![Polycom®]

Polycom® UC Software 5.6.0

Contents

Conventions Used in Polycom Guides

Polycom guides contain terms, graphical elements, and a few typographic conventions. Familiarizing yourself with these terms, elements, and conventions will help you successfully perform tasks.

Information Elements

Polycom guides may include any of the following icons to alert you to important information.

Information Elements

Name	Icon	Description
Note		The Note icon highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.
Important		Important highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.
Caution		The Caution icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.
Warning		The Warning icon highlights an action you must perform (or avoid) to prevent issues that may cause you to lose information or your configuration setup, and/or affect phone or network performance.
Web Info		The Web Info icon highlights supplementary information available online such as documents or downloads on support.polycom.com or other locations.

Typographic Conventions

A few typographic conventions, listed next, are used in Polycom guides to distinguish types of in-text information.

Typographic Conventions

Convention	Description
Bold	Highlights interface items such as menus, menu selections, window and dialog names, soft keys, file names, and directory names when they are involved in a procedure or user action. Also used to highlight text to be entered or typed.
Italics	Used to emphasize text, to show example values or inputs (in this form: *<example>*), and to show titles of reference documents available from the Polycom Support Web site and other reference sites.
Blue Text	Used for cross references to other sections within this document and for hyperlinks to external sites and documents.
Courier	Used for code fragments, parameter names and permitted values.

Get Started

The Polycom® Unified Communications (UC) Software Administrator Guide provides general guidance on installing, provisioning, and managing Polycom phones. This guide helps you:

- Set up a large-scale provisioning environment
- Set up a VoIP network and provisioning server
- Configure phone features and user settings
- Troubleshoot, update, and maintain phones and UC Software

This Polycom UC Software Administrator Guide applies to the following Polycom devices except where noted:

- Polycom VVX business media phones, including the VVX 101, 201, 300 series (300/301/310/311), 400 series (400/401/410/411), 500 series (500/501) 600 series (600/601), and 1500
- Polycom VVX D60 Wireless Handset and Base Station
- Polycom VVX Expansion Modules
- Polycom SoundStructure® VoIP Interface

> To deploy Polycom devices with Microsoft Lync Server or Skype for Business, see *Polycom UC Software with Microsoft Lync Server and Skype for business - Deployment Guide* on Polycom Voice Support.

Audience and Purpose of This Guide

The primary audience for this guide is the person administering the session initiation protocol (SIP) server, provisioning servers, VoIP network, and Polycom UC Software that enable you to configure and manage phone features. This guide is not intended for end users. This guide provides information primarily for mid-level administrators with experience in networking who understand the basics of open SIP networks and VoIP endpoint environments. This guide indicates where information might be useful for novice administrators, and provides tips for advanced administrators where applicable.

Phone Deployment Scenarios

Because phone deployments vary, and administrators typically set up and maintain large-scale device deployments, Polycom cannot recommend a specific deployment scenario. For large-scale deployments, Polycom recommends setting up a provisioning server on the local area network (LAN) or on the Internet. For this reason, this administrator guide focuses on large-scale UC Software VoIP environments set up on

a central SIP and provisioning server. Administrators typically use the administrator guide in three large-scale device deployment scenarios:

● **Enterprise deployment**. An administrator sets up and maintains a deployment for a single organization and all users are in one physical location.

● **Multisite enterprise**. An administrator sets up and maintains a deployment for an organization and users are spread out over several locations varying in size.

● **Service Provider Deployment**. Service providers provide devices and service to a number of organizations and users spread out over several locations each varying in size.

Requirements

This section lists the general knowledge, skill, and technological requirements needed to deploy and provision Polycom devices and configure features.

General Knowledge Requirements

Before reading this guide, you should be familiar with the following:

● Computer networking and driver administration for your operating system

● SIP networks

● VoIP environments and technologies

● An XML editor

Polycom-Specific Skills

You need the following Polycom-specific skills to successfully deploy and configure Polycom devices:

● Polycom provisioning methods

● Polycom UC Software and XML configuration files

● Configuration parameters and values for end-user device features

● Troubleshooting your Polycom devices

● Maintaining and updating devices and software

Technological Requirements

You need the following to operate Polycom phones as SIP endpoints in large-scale deployments:

● A working IP network

● Routers configured for VoIP

● VoIP gateways configured for SIP

● The latest (or a compatible version) Polycom UC Software image

- An active, configured call server to receive and send SIP messages. For information on IP PBX and softswitch vendors, see Polycom Desktop Phone Compatibility. If you are using the Polycom RealPresence Trio Solution, see Polycom RealPresence Trio and SoundStation IP Platform Compatibility. At minimum, your call server requires:
  - ➢ A call server address that registers voice endpoints with the SIP server
  - ➢ SIP authentication user name and password the phone uses to respond to any SIP authentication challenges from the SIP server.
- An XML editor—such as XML Notepad—to create and edit configuration files

Get Help

For more information about installing, configuring, and administering Polycom products, refer to Documents and Downloads at Polycom Support.

To access Polycom UC Software releases and documentation, see Polycom Voice Support.

To access the user guide for Polycom voice products, refer to the product support page for your phone at Polycom Voice Support.

To find help or technical support for your phones, you can search for Polycom documentation at the Polycom Unified Communications (UC) Software Resource Center.

You can find Request for Comments (RFC) documents by entering the RFC number at http://www.ietf.org/rfc.html.

The Polycom Community

The Polycom Community gives you access to the latest developer and support information and enables you to participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.

For support or service, please contact your Polycom reseller or visit support.polycom.com for software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

We are constantly working to improve the quality of our documentation, and we would appreciate your feedback. Please send email to VoiceDocumentationFeedback@polycom.com.
Polycom recommends that you record the phone model numbers, software versions (for both the Updater and UC Software), and partner platform for future reference.

Phone models:

Updater version:

UC Software version:

Partner Platform:

Network Settings Configuration

Polycom UC Software supports the deployment of Polycom phones for your device network. This section explains how to establish phone connection to the network and how to configure network settings.

Ethernet Line Rates

The phones automatically negotiate the Ethernet rate and no special configuration is required. Typical network equipment supports one of the three following Ethernet line rates:

- 10 Mbps.
- 100 Mbps.
- 1000 Mbps.

While you can change the line rates and duplex configuration, Polycom recommends keeping the default settings.

Supported Denial of Service Filters

The phone supports two filters to prevent Denial of Service (DoS):

- **Storm Filtering**   This filter is enabled by default.
- **VLAN Filtering**   VLAN filtering cannot be disabled.

When these filters are enabled, Ethernet packets are filtered to prevent overflow caused by bad or excessive data. Support for Storm and VLAN filtering varies by device.

Related Topics

Extensible Authentication Protocol Method for 802.1x Parameters

Supported 802.1x Configurations

Polycom phones support the following EAP authentication methods:

- EAP-TLS (requires Device and CA certificates)
- EAP-PEAPv0/MSCHAPv2 (requires CA certificates)
- EAP-PEAPv0/GTC (requires CA certificates)
- EAP-TTLS/MSCHAPv2 (requires CA certificates)
- EAP-TTLS/GTC (requires CA certificates)
- EAP-FAST (optional Protected Access Credential (PAC) file, if not using in-band provisioning)
- EAP-MD5

For more information about EAP methods, see RFC 3748: Extensible Authentication Protocol.

Link Layer Discovery Protocol and Supported Type Length Values

A Link Layer Discovery Protocol (LLDP) frame must contain all mandatory Type Length Values (TLVs). Polycom phones running UC Software support LLDP frames with both mandatory and optional TLVs.

The phones cannot determine their physical location automatically or provision to a statically configured location. Hence, they do 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.

The LLDP feature supports VLAN discovery and LLDP power management, but not power negotiation. LLDP has a higher priority than Cisco Discovery Protocol (CDP) and DHCP VLAN discovery.

LLDP-MED Location Identification

According to section 10.2.4.4 of the LLDP-MED standard, LLDP-MED devices must 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 phones do not have the capability to determine their physical location automatically or provision to a statically configured location. As a result, Polycom phones do 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.

Supported TLVs

Polycom phones support the following mandatory and optional TLVs:

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 configuration 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.

The basic TLV format is as follows:

- TLV Type (7 bits) [0-6]
- TLV Length (9 bits) [7-15]
- TLV Information (0-511 bytes)

The following table lists the supported TLVs:

Supported TLVs

Name	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
Chassis-Id[1]	**1**	**6**	**0x0206**	**-**	**5**
IP address of phone (4 bytes). Note that 0.0.0.0 is not sent until the phone has a valid IP address.					
Port-Id[1]	**2**	**7**	**0x0407**	**-**	**3**
The MAC address of the phone (6 bytes).					
TTL	**3**	**2**	**0x0602**	**-**	**-**
The TTL value is 120/0 sec.					
Port description	**4**	**1**	**0x0801**	**-**	**-**
Port description 1.					
System name	**5**	**min len > 0, max len <= 255**	**-**	**-**	**-**
Refer to System and Model Names.					
System description	**6**	**min len > 0, max len <= 255**	**-**	**-**	**-**
Manufacturer's name - "Polycom"; Hardware version; Application version; BootROM version.					
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.					
Management Address	**8**	**12**	**0x100c**	**-**	**-**
Address String Len - 5, IPV4 subtype, IP address, Interface subtype - "Unknown", Interface number - "0", ODI string Len - "0".					

Supported TLVs

Name	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
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.

Name	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
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: After 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.

Name	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
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 Network policy TLV is received from the switch.), Tagged/Untagged, VlanId, L2 priority and DSCP.

Name	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
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 Network policy 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.

Name	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
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 Network policy TLV is received from the switch.), Tagged/Untagged, VlanId, L2 priority and DSCP.
Note: Video conferencing TLV is sent only from video-capable phones: VVX 500/501, 600/601, and 1500 business media phones.

Name	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
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.

Name	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
Extended power via MDI	127	7	0xfe07	0x0012bb	4

PowerType -PD device PowerSource-PSE&local Power Priority -Unknown PowerValue

Supported TLVs

Name	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
LLDP-MED inventory hardware revision	**127**	**min len > 0, max len <= 32**	-	**0x0012bb**	**5**
Hardware part number and revision.					
LLDP-MED inventory firmware revision	**127**	**min len > 0, max len <= 32**	-	**0x0012bb**	**6**
BootROM revision.					
LLDP-MED inventory software revision	**127**	**min len > 0, max len <= 32**	-	**0x0012bb**	**7**
Application (SIP) revision.					
LLDP-MED inventory serial number	**127**	**min len > 0, max len <= 32**	-	**0x0012bb**	**8**
MAC Address (ASCII string).					
LLDP-MED inventory manufacturer name	**127**	**11**	**0xfe0b**	**0x0012bb**	**9**
Polycom.					
LLDP-MED inventory model name	**127**	**min len > 0, max len <= 32**	-	**0x0012bb**	**10**
LLDP-MED inventory asset ID	**127**	**4**	**0xfe08**	**0x0012bb**	**11**
Empty (Zero length string).					
End of LLDP DU	**0**	**0**	**0x0000**	-	-

[1] For other subtypes, refer to IEEE 802.1AB, March 2005.

[2] For other application types, refer to TIA Standards 1057, April 2006.

[3] At this time, this TLV is not sent by the phone.

DHCPv6 or DHCPv4 Parameters

After establishing network connectivity, the phone needs to acquire several IPv6 or IPv4 network settings. These settings are typically obtained automatically from a Dynamic Host Configuration Protocol (DHCPv6 or DHCPv4) server.

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

You have the option to configure IPv4 or IPV6 network settings manually from the phone screen or using `device.set` capability. When making the DHCP request, the phone includes information in Option 60 that can assist the DHCP server in delivering the appropriate settings to the device.

For more information on DHCP options, see RFC2131 and RFC 2132

For more information on *Using DHCP Vendor Identifying Options with Polycom Phones, see Technical Bulletin 54041* at Polycom Engineering Advisories and Technical Notifications.

IPv4 Network Parameters

The following table lists the ways a phone can obtain IPv4 and related parameters in an IPv4 network:

Parameter	DHCPv4 Option	DHCPv4	DHCPv4 INFORM	Configuration File (application only)	Device Settings
IPv4 address	No	Yes	No	No	Yes
Subnet mask	1	Yes	No	No	Yes
IPv4 Gateway	3	Yes	No	No	Yes
Boot server address		Yes	Yes	No	Yes
SIP server address	151 You can change this value by changing the device setting.	Yes	No	Yes	Yes
SNTP server address	Look at option 42, then option 4.	Yes	No	Yes	Yes
SNTP GMT offset	2	Yes	No	Yes	Yes
Syslog		Yes	No	No	Yes
DNS server IP address	6	Yes	No	Yes	Yes
DNS INFORM server IP address	6	•	-	-	•

DNS domain	15	Yes	No	Yes	Yes
VLAN ID		**Warning**: Link Layer Discovery Protocol (LLDP) overrides Cisco Discovery Protocol (CDP). CDP overrides Local FLASH which overrides DHCP VLAN Discovery.			

IPv6 Network Parameters

The following table lists the ways a phone can obtain IPv6 and related parameters in an IPv6 network:.

IPv6 Network Parameters

Parameter	SLAAC[1]	DHCPv6 Option	DHCPv6	DHCPv6 INFORM	Configuration File (application only)	Device Settings
IPv6 Global Address	Yes	No	Yes	No	No	Yes
IPv6 ULA Address	Yes	No	Yes	No	No	Yes
IPv6 Gateway	Yes	No	No	No	No	Yes
Boot server IPv6 Address	No	Custom[2]	Yes	No	No	Yes
SIP server IPv6 Address	No	22/21	Yes	No	Yes	No
SNTP server IPv6 address	No	31	Yes	No	Yes	Yes
SNTP GMT offset	No	Custom[2]	Yes	No	Yes	Yes
Syslog IPv6 Address	No	Custom[2]	Yes	No	Yes	Yes
DNS server IPv6 address	No	23	Yes	No	Yes	Yes
IPv6 DNS domain	No	23	Yes	No	Yes	Yes
VLAN ID		**Warning**: Link Layer Discovery Protocol (LLDP) overrides Cisco Discovery Protocol (CDP). CDP overrides Local FLASH which overrides DHCP VLAN Discovery.				

[1] Stateless Address Auto Configuration.

[2] Polycom defined subcodes for these parameters as part of the DHCPv6 Vendor-Specific Information Option. Refer to section Example Configuration: Polycom Vendor-Specific Information Options in DHCPv6.

Example Configuration: Polycom Vendor-Specific Information Options in DHCPv6

You can obtain the CDP Compatibility value from a connected Ethernet switch if the switch supports CDP.

In DHCPv6, there are no standard options defined for Boot Server IPv6 address, Syslog Server IPv6 Address, SNTP GMT Offset, and VLAN List. Polycom has defined subcodes for this specific information as part of the DHCPv6 Vendor-Specific Information Option.

The following is an example configuration on a Linux DHCPv6 server for Polycom subcode definitions:

```
# Define PLCM options
option space plcm code width 2 length width 2 hash size 4;
option vsio.plcm code 13885 = encapsulate plcm;


option plcm.boot-server code 1 = string;
option plcm.time-offset code 2 = signed integer 32;
option plcm.syslog-server code 3 = string;
option plcm.vlan-list code 4 = string;


option plcm.boot-server "2620:0:1aa0:8071:d485:f47d:5de5:be04";
option plcm.time-offset 19850;
option plcm.syslog-server "2620:0:1aa0:8071:d485:f47d:5de5:be04";
option plcm.vlan-list "VLAN-A=513;";
```

You can configure parameter values for the **SNTP server address** and **SNTP GMT offset** to override the DHCP value. Refer to `tcpIpApp.sntp.address.overrideDHCP` for more information.

Provisioning Server Discovery Methods

After the phone has established network settings, it must discover a provisioning server to obtain software updates and configuration settings:

* **Static**   You can manually configure the server address from the phone's user interface or the Web Configuration Utility, or you can provision a server address using `device.prov.serverName` and corresponding device parameters.
* **DHCP**   A DHCP option is used to provide the address or URL between the provisioning server and the phone.
* **DHCP INFORM**   The phone makes an explicit request for a DHCP option (which can be answered by a server that is not the primary DHCP server). For more information, see RFC 3361and RFC 3925.
* **Quick Setup**   This feature takes users directly to a screen to enter the provisioning server address and information. This is simpler than navigating the menus to the relevant places to configure the provisioning parameters. For more information, see *Using Quick Setup with Polycom Phones: Technical Bulletin 45460 at* Polycom Engineering Advisories and Technical Notifications.
* **ZTP**   If a provisioning server address is not discovered automatically using DHCP and a static address has not been entered, the phone contacts the Polycom ZTP server and requests initial configuration files, including the address of the service provider or enterprise provisioning server.

Supported Provisioning Protocols

By default, Polycom phones are shipped with FTP enabled as the provisioning protocol. You can configure the phone using the following supported provisioning protocols:

- Trivial File Transfer Protocol (TFTP)
- File Transfer Protocol (FTP)
- Hyper Text Transfer Protocol - Secure (HTTPS)
- File Transfer Protocol - Secure (FTPS)

Virtual Local Area Network (VLAN) ID Assignment Using DHCP

In deployments where it is possible or desirable to assign a Virtual Local Area Network (VLAN) using LLDP, CDP, or Static methods, you can assign a VLAN ID to the phones by distributing the VLAN ID via DHCP.

When using this method to assign the phone's VLAN ID, the phone first boots on the Native VLAN/Data VLAN and then obtains its intended VLAN ID from the DHCP offer before it continues booting on the newly obtained VLAN.

> If a VLAN tag is assigned by CDP or LLDP, DHCP VLAN tags are ignored.

Valid DVD String DHCP Options

The 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 semi colon ";"
- All characters after the semi colon ";" are ignored
- There must be no white space before the semi colon ";"
- VLAN IDs may be decimal, hex, or octal

The following DVD strings result in the phone using VLAN 10:

- VLAN-A=10;
- VLAN-A=0x0a;
- VLAN-A=012;

Assign a VLAN ID Using DHCP

When the VLAN Discovery in the DHCP menu is set to Fixed, the phone examines DHCP options 128,144, 157, and 191 in that order for a valid Digital Versatile Disk DHCP VLAN Discovery string. If DHCP option 128 is configured for SIP outbound proxy, do not configure VLAN Discovery option 128 to Fixed.

When set to Custom, a value set in the VLAN ID Option is examined for a valid DVD string.

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**.

Parse Vendor ID Information

As a part of configuration, the Vendor ID information must be parsed with the Polycom phone. Polycom follows RFC 3925 which specifies use of a unique Internet Assigned Numbers Authority (IANA) private enterprise number. The private enterprise number assigned to Polycom is 13885 (0x0000363D) and is represented as an array of binary data.

To parse vendor ID information:

1 Check for the Polycom signature at the start of the option: `4 octet: 00 00 36 3d`

2 Obtain 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).

Example: DHCP Option 60 Packet Decode

The following example is a sample decode of a packet (DHCP Option 60) from a VVX 500/501:

`3c 7a`

➢ Option 60, length of Option data (part of the DHCP specification)

`00 00 36 3d`

➢ Polycom signature (always 4 octets)

`75`

➢ Length of Polycom data

`01 07 50 6f 6c 79 63 6f 6d`

➢ sub-option 1 (company), length, "Polycom"

`02 0b 56 56 58 2d 56 56 58 5f 34 31 30`

➢ sub-option 2 (part), length, "VVX-VVX_500/501"

`03 10 33 31 31 31 2d 34 36 31 36 32 2d 30 30 31 2c 37`

➢ sub-option 3 (part number), length, "3111-44500-001,7"

`04 1e 53 49 50 2f 35 2e 32 2e 30 2e 58 58 58 58 2f 30 36 2d 41 75 67 2d 31 34 20 32 30 3a 35 35`

➢ sub-option 4 (Application version), length, "SIP/5.2.0.XXXX/06-Aug-14 20:55"

`05 1d 55 50 2f 35 2e 34 2e 30 2e 58 58 58 58 2f 30 36 2d 41 75 67 2d 31 34 20 32 31 3a 30 34`

➢ sub-option 5 (Updater version), length, "UP/5.4.0.XXXX/06-Aug-14 21:04"

`06 0c 64 73 6c 66 6f 72 75 6d 2e 6f 72 67`

➢ sub-option 6 "dslforum.org"

Ethernet Network Connection Methods

You can connect the phone to a network using Ethernet with the following methods:

● Virtual Local Area Networks (VLANs)
● Type of Service (ToS) and Differentiated Services Code Point (DSCP)
● IEEE 802.1p/Q

Virtual Local Area Networks (VLANs)

Settings from higher priority methods override settings from lower priority methods. If the phone receives a Virtual Local Area Network (VLAN) setting from more than one of the following methods, the priority is as follows:

1 **LLDP**   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.

2 **CDP**   Cisco Discovery Protocol (CDP) is a proprietary Data Link Layer network protocol. CDP Compatible follows the same set of rules.

3 **DVD (VLAN via DHCP)**   Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used in IP networks. Note that use of DHCP for assigning VLANs is not standardized and is recommended only if the switch equipment does not support LLDP or CDP Compatible methods.

4 **Static**   The VLAN ID can be manually set by entering it through the phone's menu.

Vendor Specific DHCP Options

DHCP Option 60 controls how the phone identifies itself to a DHCP server for Polycom-specific options that must be returned.

If Option 60 format is set to RFC 3925, all returned values of Option 43 are ignored. If the format is set to an ASCII string, the Option 43 would have a hexadecimal string value encapsulating sub-options that override options received outside DHCP Option 43.

If you do not have control of your DHCP server or do not have the ability to set the DHCP options, enable the phone to automatically discover the provisioning server address. You can do this by connecting to a secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server value. For more information, see RFC 3361 and RFC 3925.

The following table lists supported DHCP Option 43 individual sub-options and combination sub-options:

DHCP Option 43 Configuration Options

Option	Results
Option 1- subnet mask	The phone parses the value from Option 43.
Option 2 - Time offset	The phone parses the value.
Option 3 - Router	The phone parses the value.
Option 4 - TIME/ITP server address (RFC 868)	The phone parses the value.
Option 6 - Domain Name Server	The phone parses the value.

DHCP Option 43 Configuration Options (continued)

Option	Results
Option 7 - Domain Log server	The phone parses the value.
Option 15 - Domain Name	The phone parses the value.
Option 42 - Network Time Protocol server/SNTP server address (RFC 1769)	The phone parses the value.
Option 66 - Provisioning Server Address	The phone parses the value.
Option 128 - 255	Available option range for configuring a custom boot server address when option 66 is not used.
Sub-options configured in Option 43	
Options 1, 2, 3, 4, 5, 6, 7, 15, 42, and 66	The phone parses the value.
Option 128 - 255	Available option range for configuring a custom boot server address when option 66 is not used.

Type of Service (ToS) and Differentiated Services Code Point (DSCP)

Type of Service (ToS) and the Differentiated Services Code Point (DSCP) allows specification of a datagrams desired priority and routing through low-delay, high-throughput, or highly-reliable networks.

The IP ToS header consists of four ToS bits and a 3-bit precedence field.

DSCP replaces the older ToS specification and uses a 6-bit DSCP in the 8-bit differentiated services field (DS field) in the IP header.

Related Topics:

IP Type-of-Service Parameters

IEEE 802.1p/Q

The phone tags all Ethernet packets it transmits with an 802.1Q VLAN header when the following occurs:

- A valid VLAN ID specified in the phone's network configuration.
- The phone is instructed to tag packets through Cisco Discovery Protocol (CDP) running on a connected Ethernet switch.
- A VLAN ID is obtained from DHCP or CDP.

Related Topics:

IEEE 802.1p/Q Parameters

Provisioning and Configuring Phones with Polycom UC Software

This section provides an overview of how to deploy Polycom phones using Polycom UC Software.

Polycom UC Components

This section is intended for administrators not familiar with Polycom UC Software. This section provides general information about the following UC Software components:

- The Updater
- The Polycom UC Software File Image
- XML Resource Files, Configuration Templates, and the XML Schema File

The Updater

The Updater is a small application that resides in the flash memory on the phone. Polycom phones come installed with the Updater.

When you start/boot/reboot the phone, the Updater automatically performs the following tasks:

1 The setup menu displays so you can set various network and provisioning options.

   The Updater requests IP settings and accesses the provisioning server (also called the boot server) to look for changes to the Updater software. If updates are found, they are downloaded and saved to flash memory, which overwrites itself after verifying the integrity of the download.

2 If new updates are downloaded, the Updater formats the file system, removes any application software and configuration files that were present.

3 The Updater downloads the master configuration file.

   The Updater and the application use this file to acquire a list of other files that the phone needs.

4 The Updater 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 from the one stored in device settings, or there is no file stored in flash memory, the application file is downloaded.

5 The Updater extracts the Polycom UC Software from flash memory.

6 The Updater installs the application into RAM, and then uploads an event log file from the boot cycle.

7 The Updater completes the cycle, and the Polycom UC Software begins running the phone's operations.

The Polycom UC Software File Image

Polycom UC Software is a binary file image and contains a digital signature that prevents tampering or the loading of rogue software images. Each release of software is a new image file. Both the Updater and Polycom UC Software run on all Polycom device models.

Polycom UC Software manages the protocol stack, the digital signal processor (DSP), the user interface, the network interaction, and implements the following functions and features on the phones:

- VoIP signaling for a wide range of voice and video telephony functions using SIP signaling for call setup and control.
- SIP and H.323 signaling for video telephony.
- Industry-standard security techniques for ensuring that all provisioning, signaling, 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.

XML Resource Files, Configuration Templates, and the XML Schema File

Polycom UC Software includes a number of resource files, template configuration files, and an XML schema file that provides examples of parameter types and permitted value types. The resource and configuration files contains parameters you can use to configure features and apply settings to phones. Configuration files are for use with the centralized provisioning method as explained in Centralized Provisioning.

Resource Files

The UC Software download contains optional resource configuration files you can apply to the phones. In addition, you can allow phone-specific override files containing user settings to be uploaded to the central server. Resource and override files include:

- Language dictionaries for the phone menu and Web Configuration Utility.
- Configuration override files that store settings made from the phone menu and Web Configuration Utility. To allow override files to be uploaded to the central server, refer to Setting Server Permissions for Override Files.
- Ringtones.
- Log files.
- A template contact directory `000000000000-directory~.xml`.
- A licensing directory.

Configuration Templates

The following table lists the template directories and files included in the UC Software download.

Note that `techsupport.cfg` is available from Polycom Customer Support for troubleshooting and debugging.

Configuration File Templates

Name	Description	Deployment Scenarios
Directories		
PartnerConfig	Contains configuration file specific to the following third-party servers: • Alcatel-Lucent • BroadSoft • GENBAND • Microsoft • Sylantro	For use with third-party servers.
Config		
applications.cfg	For applications, browser, microbrowser, XMP-API	Typical Hosted Service Provider Typical IP-PBX
device.cfg	Network Configuration parameters	Troubleshooting Administrative settings
features.cfg	Features including corporate directory, USB recording, presence, ACD	Typical Hosted Service Provider Typical IP-PBX
firewall-nat.cfg	Firewall parameters	
H323.cfg	H.323 video use	Typical Hosted Service Provider using VVX 500/501, 600/601, and 1500 for video calls
lync.cfg	Microsoft Skype for Business parameters	Typical Microsoft Skype for Business environment
polycomConfig.xsd*	See XML Resource Files, Configuration Templates, and the XML Schema File	
pstn.cfg		
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

Configuration File Templates

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`	Multi-site operations	Typical Hosted Service Provider Typical IP-PBX
`techsupport.cfg`	Available by special request from Polycom Customer Support.	Use for troubleshooting and debugging only
`video.cfg`	VVX 500/501, 600/601, and 1500 video	Typical Hosted Service Provider if using VVX 500/501, 600/601, and 1500 for video calls
`video-integration.cfg`		

Using Correct Parameter XML Schema, Value Ranges, and Special Characters

The configuration parameters available in the UC Software templates use a variety of value types. UC Software includes an XML schema file—`polycomConfig.xsd`—that provides information about parameter type, permitted values, default values, and valid enumerated type values. View this template file with an XML editor.

Polycom configuration parameters support the following value types:

- Boolean
- Enumerated
- Integer
- String

The following rules apply to UC Software parameter values:

- Boolean values are not case sensitive.
- UC Software interprets `Null` as empty.
- The values `0, false,` and `off` are supported and interchangeable.
- The values `1, true,` and `on` are supported and interchangeable. This administrator guide documents only `0` and `1`.

The following rules apply when you set a parameter with a numeric value outside of its valid range:

- If the value is greater than the allowable range, the maximum allowable value is used.
- If the value is less than the allowable range, the minimum allowable value is used.

- If you insert invalid parameter values into the configuration file, the value is ignored and the default value is used. Examples of invalid parameter values include enumerated values that do not match values defined in the UC Software, numeric parameters set to non-numeric values, string parameters whose value is too long or short, and null strings in numeric fields. Invalid values are logged in the phone's log files.

To enter special characters in a configuration file, enter the appropriate sequence using an XML editor:

- & as `&`
- " as `"`
- ' as `'`
- < as `<`
- > as `>`
- random numbers as `&0x12;`

Set Up a Network for Polycom UC Software

A typical large-scale VoIP deployment requires administrators to complete each of the following tasks. Note that deployment scenarios vary and Polycom cannot recommend a specific environment.

To set up a centralized provisioning environment:

1 Create user accounts on the SIP call server.

2 (Optional) Set up a provisioning server. In some cases a provisioning server is built into the SIP call server and if not, administrators must set up their own provisioning server. For details, refer to Setting Up a Provisioning Server.

Polycom strongly recommends setting up a provisioning server for large-scale VoIP device deployments. A provisioning server maximizes the flexibility you have when installing, configuring, upgrading, and maintaining the phones, and enables you to store configuration, log, directory, and override files on the server.

3 (Optional) Configure security options on your network.

   ➢ 802.1X

   ➢ Virtual local area networks (VLANs)

   ➢ File transfers using HTTPS

   ➢ SIP signaling over Transport Layer Security (TLS)

   ➢ Set permissions for configuration and override files. Refer to Setting Server Permissions for Override Files.

4 Set up Dynamic Host Configuration Protocol (DHCP).

5 Set up Domain Name System (DNS). Polycom supports the following DNS records types:

   ➢ DNS A record

   ➢ Service (SRV) record for redundancy

   ➢ Name Authority Pointer (NAPTR)

6 Connect the phones to the network.

7 Deploy phones from the provisioning server as shown in Deploy Devices from a Provisioning Server.

Polycom Provisioning Methods

Polycom provides several methods to provision phones. The method you use depends on the number of phones and how you want to apply features and settings. Methods available can vary by device model.

You can use multiple methods concurrently to provision and configure features, but there is a priority among the methods when you use multiple methods concurrently—settings you make using a higher priority configuration method override settings made using a lower priority method. When using multiple configuration methods, a setting you make using a lower-priority method does not apply to or override a duplicate setting made using a higher-priority method. The provisioning and configuration methods in order of priority are as follows:

- Quick Setup
- Phone menu
- Web Configuration Utility
- Centralized provisioning

Note that features and settings vary by method, by device, and by UC Software release. For this reason, Polycom recommends limiting the methods you use concurrently to avoid confusion about where a phone is receiving settings.

Quick Setup of Polycom Phones

Quick Setup enables administrators or users to access the provisioning server and configure the phone for provisioning. For more detail details on how to configure quick setup, see Technical Bulletin 45460: Using Quick Setup with Polycom Phones.

After the initial configuration is complete, you can continue to show or hide the QSetup option.

Related Topics

Quick Setup Soft Key Parameters

Provision Using the Phone Menu

You can use the phone menu system to provision a single phone and to configure features on one phone. If you are provisioning more than 10 to 20 phones, Polycom recommends using centralized provisioning as your primary provisioning method.

You can use the menu system as the sole configuration method or in conjunction with other methods. Menu systems and interface settings vary by device and by UC Software release. Settings you make from the phone menu override settings you make using the Web Configuration Utility and central provisioning server. However, the phone menu does not contain all of the settings available with centralized provisioning.

The phone menu system makes settings available to users and administrators; settings available to administrators only can be accessed on the Advanced menu and require an administrator password. For

information on setting passwords, see Administrator and User Passwords. Some settings require a device restart or reboot.

Provision Using the Web Configuration Utility

The Web Configuration Utility is a web-based interface that is useful for remote provisioning and configuration. This utility allows you to update the software and configure the phone's current settings. You can either import the settings in a configuration file to the phone or export a configuration file containing phone's current settings to your computer to make changes.

> Note: The Web Configuration Utility does not contain all of the settings available with centralized provisioning. Polycom recommends using centralized provisioning as your primary provisioning method when provisioning more than 10 to 20 phones.

There is a priority order when using multiple methods concurrently to provision and configure features. Settings you make from the Web Configuration Utility override settings you make on the central provisioning server and can be overridden by settings you configure from the phone menu. If you want to remove settings applied on a particular page from the Web Configuration Utility, click the Reset to Default button in the Web Configuration Utility.

For more detailed help using the Web Configuration Utility, see the *Polycom Web Configuration Utility User Guide* on Polycom UC Software Support Center.

For more information on priority order to follow when using multiple methods, Polycom Provisioning Methods.

Import Configuration Files to the Phone

You can import the changes made to the current phone's settings and configuration files by you from your computer to another phone using the Web Configuration Utility.

To import configuration files to the phone:

1   Find your phone's IP address on your phone's keypad or touchscreen interface.

2   Enter the phone's IP address into the address bar of a web browser from your computer.

3   Choose your login option as **Admin** on the Web Configuration Utility login screen and enter the corresponding password (default `456`).

4   Go to **Utilities > Import Configuration > Choose File**.

5   Choose the configuration files from your computer to upload.

6   Click **Import**.

   The Web Configuration Utility imports the selected file to your phone.

Export Configuration Files from the Phone

You can export the phone's configuration file to your computer and make changes to the phone's current settings. You can apply these settings to another phone by importing the configuration files using the Web Configuration Utility.

To export the configuration files to your computer:

1 Find your phone's IP address on your phone's keypad or touchscreen interface.

2 Enter the phone's IP address into the address bar of a web browser from your computer.

3 Choose your login option as **Admin** on the Web Configuration Utility login screen and enter the corresponding password (default `456`).

4 Navigate to **Utilities > Import & Export Configuration**.

5 Choose the files to export from the drop-down list of **Export Configuration file** under **Export Configuration** pane.

6 Click **Export**.

The Web Configuration Utility exports the selected file to your computer.

For information on using the phone menu to upload configuration files containing the phone's local settings to the provisioning server, refer to Upload a Phone's Configuration

Centralized Provisioning

This section provides important points about using Polycom UC Software in large-scale deployments.

● Centralized provisioning enables you to provision phones from a provisioning server that you set up, and maintain a set of configuration files for all phones on a central provisioning server. The centralized provisioning method is recommended for phone deployment of 20 or more phones. After phones are provisioned with UC Software, you can configure features and settings for all phones with the UC Software configuration files that you store and modify on your provisioning server. For information about configuring features and settings, refer to Master Configuration File

● Most configuration parameters are located in only one template file; however, some are included in two or more files. The template configuration files are flexible: you can rearrange the parameters within the template, move parameters to new files, or create your own configuration files from parameters you want. This flexibility is especially useful when you want to apply specific settings to a group of phones. You can create and name as many configuration files as you want and your configuration files can contain any combination of parameters. For a list of all template files included in the UC Software, refer to XML Resource Files, Configuration Templates, and the XML Schema File.

● You must write the name of configuration files to the CONFIG_FILES field of the master configuration file in the order you want the settings applied. The files you enter to the CONFIG_FILES field are read from left to right. Duplicate settings are applied from the configuration file in the order you list them. For details about the master configuration file fields, refer to Master Configuration File Fields.

● Polycom phones boot up without the use of configuration files, and you can specify a SIP server address and a registration address (the equivalent of a phone number) in a configuration file before or after the phone boots up. If a phone cannot locate a provisioning server upon boot up, and has not been configured with settings from any other source, the phone operates with internally stored default values. If the phone has been previously configured with settings from a provisioning server and cannot locate the server when booting up, the phone operates with those previous settings.

● If settings you make from the central server are not working, check first for priority settings applied from the phone menu system or Web Configuration Utility, and second for duplicate settings in your configuration files. For information about configuration setting priority, refer to Polycom Provisioning Methods.

Setting Up a Provisioning Server

After you set up a VoIP network and create accounts on the SIP call server, shown in Set Up a Network for Polycom UC Software, you need to install provisioning tools on your computer and set up a centralized provisioning server to provision the phones and configure settings. Polycom phones support the FTP, TFTP, HTTP, and HTTPS protocols and use FTP by default. The example shown in this section uses FTP and a personal computer (PC) as the provisioning server.

Note: Polycom recommends that you use RFC-compliant servers.

Install Provisioning Tools

Before you begin provisioning devices with UC Software, install tools on your computer and gather some information.

To install and set up provisioning tools:

1 If using Power over Ethernet (PoE) with the phone, obtain a PoE switch and network cable.

2 Install an XML editor, such as XML Notepad 2007, on your computer.

3 Install an FTP server application on your computer. FileZilla and *wftpd* are free FTP applications for windows and *vsftpd* is typically available with all standard Linux distributions.

4 Take note of the following:

   ➢ **SIP Server address**. This is the hostname or IP address of the call server that handles VoIP services on your network.

   ➢ **SIP account information**. This may include SIP credentials such as a user name and password, and the phone's registration address. Although a user name and password are not required to get the phone working, Polycom strongly recommends using them for security reasons.

   ➢ **MAC address**. Each phone has a unique 12-digit serial number just above the phone's bar code on a label on the back of the phone. Collect the MAC address for each phone in your deployment.

   ➢ **Your computer's IP address**. To use your computer as the provisioning boot server, you need your computer's IP address. Jot this number down as you need it at the end of the provisioning process.

Set Up a Provisioning Server

After you install provisioning tools, set up the provisioning server.

To set up the provisioning server:

1 Provide power to the phone using a PoE switch, if available, or, if no PoE switch is available, using an external power adapter and a network cable to connect the phone to your network.

2 Install and set up an FTP application. FileZilla and *wftpd* are free FTP applications for Windows and *vsftpd* is typically available with all standard Linux distributions.

3 Create a root FTP directory on the provisioning computer with full read and write access to all directories and files. You will be placing configuration files in this root directory.

4 In your FTP server application, create a user account for the phone to use and take note of the user name and password as you will need these later in the provisioning process. Launch the FTP application and keep it running at all times so that the phones can communicate with the UC Software.

5 Download the UC software version(s) to your root directory from the Polycom UC Software Support Center. To match a phone model with a correct Polycom UC Software release, refer to the Polycom UC Software Release Matrix for VVX Phones and SoundStructure.

You can choose the combined UC Software package or the split UC Software package, both in ZIP file format.

➢ The combined version contains all files for all phone models.

➢ The split software package is smaller, downloads more quickly, and contains **sip.ld** files for each phone model, enabling you to choose provisioning software for your phone model(s) and maintain software versions for each model in the same root directory.

6 To apply security settings to your configuration files, refer to the section Configuration File Encryption.

Configuring Multiple Servers

You can configure multiple (redundant) provisioning servers—one logical server with multiple addresses—by mapping the provisioning server DNS name to multiple IP addresses. If you set up multiple provisioning servers, you must be able to reach all of the provisioning servers with the same protocol and the contents on each provisioning server must be identical. The default number of provisioning servers is one and the maximum number is eight. For more information on the protocol used, see Supported Provisioning Protocols.

You can configure the number of times each server is tried for a file transfer and how long to wait between each attempt. You can also configure the maximum number of servers to try.

Setting Server Permissions for Override Files

By default, phones you provisioning from a central server attempt to upload a number of phone-specific files to the server. If you want to allow the phone to upload these files to the server, you must have read, write, and delete permissions on the server account and provide enable, read, and write access to those files. To organize these files, Polycom recommends creating a separate directory on the server for each file type you want to allow uploads for:

● Log files.

● Configuration override files from the local phone interface and Web Configuration Utility. For more information about the priority of override files, refer to Polycom Provisioning Methods. For information about override files, refer to Override Files.

● A contact directory.

● A license directory.

Each directory can have different access permissions, for example, you can allow log, contacts, and overrides to have full read and write access, and a license directory to have read-only access. However, where the security policy permits, Polycom recommends allowing these file uploads to the provisioning

server to allow greater manageability and can help Polycom provide customer support when diagnosing issues with the phone. All other files that the phone needs to read, such as the application executable and standard configuration files, should be read-only. Ensure that the file permissions you create provide the minimum required access and that the account has no other rights on the server.

Note that as of Polycom UC Software 4.0.0, you can create user-specific configuration files that enable phone users to use their features and settings from any phone in an organization. For instructions, refer to the section Set User Profiles.

Override Files

When settings are modified from the phone user interface or Web Configuration Utility (user or administrator), the phone attempts to upload override files with settings to the central server. When using a central provisioning server as part of your VoIP environment, you have the option to store the override file to the phone, or you can permit the phone to upload the override file to the provisioning server by giving the phone write access to the provisioning server. Allowing the phone access to the provisioning server enables user settings to survive restarts, reboots, and software upgrades administrators apply to all phones from the provisioning server.

You can also use the override files to save user custom preferences and to apply specific configurations to a device or device group. If you permit the phone to upload to the provisioning server, the override file is by default named either `<MAC Address>-phone.cfg` or `<MAC Address>-web.cfg` depending on the whether the change was made from the phone or Web Configuration Utility respectively.

If you reformat the phone's file system, the override file is deleted. If you need to clear phone settings and features applied by override files, refer to Update Configuration from the Phone Menu.

Deploy Devices from a Provisioning Server

After setting up your provisioning server(s), you can deploy devices. This section shows you how to deploy your Polycom devices from the provisioning server using Polycom UC Software.

> Note: If SNTP settings are not available through DHCP, you may need to edit the SNTP GMT offset or SNTP server address for the correct local conditions. Changing the default daylight savings parameters might be necessary outside of North America. If the local security policy dictates, you might need to disable the local Web (HTTP) server or change its signaling port.

To deploy phones with a provisioning server:

1 Using the list of MAC addresses of each phone you are deploying, create a per-phone `phone<MACaddress>.cfg` file.

Do not use the following file names as your per-phone file name: `<MACaddress>-phone.cfg`, `<MACaddress>-web.cfg`, `<MACaddress>-app.log`, `<MACaddress>-boot.log`, or `<MACaddress>-license.cfg`. These file names are used by the phone to store overrides and logging information.

2 Add the SIP server registration information and user account information to parameters in the per-phone file, for example `reg.1.address, reg.1.auth.userId, reg.1.auth.password, reg.1.label, reg.1.type`.

3 Create a per-site `site<location>.cfg` file.

For example, add the SIP server or feature parameters such as `voIpProt.server.1.address` and `feature.corporateDirectory.enabled`.

4 Create a master configuration file by performing the following steps:

a Enter the name of each per-phone and per-site configuration file created in steps 2 and 3 in the CONFIG_FILES attribute of the master configuration file (`000000000000.cfg`). For help using the master configuration file, refer to Master Configuration File Fields and Master Configuration File.

For example, add a reference to `phone<MACaddress>.cfg` and `sipVVX500.cfg`.

b (Optional) Edit the LOG_FILE_DIRECTORY attribute of master configuration file to point to the log file directory.

c (Optional) Edit the CONTACT_DIRECTORY attribute of master configuration file to point to the organization's contact directory.

(Optional) Edit the USER_PROFILES_DIRECTORY attribute of master configuration file if you intend to enable the user login feature. For more information, see the section User Profiles.

d (Optional) Edit the CALL_LISTS_DIRECTORY attribute of master configuration file to point to the user call lists.

5 Perform the following steps to configure the phone to point to the IP address of the provisioning server and set up each user:

a On the phone's **Home** screen or idle display, select **Settings > Advanced > Admin Settings > Network Configuration > Provisioning Server**. When prompted for the administrative password, enter **456**.

The Provisioning Server entry is highlighted.

b Press **Select**.

c Scroll down to **Server Type** and ensure that it is set to **FTP**.

d Scroll down to **Server Address** and enter the IP address of your provisioning server.

e Press **Edit** to edit the value and **OK** to save your changes.

f Scroll down to **Server User** and **Server Password** and enter the user name and password of the account you created on your provisioning server, for example, `bill1234` and `1234`, respectively.

g Press **Back** twice.

h Scroll down to **Save & Reboot**, and then press **Select**.

The phone reboots and the UC Software modifies the `APPLICATION APP_FILE_PATH` attribute of the master configuration file so that it references the appropriate sip.ld files.

After this step, the UC Software reads the unmodified `APPLICATION APP_FILE_PATH` attribute. Then, the phone sends a DHCP Discover packet to the DHCP server. You can locate this in the Bootstrap Protocol/option 'Vendor Class Identifier' section of the packet which includes the phone's part number and the BootROM version. For more information, see the section Parse Vendor ID Information.

6 Ensure that the configuration process completed correctly:

a On the phone, press **Settings** (**Menu** if using a VVX 1500) **> Status > Platform > Application > Main** to see the UC Software version and **Status > Platform > Configuration** to see the configuration files downloaded to the phone.

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

The phone uploads two logs files to the LOG_DIRECTORY directory: ***<MACaddress>*-app.log** and ***<MACaddress>*-boot.log**.

You can now instruct your users to begin making calls.

> Tip: To view phone provisioning information, use the multiple key combination shortcut by simultaneously pressing 1-4-7 to display:
> - Phone IP address
> - Phone MAC address
> - VLAN ID
> - Boot server type (FTP, TFTP, HTTP, HTTPS)

Master Configuration File Fields

The centralized provisioning method requires you to use a master configuration file, named `00000000000.cfg` in the UC Software download. Familiarize yourself with the master configuration file fields to use centralized provisioning effectively.

Default fields in the master configuration file
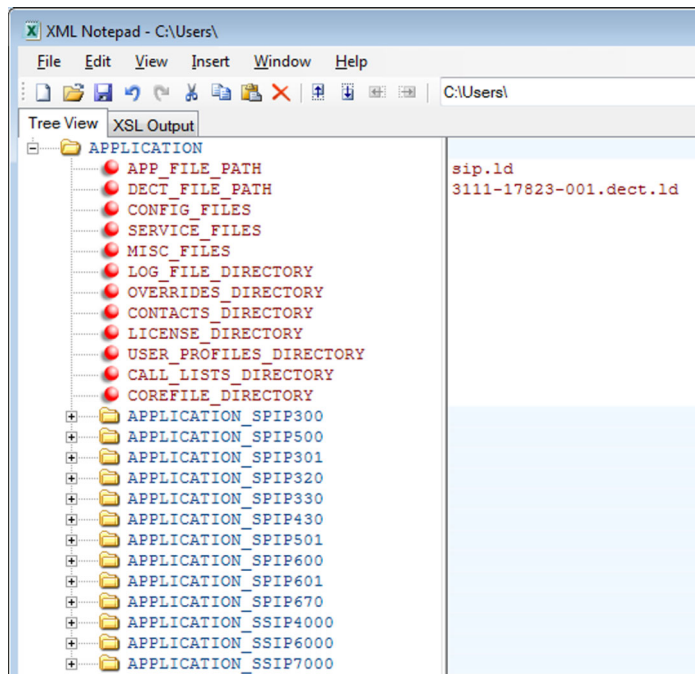
The following describes the XML field attributes in the master configuration file and the APPLICATION directories.

- **APP_FILE_PATH**   The path name of the UC Software application executable. The default value is `sip.ld`. Note that the phone automatically searches for the sip.ld and `<part number>.sip.ld`. This field can have a maximum length of 255 characters. If you want the phone to search for a sip.ld file

in a location other than the default or use a different file name, or both, modify the default. For example, you can specify a URL with its own protocol, user name, and password: `http://usr:pwd@server/dir/sip.ld`.

● **DECT_FILE_PATH**   The path for the application executable for the Polycom® VVX® D60 Wireless Handset. The default value is 3111-17823-001.dect.ld. When the software for a VVX business media phone with a paired VVX D60 Base Station is updated, the phone also searches for the dect.ld for any updates to the base station software.

If you want the phone to search for the 3111-17823-001.dect.ld in a location other than the default or use a different file name, or both, modify the default. For example, you can specify a URL with its own protocol, user name, and password: http://usr:pwd@server/dir/3111-17823-001.dect.ld.

● **CONFIG_FILES**   Enter the names of your configuration files here as a comma-separated list. Each file name has a maximum length of 255 characters and the entire list of file names has a maximum length of 2047 characters, including commas and white space. If you want to use a configuration file in a different location or use a different file name, or both, you can specify a URL with its own protocol, user name and password, for example: `ftp://usr:pwd@server/dir/phone2034.cfg`. The files names you enter to the CONFIG_FILES field write are read from left to right. Duplicate settings are applied from the configuration file in the order you list them

● **MISC_FILES**   A comma-separated list of files. Use this to list volatile files that you want phones to download, for example, background images and ringtone .wav files. The phone downloads files you list here when booted, which can decrease access time.

● **LOG_FILE_DIRECTORY**   An alternative directory for log files. You can also specify a URL. This field is blank by default.

● **CONTACTS_DIRECTORY**   An alternative directory for user directory files. You can also specify a URL. This field is blank by default.

● **OVERRIDES_DIRECTORY**   An alternative directory for configuration overrides files. You can also specify a URL. This field is blank by default.

● **LICENSE_DIRECTORY**   An alternative directory for license files. You can also specify a URL. This field is blank by default.

● **USER_PROFILES_DIRECTORY**   An alternative directory for the `<user>.cfg` files.

● **CALL_LISTS_DIRECTORY**   An alternative directory for user call lists. You can also specify a URL. This field is blank by default.

● **COREFILE_DIRECTORY**   An alternative directory for Polycom device core files to use to debug problems. This field is blank by default.

The directories labeled APPLICATION_SPIPXXX indicate phone models that are not compatible with the latest UC Software version. If you are using any of the phone models listed in these directories, open the directory for the phone model you are deploying, and use the available fields to provision and configure your phones.

Alternatively, you can specify the location of a master configuration file you want the phones to use, for example, `http://usr:pwd@server/dir/example1.cfg`. The file name must be at least five characters long and end with `.cfg`. If the phone cannot find and download a location you specify, the phone searches for and uses a per-phone master configuration file and then the default master configuration file.

Master Configuration File

The master configuration file maximizes the flexibility you have to customize features and settings for your devices in large deployments. You can use the master configuration file to configure features and apply settings for:

- All phones
- Different groups of phones
- Specific phone models
- A single phone

You can use the default name `000000000000.cfg` or configure features and settings for phone groups by renaming the master configuration file. You can use any of these methods concurrently within the same deployment. There are two ways rename the master configuration file:

- Define a `MACaddress.cfg` file
- Use a variable substitution

The method you use depends on your deployment scenario and understanding all naming schemes can help you to deploy and manage your phones efficiently.

Find a Phone's MAC Address

Each phone has a unique a-f hexadecimal digit called a MAC address, also known as the serial number (SN). You can use the MAC address to create variables in the name of the master configuration file, or to specify phone-specific configuration files. There are three ways to find a phone's MAC address.

To find a phone's MAC Address:

» Find the MAC Address by doing one of the following:

➢ Look on the label on the back of the phone

➢ On the phone's menu system, go to **Settings** (**Menu** if using a VVX 1500) **> Status > Platform > Phone > S/N:**

➢ Use a multikey shortcut by simultaneously pressing **1-4-7**

Define a Per-Phone `MACaddress.cfg` File

You can create a `MACaddress.cfg` file for each phone by making a copy and renaming the master configuration file template. Note that you can use only lower-case letters, for example, `0004f200106c.cfg.`

The advantage of using this method is a high degree of control over each phone. If you want to modify or add settings on a per-phone basis, add a new configuration file to the CFG_FILES field of each `user-<MACaddress>.cfg` phone file or make changes to an existing configuration file.

For large deployments, this naming scheme can require some file management as you need to create and edit at least two unique files for each phone in your deployment, the `MACaddress.cfg` file and one or more configuration files unique to each phone.

Note: Do not use the following names as extensions for per-phone files: `<MACaddress>-phone.cfg`, `<MACaddress>-Web.cfg`, `<MACaddress>-app.log`, `<MACaddress>-boot.log`, or `<MACaddress>-license.cfg`. These filenames are used by the phone to store override files and logging information.

To create a per-phone MAC address configuration files:

1 Create a copy of the master configuration file template for each phone.

2 Create a `MACaddress.cfg` file for each phone, replacing `000000000000` with the unique MAC address of each phone you are configuring, for example `0004f2123456.cfg`.

   You can find the MAC address of your phone on a label on back of the phone.

3 Create a file for each phone containing information unique to each phone, for example, registration information. You can use the template files in the UC Software download, or you can create your own configuration file using parameters from the UC Software template files. Give your files a name that indicates the file contents or purpose. For example, you might use parameters from the `reg-basic.cfg` template file to create a registration file named `reg-basic_john_doe.cfg`.

4 Enter the name of the file you created in step two in the CONFIG_FILES field of the `MACaddress.cfg` file you created in step one for each phone.

5 Save the master configuration file.

Configure Phones Using a Variable Substitution

This method enables you to configure all phones using a single master configuration file instead of a `MACaddress.cfg` file for each phone. This method follows from the phone's programmed behavior: the phone looks first for a file containing its own MAC address and if it cannot find that, uses the default `000000000000.cfg` master configuration file.

This method is useful if you need to maintain or modify settings common to all of the phones in your deployment. To apply a common configuration to all phones, you need only create one new configuration file and add it to the CONFIG_FILES field of the `000000000000.cfg` master file. If you want to add a new phone to your deployment, you need only create one new file.

For more information on creating phone groups and using variable substitutions, see the section Using a Variable in the Master Configuration File.

To configure using a variable substitution:

1 Create a file for each phone containing information unique to each phone, for example, registration information. The name of this file must contain the phone's unique MAC address, for example, `reg-basic_0004f2000001.cfg`. Each of these phone-specific configuration files must be named identically, varying only in the MAC address of each phone.

2 Enter the name of any one of your phone-specific files to the CONFIG_FILES field of the master configuration file.

3 Modify the file name in the CONFIG_FILES field by replacing the phone-specific MAC address with the variable [PHONE_MAC_ADDRESS] and include the square brackets. You must enter the variable in the same place you entered the phone's MAC address in the phone-specific file.

   For example, modify `reg-basic_0004f2000001.cfg` to `reg-basic_[PHONE_MAC_ADDRESS].cfg`.
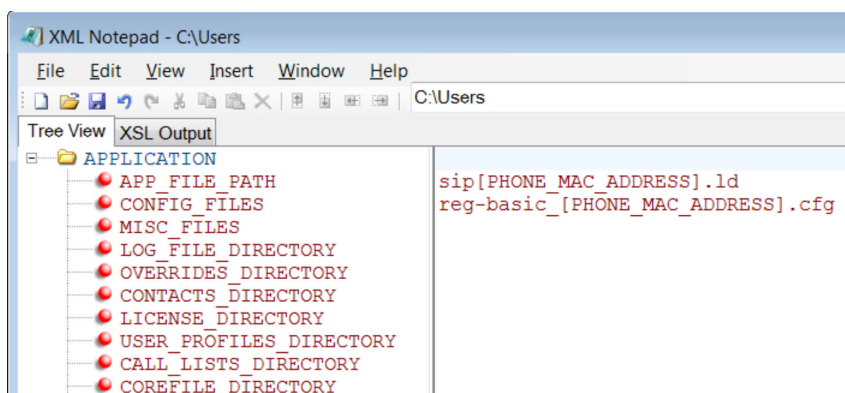
4 Save the master configuration file.

Configuring Phone Groups with the Master Configuration File

If you want to apply features or settings to a specific group of phones, you can create phone groups by:

- Using a variable to define per-phone configuration files.
- Appending a phone model name or part number to a configuration file.

Using a Variable in the Master Configuration File

You can use any of the following variable strings to create custom device groups:

- [PHONE_MODEL]
- [PHONE_PART_NUMBER]
- [PHONE_MAC_ADDRESS]

To get the model number or part number of a device, refer to System and Model Names.

To find the MAC address of a device, refer to Find a Phone's MAC Address.

Apply Features and Settings to a Group of Phones

You can apply features and settings to a phone group by phone model name or part number. Note that if you create groups using the part number and model name for the same type of phone, the part number has priority over the model name, which has precedence over the original firmware version. The following is an example configuration for a group of VVX 500 business media phones.

To apply settings to a group of phones:

1 Create a configuration file with the settings you want to apply. This example uses the VVX 500 business media phones.

2 Rename the file using the part number or model name as a variable, for example:

➢ `3111-44500-001.cfg`

> ➤ `VVX500.cfg`

3 Add the file name to the CONFIG_FILES field of the master configuration file.

Polycom Phone Model Names and Part Numbers

The following table lists the product names, model names, and part numbers for Polycom devices.

Product Name, Model Name, and Part Number

Product Name	Model Name	Part Number
SoundStructure VoIP Interface	SSTRVOIP	3111-33215-001
VVX D60 Wireless Handset	VVXD60	3111-17823-001
VVX 101	VVX101	3111-40250-001
VVX 201	VVX201	3111-40450-001
VVX 300	VVX300	3111-46135-002
VVX 301	VVX301	3111-48300-001
VVX 310	VVX310	3111-46161-001
VVX 311	VVX311	3111-48350-001
VVX 400	VVX400	3111-46157-002
VVX 401	VVX401	3111-48400-001
VVX 410	VVX410	3111-46162-001
VVX 411	VVX411	3111-48450-001
VVX 500	VVX500	3111-44500-001
VVX 501	VVX501	3111-48500-001
VVX 600	VVX600	3111-44600-001
VVX 601	VVX601	3111-48600-001
VVX 1500	VVX1500	2345-17960-001

Audio Features

After you set up your Polycom phones on the network, users can send and receive calls using the default configuration. However, you might consider configuring modifications that optimize the audio quality of your network.

This section describes the audio sound quality features and options you can configure for your Polycom phones. Use these features and options to optimize the conditions of your organization's phone network system.

Automatic Gain Control

Automatic Gain Control (AGC) is applicable to conference phone models and is used to boost the transmit gain of the local talker in certain circumstances. This increases the effective user-phone radius and helps you to hear all participants equally. This feature is enabled by default.

Background Noise Suppression

Background noise suppression is designed primarily for handsfree operation and reduces background noise, such as from fans, projectors, or air conditioners, to enhance communication. This feature is enabled by default.

Comfort Noise

Comfort Noise ensures a consistent background noise level to provide a natural call experience and is enabled by default.

Comfort noise fill is unrelated to Comfort Noise packets generated if Voice Activity Detection is enabled.

Voice Activity Detection

Voice activity detection (VAD) conserves network bandwidth by detecting periods of silence in the transmit data path so the phone doesn't have to transmit unnecessary data packets for outgoing audio.

For compression algorithms without an inherent VAD function, such as G.711, the phone uses the codec-independent comfort noise transmission processing specified in RFC 3389. The RFC 3389 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.

Related Topics

Voice Activity Detection Parameters

Comfort Noise Payload Packets

When enabled, the Comfort Noise payload type is negotiated in Session Description Protocol (SDP) with the default of 13 for 8 KHz codecs, and a configurable value between 96 and 127 for 16 KHz codecs.

Related Topics

Comfort Noise Payload Packets Parameters

Synthesized Call Progress Tones

Polycom phones play call signals and alerts, called call progress tones, that include busy signals, ringback sounds, and call waiting tones. The built-in call progress tones match standard North American tones. If you want to customize the phone's call progress tones to match the standard tones in your region, contact Polycom Support.

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 or 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. This feature is enabled by default.

Dual-Tone Multi-Frequency Tones

The phone generates dual-tone multi-frequency (DTMF) tones, also called touch tones, in response to user dialing on the dialpad. 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 endpoint. The phone generates RFC 2833 (DTMF only) events but does not regenerate—or otherwise use—DTMF events received from the remote end of the call.

Related Topics

DTMF Tone Parameters

Acoustic Echo Cancellation

Polycom phones use advanced acoustic echo cancellation (AEC) for handsfree operation using the speakerphone. The phones use both linear and non-linear techniques to aggressively reduce echo while permitting natural, full-duplex communication patterns.

You can configure the Acoustic Echo Cancellation (AEC) feature to remove the echo of the local loudspeaker from the local microphone without removing the near-end speech.
The AEC feature includes the following:

- Talk State Detector: Determines whether the near-end user, far-end user, or both are speaking.
- Linear Adaptive Filter: Adaptively estimates the loudspeaker-to-microphone echo signal and subtracts that estimate from the microphone signal.
- Non-linear Processing: Suppresses any echo remaining after the Linear Adaptive Filter.

The phones also support headset echo cancellation.

See the table Supported Audio Codecs for a list of audio codecs available for each phone and their priority.

Related Topics

Acoustic Echo Cancellation Parameters

Supported Audio Codecs

Context Sensitive Volume Control

In some countries, regulations state that a phone's receiver volume must be reset to a nominal level for each new call. Transmit levels are fixed according to the TIA/EIA-810-A standard. The next table lists parameters that configure the receiver volume to reset and persist across calls each time a user makes changes to the default volume level. You can adjust the volume of phone sound effects—such as the ringer and the volume of receiving call audio—separately for the speakerphone, handset, and headset.

Related Topics

Context Sensitive Volume Control Parameters

Polycom Acoustic Fence™

Available on all VVX business media phones, the Polycom Acoustic Fence feature enhances background noise suppression when users are using the phone handset or a headset connected to the headset port. This feature is particularly useful in call center environments where background noise can impact far-end audio quality.

Only headsets connected using an RJ-9 port at the rear of the phone (the headset port) can make use of the Acoustic Fence.

The Acoustic Fence is not available for USB or Bluetooth headset use.

Related Topics

Acoustic Fence Parameters

Bluetooth Headset Support

You can enable users to connect Bluetooth v2.1-compatible headsets with VVX 600/601 business media phones.

Note that using a Bluetooth headset can affect voice quality on the phone due to inherent limitations with Bluetooth technology. Users may not experience the highest voice quality when using a Bluetooth headset while the 2.4 GHz band is enabled or while they are in an environment with many other Bluetooth devices.

Related Topics

Bluetooth Headset Support Parameters

Location of Audio Alerts

You can choose where all audio alerts, including incoming call alerts, are played on Polycom phones. You can specify the audio to play from the handsfree speakerphone (default), the handset, the headset, or the active location. If you choose the active location, audio alerts play out through the handset or headset if they are in use. Otherwise, alerts play through the speakerphone.

Related Topics

Audio Alert Parameters

Ringtones

Ringtones are used to define a simple ring class that are applied based on credentials that are usually carried within the network protocol. The ring class includes parameters such as call-waiting and ringer index, if appropriate.

The ring class can use one of the following types of rings:

- **Ring**   Plays a specified ring pattern or call waiting indication.
- **Visual**   Provides a visual indication (no audio) of an incoming call, no ringer needs to be specified.
- **Answer**   Provides auto-answer on an incoming call.
- **Ring-answer**   Provides auto-answer on an incoming call after a certain number of rings.

> Note that auto-answer for an incoming call works only when there is no other call in progress on the phone, including no other calls in progress on shared or monitored lines. However, if a phone initiates a call on a shared or monitored line, auto-answer works.

Supported Ring Classes

The phone supports the following ring classes:

- default
- **v**isual
- answerMute
- autoAnswer
- ringAnswerMute
- ringAutoAnswer
- internal
- external
- emergency
- precedence
- splash
- custom<*y*> where y is 1 to 17.

Related Topics

Ringtone Parameters

Distinctive Ringtones

This feature enables you to apply a distinctive ringtone to a registered line, a specific contact, or type of call, including internal or external calls.

You can set up distinctive ringing using more than one of the following methods, however, the phone uses the highest priority method:

- Assign ringtones to specific contacts in the contact directory. This option is the first and highest in priority.
- Use the `voIpProt.SIP.alertInfo.x.value` and `voIpProt.SIP.alertInfo.x.class` parameters in the **sip-interop.cfg** template to map calls to specific ringtones. The value you enter depends on the call server. This option requires server support and is second in priority.
- Users can select a ringtone for each registered line on the phone from the phone menu. This option has the lowest priority.

> You can use the SIP alert-info header to delay the auto-answer feature. If you set **delay=0** in the **SIP.alert-Info** header, the phone immediately auto-answers incoming calls without ringing. If you set **delay=x** where x=time in seconds, the phone rings for that duration of time before auto-answering incoming calls.

Related Topics

Distinctive Ringtone Parameters

Ringtone Patterns

The following table lists the ring pattern names and their default descriptions. Note that sampled audio files 1 to 10 listed in the table all use the same built-in file unless that file has been replaced with a downloaded file.

Sampled audio files 1 to 10 all use the same built-in file unless that file has been replaced with a downloaded file.

Ringtone Pattern Names

Parameter Name	Ringtone Name	Description
ringer1	Silent Ring	Silent ring Note: Silent ring provides a visual indication of an incoming call, but no audio indication.
ringer2	Low Trill	Long single A3 Db3 major warble
ringer3	Low Double Trill	Short double A3 Db3 major warble
ringer4	Medium Trill	Long single C3 E3 major warble
ringer5	Medium Double Trill	Short double C3 E3 major warble
ringer6	High Trill	Long single warble 1
ringer7	High Double Trill	Short double warble 1
ringer8	Highest Trill	Long single Gb3 A4 major warble
ringer9	Highest Double Trill	Short double Gb3 A4 major warble
ringer10	Beeble	Short double E3 major
ringer11	Triplet	Short triple C3 E3 G3 major ramp
ringer12	Ringback-style	Short double ringback
ringer13	Low Trill Precedence	Long single A3 Db3 major warble Precedence
ringer14	Ring Splash	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
ringer21	-	Sampled audio file 7
ringer22	-	Sampled audio file 8
ringer23	-	Sampled audio file 9
ringer24	-	Sampled audio file 10

Sound Effects

The phone uses built-in sampled audio files (SAF) in wave file format for some sound effects. You can customize the audio sound effects that play for incoming calls and other alerts using synthesized tones or sampled audio files with .wav files you download from the provisioning server or Internet.

Ringtone files are stored in volatile memory which allows a maximum size of 600 kilobytes (614400 bytes) for all ringtones.

Sampled Audio Files

The phone uses built-in sampled audio files (SAF) in wave file format for some sound effects. You can add files downloaded from the provisioning server or from the Internet. Ringtone files are stored in volatile memory, which allows a maximum size of 600 kilobytes (614400 bytes) for all ringtones.

The phones support the following sampled audio WAVE (.wav) file formats:

- mono 8 kHz G.711 u-Law—Supported on all phones
- mono G.711 (13-bit dynamic range, 8-khz sample rate)
- G.711 A-Law—Supported on all phones
- mono L16/8000 (16-bit dynamic range, 8-kHz sample rate)—Supported on all phones
- mono 8 kHz A-law/mu-law—Supported on all phones
- L8/16000 (16-bit, 8 kHz sampling rate, mono)—Supported on all phones
- mono L16/16000 (16-bit dynamic range, 16-kHz sample rate)
- L16/16000 (16-bit, 16 kHz sampling rate, mono)—Supported on all phones
- L16/32000 (16-bit, 32 kHz sampling rate, mono)—Supported on VVX 500/501, 600/601, and 1500
- L16/44100 (16-bit, 44.1 kHz sampling rate, mono)—Supported on VVX 500/501, 600/601, and 1500
- L16/48000 (16-bit, 48 kHz sampling rate, mono)—Supported on VVX 500/501, 600/601, and 1500

Default Sample Audio Files

The following table defines the phone's default use of the sampled audio files.

Default Sample Audio File Usage

Sampled Audio File Number	Default Use (Pattern Reference)
1	Ringer 12 (`se.pat.misc.welcome`) Ringer 15 (`se.pat.ringer.ringer15`)
2	Ringer 16 (`se.pat.ringer.ringer16`)
3	Ringer 17 (`se.pat.ringer.ringer17`)
4	Ringer 18 (`se.pat.ringer.ringer18`)
5	Ringer 19 (`se.pat.ringer.ringer19`)
6	Ringer 20 (`se.pat.ringer.ringer20`)

Default Sample Audio File Usage (continued)

Sampled Audio File Number	Default Use (Pattern Reference)
7	Ringer 21 (`se.pat.ringer.ringer21`)
8	Ringer 22 (`se.pat.ringer.ringer22`)
9	Ringer 23 (`se.pat.ringer.ringer23`)
10	Ringer 24 (`se.pat.ringer.ringer24`)
11 to 24	Not Used

Related Topics

Sampled Audio File Parameters

Sound Effect Patterns

You can specify the sound effects that play for different phone functions and specify the sound effect patterns and the category.

Sound effects are defined by patterns: sequences of chord-sets, silence periods, and wave files. You can also configure sound effect patterns and ringtones. The phones use both synthesized and sampled audio sound effects.

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 instructions shown in the next table.

Sound Effects Pattern Types

Instruction	Meaning
sampled (n)	**Play sampled audio file n**

Example:
```
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)**

Example:
```
se.pat.callProg.busyTone.inst.2.type = "chord" (chord set instruction type)
se.pat.callProg.busyTone.inst.2.value = "busyTone" (specifies sampled audio file busyTone)
se.pat.callProg.busyTone.inst.2.param = "2000" (override ON duration of chord set to 2000 milliseconds)
```

silence (d)	**Play silence for d milliseconds (Rx audio is not muted)**

Example:
```
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)
```

Sound Effects Pattern Types (continued)

Instruction	Meaning
branch (n)	**Advance n instructions and execute that instruction (n must be negative and must not branch beyond the first instruction)**

Example:

`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)

Related Topics

Sound Effect Pattern Parameters

Call Progress Tones

The following table lists the call progress pattern names and their descriptions.

Call Progress Tone Pattern Names

Call Progress Pattern Name	Description
alerting	Alerting
bargeIn	Barge-in tone
busyTone	Busy tone
callWaiting	Call waiting tone
callWaitingLong	Call waiting tone long (distinctive)
callWaitingRingback	Call Waiting RingBack Tone
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
preemption	Preemption tone
precedence	Precedence tone
recWarning	Record warning
reorder	Reorder tone
ringback	Ringback tone

Call Progress Tone Pattern Names (continued)

Call Progress Pattern Name	Description
secondaryDialTone	Secondary dial tone
stutter	Stuttered dial tone

Miscellaneous Patterns

The following table lists the miscellaneous patterns and their descriptions.

Miscellaneous Pattern Names

Parameter Name	Miscellaneous pattern name	Description
instantmessage	instant message	New instant message
localHoldNotification	local hold notification	Local hold notification
messageWaiting	message waiting	New message waiting indication
negativeConfirm	negative confirmation	Negative confirmation
positiveConfirm	positive confirmation	Positive confirmation
remoteHoldNotification	remote hold notification	Remote hold notification
welcome	welcome	Welcome (boot up)

Supported Audio Codecs

The following table details the supported audio codecs and priorities for Polycom phone models.

Note the following limitations when using the Opus codec:

- VVX 301, 311, 401, 411, 500, and 600 business media phones support a single Opus stream. Users can establish only one call at a time when using the Opus codec on these phones.
- VVX 500 and 600 do not support video when using Opus.
- VVX 500 and 600 do not support local conferences when using Opus.
- Opus is not compatible with G.729 and iLBC. If you set Opus to the highest priority, G.729 and iLBC are not published; if you set G.729 and iLBC to the highest priority, Opus is not published.

> On the VVX 500/501 and 600/601, when you enable video, the G.722.1C codec is disabled.

Audio Codec Priority

Phone	Supported Audio Codecs	Priority
VVX 101, 201	G.711µ-law	6
	G.711a-law	7
	G.722	4
	G.729AB	8
	iLBC (13.33kbps, 15.2kbps)	0, 0
VVX 300/301, 310/311, 400/401, 410/411 * Note: VVX 301, 311, 401, 411 support a single Opus stream. VVX 300, 310, 400, 410 do not support Opus.	G.711µ-law	6
	G.711a-law	7
	G.722	4
	G.722.1 (24kbps, 32kbps)	5
	G.729AB	8
	iLBC (13.33kbps, 15.2kbps)	0, 0
	Opus*	0
	Siren 7	0
VVX 500/501, 600/601 • VVX 500 and 600 support a single Opus stream. • VVX 500 and 600 do not support both Opus and video.	G.711 µ -law	6
	G.711a-law	7
	G.722	4
	G.722.1 (24kbps, 32kbps)	5
	G.722.1C (48kbps)	2
	G.729AB	8
	Opus*	0
	iLBC (13.33kbps, 15.2kbps)	0, 0
	Siren 7	0

Audio Codec Priority (continued)

VVX 1500	G.711 μ -law	6
	G.711a-law	7
	G.719 (64kbps)	0
	G.722	4
	G.722.1 (24kbps, 32kbps)	5
	G.722.1C (48kbps)	2
	G.729AB	8
	Siren14 (48kbps)	3
	iLBC (13.33kbps, 15.2kbps)	0, 0
SoundStructure VoIP Interface	G.711 μ -law	6
	G.711a-law	7
	G.722	4
	G.722.1 (24kbps, 32kbps)	5
	G.722.1C (48kbps)	2
	G.729AB	8
	iLBC (13.33kbps, 15.2kbps)	0, 0
	Siren 7	0

Supported Audio Codec Specifications

The following table summarizes the specifications for audio codecs supported on Polycom phones.

Audio Codec Specifications

Algorithm	Reference	Raw Bit Rate	IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
G.711 μ -law	RFC 1890	64 Kbps	80 Kbps	8 Ksps	20 ms	3.5 KHz
G.711 a-law	RFC 1890	64 Kbps	80 Kbps	8 Ksps	20 ms	3.5 KHz
G.719	RFC 5404	32 Kbps 48 Kbps 64 Kbps	48 Kbps 64 Kbps 80 Kbps	48 Ksps	20 ms	20 KHz
G.711	RFC 1890	64 Kbps	80 Kbps	16 Ksps	20 ms	7 KHz
G.722[1]	RFC 3551	64 Kbps	80 Kbps	16 Ksps	20 ms	7 KHz

Audio Codec Specifications

Algorithm	Reference	Raw Bit Rate	IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
G.722.1	RFC 3047	24 Kbps 32 Kbps	40 Kbps 48 Kbps	16 Ksps	20 ms	7 KHz
G.722.1C	G7221C	224 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 Ksps	20 ms	14 KHz
G.729AB	RFC 1890	8 Kbps	24 Kbps	8 Ksps	20 ms	3.5 KHz
Opus	RFC 6716	8 - 24 Kbps	24 - 40 Kbps	8 Ksps 16 Ksps	20 ms	3.5 KHz 7 KHz
Lin16	RFC 1890	128 Kbps 256 Kbps 512 Kbps 705.6 Kbps 768 Kbps	132 Kbps 260 Kbps 516 Kbps 709.6 Kbps 772 Kbps	8 Ksps 16 Ksps 32 Ksps 44.1 Ksps 48 Ksps	10 ms	3.5 KHz 7 KHz 14 KHz 20 KHz 22 KHz
Siren 7	SIREN7	16 Kbps 24 Kbps 32 Kbps	32 Kbps 40 Kbps 48 Kbps	16 Ksps	20 ms	7 KHz
Siren14	SIREN14	24 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 Ksps	20 ms	14 KHz
Siren22	SIREN22	32 Kbps 48 Kbps 64 Kbps	48 Kbps 64 Kbps 80 Kbps	48 Ksps	20 ms	22 KHz
iLBC	RFC 3951	13.33 Kbps 15.2 Kbps	31.2 Kbps 24 Kbps	8 Ksps	30 ms 20 ms	3.5 KHz

[1] Per RFC 3551. Even though the actual sampling rate for G.722 audio is 16,000 Hz (16ksps), the RTP clock rate advertised for the G.722 payload format is 8,000 Hz because that value was erroneously assigned in RFC 1890 and must remain unchanged for backward compatibility.

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 for both the receive and transmit signals consumes about 100kbps of network bandwidth (two-way audio).

Related Topics

Audio Codec Parameters

IEEE 802.1p/Q

The phone tags all Ethernet packets it transmits with an 802.1Q VLAN header when the following occurs:

- A valid VLAN ID is specified in the phone's network configuration.
- The phone is instructed to tag packets through Cisco Discovery Protocol (CDP) running on a connected Ethernet switch.
- A VLAN ID is obtained from DHCP or LLDP

Related Topics

IEEE 802.1p/Q Parameters

Voice Quality Monitoring (VQMon)

You can configure the phones to generate various quality metrics that you can use to monitor sound and listening quality. These metrics can be sent between the phones in RTCP XR packets, which are compliant with RFC 3611—RTP Control Extended Reports (RTCP XR). The packets are sent to a report collector as specified in draft RFC Session initiation Protocol Package for Voice Quality Reporting Event. The metrics can also be sent as `SIP PUBLISH` messages to a central voice quality report collector.

You can use Real Time Control Protocol Extended Report (RTCP XR) to report voice quality metrics to remote endpoints. This feature supports RFC6035 compliance as well as draft implementation for voice quality reporting.

You need a license key to activate the VQMon feature on the VVX 300/301, 310/311, 400/401, and 410/411 business media phones. This feature is available for open SIP environments, but is not available with Skype for Business Server. For more information on VQMon, contact your Certified Polycom Reseller.

VQMon Reports

You can enable three types of voice quality reports:

- **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.

You can generate a wide range of performance metrics using the parameters shown in the following table. 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 generated using other metrics as input, such as listening Mean Opinion Score (MOS), conversational MOS, listening R-factor, and conversational R-factor.

Related Topics

VQMon Parameters

Video Features

After you set up Polycom phones on your network with the default configuration, users can place and answer video calls, if supported. This section provides information on making custom configurations to optimize video calling for Polycom phones. Polycom Open SIP 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.

The Polycom VVX 500/501 and 600/601 with the Polycom VVX Camera and VVX 1500 phones with a built-in camera support transmission and reception of high quality video images.

Video and Camera Options

By default, at the start of a video call, the VVX 1500 and VVX phones using the VVX Camera transmit 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 Stop or Start soft key.

You can use the parameters in the following sections to configure video transmission, the video and local camera view, and video camera options.

Related Topics

Video Transmission Parameters

Video and Camera View Parameters

Video Camera Parameters

Video Codec Parameters

Supported Video Codecs

See the following table for a summary of video codecs supported on VVX business media phones.

Video Codec Specifications

Algorithm	MIME Type	Frame Size	Bit Rate (kbps)	Frame Rate (fps)
H.261	H261/90000	Tx Frame size: CIF, QCIF, SQCIF RX Frame size: CIF, QCIF	64 to 768	5 to 30

Video Codec Specifications (continued)

H.263	H263/90000, H263-1998/90000	Tx Frame size:CIF, QCIF Rx Frame size:CIF, QCIF, SQCIF, QVGA, SVGA, SIF	64 to 768 kbps	5 to 30
H.264	H264/90000	Tx Frame size:CIF, QCIF VVX 5xx and 6xx with a VVX Camera support sending 720p resolution for Tx Frame size Rx Frame size:CIF, QCIF, SQCIF, QVGA, SVGA, SIF	64 to 768	5 to 30

H.323 Protocol

VVX 1500 phones and VVX camera-enabled VVX 500/501 and 600/601 phones support telephony signaling via the H.323 protocols. H.323 protocol enables direct communication with H.323 endpoints, gatekeepers, call servers, media servers, and signaling gateways.

> You need a license key to activate H.323 video on your VVX 1500 phone; the license is installed on the VVX 1500D. For more information, contact your Certified Polycom Channel Partner.

SIP and H.323 Protocol

The VVX 500/501, 600/601, and 1500 phones can support both SIP and H.323 signaling simultaneously, and the phones support bridging both types of calls during multi-party conference calls. The phone can automatically detect the correct or optimal signaling protocol when dialing a call from the contact directory or the corporate directory.

While SIP supports server redundancy and several transport options, only a single configured H.323 gatekeeper address per phone is supported. The phone does not require H.323 gatekeepers, but you can use them if available. If an H.323 gatekeeper is not configured or is unavailable, you can still enable the phones to make H.323 calls.

Support of the SIP protocol for telephony signaling can be disabled on the VVX 500/501, 600/601, and 1500 such that all calls route via the H.323 protocol.

H.323 and SIP Protocol Limitations and Restrictions

The following information should be noted for H.323 Protocol:

● If the phone has only the H.323 protocol enabled, the phone cannot be used to answer SIP calls.

● If the phone has only the SIP protocol enabled, the phone cannot be used to answer H.323 calls.

● If both SIP and H.323 protocols are disabled by mistake, the phone continues 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 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 from the directory.

- 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, when more than one protocol is available, each protocol displays as a soft key and the user can choose which protocol to use.

- Calls made using H.323 cannot be forwarded or transferred, and the following conditions apply:

  ➢ The Transfer and Forward soft keys do not display during an H.323 call.

  ➢ The Forward soft key does not display on the idle screen if the primary line is an H.323 line.

  ➢ If a user presses the Transfer soft key during an H.323 call, 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 call and one of the parties is connected by H.323, that party is not transferred to the other party that was part of the conference call.

Supported H.323 Video Standards

The following table lists the standards the H.323 feature supports.

Supported Video Standards

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
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

Related Topics

H.323 Protocol Parameters

FQDN Support for H.323 Gatekeeper Failover

This enhancement, available only for registration failover scenarios, enables fully qualified domain name (FQDN) configuration for H.323 Gatekeeper. Gatekeeper IP addresses are resolved from a DNS server when the Gatekeeper sends a DNS A query or through the local static cache. This enhancement supports a maximum of two IP addresses based on the DNS response irrespective of the number of records received.

Note that this enhancement does not apply if you are using the parameter `voIpProt.H323.autoGateKeeperDiscovery` for auto-discovery.

Toggling Between Audio-only or Audio-Video Calls

When this feature is enabled on the VVX 1500, and VVX camera-enabled VVX 500/501 and 600/601 business media phones, a soft key displays to enable users to toggle calls between audio-only or audio-video.

This feature applies only to outbound calls from your phone; incoming video calls to your phone are answered using video even when you set the feature to use audio-only.

When the phone is registered, you can:

- Use `video.callMode.default` to begin calls as audio-video or audio only. By default, calls begin as audio-video. After a video call has ended, the phone returns to audio-only.
- Use `up.homeScreen.audioCall.enabled` to enable a Home screen icon that allows you to make audio-only calls. Far-end users can add video during a call if the far-end device is video capable.

Related Topics

I-Frames

When video streams initialize, devices transmit video packets called I-frames (reference frames) that contain information to display a complete picture. Subsequent video packets, known as P-frames, are smaller and not as complete to consume less bandwidth. Due to packet loss, jitter, or corruption, devices occasionally need to make multiple requests for a complete I-frame in order to reset the full frame, after which devices can revert to P-frame updates.

You can set parameters to control an I-frame request. The following table indicates parameter dependencies and messaging behavior when setting an I-frame request method.

I-Frame Parameter Dependencies

video. forceRtcpVideoCodecControl	video. dynamicControlMethod	voIpProt. SDP.offer.rtcpVideoCodecControl	Behavior when requesting video I-frame updates
0	0 (n/a)	0	Only SIP INFO messages are sent. No RTCP-FB is offered in SDP.
0	1 (n/a)	0	Only SIP INFO messages are sent. No RTCP-FB is offered in SDP.
0	0 (n/a)	1	RTCP-FB is offered in SDP. If SDP responses do not contain the required RTCP-FB attribute, then only SIP INFO requests are used.

I-Frame Parameter Dependencies (continued)

video. forceRtcpVideoCodecControl	video. dynamicControlMethod	volpProt. SDP.offer.rtcpVideoCodecControl	Behavior when requesting video I-frame updates
0	1 (n/a)	1	RTCP-FB is offered in SDP. If SDP responses do not contain the required RTCP-FB attribute, then only SIP INFO requests are used.
1	0	0	The SDP attribute a=rtcp-fb is not included in SDP offers. Both RTCP-FB and SIP INFO messages are attempted.
1	1	0	The SDP attribute a=rtcp-fb is not included in SDP offers. Both RTCP-FB and SIP INFO messages are attempted. If no RTCP-FB messages are received, only SIP INFO messages are sent. If no response is received for SIP INFO messages then, again, both RTCP-FB and SIP INFO messages are attempted.
1	0	1	RTCP-FB is offered in SDP. Even if the SDP response does not include an accepted a=rtcp-fb attribute both RTCP-FB and SIP INFO messages are sent.
1	1	1	RTCP-FB is offered in SDP. Even if the SDP response does not include an accepted a=rtcp-fb attribute both RTCP-FB and SIP INFO messages are sent initially. If no RTCP-FB response is received, only SIP INFO messages are sent afterwards.

Phone Display and Appearances

This section provides information on setting up features involving the phone's user interface.

Time Zone Location Description

The following two parameters configure a time zone location description for their associated GMT offset:

- `device.sntp.gmtOffsetcityID`

  If you are not provisioning phones manually from the phone menu or Web Configuration Utility and you are setting the `device.sntp.gmtOffset` parameter, then you must configure `device.sntp.gmtOffsetcityID` to ensure that the correct time zone location description displays on the phone menu and Web Configuration Utility. The time zone location description is set automatically if you set the `device.sntp.gmtOffset` parameter manually using the phone menu or Web Configuration Utility.

- `tcpIpApp.sntp.gmtOffsetcityID`

  If you are not provisioning phones manually from the Web Configuration Utility and you are setting the `tcpIpApp.sntp.gmtOffset` parameter, then you must configure `tcpIpApp.sntp.gmtOffsetcityID` to ensure that the correct time zone location description displays on the Web Configuration Utility. The time zone location description is set automatically if you set the `tcpIpApp.sntp.gmtOffset` parameter manually using the Web Configuration Utility.

Related Topics

Time Zone Location Parameters

Time and Date

A clock and calendar display on the phones by default. You can choose how to display the time and date for your time zone in several formats, or you can disable the display of the time and date. You can also set the time and date format to display differently when the phone is in certain modes. For example, the display format can change when the phone goes from idle mode to an active call.

To have the most accurate time, you have to synchronize the phone to the Simple Network Time Protocol (SNTP) time server. Until a successful SNTP response is received, the phone continuously flashes the time and date to indicate that they are not accurate.

The time and date display on the phones in PSTN mode and are set by an incoming call with a supported caller ID standard, or when the phone is connected to Ethernet and you enable the date and time display.

Related Topics

Time and Date Display Parameters

Date Formats

Use the following table to choose values for the `lcl.datetime.date.format` and `lcl.datetime.date.longformat` parameters. The table shows values for Friday, August 19, 2011 as an example.

Date Formats

lcl.datetime.date.format	lcl.datetime.date.longformat	Date Displayed on Phone
dM,D	0	19 Aug, Fri
dM,D	1	19 August, Friday
Md,D	0	Aug 19, Fri
Md,D	1	August 19, Friday
D,dM	0	Fri, 19 Aug
D,dM	1	Friday, August 19
DD/MM/YY	n/a	19/08/11
DD/MM/YYYY	n/a	19/08/2011
MM/DD/YY	n/a	08/19/11
MM/DD/YYYY	n/a	08/19/2011
YY/MM/DD	n/a	11/08/19
YYYY/MM/DD	n/a	2011/08/11

Phone Theme

The VVX 500/501 and 600/601 business media phones include two display themes, Classic and Modern, that determine how the user interface displays on the phone. The following figure shows the differences between the two themes.

Classic   Modern
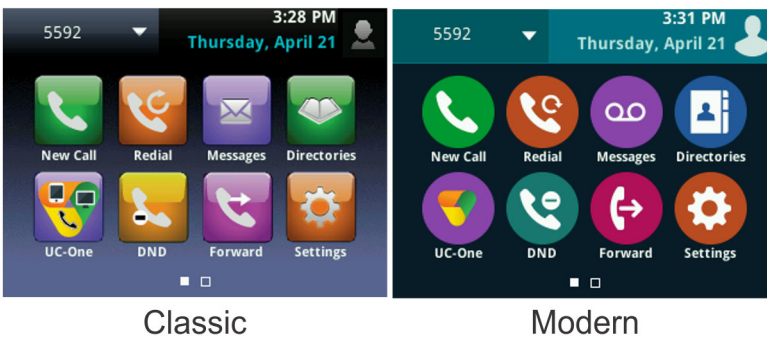
Related Topics

Phone Theme Parameters

Default Off-Hook Phone Screen

On VVX 500, 501, 600, and 601 business media phones, you can configure the default phone screen that displays when the phone goes off-hook or is in a call. You can configure which screens to display as follows:

- Set the Active Call or Lines screen to display when the phone is in an active call.

  Displaying the Lines screen during an active call enables users to see the status of any lines, buddies, and BLF contacts they are monitoring.

- Set the Home or Lines screen to display when the phone is off-hook.

  Displaying the Lines screen when the phone goes off hook enables users to quickly select a favorite or BLF line to dial. In this scenario, when users start to enter a number from the keypad, the phone switches to the dialer screen.

Related Topics

Default Off-Hook Phone Screen Parameters

Graphic Display Background

You can display a graphic image on the background of the all VVX business media phones and connected VVX Color Expansion Modules. The VVX phones display a default background picture. You can configure a specified background picture or design, such as a company logo, or you can import a set of custom images that users can choose from.

All Polycom phones support JPEG, BMP, and PNG image file formats; progressive/multi-scan JPEG images are not supported.

Maximum Image Size

Refer to the following table for the maximum image size supported for each VVX business media phone.

For detailed instructions on adding a graphic display to a VVX phone, see the *Polycom VVX Business Media Phones User Guide*.

Maximum Image Size

Phone	Screen Size
VVX 300 series	208x104 pixels (Grayscale)
VVX 400 series	320x240 pixels
VVX 500 series	320x240 pixels
VVX 600 series	480x272 pixels
VVX 1500	800x480 pixels
VVX Color Expansion Module	272x480 pixels

Related Topics

Graphic Display Background Parameters

Digital Picture Frame

On the VVX phones, you can display a slide show of images stored on a USB drive on the phone's idle screen. For images to display, the images must be saved in JPEG, BMP, or PNG format on the top directory of a USB device that is attached to the phone. The phone can display a maximum image size of 9999x9999 pixels and a maximum of 1000 images.

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

You can access the digital picture frame on the web using *PicFrame:// URL*.

Related Topics

Digital Picture Frame Parameters

Background Image Lock

By default, users can set a background image for their phones using the phone, a USB drive attached to the phone, or the Web Configuration Utility. You can disable the user's ability to set images as a background when viewing images on a USB attached to the phone, which is a part of the Digital Picture Frame feature.

Disabling this feature removes the following options for users:

● Access to the Background menu on the phone

● The Set Background icon to set a background from an image on a USB drive attached to the phone

● The Background menu option in the Preferences menu in the Web Configuration Utility

Phone Languages

All phones support the following languages: Arabic, Simplified Chinese, Traditional Chinese, Danish, Dutch, English, French, German, Italian, Japanese, Korean, Norwegian, Polish, Brazilian Portuguese, Russian, Slovenian, International Spanish, and Swedish.

Each language is stored as a language file in the **VVXLocalization** folder, which is included with the Polycom UC Software package. If you want to edit the language files, you must use a Unicode-compatible XML editor such as XML Notepad 2007 and familiarize yourself with the guidelines on basic and extended character support (see <ml/>).

At this time, the updater is available in English only.

Related Topics

Digital Picture Frame Parameters

Add a Language for the Phone Display and Menu

Use the multilingual parameters to add a new language to your provisioning server directory to display on the phone screen and menu.

To add a new language:

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 VVXLocalization folder on the provisioning server.

4 Add an `lcl.ml.lang.clock.menu.x` parameter 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` parameters and set them according to the regional preferences.

6 (Optional) Set `lcl.ml.lang` to be the new `language_region` string.

Pinyin Text Input

Pinyin is the phonetic system used to transcribe Mandarin pronunciation of Chinese into Latin characters. The pinyin text input feature on VVX business media phones uses Nuance XT9® Smart Input to enable users to enter Chinese characters into text input fields using the phone's dial pad keys or on-screen keyboard. The pinyin text input feature is not supported on VVX 101 and 201 phones.

To enable users to use the pinyin text input feature on Polycom phones, download a license key to the user's phone.

> For complete information on the pinyin text input feature, see the *Polycom VVX Business Media Phones User Guide*.

Digital Phone Label

You can configure the Digital Phone Label feature to display the complete registration line address in the status bar of the phone's screen.

The Digital Phone Label feature supports VVX 3xx/4xx/5xx/6xx business media phones and is not available for Skype for Business.

The following illustrates a successfully configured registration line in the address bar.

Related Topics

Digital Phone Label Parameters

Unique Line Labels for Registration Lines

You can configure unique labels on line keys for registration lines. You must configure multiple line keys on the phone for a registration in order to configure unique line labels. For example, you can set different names to display for the registration *4144* that displays on four line keys.

If you configure the line to display on multiple line keys without a unique label assigned to each line, the lines are labeled automatically in numeric order. For example, if you have four line keys for line 4144 labeled Polycom, the line keys are labeled as 1_Polycom, 2_ Polycom, 3_ Polycom, and 4_ Polycom. This also applies to lines without labels.

Related Topics

Unique Line Labels for Registration Lines Parameters

LED Indicators

The LED indicators on VVX phones and expansion modules alert users to the different states of the phone and remote contacts. You can turn LED indicators on or off, and set the pattern, color, and duration of a pattern for all physical keys on the phones.

You can set the pattern, color, and duration for the following LED indicators on VVX phones:

- Line keys
- Message Waiting Indicator (MWI)
- Headset key (excluding VVX 101 and 201)

Related Topics

LED Behavior Parameters

LED Indicator Pattern Types

Enter one of the values in the following table to indicate the LED indicator pattern type.

LED Indicator Pattern Type

Pattern Type	Function
powerSaving	Sets the behavior for Message Waiting Indicator when the phone is in Power Saving mode.
active	Sets the pattern for line keys during active calls.
on	Turns on the LED indicator pattern.
off	Turns off the LED indicator pattern.
offering	Sets the pattern for line keys during incoming calls.
flash	Sets the pattern for line keys during held calls and the Message Waiting Indicator when there are unread voicemail messages.
lockedOut	Sets the pattern for line keys when a remote party is busy on a shared line.
FlashSlow	Sets the pattern for the Headset key when Headset Memory Mode is enabled.
held	Sets the pattern for line keys during a held call.
remoteBusyOffering	Sets the pattern for line keys for monitored BLF contacts.

LED Pattern Examples

This section includes example configurations you can use to set the patterns of LED indicators for VVX phones and expansion modules.

Example: Disable the Headset Key LED in Headset Memory Mode

By default, the Headset key on all VVX phones, excluding VVX 101 and 201, glows green for analog headsets and blue for USB headsets. The Headset key also flashes by default if Headset Memory Mode is enabled.

The default configuration is listed in the following table.

Parameter / Value	Function
`ind.pattern.flashSlow.step.1.state="1"`	Turns on the LED indicator.
`ind.pattern.flashSlow.step.1.duration="100"`	Sets the duration of the pattern.
`ind.pattern.flashSlow.step.2.state="0"`	Turns off the LED indicator for the second step.
`ind.pattern.flashSlow.step.2.duration="2900"`	Sets the duration for the second step in which the LED indicator is off. After this duration, the pattern repeats.

You can disable and turn off the flash pattern for the Headset key when Headset Memory Mode is enabled.

To disable the flash pattern for the Headset key:

» Set the parameter `ind.pattern.flashSlow.step.1.state` to 0.

Example: Set an LED Pattern for Active Calls

In the following example, during an active call, the line key alternates green and red.

To configure a line key LED pattern to alternate green and red for active calls:

» Configure the pattern as follows:

➢ `ind.pattern.active.step.1.color=`"Green"

➢ `ind.pattern.active.step.1.state=`"1"

➢ `ind.pattern.active.step.1.duration=`"1000"

➢ `ind.pattern.active.step.2.color=`"Red"

➢ `ind.pattern.active.step.2.state=`"1"

➢ `ind.pattern.active.step.2.duration=`"1000"

Example: Turn Off the Message Waiting Indicator in Power Saving Mode

When Power Saving mode is enabled, the screen darkens, and the MWI flashes red. By default, the powerSaving pattern has two steps before the pattern is repeated: a quick on period and then a long off period.

By default, the following parameters set the behavior of the MWI during Power Saving mode.

Parameter / Value	Function
`ind.pattern.powerSaving.step.1.state=`"1"	Turns on the LED indicator.
`ind.pattern.powerSaving.step.1.duration=`"100"	Sets the duration of the pattern.
`ind.pattern.powerSaving.step.2.state=`"0"	Turns off the LED indicator for the second step.
`ind.pattern.powerSaving.step.2.duration=`"2900"	Sets the duration for the second step in which the LED indicator is off. After this duration, the pattern repeats.

You can turn off the MWI or change the duration of the pattern steps.

To disable the pattern for the MWI in Power Saving mode:

» Set the parameter `ind.pattern.powerSaving.step.1.state` to 0.

Example: Change the Color of Line Key Indicators for Incoming Calls

When a phone receives an incoming call, the line key LED indicator flashes green. You can change the color of the indicator to Yellow or Red for incoming calls.

By default, the following parameters set the behavior of the line key LED indicators for incoming calls.

Parameter / Value	Function
`ind.pattern.offering.step.1.state="1"`	Turns on the LED indicator.
`ind.pattern.offering.step.1.duration="5000"`	Sets the duration of the pattern in step 1.
`ind.pattern.offering.step.1.color="Yellow"`	Sets the color of the LED indicator for the pattern.
`ind.pattern.offering.step.2.state="0"`	Turns off the LED indicator for the second step.
`ind.pattern.offering.step.2.duration="5000"`	Sets the duration of the pattern in step 2.
`ind.pattern.offering.step.2.color="Yellow"`	Value is ignored because step 2 state=0
`ind.pattern.offering.step.3.state="1"`	Turns on the LED indicator.
`ind.pattern.offering.step.3.duration="5000"`	Sets the duration of the pattern.
`ind.pattern.offering.step.3.color="Red"`	Sets the color of the LED indicator for the pattern. After this duration, the pattern repeats.

To change the color of the line key indicator:

» Set the parameter `ind.pattern.offering.step.1.color` to Yellow.

Capture Your Device's Current Screen

You can capture your phone or expansion module's current screen. Note that the RealPresence Trio solution does not support expansion modules.

Before you can take a screen capture, you must provide power and connect the expansion module to a phone, and enable the phone's web server using the parameter `httpd.enabled`.

To capture a device's current screen:

1   In the `sip-interop.cfg` template, locate the parameter `up.screenCapture.enabled`.

You can add the sip-interop.cfg template to the CONFIG-FILES field of the master configuration file, or copy the parameter to an existing configuration file.

2   Set the value to `1` and save the configuration file.

3   On the device, go to **Settings > Basic > Preferences > Screen Capture**.

Note you must repeat step 3 each time the device restarts or reboots.

4   Locate and record the phone's IP address at **Status > Platform > Phone > IP Address**.

5   Set the phone to the screen you want to capture.

6   In a web browser address field, enter `https://<phoneIPaddress>/captureScreen` where `<phoneIPaddress>` is the IP address you obtained in step 5.

The web browser displays an image showing the phone's current screen. You can save the image can be saved as a BMP or JPEG file.

User Accounts and Contacts

User Profiles

When you set up user profiles, you enable users to access their personal phone settings, including their contact directory, speed dials, and other phone settings from any phone on the network. This feature is particularly useful for remote and mobile workers who do not have a dedicated work space and conduct their business in more than one location. This feature is also useful if an office has a common conference phone from which multiple users need to access their personal settings.

> Important: You can configure all company phones so that anyone can call authorized and emergency numbers when not logged in to a phone. For more information, see `dialplan.routing.emergency.outboundIdentity`.

If you set up the user profile feature, a user can log in to a phone by entering their user ID and password. The default password is **123**. If the user profile feature is set up on your company's phones, users can:

- Log in to a phone to access their personal phone settings.
- Place a call to an authorized number from a phone that is in the logged out state.
- Change their user password.
- Log out of a phone after they finish using it.

If a user changes any settings while logged in to a phone, the settings save and display the next time the user logs in to another phone. When a user logs out, the user's personal phone settings are no longer displayed.

Related Topics

User Profile Parameters

Remotely Logging Out Users

Note that if an unexpected reboot occurs while a user is logged in, the user is not logged out and the phone returns to the user profile after reboot.

If a user is not logged out from a phone and other users are not prevented from logging in, the user can ask the administrator to log out remotely. Administrators can log out a user remotely with a checksync event in the NOTIFY by setting the parameter `profileLogout=remote`.

Server Authentication of User Profiles

Instead of phone-based authentication of user profiles, you can configure server authentication. When you enable server authentication, you set up user accounts on the provisioning server and each user can authenticate their phone by entering correct server credentials.

The phone downloads log files app.log and boot.log from the generic profile on the provisioning server regardless of user logins.

User Profiles with Server Authentication

You can create a generic user profile or a particular user profile when using server authentication.

Create a Generic Profile Using Server Authentication

Create a generic profile and generic credentials on the provisioning server when a user is not logged into the phone.

If you enable server authentication of user profiles, the following parameters do not apply and you do not need to configure them:

* `prov.login.defaultUser`
* `prov.login.defaultPassword`
* `prov.login.defaultOnly`
* `prov.login.localPassword`
* `prov.login.localPassword.hashed`

To create a generic profile:

1 On the server, create an account and directory for the generic profile, for example, '*Generic_Profile*'.

2 In the *Generic_Profile* directory, create a configuration file for a generic profile the phone uses by default, for example, *genericprofile*.cfg.

3 In *genericprofile*.cfg, include registration and server details and set all phone feature parameters. You must set the following parameters to use server authentication:

> ➢ `prov.login.enabled="1"`

> ➢ `prov.login.useProvAuth="1"`

> ➢ `prov.login.persistent="1"`

Note that if you enable `prov.login.enabled=1` and do not enable `prov.login.useProvAuth=0`, users are authenticated by a match with credentials you store in the user configuration file *<user>*.cfg.

4 Create a master configuration file 000000000000.cfg for all the phones, or a *<MACAddress>*.cfg for each phone, and add *genericprofile*.cfg to the CONFIG_FILES field.

For information about using the master configuration file, see 'Provision and Configure Phones with Polycom UC Software' in the UC Software Administrator's Guide on Polycom Voice Support.

5 Set the provisioning server address and provisioning server user name and password credentials for the generic user account on the phone at **Settings > Advanced > Provisioning Server** details and inform users of their user profile credentials.

The following override files are uploaded to the generic profile directory:

● Log files
● Phone menu settings

- Web Configuration Utility settings
- Call logs
- Contact directory file

Create a User Profile Using Server Authentication

Create a user profile in the Home directory of each user with a user-specific configuration file that you store on the provisioning server with a unique name as well as user-specific files such as settings, directory, and call lists.

When a user logs in with credentials, the phone downloads the user profile from the provisioning server. When the user logs out, the phone downloads the default user profile using the generic credentials.

To create a user profile:

1   On the server, create an account and a directory for each user, for example, '*User1*', '*User2*".

2   In each user directory, create a configuration file for each user, for example, *User1*.cfg, *User2*.cfg, that contains the user's registration details and feature settings.

The following override files are uploaded to the generic profile account on the server:

- Log files
- Web Configuration Utility settings

The following override files are uploaded to the user profile account on the server:

- Phone menu settings
- Contact directory file

User Profiles Without Server Authentication

You can create default credentials and user profiles without use of server authentication.

Create Default Credentials and a Profile for a Phone

You can choose to define default credentials for a phone, which the phone uses to automatically log itself in each time an actual user logs out or the phone restarts or reboots. When the phone logs itself in using the default login credentials, a default phone profile displays, and users retain the option to log in and view their personal settings.

You can create a new phone configuration file for the default profile, then add and set the attributes for the feature. You can also update an existing phone configuration file to include the user login parameters you want to change.

> Important: Polycom recommends that you create a single default user password for all users.

To create default credentials and a profile for a phone:

1 Create a **site.cfg** file for the phone and place it on the provisioning server.

You can base your file on the sample configuration template in your software package. To find the file, navigate to **<provisioning server location>/Config/site.cfg**.

2 In **site.cfg**, open the **<prov.login/>** attribute, then add and set values for the user login attributes.

Create a User Configuration File

Create a configuration file for each user that you want to enable to log in to the phone. The name of the file should specify the user's login ID. In the file, specify any user-specific settings that you want to define for the user.

If a user updates their password or other user-specific settings on the phone, the updates are stored in **<user>-phone.cfg**, not **<MACaddress>-phone.cfg**.

If a user updates their contact directory while logged in to a phone, the updates are stored in **<user>-directory.xml**. Directory updates display each time the user logs in to a phone. For certain phones (for example, the VVX 1500 phone), an up-to-date call lists history is defined in **<user>-calls.xml**. This list is retained each time the user logs in to their phone. The following is a list of configuration parameter precedence (from first to last) for a phone that has the user profile feature enabled:

● <user>-phone.cfg
● Web Configuration Utility
● Configuration files listed in the master configuration file (including <user>.cfg)
● Default values

Note: To convert a phone-based deployment to a user-based deployment, copy the **<MACaddress>-phone.cfg** file to **<user>-phone.cfg** and copy **phoneConfig<MACaddress>.cfg** to **<user>.cfg**.

To create a user configuration file:

1 On the provisioning server, create a user configuration file for each user.

2 Name each file the ID the user will use to log in to the phone. For example, if the user's login ID is **user100**, the name of the user's configuration file is **user100.cfg**.

3 In each <user>.cfg file, you are required to add and set values for the user's login password.

4 Add and set values for any user-specific parameters, such as:

➢ Registration details such as the number of lines the profile displays and line labels.

➢ Feature settings such as microbrowser settings).

Caution: If you add optional user-specific parameters to <user>.cfg, add only those parameters that will not cause the phone to restart or reboot when the parameter is updated. For information on which parameters cause the phone to restart or reboot, see the reference section Configuration Parameters.

Local Contact Directory

Polycom phones feature a contact directory file you can use to store frequently used contacts. The UC Software package includes a template contact directory file named **000000000000-directory~.xml** that is loaded to the provisioning server the first time you boot up a phone with UC Software or when you reset the phone to factory default settings.

When you first boot the phone out of the box or when you reset the phone to factory default settings, the phone looks for contact directories in the following order:

- An internally stored local directory

- A personal **<MACaddress>-directory.xml** file

- A global **000000000000-directory.xml** file when the phone substitutes <000000000000> for its own MAC address.

The Contact Directory is the central database for several phone features including speed dial (see Speed Dials), distinctive incoming call treatment (see Distinctive Incoming Call Treatment), presence (see Presence Status), and instant messaging (see Instant Messaging).

You can configure the phones to hide the Contact Directory and Favorites options from all screens in the user interface on all VVX phones except the VVX 1500 phone. You can also set the local directory as read-only and restrict users from modifying the speed dials only.

In addition, make sure the `dir.local.readonly` parameter is enabled to restrict the users to modify speed dials.

Related Topics

Local Contact Directory Parameters

Maximum Capacity of the Local Contact Directory

The following table lists the maximum number of contacts and maximum file size of the local Contact Directory for each phone. To conserve phone memory, use the parameter `dir.local.contacts.maxNum` to set a lower maximum number of contacts for the phones.

Maximum File Size and Number of Contacts

Phone	Maximum File Size	Maximum Number of Contacts in File
VVX 300/301/310/311	4MB	500
VVX 400/401/410/411	4MB	500
VVX 500/501 and 600/601	4MB	500
VVX 1500	102400 bytes Non-volatile: 100KB	9999
SoundStructure VoIP Interface	Not applicable	Not applicable

Creating Per-Phone Directory Files

To create a per-phone, personal directory file, replace *<000000000000>* in the global file name with the phone's MAC address: ***<MACaddress>-directory.xml***. Any changes users make to the contact directory from the phone are stored on the phone drive and uploaded to the provisioning server in the personal directory (***<MACaddress>-directory.xml***) file, which enables you to preserve a contact directory during reboots.

To create a global directory file that you can use to maintain the directory for all phones from the provisioning server, remove the tilde (~) from the template file name **000000000000-directory.xml**. When you update the global directory file on the provisioning server, the updates are downloaded onto the phone and combined with the phone specific directory.

Maintaining Per-Phone Directory Files

Using the parameter `voIpProt.SIP.specialEvent.checkSync.downloadDirectory`, you can configure the phones to download the updated directory files upon receipt of a `checksync NOTIFY` message. The files are downloaded when the phone restarts, reboots, or when the phone downloads any software or configuration updates.

Any changes to either the global or personal directory files are reflected in the directory on the phone after a restart or a `checksync NOTIFY` message. When merging the two files, the personal directory always takes precedence over the changes in the global directory. Thus, if a user modifies a contact from the global directory, the contact is saved in the personal directory file, and the contact from the global directory is ignored when the files are next uploaded.

As of UC Software 5.4.0 and later, the phone requests both the per-phone <MACaddress>-directory.xml and global contact directory 000000000000-directory.xml files and merges them for presentation to the user. If you created a per-phone <MACaddress>-directory.xml for a phone, and you want to use the 000000000000-directory.xml file, add the 000000000000-directory.xml file to the provisioning server and update the phone's configuration.

> You can duplicate contacts in the Contact Directory on phones registered with the GENBAND server.

> Note: To avoid users accidentally deleting the definitions in the contact directory, make the contact directory file read only.

Speed Dials

You can link entries in the local contact directory to speed dial contacts to line keys on the Home or Lines screen to enable users to place calls quickly using dedicated speed dial buttons. To set up speed dial through the phone's contact directory, refer to Local Contact Directory.

Speed Dial Index Range

You can assign contacts as speed dials using the speed dial index ranges listed in the following table.

Speed Dial Index Ranges

Phone Model	Range
VVX 101, 201	1 – 99
VVX 300 series, 400 series, 500 series, and 600 series	1 – 500
VVX 1500	1 – 9999 The maximum number may be limited by the phone's available memory.
SoundStructure VoIP Interface	Not applicable.

Speed Dial Parameters

After setting up you per-phone directory file (***<MACaddress>-*directory.xml),** enter a number in the speed dial `<sd>` field to display a contact directory entry as a speed dial contact on the phone. Speed dial entries automatically display on unused line keys on the phone and are assigned in numerical order. Refer to Local Contact Directory.

Note that on some call servers, enabling presence for an active speed dial contact displays that contact's status on the speed dial's line key label.

Use the parameters in the following table, which identifies the directory XML file and the parameters you need to set up your speed dial contacts.

Configure the Speed Dial Feature

Parameter Function	**template** > parameter
Enter a speed dial index number in the <sd>x</sd> element in the <MAC address>-directory.xml file to display a contact directory entry as a speed dial key on the phone. Speed dial contacts are assigned to unused line keys and to entries in the phone's speed dial list in numerical order.	
The template contact directory file.	000000000000-directory~.xml

Corporate Directory

You can connect phones to a corporate directory server that supports the Lightweight Directory Access Protocol (LDAP), version 3. After you set up the corporate directory on the phones, users can search for contacts in the directory, place calls to directory contacts, and save entries to the local contact directory on the phone.

Polycom phones currently support the following LDAP servers:

- 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

Polycom phones also support corporate directories that support server-side sorting and those that do not. For servers that do not support server-side sorting, sorting is performed on the phone.

> Note: Polycom recommends using corporate directories that have server-side sorting for better performance. Consult your LDAP administrator when making any configuration changes for the corporate directory. For more information on LDAP attributes, see *RFC 4510 - Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*.

Related Topics

Corporate Directory Parameters

Call Logs

The phone records and maintains user phone events to a call log, which contains call information such as remote party identification, time and date of the call, and call duration. The log is stored on the provisioning server as an XML file named **<*MACaddress*>-calls.xml**. If you want to route the call logs to another server, use the `CALL_LISTS_DIRECTORY` field in the master configuration file. All call logs are enabled by default.

The phones automatically maintain the call log in three separate call lists that users can access: Missed Calls, Received Calls, and Placed Calls. Users can clear lists manually on their phones, or delete individual records or all records in a group (for example, all missed calls).

Related Topics

Call Log Parameters

Call Log Elements and Attributes

The following table describes each element and attribute that displays in the call log. You can place the elements and attributes in any order in your configuration file.

Call Log Elements and Attributes

Element	Permitted Values
direction	In, Out
Call direction with respect to the user.	
disposition	Busy, Forwarded, Normal, Partial, Preempted, Rejected, RemotelyHandled, Transferred
Indicates what happened to the call. When a call entry is first created, the disposition is set to Partial.	
line	Positive integer
The line (or registration) index.	

Call Log Elements and Attributes

protocol	SIP or H323
The line protocol.	
startTime	String
The start time of the call. For example: 2010-01-05T12:38:05 in local time.	
duration	String
The duration of the call, beginning when it is connected and ending when the call is terminated. For example: `PT1H10M59S`.	
count	Positive Integer
The number of consecutive missed and abandoned calls from a call destination.	
destination	Address
The original destination of the call. For outgoing calls, this parameter designates the outgoing call destination; the name is initially supplied by the local phone (from the name field of a local contact entry) but may later be updated via call signaling. This field should be used for basic redial scenarios. For incoming calls, the called destination identifies the requested party, which may be different than any of the parties that are eventually connected (the destination may indicate a SIP URI which is different from any SIP URI assigned to any lines on the phone).	
source	Address
The source of the call (caller ID from the call recipient's perspective).	
Connection	Address
An array of connected parties in chronological order. As a call progresses, the connected party at the far end may change, for example, if the far end transfers the call to someone else. The connected element allows the progression of connected parties, when known, to be saved for later use. All calls that contain a connected state must have at least one connection element created.	
finalDestination	Address
The final connected party of a call that has been forwarded or transferred to a third party.	

Microsoft Exchange Integration

Exchange Integration is available for Skype for Business, Office 365, and Lync Server 2010 and 2013 deployments. This feature enables set up of visual voicemail, call log synchronization, Outlook contact search, and Skype for Business Address Book Service (ABS) adaptive search. Each of these features is enabled by default on Polycom phones registered with Skype for Business.

> Note: If your Polycom phones are configured with G.722 and users find that they do not hear audio when retrieving voicemail from the Microsoft Skype for Business Server, you need to make the following changes to parameters in the site.cfg template file:
> * Change `voice.codecPref.G7221.24kbps` from 0 to 5.
> * Change `voice.codecPref.G7221.32kbps` from 5 to 0.
>
> Add `voice.audioProfile.G7221.24kbps.payloadType` and set it to 112.

After the phone is connected, you can:

* Verify which Exchange Server services are not working on each phone by going to **Status > Diagnostics > Warnings** on the phone.
* View the status of each service in the Web Configuration Utility.

Enabling Microsoft Exchange Integration

You can enable Exchange integration using one of the following methods:

* As of UC Software 5.3.0, Polycom phones support Exchange Server auto-discover.
* Centralized provisioning.
* On a per-phone basis with the Web Configuration Utility.
* When using a UC Software release prior to 5.3.0, you can enable the exchange calendar using centralized provisioning or with the Web Configuration Utility. Note that the Web Configuration is disabled by default when the phone is registered with Skype for Business and you must enable it.

> Note: If you enter sign-in credentials to the configuration file, phone users must enter credentials to the phone Sign In screen.

Enable Microsoft Exchange Calendar Using Centralized Provisioning

You have the option to enable Skype for Business Exchange calendar using the following parameters on your central provisioning server.

To enable the exchange calendar from a provisioning server:

1   Add the following parameter to one of your configuration files:
    ➢ `feature.exchangeCalendar.enabled=1`
    ➢ `exchange.server.url=https://<example URL>`

Enable Microsoft Exchange Calendar Using the Web Configuration Utility

You have the option to use the Web Configuration Utility to manually enable Skye for Business Exchange Calendar. This is useful for troubleshooting if auto-discovery is not working or misconfigured. This method applies only to a single phone at a time.

To enable the exchange calendar manually:

1 Enable access to the Web Configuration Utility if the phone is registered with Skype for Business.

2 Log in to the Web Configuration Utility as Admin (default password 456).

3 Go to **Settings > Applications > Exchange Applications**, and expand **Exchange Applications**, as shown next.

4 In the **Exchange Calendar** field, select **Enable**.

5 Enter the exchange web services URL using a Microsoft Exchange Server URL, for example `https://<mail.com>/ews/exchange.asmx`. In this example, the URL part `<mail.com>` is specific to an organization

6 At the bottom of the browser page, click **Save**.

7 When the confirmation dialog displays, click **Yes**.

Your Exchange Calendar is successfully configured and the Calendar icon displays on your phone screen.

Setting Up Calendar Features

Take note of the following when setting up calendar features.

> Web Info: For help with Lync Server 2010, refer to Microsoft Configure Exchange Services for the Autodiscover Service.
> For help with Lync Server 2013, refer to Microsoft Configuring Unified Messaging on Microsoft Exchange Server to work with Lync Server 2013.

● Visual voicemail. On the server, enable unified messaging and enable messages to play on the phone for each user. If you disable `feature.exchangeVoiceMail.enabled`, the Message Center and Skype for Business Voice mail menus display the message. Skype for Business Server only plays voicemail and you cannot download voicemails or play locally on the phone.

● Call log synchronization. On the server, enable the option to save calls logs to each user's conversation history in Outlook.

● ABS adaptive search. On the server, enable the ABS service. There are three possible configurations.

  ➢ Outlook and ABS are both enabled by default. When both are enabled, the phone displays the Skype for Business Directory.

  ➢ If you disable Outlook and enable only ABS, the phone displays the Skype for Business Directory.

  ➢ If you enable Outlook and disable ABS, the Outlook Contact Search displays in Directories.

Related Topics

Microsoft Exchange Integration Parameters

Call Controls

This section shows you how to configure call control features.

Microphone Mute

All phones have a microphone mute button. By default, when you activate microphone mute, a red LED glows or a mute icon displays on the phone screen, depending on the phone model you are using.

You cannot configure the microphone mute feature.

Persistent Microphone Mute

With this feature, you can enable the microphone mute to persist across all calls managed on a phone. By default, users can mute the microphone during an active call, and the microphone is unmuted when the active call ends. With persistent microphone mute enabled, when a user mutes the microphone during an active call, the microphone remains muted for all following calls until the user unmutes the microphone or the phone restarts.

\When a user mutes the microphone when the phone is idle, the mute LED glows but no icon displays on the screen. When a user initiates a new active call with the microphone muted, the mute LED glows and a Mute icon displays on the phone screen.

Related Topics

Persistent Microphone Mute Parameters

Call Timer

By default, a call timer displays on the phone's screen during calls, and a separate call duration timer displays the hours, minutes, and seconds for each call in progress.

You cannot configure the display of the call timer.

Called Party Identification

By default, the phone displays and logs the identity of all parties called from the phone. The phone obtains called party identities from network signaling. Because called party identification is a default feature, the phone displays caller IDs matched to the call server and does not match IDs to entries in the contact directory or corporate directory.

Connected Party Identification

By default, the phone displays and logs the identities of remote parties you connect to if the call server can derive the name and ID from network signaling. In cases where remote parties have set up certain call features, the remote party you connect to—and the caller ID that displays on the phone—may be different than the intended party's. For example, Bob places a call to Alice, but Alice has call diversion configured to divert Bob's incoming calls to Fred. In this case, the phone logs and displays the connection between Bob and Fred. The phone does not match party IDs to entries in the contact directory or the corporate directory.

Calling Party Identification

By default, the phone displays the identity of incoming callers if available to the phone through the network signal. If the incoming call address has been assigned to the contact directory, you can enable the phones to display the name assigned to contacts in the contact directory. However, the phone cannot match the identity of calling parties to entries in the corporate directory.

Related Topics

Calling Party Identification Parameters

Remote Party Caller ID from SIP Messages

You can specify which SIP request and response messages to use to retrieve caller ID information.

Related Topics

Remote Party Caller ID from SIP Messages Parameters

Connected Line Identification

You can view the identity of the callee on the caller's phone screen. If the contact details are stored on your phone, the saved contact name and number will be displayed.

Calling Line Identification

The Calling Line Identity Presentation (CLIP) displays the phone number of the caller on the phone screen.

Related Topics

Calling Line Identification Parameters

SIP Header Warnings

You can configure the warning field from a SIP header to display a pop-up message on the phone, for example, when a call transfer failed due to an invalid extension number. You can display pop-up messages

in any language supported by the phone. The messages display for three seconds unless overridden by another message or action.

For a list of supported SIP header warnings, see the article 'Supported SIP Request Headers' in Polycom Knowledge Base.

Related Topics

SIP Header Warning Parameters

Accessing URLs in SIP Messages

When this feature is enabled, the server attaches a URL to incoming and active calls. The web browser or microbrowser can read this URL and present it as web content that displays on the phone screen. This feature is supported on VVX 500/501 and 1500 phones.

This feature is flexible and can be used in some of the following ways:

● In a Call Center environment, the phone displays extended information about a customer before the agent takes the call. The phone can also display a script of questions for the agent to ask during the call.

● In a hotel, a guest can view the restaurant menu on the phone.

Related Topics

Access URL in SIP Messages Parameters

Distinctive Incoming Call Treatment

You can apply distinctive treatment to specific calls and contacts in the contact directory. You can set up distinctive treatment for each of your contacts by specifying a Divert Contact, enabling Auto-Reject, or enabling Auto-Divert for a specific contact in the local contact directory. You can also apply distinctive treatment to calls and contacts through the phone's user interface.

If you enable both the auto divert and auto reject features, auto divert has precedence over auto reject.

Distinctive Call Waiting

You can use the alert-info values and class fields in the SIP header to map calls to distinct call-waiting types. You can apply three call waiting types: beep, ring, and silent. The following table shows you the parameters you can configure for this feature. This feature requires call server support.

Related Topics

Distinctive Call Waiting Parameters

Presence Status

You can enable users to monitor the status of other remote users and phones. By adding remote users to a buddy list, users can monitor changes in the status of remote users in real time or they can monitor remote users as speed-dial contacts. Users can also manually specify their status in order to override or mask automatic status updates to others and can receive notifications when the status of a remote line changes.

Polycom phones support a maximum of 64 buddies for Open SIP server platforms and 200 contacts on the Skype for Business server. For information on Skype for Business contacts, refer to the *Polycom UC Software with Skype for Business - Deployment Guide* on Polycom Voice Support.

Related Topics

Presence Status Parameters

Do Not Disturb

You can enable Do Not Disturb (DND) locally on the phone or on the server. The local DND feature is enabled by default, and users can enable or disable DND for all or individual registered lines on the phone. When enabled, users are not notified of incoming calls placed to their line.

Server-Based Do Not Disturb

If you want to enable server-based DND, you must enable the feature on both a registered phone and on the server. The following conditions apply for server-based DND:

● Server-based DND can be applied to multiple registered lines on a phone; however, applying DND to individual registrations is not supported.

● Server-based DND cannot be enabled on a phone configured as a shared line.

● If server-based DND is enabled but not turned on when the DND feature is enabled on the phone, the "Do Not Disturb" message displays on the phone, but incoming calls continue to ring.

● Server-based DND disables local Call Forward and DND, however, if an incoming is not routed through the server, an audio alert still plays on the phone.

Related Topics

Do Not Disturb Parameters

Remote Party Disconnect Alert Tone

Remote Party Disconnect Alert Tone alerts users when the call has been disconnected by a remote party or network. When a remote party or network on an active call gets disconnected, an alert is played to notify the user about the lost connection. The tone is played only for an active call.

Related Topics

Remote Party Disconnect Alert Tone Parameters

Call Waiting Alerts

By default, the phone alerts users to incoming calls while a user is in an active call. You can choose to disable these call waiting alerts and specify ringtones for incoming calls. In addition, you can configure the phone to display the **Call Waiting** menu under the **Preferences** option on the phone.

Related Topics

Call Waiting Alert Parameters

Missed Call Notifications

By default, a counter with the number of missed calls displays on the Recent Calls icon on the phone. You can configure the phone to record all missed calls or to display only missed calls that arrive through the SIP server. You can also enable missed call notifications for each registered line on a phone.

Related Topics

Missed Call Notification Parameters

Last Call Return

The phone supports redialing the last received call. This feature requires 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. When enabled, the phone displays an LCR soft key that users can select to place a call to the phone address that last called them.

Related Topics

Last Call Return Parameters

Call Hold

Call hold enables users to pause activity on an active call so that they can use the phone for another task, such as searching the phone's menu for information. When an active call is placed on hold, a message displays informing the held party that they are on hold.

If supported by the call server, you can enter a music-on-hold URI. For more information, see RFC Music on Hold draft-worley-service-example.

Related Topics

BroadSoft Server-Based Redial Parameters

Hold Implementation

The phone supports two currently accepted means of signaling hold. The phone can be configured to use either hold signaling method. The phone supports both methods when signaled by the remote endpoint.

Supported Hold Methods

Method	Notes
Signal the media directions with the "a" SDP media attributes sendonly, recvonly, inactive, or sendrecv.	Preferred method.
Set the "c" destination addresses for the zmedia streams in the SDP to zero. For example, c=0.0.0.0	No longer recommended due to RTCP problems associated with this method. Receiving sendrecv, sendonly, or inactive from the server causes the phone to revert to the other hold method.

Call Park and Retrieve

This feature enables users to park an active call on a separate call orbit and retrieve parked calls from the call orbit on any phone. Whereas call hold keeps the held call on the same line, call park moves the call to a separate address where the call can be retrieved by any phone. This feature requires support from a SIP server and setup of this feature depends on the SIP server. For example, while some SIP servers implement group call pick-up using a particular star-code sequence, others implement the feature using network signaling.

Related Topics

Call Park and Retrieve Parameters

Call Transfer

The call transfer feature enables users to transfer an existing active call to a third-party address. You can configure the call transfer feature and set the default transfer type.

Users can perform the following types of call transfers:

● **Blind Transfer**—Users complete a call transfer without speaking with the other party first.

● **Consultative Transfer**—Users speak with the other party before completing the transfer.

By default, users can complete a call transfer without waiting for the other party to answer the call first, which is a Blind Transfer. In this case, Party A can transfer Party B's call to Party C before Party C answers the transferred call. You can disable the blind transfer feature so that users must wait for the other party to answer before completing the transfer.

Related Topics

Call Transfer Parameters

Call Forwarding

Polycom phones support a flexible call forwarding feature that enables users to forward incoming calls to another contact or phone line. Users can enable call forwarding in the following ways:

● To all calls

● To incoming calls from a specific caller or extension

● During an incoming call

● When the phone is busy

● When do not disturb is enabled

● After a set number of rings before the call is answered

● To a predefined destination chosen by the user

If you are registering phones with the Skype for Business Server, the following call forwarding options are available on Skype for Business-enabled phones:

● Forward to a contact

● Forward to voicemail

● Forward to Delegates

● Simultaneously Ring Delegates

● Simultaneously Ring Group Contacts

Server-Based Call Forwarding

To enable server-based call forwarding, you must enable the feature on both the server and the registered phone. If you enable server-based call forwarding on one registration, other registrations are not affected.

The following conditions apply for server-based call forwarding:

● If server-based call forwarding is enabled, but inactive, when a user presses the Forward soft key, the 'moving arrow' icon does not display on the phone and incoming calls are not forwarded.

The call server uses the Diversion field with a SIP header to inform the phone of a call's history. For example, when you enable call forwarding, the Diversion header allows the receiving phone to indicate who the call was from, and the phone number it was forwarded from.

Call Forward on Shared Lines

You can enable server-based call forwarding for shared lines. If using BroadWorks R20 server, note the following:

● Local call-forwarding is not supported on shared lines.

● Dynamic call forwarding—forwarding incoming calls without answering the call—is not supported.

> Note: The server-based and local call forwarding features do not work with the shared call appearance (SCA) and bridged line appearance (BLA) features. In order to enable users to use call forwarding, disable SCA or BLA enabled.

Related Topics

Call Forwarding Parameters

Automatic Off-Hook Call Placement

You can configure the phone to automatically place a call to a specified number when the phone goes off-hook, which is sometimes referred to as Hot Dialing. The phone goes off-hook when a user lifts the handset, selects New Call, or presses the headset or speakerphone buttons on the phone.

Related Topics

Automatic Off-Hook Call Placement Parameters

Directed Call Pickup

Directed call pickup enables users to pick up incoming calls to another phone by dialing the extension of that phone. This feature requires support from a SIP server and setup of this feature depends on the SIP server. For example, while some SIP servers implement directed call pick-up using a star-code sequence, others implement the feature using network signaling.

Related Topics

Directed Call Pickup Parameters

Group Call Pickup

This feature enables users to pick up incoming calls to any phone within a predefined group of phones, without dialing the extension of another phone.

Related Topics

Group Call Pickup Parameters

Multiple Line Registrations

Polycom phones can have multiple line registrations. Each registration requires an address or phone number. Phones registered with Microsoft Skype for Business Server support only one Skype for Business registration.

When multiple registrations are available, users can select which registration to use for certain features, including which registration to use for outgoing calls or when initiating new instant messages.

Maximum Number of Registrations

The maximum number of registrations vary by phone and are listed in the following table.

In addition to the maximum registrations listed in the table, you can also add up to three VVX Expansion Modules to a single VVX 300 series, 400 series, 500 series, or 600 series phone to increase the total number of registrations to 34. For more information, see Polycom VVX Expansion Modules.

Maximum Number of Registrations Per Phone

Phone Model Name	Maximum Registrations
VVX 101	One (1)
VVX 201	Two (2)
VVX 300/301/310/311	Thirty four (34)
VVX 400/401/410/411	Thirty four (34)
VVX 500/501	Thirty four (34)
VVX 600/601	Thirty four (34)
VVX 1500	Twenty four (24)

Related Topics

Multiple Line Registrations Parameters

Multiple Line Keys Per Registration

You can assign a single registered phone line address to multiple line keys on Polycom phones. This feature can be useful for managing a high volume of calls to a single line. This feature is not supported when registered with Microsoft Skype for Business Server.

Related Topics

Multiple Line Keys Per Registration Parameters

Multiple Call Appearances

You can enable each registered phone line to support multiple concurrent calls and have each concurrent call display on the phone's user interface. For example, with multiple call appearances, users can place one call on hold, switch to another call on the same registered line, and have both calls display on the phone.

This feature is one of several features associated with flexible call appearances. If you want to enable multiple line keys per registration, see the section Multiple Line Keys Per Registration. If you assign a registered line to multiple line keys, the default number of concurrent calls applies to all line keys.

Related Topics

Multiple Call Appearance Parameters

Flexible Call Appearances

A number of features are associated with flexible call appearances, including Multiple Line Registrations, Multiple Line Keys Per Registration, and Multiple Call Appearances. Use the following table to understand how you can organize registrations, line keys per registration, and concurrent calls per line key.

The following table includes the following types of call appearances:

- **Registrations**—The maximum number of user registrations
- **Line Keys**—The maximum number of line keys
- **Line Keys Per Registration**—The maximum number of line keys per user registration
- **Calls Per Line Key**—The maximum number of concurrent calls per line key
- **Concurrent Calls (including Conference Legs)**—The runtime maximum number of concurrent calls, and the number of conference participants minus the conference initiator.

Flexible Call Appearances

Phone Model	Registrations	Line Keys	Line keys Per Registration	Calls Per Line Key	Concurrent Calls*
VVX 101, 201	1	2	2	8	8 (2)
VVX 300/301/310/311	34	48	48	24	24 (2)
VVX 400/401/410/411	34	48	48	24	24 (2)
VVX 500/501	34	48	48	24	24 (2)
VVX 600/601	34	48	48	24	24 (2)
VVX 1500	24	24	24	24	24 (2)
SoundStructure VOIP Interface **	12	12	12	24	24 (2)

* Note that each conference leg counts as one call. The total number of concurrent calls in a conference indicated in this table includes all conference participants minus the moderator.

** For more information on using line and call appearances with the SoundStructure VOIP Interface, refer to the SoundStructure Design Guide, available at Polycom Support.

Bridged Line Appearance

Bridged line appearance connects calls and lines to multiple phones. With bridged line appearance enabled, an active call displays simultaneously on multiple phones in a group. By default, the answering phone has sole access to the incoming call, which is called line seize. If the answering phone places the call on hold, that call becomes available to all phones of that group. All call states—active, inactive, on hold—are displayed on all phones of a group.

> Important: Shared call appearances and bridged line appearances are similar signaling methods that enable more than one phone to share the same line or registration. The methods you use vary with the SIP call server you are using. In the configuration files, bridged lines are configured by shared line parameters. The barge-in feature is not available with bridged line appearances; it is available only with shared call appearances.

Bridged Line Appearance Signaling

A bridged line is an address of record managed by a server. The server allows multiple endpoints 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 event used is 'dialog' for bridged line appearance subscribe and notify.

Related Topics

Bridged Line Appearance Parameters

Voicemail

When you configure Polycom phones with a SIP URL that integrates with a voicemail server contact, users receive a visual and audio alert when they have new voicemail messages available on their phone.

Related Topics

Voicemail Parameters

Local Call Recording

Local call recording enables you to record audio calls to a USB device connected to the phone. You can play back recorded audio on the phone or devices that run applications like Windows Media Player® or iTunes® on a Windows® or Apple® computer. To use this feature, ensure that the USB port is enabled.

Audio calls are recorded in **.wav** format and include a date/time stamp. The phone displays the recording time remaining on the attached USB device, and users can browse all recorded files using the phone's menu.

> Important: Federal, state, and/or local laws may legally require that you notify some or all of the call parties when a call recording is in progress.

This feature is available on the following phones:

- VVX 401/411
- VVX 5xx series
- VVX 6xx series
- VVX 1500

> For a list of supported USB devices, see *Technical Bulletin 38084: Supported USB Devices for Polycom SoundPoint IP 650 and VVX Phones* at Polycom Engineering Advisories and Technical Notifications.

Related Topics

Local Call Recording Parameters

Centralized Call Recording

This feature enables users to record audio and video calls and control call recording directly from phones registered with BroadSoft BroadWorks r20 server. Users can manage recorded audio and video files on a third-party call recording server.

By default, far-side participants are not alerted when calls are being recorded. The BroadWorks r20server provides administrators with the option to enable an announcement to play at the beginning of a call when a call is being recorded. If a call recorded is in progress when the call is transferred, the recording continues for the new call.

> ⚠️ You can record calls using a central server or locally using the phone's USB call recording feature – you cannot use both at the same time. By default, both features are disabled. If you enable one call recording feature, ensure that the other is disabled. Use either centralized or the local call recording; do not use both.

Related Topics

Centralized Call Recording Parameters

Call Recording Modes

Set the call recording modes on the BroadSoft BroadWorks R20 server using the following call recording modes:

● **Never Mode**   Call recording is never initiated and the phone never displays call recording soft keys.

● **Always Mode**   The entire incoming or outgoing call is recorded and no control options are available to users. During active calls, the phone displays a Record symbol. Call recording stops when the call ends and the call is stored on the server.

● **Always with Pause/Resume Support Mode**   Call recording starts automatically when the call connects and the Pause and Resume soft key are available. The phone display indicates the status of the call recording state. Call recording stops when the call ends and the recorded part of the call is stored on the server.

● **On Demand Mode**   Call recording starts on the server when the call connects, but the recorded file is not saved until the user initiates the recording. When the user presses the Start soft key, the recording is saved to the server and the phone displays the Pause and Resume soft keys.

● **On Demand Mode with User-Initiated Start Mode**   Call recording does not begin automatically and a Record soft key displays. If users want to record an active call, they need to press **Record > Start** to start recording and save the recording to the server. While recording, the phone displays the Pause, Resume, and Stop soft keys.

● **Recording two separate calls and creating a conference**   This mode enables users to record two participants as separate call sessions when connected in a conference call. The server stores the conference call as two separate recording sessions.

Busy Lamp Field (BLF)

The Busy Lamp Field (BLF) feature enables the following functions to the users:

- Monitor the status of lines on remote phones
- Display remote party information
- Answer incoming calls to remote phones (called directed call pickup)
- Park and retrieve calls

When BLF is enabled, a BLF line key icon displays on the phone screen for users monitoring remote phones. The BLF line key displayed indicates that BLF related features are available.

BLF Types

VVX business media phones support the following types of BLF:

- A basic version of BLF, available on VVX 1500, enables users to be monitored and to monitor idle and active phone states. The basic version of BLF enables VVX 1500 phones registered to users to fully monitor other VVX 1500 phones. However, VVX 1500 phones monitoring other VVX phones are notified of the idle and active states of monitored phones only, and are not notified of incoming calls to the monitored phones.
- An enhanced BLF, not supported on VVX 1500, notifies users of all states of monitored phones, including the active, idle, and ringing states.

Note that BLF is not available with Polycom phones registered with Skype for Business Server.

BLF Icons

The following table shows the BLF key icons that display on the phone.

BLF Line Key Icons

States	Line Icons
Monitored line is idle	
Monitored line is busy	
Monitored line is ringing	

 For information on how to manage calls to monitored phones, see the section "Handling Remote Calls on Attendant Phones" in *Technical Bulletin 62475: Using Statically Configured Busy Lamp Field with Polycom SoundPoint IP and VVX Phones* at Polycom Engineering Advisories and Technical Notifications.

BLF Feature Options

The BLF feature must be supported by a call server and the specific functions vary with the call server you use. You may need to consult your SIP server partner or Polycom channel partner to find out how to configure BLF feature options.

You can configure the following feature options for BLF:

- Line key labels
- Enhanced feature keys
- Call appearances display
- Call waiting audio notifications
- Caller ID information display
- One-touch call park and retrieve
- One-touch directed call pickup

BLF Configuration Methods

Typically, call servers support one of two methods of BLF configuration. Using the first method, you subscribe to a BLF resource list that is set up on your call server. Using the second method, you enter BLF resources to a configuration file and the call server directs the requests to those BLF resources. If you are unsure which method to use, consult your SIP server partner or Polycom Channel partner. This section shows you how to set up BLF using both methods.

Use this feature with TCPpreferred transport (see <server/>). When using BLF with BroadSoft, the initial subscription to BLF can receive very large responses as the number of monitored resources increases. This requires packet fragmentation which may be unreliable in its transmission across the network. In such cases, it is recommended to use TCP for BLF either by changing all SIP services to TCP or by adding the TCP transport attribute to your attendant.uri parameter.

For example:attendant.uri=1234blf@example

BLF Resource List Subscription on a Call Server

To subscribe to a BLF list on a call server, you must access the call server and set up a list of monitored resources. The call server provides you with an address for that BLF resource list. To subscribe to that list, enter the address and any other information specific to your call server in the `attendant.uri` field located in the **features.cfg** template file.
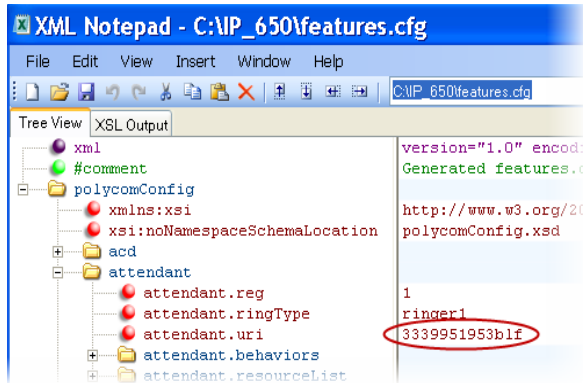
BLF Resource Specification in the Configuration File

To specify BLF resources in the configuration file, use the **features.cfg** template file and enter the address (phone number) of the BLF resource of the monitored contact, the label that displays beside the line key on the phone, and the type of resource being monitored. Multiple registrations are available for a single SIP server. Your call server must support dialog even package defined in RFC 4235 in order to configure BLF using this method. In the following example, the phone is monitoring *Craig Blunt* and *Lucy Patterson.*
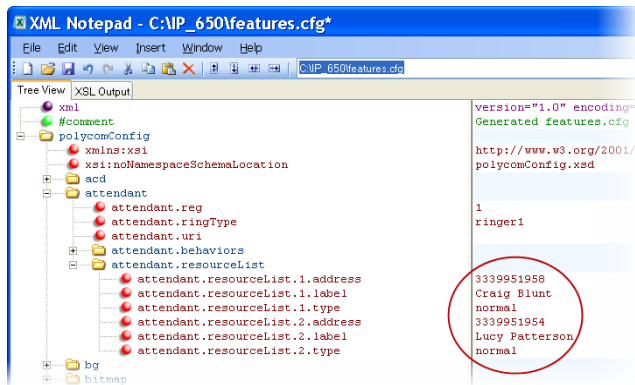
Specifying the type of monitored resource as `normal` or `automata` changes the default actions of key presses. Enter `normal` as the resource type if the monitored resource type is a phone and `automata` as the resource type if the monitored resource type is, for example, a call orbit. If you select `normal`, pressing the BLF line key places an active call on hold before dialing the selected BLF phone. If you select `automata`, pressing the BLF line key immediately transfers active calls to that resource. To learn how to configure a park orbit and for examples, refer to the section Enhanced Feature Keys.

Related Topics

Busy Lamp Field Configuration Parameters

Instant Messaging

All VVX business media phones can send and receive instant text messages. When instant messaging is enabled, the phone's message waiting indicator (MWI) visually alerts users new instant messages; you can also set audio alerts.

Support for Instant Messaging varies by call server. Consult your SIP server partner to find out if this feature is supported. Instant Messaging is not with Skype for Business.

Related Topics

Instant Messaging Parameters

Local and Centralized Conference Calls

You can set up local or centralized audio and video conferences for VVX business media phones. Local conferences require a host phone to process the audio and video of all parties. Alternatively, users can use an external audio bridge, available via a central server, to create a centralized conference call. All Polycom phones support local- and server-based centralized conferencing. Polycom recommends using centralized conferencing for conferences with four or more parties. The availability of centralized conferencing and features can vary by the call platform you use.

VVX business media phones and SoundStructure VoIP Interface support a maximum of three participants in local conference calling.

Related Topics

Local and Centralized Conference Call Parameters

Conference Management

This feature enables users to add, hold, mute, and remove conference participants, as well as obtain additional information about participants. VVX phone users can also choose which conference call participants to exchange video with.

When you enable conference management, a **Manage** soft key displays on the phone during a conference, and users can use the soft key to access conference management options.

Related Topics

Conference Management Parameters

Local Digit Map

The local digit map feature allows the phone to automatically call a dialed number when configured. Note that digit maps do not apply to on-hook dialing.

Digit maps are defined by a single string or a list of strings. If a dialed number matches any string of a digit map, the call is automatically placed. If a dialed number matches no string—an impossible match—you can

specify the phone's behavior. If a number ends with #, you can specify the phone's behavior, called trailing # behavior. You can also specify the digit map timeout, the period of time after you dial a number that the call is placed. The configuration syntax of the digit map is based on recommendations in section 2.1.5 of RFC 3435.

> For instructions on how to modify the local digit map, see *Technical Bulletin 11572: Changes to Local Digit Maps on SoundPoint IP, SoundStation IP, and Polycom VVX 1500 Phones* at Polycom Engineering Advisories and Technical Notifications.

Related Topics

Local Digit Maps Parameters

Open SIP Digit Map

If you are using a list of strings, each string in the list can be specified as a set of digits or timers, or as an expression which the gateway uses to find the shortest possible match.

The following is a list of digit map string rules for open SIP environments.

- The following letters are case sensitive: *x*, *T*, *R*, *S*, and *H*.
- You must use only *, #, +, or 0–9 between the second and third *R*.
- If a digit map does not comply, it is not included in the digit plan as a valid map. That is, no match is made.
- There is no limit to the number of R triplet sets in a digit map. However, a digit map that contains less than a full number of triplet sets (for example, a total of 2 Rs or 5 Rs) is considered an invalid digit map.
- Digit map extension letter R indicates that certain matched strings are replaced. Using a *RRR* syntax, you can replace the digits between the first two *Rs* with the digits between the last two *Rs*. For example, *R555R604R* would replace 555 with 604. 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.
- If you use T in the left part of *RRR's* syntax, the digit map will not work. For example, *R0TR322R* will not work.

The following examples illustrate the semantics of the syntax:

- `R9R604Rxxxxxxx`—Replaces *9* with *604*
- `xxR601R600Rxx`—When applied to *1160122* gives *1160022*
- `R9RRxxxxxxx`—Remove *9* at the beginning of the dialed number (replace 9 with nothing)
  - ➢ 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 (replace nothing with *604*)
  - ➢ For example, if a customer dials *4539400*, *604* is added to the front of the number, so a call to 6044539400 is placed.
- `xR60xR600Rxxxxxxx`—Replace any 60x 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 (.) that 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.

> Only VVX 500/510, 600/611, and 1500 phones support the H. On all other phones, the H is ignored and users need to perform the Send operation 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 is placed after the user dials the last digit.

Generating Secondary Dial Tone with Digit Maps

You can regenerate a dial tone by adding a comma "**,**" to the digit map. You can dial seven-digit numbers after dialing "8" as shown next in the example rule `8,[2-9]xxxxxxT`:

```
[2-9]11|0T|011xxx.T|[0-1][2-9]xxxxxxxxx|8,[2-9]xxxxxxT|[2-9]xx.T
```

By adding the digit "8", the dial tone plays again, and users can complete the remaining seven-digit number. In this example, if users also have a 4-digit extension that begins with "8", then users will hear dial tone after the first "8" was dialed because "8" matches the "8" in the digit map.

If you want to generate dial tone without the need to send the "8", replace one string with another using the special character "R" as shown next in the rule **R8RR**. In the following example, replace "8" with an empty string to dial the seven-digit number:

```
[2-9]11|0T|011xxx.T|[0-1][2-9]xxxxxxxxx|R8RR,[2-9]xxxxxxT|[2-9]xx.T
```

Shared Lines

Shared Call Appearances

Shared call appearance enables an active call to display simultaneously on multiple phones in a group. All call states of a call—active, inactive, on hold—are displayed on all phones of a group.

By default, the answering phone has sole access to the incoming call, which is called line seize. If the answering phone places the call on hold, that call becomes available for pickup to all phones in that group. You can enable other phones in the group the ability to enter a conversation on one of the group phones, which is referred to as a barge in.

> Note: Shared call appearances and bridged line appearances are similar signaling methods that enable more than one phone to share the same line or registration. The method you use varies with the SIP call server you are using.

Related Topics

Shared Call Appearances Parameters

Shared Call Appearance Signaling

A shared line is an address of record managed by a call server. The server allows multiple endpoints to register locations against the address of record.

Polycom devices support Shared Call Appearance (SCA) using the SUBSCRIBE-NOTIFY method specified in RFC 6665. The events used are:

- *call-info* for call appearance state notification
- *line-seize* for the phone to ask to seize the line

Private Hold on Shared Lines

Enable the private hold feature to enable users to hold calls without notifying other phones registered with the shared line. When you enable the feature, users can hold a call, transfer a call, or initiate a conference call and the shared line displays as busy to others sharing the line.

Related Topics

Private Hold on Shared Lines Parameters

Intercom Calls

The Intercom feature enables users to place an intercom call that is answered automatically on the dialed contact's phone. This is a server-independent feature provided the server does not alter the Alert-Info header sent in the INVITE.

Creating a Custom Intercom Soft Key

By default, an Intercom soft key displays on the phone, but you have the option to provide users the ability to initiate intercom calls directly to a specified contact using enhanced feature keys (EFKs). You do not need to disable the default Intercom soft key to create a custom soft key.

For information on configuring EFK functions, see the section Enhanced Feature Keys.

For example, you can create an intercom action string for a custom soft key in one of the following ways:

- $FIntercom$

  This is an F type macro that behaves as a custom Intercom soft key. Pressing the soft key opens the Intercom dial prompt users can use to place an Intercom call by entering the destination's digits and using a speed dial or BLF button.

- <number>$Tintercom$

  This is a T type macro that enables you to specify a Direct intercom button that always calls the number you specify in <number>. No other input is necessary.

Related Topics

Intercom Calls Parameters

Push-to-Talk

The push-to-talk (PTT) is a collaborative tool that enables users to exchange broadcasts to users subscribed to any of the 25 PTT channels, much like a walkie-talkie. Users can transmit pages and PTT broadcasts using their handset, headset, or speakerphone. PTT broadcasts can be received on the speakerphone, handset, and headset.

PTT mode is intended primarily for Wi-Fi phones. In PTT mode, the phone behaves like a walkie-talkie. Users can broadcast audio to a PTT channel and recipients subscribed to that channel can respond to messages.

You can specify the same IP multicast address in the parameter `ptt.address` for both PTT and group paging. Use the parameters in the following table to configure this feature.

> The push-to-talk and group paging features use an IP multicast address. If you want to change the default IP multicast address, ensure that the new address does not already have an official purpose as specified in the IPv4 Multicast Address Space Registry.

Related Topics

Push-to-Talk Parameters

Group Paging

The Group Paging feature is available on VVX business media phones and RealPresence Trio solution. Group Paging enables users to make pages —one-way audio announcements—to users subscribed to a page group. There are 25 groups/channels users can subscribe to. If you are using Group Paging with RealPresence Trio solution, you can only receive incoming pages. You cannot use RealPresence Trio solution to send outgoing pages.

Group paging users can send announcements to recipients subscribed to any of the 25 paging groups. Any announcements sent to the paging group play through the phone's speakerphone.

Administrators must enable paging before users can subscribe to a page group. You can specify the same IP multicast address in the parameter `ptt.address` for both PTT and paging mode.

> Web Info: The push-to-talk and group paging features use an IP multicast address. If you want to change the default IP multicast address, ensure that the new address does not already have an official purpose as specified in the IPv4 Multicast Address Space Registry.

Related Topics

Group Paging Parameters

Hoteling

The Hoteling feature enables users to log in to a guest profile to use any available shared phone. After logging in, users have access to their own guest profile and settings on the shared phone. When hoteling is enabled, the **Guest In** soft key displays for users to log in to the phone.

This feature is not supported on VVX 101 and 201 phones.

> For additional details on configuring the hoteling feature, see *Using Hoteling on Polycom Phones*: *Feature Profile 76554* at Polycom Engineering Advisories and Technical Notifications.

Related Topics

Hoteling Parameters

SIP-B Automatic Call Distribution

You can enable users to use VVX business media phones in a call center agent/supervisor role on a supported call server. This feature supports ACD agent availability, which depends on support from a SIP server.

You can view or hide the menu items on the Automatic Call Distribution (ACD) menus. You can configure the phone to hide or display the ACD soft keys such as **ASignIN** or **ASignOut**, and **Available**.

Related Topics

SIP-B Automatic Call Distribution Parameters

ACD Agent Availability Parameters

Feature-Synchronized Automatic Call Distribution (ACD)

Feature-synchronized automatic call distribution (ACD) assists organizations in handling a large number of incoming phone calls to a call center with users in agent/supervisor roles. Feature-synchronized ACD is distinct from and provides more advanced ACD functions than the Hoteling feature (see Hoteling). This feature is not supported on VVX 101 and 201 phones.

Feature-synchronized ACD is available in the following services.

- Standard—Standard service enables call center agents to sign in to a shared phone. When an agent is signed in, the phone displays the current state of the agent, for example, whether the agent is available or unavailable to take new calls.

- Premium—Premium service offers two additional features: *Hoteling* and *Queue Status Notification*.

  - ➢ Hoteling enables agents to use their agent credentials to log in to any available phone. If you want to enable the hoteling feature with feature-synchronized ACD, see the section Hoteling.

  - ➢ Queue status notification enables agents to view the queue status of a call center so that agents can adjust their call response.

The capabilities of this feature vary with the SIP call server. Consult your call server provider for information and for documentation. The SIP signaling used for this implementation is described in the BroadSoft BroadWorks document *Device Key Synchronization Requirements Document; Release R14 sp2; Document version 1.6*.

> For more information on standard and premium ACD as well as the hoteling and queue status notification enhancements, see *Feature Profile 76179: Using Premium Automatic Call Distribution for Call Centers* at Polycom Engineering Advisories and Technical Notifications.

Related Topics

Feature-Synchronized Automatic Call Distribution Parameters

Customize Devices

This section provides information on customizing Polycom phones.

Microbrowser and Web Browser

VVX business media phones support a full web browser and a microbrowser, also known as the idle browser. Note that the exact functions and performance of the microbrowser and web browser vary by phone model.

For more information on creating applications for the phones, see the P*olycom Web Application Developer's Guide* at Polycom UC Software Support Center.

> The browser restarts in the following situations:
> * The browser uses over 30MB of memory
> * The amount of free memory on the phone is below 6MB
> * The real time is between 1am to 5am.
> After the browser restarts, the last displayed web page is restored.

Related Topics

Microbrowser and Web Browser Parameters

Soft Keys

You can create custom soft keys on all VVX phones to enable users to access frequently used functions, create menu shortcuts to frequently used phone settings, or create a soft key in place of a hard key not available on the phone. For example, if the phone does not have a Do Not Disturb hard key, you can create a Do Not Disturb soft key.

You can create custom soft keys as any of the following:

* An enhanced feature key sequence (see Enhanced Feature Keys)
* A speed dial contact directory entry
* An enhanced feature key macro (see Macro Definitions)
* A URL
* A chained list of actions

Call State for Custom Soft Keys

You can configure soft keys to display certain functions depending on the phone's menu level or call state. For example, you can make a Call Park soft key available when the phone is in an active call state.

You can configure custom soft keys to display for 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 a 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.

Disabling Default Soft Keys

You can disable the display of any of the following default soft key to make room for custom soft keys:

- New Call
- End Call
- Split
- Join
- Forward
- Directories
- MyStatus and buddies
- Hold, transfer, and conference

Related Topics

Soft Key Parameters

Example Soft Key Configurations

This section provides a few examples of available soft key configurations to you can configure on the phones.

Example: Send-to-Voicemail Soft Key

Use the following example configuration to automatically transfer an active call to a BroadSoft voicemail. In this example, *55* is the star code for BroadSoft voicemail, and *8545* is the extension of the voicemail line the call transfers to. The exact star code to transfer the active call to voicemail depends on your call server.

Enabling the parameter `softkey.1.use.active` causes the soft key to display when a call becomes active on the line. When you press the soft key—labeled *VMail* in this example—the call is placed on hold and automatically transferred to a BroadSoft voicemail.

To map a send-to-voicemail enhanced feature key sequence to a soft key:

   1 Update the configuration file as follows:

> ➢ `softkey.1.label="VMail"`
> ➢ `softkey.1.action="$FTransfer$$Cpause1$$FDialpadStar$$FDialpad5$$FDialpad5$$FDialpad8$$FDialpad5$$FDialpad4$$FDialpad5$$FSoftKey1$"`
> ➢ `softkey.1.enable="1"`
> ➢ `softkey.1.use.active="1"`

   2 Reboot the phone.

      When an incoming call connects and becomes active, the **VMail** soft key displays.

Example: Send-to-Voicemail Prompt

Use the following example to enable users to enter a voicemail extension to transfer an active call to BroadSoft voicemail. In this example, **55* is the star code used for BroadSoft voicemail. The exact star code to transfer the active call to voicemail depends on your call server.

Enabling the parameter `softkey.1.use.active` causes the soft key to display when a call becomes active on the line. When a user presses the soft key, the call is placed on hold and a field prompts the user to enter the extension of a voicemail line to transfer the call to. The `efk.prompt*` parameters control the numeric prompt field users enter the extension into.

Note that this example works only on line 1 of the phone.

To create a send-to-voicemail prompt that allows a mailbox number entry:

   1 Update the configuration file as follows:

> ➢ `softkey.1.label="VMail"`
> ➢ `softkey.1.action="^*55$P1N10$$Tinvite$"`
> ➢ `softkey.1.enable="1"`
> ➢ `softkey.1.use.active="1"`
> ➢ `efk.efkprompt.1.label="Voice Mail"`
> ➢ `efk.efkprompt.1.status="1"`
> ➢ `efk.efkprompt.1.type="numeric"`

   2 Reboot the phone.

      When an incoming call connects and becomes active, the **VMail** soft key displays.

   3 Press the **VMail** soft key.

      A field displays prompting you to enter an extension.

   4 Enter the extension you want to transfer the call to.

   5 Press the **Enter** soft key.

Example: Speed Dial Soft Key with a Pause

Use the following example to configure a soft key to automatically dial a number with a pause in the dialing sequence. In this example, use `$CpauseX$` where `X` is the number of seconds to pause—7 in this example. Adding this pause function enables users to automatically dial into a conference ID that requires an entry code after the conference call is connected.

To program a pause into a soft key dial number:

» Update the configuration file as follows:

➢ `softkey.1.label="VMail"`

➢ `softkey.1.action="$S1$$Tinvite$$Cwc$$Cpause7$$FDialpad8$$FDialpad5$$FDialpad4$$F`
  `Dialpad5$"`

➢ `softkey.1.enable="1"`

➢ `softkey.1.use.idle="1"`

➢ `feature.enhancedFeatureKeys.enabled="1"`

The values for this example are explained as follows:

● `$S1$`—Speed dial line 1

● `$S1$$Tinvite$$`—The phone sends an invite to $S1$

● `$Cwc$`—The phone waits for the call to connect

● `$Cpause7$`—The phone waits for 7 seconds before dialing the remaining numbers

● `$FDialpad8$$FDialpad5$$FDialpad4$$FDialpad5$`—The phone enters the entry code 8545.

Example: Directory-Linked Speed Dial Soft Key with a Pause

Use the following example to add a speed dial line key linked to a directory file with a pause in the dialing sequence.

To program a pause into a directory-linked speed dial line key:

1 Update the configuration file as follows:

➢ `feature.enhancedFeatureKeys.enabled="1"`

➢ `efk.efklist.1.action.string="501$Tinvite$$Cwc$$Cpause7$1234#$Tdtmf$"`
  `efk.efklist.1.label="number"`

➢ `efk.efklist.1.mname="number"`

➢ `efk.efklist.1.status="1"`

2 In a contact directory file or speed dial file (000000000000-directory.xml or
  <MACaddress>-directory.xml), add the following:

➢ `<fn>Call Number</fn>`

➢ `<ct>!number</ct>`

➢ `<sd>99</sd>`

The following values are included in the action string: `<ct>"501$Tinvite$$Cwc$$Cpause7$12`
`34#$Tdtmf$":`

- `501$Tinvite$` Dial 501
- `$Cwc$` Wait for the call to connect
- `$Cpause7$` A seven second pause
- `1234#$Tdtmf$` Send 1234 dual-tone multi-frequency

The following EFK commands are linked to the directory file:

- The parameter `efk.efklist.1.mname="number"` is linked to the speed dial contact `<ct>!number</ct>` of the directory file
- Use `<fn>Call Number</fn>` to define the name that displays on the key
- Use `<sd>99</sd>` to identify which directory entry to link to the key

> For more example configurations, see the two following documents at Polycom Engineering Advisories and Technical Notifications:
>
> • *Using Enhanced Feature Keys and Configurable Soft Keys on Polycom Phones: Technical Bulletin 42250*
> • *Using Enhanced Feature Keys (EFK) Macros to Change Soft Key Functions on Polycom Community: Feature Profile 42250*

Enhanced Feature Keys

Enhanced feature keys (EFK) enables you to customize the functions of a phone's line, soft, and hard keys to assign frequently used functions to keys or to create menu shortcuts to frequently used phone settings.

Enhanced feature key functionality is implemented using star code sequences like *89* and SIP messaging. Star code sequences that define EFK functions are written as macros that you apply to line and soft keys. The EFK macro language was designed to follow current configuration file standards and to be extensible (see Macro Definitions).

> For instructions and details on how to use enhanced feature keys, see *Using Enhanced Feature Keys and Configurable Soft Keys on Polycom Phones: Technical Bulletin 42250.* at Polycom Engineering Advisories and Technical Notifications.

Some Guidelines for Configuring Enhanced Feature Keys

Use the following guidelines to help you to configure enhanced feature keys (EFKs) efficiently:

- Activation of EFK functions requires valid macro construction.
- All failures are logged in the phone's app logs at level 4 (Minor Error).
- If two macros have the same name, the first one is used and the subsequent one is ignored.
- 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.
- "!" and "^" macro prefixes cannot be mixed in the same macro line.

- The sequence of characters must be prefixed by either "!" or "^" to 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.

- 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 after you reach 50 macro substitutions).

Related Topics

Soft Key Parameters

Contact Directory Macros

Because line keys and their functions are linked to fields in the contact directory file, you need to match the contact field (ct) in the directory file to the macro name field (mname) in the configuration file that contains the EFK parameters. When you enter macro names to the contact field (ct) in the directory file, add the '!' prefix to the macro name. The template directory configuration file is named **000000000000-directory~.xml**. To use this file, remove the tilde (~) from the file name. For more detailed information on using the contact directory, see Local Contact Directory.

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 macro labels cannot contain these special characters. If they do, you may experience unpredictable behavior.

Enhanced Feature Key Example Configurations

The following configurations shown in the below illustration were set in the features.cfg file:

- For the `efk.efklist.x.*` parameters, the following configurations were applied:

- Line key 1 has been assigned a Call Park address (1955) and line key 2 a call retrieve function.
- The parameter `acton.string` shows the macro definition for these two functions.
- Status is enabled and a label has been specified to display next to the line key.
- The entry in the `mname` parameter corresponds to the `contact (ct)` field in the contact directory.
- For the `efk.prompt.*` parameters, the following configurations were applied:
  - `Status` is enabled.
  - The label on the user prompt has been defined as *Enter Number:* and this prompt displays on the phone screen.
  - The `type` parameter has been set to `numeric` to allow only numbers.
  - `userfeedback` is specified as `visible`, which enables users to see the numbers entered into the prompt.
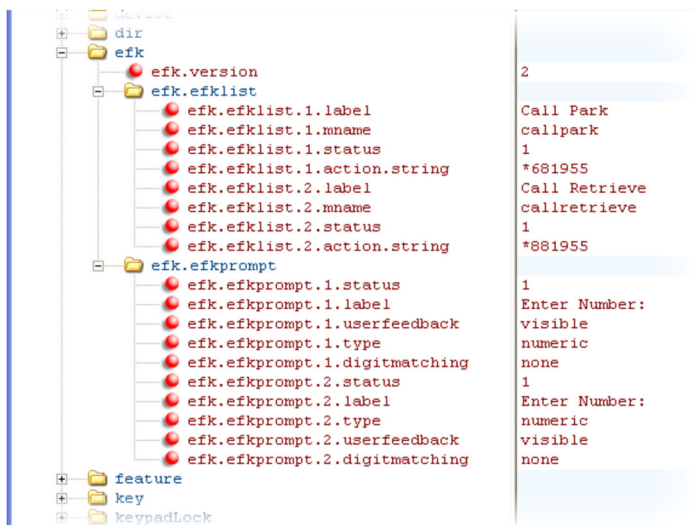
Macro Definitions

The `efk.efklist.x.action.string` can be defined by any of the following:

- Macro Actions
- Prompt Macro Substitution
- Expanded Macros

Macro Actions

The action string is executed in the order it displays. User input is collected before any action is taken. The action string can contain the fields shown in the following table.

Macro Actions and Descriptions

$L<label>$

This is the label for the entire operation. The value can be any string including the null string (in this case, no label displays). This label is used if no other operation label collection method worked (up to the point where this field is introduced). Make this the first entry in the 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 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`
`intercom`
Polycom recommends that you always define this field. If it is not defined, the supplied digits are 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 (see Prompt Macro Substitution).

$S<speed dial index>$

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.

$F<internal function>$

An internal key function. For more information, see Mapping Internal Key Functions.

URL

A URL. Only one per action string is supported.

Prompt Macro Substitution

The macros provide a generic and easy way to manage and define the prompt to be displayed to the user, the maximum number of characters that the user can input, and the action that the phone performs after 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.

For example, the `efk.efklist.x.action.string` can be defined by a macro substitution string, PnNn, where the following applies:

- *Pn* is the prompt x as defined by `efk.efkprompt.x`.
- *Nn* is the number of digits or letters that the user can enter. The value must be between 1 and 32 characters otherwise the macro execution fails. The user must press the **Enter** soft key to complete data entry.

Expanded Macros

Expanded macros are prefixed with the ^ character and are inserted directly into the local directory contact (ct) field. For more information, see Local Contact Directory.

Example Macros

The action string
`$Changup$*444*$P1N4$$Tinvite$$Cwaitconnect$$P2N3$$Cpause2$$Tdtmf$$Changup$` is executed in order 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 After connection, there is a two second pause, and then the string *567* is sent using DTMF dialing on the active call.
6 The active call is disconnected.

Because line keys and their functions are linked to fields in the directory file, the macro name you enter in `efk.list.x.mname` must match the name you enter to the `contact (ct)` field in the directory file. The macro name you enter in the `(ct)` field of the directory file must begin with the '!' prefix.

Flexible Line Key Assignment

You can enable users to assign a line key function to any line key on the phone. By default, functions are assigned to line keys in succession—the order in which the line key displays on the phone. Flexible Line Keys (FLK) enables you to break that ordering and assign a line key function to a line key that displays anywhere on the phone's screen. You can apply this feature to any line key function, including line appearance, speed dial, busy lamp field (BLF), and presence.

This feature is available on the VVX 300 series, 400 series, 500 series, 600 series, and VVX Expansion Modules.

> Line keys on VVX phones and expansion modules are numbered sequentially, and the line keys on VVX expansion modules depend on how many lines your phone supports. For example, a VVX 600/601 phone supports 16 lines, numbered 1-16. The first line on an expansion module connected to a VVX 600/601 phone is line 17.

Assigning BLF and Presence to Line Keys

Specific conditions apply when you assign BLF or presence to line keys. If you are assigning BLF or presence to a line key, assign that line key to `index=0` to indicate automatic ordering. BLF and presence line keys are self-ordering, meaning that if you have these features assigned to multiple line keys, you can specify the location of the BLF or presence line key but not the order in which they display. For example, you can assign a BLF line key to index 1, 3, and 5 but you cannot specify how the contacts are ordered, which BLF contacts display on line keys 1, 3, and 5.

In addition, to assign BLF and presence to a line key, you need to assign a corresponding registration line. You can configure multiple line keys per registration if each line key has a corresponding `reg.x.lineKeys` parameter.

Related Topics

Flexible Line Keys Parameters

Flexible Line Key Assignment Categories and Index

The FLK category specifies the function of the line key. The index specifies the order in which the line keys display on the phone screen. Use the following table to help you assign a category and an index to the line keys on your phone. Note that the category Unassigned leaves the line key blank.

Flexible Line Keys Categories and Index

Category	Unassigned	line	BLF	Speed Dial	Presence
Index	Null	The line index number	0	The speed dial index number	0

Phone Keypad

You can customize many of the default key functions on the phone's keypad interface. Polycom recommends that you configure only those phone keys with removable key caps, which includes Directories, Applications, Conference, Transfer, Redial, Menu, Messages, Do Not Disturb, and Call Lists.

> ⚠ Polycom recommends that you remap only those keys with removable key caps. If you remap other keys, your phone may not work properly. You should not remap the following keys: the dial pad, volume control, handsfree, mute, headset, hold, and the navigation arrow keys.

Related Topics

Phone Keypad Parameters

Multiple Key Combinations

You can reboot the phone, reset the phone to factory default values, upload log files from the phone to your provisioning server, set the Base Profile, and view phone details with a multiple key combination (MKC) on your Polycom phones.

Web Info: Resetting and rebooting your phone

For other methods for resetting and rebooting your Polycom phones, refer to *Updating, Troubleshooting, and Resetting SoundPoint IP, SoundStation IP, and VVX 1500 Phones*: *Quick Tip 18298 at* Polycom Engineering Advisories and Technical Notifications.

Rebooting the Phone with a MKC

You can reboot the phones with a multiple key combination (MKC) that varies by phone model. Rebooting the phone downloads new software and new configuration files if available on the provisioning server.

Depending on your phone model, press and hold the following keys simultaneously until you hear a confirmation tone (for about three seconds).

Phone Reboot Multiple Key Combinations

Phone Model	MKC
VVX 101, 201	0, 1, and 3
VVX 300, 310	0, 1, and 3
VVX 301, 311	0, 1, and 3
VVX 400, 410	0, 1, and 3
VVX 401, 411	0, 1, and 3
VVX 500, 501	0, 1, and 3
VVX 600, 601	0, 1, and 3
VVX 1500	Delete, Volume-, Volume+, and Select

Resetting the Phone to Defaults with a MKC

You can reset a phone to factory default settings with a multiple key combination (MKC) that varies by phone model. This is useful when you use more than one method to configure phones and phone features. Resetting the phone to defaults clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to 456.

Resetting to factory defaults also resets the administrator password (factory default password is 456). Polycom recommends that you change the administrative password from the default value.

> **Settings: Resetting a VVX 1500 D to default values disables the H.323 protocol**
> After you reset to factory defaults on a Polycom VVX 1500 D phone, you must re-enable the H.323 protocol through a configuration file change or by using the Web Configuration Utility. Refer to the section H.323 Protocol Parameters.

Depending on your phone model, press and hold the following keys simultaneously during the updater/BootROM countdown process until the administrator password prompt displays.

Factory Default Multiple Key Combinations

Phone Model	MKC
VVX 101, 201	1, 3, and 5
VVX 300, 310	1, 3, and 5
VVX 301, 311	1, 3, and 5
VVX 400, 410	1, 3, and 5
VVX 401, 411	1, 3, and 5
VVX 500, 501	1, 3, and 5
VVX 600, 601	1, 3, and 5
VVX 1500	4, 6, 8, and * dial pad keys

Uploading Log Files with a MKC

You can use a a multiple key combination (MKC) to upload log files to your provisioning server with a multiple key combination that varies by phone model. Uploading log files copies the log files from the phone to the provisioning server. and creates new files named ***<MACaddress>-now-xxx.log***.

Depending on your phone model, press and hold one the following keys simultaneously for about three seconds until you hear a confirmation tone.

Log Upload Multiple Key Combinations

Phone Model	MKC
VVX 101, 201	1, 5, and 9
VVX 300, 310	1, 5, and 9
VVX 301, 311	1, 5, and 9
VVX 400, 410	1, 5, and 9
VVX 401, 411	1, 5, and 9
VVX 500, 501	1, 5, and 9

Log Upload Multiple Key Combinations

Phone Model	MKC
VVX 600, 601	1, 5, and 9
VVX 1500	Up, Down, Left, and Right arrow keys

Set the Base Profile with a MKC

You can set the base profile with a multiple key combination (MKC), which allows for quick setup of Polycom phones with Microsoft Lync Server and Skype for Business Server.

Depending on your phone model, press and hold the following keys simultaneously for about three seconds until you hear a confirmation tone.

Factory Default Multiple Key Combinations

Phone Model	MKC
VVX 101, 201	1, 4, and 9
VVX 300, 310	1, 4, and 9
VVX 301, 311	1, 4, and 9
VVX 400, 410	1, 4, and 9
VVX 401, 411	1, 4, and 9
VVX 500, 501	1, 4, and 9
VVX 600, 601	1, 4, and 9
VVX 1500	1, 4, and 9

View Phone Details with a MKC

You can use a multiple key combination to view frequently-used administrator phone details including:

- IP Address
- Boot Server Type
- MAC Address
- VLAN
- Boot Server Address
- UC Software version

To view VVX phone details on the phone:

» Press and hold keys **1**,**4**, and **7**.

Defining the Phone Key Layout

You can redefine certain hard key functions using parameters in the configuration files. The following figures and tables show the default key layouts for the following phone models:

- VVX 101 and 201 Default Key Functions
- VVX 3xx Default Key Functions
- VVX 4xx Default Key Functions
- VVX 5xx Default Key Functions
- VVX 6xx Default Key Functions
- VVX 1500 Default Key Functions

VVX 101 and 201 Business Media Phones Key Layout

The following figure and table show the available phone key functions.
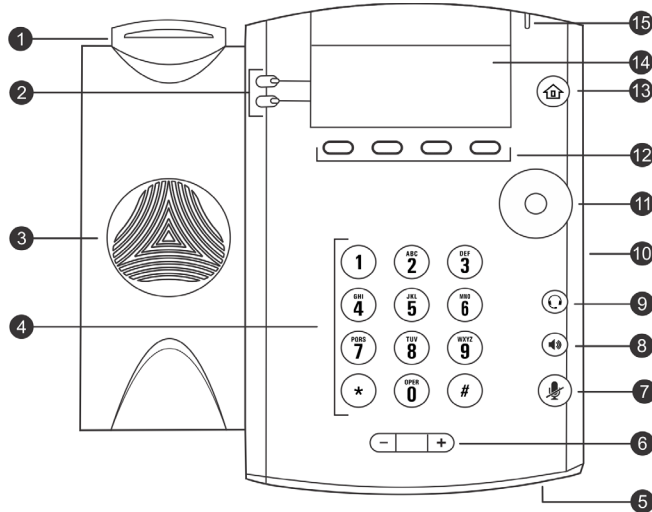
VVX 101 and 201 Default Key Functions

KEY ID	Function	KEY ID	Function
1	Hookswitch	9	Headset key
2	Line keys	10	Security slot (on side)
3	Speaker	11	Navigation keys / Select key
4	Dial pad keys	12	Soft keys
5	Microphone	13	Home key
6	Volume keys	14	Screen
7	Mute key	15	Message Waiting Indicator
8	Speakerphone key		

VVX 300, 301, 310, and 311 Business Media Phones Key Layout

The following figure and table show the available phone key functions. IDs that have no function are described as n/a.

Key ID

VVX 3xx Default Key Functions

KEY ID	Function	KEY ID	Function	KEY ID	Function	KEY ID	Function
1	n/a	15	Dialpad7	29	SoftKey1	43	n/a
2	Dialpad2	16	Dialpad8	30	n/a	44	n/a
3	ArrowLeft	17	Dialpad9	31	SoftKey4	45	n/a
4	ArrowRight	18	Select	32	Line2	46	n/a
5	Dialpad3	19	Hold	33	Line3	47	n/a
6	VolDown	20	Transfer	34	Line4	48	n/a
7	VolUp	21	Messages	35	n/a	49	n/a
8	Dialpad4	22	DialpadStar	36	n/a	50	n/a
9	Dialpad5	23	Dialpad0	37	n/a	51	Line1
10	Headset	24	DialpadPound	38	n/a	52	Line5
11	ArrowDown	25	Dialpad1	39	n/a	53	Line6

VVX 3xx Default Key Functions

KEY ID	Function	KEY ID	Function	KEY ID	Function	KEY ID	Function
12	ArrowUp	26	Home	40	Dialpad6		
13	Handsfree	27	SoftKey3	41	n/a		
14	MicMute	28	SoftKey2	42	n/a		

VVX 400, 401, 410, and 411 Business Media Phones Key Layout

The following figure and table show the available phone key functions. IDs that have no function are described as n/a.

Key ID

VVX 4xx Default Key Functions

KEY ID	Function	KEY ID	Function	KEY ID	Function	KEY ID	Function
1	n/a	15	Dialpad7	29	SoftKey1	43	n/a
2	Dialpad2	16	Dialpad8	30	n/a	44	n/a
3	ArrowLeft	17	Dialpad9	31	SoftKey4	45	n/a
4	ArrowRight	18	Select	32	Line2	46	n/a
5	Dialpad3	19	Hold	33	Line3	47	n/a
6	VolDown	20	Transfer	34	Line4	48	n/a
7	VolUp	21	Messages	35	Line8	49	n/a
8	Dialpad4	22	DialpadStar	36	Line9	50	n/a
9	Dialpad5	23	Dialpad0	37	Line10	51	Line1
10	Headset	24	DialpadPound	38	n/a	52	Line5
11	ArrowDown	25	Dialpad1	39	n/a	53	Line6

VVX 4xx Default Key Functions

KEY ID	Function	KEY ID	Function	KEY ID	Function	KEY ID	Function
12	ArrowUp	26	Home	40	Dialpad6	54	Line7
13	Handsfree	27	SoftKey3	41	n/a	55	Line11
14	MicMute	28	SoftKey2	42	n/a	56	Line12

VVX 500 and 501 Business Media Phones Key Layout

The following figure and table show the available phone key functions. IDs that have no function are described as n/a.

VVX 5xx Default Key Functions

KEY ID	Function	KEY ID	Function	KEY ID	Function	KEY ID	Function
1	Dialpad1	12	Headset	23	Dialpad0	34	n/a
2	Dialpad2	13	n/a	24	DialpadPound	35	n/a
3	VolDown	14	n/a	25	n/a	36	n/a
4	VolUp	15	Dialpad7	26	Home	37	n/a
5	Dialpad3	16	Dialpad8	27	n/a	38	n/a
6	n/a	17	Dialpad9	28	n/a	39	n/a
7	n/a	18	MicMute	29	n/a	40	Dialpad6
8	Dialpad4	19	n/a	30	n/a	41	n/a
9	Dialpad5	20	n/a	31	n/a	42	n/a
10	n/a	21	n/a	32	n/a		
11	Handsfree	22	DialpadStar	33	n/a		

VVX 600 and 601 Business Media Phones Key Layout

The following figure and table show the available phone key functions. IDs that have no function are described as n/a.

VVX 6xx Default Key Functions

KEY ID	Function	KEY ID	Function	KEY ID	Function	KEY ID	Function
1	Dialpad1	12	Headset	23	Dialpad0	34	n/a
2	Dialpad2	13	n/a	24	DialpadPound	35	n/a
3	VolDown	14	n/a	25	n/a	36	n/a
4	VolUp	15	Dialpad7	26	Home	37	n/a
5	Dialpad3	16	Dialpad8	27	n/a	38	n/a
6	n/a	17	Dialpad9	28	n/a	39	n/a
7	n/a	18	MicMute	29	n/a	40	Dialpad6
8	Dialpad4	19	n/a	30	n/a	41	n/a
9	Dialpad5	20	n/a	31	n/a	42	n/a
10	n/a	21	n/a	32	n/a		
11	Handsfree	22	DialpadStar	33	n/a		

VVX 1500 Business Media Phone Key Layout

The following figure and table show the available phone key functions. IDs that have no function are described as n/a.
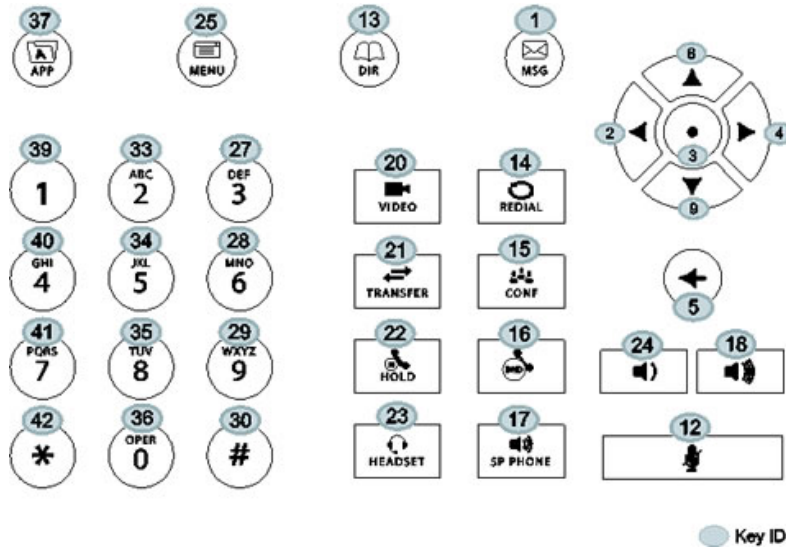
VVX 1500 Default Key Functions

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	VolDown	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		

Mapping Internal Key Functions

A complete list of internal key functions for enhanced feature keys and hard key mappings is shown in the table Key Labels and Internal Functions.

Note the following guidelines:

- The **Function** value is case sensitive.
- Some functions are dependent on call state. Generally, if the soft key displays on a call screen, the soft key function is executable.
- Some functions depend on the feature being enabled. For example, the BuddyStatus and MyStatus soft keys require the presence feature to be enabled.
- Hard key remappings do not require the enhanced feature key feature to be enabled. This includes the speed dial function on older platforms. On newer platforms, use line key functions.

The table below shows only line1 to line 6 functions.

Key Labels and Internal Functions

Function	Description	Notes
ACDAvailable	Status for Automatic Call Distribution when available.	
ACDLogin	Login to Automatic Call Distribution.	
ACDLogout	Logout from Automatic Call Distribution.	
ACDUnavailable	Status for Automatic Call Distribution when unavailable.	
Answer	Answer an incoming call.	Call screen only
Applications	Main Browser	
ArrowDown	Move arrow down	
ArrowLeft	Move arrow left	
ArrowRight	Move arrow right	
ArrowUp	Move arrow up	
BargeIn	Barge In to show appearances, Barge In	Call screen only
BuddyStatus	Status of the contacts added to Buddy list.	
Callers	Displays the list of callers.	
CallList	Displays the call logs.	
CallPark	Park an active call.	Call screen only
CallPickup	Call pick-up on the phone.	Call screen only
Conference	Begin a conference call.	Call screen only
Delete	Delete the selected item.	
Dialpad0	Dialpad 0	

Key Labels and Internal Functions

Function	Description	Notes
Dialpad1	Dialpad 1	
Dialpad2	Dialpad 2	
Dialpad3	Dialpad 3	
Dialpad4	Dialpad 4	
Dialpad5	Dialpad 5	
Dialpad6	Dialpad 6	
Dialpad7	Dialpad 7	
Dialpad8	Dialpad 8	
Dialpad9	Dialpad 9	
DialpadPound	Dialpad pound sign	
DialpadStar	Dialpad star sign	
DialpadURL	Navigate to a specific address or location.	Call screen only
DirectedPickup	Directed call pick-up on the phone.	Call screen only
Directories	Displays the directory items.	
Divert	Forward a call.	
DoNotDisturb	Do Not Disturb menu	
EnterRecord	Enter a call record.	Call screen only
Exit	Exit existing menu.	Menu only
GroupPickup	Group call pick-up on the phone.	
Handsfree	Use handsfree	
Headset	Use headset	Desktop phones only
Hold	Toggle hold	
Join	Joins a call to an active call to make a conference.	Call screen only
LCR	Last Call Return	
Line1	Line Key 1	
Line2	Line Key 2	
Line3	Line Key 3	
Line4	Line Key 4	

Key Labels and Internal Functions

Function	Description	Notes
Line5	Line Key 5	
Line6	Line Key 6	
ListenMode	Turn on speaker to listen only.	
LockPhone	Lock the phone.	
Menu	Displays the main menu.	
Messages	Messages menu	
MicMute	Mute the microphone.	
MyStatus	View my status.	
NewCall	Place a new call.	Call screen only
Null	Do nothing	
Offline	Offline for presence	
Page	Group Paging	
ParkedPickup	Specifies how the phone performs a parked call pick-up.	Call screen only
QuickSetup	Quick Setup feature	Call screen only
Redial	Redial the last dialed number.	Call screen only
Select	Select an item.	
ServerACDAgentAvailable	Status for server-based Automatic Call Distribution agent when available.	
ServerACDAgentUnavailable	Status for server-based Automatic Call Distribution agent when unavailable.	
ServerACDSignIn	Login to a server-based Automatic Call Distribution.	
ServerACDSignOut	Logout from a server-based Automatic Call Distribution.	
Setup	Settings menu	
Silence	Silence the call ringer.	Call screen only
SoftKey1	SoftKey 1	
SoftKey2	SoftKey 2	
SoftKey3	SoftKey 3	

Key Labels and Internal Functions

Function	Description	Notes
SoftKey4	SoftKey 4	
Softkey5	Softkey 5	
SpeedDial	Place a call to a number assigned to the SpeedDial.	
Split	Split a conference call.	Call screen only
Talk	Push-to-Talk	
Transfer	Transfer a call	Call screen only
Video	Enables the video in a call.	Polycom VVX 500/501, 600/601, and 1500 business media phones.
VolDown	Set volume down	
VolUp	Set volume up	

Network

Polycom's Open SIP UC Software enables you to make custom network configurations.

Two-Way Active Measurement Protocol

Polycom UC Software supports Two-Way Active Measurement Protocol (TWAMP), which is RFC 5357 compliant, to check network performance by measuring the round-trip time between two devices using TWAMP protocols. TWAMP defines the following protocols:

● TWAMP Control protocol, which uses TCP.

● TWAMP Test protocol, which uses UDP.

TWAMP Limitations

TWAMP includes the following limitations:

● TWAMP Control and Test protocols only support unauthenticated mode

● A maximum of 10 clients can establish a connection with the server

● The server is limited to handle a maximum of 10 sessions per client

Related Topics

Two-Way Active Measurement Protocol Configuration Parameters

3GPP Technical Specifications

For an IP Multimedia Subsystem (IMS) environment, Polycom has introduced support for a subset of the 3rd Generation Partnership Project technical specifications (3GPP TS) 24.229, 24.615, and 24.629. In addition, Polycom phones provide partial or complete support for the following RFCs:

● RFC 3327

● RFC 3608

● RFC 3680

● RFC 6665

● RFC 6228

● RFC 3261

● RFC 5009

● RFC 7462

- RFC 7329
- RFC 6026
- RFC 3581
- RFC 6947

VVX business media phones support the following IMS feature enhancements:

- The call waiting ring-back tone plays to inform users that a call is waiting at the far end.
- The SIP Response Code 199 (defined in RFC 6228) is supported.
- The Path extension header field in the SIP Register request message allows accumulating and transmitting the list of proxies between a user agent and Registrar server.
- The caller phone can support the p-early-media SIP header that determines whether the caller phone should play a network-provided media or its own media as a ring back tone.
- The VQMon messages generated by the phone can contain service route information in SIP route headers.
- In a NAT network, a phone may need to send keep-alive messages to maintain the IP addresses mapping in the NAT table.

Related Topics

3GPP Technical Specifications Parameters

Technical Report-069

Technical Report-069 (TR-069) enables you to remotely manage end-user devices. As a bidirectional SOAP/HTTP-based protocol, TR-069 enables secure communication between Auto Configuration Servers (ACS) and Polycom phones. Using TR-069, you can remotely configure and manage Polycom phones by provisioning systems that comply with TR-069 technical specification.

Configuring TR-069

You can configure the TR-069 feature through the phone menu, Web Configuration Utility, or configuration parameters on a central server. You can configure Polycom phones with an ACS server, including user name and password, using DHCP Option 43 for IPv4 and DHCP Option 17 for IPv6.

Configure TR-069 Settings on the Phone Menu

You can configure TR-069 settings on the phone menu.

To configure TR-069 settings on the phone menu:

1   Go to **Settings > Advanced > Administration Settings > Network Configuration**.
2   Select **TR-069**, and select **Enabled**.
3   In the**TR069 Menu**, select **ACS Configuration** and enter values for the following settings:
    ➢ URL
    ➢ Username

> ➢ Password
> ➢ Periodic Inform
> ➢ Inform Interval

4 In **Phone/CPE Configuration**, configure a user name and password.

5 In **Upgrade Management**, select **Enable** or **Disable**.

Configure TR-069 from the Web Configuration Utility

You can configure TR-069 from the Web Configuration Utility.

To configure the TR-069 from the Web Configuration Utility:

» In the Web Configuration Utility, navigate to **Settings > Provisioning Server > TR-069 Menu**.

Related Topics

TR-069 Parameters

Map TR-106 Parameters to Polycom Parameters

The data model TR-106 defines the TR-069 ACS parameter details. The parameters listed as 'Internal Value' are not directly mapped to a configuration parameter on the phone, and the phone generates these values dynamically to provide to the ACS server.

The following table lists the TR-106 parameters and their corresponding Polycom parameters.

TR-106 Parameters to Polycom Parameters

TR-106 ACS parameter names	Parameter (Polycom parameter names)	Writable
Device		
Device.DeviceInfo		
Manufacturer	Internal Value	No
ManufacturerOUI	Internal Value	No
ModelName	Internal Value	No
ProductClass	Internal Value	No
SerialNumber	Internal Value	No
HardwareVersion	Internal Value	No
SoftwareVersion	Internal Value	No
UpTime	Internal Value	No
Device.ManagementServer.		
URL	device.tr069.acs.url	Yes

TR-106 Parameters to Polycom Parameters

TR-106 ACS parameter names	Parameter (Polycom parameter names)	Writable
Username	device.tr069.acs.username	Yes
Password	device.tr069.acs.password	Yes
PeriodicInformEnable	device.tr069.periodicInform.enabled	Yes
PeriodicInformInterval	device.tr069.periodicInform.interval	Yes
ConnectionRequestURL	Internal Value	No
ConnectionRequestUsername	device.tr069.cpe.username	Yes
ConnectionRequestPassword	device.tr069.cpe.password	Yes
UpgradesManaged	device.tr069.upgradesManaged.enabled	Yes
STUNServerAddress	tcpIpApp.ice.stun.server	Yes
STUNServerPort	tcpIpApp.ice.stun.udpPort	Yes
STUNUsername	tcpIpApp.ice.username	Yes
STUNPassword	tcpIpApp.ice.password	Yes
Device.LAN.		
IPAddress	Internal Value	No
SubnetMask	Internal Value	No
DNSServers	Internal Value	No
MACAddress	Internal Value	No
MACAddressOverride	Internal Value	No

Map TR-104 Parameters to Polycom Parameters

The data model TR-104 defines the TR-069 ACS parameter details. The parameters listed as 'Internal Value' are not directly mapped to a configuration parameter on the phone and the phone generates these values dynamically to provide to the ACS server.

The following table list the TR-104 parameters and their corresponding Polycom parameters.

TR-104 Parameters to Polycom Parameters

TR-104 ACS parameter names	CPE Parameter (Polycom parameter names)	Writable
VoiceService.{i}.VoiceProfile.{i}.		
DigitMap	dialplan.digitmap	Yes
VoiceService.{i}.VoiceProfile.{i}.SIP.		
RegistrarServer	voIpProt.server.X.address	Yes

TR-104 Parameters to Polycom Parameters

TR-104 ACS parameter names	CPE Parameter (Polycom parameter names)	Writable
RegistrarServerPort	voIpProt.server.X.port	Yes
OutboundProxy	voIpProt.SIP.outboundProxy.address	Yes
OutboundProxyPort	voIpProt.SIP.outboundProxy.port	Yes
RegisterExpires	voIpProt.server.X.expires	Yes
RegistersMinExpires	voIpProt.server.X.expires.overlap	Yes
RegisterRetryInterval	voIpProt.server.X.retryTimeOut	Yes
VoiceService.{i}.VoiceProfile.{i}.SIP.EventSubscribe.{i}.		
ExpireTime	voIpProt.server.X.subscribe.expires	Yes
VoiceService.{i}.VoiceProfile.{i}.H323.		
Gatekeeper	voIpProt.server.H323.X.address	Yes
GatekeeperPort	voIpProt.server.H323.X.port	Yes
VoiceService.{i}.VoiceProfile.{i}.RTP.		
LocalPortMin	tcpIpApp.port.rtp.mediaPortRangeStart	Yes
LocalPortMax	tcpIpApp.port.rtp.mediaPortRangeEnd	Yes
VoiceService.{i}.VoiceProfile.{i}.RTP.SRTP.		
Enable	sec.srtp.enable	Yes
VoiceService.{i}.VoiceProfile.{i}.ButtonMap.Button.{i}.		
ButtonName	softkey.X.label	Yes
FacilityAction	softkey.X.action	Yes
UserAccess	softkey.X.enable	Yes
VoiceService.{i}.VoiceProfile.{i}.Line.{i}.		
DirectoryNumber	reg.X.address	Yes
VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.		
AuthUserName	reg.X.auth.userId	Yes
AuthPassword	reg.X.auth.password	Yes
VoiceService.{i}.VoiceProfile.{i}.Line.{i}.CallingFeatures.		
CallForwardUnconditionalEnable	reg.X.fwdStatus	Yes
CallForwardUnconditionalNumber	reg.X.fwdContact	Yes
CallForwardOnBusyEnable	reg.X.fwd.busy.status	Yes

TR-104 Parameters to Polycom Parameters

TR-104 ACS parameter names	CPE Parameter (Polycom parameter names)	Writable
CallForwardOnBusyNumber	reg.X.fwd.busy.contact	Yes
CallForwardOnNoAnswerEnable	reg.X.fwd.noanswer.status	Yes
CallForwardOnNoAnswerNumber	reg.X.fwd.noanswer.contact	Yes
CallForwardOnNoAnswerRingCount	reg.X.fwd.noanswer.ringCount	Yes
DoNotDisturbEnable	divert.dnd.X.enabled	Yes

Supported TR-069 Remote Procedure Call (RPC) Methods

The following table lists the supported RPC methods.

RPC Methods

RPC Method	Description
GetRPCMethods	Discovers the set of methods supported by the phone.
SetParameterValues	Modifies the value of one or more phone parameters.
GetParameterValues	Obtains the value of one or more phone parameters.
GetParameterNames	Discovers the parameters accessible on a particular phone.
GetParameterAttributes	Reads the attributes associated with one or more phone parameters.
SetParameterAttributes	Modifies attributes associated with one or more phone parameters.
Reboot	Reboots the phone.
Download	Causes the phone to download a specified file from the designated location. Supported file types for download: Firmware Image Configuration File
FactoryReset	Resets the phone to its factory default state.
TransferComplete	Informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	Adds a new instance of an object defined on the phone.
DeleteObject	Removes a particular instance of an object.

Advice of Charge

In an IP Multimedia Subsystem (IMS) environment, Polycom phones support the Advice of Charge (AoC) feature as defined in Technical Specification (TS) 24.647 version 9.1.0 Release 9.

You can enable Polycom phones to display call charges information, which can include:

- Call setup charge and call tariff information – Displayed at the beginning of a call.
- Cumulative call cost – Displayed on an ongoing call.
- Complete call cost – Displayed after a call ends.

Related Topics

Advice of Charge Parameters

IPv6 Protocol Support

VVX business media phones support IPv6 and you can configure the phones to operate in IPv4, IPv6, or dual stack (IPv4/IPv6) mode.

You can enable and configure IPv6 support from the phone menu, the Web Configuration Utility, or with centralized provisioning.

Related Topics

IPv6 Parameters

Real-Time Transport Protocol (RTP) Ports

You can configure RTP ports for your environment in the following ways:

- Filter incoming packets by IP address or port.
- Reject packets arriving from a non-negotiated IP address, an unauthorized source, or non-negotiated port for greater security.
- Enforce symmetric port operation for RTP packets. When the source port is not set to the negotiated remote sink port, arriving packets are rejected.
- Fix the phone's destination transport port to a specified value regardless of the negotiated port.

  This is useful for communicating through firewalls. When you use a fixed transport port, all RTP traffic is sent to and arrives on that specified port. Incoming packets are sorted by the source IP address and port, which allows multiple RTP streams to be multiplexed.

- Specify the phone's RTP port range.

  Since the phone supports conferencing and multiple RTP streams, the phone can use several ports concurrently. Consistent with RFC 1889, 3550, and 3551, the next-highest odd-numbered port is used to send and receive RTP.

Related Topics

RTP Ports Parameters

Network Address Translation (NAT)

Network Address Translation (NAT) enables a local area network (LAN) to use one set of IP addresses for internal traffic and another set for external traffic. The phone's signaling and RTP traffic use symmetric ports. Note that the source port in transmitted packets is the same as the associated listening port used to receive packets.

Related Topics

Network Address Translation Parameters

Bluetooth Headset Support Parameters

Server Redundancy

Server redundancy is often required in VoIP deployments to ensure continuity of phone service if, for example, the call server is taken offline for maintenance, the server fails, or the connection between the phone and the server fails. Polycom phones support Failover and Fallback server redundancy types. In some cases, you can deploy a combination of the two server redundancy types. Consult your SIP server provider for recommended methods of configuring phones and servers for failover configuration.

> Note: The concurrent failover/fallback feature is not compatible with Microsoft environments.

For more information, see *Technical Bulletin 5844: SIP Server Fallback Enhancements on Polycom Phones* and *Technical Bulletin 66546: Configuring Optional Re-Registration on Failover Behavior*.

Related Topics

Server Redundancy Parameters

DNS SIP Server Name Resolution

If a DNS name is given for a proxy/registrar address, the IP addresses associated with that name is discovered as specified in RFC3263. If a port is given, the only lookup is an A record. If no port is given, NAPTR and SRV records are 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, port 5060 is used. If the registration type is TLS, port 5061 is used.

> Caution: Failure to resolve a DNS name is treated as signaling failure that causes a failover.

The following configuration causes the phone to build an SRV request based on the address you provide, including all subdomains. Use the format:

- `voIpProt.SIP.outboundProxy.address`="<*sip.example.com*>"

● `voIpProt.SIP.outboundProxy.port="0"`

This SRV request produces a list of servers ordered by weight and priority, enabling you to specify sub-domains for separate servers, or you can create partitions of the same system. Please note that while making SRV queries and transport is configured as TCP, the phone adds the prefix `<_service._proto.>` to the configured address/FQDN but does not remove the sub-domain prefix, for example `sip.example.com` becomes `_sip._tcp.sip.example.com`. A single SRV query can be resolved into many different servers, session border controllers (SBCs), or partitions ordered by weight and priority, for example, `voice.sip.example.com` and *video.sip.example.com*. Alternatively, use DNS NAPTR to discover what services are available at the root domain.

Customer Phone Configuration

The phones at the customer site are configured as follows:

● Server 1 (the primary server) is configured with the address of the service provider call server. The IP address of the server(s) is provided by the DNS server, for example: `reg.1.server.1.address=voipserver.serviceprovider.com`.

● Server 2 (the fallback server) is 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`.

> Caution: Be careful when using multiple servers per registration. It is possible to configure the phone for more than two servers per registration but ensure that the phone and network load generated by registration refresh of multiple registrations does not become excessive. This is of particular concern when a phone has multiple registrations with multiple servers per registration and some of these servers are unavailable.

For Outgoing Calls (INVITE Fallback)

When the user initiates a call, the phone completes the following steps to connect the call:

1 The phone tries to call the working server.

2 If the working server does not respond correctly to the INVITE, the phone tries and makes 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 tries 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 fails.

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

● 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, see <server/>.

Caution: 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 attempts to contact the DNS server to resolve the address of all servers in its list before initiating a call. These attempts timeout, but the timeout mechanism can cause long delays (for example, two minutes) before the phone call proceeds using the working server. To prevent this issue, long TTLs should be used. Polycom recommends deploying an on-site DNS server as part of the redundancy solution.

Phone Operation for Registration

After the phone has booted up, it registers to all configured servers.

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

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

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

Recommended Practices for Fallback Deployments

In situations where server redundancy for fallback purpose is used, the following measures should be taken to optimize the solution:

- Deploy an on-site DNS server to avoid long call initiation delays that can result if the DNS server records expire.
- Do not use `OutBoundProxy` configurations on the phone if the `OutBoundProxy` could be unreachable when the fallback occurs.
- Avoid using too many servers as part of the redundancy configuration as each registration generates more traffic.
- Educate users as to the features that are not available when in fallback operating mode.

Note: The concurrent/registration failover/fallback feature is not compatible with Microsoft environments.

Static DNS Cache

Failover redundancy can be used only when the configured IP server hostname resolves (through SRV or A record) to multiple IP addresses. Unfortunately, the DNS cache cannot always be configured to take advantage of failover redundancy.

You can statically configure a set of DNS NAPTR SRV and/or A records into the phone.

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, see RFC2308.

Configuring Static DNS

Phones configured with a DNS server behave as follows:

1. The phone makes an initial attempt to resolve a hostname that is within the static DNS cache. For example, a query is made to the DNS if the phone registers with its SIP registrar.

2. 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.

3. After the configured time interval has elapsed, a resolution attempt of the hostname again results in a query to the DNS.

4. 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.

If a phone is not configured with a DNS server, when the phone attempts to resolve a hostname within the static DNS cache, it always returns the results from the static cache.
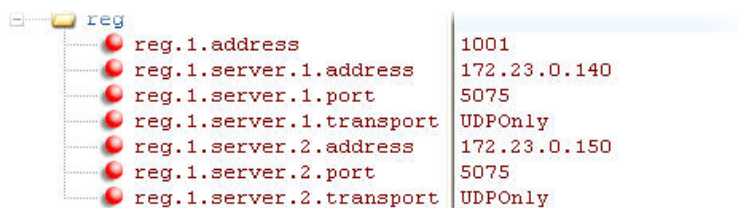
Related Topics

Static DNS Parameters

Example Static DNS Cache Configuration

The following example shows how to configure static DNS cache using A records IP addresses in SIP server address fields. The addresses listed in this example are read by Polycom UC Software in the order listed.

When the static DNS cache is not used, the **site.cfg** configuration looks as follows:

```
⊟──🗀 reg
    ─🔴 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 **site.cfg** configuration looks as follows:

```
reg
    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
```

Example: Static DNS Cache with A Records

This example shows how to configure static DNS cache where your DNS provides A records for `reg.x.server.x.address` but not SRV. In this case, the static DNS cache on the phone provides SRV records. For more information, see RFC 3263.

When the static DNS cache is not used, the **site.cfg** configuration looks as follows:

```
reg
    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 **site.cfg** configuration looks as follows:

```
reg
    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: Static DNS Cache with NAPTR and SRV Records

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

When the static DNS cache is not used, the **site.cfg** configuration looks as follows:

```
reg
    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

reg
    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 **site.cfg** configuration looks as follows:

```
reg
    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.

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.

Related Topics

IP Type-of-Service Parameters

SIP Instance Support

In environments where multiple phones are registered using the same address of record (AOR), the phones are identified by their IP address. However, firewalls set up in these environments can regularly change the IP addresses of phones for security purposes. You can configure SIP instance to identify individual phones instead of using IP addresses. This feature complies with RFC 3840.

This feature is not available on VVX 101 and 201 business media phones.

Related Topics

SIP Instance Parameters

Provisional Polling of Polycom Phones

You can configure phones to poll the server for provisioning updates automatically, and you can set the phone's automatic provisioning behavior to one of the following:

* **Absolute**—The phone polls at the same time every day.
* **Relative**—The phone polls every x seconds, where x is a number greater than 3600.
* **Random**—The phone polls randomly based on a set time interval.
  * ➢ If the time period is less than or equal to one day, the first poll is at a random time between when the phone starts up and the polling period. Afterwards, the phone polls every x seconds.
  * ➢ If you set the polling period to be greater than one day with the period rounded up to the nearest day, the phone polls on a random day based on the phone's MAC address and within a random time set by the start and end polling time.

Related Topics

Provisional Polling Parameters

Example Provisional Polling Configuration

The following are examples of polling configurations you can set up:

* If `prov.polling.mode` is set to rel and `prov.polling.period` is set to *7200*, the phone polls every two hours.

- If `prov.polling.mode` is set to abs and `prov.polling.timeRandomEnd` is set to *04:00*, the phone polls at 4am every day.

- If `prov.polling.mode` is set to random, `prov.polling.period` is set to *604800 (7 days)*, `prov.polling.time` is set to `01:00`, `prov.polling.timeRandomEnd` is set to *05:00*, and you have 25 phones, a random subset of those 25 phones, as determined by the MAC address, polls randomly between 1am and 5am every day.

- If `prov.polling.mode` is set to *abs* and `prov.polling.period` is set to *2328000*, the phone polls every 20 days.

SIP Subscription Timers

You can configure a subscription expiry independently of the registration expiry. You can also configure an overlap period for a subscription independently of the overlap period for the registration, and a subscription expiry and subscription overlap for global SIP servers and per-registration SIP servers. Note that per-registration configuration parameters override global parameters. If you have not explicitly configured values for any user features, the default subscription values are used.

Related Topics

SIP Subscription Timers Parameters

Incoming Network Signaling Validation

You can choose from the following optional levels of security for validating incoming network signaling:

- Source IP address validation
- Digest authentication
- Source IP address validation and digest authentication

Related Topics

Network Signaling Validation Parameters

System and Model Names

The following table outlines the system and model names that Polycom phones transmit with network protocols. If you need to customize your network for a specific phone model, you can parse the network packets for these strings.

System and Model Names

Model	System Name	Model Name
VVX 101	Polycom VVX 101	VVX-VVX_101
VVX 201	Polycom VVX 201	VVX-VVX_201
VVX 300	Polycom VVX 300	VVX-VVX_300

System and Model Names

Model	System Name	Model Name
VVX 301	Polycom VVX 301	VVX-VVX_301
VVX 310	Polycom VVX 310	VVX-VVX_310
VVX 311	Polycom VVX 311	VVX-VVX_311
VVX 400	Polycom VVX 400	VVX-VVX_400
VVX 401	Polycom VVX 401	VVX-VVX_401
VVX 410	Polycom VVX 410	VVX-VVX_410
VVX 411	Polycom VVX 411	VVX-VVX_411
VVX 500	Polycom VVX 500	VVX-VVX_500
VVX 501	Polycom VVX 501	VVX-VVX_501
VVX 600	Polycom VVX 600	VVX-VVX_600
VVX 601	Polycom VVX 601	VVX-VVX_601
VVX 1500	Polycom VVX 1500	VVX-VVX_1500
SoundStructure	SoundStructure VoIP Interface	SoundStructure VoIP Interface

Security

Polycom's Open SIP UC Software enables you to optimize security settings.

Administrator and User Passwords

When you set the Base Profile to Skype or update your phones to UC Software 5.x.x or later, the phones display a message prompting you to change the default administrator password (456). Polycom strongly recommends that administrators change the default password. This password is not the Skype for Business user Sign In password. The default administrator password enables administrators to access advanced settings menu on the phone menu and to log in to a phone's Web Configuration Utility as an administrator.

You can change the default password using any of the following methods:

- The popup prompt when the phone first registers
- Phone menu
- Web Configuration Utility
- Use the parameter `reg.1.auth.password` in the template configuration file

You must have a user or administrator password before you can access certain menu options on the phone and in the Web Configuration Utility. You can use the following default passwords to access menu options on the phone and to access the Web Configuration Utility:

- Administrative password: **456**
- User password: **123**

You can use an administrator password where a user password is required, and you will see all of the user options. If the phone requires the administrator password, you can use the user password, but you are presented with limited menu options. Note that the Web Configuration Utility displays different features and options depending on which password is used.

Change the Default Administrator Password on the Phone

If you do not change the default administrative password, the phone displays a warning and a reminder message each time the phone reboots. If you are registering Polycom phones with Microsoft Skype for Business Server, a message displays on the phone screen prompting you to change the default password.

To change the default administrator password on the phone:

1   On the phone, navigate to **Settings > Advanced**, and enter the default password.

2 Select **Administration Settings > Change Admin Password**.

3 Enter the default password, enter a new password, and confirm the new password.

Change the Default Passwords in the Web Configuration Utility

You can change the administrator and user passwords on a per-phone basis using the Web Configuration Utility. If the default administrative password is in use, a warning displays in the Web Configuration Utility.

To change the default password in the Web Configuration Utility:

1 In the Web Configuration Utility, select **Settings > Change Password**.

2 Update the passwords for the **Admin** and **User**.

Related Parameters

Administrator and User Password Parameters

Security Banner on the Web Configuration Utility

You can enable or disable the security banner on the Web Configuration Utility. In addition, you can configure a custom text message to be displayed on the security banner of your phone's user interface.

Related Topics

Web Configuration Utility Security Banner Parameters

Locking the Web Configuration Utility after Failed Login Attempts

For additional security, you can lock access to the Web Configuration Utility after a set amount of failed user login attempts and configure a period of time after which a user can attempt to log in again.

Related Topics

Web Configuration Utility Security Banner Parameters

Disabling External Ports and Features

You can disable unused external phone ports and features to increase the security of devices in your deployment. You can disable the following ports and features:

- Web Configuration Utility
- PC port

- Aux port
- USB Port
- Speakerphone
- Call forwarding
- Do Not Disturb
- Push-to-Talk (PTT)
- Auto Answer
- Applications icon
- Headset
- Handset
- Bluetooth

> Note: At least one audio port must be enabled to send and receive calls.

Related Topics

Configuring External Ports and Features

Visual Security Classification

The security classification of a call is determined by the lowest security classification among all participants connected to a call. For example, a Top Secret classification displays when all participants in a call have a Top Secret classification level.

> Caution: Call classification is determined by the lowest classification among all participants in the call. You can safely exchange information classified no higher than the call's security classification. For example, if User A is classified as Top Secret and User B has a lower classification level of Restricted, User A and B are connected to the call as Restricted.

Phone users can modify their assigned security classification level to a value lower than their assigned level during a call. When the call is over, the server resets the user's classification level to its original state.

Related Topics

Visual Security Classification Parameters

Configuration File Encryption

Polycom phones can download encrypted files from the provisioning server and encrypt files before uploading them to the provisioning server.

You can encrypt all configuration files except the master configuration file, contact directory files, and configuration override files from the Web Configuration Utility and local device interface. You can also determine whether encrypted files are the same as unencrypted files and use the SDK to facilitate key generation. You cannot encrypt the master configuration file.

To encrypt files, you must provide the phone an encryption key. You can generate your own 32 hex-digit, 128 bit key or use the Polycom Software Development Kit (SDK) to generate a key and to encrypt and decrypt configuration files on a UNIX or Linux server. The SDK is distributed as source code that runs under the UNIX operating system. Note that the SDK generates a random key and applies Advanced Encryption Standard (AES) 128 in Cipher Block Chaining (CBC) mode, for example:

`Crypt=1;KeyDesc=companyNameKey1;Key=06a9214036b8a15b512e03d53412006;`

> Web Info: To request the SDK and quickly install the generated key, see *When Encrypting Polycom UC Software Configuration Files*: *Quick Tip 67442 at* Polycom Engineering Advisories and Technical Notifications.

You can use the following parameters to set the key on the phone:

- `device.set`
- `device.sec.configEncryption.key`
- `device.sec.configEncryption.key.set`

If the phone doesn't have a key, you must download the key to the phone in plain text, which is a potential security concern if you are not using HTTPS. If the phone already has a key, you can download a new key. Polycom recommends naming each key uniquely to identify which key was used to encrypt a file.

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**.

> Troubleshooting: If a phone downloads an encrypted file that it cannot decrypt, the action is logged, and an error message displays. The phone continues to do this until the provisioning server provides an encrypted file that can be read, an unencrypted file, or until the file is removed from the list in the master configuration file.

Change the Encryption Key on the Phone and Server

To maintain secure files, you can change the encryption key on the phones and the server.

To change an encryption key on the phone:

1 Place all encrypted configuration files that you want to use the new key on the provisioning server.

   The phone may reboot multiple times.

   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.

2 Put the new key into a configuration file that is in the list of files downloaded by the phone, specified in **000000000000.cfg** or **<MACaddress>.cfg**.

3 Use the `device.sec.configEncryption.key` parameter to specify the new key.

4   Provision the phone again so that it downloads the new key. The phone automatically reboots a second time to use 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 replaces them when it successfully boots.

Check an Encrypted File

You can check whether or not an encrypted file and an unencrypted file are the same.

To check whether an encrypted file is the same as an unencrypted file:

1   Run the *configFileEncrypt* utility, available from Polycom Support, on the unencrypted file with the "-d" option, which shows the "digest" field.

2   View the encrypted file with text editor, and check the Digest=…." field. If the two fields are the same, then the encrypted and unencrypted file are the same.

Related Topics

Configuration File Encryption Parameters

Digital Certificates

Polycom phones are installed with a Polycom-authenticated RSA certificate. You can use this certificate to create a secure connection between the phone and server when initiating TLS communications over protocols such as HTTPS and SIP. You can download the Polycom Root CA at http://pki.polycom.com/pki. The certificate is set to expire on March 9, 2044.

> For details on installing digital credentials on VVX phones, see *Device Certificates on Polycom SoundPoint IP, SoundStation IP, and VVX Phones: Technical Bulletin 37148* at Polycom Engineering Advisories and Technical Notifications.

X.509 Certificates

Polycom uses the X.509 standard, which defines what information can go into a certificate. An X.509 digital certificate is a digitally signed statement. 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 in turn affects what information can be specified in the certificate.

●   **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 and indicates that you trust the entity that signed this certificate.

- **Validity Period.** Each certificate is valid 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 that specifies to which public key cryptographic system this key belongs and any associated key parameters.

Subject Alternative Names

Polycom supports the use of Subject Alternative Names (SAN) with TLS security certificates. Polycom does not support the use of the asterisk (*) or wildcard characters in the Common Name field of a Certificate Authority's public certificate. If you want to enter multiple hostnames or IP addresses on the same certificate, use the SAN field.

The following is an example of a Polycom device certificate when viewed in a browser.
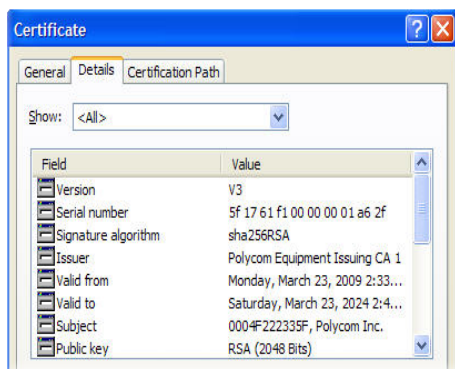
For more information on digital certificates, see Public Key Infrastructure (X.509) and RFC 2459: Internet X.509 Public Key Infrastructure.

Web Info: You can install custom device certificates on your Polycom phones in the same way custom CA certificates are installed. See *Technical Bulletin 17877: Using Custom Certificates With Polycom Phones* for more information.

Check for a Device Certificate

The device certificate and associated private key are stored on the phone in its non-volatile memory as part of the manufacturing process. You can check if a phone has a device certificate pre-installed.

To check for a device certificate on a Polycom phone:

1 Navigate to **Settings > Advanced > Administration Settings > TLS Security > Custom Device Credentials**.

2 Select a credential and press **Info** to view the certificate.

One of the following messages is displayed:

➢ Installed or Factory Installed is displayed if the certificate is available in flash memory, all the certificate fields are valid (listed above), and the certificate has not expired.

➢ 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).

➢ Invalid is displayed if the certificate is not valid.

> Note: If your phone reports the device certificate as self-signed rather than Factory installed, return the equipment to receive a replacement.

You can also quickly check if a Polycom device certificate is installed on the phone by navigating to **Settings > Status > Platform > Phone**.

Generating a Certificate Signing Request

If you need a certificate to perform a number of tasks, such as for multiple TLS authentication, you can request a certificate from the phone. By default, the phone requests a 2048-bit certificate with 'sha256WithRSAEncryption' as the signature algorithm. You can use OpenSSL or another certificate signing request utility if you require a stronger certificate.

Obtain a Certificate

The following provides general instructions on how to obtain a certificate.

To obtain a certificate:

1 Request a certificate from a Certificate Authority (CA) by creating a certificate signing request (CSR).

2 Forward the CSR to a CA to create a certificate. If your organization doesn't have its own CA, you need to forward the CSR to a company like Symantec.

   If successful, the CA sends back a certificate that has been digitally signed with their private key.

After you receive the certificate, you can download it to the phone in the following ways:

● Using a configuration file

● Through the phone's user interface

● Through the Web Configurable Utility

Generate a Signing Request

The following shows you how to generate a signing request on a Polycom device.

To generate a certificate signing request on a Polycom phone:

1 Navigate to **Settings > Advanced > Admin Settings > Generate CSR**.

2 When prompted, enter the administrative password and press **Enter**. The default administrative password is **456**.

3   From the **Generate CSR Screen**, fill in the **Common Name** field - the Organization, Email Address, Country, and State fields are optional.

4   Press **Generate**.

A message "CSR generation completed" displays on the phone's screen. The MAC.csr (certificate request) and MAC-private.pem (private key) are uploaded to the phone's provisioning server.

Transport Layer Security Profiles

The Transport Layer Security (TLS) profiles describe a collection of custom CA and device certificates installed on the Polycom phones and the features where these certificates are used for authentication.

Polycom phones trusts certificates issued by widely recognized certificate authorities when trying to establish a connection to a provisioning server for application provisioning.

Customizing Certificates

You can add custom CA and device certificates to the phone and set up the phone to use the certificates for different features. For example, the phone's factory-installed or custom device certificate can be used for authentication when phone provisioning is performed by an HTTPS server. A custom CA certificate could also be used when accessing content through the microbrowser or browser.

Determining TLS Platform Profiles or TLS Application Profiles

After you install certificates on the phone, you can to determine which TLS platform profiles or TLS application profiles use these certificates. By default, TLS Platform Profile 1 uses every CA certificate and the default device certificate. Also, each TLS application uses TLS Platform Profile 1 as the default profile. You can quickly apply a CA certificate to all TLS applications by installing it on the phone and keeping the default TLS profile and default TLS application values.

Lastly, you must choose which TLS platform profile or application profile to use for each TLS application. The profiles can be used for phone provisioning, with the applications running on the microbrowser and browser, and for 802.1X, LDAP, and SIP authentication. Some applications, such as Syslog, can only use a TLS platform profile, not a TLS application profile. See <TLS/> for the list of applications.

For more information on device (or digital) certificates installed on the phones at the factory, see the section Digital Certificates.

> Web Info: For more information on using custom certificates, see *Technical Bulletin 17877: Using Custom Certificates With Polycom Phones*.

Related Topics

TLS Platform Profile and Application Profile Parameters

TLS Protocol Configuration for Supported Applications

You can configure the TLS Protocol for the following supported applications:

- Browser
- LDAP
- SIP
- SOPI
- Web server
- XMPP
- Exchange services
- Syslog
- Provisioning
- 802.1x

Related Topics

TLS Protocol Parameters

FIPS 140-2 Compliance Support

The Federal Information Processing Standard (FIPS 140-2) compliance is a cryptographic function. You can configure phones to use the FIPS 140-2 compliant cryptography using any one of the following methods:

- Phones user interface
- Web Configuration Utility
- Phone's Updater user interface
- FIPS 140-2 parameters

This feature is not supported on VVX 501 and 601 business media phones.

Related Topics

FIPS 140-2 Parameters

Download Certificates to a Polycom Phone

You can download and install up to eight CA certificates and eight device certificates on a Polycom phone. After installing the certificates, you can refresh the certificates when they expire or are revoked, and you can delete any CA certificate or device certificate that you install.

> For VVX 1500 phones, the maximum certificate size on Platform CA1 is 1536KB and 4KB for Platform CA2.

To download a certificate to a Polycom phone:

1 Navigate to **Settings > Advanced > Administrative Settings > TLS Security** and select **Custom CA Certificates** or **Custom Device Certificates**.

2 Select **Install**.

3 Enter the URL where the certificate is stored.

For example, *http://bootserver1.polycom.com/ca.crt*

The certificate is downloaded, and the certificate's MD5 fingerprint displays to verify that the correct certificate is to be installed.

4 Select **Accept**.

The certificate is installed successfully.

Mutual Transport Layer Security Authentication

Mutual Transport Layer Security (TLS) authentication is optional and initiated by the server. When the phone acts as a TLS client and the server is configured to require mutual TLS, the server requests and then validates the client certificate. If the server is configured to require mutual TLS, a device certificate and an associated private key must be loaded on the phone.

This feature requires that the phone being used has a Polycom factory-installed device certificate or a custom device certificate installed on it. In cases where a phone does not have device certificates, the phone authenticates to the server as part of the TLS authentication, but the server cannot cryptographically authenticate the phone. This is sometimes referred to as server authentication or single-sided authentication. For more information, refer to the section Digital Certificates.

The device certificate stored on the phone is used by the following:

● 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
● 802.1X authentication, if the server is configured for mutual authentication (optional for EAP-TLS)

> Note: Users cannot modify or update the digital certificate or the associated private key installed on the phone during manufacturing. Users can install a custom device certificate to be used instead of, or in addition to, the factory-installed certificate.

Polycom Root Certificate Authority

You can download the Polycom Root CA from http://pki.polycom.com/pki. 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 or your organization's CA must be downloaded onto the HTTPS server.

The following lists the tested and verified operating system and web server combinations:

- Microsoft Internet Information Services 6.0 on Microsoft Windows Server 2003
- Apache v1.3 on Microsoft Windows XP

Web Info: For more information on using Mutual TLS with Microsoft Internet Information Services (IIS) 6.0, see *Mutual Transport Layer Security Provisioning Using Microsoft Internet Information Services 6.0: Technical Bulletin 52609* at Polycom Engineering Advisories and Technical Notifications.

Configurable TLS Cipher Suites

You can control which cipher suites to offer and accept during TLS session negotiation. The phone supports the cipher suites listed in the following table. The 'Null Cipher' listed in the following table is a special case option which does not encrypt the signaling traffic, and is useful for troubleshooting purposes.

TLS Cipher Suites

Cipher	Cipher Suite
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

Related Topics

TLS Cipher Suite Parameters

Secure Real-Time Transport Protocol

Secure Real-Time Transport Protocol (SRTP) encrypts audio stream(s) to prevent interception and eavesdropping on phone calls. When this feature is enabled, the phones negotiate the type of encryption and authentication to use for the session with the other endpoint.

Web Info: For more information on SRTP, see RFC 3711. For the procedure describing how two phones set up SRTP for a call, see RFC 4568.

SRTP 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 sounds like noise and cannot be understood. Only the receiver knows the key to restore the data.

If the call is completely secure (RTP authentication and encryption and RTCP authentication and RTCP encryption are enabled), a padlock symbol displays.

Related Topics

SRTP Parameters

Phone Lock

This feature enables users to lock their phones to prevent access to menus or directories.

If the enhanced feature key (EFK) feature is enabled, you can display a Lock button on the phone to enable users to quickly lock their phones.

After the phone is locked, users can only place calls to emergency and authorized numbers. You can specify which authorized numbers users can call.

If a user forgets their password, you can unlock the phone either by entering the administrator password or by disabling and re-enabling the phone lock feature. The latter method facilitates remote unlocking and avoids disclosing the administrator password to the user.

> Note: If a locked phone has a registered shared line, calls to the shared line display on the locked phone and the phone's user can answer the call.

Related Topics

Phone Lock Parameters

Secondary Port Link Status Report

Polycom devices can detect an externally connected host connection/disconnection, informing the authenticator switch to initiate the authentication process or drop an existing authentication. This feature extends Cisco Discovery Protocol (CDP) to include a Second Port Status Type, Length, Value (TLV) that informs an authenticator switch of the status of devices connected to a device's secondary PC port.

This feature ensures the following:

- The port authenticated by the externally attached device switches to unauthenticated upon device disconnection so that other unauthorized devices cannot use it.

- The externally attached device can move to another port in the network and start a new authentication process.

- To reduce the frequency of CDP packets, the phone does not send link up status CDP packets before a certain time period. The phone immediately sends all link-down indication to ensure that the port security is not compromised.

- If the externally attached device (the host) supports 802.1X authentication, then the device can send an EAPOL-Logoff on behalf of the device after it is disconnected from the secondary PC port. This informs the authenticator switch to drop the authentication on the port corresponding with the previously attached device.

Related topics

Secondary Port Link Status Report Parameters

802.1X Authentication

Polycom phones support standard IEEE 802.1X authentication and the following EAP authentication methods:

- EAP-TLS (requires Device and CA certificates)
- EAP-PEAPv0/MSCHAPv2 (requires CA certificates)
- EAP-PEAPv0/GTC (requires CA certificates)
- EAP-TTLS/MSCHAPv2 (requires CA certificates)
- EAP-TTLS/GTC (requires CA certificates)
- EAP-FAST (optional Protected Access Credential (PAC) file, if not using in-band provisioning)
- EAP-MD5

The following figure shows a typical 802.1X network configuration with wired Polycom phones.

A typical 802.1X network configuration
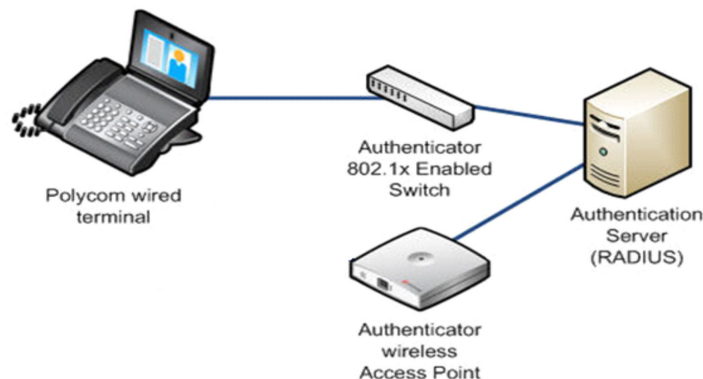
Related Topics

802.1X Authentication Parameters

Locking the Basic Settings Menu

By default, all users can access the Basic settings menu available on the RealPresence Trio 8800 system and VVX phones. From this menu, users can customize non-administrative features on their phone. You can choose to lock the Basic settings menu to allow certain users access to the basic settings menu.

If enabled, you can use the default user password (123) or administrator password (456) to access the Basic settings menu, unless the default passwords are not in use.

Related topics

Basic Settings Menu Lock Parameters

Hardware and Accessories

This section provides information on configuring phone hardware.

Ethernet Switch Connection

VVX business media phones have two Ethernet ports—labeled LAN and PC— and an embedded Ethernet switch that runs at full line rate. The SoundStructure VoIP Interface has one Ethernet port, labeled LAN. The Ethernet switch enables you to connect a personal computer and other Ethernet devices to the office LAN by daisy-chaining through the phone, eliminating the need for a stand-alone hub.

You can power each phone through an AC adapter or through a Power over Ethernet (PoE) cable connected to the phone's LAN port. If you are 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 so that audio packets from the phone have priority over packets from the PC port.

Headset and Speakerphone

All VVX phones are equipped with a handset and a dedicated RJ9 headset port. While handsets are shipped with all VVX phones, headsets are not provided. The following VVX business media phones are also equipped with a USB port you can use for a USB headset or other USB device:

- VVX 401/411
- VVX 500/501
- VVX 600/601

By default, VVX phones have dedicated keys to switch to speakerphone or headset. You can enable or disable the handsfree speakerphone mode and headset mode.

Related Topics

Headset and Speakerphone Parameters

USB Port Lock

The USB port lockdown feature enables you to choose which of the phone's USB ports to power on or off.

The port lockdown feature is available on the VVX401/411, 500/501, 600/601, and 1500 phones.

- VVX 401/411 have a single USB port at rear of the phone.
- VVX 1500 has a single USB port at the right side of the phone.

● VVX 500/501 and 600/601 phones support two USB ports, one port on the top and rear of the phones.

The top USB port on the VVX 500/501 and 600/601 supports the VVX Camera. Top and rear USB ports are enabled by default.

The phone ports support various USB devices such as USB mass storage devices and a USB headset. The following features are not available when you disable a USB port:

● Call recording

● Picture frame

● USB headset

● USB camera for video calls on the VVX 500/501 and 600/601 - no video calls

● USB charging device on the rear port of the VVX 500/501 and 600/601

> When you connect a power adapter to a VVX 500/501, the USB ports are powered on even if the parameters `feature.usbTop.power.enabled` and `feature.usbRear.power.enabled` are disabled. This can cause issues during phone reboots when USB devices are connected to the phone.

Related Topics

USB Port Lockdown Parameters

Polycom VVX Expansion Modules

The Polycom VVX Expansion Modules are consoles you can connect to VVX business media phones to add additional lines. VVX Expansion Modules enable users to efficiently perform the following tasks:

● Handle large call volumes on a daily basis

● Expand the functions of their phone

● Accept, screen, dispatch, and monitor calls

● Reduce the number of lost customer calls

● Shorten transaction times

● Increase the accuracy of call routing

Polycom VVX Expansion Modules are available for the following Polycom VVX business media phones running UC Software 4.1.6 or later:

● VVX 300 series and 400 series

● VVX 500 series and 600 series

> For all documents that help you set up and use the Polycom VVX expansion modules with your VVX phones see Polycom VVX Expansion Modules Support page.

VVX Expansion Module Features

The following features are available on the VVX LCD Color Expansion Modules and VVX Expansion Modules with a paper display:

- **VVX Expansion Modules – LCD Color Display**—VVX Color Expansion Modules feature an easy-to-navigate 272x480 LCD display. Each color expansion module provides users with 28 line keys and 3 display pages, supporting a total of 84 lines that you can set up as registrations, favorites, busy lamp field contacts, or Microsoft Skype for Business presence contacts. You can connect up to three color expansion modules to a phone to support an additional 252 line keys per phone.

  If you are registering Polycom phones with Skype for Business Server, you can use only the LCD color display expansion modules; you cannot use the paper display expansion modules for phones registered with Skype for Business Server.

- **VVX Expansion Modules – Paper Display**—VVX Expansion Modules with a paper display provide users with 40 line keys that you can set up as registrations, favorites, or busy lamp field contacts. You can connect up to three expansion modules to your phone to support an additional 120 line keys per phone.

The following figure illustrates the LCD color and paper expansion modules.

Expansion Module LCD color display and paper display

Expansion Module Line Keys

The line keys on VVX phones and expansion modules are numbered sequentially, and the line key numbering on an expansion module depends on how many lines the phone supports. For example, a VVX 600/601 phone supports 16 lines, numbered 1-16. The first line on an expansion module connected to a VVX 600/601 phone is line 17.

For a list of the maximum registrations and other call appearances supported on each phone model, refer to the table Flexible Call Appearances.

VVX Expansion Module Power Values

Polycom VVX phones use more power when you connect an expansion module. The following table outlines the power each phone uses when you connect an expansion module, as well as the power value sent in LLDP-MED. For a list of power values for all Polycom phones without an expansion module attached, see Power Values.

VVX Expansion Module Power Values

Model	Power Usage (Watts)	Power Value Sent in LLDP-MED Extended Power Via MDI TLV
VVX 300/301	5.0	5000mW
VVX 310/311	5.0	5000mW
VVX 400/401	5.0	5000mW
VVX 410/411	5.0	5000mW
VVX 500/501	8.0	8000mW
VVX 600/601	8.0	8000mW

Generate a Line Key PDF for Paper VVX Expansion Modules

Using the Web Configuration Utility, you can generate and download a PDF file with the line key configuration for each paper display expansion module connected to a VVX phone. The generated PDF enables you to print line key information for line keys on your expansion modules and insert the PDF as a directory card on expansion modules.

To generate and download the line key information PDF using the Web Configuration Utility:

1 In a web browser, enter your phone's IP address into the address bar.

2 Log in as an **Admin**, enter the password, and select **Submit**.

3 Select **Utilities > EM Directory**.

4 Select the expansion module you want to generate a PDF for. For example, select EM1.

5 In the confirmation dialog, select **Yes** to download the PDF for the configured lines for your expansion module.

6 Select **Save > Open**.

The PDF with the configured line key information for your expansion module displays.

After you download the PDF with configured line key information for your expansion module, you can print the PDF and insert the PDF as the directory card for the expansion module.

Smart Paging on VVX Expansion Modules

The smart paging feature arranges line key assignments and distributes pages on the VVX Color Expansion Modules based on the number of expansion modules connected to a VVX phone. Smart paging is automatically enabled for color expansion modules connected to VVX phones with UC Software 5.1.0 or later, and is not available on the VVX Expansion Modules with a paper display.

Note that when the flexible line key feature is enabled, the expansion module ignores the smart paging configuration and line key assignments display on the designated line key.

> Smart paging applies only when you connect more than one expansion module to a VVX phone. If you connect one expansion module, the order of pages is sequential even if smart paging is disabled.

Smart Paging Distribution Scenarios

When you enable smart paging, the pages on the color expansion module are distributed across the connected expansion modules, as described in the following scenarios.

● If only one expansion module is connected to the VVX phone, the pages are ordered sequentially on the module: pages 1, 2, and 3.

● If two expansion modules are connected, the pages are ordered non-sequentially across both expansion modules where pages 1, 3, and 4 are on the first expansion module, and pages 2, 5, and 6 are on the second expansion module.
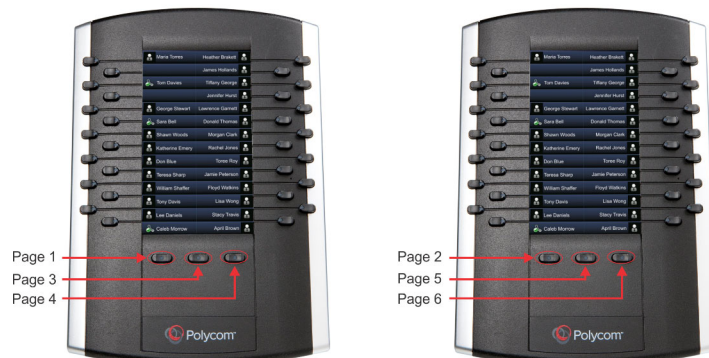
● If you are using three connected expansion modules, the pages are distributed across all modules where pages 1, 4, and 5 are on the first expansion module, pages 2, 6, and 7 are on the second expansion module, and pages 3, 8, and 9 are on the third expansion module.

Page 1
Page 4
Page 5

Page 2
Page 6
Page 7

Page 3
Page 8
Page 9

Related Topics

Configuring Smart Paging

Power-Saving

The power-saving feature automatically turns off the phone's LCD display when not in use. Power-saving is available for the following phones:

- VVX 201 phones
- VVX 300/301/310/311 phones
- VVX 400/401/410/411 phones
- VVX 500/501 phones
- VVX 600/601 phones
- VVX1500 phones.

Power-saving is enabled by default for the VVX 500/501, 600/601, and 1500 phones.

You can configure the following power-saving options:

- Turn on the phone's power-saving feature during non-working hours and working hours.

  If you want to turn on power-saving during non-working hours, you can configure the power-saving feature around your work schedule.

- On the VVX 1500, use the `powerSaving.userDetectionSensitivity.*` parameters to configure the sensitivity of the built-in motion detection system and an idle time after which the phone enters the power-saving mode.

When you enable power-saving mode and the phone is in low power state, the red LED indicator flashes at three second intervals to show that the phone still has power.

> Note: When you enable power-saving mode on VVX 500 and 600, the phone display screen does not automatically turn back on after going idle.

Related Topics

Power-Saving Parameters

Polycom Desktop Connector

With the Polycom® Desktop Connector™ application installed on a computer, users can use their mouse and keyboard to enter information and navigate screens on a VVX business media phone without having to use the phone's keypad or touchscreen. The Polycom Desktop Connector application is compatible with computers running Microsoft® Windows XP®, Windows Vista®, and Windows® 7.

After the Polycom Desktop Connector is installed, users need to use one of two methods to pair the VVX phone and the computer:

● Direct—If the phone is connected directly to the computer over Ethernet, users can select Reconnect to connect the phone with the desktop application.

● Indirect—If the phone is connected to the computer through a switch or hub, users can enter the computer's IP address into the phone's user interface and select Reconnect.

> For details on how to install Polycom Desktop Connector application and enable it for use on VVX phones, see the latest *Polycom VVX Business Media Phones User Guide* at Latest Polycom UC Software Release.

Related Topics

Configuring Polycom Desktop Connector

Polycom VVX D60 Wireless Handset and Base Station

The Polycom® VVX® D60 Wireless Handset provides busy users with the superior voice quality and features of a VVX business media phone that they can use to manage calls when they are away from their desk. You can pair one base station and register up to 5 wireless handsets to the VVX 300 series, 400 series, 500 series, and 600 series phones.

Related Topics

Parameters for VVX D60 Wireless Handsets

Features Supported on VVX D60 Wireless Handsets

The following table includes common features that are and are not supported on VVX D60 wireless handsets.

Supported Features on VVX D60 Wireless Handsets

Feature	Supported
Busy Lamp Field (BLF)	Yes (on paired VVX)
Hunt Groups	Yes (on paired VVX)
Local Conference Calling	Yes
Push-to-Talk	No
Shared Line Appearance/Shared Call Appearances	Yes (BroadSoft only)
Simultaneous Calls (G.729 Encode/Decode)	Yes (maximum 4 active calls)
Skype for Business Line Registration	No
USB Call Media Recording (CMR)	No
VVX Camera	Yes
VVX Expansion Module	Yes
Flexible Line Keys (FLK)	Yes (on paired VVX)
Automatic Call Distribution (ACD) / Hoteling	No
CDP support on VVX D60 base station	Yes
Call HandOff Between VVX D60 Handsets and VVX Business Media Phones on twinned lines	Yes

Supported Features on VVX D60 Wireless Handsets

Feature	Supported
Configure maximum number of handsets	Yes
Pairing using Mac address of VVX D60	Yes

The VVX D60 base station can access Voice VLAN through Link-Layer Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP). The VVX D60 base station supports CDP and is enabled by default on the VVX D60 base station.

> After connecting the D60 base station to a LAN port, allow the base station at least one minute to connect to the voice VLAN network and to acquire an IP address. Wait at least one minute after connecting the base station to a LAN port before pairing the base station with a VVX business media phone.

Pairing a VVX Business Media Phone with a VVX D60 Base Station

You can pair the VVX D60 base station and register the wireless handset to a VVX business media phone using the local phone interface, the Web Configuration Utility, or through the provisioning server. You can use the following methods to pair the base station with a VVX business media phone:

- PC Port pairing
- Automatic pairing
- Manual pairing
- MAC address pairing

Limitations to MAC Address Pairing

The limitations for pairing of VVX business media phones and the VVX D60 base station through MAC address are as follows:

- User actions are given higher precedence. Consider the user unpairs the VVX D60 base station that is paired to the VVX business media phone using the configuration file and then the user pairs manually through automatic pairing or PC port pairing. In this case, if the VVX business media phone restarts due to a power outage or software update, then the VVX business media phone re-pairs with the VVX base station which is paired using the non-MAC based pairing mode.
- If the user unpairs the VVX D60 base station, then the base station does not pair automatically with the VVX business media phone.
- If the device is currently paired and the current pairing mode is other than through the MAC address, the VVX business media phone logs a warning provided the configuration parameter `VVXD60.base.mac` is set.
- The configuration parameter `VVXD60.base.mac` is applied only if `feature.dect.enabled` is enabled.

Get the IP Address of the Base Station

If you use Manual Pairing to pair the base station with the VVX business media phone, you need to use your computer to get the IP address of the base station. You can use either the Static or DHCP IP address to pair the base station with the phone.

To get the static or DHCP IP address of the base station:

1 Connect the Ethernet cable from the PC port on the base station to an Ethernet port on a computer.

2 On the computer, navigate to **Network and Sharing Center**, then select **Local Area Connection**.

3 Click **Properties**, select **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**.

4 Select **Use the following IP address**, then enter the following values into the associated fields:

  ➢ IP Address: **192.168.0.10**

  ➢ Subnet mask: **255.255.255.0**

  ➢ Default Gateway: **192.168.0.1**

5 Click **OK**.

6 In a web browser, enter **https://192.168.0.2**.

7 In the Web Configuration Utility, enter the following default credentials:

  ➢ User name: **Polycom**

  ➢ Password: **456**

8 Navigate to **Settings > Network Settings**.

  The IP address of the base station displays in the IP Settings tab.

VVX D60 Base Station Pairing Permissions

By default, users are not allowed to pair or unpair a VVX D60 base station with a VVX business media phone. Administrators can control whether users are allowed to pair a base station only, unpair a base station only, or pair and unpair a base station with a VVX business media phone. The administrator can use the parameter `VVXD60.allowPairing` to configure this feature. For more information on configuring this feature using configuration parameter, see Features Supported on VVX D60 Wireless Handsets.

Pairing the Base Station using the Web Configuration Utility

You can pair the VVX D60 base station using the Web Configuration Utility in the following methods:

● PC Port pairing

● Automatic pairing

● Manual pairing

● MAC address pairing

Pair using PC Port Pairing

When the Ethernet cable is connected to the LAN port on the VVX D60 base station and the PC port on a VVX phone, the phone initiates SSH tunneling and pairs with the base station automatically.

To pair the base station via the PC port:

1   Sign into the Web Configuration Utility, and navigate to **Settings > VVX D60 Settings**.

2   Click the **VVX D60 Profile** check box and select **PC Port** in the **Pairing Mode** drop-down.

Pair using Automatic Pairing

When the Ethernet cable is connected from the base station LAN port into a LAN outlet, the phone pairs with the base station automatically.

All base stations on the network are displayed automatically in the VVX Web Configuration Utility as long as the devices are on the same subnetwork and VLAN.

To pair with the base station via Automatic Pairing:

1   Sign into the Web Configuration Utility, and navigate to **Settings > VVX D60 Settings**.

2   Click the **VVX D60 Profile** check box and select **Automatic** in the **Pairing Mode** drop-down.

A list of discovered base stations and wireless handsets display.

3   Select a base station and click **Pair**.

Pair using Manual Pairing

When the Ethernet cable is connected from the base station LAN port to the VVX phone's PC port or when the Ethernet cable is connected from the base station LAN port into a LAN outlet, you can manually enter the base station IP address to pair with a VVX business media phone. Manual pairing enables you to pair the base station with the phone without the base station being on the same subnetwork or VLAN as the VVX phone.

> When the VVX D60 base station is connected to a subnet that is different than that of the VVX business media phone, Polycom recommends that you either configure the IP address of the VVX D60 base station statically or via static DHCP. This will help to minimize pairing issues if the IP address of the VVX D60 base station changes.

To pair with the base station via Manual Pairing:

1   Sign into the Web Configuration Utility, and navigate to **Settings > VVX D60 Settings**.

2   Click the **VVX D60 Profile** check box and select **Manual** in the **Pairing Mode** drop-down.

3   Enter the IP address of the base station.

The base station's information displays.

Pair using MAC Address Pairing

When the Ethernet cable is connected from the base station LAN port into a LAN outlet or an outlet with external power supply of the VVX D60 base station, you can manually select to pair using the MAC address.

To manually pair using the Web Configuration Utility:

1 Sign into the Web Configuration Utility, and navigate to **Settings > VVX D60 Settings**.

2 Click the **VVX D60 Profile** check box and select **MAC Address** in the **Pairing Mode** drop-down.

3 Enter the **base station MAC Address**.

4 Click **Pair**.

Pairing the Base Station using the Local Phone Interface

You can pair the VVX D60 base station using the local phone interface in the following methods:

● PC Port pairing

● Automatic pairing

● Manual pairing

● MAC address pairing

Pair using PC Port Pairing

When the Ethernet cable is connected from the base station LAN port to the PC port on the VVX phone, the phone pairs with the base station automatically.

To pair with the base station via PC Port Pairing:

1 On the phone, navigate to **Settings > Advanced**, and enter the password.

2 Select **Administration Settings > VVX D60 Configuration**.

3 Select **VVX D60 Profile**, then select **Enable**.

4 On the **VVX D60 Configuration** screen, select **base station**, then select **PC Port Pairing**.

Pair using Automatic Pairing

When the Ethernet cable is connected from the base station LAN port into a LAN outlet, the phone pairs with the base station automatically.

All base stations on the network are displayed automatically on the VVX phone as long as the devices are on the same subnetwork or VLAN.

To pair with the base station via Automatic Pairing:

1 On the phone, navigate to **Settings > Advanced**, and enter the password.

2 Select **Administration Settings > VVX D60 Configuration**.

3 Select **VVX D60 Profile**, then select **Enable**.

4 On the **VVX D60 Configuration** screen, select **base station**, then select **Auto Pairing**.

Pair using Manual Pairing

When the Ethernet cable is connected from the base station LAN port to the VVX PC port or when the Ethernet cable is connected from the base station LAN port into a LAN outlet, you can manually enter the base station IP address to pair with a VVX phone. Manual pairing enables you to pair the base station with the phone without the base station being on the same subnetwork or VLAN as the VVX phone.

To pair with the base station using manual pairing:

1 On the phone, navigate to **Settings > Advanced**, and enter the password.

2 Select **Administration Settings > VVX D60 Configuration**.

3 Select **VVX D60 Profile**, then select **Enable** and go to the previous menu

4 On the **VVX D60 Configuration** screen, select **base station**, then select **Manual Pairing**.

5 Enter the IP address of the base station, then select **Pair**.

The base station's information displays.

Pair using MAC Address Pairing

When the Ethernet cable is connected from the base station LAN port into a LAN outlet, you can manually select to pair using the MAC address. If the phone is already configured with a MAC address using configuration parameter, you can choose **Skip**.

To pair with the base station using manual pairing:

1 On the phone, navigate to **Settings > Advanced**, and enter the password.

2 Select **Administration Settings > VVX D60 Configuration**.

3 On the **VVX D60 Configuration** screen, do one of the following:

➢ Select **Skip** to manually pair with a different base station.

➢ Select **Continue** to pair with the configured MAC address.

If you select neither **Skip** nor **Continue**, a timer is displayed and the VVX business media phone pairs with the configured MAC address.

4 On the **Manual Pairing** screen, select **base station MAC ID**.

5 Edit the configured **base station MAC ID** with the new address.

The configuration parameter for the VVX business media phone gets updated with the new MAC address.

Unpairing the Base Station for MAC Address-Based Pairing

You can unpair the VVX D60 base station by removing the corresponding MAC address in the configuration parameter `VVXD60.base.mac`. If the MAC address configured in the parameter `VVXD60.base.mac` is

modified, the VVX business media phone unpairs the existing VVX D60 base station and tries to pair with VVX D60 base station with the modified MAC address.

Continuous Attempt to Re-pair with a VVX D60 Base Station

If the VVX business media phone unpairs from a previously paired VVX D60 base station for any reason, such as a power outage, the phone will continuously attempt to pair with the base station again until the phone and base station are successfully paired.

This is achieved with the following mechanisms:

- A unicast re-pairing beacon packet is sent to the last known IP address of the VVX D60 base station.
- Three seconds later, a broadcast re-pairing beacon packet is sent to the broadcast address. This is used in case the IP address of the VVX D60 base station has changed.
- The VVX phone waits for a random time interval, between 30 and 60 seconds before resending the unicast and broadcast re-pairing beacon packets.

If the VVX D60 base station and the VVX business media phone are in the same subnet, the VVX phone tries to send the unicast re-pairing beacon packet three times; after the third attempt, only the broadcast re-pairing beacon packet is tried indefinitely. If the VVX D60 base station and VVX business media phone are in different subnets, the VVX phone tries to send resend the unicast and broadcast re-pairing beacon packets.

If a user no longer wants the base station to pair with the phone, the user must contact a system administrator to cancel the pairing attempt.

After powering on, the VVX D60 base station may take up to 60 seconds to re-pair with the VVX business media phone.

Registering Handsets for VVX D60 Base Station

You can control the number of handsets that can be registered to the VVX D60 base station. A minimum of one and a maximum of five handsets can be configured for a VVX D60 base station. This is configurable from the VVX business media phone and Web Configuration Utility. Upon pairing, the VVX business media phone makes sure that maximum handsets registered to the paired VVX D60 base station is lesser or equal to the configured value. After reaching the maximum limit of handsets, the VVX D60 base station and the VVX business media phone does not provide any mechanism to register a new handset. The administrator can use the parameter `VVXD60.handset.maxCount` to configure this feature. For more information on configuring this feature using configuration parameter, see Features Supported on VVX D60 Wireless Handsets.

If the VVX D60 base station is registered with more handsets than the configured number of handsets, then the handsets will be deleted in the following order:

- Blocked → Unavailable → Available (the last handset that was registered among the available handsets)

Maximum Number of Handsets

You can use the Web Configuration Utility or local phone interface to configure the maximum number of handsets that can be registered to the VVX D60 base station.

Set the Maximum Number of Registered Handsets using the Web Configuration Utility

You can configure the number of VVX D60 handsets that can be configured for a VVX base station using the Web Configuration Utility.

To configure the number of VVX D60 handsets using the Web Configuration Utility:

1   On the Web Configuration Utility, login as the administrator and navigate to **Settings > VVX D60 Settings**.
2   In the **Max Configurable Handsets** page displayed, enter the number of headsets to be registered to the VVX D60 base station.

Set the Maximum Number of Registered Handsets using the Local Phone Interface

You can configure the number of VVX D60 handsets that can be configured for a VVX base station using the VVX business media phone interface.

To configure the number of VVX D60 handsets using the VVX business media phone:

1   On the VVX business media phone, navigate to **Settings > Advanced Settings > Administration Settings > VVX D60 Settings > Handset Configuration**.
2   In the **Max Configurable Handsets** page displayed, enter the number of headsets to be registered to the VVX D60 base station.

Register a VVX D60 Wireless Handset

After the base station is paired with the VVX phone, you can register up to five wireless handsets to the base station.

To register the wireless handset with the base station:

1   On the wireless handset, navigate to **Settings > Features > Registration**.
2   Select **Register**.
3   Press and hold the **Find** button on the base station for a few seconds.
4   On the wireless handset, confirm the registration with the base station.

Unregister a VVX D60 Wireless Handset

You can unregister a wireless handset from the base station when you need to replace a wireless handset with another one.

To unregister a wireless handset:

1　On the wireless handset, navigate to **Settings > Features > Registration**.

2　Select **Deregister**.

3　Confirm you want to unregister the wireless handset.

Set a Unique Name for the Base Station and Wireless Handset

In the Web Configuration Utility, you can set a unique name for each base station and wireless handset to distinguish between multiple sets of base stations and wireless handsets. You can also set a unique name for the base station and wireless handsets from the local phone interface.

Note that the Intercom feature must be enabled to change the name of a wireless handset. You cannot set a unique name for a wireless handset if the Intercom feature is disabled.

To set a unique name for the base station and registered wireless handsets:

1　In the Web Configuration Utility, navigate to **Settings > VVX D60 Settings**.

2　Under **base station Settings**, enter a unique name in the **Name** field.

3　Under **Handset Settings**, enter a unique name in the **Display Name** field for each registered handset.

Assigning Lines to the VVX D60 Wireless Handset

After you have paired the base station to a VVX phone and registered wireless handsets to the base station, you can assign lines to each wireless handset. You can assign up to five lines to each wireless handset.

When assigning lines, keep the following in mind:

● The first line is assigned to the VVX phone.

● For Private Lines, you can assign each line to the VVX phone or the Wireless Handset or both.

● For Shared lines (SCA/SLA), you can assign each line only to one device: VVX phone or Wireless Handset.

Assign Lines using the Web Configuration Utility

You can assign lines to the wireless handset using the Web Configuration Utility.

To assign lines to a VVX wireless handset:

    1 In the Web Configuration Utility, navigate to **Settings > VVX D60 Settings**.

    2 In the Handset Settings section, click **Map Lines**.

    3 Choose the lines you want to map to a registered wireless handset.

    4 Click **Update**.

Assign Lines using the Phone Interface

You can assign lines to the wireless handset from the Advanced settings menu on the VVX phone.

To assign lines to a VVX wireless handset:

    1 On the phone, navigate to **Settings > Advanced**, then enter your password.

    2 Select **Administration Settings > VVX D60 Configuration > Map Lines**.

    3 Choose a line, then choose a registered wireless handset for the line.

Update the VVX D60 Wireless Handset Software

When you update the VVX host phone with the latest supported software version using the master configuration file that includes the file path to the dect.ld, the software on the base station and wireless handsets update automatically within two minutes after they are paired and registered with the VVX business media phone. The base station updates first, then each wireless handset is updated sequentially with the first registered handset updating first, followed by each remaining handset.

Refer to the section `Master Configuration File` for more information on the fields in the master configuration file.

To update the wireless handset software:

    1 Place the handset in the base station or charging cradle, and ensure the handset battery is charged to at least 50%.

    2 When prompted, accept the update notification.

       If you do not accept the update notification, the wireless handset will begin the update 20 seconds after the notification displays.

If the base station or any of the wireless handsets fail to update, refer to the section `Wireless Handset Software Upgrade Issues` for troubleshooting tips.

Update the Wireless Handset Software Manually

If the software update notification does not display on the wireless handset within five minutes of registering the wireless handset, you can check for configuration updates and manually update the software from the VVX host phone.

To update the wireless handset software manually:

1   Place the handset in the base station or charging cradle, and ensure the handset battery is charged to at least 50%.

2   On the VVX host phone, navigate to **Settings > Basic > Update Configuration**.

    If there is a software update available, the wireless handsets update sequentially with the first registered handset updating first.

Configure VVX D60 Network Settings

By default, you can edit network settings for the VVX D60 base station. You can use the Web Configuration Utility to make changes to the base station's network settings.

To configure VVX D60 network settings:

1   In a web browser, enter `https://<IP address of D60 base station>`

2   In the Web Configuration Utility, enter the following default credentials:

    ➢ User name: **Polycom**

    ➢ Password: **456**

3   Navigate to **Settings > Network Settings**.

4   Update the desired network settings - IP settings, LLDP, CDP, VLAN, QOS, SNTP address and DNS.

5   Click **Submit.**

Device and Software Support

This section provides information on updating and maintaining your devices and the UC Software.

You can upgrade the software that is running on the Polycom phones in your organization. The upgrade process varies with the version of Polycom UC Software that is currently running on your phones and with the version that you want to upgrade to.

- As of UC Software 5.3.0, you can update software with the user-controlled software update feature explained in the section User-Controlled Software Update.
- If you are updating software from UC Software 4.0.x, see the section Update Phones from UC Software 4.0.x.

The Updater, UC Software executable, and configuration files can all be updated using centralized provisioning.

Updating UC Software on a Single Phone

You can use the software upgrade tool in the Web Configuration Utility to update the UC Software version running on a single phone. For instructions, see *Use the Software Upgrade Tool in the Web Configuration Utility: Feature Profile 67993* at Polycom Engineering Advisories and Technical Notifications.

Configuration changes made to individual phones using the Web Configuration Utility override configuration settings made using central provisioning. For information about using multiple provisioning methods, refer to Polycom Provisioning Methods.

User-Controlled Software Update

This feature is available on VVX business media phones as of UC Software 5.3.0 and enables phone users to choose when to accept software updates the administrator sends to the phones. Administrators can send an earlier or a later software version than the current version on the phone.

User-controlled updates apply to configuration changes and software updates you make on the server and Web Configuration Utility. If a user postpones a software update, configuration changes and software version updates from both the server and Web Utility are postponed. When the user chooses to update, configuration and software version changes from both the server and Web Utility are sent to the phone.

This feature does not work if you have enabled ZTP or Skype for Business Device Update, and is not available with Skype for Business.

Related Topics

User-Controlled Software Update Parameters

Ports Used on Polycom Phones

The following table lists the ports currently used by the Polycom UC Software.

Ports Used by Polycom Phones

Port Number	Protocol	Outgoing	Incoming	UDP or TCP
21	FTP	Provisioning, Logs		TCP
22	SSH	Admin	Admin	TCP
23	Telnet[1]	Admin		TCP
53	DNS			UDP
67	DHCP	Server		UDP
68	DHCP	Client		UDP
69	TFTP	Provisioning, Logs		UDP
80	HTTP	Provisioning, Logs, Pull Web interface, Poll		TCP
123	NTP	Time Server		UDP
389	LDAP			
443	HTTPS	Provisioning, Logs	HTTP Pull Web interface, HTTP Push	TCP
514	Syslog	Logs		
636	LDAP			
1719	H.323[2]	RAS Signaling	RAS Signaling	
1720	H.323[2]	Signaling	Signaling	
2222	RTP[3]	Media Packets	Media Packets	
2223	RTCP[3]	Media Packet Statistics	Media Packet Statistics	
5060	SIP	SIP signaling	SIP signaling	
5061	SIP over TLS	Secure signaling	Secure signaling	
24800	PDC	PDC Client messages	PDC Server messages	TCP

[1] Telnet is disabled by default on VVX phones.

[2] H.323 is available only on the VVX 500/501, 600/601, and 1500.

[3] RTP and RTCP can use any even port between 2222 and 2269 (2317 on VVX 500/501, 600/601, or 1500), but you can configure ports by setting `tcpIpApp.port.rtp.mediaPortRangeStart`.

Updating to a Previous UC Software Release

If you are using UC Software 4.0.0 or later and want to update to a previous software release, follow the instructions in *Upgrading Polycom Phones to and Downgrading Phones from Polycom UC Software 4.0.0*: T*echnical Bulletin 64731 at* Polycom Engineering Advisories and Technical Notifications.

Update Phones from UC Software 4.0.x

If your Polycom phones are running UC Software 4.0.x or later, you can update to a later UC Software version using the instructions in this section. If your phones are running a software release earlier than UC Software 4.0.x, you can update to UC Software 4.0.x following the instructions in *Technical Bulletin 64731: Upgrading Polycom Phones to and Downgrading Phones From Polycom UC Software 4.0.0* at Polycom Engineering Advisories and Technical Notifications.

> To ensure predictable phone behavior, the configuration files listed in CONFIG_FILES attribute of the master configuration file must be updated when the software is updated. For information on this attribute refer to Master Configuration File Fields.

To update phones to a version later than Polycom UC Software 4.0.1:

1 Back up your existing application and configuration files.

2 Create your new configuration using UC Software 4.1.0.

   Configuration file changes and enhancements are explained in the Release Notes that accompany the software.

3 Save the new configuration files and images (such as sip.ld) on your provisioning server.

4 Reboot the phones using an automatic method such as polling or check-sync.

   ➢ Reboot your phone manually as a backup option only if another reboot method fails. For details on manually rebooting a phone, refer to Multiple Key Combinations.

   ➢ You can boot the phones remotely through the SIP signaling protocol. Refer to <voIpProt.SIP.specialEvent.*/>.

You can configure the phones to periodically poll the provisioning server for changed configuration files or application executables. If a change is detected, the phone may reboot to download the change.

Trusted Certificate Authority List

Polycom maintains and publishes a list of trusted certificate authorities (CAs) supported by each major Polycom UC Software release. To find the list of supported CAs for your UC Software version, see *Certificate Updates for Polycom UC Software – Technical Update* for your UC Software version at Voice Support. Polycom publishes the following details for each trusted CA:

● Certificate Common Name (CN)

● RSA public key size

● Signature algorithm

● Start and end date of certificate validity

Polycom makes every effort to maintain a built-in list of the most commonly used Certificate Authority (CA) certificates. Due to memory constraints, we cannot ensure a complete set of certificates.

If you are using a certificate from a commercial CA not currently support, you can submit a feature request for Polycom to add your CA to the trusted list. You can also load your particular CA certificate into the phone using the custom certificate method shown in *Using Custom Certificates on Polycom Phones - Technical Bulletin 17877* at Polycom Engineering Advisories and Technical Notifications.

OpenSSL Versions List

This section lists Open SSL versions used for each UC Software release.

OpenSSL Versions

UC Software Version	OpenSSL Version
UC Software 5.6.0	OpenSSL 1.0.2j 26 Sep 2016
UC Software 5.5.2	OpenSSL 1.0.2j 26 Sep 2016
UC Software 5.5.1	OpenSSL 1.0.1p 9 Jul 2015
UC Software 5.5.0	OpenSSL 1.0.1p 9 Jul 2015
UC Software 5.4.6	OpenSSL 1.0.1p 9 Jul 2015
UC Software 5.4.5	OpenSSL 1.0.1p 9 Jul 2015
UC Software 5.4.4	OpenSSL 1.0.1p 9 Jul 2015
UC Software 5.4.3	OpenSSL 1.0.1p 9 Jul 2015
UC Software 5.4.1	OpenSSL 1.0.1m 19 March 2015
UC Software 5.4.0	OpenSSL 1.0.1m 19 March 2015
UC Software 5.3.3	OpenSSL 1.0.1m 15 Oct 2014
UC Software 5.3.2	OpenSSL 1.0.1m 15 Oct 2014
UC Software 5.3.1	OpenSSL 1.0.1m 15 Oct 2014
UC Software 5.3.0	OpenSSL 1.0.1j 15 Oct 2014
UC Software 5.2.2	OpenSSL 1.0.1j 15 Oct 2014
UC Software 5.2.0	OpenSSL 1.0.1h 5 Jun 2014
UC Software 5.1.3	OpenSSL 1.0.1h 5 Jun 2014
UC Software 5.1.2	OpenSSL 1.0.1h 5 Jun 2014
UC Software 5.1.0	OpenSSL 1.0.1h 5 Jun 2014
UC Software 5.0.2	OpenSSL 1.0.1c 10 May 2012
UC Software 5.0.1	OpenSSL 1.0.1c 10 May 2012

OpenSSL Versions

UC Software Version	OpenSSL Version
UC Software 5.0.0	OpenSSL 1.0.1c 10 May 2012
UC Software 4.1.8	OpenSSL 1.0.1h 5 Jun 2014
UC Software 4.1.6	OpenSSL 1.0.1c 10 May 2012
UC Software 4.0.11	OpenSSL 0.9.8zg 11 Jun 2015
UC Software 4.0.10	OpenSSL 0.9.8zc 11 Jun 2015
UC Software 4.0.9	OpenSSL 0.9.8zc 15 Oct 2014
UC Software 4.0.8	OpenSSL 0.9.8zc 15 Oct 201
UC Software 4.0.0 - 4.0.7	OpenSSL 0.9.8k 25 Mar 2009

Third-Party Servers

This section provides information on configuring phones and features with third-party servers.

Alcatel-Lucent Converged Telephony Server

This section shows you how to configure Polycom phones with Alcatel-Lucent (ALU) Converged Telephony Server (CTS).

Advanced Conferences

When users are signed into the ALU CTS on VVX phones, they can initiate ad-hoc conference calls with two or more contacts. Users can also create a participant list and manage conference participants. This feature is not supported on VVX 101 and 201 phones.

Advance Conference includes the following features:

- **Roster**   Provides a list of participants in the conference
- **Conference Controller**   The person who creates the conference and can add or drop participants, and mute and unmute participants.
- **Push-to-Conference**   Enables users to create a list of participants when initiating a conference call.
- Join two calls into a conference call
- Join a call to an active call to make a conference call

Related Topics

Configuring Advanced Conferences

Shared Call Appearance

The Shared Call Appearance feature enables users who share a line to monitor and bridge into calls on the shared line. Each line supports up to 21 call appearances. This feature is disabled by default. You can enable the feature and configure the hold request for the line. This feature is supported on VVX 300 series, VVX 400 series, VVX 500 series, and VVX 600 series phones.

Note the following when using shared call appearance with ALU CTS:

- Members of the SCA group cannot resume remotely held calls.
- The phones support 21 shared call appearances per line.

- The maximum number of calls associated with a shared call appearance group is the same as the number of calls provisioned for that shared line.
- An incoming call to a shared call appearance group can be presented to the group as long as there is one available idle call appearance.
- All shared call appearances are able to receive and originate calls, regardless of the call activity on the other shared call appearances.
- Users can bridge into an active SCA call that is in shared mode.

Related Topics

Configuring Shared Call Appearance

Bridge In for Shared Call Appearance

Bridge In is for Shared Call Appearance lines registered with the ALU CTS. This feature enables multiple users in a Shared Call Appearance group to view and bridge into active calls on a shared line. By default, group members can bridge into active calls only. Users cannot bridge into held or incoming calls. Multiple people can bridge into one active call.

This feature is not supported on VVX 1500 business media phones.

Related Topics

Configuring Bridge In

Barge-In for Busy Lamp Field Lines

This feature enables users to barge in on active and held calls on Busy Lamp Field (BLF) lines and supports three barge-in modes: Normal, Whisper and Silent. The Barge In feature for BLF lines is disabled by default.

This feature is not supported on VVX 1500 business media phones.

Related Topics

Configuring Barge In

Dual Tone Multi Frequency (DTMF) Relay

This feature enables users to press DTMF commands during active SIP audio calls and conference calls to perform actions. This feature is not supported for H.323 calls.

Related Topics

Configuring DTMF Relay

Visitor Desk Phone

Visitor desk phone (VDP) enables users registered with the ALU CTS to access personal settings on a shared phone after logging in. After the user logs in, the user profile configuration file is downloaded to the phone, and the user can access any enabled services, such as message-waiting indicator, busy lamp field, or shared call appearance. VDP is not supported on VVX 1500 business media phones.

If a user logs into a second phone when already logged into a first phone, the user is automatically logged out of the first phone. When logged in or out, users can dial an access code to play a message indicating if that user is logged in to a phone and the remaining time in a session.

On the server, you can configure the duration of a login period after which the user must re-enter credentials to the phone. When the time is nearing expiration, the server calls the phone and plays a message indicating the remaining time and prompts the user to re-enter credentials to extend the session.

Related Topics

Configuring Visitor Desk Phone

GENBAND Server

GENBAND's application server, also called EXPERiUS™ A2, provides full-featured, IP-based multimedia communications applications for business and consumers. You can deploy EXPERiUS A2 as a standalone server or in combination with a GENBAND CONTiNUUM™ C20 server; features vary depending on your deployment.

Polycom has performed interoperability tests with GENBAND C20 with Polycom VVX 300 series, 400 series, 500 series, 600 series, and 1500 phones.

The following features are available for phones registered with the GENBAND servers:

- **MADN-SCA**—A shared group feature that provides support for conference barge in, privacy, and remote call appearance. MADN-SCA requires you to deploy EXPERiUS A2 and CONTiNUUM C20 server.
- **Global Address Book**—The global address book (GAB) feature is a corporate directory application managed by the GENBAND server.
- **Personal Address Book**—The personal address book (PAB) feature is managed by the GENBAND server and allows multiple clients (phones, computer software) to read and modify a user's personal directory of contacts. When one client changes a contact all other clients are immediately notified of the change by the GENBAND server.
- **E.911**—Enhanced 911 services specific to GENBAND C20 server implementation.

Multiple Appearance Directory Number – Single Call Appearance (MADN-SCA)

Multiple appearance directory number—single call appearance (MADN-SCA) enables a group of users to share a single directory number that displays as a single line to each member of the group. When this feature is enabled, users can initiate or receive calls on this shared line. MADN-SCA requires you to deploy EXPERiUS A2 and CONTiNUUM C20 server.

Only one call can be active on the line at a time on the MADN-SCA shared line. When a call is in progress, any incoming calls to the line receive a busy tone.

Related Topics

Configuring MADN-SCA

Configuring Privacy on a MADN-SCA Line

In the UC Software download, Polycom provides the following two sample enhanced feature key (EFK) macros that you can configure to display on the phone to change privacy states: `privacyReleaseRestoreESK.cfg` and `privacyEnableESK.cfg`.

When you set the line to shared, an incoming call alerts all the members of the group simultaneously, and the call can be answered by any group member. On the server, you can configure a privacy setting that determines whether or not, after the call is answered, other members of the group can barge in to the same call and whether or not a call on hold can be picked up by other members of the group.

Optionally, you can configure star codes on the server that you can dial on the phone to toggle the privacy setting during a single active call. Note the following call behavior. If the line is configured for privacy by default, you can use a star code to toggle privacy on and off during an active call. When the call ends, the line resets to privacy settings. If the line is configured on the server with privacy off, you can use a star code to toggle to privacy on during an active call but you cannot toggle back to privacy off during the call. When the call ends, the line resets to privacy off.

Example MADN-SCA Configuration

The following example configuration shows the minimum configuration you need to enable MADN-SCA on the phone. You can use the parameters in the template configuration files or create your own configuration file from the parameters.

To configure MADN-SCA:

1. Enter values for the following parameters in a configuration file and save. The value `8630@polycom.com` is an example registration address.
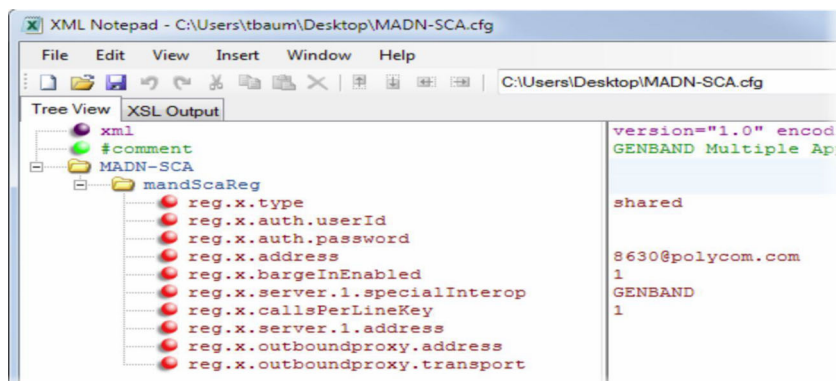
2. Enter the name of the configuration file to the CONFIG_FILES field of the master configuration file and save.

Global Address Book (GAB)

GENBAND's global address book (GAB) is a read-only global directory set up by an administrator and can co-exist with other corporate directories on the phone.

Related Topics

Configuring the Global Address Book

Example GAB Configuration

The following example shows the minimum parameters you need to configure to enable GAB on the phone.

To configure GAB:

1 Enable GAB by configuring the values in `feature.corporateDirectory.alt` and `dir.corp.alt`. The following illustration includes an example GAB address book parameters in `dir.corp.alt.attribute`.
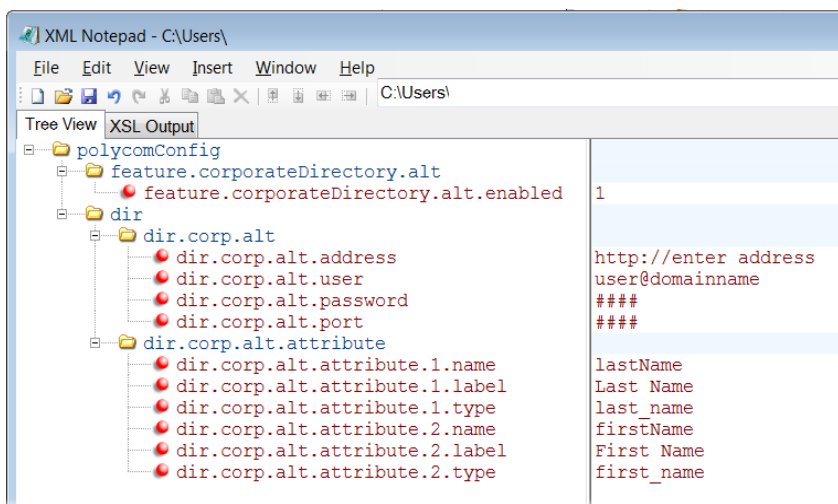
2 Save the configuration file.

3 Enter the name of the configuration file to the CONFIG_FILES field of the master configuration file and save.

Personal Address Book (PAB)

The personal address book (PAB) enables users to read and modify a personal directory of contacts on their phone. When users modify contact information using any soft client, desk phone, or mobile client registered to the same line, the change is made on all other clients, and users are notified immediately of the change by the GENBAND server.

Related Topics

Configuring the Personal Address Book

Example PAB Configuration

The following example shows an example PAB configuration.

To configure PAB:

1 Enter the values shown for the following parameters and save the configuration file.
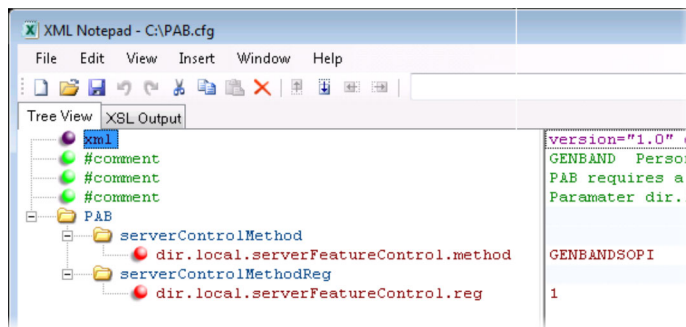
2 Enter the configuration file to the CONFIG_FILES field of the master configuration file and save.

Enhanced 911 (E.911) Location

With the Enhanced 911 (E.911) feature, you can set the location of the phone for emergency calls on the phone or on the provisioning server. When the phone starts up, the phone prompts users to choose a location, which is stored on the phone. The location that users set for the phone is used to identify the phone location to 911 operators dispatching emergency services. This feature is available for all VVX phones and is disabled by default only in a GENBAND environment.

By default, users can make a 911 call when the phone is locked, regardless of the call state, or when other features are in use. When a 911 call is in progress, the call control option does not display, users cannot use the hard keys to control a call, and DND or call forwarding are disabled.

Manually Set the Phone's Location

Users can set their location for emergency call on the phone.

To set the location information on the phone:

1 Register the phone.

The phone displays a warning message to "Set your location" for 10 seconds.

2 Press the warning message to enter a location. If the warning message disappears, on the phone, go to **Settings > Status > Diagnostics > Warnings**.

3 Select **Details** to enter a location to the location tree navigation menu.

4 Choose a location and press **Save**.

5 On the phone, go to **Status > Location Information**.

The location information displays in the **Status** menu.

The following figure shows the menu structure for setting the Location Status on VVX phones.

Location menu structure for VVX 500/501, 600/601, 1500

Related Topics

Configuring E.911

BroadSoft BroadWorks Server

This section shows you how to configure Polycom devices with BroadSoft Server options. You can use the features available on the BroadWorks R18 server or the BroadWorks R20 or later server with the following phones: VVX 300 series, 400 series, 500 series, 600 series, and 1500 phones.

Note that you cannot register lines with the BroadWorks R18 server and the R20 and later server on the same phone. All lines on the phone must be registered to the same BroadWorks server.

Some BroadSoft features require you to authenticate the phone with the BroadWorks XSP service interface as described in the section Authentication with BroadWorks Xtended Service Platform (XSP) Service Interface.

Authentication with BroadWorks Xtended Service Platform (XSP) Service Interface

You can configure Polycom phones to use advanced features available on the BroadSoft BroadWorks server. The phones support the following advanced BroadSoft features:

- BroadSoft Enhanced Call Park
- Executive-Assistant
- BroadSoft UC-One directory, favorites, and presence
- BroadSoft UC-One personal call control features

To use these features on Polycom devices with a BroadWorks server, you must authenticate the phone with the BroadSoft XSP service interface.

Related Topics

Configuring Authentication for BroadWorks XSP

BroadWorks Call Decline Policy

For shared lines in a BroadSoft BroadWorks environment, you can enable users to reject calls to a shared line. By default, users cannot reject calls to a shared line on Polycom phones. When this feature is enabled and a user rejects a call to the shared line, the call is rejected on all phones registered with the shared line.

Related Topics

BroadWorks Call Decline Parameters

Flexible Seating

Flexible Seating enables a user of an assigned primary phone to simultaneously access a registered line as a guest from an alternate host phone. The user's primary registration is active on the primary and host phone. Users can access the BroadSoft UC-One contact directory and favorites on the host phone, but the Polycom contact directory and favorites are not available.

Note that Flexible Seating is different from the Hoteling feature in that it provides only the primary registration's label on the host phone without any synchronization of features or settings.

The following conditions apply to the Flexible Seating feature:

● The primary phone and host phone do not sync automatically, but you can manually sync the phones on the BroadSoft BroadWorks server.

● The phone configured for the host user cannot accept incoming calls. The host user can make only emergency outgoing calls that are defined by the BroadWorks server.

● If the Phone Lock feature is enabled, numbers defined in the authorized call list are not allowed for outgoing calls except the emergency numbers set on the BroadWorks server.

● The host user account is intended to be used as a placeholder account that supports guest users and is not intended to be assigned to an actual phone user.

● The guest user cannot change the user password when Flexible Seating is enabled for the phone. You can change the host phone's user password from the Web Configuration Utility at any time. You can change the host phone's user password from the phone screen only when the guest user is not logged in.

Flexible Seating is not compatible with the following features:

● Hoteling

● Visitor Desk Phone (VDP)

● User Profile Feature

● Local Call Forwarding

● Local DND

On the BroadWorks server, you can set a period of time when the server automatically logs out a user from a phone in case a user does not log out.

Guest Profile PIN

You can configure a PIN for each guest profile, which enables users to access their guest profile on a host phone using a PIN. The PIN prevents other users from logging into a guest phone without the phone

password or guest PIN. The guest profile PIN takes precedence over the local phone password and the guest user must log out of the phone with the PIN before another user can log in with their password.

Related Topics

Flexible Seating Parameters

BroadSoft BroadWorks Configuration Tags

The following table shows the Polycom parameters you can map to the corresponding BroadSoft tags.

Polycom Configuration Parameter	BroadSoft Tag
`hoteling.reg`	%BWHOTELINGLINE-x%
`hotelingMode.type`	%BWHOTELINGMODE-x%

Executive-Assistant

Using configuration files, you can enable the BroadSoft Executive-Assistant feature on lines registered with the BroadWorks R20 or later server, and assign lines as an executive or an assistant. Note that all corresponding Executive and Assistant lines must be registered to the same server.

After you enable the feature, users set as executives or assistants can set basic filters to control which calls are sent directly to an assistant to answer or sent to the executive first. Executives and assistants can also enable screening, which enables the executive's phone to display the incoming call notification for all filtered calls.

To use this feature on Polycom phones registered with a BroadWorks server, you must authenticate the phone with the BroadSoft XSP service interface.

In addition, you can configure your phone to control the display of **Exec** soft key on the idle screen of the phone. You can also simplify the Executive-Assistant menu by adding or removing **Pick Call** and **Barge-in** soft keys from the menu.

Related Topics

Executive-Assistant Parameters

Enhanced Call Park

You can configure BroadWorks Enhanced Call Park per registered line. The following features are available for Enhanced Call Park:

- You can configure Enhanced Call Park only using configuration files; you cannot configure the feature on the Web Configuration Utility or from the local phone interface.
- You can configure Enhanced Call Park for private lines and shared lines. No configuration is necessary to enable the call park notification for monitored BLF lines.
- The default star codes set for the `call.parkedCallRetrieveString` is *88.

Related Topics

Configuring Enhanced Call Park

BroadSoft Directory Support

The BroadSoft directories enable users to search and view their personal, group, or enterprise contacts. When the BroadSoft directories are integrated with Polycom BroadSoft UC-One Application, users can access the different types of directories and search for contacts. There are five types of BroadSoft Directories:

- **Enterprise Directory.** This directory enables users to search and view Active Directory global address list of an enterprise. Users can query by first name, last name, phone number, extension and mobile number, and access contact information.
- **Group Directory.** This directory enables users to view the contact details such as work, extension, and mobile numbers of contacts. Users can place a call to anyone in the user's group.
- **Group Common Directory.** This directory enables users to view the contact details such as names and phone numbers of common contacts listed in the Group Common Directory.
- **Enterprise Common Directory.** This directory enables users to view the contact details such as names and phone numbers of common contacts listed in the Enterprise Common Directory.
- **Personal Directory.** This directory enables users to view the contact details such as names and phone numbers of the contacts in the user's personal directory stored on the server. You must enable this feature to allow users to add, delete, or edit the contacts in the BroadSoft Personal Directory.

Related Topics

BroadSoft Directory Parameters

Polycom BroadSoft UC-One Application

The Polycom BroadSoft UC-One application integrates with BroadSoft Enterprise Directory and BroadCloud services—a set of hosted services by BroadSoft—to provide the following features:

- **BroadSoft Directory**—Displays information for all users in the enterprise, for example, work and mobile phone numbers.
- **BroadCloud Presence**—Enables users to share presence information with the BroadTouch Business Communicator (BTBC) client application.
- **BroadCloud Favorites**—Enables users to mark contacts as favorites with the BroadTouch Business Communicator (BTBC) client application.

These features are available on Polycom VVX 300, 400, 500 and VVX 600 series business media phones These features require support from the BroadSoft BroadWorks R18 SP1 platform with patches and BroadSoft BroadCloud services. For details on how to set up and use these features, see the latest *Polycom VVX Business Media Phones - User Guide* at Latest Polycom UC Software Release.

Polycom's BroadSoft UC-One application enables you to:

- Access the BroadSoft Directory
- Search for contacts in BroadSoft Directory
- View BroadSoft UC-One contacts and groups

- View the presence status of BroadSoft UC-One contacts
- View and filter BroadSoft UC-One contacts
- Activate and control BroadSoft UC-One personal call control features.

Configuring BroadSoft UC-One

You can configure the UC-One Call Settings menu and feature options on the phone, in the Web Configuration Utility, and using configuration parameters.

Configure BroadSoft UC-One on the Phone

You can enable the BroadSoft UC-One feature directly from the phone.

To enable UC-One Call Settings in the Web Configuration Utility:

1 Navigate to **Settings > UC-One**.
2 Under **General**, click **Enable** for **BroadSoft UC-One**.
   This enables the UC-One Call Settings menu to display on the phone.

Configure BroadSoft UC-One in the Web Configuration Utility

You can enable the BroadSoft UC-One feature and feature options in the Web Configuration Utility.

To enable UC-One Call Settings menu options:

1 In the Web Configuration Utility, navigate to **Settings > UC-One**.
2 Under **Call Settings Features**, enable each feature menu you want available on the phone.

Related Topics

BroadSoft UC-One Configuration Parameters

Enterprise Directory Default Search

You can view an initial list of contacts in the Enterprise directory. After you enable the feature, users can view a list of contacts by default without the need to enter a name in the search box of the directory.

Related Topics

Enterprise Directory Search Parameters

BroadSoft Server-Based Call Logs

You can configure the phone to view the list of call logs when the user taps the **Recent** soft key on the phone's screen. When you enable this feature, users can view the call logs retrieved from the server on the phone.

Related Topics

BroadSoft Server-Based Call Logs Parameters

BroadSoft Server-Based Redial

You can configure the phone to support BroadSoft Server-Based Redial feature, which allows users to redial the last number dialed from any device connected to the same line or registration. When enabled, the **Redial** soft key displays on the phone screen. Users can select this soft key to place a call to the last dialed number.

Related Topics

BroadSoft Server-Based Redial Parameters

Anonymous Call Rejection

Anonymous Call Rejection enables users to automatically reject incoming calls from anonymous parties who have restricted their caller identification. After you enable the feature for users, users can turn call rejection on or off from the phone. When a user turns Anonymous Call Rejection on, the phone gives no indication that an anonymous call was received.

You can configure this option in the Web Configuration Utility.

Related Topics

Configuring Anonymous Call Rejection

Configure Anonymous Call Rejection using the Web Configuration Utility

You can configure Anonymous Call Rejection in the Web Configuration Utility.

To enable Anonymous Call Rejection in the Web Configuration Utility:

1   Navigate to **Settings > UC-One**.
2   Under the **Call Setting Features**, click **Enable** for **Anonymous Call Rejection**.

Simultaneous Ring Personal

The Simultaneous Ring feature enables users to add phone numbers to a list of contacts whose phones ring simultaneously when the user receives an incoming call. When you enable the display of the Simultaneous Ring menu option on the phone, users can turn the feature on or off from the phone and define which numbers should be included in the Simultaneous Ring group.

Related Topics

Configuring Simultaneous Ring Personal

Line ID Blocking

You can enable or disable the display of the Line ID Blocking menu option on the phone. When you enable the menu for users, users can choose to hide their phone number before making a call.

Related Topics

Configuring Line ID Blocking

BroadWorks Anywhere

BroadWorks Anywhere enables users to use one phone number to receive calls to and dial out from their desk phone, mobile phone, or home office phone. When you enable this feature, users can move calls between phones and perform phone functions from any phone. When enabled, the BroadWorks Anywhere settings menu displays on the phone and users can turn the feature on or off and add BroadWorks Anywhere locations on the phone.

You can configure a soft key for the BroadWorks Anywhere feature that enables users to navigate directly to the feature menu using an Enhanced Feature Key (EFK). This allows users to bypass navigating to **Settings > Features > UC-One Call Settings > BroadWorks Anywhere**. You can configure the soft key using the following EFK macro to support this feature:

● **$FBWSAnyWhere$**

Related Topics

Configuring BroadWorks Anywhere

BroadSoft Server-based Call Waiting

You can configure the phone to support server-based call waiting, which enables the server to manage incoming calls while a user is in an active call.

When a user changes the call waiting state, the phone sends a request to the server to update to the new state. You can also configure the phone to specify the ringtone for incoming calls, when another call is in progress.

Related Topics

BroadSoft Server-based Call Waiting Parameters

Remote Office

Remote Office enables users to set up a phone number on their office phone to forward incoming calls to a mobile device or home office number. When enabled, this feature enables users to answer incoming calls to the office phone on the phone, and any calls placed from that phone show the office phone number.

Related Topics

Configuring Remote Office

BroadSoft UC-One Credentials

Enabling this feature allows users to enter their BroadWorks UC-One credentials on the phone instead of in the configuration files. The parameters `reg.x.broadsoft.useXspCredentials,` and `feature.broadsoftUcOne.enabled` must be enabled to display the UC-One Credentials menu option on the phone.

Related Topics

Configuring BroadSoft UC-One Credentials

Skype for Business

Skype for Business and Lync Server provides a unified communications (UC) solution that enables customers, colleagues, and business partners to communicate instantly by voice, video, or messaging through a single interface, regardless of their location or network. Note that the concurrent failover/fallback feature is not compatible in a Microsoft environment.

For full administrator instructions on deploying and setting up features with Skype for Business and Lync Server, see the latest *Polycom UC Software with Skype for Business - Deployment Guide* on Polycom Support.

The features available when you are registered with Skype for Business Server vary with the Polycom phone model and Polycom UC Software version you are using. UC Software 5.3.0 or later does not support the use of VVX 1500 business media phone with the Skype for Business Server.

If you are using UC Software 5.3.0 or later with Skype for Business and want to change default settings or customize your deployment, you must set up a provisioning server.

Polycom UC Software supports the following devices with Skype for Business and Lync Server and:

- VVX 201, 300 series, 400 series, 500 series, and 600 series business media phones
- SoundStructure VoIP Interface

Polycom UC Software enables you to register a single phone line with Skype for Business Server; you cannot register multiple lines with Skype for Business Server. When you register a line on a Polycom phone using Skype for Business Server you cannot register lines with another server.

Device Parameters

The `<device/>` parameters—also known as device settings—contain default values that you can use to configure basic settings for multiple phones within your network.

Polycom provides a global `device.set` parameter that you must enable to install software and change device parameters. In addition, each `<device/>` parameter has a corresponding `.set` parameter that enables or disables the value for that device parameter. You need to enable the corresponding `.set` parameter for each parameter you want to apply.

After you complete the software installation or configuration changes to device parameters, remove `device.set` to prevent the phones from rebooting and triggering a reset of device parameters that phone users might have changed after the initial installation.

If you configure any parameter values using the <device/> parameters, any subsequent configuration changes you make from the Web Configuration Utility or phone local interface do not take effect after a phone reboot or restart.

The `<device/>` parameters are designed to be stored in flash memory and for this reason the phone does not upload `<device/>` parameters to the `<MAC>-web.cfg` or `<MAC>-phone.cfg` override files if you make configuration changes through the Web Configuration Utility or phone interface. This design protects your ability to manage and access the phones using the standard set of parameters on a provisioning server after the initial software installation.

Changing Device Parameters

Keep the following in mind when modifying device parameters:

- Note that some parameters may be ignored. For example, if DHCP is enabled, it will still override the value set with `device.net.ipAddress`.
- Though individual parameters are checked to see whether they are in range, the interaction between parameters is not checked. If a parameter is out of range, an error message displays in the log file and the parameter is not be used.
- Incorrect configuration can put the phones into a reboot loop. For example, server A has a configuration file that specifies that server B should be used, and server B has a configuration file that specifies that server A should be used.

To detect errors, including IP address conflicts, Polycom recommends that you test the new configuration files on two phones before initializing all phones.

Related Topics

Types of Device Parameters

Device Parameters

Configuration Parameters

This section is a reference guide to the UC Software configuration parameters you use to configure devices and call controls. This section provides a description of each configuration parameter, and permitted and default values.

Provisioning and Configuring Phones

This section list parameters to provision and configure phones.

Quick Setup Soft Key Parameters

The following table lists the parameters that configures Quick Setup Soft Key.

Quick Setup Soft Key Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cf g`	`prov.quickSetup.e nabled`	0 (default) - Disables the quick setup feature. 1 - Enables the quick setup feature.	No

Configure Network Settings

This section lists parameters that configure the deployment network.

Extensible Authentication Protocol Method for 802.1x Parameters

To set up an Extensible Authentication Protocol (EAP) method that requires a device or a CA certificate, configure TLS Platform Profile 1 or TLS Platform Profile 2.

You can use the parameters in the following table to configure 802.1X authentication.

Set EAP Method 802.1x Parameters

Template	Parameters	Permitted Values	Change Causes Restart or Reboot
device.cfg	device.net.dot1x.enabled	Enable or disable the 802.1X feature. 0 (default) – Disables 802.1X authentication. 1 – Enables 802.1X authentication.	No
device.cfg	device.net.dot1x.identity	Specify the identity (user name) for authentication. Null (default). 0-255 - String length.	No
device.cfg	device.net.dot1x.method	Specify the 802.1X EAP method. EAP-None – No authentication EAP-TLS, EAP-PEAPv0-MSCHAPv2, EAP-PEAPv0-GTC, EAP-TTLS-MSCHAPv2, EAP-TTLS-GTC, EAP-FAST, EAP-MD5	No
device.cfg	device.net.dot1x.password	The password for 802.1X authentication. Null (default). 0-255 - String length.	No
device.cfg	device.net.dot1x.eapFastInBandProv	Enable EAP In-Band Provisioning for EAP-FAST. 0 (default) - Disabled 1 - Unauthenticated, active only when the EAP method is EAP-FAST.	No
device.cfg	device.pacfile.data	Specify a PAC file for EAP-FAST (optional). Null (default) 0-2048 - String length.	No
device.cfg	device.pacfile.password	The optional password for the EAP-FAST PAC file. Null (default). 0-255 - String length.	No

IP Type-of-Service Parameters

The IP ToS can be configured specifically for RTP packets and call control packets, such as SIP signaling packets.

IP Type-of-Service Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	qos.ip.callControl.dscp	Specify the DSCP of packets. Null (default) 0 to 63 Null: other `qos.ip.rtp.*` parameters are used. Not Null: Overrides other `qos.ip.rtp.*`parameters.	Yes
site.cfg	qos.ip.callControl.max_reliability	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
site.cfg	qos.ip.callControl.max_throughput	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
site.cfg	qos.ip.callControl.min_cost	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
site.cfg	qos.ip.callControl.min_delay	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
site.cfg	qos.ip.callControl.precedence	Set the precedence in the IP ToS field of the IP header used for call control. 5 (default) 0-7	Yes

`site.cfg`	`qos.ip.rtp.dscp`	Specify the DSCP of packets. Null (default) 0 to 63 Null: other `qos.ip.rtp.video*` parameters are used. Not Null: Overrides other `qos.ip.rtp.video*`parameters.	Yes
`site.cfg`	`qos.ip.rtp.max_relia bility`	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
`site.cfg`	`qos.ip.rtp.max_throu ghput`	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
`site.cfg`	`qos.ip.rtp.min_cost`	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
`site.cfg`	`qos.ip.rtp.min_delay`	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
`site.cfg`	`qos.ip.rtp.precedenc e`	Set the precedence in the IP ToS field of the IP header used for RTP. 5 (default) 0-7	Yes
`site.cfg`	`qos.ip.rtp.video.dsc p`	Specify the DSCP of packets. Null (default) 0 to 63 Null: other `qos.ip.rtp.video*` parameters are used. Not Null: Overrides other `qos.ip.rtp.video*`parameters.	Yes

site.cfg	qos.ip.video.max_rel iability	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
site.cfg	qos.ip.video.max_thr oughput	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
site.cfg	qos.ip.video.min_cos t	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
site.cfg	qos.ip.video.min_del ay	0 (default) – The bit in the IP ToS field of the IP header is not set. 1 – The bit in the IP ToS field of the IP header is set.	Yes
site.cfg	qos.ip.video.precede nce	Set the precedence in the IP ToS field of the IP header. 5 (default) 0-7	Yes

IEEE 802.1p/Q Parameters

Use the following table to set values. 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.

IEEE 802.1p/Q Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	qos.ethernet.other.u ser_priority	Set user priority for packets without a per-protocol setting. 2 (Default) 0 - 7	No
site.cfg	qos.ethernet.rtp.vid eo.user_priority	Set user-priority used for Video RTP packets. 5 (Default) 0 - 7	No

site.cfg	qos.ethernet.rtp.user_priority	Choose the priority of voice Real-Time Protocol (RTP) packets. 5 (Default) 0 - 7	No
site.cfg	qos.ethernet.callControl.user_priority	Set the user-priority used for call control packets. 5 (Default) 0 - 7	No

Audio Features

This section lists parameters to configure audio features.

Voice Activity Detection Parameters

The following table lists the parameters you can use to configure Voice Activity Detection.

Voice Activity Detection Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.vad.signalAnnexB	0—There is no change to SDP. If `voice.vadEnable` is set to 0, add parameter line `a=fmtp:18 annexb="no"` below the `a=rtpmap…` parameter line (where "18" could be replaced by another payload). 1 (default)—Annex B is used and a new line is added to SDP depending on the setting of `voice.vadEnable`. If `voice.vadEnable` is set to 1, add parameter line `a=fmtp:18 annexb="yes"` below `a=rtpmap…` parameter line (where '18' could be replaced by another payload).	No

Voice Activity Detection Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.vadEnable	0 - Disable Voice activity detection (VAD). 1 - Enable VAD.	No
site.cfg	voice.vadThresh	The threshold for determining what is active voice and what is background noise in dB. 25 (default) integer from 0 - 30 Sounds louder than this value are considered active voice, and sounds quieter than this threshold are considered background noise. This does not apply to G.729AB codec operation which has its own built-in VAD function.	No

Comfort Noise Payload Packets Parameters

The following table includes the parameters you can use to configure Comfort Noise payload packets.

Comfort Noise Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.CNControl	Publishes support for Comfort Noise in the SDP body of the INVITE message and includes the supported comfort noise payloads in the media line for audio. 1 (default)—Either the payload type 13 for 8 KHz sample rate audio codec is sent for Comfort Noise, or the dynamic payload type for 16 KHz audio codecs are sent in the SDP body. 0—Does not publish support or payloads for Comfort Noise.	No
site.cfg	voice.CN16KPayload	Alters the dynamic payload type used for Comfort Noise RTP packets for 16 KHz codecs. 96 to 127 122 (default)	No

DTMF Tone Parameters

The following table includes the parameters you can use to set up DTMF tones.

DTMF Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.1.telephony`	1 (default) - Allows the phone to publish its capability in an SDP offer or answer to send and receive the DTMF tones over RFC-2833. 0 - Disables the phone's capability to send and receive the DTMF tones through RFC-2833 in an SDP offer or answer.	No
`sip-interop.cfg`	`tone.dtmf.chassis.masking`	0 (default) - DTMF tones play through the speakerphone in handsfree mode. 1 - Set to 1 only if `tone.dtmf.viaRtp` is set to 0. DTMF tones are substituted with non-DTMF pacifier tones when dialing in handsfree mode to prevent tones from broadcasting to surrounding telephony devices or inadvertently transmitted in-band due to local acoustic echo.	Yes
`sip-interop.cfg`	`tone.dtmf.level`	The level of the high frequency component of the DTMF digit measured in dBm0; the low frequency tone is two dB lower. -15 -33 to 3	Yes
`sip-interop.cfg`	`tone.dtmf.offTime`	When a sequence of DTMF tones is played out automatically, specify the length of time in milliseconds the phone pauses between digits. This is also the minimum inter-digit time when dialing manually. 50 ms positive integer	Yes

DTMF Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	tone.dtmf.onTime	Set the time in milliseconds DTMF tones play on the network when DTMF tones play automatically. The time you set is also the minimum time the tone plays when manually dialing. 50 ms (default) 1 - 65535 ms	Yes
sip-interop.cfg	tone.dtmf.rfc2833Control	Specify if the phone uses RFC 2833 to encode DTMF tones. 1 (default) - The phone indicates 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 and always honor the DTMF format present in the offer.	Yes
sip-interop.cfg	tone.dtmf.rfc2833Payload	Specify the phone-event payload encoding in the dynamic range to be used in SDP offers. Skype (default) - 101 Generic (default) -127 96 to 127	Yes
sip-interop.cfg	tone.dtmf.viaRtp	1 (default) - Encode DTMF in the active RTP stream. Otherwise, DTMF may be encoded within the signaling protocol only when the protocol offers the option. If you set this parameter to 0, you must set tone.dtmf.chassis.masking to 1.	Yes
sip-interop.cfg	tone.localDtmf.onTime	Set the time in milliseconds DTMF tones play for when the phone plays out a DTML tone sequence automatically. 50 ms (default) 1 - 65535 ms	No

Acoustic Echo Cancellation Parameters

The following table includes the parameters you can use to set up Acoustic Echo Cancellation.

Acoustic Echo Cancel (AEC) Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.aec.hf.ena ble	0—Disables the AEC function for handsfree options. 1 (default)—Enables the AEC function for handsfree options. Polycom does not recommend disabling this parameter.	No
site.cfg	voice.aec.hs.ena ble	0—Disables the AEC function for the handset. 1 (default)—Enables the AEC function for the handset.	No
debug.cfg	voice.aes.hf.dup lexBalance	0 - Max Echo Control (default) - Balances the Acoustic Echo Suppression to maximize the echo control, allowing the near-end and far-end users to speak simultaneously with minimal full duplex in handsfree mode. 1 - Max Full Duplex: Balances the Acoustic Echo Suppression to maximize full duplex. This makes the phone handsfree more susceptible to echo during continuous double-talk or when moving the phone or objects near the phone.	No

Context Sensitive Volume Control Parameters

The following table includes the parameters you can use to configure Context Sensitive Volume Control.

Context Sensitive Volume Control Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.volume.persist.bluetooth.headset	Specifies if a Bluetooth headset should be used for every call (VVX 600/601 only). 0 (default) —Does not use the Bluetooth headset for all calls. 1 —Uses the Bluetooth headset for all calls.	No
site.cfg	voice.volume.persist.handset	Specifies whether the handset's volume level persists and stays at the same level between calls. 0 (default)—The handset volume automatically resets to a nominal level after each call. 1—The volume for each call is the same as the previous call.	No
site.cfg	voice.volume.persist.handsfree	Specifies whether the speakerphone volume persists and stays at the same level between calls. 0— The speakerphone volume automatically resets to a nominal level after each call. 1 (default)—The volume for each call is the same as the previous call	No

Context Sensitive Volume Control Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`voice.volume.per sist.usb.handsfr ee`	Specifies if a USB headset should be used for every call 0 (default)— Does not use USB headset automatically for calls. 1—Uses the USB headset automatically for all calls.	No
`site.cfg`	`voice.volume.per sist.usbHeadset`	Specifies if a USB headset should be used for every call 0 (default)— Does not use USB headset automatically for calls. 1—Uses the USB headset automatically for all calls.	No

Acoustic Fence Parameters

The following table includes the noise suppression parameters you can use to configure Polycom Acoustic Fence.

Acoustic Fence Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`voice.ns.hd.enab le`	0 — Disables noise suppression for headsets. 1 (default) — Enables noise suppression for headsets.	No
`features.cfg`	`voice.ns.hd.enha nced`	The parameter `voice.ns.hd.enable` must also be set to 1 to use this parameter. 0 (default) —Disables Acoustic Fence noise suppression for headsets. 1 —Enables Acoustic Fence noise suppression for headsets.	No

Acoustic Fence Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`voice.ns.hd.nonStationaryThresh`	Sets the Acoustic Fence noise suppression threshold for headsets. A lower value allows more background sound to enter, and a higher value suppresses background noise. 1 to 10 8 (default) High values can suppress the speaker's voice and impact far-end audio quality.	No
`features.cfg`	`voice.ns.hs.enable`	0 (default)—Disables noise suppression for handsets. 1—Enables noise suppression for handsets.	No
`features.cfg`	`voice.ns.hs.enhanced`	The parameter `voice.ns.hs.enable` must also be set to 1 to use this parameter. 0 (default)—Disables Acoustic Fence noise suppression for handsets. 1 —Enables Acoustic Fence noise suppression for handsets.	No
`features.cfg`	`voice.ns.hs.nonStationaryThresh`	Sets the Acoustic Fence noise suppression threshold for handsets. A lower value allows more background sound to enter, and a higher value suppresses background noise. 1 to 10 8 (default) High values can suppress the speaker's voice and impact far-end audio quality.	No

Bluetooth Headset Support Parameters

The following table lists the parameters you can use to configure Bluetooth headset features.

Bluetooth Headset Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.bluet ooth.enabled	1 (default) - Enables a user to pair and connect a Bluetooth headset. 0 - Disables support for Bluetooth headsets.	No
features.cfg	bluetooth.rad ioOn	0 (default)—Turns off the Bluetooth radio. 1—Turns on the Bluetooth radio to enable other devices to detect and connect to the device over Bluetooth.	No

Audio Alert Parameters

Use the parameters in the following table to specify where audio alerts and sound effects play.

Audio Alert and Sound Effect Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
techsupport. cfg	se.appLocalE nabled	1 (default)—Enable audio alerts and sound effects. 0—Disable audio alerts and sound effects	Yes
reg-advanced .cfg	se.destinati on	Set where alerts and sound effects play out. chassis (default) —Alerts and sound effects play out through the phone's speakerphone. headset (if connected) handset active —Alerts play from the destination that is currently in use. For example, if a user is in a call on the handset, a new incoming call rings on the handset.	No
site.cfg	se.stutterOn VoiceMail	1 (default)—A stuttered dial tone is used instead of a normal dial tone to indicate that one or more voicemail messages are waiting at the message center. 0—A normal tone is used to indicate that one or more voicemail messages are waiting at the message center.	No

Ringtone Parameters

The following parameters configure ringtones.

Ringtone Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	se.rt.enabled	0—The ringtone feature is not enabled. 1 (default)—The ringtone feature is enabled.	No
reg-advanced	se.rt.modification.enabled	Determines whether or not users are allowed to modify the pre-defined ringtone from the phone's user interface. 0 1 (default)	No
sip-interop.cfg	se.rt.<ringClass>.callWait	The call waiting tone used for the specified ring class. The call waiting pattern should match the pattern defined in Call Progress Tones. callWaiting (default) callWaitingLong precedenceCallWaiting	No
sip-interop.cfg	se.rt.<ringClass>.name	The answer mode for a ringtone, which is used for to identify the ringtone in the user interface. UTF-8 encoded string	No
sip-interop.cfg	se.rt.<ringClass>.ringer	The ringtone used for this ring class. The ringer must match one listed in Ringtones. default ringer1 to ringer24 ringer2 (default)	No
sip-interop.cfg	se.rt.<ringClass>.timeout	The duration of the ring in milliseconds before the call is auto answered, which only applies if the type is set to ring-answer. 1 to 60000 2000 (default	No
sip-interop.cfg	se.rt.<ringClass>.type	The answer mode for a ringtone. ring visual answer ring-answer	No

Distinctive Ringtone Parameters

The following table includes the parameters you can use to configure distinctive ringtones for a line, contact, or type of call.

Distinctive Ringtone Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.alertInfo.x.class`	Alert-Info fields from INVITE requests are compared 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 is applied. default (default) See the list of ring classes in Ringtone Parameters.	No
`sip-interop.cfg`	`voIpProt.SIP.alertInfo.x.value`	Specify a ringtone for single registered line using a string to match the Alert-Info header in the incoming INVITE. NULL (default)	No
`reg-advanced.cfg`	`reg.x.ringType`	The ringer to be used for calls received by this registration. The default is the first non-silent ringer. If you use the configuration parameters ringer13 and ringer14 on a single registered line, the phone plays SystemRing.wav. default (default) ringer1 to ringer24	No

Sampled Audio File Parameters

Your custom sampled audio files must be available at the path or URL specified in the parameter `saf.x` so the phone can download the files. Make sure to include the name of the file and the .wav extension in the path.

Use the parameters in the following tables to customize this feature.

In the following table, *x* is the sampled audio file number.

Sample Audio File Parameter

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`saf.x`	Specify a path or URL for the phone to download a custom audio file. Null (default)—The phone uses a built-in file. Path Name —During startup, the phone attempts to download the file at the specified path in the provisioning server. URL— During startup, the phone attempts to download the file from the specified URL on the Internet. Must be a RFC 1738-compliant URL to an HTTP, FTP, or TFTP wave file resource. If using TFTP, the URL must be in the following format: `tftp://<host>/[pathname]<filename>`. For example: `tftp://somehost.example.com/sounds/example.wav`. To use a welcome sound, enable the parameter `up.welcomeSoundEnabled` and specify a file in `saf.x`. The default UC Software welcome sound file is `Welcome.wav`.	No

Sound Effect Pattern Parameters

There are three categories of sound effect patterns that you can use to replace `cat` in the parameter names: `callProg` (Call Progress Patterns), `ringer` (Ringer Patterns) and `misc` (Miscellaneous Patterns).

Keep the following in mind when using the parameters in the following table:

- Xis the pattern name.
- Y is the instruction number.
- Both x and y need to be sequential.
- `Cat` is the sound effect pattern category.

Sound Effects Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`region.cfg`	`se.pat.callProg.secondaryDialTone.name`	1-255	No
`region.cfg`	`se.pat.callProg.secondaryDialTone.inst.1.type`	0-255	No

Sound Effects Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`region.cfg`	`se.pat.callProg.secondaryDialT` `one.inst.1.value`	0-50	No
`region.cfg`	`se.pat.callProg.secondaryDialT` `one.inst.1.atte`	Sound effects name, where cat is `callProg`, `ringer`, or `misc`. UTF-8 encoded string	No
`region.cfg`	`se.pat.cat.x.inst.y.type`	Sound effects name, where cat is `callProg`, `ringer`, or `misc`. sample chord silence branch	No
`region.cfg`	`se.pat.cat.x.inst.y.value`	The instruction: `sampled` – sampled audio file number, `chord` – type of sound effect, `silence` – silence duration in ms, `branch` – number of instructions to advance. String	No

Audio Codec Parameters

You can configure a set of codec properties to improve consistency and reduce workload on the phones.

Use the parameters in the following table to specify the priority for audio codecs on your Polycom phones. If 0 or Null, the codec is disabled. A value of 1 is the highest priority.

If a phone does not support a codec, it treats the setting as if it were 0 and not offer or accept calls with that codec. The phone ignores the unsupported codec and continues to the codec next in priority. For example, using the default values, the VVX 310 doesn't support G.722.1C or G.719 and uses G.722.1 as the highest-priority codec.

Audio Codec Parameters

Template	Parameters	Permitted Values	Default	Change Causes Restart or Reboot
`site.cfg`		0 to 27		No
	`voice.codecPref.G711_A`		7	
	`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.G7221.24kbps`		0	
	`voice.codecPref.G7221.32kbps`		0	
	`voice.codecPref.G7221_C.24kbps`		5	
	`voice.codecPref.G7221_C.32kbps`		0	
	`voice.codecPref.G7221_C.48kbps`		0	
	`voice.codecPref.G729_AB`		2	
	`voice.codecPref.iLBC.13_33kbps`		8	
	`voice.codecPref.iLBC.15_2kbps`		0	
	`voice.codecPref.Lin16.8ksps`		0	
	`voice.codecPref.Lin16.16ksps`		0	
	`voice.codecPref.Lin16.32ksps`		0	
	`voice.codecPref.Lin16.44_1ksps`		0	
	`voice.codecPref.Lin16.48ksps`		0	
	`voice.codecPref.Siren7.16kbps`		0	
	`voice.codecPref.Siren7.24kbps`		0	
	`voice.codecPref.Siren7.32kbps`		0	
	`voice.codecPref.Siren14.24kbps`		0	
	`voice.codecPref.Siren14.32kbps`		0	
	`voice.codecPref.Siren14.48kbps`		0	
			3	

IEEE 802.1p/Q Parameters

You can set the 802.1p/Q user priority and configure user priority specifically for RTP packets and call control packets, such as SIP signaling packets, with default settings configurable for all other packets.

IEEE 802.1p/Q Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`qos.ethernet.other.user_priority`	Set the user priority for packets without a per-packet protocol setting (including 802.1p/Q). 2 (default) 0 - 7	No

VQMon Parameters

All of the parameters that configure Voice Quality Monitoring in the following table are located in the features.cfg template.

Voice Quality Monitoring Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`voice.qualityMonitoring.collector.alert.moslq.threshold.critical`	Specify the threshold value of listening MOS score (MOS-LQ) that causes the phone to send a critical alert quality report. Configure the desired MOS value multiplied by 10. For example, a value of 28 corresponds to the MOS score 2.8. 0 (default) - Critical alerts are not generated due to MOS-LQ. 0 - 40	Yes
`features.cfg`	`voice.qualityMonitoring.collector.alert.moslq.threshold.warning`	Specify the 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. For example, a configured value of 35 corresponds to the MOS score 3.5. 0 (default) - Warning alerts are not generated due to MOS-LQ. 0 - 40	Yes

Voice Quality Monitoring Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`voice.qualityMonitoring.collector.alert.delay.threshold.critical`	Specify the threshold value of one way-delay (in milliseconds) that causes the phone to send a critical alert quality report. One-way delay includes both network delay and end system delay. 0 (default) - Critical alerts are not generated due to one-way delay. 0 - 2000 ms	Yes
`features.cfg`	`voice.qualityMonitoring.collector.alert.delay.threshold.warning`	Specify the threshold value of one-way delay (in milliseconds) that causes the phone to send a critical alert quality report. One-way delay includes both network delay and end system delay. 0 (default) - Warning alerts are not generated due to one-way delay. 0 - 2000 ms	Yes
`features.cfg`	`voice.qualityMonitoring.collector.enable.periodic`	0 (default) - Periodic quality reports are not generated. 1 - Periodic quality reports are generated throughout a call.	Yes
`features.cfg`	`voice.qualityMonitoring.collector.enable.session`	0 (default) - Quality reports are not generated at the end of each call. 1 - Reports are generated at the end of each call.	Yes
`features.cfg`	`voice.qualityMonitoring.collector.enable.triggeredPeriodic`	0 (default) - Alert states do not cause periodic reports to be generated. 1 - Periodic reports are generated if an alert state is critical. 2 - Period reports are generated when an alert state is either warning or critical. Note: This parameter is ignored when `voice.qualityMonitoring.collector.enable.periodic` is 1, since reports are sent throughout the duration of a call.	Yes
`features.cfg`	`voice.qualityMonitoring.collector.period`	The time interval (in milliseconds) between successive periodic quality reports. 5 (default) 5 - 900 ms	Yes

Voice Quality Monitoring Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`voice.qualityMonitoring.collector.server.x.address`	The server address of a SIP server (report collector) that accepts voice quality reports contained in SIP PUBLISH messages. Set x to 1 as only one report collector is supported at this time. NULL (default) IP address or hostname	Yes
`features.cfg`	`voice.qualityMonitoring.collector.server.x.outboundProxy.address`	This parameter directs SIP messages related to voice quality monitoring to a separate proxy. No failover is supported for this proxy, and voice quality monitoring is not available for error scenarios. NULL (default) IP address or FQDN	No
`features.cfg`	`voice.qualityMonitoring.collector.server.x.outboundProxy.port`	Specify the port to use for the voice quality monitoring outbound proxy server. 0 (default) 0 to 65535	No
`features.cfg`	`voice.qualityMonitoring.collector.server.x.outboundProxy.transport`	Specify the transport protocol the phone uses to send the voice quality monitoring SIP messages. DNSnaptr (default) TCPpreferred UDPOnly TLS TCPOnly	No
`features.cfg`	`voice.qualityMonitoring.failover.enable`	Set the port of a SIP server (report collector) that accepts voice quality reports contained in SIP PUBLISH messages. Set x to 1 as only one report collector is supported at this time. 5060 (default) 1 to 65535	No

Voice Quality Monitoring Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	voice.qualityMonitoring.failover.enable	1 (default) - The phone performs a failover when voice quality SIP PUBLISH messages are unanswered by the collector server. 0 - No failover is performed; note, however, that a failover is still triggered for all other SIP messages. This parameter is ignored if voice.qualityMonitoring.collector.server.x.outboundProxy is enabled.	No
features.cfg	voice.qualityMonitoring.location	Specify the device location with a valid location string. If you do not configure a location value, you must use the default string 'Unknown'. Unknown (default)	No
features.cfg	voice.qualityMonitoring.rfc6035.enable	0 (default) - The existing draft implementation is supported. 1 - Complies with RFC6035.	No
features.cfg	voice.qualityMonitoring.rtcpxr.enable	0 (default) - RTCP-XR packets are not generated. 1 - The packets are generated.	Yes

Video Features

This section lists parameters that configure video features.

Video Transmission Parameters

Use the parameters in the following table to configure video transmission.

Video Transmission Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.autoFullScreen	0 (default) — Video calls only use the full screen layout if it is explicitly selected by the user. 1 — Video calls use the full screen layout by default, such as when a video call is first created or when an audio call transitions to a video call	No
video.cfg	video.autoStartVideoTx	This parameter controls video sent to the far side. Video from the far side always displays if available, and far side users can control when to send video. 1 (default) — Video transmission to the far side begins when a user starts a call. 0 — Video transmission does not start until a user manually starts video using the Start Video soft key.	No
video.cfg	video.callRate	The default call rate (in kbps) to use when initially negotiating bandwidth for a video call. 512 (default) - The overlay does not time out. 128 - 2048	No
video.cfg	video.forceRtcpVideoCodecControl	0 (default) — RTCP feedback messages depend on a successful SDP negotiation of a=rtcp-fb and are not used if that negotiation is missing. 1 — The phone is forced to send RTCP feedback messages to request fast I-frame updates along with SIP INFO messages for all video calls irrespective of a successful SDP negotiation of a=rtcp-fb. For an account of all parameter dependencies when setting I-frame requests, refer to the section I-Frames.	No

Video Transmission Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`video.cfg`	`video.maxCallRate`	Sets the maximum call rate that the users can select. The value set on the phone cannot exceed this value. If `video.callRate` exceeds this value, this parameter overrides `video.callRate` and this value is used as the maximum. 768 (default) 128 - 2048	No
`video.cfg`	`video.quality`	The optimal quality for video that is sent in a call or a conference. Motion — for outgoing video that has motion or movement. Sharpness — for outgoing video that has little or no movement. NULL (default) — for outgoing video that has little or no movement. Note: If `motion` is not selected, moderate to heavy motion can cause some frames to be dropped.	No

Video and Camera View Parameters

Use the parameters in the following table to set the video and local camera view settings.

Video and Camera View Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`video.cfg`	`video.screenMode`	Specify the view of the video window in normal viewing mode. normal (default) full crop	No
`video.cfg`	`video.screenModeFS`	Specify the view of the video window in full screen viewing mode. normal (default)	No

Video and Camera View Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.localCameraView.fullscreen.enabled	Determines whether the local camera view is shown in the full screen layout. 1 (default) — The local camera view is shown. 0 — The local camera view is not shown.	No
video.cfg	video.localCameraView.fullscreen.mode	Determines how the local camera view is shown. Side-by-side (default) — The local camera view displays side-by-side with the far end window. PIP — The local camera view displays as a picture-in-picture with the far end window	No

Video Camera Parameters

Use the parameters in the following table to configure the video camera options.

Video Camera Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.camera.brightness	Sets the brightness level. The value range is from 0 (Dimmest) to 6 (Brightest). 3 (default) 0 - 6	No
video.cfg	video.camera.contrast	Sets the contrast level. The value range is from 0 (no contrast increase) to 3 (most contrast increase), and 4 (noise reduction contrast). 0 (default) 0 - 4	No
video.cfg	video.camera.flickerAvoidanced	Sets the flicker avoidance. 0 (default) — flicker avoidance is automatic. 1 — 50hz AC power frequency flicker avoidance (Europe/Asia). 2 — 60hz AC power frequency flicker avoidance (North America).	No

Video Camera Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.camera.frameRate	Sets the target frame rate (frames per second). Values indicate a fixed frame rate from 5 (least smooth) to 30 (most smooth). 25 (default) 5 - 30 If `video.camera.frameRate` is set to a decimal number, the value 25 is used instead.	No
video.cfg	video.camera.saturation	Sets the saturation level. The value range is from 0 (Lowest) to 6 (Highest). 3 (default) 0 - 6	No
video.cfg	video.camera.sharpnes	Sets the sharpness level. The value range is from 0 (Lowest) to 6 (Highest). 3 (default) 0 - 6	No

Video Codec Parameters

Use the parameters in the following table to prioritize and adjust the video codecs that your VVX phones use.

Video Codec Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.codecPref.H261	0 - 8 6(default)	No
video.cfg	video.codecPref.H264	0 - 8 4 (default)	No
video.cfg	video.codecPref.H263 1998	0 - 8 4 (default)	No
video.cfg	video.codecPref.H263	0 - 8 5 (default)	No

H.323 Protocol Parameters

Use the parameters in the following table to:

- Configure SIP and H.323 protocols
- 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.

- 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 display, and users must select one to place the call.

- Configure auto-answering on H.323 calls only.
- Set the preferred protocol to SIP.
- Set to configure one SIP line, one H.323 line, and a dual protocol line—both SIP and H.323 can be used.
- Set the preferred protocol for off-hook calls on the third (dual protocol) line to SIP.

H.323 Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.manualProtocolRouting	Specifies whether to choose a protocol routing or use a default protocol. 1 (Default) - User is presented with a protocol routing choice in situations where a call can be placed using either protocol (for example, with SIP and H.323 protocols). 0 - Default protocol is used and the user does not choose. Supports VVX 500/501, 600/601, and 1500 phones.	No
features.cfg	up.manualProtocolRouting.softKeys	Display soft keys that control **Manual Protocol Routing** options. 1 (Default) - Soft keys are enabled. Use soft keys to choose between the SIP or H.323 protocol. 0 - Soft keys for protocol routing do not display. You can use this parameter with the VVX 500/501, 600/601, and 1500 phones.	No
reg-advanced.cfg, h323.cfg	call.autoAnswer.H323	This parameter is available for the VVX 500/501, 600/601, and 1500. 0 (default) - Disable auto-answer for H.323 calls. 1 - Enable auto-answer for H.323 calls.	No

H.323 Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cf g`	`call.enableOnNotRegist ered`	1 (default) - Users can make calls when the phone is not registered. When set to 1, Polycom VVX 500/501, 600/601, and 1500 business media phones can make calls using the H.323 protocol even though an H.323 gatekeeper is not configured. 0 - Calls are not permitted without registration.	Yes
`reg-advanced.c fg, video.cfg`	`call.autoAnswer.videoM ute`	You can use this parameter for the VVX 500/501, 600/601, and 1500 business media phones. 0 (default) - Video begins transmitting (video Tx) immediately after a call is auto-answered. 1 - Video transmission (video Tx) is initially disabled after a call is auto-answered.	No
`video.cfg`	`call.autoRouting.prefe rredProtocol`	You can use this parameter for the VVX 500/501, 600/601, and 1500 business media phones. SIP (default) - Calls are placed via SIP if available or via H.323 if SIP is not available. H323 - Calls are placed via H.323 if available, or via SIP if H.323 is not available.	No
`sip-interop.cf g`	`call.autoRouting.prefe rence`	You can use this parameter for the VVX 500/501, 600/601, and 1500 business media phones. 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 is used (`call.autoRouting.preferredProtoc ol`). protocol - The first available line with the preferred protocol activated is used, if available. If not available, the first available line is used. Note that auto-routing is used when manual routing selection features (`up.manualProtocolRouting`) are disabled.	No

H.323 Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.protocol.H323`	You can use this parameter for the VVX 500/501, 600/601, and 1500. 0 (default) - H.323 signaling is not enabled for registration x. 1 - H.323 signaling is enabled for registration x.	No
`site.cfg`	`reg.x.server.H323.y.address`	Address of the H.323 gatekeeper. Null (default) IP address or hostname	No
`site.cfg`	`reg.x.server.H323.y.port`	Port to be used for H.323 signaling. If set to Null, 1719 (H.323 RAS signaling) is used. 0 (default) 0 to 65535	No
`site.cfg`	`reg.x.server.H323.y.expires`	Desired registration period. 3600 positive integer	No
`h323.cfg`	`voIpProt.H323.autoGateKeeperDiscovery`	1 (default) - The phone will attempt to discover an H.323 gatekeeper address via the standard multi cast technique, provided that a statically configured gatekeeper address is not available. 0 - The phone will not send out any gatekeeper discovery messages.	Yes
`h323.cfg`	`voIpProt.H323.blockFacilityOnStartH245`	0 (default) - facility messages when using H.245 are not removed. 1 - facility messages when using H.245 are removed.	Yes
`h323.cfg`	`voIpProt.H323.dtmfViaSignaling.enabled`	1 (default) - The phone will use the H.323 signaling channel for DTMF key press transmission. 0 - The phone will not use H.323 signaling channel for DTMF key press transmission.	Yes

H.323 Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`h323.cfg`	`voIpProt.H323.dtmfViaSignaling.H245alphanumericMode`	1 (default) - The phone will support H.245 signaling channel alphanumeric mode DTMF transmission. 0 - The phone will not support H.245 signaling channel alphanumeric mode DTMF transmission Note: If both alphanumeric and signal modes can be used, the phone gives priority to DTMF.	Yes
`h323.cfg`	`voIpProt.H323.dtmfViaSignaling.H245signalMode`	1 (default) - The phone will support H.245 signaling channel signal mode DTMF transmission. 0 - The phone will not support H.245 signaling channel signal mode DTMF transmission.	Yes
`h323.cfg`	`voIpProt.H323.enable`	0 (default) - The H.323 protocol is not used for call routing, dial plan, DTMF, and URL dialing. 1 - The H.323 protocol is used for call routing, dial plan, DTMF, and URL dialing.	Yes
`h323.cfg`	`voIpProt.H323.local.port`	Local port for sending and receiving H.323 signaling packets. 0 - 1720 is used for the local port but is not advertised in the H.323 signaling. 0 to 65535 - The value is used for the local port and it is advertised in the H.323 signaling.	Yes
`sip-interop.cfg`	`voIpProt.H323.local.RAS.port`	Specifies the local port value for RAS signaling. 1719 (default) 1 to 65535	Yes
`h323.cfg`	`voIpProt.server.H323.x.address`	Address of the H.323 gatekeeper. Only one H.323 gatekeeper per phone is supported. If more than one is configured, only the first is used. Null (default) IP address or hostname	No

H.323 Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`h323.cfg`	`voIpProt.server.H323.x.port`	Port to be used for H.323 signaling. The H.323 gatekeeper RAS signaling uses UDP, while the H.225/245 signaling uses TCP. 1719 (default) 0 to 65535	No
`h323.cfg`	`voIpProt.server.H323.x.expires`	Desired registration period. 3600 (default) positive integer.	No
`site.cfg`	`sec.H235.mediaEncryption.enabled`	1 (default) - The H.235 media encryption is enabled and negotiated. 0 - The H.235 media encryption is disabled.	Yes
`site.cfg`	`sec.H235.mediaEncryption.offer`	0 (default) - The media encryption offer is not initiated with the far-end. 1 - If the `sec.H235.mediaEncryption.enabled` is also 1, media encryption negotiations is initiated with the far-end; however, successful negotiations are not a requirement for the call to complete.	Yes
`site.cfg`	`sec.H235.mediaEncryption.require`	0 (default) - The media encryption requirement is not required. 1 - If the `sec.H235.mediaEncryption.enabled` is also 1, media encryption negotiations are initiated or completed with the far end, and if negotiations fail, the call is dropped.	Yes

Audio-only or Audio-Video Call Parameters

The following parameters configure whether the phone starts a call with audio and video.

Audio-only or Audio-Video Call Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`up.homeScreen.audioCall.enabled`	0 (default) - Disable a Home screen icon that allows users to make audio-only calls. 1 - Enable a Home screen icon that allows users to make audio-only calls. Devices that support video calling show an 'Audio Call' button on the Home screen to initiate audio-only calls.	No
`video.cfg`	`video.autoStartVideoTx`	1 (default) - Automatically begin video to the far side when you start a call. 0 - Video to the far side does not begin. Note that when the phone Base Profile is set to Skype or Lync, the default is 1.	No
`video.cfg`	`video.callMode.default`	**VVX phones** Allow the user to begin calls as audio-only or with video. When you set this parameter to 'video', the VVX 500/501 and 600/601 display a Video Mode soft key and the VVX 1500 displays a video icon. audio (default) Calls begin with audio only. video - Calls begin with video.	No

Phone Display and Appearances

This section lists parameters that configure phone and device display.

Time and Date Display Parameters

Use the parameters in the following table to configure time and display options.

Time and Date Display Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.localClockEnabled	Specifies whether or not the date and time are shown on the idle display. 1 (Default) - Date and time and shown on the idle display. 0 - Date and time are not shown on the idle display.	No
site.cfg	lcl.datetime.date.dateTop	1 (default) - Displays the date above time. 0 - Displays the time above date.	No
site.cfg	lcl.datetime.date.format	The phone displays day and date. "D,dM" (default) String 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 = Thursday, 3 July or Md,D = July 3, Thursday.	No
site.cfg	lcl.datetime.date.longFormat	1 (default) - Displays the day and month in long format (Friday/November). 0 - Displays the day and month in abbreviated format (Fri/Nov).	No
site.cfg	lcl.datetime.time.24HourClock	1 (default) - Displays the time in 24-hour clock mode. 0 - Does not display the time in 24-hour clock mode.	No
site.cfg	tcpIpApp.sntp.address	Specifies the SNTP server address. NULL (default) Valid hostname or IP address.	No
site.cfg	tcpIpApp.sntp.AQuery	Specifies a query to return hostnames. 0 (default) - Queries to resolve the SNTP hostname are performed using DNS SRV. 1 - Query the hostname for a DNS A record.	No
site.cfg	tcpIpApp.sntp.address.overrideDHCP	0 (Default) - DHCP values for the SNTP server address are used. 1 - SNTP parameters override the DHCP values.	No

Time and Date Display Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.sntp.daylight Savings.enable	1 (Default) - Daylight savings rules apply to the displayed time. 0 - Daylight savings time rules are not applied to the displayed time.	No
site.cfg	tcpIpApp.sntp.daylight Savings.fixedDayEnable	0 (Default) - Month, date, and dayOfWeek are used in the DST calculation. 1 - Only month and date are used in the DST calculation.	No
site.cfg	tcpIpApp.sntp.daylight Savings.start.date	Start date for daylight savings time. Range is 1 to 31. 8 (Default) - Second occurrence in the month after DST starts. 0 - If fixedDayEnable is set to 0, this value specifies the occurrence of dayOfWeek when DST should start. 1 - If fixedDayEnable is set to 1, this value is the day of the month to start DST. 15 - Third occurrence. 22 - Fourth occurrence. Example: If value is set to 15, DST starts on the third dayOfWeek of the month.	No
site.cfg	tcpIpApp.sntp.daylight Savings.start.dayOfWee k	Specifies the day of the week to start DST. Range is 1 to 7. 1 (Default) - Sunday 2 - Monday... 7 - Saturday This parameter is not used if fixedDayEnable is set to 1.	No
site.cfg	tcpIpApp.sntp.daylight Savings.start.dayOfWee k.lastInMonth	0 (Default) 1 - DST starts on the last dayOfWeek of the month and the start.date is ignored. This parameter is not used if fixedDayEnable is set to 1.	No
site.cfg	tcpIpApp.sntp.daylight Savings.start.month	Specifies the month to start DST. Range is 1 to 12. 3 (Default) - March 1 - January 2 - February... 12 - December	No

Time and Date Display Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.sntp.daylight Savings.start.time	Specifies the time of day to start DST in 24-hour clock format. Range is 0 to 23. 2 (Default) - 2 a.m. 0 - 12 a.m. 1 - 1 a.m.... 12 - 12 p.m. 13 - 1 p.m... 23 - 11 p.m.	No
site.cfg	tcpIpApp.sntp.daylight Savings.stop.date	Specifies the stop date for daylight savings time. Range is 1 to 31. 1 (Default) - If fixedDayEnable is set to 1, the value of this parameter is the day of the month to stop DST. Set 1 for the first occurrence in the month. 0 - If fixedDayEnable is set to 0, this value specifies the dayOfWeek when DST should stop. 8 - Second occurrence. 15 - Third occurrence. 22 - Fourth occurrence. Example: If set to 22, DST stops on the fourth dayOfWeek in the month.	No
site.cfg	tcpIpApp.sntp.daylight Savings.stop.dayOfWeek	Day of the week to stop DST. Range is 1 to 7. 1 (default) - Sunday 2 - Monday 3 - Tuesday 7 - Saturday Parameter is not used if fixedDayEnable is set to 1.	No
site.cfg	tcpIpApp.sntp.daylight Savings.stop.dayOfWeek .lastInMonth	1 - DST stops on the last dayOfWeek of the month and the stop.date is ignored). Parameter is not used if fixedDayEnable is set to 1.	No
site.cfg	tcpIpApp.sntp.daylight Savings.stop.month	Specifies the month to stop DST. Range is 1 to 12. 11 - November 1 - January 2 - February… 12 - December	No

Time and Date Display Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.sntp.daylight Savings.stop.time	Specifies the time of day to stop DST in 24-hour clock format. Range is 0 to 23. 2 (Default) - 2 a.m. 0 - 12 a.m. 1 - 1 a.m.... 12 - 12 p.m. 13 - 1 p.m... 23 - 11 p.m.	No
site.cfg	tcpIpApp.sntp.gmtOffse t	Specifies the offset in seconds of the local time zone from GMT. 0 (Default) - GMT 3600 seconds = 1 hour -3600 seconds = -1 hour Positive or negative integer	No
site.cfg	tcpIpApp.sntp.gmtOffse tcityID	Range is 0 to127. NULL (Default) For descriptions of all values, refer to Time Zone Location Description.	No
site.cfg	tcpIpApp.sntp.gmtOffse t.overrideDHCP	0 (Default) - The DHCP values for the GMT offset are used. 1 - The SNTP values for the GMT offset are used.	No

Time and Date Display Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.sntp.resyncPeriod	Specifies the period of time (in seconds) that passes before the phone resynchronizes with the SNTP server. 86400 (Default). 86400 seconds is 24 hours. Positive integer	No
site.cfg	tcpIpApp.sntp.retryDnsPeriod	Sets a retry period for DNS queries. 86400 (Default). 86400 seconds is 24 hours. 60 – 2147483647 seconds The DNS retry period is affected by other DNS queries made on the phone. If the phone makes a query for another service during the retry period, such as SIP registration, and receives no response, the Network Time Protocol (NTP) DNS query is omitted to limit the retry attempts to the unresponsive server. If no other DNS attempts are made by other services, the retry period is not affected. If the DNS server becomes responsive to another service, NTP immediately retries the DNS query.	No

Phone Theme Parameters

Use the parameters in the following table to configure a theme for the VVX 500/501 and 600/601 business media phones.

Phone Theme Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg	device.theme	Classic (default) - The phone uses the Classic theme. Modern - The phone uses the Modern theme.	No
device.cfg	device.theme.set	1 (Default) - The phone supports both the Classic and Modern theme. The device.theme parameter specifies which theme to use. 0 - The phone supports only Modern theme.	No

Default Off-Hook Phone Screen Parameters

Use the parameters in the following table to set the default screen that displays when the phone is off-hook or in a call.

Default Phone Screen Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.LineViewCall Status.enabled	0 (Default) - In an active call, the active call screen displays. Any incoming or outgoing call triggers display of the active call screen. 1 - During an incoming call and in an active call, the line view displays and call details display on the status ribbon.	No
features.cfg	up.LineViewCall StatusTimeout	Specify the timeout period after which the phones go back to the Line Screen when the user goes to the Active Call Screen from the Line View. Available on VVX 500 and 600 business media phones. 10 (default) - The phone returns to the line screen after 10 seconds. 2 - 10 - Specify the seconds after which the phone returns to the line screen.	No
features.cfg	up.OffHookLineV iew.enabled	0 (Default) - After the phone goes off-hook, the phone displays the dialing screen. 1 - After the phone goes off hook, the phone displays the line screen.	No

Graphic Display Background Parameters

The configured background image displays across the entire phone screen, and the time, date, line and key labels display over the background. If you want the background image to display more visibly from behind line key labels, use up.transparentLines to render line key labels transparent—this option is available only on the VVX 500/501 and 600/601 business media phones.

Use the parameters in the following table to configure graphic display background on VVX business media phones and connected expansion modules.

Graphic Display Background Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	bg.background.enabled	0 (default) - The user cannot set the background image of the phone screen and the background image option is not available on the phone menu or in the Web Configuration Utility when logged in as a user. In addition, the icon to set the displayed image as a background in the picture frame menu does not display. 1 - The user can set the background image on the phone screen from the phone menu or when logged into the Web Configuration Utility.	No
features.cfg	bg.color.bm.x.em.name	Specify the name of the Expansion Module (EM) background image file including extension with a URL or file path of a BMP or JPEG image. Note: If the file is missing or unavailable, the built-in default solid pattern is displayed.	No
features.cfg	bg.color.bm.x.name	Specify the name of the phone screen background image file including extension with a URL or file path of a BMP or JPEG image. Note: If the file is missing or unavailable, the built-in default solid pattern is displayed.	No

Graphic Display Background Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot

`features.cfg`	`bg.color.selection`	Specify which type of background (w) and index (x) for that type is selected on reboot. The default selection is 1,1 the first solid background.
		
		Use w=1 and x=1 (1,1) to select the built-in image.
		
		Use w=2 and x= 1 to 4 to select one of the four `solid` backgrounds.
		
		Use w=3 and x= 1 to 6 to select one of the six background `bm` images
		
		You can set backgrounds for specific phone models by adding the model name, for example:
		
		`bg.color.VVX500.selection,`
		`bg.color.VVX1500.selection`
		
		Note that although the VVX 300 series phones use a grayscale background, you can use this parameter to set the background.
		
		1,1 (default)
		
		w,x
			No

`features.cfg`	`up.transparentLines`	Enable or disable transparent line key labels on the VVX 500/501 and 600/601.	
`features.cfg`	`up.transparentLines`	0 (Default) - Line keys block display of the background image. 1 - Line keys are transparent and allow the background image to display behind the line labels. Applies only to the VVX 500/501 and 600/601 business media phones.	No

Digital Picture Frame Parameters

The parameters you can configure are listed in the following table.

Digital Picture Frame Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.pictureFrame.e nabled	For the VVX 500/501, 600/601, and 1500 only. 1 (default) - Enable the digital picture frame. 0 - Disable the digital picture frame.	Yes
features.cfg	up.pictureFrame.folder	Path name for images. NULL (Default) - Images stored in the root folder on the USB flash drive are displayed. string - 0 to 40 characters Example: If images are stored in the /images/phone folder on the USB flash drive, set this parameter to images/phone. For the VVX 500/501, 600/601, and 1500 only.	No
features.cfg	up.pictureFrame.timePe rImage	For the VVX 500/501, 600/601, and 1500 only. The number of seconds to display each picture frame image. Range is 3 to 300 seconds. 5 (Default)	No

Phone Language Parameters

You can select the language that displays on the phone using the parameters in the following table.

Phone Language Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg`	`device.spProfile`	NULL (default) - The default language is an empty string (`lcl.ml.lang=""`), which is English. DT - The default language is German (`lcl.ml.lang="German_Germany"`).	No
`site.cfg`	`lcl.ml.lang`	Null (default) - Sets the phone language to US English. String - Sets the phone language specified in the `lcl.ml.lang.menu.x.label` parameter.	No
`site.cfg`	`lcl.ml.lang.menu.x`	Specifies the dictionary files for the supported languages on the phone. Null (default) String Dictionary files must be sequential. The dictionary file cannot have caps, and the strings must exactly match a folder name of a dictionary file.	No
`site.cfg`	`lcl.ml.lang.menu.x.label`	Specifies the phone language menu label. The labels must be sequential. Null (default) String	Yes

Time Zone Location Parameters

The following parameters configure time zone location.

TimeZone Location Parameters

Permitted Values	Permitted Values
0 (GMT -12:00) Eniwetok,Kwajalein	61 (GMT +2:00) Helsinki,Kyiv
1 (GMT -11:00) Midway Island	62 (GMT +2:00) Riga,Sofia
2 (GMT -10:00) Hawaii	63 (GMT +2:00) Tallinn,Vilnius
3 (GMT -9:00) Alaska	64 (GMT +2:00) Athens,Istanbul
4 (GMT -8:00) Pacific Time (US & Canada)	65 (GMT +2:00) Damascus
5 (GMT -8:00) Baja California	66 (GMT +2:00) E.Europe
6 (GMT -7:00) Mountain Time (US & Canada)	67 (GMT +2:00) Harare,Pretoria
7 (GMT -7:00) Chihuahua,La Paz	68 (GMT +2:00) Jerusalem
8 (GMT -7:00) Mazatlan	69 (GMT +2:00) Kaliningrad (RTZ 1)
9 (GMT -7:00) Arizona	70 (GMT +2:00) Tripoli
10 (GMT -6:00) Central Time (US & Canada)	
11 (GMT -6:00) Mexico City	71 (GMT +3:00) Moscow
12 (GMT -6:00) Saskatchewan	72 (GMT +3:00) St.Petersburg
13 (GMT -6:00) Guadalajara	73 (GMT +3:00) Volgograd (RTZ 2)
14 (GMT -6:00) Monterrey	74 (GMT +3:00) Kuwait,Riyadh
15 (GMT -6:00) Central America	75 (GMT +3:00) Nairobi
16 (GMT -5:00) Eastern Time (US & Canada)	78 (GMT +3:00) Baghdad
17 (GMT -5:00) Indiana (East)	76 (GMT +3:00) Minsk
18 (GMT -5:00) Bogota,Lima	77 (GMT +3:30) Tehran
19 (GMT -5:00) Quito	79 (GMT +4:00) Abu Dhabi,Muscat
20 (GMT -4:30) Caracas	80 (GMT +4:00) Baku,Tbilisi
21 (GMT -4:00) Atlantic Time (Canada)	81 (GMT +4:00) Izhevsk,Samara (RTZ 3)
22 (GMT -4:00) San Juan	82 (GMT +4:00) Port Louis
23 (GMT -4:00) Manaus,La Paz	83 (GMT +4:00) Yerevan
24 (GMT -4:00) Asuncion,Cuiaba	84 (GMT +4:30) Kabul
25 (GMT -4:00) Georgetown	85 (GMT +5:00) Ekaterinburg (RTZ 4)
26 (GMT -3:30) Newfoundland	86 (GMT +5:00) Islamabad
27 (GMT -3:00) Brasilia	87 (GMT +5:00) Karachi
28 (GMT -3:00) Buenos Aires	88 (GMT +5:00) Tashkent
29 (GMT -3:00) Greenland	89 (GMT +5:30) Mumbai,Chennai
30 (GMT -3:00) Cayenne,Fortaleza	90 (GMT +5:30) Kolkata,New Delhi

Permitted Values		Permitted Values	
31	(GMT -3:00) Montevideo	91	(GMT +5:30) Sri Jayawardenepura
32	(GMT -3:00) Salvador	92	(GMT +5:45) Kathmandu
33	(GMT -3:00) Santiago	93	(GMT +6:00) Astana,Dhaka
34	(GMT -2:00) Mid-Atlantic	94	(GMT +6:00) Almaty
35	(GMT -1:00) Azores	95	(GMT +6:00) Novosibirsk (RTZ 5)
36	(GMT -1:00) Cape Verde Islands	96	(GMT +6:30) Yangon (Rangoon)
37	(GMT 0:00) Western Europe Time	97	(GMT +7:00) Bangkok,Hanoi
38	(GMT 0:00) London,Lisbon	98	(GMT +7:00) Jakarta
39	(GMT 0:00) Casablanca	99	(GMT +7:00) Krasnoyarsk (RTZ 6)
40	(GMT 0:00) Dublin	100	(GMT +8:00) Beijing,Chongqing
41	(GMT 0:00) Edinburgh	101	(GMT +8:00) Hong Kong,Urumqi
42	(GMT 0:00) Monrovia	102	(GMT +8:00) Kuala Lumpur
43	(GMT 0:00) Reykjavik	103	(GMT +8:00) Singapore
44	(GMT +1:00) Belgrade	104	(GMT +8:00) Taipei,Perth
45	(GMT +1:00) Bratislava	105	(GMT +8:00) Irkutsk (RTZ 7)
46	(GMT +1:00) Budapest	106	(GMT +8:00) Ulaanbaatar
47	(GMT +1:00) Ljubljana	107	(GMT +9:00) Tokyo,Seoul,Osaka
48	(GMT +1:00) Prague	108	(GMT +9:00) Sapporo,Yakutsk (RTZ 8)
49	(GMT +1:00) Sarajevo,Skopje	109	(GMT +9:30) Adelaide,Darwin
50	(GMT +1:00) Warsaw,Zagreb	110	(GMT +10:00) Canberra
51	(GMT +1:00) Brussels	111	(GMT +10:00) Magadan (RTZ 9)
52	(GMT +1:00) Copenhagen	112	(GMT +10:00) Melbourne
53	(GMT +1:00) Madrid,Paris	113	(GMT +10:00) Sydney,Brisbane
54	(GMT +1:00) Amsterdam,Berlin	114	(GMT +10:00) Hobart
55	(GMT +1:00) Bern,Rome	115	(GMT +10:00) Vladivostok
56	(GMT +1:00) Stockholm,Vienna	116	(GMT +10:00) Guam,Port Moresby
57	(GMT +1:00) West Central Africa	117	(GMT +11:00) Solomon Islands
58	(GMT +1:00) Windhoek	118	(GMT +11:00) New Caledonia
59	(GMT +2:00) Bucharest,Cairo	119	(GMT +11:00) Chokurdakh (RTZ 10)
60	(GMT +2:00) Amman,Beirut	120	(GMT +12:00) Fiji Islands
		121	(GMT +12:00) Auckland,Anadyr
		122	(GMT +12:00) Petropavlovsk-Kamchatsky (RTZ 11)
		123	(GMT +12:00) Wellington
		124	(GMT +12:00) Marshall Islands
		125	(GMT +13:00) Nuku'alofa
		126	(GMT +13:00) Samoa

Digital Phone Label Parameters

When enabled, the `lcl.status.LineInfoAtTopText` parameter provides the text to be displayed in the status bar of the phone. You can enable the feature by setting the value of the `lcl.status.LineInfoAtTop` parameter to 1.

Registration Line Address Bar Parameter

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	lcl.status.LineInfoAtTop	Displays the complete registration line address in the status bar of the phones screen. 0 (default) – Does not display the registration line address in the status bar of the phone's screen. 1 –The lcl.status.LineInfoAtTopText parameter provides the text to be displayed in the status bar of the phone.	No
site.cfg	lcl.status.LineInfoAtTopText	Provides the text be displayed on the phones screen. Null (default) String (14 maximum characters)	No

Unique Line Labels for Registration Lines Parameters

When using this feature with the parameter `reg.x.label.y` where x=2 or higher, multiple line keys display for the registered line address.

Configure Unique Line Labels

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.line.y.label`	Configure a unique line label for a shared line that has multiple line key appearances. This parameter takes effect when `up.cfgUniqueLineLabel=1`. If `reg.x.linekeys=1`, this parameter does not have any effect. x = the registration index number starting from 1. y = the line index from 1 to the value set by `reg.x.linekeys`. Specifying a string sets the label used for the line key registration on phones with multiple line keys. If no parameter value is set for `reg.x.line.y.label`, the phone automatically numbers multiple lines by prepending "<y>_" where <y> is the line index from 1 to the value set by `reg.x.linekeys`. • The following examples show labels for line 1 on a phone with user registration 1234, where `reg.x.linekeys=2`: ⤷ If no label is configured for registration, the labels are "1_1234" and "2_1234". ⤷ If `reg.1.line.1.label=Polycom` and `reg.1.line.2.label=VVX`, the labels display as 'Polycom' and 'VVX'.	No

Configure Unique Line Labels

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.cfgLabelElide	Controls the alignment of the line label. When the line label is an alphanumeric or alphabetic string, the label aligns right. When the line label is a numeric string, the label aligns left. None (Default) Right Left	No
features.cfg	up.cfgUniqueLineLabel	Allow unique labels for the same registration that is split across multiple line keys using reg.X.linekeys. 0 (Default) - Use the same label on all line keys. 1 - Display a unique label as defined by reg.X.line.Y.label. If reg.X.line.Y.label is not configured, then a label of the form <integer>_ will be applied in front of the applied label automatically.	No

LED Behavior Parameters

The LED pattern parameters listed in the following table configure the pattern state, color, and duration of the LED indicators and the pattern types on Polycom devices and expansion modules. For example configurations, refer to LED Pattern Examples.

For each parameter, specify x, y, and a permitted value:

- Specify an LED pattern using the LED pattern parameters.
- For x, specify an LED pattern type.
- For y, specify the step in the LED pattern with a number between 1-20.

Use the parameters in the following table lists to set the pattern state, color, and duration of the LED indicators on VVX phones and expansion modules.

LED Behavior Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`ind.pattern.x.step.y.state`	0 - Turn off the LED indicator. 1 - Turn on the LED indicator.	No
`features.cfg`	`ind.pattern.x.step.y.color`	Specify the color of the LED indicator. The Yellow value is available only for VVX 300 and 400 series phones. The Yellow value is not available for line key indicators on VVX 101 and 201 phones or VVX Expansion Modules. Red Green Yellow	No
`features.cfg`	`ind.pattern.x.step.y.duration`	Specify the duration of the pattern in milliseconds from 0 to infinite.	No

User Accounts and Contacts

This section lists parameters that configure user accounts and contacts

User Profile Parameters

Before you configure user profiles, you must complete the following:

- Create a phone configuration file, or update an existing file, to enable the feature's settings.
- Create a user configuration file in the format **<user>.cfg** to specify the user's password, registration, and other user-specific settings that you want to define.

> Important: You can reset a user's password by removing the password parameter from the override file. This causes the phone to use the default password in the <user>.cfg file.

When you set up the user profile feature, you can set the following conditions:

- If users are required to always log in to use a phone and access their personal settings.
- If users are required to log in and have the option to use the phone as is without access to their personal settings.
- If users are automatically logged out of the phone when the phone restarts or reboots.

● If users remain logged in to the phone when the phone restarts or reboots.

Use the parameters in the following table to enable users to access their personal phone settings from any phone in the organization.

User Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	prov.login.automaticLogout	Specify the amount of time before a non-default user is logged out. 0 minutes (default) 0 to 46000 minutes	No
site.cfg	prov.login.defaultOnly	0 (default) - The phone cannot have users other than the default user. 1 - The phone can have users other than the default user.	No
site.cfg	prov.login.defaultPassword	Specify the default password for the default user. NULL (default)	No
site.cfg	prov.login.defaultUser	Specify the name of the default user. If a value is present, the user is automatically logged in when the phone boots up and after another user logs out. NULL (default)	No
site.cfg	prov.login.enabled	0 (default) - The user profile is disabled. 1 - The user profile feature is enabled.	No
site.cfg	prov.login.localPassword.hashed	0 (default) - The user's local password is formatted and validated as clear text. 1 - The user's local password is created and validated as a hashed value.	No
site.cfg	prov.login.localPassword	Specify the password used to validate the user login. The password is stored either as plain text or as an encrypted SHA1 hash. 123 (default)	No

User Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	prov.login.persis tent	0 (default) - Users are logged out if the handset reboots. 1 - Users remain logged in when the phone reboots.	No
site.cfg	prov.login.requir ed	0 (default) - The user does not have to log in. 1 - The user must log in when the login feature is enabled.	No
site.cfg	prov.login.usePro vAuth	0 (default) - The phone do not user server authentication. 1 - The phones use server authentication and user login credentials are used as provisioning server credentials.	No
site.cfg	voIpProt.SIP.spec ialEvent.checkSyn c.downloadCallLis t	0 (default) - The phone does not download the call list for the user after receiving a checksync event in the NOTIFY. 1 - The phone downloads the call list for the user after receiving a checksync event in the NOTIFY.	No

Local Contact Directory Parameters

The following parameters configure the local contact directory.

Local Contact Directory Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.local.con tacts.maxNum	Set the maximum number of contacts that can be stored in the Local Contact Directory. The maximum number varies by phone model, refer to section 'Maximum Capacity of the Local Contact Directory'. 1 - 3000	No
features.cfg	dir.local.pas swordProtecte d	0 (default) - Disable password protection of the local Contact Directory. 1 - Enables password protection of the local Contact Directory.	No

Local Contact Directory Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`dir.local.readonly`	0 (default) - Disable read only protection of the local Contact Directory. 1 - Enable read-only protection of the local Contact Directory.	No
`features.cfg`	`feature.directory.enabled`	0 (default) - The local contact directory is disabled when the RealPresence Trio solution Base Profile is set to Lync. 1 - The local directory is enabled when the RealPresence Trio solution Base Profile is set to Lync.	No
`features.cfg`	`dir.search.field`	Specify whether to search the directory by first name or last name. 0 (default) - Contact directory searches are sorted by contact's last name. 1 - Contact directory searches are sorted by first name.	No
`site.cfg`	`voIpProt.SIP.specialEvent.checkSync.downloadDirectory`	0 (default) - The phone downloads updated directory files after receiving a checksync NOTIFY message. 1 - The phone downloads the updated directory files along with any software and configuration updates after receiving a checksync NOTIFY message. The files are downloaded when the phone restarts, reboots, or when the phone downloads any software or configuration updates. Note: The parameter `hotelingMode.type` set to `2` or `3` overrides this parameter.	No

Local Contact Directory Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.local.pass wordProtected	Specify whether you are prompted for an Admin/User password when adding, editing, or deleting contacts in the Contact Directory.	No
features.cfg	dir.local.UIen abled	1 (default) - Displays Favorites and Contact Directory options in the Directories menu, and displays the Favorites quick access menu on the Home screen of the VVX 500/501 and 600/601 business media phones. 0 – Hides the Contact Directory and Favorites options in the Directories menu and the dial pad. On VVX 500/501 and 600/601 business media phones, hides the Favorites quick access menu on the Home screen.	No

Corporate Directory Parameters

Use the parameters in the following table to configure this feature. Note that the exact configuration of a corporate directory depends on the LDAP server you use.

Web Info: For detailed explanations and examples of all currently supported LDAP directories, see *Technical Bulletin 41137*: *Best Practices When Using Corporate Directory on Polycom Phones* at Polycom Engineering Advisories and Technical Notifications.

Use the Corporate Directory

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.address	Set the IP address or hostname of the LDAP server interface to the corporate directory. Null (default) IP address Hostname FQDN	Yes
features.cfg	dir.corp.alt.address	Enter the URL address of the GAB service provided by the server. Null (default) Hostname FQDN	No
features.cfg	dir.corp.alt.attribute.x.filter	Enter a filter to use to set a predefined search string through configuration files. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.attribute.x.label	Enter a label to identify a user. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.attribute.x.name	Enter the name of the parameter to match on the server. Each name must be unique; however, a global address book entry can have multiple parameters with the same name. You can configure up to eight parameters (x = 1 to 8). Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.attribute.x.sticky	0 (default) —the filter string criteria for attribute x is reset after a reboot. 1—the filter string criteria is retained through a reboot. If you set an attribute to be sticky (set this parameter to 1), a '*' displays before the label of the attribute on the phone.	No

Use the Corporate Directory

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.alt.attribute.x.type	Define how x is interpreted by the phone. Entries can have multiple parameters of the same type. first_name last_name (default) phone_number SIP_address Other—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 global address book directory.	No
features.cfg	dir.corp.alt.auth.useLoginCredentials	0 (default) 1	No
features.cfg	dir.corp.alt.autoQuerySubmitTimeout	0 (default) 0 - 60	No
features.cfg	dir.corp.alt.password	Enter the password used to authenticate to the GENBAND server. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.port	Set the port that connects to the server if a full URL is not provided. 0 (default) Null 1 to 65535	No
features.cfg	dir.corp.alt.protocol	Set a directory protocol used to communicate to the corporate directory. sopi (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.transport	Choose a transport protocol used to communicate to the corporate directory. TCP (default) TLS	No

Use the Corporate Directory

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.alt.user	Enter the user name used to authenticate to the GENBAND server. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.viewPersistence	Determine if the results from the last address directory search displays on the phone. 0 (default) 1	No
features.cfg	dir.corp.attribute.x.addstar	Determine if the wild-card character, asterisk(*), is appended to the LDAP query field. 0 1 (default)	Yes
features.cfg	dir.corp.attribute.x.filter	Set the filter string for this parameter, which is edited when searching. Null (default) UTF-8 encoding string	Yes
features.cfg	dir.corp.attribute.x.label	Enter the label that shows when data is displayed. Null (default) UTF-8 encoding string	Yes
features.cfg	dir.corp.attribute.x.name	Enter the name of the parameter to match on the server. Each name must be unique; however, a global address book entry can have multiple parameters with the same name. You can configure up to eight parameters (x = 1 to 8). Null (default) UTF-8 encoding string	Yes
features.cfg	dir.corp.attribute.x.searchable	Determine whether quick search on parameter x (if x is 2 or more) is enabled or disabled. 0 (default) 1	Yes

Use the Corporate Directory

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.attribute.x.sticky	0 (default) —the filter string criteria for attribute x is reset after a reboot. 1—the filter string criteria is retained through a reboot. If you set an attribute to be sticky (set this parameter to 1), a '*' displays before the label of the attribute on the phone.	Yes
features.cfg	dir.corp.attribute.x.type	Define how x is interpreted by the phone. Entries can have multiple parameters of the same type. first_name last_name (default) phone_number SIP_address H323_address URL other 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 global address book directory.	Yes
features.cfg	dir.corp.auth.useLoginCredentials	0 (default) 1	No
features.cfg	dir.corp.autoQuerySubmitTimeout	Set the timeout (in seconds) between when the user stops entering characters in the quick search and when the search query is automatically submitted. 0 (default)—there is no timeout and automatic submit is disabled. 0 - 60 seconds	Yes
features.cfg	dir.corp.backGroundSync.period	Set the time (in seconds) the corporate directory cache is refreshed after the corporate directory feature has not been used for the specified period of time. 86400 (default) **3600 to 604800**	Yes

Use the Corporate Directory

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.backGroundSync	Determine if background downloading from the LDAP server is allowed. 0 (default) 1	Yes
features.cfg	dir.corp.baseDN	Enter the base domain name, which is the starting point for making queries on the LDAP server. Null (default) UTF-8 encoding string	Yes
features.cfg	dir.corp.bindOnInit	Determine if bind authentication is used on initialization. 0 1 (default)	Yes
features.cfg	dir.corp.cacheSize	The maximum number of entries that can be cached locally on the VVX business media phones. 32 to 64 64 (default)	No
features.cfg	dir.corp.cacheSize	Determine the maximum number of entries that can be cached locally on the phone. 128 (default) 32 to 256 For VVX 101, the permitted values are 32 to 64 where 64 is the default.	Yes
features.cfg	dir.corp.customError	Enter the error message to display on the phone when the LDAP server finds an error. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.domain	0 to 255	No
features.cfg	dir.corp.filterPrefix	Enter the predefined filter string for search queries. (objectclass=person) (default) UTF-8 encoding string	Yes

Use the Corporate Directory

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`dir.corp.pageSize`	Set the maximum number of entries requested from the corporate directory server with each query. 32 (default) 8 to 64 For VVX 101, the permitted values are 8 to 32 where 16 is the default.	Yes
`features.cfg`	`dir.corp.password`	Enter the password used to authenticate to the LDAP server. Null (default) UTF-8 encoding string	Yes
`features.cfg`	`dir.corp.port`	Enter the port that connects to the server if a full URL is not provided. 389 (default for TCP) 636 (default for TLS) 0 Null 1 to 65535	Yes
`features.cfg`	`dir.corp.querySupportedControlOnInit`	Determine if the phone makes an initial query to check the status of the server when booting up. 0 1 (default)	No
`features.cfg`	`dir.corp.scope`	sub (default)—a recursive search of all levels below the base domain name is performed. one —a search of one level below the base domain name is performed. base—a search at the base domain name level is performed.	Yes
`features.cfg`	`dir.corp.sortControl`	Determine how a client can make queries and sort entries. 0 (default)—leave sorting as negotiated between the client and server. 1—force sorting of queries, which causes excessive LDAP queries and should only be used to diagnose LDAP servers with sorting problems.	Yes

Use the Corporate Directory

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.transport	Specify whether a TCP or TLS connection is made with the server if a full URL is not provided. TCP (default) TLS Null	Yes
features.cfg	dir.corp.user	Enter the user name used to authenticate to the LDAP server. Null (default) UTF-8 encoding string	Yes
features.cfg	dir.corp.viewPersistence	0 (default) — the corporate directory search filters and browsing position are reset each time the user accesses the corporate directory. 1— the search filters and browsing position from the previous session are displayed each time the user accesses the corporate directory.	Yes
features.cfg	dir.corp.vlv.allow	Determine whether virtual view list (VLV) queries are enabled and can be made if the LDAP server supports VLV. 0 (default) 1	Yes
features.cfg	dir.corp.vlv.sortOrder	Enter the list of parameters, in exact order, for the LDAP server to use when indexing. For example: sn, givenName, telephoneNumber. Null (default) list of parameters	Yes

Call Log Parameters

Use the parameters in the following table to configure call logs

Call Log Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.callLis tMissed.enabled	0 (Default) - The missed call list is disabled 1 - The missed call list is enabled. To enable the missed, placed, or received call lists, feature.callList.enabled must be enabled.	No
features.cfg	feature.callLis tPlaced.enabled	0 (Default) - The placed call list is disabled 1 - The placed call list is enabled. To enable the missed, placed, or received call lists, feature.callList.enabled must be enabled.	No

Call Log Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.callLis tReceived.enabl ed`	0 (Default) - The received call list is disabled 1 - The received call list is enabled. To enable the missed, placed, or received call lists, `feature.callList.enabled` must be enabled.	
`features.cfg`	`feature.exchang eCallLog.enable d`	If Base Profile is: Generic – 0 (default) Skype for Business - 1 (default) 1 - The Exchange call log feature is enabled, user call logs are synchronized with the server, and the user call log history of Missed, Received, and outgoing calls can be retrieved on the phone. You must also enable the parameter `feature.callList.enabled` to use the Exchange call log feature. • The value of the configuration parameter `callLists.collapseDupl icates` that collapses call lists has no effect in a Skype for Business environment. • The local call logs are not generated when the following parameters are disabled: ⬥ `feature.callListMisse d.enabled` ⬥ `feature.callListPlace d.enabled` ⬥ `feature.callListRecei ved.enabled` 0 - The Exchange call log feature is disabled, the user call logs history cannot be retrieved from the Exchange server, and the phone generates call logs locally.	

Microsoft Exchange Integration Parameters

The following table lists parameters that configure Microsoft Exchange integration.

Exchange Integration Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`applicatio ns.cfg`	`exchange.meeting.alert.fo llowOfficeHours`	1 - Audible alerts occur during business hours. 0 - Audible alerts occur at all times.	No
`applicatio ns.cfg`	`exchange.meeting.alert.to nePattern`	positiveConfirm (default) - Set the tone pattern of the reminder alerts using any tone specified by `se.pat.*`. See section Customize Audio Sound Effects in the UC Software Administrator Guide.	No
`applicatio ns.cfg`	`exchange.meeting.alert.to neVolume`	10 (default) - Set the volume level of reminder alert tones. 0 - 17	No
`applicatio ns.cfg`	`exchange.meeting.parseOpt ion`	Indicates the field in the meeting invite from which the VMR or meeting number should be fetched. Location (default) All LocationAndSubject Description	
`applicatio ns.cfg`	`exchange.meeting.phonePat tern`	NULL (default) string The pattern used to identify phone numbers in meeting descriptions, where "x" denotes any digit and "|" separates alternative patterns (for example, xxx-xxx-xxxx|604.xxx.xxxx).	No
`applicatio ns.cfg`	`exchange.meeting.reminder Enabled`	1 (default) - Meeting reminders are enabled. 0 - Meeting reminders are disabled.	No

Exchange Integration Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applicatio ns.cfg	exchange.meeting.reminder Interval	300 seconds (default) 60 - 900 seconds Set the interval at which phones display reminder messages.	No
applicatio ns.cfg	exchange.meeting.reminder Sound.enabled	1 - The phone makes an alert sound when users receive reminder notifications of calendar events. 0 - The phone does not make an alert sound when users receives reminder notifications of calendar events. Note that when enabled, alert sounds take effect only if exchange.meeting.remin derEnabled is also enabled.	No
applicatio ns.cfg	exchange.meeting.reminder Type	Customize the calendar reminder and tone. 2 (default) - Reminder is always audible and visual. 1 - The first reminder is audible and visual reminders are silent. 0 - All reminders are silent.	No
applicatio ns.cfg	exchange.server.url	NULL (default) string The Microsoft Exchange server address.	No
applicatio ns.cfg	feature.EWSAutodiscover.e nabled	If you configure exchange.server.url and set this parameter to 1, preference is given to the value of exchange.server.url. 1 (default) - Exchange autodiscovery is enabled and the phone automatically discovers the Exchange server using the email address or SIP URI information. 0 - Exchange autodiscovery is disabled on the phone and you must manually configure the Exchange server address.	No

Exchange Integration Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.exchangeCalendar.enabled`	For the RealPresence Trio 8800 solution, VVX 300/301, 310/311, 400/401, 410/411, 500/501, 600/601 and 1500 phones, and the CX5500 Unified Conference Station. 0 (default) - The calendaring feature is disabled. 1 - The calendaring feature is enabled. You must enable this parameter if you also enable `feature.exchangeCallLog.enabled`. If you disable `feature.exchangeCalendar.enabled`, also disable `feature.exchangeCallLog.enabled` to ensure call log functionality.	No
`features.cfg`	`feature.exchangeCallLog.enabled`	1 (default) - The Exchange call log feature is enabled and the user call log history of Missed, Received, and outgoing calls can be retrieved on the phone. You must also enable the parameter `feature.exchangeCalendar.enabled` to use the Exchange call log feature. If you disable `feature.exchangeCalendar.enabled`, also disable `feature.exchangeCallLog.enabled` to ensure call log functionality. 0 (default) - The Exchange call log feature is disabled and the user call logs history cannot be retrieved from the Exchange server.	No

Exchange Integration Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.c fg	feature.exchangeContacts. enabled	1 (default) - The Exchange call log feature is enabled and the user call log history of Missed, Received, and outgoing calls can be retrieved on the phone. 0 - The Exchange call log feature is disabled and the user call logs history cannot be retrieved from the Exchange server. You must also enable the parameter feature.exchangeCallLog.e nabled to use the Exchange call log feature.	No
features.c fg	feature.exchangeVoiceMail .enabled	1 (default) - The Exchange voicemail feature is enabled and users can retrieve voicemails stored on the Exchange server from the phone. 0 - The Exchange voicemail feature is disabled and users cannot retrieve voicemails from Exchange Server on the phone. You must also enable feature.exchangeCalendar. enabled to use the Exchange contact feature.	No
features.c fg	feature.exchangeVoiceMail .skipPin.enabled	1 (default) - 0 -	No
features.c fg	feature.lync.abs.enabled	1 - Enable comprehensive contact search in the Skype for Business address book service. 0 - Disable comprehensive contact search in the Skype for Business address book service.	No

Exchange Integration Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.lync.abs.maxResult	12 (default) 5 - 50 The value for this parameter defines the maximum number of contacts to display in a Skype for Business address book service contact search.	No
features.cfg	up.oneTouchDirectory	1 - The Skype for Business Search icon displays on the Home screen. 0 - The Skype for Business Search icon does not display on the Home screen.	No
features.cfg	up.oneTouchVoiceMail[1]	0 - The phone displays a summary page with message counts. The user must press the Connect soft key to dial the voicemail server. 1 - The phone dials voicemail services directly (if available on the call server) without displaying the voicemail summary.	No

Call Controls

This section lists parameters that configure call controls.

Persistent Microphone Mute Parameters

Use the following parameter to enable persistent microphone mute.

Persistent Microphone Mute Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.persistentMute.enabled	0 (default) - Mute ends when the active call ends or when the phone restarts. 1 - Enable the persistent mute feature.	Yes

Calling Party Identification Parameters

Use the parameters in the following table to configure Calling Party Identification.

Calling Party Identification Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-basic.cfg	call.callsPerLineKey	Set the maximum number of concurrent calls per line key. This parameter applies to all registered lines. Note that this parameter can be overridden by the per-registration parameter reg.x.callsPerLineKey. The maximum number of concurrent calls per line key varies by phone model and is listed for each phone in the column *Calls Per Line Key* in the table Flexible Call Appearances. 24 1 - 24 VVX 101, 201 8 (default) 1- 8	No
features.cfg	up.useDirectoryNames	1 (default) - The name field in the local contact directory is used as the caller ID for incoming calls from contacts in the local directory. Note: Outgoing calls and corporate directory entries are not matched. 0 - Names provided through network signaling are used for caller ID.	No

Remote Party Caller ID from SIP Messages Parameters

Use the following parameters to specify which SIP request and response messages to use to retrieve caller ID information.

Remote Party Caller ID from SIP Messages Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-inte rop.cfg`	`voIpProt.SIP.CID.re quest.sourceSipMess age`	Specify which header in the SIP request to retrieve remote party caller ID from. You can use: • `voIpProt.SIP.callee.sourc ePreference` • `voIpProt.SIP.caller.sourc ePreference` • `voIpProt.SIP.CID.sourcePr eference` UPDATE takes precedence over the value of this parameter. NULL (default) - Remote party caller ID information from INVITE is used. INVITE PRACK ACK This parameter does not apply to shared lines.	No
`sip-inte rop.cfg`	`voIpProt.SIP.CID.re sponse.sourceSipMes sage`	Specify which header in the SIP request to retrieve remote party caller ID from. You can use: • `voIpProt.SIP.callee.sourc ePreference` • `voIpProt.SIP.caller.sourc ePreference` • `voIpProt.SIP.CID.sourcePr eference` NULL (default) - The remote party caller ID information from the last SIP response is used. 100, 180, 183, 200 This parameter does not apply to shared lines.	No

Calling Line Identification Parameters

You can configure this feature by using the parameters in the following table.

Calling Line Identification Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	`voIpProt.SIP.CID.sourcePreference`	Uses the value of this parameter to display the caller's identity, if the priority order for incoming and outgoing calls are not configured. Null (default) Supported Headers Default Order: P-Asserted-Identity,Remote-Party-ID,From String By default, callee and caller display will be considered in the order given in `voIpProt.SIP.CID.sourcePreference`. If `voIpProt.SIP.callee.sourcePreference` or `voIpProt.SIP.caller.sourcePreference` are configured then callee order will be taken from `voIpProt.SIP.callee.sourcePreference` for outgoing calls and caller order will be taken from `voIpProt.SIP.caller.sourcePreference` for incoming calls.	No

Calling Line Identification Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	`voIpProt.SIP.caller.source Preference`	Set the priority order to display the caller's identity for incoming calls. Null (default) Supported Headers Default Order: P-Asserted-Identity,Remote-Party-ID,From String	No
features.cfg	`voIpProt.SIP.callee.source Preference`	Set the priority order to display the callee's identity for outgoing calls. Null (default) Supported Headers Default Order: P-Asserted-Identity,Remote-Party-ID,From String	No

SIP Header Warning Parameters

You can use the parameters in the following table to enable the warning display or specify which warnings to display.

SIP Header Warning Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.header.warning.enable	0 (default) - The warning header is not displayed. 1 - The warning header is displayed if received.	No
sip-interop.cfg	voIpProt.SIP.header.warning.codes.accept	Specify a list of accepted warning codes. Null (default) - 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	No

Access URL in SIP Messages Parameters

You can configure the retrieval method for web content and enable users to choose to retrieve web content using either Active or Passive mode. If your call server supports access URLs, you can also specify active or passive retrieval in the SIP header. If parameters in the SIP signal conflict with the file configuration, parameters in the SIP signaling take precedence.

You can also enable new web content to be added to the Settings menu on the phone, and users can set the default display mode for individual URLs to active or passive from the phone's menu.

Access URL in SIP Messages Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	mb.ssawc.enabled	0 (default) - Spontaneous display of web content is disabled. 1 - Spontaneous web content display is enabled.	No
features.cfg	mb.ssawc.call.mode	passive (default) - Web content is displayed only when requested by the user. Passive mode is recommended when the microbrowser is used for other applications. When passive mode is enabled, an icon displays beside a call appearance indicating that web content is available, and the user can press Select to view the content. Active - Web content is retrieved spontaneously and displayed immediately.	No

Distinctive Call Waiting Parameters

You can use the alert-info values and class fields in the SIP header to map calls to distinct call-waiting types. You can apply three call waiting types: beep, ring, and silent. The following table lists available parameters. This feature requires call server support.

Distinctive Call Waiting Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.alertInfo.x.class	Alert-Info fields from INVITE requests are compared 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 is applied. default (default)	No
sip-interop.cfg	voIpProt.SIP.alertInfo.x.value	Specify a ringtone for single registered line using a string to match the Alert-Info header in the incoming INVITE. NULL (default)	No

Presence Status Parameters

Use the parameters in the following table to enable the presence feature and display the **MyStatus** and **Buddies** soft keys on the phone.

Presence Status Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.presence.enabled	0 (default) - Disable the presence feature—including buddy managements and user status. 1 - Enable the presence feature with the buddy and status options.	No

Presence Status Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	pres.idleSoftkeys	1 (default) - The **MyStat** and **Buddies** presence idle soft keys display. 0 - The **MyStat** and **Buddies** presence idle soft keys do not display.	No
features.cfg	pres.reg	The valid line/registration number that is used for presence. This registration sends a SUBSCIRBE for presence. If the value is not a valid registration, this parameter is ignored. 1 (default) 1 - 34	No

Do Not Disturb Parameters

Use the parameters in the following table to configure the local DND feature.

Do Not Disturb Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.dnd`	0 (default) - Disable server-based DND. 1 - Server-based DND is enabled. Server and local phone DND are synchronized.	No
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.localProcessing.dnd`	This parameter depends on the value of `voIpProt.SIP.serverFeatureControl.dnd`. If set to 1 (default) and `voIpProt.SIP.serverFeatureControl.dnd` is set to 1, the phone and the server perform DND. If set to 0 and `voIpProt.SIP.serverFeatureControl.dnd` is set to 1, DND is performed on the server-side only, and the phone does not perform local DND. If both `voIpProt.SIP.serverFeatureControl.localProcessing.dnd` and `voIpProt.SIP.serverFeatureControl.dnd` are set to 0, the phone performs local DND and the `localProcessing` parameter is not used.	No

Do Not Disturb Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`call.rejectBusyOnDnd`	If 1 (default), and DND is turned on, the phone rejects incoming calls with a busy signal. If 0, and DND is turned on, the phone gives a visual alert of incoming calls and no audio ringtone alert. Note: This parameter does not apply to shared lines since not all users may want DND enabled.	No
`reg-advanced.cfg`	`call.donotdisturb.perReg`	This parameter determines if the do-not-disturb feature applies to all registrations on the phone or on a per-registration basis. 0 (default) - DND applies to all registrations on the phone. 1 - Users can activate DND on a per-registration basis. Note: If `voIpProt.SIP.serverFeatureControl.dnd` is set to 1 (enabled), this parameter is ignored.	No

Remote Party Disconnect Alert Tone Parameters

You can configure this feature by using the parameter in the following table.

Remote Party Disconnect Alert Tone Parameters

Template	Parameter	Permitted Values
`features.cfg`	`call.remoteDisconnect.toneType`	Choose an alert tone to play when the remote party disconnects call. Silent (Default) messageWaiting, instantMessage, remoteHoldNotification, localHoldNotification, positiveConfirm, negativeConfirm, welcome, misc1, misc2, misc3, misc4, misc5, misc6, misc7, custom1, custom2, custom3, custom4, custom5, custom6, custom7, custom8, custom9, custom10

Call Waiting Alert Parameters

Use the parameters in the following table to configure call waiting alerts.

Call Waiting Alert Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	call.callWaiting. enable	Enable or disable call waiting. 1 (default) - The phone alerts you to an incoming call while you are in an active call. If 1, and you end the active call during a second incoming call, you are alerted to the second incoming call. 0 - You are not alerted to incoming calls while in an active call and the incoming call is treated as if you did not answer it.	No
sip-interop.cfg	call.callWaiting. ring	Specifies the ringtone of incoming calls when another call is active. If no value is set, the default value is used. beep (default) ring silent	No

Missed Call Notification Parameters

Use the following table to configure options for missed call notifications.

Missed Call Notification Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`call.missedCallTracking.x.enabled`	1 (default) - Missed call tracking for a specific registration is enabled. If `call.missedCallTracking.x.enabled` is set to 0, then the missed call counter is not updated regardless of what `call.serverMissedCalls.x.enabled` is set to (and regardless of how the server is configured) and the missed call list does not display in the phone menu. If `call.missedCallTracking.x.enabled` is set to 1 and `call.serverMissedCalls.x.enabled` is set to 0, then the number of missed calls 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 missed calls depends on how the server is configured.	Yes
`reg-advanced.cfg`	`call.serverMissedCall.x.enabled`	0 (default) - All missed-call events increment the counter for a specific registration. 1 - Only missed-call events sent by the server will increment the counter. Note: This feature is supported only with the BroadSoft Synergy call server (previously known as Sylantro).	Yes

Last Call Return Parameters

The last call return string value that you enter for parameter `call.lastCallReturnString` depends on the call server you use. Consult with your call server provider for the last call return string.

Last Call Return Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.lastCallReturn.enabled`	0 (default) - Disable last call return feature. 1 - Enable last call return.	No
`sip-interop.cfg`	`call.lastCallReturnString`	Specify the string sent to the server when the user selects the last call return action. The string is usually a star code. *69 (default) string - maximum 32 characters	No

BroadSoft Server-Based Redial Parameters

See the following table for a list of available parameters you can configure for this feature.

BroadSoft Server-Based Redial Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	`feature.broadsoft.basicCallLogs.redial.enabled`	0 (default) - Disables the option to redial the last number. 1 - Enables the phone to redial the last number.	No

Call Hold Parameters

See the following table for a list of available parameters you can configure for this feature.

Call Hold Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.useRFC2543hold	0 (default) - SDP media direction parameters (such as a=sendonly) per RFC 3264 when initiating a call. 1 - the obsolete c=0.0.0.0 RFC2543 technique is used when initiating a call.	No
sip-interop.cfg	voIpProt.SIP.useSendonlyHold	1 (default) - The phone will send a reinvite with a stream mode parameter of "sendonly" when a call is put on hold. 0 - The phone will send a reinvite with a stream mode parameter 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).	No
sip-interop.cfg	call.hold.localReminder.enabled	0 (default) - Users are not reminded of calls that have been on hold for an extended period of time. 1 - Users are reminded of calls that have been on hold for an extended period of time.	Yes
sip-interop.cfg	call.hold.localReminder.period	Specify the time in seconds between subsequent hold reminders. 60 (default)	Yes
sip-interop.cfg	call.hold.localReminder.startDelay	Specify a time in seconds to wait before the initial hold reminder. 90 (default)	Yes
sip-interop.cfg	voIpProt.SIP.musicOnHold.uri	A URI that provides the media stream to play for the remote party on hold. This parameter is used if reg.x.musicOnHold.uri is Null. Null (default) SIP URI	No

Call Park and Retrieve Parameters

The configuration parameters for the call park and retrieve feature are located in two template files. You can enable the feature using the **features.cfg** template file or the `sip-interop.cfg` file.

Use the parameters in the following table to configure this feature.

Call Park and Retrieve Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.callPark.enabled`	0 (default) - Disables the call park and call retrieve features. 1 - Enables the call park and call retrieve features.	Yes
`sip-interop.cfg`	`call.parkedCallRetrieveMethod`	The method the phone uses to retrieve a BLF resource's call which has dialog state confirmed. legacy (default) – Indicates that the phone uses the method specified in `call.parkedCallRetrieveString`. `native` – Indicates that the phone uses a native protocol method (in this case SIP INVITE with the Replaces header).	No
`sip-interop.cfg, site.cfg`	`call.parkedCallRetrieveString`	The star code that initiates retrieval of a parked call. Null (default) Permitted values are star codes.	No

Call Transfer Parameters

Use the following table to specify call transfer behavior.

Call Transfer Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.allowTransferOnProceeding	1 (default) - Transfer during the proceeding state of a consultation call is enabled. 0 - Transfer during the proceeding state of a consultation call is enabled 2 - Phones will accept an INVITE with replaces for a dialog in early state. This is needed when using transfer on proceeding with a proxy call server such as openSIPS, reSIProcate or SipXecs.	No
features.cfg	call.defaultTransferType	Set the transfer type the phone uses when transferring a call. Generic Base Profile: Consultative (default) - Users can immediately transfer the call to another party. Skype Base Profile: Blind (default) - The call is placed on hold while a new call is placed to the other party.	No

Call Forwarding Parameters

Use the parameters in the following table to configure feature options for call forwarding. No parameters are needed to enable call forwarding on Skype for Business-enabled phones.

Call Forwarding Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.cf`	0 (default) - The server-based call forwarding is not enabled. 1 - The server-based call forwarding is enabled.	Yes
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.localProcessing.cf`	This parameter depends on the value of `voIpProt.SIP.serverFeatureControl.cf`. 1 (default) - If set to 1 and `voIpProt.SIP.serverFeatureControl.cf` is set to 1, the phone and the server perform call forwarding. 0 - If set to 0 and `voIpProt.SIP.serverFeatureControl.cf` is set to 1, call forwarding is performed on the server side only, and the phone does not perform local call forwarding. If both `voIpProt.SIP.serverFeatureControl.localProcessing.cf` and `voIpProt.SIP.serverFeatureControl.cf` are set to 0, the phone performs local call forwarding and the `localProcessing` parameter is not used.	No
`sip-interop.cfg`	`voIpProt.SIP.header.diversion.enable`	0 (default) - If set to 0, the diversion header is not displayed. 1 - If set to 1, the diversion header is displayed if received.	Yes
`sip-interop.cfg`	`voIpProt.SIP.header.diversion.list.useFirst`	1 (default) - If set to 1, the first diversion header is displayed. 0 - If set to 0, the last diversion header is displayed.	Yes

Call Forwarding Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	divert.x.contact	All automatic call diversion features uses this forward-to contact. All automatically forwarded calls are directed to this contact. The contact can be overridden by a busy contact, DND contact, or no-answer contact as specified by the `busy`, `dnd`, and `noAnswer` parameters that follow. Null (default) string - Contact address that includes 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)	Yes
site.cfg	divert.x.sharedDisabled	1 (default) - Disables call diversion features on shared lines. 0 - Enables call diversion features on shared lines.	Yes
site.cfg	divert.x.autoOnSpecificCaller	1 (default) - Enables the auto divert feature of the contact directory for calls on registration x. You can specify to divert individual calls or divert all calls. 0 - Disables the auto divert feature of the contact directory for registration x.	Yes
site.cfg	divert.busy.x.enabled	1 (default) - Diverts calls registration x is busy. 0 - Does not divert calls if the line is busy.	Yes
site.cfg	divert.busy.x.contact	Calls are sent to the busy contact's address if it is specified; otherwise calls are sent to the default contact specified by `divert.x.contact`. Null (default) string - contact address.	Yes
site.cfg	divert.dnd.x.enabled	0 (default) - Divert calls when DND is enabled on registration x. 1 - Does not divert calls when DND is enabled on registration x.	Yes
site.cfg	divert.dnd.x.contact	Calls are sent to the DND contact's address if it is specified; otherwise calls are sent to the default contact specified by `divert.x.contact`. Null (default) string - contact address.	Yes

Call Forwarding Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`divert.fwd.x.enabled`	1 (default) - Users can forward calls on the phone's Home screen and use universal call forwarding. 0 - Users cannot enable universal call forwarding (automatic forwarding for all calls on registration x).	Yes
`site.cfg`	`divert.noanswer.x.enabled`	1 (default) - Unanswered calls after the number of seconds specified by timeout are sent to the no-answer `contact`. 0 - Unanswered calls are diverted if they are not answered.	Yes
`site.cfg`	`divert.noanswer.x.contact`	Null (default) - The call is sent to the default contact specified by `divert.x.contact`. string - contact address	Yes
`site.cfg`	`divert.noanswer.x.timeout`	55 (default) - Number of seconds for timeout. positive integer	Yes
`reg-advanced.cfg`	`reg.x.fwd.busy.contact`	The forward-to contact for calls forwarded due to busy status. Null (default) - The contact specified by `divert.x.contact` is used. string - The contact specified by `divert.x.contact` is not used	No
`reg-advanced.cfg`	`reg.x.fwd.busy.status`	0 (default) - Incoming calls that receive a busy signal is not forwarded 1 - Busy calls are forwarded to the contact specified by `reg.x.fwd.busy.contact`.	No
`reg-advanced.cfg`	`reg.x.fwd.noanswer.contact`	Null (default) - The forward-to contact specified by `divert.x.contact` is used. string - The forward to contact used for calls forwarded due to no answer.	No
`reg-advanced.cfg`	`reg.x.fwd.noanswer.ringCount`	The number of seconds the phone should ring for before the call is forwarded because of no answer. The maximum value accepted by some call servers is 20. 0 - (default) 1 to 65535	No

Call Forwarding Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.fwd.noanswer.status`	0 (default) - The calls are not forwarded if there is no answer. 1 - The calls are forwarded to the contact specified by `reg.x.noanswer.contact` after ringing for the length of time specified by `reg.x.fwd.noanswer.ringCount`.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.cf`	This parameter overrides `voIpProt.SIP.serverFeatureControl.cf`. 0 (default) - The server-based call forwarding is disabled. 1 - server based call forwarding is enabled.	Yes
`site.cfg`	`divert.x.sharedDisabled`	1 (default) - Disables call diversion features on shared lines. 0 - Enables call diversion features on shared lines.	Yes
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.cf`	0 (default) - Disable server-based call forwarding. 1 - Enable server-based call forwarding. This parameter overrides `reg.x.serverFeatureControl.cf`.	Yes
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.localProcessing.cf`	1 (default) - Allows to use the value for `voIpProt.SIP.serverFeatureControl.cf`. 0 - Does not use the value for This parameter depends on the value of `voIpProt.SIP.serverFeatureControl.cf`.	No

Call Forwarding Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.serverFeatureControl.localProcessing.cf`	This parameter overrides `voIpProt.SIP.serverFeatureControl.localProcessing.cf`. 0 (default) - If `reg.x.serverFeatureControl.cf` is set to 1 the phone does not perform local Call Forward behavior. 1 - The phone performs local Call Forward behavior on all calls received.	No
`sip-interop.cfg`	`call.shared.disableDivert`	1 (default) - Enable the diversion feature for shared lines. 0 - Disable the diversion feature for shared lines. Note that this feature is disabled on most call servers.	Yes

Automatic Off-Hook Call Placement Parameters

As shown in the following table, you can specify an off-hook call contact, enable or disable the feature for each registration, and specify a protocol for the call.

If you are provisioning the VVX 500 series, 600 series, or 1500 phones, you can specify whether the automatic call uses the SIP (audio only) protocol or the H.323 (video) protocol.

Automatic Off-Hook Call Placement Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`call.autoOffHook.x.contact`	Enter a SIP URL contact address. The contact must be an ASCII-encoded string containing digits, either the user part of a SIP URL (for example, 6416), or a full SIP URL (for example, 6416@polycom.com). NULL (default)	No
`reg-advanced.cfg`	`call.autoOffHook.x.enabled`	0 (default) - No call is placed automatically when the phone goes off hook, and the other parameters are ignored. 1 - When the phone goes off hook, a call is automatically placed to the contact you specify in `call.autoOffHook.x.contact` and using the protocol you specify in `call.autoOffHook.x.protocol.` Only the VVX 500/501, 600/601, and 1500 phones use the `protocol` parameter. If no protocol is specified, the phone uses the protocol specified by `call.autoRouting.preferredProtocol`. If a line is configured for a single protocol, the configured protocol is used.	No
`reg-advanced.cfg`	`call.autoOffHook.x.protocol`	Specify the calling protocol. Only the VVX 500/501, 600/601, and 1500 business media phones use the `protocol` parameter. If no protocol is specified, the phone uses the protocol specified by `call.autoRouting.preferredProtocol`. If a line is configured for a single protocol, the configured protocol is used. NULL (default) SIP H323	No

Directed Call Pickup Parameters

You can enable directed call pickup in the **features.cfg** template file and the `sip-interop.cfg` file.

The parameters you use to configure this feature depends on your call server. To enable or disable this feature for Sylantro call servers, set the parameter `feature.directedCallPickup.enabled` to 1.

To configure this feature for all other call servers, use the following parameters:

- `call.directedCallPickupMethod`
- `call.directedCallPickupString`

Note that the pickup string can be different for different call servers, so check with your call server provider if you configure legacy mode for directed call pickup.

The following table lists the configuration parameters for the directed call pick-up feature.

Directed Call Pickup Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.directedCallPickup.enabled`	0 (default) - Disables the directed call pickup feature. 1 - Enables the directed call pickup feature.	Yes
`sip-interop.cfg`	`call.directedCallPickupMethod`	Specifies how the phone performs a directed call pick-up from a BLF contact. legacy (default) – Indicates that the phone uses the method specified in `call.directedCallPickupString`. `native` – Indicates that the phone uses a native protocol method (in this case SIP INVITE with the Replaces header.	No
`sip-interop.cfg, site.cfg`	`call.directedCallPickupString`	The star code to initiate a directed call pickup. *97 (default) Note: The default value supports the BroadWorks calls server only. You must change the value if your organization uses a different call server.	No
`sip-interop.cfg`	`voIpProt.SIP.strictReplacesHeader`	This parameter applies only to directed call pick-up attempts initiated against monitored BLF resources. 1 (default) – The phone requires call-id, to-tag, and from-tag to perform a directed call-pickup when `call.directedCallPickupMethod` is configured as native. 0 – Call pick-up requires a call id only.	No

Group Call Pickup Parameters

This feature requires support from a SIP server and setup of this feature depends on the SIP server. For example, while some SIP servers implement group call pick-up using a particular star-code sequence, others implement the feature using network signaling.

Use the parameter in the following table to enable this feature.

Group Call Pickup Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.groupCallPickup.enabled`	0 (default) - Disable SIP-B Group Call Pickup feature. 1 - Enable SIP-B Group Call Pickup feature.	Yes

Multiple Line Registrations Parameters

Each registration can be mapped to one or more line keys, however, a line key can be used for only one registration.

This feature is one of several features associated with Flexible Call Appearances. For the maximum number of call appearances you can set per phone, see Flexible Call Appearances.

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.authOptimizedInFailover`	0 (default) - The first new SIP request is sent to the server with the highest priority in the server list when failover occurs. 1 - The first new SIP request is sent to the server that sent the proxy authentication request when failover occurs.	No
`sip-interop.cfg`	`voIpProt.SIP.callinfo.precedence.overAlertinfo`	0 (default) - Give priority to call-info header with answer-after string over alert-info feature is disabled. 1 - Give priority to call-info header with answer-after string over alert-info feature is enabled.	No
`sip-interop.cfg`	`voIpProt.SIP.CID.sourcePreference`	Specify the priority order for the sources of caller ID information. The headers can be in any order. Null (default) - caller ID information comes from `P-Asserted-Identity`, `Remote-Party-ID`, and `From` in that order. ASCII string up to 120 characters long - The values `From,P-Asserted-Identity, Remote-Party-ID` and `P-Asserted-Identity,From, Remote-Party-ID` are also valid.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.compliance.RFC3261.validate.contentLanguage	1 (default) - Validation of the SIP header content language is enabled. 0 - Validation of the SIP header content language is disabled	No
sip-interop.cfg	voIpProt.SIP.compliance.RFC3261.validate.contentLength	1 (default) - Validation of the SIP header content length is enabled. 0 - Validation of the SIP header content length is disabled	No
sip-interop.cfg	voIpProt.SIP.compliance.RFC3261.validate.uriScheme	1 (default) - Validation of the SIP header URI scheme is enabled. 0 - Validation of the SIP header URI scheme is disabled	No
sip-interop.cfg	voIpProt.SIP.conference.parallelRefer	0(deafult) - A parallel REFER is not sent to the call server. 1 - A parallel REFER is not sent to the call server. Note: This parameter must be set for Siemens OpenScape Centralized Conferencing.	No
sip-interop.cfg	voIpProt.SIP.connectionReuse.useAlias	0 (default) - The alias parameter is not added to the via header 1 - The phone uses the connection reuse draft which introduces "alias".	No
sip-interop.cfg	voIpProt.SIP.csta	0 (default) - The uaCSTA (User Agent Computer Supported Telecommunications Applications) feature is disabled. 1 - The uaCSTA feature is enabled (If reg.x.csta is set, it will override this parameter).	No
sip-interop.cfg	voIpProt.SIP.dialog.strictXLineID	0 (default) - The phone will not look for x-line-id (call appearance index) in a SIP INVITE message. 1 - The phone will look for x-line-id (call appearance index) in a SIP INVITE message	No
sip-interop.cfg	voIpProt.SIP.dialog.usePvalue	0 (default) - Phone uses a pval field name in Dialog. 1 - Phone uses a pvalue field name in Dialog.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.dialog.useSDP`	0 (default) - A new dialog event package draft is used (no SDP in dialog body). 1 - Use this setting to send SDP in the dialog body for backwards compatibility	No
`sip-basic.cfg`	`voIpProt.SIP.enable`	A flag to determine if the SIP protocol is used for call routing, dial plan, DTMF, and URL dialing. 1 (default) - The SIP protocol is used. 0 - The SIP protocol is not used.	Yes
`sip-interop.cfg`	`voIpProt.SIP.failoverOn503Response`	A flag to determine whether or not to trigger a failover if the phone receives a 503 response. You must use a registration expiry of 66 seconds or greater for failover with a 503 response to work properly. This rule applies both to the phone configuration (`reg.x.server.y.expires` and `voIpProt.server.x.expires`) as well as the 200 OK register response from the server. 1 (default) 0	No
`sip-interop.cfg`	`voIpProt.SIP.header.warning.codes.accept`	Specify a list of accepted warning codes. Null (default) - All codes are accepted only codes between 300 and 399 are supported. comma separated list	No
`sip-interop.cfg`	`voIpProt.SIP.IM.autoAnswerDelay`	The time interval from receipt of the instant message invitation to automatically accepting the invitation. 10 (default) 0 to 40	No
`sip-interop.cfg`	`voIpProt.SIP.keepalive.sessionTimers`	0 (default) - The session timer is disabled. 1 - The session timer is enabled.	No
`sip-interop.cfg`	`voIpProt.SIP.lineSeize.retries`	Controls the number of times the phone will retry a notify when attempting to seize a line (BLA). 10 (default) 3 to 10	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.local.port	The local port for sending and receiving SIP signaling packets. 5060 - The value is used for the local port but is not advertised in the SIP signaling. 0 to 65535 - If set to 0,the 5060 value is used for the local port but is not advertised in the SIP signaling. For other values, that value is used for the local port and it is advertised in the SIP signaling	Yes
sip-interop.cfg	voIpProt.SIP.looseContact	0 (default) - The port parameter is added to the contact header in TLS case. 1 - The port parameter is not added to the contact header or SIP messages.	No
sip-interop.cfg	voIpProt.SIP.ms-forking	This parameter is applies when installing Microsoft Live Communications Server. 0 (default) - Support for MS-forking is disabled. 1 - Support for MS-forking is enabled. Note: If any endpoint registered to the same account has MS-forking disabled, all other endpoints default back to non-forking mode. Windows Messenger does not use MS-forking so be aware of this behavior if one of the endpoints is using Windows Messenger.	No
sip-interop.cfg	voIpProt.SIP.newCallOnUnRegister	1 (default) - The phone generate new Call-ID and From tag during re-registration. 0 - The phone does not generate new Call-ID and From tag during re-registration.	No
sip-basic.cfg	voIpProt.SIP.outboundProxy.address	The IP address or hostname of the SIP server to which the phone sends all requests. Null (default) IP address or hostname	No
sip-interop.cfg	voIpProt.SIP.outboundProxy.port	The port of the SIP server to which the phone sends all requests. 0 (default) 0 to 65535	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.outboundProxy.failOver.failBack.mode`	Duration (default) - The phone tries the primary server again after the time specified by `reg.x.outboundProxy.failOver.failBack.timeout` expires. newRequests - All new requests are forwarded first to the primary server regardless of the last used server. DNSTTL - The phone tries the primary server again after a timeout equal to the DNS TTL configured for the server that the phone is registered to. registration - The phone tries the primary server again when the registration renewal signaling begins.	No
`sip-interop.cfg`	`voIpProt.SIP.outboundProxy.failOver.failBack.timeout`	The time to wait (in seconds) before failback occurs (overrides `voIpProt.server.x.failOver.failBack.timeout`). 3600 (default) -If the fail back mode is set to Duration, the phone waits this long after connecting to the current working server before selecting the primary server again. 0, 60 to 65535 -If set to 0, the phone will not fail-back until a fail-over event occurs with the current server.	No
`sip-interop.cfg`	`voIpProt.SIP.outboundProxy.failOver.failRegistrationOn`	1 (default) - When set to 1, and the reRegisterOn parameter is enabled, the phone will silently invalidate an existing registration (if it exists), at the point of failing over. 0 - When set to 0, and the reRegisterOn parameter is enabled, existing registrations will remain active. This means that the phone will attempt failback without first attempting to register with the primary server to determine if it has recovered. Note: `voIpProt.SIP.outboundProxy.failOver.reRegisterOn` must be enabled.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.outboundProxy.failOver.onlySignalWithRegistered`	1 (default) - No signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. 0 - signaling will be accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred). This parameter overrides `voIpProt.server.x.failOver.onlySignalWithRegistered`. Note: `reRegisterOn` and `failRegistrationOn` parameters must be enabled	No
`sip-interop.cfg`	`voIpProt.SIP.outboundProxy.failOver.reRegisterOn`	This parameter overrides the `voIpProt.server.x.failOver.reRegisterOn`. 0 (default) - The phone won't attempt to register with the secondary server, since the phone will assume that the primary and secondary servers share registration information. 1 - The phone will attempt to register with the secondary server. If the registration succeeds signaling will proceed with the secondary server.	No
`sip-interop.cfg`	`voIpProt.SIP.outboundProxy.transport`	DNSnaptr (default) - 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. TCPpreferred - TCP is the preferred transport, UDP is used if TCP fails. UDPOnly - Only UDP will be used. TLS - If TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061. TCPOnly - Only TCP will be used.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.pingInterval	The number in seconds to send PING message. 0 (default) - This feature is disabled. 0 to 3600 - This feature is enabled.	No
sip-interop.cfg	voIpProt.SIP.pingMethod	The ping method to be used. PING (default) OPTIONS	No
sip-interop.cfg	voIpProt.SIP.presence.nortelShortMode	Different headers sent in SUBSCRIBE when used for presence on an 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. 0 (default) 1	Yes
sip-interop.cfg	voIpProt.SIP.requestValidation.digest.realm	Determines the string used for Realm. PolycomSPIP (default) string	Yes
sip-interop.cfg	voIpProt.SIP.requestValidation.x.method	Null (default) - no validation is made. 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.	Yes
sip-interop.cfg	voIpProt.SIP.requestValidation.x.request	Sets the name of the method for which validation will be applied. Null (default) INVITE, ACK, BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE Note: Intensive request validation may have a negative performance impact due to the additional signaling required in some cases.	Yes

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.requestValidation.x.request.y.event`	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`. Null (default) - all events will be validated. A valid string - specified event will be validated.	Yes
`sip-interop.cfg`	`voIpProt.SIP.requestURI.E164.addGlobalPrefix`	0 (default) - '+' global prefix is not added to the E.164 user parts in sip: URIs. 1 - '+' global prefix is added to the E.164 user parts in sip: URIs.	No
`sip-interop.cfg`	`voIpProt.SIP.sendCompactHdrs`	0 (default) - SIP header names generated by the phone use the long form, for example `From`. 1 - SIP header names generated by the phone use the short form, for example `f`.	No
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.missedCalls`	0 (default) - Server-based missed calls is not enabled. 1 - Server-based missed calls is enabled. The call server has control of missed calls.	Yes
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.securityClassification`	0 (default) - The visual security classification feature for all lines on a phone is disabled. 1 - The visual security classification feature for all lines on a phone is enabled.	No
`site.cfg`	`voIpProt.SIP.specialEvent.checkSync.alwaysReboot`	0 (default) - The phone will only reboot if necessary. Many configuration parameter changes can be applied dynamically without the need for a reboot. 1 - The phone always reboot when a NOTIFY message is received from the server with event equal to check-sync even if there has not been a change to software or configuration.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`voIpProt.SIP.specialEvent.checkSync.downloadCallList`	0 (default) - The phone does not download the call list for the logged-in user when a check sync event's NOTIFY message is received from the server. 1 - The phone downloads the call list for the logged-in user when a check sync event's NOTIFY message is received from the server.	No
`sip-interop.cfg`	`voIpProt.SIP.strictLineSeize`	0 (default) - Dial prompt is provided immediately when you attempt to seize a shared line without waiting for a successful OK from the call server. 1 - The phone is forced to wait for a 200 OK response when receiving a TRYING notify.	No
`sip-interop.cfg`	`voIpProt.SIP.strictUserValidation`	0 (default) - The phone is forced to match the user portion of signaling exactly. 1 - The phone will use the first registration if the user part does not match any registration.	No
`sip-interop.cfg`	`voIpProt.SIP.supportFor100rel`	1 (default) - The phone advertises support for reliable provisional responses in its offers and responses. 0 - The phone will not offer 100rel and will reject offers requiring 100rel.	No
`sip-interop.cfg`	`voIpProt.SIP.tcpFastFailover`	0 (default) - A full 32 second RFC compliant timeout is used. 1 - A failover occurs based on the values of `reg.x.server.y.retryMaxCount` and `voIpProt.server.x.retryTimeOut`.	No
`sip-interop.cfg`	`voIpProt.SIP.tlsDsk.enable`	0 (default) - TLS DSK is disabled. 1 - TLS DSK is enabled.	No
`sip-interop.cfg`	`voIpProt.SIP.turnOffNonSecureTransport`	0 (default) - Stop listening to port 5060 when using AS-SIP feature is disabled. 1 - Stop listening to port 5060 when using AS-SIP feature is enabled.	Yes
`sip-interop.cfg`	`voIpProt.SIP.use486forReject`	0 (default) - The phone will not transmit 486 response. 1 - The phone will not transmit 486 response.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.useContactInReferTo`	0 (default) - The "To URI" is used in the REFER. 1 - The "Contact URI" is used in the REFER.	No
`sip-interop.cfg`	`voIpProt.SIP.useRFC2543hold`	0 (default) - SDP media direction parameters (such as a=sendonly) per RFC 3264 when initiating a call. 1 - the obsolete c=0.0.0.0 RFC2543 technique is used when initiating a call.	No
`sip-interop.cfg`	`voIpProt.SIP.useRFC3264HoldOnly`	0 (default) - When set to 0, and no media direction is specified, the phone enters backward compatibility mode when negotiating SDP and responds using the c=0.0.0.0 RFC 2543 signaling method. 1 - When set to 1, and no media direction is specified, the phone uses `sendrecv` compliant with RFC 3264 when negotiating SDP and generates responses containing RFC 3264-compliant media attributes for calls placed on and off hold by either end. Note: `voIpProt.SIP.useSendonlyHold` applies only to calls on phones that originate the hold.	No
`sip-interop.cfg`	`voIpProt.SIP.callinfo.precedence.overAlertinfo`	0 (default) - The alert-info is given priority over call-info header. 1 - The call-info header with answer-after string is given priority over alert-info header.	No
`sip-interop.cfg`	`voIpProt.SIP.renewSubscribeOnTLSRefresh`	1 (default) – For an as-feature-event, the SUBSCRIBE message is sent along with the RE-REGISTER when Transport Layer Security (TLS) breaks. 0 – The SUBSCRIBE and RE-REGISTER messages is sent at different times.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.alertInfo.x.class`	Alert-Info fields from INVITE requests are compared 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 is applied. default (default) See the list of ring classes in Ringtone Parameters.	No
`sip-interop.cfg`	`voIpProt.SIP.alertInfo.x.value`	Specify a ringtone for single registered line using a string to match the Alert-Info header in the incoming INVITE. NULL (default)	No
`site.cfg`	`voIpProt.SIP.specialEvent.checkSync.downloadCallList`	0 (default) - The phone does not download the call list for the user after receiving a checksync event in the NOTIFY. 1 - The phone downloads the call list for the user after receiving a checksync event in the NOTIFY.	No
`site.cfg`	`voIpProt.SIP.specialEvent.checkSync.downloadDirectory`	0 (default) - The phone downloads updated directory files after receiving a checksync NOTIFY message. 1 - The phone downloads the updated directory files along with any software and configuration updates after receiving a checksync NOTIFY message. The files are downloaded when the phone restarts, reboots, or when the phone downloads any software or configuration updates. Note: The parameter `hotelingMode.type` set to `2` or `3` overrides this parameter.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.CID.request.sourceSipMessage`	Specify which header in the SIP request to retrieve remote party caller ID from. You can use: • `voIpProt.SIP.callee.sourcePreference` • `voIpProt.SIP.caller.sourcePreference` • `voIpProt.SIP.CID.sourcePreference` UPDATE takes precedence over the value of this parameter. NULL (default) - Remote party caller ID information from INVITE is used. INVITE PRACK ACK This parameter does not apply to shared lines.	No
`sip-interop.cfg`	`voIpProt.SIP.CID.response.sourceSipMessage`	Specify which header in the SIP request to retrieve remote party caller ID from. You can use: • `voIpProt.SIP.callee.sourcePreference` • `voIpProt.SIP.caller.sourcePreference` • `voIpProt.SIP.CID.sourcePreference` NULL (default) - The remote party caller ID information from the last SIP response is used. 100, 180, 183, 200 This parameter does not apply to shared lines.	No
`features.cfg`	`voIpProt.SIP.Caller.SourcePreference`	Set priority order to display the caller's identity for incoming calls. Null (default) Supported Headers Default Order: P-Asserted-Identity,Remote-Party-ID,From String	`features.cfg`

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`voIpProt.SIP.Callee.SourcePreference`	Set priority order to display the callee's identity for outgoing calls. Null (default) Supported Headers Default Order: P-Asserted-Identity,Remote-Party-ID,From String	`features.cfg`
`sip-interop.cfg`	`voIpProt.SIP.header.warning.enable`	0 (default) - The warning header is not displayed. 1 - The warning header is displayed if received.	No
`sip-interop.cfg`	`voIpProt.SIP.header.warning.codes.accept`	Specify a list of accepted warning codes. Null (default) - 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`	No
`sip-interop.cfg`	`voIpProt.SIP.alertInfo.x.class`	Alert-Info fields from INVITE requests are compared 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 is applied. default (default)	No
`sip-interop.cfg`	`voIpProt.SIP.alertInfo.x.value`	Specify a ringtone for single registered line using a string to match the Alert-Info header in the incoming INVITE. NULL (default)	No
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.dnd`	0 (default) - Disable server-based DND. 1 - Server-based DND is enabled. Server and local phone DND are synchronized.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.localProcessing.dnd`	This parameter depends on the value of `voIpProt.SIP.serverFeatureControl.dnd`. If set to 1 (default) and `voIpProt.SIP.serverFeatureControl.dnd` is set to 1, the phone and the server perform DND. If set to 0 and `voIpProt.SIP.serverFeatureControl.dnd` is set to 1, DND is performed on the server-side only, and the phone does not perform local DND. If both `voIpProt.SIP.serverFeatureControl.localProcessing.dnd` and `voIpProt.SIP.serverFeatureControl.dnd` are set to 0, the phone performs local DND and the `localProcessing` parameter is not used.	No
`sip-interop.cfg`	`voIpProt.SIP.useRFC2543hold`	0 (default) - SDP media direction parameters (such as a=sendonly) per RFC 3264 when initiating a call. 1 - the obsolete c=0.0.0.0 RFC2543 technique is used when initiating a call.	No
`sip-interop.cfg`	`voIpProt.SIP.useSendonlyHold`	1 (default) - The phone will send a reinvite with a stream mode parameter of "sendonly" when a call is put on hold. 0 - The phone will send a reinvite with a stream mode parameter 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).	No
`sip-interop.cfg`	`voIpProt.SIP.musicOnHold.uri`	A URI that provides the media stream to play for the remote party on hold. This parameter is used if `reg.x.musicOnHold.uri` is Null. Null (default) SIP URI	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.allowTransferOnProceeding`	1 (default) - Transfer during the proceeding state of a consultation call is enabled. 0 - Transfer during the proceeding state of a consultation call is enabled 2 - Phones will accept an INVITE with replaces for a dialog in early state. This is needed when using transfer on proceeding with a proxying call server such as openSIPS, reSIProcate or SipXecs.	No
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.cf`	0 (default) - The server-based call forwarding is not enabled. 1 - The server-based call forwarding is enabled.	Yes
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.localProcessing.cf`	This parameter depends on the value of `voIpProt.SIP.serverFeatureControl.cf`. 1 (default) - If set to 1 and `voIpProt.SIP.serverFeatureControl.cf` is set to 1, the phone and the server perform call forwarding. 0 - If set to 0 and `voIpProt.SIP.serverFeatureControl.cf` is set to 1, call forwarding is performed on the server side only, and the phone does not perform local call forwarding. If both `voIpProt.SIP.serverFeatureControl.localProcessing.cf` and `voIpProt.SIP.serverFeatureControl.cf` are set to 0, the phone performs local call forwarding and the `localProcessing` parameter is not used.	No
`sip-interop.cfg`	`voIpProt.SIP.header.diversion.enable`	0 (default) - If set to 0, the diversion header is not displayed. 1 - If set to 1, the diversion header is displayed if received.	Yes
`sip-interop.cfg`	`voIpProt.SIP.header.diversion.list.useFirst`	1 (default) - If set to 1, the first diversion header is displayed. 0 - If set to 0, the last diversion header is displayed.	Yes

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.serverFeatureControl.cf	0 (default) - Disable server-based call forwarding. 1 - Enable server-based call forwarding. This parameter overrides `reg.x.serverFeatureControl.cf`.	Yes
sip-interop.cfg	voIpProt.SIP.serverFeatureControl.localProcessing.cf	1 (default) - Allows to use the value for `voIpProt.SIP.serverFeatureControl.cf`. 0 - Does not use the value for This parameter depends on the value of `voIpProt.SIP.serverFeatureControl.cf`..	No
sip-interop.cfg	voIpProt.SIP.strictReplacesHeader	This parameter applies only to directed call pick-up attempts initiated against monitored BLF resources. 1 (default) – The phone requires call-id, to-tag, and from-tag to perform a directed call-pickup when `call.directedCallPickupMethod` is configured as native. 0 – Call pick-up requires a call id only.	No
sip-interop.cfg	voIpProt.SIP.serverFeatureControl.callRecording	0 (default) - The BroadSoft BroadWorks v20 call recording feature for multiple phones is disabled. 1 - The BroadSoft BroadWorks v20 call recording feature for multiple phones is enabled.	No
sip-interop.cfg	voIpProt.SIP.strictReplacesHeader	This parameter applies only to directed call pick-up attempts initiated against monitored BLF resources. 1 (default) – The phone requires call-id, to-tag, and from-tag to perform a directed call-pickup when `call.directedCallPickupMethod` is configured as native. 0 – Call pick-up requires a call id only.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.useLocalTargetUriforLegacyPickup	1 (default) – The target URI in BLF signaling uses the complete address as provided in the XML dialog document. 0 – Only the user portion of the target URI in the XML dialog document is used and the current registrar's domain is appended to create the address for pickup or retrieval.	No
sip-interop.cfg	voIpProt.SIP.conference.address	Null (default) - Conferences are set up on the phone locally. String 128 max characters - Enter a conference address. Conferences are set up by the server using the conferencing agent specified by this address. Acceptable values depend on the conferencing server implementation policy.	No
sip-interop.cfg	voIpProt.SIP.specialEvent.lineSeize.nonStandard	Controls the response for a line-seize event SUBSCRIBE. 1 (default) - This speeds up the processing of the response for line-seize event. 0 - This will process the response for the line seize event normally	Yes
sip-interop.cfg	voIpProt.SIP.intercom.alertInfo	The string you want to use in the Alert-Info header. You can use the following characters: '@', '-' ,'_' , '.' . If you use any other characters, NULL, or empty spaces, the call is sent as normal without the Alert-Info header. Intercom (default) Alpha - Numeric string	No
sip-interop.cfg	voIpProt.SIP.alertInfo.x.value	Specify a ringtone for single registered line using a string to match the Alert-Info header in the incoming INVITE. NULL (default)	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.alertInfo.x.class`	Alert-Info fields from INVITE requests are compared 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 is applied. default (default) See the list of ring classes in Ringtone Parameters.	No
`sip-interop.cfg`	`voIpProt.SIP.acd.signalingMethod`	0 (default) - The 'SIP-B' signaling is supported. (This is the older ACD functionality.) 1 - The feature synchronization signaling is supported. (This is the new ACD functionality.)	Yes
`sip-interop.cfg`	`voIpProt.SIP.acd.signalingMethod`	0 (default) - The 'SIP-B' signaling is supported. (This is the older ACD functionality.) 1 - The feature synchronization signaling is supported. (This is the new ACD functionality.)	Yes
`sip-interop.cfg`	`voIpProt.SIP.header.pEarlyMedia.support`	0 (Default) - The p-early-media header is not supported by the caller phone. 1 - The p-early-media header is supported by the caller phone.	
`sip-interop.cfg`	`voIpProt.SIP.IMS.enable`	This parameter applies to all registered or unregistered SIP lines on the phone. 0 (Default) - The phone does not support IMS features introduced in UC Software 5.5.0. 1 - The phone supports IMS features introduced in UC Software 5.5.0.	
`features.cfg`	`voIpProt.SIP.regevent`	0 (default) - The phone is not subscribed to registration state change notifications for all phone lines. 1 - The phone is subscribed to registration state change notifications for all phone lines. This parameter is overridden by the per-phone parameter `reg.x.regevent`.	

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.rejectNDUBInvite	Specify whether or not the phone accepts a call for all registrations in case of a Network Determined User Busy (NDUB) event advertised by the SIP server. 0 (Default) - If an NDUB event occurs, the phone does not reject the call for all line registrations. 1 - If an NDUB event occurs, the phone rejects the call with a 603 Decline response code for all line registrations.	
reg-basic.cfg	voIpProt.SIP.supportFor199	Determine support for the 199 response code. For details on the 199 response code, see RFC 6228. 0 (Default) - The phone does not support the 199 response code. 1- The phone supports the 199 response code.	
sip-interop.cfg	voipProt.SIP.anat.enabled	Enables or disables Alternative Network Address Types (ANAT). 0 (default) - ANAT is disabled. 1 - ANAT is enabled.	No
sip-interop.cfg	voIpProt.SIP.requestValidation.x.method	Null (default) - no validation is made. 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.	Yes
sip-interop.cfg	voIpProt.SIP.requestValidation.x.request	Sets the name of the method for which validation will be applied. Null (default) INVITE, ACK , BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE Note: Intensive request validation may have a negative performance impact due to the additional signaling required in some cases.	Yes

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.requestValidation.x.request.y.event`	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`. Null (default) - all events will be validated. A valid string - specified event will be validated.	Yes
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.securityClassification`	0 (default) - The visual security classification feature for all lines on a phone is disabled. 1 - The visual security classification feature for all lines on a phone is enabled.	Yes
`sip-interop.cfg`	`voIpProt.SIP.dtmfViaSignaling.rfc2976`	Enable or disable DTMF relays for active SIP calls. Not supported for H.323 calls. 0 (default) - DTMF digit information is not sent 1 - DTMF digit information is sent in RFC2976 SIP INFO packets during a call.	Yes
`sip-interop.cfg`	`voIpProt.SIP.dtmfViaSignaling.rfc2976.nonLegacyEncoding`	Controls the behavior of the Star and Pound keys used for DTMF relays for active SIP calls. Not supported for H.323 calls. 0 (default) - The phone sends 10 when the Star key (*) is pressed and 11 when the Pound key (#) is pressed. 1 - The phone sends an asterisk (*) when the Star key is pressed and a hashtag (#) when the Pound key is pressed.	Yes

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.server.x.failOver.failBack.mode`	Specify the failover failback mode. duration (default) - The phone tries the primary server again after the time specified by `voIpProt.server.x.failOver.failBack.timeout` newRequests - All new requests are forwarded first to the primary server regardless of the last used server. DNSTTL - The phone tries the primary server again after a timeout equal to the DNS TTL configured for the server that the phone is registered to. registration - The phone tries the primary server again when the registration renewal signaling begins.	No
`sip-interop.cfg`	`voIpProt.server.x.failOver.failBack.timeout`	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 result in a timeout of 60 and 0 means do not fail-back until a fail-over event occurs with the current server. 3600 (default) 0, 60 to 65535	No
`sip-interop.cfg`	`voIpProt.server.x.failOver.failRegistrationOn`	1 (default) - When set to 1, and the reRegisterOn parameter is enabled, the phone silently invalidates an existing registration (if it exists), at the point of failing over. 0 - When set to 0, and the reRegisterOn parameter is enabled, existing registrations remain active. This means that the phone attempts failback without first attempting to register with the primary server to determine if it has recovered.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.server.x.failOver.onlySignalWithRegistered	1 (default) - When set to 1, and the reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. If the phone attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call ends. No SIP messages are sent to the unregistered server. 0 - When set to 0, and the reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred).	No
sip-interop.cfg	voIpProt.server.x.failOver.reRegisterOn	0 (default) - When set to 0, the phone won't attempt to register with the second. 1 - When set to 1, the phone attempts to register with (or by, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling proceeds with the secondary server.	No
sip-interop.cfg	voIpProt.server.x.subscribe.expires	The phone's requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period. 3600 - (default) 10 – 2147483647	No
sip-interop.cfg	voIpProt.server.x.subscribe.expires.overlap	The number of seconds before the expiration time returned by server x after which the phone attempts to resubscribe. If the server value is less than the configured overlap value, the phone tries to resubscribe at half the expiration time returned by the server. 60 - (default) 5 – 65535 seconds	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.server.y.subscribe.expires`	The phone's requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period. 3600 seconds - (default) 10 – 2147483647 (seconds) You can use this parameter in conjunction with `reg.x.server.y.subscribe.expires.overlap`.	No
`reg-advanced.cfg`	`reg.x.server.y.subscribe.expires.overlap`	The number of seconds before the expiration time returned by server x after which the phone attempts to resubscribe. If the server value is less than the configured overlap value, the phone tries to resubscribe at half the expiration time returned by the server. 60 seconds (default) 5 – 65535 seconds	No
`sip-interop.cfg`	`voIpProt.server.x.specialInterop`	Enables server-specific features for all registrations. Standard (default) VVX 101 = Standard, GENBAND, GENBAND-A2, ALU-CTS, DT VVX 201 = Standard, GENBAND, GENBAND-A2, ALU-CTS, ocs2007r2, lync2010 All other phones = Standard, GENBAND, GENBAND-A2, ALU-CTS, DT, ocs2007r2, lync2010, lcs2005	No
`sip-basic.cfg`	`voipProt.server.x.address`	The IP address or hostname and port of a SIP server that accepts registrations. Multiple servers can be listed starting with x=1 to 4 for fault tolerance. Null (default), IP address, or hostname	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.server.x.expires`	The phone's requested registration period in seconds. 3600 (default) positive integer, minimum 10 The period negotiated with the server may be different. The phone attempts to re-register at the beginning of the overlap period. For example, if expires="300" and overlap="5", the phone re-registers after 295 seconds (300-5).	No
`sip-interop.cfg`	`voIpProt.server.x.expires.lineSeize`	Requested line-seize subscription period. 30 (default) positive integer, minimum 10	No
`sip-interop.cfg`	`voIpProt.server.x.expires.overlap`	The number of seconds before the expiration time returned by server x at which the phone should try to re-register. If the server value is less than the configured overlap value, the phone tries to re-register at half the expiration time returned by the server. 60 (default) 5 to 65536	No
`sip-basic.cfg`	`voIpProt.server.x.port`	The port of the server that specifies registrations. 0 (default) - If 0, the port used depends on `voIpProt.server.x.transport`. 1 to 65535	No
	`voIpProt.server.x.protocol.SIP`	1 (default) - Server is a SIP proxy/registrar 0 - If set to 0, and the server is confirmed to be a SIP server, then the value is assumed to be 1.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.server.x.registerRetry.baseTimeOut`	`reg.x.server.y.registerRetry.baseTimeOut` takes precedence.The base time period to wait before a registration retry. Used in conjunction with `voIpProt.server.x.registerRetry.maxTimeOut` to determine how long to wait. The algorithm is defined in RFC 5626. If both parameters `voIpProt.server.x.registerRetry.baseTimeOut` and `reg.x.server.y.registerRetry.baseTimeOut` are set, the value of 60 - (default) 10 - 120	No
`sip-interop.cfg`	`voIpProt.server.x.registerRetry.maxTimeOut`	The maximum time period to wait before a registration retry. Used in conjunction with `voIpProt.server.x.registerRetry.maxTimeOut` to determine how long to wait. The algorithm is defined in RFC 5626. If both parameters `voIpProt.server.x.registerRetry.maxTimeOut` and `reg.x.server.y.registerRetry.maxTimeOut` are set, the value of `reg.x.server.y.registerRetry.maxTimeOut` takes precedence. 60 - (default) 10 - 1800	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.server.x.transport`	The transport method the phone uses to communicate with the SIP server. Null or DNSnaptr (default) - 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. TCPpreferred - TCP is the preferred transport; UDP is used if TCP fails. UDPOnly - Only UDP will be used. TLS - If TLS fails, transport fails. Leave port field empty (will default to 5061) or set to 5061. TCPOnly - Only TCP will be used.	No
`sip-interop.cfg`	`voIpProt.server.x.expires`	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. 3600 (default) positive integer, minimum 10	No
`sip-interop.cfg`	`voIpProt.server.x.expires.overlap`	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 the server value is less than the configured overlap value. 60 (default) 5 to 65535	No
`sip-interop.cfg`	`voIpProt.server.x.expires.lineSeize`	Requested line-seize subscription period. 30 (default) positive integer, minimum 0 was 10	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.server.x.register`	1 (default) - Calls can not be routed to an outbound proxy without registration. 0 - Calls can be routed to an outbound proxy without registration. For more information, see *Technical Bulletin 5844: SIP Server Fallback Enhancements on Polycom Phones*.	No
`sip-interop.cfg`	`voIpProt.server.x.retryTimeOut`	0 (default) - Use standard RFC 3261 signaling retry behavior. 0 to 65535 - The amount of time (in milliseconds) to wait between retries.	No
`sip-interop.cfg`	`voIpProt.server.x.retryMaxCount`	The number of retries that will be attempted before moving to the next available server. 3 (default) 0 to 20 - If set to 0, 3 is used.	No
`sip-interop.cfg`	`voIpProt.server.x.useOutboundProxy`	1 (default) - Enables to use the outbound proxy specified in `voIpProt.SIP.outboundProxy.address` for server x. 0 - Enables not to use the outbound proxy specified in `voIpProt.SIP.outboundProxy.address` for server x.	No
`reg-advanced.cfg`	`reg.x.ringType`	The ringer to be used for calls received by this registration. The default is the first non-silent ringer. If you use the configuration parameters ringer13 and ringer14 on a single registered line, the phone plays SystemRing.wav. default (default) ringer1 to ringer24	No
`sip-interop.cfg`	`reg.x.protocol.H323`	You can use this parameter for the VVX 500/501, 600/601, and 1500. 0 (default) - H.323 signaling is not enabled for registration x. 1 - H.323 signaling is enabled for registration x.	No
`site.cfg`	`reg.x.server.H323.y.address`	Address of the H.323 gatekeeper. Null (default) IP address or hostname	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.server.H323.y.port`	Port to be used for H.323 signaling. If set to Null, 1719 (H.323 RAS signaling) is used. 0 (default) 0 to 65535	No
`site.cfg`	`reg.x.server.H323.y.expires`	Desired registration period. 3600 positive integer	No
`site.cfg`	`reg.x.line.y.label`	Configure a unique line label for a shared line that has multiple line key appearances. This parameter takes effect when `up.cfgUniqueLineLabel=1`. If `reg.x.linekeys=1`, this parameter does not have any effect. x = the registration index number starting from 1. y = the line index from 1 to the value set by `reg.x.linekeys`. Specifying a string sets the label used for the line key registration on phones with multiple line keys. If no parameter value is set for `reg.x.line.y.label`, the phone automatically numbers multiple lines by prepending "<y>_" where <y> is the line index from 1 to the value set by `reg.x.linekeys`. • The following examples show labels for line 1 on a phone with user registration 1234, where `reg.x.linekeys=2`: ⌃ If no label is configured for registration, the labels are "1_1234" and "2_1234". ⌃ If `reg.1.line.1.label=Polycom` and `reg.1.line.2.label=VVX`, the labels display as 'Polycom' and 'VVX'.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	reg.x.fwd.busy.contact	The forward-to contact for calls forwarded due to busy status. Null (default) - The contact specified by divert.x.contact is used. string - The contact specified by divert.x.contact is not used	No
reg-advanced.cfg	reg.x.fwd.busy.status	0 (default) - Incoming calls that receive a busy signal is not forwarded 1 - Busy calls are forwarded to the contact specified by reg.x.fwd.busy.contact.	No
reg-advanced.cfg	reg.x.fwd.noanswer.contact	Null (default) - The forward-to contact specified by divert.x.contact is used. string - The forward to contact used for calls forwarded due to no answer.	No
reg-advanced.cfg	reg.x.fwd.noanswer.ringCount	The number of seconds the phone should ring for before the call is forwarded because of no answer. The maximum value accepted by some call servers is 20. 0 - (default) 1 to 65535	No
reg-advanced.cfg	reg.x.fwd.noanswer.status	0 (default) - The calls are not forwarded if there is no answer. 1 - The calls are forwarded to the contact specified by reg.x.noanswer.contact after ringing for the length of time specified by reg.x.fwd.noanswer.ringCount.	No
reg-advanced.cfg	reg.x.serverFeatureControl.cf	This parameter overrides voIpProt.SIP.serverFeatureControl.cf. 0 (default) - The server-based call forwarding is disabled. 1 - server based call forwarding is enabled.	Yes

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.serverFeatureControl.localProcessing.cf`	This parameter overrides `voIpProt.SIP.serverFeatureControl.localProcessing.cf`. 0 (default) - If `reg.x.serverFeatureControl.cf` is set to 1 the phone does not perform local Call Forward behavior. 1 - The phone performs local Call Forward behavior on all calls received.	No
`reg-advanced.cfg`	`reg.x.lineKeys`	Specify the number of line keys to use for a single registration. The maximum number of line keys you can use per registration depends on your phone model. 1 (default) 1 to max	No
`reg-advanced.cfg`	`reg.x.type`	private (default) - Use standard call signaling. shared - Use augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.	No
`reg-advanced.cfg`	`reg.x.thirdPartyName`	Null (default) - In all other cases. string address -This field must match the `reg.x.address` value of the registration which makes up the part of a bridged line appearance (BLA).	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.callRecording`	1 (default) - BroadSoft BroadWorks v20 call recording feature for individual phone lines is enabled. 0 - BroadSoft BroadWorks v20 call recording feature for individual phone lines is disabled.	No
`reg-basic.cfg`	`reg.x.address`	The user part (for example, 1002) or the user and the host part (for example, `1002@polycom.com`) of the registration SIP URI or the H.323 ID/extension. Null (default) string address	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.type`	private (default) - Use standard call signaling. shared - Use augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.	No
`sip-interop.cfg`	`reg.x.protocol.H323`	You can use this parameter for the VVX 500/501, 600/601, and 1500. 0 (default) - H.323 signaling is not enabled for registration x. 1 - H.323 signaling is enabled for registration x.	No
`site.cfg`	`reg.x.server.H323.y.address`	Address of the H.323 gatekeeper. Null (default) IP address or hostname	No
`site.cfg`	`reg.x.server.H323.y.port`	Port to be used for H.323 signaling. If set to Null, 1719 (H.323 RAS signaling) is used. 0 (default) 0 to 65535	No
`site.cfg`	`reg.x.server.H323.y.expires`	Desired registration period. 3600 positive integer	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot

`site.cfg`	`reg.x.line.y.label`	Configure a unique line label for a shared line that has multiple line key appearances. This parameter takes effect when `up.cfgUniqueLineLabel=1`. If `reg.x.linekeys=1`, this parameter does not have any effect.
		
		x = the registration index number starting from 1.
		
		y = the line index from 1 to the value set by `reg.x.linekeys`. Specifying a string sets the label used for the line key registration on phones with multiple line keys.
		
		If no parameter value is set for `reg.x.line.y.label`, the phone automatically numbers multiple lines by prepending "<y>_" where <y> is the line index from 1 to the value set by `reg.x.linekeys`.
		
		• The following examples show labels for line 1 on a phone with user registration 1234, where `reg.x.linekeys=2`:
		  ⌃ If no label is configured for registration, the labels are "1_1234" and "2_1234".
		  ⌃ If `reg.1.line.1.label=Polycom` and `reg.1.line.2.label=VVX`, the labels display as 'Polycom' and 'VVX'.
			No

`reg-advanced.cfg`	`reg.x.callsPerLineKey`	Set the maximum number of concurrent calls for a single registration x. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all phones sharing that registration. This per-registration parameter overrides `call.callsPerLineKey`. 24 (default) 1-24 VVX 101, 201 8 (default) 1 - 8	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.header.pearlymedia.support`	0 (Default) - The p-early-media header is not supported on the specified line registration. 1 - The p-early-media header is supported by the specified line registration.	No
`reg-basic.cfg`	`reg.X.insertOBPAddressInRoute`	1 (Default) - The outbound proxy address is added as the topmost route header. 0 - The outbound proxy address is not added to the route header.	No
`features.cfg`	`reg.x.path`	0 (Default) - The path extension header field in the Register request message is not supported for the specific line registration. 1 - The phone supports and provides the path extension header field in the Register request message for the specific line registration.	No
`features.cfg`	`reg.x.regevent`	0 (default) - The phone is not subscribed to registration state change notifications for the specific phone line. 1 - The phone is subscribed to registration state change notifications for the specific phone line. This parameter overrides the global parameter `voIpProt.SIP.regevent`.	No
`reg-advanced.cfg`	`reg.x.rejectNDUBInvite`	Specify whether or not the phone accepts a call for a particular registration in case of a Network Determined User Busy (NDUB) event advertised by the SIP server. 0 (Default) - If an NDUB event occurs, the phone does not reject the call. 1 - If an NDUB event occurs, the phone rejects the call with a 603 Decline response code.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.server.y.specialInterop`	Specify the server-specific feature set for the line registration. Standard (Default) VVX 101: Standard GENBAND ALU-CTS DT VVX 201: Standard, GENBAND ALU-CTS ocs2007r2 lync2010 All other phones: Standard GENBAND ALU-CTS ocs2007r2 lync2010 lcs2005	
`sip-interop.cfg`	`reg.x.gruu`	1 - The phone sends sip.instance in the REGISTER request. 0 (default) - The phone does not send sip.instance in the REGISTER request.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.securityClassification`	0 (default) - The visual security classification feature for a specific phone line is disabled. 1 - The visual security classification feature for a specific phone line is enabled.	No
`reg-advanced.cfg`	`reg.x.terminationType`	Determines the type of termination that is used for the line where the line can be managed automatically on the VVX, the wireless handset, or on both. X = each registration index. NULL (default) VVX, DECT, or VVX-DECT	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg` `reg-advanced.cfg`	`reg.x.acd-login-logout` `reg.x.acd-agent-available`	0 (default) - The ACD feature is disabled for registration. 1 - If both ACD login/logout and agent available are set to 1 for registration x, the ACD feature is enabled for that registration.	No
`reg-advanced.cfg`	`reg.x.advancedConference.maxParticipants`	Sets the maximum number of participants allowed in a push to conference for advanced conference calls. The number of participants configured must match the number of participants allowed on the ALU CTS. 3 (default) 0 - 25	No
`reg-advanced.cfg`	`reg.x.advancedConference.pushToConference`	0 (default) - Disable push-to-conference functionality. 1 - Enable push-to-conference functionality.	No
`reg-advanced.cfg`	`reg.x.advancedConference.subscribeForConfEvents`	1 (default) - Conference participants to receive notifications for conference events is enabled. 0 - Conference participants to receive notifications for conference events is disabled.	No
`reg-advanced.cfg`	`reg.x.advancedConference.subscribeForConfEventsOnCCPE`	1 (default) - Enable the conference host to receive notifications for conference events. 0 - Disable the conference host to receive notifications for conference events.	No
`reg-advanced.cfg`	`reg.x.auth.domain`	The domain of the authorization server that is used to check the user names and passwords. Null (default) string	No
`reg-advanced.cfg`	`reg.x.auth.optimizedInFailover`	The destination of the first new SIP request when failover occurs. 0 (default) - The SIP request is sent to the server with the highest priority in the server list. 1 - The SIP request is sent to the server which sent the proxy authentication request.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-basic.cfg	reg.x.auth.password	The password to be used for authentication challenges for this registration. Null (default) string - It overrides the password entered into the Authentication submenu on the Settings menu of the phone.	No
reg-basic.cfg	reg.x.auth.userId	User ID to be used for authentication challenges for this registration. Null (default) string - If the User ID is non-Null, it overrides the user parameter entered into the Authentication submenu on the Settings menu of the phone.	No
reg-advanced.c fg	reg.x.auth.useLoginCre dentials	0 - (default) The Login credentials are not used for authentication to the server on registration x. 1 - The login credentials are used for authentication to the server.	No
reg-advanced.c fg	reg.x.bargeInEnabled	0 (default) - barge-in is disabled for line x. 1 - barge-in is enabled (remote users of shared call appearances can interrupt or barge in to active calls).	No
	reg.x.bridgeInEnabled	0 (default) - Bridge In feature is disabled. 1 - Bridge In feature is enabled.	No
features.cfg	reg.x.broadsoft.userId	Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface. Null (default) string	No
features.cfg	reg.x.broadsoft.useXsp Credentials	If this parameter is disabled, the phones use standard SIP credentials to authenticate. 1 (default) - Use this value, if phone lines are registered with a server running BroadWorks R19 or earlier. 0 - Set to 0, if phone lines are registered with a server running BroadWorks R19 SP1 or later.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	reg.x.broadsoft.xsp.password	Enter the password associated with the BroadSoft user account for the line. Required only when reg.x.broadsoft.useXspCredentials =1. Null (default) string	No
reg-advanced.cfg	reg.x.csta	0 (default) - The uaCSTA (User Agent Computer Supported Telecommunications Applications) feature is disabled. 1 - uaCSTA is enabled (overrides the global parameter voIpProt.SIP.csta.)	No
reg-advanced.cfg	reg.x.displayName	The display name used in SIP signaling and/or the H.323 alias used as the default caller ID. Null (default) UTF-8 encoded string	No
features.cfg	reg.x.enablePvtHoldSoftKey	This parameter applies only to shared lines. 0 (default) - To disable user on a shared line to hold calls privately. 1 - To enable users on a shared line to hold calls privately.	No
reg-advanced.cfg	reg.x.enhancedCallPark.enabled	0 (default) - To disable the BroadWorks Enhanced Call Park feature. 1 - To enable the BroadWorks Enhanced Call Park feature.	No
	reg.x.filterReflectedBlaDialogs	1 (default) - bridged line appearance NOTIFY messages are ignored. 0 - bridged line appearance NOTIFY messages is not ignored	No
reg-advanced.cfg	reg.x.fwd.busy.contact	The forward-to contact for calls forwarded due to busy status. Null (default) - The contact specified by divert.x.contact is used. string - The contact specified by divert.x.contact is not used	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.fwd.busy.status`	0 (default) - Incoming calls that receive a busy signal is not forwarded 1 - Busy calls are forwarded to the contact specified by `reg.x.fwd.busy.contact.`	No
`reg-advanced.cfg`	`reg.x.fwd.noanswer.contact`	Null (default) - The forward-to contact specified by `divert.x.contact` is used. string - The forward to contact used for calls forwarded due to no answer.	No
`reg-advanced.cfg`	`reg.x.fwd.noanswer.ringCount`	The number of seconds the phone should ring for before the call is forwarded because of no answer. The maximum value accepted by some call servers is 20. 0 - (default) 1 to 65535	No
`reg-advanced.cfg`	`reg.x.fwd.noanswer.status`	0 (default) - The calls are not forwarded if there is no answer. 1 - The calls are forwarded to the contact specified by `reg.x.noanswer.contact` after ringing for the length of time specified by `reg.x.fwd.noanswer.ringCount.`	No
`debug.cfg`	`reg.x.gruu`	Specify if the phone sends sip.instance in the REGISTER request. 0 (default) 1	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-basic.cfg`	`reg.x.label`	The text label that displays next to the line key for registration x. The maximum number of characters for this parameter value is 256; however, the maximum number of characters that a phone can display on its user interface varies by phone model and by the width of the characters you use. Parameter values that exceed the phone's maximum display length are truncated by ellipses (…). The rules for parameter up.cfgLabelElide determine how the label is truncated. Null (default) - the label is determined as follows: • If `reg.1.useteluriAsLineLabel=1`, then the tel URI/phone number/address displays as the label. • If `reg.1.useteluriAsLineLabel=0`, then the value for `reg.x.displayName`, if available, displays as the label. If `reg.x.displayName` is unavailable, the user part of `reg.x.address` is used. UTF-8 encoded string	No
`reg-basic.cfg`	`reg.x.lineAddress`	The line extension for a shared line. This parameter applies to private lines and BroadSoft call park and retrieve. If there is no extension provided for this parameter, the call park notification is ignored for the shared line. Null (default) String	No
`reg-advanced.cfg`	`reg.x.lineKeys`	Specify the number of line keys to use for a single registration. The maximum number of line keys you can use per registration depends on your phone model. 1 (default) 1 to max	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`lync.cfg`	`reg.x.lisdisclaimer`	This parameter sets the value of the location policy disclaimer. For example, the disclaimer may be "Warning: If you do not provide a location, emergency services may be delayed in reaching your location should you need to call for help." Null (default) string, 0 to 256 characters	No
`reg-advanced.cfg`	`reg.x.musicOnHold.uri`	A URI that provides the media stream to play for the remote party on hold. Null (default) - This parameter does not overrides `voIpProt.SIP.musicOnHold.uri`. a SIP URI - This parameter overrides `voIpProt.SIP.musicOnHold.uri`.	No
`reg-advanced.cfg`	`reg.x.offerFullCodecListUponResume`	1 (default) - The phone sends full audio and video capabilities after resuming a held call irrespective of the audio and video capabilities negotiated at the initial call answer. 0 - The phone does not send full audio and video capabilities after resuming a held call.	No
`reg-basic.cfg`	`reg.x.outboundProxy.address`	The IP address or hostname of the SIP server to which the phone sends all requests. Null (default) IP address or hostname	No
`sip-interop.cfg`	`reg.x.outboundProxy.failOver.failBack.mode`	The mode for failover failback (overrides `reg.x.server.y.failOver.failBack.mode`). duration - (default) The phone tries the primary server again after the time specified by `reg.x.outboundProxy.failOver.failBack.timeout` expires. newRequests - All new requests are forwarded first to the primary server regardless of the last used server. DNSTTL - The phone tries the primary server again after a timeout equal to the DNS TTL configured for the server that the phone is registered to.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	reg.x.outboundProxy.failOver.failBack.timeout	3600 (default) -The time to wait (in seconds) before failback occurs (overrides reg.x.server.y.failOver.failBack.timeout). 0, 60 to 65535 - The phone does not fail back until a failover event occurs with the current server.	No
reg-advanced.cfg	reg.x.outboundProxy.failOver.failRegistrationOn	1 (default) - The reRegisterOn parameter is enabled, the phone silently invalidates an existing registration. 0 - The reRegisterOn parameter is enabled, existing registrations remain active.	No
reg-advanced.cfg	reg.x.outboundProxy.failOver.onlySignalWithRegistered	1 (default) - The reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. 0 - The reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed.	No
reg-advanced.cfg	reg.x.outboundProxy.failOver.reRegisterOn	This parameters overrides reg.x.server.y.failOver.reRegisterOn. 0 (default) - The phone won't attempt to register with the secondary server. 1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server.	No
reg-advanced.cfg	reg.x.outboundProxy.port	The port of the SIP server to which the phone sends all requests. 0 - (default) 1 to 65535	No
reg-advanced.cfg	reg.x.outboundProxy.transport	The transport method the phone uses to communicate with the SIP server. DNSnaptr (default) DNSnaptr, TCPpreferred, UDPOnly, TLS, TCPOnly	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.protocol.SIP`	You can use this parameter for the VVX 500/501, 600/601, and 1500. 1 (default) - SIP signaling is enabled for this registration. 0 - SIP signaling is not enabled for this registration.	No
`sip-interop.cfg`	`reg.x.proxyRequire`	Null (default) - No Proxy-Require is sent. string - Needs to be entered in the Proxy-Require header.	No
`reg-advanced.cfg`	`reg.x.ringType`	The ringer to be used for calls received by this registration. ringer2 (default) - Is the first non-silent ringer. ringer1 to ringer24 - To play ringer on a single registered line.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.callRecording`	1 (default) - BroadSoft BroadWorks v20 call recording feature for individual phone lines is enabled. 0 - BroadSoft BroadWorks v20 call recording feature for individual phone lines is disabled.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.cf`	This parameter overrides `voIpProt.SIP.serverFeatureControl.cf.` 0 (default) - The server-based call forwarding is disabled. 1 - server based call forwarding is enabled.	Yes
`reg-advanced.cfg`	`reg.x.serverFeatureControl.dnd`	This parameter overrides `voIpProt.SIP.serverFeatureControl.dnd.` 0 (default) - server-based do-not-disturb (DND) is disabled. 1 - server-based DND is enabled and the call server has control of DND.	Yes

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.serverFeatureControl.localProcessing.cf`	This parameter overrides `voIpProt.SIP.serverFeatureControl.localProcessing.cf`. 0 (default) - If `reg.x.serverFeatureControl.cf` is set to 1 the phone does not perform local Call Forward behavior. 1 - The phone performs local Call Forward behavior on all calls received.	No
`sip-interop.cfg`	`reg.x.serverFeatureControl.localProcessing.dnd`	This parameter overrides `voIpProt.SIP.serverFeatureControl.localProcessing.dnd`. 0 (default) - If `reg.x.serverFeatureControl.dnd` is set to 1, the phone does not perform local DND call behavior. 1 - The phone performs local DND call behavior on all calls received.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.securityClassification`	0 (default) - The visual security classification feature for a specific phone line is disabled. 1 - The visual security classification feature for a specific phone line is enabled.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.signalingMethod`	Controls the method used to perform call forwarding requests to the server. serviceMsForwardContact (default) string	No
`sip-interop.cfg`	`reg.x.srtp.enable`	1 (default) - The registration accepts SRTP offers. 0 - The registration always declines SRTP offers.	Yes
`sip-interop.cfg`	`reg.x.srtp.offer`	This parameter applies to the registration initiating (offering) a phone call. 0 (default) - No secure media stream is included in SDP of a SIP INVITE. 1 - The registration includes a secure media stream description along with the usual non-secure media description in the SDP of a SIP INVITE.	Yes

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.srtp.require`	0 (default) - Secure media streams are not required. 1 - The registration is only allowed to use secure media streams.	Yes
`sip-interop.cfg`	`reg.x.srtp.simplifiedBestEffort`	This parameter overrides `sec.srtp.simplifiedBestEffort`. 1 (default) - Negotiation of SRTP compliant with Microsoft Session Description Protocol Version 2.0 Extensions is supported. 0 - No SRTP is supported.	No
`sip-interop.cfg`	`reg.x.strictLineSeize`	0 (default) - Dial prompt is provided immediately without waiting for a successful OK from the call server. 1 - The phone is forced to wait for 200 OK on registration x when receiving a TRYING notify. This parameter overrides voIpProt.SIP.strictLineSeize for registration x.	No
`sip-interop.cfg`	`reg.x.tcpFastFailover`	0 (default) - A full 32 second RFC compliant timeout is used. 1 - failover occurs based on the values of `reg.x.server.y.retryMaxCount` and `voIpProt.server.x.retryTimeOut`.	No
`reg-advanced.cfg`	`reg.x.thirdPartyName`	Null (default) - In all other cases. string address -This field must match the `reg.x.address` value of the registration which makes up the part of a bridged line appearance (BLA).	No
`reg-advanced.cfg`	`reg.x.useCompleteUriForRetrieve`	This parameters overrides `voipPort.SIP.useCompleteUriForRetrieve`. 1 (default) - The target URI in BLF signaling uses the complete address as provided in the XML dialog document. 0 - Only the user portion of the XML dialog document is used and the current registrar's domain is appended to create the full target URI.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.server.H323.y.address`	Address of the H.323 gatekeeper. Null (default) IP address or hostname	No
`site.cfg`	`reg.x.server.H323.y.port`	Port to be used for H.323 signaling. If set to Null, 1719 (H.323 RAS signaling) is used. 0 (default) 0 to 65535	No
`site.cfg`	`reg.x.server.H323.y.expires`	Desired registration period. 3600 positive integer	No
`site.cfg`	`reg.x.server.y.address`	If this parameter is set, it takes precedence even if the DHCP server is available. Null (default) - SIP server does not accepts registrations. IP address or hostname - SIP server that accepts registrations. If not Null, all of the parameters in this table override the parameters specified in `voIpProt.server.*`	No
`reg-advanced`	`reg.x.server.y.expires`	The phone's requested registration period in seconds. The period negotiated with the server may be different. The phone attempts to re-register at the beginning of the overlap period. 3600 - (default) positive integer, minimum 10	No
`reg-advanced`	`reg.x.server.y.expires.lineSeize`	Requested line-seize subscription period. 30 - (default) 0 to 65535	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced	reg.x.server.y.expires.overlap	The number of seconds before the expiration time returned by server x at which the phone should try to re-register. The phone tries to re-register at half the expiration time returned by the server if the server value is less than the configured overlap value. 60 (default) 5 to 65535	No
site.cfg	reg.x.server.y.failOver.failBack.mode	duration (default) - The phone tries the primary server again after the time specified by reg.x.server.y.failOver.failBack.timeout. newRequests - All new requests are forwarded first to the primary server regardless of the last used server. DNSTTL - The phone tries the primary server again after a timeout equal to the DNS TTL configured for the server that the phone is registered to. registration - The phone tries the primary server again when the registration renewal signaling begins. This parameter overrides voIpProt.server.x.failOver.failBack.mode)	No
site.cfg	reg.x.server.y.failOver.failBack.timeout	3600 (default) - The time to wait (in seconds) before failback occurs. 0 - The phone does not fail back until a failover event occurs with the current server. 60 to 65535 - If set to Duration, the phone waits this long after connecting to the current working server before selecting the primary server again.	No
site.cfg	reg.x.server.y.failOver.failRegistrationOn	1 (default) - The reRegisterOn parameter is enabled, the phone silently invalidates an existing registration (if it exists), at the point of failing over. 0 - The reRegisterOn parameter is disabled, existing registrations remain active.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	reg.x.server.y.failOver.onlySignalWithRegistered	1 (default) - Set to this value and reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. If the phone attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call ends. No SIP messages are sent to the unregistered server. 0 - Set to this value and reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred).	No
site.cfg	reg.x.server.y.failOver.reRegisterOn	0 (default) - The phone does not attempt to register with the secondary server, since the phone assumes that the primary and secondary servers share registration information. 1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling proceeds with the secondary server. This parameter overrides voIpProt.server.x.failOver.reRegisterOn.	No
site.cfg	reg.x.server.y.port	Null (default) - The port of the SIP server does not specifies registrations. 0 - The port used depends on reg.x.server.y.transport. 1 to 65535 - The port of the SIP server that specifies registrations.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.server.y.register`	1 (default) - Calls can not be routed to an outbound proxy without registration. 0 - Calls can be routed to an outbound proxy without registration. See voIpProt.server.x.register for more information, see *SIP Server Fallback Enhancements on Polycom Phones - Technical Bulletin 5844* on Polycom Engineering Advisories and Technical Notifications.	No
`sip-interop.cfg`	`reg.x.server.y.registerRetry.baseTimeOut`	For registered line x, set y to the maximum time period the phone waits before trying to re-register with the server.Used in conjunction with `reg.x.server.y.registerRetry.maxTimeOut` to determine how long to wait. 60 (default) 10 - 120 seconds	No
`sip-interop.cfg`	`reg.x.server.y.registerRetry.maxTimeout`	For registered line x, set y to the maximum time period the phone waits before trying to re-register with the server. Use in conjunction with `reg.x.server.y.registerRetry.baseTimeOut` to determine how long to wait. The algorithm is defined in RFC 5626. 180 - (default) 60 - 1800 seconds	No
`reg-advanced.cfg`	`reg.x.server.y.retryMaxCount`	The number of retries attempted before moving to the next available server. 3 - (default) 0 to 20 - 3 is used when the value is set to 0.	No
`reg-advanced.cfg`	`reg.x.server.y.retryTimeOut`	0 (default) - Use standard RFC 3261 signaling retry behavior. 0 to 65535 - The amount of time (in milliseconds) to wait between retries.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.server.y.subscribe.expires`	The phone's requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period. 3600 seconds - (default) 10 – 2147483647 (seconds) You can use this parameter in conjunction with `reg.x.server.y.subscribe.expires.overlap`.	No
`reg-advanced.cfg`	`reg.x.server.y.subscribe.expires.overlap`	The number of seconds before the expiration time returned by server x after which the phone attempts to resubscribe. If the server value is less than the configured overlap value, the phone tries to resubscribe at half the expiration time returned by the server. 60 seconds (default) 5 – 65535 seconds	No
`site.cfg`	`reg.x.server.y.transport`	The transport method the phone uses to communicate with the SIP server. DNSnaptr (default) - If `reg.x.server.y.address` is a hostname and `reg.x.server.y.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.server.y.address` is an IP address, or a port is given, then UDP is used. TCPpreferred - TCP is the preferred transport; UDP is used if TCP fails. UDPOnly - Only UDP is used. TLS - If TLS fails, transport fails. Leave port field empty (defaults to `5061`) or set to `5061`. TCPOnly - Only TCP is used.	No
`site.cfg`	`reg.x.server.y.useOutboundProxy`	1 (default) - Enables to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x. 0 - Disable to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x.	No

Multiple Registrations Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`reg.x.enablePvtHoldSoftKey`	This parameter applies only to shared lines. 0 (default) - To disable user on a shared line to hold calls privately. 1 - To enable users on a shared line to hold calls privately.	No
`reg-advanced.cfg` `reg-advanced.cfg`	`reg.x.acd-login-logout` `reg.x.acd-agent-available`	0 (default) - The ACD feature is disabled for registration. 1 - If both ACD login/logout and agent available are set to 1 for registration x, the ACD feature is enabled for that registration.	No
`reg-advanced.cfg`	`reg.x.acd-agent-available`	0 (default) - The ACD feature is disabled for registration. 1 - If both ACD login/logout and agent available are set to 1 for registration x, the ACD feature is enabled for that registration.	No

Multiple Line Keys Per Registration Parameters

Use the parameter in the following table to configure this feature. This feature is one of several features associated with Call Appearances.

Multiple Line Keys Per Registration Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.lineKeys`	Specify the number of line keys to use for a single registration. The maximum number of line keys you can use per registration depends on your phone model. 1 (default) 1 to max	No

Multiple Call Appearance Parameters

Use the parameters in the following table to set the maximum number of concurrent calls per registered line and the default number of calls per line key.

Note that you can set the value for the `reg.1.callsPerLineKey` parameter to a value higher than 1, for example, 3. After you set the value to 3, for example, you can have three call appearances on line 1. By default, any additional incoming calls are automatically forwarded to voicemail. If you set more than two call appearances, a call appearance counter displays at the top-right corner on the phone.

Multiple Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-basic.cfg`	`call.callsPerLineKey`	Set the maximum number of concurrent calls per line key. This parameter applies to all registered lines. Note that this parameter can be overridden by the per-registration parameter `reg.x.callsPerLineKey`. The maximum number of concurrent calls per line key varies by phone model and is listed for each phone in the column *Calls Per Line Key* in the table Flexible Call Appearances. 24 1 - 24 VVX 101, 201 8 (default) 1- 8	No
`reg-advanced.cfg`	`reg.x.callsPerLineKey`	Set the maximum number of concurrent calls for a single registration x. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all phones sharing that registration. This per-registration parameter overrides `call.callsPerLineKey`. 24 (default) 1-24 VVX 101, 201 8 (default) 1 - 8	No

Bridged Line Appearance Parameters

To begin using bridged line appearance, you must get a registered address dedicated for use with bridged line appearance from your call server provider. This dedicated address must be assigned to a phone line in the `reg.x.address` parameter of the **reg-basic.cfg** template.

Use the parameters in the following table to configure this feature.

Bridged Line Appearance Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`call.shared.disableDivert`	1 (default) - Enable the diversion feature for shared lines. 0 - Disable the diversion feature for shared lines. Note that this feature is disabled on most call servers.	Yes
`reg-advanced.cfg`	`reg.x.type`	private (default) - Use standard call signaling. shared - Use augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.	No
`reg-advanced.cfg`	`reg.x.thirdPartyName`	Null (default) - In all other cases. string address -This field must match the `reg.x.address` value of the registration which makes up the part of a bridged line appearance (BLA).	No
`site.cfg`	`divert.x.sharedDisabled`	1 (default) - Disables call diversion features on shared lines. 0 - Enables call diversion features on shared lines.	Yes

Voicemail Parameters

Use the parameters in the following table to configure voicemail and voicemail settings.

Voicemail Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-basic.cfg`	`msg.mwi.x.call BackMode`	The message retrieval mode and notification for registration x. registration (default) - The registration places a call to itself (the phone calls itself). contact - a call is placed to the contact specified by `msg.mwi.x.callback`. disabled - Message retrieval and message notification are disabled.	No
`sip-interop.cf g`	`msg.mwi.x.call Back`	The contact to call when retrieving messages for this registration if `msg.mwi.x.callBackMode` is set to `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 (default)	No
`sip-interop.cf g`	`msg.mwi.x.subs cribe`	Specify the URI of the message center server. 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) If non-Null, the phone sends a SUBSCRIBE request to this contact after boot-up. NULL (default)	
`site.cfg`	`mwi.backLight. disable`	Specify if the phone screen backlight illuminates when you receive a new voicemail message. 0 (default) - Disable the back light message alert. 1 - Enable the back light message alert.	Yes

Voicemail Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`up.mwiVisible`	Specify if message waiting indicators (MWI) display or not. 0 (default) - If `msg.mwi.x.callBackMode=0`, MWI do not display in the message retrieval menus. 1 - MWI display.	Yes
`sip-interop.cfg`	`up.oneTouchVoiceMail`	0 (default) - The phone displays a summary page with message counts. 1 - You can call voicemail services directly from the phone, if available on the call server, without displaying the voicemail summary.	Yes

Local Call Recording Parameters

Use the parameters in the following table to configure local call recording.

Local Call Recording Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.callRecording.enabled`	0 (default) - Disable audio call recording. 1 - Enable audio call recording.	Yes

Centralized Call Recording Parameters

You must enable this feature on the BroadSoft BroadWorks r20 server and on the phones using the configuration parameters listed in the following table. On the BroadSoft server, assign phone users one of several call recording modes listed in Call Recording Modes.

Use the configuration parameters in the following table to enable this feature on the phone.

Centralized Call Recording Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.callRecording`	0 (default) - The BroadSoft BroadWorks v20 call recording feature for multiple phones is disabled. 1 - The BroadSoft BroadWorks v20 call recording feature for multiple phones is enabled.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.callRecording`	1 (default) - BroadSoft BroadWorks v20 call recording feature for individual phone lines is enabled. 0 - BroadSoft BroadWorks v20 call recording feature for individual phone lines is disabled.	No

Busy Lamp Field Configuration Parameters

Use the parameters in the following table to configure the BLF feature.

Busy Lamp Field Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`attendant.behaviors.display.remoteCallerID.automata`	These parameters depend on the value set for the parameter `attendant.resourceList.x.type`. If the parameter `attendant.resourceList.x.type` is set to automata, use the parameter `attendant.behaviors.display.remoteCallerID.automata`. 1 (default) – Automata remote party caller ID information is presented to the attendant. 0 – The string `unknown` is substituted for both name and number information.	No
`features.cfg`	`attendant.behaviors.display.remoteCallerID.normal`	These parameters depend on the value set for the parameter `attendant.resourceList.x.type`. If the parameter `attendant.resourceList.x.type` is set to normal, use the parameter `attendant.behaviors.display.remoteCallerID.normal`. 1 (default) – Normal remote party caller ID information is presented to the attendant. 0 – The string `unknown` is substituted for both name and number information.	No

Busy Lamp Field Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`attendant.behaviours.display.spontaneousCallAppearances.automata`	Specifies how call appearances display on the attendant phone. 0 (default) – The call appearance is not spontaneously presented to the attendant. The information displayed after a press and hold of a resource's line key is unchanged by this parameter. 1 – The automata call appearance is spontaneously presented to the attendant when calls are alerting on a monitored resource (and a ring tone is played). Note that the values of these call appearance parameters depend on the values applied to `attendant.resourceList.x.type`.	No
`features.cfg`	`attendant.behaviours.display.spontaneousCallAppearances.normal`	Specifies how call appearances display on the attendant phone. 1 (default) – The normal call appearance is spontaneously presented to the attendant when calls are alerting on a monitored resource (and a ring tone is played). 0 – The call appearance is not spontaneously presented to the attendant. The information displayed after a press and hold of a resource's line key is unchanged by this parameter. Note that the values of these call appearance parameters depend on the values applied to `attendant.resourceList.x.type`.	No
`features.cfg`	`attendant.callWaiting.enable`	0 (default) – The phone does not generate acoustic indication of call waiting for attendant calls monitored by BLF. 1 – The phone generates an acoustic indication of call waiting for attendant calls monitored by BLF.	No

Busy Lamp Field Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`attendant.callWaiting.ring`	This parameter is valid only if `attendant.callWaiting.enable` is set to 1. Specifies the ring type to be used for notifying an attendant call if there is an active call already present on the phone. Silent – No acoustic indication is provided. beep – Beep tone is played when there is an active call on the phone and an attendant call is received. ring — Ring tone configured in `attendant.ringType` is used to alert the user when there is an active call on the phone and an attendant call is received.	No
`features.cfg`	`attendant.reg`	Specifies an index number for the BLF resource. The index of the registration is used to send a SUBSCRIBE to the list SIP URI specified in `attendant.uri`. For example, `attendant.reg = 2` means the second registration is used. 1 (default) Permitted value is any positive integer.	No

Busy Lamp Field Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`attendant.resourceList.x.address`	The user referenced by `attendant.reg=""` subscribes to this URI for dialog. If a user part is present, the phone subscribes to a sip URI constructed from the user part and domain of the user referenced by `attendant.reg`. Transport for BLF subscriptions may be modified by including a transport parameter into the subscription address. For example: sip:blf12345@domain.com;transport=tcp Permitted value is a string that constitutes a valid SIP URI (sip:6416@polycom.com) or contains the user part of a SIP URI (6416). Null (default)	No

Busy Lamp Field Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`attendant.resourceList.x.bargeInMode`	Enable or disable barge-in and choose the default barge-in mode. This parameter applies to the Alcatel-Lucent CTS only. Null (default) – If no value is entered, the Barge In feature is disabled. All – Press and hold the BLF line to display all barge-in options. Quick press to barge-in as Normal. Normal – Barge-in plays an audio tone to indicate the arrival of a new participant to the call and all call participants can interact. Listen – The user barging in can listen on the call only. Their outbound audio is not transmitted to either party. Whisper – The user barging in can hear all parties but their audio is only transmitted to the user they are monitoring.	No
`features.cfg`	`attendant.resourceList.x.callAddress`	If the BLF call server is not at the same address as the BLF presence server, calls are sent to this address instead of the address specified by `attendant.resourceList.x.address`. Null (default)	No
`features.cfg`	`attendant.resourceList.x.label`	The text label displays adjacent to the associated line key. If set to Null, the label is derived from the user part of `attendant.resourceList.x.address`. Null (default) Permitted value is a UTF-8 encoded string.	No

Busy Lamp Field Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`attendant.resourceList.x.proceedingIsRecipient`	A flag to determine if pressing the associated line key for the monitored user picks up the call. 1 – If the call server does not support inclusion of the direction attribute in its dialog XML. 0 (default)	No
`features.cfg`	`attendant.resourceList.x.requestSilentBargeIn`	0 (default) – A tone plays when a contact barges in on a call. 1 – No tone is played when a contact barges in on a call.	No
`features.cfg`	`attendant.resourceList.x.type`	The type of resource being monitored and the default action to perform when pressing the line key adjacent to monitored user x. `normal (default)` – The default action 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. Note that the value `normal` applies the call appearance setting `attendant.behaviors.display.*.normal`. `automata` – The default action 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. Note that the value `automata` applies the call appearance setting `attendant.behaviors.display.*.automata=0`.	No
`features.cfg`	`attendant.restrictPickup`	0 (default) - The attendant can pick up calls to monitored users that show as ringing. 1 - The attendant cannot pick up the monitored call.	No

Busy Lamp Field Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`attendant.ringType`	The ringtone that plays when a BLF dialog is in the offering state. ringer1 (default) ringer1 – ringer 24	No
`features.cfg`	`attendant.uri`	The list SIP URI on the server. If this is just a user part, the URI is constructed with the server hostname/IP. Note: If this parameter is set, then the individually addressed users configured by `attendant.resourceList` and `attendant.behaviors` are ignored. Null (default) Strings are permitted.	No
`sip-interop.cfg`	`call.directedCallPickupMethod`	Specifies how the phone performs a directed call pick-up from a BLF contact. legacy (default) – Indicates that the phone uses the method specified in `call.directedCallPickupString`. `native` – Indicates that the phone uses a native protocol method (in this case SIP INVITE with the Replaces header.	No
`sip-interop.cfg`, `site.cfg`	`call.directedCallPickupString`	The star code to initiate a directed call pickup. *97 (default) Note: The default value supports the BroadWorks calls server only. You must change the value if your organization uses a different call server.	No

Busy Lamp Field Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`call.parkedCallRetrieveMethod`	The method the phone uses to retrieve a BLF resource's call which has dialog state confirmed. legacy (default) – Indicates that the phone uses the method specified in `call.parkedCallRetrieveString`. `native` – Indicates that the phone uses a native protocol method (in this case SIP INVITE with the Replaces header).	No
`sip-interop.cfg`, `site.cfg`	`call.parkedCallRetrieveString`	The star code that initiates retrieval of a parked call. Null (default) Permitted values are star codes.	No
`sip-interop.cfg`	`voipPort.SIP.useCompleteUriForRetrieve`	1 (default) – The target URI in BLF signaling uses the complete address as provided in the XML dialog document. 0 – Only the user portion of the target URI in the XML dialog document is used and the current registrar's domain is appended to create the address for retrieval.	No

Busy Lamp Field Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.strictReplacesHeader	This parameter applies only to directed call pick-up attempts initiated against monitored BLF resources. 1 (default) – The phone requires call-id, to-tag, and from-tag to perform a directed call-pickup when `call.directedCallPickupMethod` is configured as native. 0 – Call pick-up requires a call id only.	No
sip-interop.cfg	voIpProt.SIP.useLocalTargetUriforLegacyPickup	1 (default) – The target URI in BLF signaling uses the complete address as provided in the XML dialog document. 0 – Only the user portion of the target URI in the XML dialog document is used and the current registrar's domain is appended to create the address for pickup or retrieval.	No

Instant Messaging Parameters

Use the parameters in the following table to configure this feature.

Instant Messaging Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.messaging.enabled	0 (default) - Disable instant messaging. 1 - Enable instant messaging.	Yes

Local and Centralized Conference Call Parameters

Use the parameters in the following table to set up a conference type and the options available for each type of conference.

You can specify whether, when the host of a three-party local conference leaves the conference, the other two parties remain connected or disconnected. If you want the other two parties remain connected, the phone performs a transfer to keep the remaining parties connected. If the host of four-party local conference leaves the conference, all parties are disconnected and the conference call ends. If the host of a centralized

conference leaves the conference, each remaining party remains connected. For more ways to manage conference calls, see Conference Management.

Local and Centralized Conference Call Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	call.localConferenceCallHold	0 (default) - The host cannot place parties on hold. 1 - During a conference call, the host can place all parties or only the host on hold.	No
sip-interop.cfg	call.transferOnConferenceEnd	1 (default) - After the conference host exits the conference, the remaining parties can continue. 0 - After the conference host exits the conference, all parties are exited and the conference ends.	No
sip-interop.cfg	call.singleKeyPressConference	Specify whether or not all parties hear sound effects while setting up a conference. 0 (default) - Phone sound effects are heard only by the conference initiator. 1 - A conference is initiated when a user presses Conference the first time. Also, all sound effects (dial tone, DTMF tone while dialing and ringing back) are heard by all participants in the conference.	No
sip-interop.cfg	voIpProt.SIP.conference.address	Null (default) - Conferences are set up on the phone locally. String 128 max characters - Enter a conference address. Conferences are set up by the server using the conferencing agent specified by this address. Acceptable values depend on the conferencing server implementation policy.	No

Conference Management Parameters

Use the parameters in the following table to enable this feature.

Conference Management Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.nWayConference.enabled`	0 (default) - Disable the n-way conferencing managing feature. You can hold three-way conferences but the options to manage the conference do not display. 1 - Enable n-way conferencing. You can hold conferences with the maximum number of parties, and the options to manage the conference display.	No

Local Digit Maps Parameters

Polycom support for digit map rules varies for open SIP servers and Microsoft Skype for Business Server. Use the parameters in the following table to configure this feature.

Configure the Local Digit Map

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`dialplan.applyToCallListDial`	Choose whether the dial plan applies to numbers dialed from the received call list or missed call list, including sub-menus. 1 (default) 0	Yes
`site.cfg`	`dialplan.applyToDirectoryDial`	Choose whether the dial plan is applied to numbers dialed from the directory or speed dial, including auto-call contact numbers. 0 (default) 1	Yes
`site.cfg`	`dialplan.applyToForward`	Choose whether the dial plan applies to forwarded calls. 0 1	Yes
`site.cfg`	`dialplan.applyToTelUriDial`	Choose whether the dial plan applies to URI dialing. 1 (default) 0	Yes

Configure the Local Digit Map

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	dialplan.applyToUserDial	Choose whether the dial plan applies to calls placed when the user presses **Dial**. 1 (default) 0	Yes
site.cfg	dialplan.applyToUserSend	Choose whether the dial plan applies to calls placed when the user presses **Send**. 1 (default) 0	Yes
site.cfg	dialplan.conflictMatchHandling	0 (default for Generic Profile) 1 (default for Skype Profile)	
site.cfg	dialplan.digitmap.timeOut	Specify a timeout in seconds for each segment of the digit map using a string of positive integers separated by a vertical bar (	). After a user presses a key, the phone waits this many seconds before matching the digits to a dial plan and dialing the call. (Default) 3 | 3 | 3 | 3 | 3| 3 If there are more digit maps than timeout values, the default value 3 is used. If there are more timeout values than digit maps, the extra timeout values are ignored.	Yes

Configure the Local Digit Map

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`dialplan.digitmap`	Specify the digit map used for the dial plan using a string compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435. This parameter enables the phone to automatically initiate calls to numbers that match a digit map pattern. (Default)`[2-9]11|0T|+011xxx.T|0[2-9]xxxxxxxxx|+1[2-9]xxxxxxx|[2-9]xxxxxxxxx|[2-9]xxxT` The string is limited to 2560 bytes and 100 segments of 64 bytes, and the following characters are allowed in the digit map • A comma (,), which turns dial tone back on. • A plus sign (+) is allowed as a valid digit • The extension letter R	Yes
`debug.cfg`	`dialplan.filterNonDigitUriUsers`	Determine whether to filter out (+) from the dial plan. 0 (default) 1	Yes
`site.cfg`	`dialplan.impossibleMatchHandling`	0 (default)—The digits entered up to and including the point an impossible match occurred are sent to the server immediately. 1—The phone gives a reorder tone. 2—Users can accumulate digits and dispatch the call manually by pressing **Send**. If a call orbit number begins with pound (#) or asterisk (*), you need to set the value to 2 to retrieve the call using off-hook dialing.	Yes
`site.cfg`	`dialplan.removeEndOfDial`	Sets if the trailing # is stripped from the digits sent out. 1 (default) 0	Yes

Configure the Local Digit Map

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`dialplan.routing.emergency.outboundIdentity`	Choose how your phone is identified when you place an emergency call. NULL (default) 10-25 digit number SIP TEL URI If using a URI, the full URI is included verbatim in the P-A-I header. For example: • `dialplan.routing.emergency.outboundIdentity` = 5551238000 • `dialplan.routing.emergency.outboundIdentity` = sip:john@emergency.com • `dialplan.routing.emergency.outboundIdentity` = tel:+16045558000	No
`site.cfg`	`dialplan.routing.emergency.preferredSource`	Set the precedence of the source of emergency outbound identities. ELIN (default)— the outbound identity used in the SIP P-Asserted-Identity header is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN). Config— the parameter `dialplan.routing.emergency.outboundIdentity` has priority when enabled, and the LLDP-MED ELIN value is used if `dialplan.routing.emergency.outboundIdentity` is NULL.	No
`site.cfg`	`dialplan.routing.emergency.x.description`	Set the label or description for the emergency contact address. x=1: Emergency, Others: NULL (default) string x is the index of the emergency entry description where x must use sequential numbering starting at 1.	Yes

Configure the Local Digit Map

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`dialplan.routing.emergency.x.server.y`	Set the emergency server to use for emergency routing (`dialplan.routing.server.x.address` where x is the index). x=1: 1, Others: Null (default) positive integer x is the index of the emergency entry and y is the index of the server associated with emergency entry x. For each emergency entry (x), one or more server entries (x,y) can be configured. x and y must both use sequential numbering starting at 1.	Yes
`site.cfg`	`dialplan.routing.emergency.x.value`	Set the emergency URL values that should be watched for. When the user dials one of the URLs, the call is directed to the emergency server defined by `dialplan.routing.server.x.address`. x=1: 911, others: Null (default) SIP URL (single entry) x is the index of the emergency entry description where x must use sequential numbering starting at 1.	No
`site.cfg`	`dialplan.routing.server.x.address`	Set the IP address or hostname of a SIP server to use for routing calls. Multiple servers can be listed starting with x=1 to 3 for fault tolerance. Null (default) IP address hostname Blind transfer for 911 or other emergency calls may not work if registration and emergency servers are different entities.	Yes

Configure the Local Digit Map

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`dialplan.routing.server.x.port`	Set the port of a SIP server to use for routing calls. 5060 (default) 1 to 65535	Yes
`site.cfg`	`dialplan.routing.server.x.transport`	Set the DNS lookup of the first server to use and dialed if there is a conflict with other servers. DNSnaptr (default) TCPpreferred UDPOnly TLS TCPOnly For example, if `dialplan.routing.server.1.transport` = "UDPOnly" and `dialplan.routing.server.2.transport` = "TLS", then UDPOnly is used.	Yes
`site.cfg`	`dialplan.userDial.timeOut`	Specify the time in seconds that the phone waits before dialing a number entered while the phone is on hook. 0 (default for Generic Profile) 0-99 seconds You can apply `dialplan.userDial.timeOut` only when its value is lower than `up.IdleTimeOut.`	No

Shared Lines

The PTT (push-to-talk) parameter is used to configure Push-to-Talk features. The parameters in the next table configure the PTT mode and page mode features.

Shared Call Appearances Parameters

This feature is dependent on support from a SIP call server. To enable shared call appearances on your phone, you must obtain a shared line address from your SIP service provider.

Use the parameters in the following table to configure options for this feature.

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-basic.cfg`	`reg.x.address`	The user part (for example, 1002) or the user and the host part (for example, `1002@polycom.com`) of the registration SIP URI or the H.323 ID/extension. Null (default) string address	No
`reg-advanced.cfg`	`reg.x.type`	private (default) - Use standard call signaling. shared - Use augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.	No
`sip-interop.cfg`	`call.shared.reject`	For shared line calls on the BroadWorks server. 0 - The phone displays a Reject soft key to reject an incoming call to a shared line. 1 - The Reject soft key does not display.	No
`sip-interop.cfg`	`call.shared.exposeAutoHolds`	0 (default) - No re-INVITE is sent to the server when setting up a conference on a shared line. 1 - A re-INVITE is sent to the server when setting up a conference on a shared line.	Yes
`sip-interop.cfg`	`call.shared.oneTouchResume`	0 (default) - Selecting the shared line opens all current calls that the user can choose from. 1 - All users on a shared line can resume held calls by pressing the shared line key. If more than one call is on hold, the first held call is selected and resumed. A quick press and release of the line key resumes a call whereas pressing and holding down the line key shows a list of calls on that line.	Yes
`sip-interop.cfg`	`call.shared.preferCallInfoCID`	0 (default) - Caller ID received from 200OK is ignored if NOTIFY message includes display information. 1 - Caller ID received from 200OK is displayed if NOTIFY message includes display information.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg, site.cfg`	`call.shared.remoteActiveHoldAsActive`	1 (default) - Shared remote active/hold calls are treated as a active call on the phone. 0 - Shared remote active/hold calls are not treated as a active call on the phone.	No
`sip-interop.cfg`	`call.shared.seizeFailReorder`	1 (default) - Play a re-order tone locally on shared line seize failure. 0 - Do not play a re-order tone locally on shared line seize failure.	Yes
`sip-interop.cfg`	`voIpProt.SIP.specialEvent.lineSeize.nonStandard`	Controls the response for a line-seize event SUBSCRIBE. 1 (default) - This speeds up the processing of the response for line-seize event. 0 - This will process the response for the line seize event normally	Yes
`reg-advanced.cfg`	`reg.x.ringType`	The ringer to be used for calls received by this registration. The default is the first non-silent ringer. If you use the configuration parameters ringer13 and ringer14 on a single registered line, the phone plays SystemRing.wav. default (default) ringer1 to ringer24	No
`sip-interop.cfg`	`reg.x.protocol.H323`	You can use this parameter for the VVX 500/501, 600/601, and 1500. 0 (default) - H.323 signaling is not enabled for registration x. 1 - H.323 signaling is enabled for registration x.	No
`site.cfg`	`reg.x.server.H323.y.address`	Address of the H.323 gatekeeper. Null (default) IP address or hostname	No
`site.cfg`	`reg.x.server.H323.y.port`	Port to be used for H.323 signaling. If set to Null, 1719 (H.323 RAS signaling) is used. 0 (default) 0 to 65535	No
`site.cfg`	`reg.x.server.H323.y.expires`	Desired registration period. 3600 positive integer	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.line.y.label`	Configure a unique line label for a shared line that has multiple line key appearances. This parameter takes effect when `up.cfgUniqueLineLabel=1`. If `reg.x.linekeys=1`, this parameter does not have any effect. x = the registration index number starting from 1. y = the line index from 1 to the value set by `reg.x.linekeys`. Specifying a string sets the label used for the line key registration on phones with multiple line keys. If no parameter value is set for `reg.x.line.y.label`, the phone automatically numbers multiple lines by prepending "<y>_" where <y> is the line index from 1 to the value set by `reg.x.linekeys`. • The following examples show labels for line 1 on a phone with user registration 1234, where `reg.x.linekeys=2`: ⌃ If no label is configured for registration, the labels are "1_1234" and "2_1234". ⌃ If `reg.1.line.1.label=Polycom` and `reg.1.line.2.label=VVX`, the labels display as 'Polycom' and 'VVX'.	No
`reg-advanced.cfg`	`reg.x.callsPerLineKey`	Set the maximum number of concurrent calls for a single registration x. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all phones sharing that registration. This per-registration parameter overrides `call.callsPerLineKey`. 24 (default) 1-24 VVX 101, 201 8 (default) 1 - 8	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	reg.x.header.pearlymedia.support	0 (Default) - The p-early-media header is not supported on the specified line registration. 1 - The p-early-media header is supported by the specified line registration.	No
reg-basic.cfg	reg.X.insertOBPAddressInRoute	1 (Default) - The outbound proxy address is added as the topmost route header. 0 - The outbound proxy address is not added to the route header.	No
features.cfg	reg.x.path	0 (Default) - The path extension header field in the Register request message is not supported for the specific line registration. 1 - The phone supports and provides the path extension header field in the Register request message for the specific line registration.	No
features.cfg	reg.x.regevent	0 (default) - The phone is not subscribed to registration state change notifications for the specific phone line. 1 - The phone is subscribed to registration state change notifications for the specific phone line. This parameter overrides the global parameter voIpProt.SIP.regevent.	No
reg-advanced.cfg	reg.x.rejectNDUBInvite	Specify whether or not the phone accepts a call for a particular registration in case of a Network Determined User Busy (NDUB) event advertised by the SIP server. 0 (Default) - If an NDUB event occurs, the phone does not reject the call. 1 - If an NDUB event occurs, the phone rejects the call with a 603 Decline response code.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.server.y.specialInterop`	Specify the server-specific feature set for the line registration. Standard (Default) VVX 101: Standard GENBAND ALU-CTS DT VVX 201: Standard, GENBAND ALU-CTS ocs2007r2 lync2010 All other phones: Standard GENBAND ALU-CTS ocs2007r2 lync2010 lcs2005	
`sip-interop.cfg`	`reg.x.gruu`	1 - The phone sends sip.instance in the REGISTER request. 0 (default) - The phone does not send sip.instance in the REGISTER request.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.securityClassification`	0 (default) - The visual security classification feature for a specific phone line is disabled. 1 - The visual security classification feature for a specific phone line is enabled.	No
`reg-advanced.cfg`	`reg.x.terminationType`	Determines the type of termination that is used for the line where the line can be managed automatically on the VVX, the wireless handset, or on both. X = each registration index. NULL (default) VVX, DECT, or VVX-DECT	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg` `reg-advanced.cfg`	`reg.x.acd-login-logout` `reg.x.acd-agent-available`	0 (default) - The ACD feature is disabled for registration. 1 - If both ACD login/logout and agent available are set to 1 for registration x, the ACD feature is enabled for that registration.	No
`reg-advanced.cfg`	`reg.x.advancedConference.maxParticipants`	Sets the maximum number of participants allowed in a push to conference for advanced conference calls. The number of participants configured must match the number of participants allowed on the ALU CTS. 3 (default) 0 - 25	No
`reg-advanced.cfg`	`reg.x.advancedConference.pushToConference`	0 (default) - Disable push-to-conference functionality. 1 - Enable push-to-conference functionality.	No
`reg-advanced.cfg`	`reg.x.advancedConference.subscribeForConfEvents`	1 (default) - Conference participants to receive notifications for conference events is enabled. 0 - Conference participants to receive notifications for conference events is disabled.	No
`reg-advanced.cfg`	`reg.x.advancedConference.subscribeForConfEventsOnCCPE`	1 (default) - Enable the conference host to receive notifications for conference events. 0 - Disable the conference host to receive notifications for conference events.	No
`reg-advanced.cfg`	`reg.x.auth.domain`	The domain of the authorization server that is used to check the user names and passwords. Null (default) string	No
`reg-advanced.cfg`	`reg.x.auth.optimizedInFailover`	The destination of the first new SIP request when failover occurs. 0 (default) - The SIP request is sent to the server with the highest priority in the server list. 1 - The SIP request is sent to the server which sent the proxy authentication request.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-basic.cfg	reg.x.auth.password	The password to be used for authentication challenges for this registration. Null (default) string - It overrides the password entered into the Authentication submenu on the Settings menu of the phone.	No
reg-basic.cfg	reg.x.auth.userId	User ID to be used for authentication challenges for this registration. Null (default) string - If the User ID is non-Null, it overrides the user parameter entered into the Authentication submenu on the Settings menu of the phone.	No
reg-advanced.cfg	reg.x.auth.useLoginCredentials	0 - (default) The Login credentials are not used for authentication to the server on registration x. 1 - The login credentials are used for authentication to the server.	No
reg-advanced.cfg	reg.x.bargeInEnabled	0 (default) - barge-in is disabled for line x. 1 - barge-in is enabled (remote users of shared call appearances can interrupt or barge in to active calls).	No
	reg.x.bridgeInEnabled	0 (default) - Bridge In feature is disabled. 1 - Bridge In feature is enabled.	No
features.cfg	reg.x.broadsoft.userId	Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface. Null (default) string	No
features.cfg	reg.x.broadsoft.useXspCredentials	If this parameter is disabled, the phones use standard SIP credentials to authenticate. 1 (default) - Use this value, if phone lines are registered with a server running BroadWorks R19 or earlier. 0 - Set to 0, if phone lines are registered with a server running BroadWorks R19 SP1 or later.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`reg.x.broadsoft.xsp.pa ssword`	Enter the password associated with the BroadSoft user account for the line. Required only when `reg.x.broadsoft.useXspCredentials =1`. Null (default) string	No
`reg-advanced.c fg`	`reg.x.csta`	0 (default) - The uaCSTA (User Agent Computer Supported Telecommunications Applications) feature is disabled. 1 - uaCSTA is enabled (overrides the global parameter `voIpProt.SIP.csta`.)	No
`reg-advanced.c fg`	`reg.x.displayName`	The display name used in SIP signaling and/or the H.323 alias used as the default caller ID. Null (default) UTF-8 encoded string	No
`features.cfg`	`reg.x.enablePvtHoldSof tKey`	This parameter applies only to shared lines. 0 (default) - To disable user on a shared line to hold calls privately. 1 - To enable users on a shared line to hold calls privately.	No
`reg-advanced.c fg`	`reg.x.enhancedCallPark .enabled`	0 (default) - To disable the BroadWorks Enhanced Call Park feature. 1 - To enable the BroadWorks Enhanced Call Park feature.	No
	`reg.x.filterReflectedB laDialogs`	1 (default) - bridged line appearance NOTIFY messages are ignored. 0 - bridged line appearance NOTIFY messages is not ignored	No
`reg-advanced.c fg`	`reg.x.fwd.busy.contact`	The forward-to contact for calls forwarded due to busy status. Null (default) - The contact specified by `divert.x.contact` is used. string - The contact specified by `divert.x.contact` is not used	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.fwd.busy.status`	0 (default) - Incoming calls that receive a busy signal is not forwarded 1 - Busy calls are forwarded to the contact specified by `reg.x.fwd.busy.contact`.	No
`reg-advanced.cfg`	`reg.x.fwd.noanswer.contact`	Null (default) - The forward-to contact specified by `divert.x.contact` is used. string - The forward to contact used for calls forwarded due to no answer.	No
`reg-advanced.cfg`	`reg.x.fwd.noanswer.ringCount`	The number of seconds the phone should ring for before the call is forwarded because of no answer. The maximum value accepted by some call servers is 20. 0 - (default) 1 to 65535	No
`reg-advanced.cfg`	`reg.x.fwd.noanswer.status`	0 (default) - The calls are not forwarded if there is no answer. 1 - The calls are forwarded to the contact specified by `reg.x.noanswer.contact` after ringing for the length of time specified by `reg.x.fwd.noanswer.ringCount`.	No
`debug.cfg`	`reg.x.gruu`	Specify if the phone sends sip.instance in the REGISTER request. 0 (default) 1	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-basic.cfg`	`reg.x.label`	The text label that displays next to the line key for registration x. The maximum number of characters for this parameter value is 256; however, the maximum number of characters that a phone can display on its user interface varies by phone model and by the width of the characters you use. Parameter values that exceed the phone's maximum display length are truncated by ellipses (…). The rules for parameter up.cfgLabelElide determine how the label is truncated. Null (default) - the label is determined as follows: • If `reg.1.useteluriAsLineLabel=1`, then the tel URI/phone number/address displays as the label. • If `reg.1.useteluriAsLineLabel= 0`, then the value for `reg.x.displayName`, if available, displays as the label. If `reg.x.displayName` is unavailable, the user part of `reg.x.address` is used. UTF-8 encoded string	No
`reg-basic.cfg`	`reg.x.lineAddress`	The line extension for a shared line. This parameter applies to private lines and BroadSoft call park and retrieve. If there is no extension provided for this parameter, the call park notification is ignored for the shared line. Null (default) String	No
`reg-advanced.cfg`	`reg.x.lineKeys`	Specify the number of line keys to use for a single registration. The maximum number of line keys you can use per registration depends on your phone model. 1 (default) 1 to max	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`lync.cfg`	`reg.x.lisdisclaimer`	This parameter sets the value of the location policy disclaimer. For example, the disclaimer may be "Warning: If you do not provide a location, emergency services may be delayed in reaching your location should you need to call for help." Null (default) string, 0 to 256 characters	No
`reg-advanced.cfg`	`reg.x.musicOnHold.uri`	A URI that provides the media stream to play for the remote party on hold. Null (default) - This parameter does not overrides `voIpProt.SIP.musicOnHold.uri`. a SIP URI - This parameter overrides `voIpProt.SIP.musicOnHold.uri`.	No
`reg-advanced.cfg`	`reg.x.offerFullCodecListUponResume`	1 (default) - The phone sends full audio and video capabilities after resuming a held call irrespective of the audio and video capabilities negotiated at the initial call answer. 0 - The phone does not send full audio and video capabilities after resuming a held call.	No
`reg-basic.cfg`	`reg.x.outboundProxy.address`	The IP address or hostname of the SIP server to which the phone sends all requests. Null (default) IP address or hostname	No
`sip-interop.cfg`	`reg.x.outboundProxy.failOver.failBack.mode`	The mode for failover failback (overrides `reg.x.server.y.failOver.failBack.mode`). duration - (default) The phone tries the primary server again after the time specified by `reg.x.outboundProxy.failOver.failBack.timeout` expires. newRequests - All new requests are forwarded first to the primary server regardless of the last used server. DNSTTL - The phone tries the primary server again after a timeout equal to the DNS TTL configured for the server that the phone is registered to.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	reg.x.outboundProxy.failOver.failBack.timeout	3600 (default) -The time to wait (in seconds) before failback occurs (overrides reg.x.server.y.failOver.failBack.timeout). 0, 60 to 65535 - The phone does not fail back until a failover event occurs with the current server.	No
reg-advanced.cfg	reg.x.outboundProxy.failOver.failRegistrationOn	1 (default) - The reRegisterOn parameter is enabled, the phone silently invalidates an existing registration. 0 - The reRegisterOn parameter is enabled, existing registrations remain active.	No
reg-advanced.cfg	reg.x.outboundProxy.failOver.onlySignalWithRegistered	1 (default) - The reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. 0 - The reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed.	No
reg-advanced.cfg	reg.x.outboundProxy.failOver.reRegisterOn	This parameters overrides reg.x.server.y.failOver.reRegisterOn. 0 (default) - The phone won't attempt to register with the secondary server. 1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server.	No
reg-advanced.cfg	reg.x.outboundProxy.port	The port of the SIP server to which the phone sends all requests. 0 - (default) 1 to 65535	No
reg-advanced.cfg	reg.x.outboundProxy.transport	The transport method the phone uses to communicate with the SIP server. DNSnaptr (default) DNSnaptr, TCPpreferred, UDPOnly, TLS, TCPOnly	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.protocol.SIP`	You can use this parameter for the VVX 500/501, 600/601, and 1500. 1 (default) - SIP signaling is enabled for this registration. 0 - SIP signaling is not enabled for this registration.	No
`sip-interop.cfg`	`reg.x.proxyRequire`	Null (default) - No Proxy-Require is sent. string - Needs to be entered in the Proxy-Require header.	No
`reg-advanced.cfg`	`reg.x.ringType`	The ringer to be used for calls received by this registration. ringer2 (default) - Is the first non-silent ringer. ringer1 to ringer24 - To play ringer on a single registered line.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.callRecording`	1 (default) - BroadSoft BroadWorks v20 call recording feature for individual phone lines is enabled. 0 - BroadSoft BroadWorks v20 call recording feature for individual phone lines is disabled.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.cf`	This parameter overrides `voIpProt.SIP.serverFeatureControl.cf.` 0 (default) - The server-based call forwarding is disabled. 1 - server based call forwarding is enabled.	Yes
`reg-advanced.cfg`	`reg.x.serverFeatureControl.dnd`	This parameter overrides `voIpProt.SIP.serverFeatureControl.dnd.` 0 (default) - server-based do-not-disturb (DND) is disabled. 1 - server-based DND is enabled and the call server has control of DND.	Yes

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.serverFeatureControl.localProcessing.cf`	This parameter overrides `voIpProt.SIP.serverFeatureControl.localProcessing.cf`. 0 (default) - If `reg.x.serverFeatureControl.cf` is set to 1 the phone does not perform local Call Forward behavior. 1 - The phone performs local Call Forward behavior on all calls received.	No
`sip-interop.cfg`	`reg.x.serverFeatureControl.localProcessing.dnd`	This parameter overrides `voIpProt.SIP.serverFeatureControl.localProcessing.dnd`. 0 (default) - If `reg.x.serverFeatureControl.dnd` is set to 1, the phone does not perform local DND call behavior. 1 - The phone performs local DND call behavior on all calls received.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.securityClassification`	0 (default) - The visual security classification feature for a specific phone line is disabled. 1 - The visual security classification feature for a specific phone line is enabled.	No
`reg-advanced.cfg`	`reg.x.serverFeatureControl.signalingMethod`	Controls the method used to perform call forwarding requests to the server. serviceMsForwardContact (default) string	No
`sip-interop.cfg`	`reg.x.srtp.enable`	1 (default) - The registration accepts SRTP offers. 0 - The registration always declines SRTP offers.	Yes
`sip-interop.cfg`	`reg.x.srtp.offer`	This parameter applies to the registration initiating (offering) a phone call. 0 (default) - No secure media stream is included in SDP of a SIP INVITE. 1 - The registration includes a secure media stream description along with the usual non-secure media description in the SDP of a SIP INVITE.	Yes

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.srtp.require`	0 (default) - Secure media streams are not required. 1 - The registration is only allowed to use secure media streams.	Yes
`sip-interop.cfg`	`reg.x.srtp.simplifiedBestEffort`	This parameter overrides `sec.srtp.simplifiedBestEffort`. 1 (default) - Negotiation of SRTP compliant with Microsoft Session Description Protocol Version 2.0 Extensions is supported. 0 - No SRTP is supported.	No
`sip-interop.cfg`	`reg.x.strictLineSeize`	0 (default) - Dial prompt is provided immediately without waiting for a successful OK from the call server. 1 - The phone is forced to wait for 200 OK on registration x when receiving a TRYING notify. This parameter overrides voIpProt.SIP.strictLineSeize for registration x.	No
`sip-interop.cfg`	`reg.x.tcpFastFailover`	0 (default) - A full 32 second RFC compliant timeout is used. 1 - failover occurs based on the values of `reg.x.server.y.retryMaxCount` and `voIpProt.server.x.retryTimeOut`.	No
`reg-advanced.cfg`	`reg.x.thirdPartyName`	Null (default) - In all other cases. string address -This field must match the `reg.x.address` value of the registration which makes up the part of a bridged line appearance (BLA).	No
`reg-advanced.cfg`	`reg.x.useCompleteUriForRetrieve`	This parameters overrides `voipPort.SIP.useCompleteUriForRetrieve`. 1 (default) - The target URI in BLF signaling uses the complete address as provided in the XML dialog document. 0 - Only the user portion of the XML dialog document is used and the current registrar's domain is appended to create the full target URI.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.server.H323.y.address`	Address of the H.323 gatekeeper. Null (default) IP address or hostname	No
`site.cfg`	`reg.x.server.H323.y.port`	Port to be used for H.323 signaling. If set to Null, 1719 (H.323 RAS signaling) is used. 0 (default) 0 to 65535	No
`site.cfg`	`reg.x.server.H323.y.expires`	Desired registration period. 3600 positive integer	No
`site.cfg`	`reg.x.server.y.address`	If this parameter is set, it takes precedence even if the DHCP server is available. Null (default) - SIP server does not accepts registrations. IP address or hostname - SIP server that accepts registrations. If not Null, all of the parameters in this table override the parameters specified in `voIpProt.server.*`	No
`reg-advanced`	`reg.x.server.y.expires`	The phone's requested registration period in seconds. The period negotiated with the server may be different. The phone attempts to re-register at the beginning of the overlap period. 3600 - (default) positive integer, minimum 10	No
`reg-advanced`	`reg.x.server.y.expires.lineSeize`	Requested line-seize subscription period. 30 - (default) 0 to 65535	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced	reg.x.server.y.expires.overlap	The number of seconds before the expiration time returned by server x at which the phone should try to re-register. The phone tries to re-register at half the expiration time returned by the server if the server value is less than the configured overlap value. 60 (default) 5 to 65535	No
site.cfg	reg.x.server.y.failOver.failBack.mode	duration (default) - The phone tries the primary server again after the time specified by reg.x.server.y.failOver.failBack.timeout. newRequests - All new requests are forwarded first to the primary server regardless of the last used server. DNSTTL - The phone tries the primary server again after a timeout equal to the DNS TTL configured for the server that the phone is registered to. registration - The phone tries the primary server again when the registration renewal signaling begins. This parameter overrides voIpProt.server.x.failOver.failBack.mode)	No
site.cfg	reg.x.server.y.failOver.failBack.timeout	3600 (default) - The time to wait (in seconds) before failback occurs. 0 - The phone does not fail back until a failover event occurs with the current server. 60 to 65535 - If set to Duration, the phone waits this long after connecting to the current working server before selecting the primary server again.	No
site.cfg	reg.x.server.y.failOver.failRegistrationOn	1 (default) - The reRegisterOn parameter is enabled, the phone silently invalidates an existing registration (if it exists), at the point of failing over. 0 - The reRegisterOn parameter is disabled, existing registrations remain active.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.server.y.failOver.onlySignalWithRegistered`	1 (default) - Set to this value and reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. If the phone attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call ends. No SIP messages are sent to the unregistered server. 0 - Set to this value and reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred).	No
`site.cfg`	`reg.x.server.y.failOver.reRegisterOn`	0 (default) - The phone does not attempt to register with the secondary server, since the phone assumes that the primary and secondary servers share registration information. 1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling proceeds with the secondary server. This parameter overrides `voIpProt.server.x.failOver.reRegisterOn`.	No
`site.cfg`	`reg.x.server.y.port`	Null (default) - The port of the SIP server does not specifies registrations. 0 - The port used depends on `reg.x.server.y.transport`. 1 to 65535 - The port of the SIP server that specifies registrations.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.server.y.register`	1 (default) - Calls can not be routed to an outbound proxy without registration. 0 - Calls can be routed to an outbound proxy without registration. See voIpProt.server.x.register for more information, see *SIP Server Fallback Enhancements on Polycom Phones - Technical Bulletin 5844* on Polycom Engineering Advisories and Technical Notifications.	No
`sip-interop.cfg`	`reg.x.server.y.registerRetry.baseTimeOut`	For registered line x, set y to the maximum time period the phone waits before trying to re-register with the server.Used in conjunction with `reg.x.server.y.registerRetry.maxTimeOut` to determine how long to wait. 60 (default) 10 - 120 seconds	No
`sip-interop.cfg`	`reg.x.server.y.registerRetry.maxTimeout`	For registered line x, set y to the maximum time period the phone waits before trying to re-register with the server. Use in conjunction with `reg.x.server.y.registerRetry.baseTimeOut` to determine how long to wait. The algorithm is defined in RFC 5626. 180 - (default) 60 - 1800 seconds	No
`reg-advanced.cfg`	`reg.x.server.y.retryMaxCount`	The number of retries attempted before moving to the next available server. 3 - (default) 0 to 20 - 3 is used when the value is set to 0.	No
`reg-advanced.cfg`	`reg.x.server.y.retryTimeOut`	0 (default) - Use standard RFC 3261 signaling retry behavior. 0 to 65535 - The amount of time (in milliseconds) to wait between retries.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.server.y.subscribe.expires`	The phone's requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period. 3600 seconds - (default) 10 – 2147483647 (seconds) You can use this parameter in conjunction with `reg.x.server.y.subscribe.expires.overlap`.	No
`reg-advanced.cfg`	`reg.x.server.y.subscribe.expires.overlap`	The number of seconds before the expiration time returned by server x after which the phone attempts to resubscribe. If the server value is less than the configured overlap value, the phone tries to resubscribe at half the expiration time returned by the server. 60 seconds (default) 5 – 65535 seconds	No
`site.cfg`	`reg.x.server.y.transport`	The transport method the phone uses to communicate with the SIP server. DNSnaptr (default) - If `reg.x.server.y.address` is a hostname and `reg.x.server.y.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.server.y.address` is an IP address, or a port is given, then UDP is used. TCPpreferred - TCP is the preferred transport; UDP is used if TCP fails. UDPOnly - Only UDP is used. TLS - If TLS fails, transport fails. Leave port field empty (defaults to `5061`) or set to `5061`. TCPOnly - Only TCP is used.	No

Shared Call Appearances Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.server.y.useOutboundProxy`	1 (default) - Enables to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x. 0 - Disable to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x.	No
`site.cfg`	`divert.x.sharedDisabled`	1 (default) - Disables call diversion features on shared lines. 0 - Enables call diversion features on shared lines.	Yes

Private Hold on Shared Lines Parameters

You can configure private hold only using configuration files; you cannot configure the feature on the Web Configuration Utility or from the local phone interface.

Use the parameters in the following table to configure this feature.

Private Hold Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`call.shared.exposeAutoHolds`	0 (default) - No re-INVITE is sent to the server when setting up a conference on a shared line. 1 - A re-INVITE is sent to the server when setting up a conference on a shared line.	Yes
`features.cfg`	`reg.x.enablePvtHoldSoftKey`	This parameter applies only to shared lines. 0 (default) - To disable user on a shared line to hold calls privately. 1 - To enable users on a shared line to hold calls privately.	No

Intercom Calls Parameters

Use the parameters in the table to configure the behavior of the calling and answering phone.

Intercom Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.intercom.enable`	0 (default) - Disable the Intercom feature. 1 - Enable the Intercom feature.	No
`features.cfg`	`homeScreen.intercom.enable`	1 (default) - Enable the Intercom icon on the phone Home screen. 0 - Disable the Intercom icon on the phone Home screen.	No
`features.cfg`	`softkey.feature.intercom`	1 (default) - Enables the **Intercom** soft key. 0 - Disables the **Intercom** soft key.	No
`sip-interop.cfg`	`voIpProt.SIP.intercom.alertInfo`	The string you want to use in the Alert-Info header. You can use the following characters: '@', '-' ,'_' , '.' . If you use any other characters, NULL, or empty spaces, the call is sent as normal without the Alert-Info header. Intercom (default) Alpha - Numeric string	No
`sip-interop.cfg`	`voIpProt.SIP.alertInfo.x.value`	Specify a ringtone for single registered line using a string to match the Alert-Info header in the incoming INVITE. NULL (default)	No
`sip-interop.cfg`	`voIpProt.SIP.alertInfo.x.class`	Alert-Info fields from INVITE requests are compared 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 is applied. default (default) See the list of ring classes in Ringtone Parameters.	No

Push-to-Talk Parameters

Administrators must enable group paging and PTT before users can subscribe to a PTT channel.

PTT works in conjunction with group paging, and you can enable PTT or group paging, or enable both to operate simultaneously.

Push-To-Talk Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`ptt.address`	The multicast IP address to send page audio to and receive page audio from. 224.0.1.116 (default) multicast IP address.	
`site.cfg`	`ptt.allowOffHookPages`	0 (default) - PTT messages do not play out on the phone during an active call and the user must accept incoming PTT messages to play out. 1 - PTT messages play out even when there is an active call on the phone.	
`site.cfg`	`ptt.callWaiting.enable`	0 (default) - Incoming PTT sessions do not produce standard call waiting. 1 - Incoming PTT sessions produce standard call waiting behavior on the active audio channel.	
`features.cfg`	`ptt.channel.x.allowReceive`	1 (default) - The channel x receive incoming PTT messages. 0 - The channel x does not receive incoming PTT messages.	
`features.cfg`	`ptt.channel.x.allowTransmit`	1 (default) - Outgoing PTT messages are allowed on channel x. 0 - Outgoing PTT messages are not allowed on channel x.	
`features.cfg`	`ptt.channel.x.available`	1 (default) - Channel x is available. 0 - Channel x is not available.	
`features.cfg`	`ptt.channel.x.label`	Specify a label for channel x. Null (default) string	
`features.cfg`	`ptt.channel.x.subscribed`	0 (default) - The PPT is not subscribed for channel x. 1 - 25 - The PTT is subscribed for channel x.	
`site.cfg`	`ptt.codec`	Specify codec to use for PTT. G.722 (default) G.711Mu, G.726QI, G.722	
`site.cfg`	`ptt.compatibilityMode`	0 (default) - The PTT codec used is controlled by the `ptt.codec` and `ptt.pageMode.codec` parameters. 1 - The codec used for PTT will be G726QI and payload size used will be 30.	

Push-To-Talk Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	ptt.defaultChannel	Specify the default channel number used for PTT transmissions. 1 (default) 1 - 25	
site.cfg	ptt.emergencyChannel	Specify the channel to use for emergency PTT transmissions. 25 (default) 1 - 25	
site.cfg	ptt.emergencyChannel.volume	The volume of emergency pages relative to the maximum speakerphone volume of the phone. Positive values are louder than the maximum and negative values are quieter. The gain to use for emergency page/PTT is the maximum termination gain plus this parameter. **Note**: To enter a negative number, press the * key first. -10 (default) -57 - 0	
site.cfg	ptt.port	Specify the port values to send and receive audio. 5001 (default) 0 - 65535	
site.cfg	ptt.pageMode.allowOffHookPages	0 (default) - Group pages do not play out on the phone during an active call except for Priority and Emergency pages. 1 - Group pages play out on the handset during an active call.	
site.cfg	ptt.pageMode.codec	The audio codec to use for outgoing group pages. Incoming pages are decoded according to the codec specified in the incoming message. G.722 (default) G.711Mu, G.726QI, or G.722	
site.cfg	ptt.pageMode.defaultGroup	The paging group used to transmit an outgoing page if the user does not explicitly specify a group. 1 (default) 1 to 25	
site.cfg	ptt.pageMode.displayName	This display name is shown in the caller ID field of outgoing group pages. If Null, the value from reg.1.displayName is used. NULL (default) up to 64 octet UTF-8 string	

Push-To-Talk Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	ptt.pageMode.e mergencyGroup	The paging group used for emergency pages. 25 (default) 1 to 25	
site.cfg	ptt.pageMode.p ayloadSize	The page mode audio payload size. 20 (default) 10, 20, ..., 80 milliseconds	
site.cfg	ptt.pageMode.p riorityGroup	The paging group to use for priority pages. 24 (default) 1 to 25	
site.cfg	ptt.pageMode.t ransmit.timeou t.continuation	The time (in seconds) to add to the initial timeout (ptt.pageMode.transmit.timeout.initial) for terminating page announcements. If this value is non-zero, **Extend** displays on the phone. Pressing **Extend** continues the initial timeout for the time specified by this parameter. If 0, announcements cannot be extended. 60 (default) 0 to 65535	
site.cfg	ptt.pageMode.t ransmit.timeou t.initial	The number of seconds to wait before automatically terminating an outgoing page announcement 0 (default) -The page announcements do not automatically terminate. 0 to 65535 - The page announcements automatically terminate.	
site.cfg	ptt.payloadSiz e	Specify the payload size for PTT transmissions. 20 (default) 10, 20, 30, 40, 50, 60, 70, 80	
site.cfg	ptt.priorityCh annel	Specify the channel number to use for priority PTT transmissions. 24 (default) 1 - 25	
site.cfg	ptt.pttMode.en able	0 (default) - PTT is disabled 1 - PTT is enabled.	
site.cfg	ptt.volume	Controls the volume level for pages without changing the volume level for incoming calls. -20 (default) -57 to 0	

Push-To-Talk Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`techsupport.cfg`	`voice.handsetHeadset.rxdg.offset`	This parameter allows a digital Rx boost for the handset and headset. 0 (default) 9 to -12 – Specify the number of decibels to Offset the RxDg range of the handset and headset.	
`techsupport.cfg`	`voice.handsfreePtt.rxdg.offset`	This parameter allows a digital Rx boost for Push-to-Talk. 0 (default) 9 to -12 – Specify the number of decibels to offsets the RxDg range of the handsfree and handsfree Push-to-Talk (PTT).	

Group Paging Parameters

Administrators must enable paging and PTT before users can subscribe to a page group. Use the parameters in the following table to configure this feature.

> Important: The default port used by Group Paging conflicts with the UDP port 5001 used by Polycom® People+Content™ on the RealPresence Trio system. Since the port used by People+Content is fixed and cannot be configured, configure one of the following workarounds:
> - Configure a different port for Group Paging using parameter `ptt.port` or
> - Disable People+Content IP using parameter `content.ppcipServer.enabled="0"`.

Group Paging Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`ptt.address`	The multicast IP address to send page audio to and receive page audio from. 224.0.1.116 (default) multicast IP address.	
`site.cfg`	`ptt.pageMode.displayName`	This display name is shown in the caller ID field of outgoing group pages. If Null, the value from `reg.1.displayName` is used. PTT (default) up to 64 octet UTF-8 string	
`site.cfg`	`ptt.pageMode.enable`	0 (default) - The group paging is disabled. 1 - The group paging is enabled.	

Group Paging Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.c fg	ptt.pageMode.g roup.x.availab le	Make the group available to the user. 1 (default) - Group available to the user is enabled. 0 - Group available to the user is disabled.	
features.c fg	ptt.pageMode.g roup.x.allowRe ceive	1 (default) - The phone can receive pages on the specified group. 0 -The phone cannot receive pages on the specified group.	
features.c fg	ptt.pageMode.g roup.x.allowTr ansmit	Allows outgoing announcements to the group 1 (default) 0	
features.c fg	ptt.pageMode.g roup.x.label	The label to identify the group ch24: Priority,ch25: Emergency, others:Null ch1, 24, 25: 1, others: 0 (default) string	
features.c fg	ptt.pageMode.g roup.x.subscri bed	Subscribe the phone to the group. A page mode group x, where x= 1 to 25. The label is the name used to identify the group during pages. If available is disabled (0), the user cannot access the group or subscribe and the other page mode group parameters is ignored. If enabled, the user can access the group and choose to subscribe. If allowTransmit is disabled (0), the user cannot send outgoing pages to the group. If enabled, the user may send outgoing pages. 1 (default) - If enabled, the phone subscribes to the group. 0 - If disabled, the phone does not subscribe to the group.	
techsuppor t.cfg	voice.ringerPa ge.rxdg.offset	Use this parameter for handsfree paging Rx in high noise environments. 0 (default) 9 to -12 – Raise or lower the volume of the ringer and handsfree page by the specified number of decibels.	

Hoteling Parameters

To enable Hoteling, you must configure Polycom phones with the BroadSoft BroadWorks R17 platform.

You cannot use Hoteling in conjunction with the feature-synchronized automatic call distribution (ACD) feature and you must disable all ACD parameters to use the Hoteling feature. If both features are enabled at the same time, ACD take precedence and the Hoteling GuestIn/GuestOut soft keys do not display. For information, see the section Feature-Synchronized Automatic Call Distribution (ACD).

Use the parameters in the following table to configure Hoteling.

Hoteling Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.hoteling.enabled	0 (default) - Enable Hoteling. 1 - Disable Hoteling.	No
features.cfg	hoteling.reg	Specify the line registration to use for Hoteling. You must disable the Automatic Call Distribution (ACD) feature and all ACD parameters to use Hoteling. 1 (default) 1 - 34	No

SIP-B Automatic Call Distribution Parameters

Use the parameters in the following table to configure this feature.

SIP-B Automatic Call Distribution

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.acdLoginLogout.enabled	0 (default) - Disables the ACD login/logout feature. 1 - Enables the ACD login/logout feature.	Yes
reg-advanced.cfg reg-advanced.cfg	reg.x.acd-login-logout reg.x.acd-agent-available	0 (default) - The ACD feature is disabled for registration. 1 - If both ACD login/logout and agent available are set to 1 for registration x, the ACD feature is enabled for that registration.	No

SIP-B Automatic Call Distribution

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.acd.signalingMethod`	0 (default) - The 'SIP-B' signaling is supported. (This is the older ACD functionality.) 1 - The feature synchronization signaling is supported. (This is the new ACD functionality.)	Yes
features.cfg	`acd.simplifiedAgentStateControl`	0 (default) - Displays menu items. 1 - Hides ASignIN and associated soft keys. Also hides menu items under Menu > Settings > Feature > ACD.	No

ACD Agent Availability Parameters

Use the parameters in this table to configure ACD agent availability for SIP-B Automatic Call Distribution.

ACD Agent Availability

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.acdAgentAvailability.enabled`	0 (default) - Disables the ACD agent available/unavailable feature. 1 - Enables the ACD agent available/unavailable feature.	No
`reg-advanced.cfg`	`reg.x.acd-agent-available`	0 (default) - The ACD feature is disabled for registration. 1 - If both ACD login/logout and agent available are set to 1 for registration x, the ACD feature is enabled for that registration.	No

Feature-Synchronized Automatic Call Distribution Parameters

In addition to the parameters in the following table, you must configure the `feature.enhancedFeaturekeys.enabled` parameter, the `feature.acd*`parameters, and the `acd.reg` and `acd.stateAtSignIn` parameters. If you want to use reason codes, enable `acd.unavailreason.active` and enter the reason codes in the `acd.x.unavailreason.codeName` and `acd.x.unavailreason.codeValue` parameters. You can define up to 100 reason codes.

Use the parameters in the following table to configure this feature.

Feature Synchronized Automatic Call Distribution

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.acdLoginLogout.enabled	0 (default) - Disables the ACD login/logout feature. 1 - Enables the ACD login/logout feature.	Yes
features.cfg	feature.acdAgentAvailability.enabled	0 (default) - Disables the ACD agent available/unavailable feature. 1 - Enables the ACD agent available/unavailable feature.	No
features.cfg	feature.acdPremiumUnavailability.enabled	0 (default) - Disables the premium ACD unavailability feature. 1 - Enables the premium ACD unavailability feature and unavailability reason codes can be used (if the other ACD feature parameters are also be enabled).	Yes
features.cfg	feature.acdServiceControlUri.enabled	0 (default) - Disables the ACD service control URI feature. 1 - Enables the ACD service control URI feature.	Yes
features.cfg, wireless.cfg	acd.reg	Set the registration line index used to support BroadSoft server-based ACD. 1 (default) 1 - 34	Yes
features.cfg, wireless.cfg	acd.stateAtSignIn	1 (default) - The user is available at sign in. 0 - the user is not available at sign in.	No
features.cfg	acd.x.unavailreason.active	This parameter configures the unavailable reason codes used for premium feature-synchronized ACD features, where x is the index of up to 100 codes. 0 (default) - The reason code is inactive. 1 - The reason code is active.	No

Feature Synchronized Automatic Call Distribution

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	acd.x.unavailreason.codeValue	This parameter configures the unavailable reason codes used for premium feature-synchronized ACD features, where x is the index of up to 100 codes. Enter a reason code value, for example, 1000100000. NULL (default) string	Yes
features.cfg	acd.x.unavailreason.codeName	This parameter configures the unavailable reason codes used for premium feature-synchronized ACD features, where x is the index of up to 100 codes. The reason code name, for example, Out to Lunch. NULL (default) string	Yes
sip-interop.cfg	voIpProt.SIP.acd.signalingMethod	0 (default) - The 'SIP-B' signaling is supported. (This is the older ACD functionality.) 1 - The feature synchronization signaling is supported. (This is the new ACD functionality.)	Yes

For details on how to configure phones for feature-synchronized ACD, see *Feature Profile 57216: Using Feature-Synchronized Automatic Call Distribution with Polycom Phones* at Polycom Engineering Advisories and Technical Notifications.

Customize Devices

This section lists parameters that configure enable you to customize devices.

Microbrowser and Web Browser Parameters

You can configure the microbrowser and web browser to display a non-interactive web page on the phone's idle screen, and you can specify an interactive home web page that users can launch in a web browser.

Use the Microbrowser and the Web Browser

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`applications.cfg`	`mb.proxy`	Specify the Application browser home page, a proxy to use, and size limits.	
`applications.cfg`	`mb.idleDisplay.home`	Displays the URL of the microbrowser home page when the microbrowser Home page screen is idle. Null (default) valid HTTP URL, String (maximum 255 characters) For example: `http://www.example.com/xhtml/frontpage`. The microbrowser idle display displaces the idle display indicator.	No
`applications.cfg`	`mb.idleDisplay.refresh`	0 (default) - The microbrowser's idle display does not refresh Integer > 5 - Displays the microbrowser's idle display refresh time period in seconds. If an HTTP Refresh header is detected, it is respected, even if this parameter is set to 0. The refresh parameter is respected only in the event that a refresh fails. Once a refresh is successful, the value in the HTTP refresh header, if available, is used.	No
`applications.cfg`	`mb.idleRefresh.onFailure`	Helps reduce the requests from the phone when the idle display server is unavailable and specifies a delay in seconds when the phone sends refresh requests to the idle browser. This delay applies only when the server returns HTTP 5xx errors. 60 seconds (default) 60 - 655350 seconds To control the refresh times when the server is functioning, use `mb.idleDisplay.refresh`.	No
`applications.cfg`	`mb.main.autoBackKey`	1 (default) - The phone automatically supplies a **Back** soft key in all main browser screens. 0- The phone does not provide a **Back** soft key.	Yes

Use the Microbrowser and the Web Browser

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applications.cfg	mb.main.home	Specifies the URL of the microbrowser's home page. For example: http://www.example.com/xhtml/frontpage/home. Null (default) valid HTTP URL, String (maximum 255 characters)	No
applications.cfg	mb.main.idleTimeout	Specifies the timeout in seconds for the interactive browser. If the interactive browser remains idle for a defined period of time, the phone returns to the idle browser. If set to 0, there is no timeout. 40 (default) 0 - 600	No
applications.cfg	mb.main.loadWebImages	1 (default) - Enables the loading of images in a browser. 0 - Disables the loading of images in a browser.	No
applications.cfg	mb.main.reloadPage	0 (default) - The microbrowser displays the content of the most recently viewed web page 1 - The microbrowser loads the URL configured in mb.main.home each time the browser is launched.	No
applications.cfg	mb.main.statusbar	0 (default) - The status bar does not gets displayed. 1 - The status bar and status messages are displayed.	No
applications.cfg	mb.main.toolbar.autoHide.enabled	1 (default) - The toolbar is not displayed. 0 - The toolbar displays continuously.	No
applications.cfg	mb.main.proxy	Specifies the address of the HTTP proxy to be used by the microbrowser. Null (port: 8080) (default) domain name or IP address in the format <address>:<port>	No
features.cfg	mb.ssawc.enabled	0 (default) - Spontaneous display of web content is disabled. 1 - Spontaneous web content display is enabled.	No

Use the Microbrowser and the Web Browser

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	mb.ssawc.call.mode	passive (default) - Web content is displayed only when requested by the user. Passive mode is recommended when the microbrowser is used for other applications. When passive mode is enabled, an icon displays beside a call appearance indicating that web content is available, and the user can press Select to view the content. Active - Web content is retrieved spontaneously and displayed immediately.	No
applications.cfg	apps.telNotification	Specify the Telephony Event Notification events to be recorded and the URL where notifications are sent.	
applications.cfg	apps.telNotification.callStateChangeEvent	0 (default) - Call state change notification is disabled. 1 - Call state notification is enabled.	No
applications.cfg	apps.telNotification.incomingEvent	0 (default) - Incoming call notification is disabled. 1 - Incoming call notification is enabled.	No
applications.cfg	apps.telNotification.lineRegistrationEvent	0 (default) - Line registration notification is disabled. 1 - Line registration notification is enabled.	No
applications.cfg	apps.telNotification.offhookEvent	0 (default) - Disable off-hook notification. 1 - Enable off-hook notification.	No
applications.cfg	apps.telNotification.onhookEvent	0 (default) - Disable on-hook notification. 1 - Enable on-hook notification.	No
applications.cfg	apps.telNotification.outgoingEvent	0 (default) - Disable outgoing call notification. 1 - Enable outgoing call notification.	No
applications.cfg	apps.telNotification.URL	The URL to which the phone sends notifications of specified events. You can use HTTP or HTTPS. NULL (default) string	No

Use the Microbrowser and the Web Browser

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applications.cfg	apps.telNotification.x.URL	The URL to which the phone sends notifications of specified events, where x 1 to 9. You can use HTTP or HTTPS. NULL (default) string	No
applications.cfg	apps.telNotification.userLogInOutEvent	0 (default) - Disable user login/logout notification. 1 - Enable user login/logout notification.	No
applications.cfg	apps.statePolling	Specify phone state polling settings, such as response mode, the poll URL, and a user name and password.	
applications.cfg	apps.statePolling.password	Enter the password that the phone requires to authenticate phone state polling. NULL (default) string	No
applications.cfg	apps.statePolling.URL	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 parameters apps.statePolling.URL, apps.statePolling.username, and apps.statePolling.password must be set to non-null values. NULL (default) string	No
applications.cfg	apps.statePolling.responseMode	1 (default) - Polled data you request is sent to a configured URL. 0 - Polled data is sent in the HTTP response.	No
applications.cfg	apps.statePolling.username	Enter the user name that the phone requires to authenticate phone state polling. NULL (default) string	No
applications.cfg	apps.push	Specify the push server settings, including message type, port, tunnel, and a user name and password.	

Use the Microbrowser and the Web Browser

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applications.cfg	apps.push.alertSound	0 (default) - There is no sound when an alert is pushed. 1 - There is sound when an alert is pushed.	No
applications.cfg	apps.push.messageType	Choose a priority level for push messages from the application server to the phone. 0 (None) - (default) - Discard push messages 1 (Normal) Allows only normal push messages 2 (Important) Allows only important push messages 3 (High) Allows only priority push messages 4 (Critical) Allows only critical push 5 (All) Allows all push messages	No
applications.cfg	apps.push.password	The password to access the push server URL. NULL (default) string	No
applications.cfg	apps.push.secureTunnelEnabled	1 (default) - The web server is connected through a secure tunnel. 0 - The web server is not connected through a secure tunnel.	No
applications.cfg	apps.push.secureTunnelPort	Specify the port the phone uses to communicate to the web server when the secure tunnel is used. 443 (default) 1 - 65535	No
applications.cfg	apps.push.secureTunnelRequired	1 (default) - Communications to the web server require a secure tunnel. 0 - Communications to the web server do not require a secure tunnel.	No

Use the Microbrowser and the Web Browser

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`applications.cfg`	`apps.push.serverRootURL`	The URL of the application server you enter here is combined with the phone address and sent to the phone's browser. For example, if the application server root URL is `http://172.24.128.85:8080/sampleapps` and the relative URL is `/examples/sample.html`, the URL sent to the microbrowser is `http://172.24.128.85:8080/sampleapps/examples/sample.html`. You can use HTTP or HTTPS. NULL (default) URL	No
`applications.cfg`	`apps.push.username`	The user name to access the push server URL. To enable the push functionality, you must set values for the parameters `apps.push.username` and `apps.push.password` (not null). NULL (default) string	No

Soft Key Parameters

You can create up to 10 custom soft keys. If you configure more soft keys than what can fit on the phone's screen, a **More** soft key displays. Users can use the **More** soft key to display any additional soft keys available.

If you want the phone to display both default and custom soft keys, you can configure them in any order. However, the order in which soft keys display depends on the phone's menu level and call state. If you have configured custom soft keys to display with the default soft keys, the order of the soft keys may change.

The Hold, Transfer, and Conference soft keys are grouped together to avoid usability issues. You may experience errors if you try to insert a soft key between these three grouped soft keys.

The following table shows you the parameters for configuring soft keys. Note that this feature is part of enhanced feature keys (EFK), and you must enable the EFK parameters to configure soft keys. See the section Enhanced Feature Keys for details about configuring soft keys and line keys.

Configure Soft Keys

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.enhancedFeatureKeys.enabled	0 (default) - Disables the enhanced feature keys feature. 1 - Enables the enhanced feature keys feature.	No
features.cfg	softkey.x.action	Controls the action or function for the custom soft key x. Null (default) macro action string, 2048 characters This value uses the same macro action string syntax as an Enhanced Feature Key. For a list of actions, see Macro Definitions.	No
features.cfg	softkey.x.enable	0 (default) - The x soft key is disabled. 1 - The x soft key is enabled.	No
features.cfg	softkey.x.insert	0 (default) - The phone places the soft key in the first available position. 0 to 10 - The phone places the soft key in the corresponding position and moves the following soft keys by one position to the right. For example, if the soft key is set to 3, the soft key is displayed in the third position from the left. If the soft key already exists in the third position, it is moved to fourth position and the following soft keys are moved to right by one space. If softkey.x.precede is configured, this value is ignored. If the insert location is greater than the number of soft keys, the key is positioned last after the other soft keys.	No

Configure Soft Keys

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	softkey.x.label	The text displayed on the soft key label. If Null, the label is determined as follows: • If the soft key performs an Enhanced Feature Key macro action, the label of the macro defined using efk.efklist is used. • If the soft key calls a speed dial, the label of the speed dial contact is used. • If the soft key performs chained actions, the label of the first action is used. • If the soft key label is Null and none of the preceding criteria are matched, the label is blank. Null (default) String Note that the maximum number of characters for this parameter value is 16; however, the maximum number of characters that a phone can display on its user interface varies by phone model and by the width of the characters used. Parameter values that exceed the phone's maximum display length are truncated by ellipses (…). The phone truncates the beginning of numerical labels (for example, …4567) and truncates the end of alphabetical labels (for example, Abcd…).	No
features.cfg	softkey.x.precede	0 (default) - The phone locates the soft key in the first available position from left. 1 - The phone locates the soft key before the default soft key position.	No
features.cfg	softkey.x.use	Specify which call states the soft key displays in.	
features.cfg	softkey.x.use.active	0 (default) - Does not display the soft key x during an active call. 1 - Displays the soft key x during an active call.	No

Configure Soft Keys

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`softkey.x.use.alerting`	0 (default) - Does not display the soft key x in an alerting state during an active call. 1 - Displays the soft key x in an alerting state during an active call.	No
`features.cfg`	`softkey.x.use.dialtone`	0 (default) - Does not display the soft key in the dial tone state during an active call. 1 - Displays the soft key x in the dial tone state during an active call.	No
`features.cfg`	`softkey.x.use.hold`	0 (default) - Does not display the soft key x in the hold state during an active call. 1 - Displays the soft key x in the hold state during an active call.	No
`features.cfg`	`softkey.x.use.idle`	0 (default) - Does not display the soft key x in the idle state during an active call. 1 - Displays the soft key x in the idle state during an active call.	No
`features.cfg`	`softkey.x.use.park`	0 (default) - Does not display the soft key x in the parked state during an active call. 1 - Displays the soft key x in the parked state during an active call.	No
`features.cfg`	`softkey.x.use.proceeding`	0 (default) - Does not display the soft key x in the proceeding state during an active call. 1 - Displays the soft key x in the proceeding state during an active call.	No
`features.cfg`	`softkey.x.use.setup`	0 (default) - Does not display the soft key x in the setup state during an active call. 1 - Displays the soft key x in the setup state during an active call.	No
`features.cfg`	`softkey.feature.`	To display soft keys for various phone features, including default soft keys.	
`features.cfg`	`softkey.feature.intercom`	1 (default) - Enables the **Intercom** soft key. 0 - Disables the **Intercom** soft key.	No

Configure Soft Keys

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	softkey.feature.doNotDisturb	1 (default) – Enables the DND soft key on the phone. 0 – Disables the DND soft key on the phone.	
features.cfg	softkey.feature.basicCallManagement.redundant	1 (default) - Displays the **Hold**, **Transfer**, and **Conference** soft keys. 0 - Does not display the **Hold**, **Transfer**, and **Conference** soft keys.	No
features.cfg	softkey.feature.buddies	1 (default) - Displays the **Buddies** soft key. 0 - Does not display the **Buddies** soft key.	No
features.cfg	softkey.feature.callers	0 (default) - Displays the **Callers** soft key for all platforms. 1 - Does not display the **Callers** soft key for all platforms.	No
features.cfg	softkey.feature.directories	1 (default) - Displays the Directories (Dir) soft key. 0 - Does not display the Directories (Dir) soft key.	Yes
features.cfg	softkey.feature.doNotDisturb	1 (default) - Enables the **DND** soft key. 0 - Disables the **DND** soft key.	No
features.cfg	softkey.feature.endcall	1 (default) - Displays the **End Call** soft key. 0 - Does not display the **End Call** soft key.	No
features.cfg	softkey.feature.forward	1 (default) - Displays the **Forward** soft key. 0 - Does not display the **Forward** soft key.	No
features.cfg	softkey.feature.join	1 (default) - Displays the **Join** soft key. 0 - Does not display the **Join** soft key.	No
features.cfg	softkey.feature.mystatus	1 (default) - Displays the **MyStatus** soft key (if pres.idleSoftKeys is set to 1). 0 - Does not display the **MyStatus** soft key.	No
features.cfg	softkey.feature.newcall	1 (default) - Displays the **New Call** soft key is displayed. 0 - Does not display the **New Call** soft key.	No

Configure Soft Keys

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	softkey.feature.redial	0 (default) - Displays the Redial soft key. 1 - Does not display the Redial soft key. The parameter feature.enhancedFeatureKeys.enabled must be set to 1 first to configure this feature, and the parameter efk.softkey.alignleft must be set to 1 to move enabled soft keys into the positions of disabled soft keys.	No
features.cfg	softkey.feature.split	1 (default) - Displays the **Split** soft key to split the conference call to individual calls. 0 - Does not display the **Split** soft key.	No

Enhanced Feature Keys Parameters

The rules for configuring EFK for line keys, soft keys, and hard keys vary. Before configuring EFK, refer to Macro Definitions to become familiar with the macro language.

Note that the configuration file changes and the enhanced feature key definitions can be included together in one configuration file. However, Polycom recommends creating a new configuration file to make configuration changes.

See the following table for the parameters you can configure and a brief explanation of how to use the contact directory to configure line keys.

Enhanced Feature Keys Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced .cfg	reg.x.callsPerLineKey	Set the maximum number of concurrent calls for a single registration x. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all phones sharing that registration. This per-registration parameter overrides call.callsPerLineKey. 24 (default) 1-24 VVX 101, 201 8 (default) 1 - 8	No
features.cfg	feature.enhancedFeatur eKeys.enabled	0 (default) - Disables the enhanced feature keys feature. 1 - Enables the enhanced feature keys feature.	No
features.cfg	efk.efklist.x.action.s tring	The action string contains a macro definition of the action that the feature key performs. Null (default) String (maximum of 64 characters) If EFK is enabled, this parameter must have a value (it cannot be Null). For a list of macro definitions and example macro strings, see Macro Definitions.	No
features.cfg	efk.efklist.x.label	The text string used as a label on any user text entry screens during EFK operation. Null (default) - The Null string is used. String (maximum of 64 characters) If the label does not fit on the screen, the text is shortened and '…' is appended.	No
features.cfg	efk.efklist.x.mname	The unique identifier used by the speed dial configuration to reference the enhanced feature key entry. Cannot start with a digit. Note that this parameter must have a value, it cannot be Null. expanded_macro (default) String (maximum of 64 characters)	No

Enhanced Feature Keys Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	efk.efklist.x.status	0 (default) - Disables the key x. Null - Disables the key x. 1 -Enables the key x.	No
features.cfg	efk.efklist.x.type	The SIP method to be performed. invite (default) - Performs the required action using the SIP INVITE method. Null - default of INVITE is used. This parameter is included for backwards compatibility. Do not use if possible. If efk.x.action.string contains types, this parameter is ignored.	No
features.cfg	efk.efkprompt.x.label	The prompt text on the user prompt screen. Null (default) - No prompt displays. String If the label does not fit on the screen, the label is shortened and '…' is appended.	Yes
features.cfg	efk.efkprompt.x.status	This parameter must have a value, it cannot be Null. 0 (default) - Disables the key. 1 - Enabled the key. If a macro attempts to use a prompt that is disabled or invalid, the macro execution fails.	Yes

Enhanced Feature Keys Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	efk.efkprompt.x.type	The type of characters entered by the user. text (default) - The characters are interpreted as letters. numeric - The characters are interpreted as numbers. If Null, numeric is used. If this parameter has an invalid value, this prompt, and all parameters depending on this prompt, are invalid. Note: A mix of numeric and text is not supported.	Yes
features.cfg	efk.efkprompt.x.userfeedback	The user input feedback method. visible (default) - The text is visible. masked - The text displays as asterisk characters (*), which can be used to mask password fields. If Null, visible is used. If this parameter has an invalid value, this prompt, and all parameters depending on this prompt, are invalid.	Yes

Flexible Line Keys Parameters

Line keys that you configure using this feature override the default line key assignments as well as any custom line key configurations you may have made. To use this feature, you need to specify the function of each line key on the phone. You do this by assigning a category (lineKey.x.category) and an index (lineKey.x.index) to each line key, both of which are explained in the Enhanced Feature Key Example Configurations.

Use the parameters in the following table to configure this feature.

Flexible Line Keys Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced .cfg`	`lineKey.reassignment.e nabled`	Specify at least two calls per line key. 0 (default) - Disable the flexible line key assignment. 1 - Enable the flexible line key assignment.	Yes
`reg-advanced .cfg`	`lineKey.x.category`	Specify the line key category. Unassigned (default) Line BLF SpeedDial Presence	Yes
`reg-advanced .cfg`	`lineKey.x.index`	Specify the line key number (dependent on category). 0 (default) - The index value for BLF or presence. 0- 9999	Yes

Phone Keypad Parameters

You can configure phone keys in the following ways:

- Assign a function or feature to a key
- Turn a phone key into a speed dial
- Assign enhanced feature key (EFK) operations to a phone key

  For example, you can map a phone menu path to a single key press using a macro code. See Enhanced Feature Keys.

- Delete all functions and features from a phone key

Use the parameters in the following table to change the layout of your phone's keypad.

Phone Keypad Parameters

Template	Parameters	Permitted Values	Change Causes Restart or Reboot
features.cfg	key.x.function.prim	Set the primary key function for key y on phone model x. Null (default) String (maximum of 255 characters)	No
features.cfg	key.x.subPoint.prim	Set the secondary key function for key y on phone model x. Null (default) String (maximum of 255 characters)	No

Network

This section lists parameters that configure network settings.

Two-Way Active Measurement Protocol Configuration Parameters

The following table includes the new or modified parameters for the two-way active measurement protocol feature.

Two-Way Active Measurement Protocol Configuration Parameters

Template	Parameters	Permitted Values	Change Causes Restart or Reboot
site.cfg	feature.twamp.enabled	0 (default) - Disable TWAMP protocol support. 1 - Enable TWAMP protocol support.	No
site.cfg	twamp.port.udp.PortRangeEnd	Set the TWAMP UDP session max port range value. 60000 (default) 1024 - 65486	No

Two-Way Active Measurement Protocol Configuration Parameters

Template	Parameters	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`twamp.port.udp.Port RangeStart`	Set the TWAMP UDP session start port range value. 40000 (default) 1024 - 65485	No
`site.cfg`	`twamp.udp.maxSessio n`	Set the maximum UDP session supported by TWAMP. 1 (default) 1 - 10	No

3GPP Technical Specifications Parameters

Use the 3GPP parameters in the following table to figure IMS features.

3GPP Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`nat.keepalive.tcp .payload`	Configure a customizable string as the payload of a TCP keep-alive message. The string value cannot be blank. CRLFCRLFCRLFCRLFCRLFC RLFCRLFCRLF (default)	No
`sip-interop.cfg`	`nat.keepalive.udp .payload`	Configure a customizable string as the payload of a UDP keep-alive message. You can leave the string value blank to configure an empty payload. CRLFCRLF (default)	No
`reg-advanced.cfg`	`reg.x.header.pear lymedia.support`	0 (Default) - The p-early-media header is not supported on the specified line registration. 1 - The p-early-media header is supported by the specified line registration.	No
`reg-basic.cfg`	`reg.X.insertOBPAd dressInRoute`	1 (Default) - The outbound proxy address is added as the topmost route header. 0 - The outbound proxy address is not added to the route header.	No

3GPP Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	reg.x.path	0 (Default) - The path extension header field in the Register request message is not supported for the specific line registration. 1 - The phone supports and provides the path extension header field in the Register request message for the specific line registration.	No
features.cfg	reg.x.regevent	0 (default) - The phone is not subscribed to registration state change notifications for the specific phone line. 1 - The phone is subscribed to registration state change notifications for the specific phone line. This parameter overrides the global parameter voIpProt.SIP.regevent.	No
reg-advanced.cfg	reg.x.rejectNDUBInvite	Specify whether or not the phone accepts a call for a particular registration in case of a Network Determined User Busy (NDUB) event advertised by the SIP server. 0 (Default) - If an NDUB event occurs, the phone does not reject the call. 1 - If an NDUB event occurs, the phone rejects the call with a 603 Decline response code.	No

3GPP Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	reg.x.server.y.sp ecialInterop	Specify the server-specific feature set for the line registration. Standard (Default) VVX 101: Standard GENBAND ALU-CTS DT VVX 201: Standard, GENBAND ALU-CTS ocs2007r2 lync2010 All other phones: Standard GENBAND ALU-CTS ocs2007r2 lync2010 lcs2005	
features.cfg	voice.qualityMoni toring.processSer viceRoute.enable	0 (Default) - The VQMon messages generated by the phone do not contain service route information in SIP route headers. 1 - The VQMon messages generated by the phone contain service route information, if available, in SIP route headers.	Yes
sip-interop.cfg	voIpProt.SIP.head er.pEarlyMedia.su pport	0 (Default) - The p-early-media header is not supported by the caller phone. 1 - The p-early-media header is supported by the caller phone.	

3GPP Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SIP.IMS.enable	This parameter applies to all registered or unregistered SIP lines on the phone. 0 (Default) - The phone does not support IMS features introduced in UC Software 5.5.0. 1 - The phone supports IMS features introduced in UC Software 5.5.0.	
features.cfg	voIpProt.SIP.regevent	0 (default) - The phone is not subscribed to registration state change notifications for all phone lines. 1 - The phone is subscribed to registration state change notifications for all phone lines. This parameter is overridden by the per-phone parameter reg.x.regevent.	
sip-interop.cfg	voIpProt.SIP.rejectNDUBInvite	Specify whether or not the phone accepts a call for all registrations in case of a Network Determined User Busy (NDUB) event advertised by the SIP server. 0 (Default) - If an NDUB event occurs, the phone does not reject the call for all line registrations. 1 - If an NDUB event occurs, the phone rejects the call with a 603 Decline response code for all line registrations.	
reg-basic.cfg	voIpProt.SIP.supportFor199	Determine support for the 199 response code. For details on the 199 response code, see RFC 6228. 0 (Default) - The phone does not support the 199 response code. 1- The phone supports the 199 response code.	

TR-069 Parameters

Polycom provides parameters for the TR-104 and TR-106 data models that support provisioning of TR-069-enabled devices by an Auto-Configuration Server (ACS). TR-104 is a parameter data model for VoIP-only devices, and TR-106 is a parameter data model for all TR-069-enabled devices.

Use the parameters in the following table to configure this feature.

TR-069 Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg; tr069.cfg`	`device.feature.tr069.en abled`	0 (default) - Disables TR-069 feature 1 - Enables TR-069 feature	No
`device.cfg; tr069.cfg`	`device.feature.tr069.en abled.set`	0 (default) 1	No
`tr069.cfg`	`device.tr069.acs.passwo rd`	Sets the TR-069 ACS server password used to authenticate the phone. `Null` (default) String (256 maximum characters)	No
`tr069.cfg`	`device.tr069.acs.url`	Sets the URL for the TR-069 ACS server. `Null` (default) URL (256 maximum characters)	No
`tr069.cfg`	`device.tr069.acs.userna me`	Sets the TR-069 ACS server user name used to authenticate the phone. `PlcmSpip` (default) String (256 maximum characters)	No
`tr069.cfg`	`device.tr069.cpe.passwo rd`	Specifies the TR-069 CPE password, which authenticates a connection request from the ACS server. `Null` (default) String (256 maximum characters)	No

TR-069 Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
tr069.cfg	device.tr069.cpe.username	Specifies the TR-069 CPE user name, which authenticates a connection request from the ACS server. PlcmSpip (default) String (256 maximum characters)	No
tr069.cfg	device.tr069.periodicInform.enabled	Indicates whether the CPE must periodically send CPE information to ACS using the Inform method call. 0 (default) - Periodic Inform call is disabled. 1 - Periodic Inform call is enabled.	No
tr069.cfg	device.tr069.periodicInform.interval	Specifies the time interval in seconds in which the CPE must attempt to connect with the ACS to send CPE information if device.tr069.periodicInform.enabled ="1". 18000 (default) 0 to 36000	No
tr069.cfg	device.tr069.upgradesManaged.enabled	Indicates whether the ACS manages image upgrades for the phone or not. 0 (default) - The phone uses ACS or provisioning server for upgrade. 1 - The phone upgrades only from the ACS server.	No
tr069.cfg	log.level.change.tr069	Sets the log levels for the TR-069 feature. 4 (default) 0 - 6	No

Advice of Charge Parameters

The following parameters configure the Advice of Charge (AoS) feature. Before configuring AoS parameters, you must set `voIpProt.SIP.IMS.enable to 1`.

Advice of Charge Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.aoc.enable`	0 (Default) - The phone does not display call charge information. 1 - The phone displays call charge information.	No
`features.cfg`	`feature.adviceOfCharge.allowAudioNotification`	0 (Default) - There is no audio beep sound when the call charges information is updated on the phone display. 1 - The phone gives an audio beep when the call charges information is updated on the phone display.	No

IPv6 Parameters

Use the parameters in the following table to enable and configure IPv6.

IPv6 Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, site.cfg	device.dhcp.bootSrvUseOpt	Specifies the source for the boot server address for the phone. It can take values from 0 to 9. In IPv4 mode, the following values are applicable: • 0 (Default) - The phone gets the boot server address from Option 66. • 1 - The phone gets the boot server details from the custom option number provided through DHCP. • 2 - The phone uses the boot server configured through the Server Menu. • 3 - The phone uses the custom option first or uses Option 66 if the custom option is not present In IPv6 mode, the following values are applicable: • 4 - The phone uses the boot server configured through the Server menu. • 5 - The phone uses the boot server option provided through DHCPv6. In Dual Stack Mode (IPv4/IPv6 mode), the following values are applicable: • 6 - The phone uses the boot server configured through the Server menu. • 7 - The phone gets the boot server details from DHCPv6 option or the Option 66 on DHCP server. • 8 - The phone gets the boot server details through DHCPv6 or through the custom option configured on DHCP server for the provisioning. • 9 - The phone gets the boot server from DHCPv6 option or custom option or option 66 configured on DHCP server for the provisioning.	No
device.cfg; wireless.cfg	device.ipv6.icmp.echoReplies	NULL (default) 0 1	No
device.cfg; wireless.cfg	device.ipv6.icmp.echoReplies.set	0 (default) 1	No

IPv6 Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg; wireless.cfg`	`device.ipv6.icmp.g enDestUnreachable`	0 1	No
`device.cfg; wireless.cfg`	`device.ipv6.icmp.g enDestUnreachable. set`	0 1	No
`device.cfg; wireless.cfg`	`device.ipv6.icmp.i gnoreRedirect`	0 1	No
`device.cfg; wireless.cfg`	`device.ipv6.icmp.i gnoreRedirect.set`	0 1	No
`device.cfg; wireless.cfg`	`device.ipv6.icmp.t xRateLimiting`	0 1	No
`device.cfg; wireless.cfg`	`device.ipv6.icmp.t xRateLimiting.set`	0 - 6000	No
`device.cfg, site.cfg`	`device.net.ipStack`	Configures the IPv4, IPv6, or dual stack mode for the phone. `0` (Default) - IPv4 is enabled and IPv6 is disabled. `1` - IPv6 is enabled and IPv4 is disabled. `2` - Dual stack is enabled and phone operates on both IPv4 and IPv6 networks at the same time.	No
`device.cfg, site.cfg`	`device.net.ipv6Add rDisc`	Specify whether the IPv6 address and related parameters for the phone are obtained from DHCPv6 or SLAAC or statically configured for the phone. `1` (Default) -IPv6 global address and options are configured from DHCPv6. `2` - IPv6 global address is configured using prefixes received from Router Advertisements (RA) and options are configured from stateless DHCPv6. `0` - IPv6 global address and options must be configured manually.	No
`device.cfg, site.cfg`	`device.net.ipv6Add ress`	Specify a valid global IPv6 unicast address for the phone. Null (default)	No
`device.cfg, site.cfg`	`device.net.ipv6Gat eway`	Specify theIPv6 address of the default gateway for the phone. Null (default)	No

IPv6 Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, site.cfg	device.net.ipv6LinkAddress	Specifies a valid Link Local IPv6 address for the phone. Null (default)	No
device.cfg, site.cfg	device.net.ipv6PrivacyExtension	Configure whether or not the IPv6 global and link local addresses are in 64-bit Extended Unique Identifier (EUI-64) format. 0 (Default) - IPv6 global and link local addresses are in EUI-64 format. 1 - Global and link local IPv6 addresses are not in EUI-64 format. Instead, the last 48 bits for the IPv6 address are generated randomly.	No
device.cfg, site.cfg	device.net.ipv6ULAAddress	Specifies a valid Unique Local IPv6 address (ULA) for the phone. Null (default)	No
device.cfg, site.cfg	device.net.preferredNetwork	Specify IPv4 or IPv6 as the preferred network in a Dual Stack mode. 1 (default) - Specifies IPv6 as a preferred network. 0 - Specifies IPv4 as a preferred network.	No
device.cfg, site.cfg	ipv6.mldVersion	1 2 (default)	No
sip-interop.cfg	voipProt.SIP.anat.enabled	Enables or disables Alternative Network Address Types (ANAT). 0 (default) - ANAT is disabled. 1 - ANAT is enabled.	No

RTP Ports Parameters

Use the parameters in the following table to configure RTP packets and ports.

Configure Real-Time Transport Protocol Ports

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.port.rtp.filterByIp[1]	IP addresses can be negotiated through the SDP or H.323 protocols. 1 (Default) - Phone rejects RTP packets that arrive from non-negotiated IP addresses. The H.323 protocol is supported on the VVX 500/501, 600/601, and 1500 phones.	Yes
site.cfg	tcpIpApp.port.rtp.filterByPort[1]	Ports can be negotiated through the SDP protocol. 0 (Default) 1 - Phone rejects RTP packets arriving from (sent from) a non-negotiated port.	Yes
site.cfg	tcpIpApp.port.rtp.forceSend[1]	Send all RTP packets to, and expect all RTP packets to arrive on, this port. Range is 0 to 65535. 0 (Default) - RTP traffic is not forced to one port. Both tcpIpApp.port.rtp.filterByIp and tcpIpApp.port.rtp.filterByPort must be set to 1.	Yes
site.cfg	tcpIpApp.port.rtp.mediaPortRangeStart[1]	Set the starting port for RTP port range packets. Use an even integer ranging from 1024 to 65440. 2222 (Default) Each call increments the port number +2 to a maximum of 24 calls after the value resets to the starting point. Because port 5060 is used for SIP signaling, ensure that port 5060 is not within this range when you set this parameter. A call that attempts to use port 5060 has no audio.	Yes

Network Address Translation Parameters

You can configure the external IP addresses and ports used by the NAT on the phone's behalf on a per-phone basis. Use the parameters in the following table to configure NAT.

Network Access Translation Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`nat.ip`	Specifies the IP address to advertise within SIP signaling. This should match the external IP address used by the NAT device. Null (default) IP address	Yes
`sip-interop.cfg`	`nat.keepalive.interval`	The keep-alive interval in seconds. Sets the interval at which phones sends a keep-alive packet to the gateway/NAT device to keep the communication port open so that NAT can continue to function. If Null or 0, the phone does not send out keep-alive messages. 0 (default) 0 - 3600	No
`sip-interop.cfg`	`nat.mediaPortStart`	The initially allocated RTP port. Overrides the value set for `tcpIpApp.port.rtp.mediaPortRangeStart` parameter. 0 (default) 0 - 65440	Yes
`sip-interop.cfg`	`nat.signalPort`	The port used for SIP signaling. Overrides the `voIpProt.local.port` parameter. 0 (default) 1024 - 65535	No

Server Redundancy Parameters

Use the parameters in the following table to set up server redundancy for your environment.

Set Up Server Redundancy

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.server.x.failOver.failBack.mode`	Specify the failover failback mode. duration (default) - The phone tries the primary server again after the time specified by `voIpProt.server.x.failOver.failBack.timeout` newRequests - All new requests are forwarded first to the primary server regardless of the last used server. DNSTTL - The phone tries the primary server again after a timeout equal to the DNS TTL configured for the server that the phone is registered to. registration - The phone tries the primary server again when the registration renewal signaling begins.	No
`sip-interop.cfg`	`voIpProt.server.x.failOver.failBack.timeout`	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 result in a timeout of 60 and 0 means do not fail-back until a fail-over event occurs with the current server. 3600 (default) 0, 60 to 65535	No
`sip-interop.cfg`	`voIpProt.server.x.failOver.failRegistrationOn`	1 (default) - When set to 1, and the reRegisterOn parameter is enabled, the phone silently invalidates an existing registration (if it exists), at the point of failing over. 0 - When set to 0, and the reRegisterOn parameter is enabled, existing registrations remain active. This means that the phone attempts failback without first attempting to register with the primary server to determine if it has recovered.	No

Set Up Server Redundancy

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.server.x.failOver.onlySignalWithRegistered	1 (default) - When set to 1, and the reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. If the phone attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call ends. No SIP messages are sent to the unregistered server. 0 - When set to 0, and the reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred).	No
sip-interop.cfg	voIpProt.server.x.failOver.reRegisterOn	0 (default) - When set to 0, the phone won't attempt to register with the second. 1 - When set to 1, the phone attempts to register with (or by, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling proceeds with the secondary server.	No
reg-advanced.cfg	reg.x.auth.optimizedInFailover	The destination of the first new SIP request when failover occurs. 0 (default) - The SIP request is sent to the server with the highest priority in the server list. 1 - The SIP request is sent to the server which sent the proxy authentication request.	No

Set Up Server Redundancy

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`reg.x.outboundProxy.failOver.failBack.mode`	The mode for failover failback (overrides `reg.x.server.y.failOver.failBack.mode`). duration - (default) The phone tries the primary server again after the time specified by `reg.x.outboundProxy.failOver.failBack.timeout` expires. newRequests - All new requests are forwarded first to the primary server regardless of the last used server. DNSTTL - The phone tries the primary server again after a timeout equal to the DNS TTL configured for the server that the phone is registered to.	No
`reg-advanced.cfg`	`reg.x.outboundProxy.failOver.failBack.timeout`	3600 (default) -The time to wait (in seconds) before failback occurs (overrides `reg.x.server.y.failOver.failBack.timeout`). 0, 60 to 65535 - The phone does not fail back until a failover event occurs with the current server.	No
`reg-advanced.cfg`	`reg.x.outboundProxy.failOver.failRegistrationOn`	1 (default) - The reRegisterOn parameter is enabled, the phone silently invalidates an existing registration. 0 - The reRegisterOn parameter is enabled, existing registrations remain active.	No
`reg-advanced.cfg`	`reg.x.outboundProxy.failOver.onlySignalWithRegistered`	1 (default) - The reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. 0 - The reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed.	No

Set Up Server Redundancy

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.outboundProxy.failOver.reRegisterOn`	This parameters overrides `reg.x.server.y.failOver.reRegisterOn`. 0 (default) - The phone won't attempt to register with the secondary server. 1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server.	No
`reg-advanced.cfg`	`reg.x.outboundProxy.port`	The port of the SIP server to which the phone sends all requests. 0 - (default) 1 to 65535	No
`reg-advanced.cfg`	`reg.x.outboundProxy.transport`	The transport method the phone uses to communicate with the SIP server. DNSnaptr (default) DNSnaptr, TCPpreferred, UDPOnly, TLS, TCPOnly	No

Static DNS Parameters

Use the following table to configure static DNS settings.

Static DNS Cache Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-basic.cfg`	`reg.x.address`	The user part (for example, 1002) or the user and the host part (for example, `1002@polycom.com`) of the registration SIP URI or the H.323 ID/extension. Null (default) string address	No
`sip-interop.cfg`	`reg.x.server.y`	Specify the call server used for this registration.	

Static DNS Cache Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	reg.x.server.y.specialInterop	Specify the server-specific feature set for the line registration. Standard (Default) VVX 101: Standard GENBAND ALU-CTS DT VVX 201: Standard, GENBAND ALU-CTS ocs2007r2 lync2010 All other phones: Standard GENBAND ALU-CTS ocs2007r2 lync2010 lcs2005	
site.cfg	reg.x.server.y.address	If this parameter is set, it takes precedence even if the DHCP server is available. Null (default) - SIP server does not accepts registrations. IP address or hostname - SIP server that accepts registrations. If not Null, all of the parameters in this table override the parameters specified in voIpProt.server.*	No
reg-advanced	reg.x.server.y.expires	The phone's requested registration period in seconds. The period negotiated with the server may be different. The phone attempts to re-register at the beginning of the overlap period. 3600 - (default) positive integer, minimum 10	No

Static DNS Cache Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced	reg.x.server.y.expires.lineSeize	Requested line-seize subscription period. 30 - (default) 0 to 65535	No
reg-advanced	reg.x.server.y.expires.overlap	The number of seconds before the expiration time returned by server x at which the phone should try to re-register. The phone tries to re-register at half the expiration time returned by the server if the server value is less than the configured overlap value. 60 (default) 5 to 65535	No
site.cfg	reg.x.server.y.failOver.failBack.mode	duration (default) - The phone tries the primary server again after the time specified by reg.x.server.y.failOver.failBack.timeout. newRequests - All new requests are forwarded first to the primary server regardless of the last used server. DNSTTL - The phone tries the primary server again after a timeout equal to the DNS TTL configured for the server that the phone is registered to. registration - The phone tries the primary server again when the registration renewal signaling begins. This parameter overrides voIpProt.server.x.failOver.failBack.mode)	No
site.cfg	reg.x.server.y.failOver.failBack.timeout	3600 (default) - The time to wait (in seconds) before failback occurs. 0 - The phone does not fail back until a failover event occurs with the current server. 60 to 65535 - If set to Duration, the phone waits this long after connecting to the current working server before selecting the primary server again.	No

Static DNS Cache Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	reg.x.server.y.failOver.failRegistrationOn	1 (default) - The reRegisterOn parameter is enabled, the phone silently invalidates an existing registration (if it exists), at the point of failing over. 0 - The reRegisterOn parameter is disabled, existing registrations remain active.	No
site.cfg	reg.x.server.y.failOver.onlySignalWithRegistered	1 (default) - Set to this value and reRegisterOn and failRegistrationOn parameters are enabled, no signaling is accepted from or sent to a server that has failed until failback is attempted or failover occurs. If the phone attempts to send signaling associated with an existing call via an unregistered server (for example, to resume or hold a call), the call ends. No SIP messages are sent to the unregistered server. 0 - Set to this value and reRegisterOn and failRegistrationOn parameters are enabled, signaling is accepted from and sent to a server that has failed (even though failback hasn't been attempted or failover hasn't occurred).	No
site.cfg	reg.x.server.y.failOver.reRegisterOn	0 (default) - The phone does not attempt to register with the secondary server, since the phone assumes that the primary and secondary servers share registration information. 1 - The phone attempts to register with (or via, for the outbound proxy scenario), the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling proceeds with the secondary server. This parameter overrides voIpProt.server.x.failOver.reRegisterOn.	No
site.cfg	reg.x.server.y.port	Null (default) - The port of the SIP server does not specifies registrations. 0 - The port used depends on reg.x.server.y.transport. 1 to 65535 - The port of the SIP server that specifies registrations.	No

Static DNS Cache Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`reg.x.server.y.register`	1 (default) - Calls can not be routed to an outbound proxy without registration. 0 - Calls can be routed to an outbound proxy without registration. See voIpProt.server.x.register for more information, see *SIP Server Fallback Enhancements on Polycom Phones - Technical Bulletin 5844* on Polycom Engineering Advisories and Technical Notifications.	No
`sip-interop.cfg`	`reg.x.server.y.registerRetry.baseTimeOut`	For registered line x, set y to the maximum time period the phone waits before trying to re-register with the server.Used in conjunction with `reg.x.server.y.registerRetry.maxTimeOut` to determine how long to wait. 60 (default) 10 - 120 seconds	No
`sip-interop.cfg`	`reg.x.server.y.registerRetry.maxTimeout`	For registered line x, set y to the maximum time period the phone waits before trying to re-register with the server. Use in conjunction with `reg.x.server.y.registerRetry.baseTimeOut` to determine how long to wait. The algorithm is defined in RFC 5626. 180 - (default) 60 - 1800 seconds	No
`reg-advanced.cfg`	`reg.x.server.y.retryMaxCount`	The number of retries attempted before moving to the next available server. 3 - (default) 0 to 20 - 3 is used when the value is set to 0.	No
`reg-advanced.cfg`	`reg.x.server.y.retryTimeOut`	0 (default) - Use standard RFC 3261 signaling retry behavior. 0 to 65535 - The amount of time (in milliseconds) to wait between retries.	No

Static DNS Cache Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.c fg`	`reg.x.server.y.subscri be.expires`	The phone's requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period. 3600 seconds - (default) 10 – 2147483647 (seconds) You can use this parameter in conjunction with `reg.x.server.y.subscribe.expires. overlap`.	No
`reg-advanced.c fg`	`reg.x.server.y.subscri be.expires.overlap`	The number of seconds before the expiration time returned by server x after which the phone attempts to resubscribe. If the server value is less than the configured overlap value, the phone tries to resubscribe at half the expiration time returned by the server. 60 seconds (default) 5 – 65535 seconds	No
`site.cfg`	`reg.x.server.y.transpo rt`	The transport method the phone uses to communicate with the SIP server. DNSnaptr (default) - If `reg.x.server.y.address` is a hostname and `reg.x.server.y.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.server.y.address` is an IP address, or a port is given, then UDP is used. TCPpreferred - TCP is the preferred transport; UDP is used if TCP fails. UDPOnly - Only UDP is used. TLS - If TLS fails, transport fails. Leave port field empty (defaults to `5061`) or set to `5061`. TCPOnly - Only TCP is used.	No
`site.cfg`	`reg.x.server.y.useOutb oundProxy`	1 (default) - Enables to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x. 0 - Disable to use the outbound proxy specified in `reg.x.outboundProxy.address` for server x.	No

Static DNS Cache Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	divert.x.sharedDisabled	1 (default) - Disables call diversion features on shared lines. 0 - Enables call diversion features on shared lines.	Yes
site.cfg	dns.cache.A.x.	Specify the DNS A address, hostname, and cache time interval.	
site.cfg	dns.cache.A.x.address	Null (default) IP version 4 address	No
site.cfg	dns.cache.A.x.name	Null (default) valid hostname	No
site.cfg	dns.cache.A.x.ttl	The TTL describes the time period the phone uses the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry and it resets TTL timer again. 300 (default) 300 to 536870912 (2^29), seconds	No
site.cfg	dns.cache.NAPTR.x.	Specify the DNS NAPTR parameters, including: name, order, preference, regexp, replacement, service, and ttl.	
site.cfg	dns.cache.NAPTR.x.flags	The flags to control aspects of the rewriting and interpretation of the fields in the record. Characters are case-sensitive. At this time, only 'S', 'A', 'U', and 'P' are defined as flags. See RFC 2915 for details of the permitted flags. Null (default) A single character from [A-Z, 0-9]	No
site.cfg	dns.cache.NAPTR.x.name	Null (default) domain name string - The domain name to which this resource record refers.	No
site.cfg	dns.cache.NAPTR.x.order	0 (default) 0 to 65535 - An integer that specifies the order in which the NAPTR records must be processed to ensure the correct ordering of rules.	No

Static DNS Cache Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	dns.cache.NAPTR.x.preference	0 (default) 0 to 65535 - A 16-bit unsigned integer that specifies the order in which NAPTR records with equal "order" values should be processed. Low numbers are processed before high numbers.	No
site.cfg	dns.cache.NAPTR.x.regexp	This parameter is currently unused. Applied to the original string held by the client. The substitution expression is applied in order to construct the next domain name to look up. The grammar of the substitution expression is given in RFC 2915. Null (default) string containing a substitution expression	No
site.cfg	dns.cache.NAPTR.x.replacement	The next name to query for NAPTR records depending on the value of the flags field. It must be a fully qualified domain-name. Null (default) domain name string with SRV prefix	No
site.cfg	dns.cache.NAPTR.x.service	Specifies the service(s) available down this rewrite path. For more information, see RFC 2915. Null (default) string	No
site.cfg	dns.cache.NAPTR.x.ttl	The TTL describes the time period the phone uses the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry and it resets TTL timer again. 300 (default) 300 to 536870912 (2^29), seconds	No
site.cfg	dns.cache.SRV.x.	Specify DNS SRV parameters, including: name, port, priority, target, ttl, and weight.	
site.cfg	dns.cache.SRV.x.name	Null (default) Domain name string with SRV prefix	No

Static DNS Cache Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	dns.cache.SRV.x.port	The port on this target host of this service. For more information, see RFC 2782. 0 (default) 0 to 65535	No
site.cfg	dns.cache.SRV.x.priority	The priority of this target host. For more information, see RFC 2782. 0 (default) 0 to 65535	No
site.cfg	dns.cache.SRV.x.target	Null (default) domain name string - The domain name of the target host. For more information, see RFC 2782.	No
site.cfg	dns.cache.SRV.x.ttl	The TTL describes the time period the phone uses the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record retries a dynamic network request before falling back on the static entry and it resets TTL timer again. 300 (default) 300 to 536870912 (2^29), seconds	No
site.cfg	dns.cache.SRV.x.weight	A server selection mechanism. For more information, see RFC 2782. 0 (default) 0 to 65535	No
site.cfg	tcpIpApp.dns.address.overrideDHCP	Specifies how DNS addresses are set. 0 (default) - DNS address requested from the DHCP server. 1 - DNS primary and secondary address is set using the parameters tcpIpApp.dns.server and tcpIpApp.dns.altServer.	Yes
site.cfg	tcpIpApp.dns.domain.overrideDHCP	Specifies how the domain name is retrieved or set. 0 (default) - Domain name retrieved from the DHCP server, if one is available. 1 - DNS domain name is set using the parameter tcpIpApp.dns.domain.	Yes

IP Type-of-Service Parameters

Parameters listed in the table configure the following Quality of Service (QoS) options:

● The 802.1p/Q user_priority field RTP, call control, and other packets
● The "type of service" field RTP and call control packets

IP Type of Service Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	qos.ethernet.callControl.user_priority	Set the user-priority for call control packets. 5 (default) 0 - 7	Yes
site.cfg	qos.ethernet.other.user_priority	Set the user-priority for packets that do not have a per-protocol setting. 2 (default) 0 - 7	Yes
site.cfg	qos.ethernet.rtp.user_priority	Set the priority of voice Real-Time Protocol (RTP) packets. 5 (default) 0 - 7	Yes
site.cfg	qos.ethernet.rtp.video.user_priority	User-priority used for Video RTP packets. 5 (default) 0 - 7	Yes
site.cfg	qos.ethernet.tcpQosEnabled	0 (default) - The phone does not send configured QoS priorities for SIP over TCP transport. 1 - The phone sends configured QoS priorities for SIP over TCP transport.	Yes

IP Type of Service Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	qos.ip.callControl.dscp	Specify the DSCP of packets. If the value is set to the default NULL the phone uses qos.ip.callControl.* parameters. If the value is not NULL, this parameter overrides qos.ip.callControl.* parameters. • NULL (default) • 0 to 63 • EF • Any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43	Yes
site.cfg	qos.ip.callControl.max_reliability	Set the max reliability bit in the IP ToS field of the IP header used for call control. 0 (default) - The bit in the IP ToS field of the IP header is not set. 1 - The bit is set.	Yes
site.cfg	qos.ip.callControl.max_throughput	Set the throughput bit in the IP ToS field of the IP header used for call control. 0 (default) - The bit in the IP ToS field of the IP header is not set. 1 - The bit is set.	Yes
site.cfg	qos.ip.callControl.min_cost	Set the min cost bit in the IP ToS field of the IP header used for call control. 0 (default) - The bit in the IP ToS field of the IP header is not set. 1 - The bit is set.	Yes
site.cfg	qos.ip.callControl.min_delay	Set the min delay bit in the IP ToS field of the IP header used for call control. 1 (default) - The bit is set. 0 - The bit in the IP ToS field of the IP header is not set.	Yes

IP Type of Service Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	qos.ip.callControl.precedence	Set the min delay bit in the IP ToS field of the IP header used for call control. 5 (default) 0 - 7	Yes
site.cfg	qos.ip.rtp.dscp	Specify the DSCP of packets. If the value is set to the default NULL the phone uses quality.ip.rtp.* parameters. If the value is not NULL, this parameter overrides quality.ip.rtp.* parameters. • Null (default) • 0 to 63 • EF • Any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43	Yes
site.cfg	qos.ip.rtp.max_reliability	Set the max reliability bit in the IP ToS field of the IP header used for RTP. 0 (default) - The bit in the IP ToS field of the IP header is not set. 1 - The bit is set.	Yes
site.cfg	qos.ip.rtp.max_throughput	Set the throughput bit in the IP ToS field of the IP header used for RTP. 0 (default) - The bit in the IP ToS field of the IP header is not set. 1 - The bit is set.	Yes
site.cfg	qos.ip.rtp.min_cost	Set the min cost bit in the IP ToS field of the IP header used for RTP. 0 (default) - The bit in the IP ToS field of the IP header is not set. 1 - The bit is set.	Yes

IP Type of Service Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	qos.ip.rtp.min_del ay	Set the min delay bit in the IP ToS field of the IP header used for RTP. 1 (default) - The bit is set. 0 - The bit in the IP ToS field of the IP header is not set.	Yes
site.cfg	qos.ip.rtp.precede nce	Set the precedence bit in the IP ToS field of the IP header used for RTP. 5 (default) 0 - 7	Yes
site.cfg	qos.ip.rtp.video.d scp	Allows you to specify the DSCP of packets. If the value is set to the default NULL the phone uses qos.ip.rtp.video.* parameters. If the value is not NULL, this parameter overrides qos.ip.rtp.video.* parameters. • NULL (default) • 0 to 63 • EF • Any of AF11,AF12, AF13,AF21, AF22,AF23, AF31,AF32, AF33,AF41, AF42,AF43	Yes
site.cfg	qos.ip.rtp.video.m ax_reliability	Set the reliability bits in the IP ToS field of the IP header used for RTP video. 0 (default) - The bit in the IP ToS field of the IP header is not set. 1 - The bit is set.	Yes
site.cfg	qos.ip.rtp.video.m ax_throughput	Set the throughput bits in the IP ToS field of the IP header used for RTP video. 0 (default) - The bit in the IP ToS field of the IP header is not set. 1 - The bit is set.	Yes

IP Type of Service Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	qos.ip.rtp.video.min_cost	Set the min cost bits in the IP ToS field of the IP header used for RTP video. 0 (default) - The bit in the IP ToS field of the IP header is not set. 1 - The bit is set.	Yes
site.cfg	qos.ip.rtp.video.min_delay	Set the min delay bits in the IP ToS field of the IP header used for RTP video. 1 (default) - The bit is set. 0 - The bit in the IP ToS field of the IP header is not set.	Yes
site.cfg	qos.ip.rtp.video.precedence	Set the precedence bits in the IP ToS field of the IP header used for RTP video. 5 (default) 0 - 7	Yes

Provisional Polling Parameters

Use the parameters in the following table to configure provisional polling.

Note that If prov.startupCheck.enabled is set to 0, then Polycom phones do not look for the sip.ld or the configuration files when they reboot, lose power, or restart. Instead, they look only when receiving a checksync message, a polling trigger, or a manually started update from the menu or web UI.

Some files such as bitmaps, .wav, the local directory, and any custom ringtones are downloaded each time as they are stored in RAM and lost with every reboot.

Provisional Polling of Polycom Phones

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	prov.polling	To enable polling and set the mode, period, time, and time end parameters.	
site.cfg	prov.polling.enabled	0 (default) - Disables the automatic polling for upgrades. 1 - Initiates the automatic polling for upgrades.	No

Provisional Polling of Polycom Phones

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	prov.polling.mode	The polling modes for the provisioning server. abs (default) – The phone polls every day at the time specified by prov.polling.time. rel – The phone polls after the number of seconds specified by prov.polling.period. random – The phone polls at random between a starting time set in prov.polling.time and an end time set in prov.polling.timeRandomEnd. If you set the polling period in prov.polling.period to a time greater than 86400 seconds (one day) polling occurs on a random day within that polling period and only between the start and end times. The day within the period is decided based upon the phones MAC address and does not change with a reboot whereas the time within the start and end is calculated again with every reboot	No
site.cfg	prov.polling.period	The polling period is calculated in seconds and is rounded up to the nearest number of days in an absolute and random mode. If this is set to a time greater than 86400 (one day) polling occurs on a random day based on the phone's MAC address. 86400 (default) - Number of seconds in a day. Integer - An integer value greater than 3600 seconds.	No
site.cfg	prov.polling.time	The start time for polling on the provisioning server. 03:00 (default) hh:mm	No
site.cfg	prov.polling.timeRandomEnd	The stop time for polling on the provisioning server. Null (default) hh:mm	No

SIP Subscription Timers Parameters

Use the parameters in the following table to configure when a SIP subscription expires and when expirations overlap.

SIP Subscription Timers

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.server.x.subscribe.expires`	The phone's requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period. 3600 - (default) 10 – 2147483647	No
`sip-interop.cfg`	`voIpProt.server.x.subscribe.expires.overlap`	The number of seconds before the expiration time returned by server x after which the phone attempts to resubscribe. If the server value is less than the configured overlap value, the phone tries to resubscribe at half the expiration time returned by the server. 60 - (default) 5 – 65535 seconds	No
`reg-advanced.cfg`	`reg.x.server.y.subscribe.expires`	The phone's requested subscription period in seconds after which the phone attempts to resubscribe at the beginning of the overlap period. 3600 seconds - (default) 10 – 2147483647 (seconds) You can use this parameter in conjunction with `reg.x.server.y.subscribe.expires.overlap`.	No
`reg-advanced.cfg`	`reg.x.server.y.subscribe.expires.overlap`	The number of seconds before the expiration time returned by server x after which the phone attempts to resubscribe. If the server value is less than the configured overlap value, the phone tries to resubscribe at half the expiration time returned by the server. 60 seconds (default) 5 – 65535 seconds	No

Network Signaling Validation Parameters

The following table includes the parameters you can use to specify the validation type, method, and the events for validating incoming network signaling.

Network Signaling Validation Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.requestValidation.x.method`	Null (default) - no validation is made. 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.	Yes
`sip-interop.cfg`	`voIpProt.SIP.requestValidation.x.request`	Sets the name of the method for which validation will be applied. Null (default) INVITE, ACK , BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE Note: Intensive request validation may have a negative performance impact due to the additional signaling required in some cases.	Yes
`sip-interop.cfg`	`voIpProt.SIP.requestValidation.x.request.y.event`	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`. Null (default) - all events will be validated. A valid string - specified event will be validated.	Yes

SIP Instance Parameters

The parameter `reg.x.gruu` provides a contact address to a specific user agent (UA) instance, which helps to route the request to the UA instance and is required in cases in which the REFER request must be routed to the correct UA instance. Refer to the following table for information on configuring this feature.

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	reg.x.gruu	1 - The phone sends sip.instance in the REGISTER request. 0 (default) - The phone does not send sip.instance in the REGISTER request.	No

Security

This section lists parameters that configure security settings.

Administrator and User Password Parameters

Use the parameters in the following table to set the administrator and user password and configure password settings.

Local Administrator and User Password Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.pwd.length.admin[1]	The minimum character length for administrator passwords changed using the phone. Use 0 to allow null passwords. 1 (default) 0 -32	Yes
site.cfg	sec.pwd.length.user[1]	The minimum character length for user passwords changed using the phone. Use 0 to allow null passwords. 2 (default) 0 -32	Yes
features.cfg	up.echoPasswordDigits	1 (default) The phone briefly displays password characters before being masked by an asterisk. 0 - The phone displays only asterisks for the password characters.	No

Local Administrator and User Password Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot

`device.cfg,`
`site.cfg`
	`device.auth.local`
	`AdminPassword`
		Specify a local administrator password.
		0 - 32 characters
		You must use this parameter with
		`device.auth.localAdminPas`
		`sword.set="1"`
			No

`device.cfg,` `site.cfg`	`device.auth.local` `AdminPassword.set`	0 (default) - Disables overwriting the local admin password when provisioning using a configuration file. 1 - Enables overwriting the local admin password when provisioning using a configuration file.	No

Web Configuration Utility Security Banner Parameters

The following table includes the parameters of the web user interface for security banner parameters.

Web Configuration Utility Security Banner Parameters

Template	Parameter	Permitted Values
`site.cfg`	`feature.webSecurityBanner.enabled`	0 (default) – No security banner message displays on the phone's web user interface. 1 – A security banner with the configured message displays phone's web user interface. Use `feature.webSecurityBanner.msg` to configure the message.
`site.cfg`	`feature.webSecurityBanner.msg`	Customize the text in security banner. "This is default text for the security log-on banner" (default) - This text displays because the security log-on banner has been enabled and the custom text to be displayed in the security log-on banner has not been configured. 2000 characters (maximum)

Web Configuration Utility Lock Parameters

Use the following parameters to configure how the Web Configuration Utility will behave after failed login attempts.

Lock Web Configuration Utility Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	httpd.cfg.lockWebUI. enable	1 (default) - Enable the Web Configuration Login Lock feature. 0 - Disable the Web Configuration Login Lock feature.	No
site.cfg	httpd.cfg.lockWebUI. lockOutDuration	60 seconds (default) - The period of time the user is locked out of the Web Configuration Utility. The user can try logging in again after this time. 60 - 300 seconds The lock-out timer starts after the maximum number of unsuccessful attempts within the duration you configure. After the lock-out time has expired, the timers and the number of incorrect attempts resets to 60 seconds.	No

Lock Web Configuration Utility Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	httpd.cfg.lockWebUI. noOfInvalidAttempts	5 (default) - After five failed login attempts, the user is locked out of the Web Configuration Utility. Specify the maximum number of failed login attempts after which the user is locked out of the Web Configuration Utility. 3 - 20 seconds	No
site.cfg	httpd.cfg.lockWebUI. noOfInvalidAttemptsD uration	60 seconds (default) - After a user reaches the maximum failed login attempts within 60 seconds, the user is locked out of the Web Configuration Utility. After a user reaches the maximum failed login attempts within this time duration, the user is locked out of the Web Configuration Utility. The user can try logging in again after the lock-out duration set by httpd.cfg.lockWebUI.lo ckOutDuration. 60 - 300 seconds The timer starts again after the first incorrect password attempt.	No

Configuring External Ports and Features

Use the parameters in the following table to disable external ports or specific features.

Disable Unused Ports and Features

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg	device.net.etherModePC	0 (default) – Disable the PC port mode that sets the network speed over Ethernet. 1 – Enable the PC port mode that sets the network speed over Ethernet.	No
device.cfg	device.auxPort.enable	0 (default) – Disable the phone auxiliary port. 1 – Enable the phone auxiliary port.	No
site.cfg	httpd.enabled	0 (default) – Disable the complete httpd web client. 1 – Enable the complete httpd web client.	Yes
site.cfg	ptt.pttMode.enable	0 (default) – Disable push-to-talk mode. 1 - Enable push-to-talk mode.	
features.cfg	feature.callRecording.enabled	0 (default) – Disable the phone USB port for local call recording. 1 - Enable the phone USB port for local call recording.	Yes
features.cfg	up.handsfreeMode	1(default) – Enable handsfree mode. 0 – disable handsfree mode.	No
features.cfg	feature.forward.enable	1(default) – Enable call forwarding. 0 – Disable call forwarding.	No
features.cfg	homeScreen.forward.enable	1(default) – Turn on display of the call forward icon on the phone Home screen. 0 – Turn on or off display of the call forward icon on the phone Home screen.	No
features.cfg	feature.doNotDisturb.enable	1(default) – Enable Do Not Disturb (DND). 0 – Disable Do Not Disturb (DND).	Yes

Disable Unused Ports and Features

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	homeScreen.doNotDisturb.enable	1 (default) – Enables the display of the DND icon on the phone's Home screen. 0 – Disables the display of the DND icon on the phone's Home screen.	No
features.cfg	call.autoAnswerMenu.enable	1 (default) – Enables the phone's Autoanswer menu. 0 – Disables the phone's Autoanswer menu.	No
features.cfg	homeScreen.application.enable	1 (default) – Enables the Applications icon on the phone's Home screen. 0 – Disables the Applications icon on the phone's Home screen.	
features.cfg	up.headsetModeEnabled	1 (default) – Enables the headset port. 0 – Enable or disable the headset port.	No
features.cfg	softkey.feature.doNotDisturb	1 (default) – Enables the DND soft key on the phone. 0 – Disables the DND soft key on the phone.	

Visual Security Classification Parameters

To enable this feature, you must configure settings on the BroadSoft BroadWorks server v20 or higher and on the phones. If a phone has multiple registered lines, administrators can assign a different security classification to each line.

An administrator can configure security classifications as names or strings and set the priority of each on the server in addition to the default security classification level Unclassified. The default security classification Unclassified displays until you set classifications on the server. When a user establishes a call to a phone not connected to this feature, the phone displays as Unclassified.

The following table lists the parameters you can use to configure visual security classification.

Configure Visual Security Classification

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.serverFeatureControl.securityClassification`	0 (default) - The visual security classification feature for all lines on a phone is disabled. 1 - The visual security classification feature for all lines on a phone is enabled.	Yes
`reg-advanced.cfg`	`reg.x.serverFeatureControl.securityClassification`	0 (default) - The visual security classification feature for a specific phone line is disabled. 1 - The visual security classification feature for a specific phone line is enabled.	No

Configuration File Encryption Parameters

The following table lists the parameters you can use to encrypt configuration files.

Configuration File Encryption Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`sec.encryption.upload.config`	0 (default) - The file is uploaded without encryption and replaces the phone specific configuration file on the provisioning server. 1 - The file is uploaded in encrypted form and replaces the existing phone specific configuration file on the provisioning server.	No
`site.cfg`	`sec.encryption.upload.dir`	0 (default) - The contact directory is uploaded without encryption and replaces the phone specific contact directory on the provisioning server. 1 - The contact directory is uploaded in encrypted form and replaces the existing phone specific contact directory on the provisioning server.	Yes

Configuration File Encryption Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`sec.encryption.upload.overrides`	0 (default) - The MAC address configuration file is uploaded without encryption and replaces the phone specific MAC address configuration file on the provisioning server. 1 - The MAC address configuration file is uploaded in encrypted form and replaces the existing phone specific MAC address configuration file on the provisioning server.	No
`device.cfg`	`device.sec.configEncryption.key`	Set the configuration encryption key used to encrypt configuration files. string For more information, see the section Configuration File Encryption.	Yes

TLS Platform Profile and Application Profile Parameters

By default, all Polycom-installed profiles are associated with the default cipher suite and use trusted and widely recognized CA certificates for authentication.

The following table shows parameters for TLS Platform Profile 1. To configure TLS Platform Profile 2, use a 2 at the end of the parameter instead of a 1. For example, set `device.sec.TLS.profile.caCertList2` instead of `.caCertList1`.

You can use the parameters in the following table to configure the following TLS Profile feature options:

- Change the cipher suite, CA certificates, and device certificates for the two platform profiles and the six application profiles.
- Map profiles directly to the features that use certificates.

TLS Platform Profile and Application Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg, site.cfg`	`device.sec.TLS.customCaCert1`	Specify a custom certificate. Null (default) String (maximum of 12288 characters)	No
`device.cfg, site.cfg`	`device.sec.TLS.profile.caCertList1`	Specify which CA certificates to use. Null (default) String (maximum of 1024 characters)	No
`device.cfg, site.cfg`	`device.sec.TLS.profile.cipherSuite1`	Specify the cipher suite. Null (default) String (maximum of 1024 characters)	No
`device.cfg, site.cfg`	`device.sec.TLS.profile.cipherSuiteDefault1`	Null (default) 0 - Use the custom cipher suite. 1 - Use the default cipher suite.	No
`device.cfg, site.cfg`	`device.sec.TLS.profile.deviceCert1`	Specify which device certificates to use. Builtin (default) Builtin, Platform1, Platform2	No
`site.cfg`	`sec.TLS.cipherList`	Specify the cipher list. (default) ALL:!aNULL:!eNULL:!DSS:!SEED:!ECDSA:!IDEA:!MEDIUM:!LOW:!EXP:!DH:!AECDH:!PSK:!SRP:!MD5:!RC4:@STRENGTH String (maximum of 1024 characters)	No
`site.cfg`	`sec.TLS.customCaCert.x`	The custom certificate for TLS Application Profile x (x= 1 to 6). Null (default) String	No
`site.cfg`	`sec.TLS.customDeviceKey.x`	The custom device certificate private key for TLS Application Profile x (x= 1 to 6). Null (default) String	No

TLS Platform Profile and Application Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.TLS.exchangeServices.cipherList	Specifies the cipher list for Exchange services profile. (default) ALL:!aNULL:!eNULL:!DSS:!SEED:!ECDSA:!IDEA:!MEDIUM:!LOW:!EXP:!DH:!AECDH:!PSK:!SRP:!MD5:!RC4:@STRENGTH String (maximum of 1024 characters) The format for the cipher list uses OpenSSL syntax found at https://www.openssl.org/docs/man1.0.2/apps/ciphers.html	No
site.cfg	sec.TLS.profile.exchangeServices.cipherSuiteDefault	1 (default) - Use the default cipher suite of Exchange services for the TLS Application Profile. 0 - Use the custom cipher suite of Exchange services for the TLS Application Profile.	No
site.cfg	sec.TLS.profile.x.caCert.application1	1 (default) - Enable a CA Certificate for TLS Application Profile 1. 0 - Disable a CA Certificate for TLS Application Profile 1.	No
site.cfg	sec.TLS.profile.x.caCert.application2	1 (default) - Enable a CA Certificate for TLS Application Profile 2. 0 - Disable a CA Certificate for TLS Application Profile 2.	No
site.cfg	sec.TLS.profile.x.caCert.application3	1 (default) - Enable a CA Certificate for TLS Application Profile 3. 0 - Disable a CA Certificate for TLS Application Profile 3.	No
site.cfg	sec.TLS.profile.x.caCert.application4	1 (default) - Enable a CA Certificate for TLS Application Profile 4. 0 - Disable a CA Certificate for TLS Application Profile 4.	No

TLS Platform Profile and Application Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.TLS.profile.x.caCert.application5	1 (default) - Enable a CA Certificate for TLS Application Profile 5. 0 - Disable a CA Certificate for TLS Application Profile 5.	No
site.cfg	sec.TLS.profile.x.caCert.application6	1 (default) - Enable a CA Certificate for TLS Application Profile 6. 0 - Disable a CA Certificate for TLS Application Profile 6.	No
site.cfg	sec.TLS.profile.x.caCert.application7	1 (default) - Enable a CA Certificate for TLS Application Profile 7. 0 - Disable a CA Certificate for TLS Application Profile 7.	No
site.cfg	sec.TLS.profile.x.caCert.defaultList	Specifies the list of default CA Certificate for TLS Application Profile x (x=1 to 7). Null (default) String	No
site.cfg	sec.TLS.profile.x.caCert.platform1	1 (default) - Enable a CA Certificate for TLS Platform Profile 1. 0 - Disable a CA Certificate for TLS Platform Profile 1.	No
site.cfg	sec.TLS.profile.x.caCert.platform2	1 (default) - Enable a CA Certificate for TLS Platform Profile 2. 0 - Disable a CA Certificate for TLS Platform Profile 2.	No
site.cfg	sec.TLS.profile.x.cipherSuite	Specifies the cipher suite for TLS Application Profile x (x=1 to 8). Null (default) String	No
site.cfg	sec.TLS.profile.x.cipherSuiteDefault	1 (default) - Use the default cipher suite for TLS Application Profile x (x= 1 to 8). 0 - Use the custom cipher suite for TLS Application Profile x (x= 1 to 8).	No

TLS Platform Profile and Application Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.TLS.profile.x.deviceCert	Specifies the device certificate to use for TLS Application Profile x (x = 1 to 7). Polycom (default) Platform1, Platform2, Application1, Application2, Application3, Application4, Application5, Application6,Application7	No
site.cfg	sec.TLS.webServer.cipherList	Specify the cipher list for web server. (default) ALL:!aNULL:!eNULL:!DSS:!SEED:!ECDSA:!IDEA:!MEDIUM:!LOW:!EXP:!DH:!AECDH:!PSK:!SRP:!MD5:!RC4:@STRENGTH String (maximum of 1024 characters)	No

TLS Protocol Parameters

The following table includes the parameters for the TLS protocol supported applications.

TLS Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg,` `site.cfg`	`device.sec.TLS.protocol.dot1x`	Controls the TLS Protocol used for 802.1x authentication. The handshake always starts with the highest TLS version irrespective of value configured, and the configured value is the lowest TLS/SSL version used for negotiation. TLSv1_0 (default) SSLv2v3, TLSv1_0, TLSv1_1 and TLSv1_2	No
`device.cfg,` `site.cfg`	`device.sec.TLS.protocol.prov`	Controls the TLS Protocol used for provisioning. TLSv1_0 (default) SSLv2v3 Handshake from the phone starts with the highest TLS version when set to "SSLv2v3", otherwise the phone uses "TLS 1.0".	No
`device.cfg,` `site.cfg`	`device.sec.TLS.protocol.syslog`	Controls the TLS Protocol used for Syslog. The handshake from phone starts with the highest TLS version irrespective of value configured, and the configured value is the lowest TLS/SSL version used for negotiation. TLSv1_0 (default) SSLv2v3, TLSv1_1 and TLSv1_2	No

TLS Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, site.cfg	sec.TLS.protocol.brows er	Controls the TLS Protocol used for Browser signaling. Configures the phone to use the selected protocol for a handshake negotiation from the phone. The handshake from phone starts with the highest TLS version irrespective of value configured, and the configured value is the lowest TLS/SSL version used for negotiation. TLSv1_0 (default) SSLv2v3, TLSv1_1 and TLSv1_2 The microbrowser restarts when there is a change in the browser TLS protocol or TLS cipher settings, last web page displayed is not restored.	No
device.cfg, site.cfg	sec.TLS.protocol.excha ngeServices	Controls the TLS Protocol used for Exchange services application and configures the phone to use the selected protocol for a handshake negotiation from the phone. The handshake from phone starts with the highest TLS version irrespective of value configured, and the configured value is the lowest TLS/SSL version used for negotiation. TLSv1_0 (default) SSLv2v3, TLSv1_1 and TLSv1_2	No
device.cfg, site.cfg	sec.TLS.protocol.ldap	The security handshake from the phone starts with the highest TLS version irrespective of value configured, and the configured value is the lowest TLS/SSL version used for negotiation. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No

TLS Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, site.cfg	sec.TLS.protocol.sip	Configures the phone to control the settings of the selected TLS protocol used for SIP signaling for a handshake negotiation from the phone. The handshake from phone starts with the highest TLS version irrespective of value configured, and the configured value is the lowest TLS/SSL version used for negotiation. TLSv1_0 (default) SSLv2v3, TLSv1_1 and TLSv1_2	No
device.cfg, site.cfg	sec.TLS.protocol.sopi	Configures the phone to control the settings of the selected TLS protocol used for SOPI for a handshake negotiation from the phone. The handshake from the phone starts with the highest TLS version when set to "SSLv2v3", otherwise the phone uses "TLS 1.0" TLSv1_0 (default) SSLv2v3	No
device.cfg, site.cfg	sec.TLS.protocol.webServer	Configures the phone to control the settings of the selected TLS protocol used for Web Server for a handshake negotiation from the phone. The handshake from phone starts with the highest TLS version irrespective of value configured, and the configured value is the lowest TLS/SSL version used for negotiation. TLSv1_0 (default) SSLv2v3, TLSv1_1 and TLSv1_2	No
device.cfg, site.cfg	sec.TLS.protocol.xmpp	Configures the phone to use the selected protocol for a handshake negotiation from the phone. The handshake from phone starts with the highest TLS version irrespective of value configured, and the configured value is the lowest TLS/SSL version used for negotiation. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No

FIPS 140-2 Parameters

The following table includes the new or modified parameter for the FIPS 140-2 feature.

FIPS 140-2 Parameter

Template	Parameters	Permitted Values	Change Causes Restart or Reboot
site.cfg	device.sec.TLS.FIPS.enabled	0 (default) - Does not allow the phone to use the FIPS-compliant cryptography feature. 1 - Allows the phone to use the FIPS-compliant cryptography feature.	No

TLS Cipher Suite Parameters

You can use the parameters listed in the following table to configure TLS Cipher Suites.

TLS Cipher Suite Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.TLS.cipherList	String (1 - 1024 characters) RC4:@STRENGTH (default) - RealPresence Trio solution ALL:!aNULL:!eNULL:!DSS:!SEED :!ECDSA:!IDEA:!MEDIUM:!LOW:! EXP:!ADH:!ECDH:!PSK:!MD5:! RC4:@STRENGTH The global cipher list parameter. The format for the cipher list uses OpenSSL syntax found at: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.	No
site.cfg	sec.TLS.<application>.cipherList	Specify the cipher list for a specific TLS Platform Profile or TLS Application Profile.	No

SRTP Parameters

Use the session parameters in the following table to turn on or off authentication and encryption for RTP and RTCP streams. You can also turn off the session parameters to reduce the phone's processor usage.

Secure Real Time Transport Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	sec.srtp.enable	1 (default) - The phone accepts the SRTP offers. 0 - The phone declines the SRTP offers. The defaults for SIP 3.2.0 is 0 when Null or not defined.	Yes
sip-interop.cfg	sec.srtp.offer	0 (default) - The secure media stream is not included in SDP of an SIP invite. 1 - The phone includes secure media stream along with the non-secure media description in SDP of an SIP invite.	Yes
sip-interop.cfg	sec.srtp.offer.HMAC_SHA1_32	0 (default) - The AES_CM_128_HMAC_SHA1_32 crypto suite in SDP is not included. 1 - The AES_CM_128_HMAC_SHA1_32 crypto suite in SDP is included.	Yes
sip-interop.cfg	sec.srtp.offer.HMAC_SHA1_80	1 (default) - The AES_CM_128_HMAC_SHA1_80 crypto suite in SDP is included. 0 - The AES_CM_128_HMAC_SHA1_80 crypto suite in SDP is not included.	Yes
sip-interop.cfg	sec.srtp.require	0 (default) - The secure media streams are not required. 1 - The phone is only allowed to use secure media streams.	Yes
sip-interop.cfg	sec.srtp.requireMatchingTag	1 (default) - The tag values must match in the crypto parameter. 0 - The tag values are ignored in the crypto parameter.	Yes
sip-interop.cfg	sec.srtp.sessionParams.noAuth.offer	0 (default) - The authentication for RTP offer is enabled. 1 - The authentication for RTP offer is disabled.	Yes
sip-interop.cfg	sec.srtp.sessionParams.noAuth.require	0 (default) - The RTP authentication is required. 1 - The RTP authentication is not required.	Yes

Secure Real Time Transport Protocol Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`sec.srtp.sessionParams.noEncrypRTCP.offer`	0 (default) - The encryption for RTCP offer is enabled. 1 - The encryption for RTCP offer is disabled.	Yes
`sip-interop.cfg`	`sec.srtp.sessionParams.noEncrypRTCP.require`	0 (default) - The RTCP encryption is required. 1 - The RTCP encryption is not required.	Yes
`sip-interop.cfg`	`sec.srtp.sessionParams.noEncrypRTP.offer`	0 (default) - The encryption for RTP offer is enabled. 1 - The encryption for RTP offer is disabled.	Yes
`sip-interop.cfg`	`sec.srtp.sessionParams.noEncrypRTP.require`	0 (default) - The RTP encryption is required. 1 - The RTP encryption is not required.	Yes

Phone Lock Parameters

Use the parameters in the following table to enable the phone lock feature, set authorized numbers for users to call when a phone is locked, and set scenarios when the phone should be locked.

Phone Lock is different from Device Lock for Skype for Business deployments. If you enable Phone Lock and Device Lock for Skype for Business at the same time on a phone with the Base Profile set to Skype, the Device Lock feature takes precedence over Phone Lock.

Phone Lock Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.enhancedFeatureKeys.enabled`	0 (default) - Disables the enhanced feature keys feature. 1 - Enables the enhanced feature keys feature.	No
`features.cfg`	`phoneLock.Allow.AnswerOnLock`	1(default) - The phone answers any incoming call without asking to UNLOCK. 0 - The phone asks to UNLOCK before answering.	No

Phone Lock Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	phoneLock.authorized.x .description	The name or description of an authorized number. Null (default) String Up to five (x=1 to 5) authorized contacts that a user can call while their phone is locked. Each contact needs a description to display on the screen, and a phone number or address value for the phone to dial.	No
features.cfg	phoneLock.authorized.x .value	The number or address for an authorized contact. Null (default) String Up to five (x=1 to 5) authorized contacts that a user can call while their phone is locked. Each contact needs a description to display on the screen, and a phone number or address value for the phone to dial.	No
features.cfg	phoneLock.browserEnabl ed	0 (default) - The microbrowser or browser is not displayed while the phone is locked. 1 - The microbrowser or browser is displayed while the phone is locked.	No
features.cfg	phoneLock.dndWhenLocke d	0 (default) - The phone can receive calls while it is locked 1 - The phone enters Do-Not-Disturb mode while it is locked	No
features.cfg	phoneLock.enabled[1]	0 (default) - The phone lock feature is disabled 1 - The phone lock feature is enabled.	No
features.cfg	phoneLock.idleTimeout	The amount of time (in seconds) the phone can be idle before it automatically locks. If 0, automatic locking is disabled. 0 (default) 0 to 65535	No

Phone Lock Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`phoneLock.lockState`	0 (default) - The phone is unlocked. 1 - The phone is locked. The phone stores and uploads the value each time it changes via the **MAC-phone.cfg**. You can set this parameter remotely using the Web Configuration Utility.	No
`features.cfg`	`phoneLock.powerUpUnlocked`	Overrides the `phoneLock.lockState` parameter. 0 (default) - The phone retains the value in `phoneLock.lockState` parameter. 1 - You can restart, reboot, or power cycle the phone to override the value for `phoneLock.lockState` in the **MAC-phone.cfg** and start the phone in an unlocked state. You can then lock or unlock the phone locally. Polycom recommends that you do not leave this parameter enabled	No

Secondary Port Link Status Report Parameters

You can use the parameters in the following table to configure options for the Secondary Port Link Status Report feature, including the required elapse or sleep time between two CDP UPs dispatching.

Secondary Port Link Status Report Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`sec.dot1x.eapollogoff.enabled`	0 (default) - The phone does not send an EAPOL Logoff message. 1 - The phone sends an EAPOL Logoff message.	Yes
`site.cfg`	`sec.dot1x.eapollogoff.lanlinkreset`	0 (default) - The phone does not reset the LAN port link. 1 - The phone resets the LAN port link.	Yes

Secondary Port Link Status Report Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`sec.hostmovedetect.cdp.enabled`	0 (default) - The phone does not send a CDP packet. 1 - The phone sends a CDP packet.	Yes
`site.cfg`	`sec.hostmovedetect.cdp.sleepTime`	Controls the frequency between two consecutive link-up state change reports. 1000 (default) 0 to 60000 If `sec.hostmovedetect.cdp.enabled` is set to 1, there is an x microsecond time interval between two consecutive link–up state change reports, which reduces the frequency of dispatching CDP packets.	Yes

802.1X Authentication Parameters

To set up an EAP method that requires a device or CA certificate, you need to configure TLS Platform Profile 1 or TLS Platform Profile 2 to use with 802.1X. You can use the parameters in the following table to configure 802.1X Authentication. For more information see Transport Layer Security Profiles.

Web Info: For more information on EAP authentication protocol, see RFC 3748: Extensible Authentication Protocol.

Set 802.1X Authentication Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot

`device.cfg`
`site.cfg`
`wireless.cfg`
	`device.net.dot1x.enabled`	Enable or disable 802.1X authentication.
		0
		1
			Yes

`device.cfg`
`site.cfg`
`wireless.cfg`
	`device.net.dot1x.identity`[1]	Set the identity (user name) for 802.1X authentication.
		
		String
			Yes

Set 802.1X Authentication Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg`	`device.net.dot1x.method`	Specify the 802.1X EAP method. EAP-None – No authentication EAP-TLS, EAP-PEAPv0-MSCHAPv2, EAP-PEAPv0-GTC, EAP-TTLS-MSCHAPv2, EAP-TTLS-GTC, EAP-FAST, EAP-MD5	No
`device.cfg` `site.cfg` `wireless.cfg`	`device.net.dot1x.password`[1]	Set the password for 802.1X authentication. This parameter is required for all methods except EAP-TLS. String	Yes
`device.cfg`	`device.net.dot1x.eapFastInBandProv`	Enable EAP In-Band Provisioning for EAP-FAST. 0 (default) - Disabled 1 - Unauthenticated, active only when the EAP method is EAP-FAST.	No
`device.cfg`	`device.pacfile.data`	Specify a PAC file for EAP-FAST (optional). Null (default) 0-2048 - String length.	No
`device.cfg`	`device.pacfile.password`	The optional password for the EAP-FAST PAC file. Null (default). 0-255 - String length.	No

Basic Settings Menu Lock Parameters

Use the parameter in the following table to lock the Basic settings menu.

Lock the Basic Settings Menu

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.basicSettingsPasswordEnabled	Specifies that a password is required or not required to access the **Basic Settings** menu. 0 (Default) - No password is required to access the **Basic Settings** menu. 1 - Password is required for access to the **Basic Settings** menu.	No

Hardware

This section lists parameters that configure hardware and accessories.

Headset and Speakerphone Parameters

You can use the parameters in the following table to enable and disable the headset or speakerphone and control other options for the headset and speakerphone.

Configure the Headset and Speakerphone

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.headsetModeEnabled	1 (default) – Enables the headset port. 0 – Enable or disable the headset port.	No
features.cfg	up.handsfreeMode	1(default) – Enable handsfree mode. 0 – disable handsfree mode.	No
features.cfg	up.analogHeadsetOption	Electronic Hookswitch mode for the phone's analog headset jack. 0 (Default) - No EHS-compatible headset is attached. 1 - Jabra EHS-compatible headset is attached. 2 - Plantronics EHS-compatible headset is attached. 3 - Sennheiser EHS-compatible headset is attached.	No
features.cfg	up.audioMode	Specify whether you want to use the handset or headset for audio. 0 (Default) 1	No

Configure the Headset and Speakerphone

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.headset.phoneVolume Control	Controls the phone's behavior when you adjust volume at the headset. Auto (Default) - Phone automatically selects which of the above two behaviors to apply based on the type and model of headset that you attach. Disable - Phone ignores volume up/down events from the headset; pressing the headset's volume controls has no effect on the phone. Enable - Phone responds to volume up/down events from the headset, displays the volume widget in the phone's user interface and adjusts the phone's internal volume.	Yes
site.cfg	voice.volume.persist.headset	Specifies whether the headset's volume level persists and stays at the same level between calls. 0 (default)— The headset volume automatically resets to a nominal level after each call. 1—The volume for each call is the same as the previous call.	No

USB Port Lockdown Parameters

You can use the parameters in the following table to control the USB ports on the supported phones. Note the following when setting parameters:

- The parameter `feature.usbTop.power.enabled` applies only to the VVX 1500 right-side port.

- The parameter `feature.usbRear.power.enabled` applies only to the VVX 401/411 rear port.

- You can control the VVX 500/501 and 600/601 top and rear USB ports independently using `feature.usbTop.power.enabled` to control the top USB port and `feature.usbRear.power.enabled` to control the rear USB port.

- If you set the parameter `feature.usbTop.power.enabled` to 0 to disable the top USB port on VVX 500/501 and 600/601 phones, you must set the parameter `video.enable` to 0 as well.

> Two parameters `feature.usbTop.power.enabled` and `feature.usbRear.power.enabled` replace `feature.usb.power.enabled`. You must replace `feature.usb.power.enabled` with these two new parameters in your configuration file and set both parameters to 0 to disable USB ports.

Configure USB Port Lockdown

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.usbTop.power.enabled`	This parameter applies only to the VVX 1500 business media phones, which have one USB port 1 (default) - Enable power to the top USB port (port 1). 0 - Disable power to the top USB port and the phone does not detect USB devices connected to the top USB port.	No
`features.cfg`	`feature.usbRear.power.enabled`	This parameter does not apply to VVX 1500 phones. 1 (default) - Enable power to the rear USB port (port 2). 0 - Disable power to the rear USB port and the phone does not detect USB devices connected to the rear USB port.	No
`video.cfg`	`video.enable`	1 (default) - Enables video in outgoing and incoming calls. 0 - Disables video. The G.722.1C and Siren 14 codec is disabled when you enable video on the VVX 500 and 600 business media phones.	No

Configuring Smart Paging

The following table lists the configuration parameter you need to enable and disable the smart paging feature.

Configuring Smart Paging

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`em.cfg`	`up.em.smartpaging.enabled`	Enable or disable line key assignments and page distribution on VVX Expansion Modules. 1 (Default) - Smart Paging is enabled. 0 - Smart Paging is disabled. The flexible line key configuration overrides Smart Paging for the expansion module, and Smart Paging is disabled for VVX Expansion Modules with a paper display.	No

Power-Saving Parameters

Use the parameters in the following table to configure the power-saving features and feature options.

Power-Saving Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`powerSaving.enable`	Enable or disable the power-saving feature. The default value varies by phone model. VVX 201=0 (default) VVX 300/301/310/311=0 (default) VVX 400/401/410/411=0 (default) VVX 500/501, 600/601, 1500=1 (default) 1 - Enable the LCD power-saving feature. 0 - Disable The LCD power-saving feature. Note that when the phone is in power-saving mode, the LED Message Waiting Indicator (MWI) flashes. To disable the MWI LED when the phone is in power saving mode, set the parameter `ind.pattern.powerSaving.step.1.state.x` to 0 where x=your phone's model. For example, enter the parameter as `ind.pattern.powerSaving.step.1.state.VVX500` to disable the MWI for your VVX 500 phone.	No
`site.cfg`	`powerSaving.idleTimeout.offHours`	The number of idle minutes during off hours after which the phone enters power saving. 1 (default) 1 - 10	No
`site.cfg`	`powerSaving.idleTimeout.officeHours`	The number of idle minutes during office hours after which the phone enters power saving. 30 (default) 1 - 600	No

Power-Saving Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`powerSaving.idleTimeout.userInputExtension`	The number of minutes after the phone is last used that the phone enters power saving. 10 (default) 1 - 20	No

`site.cfg`	`powerSaving.officeHours.duration.Monday`
	`powerSaving.officeHours.duration.Tuesday`
	`powerSaving.officeHours.duration.Wednesday`
	`powerSaving.officeHours.duration.Thursday`
	`powerSaving.officeHours.duration.Friday`
	`powerSaving.officeHours.duration.Saturday`
	`powerSaving.officeHours.duration.Sunday`
		Set the duration of the office working hours by week day.
		Monday - Friday = 12 (default)
		Saturday - Sunday = 0
		0 - 24
			No

`site.cfg`	`powerSaving.officeHours.startHour.x`	Specify the starting hour for the day's office working hours. 7 (default) 0 - 23 Set x to Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday (refer to `powerSaving.officeHours.duration` for an example).	No

Power-Saving Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`powerSaving.userDetectionSensitivity.offHours`	Available on the VVX 1500 only. The sensitivity used to detect the presence of the phone's user during off hours. 2 (default) - The default value was chosen for good performance in a typical office environment and is biased for difficult detection during office hours. 0 - The feature is disabled. 1 - 10 - Set the sensitivity.	No
`site.cfg`	`powerSaving.userDetectionSensitivity.officeHours`	Available on the VVX 1500 only. The sensitivity used to detect the presence of the phone's user during office hours. 7 (default) - The default value was chosen for good performance in a typical office environment and is biased for easy detection during office hours. 0 - The feature is disabled. 1 - 10 - Set the sensitivity.	No

Configuring Polycom Desktop Connector

To use this feature, the phone and computer must be on the same network or directly connected through the phone's PC port. You can configure this feature using configuration parameters shown in the following table or by using the Web Configuration Utility.

Enable Polycom Desktop Connector Integration

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`applications.cfg`	`apps.ucdesktop.adminEnabled`	1 (default) - Enable he Polycom Desktop Connector for administrator configuration. 0 - Disable the Polycom Desktop Connector for administrator configuration.	Yes
`applications.cfg`	`apps.ucdesktop.desktopUserName`	The user's name, supplied from the user's computer, for example, `bsmith`. NULL (default) string	No

Enable Polycom Desktop Connector Integration

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`applications.cfg`	`apps.ucdesktop.enabled`	0 (default) - Disable the Polycom Desktop Connector for users. 1 - Enable the Polycom Desktop Connector for users.	No
`applications.cfg`	`apps.ucdesktop.orientation`	The location of the VVX 500/501 and 1500 with respect to the user's computer. For example, to the `Left` of the computer. Unspecified (default) Left Right	No
`applications.cfg`	`apps.ucdesktop.ServerAddress`	The user's computer as a fully qualified domain name (FQDN), for example, `computer@yourcompany.com`. NULL (default) string	No
`applications.cfg`	`apps.ucdesktop.ServerPort`	The port number. Note: This value should be the same as the one that is used on the user's computer, otherwise the connection is not established. 24800 (default) 1 to 65535	No

VVX D60

This section lists parameters that configure VVX D60 Base station.

Parameters for VVX D60 Wireless Handsets

The following table lists the configuration parameters you need to configure the VVX D60 feature.

Configuring the VVX D60 Accessories

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot
features.cfg, dect.cfg	feature.dect.enabled	0 (default) - Disables communication and pairing with the VVX D60 Wireless Handset and Base Station accessories. The VVX D60 menu options do not display. 1 - Enables communication and pairing with the VVX D60 Wireless Handset and Base Station accessories. The VVX D60 menu options display on the phone and in the Web Configuration Utility.	No
new.cfg, dect.cfg	VVXD60.base.mac	Specifies the VVX D60 Base Station MAC address from the provisioning server. NULL (default) string (maximum 12 alphanumeric characters)	No
dect.cfg	VVXD60.Handset.X.outGoingLineIndex	Controls the registration index that is used as the default line for outgoing calls placed on the wireless handset without selecting a line first. X refers to the wireless handset where X can be 1-5. 1 (default) 1 - 34	No
dect.cfg	VVXD60.Handset.X.line.Y	Sets the lines that will be accessible from the wireless handset where X is the wireless handset (1-5) and Y is the registered line on the VVX phone that will be mapped to the wireless handset. You can map up to five lines to a wireless handset. 0 (default) 0 to 34	No

Configuring the VVX D60 Accessories

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.termination Type`	Determines the type of termination that is used for the line where the line can be managed automatically on the VVX, the wireless handset, or on both. X = each registration index. NULL (default) VVX, DECT, or VVX-DECT	No
`techsupport.cfg, dect.cfg`	`log.level.change. dect`	Sets the logging detail level for the VVX D60 accessory. 4 (default) 0 - 6	No
`features.cfg`	`feature.VVXD60.al lowLineMappings`	0 (default) - The Map Lines menu is available only as a password-protected option in the Administrator menu and administrators can map lines on VVX phones to the Polycom D60 handset. 1 - The Map Lines menu is available to administrators and to users on VVX phones at Menu > Settings > Features > VVX D60 Configuration to map lines on VVX phones to the Polycom D60 handset.	No

Configuring the VVX D60 Accessories

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot

`new.cfg,`
`dect.cfg,`
`features.cfg`
	`feature.VVXD60.al`
	`lowPairing`
		None (default) - Users are not allowed to pair or unpair a base station from the VVX phone.
		
		Pairing - Users are allowed to pair the base station with the VVX phone, but unpairing is not allowed.
		
		Unpairing - Users are allowed to unpair the base station from the phone, but pairing is not allowed.
		
		Both - Users are allowed to pair and unpair the base station with the VVX phone.
			No

`new.cfg, dect.cfg`	`VVXD60.handset.ma` `xCount`	Determines the maximum number of handsets that is registered to the VVX D60 Base Station. 5 (default) 1 - 5	No

Device and Software Support

This section lists parameters that configure device and software support.

User-Controlled Software Update Parameters

You can set a polling policy and polling time period at which the phone polls the server for software updates and displays a notification on the phone to update software. For example, if you set the polling policy to poll every four hours, the phone polls the server for new software every four hours and displays a notification letting the user know that a software update is available. Users can choose to update the software or they postpone it to a maximum of three times for up to six hours. The phone automatically updates the software after three postponements or after six hours, whichever comes first.

The polling policy is disabled after the phone displays the software update notification.

After the software postponement ends, the phone displays the software update notification again.

User-Controlled Software Update Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	prov.usercontrol.enabled	0 (default) - The phone does not display the software update notification and options and the phone reboots automatically to update the software. 1 - The phone displays the software update notification and options and the user can control the software download.	No
site.cfg	prov.usercontrol.postponeTime	Configure a time interval for software update notifications using the format HH:MM. If you configures an invalid value the default value is used. 2 hours (default), 15 min, 1 hour, 2hours, 4 hours, 6 hours.	No

Third-Party Servers

This section lists parameters that configure third-party servers and features.

Configuring Advanced Conferences

Use the parameters in the following table to configure this feature.

When you configure the number of participants in a conference using the parameter reg.x.advancedConference.maxParticipants, make sure the number of participants you configure matches the number of participants allowed on the ALU CTS.

ALU Advanced Conferences

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.advancedConference.enabled`	0 (default) - Disables and does not display advanced conferences and conference controls for ALU advanced conferences. 1 - Enables and displays advanced conferences and conference controls for ALU advanced conferences.	No
`reg-advanced.cfg`	`reg.x.advancedConference.pushToConference`	0 (default) - Disable push-to-conference functionality. 1 - Enable push-to-conference functionality.	No
`reg-advanced.cfg`	`reg.x.advancedConference.maxParticipants`	Sets the maximum number of participants allowed in a push to conference for advanced conference calls. The number of participants configured must match the number of participants allowed on the ALU CTS. 3 (default) 0 - 25	No
`reg-advanced.cfg`	`reg.x.advancedConference.subscribeForConfEvents`	1 (default) - Conference participants to receive notifications for conference events is enabled. 0 - Conference participants to receive notifications for conference events is disabled.	No
`reg-advanced.cfg`	`reg.x.advancedConference.subscribeForConfEventsOnCCPE`	1 (default) - Enable the conference host to receive notifications for conference events. 0 - Disable the conference host to receive notifications for conference events.	No

Configuring Shared Call Appearance

Use the parameters in the following table to configure this feature.

Shared Call Appearance

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.scap.defCallTypeExclusive`	1 (default) - An outgoing call from the call group is private. After the call is answered, the user must press the **Share** soft key to make the call public so that other people on the line can bridge in.	No
`features.cfg`	`feature.scap.HoldRequestUriUserPart`	Specifies the Hold request for Shared Call Appearance calls to the ALU server. This value must match the value configured on ALU server for SCA hold request. SCAP-Hold (default) string	No

Configuring Bridge In

Use the parameter in the following table to enable this feature.

Barge In and Bridge In

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	`reg.x.bridgeInEnabled`	0 (default) - Bridge In feature is disabled. 1 - Bridge In feature is enabled.	No

Configuring Barge In

You can configure the barge-in feature, the default barge-in mode, and whether or not a tone plays when a contact barges in on a call.

Use the parameters in the following table to enable this feature.

Barge In for BLF

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`attendant.resourceList .x.bargeInMode`	Enable or disable barge-in and choose the default barge-in mode. This parameter applies to the Alcatel-Lucent CTS only. Null (default) – If no value is entered, the Barge In feature is disabled. All – Press and hold the BLF line to display all barge-in options. Quick press to barge-in as Normal. Normal – Barge-in plays an audio tone to indicate the arrival of a new participant to the call and all call participants can interact. Listen – The user barging in can listen on the call only. Their outbound audio is not transmitted to either party. Whisper – The user barging in can hear all parties but their audio is only transmitted to the user they are monitoring.	No
`features.cfg`	`attendant.resourceList .x.requestSilentBargeI n`	0 (default) – A tone plays when a contact barges in on a call. 1 – No tone is played when a contact barges in on a call.	No

Configuring DTMF Relay

Use the parameters in the following table to configure this feature.

Configure DTMF Relay

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`voIpProt.SIP.dtmfViaSignaling.rfc2976`	Enable or disable DTMF relays for active SIP calls. Not supported for H.323 calls. 0 (default) - DTMF digit information is not sent 1 - DTMF digit information is sent in RFC2976 SIP INFO packets during a call.	Yes
`sip-interop.cfg`	`voIpProt.SIP.dtmfViaSignaling.rfc2976.nonLegacyEncoding`	Controls the behavior of the Star and Pound keys used for DTMF relays for active SIP calls. Not supported for H.323 calls. 0 (default) - The phone sends 10 when the Star key (*) is pressed and 11 when the Pound key (#) is pressed. 1 - The phone sends an asterisk (*) when the Star key is pressed and a hashtag (#) when the Pound key is pressed.	Yes

Configuring Visitor Desk Phone

You can configure a common setting for all phones and any user can make calls, including emergency calls, from a phone without having to log in. After the user logs in to the shared phone, personal settings are available as a user profile in <user> phones.cfg and any changes the user makes to phone settings are stored to this file.

The file <user>-directory.xml contains the user's contact list; the phone displays directory updates to the user at each login. Calls a user makes when logged into a phone are stored in call logs <user>-calls.xml. Calls a user makes when not logged in are not stored.

Use the parameters in the following table to configure this feature.

Visitor Desk Phone

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.VDP.enabled`	0 (default) - Disable VDP and the phone does not display the Visitor Login soft key. 1 - Enable VDP and the phone displays the Visitor Login soft key.	Yes
`features.cfg`	`prov.vdp.accessCode.login`	Specifies the VDP login service access code. *771 (default) string	No
`features.cfg`	`prov.vdp.accessCode.logout`	Specifies the VDP logout service access code. *772 (default) string	No

Configuring MADN-SCA

The following table lists all parameters available for configuring MADN-SCA and feature options.

> If you configure the line-specific parameter **reg.x.server.y.address**, you must also configure values in the line-specific parameter r**eg.x.server.y.specialInterop**.
>
> If you configure the global parameter **volpProt.server.x.address**, you must also configure values in the global parameter **volpProt.server.x.specialInterop**.
>
> For all deployments, including GENBAND, line-specific configuration parameters override global configuration parameters. If you set values in both line-specific and global parameters, line-specific parameters are applied and global parameters are not applied.

MADN-SCA Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-basic.cfg`	`reg.x.address`	The user part (for example, 1002) or the user and the host part (for example, `1002@polycom.com`) of the registration SIP URI or the H.323 ID/extension. Null (default) string address	No
`reg-advanced.cfg`	`reg.x.server.y.specialInterop`	Specify the server-specific feature set for the line registration. Standard (Default) VVX 101: Standard GENBAND ALU-CTS DT VVX 201: Standard, GENBAND ALU-CTS ocs2007r2 lync2010 All other phones: Standard GENBAND ALU-CTS ocs2007r2 lync2010 lcs2005	
`sip-interop.cfg`	`voIpProt.server.x.specialInterop`	Enables server-specific features for all registrations. Standard (default) VVX 101 = Standard, GENBAND, GENBAND-A2, ALU-CTS, DT VVX 201 = Standard, GENBAND, GENBAND-A2, ALU-CTS, ocs2007r2, lync2010 All other phones = Standard, GENBAND, GENBAND-A2, ALU-CTS, DT, ocs2007r2, lync2010, lcs2005	No

MADN-SCA Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	reg.x.type	private (default) - Use standard call signaling. shared - Use augment call signaling with call state subscriptions and notifications and use access control for outgoing calls.	No
reg-advanced.cfg	reg.x.bargeInEnabled	0 (default) - barge-in is disabled for line x. 1 - barge-in is enabled (remote users of shared call appearances can interrupt or barge in to active calls).	No
reg-advanced.cfg	reg.x.callsPerLineKey	Set the maximum number of concurrent calls for a single registration x. This parameter applies to all line keys using registration x. If registration x is a shared line, an active call counts as a call appearance on all phones sharing that registration. This per-registration parameter overrides call.callsPerLineKey. 24 (default) 1-24 VVX 101, 201 8 (default) 1 - 8	No
reg-basic.cfg	reg.x.auth.userId	User ID to be used for authentication challenges for this registration. Null (default) string - If the User ID is non-Null, it overrides the user parameter entered into the Authentication submenu on the Settings menu of the phone.	No
reg-basic.cfg	reg.x.auth.password	The password to be used for authentication challenges for this registration. Null (default) string - It overrides the password entered into the Authentication submenu on the Settings menu of the phone.	No

MADN-SCA Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-basic.cfg`	`reg.x.outboundProxy.address`	The IP address or hostname of the SIP server to which the phone sends all requests. Null (default) IP address or hostname	No
`reg-advanced.cfg`	`reg.x.auth.domain`	The domain of the authorization server that is used to check the user names and passwords. Null (default) string	No
`reg-advanced.cfg`	`reg.x.thirdPartyName`	Null (default) - In all other cases. string address -This field must match the `reg.x.address` value of the registration which makes up the part of a bridged line appearance (BLA).	No

Configuring the Global Address Book

Use the parameters in the following table to configure this feature.

GAB Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.corporateDirectory.alt.enabled`	0 (default) - Disables the global address book service. 1 - Enables the global address book service.	No
`features.cfg`	`dir.corp.alt.address`	Enter the URL address of the GAB service provided by the server. Null (default) Hostname FQDN	No
`features.cfg`	`dir.corp.alt.port`	Set the port that connects to the server if a full URL is not provided. 0 (default) Null 1 to 65535	No

GAB Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.alt.user	Enter the user name used to authenticate to the GENBAND server. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.viewPersistence	Determine if the results from the last address directory search displays on the phone. 0 (default) 1	No
features.cfg	dir.corp.alt.attribute.x.filter	Enter a filter to use to set a predefined search string through configuration files. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.attribute.x.sticky	0 (default) —the filter string criteria for attribute x is reset after a reboot. 1—the filter string criteria is retained through a reboot. If you set an attribute to be sticky (set this parameter to 1), a '*' displays before the label of the attribute on the phone.	No
features.cfg	dir.corp.alt.attribute.x.label	Enter a label to identify a user. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.attribute.x.name	Enter the name of the parameter to match on the server. Each name must be unique; however, a global address book entry can have multiple parameters with the same name. You can configure up to eight parameters (x = 1 to 8). Null (default) UTF-8 encoding string	No

GAB Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.alt.attribute.x.type	Define how x is interpreted by the phone. Entries can have multiple parameters of the same type. first_name last_name (default) phone_number SIP_address Other—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 global address book directory.	No
site.cfg	dir.local.serverFeatureControl.method	Specifies a method for synchronizing the directory and server. None (default) GENBANDSOPI - Enables the GENBANDSOPI protocol on the phone to get the personnel address book service from the GENBAND server.	No

Configuring the Personal Address Book

Use the parameters in the following table to configure this feature.

Note that when you enable server control, five telephone number fields per contact are available.

PAB Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.corporateDirectory.alt.enabled	0 (default) - Disables the global address book service. 1 - Enables the global address book service.	No
features.cfg	dir.corp.alt.address	Enter the URL address of the GAB service provided by the server. Null (default) Hostname FQDN	No

PAB Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.alt.port	Set the port that connects to the server if a full URL is not provided. 0 (default) Null 1 to 65535	No
features.cfg	dir.corp.alt.user	Enter the user name used to authenticate to the GENBAND server. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.viewPersistence	Determine if the results from the last address directory search displays on the phone. 0 (default) 1	No
features.cfg	dir.corp.alt.attribute.x.filter	Enter a filter to use to set a predefined search string through configuration files. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.attribute.x.sticky	0 (default) —the filter string criteria for attribute x is reset after a reboot. 1—the filter string criteria is retained through a reboot. If you set an attribute to be sticky (set this parameter to 1), a '*' displays before the label of the attribute on the phone.	No
features.cfg	dir.corp.alt.attribute.x.label	Enter a label to identify a user. Null (default) UTF-8 encoding string	No
features.cfg	dir.corp.alt.attribute.x.name	Enter the name of the parameter to match on the server. Each name must be unique; however, a global address book entry can have multiple parameters with the same name. You can configure up to eight parameters (x = 1 to 8). Null (default) UTF-8 encoding string	No

PAB Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.alt.attribute.x.type	Define how x is interpreted by the phone. Entries can have multiple parameters of the same type. first_name last_name (default) phone_number SIP_address Other—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 global address book directory.	No
site.cfg	dir.local.serverFeatureControl.method	Specifies a method for synchronizing the directory and server. None (default) GENBANDSOPI - Enables the GENBANDSOPI protocol on the phone to get the personnel address book service from the GENBAND server.	No
site.cfg	dir.local.serverFeatureControl.reg	Specifies the phone line to enable the personal address book feature on. 1 (default) 1 -34	No
site.cfg	dir.genband.local.contacts.maxSize	Specify the maximum number of contacts available in the GENBAND personnel address book contact directory.	

Configuring E.911

Use the parameters in the following table to configure this feature.

E911 Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.genband.E911.enabled	0 (default) - Disable the GENBAND E.911 feature. 1 - Enable the GENBAND E.911 feature.	Yes
features.cfg	genband.E911.location.description	Enter a description of the location of the phone, for example, cubicle 105. Ensure that the description string you provide here is identical to the description you configure on the location server. Other (default) String up to 256 characters [platform-specific display size limitations apply]	No
features.cfg	genband.E911.location.locationID	Enter the location ID corresponding to the location description you entered in genband.E911.location.description, for example, 112876. Ensure that the location ID you enter here is identical to the one you configure on the location server. 0 (default) string	No
features.cfg	genband.E911.registration.line	Select the registration line to use to retrieve E.911 location information 1 (default) 0 - 100	No

Configuring Authentication for BroadWorks XSP

The authentication method you use depends on which version of BroadWorks you are running. If your server is running BroadWorks R19 or earlier, enable the following parameters to authenticate on the BroadWorks server using separate XSP credentials:

- dir.broadsoft.xsp.address
- reg.x.broadsoft.userId
- reg.x.broadsoft.xsp.password
- reg.x.broadsoft.useXspCredentials

If your server is running BroadWorks R19 Service Pack 1 or later, enable the following parameters to authenticate on the BroadWorks server using the same SIP credentials you used to register the phone lines: dir.broadsoft.xsp.address

- reg.x.auth.userId

- `reg.x.auth.password`
- `reg.x.broadsoft.userId`

See the following table for additional details on these parameters.

Configure BroadWorks XSP Service Interface Authentication

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`reg.x.broadsoft.xsp.password`	Enter the password associated with the BroadSoft user account for the line. Required only when `reg.x.broadsoft.useXspCredentials=1`. Null (default) string	No
`features.cfg`	`reg.x.broadsoft.userId`	Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface. Null (default) string	No
`features.cfg`	`reg.x.broadsoft.useXspCredentials`	If this parameter is disabled, the phones use standard SIP credentials to authenticate. 1 (default) - Use this value, if phone lines are registered with a server running BroadWorks R19 or earlier. 0 - Set to 0, if phone lines are registered with a server running BroadWorks R19 SP1 or later.	No
`reg-basic.cfg`	`reg.x.auth.userId`	User ID to be used for authentication challenges for this registration. Null (default) string - If the User ID is non-Null, it overrides the user parameter entered into the Authentication submenu on the Settings menu of the phone.	No
`reg-basic.cfg`	`reg.x.auth.password`	The password to be used for authentication challenges for this registration. Null (default) string - It overrides the password entered into the Authentication submenu on the Settings menu of the phone.	No

BroadWorks Call Decline Parameters

Use the parameter in the following table to enable users to reject calls on a shared line.

BroadWorks Call Decline Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`call.shared.reject`	For shared line calls on the BroadWorks server. 0 - The phone displays a Reject soft key to reject an incoming call to a shared line. 1 - The Reject soft key does not display.	No

Flexible Seating Parameters

To configure a host phone to support the primary phone's line registration, you must configure a host user profile and a guest user profile on the BroadSoft BroadWorks server. In the host user profile configuration files, add the configuration parameters shown in the following table and map these parameters to the corresponding BroadSoft BroadWorks configuration tags.

Flexible Seating Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features .cfg`	`hoteling. reg`	1 (default) - Specifies the phone line on the host phone which hosts the guest line.	No
	`hotelingM ode.type`	-1 (Default): The parameter does not exist on the BroadSoft server. 0 - Both Flexible Seating and Hoteling are disabled on the BroadSoft Device Management Server (DMS). 1 - Hoteling is enabled 2 - Flexible Seating is enabled but guest is not logged in. 3 - Flexible seating location is enabled and guest is logged in. Note: This parameter overrides `voIpProt.SIP.specialEvent.checkSy nc.downloadDirectory` when set to 2 or 3.	No

Executive-Assistant Parameters

In the BroadWorks Web Portal, you must enable the Executive Service for private and shared executive lines, and the Executive-Assistant Service for private and shared assistant lines.

The BroadWorks server allows the following configuration options: Executive private line, Executive-Assistant Service line, and a shared alias line. Administrators can set up executive and assistant lines in the following scenarios:

- A private executive line with an assistant with a private line
- Shared executive line with an assistant with a private line
- Shared executive line with a shared line alias on the assistant's phone
    - ➢ The shared line must be created as a shared location of a line with the Executive Service on the BroadWorks server.
    - ➢ In this option, the main line registration is a private line for the assistant, and the secondary registration is a shared line for the executive.

The following table includes the configuration parameters you can use to enable and configure the Executive-Assistant feature.

BroadSoft Executive-Assistant Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.BSExecutiveAssistant.enabled	`0` (default) - Disables the BroadSoft Executive-Assistant feature. `1` - Enables the BroadSoft Executive-Assistant feature.	No
features.cfg	feature.BSExecutiveAssistant.regIndex	The registered line assigned to the executive or assistant for the BroadSoft Executive-Assistant feature. `1` (default) to `255` - The registered line for the Executive or Assistant.	No
features.cfg	feature.BSExecutiveAssistant.userRole	`ExecutiveRole` (default) - Sets the registered line as an Executive line. `AssistantRole` - Sets the registered line as an Assistant line. Note: A phone can only have a line set as an Executive or an Assistant; an Executive and an Assistant line cannot be on the same phone.	No

BroadSoft Executive-Assistant Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	`feature.BSExecutiveAssistant.SimplifiedAssistant.enabled`	0 (default) - Remove the pick call and barge-in soft keys from executive actions menu. 1 - Add the pick call and barge-in soft keys from executive actions menu.	No
features.cfg	`feature.BSExecutiveAssistant.SimplifiedExec.enabled`	0 (default) - Remove the call screening option from the executive settings menu. 1 - Add the call screening option from the executive settings menu.	No

Configuring Enhanced Call Park

The following table includes the configuration parameters you can use to enable and configure this feature.

Enhanced Call Park

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`reg-advanced.cfg`	`reg.x.enhancedCallPark.enabled`	0 (default) - To disable the BroadWorks Enhanced Call Park feature. 1 - To enable the BroadWorks Enhanced Call Park feature.	No
`reg-basic.cfg`	`reg.x.lineAddress`	The line extension for a shared line. This parameter applies to private lines and BroadSoft call park and retrieve. If there is no extension provided for this parameter, the call park notification is ignored for the shared line. Null (default) String	No
`features.cfg`	`feature.enhancedCallPark.allowAudioNotification`	0 (default) - Disables the audio notifications for parked calls on private and shared lines. 1 - Enables the audio notifications for parked calls on private and shared lines.	No
`sip-interop.cfg, site.cfg`	`call.parkedCallRetrieveString`	The star code that initiates retrieval of a parked call. Null (default) Permitted values are star codes.	No

BroadSoft Directory Parameters

To perform a search and to view contacts on the BroadSoft directories, configure the directories. You can configure this feature using the parameters in the following table

BroadSoft Directory Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.broadsoftGroupDir.enabled	0 (default) - Disables Group Directory. 1 - Enables Group Directory.	No
features.cfg	feature.broadsoftdir.enabled	0 (default) - Disables Enterprise Directory. 1 - Enables Enterprise Directory.	Yes
features.cfg	feature.broadsoftPersonalDir.enabled	0 (default) - Disables Personal Directory. 1 - Enables Personal Directory.	

BroadSoft UC-One Configuration Parameters

The following table lists all parameters available to configure features in the BroadSoft UC-One application.

BroadSoft UC-One Application

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.qml.enabled	0 (default) - Disable the QML viewer on the phone. Note that the UC-One directory user interface uses QML as the user interface framework and the viewer is used to load the QML applications. 1 - Enable the QML viewer on phone.	Yes
features.cfg	feature.broadsoftdir.enabled	0 (default) - Disable simple search for Enterprise Directories. 1 - Enable simple search for Enterprise Directories.	Yes
features.cfg	feature.broadsoftUcOne.enabled	0 (default) - Disables the BroadSoft UC-One feature. 1 - Enables the BroadSoft UC-One feature.	Yes
features.cfg	feature.presence.enabled	0 (default) - Disable the presence feature—including buddy managements and user status. 1 - Enable the presence feature with the buddy and status options.	No

BroadSoft UC-One Application

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	homeScreen.UCOne.enable	1 (default) - Enable the UC-One Settings icon to display on the phone Home screen. 0 - Disable the UC-One Settings icon to display on the phone Home screen.	No
features.cfg	dir.broadsoft.xsp.address	Set the IP address or hostname of the BroadSoft directory XSP home address. Null (default) IP address Hostname FQDN	No
applications.cfg	dir.broadsoft.xsp.username	To set the BroadSoft Directory XSP home address.	
features.cfg	dir.broadsoft.xsp.password	Set the password used to authenticate to the BroadSoft Directory XSP server. Null (default) UTF-8 encoding string	No
features.cfg	xmpp.1.auth.password	Specify the password used for XMPP registration. Null (Default) UTF-8 encoded string	No
features.cfg	xmpp.1.dialMethod	For SIP dialing, the destination XMPP URI is converted to a SIP URI, and the first available SIP line is used to place the call. SIP (default) String min 0, max 256	No
features.cfg	xmpp.1.jid	Enter the Jabber identity used to register with the presence server, for example: presence.test2@polycom-alpha.eu.bc.im. Null (default) String min 0, max 256	No

BroadSoft UC-One Application

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	xmpp.1.roster.invite.accept	Choose how phone users receive the BroadSoft XMPP invitation to be added to a buddy list. prompt (default) - phone displays a list of users who have requested to add you as a buddy and you can accept or reject the invitation. Automatic	No
features.cfg	xmpp.1.server	Sets the BroadSoft XMPP presence server to an IP address, host name, or FQDN, for example: polycom-alpha.eu.bc.im. Null (default) dotted-decimal IP address, host name, or FQDN.	No
features.cfg	xmpp.1.verifyCert	Specifies to enable or disable verification of the TLS certificate provided by the BroadSoft XMPP presence server. 1 (default) 0	No

Enterprise Directory Search Parameters

The following table includes the parameter for the Enterprise Directory Search feature.

Enterprise Directory Search Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.broadsoftdir.showDefaultSearch	0 (default) – No contacts are displayed when the search box field is empty. 1 – Enables the user to view the initial list of contacts for an empty search box	

BroadSoft Server-Based Call Logs Parameters

The following table includes the parameter for the BroadSoft server based call logs feature.

BroadSoft Server Based Call Logs Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.broadsoft.callLogs`	Disabled (default) – Disable the BroadSoft server call logs feature. Basic – Enable the BroadSoft server call logs feature.	

BroadSoft Server-Based Redial Parameters

Use the following parameters to configure this feature.

BroadSoft Server-Based Redial Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.broadsoft.basicCallLogs.redial.enabled`	0 (default) - Disables the option to redial the last number. 1 - Enables the phone to redial the last number.	

Configuring Anonymous Call Rejection

You can enable the Anonymous Call Rejection feature using configuration files or the Web Configuration Utility. Use the parameters in the following table to enable this feature.

Anonymous Call Rejection

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.broadsoft.xsi.AnonymousCallReject.enabled`	0 (default) - Does not display the Anonymous Call Rejection menu to users. 1 - Displays the Anonymous Call Rejection menu and the user can turn the feature on or off from the phone.	No

Anonymous Call Rejection

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.broadsoftUcOne .enabled	0 (default) - Disables the BroadSoft UC-One feature. 1 - Enables the BroadSoft UC-One feature.	Yes
features.cfg	reg.x.broadsoft.userId	Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface. Null (default) string	No

Configuring Line ID Blocking

You can configure this feature using configuration parameters or the Web Configuration Utility. Use the parameters in the following table to enable this feature.

Line ID Blocking

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.broadsoft.xsi. LineIdblock.enabled	0 (default) - Disables and does not display the Line ID Blocking feature menu on the phone. 1 - Enables the Line ID Blocking feature menu on the phone.	No
features.cfg	feature.broadsoftUcOne .enabled	0 (default) - Disables the BroadSoft UC-One feature. 1 - Enables the BroadSoft UC-One feature.	Yes

Configuring BroadWorks Anywhere

You can configure BroadWorks Anywhere using configuration files or the Web Configuration Utility. Use the parameters in the following table to enable this feature.

BroadWorks Anywhere

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.broadsoft.xsi.BroadWorksAnywhere.enabled`	0 (default) - Disables and does not display the BroadWorks Anywhere feature menu on the phone. 1 - Enables the BroadWorks Anywhere feature menu on the phone.	No
`features.cfg`	`feature.broadsoftUcOne.enabled`	0 (default) - Disables the BroadSoft UC-One feature. 1 - Enables the BroadSoft UC-One feature.	Yes

Configuring Simultaneous Ring Personal

You can enable or disable the Simultaneous Ring feature for users using configuration files or the Web Configuration Utility. Use the parameters in the following table to enable this feature.

Simultaneous Ring

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.broadsoft.xsi.SimultaneousRing.enabled`	0 (default) - Disables and does not display the Simultaneous Ring Personal feature menu on the phone. 1 - Enables the Simultaneous Ring Personal feature menu on the phone.	No
`features.cfg`	feature.broadsoftUcOne.enabled	Enable or disable all BroadSoft UC-One features.	

Personal Directory Parameters

The following table includes the parameter for the Personal Directory feature.

Personal Directory Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`feature.broadsoftPersonalDir.enabled`	0 (default) – Personal Directory feature is disabled. 1 – Personal Directory feature is enabled and users can add, delete, or edit contacts.	

BroadSoft Server-based Call Waiting Parameters

Use the parameters in the following table to configure server-based call waiting alerts.

Server-based Call Waiting Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.broadsoft .xsi.callWaiting. enabled	0 (default) - Disable incoming calls during an active call. 1 - Enable incoming calls during an active call.	No

Configuring Remote Office

You can configure Remote Office using configuration files or the Web Configuration Utility. Use the parameters in the following table to enable this feature.

Remote Office

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.broadsoft.xsi. RemoteOffice.enabled	0 (default) - Disables the Remote Office feature menu on the phone. 1 - Enables and displays the Remote Office feature menu on the phone.	No
features.cfg	reg.x.broadsoft.userId	Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface. Null (default) string	No
features.cfg	feature.broadsoftUcOne .enabled	0 (default) - Disables the BroadSoft UC-One feature. 1 - Enables the BroadSoft UC-One feature.	Yes
features.cfg	dir.broadsoft.xsp.pass word	Set the password used to authenticate to the BroadSoft Directory XSP server. Null (default) UTF-8 encoding string	No

Configuring BroadSoft UC-One Credentials

Use the parameters in the following table to enable this feature.

Configure XSP User Name an Password

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.broadsoft.xsp.addr ess	Set the IP address or hostname of the BroadSoft directory XSP home address. Null (default) IP address Hostname FQDN	No
features.cfg	reg.x.broadsoft.userId	Enter the BroadSoft user ID to authenticate with the BroadSoft XSP service interface. Null (default) string	No
features.cfg	feature.broadsoftUcOne .enabled	0 (default) - Disables the BroadSoft UC-One feature. 1 - Enables the BroadSoft UC-One feature.	Yes
applications.c fg	dir.broadsoft.xsp.user name	To set the BroadSoft Directory XSP home address.	
features.cfg	dir.broadsoft.xsp.pass word	Set the password used to authenticate to the BroadSoft Directory XSP server. Null (default) UTF-8 encoding string	No
features.cfg	feature.broadsoftdir.e nabled	0 (default) - Disable simple search for Enterprise Directories. 1 - Enable simple search for Enterprise Directories.	Yes

Types of Device Parameters

The following table outlines the three types of <device/> parameters, their permitted values, and the default value.

Types of Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg` `site.cfg`	`device.set`[1]	0 (default)—Do not use any `device.xxx` fields to set any parameters. Set this to 0 after the initial software installation. 1—Use the `device.xxx` fields that have `device.xxx.set=1`. Set this to 1 only for the initial software installation.	Yes
`device.cfg`	`device.xxx`[1]	string	Yes
`device.cfg`	`device.xxx.set`[1]	0 (default)—Do not use the `device.xxx` value. 1—Use the `device.xxx` value. For example, if `device.net.ipAddress.set=1`, then use the value set for `device.net.ipAddress`.	Yes

Device Parameters

The following table lists each of the <device/> parameters that you can configure.

> The default values for the `<device/>` parameters are set at the factory when the phones are shipped. For a list of the default values, see the latest Product Shipping Configuration Change Notice at Polycom Engineering Advisories and Technical Notifications.

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg` `site.cfg`	`device.auth.localAdminPassword`	Set the phone's local administrative password. The minimum length is defined by `sec.pwd.length.admin`. string (32 character max)	No
`device.cfg` `reg-advanced`	`device.auth.localUserPassword`	Set the phone user's local password. The minimum length is defined by `sec.pwd.length.user`. string (32 character max)	No

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg`	`device.auxPort.enable`[1]	Enable or disable the phone auxiliary port. 0 1 (default)	Yes
`device.cfg`	`device.baseProfile`	NULL (default) Generic —Sets the base profile to Generic for OpenSIP environments. Lync —Sets this Base Profile for Skype for Business deployments.	No
`device.cfg` `site.cfg`	`device.dhcp.bootSrvOpt`[1]	When the boot server is set to Custom or Custom+Option66, specify the numeric DHCP option that the phone looks for. Null 128 to 254	Yes
`device.cfg` `site.cfg`	`device.dhcp.bootSrvOptType`[1]	Set the type of DHCP option the phone looks for to find its provisioning server if `device.dhcp.bootSrvUseOpt` is set to `Custom`. IP address —The IP address provided must specify the format of the provisioning server. String—The string provided must match one of the formats specified by `device.prov.serverName`.	Yes
`device.cfg` `site.cfg`	`device.dhcp.bootSrvUseOpt`[1]	Default—The phone looks 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 `device.prov.serverName`. Custom —The phone looks for the option number specified by `device.dhcp.bootSrvOpt`, and the type specified by `device.dhcp.bootSrvOptType` in the response received from the DHCP server. Static —The phone uses the boot server configured through the provisioning server `device.prov.*` parameters. Custom and Default —The phone uses the custom option first or use Option 66 if the custom option is not present.	Yes

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg` `site.cfg`	`device.dhcp.dh cpVlanDiscOpt`[1]	Set the DHCP private option to use when `device.dhcp.dhcpVlanDiscUseOpt` is set to `Custom`. 128 to 254	Yes
`device.cfg` `site.cfg`	`device.dhcp.dh cpVlanDiscUseO pt`[1]	Set how VLAN Discovery occurs. Disabled—no VLAN discovery through DHCP. Fixed—use predefined DHCP vendor-specific option values of 128, 144, 157 and 191 (`device.dhcp.dhcpVlanDiscOpt` is ignored). Custom—use the number specified by `device.dhcp.dhcpVlanDiscOpt`.	Yes
`device.cfg` `site.cfg`	`device.dhcp.en abled`[1]	Enable or disable DHCP. 0 1	Yes
`device.cfg` `site.cfg`	`device.dhcp.op tion60Type`[1]	Set the DHCP option 60 type. Binary—vendor-identifying information is in the format defined in RFC 3925. ASCII—vendor-identifying information is in ASCII format.	Yes
`device.cfg` `site.cfg`	`device.dns.alt SrvAddress`[1]	Set the secondary server to which the phone directs domain name system (DNS) queries. Server Address	Yes
`device.cfg` `site.cfg`	`device.dns.dom ain`[1]	Set the phone's DNS domain. String	Yes
`device.cfg` `site.cfg`	`device.dns.ser verAddress`[1]	Set the primary server to which the phone directs DNS queries. Server Address	Yes

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg` `site.cfg`	`device.hostname`[1]	Specify a hostname for the phone when using DHCP by adding a hostname string to the phone's configuration. If `device.host.hostname.set` = 1, and `device.host.hostname` = `Null`, the DHCP client uses Option 12 to send a predefined hostname to the DHCP registration server using `Polycom_<MACaddress>`. String —The maximum length of the hostname string is <=255 bytes, and the valid character set is defined in RFC 1035.	Yes
`device.cfg` `site.cfg`	`device.net.cdpEnabled`[1]	Determine if the phone attempts to determine its VLAN ID and negotiate power through CDP. 0 1	Yes
`device.cfg` `site.cfg` `wireless.cfg`	`device.net.dot1x.anonid`[1]	EAP-TTLS and EAP-FAST only. Set the anonymous identity (user name) for 802.1X authentication. String	Yes
`device.cfg` `site.cfg` `wireless.cfg`	`device.net.dot1x.enabled`[1]	Enable or disable 802.1X authentication. 0 1	Yes
`device.cfg` `site.cfg` `wireless.cfg`	`device.net.dot1x.identity`[1]	Set the identity (user name) for 802.1X authentication. String	Yes
`device.cfg` `site.cfg` `wireless.cfg`	`device.net.dot1x.method`	Specify the 802.1X authentication method, where `EAP-NONE` means no authentication. EAP-None EAP-TLS EAP-PEAPv0-MSCHAPv2 EAP-PEAPv0-GTC EAP-TTLS-MSCHAPv2 EAP-TTLS-GTC EAP-FAST EAP-MD5	No

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg` `site.cfg` `wireless.cfg`	`device.net.dot 1x.password`[1]	Set the password for 802.1X authentication. This parameter is required for all methods except EAP-TLS. String	Yes
`device.cfg` `site.cfg`	`device.net.eth erModeLAN`[1]	Set the LAN port mode that sets the network speed over Ethernet. Polycom recommends that you do not change this setting. Auto 10HD 10FD 100HD 100FD 1000FD HD means half-duplex and FD means full duplex.	Yes
`device.cfg` `site.cfg`	`device.net.eth erModePC`[1]	Set the PC port mode that sets the network speed over Ethernet. Auto (default) Disabled—disables the PC port. 10HD 10FD 100HD 100FD 1000FD HD means half-duplex and FD means full duplex.	Yes
`device.cfg` `site.cfg`	`device.net.eth erStormFilter`[1]	1—DoS storm prevention is enabled and received Ethernet packets are filtered to prevent TCP/IP stack overflow caused by bad data or too much data. 0— DoS storm prevention is disabled.	Yes
`device.cfg` `site.cfg`	`device.net.eth erStormFilterP psValue`	Set the corresponding packets per second (pps) for storm filter and to control the incoming network traffic. 17 to 40 38 (default)	No

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.net.eth erStormFilterP psValue.set	0 (default) - You cannot configure the device.net.etherStormFilterPpsValue parameter. 1 - You can configure the device.net.etherStormFilterPpsValue parameter.	No
device.cfg site.cfg	device.net.eth erVlanFilter[1]	VLAN filtering for VVX phones is done by the Linux operating system and it cannot be disabled. 0 1	Yes
device.cfg	device.net.ipA ddress[1]	Set the phone's IP address. This parameter is disabled when device.dhcp.enabled is set to 1. String	Yes
device.cfg site.cfg	device.net.IPg ateway[1]	Set the phone's default router. IP address	Yes
device.cfg site.cfg	device.net.lld pEnabled[1]	0—The phone doesn't attempt to determine its VLAN ID. 1—The phone attempts to determine its VLAN ID and negotiate power through LLDP.	Yes
device.cfg site.cfg	device.net.lld pFastStartCoun t	Specify the number of consecutive LLDP packets the phone sends at the time of LLDP discovery, which are sent every one second. 5 (default) 3 to 10	No
device.cfg site.cfg	device.net.sub netMask[1]	Set the phone's subnet mask. This parameter is disabled when device.dhcp.enabled is set to 1. subnet mask	Yes
device.cfg site.cfg	device.net.vla nId[1]	Set the phone's 802.1Q VLAN identifier. Null—No VLAN tagging. 0 to 4094	Yes
device.cfg site.cfg	device.prov.ma xRedunServers[1]	Set the maximum number of IP addresses to use from the DNS. 1 - 8	Yes

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.prov.password[1]	Set the password for the phone to log in to the provisioning server, which may not be required. If you modify this parameter, the phone re-provisions. The phone may also reboot if the configuration on the provisioning server has changed. string	Yes
device.cfg site.cfg	device.prov.redunAttemptLimit[1]	Set the maximum number of attempts to attempt a file transfer before the transfer fails. When multiple IP addresses are provided by DNS, 1 attempt is considered to be a request sent to each server. 1 to 10	Yes
device.cfg site.cfg	device.prov.redunInterAttemptDelay[1]	Set the number of seconds to wait after a file transfer fails before retrying the transfer. When multiple IP addresses are returned by DNS, this delay only occurs after each IP has been tried. 0 to 300	Yes
device.cfg site.cfg	device.prov.serverName	Enter the IP address, domain name, or URL of the provisioning server followed by an optional directory and optional configuration filename. This parameter is used if (device.dhcp.enabled is 0), if the DHCP server does not send a boot server option, or if the boot server option is static (device.dhcp.bootSrvUseOpt is static). IP address Domain name string URL If you modify this parameter, the phone re-provisions. The phone also reboots if the configuration on the provisioning server has changed.	No

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg` `site.cfg`	`device.prov.serverType`[1]	Set the protocol the phone uses to connect to the provisioning server. Active FTP is not supported for BootROM version 3.0 or later, and only implicit FTPS is supported. FTP TFTP HTTP HTTPS FTPS	Yes
`device.cfg` `site.cfg`	`device.prov.tagSerialNo`	0—The phone's serial number (MAC address) is not included in the User-Agent header of HTTPS/HTTPS transfers and communications to the microbrowser and web browser. 1— the phone's serial number is included.	No
`device.cfg` `site.cfg`	`device.prov.upgradeServer`	Specify the URL or path for a software version to download to the device. On the Web Configuration Utility, the path to the software version you specify displays in the drop-down list on the Software Upgrade page. NULL (default) string 0 -255 characters	No
`device.cfg` `site.cfg`	`device.prov.user`	The user name required for the phone to log in to the provisioning server (if required). If you modify this parameter, the phone re-provisions, and it may reboot if the configuration on the provisioning server has changed. string	No
`device.cfg` `site.cfg`	`device.prov.ztpEnabled`	Enable or disable Zero Touch Provisioning (ZTP). 0 1 For information, see Polycom Zero Touch Provisioning Solution.	No

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot

`device.cfg`
`site.cfg`
	`device.sec.con`
	`figEncryption.`
	`key`[1]
		Set the configuration encryption key used to encrypt configuration files.
		
		string
		For more information, see the section Configuration File Encryption.
			Yes

`device.cfg`
`site.cfg`
	`device.sec.cor`
	`eDumpEncryptio`
	`n.enabled`
		Determine whether to encrypt the core dump or bypass the encryption of the core dump.
		0—encryption of the core dump is bypassed.
		1 (default)—the core dump is encrypted
			No

`device.cfg`
`site.cfg`
	`device.sec.TLS`
	`.customCaCert1`
	`(TLS Platform`
	`Profile 1)`
	`device.sec.TLS`
	`.customCaCert2`
	`(TLS Platform`
	`Profile 2)`
		Set the custom certificate to use for TLS Platform Profile 1 and TLS Platform Profile 2 and TLS Application Profile 1 and TLS Application Profile 2. The parameter `device.sec.TLS.profile.caCertList` must be configured to use a custom certificate. Custom CA certificate cannot exceed 4096 bytes total size.
		
		string
		PEM format
			No

`debug.cfg`	`device.sec.TLS`
	`.customDeviceC`
	`ert1.privateKe`
	`y`
	`device.sec.TLS`
	`.customDeviceC`
	`ert2.privateKe`
	`y`
		Enter the corresponding signed private key in PEM format (X.509).
		Size constraint: 4096 bytes for the private key.
			No

`debug.cfg`	`device.sec.TLS`
	`.customDeviceC`
	`ert1.publicCer`
	`t`
	`device.sec.TLS`
	`.customDeviceC`
	`ert2.publicCer`
	`t`
		Enter the signed custom device certificate in PEM format (X.509).
		Size constraint: 8192 bytes for the device certificate.
			No

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.sec.TLS.customDeviceCert1.set device.sec.TLS.customDeviceCert2.set	Use to set the values for parameters device.sec.TLS.customDeviceCertX.publicCert and device.sec.TLS.customDeviceCertX.privateKey. Size constraints are: 4096 bytes for the private key, 8192 bytes for the device certificate. 0 (default) 1	No
device.cfg	device.sec.TLS.profile.caCertList1 (TLS Platform Profile 1) device.sec.TLS.profile.caCertList2 (TLS Platform Profile 2)	Choose the CA certificate(s) to use for TLS Platform Profile 1 and TLS Platform Profile 2 authentication: Builtin—The built-in default certificate BuiltinAndPlatform—The built-in and Custom #1 certificates BuiltinAndPlatform2—The built-in and Custom #2 certificates All—Any certificate (built in, Custom #1 or Custom #2) Platform1—Only the Custom #1 certificate Platform2—Only the Custom #2 certificate Platform1AndPlatform2—Either the Custom #1 or Custom #2 certificate	No
device.cfg site.cfg	device.sec.TLS.profile.cipherSuite1 (TLS Platform Profile 1) device.sec.TLS.profile.cipherSuite2 (TLS Platform Profile 2)	Enter the cipher suites to use for TLS Platform Profile 1 and TLS Platform Profile 2 string	No

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.sec.TLS.profile.cipherSuiteDefault1 (TLS Platform Profile 1) device.sec.TLS.profile.cipherSuiteDefault2 (TLS Platform Profile 2)	Determine the cipher suite to use for TLS Platform Profile 1 and TLS Platform profile 2. 0—The custom cipher suite is used. 1—The default cipher suite is used.	No
device.cfg site.cfg	device.sec.TLS.profile.deviceCert1 (TLS Platform Profile 1) device.sec.TLS.profile.deviceCert2 (TLS Platform Profile 2)	Choose the device certificate(s) for TLS Platform Profile 1 and TLS Platform Profile 2 to use for authentication. Builtin Platform1 Platform2	No
device.cfg site.cfg	device.sec.TLS.profileSelection.dot1x	Choose the TLS Platform Profile to use for 802.1X. PlatformProfile1 PlatformProfile2	No
device.cfg site.cfg	device.sec.TLS.profileSelection.provisioning[1]	Set the TLS Platform Profile to use for provisioning. PlatformProfile1 PlatformProfile2	Yes
device.cfg site.cfg	device.sec.TLS.profileSelection.syslog[1]	Set the TLS Platform Profile to use for syslog. PlatformProfile1 PlatformProfile2	Yes
device.cfg site.cfg	device.sec.TLS.prov.strictCertCommonNameValidation	0 1 (default)—Provisioning server always verifies the server certificate for the commonName/SubjectAltName match with the server hostname that the phone is trying to connect.	No

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.sec.TLS .syslog.strict CertCommonName Validation	0 1—Syslog always verifies the server certificate for the commonName/SubjectAltName match with the server hostname that the phone is trying to connect.	No
device.cfg site.cfg	device.sntp.gm tOffset	Set the GMT offset—in seconds—to use for daylight savings time, corresponding to -12 to +13 hours. -43200 to 46800	No
device.cfg site.cfg	device.sntp.gm tOffsetcityID	Sets the correct time zone location description that displays on the phone menu and in the Web Configuration Utility. NULL (default) 0 to 126 For descriptions of all values, refer to Time Zone Location Description.	No
device.cfg site.cfg	device.sntp.se rverName	Enter the SNTP server from which the phone obtains the current time. IP address Domain name string	No
device.cfg site.cfg	device.syslog. facility	Determine a description of what generated the log message. 0 to 23 For more information, see RFC 3164.	No
device.cfg site.cfg	device.syslog. prependMac[1]	0 1—The phone's MAC address is prepended to the log message sent to the syslog server.	Yes
device.cfg site.cfg	device.syslog. renderLevel[1]	Specify the logging level for the lowest severity of events to log in the syslog. When you choose a log level, the log includes all events of an equal or greater severity level, but it excludes events of a lower severity level. 0 or 1—SeverityDebug(7). 2 or 3—SeverityInformational(6). 4—SeverityError(3). 5—SeverityCritical(2). 6—SeverityEmergency(0).	Yes

Device Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`device.cfg` `site.cfg`	`device.syslog.serverName`	Set the syslog server IP address or domain name string. IP address Domain name string	No
`device.cfg` `site.cfg`	`device.syslog.transport`	Set the transport protocol that the phone uses to write to the syslog server. None—Transmission is turned off but the server address is preserved. UDP TCP TLS	No

Monitoring, Diagnostics and Troubleshooting

This section lists the parameters for monitoring, diagnostics and troubleshooting.

Severity of Logging Event Parameters

You can configure the severity of the events that are logged independently for each module of the Polycom UC Software. This enables you to capture lower severity events in one part of the application, and high severity events for other components. Severity levels range from 0 to 6, where 0 is the most detailed logging and 6 captures only critical errors. Note that user passwords display in level 1 log files.

You must contact Polycom Customer Support to obtain the template file `techsupport.cfg` containing parameters that configure log levels.

Severity of Events Logged

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`techsupport.cfg`	`log.level.change.module_name`	Set the severity level to log for the module name you specify. Not all modules are available for all phone models. For a list of available module names, module descriptions, and log level severity, see the Web Configuration Utility at Settings > Logging > Module Log Level Limits.	

Log File Collection and Storage Parameters

You can configure log file collection and storage using the parameters in the following table.

You must contact Polycom Customer Support to obtain the template file `techsupport.cfg` containing parameters that configure log file collection and storage.

Log File Collection and Storage Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`techsupport.cfg`	`log.render.level`	Specify the events to render to the log files. Severity levels are indicated in brackets. 0　SeverityDebug (7) 1　SeverityDebug (7) - default 2　SeverityInformational (6) 3　SeverityInformational (6) 4　SeverityError (3) 5　SeverityCritical (2) 6　SeverityEmergency (0)	
`techsupport.cfg`	`log.render.file.size`	Set the maximum file size of the log file. When the maximum size is about to be exceeded, the phone uploads all logs that have not yet been uploaded and erases half of the logs on the phone. You can use a web browser to read logs on the phone. 512 kb (default) 1 - 10240 kB	
`techsupport.cfg`	`log.render.file.uplo ad.period`	Specify the frequency in seconds between log file uploads to the provisioning server. Note: The log file is not uploaded if no new events have been logged since the last upload. 172800 seconds (default) - 48 hours	
`techsupport.cfg`	`log.render.file.uplo ad.append`	1 (default) - Log files uploaded from the phone to the server are appended to existing files. You must set up the server to append using HTTP or TFTP. 0 - Log files uploaded from the phone to the server overwrite existing files. Note that this parameter is not supported by all servers.	

Log File Collection and Storage Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
techsupport.cfg	log.render.file.upload.append.sizeLimit	Specify the maximum size of log files that can be stored on the provisioning server. 512kb (default)	
techsupport.cfg	log.render.file.upload.append.limitMode	Specify whether to stop or delete logging when the server log reaches its maximum size. delete (default) - Delete logs and start logging again after the file reaches the maximum allowable size specified by `log.render.file.upload.append.sizeLimit`. stop - Stop logging and keep the older logs after the log file reaches the maximum allowable size.	

Scheduled Logging Parameters

Scheduled logging can help you monitor and troubleshoot phone issues. Use the parameters in this table to configure scheduled logging.

You must contact Polycom Customer Support to obtain the template file techsupport.cfg containing parameters that configure scheduled logging.

Scheduled Logging Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
techsupport.cfg	log.sched.x.name	Configure the number of debug commands you want to schedule an output for. You can configure x = 1-10 debug commands per phone. If x = 1, the default command name is 'showCpuLoad'. 9 (default) If x = 2, the default command name is 'showBatteryStat'. 22 (default) 3 - 10 = No default value Values: NULL memShow checkStack ls ifShow ifShowVerbose showProcesses showCpuUsage showCpuLoad ethBufPoolShow sysPoolShow netPoolShow netRxShow endErrShow routeShow netCCB arpShow fsShow ipStatShow udpStatShow sipPrt showBatteryStat	

The following table lists parameters you can use to control telephone notification events, state polling events, and push server controls.

Application Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`applicatio ns.cfg`	`apps.ucdesktop.Serve rPort`	The port number. Note: This value should be the same as the one that is used on the user's computer, otherwise the connection is not established. 24800 (default) 1 to 65535	No

The busy lamp field (BLF)/attendant console feature enhances support for phone-based monitoring. The maximum number of BLF entries for these phones is 50. The parameters listed in the following table are supported on the VVX 300 series, 400 series, 500 series, and 600 series phones.

In the following table, x in a parameter is the number of the BLF entry in the list. If you are using static BLF, you need to configure the number of each entry.

Busy Lamp Field / Attendant Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`attendant.behaviors.display.spontaneousCallAppearances.normal`	1 (default) - The normal or automatic call appearance is spontaneously presented to the attendant when calls are alerting on a monitored resource (and a ring tone is played). 0 - The call appearance is not spontaneously presented to the attendant. The information displayed after a press and hold of a resource's line key is unchanged by this parameter. Note that the values of these call appearance parameters depend on the values applied to `attendant.resourceList.x.type`. When this parameter is set to 0, the ringtone 'Ring Splash' does not play when `attendant.ringType="ringer14"`.	No
`features.cfg`	`attendant.behaviors.display.spontaneousCallAppearances.automata`	0 (default) - The call appearance is not spontaneously presented to the attendant. The information displayed after a press and hold of a resource's line key is unchanged by this parameter. Note that the values of these call appearance parameters depend on the values applied to `attendant.resourceList.x.type`. When this parameter is set to 0, the ringtone 'Ring Splash' does not play when `attendant.ringType="ringer14"`. 1 - The normal or automatic call appearance is spontaneously presented to the attendant when calls are alerting on a monitored resource (and a ring tone is played).	No

\<bg/\>

The parameters listed in the following table control how you display background images.

Background Image Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`bg.color.selection`	Specify which type of background (w) and index (x) for that type is selected on reboot. The default selection is 1,1 the first solid background. Use w=1 and x=1 (1,1) to select the built-in image. Use w=2 and x= 1 to 4 to select one of the four `solid` backgrounds. Use w=3 and x= 1 to 6 to select one of the six background `bm` images You can set backgrounds for specific phone models by adding the model name, for example: `bg.color.VVX500.selection`, `bg.color.VVX1500.selection` Note that although the VVX 300 series phones use a grayscale background, you can use this parameter to set the background. 1,1 (default) w,x	No
`features.cfg`	`bg.color.bm.x.name`	Specify the name of the phone screen background image file including extension with a URL or file path of a BMP or JPEG image. Note: If the file is missing or unavailable, the built-in default solid pattern is displayed.	No
`features.cfg`	`bg.color.bm.x.em.name`	Specify the name of the Expansion Module (EM) background image file including extension with a URL or file path of a BMP or JPEG image. Note: If the file is missing or unavailable, the built-in default solid pattern is displayed.	No

The following table specifies the Bluetooth parameter for the VVX 600/601 phone.

Bluetooth Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	`bluetooth.paired DeviceMemorySize`	10 (default) 0 - 10	No

The phone supports an optional per-registration feature that enables automatic call placement when the phone is off-hook.

The phone supports a per-registration configuration that determines which events cause the missed-calls counter to increment.

You can enable/disable missed call tracking on a per-line basis.

In the following table, x is the registration number.

To view the list of maximum registrations for each phone model see the table Flexible Call Appearances.

Call Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`call.advancedMis sedCalls.addToRe ceivedList`	Applies to calls on that are answered remotely. 0 (default) - Calls answered from the remote phone are not added to the local receive call list. 1 - Calls answered from the remote phone are added to the local receive call list.	No
`sip-interop.cfg`	`call.advancedMis sedCalls.enabled`	Use this parameter to improve call handling. 1 (default) - Shared lines can correctly count missed calls. 0 - Shared lines may not correctly count missed calls.	No

Call Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	call.advancedMissedCalls.reasonCodes	Enter a comma-separated list of reason code indexes interpreted to mean that a call should not be considered as a missed call. 200 (default)	No
reg-advanced.cfg	call.autoAnswer.micMute	1 (default) - The microphone is initially muted after a call is auto-answered. 0 - The microphone is active immediately after a call is auto-answered.	No
reg-advanced.cfg	call.autoAnswer.ringClass	The ring class 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 are overridden such that a ringtone of visual (no ringer) applies. ringAutoAnswer (default)	No
reg-advanced.cfg	call.autoAnswer.SIP	You can use this parameter on the VVX 3xx, 4xx, 5xx, 6xx, and 1500 business media phones. 0 (default) - Disable auto-answer for SIP calls. 1 - Enable auto-answer for SIP calls.	No
features,cfg	call.autoAnswerMenu.enable	1 (default) - The autoanswer menu displays and is available to the user. 0 - The autoanswer menu is disabled and is not available to the user.	No
sip-interop.cfg	call.BlindTransferSpecialInterop	0 (default) - Do not wait for an acknowledgment from the transferee before ending the call. 1 - Wait for an acknowledgment from the transferee before ending the call.	No
sip-interop.cfg	call.dialtoneTimeOut	The time is seconds that a dial tone plays before a call is dropped. 60 (default) 0 - The call is not dropped.	Yes

Call Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	call.internationalDialing.enabled	Use this parameter to enable or disable the key tap timer that converts a double tap of the asterisk "*" symbol to the "+" symbol used to indicate an international call. 1 (default) - A quick double tap of "*" converts immediately to "+". To enter a double asterisk "**", tap "*" once and wait for the key tap timer to expire to enter a second "*". 0 - You cannot dial"+" and you must enter the international exit code of the country you are calling from to make international calls. This parameter applies to all numeric dial pads on the phone including for example, the contact directory.	Yes
sip-interop.cfg, site.cfg	call.internationalPrefix.key	0 (default) 1	No
sip-interop.cfg	call.localConferenceEnabled	1 (default) - The feature to join a conference during an active call is enabled and you can establish conferences on the phone. 0 - The feature to join a conference during an active call is disabled. When you try to join the Conference, an 'Unavailable' message displays.	Yes
sip-interop.cfg	call.offeringTimeOut	Specify a time in seconds that an incoming call rings before the call is dropped. 60 (default) 0 - No limit. Note that the call diversion, no answer feature takes precedence over this feature when enabled.	Yes
sip-interop.cfg	call.playLocalRingBackBeforeEarlyMediaArrival	1 (default) 0	No

Call Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	call.ringBackTimeOut	Specify a time in seconds to allow an outgoing call to remain in the ringback state before dropping the call. 60 (default) 0 - No limit.	Yes
sip-interop.cfg, site.cfg	call.stickyAutoLineSeize	0 - Dialing through the call list uses the line index for the previous call. Dialing through the contact directory uses a random line index. 1 - The phone uses sticky line seize behavior. This helps with features that need a second call object to work with. The phone attempts to initiate a new outgoing call on the same SIP line that is currently in focus on the LCD. Dialing through the call list when there is no active call uses the line index for the previous call. Dialing through the call list when there is an active call uses the current active call line index. Dialing through the contact directory uses the current active call line index.	Yes

Call Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg,` `site.cfg`	`call.stickyAutoL ineSeize.onHookD ialing`	0 (default) 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. A hot dial occurs on the line which is currently in the call appearance. Any new call scenario seizes the next available line.	Yes
`site.cfg`	`call.teluri.show Prompt`	1 (default) 0	No
`sip-interop.cfg`	`call.switchToLoc alRingbackWithou tRTP`	0 (default) 1	No
`sip-interop.cfg`	`call.urlModeDial ing`	0 (default) - Disable URL dialing. 1 - Enable URL dialing.	Yes
`site.cfg`	`call.urlNumberMo deToggling`	0 (default) - URL mode is used for URL calls. 1 - Number mode is used for URL calls.	No

The call lists (or call log) parameters listed in the following table are supported on VVX 300 series, 400 series, 500 series, 600 series, and 1500 phones.

Call List Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg, features.cfg	callLists.colla pseDuplicates	1 (default) - Consecutive incomplete between the same party in the same direction (outgoing/incoming) are collapsed into one record with the most recent call displaying. 0 - All calls are archived and presented in the call lists.	No
site.cfg, features.cfg	callLists.logCo nsulationCalls	Consultation calls are calls made when adding a third party to a call while the second party is on hold. 0 (default) - Consultation calls are not logged. 1 - All consultation calls are logged.	No
site.cfg, features.cfg	callLists.size	The maximum number of retained records of each call list type including incoming, outgoing, and missed calls. When the maximum number is reached, new records overwrite existing records. You can clear the list using the phone's menu system. If you want to prevent the records from uploading to the provisioning server, enter a false URL in the CALL_LISTS_DIRECTORY field in the master configuration file. 99 (default) 10 - 99	No
site.cfg, features.cfg	callLists.write Delay.journal	The delay in seconds before changes due to an in-progress call are sent to the file system as a journal. 5 (default) 1 - 600	No
site.cfg, features.cfg	callLists.write Delay.terminate d	The minimum period in seconds between writing out the complete XML file to the local file system and, optionally, to the provisioning server. 60 (default) 10 - 65536	No

Use these parameters to enable and set up the remote packet capture feature.

Remote Packet Capture Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	diags.dumpcore.enabled	Determine whether the phone generates a core file if it crashes. 1 (default) 0	Yes
techsupport.cfg	diags.pcap.enabled	Enable or disable all on-board packet capture features. 0 (default) 1	No
techsupport.cfg	diags.pcap.remote.enabled	Enable or disable the remote packet capture server. 0 (default) 1	No
techsupport.cfg	diags.pcap.remote.password	Enter the remote packet capture password. <MAC Address> (default) alphanumeric value	No
techsupport.cfg	diags.pcap.remote.port	Specify the TLS profile to use for each application. 2002 (default) Valid TCP Port	No

Per-Registration Dial Plan Parameters

All of the parameters listed in the following table are per-registration parameters that you can configure instead of the general equivalent dial plan parameters. Note that the per-registration parameters override the general parameters where x is the registration number, for example, dialplan.x.applyToTelUriDial overrides dialplan.applyToTelUriDial for registration x.

The maximum number of registrations (x) for each phone model is listed in the table Flexible Call Appearances under the column *Registrations*.

Per-Registration Dial Plan (Digit Map) Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	dialplan.userDial.timeOut	0 – 99 seconds 0 (default for Generic Profile) 3 (default for Skype Profile)	No
site.cfg	dialplan.x.applyToCallListDial	0 1 (default)	Yes
site.cfg	dialplan.x.applyToDirectoryDial	0 (default) 1	Yes
site.cfg	dialplan.x.applyToForward	0 (default) or 1	No
site.cfg	dialplan.x.applyToTelUriDial	0 1 (default)	Yes
site.cfg	dialplan.x.applyToUserDial	0 1 (default)	Yes
site.cfg	dialplan.x.applyToUserSend	0 1 (default)	Yes
site.cfg	dialplan.x.conflictMatchHandling	0 (default for Generic Profile) 1 (default for Skype Profile)	No
site.cfg	dialplan.x.digitmap.timeOut	Null (default) string - max number of characters 100	Yes
site.cfg	dialplan.x.digitmap	Null (default) string - max number of characters 2560	Yes
site.cfg	dialplan.x.e911dialmask	Null (default) string - max number of characters 256	No
site.cfg	dialplan.x.e911dialstring	Null (default) string - max number of characters 256	No

Per-Registration Dial Plan (Digit Map) Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	dialplan.x.impossibleMatchHandling	0 (default) - Digits are sent to the call server immediately. 1 - A reorder tone is played and the call is canceled. 2 - No digits are sent to the call server until the Send or Dial key is pressed. 3 - No digits are sent to the call server until the Timeout configured by dialplan.userDial.timeOut.	Yes
site.cfg	dialplan.x.originaldigitmap	Null (default) string - max number of characters 2560	No
site.cfg	dialplan.x.removeEndOfDial	0 1 (default)	Yes
site.cfg	dialplan.x.routing.emergency.y.server.z	0 (default) 1 2 3 x, y, and z = 1 to 3	Yes
site.cfg	dialplan.x.routing.emergency.y.value	Null (default) string - max number of characters 64	Yes
site.cfg	dialplan.x.routing.server.y.address	Null (default) string - max number of characters 256	Yes
site.cfg	dialplan.x.routing.server.y.port	5060 (default) 1 to 65535	Yes
site.cfg	dialplan.x.routing.server.y.transport	DNSnaptr (default) TCPpreferred UDPOnly TLS TCPOnly	Yes

This parameter definition includes:

-   Polycom BroadSoft UC-One directory definitions
-   Local contact directory for GENBAND
-   The local directory definition

**

Use the parameters listed in the following table with the Polycom BroadSoft UC-One directory.

BroadSoft UC-One Directory Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.broadsoft.regMap	Specify the registration line credentials you want to use for BroadSoft R20 Server or later to retrieve directory information from the BroadSoft UC-One directory when dir.broadsoft.useXspCredentials=0. 1 (default) 0 - Const_NumLineReg	No
features.cfg	dir.broadsoft.useXspCredentials	Specify which method of credentials the phone uses to sign in with the BroadSoft server. 1 (default)—uses BroadSoft XSP credentials. 0—uses SIP credentials from dir.broadsoft.regMap.	No

<local/>

The next table lists parameters you can configure for your local contact directory. The maximum local directory size is limited based on the amount of flash memory in the phone and varies by phone model. For maximum number of contacts and maximum file size for phone models, refer to Local Contact Directory. Polycom recommends that you configure a provisioning server that allows uploads to ensure a back-up copy of the directory when the phone reboots or loses power.

Note that on the VVX 1500, the local directory is by default stored in the phone's non-volatile device settings and you have to option to use the phone's volatile RAM and set the maximum file size.

Local Contact Directory Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
debug.cfg	dir.local.nonVolatile.maxSize	On the VVX 1500, set the maximum file size of the local contact directory stored on the phone's non-volatile memory. VVX1500 = 100KB (default) 1 - 100KB	No
debug.cfg	dir.local.volatile	0 (default) - The VVX 1500 uses non-volatile memory for the local contact directory. 1 - The VVX 1500 enables the use of volatile memory for the local contact directory.	No
debug.cfg	dir.local.volatile.maxSize	On the VVX 1500, set the maximum file size of the local contact directory stored on the phone's volatile memory. VVX1500 = 200KB (default) 1 - 200KB	No

Elements for the Local Directory Parameters

The following table describes each of the parameter elements and permitted values that you can use in the local contact directory.

Local Contact Directory Parameter Elements

Element	Definition	Permitted Values
fn	First Name	UTF-8 encoded string of up to 40 bytes[1]
The contact's first name.		
ln	Last Name	UTF-8 encoded string of up to 40 bytes[1]
The contact's last name.		
ct	Contact	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL

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. The maximum field length is 128 characters.

Note: This field cannot be null or duplicated.

Local Contact Directory Parameter Elements

sd	Speed Dial Index	VVX=Null, 1 to 9999
		RealPresence Trio=20

Associates a particular entry with a speed dial key for one-touch dialing or dialing.

lb	Label	UTF-8 encoded string of up to 40 bytes[1]

The label for the contact. 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 first and last names form the label. A space is added between first and last names.
Note: For GENBAND, the **Label** element is shown as **Nick Name**, and is a mandatory, non-duplicate field.

pt	Protocol	SIP, H323, or Unspecified

The protocol to use when placing a call to this contact.

rt	Ring Tone	Null, 1 to 21

When incoming calls match a directory entry, this field specifies the ringtone to be used.

dc	Divert Contact	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL

The address to forward calls to if the Auto Divert feature is enabled.

ad	Auto Divert	0 or 1

If set to 1, callers that match the directory entry are diverted to the address specified for the divert contact element.
Note: If auto-divert is enabled, it has precedence over auto-reject.

ar	Auto Reject	0 or 1

If set to 1, callers that match the directory entry specified for the auto-reject element are rejected.
Note: If auto divert is also enabled, it has precedence over auto reject.

bw	Buddy Watching	0 or 1

If set to 1, this contact is added to the list of watched phones.

bb	Buddy Block	0 or 1

If set to 1, this contact is blocked from watching this phone.

[1]In some cases, this will be less than 40 characters due to UTF-8's variable bit length encoding.

The parameters include:

- DNS-A
- DNS-NAPTR
- DNS-SRV

You can enter a maximum of 12 record entries for DNS-A, DNS-NAPTR, and DNS-SRV. records.

Use the following tables to configure the enhanced feature key (EFK) feature on your phone:

Enhanced Feature Key (EFK) Version Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features. cfg	efk.version	The version of the EFK elements. This parameter is not required if there are no `efk.efklist` entries. 2 (default) - Supported version for SIP 3.1 and later. 1 - Supported version for or SIP 3.0.x or earlier. Null - Disables the EFK feature.	No

Enhanced Feature Key (EFK) Soft Key Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	efk.softkey.alignleft	Use this parameter to left-align soft keys and remove blank soft keys from the order. 0 (default) 1 - Left-aligns soft keys and removes blank soft keys from the order Note: This parameter does not work with custom soft keys.	No

The feature parameters listed in the following table control the activation or deactivation of a feature at run time.

Feature Activation/Deactivation Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features .cfg	feature.bluetoot h.enabled	VVX 600/601 high-security environments. 1 (default) - Enables the Bluetooth feature. 0 - Disables the Bluetooth feature.	No
features .cfg	feature.callCent erCallInformatio n.enable	1 (default) - The phone displays a full-screen popup showing call information details. The popup closes after 30 seconds or you can press the **Exit** button to close it and return to the active call screen. 0 - The phone uses the active call screen and ACD call information is not available.	No
features .cfg	feature.callCent erStatus.enabled	0 (default) - Disable the status event threshold capability. 1 - Enable the status event threshold capability to display at the top of the phone screen.	No
features .cfg	feature.callList .enabled	1 (default) - Enables the locally controlled call list. 0 - Disables the locally controlled call list. To enable the missed, placed, or received call lists, feature.callList.enabled must be enabled.	Yes
features .cfg	feature.callList Missed.enabled	1 (default) - Enables the missed call list. 0 - Disables the missed call list. To enable the missed, placed, or received call lists, feature.callList.enabled must be enabled.	Yes
features .cfg	feature.callList Placed.enabled	1 (default) - Enables the placed call list. 0 - Disables the placed call list. To enable the missed, placed, or received call lists, feature.callList.enabled must be enabled.	Yes

Feature Activation/Deactivation Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features .cfg	feature.callList Received.enabled	1 (default) - Enables the received call list. 0 - Disables the received call list. To enable the missed, placed, or received call lists, feature.callList.enabled must be enabled.	Yes
features .cfg	feature.callReco rding.enabled	Available for devices with a USB port. 0 (default) - Disables the call recording and playback feature. 1 - Enables the call recording and playback feature.	Yes
features .cfg	feature.contacts .enabled	1 (default) - Enables display of the Contacts icon displays on the Home screen, the global menu, and in the dialer. 0 - Disables display of the Contacts icon displays on the Home screen, the global menu, and in the dialer. Requires UCS 5.4.2 RevAA or higher.	No
features .cfg	feature.corporat eDirectory.enabl ed	0 (default) - Disables the corporate directory feature. 1 - Enables the corporate directory feature.	No
features .cfg	feature.director y.enabled	1 (default) - Enables the local contact directory. 0 - Disables the local contact directory.	No
features .cfg	feature.doNotDis turb.enable	1 (default) - Enables do not disturb (DND). 0 - Disables do not disturb (DND). Users cannot enable DND and the option is removed from the phone's Features menu.	Yes
features .cfg	feature.enhanced CallDisplay.enab led	0 (default) - The phone displays the protocol at the end of the called party identification (for example, 1234567 [SIP]). 1 - The phone displays the number only (for example, 1234567).	No

Feature Activation/Deactivation Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features .cfg	feature.flexible LineKey.enable	0 (default) - Disables the Flexible Line Key feature. 1 - Enables the Flexible Line Key feature. Not available on the VVX 101, 201, or 1500 business media phones.	No
features .cfg	feature.forward. enable	1 (default) - Enables call forwarding. 0 - Disables call forwarding. Users cannot use Call Forward and the option is removed from the phone's Features menu.	No
features .cfg	feature.hoteling .enabled	0 (default) - Disable Hoteling. 1 - Enable Hoteling.	No
features .cfg	feature.nonVolat ileRingerVolume. enabled	1 (default) - User changes to the ringer volume are saved and maintained after the phone reboots. 0 - User changes to the ringer volume are reset to default after the phone reboots.	No
features .cfg	feature.persiste ntMute.enabled	0 (default) - Mute ends when the active call ends or when the phone restarts. 1 - Enable the persistent mute feature.	Yes
features .cfg	feature.ringDown load.enabled	1 (default) - The phone downloads ringtones when starting up. 0 - The phone does not download ringtones when starting up.	Yes
features .cfg	feature.uniqueCa llLabeling.enabl ed	0 (default) - Disable Unique Call Labeling. 1 - Enable Unique Call Labeling. Use reg.x.line.y.label to define unique labels.	Yes
features .cfg	feature.urlDiali ng.enabled	1 (default) - URL/name dialing is available from private lines, and unknown callers are identified on the display by their phone's IP address. 0 - URL/name dialing is not available.	No

The phone contains a local Web Configuration Utility server for user and administrator features. Note that several of these parameters can be used with Microsoft Skype for Business Server and the parameter values listed in the table Enable Web Configuration Utility have two default states: a generic default value for UC Software 5.1.0 and a different value when the phone is registered with Skype for Business Server. The following table lists the default values for both states where applicable.

The web server supports both basic and digest authentication. The authentication user name and password are not configurable for this release.

HTTPD Web Server Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`httpd.enabled`	Base Profile = Generic 1 (default) - The web server is enabled. 0 - The web server is disabled. Base Profile = Skype 0 (default) - The web server is disabled. 1 - The web server is enabled.	Yes
`site.cfg`	`httpd.cfg.enabled`	Base Profile = Generic 1 (default) - The Web Configuration Utility is enabled. 0 - The Web Configuration Utility is disabled. Base Profile = Skype 0 (default) - The Web Configuration Utility is disabled. 1 - The Web Configuration Utility is enabled.	Yes
`site.cfg`	`httpd.cfg.port`	Port is 80 for HTTP servers. Take care when choosing an alternate port. 80 (default) 1 to 65535	Yes

HTTPD Web Server Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	httpd.cfg.secureTunnelPort	The port to use for communications when the secure tunnel is used. 443 (default) 1 to 65535	Yes
site.cfg	httpd.cfg.secureTunnelRequired	1 (default) - Access to the Web Configuration Utility is allowed only over a secure tunnel (HTTPS) and non-secure (HTTP) is not allowed. 0 - Access to the Web Configuration Utility is allowed over both a secure tunnel (HTTPS) and non-secure (HTTP).	Yes

The following table lists parameters that configure the phone's Home screen display.

Home Screen Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	homeScreen.application.enable	1 (default) - Enable display of the Applications icon on the phone Home screen. 0 - Enable display of the Applications icon on the phone Home screen.	No
features.cfg	homeScreen.calendar.enable	1 (default) - Enable display of the Calendar icon on the phone Home screen. 0 - Disable display of the Calendar icon on the phone Home screen.	No
features.cfg	homeScreen.directories.enable	1 (default) - Enable display of the Directories menu icon on the phone Home screen. 0 - Disable display of the Directories menu icon on the phone Home screen.	No

Home Screen Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`homeScreen.doNotDisturb.enable`	1 (default) - VVX 0 (default) - RealPresence Trio 1 - Enable display of the DND icon on the phone Home screen. 0 - Disable display of the DND icon on the phone Home screen.	No
`features.cfg`	`homeScreen.features.enable`	1 (default) - Enable display of the Features menu icon on the phone Home screen. 0 - Disable display of the Features menu icon on the phone Home screen.	No
`features.cfg`	`homeScreen.forward.enable`	1 (default) - Enable display of the call forward icon on the phone Home screen. 0 - Disable display of the call forward icon on the phone Home screen.	No
`features.cfg`	`homeScreen.messages.enable`	1 (default) - Enable display of the Messages menu icon on the phone Home screen. 0 - Disable display of the Messages menu icon on the phone Home screen.	No
`features.cfg`	`homeScreen.newCall.enable`	1 (default) - Enable display of the New Call icon on the phone Home screen. 0 - Disable display of the New Call icon on the phone Home screen.	No
`features.cfg`	`homeScreen.redial.enable`	1 - VVX 0 - RealPresence Trio 1 - Enable display of the Redial menu icon on the phone Home screen. 0 - Disable display of the Redial menu icon on the phone Home screen.	No

Home Screen Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	homeScreen.settings.enable	1 (default) - Enable display of the Settings menu icon on the phone Home screen. 0 - Disable display of the Settings menu icon on the phone Home screen.	No
features.cfg	homeScreen.status.enable	1 (default) - Enable display of the Status menu icon on the phone Home screen. 0 - Disable display of the Status menu icon on the phone Home screen.	No

<key/>

The next table lists parameters that enable you to change the default functions of your phone's keypad keys, a process also known as remapping. If you want to change the default function of a key, you must specify the phone model number, the key you want to change, and a new function for the key.

● For a list of products and their model codes, see the section Product, Model Code, and Part Number Mapping.

● To find the key number, location of the key on each phone model, and default key functions, refer to the section Define the Phone Key Layout.

● For a list of parameter values you can assign as functions to a phone key, refer to the table Keypad Key Functions.

> **Caution: Key remapping is not recommended**
> Polycom does not recommend remapping or changing the default functions of the keys on your phone.

Key Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`key.x.y.function.prim`	Specify a phone model, key number, and function. x can be one of the VVX 300 series, 400 series, 500 series, 600 series, or VVX1500 phones. y can be one key number. For a list of functions refer to the table Keypad Key Functions	Yes

The following table lists the functions that are available for phone keys.

Keypad Key Functions

Answer	Dialpad2	Handsfree	MyStatus	SpeedDialMenu
ArrowDown	Dialpad3	Headset	Null	Talk
ArrowLeft	Dialpad4	Hold	Offline	Video
ArrowRight	Dialpad5	Home	Redial	VolDown
ArrowUp	Dialpad6	Line2	Release	VolUp
Back	Dialpad8	Line3	Select	
BuddyStatus	Dialpad9	Line4	Setup	
CallList	DialpadStar	Line5	SoftKey1	
Conference	DialPound	Line6	SoftKey2	
Delete	Directories	Messages	SoftKey3	
Dialpad0	DoNotDisturb	Menu	SoftKey4	
Dialpad1	Green	MicMute	SpeedDial	

Example Custom Key Configurations

This section provides several custom key configuration examples.

To remap the volume up key to answer a call on the VVX 300:

» Update the configuration file as follows: `key.VVX300.6.function.prim="Answer"`

» **To remap the volume down key to launch the Settings menu on the VVX 300 using a macro:**

» Update the configuration file as follows:

➢ `key.VVX300.7.function.prim="$Msetting$"`

➢ `efk.efklist.1.action.string="$FSetup$"`

➢ `efk.efklist.1.mname="setting"`

➢ `efk.efklist.1.status="1"`

To remap the Mute key to launch the Forward Menu on the VVX 500 using EFK.

» Update the configuration file as follows: `key.VVX500.18.function.prim="$FDivert$"`

To remap the Transfer key to phone lock using an EFK macro:

» Update the configuration file as follows: `key.37.function.prim="$FLockPhone$"`

To remap the Redial key:

» Update the configuration file as follows:

```
key.36.function.prim="http://vanoem02.vancouver.polycom.com:8080/MicroBrowserTest.html
"
```

You can configure the language you want the Polycom phone user interface to operate and display in. The phones support both North American and international time and date formats.

> Note: Edit the language parameters using a multilingual XML editor. If you do not use an XML editor, some of the language labels in the configuration file and in the language menu on the phone display incorrectly. 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`.

This parameter definition includes:

● Multilingual definitions
● Date and time definitions

<ml/>

The multilingual parameters listed in the following table are based on string dictionary files downloaded from the provisioning server. These files are encoded in XML format and include space for user-defined languages.

Multilingual Parameters

Templ ate	Parameter	Permitted Values	Change Causes Restart or Reboot
site. cfg	lcl.ml.lang.charset	Provides the language character set. Null (default) String	Yes
site. cfg	lcl.ml.lang.clock.x. 24HourClock	Overrides the lcl.datetime.time.24HourClock parameter. 1 (default) - Displays the time in 24-hour clock mode. 0 - Does not display the time in 24-hour clock mode.	No
site. cfg	lcl.ml.lang.clock.x. dateTop	Overrides the lcl.datetime.date.dateTop parameter. 1 (default) - Displays date above time. 0 - Displays date below time.	No
site. cfg	lcl.ml.lang.clock.x. format	Overrides the lcl.datetime.date.format parameter to display the day and date. "D,dM" (default) String 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 = Thursday, 3 July or Md,D = July 3, Thursday.	No
site. cfg	lcl.ml.lang.clock.x. longFormat	Overrides the lcl.datetime.date.longFormat parameter. 1 (default) - Displays the day and month in long format (Friday/November). 0 - Displays the day and month in abbreviated format (Fri/Nov).	No

Multilingual Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	lcl.ml.lang.japanese.font.enabled	0 (default) - The phone does not display the Japanese Kanji character font. 1 - The phone displays the Japanese Kanji character font. This parameter applies to RealPresence Trio, VVX 400, 401, 410, 411, 500, 501, 600, 601, and 1500.	Yes
region.cfg	lcl.ml.lang.list	Displays the list of languages supported on the phone. All (default) String	Yes

The basic character support includes the Unicode character ranges listed in the next table.

Unicode Ranges for Basic Character Support

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

<license/>

The parameters listed in the next table enable you to configure the feature licensing system.

Once the license is installed on a phone, it cannot be removed.

Feature License Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	license.polling.time	Specifies the time (using the 24-hour clock) to check if the license has expired. 02:00 (default 00:00 - 23:59	Yes

The event logging system supports the classes of events listed in the table Logging Levels. Two types of logging are supported:

- level, change, and render
-

Note: Logging parameter changes can impair system operation. Do not change any logging parameters without prior consultation with Polycom Technical Support.

Logging Levels

Logging Level	Interpretation
0	Debug only
1	High detail class event
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

Three formats available for the event timestamp are listed in the next table.

Event Timestamp Formats

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

<level/> <change/> and <render/>

This configuration parameter is defined in the following table.

Logging Level, Change, and Render Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
techsupport.cfg	log.level.change.xxx	Controls the logging detail level for individual components. These are the input filters into the internal memory-based log system. 4 (default) 0 - 6 Possible values for xxx are acom, ares, app1, bluet, bdiag, brow, bsdir, cap, cdp, cert, cfg, cipher, clink, clist, cmp, cmr, copy, curl, daa, dapi, dbs, dbuf, dhcpc, dis, dock, dot1x, dns, drvbt, ec, efk, ethf, flk, h323, hset, httpa, httpd, hw, ht, ib, key, ldap, lic, lldp, loc, log, mb, mobil, net, niche, ocsp, osd, pcap, pcd, pdc, peer, pgui, pmt, poll, pps, pres, pstn, ptt, push, pwrsv, rdisk, res, rtos, rtls, sec, sig, sip, slog, so, srtp, sshc, ssps, style, sync, sys, ta, task, tls, trace, ttrs, usb, usbio, util, utilm, vsr, wdog, wmgr, and xmpp.	No
techsupport.cfg	log.level.change.flk	Sets the log level for the FLK logs. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.mr	Initial logging level for the Networked Devices log module. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.mraud	Initial logging level for the Networked Devices Audio log module. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.mrmgr	Initial logging level for the Networked Devices Manager log module. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.prox	Initial logging level for the Proximity log module. 4 (default) 0 - 6	No

Logging Level, Change, and Render Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
techsuppo rt.cfg	log.level.change. ptp	Initial logging level for the Precision Time Protocol log module. 4 (default) 0 - 6	No
techsuppo rt.cfg	log.level.change. sopi	Specify the SOPI service log level for the GENBAND Global Address Book and Personnel Address Book. 4 (default) 0 - 6	No
techsuppo rt.cfg	log.render.file	Polycom recommends that you do not change this value. 1 (default) 0	No
techsuppo rt.cfg	log.render.realti me	Polycom recommends that you do not change this value. 1 (default) 0	No
techsuppo rt.cfg	log.render.stdout	Polycom recommends that you do not change this value. 0 (default) 1	No
techsuppo rt.cfg	log.render.type	Refer to the table Event Timestamp Formats for timestamp type. 2 (default) 0 - 2	No

<sched/>

The phone can be configured to schedule certain advanced logging tasks on a periodic basis. Polycom recommends that you set the parameters listed in the next table in consultation with Polycom Technical Support. Each scheduled log task is controlled by a unique parameter set starting with log.sched.x where *x* identifies the task. A maximum of 10 schedule logs is allowed.

Logging Schedule Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`techsupport.cfg`	`log.sched.x.level`	The event class to assign to the log events generated by this command. 3 (default) 0 - 5 This needs to be the same or higher than `log.level.change.slog` for these events to display in the log.	No
`techsupport.cfg`	`log.sched.x.name`	Specifies the name of an internal system command to be periodically executed. Null (default) Alphanumeric string	No
`techsupport.cfg`	`log.sched.x.period`	Specifies the time in seconds between each command execution. 15 (default) positive integer	No
`techsupport.cfg`	`log.sched.x.startDay`	When startMode is abs, specifies the day of the week to start command execution. 1=Sun, 2=Mon, ..., 7=Sat 7 (default) 0 - 7	No
`techsupport.cfg`	`log.sched.x.startMode`	Starts at an absolute or relative time to boot. Null (default) 0 - 64	No
`techsupport.cfg`	`log.sched.x.startTime`	Displays the start time in seconds since boot when startMode is rel or displays the start time in 24-hour clock format when startMode is abs. Null (default) positive integer, hh:mm	No

\<mb/\>

The next table lists parameters that configure the home page, proxy, and size limits used by the microbrowser and browser when selected to provide services. The microbrowser and web browser are supported on the VVX 300 series, 400 series, 500 series, 600 series, and 1500 phones.

Microbrowser and Web Browser Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`applications.cfg`	`mb.idleDisplay.home`	Displays the URL of the microbrowser home page when the microbrowser Home page screen is idle. Null (default) valid HTTP URL, String (maximum 255 characters) For example: `http://www.example.com/xhtml/frontpage`. The microbrowser idle display displaces the idle display indicator.	No
`applications.cfg`	`mb.idleDisplay.refresh`	0 (default) - The microbrowser's idle display does not refresh Integer > 5 - Displays the microbrowser's idle display refresh time period in seconds. If an HTTP Refresh header is detected, it is respected, even if this parameter is set to 0. The refresh parameter is respected only in the event that a refresh fails. Once a refresh is successful, the value in the HTTP refresh header, if available, is used.	No
`applications.cfg`	`mb.idleRefresh.onFailure`	Helps reduce the requests from the phone when the idle display server is unavailable and specifies a delay in seconds when the phone sends refresh requests to the idle browser. This delay applies only when the server returns HTTP 5xx errors. 60 seconds (default) 60 - 655350 seconds To control the refresh times when the server is functioning, use `mb.idleDisplay.refresh`.	No
`applications.cfg`	`mb.main.autoBackKey`	1 (default) - The phone automatically supplies a **Back** soft key in all main browser screens. 0- The phone does not provide a **Back** soft key.	Yes

Microbrowser and Web Browser Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applicati ons.cfg	mb.main.home	Specifies the URL of the microbrowser's home page. For example: `http://www.example.com/xhtml/f rontpage/home`. Null (default) valid HTTP URL, String (maximum 255 characters)	No
applicati ons.cfg	mb.main.idleTime out	Specifies the timeout in seconds for the interactive browser. If the interactive browser remains idle for a defined period of time, the phone returns to the idle browser. If set to 0, there is no timeout. 40 (default) 0 - 600	No
applicati ons.cfg	mb.main.loadWebI mages	1 (default) - Enables the loading of images in a browser. 0 - Disables the loading of images in a browser.	No
applicati ons.cfg	mb.main.reloadPa ge	0 (default) - The microbrowser displays the content of the most recently viewed web page 1 - The microbrowser loads the URL configured in `mb.main.home` each time the browser is launched.	No
applicati ons.cfg	mb.main.statusba r	0 (default) - The status bar does not gets displayed. 1 - The status bar and status messages are displayed.	No
applicati ons.cfg	mb.main.toolbar. autoHide.enabled	1 (default) - The toolbar is not displayed. 0 - The toolbar displays continuously.	No
applicati ons.cfg	mb.main.proxy	Specifies the address of the HTTP proxy to be used by the microbrowser. Null (port: 8080) (default) domain name or IP address in the format <address>:<port>	No

The next table lists parameters you can use to configure the message-waiting feature, which is supported on a per-registration basis.

The maximum number of registrations (x) for each phone model is listed in the table Flexible Call Appearances under the column *Registrations*.

Message Waiting Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`sip-inter op.cfg`	`msg.bypassInstant Message`	0 (default) -Displays the menus Message Center and Instant Messages on pressing **Messages** or **MSG** key. 1 - Bypasses these menus and goes to voicemail.	No
`sip-inter op.cfg`	`msg.mwi.x.led`	0 (default) - Red MWI LED does **not** flash when there are new unread messages for the selected line. 1 - The LED flashes as long as there are new unread voicemail messages for any line in which this is parameter is enabled. Also, x is an integer referring to the registration indexed by reg.x.	No

The parameters listed in this section control the Ethernet interface maximum transmission unit (MTU) on VVX business media phones.

Ethernet Interface MTU Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`net.interface.mtu`	Configures the Ethernet or Wi-Fi interface maximum transmission unit (MTU) on the VVX business media phones or RealPresence Trio solution. 1496 (default) 800 - 1500 This parameter affects the LAN port and the PC port.	No
`site.cfg`	`net.interface.mtu6`	Specifies the MTU range for IPv6. 1500 (default) 1280 - 1500	No
`sip-interop.cfg`	`net.lldp.extenedDiscovery`	Specifies the duration of time that LLDP discovery continues after sending the number of packets defined by the parameter `lldpFastStartCount`. 0 (default) 0 - 3600 The LLDP packets are sent every 5 seconds during this extended discovery period.	No

The next table lists parameters you can configure for the presence feature. Note that the parameter `pres.reg` is the line number used to send SUBSCRIBE. If this parameter is missing, the phone uses the primary line to send SUBSCRIBE.

Presence Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`pres.idleTimeoutoffHours.enabled`	1 (default) - Enables the off hours idle timeout feature. 0 - Disables the off hours idle timeout feature.	No
`features.cfg`	`pres.idleTimeout.officeHours.enabled`	1 (default) - Enables the office hours idle timeout feature 0 - Disables the office hours idle timeout feature	No

<prov/>

The parameters listed in the next table control the provisioning server system for your phones.

Provisioning Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`prov.autoConfigUpload.enabled`	1 (default) - Enables the automatic upload of configuration files from the phone or Web configuration utility to the provisioning server. 0 - Disabled the automatic upload of configuration files from the phone or Web configuration utility to the provisioning server.	No
`site.cfg`	`prov.configUploadPath`	Specifies the directory path where the phone uploads the current configuration file. Null (default) String	No
`site.cfg`	`prov.login.lcCache.domain`	The user's domain name to sign-in. Null (default) String	No
`site.cfg`	`prov.login.lcCache.user`	The user's sign-in name to login. Null (default) String	No
`site.cfg`	`prov.login.password.encodingMode`	The default encoding mode for the text in the Password field on the User Login screen. 123 (default) Alphanumeric	No

Provisioning Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	prov.login.userId.encodingMode	The default encoding mode for the text in the User ID field on User Login screen. Abc (default) Alphanumeric	No
region.cfg	prov.loginCredPwdFlushed.enabled	1 (default) - Resets the password field when the user logs in or logs out. 0 - Does not reset the password field when the user logs in or logs out.	No
site.cfg	prov.startupCheck.enabled	1 (default) - The phone is provisioned on startup. 0 - The phone is not provisioned on startup.	No
site.cfg	prov.quickSetup.limitServerDetails	0 (default) - Provide all the necessary details for the given fields. 1 - Enter only the user name and password fields. Other details are taken from ztp/dhcp (option66).	No
site.cfg	prov.usercontrol.enabled	0 (default) - The phone does not display the software update notification and other options. Reboots automatically to perform software upgrade. 1 - The phone displays the software update notification and other options.	No
site.cfg	prov.usercontrol.postponeTime	Sets the time interval for software update notification using the HH:MM format. 02:00 (default) 00:15 01:00 02:00 04:00 06:00	No

The parameters listed in the following table configure the phone's behavior when a request for restart or reconfiguration is received.

Configuration Request Parameter

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	request.delay.type	Specifies whether the phone should restart or reconfigure. call (default) - The request will be executed when there are no calls. audio - The request will be executed when there is no active audio.	Yes

</sec>

The parameters listed in the next table configure security features of the phone.

General Security Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.tagSerialNo	0 (default) - The phone does not display the serial number. 1 - The phone displays the serial number through protocol signaling.	Yes

This parameter also includes:

-
-
- <dot1x>
- <dot1x>
-
- <TLS/>

<encryption/>

The next table lists available encryption parameters

File Encryption Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.encryption.upload.callLists	0 (default) - The call list is uploaded without encryption. 1 - The call list is uploaded in encrypted form.	Yes
site.cfg	sec.encryption.upload.config	0 (default) - The file is uploaded without encryption and replaces the phone specific configuration file on the provisioning server. 1 - The file is uploaded in encrypted form and replaces the existing phone specific configuration file on the provisioning server.	No
site.cfg	sec.encryption.upload.dir	0 (default) - The contact directory is uploaded without encryption and replaces the phone specific contact directory on the provisioning server. 1 - The contact directory is uploaded in encrypted form and replaces the existing phone specific contact directory on the provisioning server.	Yes
site.cfg	sec.encryption.upload.overrides	0 (default) - The MAC address configuration file is uploaded without encryption and replaces the phone specific MAC address configuration file on the provisioning server. 1 - The MAC address configuration file is uploaded in encrypted form and replaces the existing phone specific MAC address configuration file on the provisioning server.	No

<srtp/>

As per RFC 3711, you cannot turn off authentication of RTCP. The next table lists SRTP parameters.

SRTP Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	sec.srtp.answerWithNewKey	1 (default) - Provides a new key when answering a call. 0 - Does not provide a new key when answering the call.	No
sip-interop.cfg	sec.srtp.enable	1 (default) - The phone accepts the SRTP offers. 0 - The phone declines the SRTP offers. The defaults for SIP 3.2.0 is 0 when Null or not defined.	Yes
sip-interop.cfg	sec.srtp.key.lifetime	Specifies the lifetime of the key used for the cryptographic parameter in SDP. Null (default) - 0 - The master key lifetime is not set. Positive integer minimum 1024 or power of 2 notation - The master key lifetime is set. Setting this parameter to a non-zero value may affect the performance of the phone.	Yes
sip-interop.cfg	sec.srtp.mki.enabled	0 (default) - The phone sends two encrypted attributes in the SDP, one with MKI and one without MKI when the base profile is set as Generic. 1 - The phone sends only one encrypted value without MKI when the base profile is set as Skype.	Yes
sip-interop.cfg	sec.srtp.mki.startSessionAtOne	0 (default) - The phone uses MKI value of 1. 1 - The MKI value increments for each new crypto key.	No
sip-interop.cfg	sec.srtp.padRtpToFourByteAlignment	0 (default) - The RTP packet padding is not required when sending or receiving video. 1 - The RTP packet padding is required when sending or receiving video.	Yes

SRTP Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	sec.srtp.require	0 (default) - The secure media streams are not required. 1 - The phone is only allowed to use secure media streams.	Yes
sip-interop.cfg	sec.srtp.requireMatchingTag	1 (default) - The tag values must match in the crypto parameter. 0 - The tag values are ignored in the crypto parameter.	Yes
sip-interop.cfg	sec.srtp.simplifiedBestEffort	1 (default) - The SRTP is supported with Microsoft Description Protocol Version 2.0 Extensions. 0 - The SRTP is not supported with Microsoft Description Protocol Version 2.0 Extensions.	No

<dot1x><eapollogoff/>

The next table lists configurable parameters.

802.1X EAP over LAN (EAPOL) Logoff Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.dot1x.eapollogoff.enabled	0 (default) - The phone does not send an EAPOL Logoff message. 1 - The phone sends an EAPOL Logoff message.	Yes
site.cfg	sec.dot1x.eapollogoff.lanlinkreset	0 (default) - The phone does not reset the LAN port link. 1 - The phone resets the LAN port link.	Yes

<hostmovedetect/>

The next table lists configurable parameters.

Host Movement Detection Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.c fg	sec.hostmovede tect.cdp.enabl ed	0 (default) - The phone does not send a CDP packet. 1 - The phone sends a CDP packet.	Yes
site.c fg	sec.hostmovede tect.cdp.sleep Time	Controls the frequency between two consecutive link-up state change reports. 1000 (default) 0 to 60000 If sec.hostmovedetect.cdp.enabled is set to 1, there is an x microsecond time interval between two consecutive link–up state change reports, which reduces the frequency of dispatching CDP packets.	Yes

<TLS/>

The next table lists configurable TLS parameters. For the list of configurable ciphers, refer to the table Configurable TLS Cipher Suites.

This parameter also includes:

-
-

TLS Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.c fg	sec.TLS.browse r.cipherList	The cipher list is for browser. The format for the cipher list uses OpenSSL syntax found at: https://www.openssl.org/docs/man1.0.2 /apps/ciphers.html. NoCipher (default) String	No
site.c fg	sec.TLS.custom DeviceCert.x	The custom device certificate for TLS Application Profile x (x= 1 to 6). Null (default) String	No

TLS Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`sec.TLS.LDAP.cipherList`	The cipher list for the corporate directory. The format for the cipher list uses OpenSSL syntax found here: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html. NoCipher (default) String	No
`site.cfg`	`sec.TLS.LDAP.strictCertCommonNameValidation`	1 (default) - Requires to validate the server certificate during an LDAP or LDAPS connection over TLS. 0 - Does not require to validate the server certificate during an LDAP or LDAPS connection over TLS.	No
`site.cfg`	`sec.TLS.profileSelection.SOPI`	Select the platform profile required for the phone. PlatformProfile1 (default) 1 - 7	No
`site.cfg`	`sec.TLS.profile.webServer.cipherSuiteDefault`	1 (default) - The phone uses the default cipher suite for web server profile. 0 - The custom cipher suite is used for web server profile.	No
`site.cfg`	`sec.TLS.prov.cipherList`	The cipher list for provisioning. The format for the cipher list uses OpenSSL syntax found here: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html. NoCipher (default) String	No
`site.cfg`	`sec.TLS.SIP.cipherList`	The cipher list for SIP. The format for the cipher list uses OpenSSL syntax found here: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html. NoCipher (default) String	No
`site.cfg`	`sec.TLS.SIP.strictCertCommonNameValidation`	1 (default) - The common name validation is enabled for SIP. 0 - The common name validation is not enabled for SIP.	No

TLS Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.TLS.SOPI.cipherList	Selects a cipher key from the list of available ciphers. NoCipher (default) 1 – 1024 character string	No
site.cfg	sec.TLS.SOPI.strictCertCommonNameValidation	Controls the strict common name validation for the URL provided by the server. 1 (default) - The SOPI verifies the server certificate to match commonName/SubjectAltName against the server hostname. 0 - The SOPI will not verify the server certificate for commonName/SubjectAltName against the server hostname.	No
site.cfg	sec.TLS.syslog.cipherList	The cipher list for syslog. The format for the cipher list uses OpenSSL syntax found here: https://www.openssl.org/docs/man1.0.2/apps/ciphers.html NoCipher (default) String	No

Profiles are a collection of related security parameters. The next table lists TLS profile parameters. There are two platform profiles and six application profiles.

You can configure the parameters listed in the next table to choose the platform profile or application profile to use for each TLS application.

The permitted values are:

- PlatformProfile1
- PlatformProfile2
- ApplicationProfile1
- ApplicationProfile2
- ApplicationProfile3
- ApplicationProfile4
- ApplicationProfile5
- ApplicationProfile6

● ApplicationProfile7

TLS Profile Selection Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`sec.TLS.profileSelection.browser`	Specifies to select a TLS platform profile or TLS application profile for the browser or a microbrowser. PlatformProfile1 (default) TLS profile	No
`site.cfg`	`sec.TLS.profileSelection.LDAP`	Specifies to select a TLS platform profile or TLS application profile for the corporate directory. PlatformProfile1 (default) TLS profile	No
`site.cfg`	`sec.TLS.profileSelection.SIP`	Specifies to select a TLS platform profile or TLS application profile for SIP operations. PlatformProfile1 (default) TLS profile	No
`site.cfg`	`sec.TLS.profileSelection.syslog`	Specifies to select a TLS platform profile for the syslog operations. PlatformProfile1 (default) PlatformProfile1 or PlatformProfile2	No
`site.cfg`	`sec.TLS.profileSelection.SOPI`	Specifies to select a TLS platform profile or TLS application profile for the GENBAND "Subscriber Open Provisioning Interface" (SOPI). PlatformProfile1 (default) TLS profile	No

\<softkey/\>

You can use the soft key parameters to customize soft keys on the phone interface. Note that `feature.enhancedFeatureKeys.enabled` must be enabled (set to 1) to use the Configurable Soft Key feature.

In the following table listing soft key configuration parameters, x=1 to a maximum number of 10 soft keys.

Soft Key Customization Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	softkey.feature.basicCallManagement.redundant	1 (default) - Displays the **Hold**, **Transfer**, and **Conference** soft keys. 0 - Does not display the **Hold**, **Transfer**, and **Conference** soft keys.	No
features.cfg	softkey.feature.buddies	1 (default) - Displays the **Buddies** soft key. 0 - Does not display the **Buddies** soft key.	No
features.cfg	softkey.feature.callers	0 (default) - Displays the **Callers** soft key for all platforms. 1 - Does not display the **Callers** soft key for all platforms.	No
features.cfg	softkey.feature.directories	1 (default) - Displays the Directories (Dir) soft key. 0 - Does not display the Directories (Dir) soft key.	Yes
features.cfg	softkey.feature.doNotDisturb	1 (default) - Enables the **DND** soft key. 0 - Disables the **DND** soft key.	No
features.cfg	softkey.feature.endcall	1 (default) - Displays the **End Call** soft key. 0 - Does not display the **End Call** soft key.	No
features.cfg	softkey.feature.forward	1 (default) - Displays the **Forward** soft key. 0 - Does not display the **Forward** soft key.	No
features.cfg	softkey.feature.join	1 (default) - Displays the **Join** soft key. 0 - Does not display the **Join** soft key.	No
features.cfg	softkey.feature.mystatus	1 (default) - Displays the **MyStatus** soft key (if pres.idleSoftKeys is set to 1). 0 - Does not display the **MyStatus** soft key.	No
features.cfg	softkey.feature.newcall	1 (default) - Displays the **New Call** soft key is displayed. 0 - Does not display the **New Call** soft key.	No

Soft Key Customization Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`softkey.feature.redial`	0 (default) - Displays the Redial soft key. 1 - Does not display the Redial soft key. The parameter `feature.enhancedFeatureKeys.enabled` must be set to 1 first to configure this feature, and the parameter `efk.softkey.alignleft` must be set to 1 to move enabled soft keys into the positions of disabled soft keys.	No
`features.cfg`	`softkey.feature.split`	1 (default) - Displays the **Split** soft key to split the conference call to individual calls. 0 - Does not display the **Split** soft key.	No

This parameter includes:

-
-
-
-
-

**

Enables you to configure how the phone reacts to DHCP changes.

DHCP Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	**`tcpIpApp.dhcp.releaseOnLinkRecovery`**	Specifies whether or not a DHCP release occurs. 1 (default) - Performs a DHCP release after the loss and recovery of the network. 0 - No DHCP release occurs.	No

<dns/>

Allows you to set Domain Name System (DNS). However, values set using DHCP have a higher priority, and values set using the <device/> parameter in a configuration file have a lower priority.

Domain Name System (DNS) Parameters

Templ ate	Parameter	Permitted Values	Change Causes Restart or Reboot
site. cfg	**tcpIpApp.dns.server**	Phone directs DNS queries to this primary server. NULL (default) IP address	Yes
site. cfg	**tcpIpApp.dns.altServer**	Phone directs DNS queries to this secondary server. NULL (default) IP address	Yes
site. cfg	**tcpIpApp.dns.domain**	Specifies the DNS domain for the phone. NULL (default) String	Yes

<port/><rtp/>

Allows you to configure RTP traffic port filtering.

RTP Port Parameters

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.port.rtp.mediaPortRangeEnd	Determines the maximum supported end range of audio ports. Range is 1024 to 65485. 2269 (Default)	Yes
site.cfg	tcpIpApp.port.rtp.videoPortRange.enable	Specifies the range of video ports. 0 - Video ports are chosen within the range specified by **tcpIpApp.port.rtp.mediaPortRangeStart** and **tcpIpApp.port.rtp.mediaPortRangeEnd**. 1 - Video ports are chosen from the range specified by **tcpIpApp.port.rtp.videoPortRangeStart** and **tcpIpApp.port.rtp.videoPortRangeEnd**. Base profile (Default) Skype = 1 (Default) Generic = 0 (Default)	No
site.cfg	tcpIpApp.port.rtp.videoPortRangeEnd	Determines the maximum supported end range of video ports. Range is 1024 to 65535. 2319 (Default)	Yes
site.cfg	tcpIpApp.port.rtp.videoPortRangeStart	Determines the start range for video ports. Range is 1024 to 65486. 2272 (Default) Used only if value of tcpIpApp.port.rtp.videoPortRange.enable is 1.	Yes

<keepalive/>

Allows you to configure TCP keep-alive on SIP TLS connections; the phone can detect a failure quickly (in minutes) and attempt to re-register with the SIP call server (or its redundant pair).

TCP Keep-Alive Parameters

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.keepalive.tcp.idleTransmitInterval	Specifies the amount of time to wait (in seconds) before sending the keep-alive message to the call server. Range is 10 to 7200. 30 (Default) If this parameter is set to a value that is out of range, the default value is used. On VVX phones and the SoundStructure VoIP interface, specifies the number of seconds TCP waits between transmission of the last data packet and the first keep-alive message.	No
site.cfg	tcpIpApp.keepalive.tcp.noResponseTransmitInterval	Specifies the amount of idle time between the transmission of the keep-alive packets the TCP stack waits on VVX phones and the SoundStructure VoIP interface. This applies whether or not the last keep-alive was acknowledged. If no response is received to a keep-alive message, subsequent keep-alive messages are sent to the call server at this interval (every x seconds). Range is 5 to 120.	No

TCP Keep-Alive Parameters

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.keepalive.tcp.sip.persistentConnection.enable[1]	Specifies whether the TCP socket connection remains open or closes. 0 (Default) - The TCP socket opens a new connection when the phone tries to send any new SIP message and closes after one minute. 1 - The TCP socket connection remains open.	Yes
site.cfg	tcpIpApp.keepalive.tcp.sip.tls.enable	Specifies whether to disable or enable TCP keep-alive for SIP signaling connections. 0 (Default) - Disables TCP keep-alive for SIP signaling connections that use TLS transport. 1 - Enables TCP keep-alive for SIP signaling connections that use TLS transport.	No

<fileTransfer/>

Allows you to configure file transfers from the phone to the provisioning server.

File Transfer Parameters

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.fileTransfer.waitForLinkIfDown	Specifies whether a file transfer from the FTP server is delayed or not attempted. 1 (Default) - File transfer from the FTP server is delayed until Ethernet comes back up. 0 - File transfer from the FTP server is not attempted.	No

Allows you to list configuration items for available tone resources and includes:

<chord/>

Chord-sets are the sound effect building blocks that use synthesized audio instead of sampled audio. Most call progress and ringer sound effects are synthesized. A chord-set is a multi-frequency note with an optional on/off cadence, and can contain up to four frequency components generated simultaneously, each with its own level.

Three chord sets are supported: `callProg`, `misc`, and `ringer`. Each chord set has different chord names, represented by *x* in the following table.

For `callProg`, *x* can be one of the following chords:

`dialTone, busyTone, ringback, reorder, stutter_3, callWaiting, callWaitingLong, howler, recWarning, stutterLong, intercom, callWaitingLong, precedenceCallWaiting, preemption, precedenceRingback,` or `spare1` to `spare6`.

For `misc`, *x* can be one of the following chords:

* `spare1` to `spare9`

For `ringer`, *x* can be one of the following chords:

* `ringback, originalLow, originalHigh,` or `spare1` to `spare19`

Chord Parameters

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot
region.cfg	`tone.chord.callProg.x.freq.y` `tone.chord.misc.x.freq.y` `tone.chord.ringer.x.freq.y`	Frequency (in Hertz) for component y. Up to six chord-set components can be specified (y=1 to 6). 0-1600 0-1600 0-1600	No
region.cfg	`tone.chord.callProg.x.level.y` `tone.chord.misc.x.level.y` `tone.chord.ringer.x.level.y`	Level of component y in dBm0. Up to six chord-set components can be specified (y=1 to 6). -57 to 3 -57 to 3 -57 to 3	No
region.cfg	`tone.chord.callProg.x.onDur` `tone.chord.misc.x.onDur` `tone.chord.ringer.x.onDur`	On duration (length of time to play each component) in milliseconds. 0=infinite positive integer positive integer positive integer	No

Chord Parameters (continued)

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot

region.cfg	`tone.chord.callProg.x.offDur`
	`tone.chord.misc.x.offDur`
	`tone.chord.ringer.x.offDur`
		Off duration (the length of silence between each chord component) in milliseconds
		
		0=infinite
		positive integer
		positive integer
		positive integer
			No

region.cfg	`tone.chord.callProg.x.repeat`
	`tone.chord.misc.x.repeat`
	`tone.chord.ringer.x.repeat`
		Number of times each ON/OFF cadence is repeated.
		
		0=infinite
		positive integer
		positive integer
		positive integer
			No

Sets phone user preferences.

User Preferences Parameters

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
features.cfg	`up.25mm`	Specifies whether to use a mobile phone or a PC to connect to the 2.5mm audio port on a conference phone. 1 (Default) - Mobile phone 2 - PC	No
features.cfg	`up.accessibilityFeatures`	Specifies whether to display accessibility features or not. 0 (Default) - Accessibility features are disabled. 1 - Screen background flashes orange for incoming calls. For VVX 1500 only.	No

User Preferences Parameters (continued)

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.backlight.idleIntensity	Brightness of the LCD backlight when the phone is idle. Range is 0 to 3. 1 (Default) - Low 0 2 - Medium 3 - High VVX 300/301/310/311 = 0, 1, 2, 3 All other phones = 1, 2, 3 If this setting is higher than active backlight brightness (onIntensity), the active backlight brightness is used.	No
features.cfg	up.backlight.onIntensity	Brightness of the LCD backlight when the phone is active (in use). Range is 0 to 3. 3 (Default) – High 1 - Low 2 - Medium VVX 300/301/310/311 = 0, 1, 2, 3 All other phones = 1, 2, 3	No
features.cfg	up.backlight.timeout	Number of seconds to wait before the backlight dims from the active intensity to the idle intensity. Range is 5 to 60. 40 (default)	No
features.cfg	up.basicSettings.networkConfigEnabled	Specifies that **Network Configuration** is shown or not shown under the **Basic Settings** menu. 0 (default) – **Network Configuration** is not shown under **Basic Settings**. 1 – **Basic Settings** menu shows **Network Configuration** with configurable network options for the user without administrator rights.	No

User Preferences Parameters (continued)

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.basicSettingsPasswordEnabled	Specifies that a password is required or not required to access the **Basic Settings** menu. 0 (Default) - No password is required to access the **Basic Settings** menu. 1 - Password is required for access to the **Basic Settings** menu.	No
features.cfg	up.cfgWarningsEnabled	Specifies whether a warning displays on a phone or not. 0 (Default) - Warning does not display. 1 - Warning is displayed on the phone if it is configured with pre-UC Software 3.3.0 parameters.	No
em.cfg	up.em.linkalivecheck.enabled	Specifies whether a host VVX phone pings expansion modules or not. 0 (Default) - Host VVX phone does not ping the expansion modules. 1 - Host VVX phone periodically sends ping packets to the expansion modules.	No
features.cfg	up.handsetModeEnabled	Enable or disable the handset port. 1 (Default) 0	No
features.cfg	up.handsfreeMode	Specifies whether the speakerphone is enabled or disabled. 1 (Default) - Speakerphone is enabled. 0 - Speakerphone is disabled (cannot be used).	No
debug.cfg	up.headsetAlwaysUseIntrinsicRinger	1 (Default) - USB headset uses the intrinsic ringer mixed with DSP ringer when the sound effect destination is the USB headset. 0	No

User Preferences Parameters (continued)

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.headsetMode	Sets the preferred audio mode of handsfree or headset. 0 (Default) - Handsfree mode is used by default instead of the handset. 1 - Headset is used as the preferred audio mode after the headset key is pressed for the first time, until the headset key is pressed again.	No
features.cfg	up.headsetModeEnabled	Specifies whether or not the headset port can be used. 1 (Default) - Headset port is enabled and can be used. 0 - Headset port is disabled and cannot be used.	No
features.cfg	up.hearingAidCompatibility.enabled	Specifies whether audio Rx equalization is enabled or disabled. 0 (Default) - Audio Rx equalization is enabled. 1 - Phone audio Rx (receive) equalization is disabled for hearing aid compatibility.	No
features.cfg	up.hideSystemIpAddress	Nowhere (default) - The IP address is displayed in the respective user interface menu. Everywhere - The IP address is not displayed.	Yes
features.cfg	up.idleBrowser.enabled	Specifies if the idle browser is enabled or disabled. 0 (Default) - Idle browser is disabled. 1 - Idle browser is enabled. If the parameter up.prioritizeBackgroundMenuItem.enabled is set to 1, displays the background or the idle browser on the phone menu.	No
features.cfg	up.idleStateView	Sets the phone default view. 0 (Default) - Call/line view is the default view. 1 - Home screen is the default view.	Yes

User Preferences Parameters (continued)

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
`sip-interop.cfg`	`up.idleTimeout`	Number of seconds the phone can be idle before automatically leaving a menu and showing the idle display. Range is 0 to 65535 seconds. 40 (Default) 0 - No timeout and the phone does not automatically exit to the idle display. 1 to 65535 - Seconds for the phone to be idle.	Yes
`features.cfg`	`up.IdleViewPreferenceRemoteCalls`	Determines when the phone displays the idle browser. 0 (Default) - Phone with only remote calls active, such as on a BLF monitored line, is treated as in the idle state and the idle browser displays. 1 - Phone with only remote calls active, such as on a BLF monitored line, is treated as in the active state and the idle browser does not display.	Yes
`sip-interop.cfg`	`up.lineKeyCallTerminate`	Specifies whether or not you can press the line key to end an active call. 0 (Default) - User cannot end an active call by pressing the line key. 1 - User can press a line key to end an active call.	No
`sip-interop.cfg`	`up.numberFirstCID`	Specifies what is displayed first on the **Caller ID** display. 0 (Default) - **Caller ID** display shows the caller's name first. 1 - Caller's phone number is shown first.	Yes

User Preferences Parameters (continued)

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.numOfDisplayColumns	Sets the maximum number of columns the VVX 500/501, 600/601, or RealPresence Trio solution display. Set the maximum number of columns that phones display. Range is 0 to 4. VVX 500/501 = 3 (Default) VVX 600/601 = 4 (Default) RealPresence Trio=3 (Default) 0 - Phones display one column.	Yes
features.cfg	up.offHookAction.none	0 (Default) 1 - When the user lifts the handset, the phone does not seize the line and the ringer continues until the user takes further action.	Yes
features.cfg	up.oneTouchDirectory	Displays the **Address Book** icon on the main menu and the **Skype for Business Directory** search option. 1 (Default) 0	No
features.cfg	up.OffHookIdleBrowserView.enabled	Specifies whether or not to display the idle browser on screen after the phone goes off hook. 0 (Default) - Idle browser does not display on screen after the phone goes off hook. 1 - Idle browser continues to display on screen after the phone goes off hook.	No
features.cfg	up.osdIncomingCall.Enabled	Specifies whether or not to display full screen popup or OSD for incoming calls. 1 (Default) - Full screen popup or OSD for incoming calls displays. 0 - Full screen popup or OSD for incoming calls does not display.	No

User Preferences Parameters (continued)

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	up.prioritizeBackgroundMenuItem.enabled	User can choose whether or not the phone background should take priority over the idle browser. 1 (Default) - If up.idleBrowser.enabled is set to 1, this parameter can be set to 1 to display a **Prioritize Background** menu to the user.	Yes
site.cfg	up.ringer.minimumVolume	Configure the minimum ringer volume. This parameter defines how many volume steps are accessible below the maximum level by the user. 16 (Default) - Full 16 steps of volume range are accessible. 0 - Ring volume is not adjustable by the user and the phone uses maximum ring volume. Example: Upon bootup, the volume is set to ½ the number of configured steps below the maximum (16). If the parameter is set to 8 on bootup, the ringer volume is set to 4 steps below maximum.	No
sip-interop.cfg	up.screenCapture.enabled	0 (Default) - Screen captures are disabled. 1 - User can enable screen captures from the **Screen Capture** menu on the phone. When the phone reboots, screen captures are disabled from the **Screen Capture** menu on the phone.	Yes

User Preferences Parameters (continued)

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.screenSaver.enabled	0 (Default) - Screen saver feature is disabled. 1 - Screen saver feature is enabled. If a USB flash drive containing images is connected to the phone, and the idle browser is not configured, a slide show cycles through the images from the USB flash drive when the screen saver feature is enabled. The images must be stored in the directory on the flash drive specified by up.pictureFrame.folder. The screen saver displays when the phone has been in the idle state for the amount of time specified by up.screenSaver.waitTime.	No
features.cfg	up.screenSaver.type	Choose the type of screen saver to display. 0 (Default) - Phone screen saver displays default images. 2 - Phone screen saver displays the idle browser. You can use this parameter with the VVX 300 and 400 series phones.	No
features.cfg	up.screenSaver.waitTime	Number of minutes that the phone waits in the idle state before the screen saver starts. Range is 1 to 9999 minutes. 15 (Default)	No
features.cfg	up.simplifiedSipCallInfo	0 (Default) - 1 - Displayed host name is trimmed for both incoming and outgoing calls and the protocol tag/information is not displayed for incoming and outgoing calls.	No
lync.cfg	up.SLA.ringType	Specifies a ring type for Shared Line Appearance (SLA) lines. ringer 2 (Default) - default, ringer1 to ringer24	No

User Preferences Parameters (continued)

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
site.cfg	up.softkey.transferTypeOption.enabled	1 (default) –The user can change the transfer type from consultative to blind and vice versa using a soft key after the user has initiated a transfer, but before completing the call to the far end. 0 – There is no option to change from consultative to blind and blind to consultative when the user is in dial prompt after pressing the Transfer soft key.	No
features.cfg	up.status.message.flash.rate	Controls the scroll rate of the status bar on VVX 300 and 400 series business media phones. Range is 2 to 8 seconds. 2 seconds (Default)	No
features.cfg	up.warningLevel	Line keys block display of the background image. All warnings are listed in the **Warnings** menu. 0 (Default) - The phone's warning icon and a pop-up message display on the phone for all warnings. 1 - Warning icon and pop-up messages are only shown for critical warnings. 2 - Phone displays a warning icon and no warning messages. For all the values, all warnings are listed in the **Warnings** menu. Access to the **Warnings** menu varies by phone model: VVX 1500 - **Menu > Status > Diagnostics > Warnings** VVX 101, 201, 300/301/310/311, 400/401/410/411, 500/501, and 600/601 - **Settings > Status > Diagnostics > Warnings**	Yes

User Preferences Parameters (continued)

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`up.welcomeSoundEnabled`	1 (Default) - Welcome sound is enabled and played each time the phone reboots. 0 - Welcome sound is disabled. To use a welcome sound you must enable the parameter `up.welcomeSoundEnabled` and specify a file in `saf.x`. The default UC Software welcome sound file is `Welcome.wav`. See the example configuration in Sound Effects.	Yes
`features.cfg`	`up.welcomeSoundOnWarmBootEnabled`	0 (Default) - Welcome sound is played when the phone powers on (cold boot), but not after it restarts or reboots (warm boot). 1 - Welcome sound plays each time the phone powers on, reboots, or restarts.	Yes

Specify the URL of a custom download server and the Polycom UC Software download server when you want the phone to check when to search for software upgrades.

Upgrade Parameters

Templates	Parameter Template	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`upgrade.custom.server.url`	The URL of a custom download server. URL (default) - NULL	No
`site.cfg`	`upgrade.plcm.server.url`	The URL of the Polycom UC Software software download. URL - `http://downloads.polycom.com/` `voice/software/`	No

<video/>

The parameters in the table are supported on the VVX 500/501, VVX 600/601, and VVX 1500, and RealPresence Trio solution.

This parameter also includes:

-
-
-

Video Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.allowWithSource	Restricts sending video codec negotiation in Session Description Protocol (SDP). 0 (default) 0 or 1 This parameter applies only for VVX 500/501 and VVX 600/601.	No
video.cfg	video.autoFullScreen	0 (default) - Video calls use the full screen layout, only if explicitly selected by the user. 1 - Video calls use the full screen layout by default.	No
video.cfg	video.autoStartVideoTx	Controls video sent to the far side. 1 (default) 0 or 1	No
video.cfg	video.callRate	Specifies the default call rate (in kbps) when negotiating the bandwidth for a video call. 512 (default) 128 - 2048	No
video.cfg	video.dynamicControlMethod	0 (default) 1 - The first I-Frame request uses the method defined by video.forceRtcpVideoCodecControl and subsequent requests alternate between RTCP-FB and SIP INFO. To set other methods for I-frame requests, refer the parameter video.forceRtcpVideoCodecControl.	No

Video Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.forceRtcpVideoCodecControl	0 (default) - The phone sends RTCP-FB messages only upon a successful SDP negotiation of a=rtcp-fb. 1 - The phone sends RTCP feedback messages to request fast update I-frames along with SIP INFO messages, irrespective of SDP negotiation.	Yes
video.cfg	video.iFrame.delay	0 (default) 1 -10 seconds - Transmits an extra I-frame after the video starts. The amount of delay from the start of video until the I-frame is sent is configurable up to 10 seconds.	Yes
video.cfg	video.iFrame.minPeriod	Time taken before sending a second I-frame in response to requests from the far end. 2 (default) 1 - 60	No
video.cfg	video.iFrame.onPacketLoss	0 (default) 1 - Transmits an I-frame to the far end when video RTP packet loss occurs.	No
video.cfg	video.maxCallRate	Sets a limit to the maximum call rate that the users can select. 768 (default) 128 to 2048 kbps If video.callRate is greater than 2048 kbps, it is considered as the maximum value.	Yes
video.cfg	video.quality	The optimal quality for video sent in a call or a conference. NULL (default) motion - if your outgoing video has motion or movement. sharpness - if your outgoing video has little or no movement. If motion is not selected, some frames are dropped due to moderate or heavy motion.	Yes

<camera/>

The settings in the next table control the performance of the camera.

Video Camera Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.camera.b rightness	Sets brightness level. 3 (Default) 0 - 6 The value range is from 0 (Dimmest) to 6 (Brightest).	No
video.cfg	video.camera.c ontrast	Sets contrast level. 0 (default) 0 - 4 The value range is from 0 (No contrast increase) to 3 (Most contrast increase), and 4 (Noise reduction contrast).	No
video.cfg	video.camera.f lickerAvoidanc e	0 (default) - Sets flicker avoidance to Automatic. 1- Sets flicker avoidance 50hz AC power frequency (Europe/Asia). 2 - Sets flicker avoidance to 60hz AC power frequency (North America).	No
video.cfg	video.camera.f rameRate	Sets target frame rate (frames per second). 25 (default) 5 - 30 The values indicate a fixed frame rate, from 5 (least smooth) to 30 (most smooth). If video.camera.frameRate is set to a decimal number, the value 25 is used.	No
video.cfg	video.camera.s aturation	Sets saturation level. 3 (default) 0 - 6 The value range is from 0 (Lowest) to 6 (Highest).	No
video.cfg	video.camera.s harpness	Sets sharpness level. 3 (default) 0 - 6 The value range is from 0 (Lowest) to 6 (Highest).	No

<codecs/>

The video codecs include:

-
-

The following table lists video codec and specifies the video codec preferences for the VVX 500/501, 600/601, and 1500 phones. To disable codecs, set the value to 0. A value of 1 indicates the codec is the most preferred and has highest priority. The VVX 500/501 and 600/601 support H.263 and H.264 and do not support H.261 or H.263 1998.

Video Codec Preference Parameters

Template	Parameter	Permitted Value	Change Causes Restart or Reboot
video.cfg	video.codecPref.H261	Sets the H.261 payload type. 6 (default) 0 - 8	No
video.cfg	video.codecPref.H264	Sets the H.264 payload type. 4 (default) 0 - 8	No
video.cfg	video.codecPref.H263 1998	Sets the H.263 payload type. 5 (default) 0 - 8	No
video.cfg	video.codecPref.H263	5 (default) 0 - 8	No
video.cfg	video.codecPref.H264	4 (default) 0 - 8	No

The next table lists settings for a group of low-level video codec parameters. For most use cases, the default values are appropriate. Polycom does not recommend changing the default values unless specifically advised to do so.

Video Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`video.cfg`	`video.profile.` `H261.annexD`	1 (default) - Enables Annex D when negotiating video calls. 0 - Disables Annex D when negotiating video calls.	Yes
`video.cfg`	`video.profile.` `H261.CifMpi`	Specifies the frame rate divider used by the phone when negotiating CIF resolution for a video call. 1 (default) 1 - 32 You can enter a value between 0 - 4. To disable, enter '0'.	Yes

`video.cfg`	`video.profile.`
	`H261.jitterBuf`
	`ferMax`
		The largest jitter buffer depth to be supported (in milliseconds).
		2000ms (default)
		(`video.profile.H261.jitter`
		`BufferMin`+ 500ms) to 2500ms.
		Jitter above 2500ms always causes packet loss. This parameter should be set to the smallest possible value that supports the network jitter.
			Yes

`video.cfg`	`video.profile.`
	`H261.jitterBuf`
	`ferMin`
		The smallest jitter buffer depth (in milliseconds) that must be achieved before the first play out.
		150ms (default)
		33ms to 1000ms
		Even if this depth is achieved initially, it may fall and the play out might still continue. This parameter should be set to the smallest possible value, at least two packet payloads, and larger than the expected short term average jitter.
			Yes

Video Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile. H261.jitterBuf ferShrink	The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. 70ms (default) 33ms to 1000ms Smaller values (33 ms) minimize the delay on trusted networks. Larger values (1000ms) minimize packet loss on networks with large jitter (3000 ms).	Yes
video.cfg	video.profile. H261.payloadTy pe	Specifies the RTP payload format type for H261 MIME type. 31 (default) 0 -127	Yes
video.cfg	video.profile. H261.QcifMpi	Specifies the frame rate divider that the phone uses when negotiating Quarter CIF resolution for a video call. 1(default) 1 - 32 You can enter a value between 0-4. To disable, enter '0'. The default frame rate divider is '1'.	Yes
video.cfg	video.profile. H263.CifMpi	Specifies the frame rate divider that the phone uses when negotiating CIF resolution for a video call. 1(default) 1 - 32 You can enter a value between 0-32. To disable, enter '0'. The default frame rate divider is '1'.	Yes
video.cfg	video.profile. H263.jitterBuf ferMax	The largest supported jitter buffer depth (in milliseconds). 2000ms (default) (video.profile.H263.jitter BufferMin + 500ms) to 2500ms Jitter above 2500ms always causes packet loss. This parameter should be set to the smallest possible value that supports the network jitter.	Yes

Video Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile. H263.jitterBuf ferMin	The smallest jitter buffer depth (in milliseconds) to be achieved for the first time, before play out begins. 150ms (default) 33ms to 1000ms Even if this depth is achieved initially, it may fall and the play out might still continue. This parameter should be set to the smallest possible value, at least two packet payloads, and larger than the expected short term average jitter.	Yes
video.cfg	video.profile. H263.jitterBuf ferShrink	The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. 70ms (default) 33ms to 1000ms Smaller values (33 ms) minimize the delay on trusted networks. Larger values (1000ms) minimize packet loss on networks with large jitter (3000 ms).	Yes
video.cfg	video.profile. H263.payloadTy pe	Specifies the RTP payload format type for H263 MIME type. 34 (default) 0 - 127	Yes
video.cfg	video.profile. H263.QcifMpi	Specifies the frame rate divider that the phone uses when negotiating Quarter CIF resolution for a video call. 1 (default) 1 - 32 You can enter a value between 0-32. To disable, enter '0'. The default frame rate divider is '1'.	Yes
video.cfg	video.profile. H263.SqcifMpi	Specifies the frame rate divider that the phone uses when negotiating Sub Quarter CIF resolution for a video call. 1 (default) 1 - 32 You can enter a value between 0-32. To disable, enter '0'. The default frame rate divider is '1'.	Yes

Video Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile. H2631998.annex F	0 (default) - Enables Annex F when negotiating video calls. 1 - Disables Annex F when negotiating video calls.	Yes
video.cfg	video.profile. H2631998.annex I	0 (default) - Enables Annex I when negotiating video calls. 1 - Disables Annex I when negotiating video calls.	Yes
video.cfg	video.profile. H2631998.annex J	0 (default) - Enables Annex J when negotiating video calls. 1 - Disables Annex J when negotiating video calls.	Yes
video.cfg	video.profile. H2631998.annex K	Specifies the value of Annex K to use when negotiating video calls. 0 (default) - Enables Annex K when negotiating video calls. 1 - Disables Annex K when negotiating video calls. 2,3,4	Yes
video.cfg	video.profile. H2631998.annex N	Specifies the value of Annex N to use when negotiating video calls. 0 (default) - Enables Annex N when negotiating video calls. 1 - Disables Annex N when negotiating video calls. 2,3,4	Yes
video.cfg	video.profile. H2631998.annex T	0 (default) - Enables Annex T when negotiating video calls. 1 - Disables Annex T when negotiating video calls.	Yes
video.cfg	video.profile. H2631998.CifMp i	Specifies the frame rate divider that the phone uses when negotiating CIF resolution for a video call. 1 (default) 1 to 32 You can enter a value between 0-32. To disable, enter '0'.	Yes

Video Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot

`video.cfg`	`video.profile.`
	`H2631998.jitte`
	`rBufferMax`
		The largest supported jitter buffer depth (in milliseconds).
		
		2000ms (default)
		
		(video.profile.H2631998.jitterBufferMin+ 500ms) to 2500ms
		
		Jitter above 2500ms always causes packet loss. This parameter should be set to the smallest possible value that supports the network jitter.
			Yes

`video.cfg`	`video.profile.`
	`H2631998.jitte`
	`rBufferMin`
		The smallest jitter buffer depth (in milliseconds) to be achieved for the first time before play out begins.
		
		150ms (default)
		
		33ms - 1000ms
		
		Even if this depth is achieved initially, it may fall and the play out might still continue. This parameter should be set to the smallest possible value, at least two packet payloads, and larger than the expected short term average jitter.
			Yes

`video.cfg`	`video.profile.`
	`H2631998.jitte`
	`rBufferShrink`
		The absolute minimum time duration (in milliseconds) of RTP packet Rx, with no packet loss between jitter buffer size shrinks.
		
		70ms (default)
		
		33ms - 1000ms
		
		Use smaller values (33 ms) to minimize the delay on trusted networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).
			Yes

`video.cfg`	`video.profile.`
	`H2631998.paylo`
	`adType`
		Specifies the RTP payload format type for H263-1998/90000 MIME type.
		
		96 (default)
		
		96 to 127
			Yes

Video Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot

`video.cfg`	`video.profile.`
	`H2631998.QcifM`
	`pi`
		Specifies the frame rate divider used by the phone when negotiating Quarter CIF resolution of a video call.
		
		1 (default) - Enables the frame rate divider used by the phone when negotiating the resolution of a video call.
		
		1 - 32
		
		0 - Disables the frame rate divider used by the phone when negotiating the resolution of a video call.
			Yes

`video.cfg`	`video.profile.`
	`H2631998.Sqcif`
	`Mpi`
		Specifies the frame rate divider that the phone uses when negotiating Sub Quarter CIF resolution for a video call.
		
		1 (default) - Enables the frame rate divider used by the phone when negotiating the resolution of a video call.
		
		1 - 32
		
		0 - Disables the frame rate divider used by the phone when negotiating the resolution of a video call.
			Yes

`video.cfg`	`video.profile.`
	`H264.jitterBuf`
	`ferMax`
		The largest jitter buffer depth to be supported (in milliseconds).
		
		2000ms (default)
		
		(`video.profile.H264.jitter`
		`BufferMin` + 500ms) to 2500ms
		
		Jitter above 2500ms always causes packet loss. This parameter should be set to the smallest possible value that supports the network jitter.
			Yes

`video.cfg`	`video.profile.`
	`H264.jitterBuf`
	`ferMin`
		The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. 150ms (default)
		
		33ms to 1000ms
		
		Even if this depth is achieved initially, it may fall and the play out might still continue. This parameter should be set to the smallest possible value, at least two packet payloads, and larger than the expected short term average jitter.
			Yes

Video Profile Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile. H264.jitterBuf ferShrink	The absolute minimum duration time (in milliseconds) of RTP packet Rx, with no packet loss between jitter buffer size shrinks. 70ms (default) 33ms to 1000ms Use smaller values (33 ms) to minimize the delay on trusted networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).	Yes
video.cfg	video.profile. H264.payloadTy pe	Specifies the RTP payload format type for H264/90000 MIME type. 109 (default) 96 to 127	Yes
video.cfg	video.profile. H264.profileLe vel	Specifies the highest profile level within the baseline profile supported in video calls. 1.3 (default) 1, 1b, 1.1, 1.2, 1.3, and 2 VVX 500/501 and VVX 600/601 phones support H.264 with a profile level of 2, and VVX 1500 phones support H.264 with a profile level of 1.3.	Yes

The parameters listed in the following tables configure phone audio.

Voice Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
debug.cfg	voice.txEq.hf.preFilter.enable	0 (default) 1 - Enables a 300 Hz high-pass filter that is applied to transmit the audio prior to encoding when a narrow band codec, such as G.711mu, G.711A, G.729, or iLBC, is in use. Enabling this filter may improve intelligibility to the far end in a noisy environment, when making narrow band calls through a PSTN gateway.	No

site.cfg	voice.txPacketDelay	Null (default)
		
		normal, Null - Audio parameters are not changed.
		
		low - If there are no precedence conflicts, the following changes are made:
		
		`voice.codecPref.G722="1"`
		
		`voice.codecPref.G711Mu="2"`
		
		`voice.codecPref.G711A="3"`
		
		`voice.codecPref.<OtherCodecs>=""`
		
		`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"`
			Yes

site.cfg	voice.txPacketFilter	Null (default) 0 - Tx filtering is not performed. 1 - Enables Narrowband Tx high pass filter.	Yes

<aes/>

Use these parameters to control the speakerphone acoustic echo suppression (AES). These parameters remove residual echo after AEC processing. Because AES depends on AEC, enable AES only when you also enable AEC using `voice.aec.hd.enable`.

Acoustic Echo Suppression Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`debug. cfg`	`voice.aes.hf.e nable`	1 (default) - Enables the handsfree AES function. 0 - Disables the handsfree AES function. Polycom recommends that you do not disable this parameter.	No
`techsu pport. cfg`	`voice.aes.hs.e nable`	1 (default) - Enables the handset AES function. 0 - Disables the handset AES function.	No

<cn/>

Use these parameters to configure the addition and volume of comfort noise during conferences.

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`debug. cfg`	`voice.cn.hf.en able`	1 (default) - Adds comfort noise added into the Tx path for hands-free operation. 0 - Comfort noise not added. Far end users should use this feature when they find the phone to be 'dead', as the near end user stops talking.	No
`debug. cfg`	`voice.cn.hf.at tn`	35 (default) - quite loud 0 - 90 Attenuation of the inserted comfort noise from full scale in decibels; smaller values insert louder noise. Use this parameter only when `voice.cn.hf.enabled` is 1.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`debug. cfg`	`voice.cn.hd.en able`	0 (default) - Comfort noise is not added into the Tx path for the headset. 1 - Adds comfort noise into the Tx path for the headset. Far end users should use this feature when they find the phone to be 'dead', as the near end user stops talking.	No
`debug. cfg`	`voice.cn.hd.at tn`	30 (default) - quite loud 0 - 90 Attenuation of the inserted comfort noise from full scale in decibels; smaller values insert louder noise. Use this parameter only when `voice.cn.hd.enabled` is 1.	No
`debug. cfg`	`voice.cn.hs.en able`	0 (default) - Comfort noise is not added into the Tx path for the handset. 1 - Adds comfort noise is added into the Tx path for the headset. Far end users should use this feature when they find the phone to be 'dead', as the near end user stops talking.	No
`site.c fg`	`voice.cn.hs.at tn`	35 (default) - quite loud 0 - 90 Attenuation of the inserted comfort noise from full scale in decibels; smaller values insert louder noise. Use this parameter only when `voice.cn.hs.enabled` is 1.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`voice.vadRxGain`	Tunes VAD or CNG interoperability in a multi-vendor environment. 0 (default) -20 to +20 dB The specified gain value in dB is added to the noise level of an incoming VAD or CNG packet, when in a narrow band call. When tuning in multi-vendor environments, the existing Polycom to Polycom phone behavior can be retained by setting `voice.vadTxGain = -voice.vadRxGain`. This parameter is ignored for HD calls.	No
`site.cfg`	`voice.vadTxGain`	Tunes VAD or CNG interoperability in a multi-vendor environment. 0 (default) -20 to +20 dB The specified gain value in dB is added to the noise level of an incoming VAD or CNG packet, when in a narrow band call. This causes the noise level to synthesize at the local phone to change by the specified amount. When tuning in multi-vendor environments, the existing Polycom to Polycom phone behavior can be retained by setting `voice.vadTxGain = -voice.vadRxGain`. This parameter is ignored for HD calls.	No

<handset/>

The parameters listed in this section control the level of sidetone on handsets of VVX business media phones.

Handset Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`techsupport.cfg`	`voice.handset.st`	Adjust the handset sidetone level from the default in 1 decibel (dB) increments. 0 (default) -12 to +12	No

<headset/>

The parameters listed in this section control the level of sidetone on headsets connected to VVX business media phones.

Headset Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
techsupport.cfg	voice.headset.st	Adjust the headset sidetone level from the default in 1 decibel (dB) increments. 0 (default)	No

<line/>

The following parameters control audio level settings for phone handset and headset.

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
techsupport.cfg	voice.lineAgc.hs.enable	0 (default) - Disables the line automatic gain control is on the handset. 1 - Enables the line automatic gain control is on the handset. This parameter applies to the VVX 300 series, 400 series, 500 series, and 600 series business media phones.	Yes
techsupport.cfg	voice.lineAgc.hd.enable	0 (default) - Disables the line automatic gain control on the headset. 1 - Enables the line automatic gain control is on the headset. This parameter applies to the VVX 300 series, 400 series, 500 series, and 600 series business media phones.	Yes

<rxQoS/>

The following table lists the jitter buffer parameters for wired network interface voice traffic and push-to-talk interface voice traffic.

Voice Jitter Buffer Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`voice.rxQoS.avgJitter`	The average jitter in milliseconds for wired network interface voice traffic. 20 (default) 0 to 80 `avgJitter` The wired interface minimum depth will be automatically configured to adaptively handle this level of continuous jitter without packet loss.	Yes
`site.cfg`	`voice.rxQoS.maxJitter`	The average jitter in milliseconds for wired network interface voice traffic. 160 (default) 0 to 200 `maxJitter` The wired interface jitter buffer maximum depth will be automatically configured to handle this level of intermittent jitter without packet loss. Actual jitter above the average but below the maximum may result in delayed audio play out while the jitter buffer adapts, but no packets will be lost. Actual jitter above the maximum value will always result in packet loss. If legacy `voice.audioProfile.x.jitterBuffer.*` parameters are explicitly specified, they will be used to configure the jitter buffer and these `voice.rxQoS` parameters will be ignored.	Yes

Voice Jitter Buffer Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.rxQoS.pt t.avgJitter	The average jitter in milliseconds for IP multicast voice traffic. 150 (default) 0 - 200 avgJitter The PTT/Paging interface minimum depth will be automatically configured to adaptively handle this level of continuous jitter without packet loss.	Yes
site.cfg	voice.rxQoS.pt t.maxJitter	The maximum jitter in milliseconds for IP multicast voice traffic. 480 (default) 20 - 500 maxJitter The PTT/Paging interface jitter buffer maximum depth will be automatically configured to handle this level of intermittent jitter without packet loss. Actual jitter above the average but below the maximum may result in delayed audio play out while the jitter buffer adapts, but no packets will be lost. Actual jitter above the maximum value will always result in packet loss. If legacy voice.audioProfile.x.jitterB uffer.* parameters are explicitly specified, they will be used to configure the jitter buffer and these voice.rxQoS parameters will be ignored for PTT/Paging interface interfaces.	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
techsupport.cfg	voice.handsfreePtt.rxdg.offset	This parameter allows a digital Rx boost for Push To Talk. 0 (default) 9 to -12 – Offsets the RxDg range of the hands-free and hands-free Push-to-Talk (PTT) by the specified number of decibels.	No
techsupport.cfg	voice.ringerPage.rxdg.offset	This parameter allows a digital Rx boost for Push To Talk. Use this parameter for handsfree paging in high noise environments. 0 (default) 9 to -12 – Raise or lower the volume of the ringer and hands-free page by the specified number of decibels.	No

You must set up the call server and DTMF signaling parameters.

This parameter includes:

-
- <SDP/>
- <H323/>

**

The next table describes VoIP server configuration parameters.

VoIP Server Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.cfg`	`voIpProt.server.dhcp.available`[1]	0 (default) - Do not check with the DHCP server for the SIP server IP address. 1 - Check with the server for the IP address.	Yes
`site.cfg`	`voIpProt.server.dhcp.option`[1]	The option to request from the DHCP server if `voIpProt.server.dhcp.available`= 1. 128 (default) to 254 If `reg.x.server.y.address` is non-Null, it takes precedence even if the DHCP server is available.	Yes
`site.cfg`	`voIpProt.server.dhcp.type`[1]	Type to request from the DHCP server if `voIpProt.server.dhcp.available` is set to 1. 0 (default) - Request IP address 1 - Request string	Yes

<SDP/>

The next table describes Session Description Protocol configuration parameters.

Session Description Protocol (SDP) Parameters

Template	Parameter Template	Permitted Values	Change Causes Restart or Reboot
`sip-in terop. cfg`	`voIpProt.SDP.a nswer.useLocal Preferences`	0 (default) - The phone's use of its own preference list is disabled. 1 -The phone uses its own preference list instead of the preference list in the offer when deciding which video codec to use. Note: If the 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.	No
`sip-in terop. cfg`	`voIpProt.SDP.e arly.answerOrO ffer`	0 (default) - SDP offer or answer is not generated. 1 - SDP offer or answer is generated in a provisional reliable response and PRACK request and response. Note: An SDP offer or answer is not generated if `reg.x.musicOnHold.uri` is set.	No
`sip-in terop. cfg`	`voIpProt.SDP.o ffer.iLBC.13_3 3kbps.includeM ode`	1(default) - The phone should include the mode=30 FMTP parameter 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, the iLBC 13.33 kbps codec is set to a higher preference. 0 - the phone should not include the mode=30 FTMP parameter in SDP offers even if iLBC 13.33 kbps codec is being advertised. See the section <codecPref/>.	No

Session Description Protocol (SDP) Parameters (continued)

Templat e	Parameter Template	Permitted Values	Change Causes Restart or Reboot
	`voIpProt.SDP.u seLegacyPayloa dTypeNegotiati on`	0 (default) - RFC 3264 is followed for transmit and receive RTP payload type values. 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.	No
`sip-in terop. cfg`	`voIpProt.SDP.o ffer.rtcpVideo CodecControl`	This parameter determines whether or not RTCP-FB-based controls are offered in Session Description Protocol (SDP) when the phone negotiates video I-frame request methods. Even when RTCP-FB-based controls are not offered in SDP, the phone may still send and receive RTCP-FB I-frame requests during calls depending on other parameter settings. For more information about video I-frame request behavior, refer to video.forceRtcpVideoCodecControl. For an account of all parameter dependencies refer to the section I-Frames. 0 (default) - The phone does not include the SDP attribute "a=rtcp-fb". 1 - The phone includes SDP attribute "a=rtcp-fb" into offers during outbound SIP calls.	No

<H323/>

The parameters listed in the next table are supported only with the Polycom VVX 500/501, 600/601, and 1500 phones.

H.323 Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
h323.cfg	voIpProt.H323.autoGateKeeperDiscovery	1 (default) - The phone will attempt to discover an H.323 gatekeeper address via the standard multi cast technique, provided that a statically configured gatekeeper address is not available. 0 - The phone will not send out any gatekeeper discovery messages.	Yes
h323.cfg	voIpProt.H323.blockFacilityOnStartH245	0 (default) - facility messages when using H.245 are not removed. 1 - facility messages when using H.245 are removed.	Yes
h323.cfg	voIpProt.H323.dtmfViaSignaling.enabled	1 (default) - The phone will use the H.323 signaling channel for DTMF key press transmission. 0 - The phone will not use H.323 signaling channel for DTMF key press transmission.	Yes
h323.cfg	voIpProt.H323.dtmfViaSignaling.H245alphanumericMode	1 (default) - The phone will support H.245 signaling channel alphanumeric mode DTMF transmission. 0 - The phone will not support H.245 signaling channel alphanumeric mode DTMF transmission Note: If both alphanumeric and signal modes can be used, the phone gives priority to DTMF.	Yes
h323.cfg	voIpProt.H323.dtmfViaSignaling.H245signalMode	1 (default) - The phone will support H.245 signaling channel signal mode DTMF transmission. 0 - The phone will not support H.245 signaling channel signal mode DTMF transmission.	Yes
h323.cfg	voIpProt.H323.enable	0 (default) - The H.323 protocol is not used for call routing, dial plan, DTMF, and URL dialing. 1 - The H.323 protocol is used for call routing, dial plan, DTMF, and URL dialing.	Yes

H.323 Protocol Parameters (continued)

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`h323.c fg`	`voIpProt.H323. local.port`	Local port for sending and receiving H.323 signaling packets. 0 - 1720 is used for the local port but is not advertised in the H.323 signaling. 0 to 65535 - The value is used for the local port and it is advertised in the H.323 signaling.	Yes
`sip-in terop. cfg`	`voIpProt.H323. local.RAS.port`	Specifies the local port value for RAS signaling. 1719 (default) 1 to 65535	Yes

The parameters listed in the next table specify the download location of the translated language files for the Web Configuration Utility.

Web Configuration Utility Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`site.c fg`	`webutility.lan guage.plcmServ erUrl`	Specifies the download location of the translated language files for the Web Configuration Utility. `http://downloads.polycom.com/ voice/software/languages/` (default) URL	No

The parameters in the following table set the XML streaming protocols for instant messaging, presence, and contact list for BroadSoft features.

XML Streaming Protocol Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	xmpp.1.auth.domain	Specify the domain name of the XMPP server. Null (Default) Other values - UTF-8 encoded string	No
features.cfg	xmpp.1.auth.useLoginCredentials	Specifies whether or not to use the login credentials provided in the phone's Login Credentials Menu for XMPP authentication. 0 (Default) 1	
features.cfg	xmpp.1.enable	Specifies to enable or disable the XMPP presence. 0 (Default) 1	No

Monitoring, Diagnostics, and Troubleshooting

Polycom phones running Polycom UC Software provide a variety of screens and logs that allow you to review information about the phone and its performance, help you diagnose and troubleshoot problems, view error messages, and test the phone's hardware.

Review the latest UC Software Release Notes on Polycom UC Software Support Center for known problems and possible workarounds. If you don't find your problem in this section or in the latest Release Notes, contact your Certified Polycom Reseller for support.

Error Message Types

The following sections cover some of the errors you might see, along with suggested actions.

Updater Error Messages and Possible Solutions

If a fatal error occurs, the phone does not boot up. If the error is not fatal, the phone boots up but its configuration might be changed. Most updater errors are logged to the phone's boot log. However, if the phone is having trouble connecting to the provisioning server, the phone is not likely to upload the boot log.

The following table describes possible solutions to updater error messages.

Updater Error Messages

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 set to a VLAN that is different from the DHCP server.
- Check the DHCP configuration.

Application <file name> is not compatible with this phone!

An application file was downloaded from the provisioning server, but it cannot be installed on this phone.
- Install a compatible software image on the provisioning server. Be aware that there are various hardware and software dependencies.

Could not contact boot server using existing configuration

The phone cannot contact the provisioning server. Possible causes include:
- Cabling issues
- DHCP configuration
- Provisioning server problems

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.

Updater Error Messages

Error, application is not present!

The phone does not have an application stored in device settings and, because the application could not be downloaded, the phone cannot boot.

• Download compatible Polycom UC Software to the phone using one of the supported provisioning protocols.

• If no provisioning server is configured on the phone, enter the provisioning server details after logging in to the Updater menu and navigating to the Provisioning Server menu.

Polycom UC Software Error Messages

If an error occurs in the UC Software, an error message and a warning icon displays on the phone. The location of the Warnings menu varies by model:

● VVX 1500 **Menu > Status > Diagnostics > Warnings**

● VVX 300/301, 310/311, 400/401, 410/411, 500/501, or 600/601 **Settings > Status > Diagnostics > Warnings**

The following table describes Polycom UC Software error messages.

Polycom UC Software Error Messages

Config file error: Files contain invalid params: \<filename1\>, \<filename2\>,...
Config file error: \<filename\> contains invalid params
The following contain pre-3.3.0 params: \<filename\>

These messages display if the configuration files contain these deprecated parameters:

• tone.chord.ringer.x.freq.x

• se.pat.callProg.x.name

• ind.anim.IP_500.x.frame.x.duration

• ind.pattern.x.step.x.state

• feature.2.name

• feature.9.name

This message also displays if any configuration file contains more than 100 of the following errors:

• Unknown parameters

• Out-of-range values

• Invalid values.

To check that your configuration files use correct parameter values, refer to Using Correct Parameter XML Schema, Value Ranges, and Special Characters.

Line: Unregistered

This message displays if a line fails to register with the call server.

Login credentials have failed. Please update them if information is incorrect.

This message displays when the user enters incorrect login credentials on the phone: **Status** > **Basic** > **Login Credentials**.

Missing files, config. reverted

Polycom UC Software Error Messages

This message displays when errors in the configuration and a failure to download the configuration files force the phone to revert to its previous (known) condition with a complete set of configuration files. This also displays if the files listed in the **<*MAC Address*>.cfg** file are not present on the provisioning server.

Network link is down

Indicates that the phone cannot establish a link to the network and persists until the link problem is resolved. Call-related functions, and phone keys are disabled when the network is down but the phone menu works.

Network Authentication Failure Error Codes

This message displays if 802.1X authentication with the Polycom phone fails. The error codes display on the phone when you press the **Details** key. Error codes are also included in the log files.

Network Authentication Failure Error Codes

Event Code	Description	Comments
1	Unknown events	An unknown event by '1' can include any issues listed in this table.
2	Mismatch in EAP Method type Authenticating server's list of EAP methods does not match with clients'.	
30xxx	TLS Certificate failure 000 - Represents a generic certificate error. The phone displays the following codes: 042 - bad cert 043 - unsupported cert 044 - cert revoked 045 - cert expired 046 - unknown cert 047 - illegal parameter 048 - unknown CA	See section 7.2 of RFC 2246 for further TLS alert codes and error codes.
31xxx	Server Certificate failure 'xxx' can use the following values: •009 - Certificate not yet Valid •010 - Certificate Expired •011 - Certificate Revocation List (CRL) not yet Valid •012 - CRL Expired	
4xxx	Other TLS failures 'xxx' is the TLS alert message code). For example, if the protocol version presented by the server is not supported by the phone, then 'xxx' is 70, and the EAP error code is 4070.	See section 7.2 of RFC 2246 for further TLS alert codes and error codes.

Network Authentication Failure Error Codes

5xxx	Credential failures
	5xxx - wrong user name or password
6xxx	PAC failures
	080 - No PAC file found
	081 - PAC file password not provisioned
	082 - PAC file wrong password
	083 - PAC file invalid attributes
7xxx	Generic failures
	001 - dot1x can not support (user) configured EAP method
	002 - dot1x can not support (user) configured security type
	003 - root certificate could not be loaded
	174 - EAP authentication timeout
	176 - EAP Failure
	185 - Disconnected

Status and Diagnostics

The phone includes a variety of information screens and tools that can help you monitor the phone and resolve problems.

View the Phone's Status

You can troubleshoot phone issues by viewing the phone's Status menu.

To view the Status menu on the phone:

1 Select **Settings** > **Status** > **Select**.
2 Scroll to a Status menu item and press **Select**. The following table lists available options:

Status Menu Descriptions

Menu Item	Menu Information
Platform	• Phone's serial number or MAC address • Current IP address • Updater version • Application version • Name of the configuration files in use • Address of the provisioning server
Network	• TCP/IP Setting • Ethernet port speed • Connectivity status of the PC port (if it exists) • Statistics on packets sent and received since last boot • Last time the phone rebooted • Call Statistics showing packets sent and received on the last call
Lines	• Detailed status of each of the phone's configured lines
Diagnostics	• Hardware tests to verify correct operation of the microphone, speaker, handset, and third party headset, if present • Tests to verify proper functioning of the phone keys • List of the functions assigned to each of the phone keys • Real-time graphs for CPU, network, and memory use

Test Phone Hardware

You can test the phone's hardware directly from the user interface.

To test phone hardware:

1 Go to **Settings** > **Status** > **Diagnostics.**

2 Choose from these tests:

➢ **Audio Diagnostics**   Test the speaker, microphone, handset, and a third party headset**.**

➢ **Keypad Diagnostics**   Verify the function assigned to each keypad key.

➢ **Display Diagnostics**   Test the LCD for faulty pixels.

➢ **LED Diagnostics**   Test the LED lights on your phone.

➢ **Touch Screen Diagnostics**   Test the touch screen response.

Upload a Phone's Configuration

You can upload the phone's current configuration files from the phone menu to help you debug configuration problems. A number of files can be uploaded to the provisioning server, one for every active source as well as the current non-default configuration set.

You can use the Web Configuration Utility to upload the files.

To upload the phone's current configuration:

1 Navigate to **Settings** > **Advanced** > **Admin Settings** > **Upload Configuration**.

2 Choose which files to upload: **All Sources**, **Configuration Files**, **Local**, **MR**, **Web**, or **SIP**. If you use the Web Configuration Utility, you can also upload **Device Settings**.

3 Press **Upload**.

4 The phone uploads the configuration file to the location you specified in the parameter `prov.configUploadPath`.

   For example, if you select **All Sources**, a file **<*MACaddress*>-update-all.cfg** is uploaded.

Perform Network Diagnostics

You can use ping and traceroute to troubleshoot network connectivity problems.

To use network diagnostics tools:

1 Go to **Settings > Status > Diagnostics > Network.**

2 Enter a URL or IP address.

3 Press **Enter**.

Reboot the Phone

You can reboot the phone from the phone menu when you want to send configuration changes requiring a reboot or restart to the phone. Parameters that require a reboot or restart are marked in the parameter tables in this guide. If a configuration change does not require a reboot or restart, you can update configuration.

To reboot the phone from the phone menu:

» On the phone, go to **Settings > Advanced > Reboot Phone**.

Restart the Phone

You can restart the phone from the phone menu when you want to send configuration changes requiring a reboot or restart to the phone. Parameters that require a reboot or restart are marked in the parameter tables in this guide. For configuration changes that do not require a reboot or restart, you can update configuration.

To restart the phone from the phone menu:

» On the phone, go to **Settings > Basic > Update Configuration**.

If new Updater or Polycom UC Software is available on the provisioning server, the phone downloads the software. If new software is available on the provisioning server, the phone downloads the software and restarts.

Update Configuration from the Phone Menu

You can update the phone configuration from the phone menu when you want to send configuration changes to the phone. Some configuration changes require a reboot or restart and parameters that require a reboot or restart are marked in the parameter tables in this guide. If there are configuration file changes or new software available on the provisioning server, your phone restarts or reboots if required.

To update configuration from the phone menu:

» On the phone, go to **Settings > Basic** > **Update Configuration**.

Reset the Phone and Configuration

You can reset part or all of the phone and phone configuration.

To access phone reset options:

1 On the phone, go to **Settings > Advanced > Administration Settings > Reset to Defaults**.

   The following table describes the phone reset options.

Phone Reset Options

Setting	Description
Reset Local Configuration	Clears the override file generated by changes using the phone user interface.
Reset Web Configuration	Clears the override file generated by changes using the Web Configuration Utility.
Reset Device Settings	Resets the phone's flash file system settings that are not stored in an override file.
	These are your network and provisioning server settings and include custom certificates and encryption keys. Local, web, and other configuration files remain intact.
Format File System	Formats the phone's flash file system and deletes the UC Software application, log files, configuration, and override files.
	Note that if the override file is stored on the provisioning server, the phone re-downloads the override file when you provision the phone again. Formatting the phone's file system does not delete those device settings affecting network and provisioning, and any certificates and encryption keys remain on the phone.
Reset to Factory	Removes the Web and local override files, any stored configuration files in the flash file system, as well as any custom certificates and encryption keys.
	All network and provisioning settings are reset but the UC Software application and updater remain intact.

Log Files

You can configure Polycom phone logging. Log file names use the following format:

```
[MAC address]_[Type of log].log
```

For example, if the MAC address of your phone is **0004f2203b0**, the app log file name is **0004f2203b0-app.log**.

Related Topics

Severity of Logging Event Parameters

Log File Collection and Storage Parameters

Scheduled Logging Parameters

Upload Logs Manually

You can manually initiate a log upload using a multiple key combination 159 on the phone.

When you manually upload log files, the word *now* is inserted into the name of the file, for example, **0004f200360b-now-boot.log**.

To manually upload logs:

    1 Press the multiple key combination **1 5 9** on the phone.

Log File Descriptions

The phone writes information into several different log files. This table describes the type of information in each.

Log File Descriptions

Log File	Description
Boot Log	Boot logs are sent to the provisioning server in a boot.log file collected from the Updater/BootROM application each time the phone boots up. The BootROM/Updater application boots the application firmware and updates is new firmware is available.
Application Log	The application log file contains complete phone functionality including SIP signaling, call controls and features, digital signal processor (DSP), and network components.
Syslog	For more information about Syslog, see Syslog on Polycom Phones - Technical Bulletin 17124.

Monitoring the Phone's Memory Usage

To ensure that your phones and their configured features operate smoothly, verify that the phones have adequate available memory resources. If you are using a range of phone features, customized configurations, or advanced features, you might need to manage phone memory resources.

If your deployment includes a combination of phone models, consider configuring each phone model separately with its own features instead of applying all phone features to all phone models.

For best performance, the phone should use no more 95% of its available memory. When the phone memory resources are low, you may notice one or more of the following symptoms:

- The phones reboot or freeze up.
- The phones do not download all ringtones, directory entries, backgrounds, or XML dictionary files.
- Applications running in the microbrowser or browser stop running or do not start.

Check Memory Usage from the Phone

You can view a graphical representation of the phone's memory usage directly on the phone.

1 Load and configure the features and files you want to make available on the phone's interface.
2 Navigate to **Settings > Status > Diagnostics > Graphs > Memory Usage.**

View Memory Usage Errors in the Application Log

Each time the phone's minimum free memory goes below about 5%, the phone displays a message in the application log that the minimum free memory has been reached. The application log file is enabled by default. The file is uploaded to the provisioning server directory on a schedule you can configure, see Upload Logs Manually

You can also upload a log file manually. For information on manually uploading log files, refer to Upload Logs Manually.

Phone Memory Resources

If you need to free memory on your phone, review the following table for the amount of memory each customizable feature uses and consider strategies for reducing the amount of memory you need the feature to use.

Phone Memory Resources

Feature	Typical Memory Size
Idle Browser	Varies, depending on number and complexity of application elements.
To reduce memory resources used by the idle browser: • Display no more than three or four application elements. • Simplify pages that include large tables or images.	
Custom Idle Display Image	15 KB
The average size of the Polycom display image is 15 KB. Custom idle display image files should also be no more than 15 KB.	
Main Browser	Varies, depending on number and complexity of applications.

Phone Memory Resources

Feature	Typical Memory Size
To reduce memory resources used by the main browser: • Display no more than three or four application elements. • Simplify pages.	
Local Contact Directory	42.5 KB
Polycom phones are optimized to display a maximum of 250 contacts. Each contact has four attributes and requires 170 bytes. A local contact directory of this size requires 42.5 KB. To reduce memory resources used by the local contact directory: • Reduce the number of contacts in the directory • Reduce the number of attributes per contact	
Corporate Directory	Varies by server
Polycom phones are optimized to corporate directory entries with 5 - 8 contact attributes each. The size of each entry and the number of entries in the corporate directory vary by server. If the phone is unable to display directory search results with more than five attributes, make additional memory resources available by reducing memory requirements of another feature.	
Ringtones	16 KB
The Polycom ringtone files range in size from 30KB to 125KB. If you use custom ringtones, Polycom recommends limiting the file size to 16KB. To reduce memory resources required for ringtones: • Reduce the number of available ringtones.	
Background Images	8 – 32 KB
Polycom phones are optimized to display background images of 50KB. To reduce memory resources required for background images: • Reduce the number and size of available background images.	
Phone Interface Language	90 - 115 KB, depending on language
The language dictionary file used for the phone's user interface ranges from 90KB to 115KB for languages that use an expanded character set. To conserve memory resources, Polycom recommends using XML language files for only the languages you need.	
Web Configuration Utility Interface	250 KB - 370 KB
The language dictionary file used for the Web Configuration Utility interface ranges from 250KB to 370KB for languages that use an expanded character set. To conserve memory resources, Polycom recommends using XML language files for only the languages you need.	

Troubleshooting

This section lists potential issues, problems, and common difficulties and possible solutions.

Power and Startup Issues

The following table describes possible solutions to power and startup issues.

Troubleshooting Power and Startup Issues

The phone has power issues or the phone has no power.

Determine whether the problem is caused by the phone, the AC outlet, or the PoE switch. Do one of the following:
* Verify that no lights appear on the unit when it is powered up.
* Check to see if the phone is properly plugged into a functional AC outlet.
* Make sure that the phone is not plugged into an outlet controlled by a light switch that is turned off.
* If the phone is plugged into a power strip, try plugging directly into a wall outlet instead.

The phone does not boot.

If the phone does not boot, there may be 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 configured with the correct address for the provisioning server on the network.

Dial Pad Issues

The following table describes possible solutions to issues with the dial pad.

Troubleshooting Dial Pad Issues

The dial pad does not work.

If the dial pad on your phone does not respond, do one of the following:
* Check for a response from other feature keys.
* Place a call to the phone from a known working telephone. Check for display updates.
* On the phone, go to **Menu > System Status > Server Status** to check if the telephone is correctly registered to the server.
* On the phone, go to **Menu > System Status > Network Statistics**. Scroll down to see whether 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 that is connected to the telephone is operational.

Screen and System Access Issues

The following table describes possible solutions to screen and system access issues.

Troubleshooting Screen and System Access Issues

There is no response from feature key presses.

If your phone keys do not respond to presses:
- 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. If successful, try to press feature keys while a call is active to access a directory or buddy status.
- On the phone, go to Navigate to **Menu > Status > Lines** to confirm the line is actively registered to the call server.
- Reboot the phone to attempt re-registration to the call server.

The display shows the message *Network Link is Down*.

This message displays when the LAN cable is not properly connected. Do one of the following:
- Check the termination at the switch or hub end of the network LAN cable.
- Check that the switch or hub is operational (flashing link/status lights).
- On the phone, go to **Menu > Status > Network**. Scroll down to verify that the LAN is active.
- Ping the phone from a computer.
- Reboot the phone to attempt re-registration to the call server. Navigate **to Menu > Settings > Advanced > Reboot Phone**).

Calling Issues

The following table provides possible solutions to generic calling issues.

Troubleshooting Calling Issues

There is no dial tone.

If there is no dial tone, power may not be correctly supplied to the phone. Try 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 you are using in-line powering, check that the switch is supplying power to the phone.

The dial tone is not present on one of the audio paths.

If dial tone is not present on one of the audio paths, do one of the following:
- Switch between handset, headset (if present), or handsfree speakerphone to see whether or not dial tone is present on another path.
- If the dial tone exists on another path, connect a different handset or headset to isolate the problem.
- Check configuration for gain levels.

The phone does not ring.

If there is no ringtone but the phone displays a visual indication when it receives an incoming call, do the following:
- Adjust the ring level from the front panel using the volume up/down keys.
- Check the status of handset, headset (if connected), and handsfree speakerphone.

Troubleshooting Calling Issues

The line icon shows an unregistered line icon.

If the phone displays an icon indicating that a line is unregistered, do the following:
• Try to re-register the line and place a call.

Display Issues

The following table provides tips for resolving display screen issues.

Troubleshooting Display Issues

There is no display or the display is incorrect.

If there is no display, power may not be correctly supplied to the phone. Do one of the following:
• Check that the display is illuminated.
• Make sure the power cable is inserted properly at the rear of the phone.
• If your are using PoE powering, check that the PoE switch is supplying power to the phone.
• Use the screen capture feature to verify whether the screen displays properly in the capture. Refer to Capture Your Device's Current Screen.

The display is too dark or too light.

The phone contrast may be set incorrectly. To adjust the contrast, do one of the following:
• Adjust the contrast.
• Reboot the phone to obtain the default level of contrast.
• Use the screen capture feature to verify whether the screen displays properly in the capture. Refer to Capture Your Device's Current Screen.

The display is flickering.

Certain types of older fluorescent lighting cause the display to flicker. If your phone is in an environment lit with fluorescent lighting, do one of the following:
• Angle or move the Polycom phone away from the lights.

The time and date are flashing.

If the time and date are flashing, the phone is disconnected from the LAN or there is no SNTP time server configured. Do one of the following:
• Reconnect the phone to the LAN.
• Configure an SNTP server.
• Disable the time and date if you do not want to connect your phone to a LAN or SNTP server.

Audio Issues

The following table describes possible solutions to audio issues.

Troubleshooting Audio Issues

There is no audio on the headset

If there is no audio on your headset, the connections may not be 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 adjust the volume.

Licensed Feature Issues

The following table describes issues for features that require a license.

Troubleshoot Feature License Issues

Voice Quality Monitoring or H.323 is not available on the phone.

If you cannot access features, check your licenses on the phone by navigating to **Menu > Status > Licenses**.
- You require a license key to activate the VQMon feature on the following VVX business media phones: 101, 201, 300, 301, 310, 311, 400, 401, 410, 411. The following phones do not require a license key to activate the VQMon feature: 500, 600, 1500, Polycom RealPresence Trio.
- You need a license to use H.323 on VVX 1500. You do not need a license to use H.323 on the VVX 500/501, 600/601. Note that H.323 is not supported on VVX 300/301, 310/311, 400/401, 410/411, and SoundStructure VOIP Interface.
- If your phone is not installed with UC Software version 4.0.0 or later, you also require a license for conference management, corporate directory, and call recording.

Software Upgrade Issues

The following table describes possible solutions to issues that may occur during or after a software upgrade.

Troubleshooting Software Upgrade Issues

Some settings or features are not working as expected on the phone.

The phone's configuration may be incorrect or incompatible.

Check for errors on the phone by navigating to **Menu > Status > Platform > Configuration**. If there are messages stating *Errors Found*, *Unknown Params,* or *Invalid values*, correct your configuration files and restart the phone.

The phone displays a *Config file error* message for five seconds after it boots up.

You are using configuration files from a UC Software version earlier than the UC Software image running on the phones. Configuration parameters and values can change each release and specific parameters may or may not be included.
- Correct the configuration files, remove the invalid parameters, and restart the phone.
- See the UC Software Administrator's Guide and Release Notes for the UC Software version you have installed on the phones.

Troubleshooting Software Upgrade Issues

When using the Web Configuration Utility to upgrade phone software, the phone is unable to connect to the Polycom Hosted Server.

Occasionally, the phone is unable to connect to the Polycom hosted server because of the following:

- The Polycom hosted server is temporarily unavailable.
- There is no software upgrade information for the phone to receive.
- The network configuration is preventing the phone from connecting to the Polycom hosted server.

Note: UC Software 4.0.0 does not support internet access for software upgrades through a web proxy.

To troubleshoot the issue:

- Try upgrading your phone later.
- Verify that new software is available for your phone using the *Polycom UC Software Release Matrix for VVX Phones*.
- Verify that your network's configuration allows the phone to connect to http://downloads.polycom.com.
- If the issue persists, try manually upgrading your phone's software.

Wireless Handset Software Upgrade Issues

If any wireless handset fails to update its software, the base station retries pushing the update to the wireless handset three times before moving to the next registered handset. If the base station or wireless handset fails to update or restarts during the update process, the base station or wireless handset restarts with the previous software version.

Try the following solutions if the base station or any of the wireless handsets fail to update:

- Manually update the wireless handset software (refer to section Update the Wireless Handset Software Manually).

- Restart the base station, then pair the base station with the VVX business media phone again.

- To restart the base station, using a paper clip, press and hold the Reset button on the back of the base station for five seconds.

- After the software process is complete for all registered wireless handsets, unregister and register any wireless handsets that failed to update.

If the base station fails to pair with the VVX business media phone after successfully updating, you need to repair the base station with the phone manually (refer to section Pairing a VVX Business Media Phone with a VVX D60 Base Station).