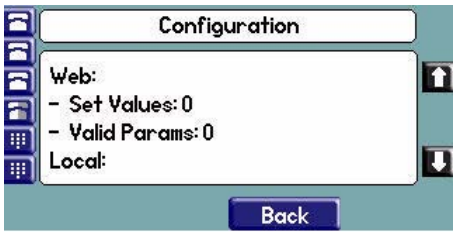
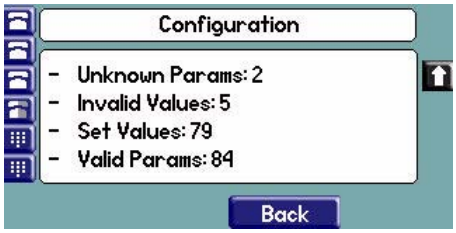
Symptom	Problem	Corrective Action
There is no audio on the headset.	The connections are not correct.	Do one of the following: • Ensure the headset is plugged into the jack marked Headset at the rear of the phone. • Ensure the headset amplifier (if present) is turned on and/or the volume is correctly adjusted).
There are audio and echo issues on the headset.	Possible issues include: • Echo on external calls through a gateway. • Internal calls (no gateway), handsfree echo. • Internal calls (no gateway), handset to handset echo.	Refer to “Technical Bulletin 16249: Troubleshooting Audio and Echo Issues on SoundPoint® IP Phones” at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Licensable Features

Symptom	Problem	Corrective Action
A user is trying to access one of the following features, but it is not available on their phone: • Corporate Directory • Recording and Playback of Audio Calls • Managing Conferences • Voice Quality Monitoring • H.323	The license is not installed on the phone or it has expired.	Do the following: • Press the **Menu** key, then select **Status > Licenses**. • Using the arrow keys, verify that the feature in question has a valid license. If no licenses are installed, the “No license installed.” message appears.

Upgrading

Symptom	Problem	Corrective Action
SoundPoint IP 300, 301, 430, 500, 501, 600, and/or 601 and/or SoundStation IP 4000 behave incorrectly or do not display new features.	New features are not supported on the SoundPoint IP 300, 301, 430, 500, 501, 600, and 601 and SoundStation IP 4000 and the configuration files have not been correctly modified. These phones will not 'understand' the new configuration parameters, and will attempt to load the new application.	The attempt to load the new application will fail since there is no IP 300/301/430/500/501/600/601/4000 image contained within the **sip.ld** file, so the phone will continue on and run the current version of application that it has in memory. It will however use the new configuration files. Refer to Supporting Legacy SoundPoint IP and SoundStation IP Phones on page 3-22.
The VVX 1500 phone will not upgrade when provisioned by a Polycom CMA system.	The VVX 1500 phone is not running Polycom UC Software 3.3.0 .	Do the following: • Upgrade the VVX 1500 phone to UC Software 3.3.0 using the provisioning server. Refer to Upgrading Polycom UC Software on page 3-20. • Ensure that the Polycom CMA system is running software version 5.0 . • Change the appropriate CMA parameters through the phone's user interface. Refer to Provisioning VVX 1500 Phones Using a Polycom CMA System on page 3-25. The software on the VVX 1500 phone can now be upgraded through the Polycom CMA system.

Symptom	Problem	Corrective Action
Certain settings or features are not working as expected on the phone.	Settings selected in the configuration files are not within the permitted range or are invalid for a particular parameter.	Do the following: • Press the **Menu** key, then select **Status > Platform > Configuration**. • Using the Down arrow key, view the configuration currently being used by the phone. For example:   • Correct the configuration files. • Restart the phone.
A screen similar to the following appears on the phone for 5 seconds. 	Pre-UC Software 3.3.0 configuration files are being used with UC Software 3.3.0 . Specifically, the following parameters are in the configuration files: • `tone.chord.ringer.1.freq.1` • `se.pat.callProg.1.name` • `ind.anim.IP_500.1.frame.1.duration` • `ind.pattern.1.step.1.state` • `feature.2.name` • `feature.9.name` Also the configuration files contain: • more than 100 “unknown” parameters • more than 100 “out-of-range” parameters • more than 100 “invalid” parameters	

A

Configuration Files

This appendix provides detailed descriptions of certain configuration files used by the Polycom® UC Software. It is a reference for all parameters that are configurable when using the centralized provisioning installation model.

This appendix contains information on:

- Master Configuration Files (**MAC-address.cfg** or **000000000000.cfg**)
- Sample Template Files
- Configuration Parameters

The configuration parameters dictate the behavior of the phone once it is running the executable specified in the master configuration file.

Warning Configuration files should only be modified by a knowledgeable system administrator. Applying incorrect parameters may render the phone unusable.

Warning The localization parameter contains language selections in the 'native' font for that language. These include fonts that are not supported in certain XML editors. If the configuration file, where the language parameter is defined, is edited using such an editor the language selections shown in the **Languages** menu on the phone may not display correctly. To confirm whether your editor properly supports these characters, view the language parameter for languages such as Chinese, Japanese, Korean, Russian— for example `lcl.ml.lang.menu.1.label` .

If you want to edit any of the XML dictionary files, you must use an XML editor that supports the same ‘native’ fonts as mentioned above.

Note The master configuration file must have the **.cfg** extension. However, none of the other configuration files need to. For example, **site.php** is a valid configuration filename (in reference to a web design php script).

Note

In the tables in the subsequent sections, "Null" should be interpreted as the empty string, that is, attributeName="" when the file is viewed in an XML editor.

To enter special characters in a configuration file, enter the appropriate sequence using an XML editor:

- & as &
- " as "
- ' as '
- < as <
- > as >

Note

You can make changes to the configuration files through the web interface to the phone. Using your chosen browser, enter the phone's IP address as the browser address. For more information, refer to Modifying Phone's Configuration Using the Web Interface on page C-25.

Changes made through the web interface are written to the web override file. These changes remain active until **Settings > Advanced > Admin Settings > Reset to defaults > Reset Web Configuration** is performed.

You can also make changes to the configuration files through the phone's user interface.

Master Configuration Files

The master configuration files can be one of:

- Specified master configuration file—The master configuration file can be explicitly specified in the provisioning server address, for example, http://usr:pwd@server/dir/example1.cfg. The filename must end with **.cfg** and be at least five characters long. If this file cannot be downloaded, the phone will search for the per-phone master configuration file (described next).
- Per-phone master configuration file—If per-phone customization is required, the file should be named **<Ethernet address>.cfg**, where Ethernet address is the MAC address of the phone in question. For a-f hexadecimal digits, use lower case only, for example, **0004f200106c.cfg**. The Ethernet address can be viewed using the **About** soft key during the auto-restart countdown of the BootROM or through the **Menu > Status > Platform > Phone** menu in the application. It is also printed on a label on the back of the phone. If this file cannot be downloaded, the phone will search for the default master configuration file (described next).
- Default master configuration file—For systems in which the configuration is identical for all phones (no per-phone **<Ethernet address>.cfg** files), the default master configuration file may be used to set the configuration for

all phones. The file named **000000000000.cfg** (<12 zeros>.cfg) is the default master configuration file and it is recommended that one be present on the provisioning server. If a phone does not find its own **<Ethernet address>.cfg** file, it will use this one, and establish a baseline configuration. This file is part of the standard Polycom distribution of configuration files. It should be used as the template for the **<Ethernet address>.cfg** files.

The default master configuration file, **000000000000.cfg**, for Polycom UC software 3.3.0 is shown below:

```
    <?xml version=”1.0” standalone=”yes”?>
    <!-- Default Master SIP Configuration File -->
    <!-- For information on configuring Polycom VoIP phones please
refer to the -->
    <!-- Configuration File Management white paper available from: -->
    <!--
http://www.polycom.com/common/documents/whitepapers/configuration_file
_management_on_soundpoint_ip_phones.pdf -->
    <!-- $RCSfile: 000000000000.cfg,v $  $Revision: 1.21 $ -->
    <APPLICATION APP_FILE_PATH="sip.ld" CONFIG_FILES="reg-basic.cfg,
sip-basic.cfg" MISC_FILES="" LOG_FILE_DIRECTORY=""
OVERRIDES_DIRECTORY="" CONTACTS_DIRECTORY="" LICENSE_DIRECTORY="">
    <APPLICATION_SPIP300 APP_FILE_PATH_SPIP300="sip_212.ld"
CONFIG_FILES_SPIP300="phone1_212.cfg, sip_212.cfg"/>
    <APPLICATION_SPIP500 APP_FILE_PATH_SPIP500="sip_212.ld"
CONFIG_FILES_SPIP500="phone1_212.cfg, sip_212.cfg"/>
    <APPLICATION_SPIP301 APP_FILE_PATH_SPIP301="sip_316.ld"
CONFIG_FILES_SPIP301="phone1_316.cfg, sip_313.cfg"/>
    <APPLICATION_SPIP430 APP_FILE_PATH_SPIP430="sip_323.ld"
CONFIG_FILES_SPIP430="phone1_323.cfg, sip_323.cfg"/>
    <APPLICATION_SPIP501 APP_FILE_PATH_SPIP501="sip_316.ld"
CONFIG_FILES_SPIP501="phone1_316.cfg, sip_313.cfg"/>
    <APPLICATION_SPIP600 APP_FILE_PATH_SPIP600="sip_316.ld"
CONFIG_FILES_SPIP600="phone1_316.cfg, sip_313.cfg"/>
    <APPLICATION_SPIP601 APP_FILE_PATH_SPIP601="sip_316.ld"
CONFIG_FILES_SPIP601="phone1_316.cfg, sip_313.cfg"/>
    <APPLICATION_SSIP4000 APP_FILE_PATH_SSIP4000="sip_316.ld"
CONFIG_FILES_SSIP4000="phone1_316.cfg, sip_316.cfg"/>
    </APPLICATION>
```

Master configuration files contain the following XML attributes:

- APP_FILE_PATH—The path name of the application executable. It can have a maximum length of 255 characters. This can be a URL with its own protocol, user name and password, for example http://usr:pwd@server/dir/sip.ld.
- CONFIG_FILES—A comma-separated list of configuration files. Each file name has a maximum length of 255 characters and the list of file names has a maximum length of 2047 characters, including commas and white space. Each configuration file can be specified as a URL with its own protocol,

user name and password, for example ftp://usr:pwd@server/dir/phone2034.cfg.

- MISC_FILES—A comma-separated list of other required files. Dictionary resource files listed here will be stored in the phone's flash file system. So if the phone reboots at a time when the provisioning server is unavailable, it will still be able to load the preferred language.
- LOG_FILE_DIRECTORY—An alternative directory to use for log files if required. A URL can also be specified. This is blank by default.
- CONTACTS_DIRECTORY—An alternative directory to use for user directory files if required. A URL can also be specified. This is blank by default.
- OVERRIDES_DIRECTORY—An alternative directory to use for configuration overrides files if required. A URL can also be specified. This is blank by default.
- LICENSE_DIRECTORY—An alternative directory to use for license files if required. A URL can also be specified. This is blank by default.

Warning

The order of the configuration files listed in CONFIG_FILES is significant:

- The files are processed in the order listed (left to right).
- The same parameters may be included in more than one file.
- The parameter found first in the list of files will be the one that is effective.

This provides a convenient means of overriding the behavior of one or more phones without changing the baseline configuration files for an entire system.

For more information, refer to the "Configuration File Management on Polycom Phones" white paper at http://www.polycom.com/global/documents/support/technical/products/voice/white_paper_configuration_file_management_on_soundpoint_ip_phones.pdf .

For more information:

- Refer to "Technical Bulletin 35311: Supporting SoundPoint IP 300, 301, 430, 500, 501, 600, and 601 and SoundStation IP 4000 Phones with SIP 2.2.0 or SIP 3.2.0 or SIP 3.2.3 and Later Releases" at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .
- Refer to "Technical Bulletin 35361: Overriding Parameters in Master Configuration File on Polycom Phones" at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html.

Example 1

If you have a requirement for different application loads on different phones on the same provisioning server, you can create a variable in the master configuration file that is replaced by the MAC address of each phone when it reboots. An example is shown below:

```
    <?xml version="1.0" standalone="yes"?>
    <!-- Default Master SIP Configuration File -->
    <!-- For information on configuring Polycom VoIP phones please
refer to the -->
    <!-- Configuration File Management white paper available from: -->
    <!--
http://www.polycom.com/common/documents/whitepapers/configuration_file
_management_on_soundpoint_ip_phones.pdf -->
    <!-- $RCSfile: 000000000000.cfg,v $  $Revision: 1.21 $ -->
    < APPLICATION APP_FILE_PATH="sip[MACADDRESS].ld"
CONFIG_FILES="reg-basic[MACADDRESS].cfg, sip-basic.cfg" MISC_FILES=""
LOG FILE DIRECTORY="" OVERRIDES_DIRECTORY="" CONTACTS_DIRECTORY=""
LICENSE_DIRECTORY=""/>
```

Example 2

If you have a requirement for separate application loads on different phones on the same provisioning server, you can modify the application that is loaded when each phone reboots. An example is below:

```
    <?xml version="1.0" standalone="yes"?>
    <!-- Default Master SIP Configuration File -->
    <!-- For information on configuring Polycom VoIP phones please
refer to the -->
    <!-- Configuration File Management white paper available from: -->
    <!--
http://www.polycom.com/common/documents/whitepapers/configuration_file
_management_on_soundpoint_ip_phones.pdf -->
    <!-- $RCSfile: 000000000000.cfg,v $  $Revision: 1.21 $ -->
    < APPLICATION APP_FILE_PATH="[PHONE_PART_NUMBER].sip.ld"
CONFIG_FILES="reg-basic.cfg, sip-basic.cfg" MISC_FILES="" LOG FILE
DIRECTORY="" OVERRIDES_DIRECTORY="" CONTACTS_DIRECTORY=""
LICENSE_DIRECTORY=""/>
```

Example 3

You can also use the substitution strings PHONE_MODEL, PHONE_PART_NUMBER, MACADRESS, and PHONE_MAC_ADDRESS in the master configuration file. For more information, refer to Product, Model, and Part Number Mapping on page C-24.

You can also direct phone upgrades to a software image and configuration files based on the phone model number and part number. All XML attributes can be modified in this manner. An example is below:

```
    <?xml version="1.0" standalone="yes"?>
    <!-- Default Master SIP Configuration File -->
    <!-- For information on configuring Polycom VoIP phones please
refer to the -->
    <!-- Configuration File Management white paper available from: -->
    <!--
http://www.polycom.com/common/documents/whitepapers/configuration_file
_management_on_soundpoint_ip_phones.pdf -->
    <!-- $RCSfile: 000000000000.cfg,v $  $Revision: 1.21 $ -->
    <APPLICATION APP_FILE_PATH="sip.ld" CONFIG_FILES="reg-basic.cfg,
sip-basic.cfg" MISC_FILES="" LOG_FILE_DIRECTORY=""
OVERRIDES_DIRECTORY="" CONTACTS_DIRECTORY="" LICENSE_DIRECTORY="" />
    <APPLICATION APP_FILE_PATH_SPIP300="SPIP300.sip.ld"
CONFIG_FILES_SPIP300="phone1_SPIP300.cfg, sip_SPIP300.cfg" />
    <APPLICATION APP_FILE_PATH_SPIP500="SPIP500.sip.ld"
CONFIG_FILES_SPIP500="phone1_SPIP500.cfg, sip_SPIP500.cfg" />
```

Sample Template Files

A number of sample template files are included with the Polycom UC software 3.3.0 release. Most configuration parameters appear in only one template file; however, some do appear in two files. The precedence order (first mentioned takes effect) still applies. The template file(s) that a parameter appears in is mentioned in the next section, Configuration Parameters, and in Configuring Your System on page 4-1.

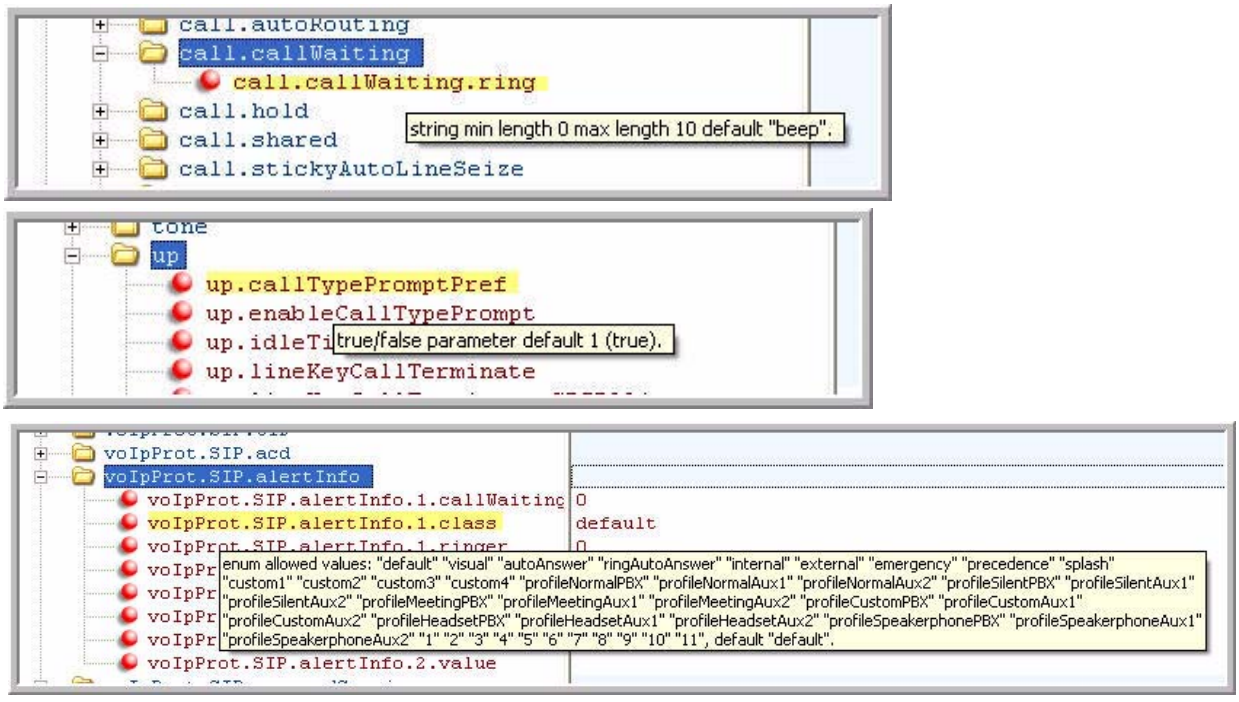
The sample template files are:

Name	Description	Deployment Scenarios
applications.cfg	For applications, browser, microbrowser, XMP-API	"Typical" Hosted Service Provider "Typical" IP-PBX
features.cfg	Features related enabling corp dir,ectory USB recording, CMA, presence, ACD, for example	"Typical" Hosted Service Provider "Typical" IP-PBX
H323.cfg	H.323 video use	"Typical" Hosted Service Provider f using VVX 1500 for video calls
reg-advanced.cfg	Advanced call server, multi-line phones	"Typical" Hosted Service Provider "Typical" IP-PBX
reg-basic.cfg	Basic registration	"Simple SIP" device "Typical" Hosted Service Provider
region.cfg	Non-North American geographies	"Typical" Hosted Service Provider "Typical" IP-PBX

Name	Description	Deployment Scenarios
sip-basic.cfg	Basic call server	“Simple SIP” device “Typical” Hosted Service Provider
sip-interop.cfg	Advanced call server, multi-line phones	“Typical” Hosted Service Provider “Typical” IP-PBX
site.cfg	Muilt-site operations	“Typical” Hosted Service Provider “Typical” IP-PBX
techsupport.cfg	Available by special request from Polycom Customer Support.	Troubleshooting
video.cfg	VVX 1500 video	“Typical” Hosted Service Provider if using VVX 1500 for video calls
video-integration.cfg	IP 7000 interoperability with Polycom HDX systems	HDX Video Integration

Along with the sample templates, an XML schema file—`polycomConfig.xsd`— is included that provides information like parameters type (boolean, integer, string, and enumerated type), permitted values, default values, and all valid enumerated type values if you view the template file in an XML editor.

For example, a string parameter and a boolean parameter are shown in the following figure.



Configuration Parameters

Note

Certain configuration parameters, previously documented in the Administrator's Guide, have been deprecated. These parameters are currently supported and may be supported in the future; however, some may be dropped in the future without prior warning.

Note

1. When certain configuration parameters are changed, a phone will reboot or restart. These parameters appear in **bold** when described in the following sections.
2. For boolean configuration parameters, the values allowed in the configuration templates are case insensitive:

   The values "0", "false", and "off" are inter-changable and supported.

   The values "1", "true", and "on" are inter-changeable and supported.

   In the following sections, only "0" and '1" are documented.
3. If a numeric parameter is set to a value outside of its valid range in a configuration file, either the maximum value will be used (if the configuration file's value is greater than the range) or the minimum value will be used (if the configuration file's value is less than the range). If a parameter's value is invalid (for example, enumerated type parameters that do not match a pre-defined value, numeric parameters that are set to a non-numeric values, string parameters that are either too long or short, or null parameters in numeric fields), the default value is used. All such situations are logged on the phone's log files.

Note

Any configuration parameters can be set up to apply to a specific phone model by appending the PHONE MODEL NUMBER descriptor to the parameter (refer to Example 3 on page A-5). For example:

```
mb.main.home="http://www.myserver.com/index.xhtml"
mb.main.home.SPIP560="http://www.myserver.com/ip560.xhtml"
mb.main.home.SSIP6000="http://172.24.44.41/"
```

All phone models except the SoundPoint IP 560 and SoundStation IP 6000 will use the myserver.com as the Microbrowser home page. The SoundPoint IP 560 will use the special ip560.html and the SoundStation IP 6000 will use the server located at 172.24.44.41 . Put the phone model at the end of parameter name.

The precedence order for configuration parameter changes is as follows (highest to lowest):

- User changes through the phone's user interface
- Web configuration through a browser
- Polycom CMA system
- Configuration files

- Default values

This section lists all possible configuration parameters in alphabetical order. These parameters include:

- <acd/>
- <apps/>
- <attendant/>
- <bg/>
- <bitmap/>
- <call/>
- <device/>
- <dialplan/>
- <dir/>
- <divert/>
- <dns/>
- <efk/>
- <feature/>
- <font/>
- <httpd/>
- <key/>
- <lcl/>
- <license/>
- <mb/>
- <msg/>
- <nat/>
- <phoneLock/>
- <pnet/>
- <powerSaving/>
- <pres/>
- <prov/>
- <qos/>
- <reg/>

- <request/>
- <roaming_buddies/>
- <roaming_privacy/>
- <saf/>
- <se/>
- <sec/>
- <softkey/>
- <tcpIpApp/>
- <tones/>
- <up/>
- <video/>
- <voice/>
- <voIpProt/>

<acd/>

Both SIP-B Automatic Call Distribution and Feature Synchronized Automatic Call Distribution features use this parameter.

This configuration parameter is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
acd.reg	1 to 34	1	The registration index used to support BroadSoft server-based ACD.
acd.stateAtSignIn	0 or 1	1	The state of the user when signing in. If set to 1, the user is available. If set to 0, the user is unavailable.

<apps/>

This attribute's settings control the telephone notification events, state polling events, and the push server controls. For more information, refer to the *Web Application Developer's Guide,* which can be found at http://www.polycom.com/voicedocumentation/.

This attribute also includes:

- <telNotification/>
- <statePolling/>
- <push/>

<telNotification/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
apps.telNotification. incomingEvent	0 or 1	0	If set to 0, incoming call notification is disabled. If set to 1, incoming call notification is enabled.
apps.telNotification. lineRegistrationEvent	0 or 1	0	If set to 0, line registration notification is disabled. If set to 1, line registration notification is enabled.
apps.telNotification. offhookEvent	0 or 1	0	If set to 0, offhook notification is disabled. If set to 1, offhook notification is enabled.
apps.telNotification. onhookEvent	0 or 1	0	If set to 0, onhook notification is disabled. If set to 1, onhook notification is enabled.
apps.telNotification. outgoingEvent	0 or 1	0	If set to 0, outgoing call notification is disabled. If set to 1, outgoing call notification is enabled.
apps.telNotification.x. URL	URL	Null	The URL to which the phone sends notifications of specified events, where x 1 to 9. The protocol used can be either HTTP or HTTPS.

<statePolling/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
apps.statePolling. password	string	Null	The password to access the state polling URL.
apps.statePolling. username	string	Null	The user name to access the state polling URL..
apps.statePolling.URL	URL	Null	The URL to which the phone sends call processing state/device/network information. The protocol used can be either HTTP or HTTPS. ***Note**: To enable state polling, the attributes `apps.statePolling.URL`, `apps.statePolling.username`, and `apps.statePolling.password` must be set to non-Null values*.

<push/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
apps.push.alertSound	0 or 1	0	Flag to determine whether or not there is a sound when an alert is pushed.
apps.push.messageType	0 to 3	0	Select the allowable push priority messages on phone. The values are: • 0: (None) Discard push messages • 1: (Critical) Allows only critical push messages • 2: (Normal) Allows only normal push messages • 3: (Both) Allows both critical and normal push messages
apps.push.password	string	Null	The password to access the push server URL.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
apps.push. serverRootURL	URL	Null	The relative URL (received from HTTP URL Push message) is appended to the application server root URL and the resultant URL is sent to the Microbrowser. For example, if the application server root URL is http://172.24.128.85:8080/sampleapps and the relative URL is /examples/sample.html, the URL that is sent to the Microbrowser is http://172.24.128.85:8080/sampleapps/examples/sample.html. The protocol used can be either HTTP or HTTPS.
apps.push.username	string	Null	The user name to access the push server URL. ***Note**: To enable the push functionality, the attributes `apps.push.username` and `apps.push.password` must be set to non-Null values.*

<attendant/>

Note These attributes are available on SoundPoint IP 32x/33x, 450, 550, 560, 650, and 670 phones only.

The Busy Lamp Field (BLF) / attendant console feature enhances support for a phone-based attendant console.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
attendant.reg	positive integer	1	For attendant console / BLF feature. This is the index of the registration which will be used to send a SUBSCRIBE to the list SIP URI specified in attendant.uri. For example, `attendant.reg = 2` means the second registration will be used.
attendant.ringType	enumerated type Refer to **reg-advanced.cfg**	ringer1	The ring tone to play when a BLF dialog is in the offering state.
attendant.uri	string	Null	For attendant console / busy lamp field (BLF) feature. This specifies the list SIP URI on the server. If this is just a user part, the URI is constructed with the server host name/IP. ***Note**: If `attendant.uri` is set, then the individually addressed users configured by `attendant.resourceList` and `attendant.behaviors` attributes are ignored.*

This attribute also includes:

- <resourceList/>
- <behaviors/>

<resourceList/>

In the following table, x is the monitored user number. For IP 450: x=1-2; IP 550, IP 560: X=1-3; IP 650, IP 670: x=1-47.

This configuration attribute is defined as follows:

Attribute	Permitted Values	Default	Interpretation
attendant.resourceList.x.address	string that constitutes a valid SIP URI (sip:6416@polycom.com) or contains the user part of a SIP URI (6416)	Null	The user referenced by `attendant.reg=""` will subscribe to this URI for dialog. If a user part is present, the phone will subscribe to a sip URI constructed from user part and the domain of the user referenced by `attendant.reg`.

Attribute	Permitted Values	Default	Interpretation
attendant.resourceList.x.label	UTF-8 encoded string	Null	Text label to appear on the display adjacent to the associated line key. If set to Null, the label will be derived from the user part of `attendant.resourceList.x.address` .
attendant.resourceList.x.type	"normal" or "automata"	“normal”	Type of resource being monitored. If set to **normal**, the default action when pressing the line key adjacent to this monitored user is to initiate a call if the user is idle or busy and to perform a directed call pickup if the user is ringing. Any active calls are first placed on hold. If set to **automata**, the default action when pressing the line key adjacent to this monitored user is to perform a park/blind transfer of any currently active call. If there is no active call and the monitored user is ringing/busy, an attempt to perform a directed call pickup/park retrieval is made.

<behaviors/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
attendant.behaviors.display. spontaneousCallAppearances.normal	0 or 1	1	A flag to determine whether or not a call appearance is spontaneously presented to the attendant when calls are alerting on a monitored resource. The information displayed after a press-and-hold of a resource's line key is unchanged by this parameter. If set to 1, the display is enabled.
attendant.behaviors.display. spontaneousCallAppearances.automata	0 or 1	0	
attendant.behaviors.display. remoteCallerID.normal	0 or 1	1	A flag to determine whether or not remote party caller ID information is presented to the attendant. If set to 0 (disabled), the string "unknown" would be substituted for both name and number information.
attendant.behaviors.display. remoteCallerID.automata	0 or 1	1	

<bg/>

The backgrounds used by the SoundPoint IP 450, 550, 560, 650, and 670 and the Polycom VVX 1500 phones are defined in this section. In the following table, *w*=1 to 3, *x*=1 to 6. `hiRes` parameters are used by SoundPoint IP 550, 560, 650, and 670 phones, `medRes` parameters are used by SoundPoint IP 450 phones, and VVX_1500 parameters are used by Polycom VVX 1500 phones.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	**Permitted Values**	**Default**	**Interpretation**
bg.VVX_1500.color.selection	w,x	1,1	Specify which type of background (w) and index for that type (x) is selected on reboot where w=1 to 3, x=1 to 6. The type of backgrounds are built-in (w=1), solids (w=2), and bitmaps (w=3). w=2 is used when selecting any image as a background. w=3 is used when selecting any image from the Digital Picture Frame as a background. This image is stored under "Local File". Only one local file at a time is supported.
bg.VVX_1500.color.bm.x.name	any string	Null	Graphic files for display on the phone. For example, if you set `bg.VVX_1500.color.bm.1.name` to **Polycom.bmp**, the user will be able to select "Polycom.bmp" as a background on the phone.
bg.hiRes.color.selection	w,x	1,1	Specify which type of background (w) and index for that type (x) is selected on reboot where w=1 to 3, x=1 to 6.
bg.hiRes.color.pat.solid.x. name	any string		Solid pattern name. For x=1: Light Blue, x=2: Teal, x=3: Tan, x=4:Null
bg.hiRes.color.pat.solid.x.red	0 to 255		The screen background layouts. For x=1, red (151), green, (207), blue (249) For x=2, red (73), green (148), blue (148) For x=3, red (245), green (157), blue (69) For x=4, red (Null), green (Null), blue (Null)
bg.hiRes.color.pat.solid.x. green	0 to 255		
bg.hiRes.color.pat.solid.x.blue	0 to 255		

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
bg.hiRes.color.bm.x.name	any string	built-in value of "Thistle"	Graphic files for display on the phone and Expansion Module. For x=1: • name is "Leaf.jpg" name is "LeafEM.jpg" For x=2: • name is "Sailboat.jpg" name is "SailboatEM.jpg" For x=3: • name is "Beach.jpg" name is "BeachEM.jpg" For x=4: • name is "Palm.jpg" name is "PalmEM.jpg" For x=5: • name is "Jellyfish.jpg" name is "JellyfishEM.jpg" For x=6: • name is "Mountain.jpg" name is "MountainEM.jpg" ***Note:*** *If the file is missing or unavailable, the built-in default solid pattern is displayed.*
bg.hiRes.color.bm.x.em.name	any string		
bg.hiRes.gray.selection	w,x	2,1	Specify which type of background (w) and index (x) for that type is selected on reboot.
bg.hiRes.gray.pat.solid.x.name	any string	White	Solid pattern name. For x=1: White, x=2: Light Gray, x=3, 4: Null
bg.hiRes.gray.pat.solid.x.red	0 to 255		The screen background layouts. For x=1, red (255), green, (255), blue (255) For x=2, red (160), green (160), blue (160) For x=3 and 4, all values are Null. ***Note****: The values for red, green, and blue must be the same to display correctly on grayscale.*
bg.hiRes.gray.pat.solid.x.green	0 to 255		
bg.hiRes.gray.pat.solid.x.blue	0 to 255		

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
bg.hiRes.gray.bm.x.name	any string		Graphic files for display on the phone and Expansion Module and also the brightness adjustment to the graphic. For x=1: • name is "Leaf.jpg" name is "LeafEM.jpg" adjustment is "0" For x=2: • name is "Sailboat.jpg" name is "SailboatEM.jpg" adjustment is "-3" For x=3: • name is "Beach.jpg" name is "BeachEM.jpg" adjustment is "0" For x=4: • name is "Palm.jpg" name is "PalmEM.jpg" adjustment is "-3" For x=5: • name is "Jellyfish.jpg" name is "JellyfishEM.jpg" adjustment is "-2" For x=6: • name is "Mountain.jpg" name is "MountainEM.jpg" adjustment is "0" ***Note:*** *If the file is missing or unavailable, the built-in default solid pattern is displayed.* ***Note:*** *The adjustment value is changed on each individual phone when the user lightens or darkens the graphic during preview.*
bg.hiRes.gray.bm.x.em.name	any string		
bg.hiRes.gray.bm.x.adj	integer		
bg.medRes.gray.selection	w,x	2,1	Specify which type of background (w) and index (x) for that type is selected on reboot.
bg.medRes.gray.pr.x.adj		-3	Specify the brightness adjustment to the graphic.
bg.medRes.gray.pat.solid.x. name	any string	White	Solid pattern name. For x=1: White, x=2: Light Gray, x=3, 4: Null

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
bg.medRes.gray.pat.solid.x.red	0 to 255		The screen background layouts. For x=1, red (255), green, (255), blue (255) For x=2, red (160), green (160), blue (160) For x=3 and 4, all values are Null. ***Note**: The values for red, green, and blue must be the same to display correctly on grayscale.*
bg.medRes.gray.pat.solid.x. green	0 to 255		
bg.medRes.gray.pat.solid.x. blue	0 to 255		
bg.medRes.gray.bm.x.name	any string		Graphic files for display on the phone and Expansion Module and also the brightness adjustment to the graphic. For x=1: • name is “Leaf256x116.jpg” adjustment is “0” For x=2: • name is “Sailboat256x116.jpg” adjustment is “-3” For x=3: • name is “Beach256x116.jpg” adjustment is “0” For x=4: • name is “Palm256x116.jpg” adjustment is “-3” For x=5: • name is “Jellyfish256x116.jpg” adjustment is “-2” For x=6: • name is “Mountain256x116.jpg” adjustment is “0” ***Note:** If the file is missing or unavailable, the built-in default solid pattern is displayed.* ***Note:** The adjustment value is changed on each individual phone when the user lightens or darkens the graphic during preview.*
bg.medRes.gray.bm.x.em. name	any string		
bg.medRes.gray.bm.x.adj	integer		

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
button.color.selection.x.y. modify	any string		The label color for soft keys and line key labels associated with the defined colored backgrounds. These values can be modified locally by the user. The format is: "rgbHILo, <parameter list>". For example: "rbgHiLo, 51, 255, 68, 255, 0, 119" is the default button color associated with the built-in background.
button.gray.selection.x.y. modify	any string		The label color for soft keys and line key labels associated with the defined gray backgrounds. These values can be modified locally by the user. The format is: "rgbHILo, <parameter list>". By default, all defaults are set to "none".

<bitmap/>

The idle display bitmaps used by all phone are defined in this section.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
bitmap.idleDisplay. name	string	Idle display bitmap name.

If you want different bitmaps on different phones, additional model-specific parameters must be created. For example:

```
bitmap.idleDisplay.name=bg1.bmp
bitmap.idleDisplay.name.SPIP670=bg2.bmp
bitmap.idleDisplay.name.SSIP7000=bg3.bmp
bitmap.idleDisplay.name.SPIP331=bg4.bmp
```

The SoundPoint IP 670 would use "bg2", the SoundStation IP 7000 would use "bg3", the SoundPoint IP 331 would use "bg4", and all other phones would use "bg1".

<call/>

This per-site and per-phone configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.autoRouting. preferredProtocol	“SIP or “H323”	SIP	If set to **SIP**, calls are placed via SIP if available, or via H.323 if SIP is not available. If set to **H323**, calls are placed via H.323 if available, or via SIP if H.323 is not available. ***Note**: This parameter is supported on the Polycom VVX 1500 only.*
call.autoRouting.preference	“line” or “protocol”	“line	If set to **line**, calls are placed via the first available line, regardless of its protocol capabilities. If the first available line has both SIP and H.323 capabilities, the preferred protocol will be used preferentially (`call.autoRouting.preferredProtocol`). If set to **protocol**, the first available line with the preferred protocol activated is used, if available, and if not available, the first available line will be used. ***Note**: Auto-routing is used when manual routing selection features are disabled. Refer to <up/> on page A-120.* ***Note**: This parameter is supported on the Polycom VVX 1500 only.*
call.callsPerLineKey	1 to 24 OR 1 to 8	24, 8 OR 4	For the SoundPoint IP 550, 560, 650, and 670, the permitted range is 1 to 24 and the default is 24. For the SoundPoint IP 32x/33x, the permitted range is 1 to 8 and the default is 4. For all other phones, the permitted range is 1 to 8 and the default is 8. This is the number of calls that may be active or on hold per line key on the phone. Note that this may be overridden by the per-registration attribute of `reg.x.callsPerLineKey`. Refer to <reg/> on page A-82.
call.dialtoneTimeOut	positive integer	60	Time in seconds to allow the dial tone to be played before dropping the call. If set to 0, the call is not dropped.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.directedCallPickupMethod	"native" or "legacy"	Null	The method the phone will use to perform a directed call pick-up of a BLF resource's inbound ringing call. "native" indicates the phone will use a native protocol method (in this case SIP INVITE with the Replaces header [4]). "legacy" indicates the phone will use the method specified in `call.directedCallPickupString`.
call.directedCallPickupString	star code	*97	The star code to initiate a directed call pickup. ***Note:*** *The default value supports the BroadWorks calls server only. You must change the value if your organization uses a different call server.*
call.enableOnNotRegistered	0 or 1	1	If set to 1, calls will be allowed when the phone is not successfully registered, otherwise, calls will not be permitted without a valid registration. ***Note****: Setting this parameter to 1 can allow Polycom VVX 1500 phones to make calls using the H.323 protocol even though an H.323 gatekeeper is not configured*.
call.lastCallReturnString	string of maximum length 32	*69	The string sent to the server when the user selects the "last call return" action.
call.localConferenceCallHold	0 or 1	0	If set to 0, a hold will happen for all legs when conference is put on hold. (old behavior). If set to 1, only the host is out of the conference, all other parties in conference continue to talk. (new behavior). Only supported for the SoundPoint IP 550, 560,650 and 670 and the SoundStation IP 7000 with an appropriate license (refer to Manage Conferences on page 4-22). For all others, set to 0.
call.offeringTimeOut	positive integer	60	Time in seconds to allow an incoming call to ring before dropping the call, 0=infinite. ***Note:*** *The call diversion, no answer feature will take precedence over this feature if enabled. For more information, refer to <noanswer/> on page A-50.*

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.parkedCallRetrieveMethod	“native” or “legacy”	Null	The method the phone will use to retrieve a BLF resource's call which has dialog state confirmed. “native” indicates the phone will use a native protocol method (in this case SIP INVITE with the Replaces header [4]). “legacy” indicates the phone will use the method specified in `call.parkedCallRetrieveString` .
call.parkedCallRetrieveString	star code	Null	The star code used to initiate retrieve of a parked call.
call.rejectBusyOnDnd	0 or 1	1	If set to 1, reject all incoming calls with the reason “busy” if do-not-disturb is enabled. ***Note:*** *This attribute is ignored when the line is configured as shared. The reason being that even though one party has turned on DND, the other person/people sharing that line do not necessarily want all calls to that number diverted away.* ***Note:*** *If server-based DND is enabled, this parameter is disabled*.
call.ringBackTimeOut	positive integer	60	Time in seconds to allow an outgoing call to remain in the ringback state before dropping the call, 0=infinite.
call. singleKeyPressConference	0 or 1	0	If set to 1, the conference will be setup after a user presses the **Conference** soft key or **Conference** key the first time. Also, all sound effects (dial tone, DTMF tone while dialing and ringing back) are heard by all existing participants in the conference. If set to 0, sound effects are only heard by conference initiator (original behavior). ***Note****: Only supported for SoundPoint IP 550, 560,650 and 670 and SoundStation IP 7000. For all others, set to 0.*

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.stickyAutoLineSeize	0 or 1	0	If set to 1, makes the phone use "sticky" line seize behavior. This will help with features that need a second call object to work with. The phone will attempt to initiate a new outgoing call on the same SIP line that is currently in focus on the LCD (this was the behavior in SIP 1.6.5). Dialing through the call list when there is no active call will use the line index for the previous call. Dialing through the call list when there is an active call will use the current active call line index. Dialing through the contact directory will use the current active call line index. If set to 0, the feature is disabled (this was the behavior in SIP 1.6.6). Dialing through the call list will use the line index for the previous call. Dialing through the contact directory will use a random line index. ***Note:*** *This may fail due to glare issues in which case the phone may select a different available line for the call.*
call.stickyAutoLineSeize.onHookDialing	0 or 1	0	If `call.stickyAutoLineSeize` is set to 1, this parameter has no effect. The regular stickyAutoLineSeize behavior is followed. If `call.stickyAutoLineSeize` is set to 0 and this parameter is set to 1, this overrides the stickyAutoLineSeize behavior for hot dial only. (Any new call scenario seizes the next available line.) If `call.stickyAutoLineSeize` is set to 0 and this parameter is set to 0, there is no difference between hot dial and new call scenarios. ***Note****: A hot dial occurs on the line which is currently in the call appearance. Any new call scenario seizes the next available line.*
call.transferOnConferenceEnd	0 or 1	1	Flag to determine whether or not to leave other parties connected when the conference host exits the conference. If set to 1, other parties are left connected (the previous behaviour). If set to 0, all parties are disconnected from the conference.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.transfer.blindPreferred	0 or 1	0	If set to 1, the blind transfer is the default mode. The **Normal** soft key is available to switch to a consultative transfer. If set to 0, the consultative transfer is the default mode. The **Blind** soft key is available to switch to a blind transfer. ***Note:*** *This parameter is supported on the SoundPoint IP 32x/33x only.*
call.urlModeDialing	0 or 1	0	Flag to determine if URL dialing is enabled or disabled.

This attribute also includes:

- <autoAnswer>
- <shared/>
- <hold/><localReminder/>
- <donotdisturb/>
- <autoOffHook/>
- <serverMissedCall/>
- <missedCallTracking/>
- <callWaiting/>

<autoAnswer>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.autoAnswer.H323	0 or 1	0	If set to 1, auto-answer is enabled for all H.323 calls. ***Note****: This parameter is supported on the Polycom VVX 1500 only.*
call.autoAnswer.micMute	0 or 1	1	If set to 1, the microphone is initially muted after a call is auto-answered.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.autoAnswer.ringClass	enumerated type Refer to **reg-advanced.cfg**	ringAutoAnswer	The ring class (`se.rt.x`) to use when a call is to be automatically answered using the auto-answer feature. If set to a ring class with a type other than "answer" or "ring-answer", the setting will be overridden such that a ring type of "visual" (no ringer) applies.
call.autoAnswer.SIP	0 or 1	0	If set to 1, auto-answer is enabled for all SIP calls. ***Note**: This parameter is supported on the Polycom VVX 1500 only.*
call.autoAnswer.videoMute	0 or 1	0	If set to 1, video Tx is initially disabled after a call is auto-answered. ***Note**: This parameter is supported on the Polycom VVX 1500 only.*

<shared/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.shared.disableDivert	0 or 1	1	If set to 1, disable diversion feature for shared lines. ***Note:** This feature is disabled on most call servers*.
call.shared.exposeAutoHolds	0 or 1	0	If set to 1, on a shared line, when setting up a conference, a re-INVITE will be sent to the server. If set to 0, no re-INVITE will be sent to the server.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.shared.oneTouchResume	0 or 1	0	If set to 1, when a shared line has a call on hold the remote user can press that line and resume the call. If more than one call is on hold on the line then the first one will be selected and resumed automatically. If set to 0, pressing the shared line will bring up a list of the calls on that line and the user can select which call the next action should be applied to. ***Note:*** *This parameter affects the SoundStation IP 5000, 6000, and 7000 phones. For other phones, a quick press and release of the line key will resume a call whereas pressing and holding down the line key will show a list of calls on that line.*
call.shared.seizeFailReorder	0 or 1	1	If set to 1, play re-order tone locally on shared line seize failure.

<hold/><localReminder/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.hold.localReminder.enabled	0 or 1	0	If set to 1, periodically notify the local user that calls have been on hold for an extended period of time.
call.hold.localReminder.period	non-negative integer	60	Time in seconds between subsequent reminders.
call.hold.localReminder.startDelay	non-negative integer	90	Time in seconds to wait before the initial reminder.

<donotdisturb/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.donotdisturb.perReg	0 or 1	0	If set to 1, the DND feature will allow selection of DND on a per-registration basis. ***NOTE:*** *If* `voIpProt.SIP.serverFeatureControl.dnd` *is set to 1 (enabled), this parameter is ignored. For more information, refer to* *<SIP/> on page A-147.*

<autoOffHook/>

An optional per-registration feature is supported which allows automatic call placement when the phone goes off-hook.

In the following table, *x* is the registration number. IP 32x/33x: *x*=1-2; IP 450: *x*=1-3; IP 550, 560: *x*=1-4; VVX 1500: *x*=1-6; IP 650, 670: *x*=1-34; IP 5000, 6000, 7000: *x*=1.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.autoOffHook.x.contact	ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)	Null	If set to 1, a call will be automatically placed to the contact specified upon going off-hook on this registration.
call.autoOffHook.x.enabled	0 or 1	0	
call.autoOffHook.x.protocol	"SIP" or "H323"	Null	On a dual-protocol line only, specifies the routing protocol to use for the auto off-hook dialing. The strings are case sensitive. If set to Null, the value of `call.autoRouting.preferredProtocol` is used. ***Note****: If a line is single-protocol configured, the configured protocol will be used in the auto off-hook dialing and any value in its* `call.autoOffHook.x.protocol` *field will be ignored.*

<serverMissedCall/>

The phone supports a per-registration configuration of which events will cause the locally displayed "missed calls" counter to be incremented.

In the following table, *x* is the registration number. IP 32x/33x: *x*=1-2; IP 450: *x*=1-3; IP 550, 560: *x*=1-4; VVX 1500: *x*=1-6; IP 650, 670: *x*=1-34; IP 5000, 6000, 7000: *x*=1.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.serverMissedCall.x.enabled	0 or 1	0	If set to 0, all missed-call events will increment the counter. If set to 1, only missed-call events sent by the server will increment the counter. ***NOTE:*** *This feature is supported with the BroadSoft® Synergy (used to be Sylantro) call server only.*

<missedCallTracking/>

You can enable/disable missed call tracking on a per-line basis.

In the following table, *x* is the registration number. IP 32x/33x: *x*=1-2; IP 450: *x*=1-3; IP 550, 560: *x*=1-4; VVX 1500: *x*=1-6; IP 650, 670: *x*=1-34; IP 5000, 6000, 7000: *x*=1.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.missedCallTracking.x.enabled	0 or 1	1	If set to 1, missed call tracking is enabled. If `call.missedCallTracking.x.enabled` is set to 0, then missedCall counter is not updated regardless of what `call.serverMissedCalls.x.enabled` is set to (and regardless of how the server is configured). There is no Missed Call List provided under Menu > Features of the phone. If `call.missedCallTracking.x.enabled` is set to 1 and call.serverMissedCalls.x.enabled is set to 0, then the number of missedCall counter is incremented regardless of how the server is configured. If `call.missedCallTracking.x.enabled` is set to 1 and `call.serverMissedCalls.x.enabled` is set to 1, then the handling of missedCalls depends on how the server is configured.

<callWaiting/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
call.callWaiting.ring	beep, ring, silent	beep	Specifies the ring tone heard on an incoming call when another call is active. If set to Null, the default value is beep.

<device/>

Any field in the BootROM setup menu and the application Line Configuration and Call Server Configuration menus can be set through a configuration file.

A DHCP server can be configured to point the phones to a provisioning server that has the required configuration files. The new settings will be downloaded by the phones and used to configure them. This removes the need for manual interaction with phones to configure basic settings. This is especially useful for initial installation of multiple phones.

These device settings are detected when the application starts. If the new settings would normally cause a reboot if they were changed in the application Network Configuration menu, then they will cause a reboot when the application starts.

The global `device.set` parameter must be enabled to use any `<device/>` parameters.

Two `device` parameters exist for every configuration parameter—`device.xxx` and `device.xxx.set`. If `device.xxx.set` is 1, the device.xxx value is used; otherwise it is not used. For example, if `device.auth.localAdminPassword.set` = 1, then the value in the `device.auth.localAdminPassword` field is used.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.auth. localAdminPassword	string	Null	The phone's local administrator password.
device.auth. localUserPassword	string	Null	The phone user's local password.
device.cma.mode	string	Null	Determine how the phone should retrieve the Polycom CMA server IP address. The possible values are: • "auto" . The phone must use SRV lookup to find the Polycom CMA server IP address. • "disabled". The Polycom CMA server is not contacted. • "static". The Polycom CMA server name or IP address is specified in `device.cma.serverName` .
device.cma.serverName	string	Null	Polycom CMA server name or IP address.
device.dhcp.bootSrvOpt	string	Null	For descriptions, refer to "DHCP Menu" in DHCP Menu on page 3-8.
device.dhcp. bootSrvOptType	string	Null	
device.dhcp. bootSrvUseOpt	string	Null	
device.dhcp.enabled	string	Null	
device.dhcp. offerTimeout	string	Null	
device.dhcp. option60Type	string	Null	
device.dhcp. dhcpVlanDiscUseOpt	string	Null	
device.dhcp. dhcpVlanDiscOpt	string	Null	
device.dns. altSrvAddress	string	Null	Secondary server to which the phone directs Domain Name System queries.
device.dns.domain	string	Null	The phone's DNS domain.
device.dns. serverAddress	string	Null	Primary server to which the phone directs Domain Name System queries.
device.em.power	string	Null	Refer to the EM Power parameter in Main Menu on page 3-7.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.logincred.domain	string	Null	The CMA account domain.
device.logincred. password	string	Null	The CMA account password.
device.logincred.user	string	Null	The CMA account username.
device.net.cdpEnabled	string	Null	If set to 1, the phone will attempt to determine its VLAN ID and negotiate power through CDP.
device.net. ether1000BTClockLAN	string	Null	Refer to the Ethernet parameters in Ethernet Menu on page 3-12.
device.net. ether1000BTClockPC	string	Null	
device.net. etherModeLAN	string	Null	
device.net.etherModePC	string	Null	
device.net. etherStormFilter	string	Null	
device.net. etherVlanFilter	string	Null	
device.net.ipAddress	string	Null	
device.net.IPgateway	string	Null	
device.net.lldpEnabled	string	Null	If set to 1, the phone will attempt to determine its VLAN ID and negotiate power through LLDP. If set to 0, the phone will not attempt to determine its VLAN ID or power management through LLDP.
device.net.subnetMask	string	Null	Refer to the Subnet Mask parameter in Main Menu on page 3-7.
device.net.vlanId	string	Null	Refer to the VLAN ID parameter in Main Menu on page 3-7.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.prov. appProvString	string	Null	For descriptions, refer to Server Menu on page 3-11.
device.prov. appProvType	string	Null	
device.prov.clinkEnabled	string	Null	
device.prov. maxRedunServers	string	Null	
device.prov. networkEnviornment	string	Null	
device.prov.password	string	Null	
device.prov. redunAttemptLimit	string	Null	
device.prov. redunInterAttemptDelay	string	Null	
device.prov.serverName	string	Null	
device.prov.serverType	string	Null	
device.prov.tagSerialNo	string	Null	
device.prov.user	string	Null	
device.sec. configEncryption.key	string	Null	Configuration encryption key that is used for encryption of configuration files.
device.sec. deviceCertEnabled	string	Null	Flag to determine whether or not a device certificate is installed on the phone.
device.sec.SSL.certList	string	Null	The type of certificate list.
device.sec.SSL. customCert	string	Null	The certificate value.
device.sntp.gmtOffset	string	Null	GMT offset in seconds, corresponding to -12 to +13 hours.
device.sntp.serverName	string	Null	Dotted-decimal IP address or domain name string. SNTP server from which the phone will obtain the current time.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.syslog.facility	string	Null	Refer to the Ethernet parameters in Syslog Menu on page 3-13.
device.syslog. prependMac	string	Null	
device.syslog. renderLevel	string	Null	
device.syslog. serverName	string	Null	
device.syslog.transport	string	Null	

<dialplan/>

Note The dial plan is not applied against Placed Call List, VoiceMail, last call return, remote control dialed numbers, and on-hook dialing.

This per-site configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dialplan.applyToCallListDial	0 or 1	1	This attribute covers dialing from Received Call List and Missed Call List including dialing from Edit or Info sub-menus. If set to 0, the digit map replacement operations are not applied against the dialed number. if set to 1, the digit map replacement operations are applied against the dialed number.
dialplan.applyToDirectoryDial	0 or 1	0	This attribute covers dialing from Directory as well as Speed Dial List. Value interpretation is the same as for `dialplan.applyToCallListDial`. ***Note:*** *An Auto Call Contact number is considered a dial from directory.*

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dialplan.applyToRemoteDialing	0 or 1	0	A flag to determine if the dial plan applies to for calls made through the Polycom HDX or SoundStructure systems. If set to 1, the dial plan applies. If set to 0, the dial plan does not apply.
dialplan.applyToTelUriDial	0 or 1	1	A flag to determine if the dial plan applies to uses of the tel:// URI. If set to 1, the dial plan applies. If set to 0, the dial plan does not apply.
dialplan.applyToUserDial	0 or 1	1	This attribute covers the case when the user presses the **Dial** soft key to send dialed number when in idle state display. Value interpretation is the same as for `dialplan.applyToCallListDial.`
dialplan.applyToUserSend	0 or 1	1	This attribute covers the case when the user presses the **Send** soft key to send the dialed number. Value interpretation is the same as for `dialplan.applyToCallListDial.`
dialplan.filterNonDigitUriUsers	0 or 1	0	If set to 1, filter out + (this is the previous behavior.) If set to 0, filter the same as with 0, but allow + .
dialplan. impossibleMatchHandling	0, 1 or 2	0	Affects digits entered while in dial mode. For example, the digits are affected after a user has picked up the handset, headset, or pressed the dial key, and not when hot dialing, contact dialing, or call list dialing. If set to 0, the digits entered up to and including the point where an impossible match occurred are sent to the server immediately. If set to 1, give reorder tone. If set to 2, allow user to accumulate digits and dispatch call manually with the Send soft key.
dialplan.removeEndOfDial	0 or 1	1	If set to 1, strip trailing # digit from digits sent out.

Per-registration dial plan configuration is also supported.

In the following table, *x* is the registration number: For IP 32x/33x: *x*=1-2; IP 450: *x*=1-3; IP 550, 560: *x*=1-4; VVX 1500: *x*=1-6; IP 650, 670: *x*=1-34; IP 5000, IP 6000, IP 7000: *x*=1.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dialplan.x.applyToCallListDial	0 or 1	1	When present, and if `dialplan.x.digitmap` is not Null, this attribute overrides `dialplan.applyToCallListDial` . For interpretation, refer to <dialplan/> on page A-34.
dialplan.x.applyToDirectoryDial	0 or 1	0	When present, and if `dialplan.x.digitmap` is not Null, this attribute overrides `dialplan.applyToDirectoryDial` . For interpretation, refer to <dialplan/> on page A-34.
dialplan.x.applyToTelUriDial	0 or 1	1	When present, and if `dialplan.x.digitmap` is not Null, this attribute overrides `dialplan.applyToTelUriDial` . For interpretation, refer to <dialplan/> on page A-34.
dialplan.x.applyToUserDial	0 or 1	1	When present, and if `dialplan.x.digitmap` is not Null, this attribute overrides `dialplan.applyToUserDial` . For interpretation, refer to <dialplan/> on page A-34.
dialplan.x.applyToUserSend	0 or 1	1	When present, and if `dialplan.x.digitmap` is not Null, this attribute overrides `dialplan.applyToUserSend` . For interpretation, refer to <dialplan/> on page A-34.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dialplan.x. impossibleMatchHandling	0, 1 or 2	0	When present, and if `dialplan.x.digitmap` is not Null, this attribute overrides `dialplan.impossibleMatchHandling` . For interpretation, refer to <dialplan/> on page A-34.
dialplan.x.removeEndOfDial	0 or 1	1	When present, and if `dialplan.x.digitmap` is not Null, this attribute overrides `dialplan.removeEndOfDial` . For interpretation, refer to <dialplan/> on page A-34.

This attribute also includes:

- <digitmap/>
- <routing/>

<digitmap/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dialplan.digitmap	string compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435. String is limited to 768 bytes and 30 segments; a comma is also allowed; when reached in the digit map, a comma will turn dial tone back on;'+' is allowed as a valid digit; extension letter 'R' is used as defined above.	[2-9]11|0T| +011xxx.T| 0[2-9]xxxxxxxxx| +1[2-9]xxxxxxxx| [2-9]xxxxxxxxx| [2-9]xxxT	When this attribute is present, number-only dialing during the setup phase of new calls will be compared against the patterns therein and if a match is found, the call will be initiated automatically eliminating the need to press Send. Attributes `dialplan.applyToCallListDial`, `dialplan.applyToDirectoryDial`, `dialplan.applyToUserDial`, and `dialplan.applyToUserSend` control the use of match and replace in the dialed number in the different scenarios.
dialplan.digitmap.timeOut	string of positive integers separated by '|'	3 | 3 | 3 | 3 | 3 | 3	Timeout in seconds for each segment of digit map. ***Note:*** *If there are more digit maps than timeout values, the default value of 3 will be used. If there are more timeout values than digit maps, the extra timeout values are ignored.*

Per-registration digit map configuration is also supported.

In the following table, *x* is the registration number: For IP 32x/33x: *x*=1-2; IP 450: *x*=1-3; IP 550, 560: *x*=1-4; VVX 1500: *x*=1-6; IP 650, 670: *x*=1-34; IP 5000, IP 6000, IP 7000: *x*=1.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	**Permitted Values**	**Default**	**Interpretation**
dialplan.x.digitmap	A string compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435; string is limited to 768 bytes and 30 segments; a comma is also allowed; a comma is also allowed; when reached in the digit map, a comma will turn dial tone back on;'+' is allowed as a valid digit; extension letter 'R' is used as defined above.	Null	When present, this attribute overrides `dialplan.digitmap` .
dialplan.x.digitmap.timeOut	string of positive integers separated by '|'	Null	When present, and if `dialplan.x.digitmap` is not Null, this attribute overrides `dialplan.digitmap.timeOut` .

<routing/>

This attribute allows the user to create a specific routing path for outgoing SIP calls independent of other "default" configurations.

This attribute also includes:

- <server/>
- <emergency/>

<server/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dialplan.routing.server.x. address	dotted-decimal IP address or host name	Null	IP address or host name and port of a SIP server that will be used for routing calls. Multiple servers can be listed starting with x=1 to 4 for fault tolerance.
dialplan.routing.server.x. port	1 to 65535	5060	
dialplan.routing.server.x. transport	DNSnaptr OR TCPpreferred OR UDPOnly OR TLS OR TCPOnly	DNSnaptr	The dnslook up of the first server to be dialed will be used, if there is a conflict with the others. For example, if `dialplan.routing.server.1.transport="UDPOnly"` and `dialplan.routing.server.2.transport = "TLS"`, then "UDPOnly" is used.

Per-registration routing server configuration is also supported.

In the following tables, *x* is the registration number: For IP 32x/33x: *x*=1-2; IP 450: *x*=1-3; IP 550, 560: *x*=1-4; VVX 1500: *x*=1-6; IP 650, 670: *x*=1-34; IP 5000, IP 6000, IP 7000: *x*=1. *y* is the index of the server.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	**Permitted Values**	**Default**	**Interpretation**
dialplan.x.routing.server.y. address	dotted-decimal IP address or host name	Null	IP address or host name and port of a SIP server that will be used for routing calls. Multiple servers can be listed starting with y=1 to 4 for fault tolerance.
dialplan.x.routing.serveryx. port	1 to 65535	5060	
dialplan.x.routing.server.y. transport	DNSnaptr OR TCPpreferred OR UDPOnly OR TLS OR TCPOnly	DNSnaptr	The dnslook up of the first server to be dialed will be used, if there is a conflict with the others. For example, if `dialplan.x.routing.server.1.transport="UDPOnly"` and `dialplan.x.routing.server.2.transport = "TLS"`, then “UDPOnly” is used.

<emergency/>

In the following tables, *x* is the index of the emergency entry description and *y* is the index of the server associated with emergency entry *x*. For each emergency entry (index *x*), one or more server entries (indexes (*x*,*y*)) can be configured. *x* and *y* must both use sequential numbering starting at 1.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dialplan.routing.emergency.x.description	String	For *x=1*, description= "Emergency", Null for all others	The name of the person who will answer the call.
dialplan.routing.emergency.x.server.y	positive integer	For *x=1*, *y =1*, Null for all others	Index representing the server defined in <server/> on page A-40 that will be used for emergency routing.
dialplan.routing.emergency.x.value	Single entry representing a SIP URL	For *x =1*, value = "911", Null for all others	This determines the URLs that should be watched for. When one of these defined URLs is detected as having been dialed by the user, the call will automatically be directed to the defined emergency server.

Per-registration routing server configuration is also supported.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dialplan.x.routing. emergency. y.value	Comma separated list of entries or single entry representing a or a combination of SIP URL.	Null	This represents the URLs that should be watched for emergency routing. When one of these defined URL is detected as being dialed by the user, the call will be automatically directed to the defined emergency server. For example: “15,17,18”, “911”, “sos”.
dialplan.x.routing. emergency.y.server.z	positive integer, 0 to 3	0 For all *x*, *y*, and *z* = 1 to 3	Index representing the server defined in <server/> on page A-40 that will be used for emergency routing.

<dir/>

This attribute includes:

- <local/>
- <corp/>

<local/>

The local directory is stored in either flash memory or RAM on the phone. The local directory size is limited based on the amount of flash memory in the phone. (Different phone models have variable flash memory.)

When the volatile storage option is enabled, ensure that a properly configured provisioning server that allows uploads is available to store a back-up copy of the directory or its contents will be lost when the phone reboots or loses power.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dir.local.contacts.maxNum	0 to 99 OR 0 to 9999	99 OR 9999	Maximum number of contacts in the local contact directory.. For IP 32x/33x and IP 7000 phones, the permitted values are 0 to 99 with a default of 99. For all other phones, the permitted values are 0 to 9999 with a default of 9999. ***Note**: The use of the value 0 is not recommended.*
dir.local.readonly	0 or 1	1	Specifies whether or not local contact directory is read only. If set to 0, the local contact directory is editable. If set to 1, the local contact directory is read only. ***Note:** If the local contact directory is read only, speed dial entry on the SoundPoint IP 32x/33x is disabled (enter the speed dial index followed by "#").*
dir.search.field	0 or 1	0	Specifies how to search the contact directory. If set to 1, search by contact's first name. If set to 0, search by contact's last name.

<corp/>

A portion of the corporate directory is stored in flash memory on the phone. The size is based on the amount of flash memory in the phone. (Different phone models have variable flash memory.)

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dir.corp.address	dotted-decimal IP address or host name or FQDN	Null	The IP address or host name of the LDAP server interface to the corporate directory. For example, host.domain.com.
dir.corp.attribute.x.filter	UTF-8 encoded string	Null	The filter string for this attribute, which is edited when searching.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dir.corp.attribute.x.label	UTF-8 encoded string	Null	A UTF-8 encoded string that is used as the label when data is displayed.
dir.corp.attribute.x.name	UTF-8 encoded string	Null	The name of the attribute to match on the server. Each name must be unique, however, an LDAP entry can have multiple attributes with the same name. Up to eight attributes can be configured (x = 1 to 8).
dir.corp.attribute.x.searchable	0 or 1	0	A flag to determine if the attribute is searchable through quick search. This flag applies for x = 2 or greater. If set to 0, quick search on this attribute is disabled. If set to 1, quick search on this attribute is enabled.
dir.corp.attribute.x.sticky	0 or 1	0	If set to 0, the filter criteria for this attribute is reset after a reboot. If set to 1, the filter criteria for this attribute is retained through a reboot. Such attributes are denoted with a "*" before the label when displayed on the phone.
dir.corp.attribute.x.type	first_name, last_name, phone_number, SIP_address, H323_address URL, other	last_name	This parameter defines how the attribute is interpreted by the phone. Entries can have multiple attributes of the same type. Type 'other' is used for display purposes only. If the user saves the entry to the local contact directory on the phone, first_name, last_name, and phone_number are copied. The user can place a call to the phone_number and SIP_address from the corporate directory.
dir.corp.autoQuerySubmitTimeout	0 to 60 seconds	0	To control if there is a timeout after the user stops entering characters in the quick search and, if there is, how long the timeout is. If set to 0, there is no timeout (disabled).

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dir.corp.backGroundSync	0 or 1	0	If set to 0, there will be no background downloading from the LDAP server. If set to 1, there will be background downloading of data from the LDAP server.
dir.corp.backGroundSync.period	3600 to 604800 seconds	86400	The corporate directory cache is refreshed after the corporate directory feature has not been used for this period of time. The default period is 24 hours. The minimum is 1 hour and the maximum is 7 days.
dir.corp.baseDN	UTF-8 encoded string	Null	The base domain name is the starting point for making queries on the LDAP server.
dir.corp.cacheSize	8 to 256	128	The maximum number of entries that can be cached locally on the phone.
dir.corp.filterPrefix	UTF-8 encoded string	(objectclass=person)	Predefined filter string. If set to Null or invalid, "(objectclass=person)" is used.
dir.corp.pageSize	8 to 64	32	The maximum number of entries requested from the corporate directory server with each query.
dir.corp.password	UTF-8 encoded string	Null	The password used to authenticate to the LDAP server.
dir.corp.port	0, Null, 1 to 65535	389 (TCP) 636 (TLS)	This parameter is used to specify the port to connect to on the server, if a full URL is not provided.
dir.corp.scope	"one", "sub", "base"	"sub"	Type of search. If set to "one", a search of the level one below the baseDN is performed. If set to "sub", a recursive search (of all levels below the baseDN) is performed. If set to "base", a search at the baseDN level is performed.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dir.corp.sortControl	0 or 1	0	Controls how client makes queries and does it sort entries locally. It should not be used by users. If set to 0, leave sorting as negotiated between client and server. If set to 1, force sorting of queries. ***Note**: Polycom does not recommend setting `dir.corp.sortControl` to 1 as it causes excessive LDAP queries. It should be used to diagnose LDAP servers with sorting problems only.*
dir.corp.transport	TCP, TLS, Null	TCP	This parameter is used to specify whether a TCP or TLS connection is made with the server, if a full URL is not provided.
dir.corp.user	UTF-8 encoded string	Null	The username used to authenticate to the LDAP server.
dir.corp.viewPersistence	0 or 1	0	If set to 0, the browse position in the data on the LDAP server and the attribute filters are reset for subsequent usage of the corporate directory. If set to 1, the browse position in the data and the attribute filters are retained for subsequent usage of the corporate directory.
dir.corp.vlv.allow	0 or 1	0	A flag to determine whether or not VLV queries can be made if the LDAP server supports VLV. If set to 0, VLV queries are disabled. If set to 1, VLV queries are enabled. ***Note**: If VLV is enabled, `dir.corp.attribute.x.searchable` is ignored.*
dir.corp.vlv.sortOrder	list of attributes	Null	The list of attributes (in the exact order) to be used by the LDAP server when indexing. For example, sn, givenName, telephoneNumber.

<divert/>

The phone has a flexible call forward/diversion feature for each registration. In all cases, a call will only be diverted if a non-Null contact has been configured.

In the following table, x is the registration number. IP 32x/33x: *x*=1-2; IP 450: *x*=1-3; IP 550, 560: *x*=1-4; VVX 1500: *x*=1-6; IP 650, 670: *x*=1-34; IP 5000: *x*=1;IP 6000: *x*=1; IP 7000: *x*=1.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
divert.x.autoOnSpecificCaller	0 or 1	1	If set to 1, calls may be diverted using the Auto Divert feature of the directory. This is a global flag. ***Note:*** *If server-based call forwarding is enabled, this parameter is disabled*.
divert.x.contact	ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com	Null	The forward-to contact used for all automatic call diversion features unless overridden by a specific contact of a per-call diversion feature (refer to below).
divert.x.sharedDisabled	0 or 1	1	If set to 1, all diversion features on that line will be disabled if the line is configured as shared.

This attribute also includes:

- <fwd/>
- <busy/>
- <noanswer/>
- <dnd/>

<fwd/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
divert.fwd.x.enabled	0 or 1	1	If set to 1, the user will be able to enable universal call forwarding through the soft key menu. ***Note:*** *If server-based call forwarding is enabled, this parameter is enabled*.

<busy/>

Calls can be automatically diverted when the phone is busy.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
divert.busy.x.contact	ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com	Null	Forward-to contact for calls forwarded due to busy status, if Null, `divert.x.contact` will be used.
divert.busy.x.enabled	0 or 1	1	If set to 1, calls will be forwarded on busy to the contact specified below. ***Note:*** *If server-based call forwarding is enabled, this parameter is disabled*.

<noanswer/>

The phone can automatically divert calls after a period of ringing.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
divert.noanswer.x.contact	ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)	Null	Forward-to contact used for calls forwarded due to no answer, if Null, `divert.x.contact` will be used.
divert.noanswer.x.enabled	0 or 1	1	If set to 1, calls will be forwarded on no answer to the contact specified. ***Note:*** *If server-based call forwarding is enabled, this parameter is disabled*.
divert.noanswer.x.timeout	positive integer	55	Time in seconds to allow altering before initiating the diversion.

<dnd/>

The phone can automatically divert calls when Do Not Disturb (DND) is enabled.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
divert.dnd.x.contact	ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)	Null	Forward-to contact used for calls forwarded due to DND status, if Null `divert.x.contact` will be used.
divert.dnd.x.enabled	0 or 1	0	If set to 1, calls will be forwarded on DND to the contact specified below. ***Note:*** *If server-based DND or server-base call forwarding is enabled, this parameter is disabled*.

<dns/>

In the tables below, a maximum of 12 entries of NAPTR, SRV, and A record can be added.

This attribute includes:

- <NAPTR/> attribute
- <SRV/>
- <A/>

<NAPTR/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dns.cache.NAPTR.x. flags	string	Null	Flags to control aspects of the rewriting and interpretation of the fields in the record. Flags are single characters from the set [A-Z, 0-9]. The alphabetic characters are case insensitive. At this time only four flag, "S", “A”, “U”, and “P” are defined. For more information, go to http://tools.ietf.org/html/rfc2915 .
dns.cache.NAPTR.x. name	domain name string	Null	The domain name to which this resource record refers.
dns.cache.NAPTR.x. order	0 to 65535	0	A 16-bit unsigned integer specifying the order in which the NAPTR records must be processed to ensure the correct ordering of rules.
dns.cache.NAPTR.x. preference	0 to 65535	0	A 16-bit unsigned integer that specifies the order in which NAPTR records with equal "order" values should be processed, low numbers being processed before high numbers.
dns.cache.NAPTR.x. regexp	string	Null	A string containing a substitution expression that is applied to the original string held by the client in order to construct the next domain name to lookup. The grammar of the substitution expression is given in RFC 2915. ***Note**: This parameter is currently unused.*
dns.cache.NAPTR.x. replacement	domain name string with SRV prefix	Null	The next name to query for NAPTR, SRV, or address records depending on the value of the flags field. It must be a fully qualified domain-name.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dns.cache.NAPTR.x. service	string		Specifies the service(s) available down this rewrite path. For more information, go to http://tools.ietf.org/html/rfc2915 .
dns.cache.NAPTR.x.ttl	300 to 65535	300	Specifies the time interval (in seconds) that the resource record may be cached before the source of the information should again be consulted.

<SRV/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dns.cache.SRV.x.name	domain name string	Null	The domain name string with SRV prefix.
dns.cache.SRV.x.port	0 to 65535	0	The port on this target host of this service. For more information, go to http://tools.ietf.org/html/rfc2782 .
dns.cache.SRV.x. priority	0 to 65535	0	The priority of this target host. For more information, go to http://tools.ietf.org/html/rfc2782 .
dns.cache.SRV.x.target	domain name string	Null	The domain name of the target host. For more information, go to http://tools.ietf.org/html/rfc2782 .
dns.cache.SRV.x.ttl	0 to 65535, seconds	300	Specifies the time interval that the resource record may be cached before the source of the information should again be consulted.
dns.cache.SRV.x. weight	0 to 65535	0	A server selection mechanism. For more information, go to http://tools.ietf.org/html/rfc2782 .

<A/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
dns.cache.A.x.address	dotted-decimal IP version 4 address	Null	IP address that hostname `dns.cache.A.x.name` maps to.
dns.cache.A.x.name	valid hostname	Null	Hostname
dns.cache.A.x.ttl	0 to 65535	300	Specifies the time interval that the resource record may be cached before the source of the information should again be consulted.

<efk/>

This section defines the additional fields to be entered into a configuration file for controlling the enhanced feature key behavior. The definition language follows the XML style notation. The following elements are part of the definition language:

- <efk/>
- <efklist/>
- <efkprompt/>
- <version/>
- Special Characters
- Macro Definition

Note Changing `<efk/>` parameters will not cause a phone to reboot or restart.

<efk/>

This element indicates the start of enhanced feature key definition section. The `efk` element has the following format:

```
<efk> ... </efk>
```

<efklist/>

This element describes behavior of enhanced feature key.

The different blocks of the enhanced feature key definitions are uniquely identified by number following `efk.efklist` prefix (for example, `efk.efklist.1.<suffix>`).

Note

In SIP 3.1, a maximum of 50 element groups is supported, however, the exact number is dependent on available RAM and processing speed. The disabled elements are included in the total count.

This element contains the following parameters:

Name	Interpretation
mname	This is the unique identifier that is used for the speed-dial configuration to reference the enhanced feature key entry. It cannot start with a digit. This parameter must have a value and it cannot be Null.
status	This parameter has the following values: • If set to 1, this key is enabled. • If set to 0 or Null, this key is disabled. If this parameter is omitted, the value 0 is used.
label	This field defines the text string that will be used as a label on any user text entry screens during enhanced feature key operation. The value can be any string including the null string (in this case, no label appears). If this parameter is omitted, the Null string is used. ***Note**: If you exceed the phone physical layout text limits, the text will be shortened and "..." will be appended.*
type	The SIP method to be performed once the macro starts executing. This parameter has the following values: • If set to "invite ", the action required is performed using the SIP INVITE method. ***Note**: This parameter is included for backwards compatibility only. Do not use if at all possible. If the action.string contains types, this parameter is ignored. If this parameter is omitted, the default is INVITE.*
action.string	The action string contains a macro definition of the action to be performed. For more information, refer to Macro Definition on page A-56. This parameter must have a value and it cannot be Null.

<efkprompt/>

This element describes the behavior of the user prompts.

The different blocks are uniquely identified by number following `efk.efkprompt` prefix (for example, `efk.efkprompt.1.<suffix>`).

Note In SIP 3.0, a maximum of four user prompts were supported. In SIP 3.1, a maximum of ten user prompts are supported.

This element contains the following parameters:

Name	Interpretation
status	This parameter has the following values: • If set to 1, this key is enabled. • If set to 0, this key is disabled. This parameter must have a value and it cannot be Null. ***Note**: If a macro attempts to use a prompt that is disabled or invalid, the macro execution fails.*
label	This parameter sets the prompt text that will be presented to the user on the user prompt screen. The value can be any string including the null string (in this case, no label appears). If this parameter is omitted, the Null string is used. ***Note**: If you exceed the phone physical layout text limits, the text will be shortened and "..." will be appended.*
userfeedback	This parameter specifies the user input feedback method. It has the following values: • If set to “visible”, the text appears as clear text. • If set to “masked”, the text appears as “*” characters. For example, if a password is entered. If this parameter is omitted, the value “visible” is used. If this parameter has an invalid value (including Null), this prompt is invalid and all parameters depending on this prompt are invalid.
type	The type of characters entered by the user. This parameter has the following values: • If set to “numeric “, the characters are interpreted as numbers. • If set to “text”, the characters are interpreted as letters. If this parameter is omitted, the value “numeric” is used. If this parameter has an invalid value (including Null), this prompt is invalid and all parameters depending on this prompt are invalid. ***Note**: A mix of numeric and text is not supported.*

<version/>

This element contains the version of the enhanced feature key elements. The `version` element has the following format:

```
<version efk.version="2"/>
```

If this parameter is omitted or has an invalid value (including Null), the enhanced feature key is disabled. This parameter is not required if there are no `efk.efklist` entries.

Note

In SIP 3.0, "1" is the only supported version. In SIP 3.1 or later, "2" is the only supported version.

Special Characters

The following special characters are used to implement the enhanced feature key functionality:

- ! — The characters following it are a macro name.
- ' or ASCII (0x27) — This character delimits the commands within the macro.
- $ — This character delimits the parts of the macro string. This character must exist in pairs, where the delimits the characters to be expanded.
- ^ — This character indicates that the following characters represent the expanded macro (as in the action string).

Macro names and action strings cannot contain these characters. If they do, unpredictable results may occur.

Macro Definition

The `action.string` in the `efklist` element can be defined by either:

- Macro Action
- Prompt Macro Substitution
- Expanded Macros

Macro Action

The action string is executed in the order it appears. User input is collected before any action is taken.

The action string contains the following fields:

Name	Interpretation
$L<label>$	This is the label for the entire operation. The value can be any string including the null string (in this case, no label appears). This label will be used if no other operation label collection method worked (up to the point where this field is introduced). Make this the first entry in action string to be sure this label is used; otherwise another label may be used and this one ignored.
digits	The digits to be sent. The appearance of this this parameter depends on the action string.
$C<command>$	This is the command. It can appear anywhere in the action string. Supported commands (or shortcuts) include: • hangup (hu) • hold (h) • waitconnect (wc) • pause <number of seconds> (p <num sec>) where the maximum value is 10
$T<type>$	The embedded action type. Multiple actions can be defined. Supported action types include: • invite • dtmf • refer ***Note**: Polycom recommends that you always define this field. If it is not defined, the supplied digits will be dialed using INVITE (if no active call) or DTMF (if an active call). The use of refer method is call server dependent and may require the addition of star codes.*
$M<macro>$	The embedded macro. The <macro> string must begin with a letter. If the macro name is not defined, the execution of the action string fails.
$P<prompt num>N<num digits>$	The user input prompt string. Refer to Prompt Macro Substitution on this page.
$S<speed dial index>$	The speed dial index. Only digits are valid. The action is found in the `contact` field of the local directory entry pointed to by the index.

Name	Interpretation
$F<internal function>$	An internal function. For more information, refer to Internal Key Functions on page C-17.
URL	A URL. Only one per action string is supported.

Prompt Macro Substitution

The `action.string` in the `efklist` element can be defined by a macro substitution string, "PnNn" where:

- Pn is the prompt x as defined in the `efk.efkprompt.x`
- Nn is the number of digits or letters that the user can enter. The maximum number is 32. The user needs to press the **Enter** soft key to complete data entry.

Note If the maximum number of characters is greater than 32 or less than one, macro execution fails.

The macros provide a generic and easy to manage way to define the prompt to be displayed to the user, the maximum number of characters that the user can input, and action that the phone performs once all user input has been collected. The macros are case sensitive.

If a macro attempts to use a prompt that is disabled, the macro execution fails. A prompt is not required for every macro.

Expanded Macros

Expanded macros are prefixed with the "^" character and are inserted directly into the local directory `contact` field. For more information, refer to Local Contact Directory File Format on page 4-10.

<feature/>

These settings control the activation or deactivation of a feature at run time.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
feature.acdAgentAvailable. enabled	0 or 1	0	The ACD agent available/unavailable feature.
feature.acdLoginLogout.enabled	0 or 1	0	The ACD login/logout feature.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
feature.acdServiceControlUri. enabled	0 or 1	0	The ACD service control URI feature. ***Note:*** *This functionality will be available in a future patch release.*
feature.callList.enabled	0 or 1	1	The locally controlled call lists. ***Note:*** *The "call list" feature can be disabled on all SoundPoint IP, SoundStation IP, and VVX phones except the SoundPoint IP 32x/33x.*
feature.callListMissed.enabled	0 or 1	1	The missed-calls list feature (the "calllist" feature must be enabled for this feature to be available).
feature.callListPlaced.enabled	0 or 1	1	The placed-calls list feature (the "calllist" feature must be enabled for this feature to be available).
feature.callListReceived.enabled	0 or 1	1	The received-calls list feature (the "calllist" feature must be enabled for this feature to be available).
feature.callPark.enabled	0 or 1	0	The call park and park-retrieve features.
feature.callRecording.enabled	0 or 1	0	The call recording and playback feature. ***Note****:This feature is supported on SoundPoint IP phones that have a USB port.*
feature.corporateDirectory. enabled	0 or 1	0	"The corporate directory feature.
feature.directedCallPickup. enabled	0 or 1	0	The directed call pickup feature.
feature.directory.enabled	0 or 1	1	The local directory feature.
feature.enhancedFeatureKeys. enabled	0 or 1	0	"The enhanced feature keys feature. ***Note****: This feature must be enabled to use the configurable soft keys feature*.
feature.groupCallPickup.enabled	0 or 1	0	The group call pickup feature.
feature.lastCallReturn.enabled	0 or 1	0	The last call return feature.
feature.messaging.enabled	0 or 1	0	The instant messaging feature.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
feature.nWayConference.enabled	0 or 1	0	The conference managing feature. If set to 0, the n-way conferencing feature is disabled, meaning that three-way conferencing can exist, but there is no manage conference page. If set to 1, the n-way conferencing feature is enabled, the maximum number of conference parties for the platform can exist, and there is a manage conference page. ***Note**: The manage conference feature is always disabled on the SoundPoint IP 32x/33x phone. The manage conference feature is always enabled on the SoundStation IP 7000 and the Polycom VVX 1500 phone.*
feature.pictureFrame.enabled	0 or 1	1	The digital picture frame feature. ***Note**:This feature is supported on the Polycom VVX 1500 only.*
feature.presence.enabled	0 or 1	0	The presence feature including management of buddies and own status.
feature.ringDownload.enabled	0 or 1	1	The run-time downloading of ringers.
feature.urlDialing.enabled	0 or 1	1	Controls whether URL/name dialing is available from a private line (it is never available from a shared line). ***Note:** The "url-dialing" feature must be disabled in order to prevent unknown callers from being identified on the display by an IP address*.

Note

`feature.nwayConference.enabled`, `feature.callRecording.enabled`, and `feature.corporateDirectory.enabled` are charged for separately. To activate these features, you must go to the Polycom Resource Center (http://extranet.polycom.com/csnprod/signon.html) to retrieve the activation code. However, these feature are included on the Polycom VVX 1500.

<font/>

These settings control the phone's ability to dynamically load an external font file during boot up. Loaded fonts can either overwrite pre-existing fonts embedded within the software (not recommended) or can extend the phone's font support for Unicode ranges not already embedded. The font file must be a Microsoft **.fnt** file format. The font file name must follow a specific pattern as described:

- Font filename: `<fontName>_<fontHeightInPixels>_<fontRange>.<fontExtension>`
- <fontName> is a free string of characters that typically carries the meaning of the font. Examples are "fontFixedSize" for a fixed-size font, or "fontProportionalSize" for a proportional size font.
- <fontHeightInPixels> describes the font height in number of screen pixels.
- <fontRange> describes the Unicode range covered by this font. Since **.fnt** are 256 characters based blocks, the <fontRange> is Uxx00_UxxFF (**.fnt** file). For more information, refer to Multilingual User Interface on page 4-31.
- <fontExtension> describes the file type. Either **.fnt** for single 256 characters font .

If it is necessary to overwrite an existing font, use these <fontName>_<fontHeightInPixels>:

SoundPoint IP 32x/33x	
"fontProp_10"	This is the font used for the idle display and default time display.
"fontPropSoftkey_10"	This is the font used for soft keys labels and menu titles.
"fontFixed7_10"	This is the font used for the status line, pop-up text, and the Microbrowser.
SoundPoint IP 450	
"fontProp_16"	This is font used for soft key labels.
"fontProp_19"	This is the font used widely in the current implementation.
"fontProp_mb	This is a small font used for the CPU/Load/Net utilization graphs.
SoundPoint IP 550, 560, 650, and 670	
"fontProp_12"	This is the font used for audio progress bar and the Microbrowser.
"fontProp_19"	This is the font used widely in the current implementation including for soft keys.
"fontProp_26"	This is the font used to display time (but not date).

"fontProp_mb"	This is a small font used for the CPU/Load/Net utilization graphs.
SoundStation IP 5000 and 6000	
"fontProp_10"	This is the font used for the idle display and the Microbrowser.
"fontPropSoftkey_10"	This is a small font used for the CPU/Load/Net utilization graphs.
"fontProp_16"	This is the font used widely in the current implementation.
SoundStation IP 7000	
"fontProp_10"	This is a small font used for the CPU/Load/Net utilization graphs.
"MobileBold_10"	This is the font used for the Microbrowser.
"MobileBold_16"	This is the font used widely in the current implementation.
"MobileBold_24"	This is the font used when entering a number for dialing.
"MobileBold_49"	This is the font used to display time (but not date).

If the <fontName>_<fontHeightInPixels> does not match any of the names above, then the downloaded font will be applied against all fonts defined in the phone, which means that you may lose the benefit of fonts being calibrated differently depending on their usage. For example, the font used to display the time on the SoundPoint IP 650 is a large font, larger than the one used to display the date, and if you overwrite this default font with a unique font, you lose this size aspect. For example:

- to overwrite the font used for SoundPoint IP 550 soft keys for ASCII, the name should be **fontPropSoftkey_10_U0000_U00FF.fnt** .
- to add support for a new font that will be used everywhere and that is not currently supported. For example, for the Eastern/Central European Czech language, this is Unicode range 100-17F, the name could be **fontCzechIP500_10_U0100_U01FF.fnt** and **fontCzechIP600_19_U0100_U01FF.fnt** .

The font delimiter is important to retrieve the different scrambled **.fnt** blocks. This font delimiter must be placed in the "copyright" attribute of the **.fnt** header. If you are simply adding or changing a few fonts currently in use, multiple **.fnt** files are recommended since they are easier to work with individually.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
font.delimiter	string up to 256 ASCII characters	Null	Delimiter required to retrieve different grouped **.fnt** blocks.
font.x.name	fontName_height_Uxx00_UxxFF.fnt	Null	Defines the font file that will be loaded from provisioning server during boot up.

<httpd/>

The phone contains a local web server for user and administrator features. This can be disabled for applications where it is not needed or where it poses a security threat. The web server supports both basic and digest authentication. The authentication user name and password are not configurable for this release.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
httpd.enabled	0 or 1	1	If set to 1, the HTTP server will be enabled.
httpd.cfg.enabled	0 or 1	1	If set to 1, the HTTP server configuration interface will be enabled.
httpd.cfg.port	1-65535	80	Port is 80 for HTTP servers. Care should be taken when choosing an alternate port.

<key/>

SoundPoint IP 32x/33x, 450, 550, 560, 650, and 670, SoundStation IP 5000, 6000 and 7000, and VVX 1500 key functions can be changed from the factory defaults, although this is typically not necessary. For each key whose function you wish to change, add an XML attribute in the format described in the following table to the `<key/>` element of the configuration file. These will override the built-in assignments.

Note The remapping of keys is not recommended.

Model (x in table below)	Key Number (y in table below)
SPIP320, SPIP321, SPIP330, SPIP331, SPIP335	1 to 34
SPIP450	1 to 35
SPIP550, SPIP560	1 to 40
SPIP650, SPIP670	1 to 42
SSIP5000	1 to 32
SSIP6000	1 to 29
SSIP7000	1 to 30
VVX1500	1 to 42

Attribute (bold = change causes restart/reboot	Permitted Values	Interpretation
key.x.y.function.prim	Functions listed below.	Sets the function for key y on platform x.
key.x.y.subPoint.prim	positive integer	Sets the sub-identifier for key functions with a secondary array identifier such as SpeedDial.

The following table lists the functions that are available:

Functions			
ArrowDown	Dialpad5	Line2	Select
ArrowLeft	Dialpad6	Line3	Setup
ArrowRight	Dialpad7	Line4	SoftKey1
ArrowUp	Dialpad8	Line5	SoftKey2
BuddyStatus	Dialpad9	Line6	SoftKey3
CallList	DialpadStar	Messages	SoftKey4
Conference	DialpadPound	Menu	SpeedDial
Delete	Directories	MicMute	SpeedDialMenu
Dialpad0	DoNotDisturb	MyStatus	Transfer
Dialpad1	Handsfree	Null	Video
Dialpad2	Headset	Offline	VolDown
Dialpad3	Hold	Redial	VolUp
Dialpad4	Line1	Release	

<lcl/>

The phone has a multilingual user interface. It supports both North American and international time and date formats.

This attribute includes:

- <ml/>
- <datetime/>

<ml/>

The multilingual feature is based on string dictionary files downloaded from the provisioning server. These files are encoded in standalone XML format. Several eastern European and Asian languages are included with the distribution. Space for user-defined languages is available.

Attribute **(bold = change causes restart/reboot)**	**Permitted Values**	**Interpretation**
lcl.ml.lang	Null OR An exact match for one of the label names stored in `lcl.ml.lang.menu.x.label`.	If Null, the default internal language (US English) will be used, otherwise, the language to be used may be specified in the format of `lcl.ml.lang.menu.x.label`. For example, to get the phone to boot up in German: `lcl.ml.lang = "Deutsch (de-de)"`.
lcl.ml.lang.clock.x.24HourClock	0 or 1	If attribute present, overrides `lcl.datetime.time.24HourClock`. If 1, display time in 24-hour clock mode rather than am/pm.
lcl.ml.lang.clock.x.dateTop	0 or 1	If attribute present, overrides `lcl.datetime.date.dateTop`. If 1, display date above time, otherwise display time above date.
lcl.ml.lang.clock.x.format	string which includes 'D', 'd' and 'M' and two optional commas	If attribute present, overrides lcl.datetime.date.format; D = day of week d = day M = month Up to two commas may be included. For example: D,dM = Thursday, 3 July or Md,D = July 3, Thursday The field may contain 0, 1 or 2 commas which can occur only between characters and only one at a time. For example: "D,,dM" is illegal.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
lcl.ml.lang.clock.x.longFormat	0 or 1	If attribute present, overrides `lcl.datetime.date.longFormat`. If 1, display the day and month in long format (Friday/November), otherwise use abbreviations (Fri/Nov).
lcl.ml.lang.list	a comma-separated list	A list of the languages supported on the phones. Phone-specific parameters are defined for the SoundPoint IP 32x/33x phones as they do not support Asian languages.

lcl.ml.lang.menu.x
lcl.ml.lang.menu.x.label
	String in the format *language_region*	Multiple `lcl.ml.lang.menu.x attributes` are supported - as many languages as are desired. However, the `lcl.ml.lang.menu.x` attributes must be sequential (`lcl.ml.lang.menu.1`, `lcl.ml.lang.menu.2`, `lcl.ml.lang.menu.3`, ..., `lcl.ml.lang.menu.N`) with no gaps and the strings must exactly match a folder name under the SoundPointIPLocalization folder on the provisioning server for the phone to be able to locate the dictionary file.
		For example:
		`lcl.ml.lang.menu.8="German_Germany"`
		`lcl.ml.lang.menu.8.label="Deutsch (de-de)"`

To add new languages to those included with the distribution:

1. Create a new dictionary file based on an existing one.
2. Change the strings making sure to encode the XML file in UTF-8 but also ensuring the UTF-8 characters chosen are within the Unicode character ranges indicated in the tables below.
3. Place the file in an appropriately named folder according to the format *language_region* parallel to the other dictionary files under the SoundPointIPLocalization folder on the provisioning server.
4. Add a `lcl.ml.lang.clock.menu.x` attribute to the configuration file.
5. Add `lcl.ml.lang.clock.x.24HourClock`, `lcl.ml.lang.clock.x.format`, `lcl.ml.lang.clock.x.longFormat` and `lcl.ml.lang.clock.x.dateTop` attributes and set them according to the regional preferences.
6. (Optional) Set `lcl.ml.lang` to be the new *language_region* string.

Basic character support includes the following Unicode character ranges	
Name	**Range**
C0 Controls and Basic Latin	U+0000 - U+007F
C1 Controls and Latin-1 Supplement	U+0080 - U+00FF
Cyrillic (partial)	U+0400 - U+045F

Extended character support available on SoundPoint IP 600 and SoundStation IP 4000 and 7000 platforms includes the following Unicode character ranges	
Name	**Range**
CJK Symbols and Punctuation	U+3000 - U+303F
Hiragana	U+3040 - U+309F
Katakana	U+30A0 - U+30FF
Bopomofo	U+3100 - U+312F
Hangul Compatibility Jamo	U+3130 - U+318F
Bopomofo Extended	U+31A0 - U+31BF
Enclosed CJK Letters and Months	U+3200 - U+327F
CJK Compatibility	U+3300 - U+33FF
CJK Unified Ideographs	U+4E00 - U+9FFF
Hangul Syllables	U+AC00 - U+D7A3
CJK Compatibility Ideographs	U+F900 - U+FAFF
CJK Half-width forms	U+FF00 - U+FFFF

Note Within a Unicode range, some characters may not be supported due to their infrequent usage

<datetime/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
lcl.datetime.date.dateTop	0 or 1	If set to 1, display date above time else display time above date.
lcl.datetime.date.format	string which includes 'D', 'd' and 'M' and two optional commas	Controls format of date string. D = day of week d = day M = month Up to two commas may be included. For example: D,dM = Thursday, 3 July or Md,D = July 3, Thursday The field may contain 0, 1 or 2 commas which can occur only between characters and only one at a time. For example: "D,,dM" is illegal.
lcl.datetime.date.longFormat	0 or 1	If set to 1, display the day and month in long format (Friday/November), otherwise, use abbreviations (Fri/Nov).
lcl.datetime.time.24HourClock	0 or 1	If set to 1, display time in 24-hour clock mode rather than a.m./p.m.

<license/>

This attribute's settings control aspects of the feature licensing system.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
license.polling.time	00:00 – 23:59	2:00am	The time to check whether or not the license has expired.

<mb/>

This attribute's settings control the home page, proxy and size limits to be used by the Microbrowser and Browser when it is selected to provide services. The Microbrowser is supported on the SoundPoint IP 450, 550, 560, 601, 650, and 670, and the SoundStation IP 6000 and 7000 phones, and the Browser is supported on the Polycom VVX 1500 phones.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	**Permitted Values**	**Default**	**Interpretation**
mb.proxy	Null or domain name or IP address in the format <address>:<port>	Null. Default port = 8080	Address of the desired HTTP proxy to be used by the Microbrowser. If blank, normal unproxied HTTP is used by the Microbrowser.
mb.ssawc.call.mode	"active" or "passive"	"passive"	Control the spontaneous display of web content. If set to "passive", the web content is displayed only when requested by the user. If set to "active", the web content is displayed immediately. ***Note:*** *This feature is charged for separately. To activate this feature, you must go to the Polycom Resource Center (http://extranet.polycom.com/csnprod/signon.html) to retrieve the activation code for this feature.*
mb.ssawc.enabled	0 or 1	0	If set to 0, spontaneous display of web content is disabled. If set to 1, spontaneous display of web content is enabled.

This attribute also includes:

- <idleDisplay/>
- <main/>
- <limits/>

<idleDisplay/>

The Microbrowser can be used to create a display that will be part of the phone's idle display. These settings control the home page and the refresh rate.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
mb.idleDisplay.home	Null or any fully formed valid HTTP URL. Length up to 255 characters.	Null	URL used for Microbrowser idle display home page. For example: http://www.example.com/xhtml/frontpage.cgi?page=home. If empty, there will be no Microbrowser idle display feature. Note that the Microbrowser idle display will displace the idle display indicator. ***Note**: If* `ind.idleDisplay.enabled` *is enabled, miscellaneous XML errors can occur on SoundPoint IP 450, 550, 560, 650, and 670 and SoundStation IP 6000 and 7000 phones.*
mb.idleDisplay.refresh	0 or an integer > 5	0	The period in seconds between refreshes of the idle display Microbrowser's content. If set to 0, the idle display Microbrowser is not refreshed. The minimum refresh period is 5 seconds (values from 1 to 4 are ignored, and 5 is used). ***Note:** If an HTTP Refresh header is detected, it will be respected, even if this parameter is set to 0. The refresh parameter will be respected only in the event that a refresh fails. Once a refresh is successful, the value in the HTTP refresh header, if available, will be used.*

<main/>

This setting controls the home page used by the Microbrowser when that function is selected.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
mb.main.autoBackKey	0 or 1	1	If set to 1, the phone will automatically supply a **Back** soft key in all main browser screens, which if pressed will take the user back through the browser history. This is the null default behavior (for backward compatibility). If set to 0, the phone will not provide a Back soft key. All soft keys will be created and controlled by the application.
mb.main.home	Any fully formed valid HTTP URL. Length up to 255 characters.	Null	URL used for Microbrowser home page. If blank, the browser will notify the user that a blank home-page was used. For example: http://www.example.com/xhtml/frontpage.cgi?page=home.
mb.main.idleTimeout	0 - 600, seconds	40	Timeout for the interactive browser. If the interactive browser remains idle for a defined period of time, the phone should return to the idle browser. If set to 0, there is no timeout. If set to value greater than 0 and less than 600, the timeout is for that number of seconds.
mb.main.statusbar	0 or 1	0	Flag to determine whether or not to turn off display of status messages. If set to 1, the display of the status bar is enabled. If set to 0, the display of the status bar is disabled.

<limits/>

These settings limit the size of object which the Microbrowser will display by limiting the amount of memory available for the Microbrowser.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
mb.limits.cache	positive integer	200 (for IP 320/330) 800 (for IP 6000, 7000) 1024 (for VVX 1500) 400 (for all other phones)	Limits the total size of objects downloaded for each page (both XHTML and images). Once this limit is reached, no more images are downloaded until the next page is requested. Units = kBytes. This value is used as referent values for 16MB of SDRAM. ***Note:*** *Increasing this value may have a detrimental effect on performance of the phone.*

<msg/>

Message-waiting indication is supported on a per-registration basis.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
msg.bypassInstantMessage	0 or 1	0	If set to 1, the display offering a choice of "Message Center" and "Instant Messages" will be bypassed when pressing the Messages key. The phone will act as if "Message Center" was chosen. Refer to Voice Mail Integration on page 4-52. Instant Messages will still be accessible from the Main Menu.

This attribute also includes:

- <mwi/>

<mwi/>

In the following table, x is the registration number. IP 32x/33x: *x*=1-2; IP 450: *x*=1-3; IP 550, 560: *x*=1-4; VVX 1500: *x*=1-6; IP 650, 670: *x*=1-34; IP 5000, 6000, 7000: *x*=1.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
msg.mwi.x.subscribe	ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)	Null	If non-Null, the phone will send a SUBSCRIBE request to this contact after boot-up.
msg.mwi.x. callBackMode	"contact" OR "registration" OR "disabled"	"registration"	Configures message retrieval and notification for the line. If set to "contact", a call will be placed to the contact specified in the callback attribute when the user invokes message retrieval. If set to "registration", a call will be placed using this registration to the contact registered (the phone will call itself). If set to "disabled", message retrieval and message notification are disabled.
msg.mwi.x.callBack	ASCII encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL (6416 or 6416@polycom.com)	Null	Contact to call when retrieving messages for this registration.

<nat/>

These parameters define port and IP address changes used in NAT traversal. The port changes will change the port used by the phone, while the IP entry simply changes the IP advertised in the SIP signaling. This allows the use of simple NAT devices that can redirect traffic, but do not allow for port mapping. For example, port 5432 on the NAT device can be sent to port 5432 on an internal device, but not port 1234.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
nat.ip	dotted-decimal IP address	Null	IP address to advertise within SIP signaling - should match the external IP address used by the NAT device.
nat.keepalive.interval	0 to 3600	0	If non-Null (or 0), the keepalive interval in seconds. This parameter is used to set the interval at which phones will send a keep-alive packet to the gateway/NAT device to keep the communication port open so that NAT can continue to function as setup initially. The Microsoft Live Communications Server 2005 keepalive feature will override this interval. If you want to deploy phones behind a NAT and connect them to Live Communications Server, the keepalive interval received from the Live Communications Server must be short enough to keep the NAT port open. Once the TCP connection is closed, the phones stop sending keep-alive packets.
nat.mediaPortStart	0 to 65440	0	If non-Null, this attribute will be used to set the initially allocated RTP port, overriding the value set for `tcpIpApp.port.rtp.mediaPortRangeStart` . Refer to <rtp/> on page A-115.
nat.signalPort	1024 to 65535	0	If non-Null, this port will be used by the phone for SIP signaling, overriding the value set for `voIpProt.local.Port` .

<phoneLock/>

Note The Enhanced Feature Key feature must be enabled if you want to use the **Lock** soft key.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	**Permitted Values**	**Default**	**Interpretation**
phoneLock.authorized.x.description	string		The label to be associated with the number displayed to the user from the phone's user interface.
phoneLock.authorized.x.value	string		The phone number associated with the authorized number selection.
phoneLock.browserEnabled	0 or 1	0	Flag to determine whether or not the microbrowser or browser is displayed.
phoneLock.dndWhenLocked	0 or 1	0	Flag to determine whether or not the phone enters *Do Not Disturb* mode when the phone is locked. Can be changed by the user from the phone user interface.
phoneLock.enabled	0 or 1	0	Flag to used to set the initial state of the phoneLock, or to 'unlock' the phone remotely (in conjunction with deleting/modifying the overrides file).
phoneLock.idleTimeout	0 to 65535	0	The idle time (seconds) until automatic locking occurs. If set to 0, there is no automatic locking.
phoneLock.lockState	0 or 1	0	Flag to determine whether or not to lock the phone on the first reboot.
phoneLock.powerUpUnlocked	0 or 1	0	Flag to determine whether or not to unlock the phone when it is powered up.

<pnet/>

Peer networking manages communications between Polycom devices. For the SoundStation IP 7000 conference phone, it manages daisy-chaining and video integration with the Polycom HDX video systems.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
pnet.hdx.ext	string	Null	The HDX Extension Number to be displayed on the IP 7000 when it is connected to an HDX system.
pnet.remoteCall. callProgAtten	-60 to 0	-15	The attenuation applied to tones played by the IP 7000 for POTS calls when it is connected to an HDX system when the HDX is the active speaker.
pnet.remoteCall. dtmfDuration	0 to 5000	300	The length of time that the DTMF tone is played on the IP 7000.
pnet.remoteCall. localDialTone	0 or 1	0	A flag to determine whether or not a dialtone is played when the IP 7000 makes an outgoing POTS call when it is connected to an HDX. If set to 1, a dial tone is played. If set to 0, a dial tone is not played.

<powerSaving/>

Note This feature is supported on the Polycom VVX 1500 only.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
powerSaving.enable	0 or 1	1	If set to 1, the LCD power saving feature is enabled. If set to 0, the LCD power saving feature is disabled.
powerSaving.idleTimeout. offHours	1 to 10	1	The off hours mode idle timeout (in minutes).

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
powerSaving.idleTimeout. officeHours	1 to 600	10	The office hours mode idle timeout (in minutes).
powerSaving.idleTimeout. userInputExtension	1 to 20	10	The minimum idle timeout after user input events (in minutes).
powerSaving.officeHours. duration.xxx	0 to 12	10 OR 0	The duration of the day's office hours, where xxx is one of "monday", "tuesday", "wednesday", "thursday", "friday", "saturday", and "sunday" . The default value for the week days is 10 (hours) and the default value for Saturday and Sunday is 0 (hours).
powerSaving.officeHours. startHour.xxx	0 to 23	8	The starting hour for the day's office hours, where xxx is one of "monday", "tuesday", "wednesday", "thursday", "friday", "saturday", and "sunday". If set to Null, the default value is 8.
powerSaving. userDetectionSensitivity. offHours	0 to 10	2	The sensitivity of the algorithm used to detect the presence of the phone's user during off hours. If set to 0, this feature is disabled. The default value was chosen for good performance in a typically office environment and is biased for difficult detection during off hours.
powerSaving. userDetectionSensitivity. officeHours	0 to 10	7	The sensitivity of the algorithm used to detect the presence of the phone's user during office hours. If set to 0, this feature is disabled. The default value was chosen for good performance in a typically office environment and is biased for easy detection during office hours.

<pres/>

The parameter `pres.reg` is the line number used to send SUBSCRIBE. If this parameter is missing, the phone will use the primary line to send SUBSCRIBE.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
pres.idleSoftkeys	0 or 1	1	If set to 0, the presence idle soft keys (**MyStat** and **Buddies**) do not appear. If set to 1, the presence idle soft keys appear.
pres.reg	positive integer	1	Specifies the line/registration number used to send SUBSCRIBE for presence. Must be a valid line/registration number. If the number is not a valid line/registration number, it is ignored.

<prov/>

This attribute's settings control aspects of the phone's provisioning server provisioning system.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
prov.configUploadPath	string	Null	The directory where the configuration file created when the user selects **Upload Configuration** is uploaded to.
prov.lineMap.cma.x	1 to 6	1	Used to map the CMA H.323 line to a SIP line. Only *x*=1 is supported.
prov.polling.enabled	0 or 1	0	If set to 1, automatic periodic provisioning server polling for upgrades is enabled.
prov.polling.mode	abs, rel	abs	Polling mode is *abs*olute or *rel*ative.
prov.polling.period	integer greater than 3600	86400	Polling period in seconds. Rounded up to the nearest number of days in *abs* mode. Measured relative to boot time in *rel* mode.
prov.polling.time	Format is hh:mm	03:00	Only used in *abs* mode. Polling time.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
prov.quickSetup.enabled	0 or 1	0	If set to 1, the quick setup feature is enabled. If set to 0, the quick setup feature is disabled.

<qos/>

These settings control the Quality of Service (QOS) options.

This attribute includes:

- <ethernet/>
- <IP/>

<ethernet/>

The following settings control the 802.1p/Q user_priority field:

- <RTP/>
- <callControl/>
- <other/>

<RTP/>

These parameters apply to RTP packets.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
qos.ethernet.rtp.user_priority	0 to 7	5	User-priority used for Voice RTP packets.
qos.ethernet.rtp.video.user_priority	0 to 7	5	User-priority used for Video RTP packets.

<callControl/>

These parameters apply to call control packets, such as the network protocol signaling.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
qos.ethernet.callControl.user_priority	0 to 7	5	User-priority used for call control packets.

<other/>

These default parameter values are used for all packets which are not set explicitly.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
qos.ethernet.other.user_priority	0 to 7	2	User-priority used for packets that do not have a per-protocol setting.

<IP/>

The following settings control the "type of service" field in outgoing packets:

- <rtp/>
- <callControl/>

<rtp/>

These parameters apply to RTP packets.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
qos.ip.rtp.dscp	0 to 63 or EF or any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43	Null	This parameter allows the DSCP of packets to be specified. If set to a value, this will override the other `qos.ip.rtp...` parameters. Default of Null which means the other `qos.ip.rtp...` parameters will be used.
qos.ip.rtp.max_reliability	0 or 1	0	If set to 1, set max-reliability bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.rtp.max_throughput	0 or 1	1	If set to 1, set max-throughput bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.rtp.min_cost	0 or 1	0	If set to 1, set min-cost bit in the IP TOS field of the IP header, or else don't set it.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
qos.ip.rtp.min_delay	0 or 1	1	If set to 1, set min-delay bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.rtp.precedence	0 to 7	5	If set to 1, set precedence bits in the IP TOS field of the IP header, or else don't set them.
qos.ip.rtp.video.dscp	0 to 63 or EF or any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43	Null	This parameter allows the DSCP of packets to be specified. If set to a value, this will override the other `qos.ip.rtp.video`... parameters. Default of Null which means the other `qos.ip.rtp.video`... parameters will be used.
qos.ip.rtp.video.max_reliability	0 or 1	0	If set to 1, set max-reliability bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.rtp.video.max_throughput	0 or 1	1	If set to 1, set max-throughput bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.rtp.video.min_cost	0 or 1	0	If set to 1, set min-cost bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.rtp.video.min_delay	0 or 1	1	If set to 1, set min-delay bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.rtp.video.precedence	0 to 7	5	If set to 1, set precedence bits in the IP TOS field of the IP header, or else don't set them.

<callControl/>

These parameters apply to call control packets, such as the network protocol signaling.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
qos.ip.callControl.dscp	0 to 63 or EF or any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43	Null	This parameter allows the DSCP of packets to be specified. If set to a value this will override the other `qos.ip.callControl...` parameters. Default of Null which means the other `qos.ip.callControl...` parameters will be used.
qos.ip.callControl.max_reliability	0 or 1	0	If set to 1, set max-reliability bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.callControl.max_throughput	0 or 1	0	If set to 1, set max-throughput bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.callControl.min_cost	0 or 1	0	If set to 1, set min-cost bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.callControl.min_delay	0 or 1	1	If set to 1, set min-delay bit in the IP TOS field of the IP header, or else don't set it.
qos.ip.callControl.precedence	0 to 7	5	If set to 1, set precedence bits in the IP TOS field of the IP header, or else don't set them.

<reg/>

SoundPoint IP 32x/33x support a maximum of two unique registrations, SoundPoint IP 450 supports three, the SoundPoint IP 550 and 560 supports four, and SoundPoint IP 650 and 670 and the Polycom VVX 1500 support six. Up to three SoundPoint IP Expansion Modules can be added to a single host SoundPoint IP 650 and 670 phone increasing the total number of buttons to 34 registrations on the IP 650 and 670. Each registration can optionally be associated with a private array of servers for completely segregated signaling. The SoundStation IP 5000, 6000, and 7000 supports a single registration.

In the following table, *x* is the registration number. IP 32x/33x: *x*=1-2; IP 450: *x*=1-3; IP 550, 560: *x*=1-4; VVX 1500: *x*=1-6; IP 650, 670: *x*=1-34; IP 5000, IP 6000, IP 7000: *x*=1.

Attribute (bold = change causes restart/reboot)	**Permitted Values**	**Default**	**Interpretation**
reg.x.acd-login-logout	0 or 1	0	If both parameters are set to 1 for a registration, the ACD feature will be enabled for that registration.
reg.x.acd-agent-available	0 or 1	0	
reg.x.address	string in the format userPart from userPart@domain	Null	The user part or the user and the host part of the phone's SIP URI or the H.323 ID/extension. For example (SIP): reg.x.address="1002" from 1002@polycom.com or reg.x.address="1002@polycom.com". For example (H.323): reg.x.address="23456"
reg.x.auth.optimizedInFailover	0 or 1	0	If set to 1, when failover occurs, the first new SIP request is sent to the server that sent the proxy authentication request. If set to 0, when failover occurs, the first new SIP request is sent to the server with the highest priority in the server list. `voIpProt.SIP.authOptimizedInFailover` and this parameter are logically OR'd to determine the value.
reg.x.auth.password	string	Null	Password to be used for authentication challenges for this registration. If non-Null, will override the "Reg Password x" parameter entered into the Authentication submenu off of the Settings menu on the phone.
reg.x.auth.userId	string	Null	User ID to be used for authentication challenges for this registration. If non-Null, will override the "Reg User x" parameter entered into the Authentication submenu off of the Settings menu on the phone.
reg.x.bargeInEnabled	0 or 1	0	Allow remote user of SCA to interrupt call. (Works in a similar way to resume.) If set to 1, barge-in is enabled for line x. If set to 0, barge-in is disabled for line x.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.callsPerLineKey	1 to 24 OR 1 to 8 OR 1 to 4	24 (for IP550, 560, 650, and 670 and VVX 1500) 8 (for all other phones)	This is the number of calls or conferences which may be active or on hold per line key associated with this registration. This overrides `call.callsPerLineKey` for this registration. Refer to <call/> on page A-21. If `reg.1.callsPerLineKey` is set to 1, call waiting can be disabled. ***Note:*** *A call active on another phone on a shared line counts as a call for every phone sharing that registration.*
reg.x.csta	0 or 1	0	If set to 1, uaCSTA is enabled. If `reg.x.csta` is 1, this attribute overrides the global CSTA flag, `voIpProt.SIP.csta` .
reg.x.displayName	UTF-8 encoded string	Null	Display name used in SIP signaling as the default caller ID. Display name used in SIP signaling and/or H.323 alias as the default caller ID.
reg.x.label	UTF-8 encoded string	Null	Text label to appear on the display adjacent to the associated line key. If omitted, the label will be derived from the user part of reg.x.address.
reg.x.lcs	0 or 1	0	If set to 1, the Microsoft Live Communications Server is supported for registration x.
reg.x.lineKeys	1 to *max*	1	*max* = the number of line keys on the phone. *max* = 1 on IP 5000, 6000, 7000, *max* = 2 on IP 32x/33x, *max* = 3 on IP 450, *max* = 4 on IP 550, 560, *max* = 6 on VVX 1500, *max* = 34 on IP 650, 670 (without any Expansion Modules attached, only 6 line keys are available) The number of line keys on the phone to be associated with registration 'x'.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.musicOnHold.uri	string	Null	A URI that provides the media stream to play for the remote party on hold. If present and not Null, this attribute overrides `voIpProt.SIP.musicOnHold.uri`.
reg.x.protocol.H323	0 or 1	0	If set to 1, H.323 signaling is enabled for this line registration. If set to 0, H.323 signaling is not enabled for this line registration.
reg.x.protocol.SIP	0 or 1	1	If set to 1, SIP signaling is enabled for this line registration. If set to 0, SIP signaling is not enabled for this line registration.
reg.x.proxyRequire	string	Null	The string that needs to appear in the “Proxy-Require” header. If Null, no "Proxy-Require" will be sent.
reg.x.ringType	enumerated type Refer to **reg-advanced.cfg**	ringer2	The ringer to be used for calls received by this registration. Default is the first non-silent ringer.
reg.x.serverFeatureControl.cf	0 or 1	0	If set to 1, server-based call forwarding is enabled. The call server has control of call forwarding. If set to 0, server-based call forwarding is not enabled. This is the old behavior. This attribute may override `voIpProt.SIP.serverFeatureControl.cf`.
reg.x.serverFeatureControl.dnd	0 or 1	0	If set to 1, server-based DND is enabled. The call server has control of DND. If set to 0, server-based DND is not enabled. This is the old behavior. This attribute may override `voIpProt.SIP.serverFeatureControl.dnd`.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.strictLineSeize	0 or 1	0	If set to 1, forces phone to wait for 200 OK on registration x when receiving a TRYING notify. If set to 0, this is old behavior. `voIpProt.SIP.strictLineSeize` and this parameter are logically OR'd to determine the value.
reg.x.tcpFastFailover	0 or 1	0	If set to 1, failover occurs based on the values of `reg.x.server.y.retryMaxCount` `voIpProt.server.x.retryTimeOut`. If set to 0, this is old behavior. `voIpProt.SIP.tcpFastFailover` and this parameter are logically OR'd to determine the value.
reg.x.thirdPartyName	string in the same format as reg.x.address	Null	This field must match the `reg.x.address` value of the other registration which makes up the bridged line appearance (BLA). It must be Null in all other cases.
reg.x.type	private OR shared	private	If set to private, use standard call signaling. If set to shared, augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.
reg.x. useCompleteUriForRetrieve	0 or 1	1	This parameters overrides `voipPort.SIP.useCompleteUriForRetrieve` . If set to 1, use complete URI to retrieve the call for certain servers.

This attribute also includes:

- <fwd/>
- <outboundProxy/>
- <server/>

<fwd/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.fwd.busy.contact	string	Null	Forward-to contact for calls forwarded due to busy status,. If Null, `divert.x.contact` will be used.
reg.x.fwd.busy.status	0 or 1	0	If set to 1, calls will be forwarded on busy to the contact specified below.
reg.x.fwd.noanswer.contact	string	Null	Forward-to contact used for calls forwarded due to no answer. If Null, `divert.x.contact` will be used.
reg.x.fwd.noanswer.ringCount	0 to 65535	0	Time in rings to allow altering before initiating the diversion.
reg.x.fwd.noanswer.status	0 or 1	0	If set to 1,calls will be forwarded on no answer to the contact specified.

<outboundProxy/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.outboundProxy.address	dotted-decimal IP address or host name	Null	IP address or host name and port of a SIP server to which the phone shall send all requests.
reg.x.outboundProxy.failOver.failBack.mode	newRequests DNSTTL registration duration	newRequests	This parameters overrides `reg.x.server.y.failOver.failBack.mode` . If set to *newRequests*, all new requests are forwarded first to the primary server regardless of the last used server. If set to *DNSTTL*, the primary server is tried again after a timeout equal to the DNS TTL configured for the server the endpoint is registered to (or via). If set to *registration*, the primary server is tried again when the registration renewal signaling begins. If set to *duration*, the primary server is tried again after the time specified by timeout expires.
reg.x.outboundProxy.failOver.failBack.timeout	0, 60 to 65535	3600	This parameters overrides `reg.x.server.y.failOver.failBack.timeout` . If `reg.x.outboundProxy.failBack.mode` is set to *duration*, this is the time in seconds after failing over to the current working server before the primary server is again selected as the first server to forward new requests to. Values between 1 and 59 will result in a timeout of 60 and 0 means do not fail-back until a fail-over event occurs with the current server.
reg.x.outboundProxy.failOver.failRegistrationOn	0 or 1	1	This parameters overrides `reg.x.server.y.failOver.failRegistrationOn` . If `reg.x.outboundProxy.failOver.RegisterOn` is set to 1 and this parameter is set to 1, the phone will silently invalidate an existing registration, if it exists, at the point of failing over.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.outboundProxy.failOver. RegisterOn	0 or 1	0	This parameters overrides `reg.x.server.y.failOver.failBack. RegisterOn .` If set to 1, the phone will first attempt to register with (or via) the server to which the signaling is to be diverted, and only upon the registration succeeding (200 OK with valid expires) will the signaling diversion proceed with that server.
reg.x.outboundProxy.port	1 to 65535	0	IP address or host name and port of a SIP server to which the phone shall send all requests.
reg.x.outboundProxy.transport	DNSnaptr or TCPpreferred or UDPOnly or TLS or TCPOnly	DNSnaptr	If set to Null or DNSnaptr: • If `reg.x.outboundProxy.address` is a hostname and reg.x.outboundProxy.port is 0 or Null, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If reg.x.outboundProxy.address is an IP address, or a port is given, then UDP is used. If set to TCPpreferred: • TCP is the preferred transport, UDP is used if TCP fails. If set to UDPOnly: • Only UDP will be used. If set to TLS: • If TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061. If set to TCPOnly: • Only TCP will be used.

<server/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.server.y.address	dotted-decimal IP address or host name	Null	Optional IP address or host name, port, transport, registration period, fail-over parameters and line seize subscription period of a SIP server that accepts registrations. Multiple servers can be listed starting with y=1 to 4 for fault tolerance. If specified, these servers may override the servers specified in `<voIpProt.server/>`. ***Note:*** *If the reg.x.server.y.address parameter is non-Null, all of the reg.x.server.y.xxx parameters will override the parameters specified in* `<voIpProt.server/>`. ***Note:*** *If the reg.x.server.y.address parameter is non-Null, it takes precedence even if the DHCP server is available.*
reg.x.server.y.port	0, Null, 1 to 65535	Null	
reg.x.server.y.transport	DNSnaptr or TCPpreferred or UDPOnly or TLS or TCPOnly	DNSnaptr	
reg.x.server.y.expires	positive integer, minimum 10	3600	
reg.x.server.y.register	0 or 1	1	
reg.x.server.y.expires.overlap	5 to 65535	60	
reg.x.server.y.retryTimeOut	0 to 65535	0	
reg.x.server.y.retryMaxCount	0 to 20	3	
reg.x.server.y.expires.lineSeize	0 to 65535	30	
reg.x.server.y.failOver.failBack.mode	newRequests DNSTTL registration duration	newRequests	This parameters overrides `voIpProt.server.x.failOver.failBack.mode`. If set to *newRequests*, all new requests are forwarded first to the primary server regardless of the last used server. If set to *DNSTTL*, the primary server is tried again after a timeout equal to the DNS TTL configured for the server the endpoint is registered to (or via). If set to *registration*, the primary server is tried again when the registration renewal signaling begins. If set to *duration*, the primary server is tried again after the time specified by timeout expires.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
reg.x.server.y.failOver.failBack. timeout	0, 60 to 65535	3600	This parameters overrides `voIpProt.server.x.failOver.failBack.timeout`. If `reg.x.server.y.failOver.failBack.mode` is set to *duration*, this is the time in seconds after failing over to the current working server before the primary server is again selected as the first server to forward new requests to. Values between 1 and 59 will result in a timeout of 60 and 0 means do not fail-back until a fail-over event occurs with the current server.
reg.x.server.y.failOver. failRegistrationOn	0 or 1	1	This parameters overrides `voIpProt.server.x.failOver.failBack.failRegistrationOn.` If `reg.x.server.y.failOver.RegisterOn` is set to 1 and this parameter is set to 1, the phone will silently invalidate an existing registration, if it exists, at the point of failing over.
reg.x.server.y.failOver. reRegisterOn	0 or 1	0	This parameters overrides `voIpProt.server.x.failOver.failBack.RegisterOn .` If set to 1, the phone will first attempt to register with (or via) the server to which the signaling is to be diverted, and only upon the registration succeeding (200 OK with valid expires) will the signaling diversion proceed with that server.
reg.x.server.y.lcs	0 or 1	0	This attribute overrides the `reg.x.lcs.` If set to 1, the Microsoft Live Communications Server is supported for registration x.
reg.x.server.H323.y.address	dotted-decimal IP address or host name	Null	Address of the H.323 gatekeeper.
reg.x.server.H323.y.port	0 to 65535	0	Port to be used for H.323 signaling. If set to Nul, 1719 (H.323 RAS signaling) is used.
reg.x.server.H323.y.expires	positive integer	3600	Desired registration period.

<request/>

This attribute includes:

- <delay/>

<delay/>

These settings control the phone's behavior when a request for restart or reconfiguration is received.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
request.delay.type	enumerated type Refer to **sip-interop.cfg**	call	Defines the strategy to adopt before a request gets executed. If set to "audio", a request can be executed as soon as there is no active audio on the phone, independently of any call state. If set to "call", a request can be executed as soon as there are no calls in any state on the phone.

<roaming_buddies/>

Note This attribute is used in conjunction with Microsoft Live Communications Server 2005 only.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
roaming_buddies.reg	positive integer	Null	Specifies the line/registration number which has roaming buddies support enabled. If Null, roaming buddies is disabled. If value < 1, then value is replaced with 1. ***Warning:*** *This parameter must be enabled (value > 0) if the call server is Microsoft Live Communications Server 2005.*

<roaming_privacy/>

Note This attribute is used in conjunction with Microsoft Live Communications Server 2005 only.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
roaming_privacy.reg	positive integer	Null	Specifies the line/registration number which has roaming privacy support enabled. If Null, roaming privacy is disabled. If value < 1, then value is replaced with 1.

<saf/>

The following sampled audio WAVE file (.wav) formats are supported:

- mono 8 kHz G.711 μ-Law
- G.711 A-Law
- L16/16000 (16-bit, 16 kHz sampling rate, mono)
- L16/32000 (16-bit, 32 kHz sampling rate, mono)
- L16/48000 (16-bit, 48 kHz sampling rate, mono)

Note L16/32000 and L16/48000 are supported on SoundStation IP 6000 and 7000 phones.

The phone uses built-in wave files for some sound effects. The built-in wave files can be replaced with files downloaded from the provisioning server or from the Internet, however, these are stored in volatile memory so the files will need to remain accessible should the phone need to be rebooted. Files will be truncated to a maximum size of 300 kilobytes.

In the following table, *x* is the sampled audio file number.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
saf.x	Null OR valid path name OR an RFC 1738-compliant URL to a HTTP, FTP, or TFTP wave file resource. ***Note:*** *Refer to the above wave file format restrictions.*	If Null, the phone will use a built-in file. If set to a path name, the phone will attempt to download this file at boot time from the provisioning server. If set to a URL, the phone will attempt to download this file at boot time from the Internet. ***Note:*** *A TFTP URL is expected to be in the format: tftp://<host>/[pathname]<filename>, for example: tftp://somehost.example.com/sounds/example.wav .*

The following table defines the default usage of the sampled audio files with the phone:

Sampled Audio File	Default use within phone (pattern reference)
1	Ringer 12 (se.pat.misc.welcome)
2	Ringer 13 (se.pat.ringer.ringer15)
3	Ringer 14 (se.pat.ringer.ringer16)
4	Ringer 15 (se.pat.ringer.ringer17)
5	Ringer 16 (se.pat.ringer.ringer18)
6	Ringer 17 (se.pat.ringer.ringer19)
7	Ringer 18 (se.pat.ringer.ringer20)
8	Ringer 19 (se.pat.ringer.ringer21)
9	Ringer 20 (se.pat.ringer.ringer22)
10	Ringer 21 (se.pat.ringer.ringer23)
11	Ringer 22 (se.pat.ringer.ringer24)
12 to 24	Not used.

Note In SIP 3.1, the SoundPoint IP welcome sound was removed from `saf.1` . If you want the welcome sound to be played when a phone reboots or restarts, set `saf.1` to **SoundPointIPWelcome.wav** .

<se/>

The phone uses both synthesized (based on the chord-sets, refer to <chord/> on page A-119) and sampled audio sound effects. Sound effects are defined by patterns: rudimentary sequences of chord-sets, silence periods, and wave files.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
se.appLocalEnabled	0 or 1	1	If set to 1, local user interface sound effects such as confirmation/error tones, will be enabled.
se.destination	“chassis” OR “headset” OR “headset” OR “active”	“chassis”	Transducer or audio device on which sound effects play out.
se.stutterOnVoiceMail	0 or 1	1	If set to 1, stuttered dial tone is used in place of normal dial tone to indicate that one or more messages (voice mail) are waiting at the message center.

This attribute also includes:

- <pat/>
- <rt/>

<pat/>

Patterns use a simple script language that allows different chord sets or wave files to be strung together with periods of silence. The script language uses the following instructions:

Instruction	Meaning	Example
sampled (n)	Play sampled audio file n	`se.pat.misc.SAMPLED_1.inst.1.type` ="sampled" (sampled audio file instruction type) `se.pat.misc.SAMPLED_1.inst.1.value` ="2" (specifies sampled audio file 2)
chord (n, d)	Play chord set n (d is optional and allows the chord set ON duration to be overridden to d milliseconds)	`se.pat.callProg.busyTone.inst.1.type` = "chord" (chord set instruction type) `se.pat.callProg.busyTone.inst.1.value` = "busyTone" `se.pat.callProg.busyTone.inst.y.param` = "2000" (override ON duration of chord set to 2000 milliseconds)
silence (d)	Play silence for d milliseconds (Rx audio is not muted)	`se.pat.callProg.bargeIn.inst.3.type` = "silence" (silence instruction type) `se.pat.callProg.bargeIn.inst.3.value` = "300" (specifies silence is to last 300 milliseconds)
branch (n)	Advance n instructions and execute that instruction (n must be negative and must not branch beyond the first instruction)	`se.pat.callProg.alerting.inst.4.type` = "branch" (branch instruction type) `se.pat.callProg.alerting.inst.4.value` = "-2" (step back 2 instructions and execute that instruction)

In the following table, *x* is the pattern name, *y* is the instruction number. Both *x* and *y* need to be sequential. There are three categories *cat* of sound effect patterns: *callProg* (Call Progress Patterns), *ringer* (Ringer Patterns) and *misc* (Miscellaneous Patterns).

Attribute (bold = change causes restart/reboot)	**Permitted Values**	**Interpretation**	
se.pat.cat.x.name	UTF-8 encoded string	Sound effects name.	
se.pat.cat.x.inst.y.type	“sampled” OR “chord” OR “silence” OR “branch”	Type of sound effect.	
se.pat.cat.x.inst.y.value	integer	Instruction type: sampled chord silence branch	Interpretation: sampled audio file number chord set number silence duration in ms number of instructions to advance

Call Progress Patterns

The following table maps call progress patterns to their usage within the phone.

Call Progress Name	**Description**
“alerting”	Alerting
“bargeIn”	Barge-in tone
“busyTone”	Busy tone
“callWaiting”	Call waiting tone
“callWaitingLong”	Call waiting tone long (distinctive)
“confirmation”	Confirmation tone
“dialTone”	Dial tone
“howler”	Howler tone (off-hook warning)
“intercom”	Intercom announcement tone
“msgWaiting”	Message waiting tone
“precedenceCallWaiting”	Precedence call waiting tone
“precedenceRingback”	Precedence ringback tone

Call Progress Name	Description
“preemption”	Preemption tone
“recWarning”	Record warning
“reorder”	Reorder tone
“ringback”	Ringback tone
“secondaryDialTone”	Secondary dial tone
“stutter”	Stuttered dial tone

Ringer Patterns

The following table maps ringer pattern names to their default descriptions.

Ringer Pattern Name	Description
“ringer1”	Silent ring
“ringer2”	Long single A3 Db3 major warble
“ringer3”	Short double A3 Db3 major warble
“ringer4”	Long single C3 E3 major warble
“ringer5”	Short double C3 E3 major warble
“ringer6”	Long single warble 1
“ringer7”	Short double warble 1
“ringer8”	Long single Gb3 A4 major warble
“ringer9”	Short double Gb3 A4 major warble
“ringer10”	Short double E3 major
“ringer11”	Short triple C3 E3 G3 major ramp
“ringer12”	Short double ringback
“ringer13”	Long single A3 Db3 major warble Precedence
“ringer14”	Splash
“ringer15”	Sampled audio file 1
“ringer16”	Sampled audio file 2
“ringer17”	Sampled audio file 3
“ringer18”	Sampled audio file 4
“ringer19”	Sampled audio file 5
“ringer20”	Sampled audio file 6

Ringer Pattern Name	Description
“ringer21”	Sampled audio file 7
“ringer22”	Sampled audio file 8
“ringer23”	Sampled audio file 9
“ringer24”	Sampled audio file 10

Note

Silent ring will only provide a visual indication of an incoming call, but no audio indication.

Sampled audio files 1 to 10 all use the same built-in file unless that file has been replaced with a downloaded file. For more information, refer to <saf/> on page A-93.

Miscellaneous Patterns

The following table maps miscellaneous patterns to their usage within the phone.

Miscellaneous pattern name	Description
“instant message”	New instant message
“local hold notification”	Local hold notification
“message waiting”	New message waiting indication
“negative confirmation”	Negative confirmation
“positive confirmation”	Positive confirmation
“remote hold notification”	Remote hold notification
“welcome”	Welcome (boot up)

<rt/>

Ring type is used to define a simple class of ring to be applied based on some credentials that are usually carried within the network protocol. The ring class includes attributes such as call-waiting and ringer index, if appropriate. The ring class can use one of four types of ring that are defined as follows:

ring	Play a specified ring pattern or call waiting indication.
visual	Provide only a visual indication (no audio indication) of incoming call (no ringer needs to be specified).
answer	Provide auto-answer on incoming call.
ring-answer	Provide auto answer on incoming call after a ring period.

Note The auto-answer on incoming call is currently only applied if there is no other call in progress on the phone at the time.

In the following table, *x* is the ring class name, which includes "default", "visual", "autoAnswer", "ringAutoAnswer", "internal", "external", "emergency", "precedence", "splash", "profileNormalPBX", "profileNormalAux1", "profileNormalAux2", "profileSilentPBX", "profileSilentAux1", "profileSilentAux2", "profileMeetingPBX", "profilemeetingAux1", "profilemeetingAux2", "profileCustomPBX", "profileCustomAux1", "profileCustomAux2", "profileHeadsetPBX", "profileHeadsetAux1", "profileHeadsetAux2", "profileSpeakerphonePBX", "profileSpeakerphoneAux1", "profileSpeakerphoneAux2", and "custom<*y*>" where *y* is 1 to 17.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
se.rt.enabled	0 or 1	Flag to determine whether or not the ring type feature is enabled within the phone.
se.rt.modification.enabled	0 or 1	Flag to determine whether or not to allow user modification (through phone's user interface) of the pre-defined ring type enabled for modification.
se.rt.x.callWait	enumerated type Refer to **sip-interop.cfg**	The call waiting tone to be used for this class of ring. The call waiting should match one defined in Call Progress Patterns on page A-97. The default call waiting tone is **CallWaiting SE** .
se.rt.x.level	-300 to 500	The gain level for ringing. The default is 0.
se.rt.x.name	UTF-8 encoded string	The answer mode for a ring type. Used for identification purposes in the user interface.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
se.rt.x.ringer	enumerated type Refer to **sip-interop.cfg**	The ring tone to be used for this class of ring. The ringer should match one of Ringer Patterns on page A-98. The default ringer is **ringer2** .
se.rt.x.timeout	1 to 60000 only relevant if the type is set to ring-answer	The duration of the ring in milliseconds before the call is auto answered. The default is 2000..
se.rt.x.type	ring OR visual OR answer OR ring-answer	The answer mode for a ring type as defined in table above.

Note If a phone has been upgraded to Polycom UC software 3.3.0 and then downgraded to SIP 3.2.3 or earlier, the ring type parameters will be unusable due to configuration parameters name changes in UC software 3.3.0 .

<sec/>

This attribute's settings affect security aspects of the phone.

Note As per the standards, you cannot turn off authentication of RTCP.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.tagSerialNo	0 or 1	0	If set to 1, the phone may advertise its serial number (Ethernet address) through protocol signaling. If set to 0, the phone does advertise its serial number.

This attribute also includes:

- <encryption/>
- <pwd/><length/>
- <srtp/>
- <H235/>
- <dot1x/> <eapollogoff/>

- <TLS/>

<encryption/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.encryption.upload.config	0 or 1	0	If set to 0, he phone-specific configuration file created when the user selects **Upload Configuration** is uploaded unencrypted. This will replace whatever phone-specific configuration file is on the server even if it is encrypted. If set to 1, the phone-specific configuration file created when the user selects **Upload Configuration** is uploaded encrypted. This will replace whatever phone-specific configuration file is on the server even if it is unencrypted.
sec.encryption.upload.dir	0 or 1	0	If set to 0, the phone-specific contact directory is uploaded to the server unencrypted regardless of how it was downloaded. This will replace whatever phone-specific contact directory is on the server even if it is encrypted. If set to 1, the phone-specific contact directory is uploaded encrypted regardless of how it was downloaded. This will replace whatever phone-specific contact directory is on the server even if it is unencrypted.
sec.encryption.upload.overrides	0 or 1	0	If set to 0, the phone-specific configuration override file (<Ethernet Address>-phone.cfg) is uploaded unencrypted regardless of how it was downloaded. This will replace the override file on the server even if it is encrypted. If set to 1, the phone-specific configuration override file is uploaded encrypted regardless of how it was downloaded. This will replace the override file on the server even if it is unencrypted.

<pwd/><length/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.pwd.length.admin	0-32	1	Password changes will need to be at least this long. Use 0 to allow null passwords.
sec.pwd.length.user	0-32	2	

<srtp/>

Note As per RFC 3711, you cannot turn off authentication of RTCP.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.srtp.enable	0 or 1	1	If set to 1, the phone accepts SRTP offers. If set to 0, the phone always declines SRTP offers. ***Note**: The default behavior changed in SIP 3.2.0 . In previous SIP releases, the default value was 0 when null or not defined.*
sec.srtp.key.lifetime	0, positive integer minimum 1024 OR power of 2 notation	Null	The master key lifetime used for the cryptographic attribute in the SDP. The value specified is the number of SRTP packets. If set to 0, the master key lifetime is not set. If set to 1 or greater, master key lifetime is set. The default setting should be suitable for most installations. When the lifetime is set greater than 0, a re-invite with a new key will be sent when the number of SRTP packets sent for an outgoing call exceeds half the value of the master key lifetime. For example, 1024 and “2^10” are valid. ***Note**: Setting this parameter to a non-zero value may affect performance of the phone.*

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.srtp.mki.enabled	0 or 1	0	The master key identifier (MKI) is an optional parameter for the cryptographic attribute in the SDP that uniquely identifies the SRTP stream within an SRTP session. MKI is expressed as a pair of decimal numbers in the form: |mki:mki_length| where mki is the MKI value and mki_length its length in bytes. If set to 1, a four-byte MKI parameter is sent within the SDP message of the SIP INVITE / 200 OK. If set to 0, the MKI parameter is not sent.
sec.srtp.offer	0 or 1	0	If set to 1, the phone includes a secure media stream description along with the usual non-secure media description in the SDP of a SIP INVITE. This is for the phone initiating (offering) a phone call. If set to 0, no secure media stream is included in SDP of a SIP invite.
sec.srtp.offer. HMAC_SHA1_32	0 or 1	0	If set to 1, a crypto line with the AES_CM_128_HMAC_SHA1_32 crypto-suite will be included in offered SDP. If set to 0, the crypto line is not included. ***Note:*** *This parameter was added in SIP 2.2.1 .*
sec.srtp.offer. HMAC_SHA1_80	0 or 1	1	If set to 1, a crypto line with the AES_CM_128_HMAC_SHA1_80 crypto-suite will be included in offered SDP. If set to 0, the crypto line is not included. ***Note:*** *This parameter was added in SIP 2.2.1 .*
sec.srtp.require	0 or 1	0	If set to 1, the phone is only allowed to use secure media streams. Any offered SIP INVITEs must include a secure media description in the SDP or the call will be rejected. For outgoing calls, only a secure media stream description is include in the SDP of the SIP INVITE, meaning that the non-secure media description is not included. If `sec.srtp.require` is set to 1, `sec.srtp.offer` is logically set to 1 no matter what the value in the configuration file. If set to 0, secure media streams are not required.
sec.srtp. requireMatchingTag	0 or 1	1	A flag to determine whether or not to check the tag value in the crypto attribute in an SDP answer. If set to 1, the tag values must match. If set to 0, the tag value is ignored.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.srtp.sessionParams. noAuth.offer	0 or 1	0	If set to 1, no authentication of RTP is offered. A session description that includes the UNAUTHENTICATED_SRTP session parameter is sent when initiating a call. If set to 0, authentication is offered.
sec.srtp.sessionParams. noAuth.require	0 or 1	0	If set to 1, no authentication of RTP is required. A call placed to a phone configured with `noAuth.require` must offer the UNAUTHENTICATED_SRTP session parameter in its SDP. If `sec.srtp.sessionParams.noAuth.require` is set to 1, `sec.srtp.sessionParams.noAuth.offer` is logically set to 1 no matter what the value in the configuration file. If set to 0, authentication is required.
sec.srtp.sessionParams. noEncrypRTCP.offer	0 or 1	0	If set to 1, no encryption of RTCP is offered. A session description that includes the UNENCRYPTED_SRTCP session parameter is sent when initiating a call. If set to 0, encryption of RTCP is offered.
sec.srtp.sessionParams. noEncrypRTCP.require	0 or 1	0	If set to 1, no encryption of RTCP is required. A call placed to a phone configured with noAuth.require must offer the UNENCRYPTED_SRTCP session parameter in its SDP. If `sec.srtp.sessionParams.noEncryptRTCP.require` is set to 1, `sec.srtp.sessionParams.noEncryptRTCP.offer` is logically set to 1 no matter what the value in the configuration file. If set to 0, encryption of RTCP is required.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.srtp.sessionParams. noEncrypRTP.offer	0 or 1	0	If set to 1, no encryption of RTP is offered. A session description that includes the UNENCRYPTED_SRTP session parameter is sent when initiating a call. If set to 0, encryption of RTP is offered.
sec.srtp.sessionParams. noEncrypRTP.require	0 or 1	0	If set to 1, no encryption of RTP is required. A call placed to a phone configured with `noAuth.require` must offer the UNENCRYPTED_SRTP session parameter in its SDP. If `sec.srtp.sessionParams.noEncryptRTP.require` is set to 1, `sec.srtp.sessionParams.noEncryptRTP.offer` is logically set to 1 no matter what the value in the configuration file. If set to 0, encryption of RTP is required.

<H235/>

Note

At this time, this attribute is used with the Polycom VVX 1500 phone only.

The H.235 Voice Profile implementation is Polycom HDX-compatible. OpenSSL-based Diffie-Hellman key exchange and AES-128 CBC encryption algorithms is used to encrypt the RTP media

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.H235. mediaEncryption. enabled	0 or 1	1	If set to 1, H.235 Voice Profile RTP media encryption will be enabled. When enabled, media encryption will be negotiated when such encryption is requested by the far end.
sec.H235. mediaEncryption.offer	0 or 1	0	If set to 1 and `sec.H235.mediaEncryption.enabled` is also set to 1, media encryption negotiations will be initiated with the far end;however, successful negotiations is not a requirement for the call to complete.
sec.H235. mediaEncryption.require	0 or 1	0	If set to 1 and `sec.H235.mediaEncryption.enabled` is also set to 1, media encryption negotiations will be initiated or completed with the far end, and if negotiations fail, the call will be dropped.

<dot1x/> <eapollogoff/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.dot1x.eapollogoff. enabled	0 or 1	0	When set to 1, the feature is enabled and phone will send EAPOL-Logoff message on behalf of the disconnected supplicant.
sec.dot1x.eapollogoff. lanlinkreset	0 or 1	0	When set to 1, the application will reset (recycle) the LAN port link in application initiation stage.

<TLS/>

For the list of supported ciphers, refer to Configurable TLS Cipher Suites on page 4-100.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
sec.TLS.browser. cipherList	String	NoCipher	Cipher list for browser.
sec.TLS.cipherList	String	"ALL:!DH:!LOW:!EXP:!MD5:@STRENGTH"	Global cipher list parameter.
sec.TLS.LDAP. cipherList	String	NoCipher	Cipher list for corporate directory.
sec.TLS.prov. cipherList	String	NoCipher	Cipher list for provisioning.
sec.TLS.SIP. cipherList	String	NoCipher	Cipher list for SIP.
sec.TLS.syslog. cipherList	String	NoCipher	Cipher list for syslog.
sec.TLS.xmpp. cipherList	String	NoCipher	Cipher list for CMA presence.

<softkey/>

Note `feature.enhancedFeatureKeys.enabled` must be enabled to use the Configurable Soft Key feature. Refer to <feature/> on page A-58.

This configuration attribute is defined as follows (where x =1 to maximum number of defined soft keys):

Attribute (bold = change causes restart/reboot)	**Permitted Values**	**Default**	**Interpretation**
softkey.feature. basicCallManagement.redundant	0 or 1	1	If set to 0 and the phone has hard keys mapped for **Hold**, **Transfer**, and **Conference** functions (all must be mapped), all of these soft keys are not displayed. If set to 1, all of these soft keys are displayed.
softkey.feature.buddies	0 or 1	1	If set to 0, the **Buddies** soft key is not displayed. If set to 1, the **Buddies** soft key is displayed. ***Note**: `pres.idleSoftKeys` must be set to 1 for this soft key to be displayed*.
softkey.feature.callers	0 or 1	0	If set to 0, the **Callers** soft key is not displayed on any phone except SoundPoint IP 32x/33x phones. If set to 1, the **Callers** soft key is displayed on all phones as follows: • In the idle state, it is displayed after the **New Call** soft key and before the **Dir** soft key. • In the dialtone state, it is displayed after the **End Call soft key** and before the **Dir** soft key. • During a conference or transfer, it is displayed before the **Cancel** soft key. ***Note**: Model-specific parameters are defined for the SoundPoint IP 32x/33x phones and their default value is 1.*

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
softkey.feature.directories	0 or 1	0	If set to 0, the **Dir** soft key is not displayed on any phone except SoundPoint IP 32x/33x phones. If set to 1, the **Dir** soft key is displayed on all phones as follows: • In the idle state, it is displayed after the **New Call** and **Callers** soft keys. • In the dialtone state, it is displayed after the **End Call** and **Callers** soft keys. • During a conference or transfer, it is displayed after the **Callers** and **Cancel** soft keys. ***Note**: Model-specific parameters are defined for the SoundPoint IP 32x/33x phones and their default value is 1.*
softkey.feature.endcall	0 or 1	1	If set to 0, the **End Call** soft key is not displayed. If set to 1, the **EndCall** soft key is displayed.
softkey.feature.forward	0 or 1	1	If set to 0, the **Forward** soft key is not displayed. If set to 1, the **Forward** soft key is displayed.
softkey.feature.join	0 or 1	1	If set to 0, the **Join** soft key is not displayed. If set to 1, the **Join** soft key is displayed.
softkey.feature.mystatus	0 or 1	1	If set to 0, the **MyStatus** soft key is not displayed. If set to 1, the **MyStatus** soft key is displayed. ***Note**:* `pres.idleSoftKeys` *must be set to 1 for this soft key to be displayed*.
softkey.feature.newcall	0 or 1	1	If set to 0, the **New Call** soft key is not displayed when there is another way to place a call. If set to 1, the **New Call** soft key is displayed.
softkey.feature.split	0 or 1	1	If set to 0, the **Split** soft key is not displayed. If set to 1, the **Split** soft key is displayed.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
softkey.x.action	string	Null	The same syntax as the enhanced feature key action. For more information, refer to Macro Definition on page A-56.
softkey.x.enable	0 or 1	0	If set to 0, the soft key is disabled. If set to 1, the soft key is enabled.
softkey.x.label	string	Null	This is the text displayed with the soft key. If set to Null, the label to display is determined as follows: • If the soft key is mapped to a enhanced feature key macro, the label of the enhanced feature key macro will be used. • If the soft key is mapped to a speed dial, the label of the corresponding directory entry will be used. If this label does not exist as well and the directory entry is a enhanced feature key macro, then the label of the enhanced feature key macro will be used. • If the soft key is mapped to chained actions, only the first one is considered for label, using the rules above. • If no labels are found after the above steps, the soft key label will be blank.
softkey.x.precede	0 or 1	0	If set to 0, the soft key replaces any empty space from the leftmost position. If set to 1, the soft key is displayed before the first standard soft key.
softkey.x.use.active	0 or 1	0	If set to 0, the soft key is not displayed in the active call state. If set to 1, the soft key is displayed in the active call state.
softkey.x.use.alerting	0 or 1	0	If set to 0, the soft key is not displayed in the alerting state. If set to 1, the soft key is displayed in the alerting state.
softkey.x.use.dialtone	0 or 1	0	If set to 0, the soft key is not displayed in the dialtone state. If set to 1, the soft key is displayed in the dialtone state.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
softkey.x.use.hold	0 or 1	0	If set to 0, the soft key is not displayed in the hold state. If set to 1, the soft key is displayed in the hold state.
softkey.x.use.idle	0 or 1	0	If set to 0, the soft key is not displayed in the idle state. If set to 1, the soft key is displayed in the idle state.
softkey.x.use.proceeding	0 or 1	0	If set to 0, the soft key is not displayed in the proceeding state. If set to 1, the soft key is displayed in the proceeding state.
softkey.x.use.setup	0 or 1	0	If set to 0, the soft key is not displayed in the setup state. If set to 1, the soft key is displayed in the setup state.

<tcpIpApp/>

This attribute includes:

- <dns/>
- <sntp/>
- <port/>
- <keepalive/>

<dns/>

The <dns/> attribute provides another way to set Domain Name System (DNS). However, any values set through DHCP will have a higher priority and any values set through the <device/> parameter will have a lower priority.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
tcpIpApp.dns.server	dotted-decimal IP address	Null	Primary server to which the phone directs DNS queries.
tcpIpApp.dns.altServer	dotted-decimal IP address	Null	Secondary server to which the phone directs DNS queries.
tcpIpApp.dns.domain	string	Null	The phone's DNS domain.

<sntp/>

The following table describes the parameters used to set up time synchronization and daylight savings time. The defaults shown will enable daylight savings time (DST) for North America.

Daylight savings defaults:

- Do not use fixed day, use first or last day of week in the month.
- Start DST on the second Sunday in March at 2 am.
- Stop DST on the first Sunday in November at 2 am.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
tcpIpApp.sntp.address	valid host name or IP address	clock	Address of the SNTP server.
tcpIpApp.sntp.address.overrideDHCP	0 or 1	0	These parameters determine whether configuration file parameters override DHCP parameters for the SNTP server address and Greenwich Mean Time (GMT) offset. If set to 0, DHCP values will override configuration file parameters. If set to 1, the configuration file parameters will override DHCP values.
tcpIpApp.sntp.daylightSavings.enable	0 or 1	1	If set to 1, apply daylight savings rules to displayed time.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
tcpIpApp.sntp.daylightSavings.fixedDayEnable	0 or 1	0	If set to 0, month, date, and dayOfWeek are used in DST date calculation. If set to 1, then only month and date are used.
tcpIpApp.sntp.daylightSavings.start.date	1 to 31	8	If `fixedDayEnable` is set to 1, use as day of the month to start DST. If `fixedDayEnable` is set to 0, us the mapping: 1 = the first occurrence of a given day-of-the-week in a month, 8 = the second occurrence of a given day-of-the-week in a month, 15 = the third occurrence of a given day-of-the-week in a month, 22 = the fourth occurrence of a given day-of-the-week in a month
tcpIpApp.sntp.daylightSavings.start.dayOfWeek	1 to 7	1	Day of week to apply DST. Mapping: 1=Sun, 2=Mon, ..., 7=Sat
tcpIpApp.sntp.daylightSavings.start.dayOfWeek.lastInMonth	0 or 1	0	If set to 1 and fixedDayEnable is set to 0, DST starts on the last day (specified by `start.dayOfWeek`) of the week in the month. The `start.date` is ignored.
tcpIpApp.sntp.daylightSavings.start.month	1 to 12	3 (March)	Month to start DST. Mapping: 1=Jan, 2=Feb, ..., 12=Dec
tcpIpApp.sntp.daylightSavings.start.time	0 to 23	2	Time of day to start DST in 24 hour clock. Mapping: 2=2 am, 14=2 pm
tcpIpApp.sntp.daylightSavings.stop.date	1 to 31	1	Day of the month to stop DST.
tcpIpApp.sntp.daylightSavings.stop.dayOfWeek	1 to 7	1	Day of week to stop DST.
tcpIpApp.sntp.daylightSavings.stop.dayOfWeek.lastInMonth	0 or 1	0	If set to 1 and fixedDayEnable set to 0, DST stops on the last day (specified by `stop.dayOfWeek`) of the week in the month. The `stop.date` is ignored.
tcpIpApp.sntp.daylightSavings.stop.month	1 to 12	11	Month to stop DST.
tcpIpApp.sntp.daylightSavings.stop.time	0 to 23	2	Time of day to stop DST in 24 hour clock.
tcpIpApp.sntp.gmtOffset	positive or negative integer	0	Offset in seconds of the local time zone from GMT. 3600 seconds = 1 hour

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
tcpIpApp.sntp.gmtOffset. overrideDHCP	0 or 1	0	These parameters determine whether configuration file parameters override DHCP parameters for the SNTP server address and GMT offset. If set to 0, DHCP values will override configuration file parameters. If set to 1, the configuration file parameters will override DHCP values.
tcpIpApp.sntp.resyncPeriod	positive integer	86400 (24 hours)	Time in seconds between Simple Network Time Protocol (SNTP) re-syncs.

<port/>

This attribute includes:

- <rtp/>

<rtp/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
tcpIpApp.port.rtp.filterByIp	0 or 1	1	If set to 1, reject RTP packets arriving from (sent from) a non-negotiated (through SDP) IP address.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
tcpIpApp.port.rtp.filterByPort	0 or 1	0	If set to 1, reject RTP packets arriving from (sent from) a non-negotiated (through SDP) port.
tcpIpApp.port.rtp.forceSend	0 to 65535	0	Send all RTP packets to, and expect all RTP packets to arrive on, the specified port. ***Note:*** *Both tcpIpApp.port.rtp.filterByIp and tcpIpApp.port.rtp.filterByPort must be enabled for this to work.*
tcpIpApp.port.rtp.mediaPortRangeStart	even integer from 1024 to 65440	2222	The specified port. Ports will be allocated from a pool starting with the specified port up to a value of (start-port + 47) for a voice-only phone or (start-port + 95) for a video phone. ***Note****: Ensure that there is no contention for port numbers. For example, do not use 5060 (default port for SIP).*

<keepalive/>

Allowing for the configuration of TCP keep-alive on SIP TLS connections, the phone can detect a failures quickly (in minutes) and attempt to re-register with the SIP call server (or its redundant pair).

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
tcpIpApp.keepalive.tcp. idleTransmitInterval	10 to 7200	30	After idle x seconds, the keep-alive message is sent to the call server. ***Note**: If this parameter is set to a value that is out of range, the default value is used.* ***Note:** On the VVX 1500 phone, `tcpIpApp.keepalive.tcp.idleTransmitInterval` is the number of seconds TCP waits between the last datat packet is transmitted and the transmission of the first keep-alive packet.*
tcpIpApp.keepalive.tcp. noResponseTransmitInterval	5 to 120	20	If no response is received to keep-alive message, another keep-alive message is sent to the call server after x seconds. ***Note**: If this parameter is set to a value that is out of range, the default value is used.* ***Note:** On the VVX 1500 phone, `tcpIpApp.keepalive.tcp.noResponseTransmitInterval` is the amount of idle time between the transmission of the keep-alive packets the TCP stack waits. This applies regardless of the last keep-alive being acknowledged or not.*
tcpIpApp.keepalive.tcp.sip.tls.enable	0 or 1	0	If set to 1, enable TCP keep-alive for SIP signaling connections that use TLS transport. If set to 0, disable TCP keep-alive for SIP signaling connections that use TLS transport.

<tones/>

This attribute describes configuration items for the tone resources available in the phone.

This attribute includes:

- <DTMF/>
- <chord/>

<DTMF/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
tone.dtmf.chassis.masking	0 or 1	0	If set to 1, DTMF tones will be substituted with a non-DTMF pacifier tone when dialing in hands-free mode. This prevents DTMF digits being broadcast to other surrounding telephony devices or being inadvertently transmitted in-band due to local acoustic echo. ***Note:*** *tone.dtmf.chassis.masking should only be enabled when tone.dtmf.viaRtp is disabled.*
tone.dtmf.level	-33 to 3	-15	Level of the high frequency component of the DTMF digit measured in dBm0; the low frequency tone will be two dB lower.
tone.dtmf.offTime	positive integer	50	When a sequence of DTMF tones is played out automatically, this is the length of time in milliseconds the phone will pause between digits; this is also the minimum inter-digit time when dialing manually.
tone.dtmf.onTime	positive integer	50	When a sequence of DTMF tones is played out automatically, this is the length of time in milliseconds the tones will be generated for; this is also the minimum time the tone will be played for when dialing manually (even if key press is shorter).

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
tone.dtmf.rfc2833Control	0 or 1	1	If set to 1, the phone will indicate a preference for encoding DTMF through RFC 2833 format in its Session Description Protocol (SDP) offers by showing support for the phone-event payload type; this does not affect SDP answers, these will always honor the DTMF format present in the offer since the phone has native support for RFC 2833.
tone.dtmf.rfc2833Payload	96-127	127	The phone-event payload encoding in the dynamic range to be used in SDP offers.
tone.dtmf.viaRtp	0 or 1	1	If set to 1, encode DTMF in the active RTP stream, otherwise, DTMF may be encoded within the signaling protocol only when the protocol offers the option. ***Note:*** *tone.dtmf.chassis.masking should be enabled when tone.dtmf.viaRtp is disabled.*

<chord/>

Chord-sets are the building blocks of sound effects that use synthesized rather than sampled audio (most call progress and ringer sound effects). A chord-set is a multi-frequency note with an optional on/off cadence. A chord-set can contain up to four frequency components generated simultaneously, each with its own level.

There are two blocks of chord sets:

- callProg (used for call progress sound effect patterns)
- ringer

All three blocks use the same chord set specification format.

In the following table:

- when *x* is "callProg":
  - *y* can be "dialTone", "busyTone", "ringback", "reorder", "stutter_3", "callWaiting", "callWaitingLong", "recWarning", "stutterLong", "intercom", "precedenceCallWaiting", "preemption", "precedenceRingback", or "spare<*x*>" where *x* is 1 to 6.
- when *x* is "ringer"

  - *y* can be "F2", "Gb2", G2", "Ab2", "A3", Bb3", "B3", C3", "Db3", "D3", Eb3", "E3", "F3", "Gb3", "G3", "Ab3", "A4", "Bb4", "B4", C4", "Db4", "D4", "Eb4", "E4", "F4", "A3Major", "Bb3Major", "B3Major", "C3Major", "Db3Major", "D3Major, "Eb3Major", "E3Major", "F3Major", "Gb3Major", "G3Major", "Ab3Major", "A4Major", "splash", "ringback", "originalLow", "originalHigh", or "spare<*x*>" where *x* is 1 to 19.

- when *x* is "misc"
  - *y* can be "spare<*x*>" where *x* is 1 to 9.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
tone.chord.*x*.y.freq.z	0-1600	Frequency for this component in Hertz; up to six chord-set components can be specified (z=1 to 6).
tone.chord.x.y.level.z	-57 to 3	Level of this component in dBm0.
tone.chord.x.y.onDur	positive integer	On duration in milliseconds, 0=infinite.
tone.chord.*x*.y.offDur	positive integer	Off duration in milliseconds, 0=infinite.
tone.chord.*x*.y.repeat	positive integer	Specifies how many times the ON/OFF cadence is repeated, 0=infinite.

<up/>

This per-site configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
up.accessibilityFeatures	0 or 1	0	If set to 1 and call is received, the background screen flashes in orange. ***Note**: This parameter is supported on the Polycom VVX 1500 only.*
up.analogHeadsetOption	0, 1, or 2	0	Selects optional external hardware for use with a headset attached to the phone's analog headset jack. If set to 0, no compatible headset is attached. If set to 1, a DHSG-compatible headset is attached and can be used as an electronic hookswitch. If set to 2, a Plantronics compatible headset is attached and can be used an electronic hookswitch.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
up.audioMode	0 or 1	0	Flag to determine whether a handset (0) or a headset (1) is connected.
up.audioSetup.auxInput	0 - Other Input, 1 - Polycom Wireless Mic, 2 - off	2	Auxiliary audio input on Polycom SoundStation IP phones only.
up.audioSetup.auxOutput	0 - Other Input, 1 - Polycom Wireless Mic, 2 - off	2	Auxiliary audio output on Polycom SoundStation IP phones only..
up.backlight.idleIntensity	0 (off), 1 (low), 2 (medium), 3 (high)	1	This parameter controls the intensity of the LCD backlight when the phone is idle. ***Note:*** *If idleIntensity is set higher than onIntensity, it will be replaced with the onIntensity value*.
up.backlight.onIntensity	0 (off), 1 (low), 2 (medium), 3 (high)	3	This parameter controls the intensity of the LCD backlight when it turns on during normal use of the phone.
up.callTypeOrderVoice	0 to 2	2	Determine whether to use SIP or the HDX PSTN interface for voice calls. Used by the SoundStation IP 7000 phone only.
up.callTypePromptPref	0 or 1	1	A flag to determine which interface is used to place calls. If set to 1, the voice interface is used. If set to 0, the video interface is used to place calls during hot-dialing or if the use presses the off-hook key on the SoundStation IP 7000 phone. ***Note****: This parameter is supported on the SoundStation IP 7000 only.*
up.enableCallTypePrompt	0 or 1	1	Enable the call type prompt. If set to 1, the call type prompt is enabled. If set to 0, the call type prompt is disabled. ***Note****: This parameter is supported on the SoundStation IP 7000 only.*
up.handsfreeMode	0 or 1	1	If set to 1, hands-free speakerphone is enabled. If set to 0, hands-free speakerphone is disabled.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
up.headsetMode	0 or 1	0	If set to 1, the headset will be selected as the preferred transducer after its first use until the headset key is pressed again; otherwise, hands-free will be selected preferentially over the headset.
up.idleBrowser.enabled	0 or 1	0	Flag to determine whether or not the background takes priority over the idle browser. Used in conjunction with `up.prioritizeBackground.enable` .
up.idleTimeout	positive integer, seconds	40	Timeout for the idle display or default call handling display. If set to 0, there is no timeout. If set to value greater than 0, the timeout is for that number of seconds (maximum 65535).
up.lineKeyCallTerminate	0 or 1	0	Flag to determine whether or not pressing of line key will end an active call. If set to 1, pressing the line key will end an active call. The default value of 0 preserves the previous behaviour.
up.localClockEnabled	0 or 1	1	Flag to determine whether or not the date and time are displayed on the idle display. If set to 1, date and time are displayed.
up.manualProtocolRouting	0 or 1	1	If set to 1, the user is presented with protocol routing choices when a call could be placed with more than one protocol from its current context. The user must choose between SIP and H.323 to place a call. ***Note**: This parameter is supported on the Polycom VVX 1500 only.*
up.manualProtocolRouting. softKeys	0 or 1	1	If set to 1 and `up.manualProtocolRouting` is set to 1, soft keys are used to provide the user with a routing choice. If set to 0, a routing confirmation dialog is presented with a choice for each possible routing. ***Note**: This parameter is supported on the Polycom VVX 1500 only.*

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
up.mwiVisible	0 or 1	0	If set is 0, the incoming MWI notifications for lines where the MWI callback mode is disabled (`msg.mwi.x.callBackMode` is set to 0) are ignored, and do not appear in the message retrieval menus. If set to 1, the MWI for lines whose MWI is disabled is displayed (pre-SIP 2.1 behavior), even though MWI notifications have been received for those lines.
up.numberFirstCID	0 or 1	0	If set to 0, caller ID display will show caller's name first. If set to 1, caller ID display will show caller's number first.
up.offHookAction.none	0 or 1	0	If set to 1, there is no sound from the phone. When the user lifts the handset, the phone does not seize the line and the ringer continues its current activity until the user takes further action. If set to 0, the behavior will be as it was in SIP 2.1.2 .
up.oneTouchVoiceMail	0 or 1	0	If set to 1, the voice mail summary display is bypassed and voice mail is dialed directly (if configured).
up.pictureFrame.timePerImage	3 to 300 seconds	5	The time to display the image. ***Note**: This parameter is supported on the Polycom VVX 1500 only.*
up.pictureFrame.folder	string	Null	The path name for images. The maximum length is 40 characters. If set to Null, images stored in the root folder on the USB flash drive are displayed. For example, if the images are stored in the "/images/phone" folder on the USB flash drive, set `up.pictureFrame.folder` to **images/phone** . ***Note**: This parameter is supported on the Polycom VVX 1500 only.*
up. prioritizeBackgroundMenuItem .enable	0 or 1	1	If set to 1, the "Prioritize Background" menu is available to the user. The user can then decide whether or not the background takes priority over the idle browser. Used in conjunction with `up.idleBrowser.enabled` .

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
up.screenCapture.enabled	0 or 1	0	Flag to determine whether or not the user can get a screen capture of the current screen shown on a phone. The flag is cleared when the phone reboots. If set to 1, the "Screen Capture" menu is available to the user. Refer to Capturing Phone's Current Screen on page C-28.
up.screenSaver.enabled	0 or 1	0	If set to 1, a USB flash drive is attached to the phone, and the idle browser is not configured, a slide show will cycle through the images from the USB flash drive. The images must stored in the appropriate directory of the USB flash drive (`up.pictureFrame.folder` in **phone1.cfg**). The slide show does not appear when the phone is in the active state. If set to 1, but there is no USB flash drive attached to the phone, there is not change on the screen. However, the screen saver will start working once a USB flash drive is attached. If set to 0, the feature is disabled. ***Note**: This parameter is supported on the Polycom VVX 1500 only.* ***Note**: If the idle browser is also enabled, the idle browser is displayed until the screen saver times out; then the screen saver appears. When the screen saver exits, the idle browser is displayed again and is up to date (it is refreshed in the background).*
up.screenSaver.waitTime	1 to 9999, minutes	15	The time to wait (In minutes) in the idle state (until the screen saver starts). ***Note**: This parameter is supported on the Polycom VVX 1500 only.*
up.toneControl.bass	-4 to 4, Null	0	Bass equalization control. Each step is an increment of 1 dB at 225 kHz and 2 dB < 225 Hz.
up.toneControl.treble	-4 to 4, Null	0	Treble equalization control. Each step is an increment of 1 dB at 3.7 kHz and 2 dB > 10 kHz.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
up.useDirectoryNames	0 or 1	0	If set to 1, the name fields of the local contact directory entries which match incoming calls will be used for caller identification display and in the call lists instead of the name provided through network signaling. ***Note**: There is no matching of outgoing calls. There is no matching to corporate directory entries.*
up.welcomeSoundEnabled	0 or 1	1	If set to 1, play welcome sound effect after a reboot.
up. welcomeSoundOnWarmBoot Enabled	0 or 1	0	If set to 1, play welcome sound effect on warm and cold boots. If set to 0, only a cold reboot will trigger the welcome sound effect.

<video/>

Note This attribute is only supported for use on the Polycom VVX 1500.

These configuration attributes are defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
video.autoFullScreen	0 or 1	0	Flag to determine whether or not video calls use the full screen layout. If set to 1, video calls will use the full screen layout by default. When a video call is first created (upon discovery that far-end is video capable) or when an audio call transitions to a video call (through far-end transfer), the full screen layout will be used. If set to 0, video calls only use the full screen layout if it is selected by the user.
video.autoStartVideoTx	0 or 1	1	Flag to determine whether or not video transmission occurs when a call starts. If set to 0, video transmission does not start. If set to 1, video transmission from the near end starts when a call starts.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
video.callRate	128 to 1024 kbps	512	The maximum call rate in kbps to use when initially negotiating the bandwidth for a video call. This value cannot exceed `video.maxCallRate`.
video.enable	0=Disable, 1=Enable	1	Flag to determine whether or not video calls are established. This applies to all calls, between two Polycom VVX 1500s and between a Polycom VVX 1500 and any other video device. If set to 1, video is sent in outgoing calls and received in incoming calls. If set to 0, video is not sent in outgoing calls and not received in incoming calls. All calls are audio only.
video. forceRtcpVideoCodecControl	0 or 1	0	If set to 1, force the Polycom VVX 1500 to send RTCP feedback messages to request fast update I-frames for all video calls.
video.maxCallRate	128 to 1024 kbps	768	Limits the maximum network bandwidth used in a call. It is used in the SDP bandwidth signaling. If honored by the far end, both Rx and Tx network bandwidth used in a call will not exceed this value (in kbps).
video.quality	"motion", "sharpness"	Null	Determine the quality of video shown in a call or conference. Use "motion" for people or other video with motion. Use "sharpness" or Null for video with little or no movement. Moderate to heavy motion can cause some frames to be dropped.
video.screenMode	"normal", "full", "crop"	"normal"	Applies to the video window shown in the normal mode. If set to "normal" or Null, all pixels are displayed, black bars appear on the top, bottom, or sides of the window, if necessary, to maintain the correct aspect ratio. If set to "full", all pixels are displayed and the image is stretched linearly and independently to fill the video frame. If set to "crop", the black bars do not appear, the image size is re-sized to maintain the correct aspect ratio, and any parts of the image that do not fit in the display are cropped.
video.screenModeFS	"normal", "full", "crop"	"normal"	Applies to the video window in Full Screen mode. The image is re-sized to maintain the correct aspect ratio and any parts of the image that do not fit in the display are cropped.

These attributes also include:

- <codecs/>
- <camera/>
- <localCameraView/>

<codecs/>

These codecs include:

- <codecPref/>
- <profile/>

<codecPref/>

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
video.codecPref.H261	1 to 4	4	Specifies the video codec preferences for the Polycom VVX 1500 phone.
video.codecPref.H264		1	
video.codecPref.H2631998		2	
video.codecPref.H263		3	

Note Codecs with a default of Null are available for test purposes only and are not expected to be used in your deployment.

<profile/>

The profile attributes can be adjusted for each of the new supported video codecs.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
video.profile.H261.annexD	0 or 1 (default)	This value is H261 format parameter ANNEXD used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H261.CifMpi	1 (default) to 32	This value is H261 format parameter CIF used to signal Polycom VVX 1500 phone receiving capability in SDP. This value also controls the TX frame size. If set to 1, CIF is used (provided the far end supports CIF=1); otherwise QCIF is used.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
video.profile.H261.jitterBufferMax	(`video.profile.H261.jitterBufferMin` + 500ms) to 2500ms, default 2000ms	The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size will always cause lost packets. This parameter should be set to the smallest possible value that will support the expected network jitter.
video.profile.H261.jitterBufferMin	33ms to 1000ms, default 150ms	The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. Once this depth has been achieved initially, the depth may fall below this point and play out will still continue. This parameter should be set to the smallest possible value which is at least two packet payloads, and larger than the expected short term average jitter.
video.profile.H261.jitterBufferShrink	33ms to 1000ms, default 70ms	The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. Use smaller values (33 ms) to minimize the delay on known good networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).
video.profile.H261.payloadType	0 to 127, default 31	RTP payload format type for H261 MIME type.
video.profile.H261.QcifMpi	1 (default) to 32	This value is H261 format parameter QCIF used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H263.CifMpi	1 (default) to 32	This value is H263/90000 format parameter CIF used to signal Polycom VVX 1500 phone receiving capability in SDP. This value also controls the TX frame size. If set to 1, CIF is used (provided the far end supports CIF=1); otherwise QCIF is used.
video.profile.H263.jitterBufferMax	(`video.profile.H263.jitterBufferMin` + 500ms) to 2500ms, default 2000ms	The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size will always cause lost packets. This parameter should be set to the smallest possible value that will support the expected network jitter.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
video.profile.H263.jitterBufferMin	33ms to 1000ms, default 150ms	The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. Once this depth has been achieved initially, the depth may fall below this point and play out will still continue. This parameter should be set to the smallest possible value which is at least two packet payloads, and larger than the expected short term average jitter.
video.profile.H263.jitterBufferShrink	33ms to 1000ms, default 70ms	The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. Use smaller values (33 ms) to minimize the delay on known good networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).
video.profile.H263.payloadType	0 to 127, default 34	RTP payload format type for H263 MIME type.
video.profile.H263.QcifMpi	1 (default) to 32	This value is H263/90000 format parameter QCIF used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H263.SqcifMpi	1 (default) to 32	This value is H263/90000 format parameter SQCIF used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H2631998.annexF	0 (default) or 1	This value is H263-1998/90000 format parameter ANNEXF used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H2631998.annexI	0 (default) or 1	This value is H263-1998/90000 format parameter ANNEXI used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H2631998.annexJ	0 (default) or 1	This value is H263-1998/90000 format parameter ANNEXJ used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H2631998.annexK	0, 1 (default), 2, 3, 4	This value is H263-1998/90000 format parameter ANNEXK used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H2631998.annexN	0, 1 (default), 2, 3, 4	This value is H263-1998/90000 format parameter ANNEXN used to signal Polycom VVX 1500 phone receiving capability in the SDP.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
video.profile.H2631998.annexT	0 (default) or 1	This value is H263-1998/90000 format parameter ANNEXT used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H2631998.CifMpi	1 (default) to 32	This value is H263-1998/90000 format parameter CIF used to signal Polycom VVX 1500 phone receiving capability in SDP. This value also controls the TX frame size. If set to 1, CIF is used (provided the far end supports CIF=1); otherwise QCIF is used.
video.profile.H2631998.jitterBufferMax	(`video.profile.H2631998.jitterBufferMin` + 500ms) to 2500ms, default 2000ms	The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size will always cause lost packets. This parameter should be set to the smallest possible value that will support the expected network jitter.
video.profile.H2631998.jitterBufferMin	33ms to 1000ms, default 150ms	The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. Once this depth has been achieved initially, the depth may fall below this point and play out will still continue. This parameter should be set to the smallest possible value which is at least two packet payloads, and larger than the expected short term average jitter.
video.profile.H2631998.jitterBufferShrink	33ms to 1000ms, default 70ms	The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. Use smaller values (33 ms) to minimize the delay on known good networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).
video.profile.H2631998.payloadType	96 (default) to 127	RTP payload format type for H263-1998/90000 MIME type.
video.profile.H2631998.QcifMpi	1 (default) to 32	This value is H263-1998/90000 format parameter QCIF used to signal Polycom VVX 1500 phone receiving capability in the SDP.
video.profile.H2631998.SqcifMpi	1 (default) to 32	This value is H263-1998/90000 format parameter SQCIF used to signal Polycom VVX 1500 phone receiving capability in the SDP.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
video.profile.H264.jitterBufferMax	(`video.profile.H264.jitterBufferMin` + 500ms) to 2500ms, default 2000ms	The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size will always cause lost packets. This parameter should be set to the smallest possible value that will support the expected network jitter.
video.profile.H264.jitterBufferMin	33ms to 1000ms, default 150ms	The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. Once this depth has been achieved initially, the depth may fall below this point and play out will still continue. This parameter should be set to the smallest possible value which is at least two packet payloads, and larger than the expected short term average jitter.
video.profile.H264.jitterBufferShrink	33ms to 1000ms, default 70ms	The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. Use smaller values (33 ms) to minimize the delay on known good networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).
video.profile.H264.payloadType	96 to 127, default 109	RTP payload format type for H264/90000 MIME type.
video.profile.H264.profileLevel	1, 1b, 1.1, 1.2, 1.3 (default)	This value is H.264's level used in the phone. The Level is a constraint set to selected key algorithm parameters, codec in different level has different ability, at this time Polycom VVX 1500 support these level (1,1b,1.1,1.2,1.3), as to detailed level definition. For more information, refer to ITU-T H.264.

<camera/>

These settings control the performance of the camera.

These configuration attributes are defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
video.camera.brightness	0 to 6	3	Set brightness level. The value range is from 0 (Dimmest) to 6 (Brightest).
video.camera.contrast	0 to 4	0	Set contrast level. The value range is from 0 (No contrast increase) to 3 (Most contrast increase, and 4 (Noise reduction contrast).
video.camera. flickerAvoidance	0 to 2	0	Set flicker avoidance. If set to 0, flicker avoidance is automatic. If set to 1, 50hz AC power frequency flicker avoidance (Europe/Asia). If set to 2, 60hz AC power frequency flicker avoidance (North America).
video.camera.frameRate	5 to 30 frames per second	25	Set target frame rate. Values indicate a fixed frame rate, from 5 (least smooth) to 30 (most smooth).
video.camera.saturation	0 to 6	3	Set saturation level. The value range is from 0 (Lowest) to 6 (Highest).
video.camera.sharpness	0 to 6	3	Set sharpness level. The value range is from 0 (Lowest) to 6 (Highest).

<localCameraView/>

These settings control how the local camera is viewed on the screen.

These configuration attributes are defined as follows:

Attribute (bold = change causes restart/reboot)	**Permitted Values**	**Default**	**Interpretation**
video.localCameraView. fullscreen.enabled	0=Disable, 1=Enable	1	Determines whether the local camera view is shown in the full screen layout . If set to 0, the local camera view is not shown. If set to 1, the local camera view is shown.
video.localCameraView. fullscreen.mode	“pip” or Null	Null	How the local camera view is shown. If set to “pip”, the local camera view appears as a picture-in-picture with the far end window. If set to Null, the local camera view appears side-by-side with the far end window.

<voice/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voice.txPacketDelay	"low", "normal", Null	Null	If set to "normal" or Null, no audio parameters are changed. If set to "low" and there are no precedence conflicts, the following changes are made: • `voice.codecPref.G722="1"` • `voice.codecPref.G711Mu="2"` • `voice.codecPref.G711A="3"` • `voice.codecPref.[All Others]=""` • `voice.audioProfile.G722.payloadSize="10"` • `voice.audioProfile.G711Mu.payloadSize="10"` • `voice.audioProfile.G711A.payloadSize="10"` • `voice.aec.hs.enable="0"` • `voice.ns.hs.enable="0"`
voice.txPacketFilter	0 or 1	Null	Flag to determine whether or not narrowband Tx high-pass filtering should be enabled. If set to 1, narrowband Tx high-pass filter is enabled. If set to 0, no Tx filtering is performed.

This attribute includes:

- <codecs/>
- <volume/>
- <vad/>
- <quality monitoring/>

<codecs/>

These codecs include:

- <codecPref/>

<codecPref/>

As of Polycom UC software 3.3.0, you ccan configure a simplified set of codec preferences for all phone models, improving consistency and reducing workload.

If you configure a codec that a particular phone does not support, the phone will ignore that preference and continue to the next configured preference. For example, using the default values, the highest-priority codec on a SoundPoint IP 650 will be G.722, since that model does not support Siren22, G.722.1C, or Siren14.

For more information on codecs on particular phones and priorities, refer to Audio Codecs on page 4-77.

Note All SoundPoint IP and SoundStation IP phones, except the SoundStation IP 5000, support both iLBC and G.729, if both are configured. The SoundStation IP 5000 phone supports iLBC or G.729AB.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voice.codecPref.G711_A	0 to 27, Null	7	Order of preference for codec. The value 0 or Null means disabled and the value 1 is the highest priority. If a particular phone model does not support a codec with non-zero setting, it will treat that setting as if it were zero and not offer or accept calls with that codec.
voice.codecPref.G711_Mu		6	
voice.codecPref. G719.32kbps		0	
voice.codecPref. G719.48kbps		0	
voice.codecPref. G719.64kbps		0	
voice.codecPref.G722		4	
voice.codecPref. G7221.16kbps		0	
voice.codecPref. G7221.24kbps		0	
voice.codecPref. G7221.32kbps		5	
voice.codecPref. G7221_C.24kbps		0	
voice.codecPref. G7221_C.32kbps		0	
voice.codecPref. G7221_C.48kbps		2	
voice.codecPref.G729_AB		8	
voice.codecPref. iLBC.13_33kbps		0	
voice.codecPref. iLBC.15_2kbps		0	
voice.codecPref. Lin16.8ksps		0	
voice.codecPref. Lin16.16ksps		0	
voice.codecPref. Lin16.32ksps		0	

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voice.codecPref. Lin16.44_1ksps	0 to 27, Null	0	Order of preference for codec.
voice.codecPref. Lin16.48ksps		0	
voice.codecPref. Siren14.24kbps		0	
voice.codecPref. Siren14.32kbps		0	
voice.codecPref. Siren14.48kbps		3	
voice.codecPref. Siren22.32kbps		0	
voice.codecPref. Siren22.48kbps		0	
voice.codecPref. Siren22.64kbps		1	

Note Some codecs with a default of 0 are available for test purposes only and are not expected to be used in your deployment.

<volume/>

The user's selection of the receive volume during a call can be remembered between calls. This can be configured per termination (handset, headset and hands-free/chassis). In some countries regulations exist which dictate that receive volume should be reset to nominal at the start of each call on handset and headset.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voice.volume.persist.handset	0 or 1	0	If set to 1, the receive volume will be remembered between calls. If set to 0, the receive volume will be reset to nominal at the start of each call.
voice.volume.persist.headset	0 or 1	0	
voice.volume.persist.handsfree	0 or 1	1	

<vad/>

These settings control the performance of the voice activity detection (silence suppression) feature.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voice.vad. signalAnnexB	0 or 1	1	If set to 1 and `voice.vadEnable` is set to 1, Annex B is used. A new line can be added to SDP depending on the setting of this parameter and the `voice.vadEnable` parameter. • If `voice.vadEnable` is set to 1, add attribute line a=fmtp:18 annexb="yes" below a=rtpmap… attribute line (where '18' could be replaced by another payload). • If `voice.vadEnable is set to 0`, add attribute line a=fmtp:18 annexb="no" below a=rtpmap… attribute line (where '18' could be replaced by another payload). If set to 0, there is no change to SDP.
voice.vadEnable	0 or 1	0	If set to 1, enable VAD.
voice.vadThresh	integer from 0 to 30	15	The threshold for determining what is active voice and what is background noise in dB. This does not apply to G.729AB codec operation which has its own built-in VAD function.

<quality monitoring/>

This attribute includes:

- <collector/>
- <alert/>
- <server/>
- <rtcpxr/>

<collector/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voice.qualityMonitoring.collector.enable.periodic	0 or 1	0	Enables generation of periodic quality reports throughout a call.
voice.qualityMonitoring.collector.enable.session	0 or1	0	Enables generation of a quality report at the end of each call.
voice.qualityMonitoring.collector.enable.triggeredPeriodic	0 to 2	0	Controls the generation of periodic quality reports triggered by alert states. If set to 0, alert states do not cause periodic reports to be generated. If set to 1, periodic reports will be generated when an alert state is critical. If set to 2, periodic reports will be generated when an alert state is either warning or critical. ***Note:*** *This parameter is ignored when* `qualityMonitoring.collector.enable.periodic` *is set 1, since periodic reports are sent throughout the duration of a call.*
voice.qualityMonitoring.collector.period	5 to 20	20	The time interval between successive periodic quality reports.

<alert/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voice.qualityMonitoring.collector.alert.moslq.threshold.critical	0 to 40	0	Threshold value of listening MOS score (MOS-LQ) that causes phone to send a critical alert quality report. Configure the desired MOS value multiplied by 10. If set to Null, critical alerts are not generated due to MOS-LQ. For example, a configured value of 28 corresponds to the MOS score 2.8.
voice.qualityMonitoring.collector.alert.moslq.threshold.warning	0 to 40	0	Threshold value of listening MOS score (MOS-LQ) that causes phone to send a warning alert quality report. Configure the desired MOS value multiplied by 10. If set to Null, warning alerts are not generated due to MOS-LQ. For example, a configured value of 35 corresponds to the MOS score 3.5.
voice.qualityMonitoring.collector.alert.delay.threshold.critical	0 to 2000	0	Threshold value of one way delay (in ms) that causes phone to send a critical alert quality report. If set to Null, critical alerts are not generated due to one way delay. One-way delay includes both network delay and end system delay.
voice.qualityMonitoring.collector.alert.delay.threshold.warning	0 to 2000	0	Threshold value of one way delay (in ms) that causes phone to send a critical alert quality report. If set to Null, warning alerts are not generated due to one way delay. One-way delay includes both network delay and end system delay.

<server/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voice.qualityMonitoring.collector.server.x.address	Dotted-decimal IP address or host name	Null	IP address or host name and port of a SIP server (report collector) that accepts voice quality reports contained in SIP PUBLISH messages. Set x to 1as only one report collector is supported at this time.
voice.qualityMonitoring.collector.server.x.port	1 to 65535	5060	Set x to 1as only one report collector is supported at this time.

<rtcpxr/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voice.qualityMonitoring.rtcpxr.enable	0 or 1	0	Enables generation of RTCP-XR packets.

<volpProt/>

This attribute includes:

- <server/>
- <SDP/>
- <SIP/>
- <H323/>

<server/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.server.dhcp.available	0 or 1	0	If set to 1, check with the DHCP server for SIP server IP address. If set to 0, do not check with DHCP server.
voIpProt.server.dhcp.option	128 to 256	128	Option to request from the DHCP server if `voIpProt.server.dhcp.available` = 1. ***Note:*** *If the reg.x.server.y.address parameter in <reg/> on page A-82 is non-Null, it takes precedence even if the DHCP server is available.*
voIpProt.server.dhcp.type	0 or 1	0	If set to 0, IP request address. If set to 1, request string. Type to request from the DHCP server if voIpProt.server.dhcp.available = 1.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.server.x.address	dotted-decimal IP address or host name	Null	IP address or host name and port of a SIP server that accepts registrations. Multiple servers can be listed starting with x=1 to 4 for fault tolerance. If port is 0: • If `voIpProt.server.x.address` is a hostname and `voIpProt.server.x.transport` is set to DNSnaptr, do NAPTR then SRV lookups. If `voIpProt.server.x.transport` is set to TCPpreferred or UDPOnly, then use 5060 and don't advertise the port number in signaling. If `voIpProt.server.x.address` is an IP address, there is no DNS lookup and 5060 is used for the port but it is not advertised in signaling. If port is 1 to 65535: • This value is used and it is advertised in signaling. ***Note:*** *If the reg.x.server.y.address parameter in <reg/> on page A-82 is non-Null, all of the reg.x.server.y.xxx parameters will override the voIpProt.server parameters.* ***Note****: The H.323 gatekeeper RAS signaling uses UDP, while the H.225/245 signaling uses TCP.*
voIpProt.server.x.port	0 to 65535	0	
voIpProt.server.x.expires	positive integer, minimum 10	3600	The phone's requested registration period in seconds. ***Note:*** *The period negotiated with the server may be different. The phone will attempt to re-register at the beginning of the overlap period. For example, if "expires"=300 and "overlap"=5, the phone will re-register after 295 seconds (300-5).*
voIpProt.server.x.expires.overlap	5 to 65535	60	The number of seconds before the expiration time returned by server x at which the phone should try to re-register. The phone will try to re-register at half the expiration time returned by the server if that value is less than the configured overlap value.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.server.x.expires.lineSeize	positive integer, minimum 0 was 10	30	Requested line-seize subscription period.
voIpProt.server.x.failOver.failBack. mode	newRequests DNSTTL registration duration	newRequests	If set to *newRequests*, all new requests are forwarded first to the primary server regardless of the last used server. If set to *DNSTTL*, the primary server is tried again after a timeout equal to the DNS TTL configured for the server the endpoint is registered to (or via). If set to *registration*, the primary server is tried again when the registration renewal signaling begins. If set to *duration*, the primary server is tried again after the time specified by timeout expires.
voIpProt.server.x.failOver. failBack.timeout	0, 60 to 65535	3600	If `voIpProt.server.x.failOver.failBack.mode` is set to *duration*, this is the time in seconds after failing over to the current working server before the primary server is again selected as the first server to forward new requests to. Values between 1 and 59 will result in a timeout of 60 and 0 means do not fail-back until a fail-over event occurs with the current server.
voIpProt.server.x.failOver. failRegistrationOn	0 or 1	1	If `voIpProt.server.x.failOver.RegisterOn` is set to 1 and this parameter is set to 1, the phone will silently invalidate an existing registration, if it exists, at the point of failing over.
voIpProt.server.x.failOver. RegisterOn	0 or 1	0	If set to 1, the phone will first attempt to register with (or via) the server to which the signalling is to be diverted, and only upon the registration succeeding (200 OK with valid expires) will the signalling diversion proceed with that server.
voIpProt.server.x.lcs	0 or 1	0	This attribute overrides the `voIpProt.SIP.lcs` . If set to 1, the proprietary "epid" parameter is added to the From field of all requests to support Microsoft Live Communications Server.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.server.x.register	0 or 1	1	If set to 0, calls can be routed to an outbound proxy without registration. Refer to `reg.x.server.y.register` in <reg/>on page *A-82*. For more information, refer to "Technical Bulletin 5844: SIP Server Fallback Enhancements on Polycom Phones" at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html
voIpProt.server.x.retryTimeOut	non-negative integer	0	If set to 0, use standard RFC 3261 signaling retry behavior. Otherwise retryTimeOut determines how often retries will be sent. Units = milliseconds. (Finest resolution = 100ms).
voIpProt.server.x.retryMaxCount	non-negative integer	3	If set to 0, 3 is used. retryMaxCount retries will be attempted before moving on to the next available server.
voIpProt.server.x.transport	DNSnaptr OR TCPpreferred OR UDPOnly OR TLS OR TCPOnly	DNSnaptr	If set to DNSnaptr: • If `voIpProt.server.x.address` is a hostname and voIpProt.server.x.port is 0 or Null, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If `voIpProt.server.x.address` is an IP address, or a port is given, then UDP is used. If set to TCPpreferred: • TCP is the preferred transport, UDP is used if TCP fails. If set to UDPOnly: • Only UDP will be used. If set to TLS: • If TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061. If set to TCPOnly: • Only TCP will be used.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.server.H323.x.address	dotted-decimal IP address or host name	Null	Address of the H.323 gatekeeper. ***Note**: Only one H.323 gatekeeper per phone is supported; if more than one is configured, only the first is used.*
voIpProt.server.H323.x.port	0 to 65535	1719	Port to be used for H.323 signaling. ***Note**: The H.323 gatekeeper RAS signaling uses UDP, while the H.225/245 signaling uses TCP.*
voIpProt.server.H323.x.expires	positive integer	3600	Desired registration period.

<SDP/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SDP.answer. useLocalPreferences	0 or 1	0	If set to 1, the phones uses its own preference list when deciding which codec to use rather than the preference list in the offer. If set to 0, it is disabled. ***Note:** If a H.323 call from a Polycom VVX 1500 selects a lower-quality codec (H.261) but the called device also support H.264, this parameter should be enabled to resolve the situation.*
voIpProt.SDP.early.answerOrOffer	0 or 1	0	If set to 1, an SDP offer or answer is generated in a provisional reliable response and PRACK request and response. If set to 0, an SDP offer or answer is not generated. ***Note**: An SDP offer or answer is not generated if the user (reg.x) is configured for the Music On Hold. Refer to <musicOnHold/> on page A-157.*

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SDP.iLBC.13_33kbps. includeMode	0 or 1	1	If set to 1, the phone should include the mode=30 FMTP attribute in SDP offers: • If `voice.codecPref.iLBC.13_33kbps` is set and `voice.codecPref.iLBC.15_2kbps` is Null. • If `voice.codecPref.iLBC.13_33kbps` and `voice.codecPref.iLBC.15_2kbps` are both set, but iLBC 13.33 kbps codec is set to a higher preference. If set to 0, the phone should not include the mode=30 FTMP attribute in SDP offers even if iLBC 13.33 kbps codec is being advertised. Refer to <codecPref/> on page A-135.
voIpProt.SDP. useLegacyPayloadTypeNegotiation	0 or 1	0	If set to 1, the phone transmits and receives RTP using the payload type identified by the first codec listed in the SDP of the codec negotiation answer. If set to 0, RFC 3264 is followed for transmit and receive RTP payload type values.

<SIP/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.acd.signalingMethod	0 or 1	0	If set to 0, the 'SIP-B' signaling is supported. (This is the older ACD functionality.) If set to 1, the feature synchronization signaling is supported. (This is the new ACD functionality.)
voIpProt.SIP. allowTransferOnProceeding	0 to 1	1	If set to 1, a transfer can be completed during the proceeding state of a consultation call. If set to 0, a transfer is not allowed during the proceeding state of a consultation call.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.authOptimizedInFailover	0 or 1	0	If set to 1, when failover occurs, the first new SIP request is sent to the server that sent the proxy authentication request. If set to 0, when failover occurs, the first new SIP request is sent to the server with the highest priority in the server list. If `reg.x.auth.optimizedInFailover` set to 0, this attribute is checked. If `voIpProt.SIP.authOptimizedInFailover` is 0, then this feature is disabled. If both attributes are set, the value of `reg.x.auth.optimizedInFailover` takes precedence.
voIpProt.SIP.CID.sourcePreference	ASCII string up to 120 characters long	Null	Source of caller ID information. If Null, caller ID information comes from "P-Asserted-Identity, Remote-Party-ID, From". For example, "From,P-Asserted-Identity, Remote-Party-ID" and "P-Asserted-Identity,From, Remote-Party-ID" are also valid.
voIpProt.SIP.conference.address	ASCII string up to 128 characters long	Null	If Null, conferences are set up on the phone locally. If set to some value, conferences are set up by the server using the conferencing agent specified by this address. The acceptable values depend on the conferencing server implementation policy.
voIpProt.SIP.connectionReuse.useAlias	0 or 1	0	If set to 0, this is the old behavior. If set to 1, phone uses the connection reuse draft which introduces "alias".
voIpProt.SIP.csta	0 or 1	0	If set to 1, uaCSTA is enabled. This parameter can be overridden by `reg.x.csta` .
voIpProt.SIP.dtmfViaSignaling.rtc2976	0 or 1	0	If set to 1, DTMF digit information is sent in RFC2976 SIP INFO packets during a call. If set to 0, no DTMF digit information is sent.
voIpProt.SIP.enable	0 or 1	1	Flag to determine whether or not the SIP protocol is used for call routing, dial plan, DTMF, and URL dialing. If set to 1, the SIP protocol is used.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.header.diversion.enable	0 or 1	0	If set to 1, the diversion header is displayed if received. If set to 0, the diversion header is not displayed.
voIpProt.SIP.header.diversion.list.useFirst	0 or 1	1	If set to 1, the first diversion header is displayed. If set to 0, the last diversion header is displayed.
voIpProt.SIP.header.warning.codes.accept	comma separated list	Null	A list of accepted warning codes. If set to Null, all codes are accepted. Only codes between 300 and 399 are supported. For example, if you want to accept only codes 325 to 330: `voIpProt.SIP.header.warning.codes.accept = 325,326,327,328,329,330` Text will be shown in the appropriate language. For more information, refer to `lcl.ml.lang.tags.x` in <ml/> on page A-65.
voIpProt.SIP.header.warning.enable	0 or 1	0	If set to 1, the warning header is displayed if received. If set to 0, the warning header is not displayed.
voIpProt.SIP.keepalive.sessionTimers	0 or 1	0	If set to 1, the session timer will be enabled. If set to 0, the session timer will be disabled, and the phone will not declare “timer” in “Support” header in INVITE. The phone will still respond to a re-INVITE or UPDATE. The phone will not try to re-INVITE or do UPDATE even if remote end point asks for it.
voIpProt.SIP.lcs	0 or 1	0	If set to 1, the proprietary “epid” parameter is added to the From field of all requests to support Microsoft Live Communications Server.
voIpProt.SIP.lineSeize.retries	3 to 10	10	Controls the number of times the phone will retry a notify when attempting to seize a line (BLA).

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.local.port	0 to 65535	5060	Local port to be used for SIP signaling. Local port for sending and receiving SIP signaling packets. If set to 0, 5060 is used for the local port but it is not advertised in the SIP signaling. If set to some other value, that value is used for the local port and it is advertised in the SIP signaling.
voIpProt.SIP.ms-forking	0 or 1	0	If set to 0, support for MS-forking is disabled. If set to 1, support for MS-forking is enabled and the phone will reject all Instant Message INVITEs. This parameter is relevant for Microsoft Live Communications Server server installations. Note that if any end point registered to the same account has MS-forking disabled, all other end points default back to non-forking mode. Windows Messenger does not use MS-forking so be aware of this behavior if one of the end points is Windows Messenger.
voIpProt.SIP.pingInterval	0 to 3600	0	The number in seconds to send "PING" message. This feature is disabled by default.
voIpProt.SIP.presence. nortelShortMode	0 or 1	0	Different headers sent in SUBSCRIBE when used for presence on a Avaya (Nortel) server. Support is indicated by adding a header “Accept-Encoding: x-nortel-short”. A PUBLISH is sent to indicate the status of the phone.
voIpProt.SIP.requestURI.E164. addGlobalPrefix	0 or 1	0	If set to 1, ‘+’ global prefix is added to E.164 user parts in sip: URIs:.
voIpProt.SIP.sendCompactHdrs	0 or 1	0	If set to 0, SIP header names generated by the phone use the long form, for example ‘From’. If set to 1, SIP header names generated by the phone use the short form, for example ‘f’.
voIpProt.SIP.serverFeatureControl. cf	0 or 1	0	If set to 1, server-based call forwarding is enabled. The call server has control of call forwarding. If set to 0, server-based call forwarding is not enabled. This is the old behavior.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.serverFeatureControl.dnd	0 or 1	0	If set to 1, server-based DND is enabled. The call server has control of DND. If set to 0, server-based DND is not enabled. This is the old behavior.
voIpProt.SIP.serverFeatureControl.localProcessing.cf	0 or 1	1	If set to 0 and `voIpProt.SIP.serverFeatureControl.cf` is set to 1, the phone will not perform local Call Forward behavior. If set to 1, the phone will perform local Call Forward behavior on all calls received.
voIpProt.SIP.serverFeatureControl.localProcessing.dnd	0 or 1	1	If set to 0 and `voIpProt.SIP.serverFeatureControl.dnd` is set to 1, the phone will not perform local DND call behavior. If set to 1, the phone will perform local DND call behavior on all calls received.
voIpProt.SIP.strictLineSeize	0 or 1	0	If set to 1, forces the phone to wait for 200 OK response when receiving a TRYING notify. If set to 0, this is old behavior.
voIpProt.SIP.strictReplacesHeader	0 or 1	1	This parameter applies only to directed call pick-up attempts initiated against monitored BLF resources. If set to 1, the phone requires call-id,to-tag, and from-tag to perform a directed call-pickup when call.directedCallPickupMethod is configured as "native". If set to 0, all that is required to perform the directed call pick-up is a call-id.
voIpProt.SIP.strictUserValidation	0 or 1	0	If set to 1, forces the phone to match user portion of signaling exactly. If set to 0, phone will use first registration if the user part does not match any registration.
voIpProt.SIP.tcpFastFailover	0 or 1	0	If set to 1, failover occurs based on the values of `reg.x.server.y.retryMaxCount` `voIpProt.server.x.retryTimeOut`. If set to 0, this is old behavior. Refer to `reg.x.tcpFastFailover` .

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.use486forReject	0 or 1	0	If set to1 and the phone is indicating a ringing inbound call appearance, phone will transmit a 486 response to the received INVITE when the **Reject** soft key is pressed. If set to 0, no 486 response is transmitted.
voipPort.SIP. useCompleteUriForRetrieve	0 or 1	1	If set to 1, use complete URI to retrieve the call for certain servers.
voIpProt.SIP.useContactInReferTo	0 or 1	0	If set to 0, the "To URI" is used in the REFER. If set to 1, the "Contact URI" is used in the REFER.
voIpProt.SIP.useRFC2543hold	0 or 1	0	If set to 1, use SDP media direction attributes (such as a=sendonly) per RFC 3264 when initiating a call, otherwise use the obsolete c=0.0.0.0 RFC2543 technique. In either case, the phone processes incoming hold signaling in either format. ***Note:*** *`voIpProt.SIP.useRFC2543hold` is effective only when the call is initiated.*
voIpProt.SIP.useSendonlyHold	0 or 1	1	If set to 1, the phone will send a reinvite with a stream mode attribute of "sendonly" when a call is put on hold. This is the same as the previous behavior. If set to 0, the phone will send a reinvite with a stream mode attribute of "inactive" when a call is put on hold. ***NOTE:*** *The phone will ignore the value of this parameter if set to 1 when the parameter* `voIpProt.SIP.useRFC2543hold` *is also set to 1 (default is 0).*

This attribute also includes:

- <outboundProxy/>
- <alertInfo/>
- <requestValidation/>
- <specialEvent/>
- <dialog/>
- <musicOnHold/>
- <compliance/>

<outboundProxy/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.outboundProxy.address	dotted-decimal IP address or host name	Null	IP address or host name and port of a SIP server to which the phone shall send all requests.
voIpProt.SIP.outboundProxy.port	0 to 65535	0	
voIpProt.SIP.outboundProxy.failOver.failBack.mode	newRequests DNSTTL registration duration	newRequests	This attribute overrides the `voIpProt.server.x.failOver.failBack.mode` . If set to *newRequests*, all new requests are forwarded first to the primary server regardless of the last used server. If set to *DNSTTL*, the primary server is tried again after a timeout equal to the DNS TTL configured for the server the endpoint is registered to (or via). If set to *registration*, the primary server is tried again when the registration renewal signalling begins. If set to *duration*, the primary server is tried again after the time specified by timeout expires.
voIpProt.SIP.outboundProxy.failOver.failBack.timeout	0, 60 to 65535	3600	This attribute overrides the `voIpProt.server.x.failOver.failBack.timeout` . If `voIpProt.SIP.outboundProxy.failOver.failBack.mode` is set to *duration*, this is the time in seconds after failing over to the current working server before the primary server is again selected as the first server to forward new requests to. Values between 1 and 59 will result in a timeout of 60 and 0 means do not fail-back until a fail-over event occurs with the current server.
voIpProt.SIP.outboundProxy.failOver.failRegistrationOn	0 or 1	1	This attribute overrides the `voIpProt.server.x.failOver.failRegistrationOn` . If `voIpProt.SIP.outboundProxy.failOver.RegisterOn` is set to 1 and this parameter is set to 1, the phone will silently invalidate an existing registration, if it exists, at the point of failing over.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.outboundProxy.failOver.RegisterOn	0 or 1	0	This attribute overrides the `voIpProt.server.x.failOver.RegisterOn` . If set to 1, the phone will first attempt to register with (or via) the server to which the signalling is to be diverted, and only upon the registration succeeding (200 OK with valid expires) will the signalling diversion proceed with that server.
voIpProt.SIP.outboundProxy.transport	DNSnaptr or TCPpreferred or UDPOnly or TLS or TCPOnly	DNSnaptr	If set to Null or DNSnaptr: • If voIpProt.SIP.outboundProxy.address is a hostname and `voIpProt.SIP.outboundProxy.port` is 0 or Null, do NAPTR then SRV look-ups to try to discover the transport, ports and servers, as per RFC 3263. If `voIpProt.SIP.outboundProxy.address` is an IP address, or a port is given, then UDP is used. If set to TCPpreferred: • TCP is the preferred transport, UDP is used if TCP fails. If set to UDPOnly: • Only UDP will be used. If set to TLS: • If TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061. If set to TCPOnly: • Only TCP will be used. ***NOTE:*** *TLS is not supported on SoundPoint IP 300 and 500 phones.*

<alertInfo/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.alertInfo.x.class	enumerated type Refer to **sip-interop.cfg**	default	Alert-Info fields from INVITE requests will be compared against as many of these parameters as are specified (x=1, 2, ..., N) and if a match is found, the behavior described in the corresponding ring class (refer to <rt/> on page A-100) will be applied.
voIpProt.SIP.alertInfo.x.value	string	Null	

<requestValidation/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.requestValidation. digest.realm	A valid string	Polycom SPIP	Determines string used for Realm.
voIpProt.SIP.requestValidation.x. method	Null or one of: “source”, “digest”, “both”, or ”all”	Null	If Null, no validation is done. Otherwise this sets the type of validation performed for the request: *source*: ensure request is received from an IP address of a server belonging to the set of target registration servers; *digest:* challenge requests with digest authentication using the local credentials for the associated registration (line); *both* or *all*: apply both of the above methods
voIpProt.SIP.requestValidation.x. request	One of: “INVITE”, “ACK” , “BYE” “REGISTER”, “CANCEL”, “OPTIONS”, “INFO”, “MESSAGE”, “SUBSCRIBE” “NOTIFY”, “REFER”, “PRACK”, or“UPDATE”	Null	Sets the name of the method for which validation will be applied. ***Note:*** *Intensive request validation may have a negative performance impact due to the additional signaling required in some cases, therefore, use it wisely.*

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.requestValidation.x. request.y.event	A valid string	Null	Determines which events specified with the Event header should be validated; only applicable when `voIpProt.SIP.requestValidation.x.request` is set to "SUBSCRIBE" or "NOTIFY". If set to Null, all events will be validated.

<specialEvent/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.specialEvent. checkSync.alwaysReboot	0 or 1	0	If set to 1, always reboot when a NOTIFY message is received from the server with event equal to check-sync. If set to 0, only reboot if any of the files listed in **<MAC-address>.cfg** have changed on the FTP server when a NOTIFY message is received from the server with event equal to check-sync.
voIpProt.SIP.specialEvent. lineSeize.nonStandard	0 or 1	1	If set to 1, process a 200 OK response for a line-seize event SUBSCRIBE as though a line-seize NOTIFY with Subscription State: active header had been received, this speeds up processing.

<dialog/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.dialog.usePvalue	0 or 1	0	If set to 0, phone uses "pval" field name in Dialog. This obeys the draft-ietf-sipping-dialog-package-06.txt draft. If set to 1, phone uses a field name of "pvalue".
voIpProt.SIP.dialog.useSDP	0 or 1	0	If set to 0, new dialog event package draft is used (no SDP in dialog body). If set to 1, for backwards compatibility, use this setting to send SDP in dialog body.

<musicOnHold/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.musicOnHold.uri	string	Null	A URI that provides the media stream to play for the remote party on hold. If `reg.x.musicOnHold` is set to Null, this attribute is checked. ***Note**: The SIP URI parameter `transport` is supported when configured with the values of UDP, TCP, or TLS.*

<compliance/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.SIP.compliance.RFC3261.validate.contentLanguage	0 or 1	1	If set to 1, validation of the SIP header content language is enabled. If set to 0, validation is disabled.
voIpProt.SIP.compliance.RFC3261.validate.contentLength	0 or 1	1	If set to 1, validation of the SIP header content length is enabled.
voIpProt.SIP.compliance.RFC3261.validate.uriScheme	0 or 1	1	If set to 1, validation of the SIP header URI scheme is enabled. If set to 0, validation is disabled.

<H323/>

Note At this time, this attribute is used with the Polycom VVX 1500 phone only.

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
voIpProt.H323. autoGateKeeperDiscovery	0 or 1	1	If set to 1, the phone will attempt to discover an H.323 gatekeeper address via the standard multicast technique, provided that a statically configured gatekeeper address is not available. If set to 0, the phone will no send out any gatekeeper discovery messages.
voIpProt.H323. blockFacilityOnStartH245	0 or 1	0	If set to 1, remove facility message when using H.245 .
voIpProt.H323.dtmfViaSignaling. enabled	0 or 1	1	If set to 1, the phone will use the H.323 signaling channel for DTMF key press transmission.
voIpProt.H323.dtmfViaSignaling. H245alphanumericMode	0 or 1	1	If set to 1, the phone will support H.245 signaling channel alphanumeric mode DTMF transmission. ***Note**: If both alphanumeric and signal mode are enabled, the phone will give preference to sending DTMF in alphanumeric mode where there is the possibility of sending in both modes.*
voIpProt.H323.dtmfViaSignaling. H245signalMode	0 or 1	1	If set to 1, the phone will support H.245 signaling channel signal mode DTMF transmission.
voIpProt.H323.enable	0 or 1	0	Flag to determine whether or not the H.323 protocol is used for call routing, dial plan, DTMF, and URL dialing. If set to 1, the H.323 protocol is used.
voIpProt.H323.local.port	0 to 65535	1720	Local port to be used for H.323 signaling. Local port for sending and receiving H.323 signaling packets. If set to 0, 1720 is used for the local port but it is not advertised in the H.323 signaling. If set to some other value, that value is used for the local port and it is advertised in the H.323 signaling.
voIpProt.H323.local.RAS.port	1 to 65535	1719	Local port for RAS signaling.

B

Session Initiation Protocol (SIP)

This chapter provides a description of the basic Session Initiation Protocol (SIP) and the protocol extensions that are supported by the current Polycom® UC Software. To find the applicable Request For Comments (RFC) document, go to http://www.ietf.org/rfc.html and enter the RFC number.

This chapter contains information on:

- Basic Protocols—All the basic calling functionality described in the SIP specification is supported. Transfer is included in the basic SIP support.
- Protocol Extensions—Extensions add features to SIP that are applicable to a range of applications, including reliable 1xx responses and session timers.

For information on supported RFC's and Internet drafts, refer to the following section, RFC and Internet Draft Support.

This chapter also describes:

- Request Support
- Header Support
- Response Support
- Hold Implementation
- Reliability of Provisional Responses
- Transfer
- Third Party Call Control
- SIP for Instant Messaging and Presence Leveraging Extensions
- Shared Call Appearance Signaling
- Bridged Line Appearance Signaling

RFC and Internet Draft Support

The following RFC's and Internet drafts are supported:

- RFC 1321—The MD5 Message-Digest Algorithm
- RFC 2327—SDP: Session Description Protocol
- RFC 2387—The MIME Multipart / Related Content-type
- RFC 2976—The SIP INFO Method
- RFC 3261—SIP: Session Initiation Protocol (replacement for RFC 2543)
- RFC 3262—Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263—Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264—An Offer / Answer Model with the Session Description Protocol (SDP)
- RFC 3265—Session Initiation Protocol (SIP) - Specific Event Notification
- RFC 3311—The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3325—SIP Asserted Identity
- RFC 3420—Internet Media Type message/sipfrag
- RFC 3515—The Session Initiation Protocol (SIP) Refer Method
- RFC 3555 — MIME Type of RTP Payload Formats
- RFC 3611 — RTP Control Protocol Extended reports (RTCP XR)
- RFC 3665—Session Initiation Protocol (SIP) Basic Call Flow Examples
- draft-ietf-sip-cc-transfer-05.txt—SIP Call Control - Transfer
- RFC 3725—Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3842—A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- RFC 3856—A Presence Event Package for Session Initiation Protocol (SIP)
- RFC 3891—The Session Initiation Protocol (SIP) "Replaces" Header
- RFC 3892—The Session Initiation Protocol (SIP) Referred-By Mechanism
- RFC 3959—The Early Session Disposition Type for the Session Initiation Protocol (SIP)
- RFC 3960—Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)

- RFC 3968—The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 3969—The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)
- RFC 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4235—An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- draft-levy-sip-diversion-08.txt—Diversion Indication in SIP
- draft-anil-sipping-bla-02.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-ietf-sip-privacy-04.txt—SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks
- draft-ietf-sipping-cc-conferencing-03.txt—SIP Call Control - Conferencing for User Agents
- draft-ietf-sipping-rtcp-summary-02.txt —Session Initiation Protocol Package for Voice Quality Reporting Event
- draft-ietf-sip-connect-reuse-04.txt—Connection Reuse in the Session Initiation Protocol (SIP)

Request Support

The following SIP request messages are supported:

Method	Supported	Notes
REGISTER	Yes	
INVITE	Yes	
ACK	Yes	
CANCEL	Yes	
BYE	Yes	
OPTIONS	Yes	
SUBSCRIBE	Yes	
NOTIFY	Yes	
REFER	Yes	
PRACK	Yes	

Method	Supported	Notes
INFO	Yes	RFC 2976, the phone does not generate INFO requests, but will issue a final response upon receipt. No INFO message bodies are parsed.
MESSAGE	Yes	Final response is sent upon receipt. Message bodies of type text/plain are sent and received.
UPDATE	Yes	

Header Support

The following SIP request headers are supported:

Note In the following table, a "Yes" in the Supported column means the header is sent and properly parsed.

Header	Supported	Notes
Accept	Yes	
Accept-Encoding	No	
Accept-Language	Yes	
Access-Network-Info	No	
Alert-Info	Yes	
Allow	Yes	
Allow-Events	Yes	
Authentication-Info	No	
Authorization	Yes	
Call-ID	Yes	
Call-Info	Yes	
Contact	Yes	
Content-Disposition	No	
Content-Encoding	No	
Content-Language	No	
Content-Length	Yes	
Content-Type	Yes	
CSeq	Yes	

Header	Supported	Notes
Date	No	
Diversion	Yes	
Error-Info	No	
Event	Yes	
Expires	Yes	
From	Yes	
In-Reply-To	No	
Max-Forwards	Yes	
Min-Expires	No	
Min-SE	Yes	
MIME-Version	No	
Organization	No	
P-Asserted-Identity	Yes	
P-Preferred-Identity	Yes	
Priority	No	
Privacy	No	
Proxy-Authenticate	Yes	
Proxy-Authorization	Yes	
Proxy-Require	Yes	
RAck	Yes	
Record-Route	Yes	
Refer-To	Yes	
Referred-By	Yes	
Referred-To	Yes	
Remote-Party-ID	Yes	
Replaces	Yes	
Reply-To	No	
Requested-By	No	
Require	Yes	
Response-Key	No	

Header	Supported	Notes
Retry-After	Yes	
Route	Yes	
RSeq	Yes	
Server	Yes	
Session-Expires	Yes	
Subject	Yes	
Subscription-State	Yes	
Supported	Yes	
Timestamp	Yes	
To	Yes	
Unsupported	Yes	
User-Agent	Yes	
Via	Yes	
Warning	Yes	Only warning codes 300 to 399
WWW-Authenticate	Yes	

Response Support

The following SIP responses are supported:

Note In the following table, a "Yes" in the Supported column means the header is sent and properly parsed. The phone may not actually generate the response.

1xx Responses - Provisional

Response	Supported	Notes
100 Trying	Yes	
180 Ringing	Yes	
181 Call Is Being Forwarded	No	
182 Queued	No	
183 Session Progress	Yes	

2xx Responses - Success

Response	Supported	Notes
200 OK	Yes	
202 Accepted	Yes	In REFER transfer.

3xx Responses - Redirection

Response	Supported	Notes
300 Multiple Choices	Yes	
301 Moved Permanently	Yes	
302 Moved Temporarily	Yes	
305 Use Proxy	No	
380 Alternative Service	No	

4xx Responses - Request Failure

Note All 4xx responses for which the phone does not provide specific support will be treated the same as 400 Bad Request.

Response	Supported	Notes
400 Bad Request	Yes	
401 Unauthorized	Yes	
402 Payment Required	No	
403 Forbidden	No	
404 Not Found	Yes	
405 Method Not Allowed	Yes	
406 Not Acceptable	No	
407 Proxy Authentication Required	Yes	
408 Request Timeout	No	
410 Gone	No	
413 Request Entity Too Large	No	
414 Request-URI Too Long	No	

Response	Supported	Notes
415 Unsupported Media Type	Yes	
416 Unsupported URI Scheme	No	
420 Bad Extension	No	
421 Extension Required	No	
423 Interval Too Brief	No	
480 Temporarily Unavailable	Yes	
481 Call/Transaction Does Not Exist	Yes	
482 Loop Detected	Yes	
483 Too Many Hops	No	
484 Address Incomplete	Yes	
485 Ambiguous	No	
486 Busy Here	Yes	
487 Request Terminated	Yes	
488 Not Acceptable Here	Yes	
491 Request Pending	No	
493 Undecipherable	No	

5xx Responses - Server Failure

Response	Supported	Notes
500 Server Internal Error	Yes	
501 Not Implemented	Yes	
502 Bad Gateway	No	
503 Service Unavailable	No	
504 Server Time-out	No	
505 Version Not Supported	No	
513 Message Too Large	No	

6xx Responses - Global Failure

Response	Supported	Notes
600 Busy Everywhere	No	
603 Decline	Yes	
604 Does Not Exist Anywhere	No	
606 Not Acceptable	No	

Hold Implementation

The phone supports both currently accepted means of signaling hold.

The first method, no longer recommended due in part to the RTCP problems associated with it, is to set the "c" destination addresses for the media streams in the SDP to zero, for example, c=0.0.0.0.

The second, and preferred, method is to signal the media directions with the "a" SDP media attributes sendonly, recvonly, inactive, or sendrecv. The hold signaling method used by the phone is configurable (refer to <SIP/>on page A-147), but both methods are supported when signaled by the remote end point.

Note Even if the phone is set to use c=0.0.0.0, it will not do so if it gets any sendrecv, sendonly, or inactive from the server. These flags will cause it to revert to the other hold method.

Reliability of Provisional Responses

The phone fully supports RFC 3262 - *Reliability of Provisional Responses*.

Transfer

The phone supports transfer using the REFER method specified in draft-ietf-sip-cc-transfer-05 and RFC 3515.

Third Party Call Control

The phone supports the delayed media negotiations (INVITE without SDP) associated with third party call control applications.

When used with an appropriate server, the User Agent Computer Supported Telecommunications Applications (uaCSTA) feature on the phone may be utilized for remote control of the phone from computer applications such as Microsoft Office Communicator.

The phone is compliant with "Using CSTA for SIP Phone User Agents (uaCSTA), ECMA TR/087" for the Answer Call, Hold Call, and Retrieve Call functions and "Services for Computer Supported Telecommunications Applications Phase III", ECMA – 269 for the Conference Call function.

This feature is enabled by configuration parameters described in <SIP/> on page A-147 and <reg/> on page A-82 and needs to be activated by a feature application key.

SIP for Instant Messaging and Presence Leveraging Extensions

The phone is compatible with the Presence and Instant Messaging features of Microsoft Windows Messenger 5.1. In a future release, support for the Presence and Instant Message recommendations in the SIP Instant Messaging and Presence Leveraging Extensions (SIMPLE) proposals will be provided by the following Internet drafts or their successors:

- draft-ietf-simple-cpim-mapping-01
- draft-ietf-simple-presence-07
- draft-ietf-simple-presencelist-package-00
- draft-ietf-simple-winfo-format-02
- draft-ietf-simple-winfo-package-02

Shared Call Appearance Signaling

A shared line is an address of record managed by a call server. The server allows multiple end points to register locations against the address of record.

The phone supports shared call appearances (SCA) using the SUBSCRIBE-NOTIFY method in the "SIP Specific Event Notification" framework (RFC 3265). The events used are:

- "call-info" for call appearance state notification
- "line-seize for the phone to ask to seize the line

Bridged Line Appearance Signaling

A bridged line is an address of record managed by a server. The server allows multiple end points to register locations against the address of record.

The phone supports bridged line appearances (BLA) using the SUBSCRIBE-NOTIFY method in the "SIP Specific Event Notification" framework (RFC 3265). The events used are:

- "dialog" for bridged line appearance subscribe and notify

C

Miscellaneous Administrative Tasks

This appendix provides information required by varied aspects of the Polycom® UC Software. This includes:

Trusted Certificate Authority List

The following certificate authorities are trusted by the phone by default:

- ABAecom (sub., Am. Bankers Assn.) Root CA
- ANX Network CA by DST

- American Express CA
- American Express Global CA
- BelSign Object Publishing CA
- BelSign Secure Server CA
- Deutsche Telekom AG Root CA
- Digital Signature Trust Co. Global CA 1
- Digital Signature Trust Co. Global CA 2
- Digital Signature Trust Co. Global CA 3
- Digital Signature Trust Co. Global CA 4
- Entrust Worldwide by DST
- Entrust.net Premium 2048 Secure Server CA
- Entrust.net Secure Personal CA
- Entrust.net Secure Server CA
- Equifax Premium CA
- Equifax Secure CA
- Equifax Secure eBusiness CA 1
- Equifax Secure eBusiness CA 2
- Equifax Secure Global eBusiness CA 1
- GeoTrust Primary Certification Authority
- GeoTrust Global CA
- GeoTrust Global CA 2
- GeoTrust Universal CA
- GeoTrust Universal CA 2
- GTE CyberTrust Global Root
- GTE CyberTrust Japan Root CA
- GTE CyberTrust Japan Secure Server CA
- GTE CyberTrust Root 2
- GTE CyberTrust Root 3
- GTE CyberTrust Root 4
- GTE CyberTrust Root 5

- GTE CyberTrust Root CA
- GlobalSign Partners CA
- GlobalSign Primary Class 1 CA
- GlobalSign Primary Class 2 CA
- GlobalSign Primary Class 3 CA
- GlobalSign Root CA
- National Retail Federation by DST
- TC TrustCenter, Germany, Class 1 CA
- TC TrustCenter, Germany, Class 2 CA
- TC TrustCenter, Germany, Class 3 CA
- TC TrustCenter, Germany, Class 4 CA
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA
- Thawte Universal CA Root
- UPS Document Exchange by DST
- ValiCert Class 1 VA
- ValiCert Class 2 VA
- ValiCert Class 3 VA
- VeriSign Class 4 Primary CA
- Verisign Class 1 Public Primary Certification Authority
- Verisign Class 1 Public Primary Certification Authority - G2
- Verisign Class 1 Public Primary Certification Authority - G3
- Verisign Class 2 Public Primary Certification Authority
- Verisign Class 2 Public Primary Certification Authority - G2
- Verisign Class 2 Public Primary Certification Authority - G3
- Verisign Class 3 Public Primary Certification Authority
- Verisign Class 3 Public Primary Certification Authority - G2

- Verisign Class 3 Public Primary Certification Authority - G3
- Verisign Class 4 Public Primary Certification Authority - G2
- Verisign Class 4 Public Primary Certification Authority - G3
- Verisign/RSA Commercial CA
- Verisign/RSA Secure Server CA

Polycom endeavors to maintain a built-in list of the most commonly used CA Certificates. Due to memory constraints, we cannot keep as thorough a list as some other applications (for example, browsers). If you are using a certificate from a commercial Certificate Authority not in the list above, you may submit a Feature Request for Polycom to add your CA to the trusted list by visiting https://jira.polycom.com:8443//secure/CreateIssue!default.jspa?os_username=jiraguest&os_password=polycom. At this point, you can use the Custom Certificate method to load your particular CA certificate into the phone (refer to "Technical Bulletin 17877: using Custom Certificates on SoundPoint IP Phones" at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html).

Encrypting Configuration Files

The phone can recognize encrypted files, which it downloads from the provisioning server and it can encrypt files before uploading them to the provisioning server. There must be an encryption key on the phone to perform these operations. Configuration files (excluding the master configuration file), contact directories, and configuration override files can be encrypted.

A separate SDK, with a readme file, is provided to facilitate key generation and configuration file encryption and decrypt on a UNIX or Linux server. The utility is distributed as source code that runs under the UNIX operating system. For more information, contact Polycom Technical Support.

A key is generated by the utility and must be downloaded to the phone so that it can decrypt the files that were encrypted on the server. The `device.sec.configEncryption.key` configuration file parameter is used to set the key on the phone. The utility generates a random key and the encryption is Advanced Encryption Standard (AES) 128 in Cipher Block Chaining (CBC) mode. An example key would look like this:

```
Crypt=1;KeyDesc=companyNameKey1;Key=06a9214036b8a15b512e03d534120006;
```

If the phone doesn't have a key, it must be downloaded to the phone in plain text (a potential security hole if not using HTTPS). If the phone already has a key, a new key can be downloaded to the phone encrypted using the old key (refer to Changing the Key on the Phone on page C-6). At a later date, new phones from the factory will have a key pre-loaded in them. This key will be changed at regular intervals to enhance security

It is recommended that all keys have unique descriptive strings in order to allow simple identification of which key was used to encrypt a file. This makes provisioning server management easier.

After encrypting a configuration file, it is useful to rename the file to avoid confusing it with the original version, for example rename **site.cfg** to **site.enc**. However, the directory and override filenames cannot be changed in this manner.

You can check whether an encrypted file is the same as an unencrypted file by:

1. Run the configFileEncrypt utility on the unencrypted file with the "-d" option. This shows the "digest" field.
2. Look at the encrypted file using WordPad and check the first line that shows a "Digest=…." field. If the two fields are the same, then the encrypted and unencrypted file are the same.

Note If a phone downloads an encrypted file that it cannot decrypt, the action is logged, an error message displays, and the phone reboots. The phone will continue to do this until the provisioning server provides an encrypted file that can be read, an unencrypted file, or the file is removed from the master configuration file list.

Note Encrypted configuration files can be decrypted on all currently supported Polycom phones (not supported on legacy phones).

The master configuration file cannot be encrypted on the provisioning server. This file is downloaded by the BootROM that does not recognize encrypted files. For more information, refer to Master Configuration Files on page 2-7.

The following configuration file changes are required to modify this feature:

Central (provisioning server)	Configuration File: **site.cfg**	Specify the phone-specific contact directory and the phone-specific configuration override file. For more information, refer to <encryption/> on page A-102.
	Configuration file: **device.cfg**	Change the encryption key. For more information, refer to <device/> on page A-30.

Changing the Key on the Phone

For security purposes, it may be desirable to change the key on the phones and the server from time to time.

To change a key:

1. Put the new key into a configuration file that is in the list of files downloaded by the phone (specified in **000000000000.cfg** or **<Ethernet address>.cfg**).

   Use the `device.sec.configEncryption.key` parameter to specify the new key.

2. Manually reboot the phone so that it will download the new key. The phone will automatically reboot a second time to use the new key.

   At this point, the phone expects all encrypted configuration files on the provisioning server to use the new key and it will continue to reboot until this is the case. The files on the server must be updated to the new key or they must be made available in unencrypted format. Updating to the new key requires decrypting the file with the old key, then encrypting it with the new key.

   Note that configuration files, contact directory files and configuration override files may all need to be updated if they were already encrypted. In the case of configuration override files, they can be deleted from the provisioning server so that the phone will replace them when it successfully boots.

Adding a Customizable Logo on the Idle Display

Note

Customizable idle display logos are not supported on the Polycom VVX 1500 phone.

As of Polycom UC Software 3.3.0, idle display "animations" are not supported.

With the configuration parameter changes in Polycom UC Software 3.3.0, the instructions on how to add a customizable idle display logo to all SoundPoint IP and SoundStation IP phones in your organization have changed. You must be running at least BootROM 4.3.0 and UC Software 3.3.0.

The screen dimensions on the phones are as shown below.

Model	Width	Height	Color Depth
IP 32x/33x	102	23	monochrome
IP 450	171	73	4-bit grayscale or monochrome
IP 550/560/650	209	109	4-bit grayscale or monochrome
IP 670	209	109	12-bit color
IP 5000	150	33	32-bit grayscale or monochrome
IP 6000	150	33	32-bit grayscale or monochrome
IP 7000	255	128	32-bit grayscale or monochrome

Logos smaller than described in the table above are acceptable, but larger logos may be truncated or interfere with other areas of the user interface.

Color	RGB Values (Decimal)	RGB Values (Hexadecimal)
Black	0,0,0	00,00,00
Dark Gray	96,96,96	60,60,60
Light Gray	160,160,160	A0,A0,A0
White	255,255,255	FF,FF,FF

The SoundPoint IP 450/550/560/650 phone support a 4-bit grayscale, which is a smooth gradient from black (0, 0, 0) to white (FF, FF, FF).

The SoundPoint IP 670 phone support a 12-bit color scale from black (0, 0, 0) to white (FFFF, FFFF, FFFF).

The SoundStation IP 5000, 6000, and 7000 phone supports a 32-bit grayscale, which is a smooth gradient from black (0, 0, 0) to white (FF, FF, FF).

Configuration File Changes

The `<bitmap>` parameters can be found in the **features.cfg** configuration file. Set `bitmap.idleDisplay.name` to the appropriate filename.

For example:

```
<bitmap
bitmap.idleDisplay.name="http://123.45.67.89/company/common/company-logo.bmp" />
```

BootROM/SIP Software Dependencies

Not withstanding the hardware backward compatibility mandate, there have been times throughout the life of the Polycom® phones where certain dependencies on specific BootROM and application versions have been necessitated.

This table summarizes some the major dependencies that you are likely to encounter:

Model	BootROM	SIP Software
IP 320/330	4.1.1 or later	2.2.2 or later
IP 321/331	4.1.3 or later	3.1.3C or later
IP 335	4.2.0B or later	4.1.2B or later
IP 450	4.1.2 or later	3.1.0C or later
IP 550[1]	3.2.2B or later	2.1 or later
IP 560[1]	4.0.1 or later	2.2.2 or later
IP 650/EM[1]	3.2.2B or later	2.0.3B or later
IP 650/BEM	4.0.1 or later	2.2.2 or later
IP 670/CEM	4.1.1 or later	3.0.3 or later
IP 5000	4.2.2 or later	3.2.3 or later
IP 6000	4.1.1 or later	3.0.2 or later
IP 7000[2]	4.1.1 or later	3.0.2 or later
VVX 1500[3]	4.1.4 or later	3.2.2 or later

Note

1. SoundPoint IP 550, 560 and 650 phones manufactured as of February 2009 have additional BootROM/SIP software dependencies. For more information, refer to “Technical Bulletin TB 46440: Notice of Product Shipping Configuration Change” at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .
2. If the SoundStation IP 7000 is connected to a Polycom HDX system, the BootROM must be 4.1.2 or later.
3. As of SIP 3.2.2, the BootROM 4.1.4 software is contained within the software distribution. Downgrading to versions pre-SIP 3.2. is not supported.

Migration Dependencies

In addition to the BootROM and application dependencies, there are certain restrictions with regard to upgrading or downgrading from one BootROM release to another BootROM release. These restrictions are typically caused by the addition of features that change the way BootROM provisioning is done, so the older version become incompatible.

There is always a way to move forward with BootROM releases, although it may be a two or three step procedure sometimes, but there are cases where it is impossible to move backward. Make special note of these cases before upgrading.

For the latest information, refer to the latest *Release Notes*.

Supported SoundStation IP 7000 / Polycom HDX Software Interoperability

To operate your SoundStation IP 7000 phone in this environment, Polycom recommends that you look at the latest *Release Notes* for the appropriate SoundStation IP7000 and Polycom HDX system software versions.

Multiple Key Combinations

On Polycom phones, certain multiple key combinations can be used to reboot the phone and restore factory defaults.

For other methods for resetting and rebooting your Polycom phones, refer to “Quick Tip 18298: Resetting and Rebooting Polycom Phones” at http://www.polycom.com/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html .

Rebooting the Phone

For the key combination, press and hold certain key combinations (depending on the phone model) simultaneously until a confirmation tone is heard or for about three seconds:

- IP 32x/33x: Volume-, Volume+, Hold, and Hands-free
- IP 450, 550, 560, 600, 601, and 650, and 670: Volume-, Volume+, Mute, and Messages
- IP 6000: *, #, Volume+, and Select
- IP 5000, 7000: *, #, Volume-, and Volume+
- VVX 1500: Delete, Volume-, Volume+, and Select

Note As of SIP 3.2.0, users can restart their phones by pressing the **Menu** key, and then selecting **Settings > Basic > Restart Phone**. New BootROM and Polycom UC Software will be downloaded to the phone as a result of this restart.

Restoring Factory Defaults

For the key combination, press and hold certain key combinations (depending on the phone model) simultaneously during the countdown process in the BootROM until the password prompt appears:

- IP 450, 550, 600, 601, and 650, and 670 and VVX 1500: 4, 6, 8 and * dial pad keys
- IP 32x/33x, 560, 5000, 7000: 1, 3, 5, and 7 dial pad keys
- IP 6000: 6, 8 and * dial pad keys

Enter the administrator password to initiate the reset. Resetting to factory defaults will also reset the administrator password (factory default password is 456). Polycom recommends that you change the administrative password from the default value.

Uploading Log Files

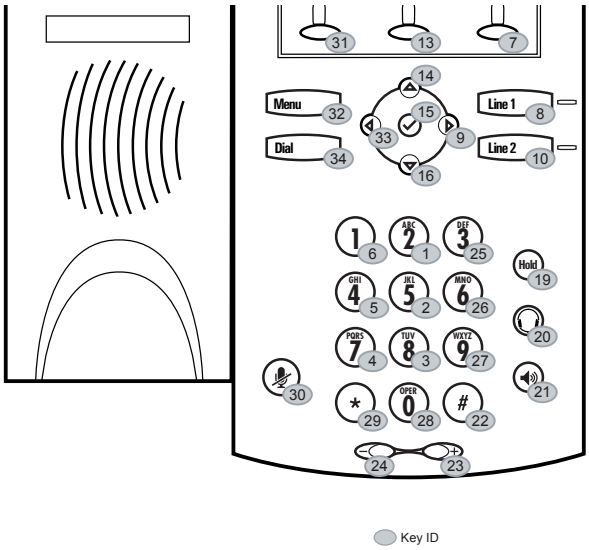
For the key combination, press and hold certain key combinations (depending on the phone model) simultaneously until a confirmation tone is heard or for about three seconds:

- IP 32x/33x: Menu, Dial, and the two Line keys
- IP 450, 550, 560, 600, 601, 650, 670, 5000, and 7000 and VVX 1500: Up, Down, Left, and Right arrow keys
- IP 6000: Menu, Exit, Off-hook/Hands-free, Redial

Default Feature Key Layouts

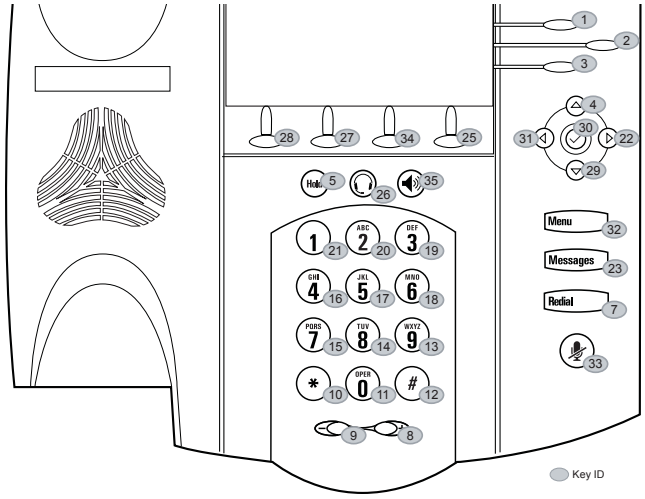
The following figures and tables show the default key layouts for the SoundPoint IP 32x/33x, 450, 550, 560, 650, and 670, SoundStation IP 5000, 6000 and 7000, and Polycom VVX 1500 models.

SoundPoint IP 320/321/330/331/335



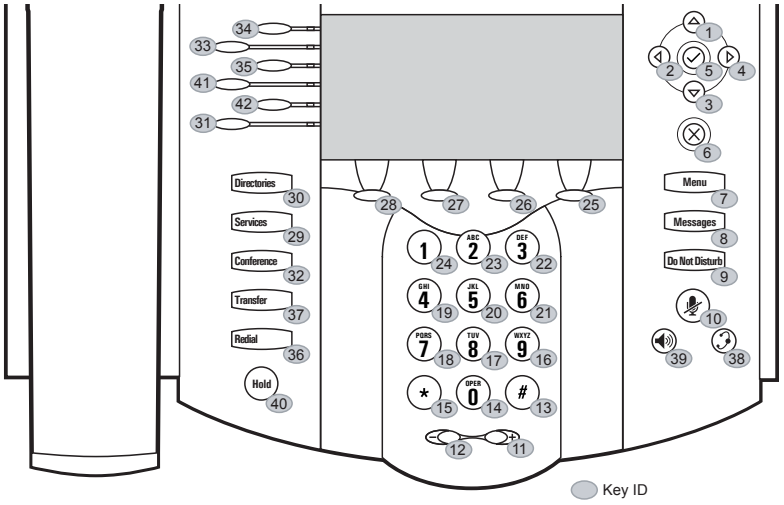
Key ID	Function	Key ID	Function	Key ID	Function	Key ID	Function
1	Dialpad2	12	n/a	23	VolUp	34	Menu
2	Dialpad5	13	SoftKey2	24	VolDown	35	n/a
3	Dialpad8	14	ArrowUp	25	Dialpad3	36	n/a
4	Dialpad7	15	Select	26	Dialpad6	37	n/a
5	Dialpad4	16	ArrowDown	27	Dialpad9	38	n/a
6	Dialpad1	17	n/a	28	Dialpad0	39	n/a
7	SoftKey3	18	n/a	29	DialpadStar	40	n/a
8	Line1	19	Hold	30	MicMute	41	n/a
9	ArrowRight	20	Headset	31	SoftKey1	42	n/a
10	Line2	21	Handsfree	32	Dial		
11	n/a	22	DialpadPound	33	ArrowLeft		

SoundPoint IP 450



Key ID	Function	Key ID	Function	Key ID	Function	Key ID	Function
1	Line1	12	DialpadPound	23	Messages	34	SoftKey3
2	Line2	13	Dialpad9	24	n/a	35	Handsfree
3	Line3	14	Dialpad8	25	Softkey4	36	n/a
4	ArrowUp	15	Dialpad7	26	Headset	37	n/a
5	Hold	16	Dialpad4	27	SoftKey2	38	n/a
6	n/a	17	Dialpad5	28	SoftKey1	39	n/a
7	Redial	18	Dialpad6	29	ArrowDown	40	n/a
8	VolUp	19	Dialpad3	30	Select	41	n/a
9	VolDown	20	Dialpad2	31	ArrowLeft	42	n/a
10	DialpadStar	21	Dialpad1	32	Menu		
11	Dialpad0	22	ArrowRight	33	MicMute		

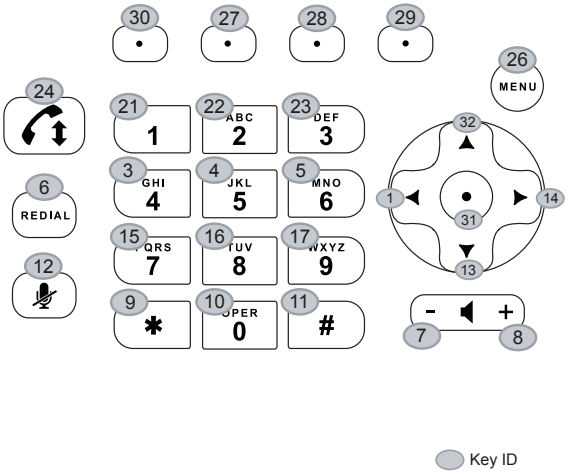
SoundPoint IP 550/560/650/670



Note The SoundPoint IP 550 and 560 has have only the top four lines keys. Key IDs 31 and 42 are not used on SoundPoint IP 550 and 560 phones.

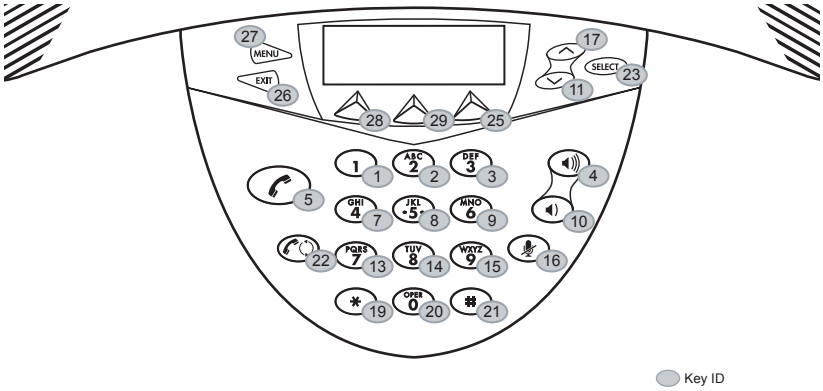
Key ID	Function	Key ID	Function	Key ID	Function	Key ID	Function
1	ArrowUp	12	VolDown	23	Dialpad2	34	Line1
2	ArrowLeft	13	DialpadPound	24	Dialpad1	35	Line3
3	ArrowDown	14	Dialpad0	25	SoftKey4	36	Redial
4	ArrowRight	15	DialpadStar	26	SoftKey3	37	Transfer
5	Select	16	Dialpad9	27	SoftKey2	38	Headset
6	Delete	17	Dialpad8	28	SoftKey1	39	Handsfree
7	Menu	18	Dialpad7	29	Applications	40	Hold
8	Messages	19	Dialpad4	30	Directories	41	Line4
9	DoNotDisturb	20	Dialpad5	31	Line6	42	Line5
10	MicMute	21	Dialpad6	32	Conference		
11	VolUp	22	Dialpad3	33	Line2		

SoundStation IP 5000



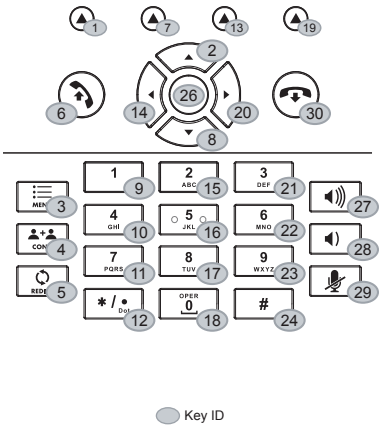
Key ID	Function	Key ID	Function	Key ID	Function	Key ID	Function
1	ArrowLeft	12	MicMute	23	Dialpad3	34	n/a
2	n/a	13	ArrowDown	24	Handsfree	35	n/a
3	Dialpad4	14	ArrowRight	25	n/a	36	n/a
4	Dialpad5	15	Dialpad7	26	Menu	37	n/a
5	Dialpad6	16	Dialpad8	27	SoftKey2	38	n/a
6	Redial	17	Dialpad9	28	SoftKey3	39	n/a
7	VolDown	18	n/a	29	SoftKey4	40	n/a
8	VolUp	19	n/a	30	SoftKey1	41	n/a
9	DialpadStar	20	n/a	31	Select	42	n/a
10	Dialpad0	21	Dialpad1	32	ArrowUp		
11	DialpadPound	22	Dialpad2	33	n/a		

SoundStation IP 6000



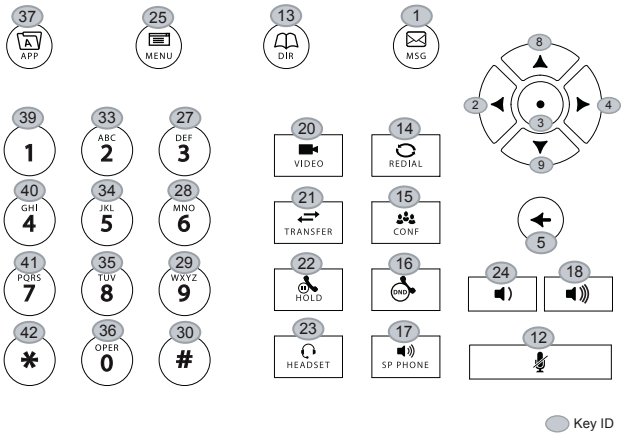
Key ID	Function	Key ID	Function	Key ID	Function	Key ID	Function
1	Dialpad1	12	n/a	23	Select	34	n/a
2	Dialpad2	13	Dialpad7	24	n/a	35	n/a
3	Dialpad3	14	Dialpad8	25	SoftKey3	36	n/a
4	VolUp	15	Dialpad9	26	Exit	37	n/a
5	Handsfree	16	MicMute	27	Menu	38	n/a
6	n/a	17	ArrowUp	28	SoftKey1	39	n/a
7	Dialpad4	18	n/a	29	SoftKey2	40	n/a
8	Dialpad5	19	DialpadStar	30	n/a	41	n/a
9	Dialpad6	20	Dialpad0	31	n/a	42	n/a
10	VolDown	21	DialpadPound	32	n/a		
11	ArrowDown	22	Redial	33	n/a		

SoundStation IP 7000



Key ID	Function	Key ID	Function	Key ID	Function	Key ID	Function
1	SoftKey1	12	DialpadStar	23	Dialpad9	34	n/a
2	ArrowUp	13	SoftKey3	24	DialpadPound	35	n/a
3	Menu	14	ArrowLeft	25	n/a	36	n/a
4	Conference	15	Dialpad2	26	Select	37	n/a
5	Redial	16	Dialpad5	27	VolUp	38	n/a
6	Handsfree	17	Dialpad8	28	VolDown	39	n/a
7	SoftKey2	18	Dialpad0	29	MicMute	40	n/a
8	ArrowDown	19	SoftKey4	30	Release	41	n/a
9	Dialpad1	20	ArrowRight	31	n/a	42	n/a
10	Dialpad4	21	Dialpad3	32	n/a		
11	Dialpad7	22	Dialpad6	33	n/a		

VVX 1500



Key ID	Function	Key ID	Function	Key ID	Function	Key ID	Function
1	Messages	12	MicMute	23	Headset	34	Dialpad5
2	ArrowLeft	13	Directories	24	n/a	35	Dialpad8
3	Select	14	Redial	25	Menu	36	Dialpad0
4	ArrowRight	15	Conference	26	n/a	37	Applications
5	Delete	16	DoNotDisturb	27	Dialpad3	38	n/a
6	n/a	17	Handsfree	28	Dialpad6	39	Dialpad1
7	n/a	18	VolUp	29	Dialpad9	40	Dialpad4
8	ArrowUp	19	n/a	30	DialpadPound	41	Dialpad7
9	ArrowDown	20	Video	31	n/a	42	DialpadStar
10	n/a	21	Transfer	32	n/a		
11	n/a	22	Hold	33	Dialpad2		

Internal Key Functions

A complete list of internal key functions for enhanced feature keys and hard key mappings is shown in the following table.

The following guidelines should be noted:

- The **Label** value is case sensitive.
- Some functions are dependent on call state. Generally, if the soft key appears on a call screen, the soft key function is executable. There are some exceptions on the SoundPoint IP 32x/33x phone (because it does not display as many soft keys).

- On the SoundPoint IP 32x/33x phone, CallPickup and ParkedPickup refer to the same function. On other phones, CallPickup refers to the soft key function that provides the menu with separate soft keys for parked pickup, directed pickup, and group pickup.
- Some functions depend on the feature being enabled. For example, BuddyStatus and MyStatus require the presence feature to be enabled.
- Hard key remappings do not require the Enhanced Feature key feature to be enabled.
- The table below shows only Line1 to Line6 functions. For the SoundPoint IP 650 and 670 phones with attached Expansion Modules, Line7 to Line48 functions are also supported.

Label	Function	Notes
ACDAvailable	ACDAvailableFromIdle	
ACDLogin	ACDLoginLogout	
ACDLogout	ACDLoginLogout	
ACDUnavailable	ACDAvailableFromIdle	
Answer	Answer	Call screen only
Applications	Main Browser	
ArrowDown	ArrowDown	
ArrowLeft	ArrowLeft	
ArrowRight	ArrowRight	
ArrowUp	ArrowUp	
BargeIn	BargInShowAppearances, BargeIn	Call screen only
BuddyStatus	Buddy Status	
Callers	Callers	
CallList	Call Lists	
CallPark	ParkEntry	Call screen only
CallPickup	CallPickupEntry	Call screen only
Conference	ConferenceCall	Call screen only
Delete	Delete	
Dialpad0	Dialpad0	
Dialpad1	Dialpad1	
Dialpad2	Dialpad2	

Label	Function	Notes
Dialpad3	Dialpad3	
Dialpad4	Dialpad4	
Dialpad5	Dialpad5	
Dialpad6	Dialpad6	
Dialpad7	Dialpad7	
Dialpad8	Dialpad8	
Dialpad9	Dialpad9	
DialpadPound	DialpadPound	
DialpadStar	DialpadStar	
DialpadURL	Dialname	Call screen only
DirectedPiclup	DirectedPickup	Call screen only
Directories	Directories	
Divert	Forward	
DoNotDisturb	Do Not Disturb menu	
Exit	Exist existing menu	Menu only
GroupPickup	GroupPickup	
Handsfree	Handsfree	
Headset	Headset	Desktop phones only
Hold	Toggle Hold	
Join	Join	Call screen only
LCR	LastCallReturn	
Line1	Line Key 1	
Line2	Line Key 2	
Line3	Line Key 3	
Line4	Line Key 4	
Line5	Line Key 5	
Line6	Line Key 6	
ListenMode	Turn on speaker to listen only	
Menu	Menu	
Messages	Messages menu	

Label	Function	Notes
MicMute	MicMute	
MyStatus	MyStatus	
NewCall	NewCall	Call screen only
Null	Do nothing	
Offline	Offline for presence	
QuickSetup	Quick Setup feature	Call screen only
EnterRecord	enterCallRecord	Call screen only
Redial	Redial	Call screen only
Release	EndCall or Cancel hot dial	SoundStation IP 7000 only
ParkedPickup	ParkedPickup	Call screen only
Select	Select	
ServerACDAgentAvailable	serverACDAgentAvailable	
ServerACDAgentUnavailable	serverACDAgentUnavailable	
ServerACDSignIn	serverACDSignIn	
ServerACDSignOut	serverACDSignOut	
Setup	Settings menu	
Silence	RingerSilence	Call screen only
SoftKey1	SoftKey1	
SoftKey2	SoftKey2	
SoftKey3	SoftKey3	
SoftKey4	SoftKey4	
SpeedDial	SpeedDial	
Split	Split	Call screen only
Transfer	Transfer	Call screen only
Video	Video Polyco	m VVX 1500 only
VolDown	VolDown	
VolUp	VolUp	

Assigning a VLAN ID Using DHCP

To assign a VLAN ID to a phone using DHCP:

>> In the DHCP menu of the Main setup menu, set **VLAN Discovery** to **Fixed** or **Custom**.

When set to Fixed, the phone will examine DHCP options 128,144, 157 and 191 (in that order) for a valid DVD string.

When set to Custom, the value set in **VLAN ID Option** will be examined for a valid DVD string.

DVD string in the DHCP option must meet the following conditions to be valid:

- Must start with ?VLAN-A=? (case-sensitive)
- Must contain at least one valid ID
- VLAN IDs range from 0 to 4095
- Each VLAN ID must be separated by a ?+? character
- The string must be terminated by a ?;?
- All characters after the ?;? will be ignored
- There must be no white space before the ?;?
- VLAN IDs may be decimal, hex, or octal

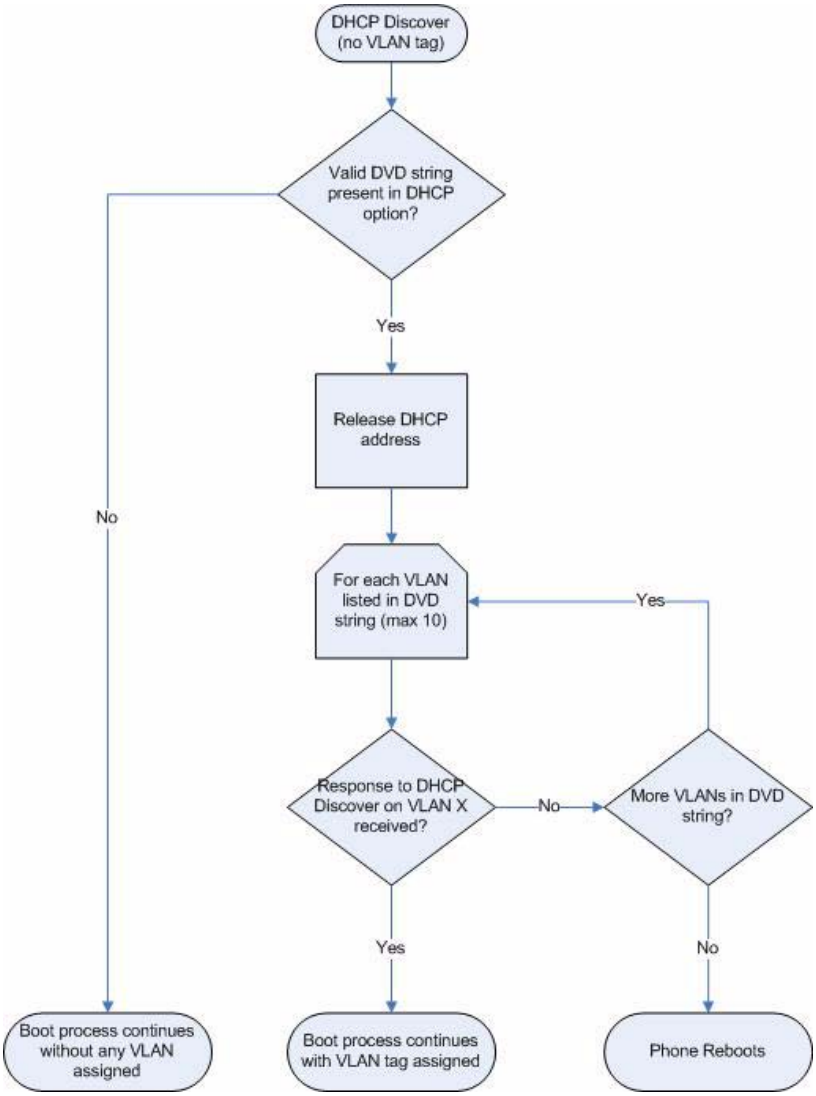
For example:

The following DVD strings will result in the phone using VLAN 10:

```
VLAN-A=10;
VLAN-A=0x0a;
VLAN-A=012;
```

Note If a VLAN tag is assigned by CDP, DHCP VLAN tags will be ignored.

The following figure shows the phone's processing to determine if the VLAN ID is valid:



Parsing Vendor ID Information

After the phone boots, it sends a DHCP Discover packet to the DHCP server. This is found in the Bootstrap Protocol/option "Vendor Class Identifier" section of the packet and includes the phone's part number and the BootROM version. The format of this option's data is not specified in RFC 2132, but is left to each vendor to define its own format. To be useful, every vendor's format must be distinguishable from every other vendor's format. To make our format uniquely identifiable, the format follows RFC 3925, which uses the

IANA Private Enterprise number to determine which vendor's format should be used to decode the remaining data. The private enterprise number assigned to Polycom is 13885 (0x0000363D).

This vendor ID information is not a character string, but an array of binary data. The steps for parsing are as follows:

1. Check for the Polycom signature at the start of the option:
   4 octet: 00 00 36 3d
2. Get the length of the entire list of sub-options:
   1 octet
3. Read the field code and length of the first sub-option, 1+1 octets
4. If this is a field you want to parse, save the data.
5. Skip to the start of the next sub-option.
6. Repeat steps 3 to 5 until you have all the data or you encounter the End-of-Suboptions code (0xFF).

For example, the following is a sample decode of a packet from an IP601:

```
3c 74
  - Option 60, length of Option data (part of the DHCP spec.)
00 00 36 3d
  - Polycom signature (always 4 octets)
6f
  - Length of Polycom data
01 07 50 6f 6c 79 63 6f 6d
  - sub-option 1 (company), length, "Polycom"
02 15 53 6f 75 6e 64 50 6f 69 6e 74 49 50 2d 53 50 49 50 5f 36 30 31
  - sub-option 2 (part), length, "SoundPointIP-SPIP_601"
03 10 32 33 34 35 2d 31 31 36 30 35 2d 30 30 31 2c 32
  - sub-option 3 (part number), length, "2345-11605-001,2"
04 1c 53 49 50 2f 54 69 70 2e 58 58 58 58 2f 30 38 2d 4a 75 6e 2d 30 37
20 31 30 3a 34 34
  - sub-option 4 (Application version), length, "SIP/Tip.XXXX/08-Jun-07
10:44"
05 1d 42 52 2f 33 2e 31 2e 30 2e 58 58 58 58 2f 32 38 2d 41 70 72 2d 30
35 20 31 33 3a 33 30
  - sub-option 5 (BootROM version), length, "BR/3.1.0.XXXX/28-Apr-05
13:30"
ff
  - end of sub-options
```

For the BootROM, sub-option 4 and sub-option 5 will contain the same string. The string is formatted as follows:

```
<apptype>/<buildid>/<date+time>
where:
<apptype> can be 'BR' (BootROM) or 'SIP' (SIP Application)
```

Product, Model, and Part Number Mapping

In SIP 2.1.2, enhancements to the master configuration file were made to allow you to direct phone upgrades to a software image and configuration files based on phone model number, firmware part number, or MAC address.

The part number specific version has precedence over the model number version, which has precedence over the original version. For example, CONFIG_FILES_2345-11560-001="phone1_2345-11560-001.cfg, sip_2345-11560-001.cfg" will override CONFIG_FILES_SPIP560="phone1_SPIP560.cfg, sip_SPIP560.cfg", which will override CONFIG_FILES="phone1.cfg, sip.cfg" for an SoundPoint IP 560.

You can also add variables to the master configuration file that are replaced when the phone reboots. The variables include PHONE_MODEL, PHONE_PART_NUMBER, and PHONE_MAC_ADDRESS.

The following table shows the product name, model name, and part number mapping for SoundPoint IP, SoundStation IP, and Polycom VVX 1500 phones:

Product Name	Model Name	Product Part Number
SoundPoint IP 300	SPIP300	2345-11300-001
SoundPoint IP 301	SPIP301	2345-11300-010
SoundPoint IP 320	SPIP320	2345-12200-002, 2345-12200-005
SoundPoint IP 321	SPIP321	2345-13600-001
SoundPoint IP 330	SPIP330	2345-12200-001, 2345-12200-004
SoundPoint IP 331	SPIP331	2345-12365-001
SoundPoint IP 335	SPIP335	2345-12375-001
SoundPoint IP 430	SPIP430	2345-11402-001
SoundPoint IP 450	SPIP450	2345-12450-001
SoundPoint IP 500	SPIP500	2345-11500-001, 2345-11500-010, 2345-11500-020
SoundPoint IP 501	SPIP501	2345-11500-030, 2345-11500-040
SoundPoint IP 550	SPIP550	2345-12500-001
SoundPoint IP 560	SPIP560	2345-12560-001
SoundPoint IP 600	SPIP600	2345-11600-001
SoundPoint IP 601	SPIP601	2345-11605-001

Product Name	Model Name	Product Part Number
SoundPoint IP 650	SPIP650	2345-12600-001
SoundPoint IP 670	SPIP670	2345-12670-001
SoundStation IP 4000	SSIP4000	2201-06642-001
SoundStation IP 5000	SSIP5000	3111-30900-001
SoundStation IP 6000	SSIP6000	3111-15600-001
SoundStation IP 7000	SSIP7000	3111-40000-001
Polycom VVX 1500	VVX1500	2345-17960-001

Disabling PC Ethernet Port

Certain SoundPoint IP phones have a PC Ethernet port. If it is unused, it can be disabled.

The PC Ethernet port can be disabled on the SoundPoint IP 33x, 450, 550, 560, 601, 650, and 670, and Polycom VVX 1500 through the menu (shown below). The Ethernet port can also be disabled through the configuration files.

To disable the Ethernet port on a supported SoundPoint IP phone:

1. Press Menu.
2. Select **Settings > Advanced > Network Configuration > Ethernet Menu**.

   You must enter the administrator password to access the network configuration. The factory default password is 456.
3. Scroll down to PC Port Mode and select **Edit**.
4. Select **Disabled,** and then press the **OK** soft key.
5. Press the **Exit** soft key.
6. Select **Save Config**.

   The Polycom phone reboots. When the reboot is complete, the PC Ethernet port is disabled.

Modifying Phone's Configuration Using the Web Interface

You can make changes to the phone's configuration through the web interface to the phone. These changes are stored in a separate file. You can remove these changes at a later time.

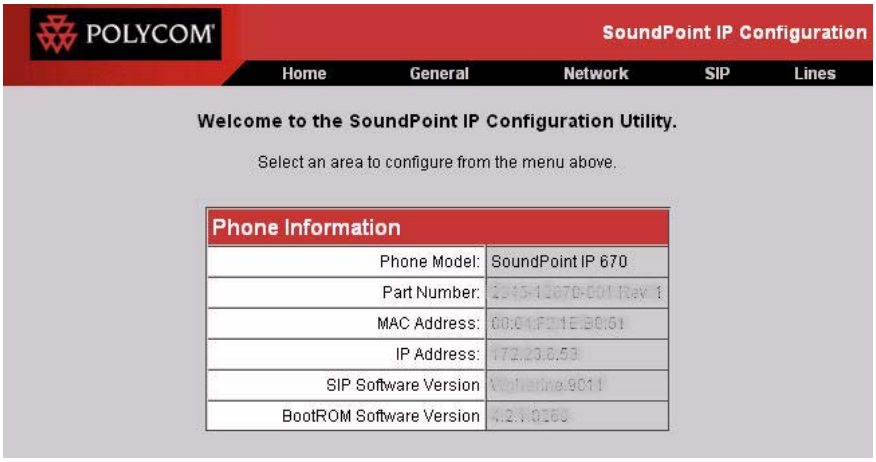
To configure your phone through the web interface:

>> Using your chosen browser, do the following:

a To get your phone's IP address, press the **Menu** key, and then selecting **Status > Platform > Phone**. Scroll down to see the IP address.

b Enter your phone's IP address as the browser address.

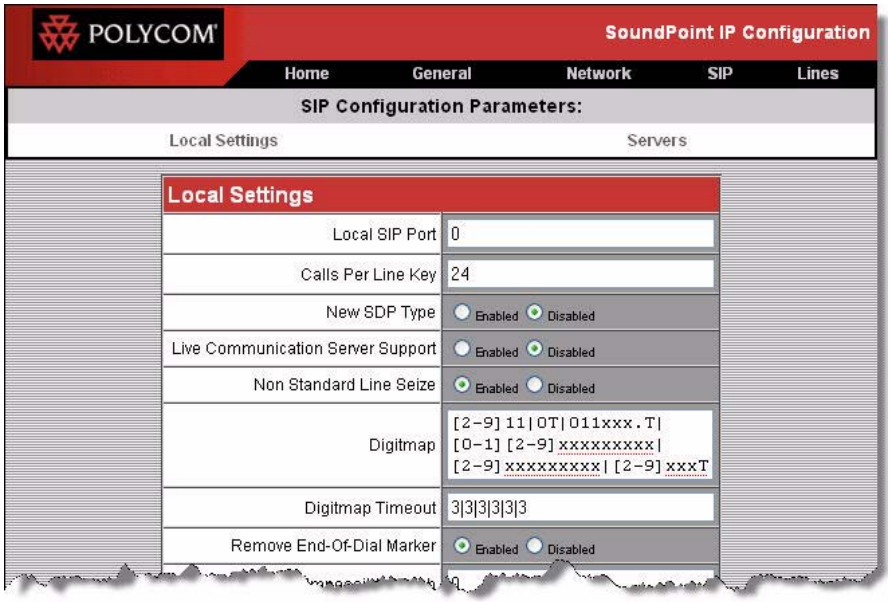
A web page similar to the one shown below appears.



c Select **SIP** from the menu tab.

You will be prompted for the SIP username and password.

A web page similar to the one shown below appears.

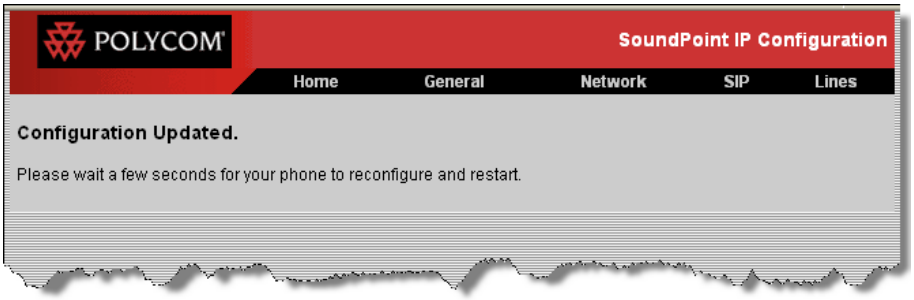


d Make the desired configuration changes.

e Scroll down to the bottom of the **Servers** section.

f Select the **Submit** button.

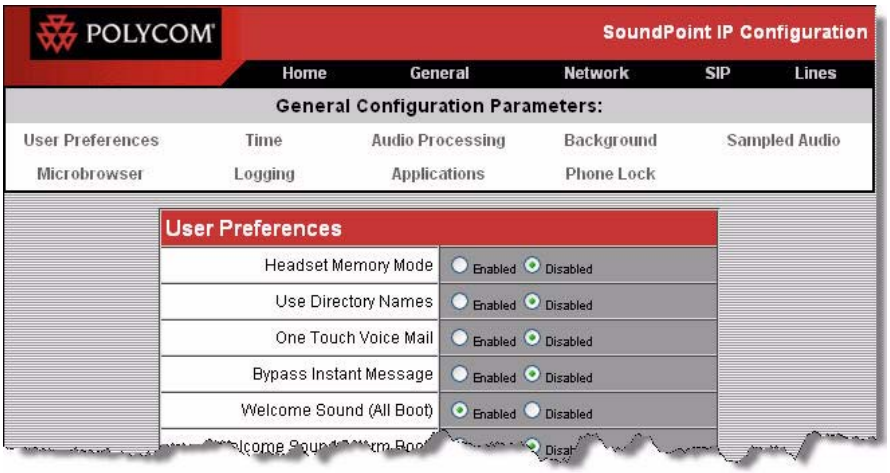
A web page similar to the one shown below appears.



Your phone will reboot.

g Select **General** from the menu tab.

A web page similar to the one shown below appears.



h If you make any changes, scroll down to the bottom of the section.

i Select the **Submit** button.

Your phone will reboot.

To remove the changes made through the web interface:

1. Press the **Menu** key, and then select **Settings > Advanced > Admin Settings > Reset to Defaults > Reset Web Configuration**.
2. Press the **Yes** soft key.

Your phone will reboot. All overrides are removed.

Capturing Phone's Current Screen

You can capture the current screen on a SoundPoint IP, SoundStation IP or VVX phone through the web interface to the phone.

To capture the phone's current screen:

1. Modify the **your** configuration file as follows:
   a. Open the file in an XML editor.
   b. Add the following line:

```
<up up.screenCapture.enabled="1" />
```

   c. Save the modified configuration file.
2. On the phone, do the following:
   a. Press the **Menu** key, and then select **Settings > Basic > Preferences > Screen Capture**.
   b. Using the arrow keys, select **Enabled**, and then press the **Select** soft key.

Note You need to re-enable the Screen Capture feature after every phone restart or reboot (repeat step 2).

1. Using your chosen browser, do the following:
   — To get your phone's IP address, press the **Menu** key, and then select **Status > Platform > Phone**. Scroll down to see the IP address.
   — As the browser address, enter **`http://<phone's IP address>/captureScreen .`**

   The current screen that is shown on the phone is shown in the browser window. The image can be saved as a **BMP** or **JPEG** file.

LLDP and Supported TLVs

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network. The protocol was formally ratified as IEEE standard 802.1AB- 2005 in May 2005. Refer to section 10.2.4.4 of the LLDP-MED standard at http://www.tiaonline.org/standards/technology/voip/documents/ANSI-TIA-1057_final_for_publication.pdf .

The LLDP feature (added in SIP 3.2.0) supports VLAN discovery and LLDP power management, but not power negotiation. LLDP has a higher priority than CDP and DHCP VLAN discovery.

The following Type Length Values (TLVs) are supported:

- Mandatory
  - Chassis ID—Must be first TLV
  - Port ID—Must be second TLV
  - Time-to-live—Must be third TLV, set to 120 seconds
  - End-of-LLDPDU—Must be last TLV
  - LLDP-MED Capabilities
  - LLDP-MED Network Policy—VLAN, L2 QoS, L3 QoS
  - LLDP-MED Extended Power-Via-MDI TLV—Power Type, Power Source, Power Priority, Power Value
- Optional
  - Port Description
  - System Name—Administrator assigned name
  - System Description—Includes device type, phone number, hardware version, and software version
  - System Capabilities—Set as "Telephone" capability
  - MAC / PHY config status—Detects duplex mismatch
  - Management Address—Used for network discovery
  - LLDP-MED Location Identification—Location data formats: Co-ordinate, Civic Address, ECS ELIN
  - LLDP-MED Inventory Management —Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer's Name, Model Name, Asset ID

An LLDP frame shall contain all mandatory TLVs. The frame will be recognized as LLDP only if it contains mandatory TLVs. for the Polycom UC Software phones will support LLDP frames with both mandatory and optional TLVs. The basic structure of an LLDP frame and a table containing all TLVs along with each field is explained in Supported TLVs on page C-30.

Note

As per section 10.2.4.4 of the LLDP-MED standard, LLDP-MED endpoint devices need to transmit Location Identification TLVs if they are capable of either automatically determining their physical location by use of GPS or radio beacon or capable of being statically configured with this information.

At present, the for the Polycom UC Software phones do not have the capability to determine their physical location automatically or provision to a statically configured location. Because of these limitations, the for the Polycom UC Software phones will not transmit Location Identification TLV in the LLDP frame. However, the location information from the switch is decoded and displayed on the phone's menu.

For more information on device configuration parameters, refer to <device/> on page A-30.

Supported TLVs

This is the basic TLV format:

TLV Type (7 bits) [0-6]	TLV Length (9 bits) [7-15]	TLV Information (0-511 bytes)

The following is a list of supported TLVs:

No	Name	Type (7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Version	
						Sub-Type	Information
1	Chassis-Id[1]	1	6	0x0206	-	5	IP address of phone (4 bytes) ***Note**: 0.0.0.0 is sent until the phone has a valid IP address.*
2	Port-Id[1]	2	7	0x0407	-	3	MAC address of phone (6 bytes)
3	TTL	3	2	0x0602	-	-	TTL value is 120/0 sec
4	Port description	4	1	0x0801	-	-	Port description 1
5	System name	5	min len > 0, max len <= 255	-	-	-	Refer to System Names on page C-35

No	Name	Type (7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Version	
						Sub-Type	Information
6	System description	6	min len > 0, max len <= 255	-	-	-	Manufacturer's name - "Polycom"; Refer to Model Names on page C-35; Hardware version; Application version; BootROM version
7	Capabilities	7	4	0x0e04	-	-	System Capabilities: Telephone and Bridge if the phone has PC port support and it is not disabled. Enabled Capabilities: Telephone and Bridge if phone has PC port support, it is not disabled and PC port is connected to PC. ***Note**:* *PC port supported Phones: IP 330, IP 331, IP 335, IP 450, IP 550, IP 560, IP 650, and IP 670.* *PC port not supported phones:* *IP 5000, IP 6000, IP 7000, IP320, and IP321*.
8	Management Address	8	12	0x100c	-	-	Address String Len - 5, IPV4 subtype, IP address, Interface subtype - "Unknown", Interface number - "0", ODI string Len - "0"
9	IEEE 802.3 MAC/PHY config/status[1]	127	9	0xfe09	0x00120f	1	Auto Negotiation Supported - "1", enabled/disabled, Refer to PMD Advertise and Operational MAU on page C-36

No	Name	Type (7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Version	
						Sub-Type	Information
10	LLDP-MED capabilities	127	7	0xfe07	0x0012bb	1	Capabilities - 0x33 (LLDP-Med capabilities, Network policy, Extended Power Via MDI-PD, Inventory) Class Type III ***Note**: Once support for configuring location Identification information is locally available:* *Capabilities - 0x37 (LLDP-Med capabilities, Network policy, Location Identification, Extended Power Via MDI-PD, Inventory)* *Class Type III*
11	LLDP-MED network policy[2]	127	8	0xfe08	0x0012bb	2	ApplicationType: Voice (1), Policy: (Unknown(=1)/Defined(=0) Unknown, if phone is in booting stage or if switch doesn't support network policy TLV. Defined, if phone is operational stage and Networkpolicy TLV is received from the switch.), Tagged/Untagged, VlanId, L2 priority and DSCP

No	Name	Type (7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Version	
						Sub-Type	Information
12	LLDP-MED network policy[2]	127	8	0xfe08	0x0012bb	2	ApplicationType: Voice Signaling (2), Policy: (Unknown(=1)/Defined(=0) Unknown, if phone is in booting stage or if switch doesn't support network policy TLV. Defined, if phone is operational stage and Networkpolicy TLV is received from the switch.),Tagged/Untagged, VlanId, L2 priority and DSCP. ***Note**: Voice signaling TLV is sent only if it contains configuration parameters that are different from voice parameters.*
13	LLDP-MED network policy[2]	127	8	0xfe08	0x0012bb	2	ApplicationType: Video Conferencing (6),Policy: (Unknown(=1)/Defined(=0) Unknown, if phone is in booting stage or if switch doesn't support network policy TLV. Defined, if phone is operational stage and Networkpolicy TLV is received from the switch.),Tagged/Untagged, VlanId, L2 priority and DSCP. ***Note**: Video Conferencing TLV is sent only from Video capable phones (currently Polycom VVX 1500 only)*.
14	LLDP-MED location identification[3]	127	min len > 0, max len <= 511	-	0x0012bb	3	ELIN data format: 10 digit emergency number configured on the switch. Civic Address: physical address data such as city, street number, and building information.

No	Name	Type (7 bits) [0-6]	Length (9 bits) [7-15]	Type Length	Org. Unique Code (3 bytes)	Version	
						Sub-Type	Information
15	Extended power via MDI	127	7	0xfe07	0x0012bb	4	PowerType -PD device PowerSource-PSE&local Power Priority -Unknown PowerValue - Refer to Power Values on page C-37
16	LLDP-MED inventory hardware revision	127	min len > 0, max len <= 32	-	0x0012bb	5	Hardware part number and revision
17	LLDP-MED inventory firmware revision	127	min len > 0, max len <= 32	-	0x0012bb	6	BootROM revision
18	LLDP-MED inventory software revision	127	min len > 0, max len <= 32	-	0x0012bb	7	Application (SIP) revision
19	LLDP-MED inventory serial number	127	min len > 0, max len <= 32	-	0x0012bb	8	MAC Address (ASCII string)
20	LLDP-MED inventory manufacturer name	127	11	0xfe0b	0x0012bb	9	Polycom
21	LLDP-MED inventory model name	127	min len > 0, max len <= 32	-	0x0012bb	10	Refer to Model Names on page C-35
22	LLDP-MED inventory asset ID	127	4	0xfe08	0x0012bb	11	Empty (Zero length string)
23	End of LLDP DU	0	0	0x0000	-	-	-

Note

1. For other subtypes, refer to IEEE 802.1AB, March 2005 at http://www.ieee802.org/1/pages/802.1ab.html .
2. For other application types, refer to TIA Standards 1057, April 2006 at http://tia.nufu.eu/std/ANSI|TIA-1057 .
3. At this time, this TLV is not sent by the phone.

System Names

Model	System Name
IP 320	Polycom SoundPoint IP 320
IP 321	Polycom SoundPoint IP 321
IP 330	Polycom SoundPoint IP 330
IP 331	Polycom SoundPoint IP 331
IP 335	Polycom SoundPoint IP 335
IP 450	Polycom SoundPoint IP 450
IP 550	Polycom SoundPoint IP 550
IP 560	Polycom SoundPoint IP 560
IP 650	Polycom SoundPoint IP 650
IP 670	Polycom SoundPoint IP 670
IP 5000	Polycom SoundStation IP 5000
IP 6000	Polycom SoundStation IP 6000
IP 7000	Polycom SoundStation IP 7000
VVX 1500	Polycom VVX 1500

Model Names

Model	Model Name
IP 320	SoundPointIP-SPIP_320
IP 321	SoundPointIP-SPIP_321
IP 330	SoundPointIP-SPIP_330
IP 331	SoundPointIP-SPIP_331
IP 335	SoundPointIP-SPIP_335
IP 450	SoundPointIP-SPIP_450
IP 550	SoundPointIP-SPIP_550

Model	Model Name
IP 560	SoundPointIP-SPIP_560
IP 650	SoundPointIP-SPIP_650
IP 670	SoundPointIP-SPIP_670
IP 5000	SoundStationIP-SSIP_5000
IP 6000	SoundStationIP-SSIP_6000
IP 7000	SoundStationIP-SSIP_7000
VVX 1500	VVX-VVX_1500

PMD Advertise and Operational MAU

Mode/Speed	PMD Advertise Capability Bit	Operational MAU Type
10BASE-T half duplex mode	1	10
10BASE-T full duplex mode	2	11
100BASE-T half duplex mode	4	15
100BASE-T full duplex mode	5	16
1000BASE-T half duplex mode	14	29
1000BASE-T full duplex mode	15	30
Unknown	0	0

Note By default, all phones have the PMD Advertise Capability set for 10HD, 10FD, 100HD and 100FD bits. For SoundPoint IP 560 and IP 670, and Polycom VVX 1500 phones that have Gigabit Ethernet support PMD Advertise Capability also contains set 1000FD bit.

Power Values

Model	Power Usage (Watts)	Power Value Sent in LLDP-MED Extended Power Via MDI TLV
IP 320/330	4.3	43
IP 321	3.5	35
IP 331	3.7	37
IP 335	3.9	39
IP 450	5.4	54
IP 550	5.9	59
IP 560	8.3	83
IP 650 with EM	12	120
IP 670 with EM	14	140
IP 5000	5.8	58
IP 6000	9.8	98
IP 7000	9.8	198
VVX 1500	11.8	118

Note By default, the power values for the SoundPoint IP 650 and 670 are sent for the phone and the Expansion Module(s). The values are not adjusted when the Expansion Module(s) are detached from the phone.

D

Technical Support Configuration Parameters

This appendix provides detailed descriptions of configuration parameters used by the Polycom® SoundPoint® IP, SoundStation® IP, and VVX® 1500 phones running Polycom® UC Software 3.3.0 that are of interest to Polycom Technical Support and Polycom Partners only.

Changes to these configuration parameters are not required in day-to-day situations, but may need to be checked and changed if a customer reports issues with the phones in their deployment.

The list of the parameters that are documented in this appendix include:

<device/>

The global `device.set` parameter must be enabled when the initial installation is done, and then it should be disabled. This prevents subsequent reboots by individual phones triggering a reset of parameters on the phone that may have been tweaked since the initial installation.

Two `device` parameters exist for every configuration parameter—`device.xxx` and `device.xxx.set`.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
device.set	0 or 1	0	If set to 0, do not use any `device.xxx` fields to set any parameters. Set this to 0 after the initial installation. If set to 1, use the `device.xxx` fields that have `device.xxx.set` = 1. Set this to 1 for the initial installation only.
device.xxx	string	Null	Configuration parameter.
device.xxx.set	0 or 1	0	If set to 0, do not use the `device.xxx` value. If set to 1, use the `device.xxx` value. For example, if `device.net.ipAddress.set` = 1, then use the contents of the `device.net.ipAddress` field.

Warning

This feature is very powerful and should be used with caution. For example, an incorrect setting could set the IP Address of multiple phones to the same value.

Note that some parameters may be ignored, for example if DHCP is enabled it will still override the value set with `device.net.ipAddress`.

Individual parameters are checked to see whether they are in range, however, the interaction between parameters is not checked. If a parameter is out of range, an error message will appear in the log file and parameter will not be used.

Incorrect configuration could cause phones to get into a reboot loop. For example, server A has a configuration file that specifies that server B should be used, which has a configuration file that specifies that server A should be used.

Polycom recommends that you test the new configuration files on two phones before initializing all phones. This should detect any errors including IP address conflicts.

<key/>

Note Use of this parameter is not supported for the VVX 1500 phone.

These settings control the scrolling behavior of keys and can be used to change key functions.

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
key.scrolling.timeout	positive integer	1	The time-out after which a key that is enabled for scrolling will go into scrolling mode until the key is released. Keys enabled for scrolling are menu navigation keys (left, right, up, down arrows), volume keys, and some context-specific soft keys. The value is an integer multiple of 500 milliseconds (1=500ms).

<lcl/>

The following `<lcl/>` parameters are of interest to Customer Support only:

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
lcl.ml.lang.tags.x	string in the format *language_region, language; preference level*	The format is: • The first two letters are the ISO-639 language abbreviation. • The next two letters are the ISO-3166 country code. • The next two letters are the ISO-639 language abbreviation. • The remainder of the string is the preference level for the display of the language, or English if the language is not available For example: `lcl.ml.lang.tags.1 = "zh-cn,zh;q=0.9,en;q=0.8"` For more information, refer to the Accept-Language header definition in the HTTP RFC 2616 at http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.4

<log/>

Warning Logging parameter changes can impair system operation. Do not change any logging parameters without prior consultation with Polycom Technical Support.

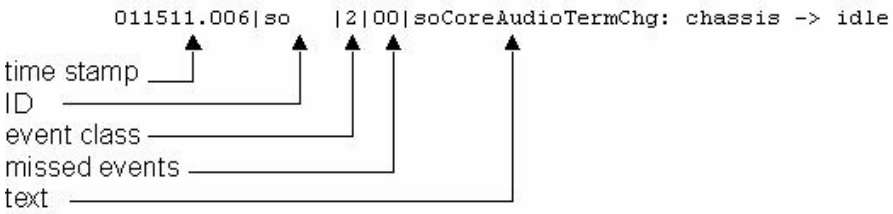
The event logging system supports the following classes of events:

Level	Interpretation
0	Debug only
1	High detail event class
2	Moderate detail event class
3	Low detail event class
4	Minor error - graceful recovery
5	Major error - will eventually incapacitate the system
6	Fatal error

Each event in the log contains the following fields separated by the | character:

- time or time/date stamp
- 1-5 character component identifier (such as "so")
- event class
- cumulative log events missed due to excessive CPU load
- free form text - the event description

Example:



Three formats are available for the event timestamp:

Type	Example
0 - seconds.milliseconds	`011511.006` -- 1 hour, 15 minutes, 11.006 seconds since booting.
1 - absolute time with minute resolution	`0210281716` -- 2002 October 28, 17:16
2 - absolute time with seconds resolution	`1028171642` -- October 28, 17:16:42

Two types of logging are supported:

- <level/><change/> and <render/>
- <sched/>

<level/><change/> and <render/>

This configuration attribute is defined as follows:

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
log.level.change.xxx	0 to 6	4	Control the logging detail level for individual components. These are the input filters into the internal memory-based log system. Possible values for xxx are acom, ares, app1, bdiag, brow, cap, cdp, cert, cfg, clink, cmp, cmr, copy, curl, dbuf, dhcpc, dis, dot1x, dns, ec, efk, ethf, h323, hset, httpa, httpd, hw, ht, ib, key, ldap, lic, lldp, log, mb, mobil, net, niche, nwmgr, oaip, osd, pcd, peer, pgui, pmt, pnetm, poll, pps, pstn, ptt, push, pwrsv, rdisk, res, rtos, sec, sig, sip, slog, so, soem, srtp, sshc, ssps, style, sync, sys, ask, trace, ttrs, usb, usbio, utilm, wdog, wlan, wmgr, and xmpp.
log.render.file	0 or 1	1	Set to 1. ***Note:*** *Polycom recommends that you do not change this value.*
log.render.file.size	positive integer, 1 to 180	16	Maximum local application log file size in Kbytes. When this size is exceeded, the file is uploaded to the provisioning server and the local copy is erased.
log.render.file.upload.append	0 or 1	1	If set to 1, use append mode when uploading log files to server. ***Note:*** *HTTP and TFTP don't support append mode unless the server is set up for this*.
log.render.file.upload.append.limitMode	delete, stop	delete	Behavior when server log file has reached its limit. delete=delete file and start over stop=stop appending to file

Attribute (bold = change causes restart/reboot)	Permitted Values	Default	Interpretation
log.render.file.upload.append.sizeLimit	positive integer	512	Maximum log file size on provisioning server in Kbytes.
log.render.file.upload.period	positive integer	172800	Time in seconds between log file uploads to the provisioning server. ***Note:*** *The log file will not be uploaded if no new events have been logged since the last upload*.
log.render.level	0 to 6	1	Specifies the lowest class of event that will be rendered to the log files. This is the output filter from the internal memory-based log system. The `log.render.level` maps to syslog severity as follows: 0 -> SeverityDebug (7) 1 -> SeverityDebug (7) 2 -> SeverityInformational (6) 3 -> SeverityInformational (6) 4 -> SeverityError (3) 5 -> SeverityCritical (2) 6 -> SeverityEmergency (0) For more information, refer to Syslog Menu on page 3-13.
log.render.realtime	0 or 1	1	Set to 1. ***Note:*** *Polycom recommends that you do not change this value.*
log.render.stdout	0 or 1	1	Set to 1. ***Note:*** *Polycom recommends that you do not change this value.*
log.render.type	0 to 2	2	Refer to above table for timestamp type.

<sched/>

The phone can be configured to schedule certain advanced logging tasks on a periodic basis. These attributes should be set in consultation with Polycom Technical Support. Each scheduled log task is controlled by a unique attribute set starting with log.sched.x where *x* identifies the task. A maximum of 10 schedule logs is allowed.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
log.sched.x.level	0 to 5, default 3	Event class to assign to the log events generated by this command. This needs to be the same or higher than log.level.change.slog for these events to appear in the log.
log.sched.x.name	alphanumeric string	Name of an internal system command to be periodically executed. To be supplied by Polycom.
log.sched.x.period	positive integer, default 15	Seconds between each command execution. 0=run once
log.sched.x.startDay	0 to 7	When startMode is *abs*, specifies the day of the week to start command execution. 1=Sun, 2=Mon, ..., 7=Sat
log.sched.x.startMode	abs, rel	Start at *abs*olute time or *rel*ative to boot.
log.sched.x.startTime	positive integer OR hh:mm	Seconds since boot when startMode is *rel* or the start time in 24-hour clock format when startMode is *abs*.

<voice/>

The following `<voice/>` parameters are of interest to Customer Support only.

Note The various .hd. parameters (such as `voice.aec.hd.enable` and `voice.ns.hd.enable`) are headset parameters. They are not connected to high definition or HD voice.

This attribute includes:

- <codecs/>
- <gain/>
- <aec/>
- <aes/>
- <ns/>

<codecs/>

These codecs include:

- <audioProfile/>

<audioProfile/>

The following profile attributes can be adjusted for each of the supported codecs. In the table, *x*=G711Mu, G711A, G719, G722, G7221, G7221C, G729AB, Lin16, Siren14, Siren22, and iLBC.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
voice.audioProfile.x.jitterBufferMax	> jitterBufferMin, multiple of 10, <=300 for IP 32x, 33x, 550, 600, and 650	The largest jitter buffer depth to be supported (in milliseconds). Jitter above this size will always cause lost packets. This parameter should be set to the smallest possible value that will support the expected network jitter. There is no jitter buffer maximum for G719, G7221, G7221C, iLBC, Lin16, Siren14, and Siren22.
voice.audioProfile.x.jitterBufferMin	20, 40, 50, 60, ... (multiple of 10)	The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. Once this depth has been achieved initially, the depth may fall below this point and play out will still continue. This parameter should be set to the smallest possible value which is at least two packet payloads, and larger than the expected short term average jitter. The IP4000 values are the same as the IP30x values. There is no jitter buffer minimum for G719, G7221, G7221C, iLBC, Lin16, Siren14, and Siren22.
voice.audioProfile.x.jitterBufferShrink	10, 20, 30, ... (multiple of 10)	The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. Use smaller values (1000 ms) to minimize the delay on known good networks. Use larger values to minimize packet loss on networks with large jitter (3000 ms). There is no jitter buffer shrink for G719, G7221, G7221C, iLBC, Lin16, Siren14, and Siren22.
voice.audioProfile.x.payloadSize	10, 20, 30, ...80	Preferred Tx payload size in milliseconds to be provided in SDP offers and used in the absence of ptime negotiations. This is also the range of supported Rx payload sizes. The payload size for G719 is further subdivided. There is no payload size for G719, G7221, G7221C, iLBC, Lin16, Siren14, and Siren22.

Attribute (bold = change causes restart/reboot)	Permitted Values	Interpretation
voice.audioProfile.x.payloadType	96 - 127 (default)	The codec payload encoding in the dynamic range to be used in SDP offers.

<gain/>

The default gain settings have been carefully adjusted to comply with the TIA-810-A digital telephony standard.

Attribute (bold = change causes restart/reboot)	Default
voice.gain.rx.analog.chassis.IP_330	0
voice.gain.rx.analog.chassis.IP_450	0
voice.gain.rx.analog.chassis.IP_5000	0
voice.gain.rx.analog.chassis.IP_6000	0
voice.gain.rx.analog.chassis.IP_650	0
voice.gain.rx.analog.chassis.IP_7000	0
voice.gain.rx.analog.chassis.VVX_1500	-3
voice.gain.rx.analog.handset	0
voice.gain.rx.analog.handset.sidetone	-20
voice.gain.rx.analog.handset.sidetone.VVX_1500	-15
voice.gain.rx.analog.handset.VVX_1500	-2
voice.gain.rx.analog.headset	0
voice.gain.rx.analog.headset.sidetone	-24
voice.gain.rx.analog.headset.sidetone.VVX_1500	-31
voice.gain.rx.analog.headset.VVX_1500	-2
voice.gain.rx.analog.ringer.IP_330	0
voice.gain.rx.analog.ringer.IP_450	0
voice.gain.rx.analog.ringer.IP_5000	0
voice.gain.rx.analog.ringer.IP_6000	0
voice.gain.rx.analog.ringer.IP_650	0
voice.gain.rx.analog.ringer.IP_7000	0
voice.gain.rx.analog.ringer.VVX_1500	0
voice.gain.rx.digital.chassis.IP_330	5

Attribute (bold = change causes restart/reboot)	Default
voice.gain.rx.digital.chassis.IP_450	5
voice.gain.rx.digital.chassis.IP_5000	11
voice.gain.rx.digital.chassis.IP_6000	5
voice.gain.rx.digital.chassis.IP_650	5
voice.gain.rx.digital.chassis.IP_7000	5
voice.gain.rx.digital.chassis.VVX_1500	0
voice.gain.rx.digital.handset	-15
voice.gain.rx.digital.handset.VVX_1500	-15
voice.gain.rx.digital.headset	-21
voice.gain.rx.digital.headset.VVX_1500	-21
voice.gain.rx.digital.ringer	-21
voice.gain.rx.digital.ringer.IP_330	-12
voice.gain.rx.digital.ringer.IP_450	-12
voice.gain.rx.digital.ringer.IP_5000	-12
voice.gain.rx.digital.ringer.IP_6000	-21
voice.gain.rx.digital.ringer.IP_650	-12
voice.gain.rx.digital.ringer.IP_7000	-21
voice.gain.rx.digital.ringer.VVX_1500	-21
voice.gain.tx.analog.chassis.IP_330	36
voice.gain.tx.analog.chassis.IP_450	36
voice.gain.tx.analog.chassis.IP_5000	0
voice.gain.tx.analog.chassis.IP_6000	0
voice.gain.tx.analog.chassis.IP_650	36
voice.gain.tx.analog.chassis.IP_7000	0
voice.gain.tx.analog.chassis.VVX_1500	-25
voice.gain.tx.analog.handset	6
voice.gain.tx.analog.handset.VVX_1500	-48
voice.gain.tx.analog.headset	3
voice.gain.tx.analog.headset.VVX_1500	-47
voice.gain.tx.digital.chassis.IP_330	12

Attribute (bold = change causes restart/reboot)	Default
voice.gain.tx.digital.chassis.IP_450	12
voice.gain.tx.digital.chassis.IP_5000	15
voice.gain.tx.digital.chassis.IP_6000	6
voice.gain.tx.digital.chassis.IP_650	12
voice.gain.tx.digital.chassis.IP_7000	6
voice.gain.tx.digital.chassis.VVX_1500	3
voice.gain.tx.digital.handset	0
voice.gain.tx.digital.handset.IP_330	10
voice.gain.tx.digital.handset.IP_450	6
voice.gain.tx.digital.handset.IP_650	6
voice.gain.tx.digital.handset.VVX_1500	12
voice.gain.tx.digital.headset	0
voice.gain.tx.digital.headset.IP_330	10
voice.gain.tx.digital.headset.IP_450	6
voice.gain.tx.digital.headset.IP_650	6
voice.gain.tx.digital.headset.VVX_1500	12
voice.handset.rxag.adjust.IP_330	1
voice.handset.rxag.adjust.IP_450	1
voice.handset.rxag.adjust.IP_650	1
voice.handset.sidetone.adjust.IP_330	3
voice.handset.sidetone.adjust.IP_450	0
voice.handset.sidetone.adjust.IP_650	0
voice.handset.txag.adjust.IP_330	18
voice.handset.txag.adjust.IP_450	18
voice.handset.txag.adjust.IP_650	18
voice.headset.rxag.adjust.IP_330	4
voice.headset.rxag.adjust.IP_450	4
voice.headset.rxag.adjust.IP_650	1
voice.headset.sidetone.adjust.IP_330	-3
voice.headset.sidetone.adjust.IP_450	-3

Attribute (bold = change causes restart/reboot)	Default
voice.headset.sidetone.adjust.IP_650	-3
voice.headset.txag.adjust.IP_330	21
voice.headset.txag.adjust.IP_450	21
voice.headset.txag.adjust.IP_650	21

<aec/>

These settings control the performance of the speakerphone acoustic echo canceller.

Attribute (bold = change causes restart/reboot)	Default
voice.aec.hd.enable	0
voice.aec.hf.enable	1
voice.aec.hs.enable	1

<aes/>

Acoustic Echo Suppression (AES) provides non-linear processing of the microphone signal to remove any residual echo remaining after linear AEC processing. Because AES depends on AEC, AES should only be enabled when AEC is also enabled. Normally, AES should be used whenever AEC is used for handsfree or handset and both are enabled by default for those terminations

These settings control the performance of the speakerphone acoustic echo suppressor.

Attribute (bold = change causes restart/reboot)	Default
voice.aes.hd.enable	0

<ns/>

These settings control the performance of the transmit background noise suppression feature.

Attribute **(bold = change causes restart/reboot)**	**Default**
voice.ns.hd.enable	0
voice.ns.hd.signalAttn	0
voice.ns.hd.silenceAttn	0
voice.ns.hf.enable	1
voice.ns.hf.signalAttn	-6
voice.ns.hf.silenceAttn	-9
voice.ns.hs.enable	1
voice.ns.hs.signalAttn	-6
voice.ns.hs.silenceAttn	-9

E

Third Party Software

This appendix provides the copyright statements for third party software products that are part of the application programs that run on Polycom SoundPoint IP, SoundStation IP, and VVX 1500 phones.

Product	License Location
c-ares	c-ares on page E-2
curl	curl on page E-3
eXpat	eXpat on page E-9
ILG JPEG	IJG JPEG on page E-9
libMng	libMng on page E-10
libPng	libPng on page E-11
libSRTP	libSRTP on page E-13
libssh2	libssh2 on page E-13
OpenLDAP	OpenLDAP on page E-15
OpenSSL	OpenSSL on page E-16
zlib	zlib on page E-18

This appendix provides the copyright statements for third party software products that are part of the application programs that run on Polycom VVX 1500 phones only.

Product	License Location
BusyBox	Refer to the “Polycom Voice OFFER of Source for GPL and LGPL Software”
dhcp	dhcp 4.0.0-14 on page E-3
droidfonts	droidfonts on page E-4
Dropbear	Dropbear on page E-7

Product	License Location
glibc	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
gloox	gloox on page E-9
libstdc++	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
Linux kernel	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
module-init-tools	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
mtd-utils	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
ncurses	ncurses on page E-14
pmap	pmap-29092002 on page E-18
procps	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
tsattach	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
tslib	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
udev	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
Webkit	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"
wrsv-ltt	Refer to the "Polycom Voice OFFER of Source for GPL and LGPL Software"

The "Polycom Voice OFFER of Source for GPL and LGPL Software" is available at http://downloads.polycom.com/voice/voip/offerForSourceVoiceProducts.html .

c-ares

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting

documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

curl

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2008, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

dhcp 4.0.0-14

Copyright (c) 2004-2009 by Internet Systems Consortium, Inc. ("ISC")

Copyright (c) 1995-2003 by Internet Software Consortium

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Internet Systems Consortium, Inc.

950 Charter Street

Redwood City, CA 94063

<info@isc.org>

http://www.isc.org/

droidfonts

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

1. You must give any other recipients of the Work or Derivative Works a copy of this License; and

2. You must cause any modified files to carry prominent notices stating that You changed the files; and

3. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from

the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

4. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any

character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Dropbear

The majority of code is written by Matt Johnston, under the license below. Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2006 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR

OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

eXpat

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

gloox

Portions of this SOFTWARE PRODUCT are © 2006 by Jakob Schroeter <js@camaya.net>. All rights reserved.

IJG JPEG

Independent JPEG Group's free JPEG software

This package contains C software to implement JPEG image encoding, decoding, and transcoding. JPEG is a standardized compression method for full-color and gray-scale images.

The distributed programs provide conversion between JPEG "JFIF" format and image files in PBMPLUS PPM/PGM, GIF, BMP, and Targa file formats. The core compression and decompression library can easily be reused in other programs, such as image viewers. The package is highly portable C code; we have tested it on many machines ranging from PCs to Crays.

We are releasing this software for both noncommercial and commercial use. Companies are welcome to use it as the basis for JPEG-related products. We do not ask a royalty, although we do ask for an acknowledgement in product literature (see the README file in the distribution for details). We hope to make this software industrial-quality --- although, as with anything that's free, we offer no warranty and accept no liability.

For more information, contact jpeg-info@jpegclub.org.

Contents of this directory

jpegsrc.vN.tar.gz contains source code, documentation, and test files for release N in Unix format.

jpegsrN.zip contains source code, documentation, and test files for release N in Windows format.

jpegaltui.vN.tar.gz contains source code for an alternate user interface for cjpeg/djpeg in Unix format.

jpegaltuiN.zip contains source code for an alternate user interface for cjpeg/djpeg in Windows format.

wallace.ps.gz is a PostScript file of Greg Wallace's introductory article about JPEG. This is an update of the article that appeared in the April 1991 Communications of the ACM.

jpeg.documents.gz tells where to obtain the JPEG standard and documents about JPEG-related file formats.

jfif.ps.gz is a PostScript file of the JFIF (JPEG File Interchange Format) format specification.

jfif.txt.gz is a plain text transcription of the JFIF specification; it's missing a figure, so use the PostScript version if you can.

TIFFTechNote2.txt.gz is a draft of the proposed revisions to TIFF 6.0's JPEG support.

pm.errata.gz is the errata list for the first printing of the textbook "JPEG Still Image Data Compression Standard" by Pennebaker and Mitchell.

jdosaobj.zip contains pre-assembled object files for JMEMDOSA.ASM.

If you want to compile the IJG code for MS-DOS, but don't have an assembler, these files may be helpful.

libMng

COPYRIGHT NOTICE:

Copyright © 2000-2008 Gerard Juyn (gerard@libmng.com)

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Gerard Juyn

(hopefully some more to come...)

The MNG Library is supplied "AS IS". The Contributing Authors disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the MNG Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.

2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.

3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors specifically permit, without fee, and encourage the use of this source code as a component to supporting the MNG and JNG file format in commercial products. If you use this source code in a product, acknowledgment would be highly appreciated.

libPng

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 1.2.6, August 15, 2004, through 1.2.40, September 10, 2009, are Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.

2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.

3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

September 10, 2009

libSRTP

Copyright (c) 2001-2005 Cisco Systems, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Cisco Systems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

libssh2

Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>

Copyright (C) 2006-2007 The Written Word, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the copyright holder nor the names of any other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ncurses

Copyright (c) 1998-2004, 2006 Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished - to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

OpenLDAP

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.

Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

OpenSSL

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

Original SSLeay License:
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.
This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscape's SSL.
This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).
Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

pmap-29092002

zlib

Jean-loup Gailly
jloup@gzip.org

Mark Adler
madler@alumni.caltech.edu

Index

POLYCOM, INC.
APPLICATION PROGRAMMING INTERFACE LICENSE ("API")
FOR SOUNDPOINT IP AND SOUNDSTATION IP PRODUCTS ("Product" or "Products").

1. Agreement. You understand and agree that by using the API you will be bound by the terms of the End User License and Warranty Terms included with the Product(s) and this document (together, the "Agreement"). In the event of any conflicts between the End User License and Warranty Terms and this document, this document shall govern with respect to the API.

2. Parties. For purposes of this Agreement "you" or "your" shall mean the individual or entity accepting this Agreement or using the API. The relationship between you and Polycom is that of licensee/licensor. No legal partnership or agency relationship is created between you and Polycom. Neither you nor Polycom is a partner, an agent or has any authority to bind the other. You agree not to represent otherwise.

3. License/Ownership. Subject to your compliance with this Agreement, Polycom hereby grants you a limited license to use the API solely for the purposes of developing and testing your own proprietary software to be used in conjunction with the Product(s). The foregoing license does not grant you any distribution rights or other rights to use the API for any other purpose and you agree that you shall not rent, lease, loan, sell, sublicense, assign or otherwise transfer any rights in the API. Polycom retains ownership of the API, and except as expressly set forth herein, no other rights or licenses are granted. Polycom may change, suspend or discontinue providing the API at any time.

4. Term/Survival. Without prejudice to any other rights, Polycom may terminate this Agreement if you fail to comply with any of the terms and conditions of this Agreement. In such an event, you must destroy all copies of the API. You may terminate this Agreement at any time by destroying the API. In the event of any termination of this Agreement, Sections 1, 2, 5, and 7-11 shall survive termination.

5. Development. Nothing in this Agreement shall impair Polycom's right to develop, acquire, license, market, promote or distribute products, software or technologies that perform the same or similar functions as, or otherwise compete with any other products, software or technologies that you may develop, produce, market, or distribute. In the absence of a separate written agreement to the contrary, Polycom shall be free to use any information, suggestions or recommendations you provide to Polycom for any purpose, subject to any applicable patents or copyrights.

6. Harmful Code. You agree not to include any "Harmful Code" in any products you develop by use of the API, including but not limited to any code that: (i) contains hidden files, "time bombs" or viruses; or (ii) can alter, damage, disclose or erase any data or other computer programs without control of a person operating the computing equipment on which it resides, or (iii) retrieves or collects information without the consent of the user or for any illegal or unauthorized purpose; or (iv) contains a key, node lock, time-out or other function whether implemented by electronic, mechanical or other means which restricts or may restrict use or access to programs or data on the Products, frequency or duration of use, or other limiting criteria; or (v) any code which may restrict, inhibit, disrupt or interfere with the functionality of the Products as provided by Polycom. You agree not to use the API for any illegal or unauthorized purpose.

7. Marketing/Trademarks. You are free to market any products you develop using the API, provided you agree not use the Polycom logo, the marks "Polycom," "SoundPoint," "SoundStation," any other marks belonging or licensed to Polycom, or any marks that are confusingly similar to marks belonging or licensed to Polycom in any way except as otherwise expressly authorized by Polycom in each instance. In no event shall you (i) expressly state or imply that any products developed by you were created by or on behalf of Polycom or are being marketed by or on behalf of Polycom; or (ii) expressly state or imply that Polycom has reviewed, sanctioned, or endorsed your product in any way.

8. No Warranty. You understand the API provided to you is supplied **"AS IS" AND "WITH ALL FAULTS" WITHOUT ANY WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY, NON-INFRINGEMENT, ACCURACY, COMPLETENESS, PERFORMANCE, AND FITNESS FOR A PARTICULAR PURPOSE, AND POLYCOM PROVIDES NO SUPPORT FOR THIS API.** You understand that Polycom is under no obligation to provide updates, enhancements, or corrections, or to notify you of any API changes that Polycom may make. In the event you market a product you develop using the API, any obligations, representations or warranties provided by you to an end user shall be solely your obligations, and in no event shall Polycom be responsible to fulfill any such obligations.

9. Indemnity. You shall indemnify and hold Polycom harmless from and against any and all costs, damages, losses, liability or expenses (including reasonable attorneys' fees) arising from your use of the API (including without limitation any actions arising from acts or omissions of your employees or agents) or any failure by you to comply with the terms of this Agreement.

10. Disclaimer of Liability. **UNDER NO CIRCUMSTANCES SHALL POLYCOM BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, DAMAGES RESULTING FROM DELAY OF DELIVERY OR FROM LOSS OF PROFITS, DATA, BUSINESS OR GOODWILL, ON ANY THEORY OF LIABILITY, WHETHER ARISING UNDER TORT (INCLUDING NEGLIGENCE), CONTRACT OR OTHERWISE, WHETHER OR NOT POLYCOM HAS BEEN ADVISED OR IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. POLYCOM'S ENTIRE LIABILITY FOR DIRECT DAMAGES UNDER THIS AGREEMENT IS LIMITED TO FIVE DOLLARS ($5.00).**

11. Miscellaneous. If any provision is found to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable. This Agreement constitutes the entire agreement between the parties with respect to its subject matter and supersedes all prior or contemporaneous understandings regarding such subject matter. No addition to or removal or modification of any of the provisions of this Agreement will be binding upon Polycom unless made in writing and signed by an authorized representative of Polycom.

YOUR USE OF THIS API ACKNOWLEDGES THAT YOU HAVE READ, UNDERSTAND AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS INDICATED ABOVE.

Corporate Headquarters:
4750 Willow Road
Pleasanton, CA 94588
U.S.A.

www.polycom.com
Phone 408-526-9000
Fax: 408-526-9100

By downloading the following Sample Applications, you agree to the below end user license agreement.

LICENSE AGREEMENT FOR DEVELOPMENT PURPOSES

This License Agreement for Development Purposes (the "Agreement") is a legal agreement between you and Polycom, Inc., a Delaware corporation ("Polycom").

The software you are about to download (the "Software") comprises sample code that may be useful in the development of applications designed to operate on or in conjunction with Polycom Products.

Polycom is willing to license the Software to you only upon the condition that you accept all of the terms contained in this agreement. Select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the downloading process will not continue.

PLEASE NOTE:

* POLYCOM OFFERS NO SUPPORT FOR THIS SOFTWARE, AND THE SOFTWARE IS BEING LICENSED WITHOUT DOCUMENTATION, WITHOUT WARRANTY, "AS-IS," AND "WITH ALL FAULTS."

* THE SOFTWARE HAS NOT BEEN TESTED BY POLYCOM AND SHOULD NOT BE LOADED ON PRODUCTION SYSTEMS.

1. GRANT OF LICENSE.

1.1. License. Subject to the terms of this Agreement, Polycom grants to you a nonexclusive, nontransferable license to copy, install, use, and modify the Software, including the Software in source code format, and to produce your own commercial or other purposes derivative works thereof. Except as provided below, this License Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights related to the Software.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

2.1. Copyright. All title and copyrights in and to the Software and any copies of the Software are owned by Polycom or its suppliers. The Software is protected by copyright laws and international treaty provisions. Title, ownership rights, and intellectual property rights in the Software shall remain in Polycom or its suppliers.

2.2. Ownership of Derivative Works. As between you and Polycom, you will own copyright and other intellectual property rights in derivative works of the Software that you develop.

2.3. Reservation. Polycom reserves all rights in the Software not expressly granted to you in this Agreement.

3. SUPPORT SERVICES.

3.1. No Support Services. Polycom provides no support services for the Software.

4. TERMINATION.

4.1. Termination. Without prejudice to any other rights, Polycom may terminate this Agreement if you fail to comply with any of the terms and conditions of this Agreement. In such event, you must destroy all copies of the Software and all of its component parts. You may terminate this Agreement at any time by destroying the Software and all of its component parts.

5. NO WARRANTY.

THE SOFTWARE IS LICENSED WITHOUT WARRANTY, "AS IS," AND "WITH ALL FAULTS." ALL WARRANTIES, TERMS OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ARE EXPRESSLY DISCLAIMED. POLYCOM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF THIS SOFTWARE.

6. LIMITATION OF LIABILITY.

6.1. Limitations. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL POLYCOM OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING. WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF POLYCOM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, POLYCOM'S ENTIRE LIABILITY SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE OR U.S. $5.00.

7. DISCLAIMER.

7.1. Disclaimer. Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages

for certain products supplied to consumers or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you.

8. EXPORT CONTROLS.

8.1. Export Controls. The Software may not be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iraq, Libya, North Korea, Yugoslavia, Iran, Syria, Republic of Serbia, or any other country to which the U.S. has embargoed goods; or (ii) to anyone on the U.S Treasury Department's List of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. By downloading or using this Software, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list. If you obtained this Software outside of the United States, you are also agreeing that you will not export or re-export it in violation of the laws of the country in which it was obtained.

9. MISCELLANEOUS.

9.1. Governing Law. This Agreement shall be governed by the laws of the State of California as such laws are applied to agreements entered into and to be performed entirely within California between California residents, and by the laws of the United States. The United Nations Convention on Contracts for the International Sale of Goods (1980) is hereby excluded in its entirety from application to this Agreement.

9.2. Venue for Resolving Disputes. Any disputes relating to this Agreement will be resolved only in the state or federal courts located in Santa Clara County, California. Each of the parties agrees to the exercise over them of the personal jurisdiction of such courts for such purpose.

9.3. U.S. Government Restricted Rights. The Software and documentation are provided with Restricted Rights. The Software programs and documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR 12.212(b), as applicable. Any use, modification, reproduction, release, performance, display, or disclosure of the Software programs and/or documentation by the U S. Government or any of its agencies shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions is deemed to be "technical data commercial items" pursuant to DFAR Section 227.7015(a). Any use, modification, reproduction, release, performance, display, or disclosure of such technical data shall be governed by the terms of DFAR Section 227.7015(b).

9.4. Relationship Between the Parties. The relationship between you and Polycom is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this

agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

9.5. Entire Agreement. This Agreement represents the complete agreement concerning this license and may be amended only by a writing executed by both parties. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

www.polycom.com

Corporate Headquarters: 4750 Willow Road, Pleasanton, CA 94588, USA Phone 408-526.9000 Fax: 408-526-9100