ADMINISTRATOR GUIDE

5.5.3 | December 2017 | 3725-20727-009A

Polycom Trio™ Solution

6001 America Center Drive
San Jose, CA 95002
USA

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

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

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to mailto:DocumentationFeedback@polycom.com.

Polycom Support Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

Before You Begin

Topics:

This guide describes how to administer, configure, and provision Polycom phones and accessories.

The information applies to the following Polycom devices except where noted:

- Polycom Trio™ 8500
- Polycom Trio™ 8800
- Polycom Trio™ Visual+

Note: The Polycom Trio 8800 and 8500 systems are also known as Polycom RealPresence Trio 8800 and 8500 systems.

Audience, Purpose, and Required Skills

This guide is written for a technical audience.

You must be familiar with the following concepts before beginning:

- Current telecommunications practices, protocols, and principles
- Telecommunication basics, video teleconferencing, and voice or data equipment
- Open SIP networks and VoIP endpoint environments

Get Help

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

Polycom and Partner Resources

In addition to this guide, the following documents and other resources provide details about Polycom UC Software:

- 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.

- For information on IP PBX and softswitch vendors, see Polycom Desktop Phone Compatibility. If you're using the Polycom Trio solution, see Polycom Trio and SoundStation IP Platform Compatibility.

To find all Polycom partner solutions, see Strategic Global Partner Solutions.

Documentation Feedback

We welcome your feedback to improve the quality of Polycom documentation.

You can email Documentation Feedback for any important queries or suggestions related to this documentation.

Getting Started

Topics:

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.

Product Overview

Polycom UC software manages the protocol stack, the digital signal processor (DSP), the user interface, and the network interaction on Polycom phones.

You can deploy Polycom UC software by configuring individual phones, but Polycom recommends setting up a provisioning server on your LAN or the internet for large-scale deployments.

UC software 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.

Supported Phones and Accessories

The following table lists the product names, model names, and part numbers for Polycom phones and devices that support Polycom UC Software.

Polycom Trio Product Name, Model Name, and Part Number

Product Name	Model Name	Part Number
Polycom Trio 8500	Polycom Trio8500	3111-66700-001
Polycom Trio 8800	Polycom Trio8500	3111-66700-001
Polycom Trio Visual+	Polycom TrioVisualPlus	3111-66420-001

Working With Polycom UC Software

Polycom phones come installed with updater software that resides in the flash memory of the phone.

When you boot up or reboot the phone, the updater automatically updates, downloads, and installs new software versions or configuration files as needed, based on the server or phone settings.

Configuring Polycom Phones

Polycom provides several methods to configure or 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 phone 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
- USB
- Polycom® Resource Manager software
- Centralized provisioning

Polycom phones can 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.

Polycom phones support FTP, TFTP, HTTP, and HTTPS protocols and use FTP by default.

Record Version Information

In case you need to contact Polycom technical support, you should record the following information for future reference:

- Phone models
- Updater version
- UC Software version
- Partner Platform

Supported Network Configurations

Topics:

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
- An active, configured call server to receive and send SIP messages and to register and authenticate voice endpoints.

  For information on IP PBX and softswitch vendors, see Polycom Desktop Phone Compatibility. If you are using the Polycom Trio Solution, see Polycom 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.

In addition to these requirements, your deployment network should work within the Polycom-supported parameters of network settings, discovery methods such as DHCP, and supported Ethernet 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.

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.

Ethernet Network Connection Methods

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

- Virtual Local Area Networks (VLANs)
- ILink Layer Discovery Protocol and Supported Type Length Values
- ILink Layer Discovery Protocol and Supported Type Length Values

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.

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.

Note: 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.

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

If DHCP option 128 is configured for SIP outbound proxy, do not configure VLAN Discovery option 128 to **Fixed**.

Procedure

1. In the DHCP menu of the Main setup menu, set **VLAN Discovery** to **Fixed** or **Custom**.

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.

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.

Name	Description	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
Chassis-Id[1]	IP address of phone (4 bytes). Note that 0.0.0.0 is not sent until the phone has a valid IP address.	1	6	0x0206	-	5
Port-Id[1]	The MAC address of the phone (6 bytes).	2	7	0x0407	-	3
TTL	The TTL value is 120/0 sec.	3	2	0x0602	-	-

Name	Description	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
Port description	Port description 1.	4	1	0x0801	-	-
System name	Refer to System and Model Names.	5	min len > 0, max len <= 255	-	-	-
System description	Manufacturer's name - “Polycom”; Hardware version; Application version; BootROM version.	6	min len > 0, max len <= 255	-	-	-
Capabilities	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.	7	4	0x0e04	-	-
Management Address	Address String Len - 5, IPV4 subtype, IP address, Interface subtype - “Unknown”, Interface number - “0”, ODI string Len - “0”.	8	12	0x100c	-	-
IEEE 802.3 MAC/PHY config/ status[1]	Auto Negotiation Supported - “1”, enabled/disabled, Refer to PMD Advertise and Operational MAU	127	9	0xfe09	0x00120f	1
LLDP-MED capabilities	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.	127	7	0xfe07	0x0012bb	1

Name	Description	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
LLDP-MED network policy[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.	127	8	0xfe08	0x0012bb	2
LLDP-MED network policy[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.	127	8	0xfe08	0x0012bb	2
LLDP-MED network policy[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.	127	8	0xfe08	0x0012bb	2
LLDP-MED location identification [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.	127	min len > 0, max len <= 511	-	0x0012bb	3

Name	Description	Type	Length	Type Length	Org. Unique Code (3 bytes)	Sub Type
Extended power via MDI	PowerType -PD device PowerSource-PSE&local Power Priority -Unknown, PD Requested Power Value depends on power configuration. If both PSE power and USB charging are disabled then it is 13W. Otherwise, it is 25.5W. This TLV is sent only by the Polycom Trio 8800 and 8500 system. The Polycom Trio Visual+ relies on a hardware handshake only for power negotiations.	127	12	0xfe07	0x00120F	4
LLDP-MED inventory hardware revision	Hardware part number and revision.	127	min len > 0, max len <= 32	-	0x0012bb	5
LLDP-MED inventory firmware revision	BootROM revision.	127	min len > 0, max len <= 32	-	0x0012bb	6
LLDP-MED inventory software revision	Application (SIP) revision.	127	min len > 0, max len <= 32	-	0x0012bb	7
LLDP-MED inventory serial number	MAC Address (ASCII string).	127	min len > 0, max len <= 32	-	0x0012bb	8
LLDP-MED inventory manufacturer name	Polycom	127	11	0xfe0b	0x0012bb	9
LLDP-MED inventory model name		127	min len > 0, max len <= 32	-	0x0012bb	10
LLDP-MED inventory asset ID	Empty (Zero length string).	127	4	0xfe08	0x0012bb	11
End of LLDPDU		0	0	0x0000	-	-

DHCPv6 or DHCPv4 Parameters

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

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.

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

[1] [1] For other subtypes, refer to IEEE 802.1AB, March 2005.
[2] [2] For other application types, refer to TIA Standards 1057, April 2006.
[3] [3] At this time, this TLV is not sent by the phone.

Parameter	DHCPv4 Option	DHCPv4	DHCPv4 INFORM	Configuration File (application only)	Device Settings
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.			

Example: DHCP Option 60 Packet Decode

The following example is a sample decode of a packet (DHCP Option 60) from the Polycom Trio 8800 system.

- Sub-option 2 (part), length, "Real PresencePolycom Trio-Polycom Trio_8800" `02 1a 52 65 61 6c 50 72 65 73 65 6e 63 65 54 72 69 6f 2d 54 72 69 6f 5f 38 38 30 30`
- Sub-option 3 (part number), length, "3111-65290-001,5" `03 10 33 31 31 31 2d 36 35 32 39 30 2d 30 30 31 2c 35`
- Sub-option 4 (Application version), length, "SIP/5.4.1.16972/04-Jan-16 16:05" `05 1d 53 49 50 2f 35 2e 34 2e 31 2e 31 36 39 37 32 2f 30 34 2d 4a 61 6e 2d 31 36 20 31 36 3a 30 35`

`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”

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:

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.
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.

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.

Procedure

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).

Supported Inbound and Outbound Ports

Topics:

The Polycom Trio 8500 and 8800 systems, and the Polycom Trio Visual+ accessory support configuration of inbound and outbound ports.

Inbound Ports for Polycom Trio 8800 and 8500 Systems

The following table lists the inbound IP ports currently used by Polycom UC Software running on Polycom Trio 8800 and 8500 systems.

Inbound IP Port Connections to Polycom Trio Systems

Inbound Port	*Type*	*Protocol*	*Function*	*Default*	*Configurable Port Number*
22	static	TCP	SSH Administration	Off	No
80	static	TCP	HTTP Pull Web interface, HTTP Push	Off	Yes
443	static	TCP	HTTP Pull Web interface, HTTP Push	On	Yes
1023	static	TCP	Telnet Diagnostics	Off	No
1024 - 65535	Dynamic	TCP/UDP	RTP media packets	On	Yes
1024 - 65535	Dynamic	TCP/UDP	RTCP media packets statistics	On	Yes
2222	Dynamic (2222 - 2269)	TCP/UDP	RTP media packets	On	Yes tcpIpApp.port.rtp.mediaPortRangeStart
2223	Dynamic (2222 - 2269)	TCP/UDP	RTCP media packets statistics	On	Yes tcpIpApp.port.rtp.mediaPortRangeStart
5001	static	TCP	People+Content IP	On	No
5060	static	TCP/UDP	SIP signaling	On	No

Inbound Port	*Type*	*Protocol*	*Function*	*Default*	*Configurable Port Number*
5061	static	TLS	SIP over TLS signaling	On	No
8001	static	TCP	HTTPS for modular room provisioning	On	Yes mr.deviceMgmt.port

Outbound Ports for Polycom Trio System

The following table lists the outbound IP ports currently used by Polycom UC Software running on Polycom Trio 8500 or 8800 system.

Outbound IP Port Connections to Polycom Trio Systems

Inbound Port	*Type*	*Protocol*	*Function*	*Default*	*Configurable Port Number*
21	static	TCP	FTP Provisioning, Logs	On	No
22	static	TCP	SSH	On	No
53	static	UDP	DNS	On	No
67	static	UDP	DHCP Server	On	No
68	static	UDP	DHCP Client		No
69	static	UDP	TFTP Provisioning, Logs		No
80	static	TCP	HTTP Provisioning, Logs, Web Interface		No
123	static	UDP	NTP time server		No
389	static	TCP/UDP	LDAP directory query		No
443	static	TCP	HTTPS Provisioning, Logs, Web Interface		No
514	static	UDP	SYSLOG		No
636	static	TCP/UDP	LDAP directory query		No
1024 - 65535	Dynamic	TCP/UDP	RTP media packets	On	Yes
1024 - 65535	Dynamic	TCP/UDP	RTCP media packets statistics	On	Yes

Inbound Port	*Type*	*Protocol*	*Function*	*Default*	*Configurable Port Number*
2222	Dynamic (2222 - 2269)	TCP/UDP	RTP media packets	On	Yes, tcpIpApp.port.rtp.mediaPortRangeStart
2223	Dynamic (2222 - 2269)	TCP/UDP	RTCP media packets statistics	On	Yes, tcpIpApp.port.rtp.mediaPortRangeStart
5060		TCP/UDP	SIP signaling	On	
5061		TCP	SIP over TLS signaling	On	
5222	static	TCP	Resource Manager: XMPP	Off	No
8001	static	TCP	HTTPS for modular room provisioning	On	Yes mr.deviceMgmt.port

Polycom Trio Visual+ Network Ports

The following table provides port usage information when configuring network equipment to support the Polycom Trio Visual+ accessory.

Network Port Connections to Polycom Trio Visual+

Inbound Port	*Type*	*Protocol*	*Function*	*Default*	*Configurable Port Number*
80	static	TCP	HTTP Provisioning, Logs, Web Interface		No
443	static	TCP	HTTPS Provisioning, Logs, Web Interface		No
5060		TCP/UDP	SIP signaling	On	
5061		TCP/UDP	SIP over TLS signaling	On	
8000	static	TCP	HTTP/HTTPS for modular room communications	On	No
8001	static	TCP	HTTP (default) or HTTPS for modular room provisioning	On	Yes mr.deviceMgmt.port

Manually Configuring Phones

Topics:

Polycom offers several methods to manually configure your phone.

You can use the phone menu to configure settings or access the phone through a web interface. When you use the web interface, you can copy settings from one phone to another.

If you need to set up more than 20 phones, Polycom recommends using a centralized provisioning server instead of manual configuration.

Configuring Phones Using the Phone Menu

You can use the menu system on your device as the sole configuration method or along with other methods.

Changes you make from the phone menu override the settings you configure using other methods.

You can access the administrator configuration settings on the **Advanced** menu, which requires an administrator password (the default is `456`). Some setting changes require a device restart or reboot.

Menu systems and interface settings vary by device and by UC Software release. For more information on using your device's phone menu, refer to your device's product documentation.

Configuring Phones Using the Web Configuration Utility

The Web Configuration Utility is a web-based interface that enables you to update the software and configure the phone's current settings.

Changes you make using the Web Configuration Utility override the settings you configure using a centralized provisioning server (if applicable).

You can also import and export configuration files using the Web Configuration Utility to configure multiple phones using the same settings.

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

Configure a Phone Using Simple Setup

You can use the Web Configuration Utility to configure the minimum settings you need for your phone to work.

Procedure

1. Enter your phone's IP address into a web browser on your computer.
2. Select **Admin** as the login type, enter the admin password (the default is `456`), and click **Submit**.
3. Click **Simple Setup** and configure the following settings:
   - **Phone Language** Phone display language
   - **SNTP Server** Server that the phone uses to calculate the display time
   - **Time Zone** Time zone where the phone is located
   - **SIP Server** Server address and port that the phone uses for line registrations
   - **SIP Outbound Proxy** Outbound proxy server address and port that the phone uses to send all SIP requests
   - **SIP Line Identification** Information your phone needs to make calls, such as the phone display name, line address, authentication credentials, and line label
4. Click **Save**.

Configuring Phones by Importing Configuration Files

After you have configured a phone, its settings are saved in its configuration file.

To save time, you can export this configuration file and import it to other phones when you want the same configuration on multiple phones.

Export a Phone Configuration File

You can export the phone's configuration file using the Web Configuration Utility to make changes to the phone's current settings.

You can also export the file from one phone so you can import it into another one.

Procedure

1. Enter your phone's IP address into a web browser on your computer.
2. Select **Admin** as the login type, enter the admin password (the default is `456`), and click **Submit**.
3. Go to **Utilities** > **Import & Export Configuration**.
4. Choose the files to export from the **Export Configuration file** drop-down menu and click **Export**.

Import a Phone Configuration File

You can import a configuration file to your phone using the Web Configuration Utility.

Procedure

1. Enter your phone's IP address into a web browser on your computer.
2. Select **Admin** as the login type, enter the admin password (the default is `456`), and click **Submit**.
3. Go to **Utilities** > **Import & Export Configuration**.
4. Click **Choose File** to select the configuration file from your computer to import and click **Import**.

Reset to Default Settings

You can reset your phone settings to default using the Web Configuration Utility.

Procedure

1. Enter your phone's IP address into a web browser on your computer.
2. Select **Admin** as the login type, enter the admin password (the default is `456`), and click **Submit**.
3. Click **Simple Setup** and then click **Reset to Default**.

Configure a Phone Using a USB Flash Drive

You can configure a Polycom Trio system or Polycom Trio Visual+ accessory with configuration files stored on a USB flash drive.

If you have other USB devices attached to a Polycom Trio system, you must remove them and make sure that the Polycom Trio system correctly recognizes the configuration USB flash drive.

Changes you make using a USB flash drive override the settings you configure using a centralized provisioning server (if applicable). When you remove the USB flash drive, the Polycom Trio system reverts to the provisioning server settings. However, the USB flash drive can initiate `direct.set` changes in the provisioning server settings. The `direct.set` changes can alter parameters on the provisioning server and change basic provisioning settings.

.

Note: Polycom Trio 8800 systems support only File Allocation Table (FAT) file systems. Polycom recommends using FAT32.

Procedure

1. Do one of the following:
   - Format a blank USB 2.0 USB flash drive using FAT32.
   - Delete all files from a previously formatted USB flash drive.
2. Download the UC Software from Polycom Support.
3. Copy the configuration files you want to use to the root of the USB flash drive.

   At a minimum, you must include the following configuration files:
   - Master configuration file: `000000000000.cfg`
   - Polycom Trio 8500: `3111-66700-001.sip.ld`
   - Polycom Trio 8800: `3111-65290-001.sip.ld`
   - Polycom Trio Visual+: `3111-66420.001.sip.ld`
4. Insert the USB flash drive into the Polycom Trio 8800, 8500,or Polycom Trio Visual+ USB port.
5. Enter the Administrator password.

   The system detects the flash drive and starts the update within 30 seconds. The mute keys' indicator lights begin to flash, indicating that the update has started.

The system reboots several times during the update. The update is complete when the indicator lights stop flashing and the **Home** screen displays.

Provisioning Phones

Topics:

You can configure and provision multiple phones with the same settings for large-scale deployments.

If you need to set up more than 20 phones, Polycom recommends using a centralized provisioning server instead of manual configuration.

Network Requirements for Provisioning

Provisioning requires that your phones can securely reach your provisioning server and that your network time settings are in sync with your phones.

Note: When you provision the Polycom Trio solution via Wi-Fi connection to the network, the Polycom Trio solution looks for files on the provisioning server using the LAN MAC address and not the Wi-Fi MAC address.

User Accounts

Each phone user must have an account on your SIP call server.

Recommended Security Settings for Provisioning

Although optional, Polycom recommends using the following security settings when using a provisioning server.

- 802.1X
- VLAN
- File transfers using HTTPS
- SIP signaling over Transport Layer Security (TLS)
- Permissions for configuration and override files

Configure File Upload Permissions

When anyone modifies settings from the phone user interface or Web Configuration Utility, the phone attempts to upload override files with settings to the central server.

When your environment includes a provisioning server, 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.

By default, provisioned phones attempt to upload phone-specific override and other configuration files to the server, but you must configure the server to allow these files to upload. Allowing these file uploads to the provisioning server gives you greater manageability for your phone deployment and help with troubleshooting issues.

Ensure that the file permissions you create provide the minimum required access and that the account has no other rights on the server. All other files that the phone needs to read, such as the application executable and standard configuration files, should be read-only.

If you reformat the phone's file system, the override file is deleted from the phone.

Procedure

1. Configure the server account with read, write, and delete permissions.
2. Create a separate directory on the server for each file type you want to upload and configure the permissions.

   Each directory can have different access permissions.

   Some example file directories include:

   - Log files
   - Override files
   - Contact directory
   - License directory
3. Edit the attributes of the master configuration file that correspond to the directories you created.
4. To allow a phone's override files to upload to the server, configure the override files with enable, read, and write access.

   The default override file names are the following:

   - Phone Menu `<MAC Address>-phone.cfg`
   - Web Configuration Utility `<MAC Address>-web.cfg`

Dynamic Host Configuration Protocol (DHCP)

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

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.

Synchronized Time Settings

Its important to use a SNTP server in your network environment.

If SNTP settings are not available through DHCP, you may need to edit the SNTP GMT offset or SNTP server address, especially for the default daylight savings parameters outside of North America. Depending on your local security policy, you might need to disable the local web (HTTP) server or change its signaling port.

DNS

You need to 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)

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). When using FTPS as the provisioning protocol:
  - Set the value of `log.render.file.size` to 512.
  - Disable the Diffie-Hellman key exchange

Setting Up Your Provisioning Server

You can use a single provisioning server or configure multiple provisioning servers.

Your provisioning servers should be RFC compliant.

Install Provisioning Tools

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

Procedure

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** Host name or IP address of the call server that handles VoIP services on your network.
   - **SIP account information** SIP account credentials 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.
   - **Phone MAC addresses** Unique 12-digit serial number just above the phone's bar code on a label on the back of the phone. You need the MAC address for each phone in your deployment.
   - **Provisioning server IP address** IP address for the system used as the provisioning server. If you want to use your computer system as the provisioning server, then you need your computer's IP address.

Set Up a Single Provisioning Server

You can set up a single provisioning server for your phone deployment.

Procedure

1. Power on the phones and connect them to your VoIP network using a Power over Ethernet (PoE) switch or external adapter and a network cable.
2. Create a root FTP directory on the provisioning computer with full read and write access to all directories and files.

   This is where you need to place configuration files.
3. In your FTP server application, create a user account for the phone to use and take note of the user name and password.
4. Launch the FTP application.

   You must keep it running during provisioning so that the phones can communicate with the UC software.
5. Download Polycom UC Software from Polycom Support and uncompress the files into your root FTP directory.

   You can choose the combined UC software package or the split UC software package.
   - 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.

Set Up Multiple Provisioning Servers

You can configure multiple (redundant) provisioning servers—one logical server with multiple addresses.

You can set up a maximum of eight 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.

Procedure

1. Power on the phones and connect them to your VoIP network using a Power over Ethernet (PoE) switch or external adapter and a network cable.
2. Create a root FTP directory on the provisioning computer with full read and write access to all directories and files.

   This is where you need to place configuration files.
3. In your FTP server application, create a user account for the phone to use and take note of the user name and password.
4. Launch the FTP application.

   You must keep it running during provisioning so that the phones can communicate with the UC software.
5. Download Polycom UC Software from Polycom Support and uncompress the files into your root FTP directory.

   You can choose the combined UC software package or the split UC software package.

   - 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. Map the provisioning server DNS name to a unique IP address for each server.
7. Configure the following settings:
   - Number of times a file transfer tries each server
   - How long to wait between each file transfer attempt
   - Maximum number of servers to which you want to try to transfer files

Test the Provisioning Settings

You can test your provisioning server setup by using the **Quick Setup** option on your device.

This option enables you 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 **Quick Setup** option.

Provisioning Phones

You provision phone features and settings with the UC software configuration files that you create and modify on your provisioning server.

You can also create and update specific phone configuration files, use variable substitution to update all phones in your deployment simultaneously, or configure phone groups.

When provisioning phones, you create configuration files as needed to support your deployment. When creating configuration files; however, do not use the following file names (the phones use these files to store override and logging information):

- `<MACaddress>-phone.cfg`
- `<MACaddress>-web.cfg`
- `<MACaddress>-app.log`
- `<MACaddress>-boot.log`
- `<MACaddress>-license.cfg`

Note: You can use the multiple key combination shortcut by simultaneously pressing **1-4-7** to display the following provisioning information on the phone:

- Phone IP address
- Phone MAC address
- VLAN ID
- Boot server type (FTP, TFTP, HTTP, HTTPS)

Provision Multiple Phones

You need to ensure that your phones are directed to the provision server.

You need to modify the default master configuration file with the provisioning server information.

Procedure

1. Create a `phone<MACaddress>.cfg` file for each phone you want to deploy.
2. Add the SIP server registration information and user account information to the appropriate parameters in the phone configuration file, such as `reg.1.address, reg.1.auth.userId, reg.1.auth.password, reg.1.label, reg.1.type` .
3. Create a `site<location>.cfg` file for each site location.

   Include SIP server or feature parameters such as `voIpProt.server.1.address` and `feature.corporateDirectory.enabled` .
4. Add the file name of each phone and site configuration file to the `CONFIG_FILES` attribute of the master configuration file, such as a reference to `phone<MACaddress>.cfg` and `sipVVX500.cfg` .
5. On each phone's **Home** screen or idle display, select **Settings** > **Advanced** > **Admin Settings** > **Network Configuration** > **Provisioning Server.**

   When prompted for the administrative password, enter `456`.

6. Press **Select**.
7. Scroll down to **Server Type** and make sure that it is set to **FTP**.
8. Scroll down to **Server Address** and enter the IP address of your provisioning server.

   Press **Edit** to edit the value and then press **OK**.
9. Scroll down to **Server User** and **Server Password** and enter the user name and password of the account you created on your provisioning server.
10. Press **Back** twice.
11. Scroll down to **Save & Reboot**, and then press **Select**.

    The phone reboots and the UC software modifies the `APP_FILE_PATH` attribute of the master configuration file so that it references the appropriate `sip.ld` files.
12. Verify that the phones are provisioned:

    a. On the phone, press **Settings** (**Menu** if using a VVX 1500) and go to **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).

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

Provision Phones Using Variable Substitution

You can configure multiple phones in your deployment using variable substitution with a single master configuration file instead of a `<MACaddress>.cfg` file for each phone.

This method is useful if you need to maintain or modify settings common to all phones in your deployment or to specific phone groups based on variables such as phone model or part number. Additionally, if you want to add a new phone to your deployment, you need only create one new file.

Procedure

1. Create a configuration file for each phone containing the information you want to configure, such as registration information.

   You must identically name each of these phone-specific configuration files except for the information you plan to substitute with a variable string, such as phone's MAC address, part number, or phone model.

   For example, create phone-specific configuration files that contain registration information and name them `reg-basic_0004f2000001.cfg` , `reg-basic_0003a7100076.cfg` , `reg-basic_0004e5800094.cfg` , and so forth.
2. Copy one of the configuration file names and modify it by replacing the specific phone information with the corresponding variable as shown in the following table (make sure you include the square brackets).

   For example, change `reg-basic_0004f2000001.cfg` to `reg-basic_[PHONE_MAC_ADDRESS].cfg` or change `reg-basic_VVX500.cfg` to `reg-basic_[PHONE_MODEL].cfg` .

Variable	Description
`[PHONE_MAC_ADDRESS]`	Use to configure all phones in your deployment
`[PHONE_PART_NUMBER]`	Use to configure all phones with a specific part number
`[PHONE_MODEL]`	Use to configure a specific phone model

3. Add the file name with the variable substitution to the `CONFIG_FILES` attribute of the master configuration file.
4. Save the master configuration file.

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.

Procedure

1. Do one of the following:
   - Look on the label on the back of the phone.
   - On the phone, press **Settings** (**Menu** if using a VVX 1500) and go to **Status** > **Platform** > **Phone** > **S/N:**.
   - Use a multi-key shortcut by simultaneously pressing **1-4-7**.

Provision an Individual Phone

You can configure phones individually by creating an individual master configuration file for each phone.

This configuration method gives you a high degree of control over each phone, but for large deployments, the file naming scheme can require additional file management as you must create and edit at least two unique files for each phone in your deployment.

Procedure

1. Create a copy of the master configuration file template for the phone and name it `<MACaddress>.cfg` , replacing `000000000000` with the unique MAC address of the phone you want to configure.

   Note that you must use only numerals and lowercase letters in the file name.
2. Create a configuration file for the phone containing its unique information such as registration information.

   Name your files based on the file contents or purpose. 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.

   For example, you might use parameters from the `reg-basic.cfg` template file to create a registration file named `reg-basic_john_doe.cfg` .

3. Enter the name of the configuration files you created to the `CONFIG_FILES` attribute of the phone's `<MACaddress>.cfg` file.
4. Save the master configuration file.

Provision a Phone Group

You can apply features and settings to a phone group by phone model name or part number.

If you create configuration files for phone groups using the part number and model name for the same type of phone, the part number configuration file has priority over the phone model configuration file.

Procedure

1. Create a configuration file with the settings you want to apply.

   Name the file using the phone group's part number or phone model name, such as `3111-44500-001.cfg` or `VVX500.cfg`.
2. Add the file name to the `CONFIG_FILES` attribute of the master configuration file.
3. Save the master configuration file.

Working with Configuration Files

Topics:

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. You use configuration files when provisioning phones via a provisioning server, although you can also export and import configuration files between individual phones.

In order to work with configuration files, you'll need to install an XML editor.

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 any or all the phones in your deployment, including various groups of phones, specific phone models, or a single phone.

The default name for the master configuration file is `00000000000.cfg` . You can use the default name or rename the master configuration file to configure features and settings for your phone deployment. The file name must contain at least five characters and end with `.cfg` .

You can also specify the location of a master configuration file you want the phones to use, for example, `http://usr:pwd@server/dir/example1.cfg` . If the phone cannot find and download a file from that location, the phone uses an individual phone master configuration file or the default master configuration file.

The master configuration file applies the settings from the component configuration files listed in the `CONFIG_FILES` attribute in the following ways:

- The files you enter are read from left to right.
- Duplicate settings are applied from the configuration file in the order you list them.

The following table describes the XML field attributes in the master configuration file and the `APPLICATION` directories.

Master Configuration File XML Field Attributes

Attribute	Description
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 files. 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.

Attribute	Description
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.

Note: 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.

XML 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
- Ringtones
- Log files
- A template contact directory 000000000000-directory~.xml
- A licensing directory

Configuration Templates

Most configuration parameters are located in only one template file, but some are included in two or more files.

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.

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		

Name	Description	Deployment Scenarios
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	
lync.cfg	Microsoft Skype for Business parameters	Typical Microsoft Skype for Business environment
polycomConfig.xsd*		
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
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

Name	Description	Deployment Scenarios
techsupport.cfg	Available by special request from Polycom Customer Support.	Use for troubleshooting and debugging only
video.cfg	Polycom Trio 8500 or 8800 system when connected and paired with Polycom Trio Visual+ accessory	Typical Hosted Service Provider if using Polycom Trio 8800 system and Polycom Trio Visual+ accessory 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. You can 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.

You must use the appropriate XML code for special characters in a configuration file:

- & as &
- ” as "
- ' as '
- < as <

- > as `>`
- random numbers as `&0x12;`

Microsoft Exchange Integration

Topics:

If you have a Skype for Business, Office 365, Lync Server 2010 or 2013 deployment, you can integrate with Microsoft Exchange Server.

You can set up 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 with the Exchange Server, you can:

- Verify the status of Exchange Server services on each phone.
- View the status of each service in the Web Configuration Utility.

Polycom Trio Solution with Skype for Business

You can deploy a Polycom Trio system with Microsoft® Skype™ for Business Online, Microsoft® Skype™ for Business 2015, Microsoft® 2013, and Microsoft® 2010 on-premises.

For a list of available features and instructions on deploying Polycom Trio solution with Skype for Business and Lync Server, see the latest *Polycom UC Software with Skype for Business Deployment Guide at PolycomPolycom Trio* on Polycom Support.

Skype for Business Private Meeting Parameters

Use the following parameters to configure Skype for Business private meetings.

Private Meeting Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	exchange.meeting.private.showAttendees	0 (default) - Meetings marked as private in Outlook do not show the list of meeting attendees and invitees on the Polycom Trio calendar. 1 - Meetings marked as private in Outlook show the list of meeting attendees and invitees on the Polycom Trio calendar.	
	exchange.meeting.private.showDescription	0 (default) - Meetings marked as private in Outlook do not display a meeting description on the Polycom Trio calendar. 1 - Meetings marked as private in Outlook display a meeting description on Polycom Trio calendar.	
	exchange.meeting.private.showLocation	0 (default) - Meetings marked as private in Outlook do not display the meeting location on the Polycom Trio calendar. 1 - Meetings marked as private in Outlook display the meeting location on the Polycom Trio calendar.	
	exchange.meeting.private.showSubject	0 (default) - Meetings marked as private in Outlook do not display a subject line on Polycom Trio calendar. 1 - Meetings marked as private in Outlook display a subject line on Polycom Trio calendar.	
	exchange.meeting.private.showMoreActions	1 (default) - Meetings marked as private in Outlook display the ‘More Actions' button, when applicable. 0 - Meetings marked as private in Outlook do not display the ‘More Actions' button.	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	exchange.meeting.private.showOrganizer	1 (default) - Meetings marked as private in Outlook display the name of the meeting organizer on the Polycom Trio calendar. 0 - Meetings marked as private in Outlook display the name of the meeting organizer on the Polycom Trio calendar.	
	exchange.meeting.private.enabled	1 (default) - The Polycom Trio considers the private meeting flag for meetings marked as private in Outlook. 0 - Treat meetings marked as private in Outlook the same as other meetings.	
	exchange.meeting.private.promptForPIN applications.cfg	0 (default) - Disable the Skype for Business Conference ID prompt that allows users to join meetings marked as 'private'. 1 - Enable the Skype for Business Conference ID prompt that allows users to join meetings marked as 'private'.	

Integrating with Microsoft Exchange

You can integrate with Microsoft Exchange using one of the following methods:

- Exchange Server auto-discover
- Provision the phone with the Microsoft Exchange address
- Web Configuration Utility

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

Provision the Microsoft Exchange Calendar

You can provision your phones with the Microsoft Exchange calendar.

When you connect a Polycom Trio 8500 or 8800 system to Skype for Business, a Calendar icon displays on the phone Home screen that enables users to access features. Users can view and join Outlook calendar events directly from Polycom Trio 8800 which displays the day and meeting view for scheduled events. You can't schedule calendar events or view email from the phone.

When you pair Polycom Trio 8500 or 8800 with Polycom Trio Visual+, you can configure if users receive reminder notifications on the display monitor and whether or not an alert sound accompanies reminder notifications.

If you are using Polycom Trio Solution, parameters are included in *Example Configuration File for Polycom Trio Collaboration Kit with Skype for Business* on **Polycom Trio** > **Documentation** > **Setup Documents**.

Procedure

1. Add the following parameters 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 can use the Web Configuration Utility to manually enable your phones with the Microsoft 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.

Procedure

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

   For instructions, see "Accessing the Web Configuration Utility" in the *Polycom UC Software with Skype for Business - Deployment Guide* on Polycom Trio.
2. Log in to the Web Configuration Utility as Admin (default password `456`).
3. Go to **Settings** > **Applications** > **Exchange Applications,** and expand **Exchange Applications**.
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.

Verify the Microsoft Exchange Integration

You can verify if all of the Exchange services are working.

Procedure

1. Go to **Status** > **Diagnostics** > **Warnings** on the phone.
2. View the status of each service in the Web Configuration Utility.

Configuring the Microsoft Exchange Server

You should configure the following settings to take advantage of Microsoft Exchange services on your phones.

Note: 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 Exchange server, you can 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.

Synchronizing Call Logs

On the Exchange server, you can enable the option to save calls logs to each user's conversation history in Outlook.

Directory Search

You can enable the ABS service on the Exchange server.

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.

Microsoft Exchange Parameters

The following table lists parameters that configure the Microsoft Exchange integration.

Microsoft Exchange Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`applications.cfg`	`exchange.meeting.alert.followOfficeHours`	1 - Audible alerts occur during business hours. 0 - Audible alerts occur at all times.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applications.cfg	exchange.meeting.alert.tonePattern	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
applications.cfg	exchange.meeting.alert.toneVolume	10 (default) - Set the volume level of reminder alert tones. 0 - 17	No
applications.cfg	exchange.meeting.allowScrollingToPast	0 (default) - Do not allow scrolling up in the Day calendar view to see recently past meetings. 1 - Allow scrolling up in the Day calendar view to see recently past meetings.	
applications.cfg	exchange.meeting.hideAllDayNotification	0 (default) - All day meeting notifications display on the Calendar screen. 1 - All day meeting notifications are hidden from the Calendar screen.	No
applications.cfg	exchange.meeting.parseOption	Indicates the field in the meeting invite from which the VMR or meeting number should be fetched. Location (default) All LocationAndSubject Description	
applications.cfg	exchange.meeting.parseWhen	NonSkypeMeeting (default) - Disable number-searching on the Calendar to look for additional numbers to dial in Skype Meeting calendar entries. Always - Enables number-searching on the Calendar to look for additional numbers to dial even for Skype Meetings.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applications.cfg	exchange.meeting.phonePattern	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
applications.cfg	exchange.meeting.reminderEnabled	1 (default) - Meeting reminders are enabled. 0 - Meeting reminders are disabled.	No
applications.cfg	exchange.meeting.reminderInterval	300 seconds (default) 60 - 900 seconds Set the interval at which phones display reminder messages.	No
applications.cfg	exchange.meeting.reminderSound.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.reminderEnabled is also enabled.	No
applications.cfg	exchange.meeting.reminderType	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
applications.cfg	exchange.meeting.showAttendees	1 (default) - Show the names of the meeting invitees. 0 - Hide the names of the meeting invitees.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applications.cfg	exchange.meeting.showDescription	1 (default) - Show Agenda/Notes in Meeting Details that displays after you tap a scheduled meeting on the Polycom Trio 8800 calendar. 0 - Hide the meeting Agenda/Notes.	No
applications.cfg	exchange.meeting.showLocation	1 (default) - Show the meeting location. 0 - Hide the meeting location.	No
applications.cfg	exchange.meeting.showMoreActions	1 (default) - Show More Actions in Meeting Details to allow users to choose a dial-in number. 0 - Hide More Actions in Meeting Details.	No
applications.cfg	exchange.meeting.showOnlyCurrentOrNext	0 (default) - Disabled the limitation to display only the current or next meeting on the Calendar. 1 - Enables the limitation to display only the current or next meeting on the Calendar.	No
applications.cfg	exchange.meeting.showOrganizer	1 (default) - Show the meeting organizer in the meeting invite. 0 - Hide the meeting organizer in the meeting invite.	No
applications.cfg	exchange.meeting.showSubject	1 (default) - Show the meeting Subject. 0 - Hide the meeting Subject.	No
applications.cfg	exchange.meeting.showTomorrow	1 (default) - Show meetings scheduled for tomorrow as well as meetings scheduled for today. 0 - Do not show meetings scheduled for tomorrow.	No
applications.cfg	exchange.menu.location	Features (default) - Displays the Calendar in the global menu under Settings > Features. Administrator - Displays the Calendar in the Admin menu at Settings > Advanced > Administration Settings.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applications.cfg	exchange.reconnectOnError	1 (default) - The phone attempts to reconnect to the Exchange server after an error. 0 - The phone does not attempt to reconnect to the Exchange server after an error.	No
applications.cfg	exchange.server.url	NULL (default) string The Microsoft Exchange server address.	No
applications.cfg	feature.EWSAutodiscover.enabled	If you configure exchange.server.url and set this parameter to 1, preference is given to the value of exchange.server.url . 1 (default) - Lync Base Profile 0 (default) - Generic Base Profile 1 - 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
applications.cfg	feature.exchangeCalendar.enabled	1 (default) - The calendaring feature is enabled. 0 - The calendaring feature is disabled. 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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.exchangeCalendar.enabled	For the Polycom 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. 1 (default) - Lync Base Profile 0 (default) - Generic Base Profile 0 - 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) - Lync Base Profile 0 (default) - Generic Base Profile 1 - 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 - The Exchange call log feature is disabled and the user call logs history cannot be retrieved from the Exchange server.	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
features.cfg	feature.exchangeContacts.enabled	1 (default) - Lync Base Profile 0 (default) - Generic Base Profile 1 - 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.enabled to use the Exchange call log feature.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	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.enabled to use the Exchange call log feature.	No
features.cfg	feature.exchangeVoiceMail.enabled	1 (default) - Lync Base Profile 0 (default) - Generic Base Profile 1 - 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.cfg	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.exchangeVoiceMail.skipPin.enabled	0 (default) - Enable PIN authentication for Exchange Voicemail. Users are required to enter their PIN before accessing Exchange Voicemail. 1 - Disable PIN authentication for Exchange Voicemail. Users are not required to enter their PIN before accessing Exchange Voicemail.	No
features.cfg	feature.exchangeVoiceMail. skipPin.enabled	1 (default) - 0 -	No
features.cfg	feature.lync.abs.enabled	1 (default) - Lync Base Profile 0 (default) - Generic Base Profile 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
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	features.contacts.readonly	0 (default) - Skype for Business Contacts are editable. 1 - Skype for Business are read-only.	No
features.cfg	up.oneTouchVoiceMail[1]	1 (default) - Lync Base Profile 0 (default) - Generic Base Profile 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

Configuring Security Options

Topics:

Polycom's Open SIP UC Software enables you to optimize security settings.

These includes changing the passwords for the phone, enabling users to lock their phones, and blocking administrator functions from phone users.

Administrator and User Passwords

You can change the default 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 you 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.

Each time you connect a Polycom Trio 8500 or 8800 system with a Polycom Trio Visual+ accessory, the Visual+ user password is reset to match the Polycom Trio system user password. You can change the Polycom Trio Visual+ password on the Polycom Trio menu or Web Configuration Utility.

When the Polycom Trio solution Base Profile is set to SkypeUSB, you can set the keyboard entry mode for the password in the Advanced menu on the phone.

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.

Procedure

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.

Procedure

1. In the Web Configuration Utility, select **Settings** > **Change Password**.
2. Update the passwords for the **Admin** and **User**.

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	The minimum character length for administrator passwords changed using the phone. Use 0 to allow null passwords. 1 (default) 0 -32	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.pwd.length.user	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
device.cfg, site.cfg	device.auth.localAdminPassword	Specify a local administrator password. 0 - 32 characters You must use this parameter with device.auth.localAdminPassword.set="1"	No
device.cfg, site.cfg	device.auth.localAdminPassword.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

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
- Host and device ports
- Bluetooth
- NFC
- Wi-Fi

Note: At least one audio port must be enabled to send and receive calls.

Disable Unused Ports and Features Parameters

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	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	ptt.pttMode.enable	0 (default) - Disable push-to-talk mode. 1 - Enable push-to-talk mode.	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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	feature.doNotDisturb.enable	1(default) - Enable Do Not Disturb (DND). 0 - Disable Do Not Disturb (DND).	Yes
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

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.

Note: 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, both 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.

Visual Security Classification Parameters

To enable the visual security classification 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

Encryption

Polycom supports the use of encryption to protect configuration files, and phone calls.

Encrypting Configuration Files

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.

Note: 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**.

Note: 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.

Procedure

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.

Configuration File Encryption Parameters

The following table provides the parameters you can use to encrypt your configuration files.

Configuration File Encryption Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg	device.sec.configEncryption.key	Set the configuration encryption key used to encrypt configuration files. string	Yes
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

Securing Phone Calls with SRTP

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.

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. Phone will send only one SRTP m-line for audio and video instead of multiple m-lines when VoSIP is enabled.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Enabling Users to Lock Phones

This feature enables users to lock their phones to prevent access to menus or directories.

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.

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	phoneLock.Allow.AnswerOnLock	1(default) - The phone answers any incoming call without asking to UNLOCK. 0 - The phone asks to UNLOCK before answering.	No
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.browserEnabled	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	phoneLock.dndWhenLocked	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
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

Locking the Basic Settings Menu

By default, all users can access the Basic settings menu available on the Polycom 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.

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

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.

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
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

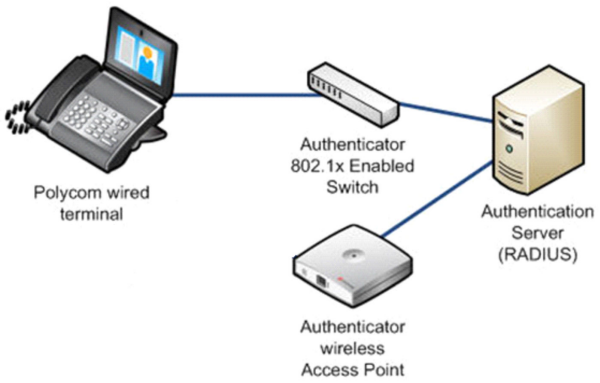
802.1X Authentication

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

A typical 802.1X network configuration



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 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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

Certificates

Topics:

Security certificates are an important element in deploying a solution that ensures the integrity and privacy of communications involving Polycom® UC Software devices.

Polycom phones are installed with a Polycom-authenticated “built-in” device certificate that you can use or you can choose to customize your security by requesting additional certificates from a certificate authority of your choice.

You can customize security configuration options to determine type of device certificate is used for each of the secure communication options. By default, all operations will utilize the factory-installed device certificate unless you specify otherwise.

Note: 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.

Certificates are used in the following situations:

- Mutual TLS Authentication: Allows a server to verify that a device is truly a Polycom device (and not a malicious endpoint or software masquerading as a Polycom device). This could be used for tasks like provisioning, or SIP signaling using TLS signaling. For example, certain partner provisioning systems use Mutual TLS as does Polycom® Zero Touch Provisioning (ZTP).
- Secure HTTP (https) access to the web server on the phone at https://<IP ADDRESS OF PHONE>. The web server is used for certain configuration and troubleshooting activities.
- Secure communications utilizing the Polycom Applications API.

There are different options for utilizing device certificates on the phone:

- Two platform device certificates. These certificates are loaded onto the device by the system administrator and can be configured to be used for any of the following purposes: 802.1X Authentication, provisioning, syslog, SIP signaling, browser communications, presence, and LDAP. Certificates for syslog, 802.1X, and provisioning must applied using TLS platform profiles.
- Six application device certificates. These certificates are loaded onto the device by the system administrator and can be used for all of the operations listed above for platform certificates. You cannot use TLS application profiles to applied certificates for 802.1X, syslog, and provisioning.

  Note: 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.

Using the Factory-Installed Certificate

A factory-installed device certificate is installed at the time of manufacture and is unique to a device (based on the MAC address) and signed by the Polycom Certificate Authority (CA).

Since it is installed at the time of manufacture, it is the easiest option for out-of-box activities, especially phone provisioning.

You can use the factory-installed certificate for all your security needs. To configure your web servers and/or clients to trust the Polycom factory-installed certificates, you must download the Polycom Root CA certificate, which is available at http://pki.polycom.com/pki. You may also need to download the Intermediate CA certificates if determined by the authenticating server.

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 you enable Mutual TLS, you must have a root CA download (the Polycom Root CA certificate or your organization's CA) on the HTTPS server.

The certificate is set to expire on March 9, 2044.

Note: 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.

Check for a Device Certificate

The 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 certificate pre-installed.

Procedure

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 displays:

   - **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.

Customizing Certificate Use

You can add custom certificates to the phone and set up the phone to use the certificates for different features.

For example, the phone's factory-installed certificate can be used for authentication when phone provisioning is performed by an HTTPS server. You can use a different certificate when accessing content through a browser.

Determining TLS Platform Profiles or TLS Application Profiles

You use TLS Platform or TLS Application profiles to customize where your installed certificates are used for authentication.

After you install certificates on the phone, you can 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.

Alternatively, you can choose which TLS platform profile or application profile to use for each TLS application. You can use platform profiles for any of the following purposes: phone provisioning, for applications running on the microbrowser and browser, and for 802.1X, LDAP, and SIP authentication. You can use application profiles for all applications except 802.1X, syslog, and provisioning.

Note: For more information on using custom certificates, see *Technical Bulletin 17877: Using Custom Certificates With Polycom Phones*.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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.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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

TLS Protocol Configuration for Supported Applications

You can configure the TLS Protocol for the following supported applications:

- LDAP
- SIP
- SOPI
- Web server
- XMPP
- Exchange services
- Syslog
- Provisioning
- 802.1x

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	Configures the lowest TLS/SSL version to use for handshake negotiation between phone and 802.1x authentication. The phone handshake starts with the highest TLS version irrespective of the value you configure. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No
device.cfg, site.cfg	device.sec.TLS.protocol.prov	Configures the lowest TLS/SSL version to use for handshake negotiation between phone and provisioning. The phone handshake starts with the highest TLS version irrespective of the value you configure. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No
device.cfg, site.cfg	device.sec.TLS.protocol.syslog	Configures the lowest TLS/SSL version to use for handshake negotiation between phone and Syslog. The phone handshake starts with the highest TLS version irrespective of the value you configure. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, site.cfg	sec.TLS.protocol.exchangeServices	Configures the lowest TLS/SSL version to use for handshake negotiation between phone and Exchange services. The phone handshake starts with the highest TLS version irrespective of the value you configure. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No
device.cfg, site.cfg	sec.TLS.protocol.ldap	Configure the lowest TLS/SSL version to use for handshake negotiation between phone and Lightweight Directory Access Protocol (LDAP). The phone handshake starts with the highest TLS version irrespective of the value you configure. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No
device.cfg, site.cfg	sec.TLS.protocol.sip	Configures the lowest TLS/SSL version to use for handshake negotiation between the phone and SIP signaling. The phone handshake starts with the highest TLS version irrespective of the value you configure. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No
device.cfg, site.cfg	sec.TLS.protocol.sopi	Configures the lowest TLS/SSL version to use for handshake negotiation between phone and SOPI. The phone handshake starts with the highest TLS version irrespective of the value you configure. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, site.cfg	sec.TLS.protocol.webServer	Configures the lowest TLS/SSL version to use for handshake negotiation between phone and web server. The phone handshake starts with the highest TLS version irrespective of the value you configure. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No
device.cfg, site.cfg	sec.TLS.protocol.xmpp	Configures the lowest TLS/SSL version to use for handshake negotiation between phone and XMPP. The phone handshake starts with the highest TLS version irrespective of the value you configure. TLSv1_0 (default) SSLv2v3 TLSv1_1 TLSv1_2	No

TLS Parameters

The next table lists configurable TLS parameters.

For the list of configurable ciphers, refer to the Secure Real-Time Transport Protocol table.

TLS Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	sec.TLS.browser.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.cfg	sec.TLS.customDeviceCert.x	The custom device certificate for TLS Application Profile x (x= 1 to 6). Null (default) String	No

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.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
site.cfg	sec.TLS.SOPI.cipherList	Selects a cipher key from the list of available ciphers. NoCipher (default) 1 - 1024 character string	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

TLS Profile Selection Parameters

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

Configurable TLS Cipher Suites

You can configure which cipher suites to offer and accept during TLS session negotiation. The following table lists supported cipher suites. NULL cipher is a special case that does not encrypt the signaling traffic.

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

Cipher	Cipher Suite
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

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) 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

Create a Certificate Signing Request

You generate a certificate signing request directly from the Polycom device.

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.

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.

You must have a provisioning server in place before generating the certificate signing request.

Procedure

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.
5. Forward the CSR to a Certificate Authority (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.

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.

You can download certificate(s) to a phone in the following ways:

- Using a configuration file
- Through the phone's user interface
- Through the Web Configurable Utility

Note: For VVX 1500 phones, the maximum certificate size on Platform CA1 is 1536KB and 4KB for Platform CA2.

Procedure

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.

Custom URL Location for LDAP Server CA Certificate

You can set the URL from where Polycom phones can download a CA certificate or a chain of CA certificates required to authenticate the LDAP server.

By default, all Polycom-installed profiles are associated with the default cipher suite and use trusted and widely recognized CA certificates for authentication. You can download and install up to seven custom CA certificates onto a Polycom phone. The certificates are installed in descending order starting with the Application CA 7 slot and continues to Application CA 1 slot depending on how many certificates are in the chain.

Note: If the custom application CA certificate slots already have CA certificates installed on your Polycom phones, downloading LDAP server CA certificates will overwrite any existing certificates on the phone in descending order starting with the seventh certificate.

Custom URL Location for LDAP Server Certificates Parameters

Use the parameter in the following table to configure this feature.

In addition to the parameter in the following table, you must also configure the following Corporate Directory parameters:

- `sec.TLS.proflieSelection.LDAP = ApplicationProfile1`

Custom URL Location for LDAP Server Certificates Parameters

Template	Parameter	Permitted Values	Change Causes Reboot or Restart
`site.cfg`	`sec.TLS.LDAP.customCaCertUrl`	Enter the URL location from where the phone can download LDAP server certificates. String (default) 0 - Minimum 255 - Maximum You must configure parameters `dir.corp.address` and `feature.corporateDirectory.enabled` as well to enable this parameter.	No

Confirm the Installed LDAP Server Certificates on the Phone

After you set the URL for the location where the phone can download the chain of CA certificates using the parameter `sec.TLS.LDAP.customCaCertUrl` and enabled the parameters `dir.corp.address` and `feature.corporateDirectory.enabled` as well, the certificates are automatically updated on the phones. You can confirm that the correct certificates were downloaded and installed on the phone.

Procedure

1. On the phone, navigate to **Settings** > **Advanced**, and enter the administrator password.
2. Select **Administrative Settings** > **TLS Security** > **Custom CA Certificates** > **Application CA placeholders**.
3. Check that correct certificates were installed on the phone.

Upgrading the Software

Topics:

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.

- You can upgrade software with the user-controlled software upgrade feature.
- If you are upgrading software from UC Software 4.0.x, update the phones from your 4.0.x version.

Upgrade UC Software Using a USB Flash Drive

You can use a USB flash drive to upgrade the software on your Polycom Trio system.

Changes you make using a USB flash drive override the settings you configure using a centralized provisioning server (if applicable). When you remove the USB flash drive, the Polycom Trio system reverts to the provisioning server settings.

Note: Polycom Trio 8800 supports only File Allocation Table (FAT) file systems. Polycom recommends using FAT32.

Procedure

1. Do one of the following:
   - Format a blank USB 2.0 USB flash drive using FAT32.
   - Delete all files from a previously formatted USB flash drive.
2. Download the UC Software from Polycom Support.
3. Copy the configuration files you want to use to the root of the USB device.

   The minimum required configuration files must be copied to the drive:
   - Master configuration file: `000000000000.cfg`.
   - Polycom Trio 8500: `3111-66700-001.sip.ld`
   - Polycom Trio 8800: `3111-65290-001.sip.ld`.
   - Polycom Trio Visual+: `3111-66420.001.sip.ld`.
4. Insert the USB flash drive into the Polycom Trio system or Polycom Trio Visual+ USB port.
5. Enter the Administrator password.

   The system detects the flash drive and starts the update within 30 seconds. The mute keys' indicator lights begin to flash, indicating that the update has started.

The system reboots several times during the update. The update is complete when the indicator lights stop flashing and the **Home** screen displays.

Upgrading UC Software on a Single Phone

You can use the software upgrade tool in the Web Configuration Utility to update the 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.

User-Controlled Software Update

This feature enables phone users to choose when to accept software updates you send to the phones.

You 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 it is not available with Skype for Business.

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	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

Diagnostics and Status

Topics:

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.

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.

Procedure

1. Select **Settings** > **Status** > **Select**.
2. Scroll to a **Status** menu item and press **Select**.

   The following table lists available options:

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 • Hardware tests to verify correct operation of the microphones and speaker. • 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.

Procedure

1. Go to **Settings** > **Status** > **Diagnostics** > **Warnings**.
2.
   - **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.
3. Choose from these tests:
   - **Audio Diagnostics** Test the speaker, microphone, handset, and a third party headset.
   - **Display Diagnostics** Test the LCD for faulty pixels.
   - **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.

Procedure

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.

Procedure

1. Go to **Settings** > **Status** > **Diagnostics** > **Network**.
2. Enter a URL or IP address.
3. Press **Enter**.

Restart the Polycom Trio Visual+

You can restart the Polycom Trio Visual+ connected to a Polycom Trio 8500 or 8800 system.

Procedure

1. On the Polycom Trio system Home screen, go to **Settings** > **Basic** > **Restart Networked Devices**.

Restart the Polycom Trio System and Polycom Trio Visual+

You can restart the Polycom Trio system and Polycom Trio Visual+ together.

Procedure

1. On the Polycom Trio system Home screen, go to **Settings** > **Basic** > **Restart System**.

Reset the Polycom Trio System to Factory Default Settings

You can reset the Polycom Trio system to factory default settings at power up.

Resetting to defaults clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to 456.

Procedure

1. Power on the Polycom Trio system.
2. When the Polycom logo shows on the screen, press and hold the four corners of the LCD display screen.
3. Let go when the Mute light begins flashing.

Reset the Polycom Trio Visual+ to Factory Default Settings

You can reset the Polycom Trio Visual+ to factory default settings from the interface at power up.

Resetting to defaults clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to 456.

Procedure

1. Power on the Polycom Trio Visual+.
2. When the pairing button light turns on, press and hold the pair button.
3. Let go of the pair button when the light begins flashing.

Access Video Transmission Diagnostics

You can access the Polycom Trio solution jitter statistics from the phone menu to evaluate video transmissions.

Procedure

1. On the Polycom Trio 8800 system Home screen, go to **Settings** > **Status** > **Diagnostics** > **Graphs** > **Networked Devices Graphs**.

Status Indicators on the Polycom Trio Solution

The Polycom Trio 8800 and 8500 systems and Polycom Trio Visual+ accessory use LED lights to indicate the status of the solution.

The following tables describe each of the status indicators on the Polycom Trio and Polycom Trio Visual+.

Polycom Trio Status Indicators

Status	Description
Off	Device is in idle state or powered off.
Green	In a call with audio unmuted.
Red	Microphones are muted. Device is in a call or in idle state.
Yellow	Power on LED diagnostic.
Amber/Red/Green/Off Repeating	Recovery in progress.

Polycom Trio Visual+ Status Indicators

Status	Description
Off	Device is not powered on
Flashing red	Device is booting up or pairing
Flashing green	Device update is in progress
Steady green	Device is powered on and paired with a Polycom Trio system.
Amber	Device is in a low power, standby state
Alternating orange/red/green/off flashes	Device is in recovery mode
Flashing red	The pairing button has been pressed
Alternating red and green flashes	Device is in pairing diagnostics mode

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.

Procedure

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.

You can also upload a log file 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.

Feature	Typical Memory Size	Description
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.	To reduce memory resources used by the main browser: • Display no more than three or four application elements. Simplify pages.

Feature	Typical Memory Size	Description
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	

System Logs

Topics:

System log files can assist when troubleshooting issues.

System log files contain information about system activities and the system configuration profile. After setting up system logging, you can retrieve a system log file.

The detailed technical data in the system log files can help Polycom Global Services resolve problems and provide technical support for your system. In such a situation, your support representative may ask you to download log archives and send them to Polycom Global Services.

You must contact Polycom Customer Support to obtain the template file `techsupport.cfg` containing parameters that configure log levels.

Configuring Log Files

You can configure log files using the logging parameters.

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` .

The phone writes information into several different log files. The following table describes the type of information in each.

When the Polycom Trio Visual+ accessory is paired with a Polycom Trio system, logging information from both devices is written to the same log files.

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.

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.

The Polycom Trio solution uploads a system log file [MAC address]-plcmsyslog.tar.gz that contains Android logs and diagnostics. This file can be ignored but does contain minimal data that may be useful to investigate Android issues.

There is no way to prevent the system log file [MAC address]-plcmsyslog.tar.gz from uploading to the server and you cannot control it using the parameters `log.render.file.upload.append.sizeLimit` and `log.render.file.upload.append.limitMode` . However, you can control the frequency of uploads using `log.render.file.upload.system.period` .

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.upload.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.upload.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.	

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.	
techsupport.cfg	log.render.file.upload.system.period	Specify the frequency in seconds the Polycom Trio system uploads the Android system log file MAC address]-plcmsyslog.tar.gz to the server. 86400 seconds (default) 0 - 2147483647 seconds	

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	

Logging Levels

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
- Schedule

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, in one of the following formats:
  - 0 - 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
- 1-5 character component identifier (such as “so”)
- Event class
- Cumulative log events missed due to excessive CPU load
- The event description

Logging Level, Change, and Render Parameters

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, 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.app	Initial logging level for the Apps log module. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.bfcp	Initial logging level for the BFCP content log module. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.fec	Sets the log level for video FEC. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.fecde	Sets high volume log level to decode video FEC. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.fecen	Sets high volume log level to encode video FEC. 4 (default) 0 - 6	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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.mrcam	Initial logging level for the Networked Devices Camera log module. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.mrcon	Initial logging level for the Networked Devices Connection 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.mrdis	Initial logging level for the Networked Devices Display 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.pec	Initial logging level for the Polycom Experience Cloud (PEC) log module. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.ppcip	Initial logging level for the People +Content IP log module. 4 (default) 0 - 6	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
techsupport.cfg	log.level.change.prox	Initial logging level for the Proximity log module. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.ptp	Initial logging level for the Precision Time Protocol log module. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.usba	Sets the logging detail level for the USB audio log. 4 (default) 0 - 6	No
techsupport.cfg	log.level.change.usbh	Sets the logging detail level for the USB HID log. 4 (default) 0 - 6	No
techsupport.cfg	log.render.file	Polycom recommends that you do not change this value. 1 (default) 0	No
techsupport.cfg	log.render.realtime	Polycom recommends that you do not change this value. 1 (default) 0	No
techsupport.cfg	log.render.stdout	Polycom recommends that you do not change this value. 0 (default) 1	No
techsupport.cfg	log.render.type	Refer to the Event Timestamp Formats table for timestamp type. 2 (default) 0 - 2	No

Logging Schedule Parameters

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.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

Upload Logs to the Provisioning Server

You can manually upload logs to the provisioning server.

When you manually upload log files, the word `now` is inserted into the name of the file, for example, `0004f200360b-now-boot.log` .

Procedure

1. Press the multiple key combination `1-5-9` on the phone.

Upload Polycom Trio System Logs

You can upload log files to your provisioning server.

Uploading log files copies the log files from the phone to the provisioning server. and creates new files named `<MACaddress>-now-xxx.log .`

Procedure

1. Go to **Settings** > **Advanced** and enter the administrator password (default `456`).
2. Go to **Administration Settings** > **Upload Configuration**.
3. Select one or more sources to upload from:
   - All Sources
   - Configuration Files
   - Local
   - MR
   - Web
   - SIP
4. Press **Upload**.

Troubleshooting

Topics:

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.

Error Message	Possible Solution
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.

Error Message	Possible Solution
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.
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**
- Polycom Trio 8800—**Settings** > **Status** > **Diagnostics** > **Warnings**.

The following table describes Polycom UC Software error messages.

Polycom UC Software Error Messages

Error Message	Cause
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	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.

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.
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	

Event Code	Description	Comments
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	

Power and Startup Issues

The following table describes possible solutions to power and startup issues.

Power or Startup Issue	Possible Solutions:
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.

Screen and System Access Issues

The following table describes possible solutions to screen and system access issues.

Issue	Possible solution
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.

Issue	Possible Solution
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 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.

Issue	Possible Solution
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.

Issue	Possible Solution
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.
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.

Software Upgrade Issues

The following table describes possible solutions to issues that may occur during or after a software upgrade.

Issue	Possible Solutions
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.

Issue	Possible Solutions
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.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.

Provisioning Issues

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.

Content

Topics:

Polycom offers several content sharing options.

Content Sharing

You can show content from a computer during in-person meetings, video conference calls, and point-to-point video calls on the Polycom Trio Visual+ system monitor.

To share content:

- The Polycom Trio Visual+ system must be paired with the Polycom Trio 8500 or 8800 system.
- The computer and Polycom Trio solution must be able to communicate on the same IP network.

You can use the following Polycom applications to share content:

- Polycom® People+Content® (PPCIP)
- Polycom® Desktop for Windows® or Mac®
- Polycom® Mobile application

You can download People+Content IP and Desktop from Polycom Support and Mobile from your mobile application store.

For information about using PPCIP on the Polycom Trio solution registered with Skype for Business, see the *Polycom Trio - User Guide* at Polycom Trio on Polycom Support.

Note: The default port used by Group Paging when enabled conflicts with the UDP port 5001 used by Polycom® People+Content™ on the Polycom 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` .
- Disable People+Content IP using parameter `content.ppcipServer.enabled="0"` .

Content Sharing Parameters

Use the parameters in the following table to configure content sharing options.

To enable device pairing with the Polycom Trio solution, use the `smartpairing*` parameters. Note that People+Content IP does not support ultrasonic SmartPairing.

Content Sharing Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	content.autoAccept.rdp	1 (default) - Content shown by far-end users is automatically accepted and displayed on the Polycom Trio solution. 0 - Near-end users are prompted to accept meeting content sent to Polycom Trio solution from a far-end user.	No
	content.bfcp.enabled	1 (default) - Enable content sharing by offering or accepting the Binary Floor Control Protocol (BFCP) in Session Description Protocol (SDP) negotiation during SIP calls. Does not apply to Skype for Business calls. 0 - Disable content sharing using BFCP.	No
	content.bfcp.port	15000 (default) - 0 - 65535 -	No
	content.bfcp.transport	UDP (default) - TCP -	No
	content.ppcipServer.enabled	1 (default) - Enable Polycom People +Content IP. 0 - Disable Polycom People+Content IP.	No
	content.ppcipServer.meetingPassword	NULL (default) - String (0 - 256 characters) -	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	`smartPairing.mode`	Enables users with People+Content IP or Desktop on a computer or Mobile on a tablet to pair with the Polycom Trio conference phone using SmartPairing. Disabled (default) - Users cannot use SmartPairing to pair with the conference phone. Manual - Users must enter the IP address of the conference phone to pair with it.	No
	`smartPairing.volume`	The relative volume to use for the SmartPairing ultrasonic beacon. 6 (default) 0 - 10	No

Polycom People+Content IP over USB

You can use Polycom® People+Content® IP (PPCIP) to share video or data from a Windows® or Mac® computer connected by USB to the Polycom Trio 8800 system when in or out of a call.

When you install PPCIP version 1.4.2 and run it unopened in the background, the PPCIP application pops up immediately when you connect the computer to Polycom Trio solution via USB.

Keep the following points in mind:

- Showing content with People+Content IP over USB provides content to a maximum of 1080p resolution on a connected Windows or Mac computer.
- Audio content is not shared.
- Content sent from People+Content is sent over USB, and no network connection is needed. This is useful for environments where guest IP access is not allowed. You can show content with People +Content IP on a computer connected by USB to Polycom Trio to a maximum of 1080p resolution on a Windows computer. You must use UC Software 5.4.3AA or later to share your desktop at up to 1080p resolution using a Mac computer connected by USB to the Polycom Trio solution.

Important: The default port used by Group Paging when enabled `ptt.pageMode.enable="1"` conflicts with the UDP port 5001 used by Polycom® People+Content™ on the Polycom Trio system. Since the port used by People+Content is fixed and cannot be configured, configure one of two workarounds:

- Configure a different port for Group Paging using parameter `ptt.port` or
- Disable People+Content IP using parameter `content.ppcipServer.enabled="0"` .

Polycom People+Content IP over USB Parameters

The following table lists parameters that configure the People+Content over USB feature.

Polycom People+Content over USB Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	`feature.usb.device.content`	1 (default) - Enable content sharing using the People+Content IP application on a computer connected by USB to Polycom Trio solution. 0 - Disable content sharing using the People+Content IP application on a computer connected by USB to Polycom Trio solution.	No

Polycom People+Content IP

You can share content from a computer over IP using Polycom® Desktop Software, Polycom® People +Content IP (PPCIP), and Polycom® ® Mobile Software.

Sharing content with Polycom People+Content IP from a computer connected over IP supports 1080p resolution with about five frames per second on the Visual+ monitor. The computer and Polycom Trio solution must be able to communicate on the same IP network and you must pair your Polycom software application with the Polycom Trio system.

When Polycom Trio is registered with Skype for Business, you can use these applications to share content only to a local monitor. You cannot share content from a Polycom Trio system over a Skype for Business call. For instructions, see the *Polycom Trio - User Guide* at Polycom Trio on Polycom Support.

Polycom People+Content IP Parameters

The following table lists parameters that configure content sharing with the Polycom Trio solution.

Content Sharing with Polycom Trio Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	content.autoAccept.rdp	(default) - Skype for Business RDP content shown by far-end users is automatically accepted and displayed. 0 - Near-end users are prompted to accept meeting content.	
`features.cfg`	`content.bfcp.port`	15000 (default) 0 - 65535	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	content.bfcp.enabled	1 (default) - Enable Binary Floor Control Protocol content to be shared during calls. 0 - Disable Binary Floor Control Protocol content.	
reg.cfg	reg.x.content.bfcp.enabled	1 (default) - Enable Binary Floor Control Protocol content to be shared during calls for the line you specify. 0 - Disable Binary Floor Control Protocol content.	
features.cfg	content.bfcp.transport	UDP (default TCP	No
features.cfg	content.ppcipServer.enabled	1 (default) - Enable Polycom People+Content IP content server for sharing. 0 - Disable Polycom People +Content IP content server.	No
features.cfg	content.ppcipServer.enabled.Trio8500	1 (default) - Enable Polycom People+Content IP content server for content sharing with Polycom Trio 8500. 0 - Disable Polycom People +Content IP content server for Polycom Trio 8500.	No
site.cfg	mr.content.rdp.tls.enabled	1 (default) - Enable TLS encryption of Skype for Business RDP content between hubs and devices. Disable TLS encryption of Skype for Business RDP content.	No
features.cfg	content.ppcipServer.enabled.Trio8800	1 (default) - Enable Polycom People+Content IP content server for content sharing with Polycom Trio 8800. 0 - Disable Polycom People +Content IP content server for Polycom Trio 8800.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	content.ppcipServer.meetingPassword	NULL (default) String (0 - 256 characters)	No

Video-based Screen Sharing Support for Polycom Trio Solution

Polycom Trio 8800 and 8500 allows you to use Video-based Screen Sharing (VbSS) with Skype for Business clients that enables both application and desktop sharing. In previous releases, Trio systems supported only Remote Desktop Protocol (RDP) for receiving content. Only systems registered to Skype for Business support VbSS content sharing.

Note: The Polycom Trio solution can only receive Skype for Business VbSS content. You cannot transmit VbSS content from the Polycom Trio solution.

The advantages of VbSS content sharing over RDP are as follows:

- The video experience is faster, with an improvement in frames-per-second.
- Works better in low bandwidth conditions, even when receiving high motion content, such as 3-D graphics.

However, if any participant in a Skype for Business conference does not support VbSS, the Skype for Business server content switches from VbSS to Remote Desktop Protocol (RDP) content.

Video-based Screen Sharing Parameter

The following table lists parameter that configures Video-based Screen Sharing with the Polycom Trio solution.

Video-based Screen Sharing Parameter

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	content.vbss.enable	1 (default) – Enables Polycom 8800 and 8500 systems to use Video-based Screen Sharing (VbSS) for receiving Skype for Business content. 0 – Polycom 8800 and 8500 systems use Remote Desktop Protocol (RDP) for receiving Skype for Business content.	No

Screen Mirroring

The Polycom Trio 8800 system provides screen mirroring locally from Apple® -certified devices and the Wireless Display feature for Miracast®-certified Android™ and Windows® devices.

Screen Mirroring with AirPlay-Certified Devices

This section provides information you need to set up and configure a Polycom Trio 8800 system to work with AirPlay-certified devices.

The following information applies to using AirPlay-certified devices with the Polycom Trio system:

- You can display local content only from your AirPlay-certified device to the Polycom Trio 8800 system monitor.
- Sharing content from direct streaming sources, such as YouTube™ or web links, is not supported.
- If you share content during a point-to-point or conference call, the content is not sent to far-end participants.
- Audio-only content is not supported. If you only want to share audio, consider using Bluetooth or USB connectivity.
- Apple Lossless Audio Codec (ALAC) is not supported.

Polycom Trio 8800 systems support the following AirPlay-certified devices:

- Apple ®
- iPad®
- iPad Pro™
- MacBook Pro®

The Polycom Trio 8800 system supports a maximum resolution and frame rate of 720p@60fps or 1080p@30fps. If configured for 1080p resolution, an iPad often sends 60fps video, which can result in latency in mirroring, visual artifacts, or both.

When the Polycom Trio 8800 system receives content from a Skype for Business client using the Remote Desktop Protocol (RDP) at the same time as content from an AirPlay-certified device, the AirPlay content takes precedence and displays. When you end AirPlay content, available Skype for Business content displays.

Requirements for Screen Mirroring with AirPlay

You must meet the following requirements to use the screen mirroring feature on an AirPlay-certified device with a Polycom Trio 8800 system:

- Polycom Trio collaboration kit running UC Software version 5.4.4AA or later
- The Polycom Trio system and Apple devices are on the same subnet.

  The devices can be on different subnets if the devices are routable and multicast DNS (Bonjour) is bridged between the subnets for discovery. The devices can also be on different subnets if AirPlay Discovery over Bluetooth is enabled, the subnets are routable to each other, and the device is within Bluetooth range.
- The screen mirroring feature uses the following ports:
  - Discovery: UDP port 5353
  - Sessions: TCP ports 7000, 7100, 8009, and 47000; UDP port 1900

Polycom Trio 8800 for AirPlay Parameters

Use the following parameters to configure the Polycom Trio 8800 system for AirPlay-certified devices.

Polycom Trio 8800 for AirPlay Parameters

Template	Parameter	Permitted Values	Restart Causes Restart or Reboot
features.cfg	content.airplayServer.authType	none (default) - No security code for AirPlay certified devices is required. passcode - Use a security code to authenticate AirPlay-certified devices.	No
features.cfg	content.airplayServer.discovery.bluetooth.enabled	Set to allow AirPlay discovery over Bluetooth. 1 (default) - Enables Polycom Trio 8800 to be discoverable to AirPlay-certified devices over Bluetooth. Turns Bluetooth radio on when feature.bluetooth.enabled = 1. 0 - Polycom Trio 8800 is not discoverable to AirPlay-certified devices over Bluetooth **Note:** Enable the parameter feature.bluetooth.enabled to use this feature.	No
features.cfg	content.airplayServer.enabled	0 (default) - Disable the content sink for AirPlay-certified devices. 1 - Enable the content sink for AirPlay-certified devices.	No
features.cfg	content.airplayServer.maxResolution	Set the content resolution. 720p (default) 1080p 1024x1024 960x960 480x480	No

Template	Parameter	Permitted Values	Restart Causes Restart or Reboot
features.cfg	content.airplayServer.name	Specify a system name for the local content sink for AirPlay certified devices. If left blank the previously configured or default system name is used. NULL (default)	No
features.cfg	content.local.authChangeInterval	Set the interval in minutes between changes to the local content authentication credentials. 1440 (default) 0 - 65535 0 - Do not change	No
features.cfg	content.local.authChangeMode	Specify when the security code for content sharing with AirPlay-certified devices changes. session (default) - Code changes at the end of each content sharing session. relativeTime - Code changes at an interval specified by the content.local.authChangeInterval parameter.	No

Troubleshooting

This section provides solutions to common issues you may have using the Polycom Trio 8800 system with AirPlay-certified devices.

The Polycom Trio 8800 system does not advertise on my device

The Polycom Trio may not be broadcasting for discovery, or the broadcasts are being blocked.

- Ensure your Apple device is on the same subnet as the Polycom Trio 8800 system and that Polycom Trio has screen mirroring enabled.

AirPlay Debugging Log Parameters

If you experience further issues using AirPlay-certified devices with the Polycom Trio 8800 system, you can enable the following logging parameters on your Polycom Trio to get extended debugging data.

Screen Mirroring Debugging Parameters

Log Component	Permitted Values
airp	Session management and communication specifically for AirPlay certified devices.

Log Component	Permitted Values
airpl	Protocol library for AirPlay-certified devices
airps	Android service AirPlay-certified devices
lc	Local Content (including for AirPlay-certified devices and PPCIP) session management

Screen Mirroring with Miracast-Certified Devices

The Wireless Display feature lets you display content locally from your Miracast-certified Android or Windows device to the Polycom Trio 8800 system monitor.

Windows or Android devices can discover and connect directly with the Polycom Trio 8800 system and do not have to be on the same network.

The Polycom Trio 8800 system supports content sharing from the following Android and Windows devices:

- Miracast-certified devices running Windows 10
- Samsung Galaxy smartphones and tablets running Android version 4.4 or earlier

Note: Polycom cannot guarantee connectivity with all Miracast-certified devices, but connectivity has been validated to work well with Samsung smartphones and tablets using Android version 4.4 or later and the Microsoft Surface® 3 Pro and Surface® 4 Pro running Windows 10.

To send content from your device, you must first connect your device wirelessly to the Polycom Trio 8800 system.

The Polycom Trio 8800 system can display content to a maximum resolution and frame rate of 720p@60fps or 1080p@30fps. If the Polycom Trio 8800 system is configured to auto-negotiate the frame rate of transmitted content, some tablets might send 1080p@60fps video, which can result in latency in mirroring, visual artifacts, or both.

Requirements

You must meet the following requirements to use the Wireless Display feature on a Miracast-certified device with the Polycom Trio 8800 system:

- Polycom Trio 8800 collaboration kit running UC Software version 5.4.4AA or later

If you do not allow auto-negotiation, some devices might fail to pick the best possible video stream parameters.

Polycom Trio 8800 for Miracast-Certified Devices Parameters

Use the following parameters to configure Wireless Display on the Polycom Trio 8800 system.

Wireless Display Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot

features.cfg	content.wirelessDisplay.sink.authorizationType	Auto (Default) - Content is automatically accepted and displays on the Polycom Trio 8800 system. Button - Users must confirm content acceptance on a popup message.	No
features.cfg	content.wirelessDisplay.sink.bitrate	Set the content maximum bitrate in Mbps 30 (default) 0 - 60 0 allows auto-negotiation.	No
features.cfg	content.wirelessDisplay.sink.enabled	0 (default) - Disable Wireless Display. 1 - Enable Wireless Display.	No
features.cfg	content.wirelessDisplay.sink.fps	Set the content frame rate in frames per second. 30 (default) 0 - 60 0 allows auto-negotiation	No
features.cfg	content.wirelessDisplay.sink.height	Set the maximum content height in pixels. 1080 (default) 0 - 1200 0 allows auto-negotiation	No
features.cfg	content.wirelessDisplay.sink.name	NULL - default Specify a system name for the local content sink for Android or Windows devices. If left blank the previously configured or default system name is used.	No
features.cfg	content.wirelessDisplay.sink.width	Set the maximum content width in pixels. 1920 (Default and Maximum) 0 allows auto-negotiation	No

Troubleshooting

This section provides solutions to common issues you may have using Wireless Display on the Polycom Trio 8800 system.

My Polycom Trio 8800 system does not advertise on my smartphone or tablet

If the Polycom Trio 8800 system does not advertise on your smartphone or tablet device, check the following:

- Ensure Wi-Fi is enabled on your device and the band is set to 2.4GHz or Auto. The Auto setting allows the connecting device better access to a free wireless channel.
- Ensure the correct country of operation is set and that both bands are selected on the Polycom Trio 8800 system by configuring the following:
  `device.wifi.country.set="1"device.wifi.country="CA"device.wifi.radio.band2_4GHz.enable.set="1"`
  `device.wifi.radio.band2_4GHz.enable="1"device.wifi.radio.band5GHz.enable.set="1"device.wifi.radio.band5GHz.enable="1"device.wifi.enabled.set="1"device.wifi.enabled="0"device.net.enabled.set="1"device.net.enabled="1"`

Note: The WLAN operating mode on the Polycom Trio 8800 system is mutually exclusive of the Wireless Display feature. You can enable Wireless Display only if wired Ethernet is used for calling and conferencing. Ensure that wired Ethernet is used for calling and conferencing by configuring the following:

Video Quality is Poor

Incorrect image resolution can cause content delays and video artifacts.

Note that the Polycom Trio 8800 system does not accept 1080@60fps video resolution.

- To resolve video quality issues, configure the following for the Polycom Trio 8800 system:
  `content.wirelessDisplay.sink.width="0"content.wirelessDisplay.sink.height="0"content.wirelessDisplay.sink.fps="0"`
- In addition, you can set a limit on the live stream parameters by setting:
  `content.wirelessDisplay.sink.fps="30"`

Wireless Display Debugging Log Parameters

If you experience further issues using Wireless Display on the Polycom Trio 8800 system, you can enable the following logging parameters on your Polycom Trio 8800 system to get extended debugging data.

Wireless Display Debugging Parameters

Parameters	Permitted Values
wdisp	Wireless Display session management and communication with the Wireless Display source
apps	Wireless Display support for Android
lc	Local Content (including Wireless Display and PPCIP) session management

Access Diagnostic Information

If you experience issues using Wireless Display on the Polycom Trio 8800 system, you can access diagnostic information from the Polycom Trio 8800 menu.

On the phone menu, go to one of the following settings:

- **Settings** > **Status** > **Diagnostics** > **Local Content Media Statistics**
- **Settings** > **Status** > **Diagnostics** > **Graphs** > **Local Video Content Statistics**
- **Settings** > **Status** > **Diagnostics** > **Graphs** > **Networked Devices Graphs**
- **Settings** > **Status** > **Diagnostics** > **Networked Devices** > **Statistics**

Hardware and Accessories

Topics:

This section provides information on powering and pairing the Polycom Trio system and Polycom Trio Visual+ acccessory, as well as information on power management.

Powering the Polycom Trio 8500 and 8800 Systems

Powering requirements and options vary between the Polycom Trio 8800 and 8500 systems.

Read the powering requirements and options carefully to understand powering for your Polycom Trio system.

Powering the Polycom Trio 8800

You can power the Polycom Trio 8800 system with Power over Ethernet (PoE) or PoE+ (IEEE 802.

3at Type 2). When the Polycom Trio 8800 system is booting up, an on-screen message indicates the available power supply type. Note that PoE+ provides Polycom Trio systems with full functionality.

The following features are not available on Polycom Trio 8800 system when using PoE:

- The Polycom Trio 8800 system LAN OUT port out does not provide PoE+ power and cannot be used to power the Polycom Trio Visual+.
- No USB charging is provided to devices (mobile phones, tablets) connected to the Polycom Trio 8800 system USB port.
- Maximum peak power to the loudspeaker is limited.

Powering the Polycom Trio 8500

You can power the Polycom Trio 8500 system with Power over Ethernet (PoE).

When the Polycom Trio 8500 system is booting up, an on-screen message indicates the available power supply type.

The Polycom Trio 8500 does not support:

- PoE+
- Power Sourcing Equipment (PSE)
- LAN Out / PC Port
- USB

The following features are not available on Polycom Trio 8500 system using PoE:

- No USB charging is provided to devices (mobile phones, tablets) connected to the Polycom Trio 8500 system USB port.
- Maximum peak power to the loudspeaker is limited.

Power the Polycom Trio 8800 System with the Optional Power Injector

If your building is not equipped with PoE+ you can use the optional power injector to provide PoE+ and full functionality to Polycom Trio 8800 system.

Note: Place the PoE injector in a clean and dry area out of a walkway, and provide sufficient space around the unit for good ventilation. Do not cover or block airflow to the PoE injector. Keep the PoE injector away from heat and humidity and free from vibration and dust.

When using the power injector to power the Polycom Trio 8800 system, you must connect cables in the following sequence:

Procedure

1. Plug the AC power cord of the power injector into the wall and use a network cable to connect the power injector to the Polycom Trio 8800 system.
2. Connect the power injector to the network with a CAT-5E or CAT-6 Ethernet cable.

The power adapter LED is green when the Polycom Trio 8800 system is correctly powered. If the LED is yellow, the power injector is bypassed and the Polycom Trio 8800 system is drawing PoE power from the outlet.

Tip: If the Polycom Trio Visual+ loses power after a Polycom Trio 8800 system reboot, unplug both devices and repeat steps 1 and 2.

If the power injector LED is yellow, turn off the PoE network port or connect the Polycom Trio system in the following sequence:

1. Power up Polycom Trio 8800 and Visual+ using the power injector but do not plug the devices into the network wall port.
2. Wait for the Polycom Trio 8800 and Visual+ systems to boot up.
3. Plug the devices into the network wall port.
4. Ensure the LED indicator on the power injector is green.

Powering the Polycom Trio Visual+ Solution

How you power the Polycom Trio Visual+ can depend on the power options your building is equipped with.

Consider the following setup points:

- If you are using PoE+ or the optional power injector, you can power the Polycom Trio Visual+ directly from the Polycom Trio system using an Ethernet cable. In this scenario, you do not need to pair the Polycom Trio system with the Polycom Trio Visual+.
- If you are using PoE, you must power the Polycom Trio Visual+ separately using an Ethernet cable or use the optional power injector. In this scenario, you must pair the Polycom Trio system with the Polycom Trio Visual+.

- If you use PoE+, you have the option to power the Polycom Trio system and Polycom Trio Visual+ separately and then pair. When powering separately, you do not need to connect the Polycom Trio system directly to Polycom Trio Visual+.

Pairing the Polycom Trio Visual+ with Polycom Trio Systems

Pair the Polycom Trio Visual+ with a Polycom Trio 8500 or Polycom Trio 8800 system to enable users to place video calls and share content.

You can pair only one Polycom Trio Visual+ to a Polycom Trio 8500 or 8800 system. Polycom recommends you plug both devices into a local gigabit switch.

You can pair the Polycom Trio Visual+ to the system using configuration files or from the Polycom Trio menu system. To pair, the Polycom Trio system and Polycom Trio Visual+ must be connected to the same subnet, and you must unblock the following network components:

- Multicast address 224.0.0.200
- Port 2000

Note: You cannot use Polycom Trio Visual+ for video calls when you connect the Polycom Trio system to your network using Wi-Fi. The Polycom Trio system and Polycom Trio Visual+ only pair when the Polycom Trio system is connected to your network over Ethernet.

Pair the Polycom Trio Solution Manually

You can manually pair the Polycom Trio Visual+ to the system from the local phone interface on Polycom Trio 8500 or 8800.

Procedure

1. Set up Polycom Trio Visual+.

   For instructions, refer to the Polycom Trio Visual+ Setup Sheet.

   The Welcome screen displays on your monitor and indicates steps to pair with a Polycom Trio system.

2. Tap the **Pair** button on Polycom Trio Visual+ to broadcast discovery to the Polycom Trio.
3. On the Polycom Trio system, go to **Settings** > **Advanced** > **Networked Devices**, and ensure that **Notification of New Devices** is **On**.
4. Choose one of the following:
   - If you have not paired the device before, tap **Pair with New Device**, tap the device you want to pair from the Discovered Devices list, and in the Details screen, tap **Pair**. All currently paired devices display under Paired Devices.
   - If the device has been paired before, select the device from the **Available Devices** list and tap **Pair**.
5. When you see the message prompting you to complete pairing, do one of the following:
   - Tap **Complete**.
   - Tap the **Pair** button on the Polycom Trio Visual+.

If pairing was successful, a success message displays on the monitor along with a self-view window, the LED light on the Polycom Trio Visual+ device is continuously green, and a paired icon displays on the phone. If pairing was unsuccessful, a message displays on the monitor that the devices could not pair. After successful pairing, if devices become disconnected for 60 seconds, a message displays that the devices have temporarily lost connection.

Polycom Trio Solution Pairing Parameters

To pair using configuration files, enter the MAC address of your Polycom Trio Visual+ device as the value for the parameter `mr.pair.uid.1 .`

The MAC address can be in either of the following formats:

- `00e0d::B09128D`
- `00E0DB09128D .`

Use the following parameters to configure this feature and additional feature options.

Pairing Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`mr.bg.showPlcmLogo`	1 (default) - The Polycom logo shows on the TV attached to the paired Polycom Trio Visual+. 0 - Hides the Polycom logo on the Polycom Trio Visual+.	No
`features.cfg`	`mr.bg.url`	Specifies the HTTP URL location of a background image to use on the TV attached to the paired Polycom Trio Visual+. The system supports PNG and JPEG images up to 2.9 MB. This background image will be used only if `mr.bg.selection= "5"` Null (default) String (maximum 256 characters)	No
	`mr.PairButton.notification`	1 (default) - The Polycom Trio system displays notifications of devices available to pair with after you press the Pair button on the Polycom Trio Visual+. 0 - The Polycom Trio system does not display pairing notifications.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	mr.audio.srtp.require	If set to 1, SRTP is used to encrypt and authenticate modular room audio signals sent between Polycom Trio 8500 or 8800 and Polycom Trio Visual+. 1 (default) 0	
features.cfg	mr.bg.selection	Sets the background image for the paired Polycom Trio Visual+ display. HallstatterSeeLake (default) Auto - Automatically cycles through background images 2, 3, 4. The background image changes each time a video call ends. BlueGradient BavarianAlps ForgetMeNotPond Custom - Use a custom background specified by mr.bg.url.	
site.cfg	mr.pair.tls.enabled	1 (default) - Enable TLS to encrypt communication between the Polycom Trio system and Polycom Trio Visual+ systems. 0 - Disable TLS for communication between Polycom Trio systems and Polycom Trio Visual+ systems.	Yes
site.cfg	mr.pair.uid.1	Enter the MAC address of the Polycom Trio Visual+ you want to pair with. Null (default) String (maximum of 64 characters)	No
site.cfg	mr.video.camera.focus.auto	0 (default) - Disable the camera's automatic focus. 1 - Enable the camera's automatic focus.	Yes
site.cfg	mr.video.camera.focus.range	Specify the distance to the camera's optimally-focused target. 0 (default) 0 - 255	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	mr.video.iFrame.minPeriod	Choose the minimum time in seconds between transmitted video i-Frames or transmitted i-Frame requests. 2 (default) 1 - 60	No
features.cfg	smartPairing.mode	Enables users with RealPresence Desktop on a laptop or RealPresence Mobile on a tablet to pair with the Polycom Trio system using SmartPairing. disabled (default) manual	
features.cfg	smartPairing.volume	The relative volume to use for the SmartPairing ultrasonic beacon. 6 (default) 0 - 10	

Identify Paired Devices

If you are using multiple Polycom Trio 8500 and 8800 systems and are not sure which Polycom Trio Visual+ is paired with which system, you can identify which accessories are paired with the system on the Polycom Trio.

Procedure

1. On the phone, go to **Settings** > **Advanced** > **Networked Devices**, and ensure that **Notification of New Devices** is **On**.
2. Select a device that displays under Paired Devices or Available Devices.
3. Tap **Identify**.

   The LED of the device you selected flashes to indicate it is paired to the system.

Place the Polycom Trio Visual+ in Pairing Diagnostic Mode

If you are using multiple Polycom Trio 8500 and 8800 systems and are not sure which Polycom Trio Visual+ is paired with which, you can place the Polycom Trio Visual+ devices in pairing diagnostic mode to distinguish between accessories.

Procedure

1. Power up the Polycom Trio Visual+ device.
2. Wait for the initial LED on state to turn off.

3. Press and hold the pairing button until the LED turns orange.
4. Release the pairing button.
   The LED blinks.
5. Wait for the device to reboot.
   The paired device's LED glows steady green.

Polycom Trio System Power Management

Power available to the Polycom Trio 8800 and 8500 system is limited and you must choose how to power the system and which features to enable or disable.

Power management options vary between the Polycom Trio 8800 and 8500. Read the powering requirements and options carefully to understand powering for your Polycom Trio system.

Polycom Trio 8500 System Power Management

The Polycom Trio 8500 supports:

- USB devices consuming < 2.5W power
- USB port over current detection

The Polycom Trio 8500 does not support:

- PoE+
- Power Sourcing Equipment (PSE)
- LAN Out / PC Port
- USB charging

USB Port Power Management

Device charging with the USB port on the Polycom Trio 8800 system is disabled by default and when disabled the USB host port provides 100mA of power for peripheral devices.

USB charging is disabled when powering the Polycom Trio Visual+ from a LAN Out port.

To enable USB charging, you must power your Polycom Trio 8800 system with an IEEE 802.3at Power over Ethernet Plus (PoE+) compliant power source. When USB charging is enabled, you can power and charge USB 2.0 compliant devices having a power draw of up to 1.500mA/7.5W.

Using Power over Ethernet (POE) Class 0

Powering the Polycom Trio 8800 system from a Power over Ethernet (POE) Class 0 source provides full core functionality and results in the following limitations:

- The LAN Out port does not provide PoE power but otherwise is fully functional.

Using Power Sourcing Equipment Power (PoE PSE Power)

You can use Power Sourcing Equipment Power (PoE PSE Power) to power a Polycom Trio Visual+ system from the LAN OUT port of the Polycom Trio 8800 system.

To use PoE PSE Power, you must power the Polycom Trio 8800 system with an IEEE 802.3at Power over Ethernet Plus (PoE+) compliant power source.

Note: You cannot enable USB Charging of the USB host port and PSE PoE Power of LAN OUT port at the same time. If both are enabled, the Polycom Trio 8800 system uses PSE PoE Power and ignores the USB charging setting.

Polycom Trio System Power Management Parameters

You can use the parameters listed to manage the Polycom Trio 8800 system's power usage.

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	poe.pse.class	Specify the LAN OUT PoE class. 0 (default) 0 - 3	No
site.cfg	poe.pse.enabled	1 (default) - The Polycom Trio 8800 LAN OUT interface provides PoE power to a connected device. 0 - PoE power is not provided by the LAN OUT port.	No
site.cfg	usb.charging.enabled	0 (default) - You cannot charge USB-connected devices from the USB charging port. 1 - Enable fast charging of devices connected by USB port up to 7.5W power / 1.5A current.	No

Power-Saving on Polycom Trio

The power-saving feature automatically turns off the phone's LCD display when not in use.

You can configure power-saving options for the Polycom Trio 8800 and 8500 systems including:

- Turn on power-saving during nonworking days and hours.
- Configure power-saving around working days and hours.
- Configure an idle inactivity time after which the phone enters power-saving mode.

When the phone is in power-saving mode, an LED light flashes at intervals to indicate power is on.

In an unused conference room where the phone is in idle mode and the display is off, the Polycom Trio solution has the capability to wake up when a user enters the room, depending on the room lighting.

Note: By default the Polycom Trio 8800 and 8500 systems enter power-saving mode after a period of idle time to conserve energy. However, Polycom Trio systems do not enter power-saving mode while idle in the Bluetooth menu. To ensure the system enters power-saving mode, you must exit the Bluetooth menu using the **Home** or **Back** key on the Bluetooth menu.

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.cecEnable`	0 (default) - The Polycom Trio Visual+ display behavior is controlled only by the value set for `powerSaving.tvStandbyMode` . 1 - When the Polycom Trio system enters power-saving mode, the Polycom Trio Visual+ display switches to standby mode and powers up when the system exits power-saving mode.	No
`site.cfg`	`powerSaving.enable`	Enable or disable the power-saving feature. The default value varies by phone model. VVX 300/301/310/311=0 (default) VVX 400/401/410/411=0 (default) VVX 500/501, 600/601, 1500=1 (default) Polycom Trio=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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
site.cfg	powerSaving.tvStandbyMode	black (default) - The Polycom Trio Visual+ displays a black screen after entering power-saving mode. noSignal - Power-saving mode turns off the HDMI signal going to the Polycom Trio Visual+ monitor.	No

Audio Features

Topics:

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.

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
site.cfg	voice.vadEnable	0 - Disable Voice activity detection (VAD). 1 - Enable VAD.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

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.

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

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.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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.rfc2833Payload_OPUS	Sets the DTMF payload required to use Opus codec. 126 (default) 96 - 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

Acoustic Echo Cancellation

Polycom phones use advanced acoustic echo cancellation (AEC) for handsfree operation using the speakerphone.

The phones significantly reduce echo while permitting natural communication.

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.

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.enable	1 (default)—Enables the AEC function for handsfree options. 0—Disables the AEC function for handsfree options. Polycom does not recommend disabling this parameter.	No
site.cfg	voice.aec.hs.enable	0—Disables the AEC function for the handset. 1 (default)—Enables the AEC function for the handset.	No

Polycom NoiseBlock

Polycom NoiseBlock technology automatically mutes the microphone during audio-only and audio/video calls when a user stops speaking.

This feature silences noises that interrupt conversations such as paper shuffling, food wrappers, and keyboard typing. When a user speaks, the microphone is automatically unmuted.

Polycom NoiseBlock Parameters

The following table includes the parameter you can use to configure the Polycom NoiseBlock feature.

Polycom NoiseBlock Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	voice.ns.hf.blocker	1 (default) - Enable Polycom NoiseBlock. 0 - Disable Polycom NoiseBlock.	No

Audio Output and Routing Options

By default, audio plays out of the Polycom Trio speakers.

When you add video capability by connecting and pairing the system with the Polycom Trio Visual+ audio/video accessory, you can choose to route audio to play out of external speakers and/or the TV/monitor speakers connected to Polycom Trio Visual+.

Using the parameter `up.audio.networkedDevicePlayout` , you can configure the following audio routing options:

- Polycom Trio 8500 / 8800 speaker only
- Polycom Trio™ Expansion Microphones

  The expansion microphones include a 2.1 m | 7 ft cable that you can attach directly to the Polycom Trio to broaden its audio range to a total of 70 ft.
- Polycom Trio Visual+ using HDMI or a connected 3.5mm analog output
- Any combination of outputs available with Polycom Trio 8500, 8800, and Polycom Trio Visual+

Audio Output and Routing Option Parameters

The following table includes the parameters you can use to set the audio output and routing options for the Polycom Trio solution.

Audio Output Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.audio.networkedDevicePlayout	PhoneOnly (default) - Audio plays out on the Polycom Trio system speakers. TvOnly - Audio plays out on the TV/monitor speakers connected by HDMI to a paired Polycom Trio Visual+ and, if connected, external speakers connected to the 3.5mm port of a paired Polycom Trio Visual+. Auto - Audio-only calls play out on the Polycom Trio system speakers. Video-call audio plays out on the TV/monitor speakers connected by HDMI to a paired Polycom Trio Visual+ and, if connected, external speakers connected to the 3.5mm port of a paired Polycom Trio Visual+.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	`feature.usb.device.hostOs`	Specify the operating system of the computer you are connecting by USB when using Polycom Trio as an audio output device. Windows (default) - The computer connected by USB to the Polycom Trio uses a Windows operating system. Other—The operating system of the computer connected via USB to the Polycom Trio system is other than Windows or Mac. Mac—The computer connected by USB to the Polycom Trio uses a Mac operating system. Confirm—The user is prompted to confirm the computer's operating system each time a USB cable is used to connect to the Polycom Trio system.	No

USB Audio Calls

You can enable users to use the Polycom Trio 8800 and 8500 system as an audio device for a tablet or laptop connected to the Polycom Trio 8800 with the USB cable supplied in the box.

When a Microsoft® Windows® computer is connected to the Polycom Trio solution using a USB cable, users can control the volume of audio and video calls from the computer or the Polycom Trio solution, and the volume is synchronized on both devices.

The Polycom Trio 8800 and 8500 systems supports Mac computers running the following software versions when connected by USB and used as an audio speakerphone:

- OS X 10.9.x (Mavericks)
- OS X 10.10.x (Yosemite)
- OS X 10.11.x (El Capitan)

USB Audio Call Parameters

The following table includes the parameters you can use to configure USB audio calls for connected devices.

USB Call Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg	device.baseProfile	NULL (default) Generic - Disables the Skype for Business graphic interface. Lync - Use this Base Profile for Skype for Business deployments. SkypeUSB - Use this Base Profile when you want to connect Polycom Trio to a Microsoft Room System or a Microsoft Surface Hub.	No
feature.cfg	voice.usb.holdResume.enable	0 (default) - The Hold and Resume buttons do not display during USB calls. 1 - The Hold and Resume buttons display during USB calls. This parameter applies only when Polycom Trio Base Profile is set to 'SkypeUSB'.	No

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.

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.appLocalEnabled	1 (default)—Enable audio alerts and sound effects. 0—Disable audio alerts and sound effects	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	se.destination	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.stutterOnVoiceMail	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

Ringtones

Ringtones are used to define a simple ring class that is applied based on credentials 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
- visual
- answerMute
- autoAnswer
- ringAnswerMute
- ringAutoAnswer
- internal

- external
- emergency
- precedence
- splash
- custom<y> where y is 1 to 17.

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.cfg	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

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`)
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

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 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	Example
sampled (n)	Play sampled audio file n	`se.pat.misc.SAMPLED_1.inst.1.type =”sampled”` (sampled audio file instruction type) `se.pat.misc.SAMPLED_1.inst.1.value =”2”` (specifies sampled audio file 2)

Instruction	Meaning	Example
chord (n, d)	Play chord set n (d is optional and allows the chord set ON duration to be overridden to d milliseconds)	`se.pat.callProg.busyTone.inst.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)	`se.pat.callProg.bargeIn.inst.3.type = "silence"` (silence instruction type) `se.pat.callProg.bargeIn.inst.3.value = "300"` (specifies silence is to last 300 milliseconds)
branch (n)	Advance n instructions and execute that instruction (n must be negative and must not branch beyond the first instruction)	`se.pat.callProg.alerting.inst.4.type = "branch"` (branch instruction type) `se.pat.callProg.alerting.inst.4.value = "-2"` (step back 2 instructions and execute that instruction)

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
region.cfg	se.pat.callProg.secondaryDialTone.inst.1.type	0-255	No
region.cfg	se.pat.callProg.secondaryDialTone.inst.1.value	0-50	No
region.cfg	se.pat.callProg.secondaryDialTone.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

Call Progress Tones

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

Call Progress Tone Pattern Names

Call Progress Pattern	Description
alerting	Alerting
bargeIn	Barge-in tone
busyTone	Busy tone
callWaiting	Call waiting tone

Call Progress Pattern	Description
callWaitingLong	Call waiting tone long (distinctive)
confirmation	Confirmation tone
dialTone	Dial tone
howler	Howler tone (off-hook warning)
intercom	Intercom announcement tone
msgWaiting	Message waiting tone
precedenceCallWaiting	Precedence call waiting tone
precedenceRingback	Precedence ringback tone
preemption	Preemption tone
precedence	Precedence tone
recWarning	Record warning
reorder	Reorder tone
ringback	Ringback tone
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 for Polycom Trio Solution

The following table includes the supported audio codecs and priorities for the Polycom Trio systems.

Note that the Opus codec 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.

Audio Codec Priority (continued)

Device Support	Supported Audio Codecs	Priority
Polycom Trio 8500, 8800	G.711 µ -law	6
Polycom Trio 8500, 8800	G.711a-law	7
Polycom Trio 8500, 8800	G.722	4
Polycom Trio 8800	G.719 (64kbps)	0
Polycom Trio 8500, 8800	G.722.1 (32kbps)	5
Polycom Trio 8500, 8800	G.722.1C (48kbps)	2
Polycom Trio 8500, 8800	G.729AB	8
Polycom Trio 8500, 8800	Opus	0
Polycom Trio 8500, 8800	iLBC (13.33kbps, 15.2kbps)	0,0
Polycom Trio 8500, 8800	Siren 7	0
Polycom Trio 8500, 8800	SILK	0

Polycom Trio Supported Audio Codec Specifications

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

Note: The network bandwidth necessary to send 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).

Audio Codec Specifications

Device Support	Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
Trio 8500, 8800	G.711 µ -law	RFC 1890	64 Kbps	80 Kbps	8 Ksps	20 ms	3.5 KHz

Device Support	Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
Trio 8500, 8800	G.711 a-law	RFC 1890	64 Kbps	80 Kbps	8 Ksps	20 ms	3.5 KHz
Trio 8800	G.719	RFC 5404	32 Kbps 48 Kbps 64 Kbps	48 Kbps 64 Kbps 80 Kbps	48 Ksps	20 ms	20 KHz
Trio 8500, 8800	G.711	RFC 1890	64 Kbps	80 Kbps	16 Ksps	20 ms	7 KHz
Trio 8500, 8800	G.722[1]	RFC 3551	64 Kbps	80 Kbps	16 Ksps	20 ms	7 KHz
Trio 8500, 8800	G.722.1	RFC 3047	24 Kbps 32 Kbps	40 Kbps 48 Kbps	16 Ksps	20 ms	7 KHz
Trio 8500, 8800	G.722.1C	G7221C	224 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 Ksps	20 ms	14 KHz
Trio 8500, 8800	G.729AB	RFC 1890	8 Kbps	24 Kbps	8 Ksps	20 ms	3.5 KHz
Trio 8500, 8800	Opus	RFC 6716	8 - 24 Kbps	24 - 40 Kbps	8 Ksps 16 Ksps	20 ms	3.5 KHz 7 KHz
Trio 8500, 8800 (*Trio 8500 supports 3.5, 7, and 14 KHz and not 20 or 22 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
Trio 8500, 8800	Siren 7	SIREN7	16 Kbps 24 Kbps 32 Kbps	32 Kbps 40 Kbps 48 Kbps	16 Ksps	20 ms	7 KHz
Trio 8500, 8800	Siren14	SIREN14	24 Kbps 32 Kbps 48 Kbps	40 Kbps 48 Kbps 64 Kbps	32 Ksps	20 ms	14 KHz
Trio 8800	Siren22	SIREN22	32 Kbps 48 Kbps 64 Kbps	48 Kbps 64 Kbps 80 Kbps	48 Ksps	20 ms	22 KHz

Device Support	Algorithm	Reference	Raw Bit Rate	Maximum IP Bit Rate	Sample Rate	Default Payload Size	Effective Audio Bandwidth
Trio 8500, 8800	iLBC	RFC 3951	13.33 Kbps15.2 Kbps	31.2 Kbps 24 Kbps	8 Ksps	30 ms20 ms	3.5 KHz
Trio 8500, 8800	SILK	SILK	6 - 20 Kbps 7 - 25 Kbps 8 - 30 Kbps 12 - 40 Kbps	36 Kbps 41 Kbps 46 Kbps 56 Kbps	8 ksps 12 ksps 16 ksps 24 ksps	20 ms	3.5 KHz 5.2 HKz 7 KHz 11 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.

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	Parameter	Permitted Value	Default	Change Causes Restart or Reboot
site.cfg	voice.codecPref.G711_A	0 to 27	7	No
site.cfg	voice.codecPref.G711_Mu	0 to 27	6	No
site.cfg	voice.codecPref.G719.32kbps	0 to 27	0	No
site.cfg	voice.codecPref.G719.48kbps	0 to 27	0	No
site.cfg	voice.codecPref.G719.64kbps	0 to 27	0	No

Template	Parameter	Permitted Value	Default	Change Causes Restart or Reboot
site.cfg	voice.codecPref.G722	0 to 27	4	No
site.cfg	voice.codecPref.G7221.24kbps	0 to 27	0	No
site.cfg	voice.codecPref.G7221.32kbps	0 to 27	0	No
site.cfg	voice.codecPref.G7221_C.24kbps	0 to 27	5	No
site.cfg	voice.codecPref.G7221_C.32kbps	0 to 27	0	No
site.cfg	voice.codecPref.G7221_C.48kbps	0 to 27	2	No
site.cfg	voice.codecPref.G729_AB	0 to 27	8	No
site.cfg	voice.codecPref.iLBC.13_33kbps	0 to 27	0	No
site.cfg	voice.codecPref.iLBC.15_2kbps	0 to 27	0	No
site.cfg	voice.codecPref.Lin16.8ksps	0 to 27	0	No
site.cfg	voice.codecPref.Lin16.16ksps	0 to 27	0	No
site.cfg	voice.codecPref.Lin16.32ksps	0 to 27	0	No
site.cfg	voice.codecPref.Lin16.44_1ksps	0 to 27	0	No
site.cfg	voice.codecPref.Lin16.48ksps	0 to 27	0	No
site.cfg	voice.codecPref.Siren7.16kbps	0 to 27	0	No
site.cfg	voice.codecPref.Siren7.24kbps	0 to 27	0	No
site.cfg	voice.codecPref.Siren7.32kbps	0 to 27	0	No

Template	Parameter	Permitted Value	Default	Change Causes Restart or Reboot
site.cfg	voice.codecPref.Siren14.24 kbps	0 to 27	0	No
site.cfg	voice.codecPref.Siren14.32 kbps	0 to 27	0	No
site.cfg	voice.codecPref.Siren14.48 kbps	0 to 27	3	No
site.cfg	voice.codecPref.Siren22.32 kbps	0 to 27	0	No
site.cfg	voice.codecPref.Siren22.48 kbps	0 to 27	0	No
site.cfg	voice.codecPref.Siren22.64 kbps	0 to 27	1	No
site.cfg	voice.codecPref.SILK.8ksps	0 to 27	0	No
site.cfg	voice.codecPref.SILK. 12ksps	0 to 27	0	No
site.cfg	voice.codecPref.SILK. 16ksps	0 to 27	0	No
site.cfg	voice.codecPref.SILK. 24ksps	0 to 27	0	No

SILK Audio Codec

Polycom VVX 501 and 601 business media phones support the SILK audio codec.

SILK Audio Codec Parameters

Use the following parameters to configure the SILK audio codec.

SILK Audio Codec Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.codecPref.SILK.8ksps	Set the SILK audio codec preference for the supported codec sample rates. 0 (default)	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.codecPref.SILK.12ksps	Set the SILK audio codec preference for the supported codec sample rates.	No
site.cfg	voice.codecPref.SILK.16ksps	Set the SILK audio codec preference for the supported codec sample rates. 0 (default)	No
site.cfg	voice.codecPref.SILK.24ksps	Set the SILK audio codec preference for the supported codec sample rates. 0 (default)	No
site.cfg	voice.audioProfile.SILK.8ksps.encMaxAvgBitrateKbps	Set the maximum average encoder output bitrate in kilobits per second (kpbs/s) for the supported SILK sample rate. 20 kbps (default) 6 – 20 kbps	No
site.cfg	voice.audioProfile.SILK.12ksps.encMaxAvgBitrateKbps	Set the maximum average encoder output bitrate in kilobits per second (kpbs/s) for the supported SILK sample rate. 25 kbps (default) 7 – 25 kbps	No
site.cfg	voice.audioProfile.SILK.16ksps.encMaxAvgBitrateKbps	Set the maximum average encoder output bitrate in kilobits per second (kpbs/s) for the supported SILK sample rate. 30 kbps (default) 8 – 30 kbps	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.audioProfile.SILK.24ksps.encMaxAvgBitrateKbps	Set the maximum average encoder output bitrate in kilobits per second (kpbs/s) for the supported SILK sample rate. 40 kbps (default) 12 – 40 kbps	No
site.cfg	voice.audioProfile.SILK.encComplexity	Specify the SILK encoder complexity. The higher the number the more complex the encoding allowed. 2 (default) 0-2	No
site.cfg	voice.audioProfile.SILK.encDTXEnable	0 (default) – Disable Enable Discontinuous transmission (DTX). 1 – Enable DTX in the SILK encoder. Note that DTX reduces the encoder bitrate to 0bps during silence.	No
site.cfg	voice.audioProfile.SILK.encExpectedPktLossPercent	Set the SILK encoder expected network packet loss percentage. A non-zero setting allows less inter-frame dependency to be encoded into the bitstream, resulting in increasingly larger bitrates but with an average bitrate less than that configured with voice.audioProfile.SILK.*. 0 (default) 0-100	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.audioProfile.SILK.encInbandFECEnable	0 (default) - Disable inband Forward Error Correction (FEC) in the SILK encoder. 1 - Enable inband FEC in the SILK encoder. A non-zero value here causes perceptually important speech information to be sent twice: once in the normal bitstream and again at a lower bitrate in later packets, resulting in an increased bitrate.	No
site.cfg	voice.audioProfile.SILK.MaxPTime	Specify the maximum SILK packet duration in milliseconds (ms). 20 ms	No
site.cfg	voice.audioProfile.SILK.MinPTime	Specify the minimum SILK packet duration in milliseconds (ms). 20 ms	No
site.cfg	voice.audioProfile.SILK.pTime	The recommended received SILK packet duration in milliseconds (ms). 20 ms	No

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

EEE 802.1p/Q Parameters

Use the following table to set values for IEEE 802.

1p/Q parameters. You can configure the user_priority specifically for RTP and call control packets, such as SIP signaling packets, with default settings configurable for all other packets.

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.

IEEE 802.1p/Q Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	qos.ethernet.other.user_priority	Set user priority for packets without a per-protocol setting. 2 (Default) 0 - 7	No
site.cfg	qos.ethernet.rtp.video.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

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.

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

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	voice.qualityMonitoring.collector.period	The time interval (in milliseconds) between successive periodic quality reports. 5 (default) 5 - 900 ms	Yes
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Topics:

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, and RFC 5168 - XML Schema for Media Control.

The Polycom Trio 8500 or 8800 system with a paired Visual+ connected to a Logitech C930e camera supports transmission and reception of high quality video images.

Video Layouts on Polycom Trio Solution

When using the Polycom Trio Visual+ with monitor, you can set how participants and content display during video calls.

Gallery View layout is supported for video and content during video calls in standard H.264 video meetings or point-to-point calls.

Video Layout Parameters for Polycom Trio Solution

The following parameters configure video layouts on the Polycom Trio solution.

Video Layout Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	`video.conf.displayLayout.PIP.peopleMode`	Choose what the PIP screen displays. selfView (default) - Display your own video. recentTalker - Display video from the current or most recent talker.	No
	`video.conf.displayLayout.gallery.allowContent`	1 (default) - Enable Gallery View layout for video and content. Content is scaled to fit into the 720p window of a gallery window. 0 - Disable Galley View layout. Content displays in a full screen window.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	video.conf.galleryView.overlayTimeout	Set the timer for the participant name overlay on the Visual+ monitor when using the Gallery View. 0 (default) - The overlay does not time out. 0 - 60000 ms	No

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.

By default, at the start of a video call, the Polycom Trio solution with the Logitech C930e camera transmits an RTP encapsulated video stream from the local camera. Users can stop and start video by pressing the ‘Stop My Video' and ‘Start My Video' buttons. When users stop video during a video call, video is reset and displays again at the start of the next video call.

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

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.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

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.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.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 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
site.cfg	call.singleKeyPressCameraControls	1 (default) - Tapping Camera in the call view directly shows the Camera Controls menu for EagleEye MSR camera. 0 - Tapping Camera in the call view shows a menu with camera preferences, presets, and camera controls menu items for EagleEye MSR camera.	No
features.cfg	homeScreen.camera.enable	Applies to the EagleEye MSR camera. 0 (default) - A Camera menu item is shown on the main menu. 1 - A Camera menu item displays on the Home Screen allowing users to pan, tilt or zoom.	No
features.cfg	up.arrow.repeatDelay	Choose the milliseconds (ms) an arrow button must be held before the arrow starts repeating in the Camera Controls menu for EagleEye MSR camera. 500 ms (default) 100 – 5000 ms	No
features.cfg	up.arrow.repeatRate	Choose the milliseconds (ms) between repeated simulated presses while an arrow button is being held down. This applies to the arrows in the Camera Controls menu for EagleEye MSR camera. 80 ms (default) 50 – 2000 ms	No
features.cfg	video.camera.controlStyle	Controls whether EagleEye MSR camera pan and tilt is controlled by directional arrow buttons or separate pan/tilt sliders. Simple (default)	No
video.cfg	video.camera.invertPanControl	Invert the direction of the pan control for the EagleEye MSR camera. 0 (default)	No
features.cfg	video.camera.preset.x.label	Enter a label for the EagleEye MSR camera preset. String 0 – 12 characters	No
features.cfg	video.camera.preset.x.pan	Set the pan for the EagleEye MSR camera presets, where x equals the preset. 0 (default) 0 - 1000	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	video.camera.preset.x.tilt	Set the tilt for the EagleEye MSR camera presets, where x equals the preset. 0 (default) 0 - 1000	No
features.cfg	video.camera.preset.x.zoom	Set the zoom for the EagleEye MSR camera presets, where x equals the preset. 0 (default) 0 - 1000	No
video.cfg	video.localCameraView.callState	Applies to the EagleEye MSR camera and Logitech C930e webcam. This parameter applies only when video.localCameraView.userControl is set to PerSession or Hidden. 1 (default) - The local camera view displays on the Polycom Trio Visual+ monitor. 0 - The local camera view does not display on the Polycom Trio Visual+ monitor.	No
video.cfg	video.localCameraView.fullscreen.enabled	Applies to the EagleEye MSR camera and Logitech C930e webcam. 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	Applies to the EagleEye MSR camera and Logitech C930e webcam. 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.cfg	video.localCameraView.idleState	Applies to the EagleEye MSR camera and Logitech C930e webcam. This parameter applies only when video.localCameraView.userControl is set to PerSession or Hidden. 1 (default) - The local camera view displays on the Polycom Trio Visual+ monitor. 0 - The local camera view does not display on the Polycom Trio Visual+ monitor.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.localCameraView.userControl	Applies to the EagleEye MSR camera and Logitech C930e webcam. Persistent (default) - The local camera view user setting is available in the phone menu and overrides the default you specify with video.localCameraView.fullScreen.enabled . PerSession: The local camera view user setting is available in the phone menu and overrides the default you specify with video.localCameraView.callState on a per-call basis. Changes the user makes from the phone menu revert to the default specified by video.localCameraView.idleState after the phone returns to the idle state. Hidden: The user control in the phone menu to show or hide the self view is not available.	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.autoWhiteBalance	For the EagleEye MSR camera and Logitech C930e webcam. 1 (default) – Auto white balance is enabled and the value of the video.camera.whiteBalance parameter is not used. 0 – Auto white balance is disabled, so the value of the video.camera.whiteBalance is used for white balance.	No
video.cfg	video.camera.backlightCompensation	0 (default) – Disable EagleEye MSR camera backlight compensation. 1 - Enable EagleEye MSR camera backlight compensation.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.camera.brightness	Sets the brightness level of video captured by the EagleEye MSR camera and Logitech C930e webcam. The value range is from 0 (Dimmest) to 1000 (Brightest). NULL (default) - Take the default value from the attached camera device. 0 - 1000	No
video.cfg	video.camera.contrast	Sets the contrast level of video captured by the EagleEye MSR camera and Logitech C930e webcam. The value range is from 0 (no contrast increase) to 3 (most contrast increase), and 4 (noise reduction contrast). NULL (default) - Take the default value from the attached camera device. 0 - 1000	No
video.cfg	video.camera.flickerAvoidance	Sets the flicker avoidance for EagleEye MSR camera and Logitech C930e webcam. 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.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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.camera.gamma	Set the factor to use for gamma correction applied to each frame of video captured by the EagleEye MSR camera. You can use this setting to correct for video that appears too dark or too light. 0 (default) 1000	No
video.cfg	video.camera.hue	Use to correct the color of video captured by the EagleEye MSR camera. 0 (default) 1000	No
features.cfg	video.camera.menuLocation	Specify if camera settings display under the Advanced menu for administrators or the Basic menu for users. Camera settings displayed in the menu apply to the EagleEye MSR camera and Logitech C930e webcam. Basic (default) Advanced	No
video.cfg	video.camera.saturation	Sets the saturation level of video captured by the EagleEye MSR camera and Logitech C930e webcam. NULL (default) - Take the default value from the attached camera device. 0 - 1000	No
video.cfg	video.camera.sharpness	Sets the sharpness level of video captured by the EagleEye MSR camera and Logitech C930e webcam. NULL (default) - Take the default value from the attached camera device. 0 - 1000	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.camera.whiteBalance	Use to correct the white balance tint of video captured by the EagleEye MSR camera and Logitech C930e webcam. NULL (default) - Take the default value from the attached camera device. 0 - 1000	No

Video Codec Parameters for Polycom Trio

To support Polycom Trio solution video interoperability with Cisco, set the following parameters:

- video.codecPref.H264HP="0"
- video.codecPref.H264HP.packetizationMode0="0"
- video.codecPref.H264="0"

Use the parameters in the following table to prioritize and adjust the video codecs used by the Polycom Trio solution.

Video Codec Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.codecPref.H264HP	Sets the H.264 High Profile video codec preference priority. 0 - 8 2 (default)	No
video.cfg	video.codecPref.H264HP.packetizationMode0	0 - 8 5 (default)	No
video.cfg	video.codecPref.H264SVC		No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.codecPref.Xdata	Sets the Remote Desktop Protocol (RDP) codec preference priority. A value of 1 indicates the codec is the most preferred and has highest priority. 0 - 8 7 (default)	No
video.cfg	video.codecPref.XH264UC	Sets the Microsoft H.264 UC video codec preference priority. 0 - 8 1 (default)	No
video.cfg	video.codecPref.XUlpFecUC	Set the forward error correction (FEC) codec priority. 0 - 8 8 (default)	No

Supported Video Codecs with Polycom Trio

Use the optional Polycom Trio Visual+ and Logitech C930e USB Webcam to add video to Polycom Trio 8500 and 8800 calls.

Polycom supports the following video standards and codecs:

- H.264 advanced video coding (AVC) baseline profile and high profile
- H.264 scalable video coding (SVC) (X-H264UC) and Remote Desktop Protocol (RDP) for desktop and application sharing. (Microsoft only)

The following table lists video codecs supported by the Polycom Trio 85500 or 8800 with the Polycom Trio Visual+.

Supported Video Codecs

Algorithm	MIME Type	Frame Size	Bit Rate (kbps)	Frame Rate (fps)
H.264	H264/90000		6144 kbps	30
XH264UC			6144 kbps	

Video Codec Parameters for Polycom Trio

To support Polycom Trio solution video interoperability with Cisco, set the following parameters:

- `video.codecPref.H264HP="0"`
- `video.codecPref.H264HP.packetizationMode0="0"`
- `video.codecPref.H264="0"`

Use the parameters in the following table to prioritize and adjust the video codecs used by the Polycom Trio solution.

Video Codec Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`video.cfg`	`video.codecPref.H264HP`	Sets the H.264 High Profile video codec preference priority. 0 - 8 2 (default)	No
`video.cfg`	`video.codecPref.H264HP.packetizationMode0`	0 - 8 5 (default)	No
`video.cfg`	`video.codecPref.H264SVC`		No
`video.cfg`	`video.codecPref.Xdata`	Sets the Remote Desktop Protocol (RDP) codec preference priority. A value of 1 indicates the codec is the most preferred and has highest priority. 0 - 8 7 (default)	No
`video.cfg`	`video.codecPref.XH264UC`	Sets the Microsoft H.264 UC video codec preference priority. 0 - 8 1 (default)	No
`video.cfg`	`video.codecPref.XUlpFecUC`	Set the forward error correction (FEC) codec priority. 0 - 8 8 (default)	No

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.

When this feature is enabled on the Polycom Trio 8500 or 8800 system using Polycom Trio Visual+ video capabilities, you can 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.

  If you set this parameter to audio, users can press a button on the Polycom Trio to add video.
- 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.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.callMode.default	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. Polycom Trio Allow the user to begin calls as audio-only or with video. video (default) audio - Set the initial call to audio only and video may be added during a call. On Polycom Trio solution, you can combine this parameter with video.autoStartVideoTx .	No

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	volpProt.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.

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

Topics:

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

Administrator Menu on Polycom Trio Systems

On the Polycom Trio 8800 and 8500 systems, you can add a new ‘Advanced' menu containing a subset of administrator settings.

The added 'Advanced' menu item does not require a password but one can be assigned to it.

After enabling this feature, the added 'Advanced' menu provides access to all administrator features except:

- Line Configuration
- Call Server Configuration
- TLS Security
- Test Automation

Administrator Menu Parameters

The following table lists the parameters to enable the new Administrator menu.

Admin Menu Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, site.cfg	device.auth.localAdvancedPassword.set	Set a password for the Advanced menu. 0 (default) - You cannot set a password for the added Advanced menu. 1 - You can set a password for the added Administrator menu.	No
device.cfg,site.cfg	device.auth.localAdvancedPassword	Enter a password for the added Administrator menu. Null (default) String (0 to 64 characters)	No
feaures.cfg	feature.advancedUser.enabled	0 (default) - The normal password-protected Advanced menu displays. 1 - Causes the 'Advanced' menu item to be renamed 'Admin' and adds a menu item 'Advanced' that contains a subset of administrator features. The new 'Advanced' menu does not require a password but you have the option to assign one to it.	No

Polycom Trio Visual+ Display

When using the Polycom Trio 8500 or 8800 system with the Polycom Trio Visual+, you can configure system information to display on the monitor connected to the Polycom Trio Visual+ system.

Polycom Trio Visual+ Display Parameters

The following table lists parameters you can use to hide or display icons and features on the Polycom Visual+ monitor when connected and paired with a Polycom Trio 8500 or 8800 system.

Polycom Trio User Interface Parameters

Phone Menu	Configuration Parameter	Permitted Values	Change Causes Restart or Reboot
Content-sharing Graphic	`mr.bg.showWelcomeInstructions`	All (default) - Display both the content-sharing graphic and welcome message on the Polycom Trio Visual+ monitor. TextOnly - Hide the content-sharing graphic. None - Hide both the content-sharing graphic and welcome message.	No
IP Address	`up.hideSystemIpAddress`	Specify where the IP address of the Polycom Trio system and Polycom Trio Visual+ are hidden from view. You can access the IP address from the phone Advanced menu if you set this parameter to 'Menus' or 'Everywhere'. • Nowhere (default) - The IP addresses display on all user interfaces. • TV - IP addresses are hidden from the TV monitor. • HomeScreen - IP addresses are hidden from the TV monitor and phone menu. • Menus - IP addresses are hidden from the TV monitor, phone Home screen, and menu. • Everywhere - IP addresses are hidden from the TV monitor, phone Home screen, and menu.	No

Phone Menu	Configuration Parameter	Permitted Values	Change Causes Restart or Reboot
Voicemail menu	`feature.exchangeVoiceMail.menuLocation`	Default (default) - Show the Voicemail menu in the global menu only when unread voicemails are available. After the voicemail is accessed, the Voicemail option no longer displays in the global menu and is accessible in the phone menu. Everywhere - Always show the Voicemail menu in the global menu and phone menu. MenusOnly - Show the Voicemail menu only in the phone Features menu.	No

Polycom Trio Solution Theme

You can set the Polycom Trio solution theme, labels, and colors that display on the user interface.

When the Polycom Trio's Base Profile is set to Skype, the Skype for Business theme displays by default.

Polycom Trio Solution Theme Parameters

The following parameters configure the Polycom Trio Solution theme.

Phone Theme Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`features.cfg`	`up.uiTheme`	Default (default) - The phone displays the default Polycom theme. SkypeForBusiness - The phone displays the Skype for Business theme.	No

Polycom Trio System Display Name

The system name displays in the Global menu of the Polycom Trio 8800 and 8500 systems and on the monitor connected to the Polycom Trio Visual+ accessory paired with a Polycom Trio system.

The system name also displays on any devices connected with the system wirelessly, such as Bluetooth or AirPlay-certified devices.

By default, the system name displays as Polycom Trio <model number> (xxxxxx) where (xxxxxx) is the last six digits of the phone's MAC address. For example, Polycom Trio 8800 (01161C).

You can configure the name that displays on the system, the connected monitor, and any devices wirelessly connected to the system. The name you configure for the system, using any of the following parameters, displays in the subsequent priority order:

- `system.name`
- `reg.1.displayname`
- `reg.1.label`
- `reg.1.address`
- Default system name

If you set the system name using the `system.name` parameter, the value you set displays for the system unless you configure a name to display for a specific feature.

The system name you set using any of the following feature parameters takes precedence over the name set in `system.name` :

- AirPlay: `content.airplayServer.name`
- Bluetooth: `bluetooth.devName`
- Wireless Display: `content.wirelessDisplay.name`

System Display Name Parameters

Set the system name using one or more of parameters in the following table.

System Display Name Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	`content.airplayServer.name`	Specify a system name for the local content sink for AirPlay-certified devices. If left blank, the previously configured or default system name is used. NULL (default) UTF-8 encoded string	No
	`content.wirelessDisplay.sink.name`	Specify a system name for the local content sink for Android or Windows devices. If left blank the previously configured or default system name is used NULL (default) UTF-8 encoded string	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	bluetooth.devName	Enter the name of the system that broadcasts over Bluetooth to other devices. NULL (default) UTF-8 encoded string	
	reg.1.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	
reg-advanced.cfg	reg.1.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	N
	reg.1.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) UTF-8 encoded string	No
	system.name	The system name that displays at the top left corner of the monitor, and at the top of the Global menu of the Polycom Trio system. String	No

Polycom Trio Solution Status Messages

You can choose to display a maximum of five multi-line messages in the Polycom Trio Visual+ Status Bar.

Each message can contain a maximum of 64 characters. If the length of the message exceeds the size of the status bar, the message wraps into multiple lines.

When you configure multiple messages, you can adjust the number of seconds each message displays.

Polycom Trio Solution Status Message Parameters

The following table lists parameters that configure status messages on the Polycom Trio solution.

Status Message Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	up.status.message.flash.rate	Specify the number of seconds to display a message before moving to the next message. 2 seconds (default) 1 - 8 seconds	No
features.cfg	up.status.message.1 up.status.message.2 up.status.message.3 up.status.message.4 up.status.message.5	<message line one> <message line two> <message line three> <message line four> <message line five>	No

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.

Time Zone Location Parameters

The following parameters configure time zone location.

Time Zone 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

Permitted Values	Permitted Values
	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

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.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
site.cfg	tcpIpApp.sntp.daylightSavings.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.daylightSavings.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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.sntp.daylightSavings.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.daylightSavings.start.dayOfWeek	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.daylightSavings.start.dayOfWeek.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.daylightSavings.start.month	Specifies the month to start DST. Range is 1 to 12. 3 (Default) - March 1 - January 2 - February... 12 - December	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.sntp.daylightSavings.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.daylightSavings.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.daylightSavings.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.daylightSavings.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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.sntp.daylightSavings.stop.month	Specifies the month to stop DST. Range is 1 to 12. 11 - November 1 - January 2 - February… 12 - December	No
site.cfg	tcpIpApp.sntp.daylightSavings.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.gmtOffset	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.gmtOffsetcityID	Range is 0 to127. NULL (Default) For descriptions of all values, refer to Time Zone Location Description.	No
site.cfg	tcpIpApp.sntp.gmtOffset.overrideDHCP	0 (Default) - The DHCP values for the GMT offset are used. 1 - The SNTP values for the GMT offset are used.	No
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

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

lcl.datetime.date.format	lcl.datetime.date.longformat	Date Displayed on Phone
YYYY/MM/DD	n/a	2011/08/11

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.

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

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
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	No

Multilingual Parameters

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

Template	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 parameterto 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

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 Polycom 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

Access the Country of Operation Menu in Set Language

You can view the list of countries listed in the **Country of Operation** menu in the language set by you on the phone.

If you set the system language as **Deutsch (de-de)**, the list of countries under this menu will be displayed in German.

Procedure

1. On the Polycom Trio 8800 system Home screen, go to **Settings** > **Advanced** > **Administration Settings** > **Network Configuration** > **network Interfaces** > **Wi-Fi Menu.**

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.

Procedure

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.

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.

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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

Polycom Trio Solution Number Formatting

By default, phone numbers entered on the system are automatically formatted with dashes between dialed numbers following the North American Numbering Plan (NANP), for example: 12223334444 displays as1-222-333-4444.

Polycom Trio Solution Number Formatting Parameters

Use the parameter in the following table to enable or disable number formatting.

Number Formatting Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	up.formatPhoneNumbers	1 (default) - Enable automatic number formatting. 0 - Disable automatic number formatting.	No

Number or Custom Label

On the Polycom Trio 8800 and 8500 systems, you can choose to display a number, an extension, or a custom label on the Home Screen below the time and date

Configure the Number or Label from the System

You can configure the display of the number or label on the Home screen from the system menu.

Procedure

1. Navigate to **Settings** > **Advanced** > **Administration Settings** > **Home Screen Label**.

Number and Label Parameters

You can configure display of the Polycom Trio 8800 number or label on the Home screen using centralized provisioning parameters.

Number and Label Display Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	homeScreen.customLabel	Specify the label to display on the phone's Home screen when homeScreen.labelType="Custom" . The label can be 0 to 255 characters. Null (default)	No
	homeScreen.labelType	Specify the type of label to display on the phone's Home screen. PhoneNumber (default) • When the phone is set to use Lync Base Profile, the phone number is derived from the Skype for Business server. • When the phone is set to use the Generic Base Profile, the phone uses the number you specify in reg.1.address . Custom - Enter an alphanumeric string between 0 and 255 characters. None - Don't display a label.	No
	homeScreen.labelLocation	Specify where the label displays on the screen. StatusBar (default) - The phone displays the custom label in the status bar at the top of the screen. BelowDate - The phone displays the custom label on the Home screen only, just below the time and date.	No

Capture Your Device's Current Screen

You can capture your phone or expansion module's current screen.

Note that the Polycom 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.

Procedure

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 as a BMP or JPEG file.

Directories and Contacts

Topics:

You can configure phones with a local contact directory and link contacts to speed dial buttons.

Additionally, call logs stored in the Missed Calls, Received Calls, and Placed Calls call lists let you view user phone events like remote party identification, time and date of call, and call duration. This section provides information on contact directory, speed dial, and call log parameters you can configure on your Polycom phone.

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.

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.

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

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.contacts.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 - 500 contacts except the VVX 101/201 which have a maximum of 99 contacts.	No
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 Polycom Trio solution Base Profile is set to Lync. 1 - The local directory is enabled when the Polycom 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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.local.UI enabled	1 (default) – The Directory menus provide access to Favorites/Speed Dial and Contact Directory entries and display the Favorites quick access menu on the Home screen of the VVX 500/501 and 600/601 business media phones. 0 – The local Contact Directory and Favorites/Speed Dial menu entries are not available. The Favorites quick access menu on the Home screen are not available on the VVX 500/501 and 600/601 business media phones. Set to 0 when dir.local.readOnly is set to 1 to add speed dials and macros on the phone and prevent user modification. If your call control platform provides direct contact integration and you want to prevent any access to the local directory, set feature.directory.enabled =0.	No
features.cfg	feature.pauseAndWaitDigitEntryControl.enabled	1 (default) - Enable processing of control characters in the contact phone number field. When enabled, ',' or 'p' control characters cause a one second pause. ';' or 'w' control character cause a user prompt that allows a user-controlled wait. Subsequent digits entered to the contact field are dialed automatically. 0 - Disable processing of control characters.	No

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
Polycom Trio 8500	4MB	2000
Polycom Trio 8800	4MB	2000

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 updated directory files. 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 restarts. 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.

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.

Note: 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.

The number of supported speed dial entries varies by phone model

Speed Dial Index Ranges

Phone Model	Range
Polycom Trio 8500	1 - 20
Polycom Trio 8800	1 - 20

Speed Dial Contacts Parameters

After setting up your 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.

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.

Speed Dial Parameters

Parameter Function	Parameter
Configure the maximum number of speed dial contacts that can display on the Polycom Trio Home screen. 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.	`dir.local.contacts.maxFavIx`
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 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

Corporate Directory Parameters

Use the parameters in the following table to configure the corporate directory.

Note that the exact configuration of a corporate directory depends on the LDAP server you use.

Note: 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.allowCredentialsFromUI.enabled	Enable users to enter LDAP credentials on the phone. 0 (default) – Users are not prompted to enter credentials on the phone when they access the Corporate Directory. 1 – Users are prompted to enter credentials on the phone when accessing the Corporate Directory for the first time. **Note:** Users are only prompted to enter their credentials when credentials are not added through configuration or after a login failure.	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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 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	Determine if background downloading from the LDAP server is allowed. 0 (default) 1	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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.bindOnInit	Determine if bind authentication is used on initialization. 1 (default) 0	Yes
features.cfg	dir.corp.cacheSize	Set 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
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	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	dir.corp.persistentCredentials	Set to securely store and encrypt LDAP directory user credentials on the phone. Enable dir.corp.allowCredentialsFromUI.enabled to allow users to enter credentials on the phone. 0 (default) 1 **Note:** If you disable the feature after enabling it, then all the saved user credentials are deleted for all users.	
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.serverSortNotSupported	0 (default) – The server supports server-side sorting. 1 – The server does not support server-side sorting, so the phone handles the sorting.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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	No
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.corporateDirectory.enabled	0 (default) - The corporate directory feature is disabled and the icon is hidden. 1 (default) - The corporate directory is enabled and the icon shows.	No

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).

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
site.cfg, features.cfg	callLists.collapseDuplicates	Lync Base Profile – 0 (default) Generic Base Profile – 1 (default) 1 – Consecutive incomplete calls to/ from the same party and in the same direction are collapsed into one record in the calls list. The collapsed entry displays the number of consecutive calls. 0 – Each call is logged individually in the calls list.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg, features.cfg	callLists.logConsultationCalls	ync Base Profile – 1 (default) Generic Base Profile – 0 (default) 0 – Consultation calls not joined into a conference call are not logged as separate calls in the calls list. 1 – Each consultation calls is logged individually in the calls list.	No
features.cfg	feature.callList.enabled	1 (default) - Allows you to enable the missed, placed, and received call lists on all phone menus including the Home screen and dial pad. 0 - Disables all call lists. Hiding call lists from the Home screen and dial pad requires UCS 5.4.2 RevAA or higher.	No
features.cfg	feature.callListMissed.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.callListPlaced.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
features.cfg	feature.callListReceived.enabled	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.	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	feature.exchangeCallLog.enabled	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.collapseDuplicates 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.callListMissed.enabled ◦ feature.callListPlaced.enabled ◦ feature.callListReceived.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.	

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 Call direction with respect to the user.	In, Out

Element	Permitted Values
disposition Indicates what happened to the call. When a call entry is first created, the disposition is set to Partial.	Busy, Forwarded, Normal, Partial, Preempted, Rejected, RemotelyHandled, Transferred
line The line (or registration) index.	Positive integer
protocol The line protocol.	SIP
startTime The start time of the call. For example: 2010-01-05T12:38:05 in local time.	String
duration The duration of the call, beginning when it is connected and ending when the call is terminated.For example: `PT1H10M59S .`	String
count The number of consecutive missed and abandoned calls from a call destination.	Positive Integer
destination 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).	Address
source The source of the call (caller ID from the call recipient's perspective).	Address
Connection	Address

Element	Permitted Values
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 The final connected party of a call that has been forwarded or transferred to a third party.	Address

Resetting Contacts and Recent Calls Lists on Polycom Trio System

You can reset the Contacts list and Recent call lists are stored locally on the Polycom Trio 8800 system to their default settings.

Procedure

1. On the phone, go to **Settings** > **Advanced**.
2. Enter the administrative password (default 456).
3. Select **Reset to defaults** > **Reset User Data**.
4. When prompted “Are you sure?”, select **Yes**.

Call Controls

Topics:

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.

However, you can configure the Polycom Trio 8800 and 8500 systems to play an audible tone when the mute status of the device is changed either from any of the mute buttons of the system (device and any connected devices) or far-end system (remote mute). This allows you to know if the system microphones are in a mute or un-mute state. In addition, you can set a periodic reminder which plays a tone periodically when the phone is in the mute state. The time interval can be set using configuration parameter and the value must not be less than 5 seconds.

Microphone Mute Parameters

The following parameters configure microphone mute status alert tones.

Mute Status Alert Tone Parameters

Template	Parameter	Permitted Description	Change Causes Restart or Reboot
features.cfg	se.touchFeedback.enabled	0 - Does not play an alert tone when the mute status is changed on the Polycom Trio 8800 or 8500 system. 1 - An alert tone is played when the mute status is changed either from the Polycom Trio 8800, 8500, or far-end system.	No
features.cfg	call.mute.reminder.period	The time interval in seconds to play an alert tone periodically when the Polycom Trio 8800 or 8500 system is in the mute state. 5 (default) 5 - 3600	No

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.

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

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.

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 . 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

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.

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
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

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.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

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.

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

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.

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
features.cfg	feature.doNotDisturb.enable	1(default) - Enable Do Not Disturb (DND). 0 - Disable Do Not Disturb (DND).	Yes
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

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	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

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.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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 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.

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

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.

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

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 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.

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

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

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.

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
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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 or6416@polycom.com).	Yes

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	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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

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 speakerphone buttons on the phone.

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.

You can specify only one line registration for the Polycom Trio 8800 system.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	call.autoOffHook.x.protocol	Specify the calling protocol. 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

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.

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 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 assign a registered line to multiple line keys, the default number of concurrent calls applies to all line keys.

Polycom Trio can have a maximum of 12 concurrent calls with only one active call in progress. You can register one line on the Polycom Trio system.

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` . 24 1 - 24 VVX 101, 201 8 (default) 1- 8	No

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

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.

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

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.

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.callBackMode	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.cfg	msg.mwi.x.callBack	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.cfg	msg.mwi.x.subscribe	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 bootup. 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

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	1 (default) - Lync Base Profile 0 (default) - Generic Base Profile 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

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.

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

Local and Centralized Conference Calls

You can set up local or centralized audio and video conferences.

When a Polycom Trio 8500 or 8800 system is paired with the Polycom Trio Visual+ system, users can initiate and join the following types of conferences:

- Local multipoint audio conference with up to four external connections
- Local video conferences
- Video calls on supported H.264 standards-compliant video bridges or services

The Polycom Trio solution can send and receive one video connection and displays the far-end device that joined the call last. Polycom Trio does not support locally-hosted multipoint video conferencing.

To enable video and content for conference calls, you must connect Polycom Trio Visual+ to a monitor and connect a Logitech Webcam C930e USB camera. When the devices are connected and paired, users can send video and share content. For details and limitations of content sharing, refer to the section Content Sharing.

Local and Centralized Conference Call Parameters

The following table lists available call management parameters.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
video.cfg	video.conf.addVideoWhenAvailable	0 (default) - When Polycom Trio system is added to a conference by another participant via digit dialing, the Polycom Trio system does not add video. 1 - When Polycom Trio system is added to a conference by another participant via digit dialing, the Polycom Trio system adds video if video is available on the conference.	No

Conference Meeting Dial-In Options

When you enable the Calendar, the Polycom Trio system displays a meeting reminder for upcoming meetings.

If a dial-in number is available for the meeting, the reminder presents a Join button that enables users to join the meeting. If a meeting lists multiple dial-in numbers or URIs for the meeting, by default, the Join button automatically dials the first number.

You have the option to configure the Polycom Trio system to offer users a list of available numbers when they tap the Join button instead of dialing the first number.

You can enable this feature using the `exchange.meeting.join.promptWithList` parameter. When enabled, the Polycom Trio system provides multiple dial-in options when the user taps the Join button on the meeting reminder. You can enable users to choose any of the following dial-in options to join a meeting:

- SIP URI
- Tel URI
- PSTN number
- IP dial

Conference Meeting Dial-In Options Parameters

The following table lists the parameters to configure the dial-in information.

SIP URI Dial-in Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
`applications.cfg`	`exchange.meeting.join.promptWithList`	Specifies the behavior of the Join button on meeting reminder pop-ups. 0 (default) - Tapping Join on a meeting reminder should show a list of numbers to dial rather than immediately dialing the first one. 1 - A meeting reminder does not show a list of numbers to dial.	No
`applications.cfg`	`exchange.meeting.parseWhen`	Specifies when to scan the meeting's subject, location, and description fields for dialable numbers. NonSkypeMeeting (default) Always Never	Yes
`applications.cfg`	`exchange.meeting.parseOption`	Specifies where to search for a dialable number. All (default)	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
applications.cfg	exchange.meeting.parseEmailsAsSipUris	List instances of text like user@domain or user@ipaddress in the meeting description or subject under the More Actions pane as dialable SIP URIs. 0 (default) - it does not list the text as a dialable SIP URI 1 - it treats user@domain or user@ipaddress as a dialable SIP URI.	Yes
applications.cfg	exchange.meeting.parseAllowedSipUriDomains	List of comma-separated domains that will be permitted to be interpreted as SIP URIs Null (default) String (maximum of 255 characters)	Yes

Hybrid Line Registration

The Polycom Trio 8500 and 8800 system supports hybrid (Skype for Business / Open SIP) registration.

You can simultaneously register one line with Skype for Business or Open SIP and a second line with another Open SIP server. Similarly, you can choose to register all lines with Open SIP sever. You can also choose the number of lines you want to use by setting the value in reg.limit parameter.

If you plan to configure and register Skype for Business on one line, make sure to always use Line 1 for Skype for Business. You cannot simultaneously register two Skype for Business lines.

In addition, you can configure the line switching feature based on dial plan when the phone is on-hook. The line switching feature enables the dialed number to switch to the corresponding line. For example, when you place a call from the phone and the number corresponds to an Open SIP line, the line switching feature enables the dialed number to switch to the corresponding line.

Moreover, for dial plan based line switching, when all the lines are registered to Open SIP, the value defined in the global parameter for a dial plan takes the priority. For example, dialplan.impossibleMatchHandling and dialplan.conflictMatchHandling . Similarly, if the line is registered to Skype for Business, the value defined in the per-registration dial plan parameter takes priority over general dial plan parameter. For example, dialplan.1.conflictMatchHandling and dialplan.1.impossibleMatchHandling .

When more than one digit maps are getting matched to the dialed number - a conflict match - and the parameter is disabled, the first matching digit map starting from left to right takes priority. However, if dialplan.conflictMatchHandling parameter is enabled, the matching digit map having the lowest timeout value takes priority.

However, line switching is configurable based on dial plan when the phone is off-hook. By default, line switching for on-hook and off-hook dialing is disabled.

Note that the Presence feature is available only on the Skype for Business line and will display the Device status. The following table list the Presence status for specific environment.

Presence Status Indicators for Hybrid Line Registration

Use Cases	Presence State on Skype for Business Line	Presence String	Presence State on Open SIP Line
Non-Skype line in a call	Busy	In a call	Not Supported
Skype line in a call	Busy	In a call	Not Supported
Content shared over PPCIP	Busy	In a call	Not Supported
Non-Skype line in conference	Busy	In a conference	Not Supported
Skype line in conference	Busy	In a conference	Not Supported
DND on Skype line	DND	Do Not Disturb	Not Supported
DND on Open SIP line	Available	Available	Not Supported

Hybrid Line Registration Limitations

The Hybrid Registration feature include the following limitations:

- Merging of local conference is only supported with open SIP registrations and not supported with Skype for Business (bridging a Skype for Business with an open SIP line is not supported).
- Local merging of two point-to-point calls made using two different lines between two Polycom Trio systems is not supported.
- Only call transfers between different SIP registrations with the same SIP call servers is supported. Call transfer between SIP registrations on different SIP call servers is not supported.
- Transport Layer Security (TLS) encryption of Real-time Transport Protocol (RTP) media for secure communication in hybrid Open SIP registrations is not supported.

Hybrid Line Registration Parameters

The following tables lists the parameters to configure dial plan and line switching for Hybrid Registration.

Dial Plan and Digit Map Parameters for Hybrid Registrations

Template	Parameter	Permitted Values	Change Causes Restart or Reboot

site.cfg	dialplan.digitmap.lineSwitching.enable	0 (default) - Disable the line switching in dial plan to switch the call to the dial plan matched line. 1 - Enable the line switching in dial plan to switch the call to the dial plan matched line. This is not applicable for off-hook dialing.	No
reg.cfg	reg.limit	Specify the maximum number of lines to use for registration. 1 (default) 12 maximum (1-3 supported)	No
sip-interop.cfg	reg.1.mergeServerDigitMapLocally	1 (default) - Allow the digit map from the in-band provisioning parameter dialplan.1.digitmap to merge with the local digit map. 0 - The digit map is not merged.	No

Configure Hybrid Line Registration using the Web Configuration Utility

You can configure the phone to support the Hybrid (Skype for Business/ Open SIP) Registration from phone's Web Configuration Utility page after enabling the feature using configuration parameter.

Make sure the to set the Base profile as Skype for Business on the Polycom Trio 8800 system.

Procedure

1. Sign in to the Polycom Trio 8800 system's Web configuration Utility page using Admin account.

   If configuring Skype for Business on Line 1, sign in to the Web Configuration Utility as Skype for Business user.
2. On the Web Configuration Utility page, navigate to Settings > Line.

   The number of lines enabled to configure is displayed.
3. Configure the Skype for Business registration on Line 1.
4. Configure the Open SIP registration on Line 2.

   You can configure other lines with Open SIP registration.

Local Digit Map

The local digit map feature allows the phone to automatically call a dialed number when configured.

Dial plans apply on-hook when no Skype for Business line is registered or when line switching is enabled and at least one line has a non-empty dial plan.

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.

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	Lync Base Profile – 1 (default) Generic Base Profile – 0 (default) 0 - The dial plan is not applied to numbers dialed from the directory or speed dial, including auto-call contact numbers. 1 - The dial plan is applied to numbers dialed from the directory or speed dial, including auto-call contact numbers.	Yes
site.cfg	dialplan.applyToForward	Lync Base Profile – 1 (default) Generic Base Profile – 0 (default) 0 - The dial plan does not apply to forwarded calls. 1 - The dial plan applies to forwarded calls.	Yes
site.cfg	dialplan.applyToTelUriDial	Choose whether the dial plan applies to URI dialing. 1 (default) 0	Yes

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

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.
		Generic Base Profile (default) –
		`[2-9]11|0T|+011xxx.T|`
		`0[2-9]xxxxxxxxx|`
		`+1[2-9]xxxxxxxx|`
		`[2-9]xxxxxxxxx|[2-9]xxxT`
		Lync Base Profile (default) – NULL
		`[2-9]11|0T|+011xxx.T|`
		`0[2-9]xxxxxxxxx|`
		`+1[2-9]xxxxxxxx|`
		`[2-9]xxxxxxxxx|[2-9]xxxT` (default)
		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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	dialplan.removeEndOfDial	Sets if the trailing # is stripped from the digits sent out. 1 (default) 0	Yes
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

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. Generic Base Profile (default) – 0 Lync Base Profile (default) – 4 0-99 seconds You can apply dialplan.userDial.timeOut only when its value is lower than up.IdleTimeOut .	No

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.

In addition, the digit map feature allows SIP URI dialing to match the URIs based on dial plan.

When making a URI call, the Polycom Trio 8500 and 8800 systems allow dial plan matching for SIP URI calls to append strings to the dialed number. SIP URI dial plan can also be used with auto line switching in Hybrid registration scenarios to automatically select the line based on dial plan.

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 an 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 you dial 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 you dial 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 you dial 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.
- `sip\:764xxxxxRR@registrar.polycomcsn.comR` - appends `@registrar.polycomcsn.com` to any URI calls matching with "764xxxxx".

  For example, if you make a SIP URI call with 76412345 then `@registrar.polycomcsn.com` is appended to the string such that the SIP URI call INVITE becomes `sip:76412345@vc.polycom.com` . Here, `@domain` string is required only for SIP URI calls from unregistered lines.
- `sip\:xxxx\@registrar\.polycomcsn\.com` - This will match with any four digit URI calls having the domain `@registrar.polycomcsn.com` .

  For example, if you configure three lines and has dial plan based line switching enabled. Now, if the third line's dial plan has `sip\:xxxx\@registrar\.polycomcsn\.com` then call will be initiated from the third line if user dial `1234@registrar.polycomcsn.com` because it matches with the third line's dial plan.
-

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
```

Enhanced 911 (E.911)

This E.911 feature allows you to configure one of three sources the phone obtains location information from:

- LLDP-MED
- DHCP via option 99
- LIS compliant with RFC 5985

Configuring the source of location information allows the phone to share its location details in the invite sent when a 911 call is made to ensure the 911 operator dispatches emergency services to the correct address.

Enhanced 911 (E.911) Parameters

Use the following parameters to configure E.911.

E.911 Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	feature.E911.HELD .server	NULL (default) Set the IP address or hostname of the Location Information Server (LIS) address. For example, host.domain.com or https://xxx.xxx.xxx.xxx.	No
site.cfg	feature.E911.HELD .username	NULL (default) Set the user name used to authenticate to the Location Information Server.	No
site.cfg	feature.E911.HELD .password	NULL (default) Set the password used to authenticate to the Location Information Server.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	feature.E911.HELD .identity	Set the vendor-specific element to include in a location request message. For example, ‘companyID’. NULL (default) String 255 character max	No
site.cfg	feature.E911.HELD .identityValue	Set the value for the vendor-specific element to include in a location request message. NULL (default) String 255 character max	No
site.cfg	feature.E911.loca tionRetryTimer	Specify the retry timeout value in seconds for the location request sent to the Location Information Server (LIS). The phone stops retries after receiving location information received the LIS. 60 seconds (default) 60 - 86400 seconds	No
site.cfg	feature.E911.HELD .nai.enable	You can include or omit the Network Access Identifier (NAI) containing the SIP user information used to subscribe to the Location Information Server (LIS). 0 (default) – The NAI is omitted as a device identity in the location request sent to the LIS. 1 - The NAI is included as a device identity in the location request sent to the LIS.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	locInfo.source	Specify the source of phone location information. This parameter is useful for locating a phone in environments that have multiple sources of location information. LLDP (default for Generic Base Profile) – Use the network switch as the source of location information. MS_E911_LIS (default for Lync Base Profile)– Use the Skype for Business Server as the source of location information. CONFIG – You can manually configure the source of location information. Skype only. LIS – Use the location information server as the source of location information. Generic Base Profile only. DHCP – Use DHCP as the source of location information. Generic Base Profile only. If location information is not available from a default or configured source, the fallback priority is as follows: Generic Base Profile: No fallback supported for Generic Base Profile Lync Base Profile: MS_E911_LIS > CONFIG > LLDP	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	feature.E911.enabled	0 (default) – Disable the E.911 feature. The INVITE sent for emergency calls from the phone does not include the geolocation header, geolocation option in supported header, geolocation-routing header, or the GEOPRIV location object. 1 – Enable the E.911 feature. The INVITE sent for emergency calls from the phone includes the geolocation header defined in RFC 6442 and PIDF presence element as specified in RFC3863 with a GEOPRIV location object specified in RFC4119 for in Open SIP environments. This parameter is mutually exclusive of the GENBAND E.911 feature and if this parameter and feature.genband.E911.enabled are enabled, this parameter takes precedence.	No
site.cfg	feature.E911.HELD.requestType	Any (default) - Send a request to the Location Information Server (LIS) to return either ‘Location by Reference’ or ‘Location by Value’. Note this is not the ‘Any’ value referred to in RFC 5985. Civic – Send a request to the LIS to return a location by value in the form of a civic address for the device as defined in RFC 5985. RefID – Send a request to the LIS to return a set of Location URIs for the device as defined in RFC 5985.	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voIpProt.SIP.header.priority.enable	0 (default) – Do not include a priority header in the E.911 INVITE message. 1 - Include a priority header in the E.911 INVITE message.	No
site.cfg	voIpProt.SIP.header.geolocation-routing.enable	0 (default) – Do not include the geolocation-routing header in the E. 911 INVITE message. 1 - Include the geolocation-routing header in the E.911 INVITE message.	No
site.cfg	feature.E911.HELD.secondary.server	Set the IP address or hostname of the secondary Location Information Server (LIS) address. For example, host.domain.com or https://xxx.xxx.xxx.xxx. NULL (default) Dotted-decimal IP address Hostname Fully-qualified domain name (FQDN)	No
site.cfg	feature.E911.HELD.secondary.username	Set a user name to authenticate to the secondary Location information Server (LIS). NULL (default) String	No
site.cfg	feature.E911.HELD.secondary.password	Set a password to authenticate to the secondary LIS. NULL (default) String	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	feature.E911.usagerule.retransmission	0 (default) - The recipient of this Location Object is not permitted to share the enclosed Location Information, or the object as a whole, with other parties. 1 - Distributing this Location is permitted.	No

Shared Lines

Topics:

This section shows you how to configure shared line features.

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.

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 . Null (default) string address	No

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	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) - The Caller-ID information received in the 200 OK status code is not ignored if the NOTIFY message received with caller information includes display information. 1 - The Caller-ID information received in the 200 OK status code is ignored if the NOTIFY message received with caller information includes display information.	No

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

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

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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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.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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
reg-advanced.cfg	reg.x.displayName	The display name used in SIP signaling 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.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
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

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
debug.cfg	reg.x.gruu	Specify if the phone sends sip.instance in the REGISTER request. 0 (default) 1	No
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

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
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

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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

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

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

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

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

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

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.

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

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 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.

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
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

Group Paging

The group paging feature is available on VVX business media phones and Polycom 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 Polycom Trio solution, you can only receive incoming pages. You cannot use Polycom 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.

Note: 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.

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.

Note: The default port used by Group Paging conflicts with the UDP port 5001 used by Polycom® People+Content™ on the Polycom 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.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.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.transmit.timeout.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.transmit.timeout.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.	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	ptt.pageMode.priorityGroup	The paging group to use for priority pages. 24 (default) 1 to 25	
site.cfg	ptt.pageMode.payloadSize	The page mode audio payload size. 20 (default) 10, 20, ..., 80 milliseconds	
site.cfg	ptt.pageMode.emergencyGroup	The paging group used for emergency pages. 25 (default) 1 to 25	
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.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	
site.cfg	ptt.pageMode.enable	0 (default) - The group paging is disabled.1 - The group paging is enabled.	
features.cfg	ptt.pageMode.group.x.available	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.cfg	ptt.pageMode.group.x.allowReceive	1 (default) - The phone can receive pages on the specified group. 0 -The phone cannot receive pages on the specified group.	
features.cfg	ptt.pageMode.group.x.allowTransmit	Allows outgoing announcements to the group 1 (default) 0	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	ptt.pageMode.group.x.label	The label to identify the group ch24: Priority,ch25: Emergency, others:Null ch1, 24, 25: 1, others: 0 (default) string	
features.cfg	ptt.pageMode.group.x.subscribed	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.	

User Profiles

Topics:

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.

Note: 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.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	prov.login.persistent	0 (default) - Users are logged out if the handset reboots. 1 - Users remain logged in when the phone reboots.	No
site.cfg	prov.login.required	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.useProvAuth	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.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

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` .

Authentication of User Profiles

When using the User Profiles feature, you can authenticate users with phone-based or server-based authentication methods. Phone-based authentication authenticates credentials entered by the user against the crednetials in the `<user>.cfg` file. Server-based authentication passes user credentials to the provisioning server for authentication.

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.

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`

Procedure

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.
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.

Procedure

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

Phone Authentication of User Profiles

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.

Procedure

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.

Procedure

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.

Network

Topics:

Polycom UC Software allows you to make custom network configurations.

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.

Polycom Trio System and Model Names

Model	System Name	Model Name
Polycom Trio 8800	Polycom Trio 8800	Polycom Trio-Polycom Trio_8800
Polycom Trio 8500	Polycom Trio 8500	Polycom Trio-Polycom Trio_8500
Polycom Trio Visual+	Polycom Trio Visual+	Polycom Trio-Polycom Trio_Visual+

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

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 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.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

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.

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

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

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 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.

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

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. You can enter a maximum of 12 record entries for DNS-A, DNS-NAPTR, and DNS-SRV. records.

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.

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 . Null (default) string address	No
sip-interop.cfg	reg.x.server.y	Specify the call server used for this registration.	

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. VVX 101: Standard (default), GENBAND, ALU-CTS, DT VVX 201: Standard (default), GENBAND, ALU-CTS, ocs2007r2, lync2010 All other phones: Standard (default), 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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

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

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

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

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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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.A.networkOverride	0 (default) - Does not allow the static DNS A record entry to take priority over dynamic network DNS. 1 – Allows the static DNS cached A record entry to take priority over dynamic network DNS. Moreover, the DNS TTL value is ignored.	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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

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

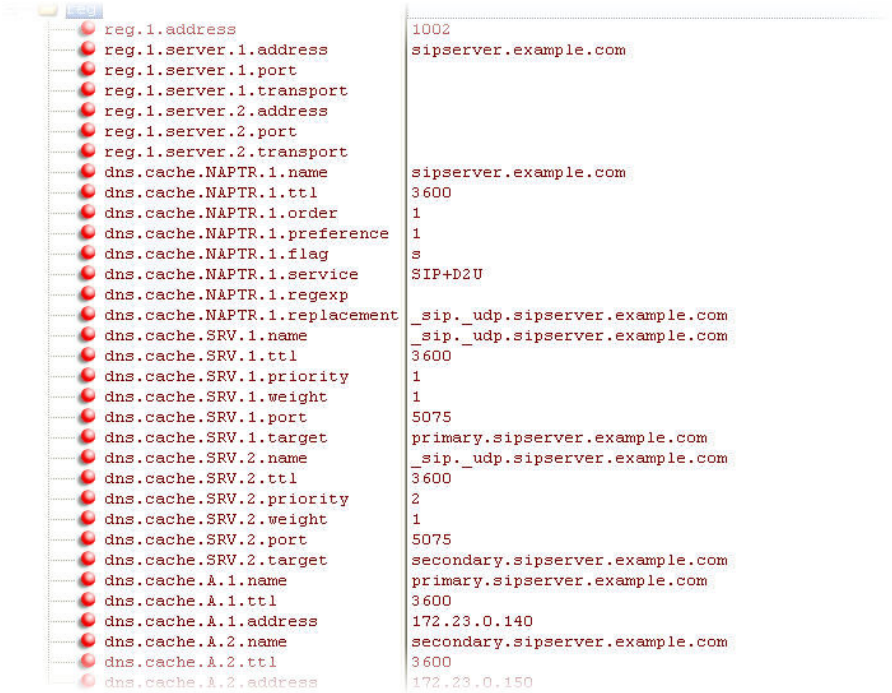
This example shows how to configure static DNS cache where your DNS provides NAPTR and SRV records for `reg.x.server.x.address` .

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.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.

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.

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.

VoIP Server Parameters

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	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	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	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

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.

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*.

Server Redundancy Parameters

Use the parameters in the following table to set up server redundancy for your environment.

Server Redundancy 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

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

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

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

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.

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

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.

RTP Ports Parameters

Use the parameters in the following table to configure RTP packets and ports.

Real-Time Transport Protocol Port Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	tcpIpApp.port.rtp.filterByIp[1]	IP addresses can be negotiated through the SDP protocols. 1 (Default) - Phone rejects RTP packets that arrive from non-negotiated IP addresses.	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.mediaPortRangeEnd	Determines the maximum supported end range of audio ports. Range is 1024 to 65485. 2269 (Default)	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Wireless Network Connectivity (Wi-Fi)

The Polycom Trio 8800 supports various wireless modes, security options, radio controls, and Quality of Service monitoring.

To ensure the best performance in your location, set a proper country code with the parameter `device.wifi.country` before enabling Wi-Fi.

Enabling Wi-Fi automatically disables the Ethernet port. You cannot use Wi-Fi and Ethernet simultaneously to connect Polycom Trio 8800 to your network. When you connect the system to your network over Wi-Fi, only audio-only calls are available. Note that Polycom Trio 8800 does not support Wi-Fi captive portals or Wireless Display (WiDi).

Note: When you provision the Polycom Trio solution via Wi-Fi connection to the network, the Polycom Trio solution looks for files on the provisioning server using the LAN MAC address and not the Wi-Fi MAC address.

The Polycom Trio solution supports the following wireless modes:

- 2.4 GHz / 5 GHz operation
- IEEE 802.11a radio transmission standard
- IEEE 802.11b radio transmission standard
- IEEE 802.11g radio transmission standard
- IEEE 802.11n radio transmission standard

Note: Note: You cannot use Polycom Trio Visual+ for video calls when you connect Polycom Trio 8800 to your network using Wi-Fi. The Polycom Trio 8800 and Polycom Trio Visual+ do not pair when the Polycom Trio 8800 is connected to your network using Wi-Fi.

Wi-Fi Parameters

The parameters you configure depend on the security mode of your organization and whether or not you enable DHCP.

Polycom Trio 8800 solution is shipped with a security-restrictive worldwide safe Wi-Fi country code setting.

The Polycom Trio solution supports the following Wi-Fi security modes:

- WEP
- WPA PSK
- WPA2 PSK
- WPA2 Enterprise

Wi-Fi Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, wireless.cfg	device.wifi.enabled	Enable or disable Wi-Fi on the Polycom Trio 8800 system. 0 (default) 1	No
device.cfg, wireless.cfg	device.wifi.country	Enter the two-letter code for the country where you are operating the Polycom Trio 8800 system with Wi-Fi enabled. NULL (default) Two-letter country code	No
device.cfg, wireless.cfg	device.wifi.dhcpEnabled	Enable or disable DHCP for Wi-Fi on the Polycom Trio 8800 system. 0 (default) 1	No
device.cfg	device.wifi.dhcpBootServer	For use with the Polycom Trio 8800 system. 0 (default) 1 2 V4 V6 Static	
device.cfg	device.wifi.ipAddress	Enter the IP address of the wireless device if you are not using DHCP on the Polycom Trio 8800 system. 0.0.0.0 (default) String	No
device.cfg, site.cfg	device.wifi.subnetMask	For use with the Polycom Trio 8800 system. Set the network mask address of the wireless device if not using DHCP. 255.0.0.0 (default) String	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, site.cfg	device.wifi.ipGateway	Enter the IP gateway address for the wireless interface if not using DHCP on the Polycom Trio 8800 system. 0.0.0.0 (default) String	No
device.cfg, wireless.cfg	device.wifi.ssid	For use with the Polycom Trio 8800 system. Set the Service Set Identifier (SSID) of the wireless network. SSID1 (default) SSID	No
device.cfg, wireless.cfg	device.wifi.securityMode	For use with the Polycom Trio 8800 system. Specify the wireless security mode. NULL (default) None WEP WPA-PSK WPA2-PSK WPA2-Enterprise	No
device.cfg, wireless.cfg	device.wifi.wep.key	For use with the Polycom Trio 8800 system. Set the length of the hexadecimal WEP key. 0 = 40-bits (default) 1 = 104-bits	No
device.cfg, wireless.cfg	device.wifi.psk.key	For use with the Polycom Trio 8800 system. Enter the hexadecimal key or ASCII passphrase. 0xFF (default) String	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg, wireless.cfg	device.wifi.wpa2Ent.method	For use with the Polycom Trio 8800 system. Set the Extensible Authentication Protocol (EAP) to use for 802.1X authentication. NULL (default) EAP-PEAPv0/MSCHAPv2 EAP-FAST EAP-TLS EAP-PEAPv0-GTC EAP-TTLS-MSCHAPv2 EAP-TTLS-GTC EAP-PEAPv0-NONE EAP-TTLS-NONE EAP-PWD	No
device.cfg, wireless.cfg	device.wifi.wpa2Ent.user	The WPA2-Enterprise user name.	No
device.cfg, wireless.cfg	device.wifi.wpa2Ent.password	The WPA2-Enterprise password.	No
device.cfg, wireless.cfg	device.wifi.radio.enable2ghz		No
device.cfg, wireless.cfg	device.wifi.radio.enable5ghz		No

Enable Wi-Fi on the Polycom Trio 8800

You can wirelessly connect the Polycom Trio 8800 to your network using Wi-Fi, which is disabled by default.

When you enable Wi-Fi, the system reboots.

Procedure

1. Go to **Settings** > **Advanced** > **Administration Settings** > **Network Configuration** > **Network Interfaces** > **Wi-Fi Menu,** and turn Wi-Fi to **On**.

   The phone restarts.

2. When the phone completes restart, go to **Settings** > **Advanced** > **Administration Settings** > **Network Configuration** > **Network Interfaces** > **Wi-Fi Menu** to view available networks.

3. Select a network you want to connect to and press **Connect**.

Third-Party Servers

Topics:

This section provides information on configuring phones and features with third-party servers.

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.

Authentication for BroadWorks XSP Parameters

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

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

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.

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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

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.

Procedure

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.

Procedure

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.

BroadSoft UC-One Directory Parameters

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

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.

Configure Anonymous Call Rejection using the Web Configuration Utility

You can configure Anonymous Call Rejection in the Web Configuration Utility.

Procedure

1. Navigate to **Settings** > **UC-One**.
2. Under the **Call Setting Features**, click **Enable for Anonymous Call Rejection**.

Anonymous Call Rejection Parameters

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

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

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.

Simultaneous Ring Parameters

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.	

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.

Line ID Blocking Parameters

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

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.

BroadWorks Anywhere Parameters

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

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.

Remote Office Parameters

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.password	Set the password used to authenticate to the BroadSoft Directory XSP server. Null (default) UTF-8 encoding string	No

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.

BroadSoft UC-One Credential Parameters

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.address	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.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	feature.broadsoftdir.enabled	0 (default) - Disable simple search for Enterprise Directories. 1 - Enable simple search for Enterprise Directories.	Yes

BroadSoft 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.

Device Parameters

Topics:

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.

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	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	string	Yes
device.cfg	device.xxx.set	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.

Note: 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. localAdminPa ssword	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. localUserPas sword	Set the phone user's local password. The minimum length is defined by sec.pwd.length.user . string (32 character max)	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg	device.auxPort.enable	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. SkypeUSB —Sets the Base Profile for connecting the Polycom Trio solution to a Microsoft Room System or a Microsoft Surface Hub.	No
device.cfg site.cfg	device.dhcp.bootSrvOpt	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	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.dhcp. bootSrvUseOp t	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.cfg site.cfg	device.dhcp. dhcpVlanDisc Opt	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. dhcpVlanDisc UseOpt	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. enabled	Enable or disable DHCP. 0 1	Yes
device.cfg site.cfg	device.dhcp. option60Type	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.a ltSrvAddress	Set the secondary server to which the phone directs domain name system (DNS) queries. Server Address	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.dns.domain	Set the phone's DNS domain. String	Yes
device.cfg site.cfg	device.dns.serverAddress	Set the primary server to which the phone directs DNS queries. Server Address	Yes
device.cfg site.cfg	device.hostname	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	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	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	Enable or disable 802.1X authentication. 0 1	Yes
device.cfg site.cfg wireless.cfg	device.net.dot1x.identity	Set the identity (user name) for 802.1X authentication. String	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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.cfg site.cfg wireless.cfg	device.net.dot1x.password	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.etherModeLAN	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.etherModePC	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.net.etherStormFilter	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.etherStormFilterPpsValue	Set the corresponding packets per second (pps) for storm filter and to control the incoming network traffic. 17 to 40 38 (default)	No
device.cfg site.cfg	device.net.etherStormFilterPpsValue.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.etherVlanFilter	VLAN filtering for VVX phones is done by the Linux operating system and it cannot be disabled. 0 1	Yes
device.cfg	device.net.ipAddress	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.IPgateway	Set the phone's default router. IP address	Yes
device.cfg site.cfg	device.net.lldpEnabled	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.lldpFastStartCount	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.net.subnetMask	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.vlanId	Set the phone's 802.1Q VLAN identifier. Null—No VLAN tagging. 0 to 4094	Yes
device.cfg site.cfg	device.prov.maxRedunServers	Set the maximum number of IP addresses to use from the DNS. 1 - 8	Yes
device.cfg site.cfg	device.prov.password	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	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	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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.cfg site.cfg	device.prov. serverType	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 (default) 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. upgradeServe r	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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 Zero-Touch Provisioning: https://support.polycom.com/content/support/North_America/USA/en/support/voice/Zero_Touch_Provisioning/zero_touch_provisioning_solution.html.	No
device.cfg site.cfg	device.sec.configEncryption.key[1]	Set the configuration encryption key used to encrypt configuration files. string For more information, see the sectionConfiguration File Encryption.	Yes
device.cfg site.cfg	device.sec.coreDumpEncryption.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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
debug.cfg	device.sec.TLS.customDeviceCert1.privateKey device.sec.TLS.customDeviceCert2.privateKey	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.customDeviceCert1.publicCert device.sec.TLS.customDeviceCert2.publicCert	Enter the signed custom device certificate in PEM format (X.509). Size constraint: 8192 bytes for the device certificate.	No
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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.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	Set the TLS Platform Profile to use for provisioning. PlatformProfile1 PlatformProfile2	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.sec.TLS.profileSelection.syslog	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.cfg site.cfg	device.sec.TLS.syslog.strictCertCommonNameValidation	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.gmtOffset	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.gmtOffsetcityID	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.serverName	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	0 1—The phone's MAC address is prepended to the log message sent to the syslog server.	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg site.cfg	device.syslog.renderLevel	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.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
device.cfg wireless.cfg	device.wifi.country	Enter the two-letter code for the country where you are operating the Polycom Trio 8800 solution with Wi-Fi enabled. NULL (default) Two-letter country code	
device.cfg wireless.cfg	device.wifi.dhcpBootServer	0 (default) 1 2 V4 V6 Static	
device.cfg wireless.cfg	device.wifi.dhcpEnabled	Enable or disable DHCP for Wi-Fi. 0 (default) 1	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg wireless.cfg	device.wifi.enabled	Enable or disable Wi-Fi. 0 (default) 1	
device.cfg wireless.cfg	device.wifi.ipAddress	Enter the IP address of the wireless device if you are not using DHCP. 0.0.0.0 (default) String	
device.cfg wireless.cfg	device.wifi.ipGateway	Enter the IP gateway address for the wireless interface if not using DHCP. 0.0.0.0 (default) String	
device.cfg wireless.cfg	device.wifi.psk.key	Enter the hexadecimal key or ASCII passphrase. 0xFF (default) String	
device.cfg wireless.cfg	device.wifi.radio.band2_4GHz.enable	For use with the Polycom Trio 8800 system. Enable or disable 2.4 GHz band for Wi-Fi. 0 (default) 1	
device.cfg wireless.cfg	device.wifi.radio.band5GHz.enable	For use with the Polycom Trio 8800 system. Enable or disable the 5 GHz band for Wi-Fi. 0 (default) 1	
device.cfg wireless.cfg	device.wifi.securityMode	Specify the wireless security mode. NULL (default) None WEP WPA-PSK WPA2-PSK WPA2-Enterprise	
device.cfg wireless.cfg	device.wifi.ssid	Set the Service Set Identifier (SSID) of the wireless network. SSID1 (default) SSID	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg wireless.cfg	device.wifi.subnetMask	Set the network mask address of the wireless device if not using DHCP. 255.0.0.0 (default) String	
device.cfg wireless.cfg	device.wifi.wep.key	Set the length of the hexadecimal WEP key. 0 = 40-bits (default) 1 = 104-bits	
device.cfg wireless.cfg	device.wifi.wpa2Ent.caCert.name	For use with the Polycom Trio 8800 system. Specify the CA certificate alias for Wi-Fi enterprise (EAP) level security. To use the default certificate, set the value to Polycom 802.1X Device Certificate. NULL (default) String (0 - 128 characters)	
device.cfg wireless.cfg	device.wifi.wpa2Ent.clientCert.name	For use with the Polycom Trio 8800 system. Specify the user or device certificate alias for Wi-Fi enterprise (EAP) level security. To use the default certificate, set the value to Polycom 802.1X Device Certificate. NULL (default) String (0 - 128 characters)	
device.cfg wireless.cfg	device.wifi.wpa2Ent.method	Set the Extensible Authentication Protocol (EAP) to use for 802.1X authentication. NULL (default) EAP-PEAPv0/MSCHAPv2 EAP-FAST EAP-TLS EAP-PEAPv0-GTC EAP-TTLS-MSCHAPv2 EAP-TTLS-GTC EAP-PEAPv0-NONE EAP-TTLS-NONE EAP-PWD	
device.cfg wireless.cfg	device.wifi.wpa2Ent.password	For use with the Polycom Trio 8800 system. Enter the WPA2-Enterprise password.	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
device.cfg wireless.cfg	device.wifi.wpa2Ent.user	For use with the Polycom Trio 8800 system. Enter the WPA2-Enterprise user name.	

Configuration Parameters

Topics:

This section is a reference guide for configuration parameters available for UC Software features.

This section provides a description and permitted values of each configuration parameter.

Quick Setup Soft Key Parameters

The following table lists the parameters that configure Quick Setup soft key.

Quick Setup Soft Key Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	prov.quickSetup.enabled	0 (default) - Disables the quick setup feature. 1 - Enables the quick setup feature.	No

Bluetooth Parameters

The following table specifies the Bluetooth parameters for the VVX 600/601 phones.

Bluetooth Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
	bluetooth.pairedDeviceMemorySize	10 (default) 0 - 10	No

Per-Registration Call Parameters

Polycom phones support an optional per-registration feature that enables automatic call placement when the phone is off-hook.

The phones also support 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.

Per-Registration Call Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	call.advancedMissedCalls.addToReceivedList	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	call.advancedMissedCalls.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
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
featurescfg	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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	Determines whether the phone plays a local ring-back after receiving a first provisional response from the far end. 1 (default) - The phone plays a local ringback after receiving the first provisional response from the far end. If early media is received later, the phone stops the local ringback and plays the early media. 0 - No local ringback plays, and the phone plays only the early media received.	No
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
sip-interop.cfg, site.cfg	call.stickyAutoLineSeize.onHookDialing	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	call.switchToLocalRingbackWithoutRTP	Determines whether local ringback plays in the event that early media stops. 0 (default) – No ringback plays when early media stops. 1 – The local ringback plays if no early media is received.	No
site.cfg	call.teluri.showPrompt	1 (default) 0	No
sip-interop.cfg	call.urlModeDialing	0 (default) - Disable URL dialing. 1 - Enable URL dialing.	Yes

Remote Packet Capture Parameters

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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.

Per-Registration Dial Plan (Digit Map) Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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. Generic Base Profile (default) – 0 Lync Base Profile (default) – 4 0-99 seconds 0-99 seconds You can apply `dialplan.userDial.timeOut` only when its value is lower than `up.IdleTimeOut` .	No

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	dialplan.x.applyToCallListDial	Generic Base Profile (default) – 1 Lync Base Profile (default) – 0 0 - The dial plan does not apply to numbers dialed from the received call list or missed call list, including sub-menus for this line. 1 - The dial plan applies to numbers dialed from the received call list or missed call list, including sub-menus for this line.	Yes
site.cfg	dialplan.x.applyToDirectoryDial	Generic Base Profile (default) – 1 Lync Base Profile (default) – 0 0 - The dial plan is not applied to numbers dialed from the directory or speed dial, including auto-call contact numbers for this line. 1 - The dial plan is applied to numbers dialed from the directory or speed dial, including auto-call contact numbers for this line.	Yes
site.cfg	dialplan.x.applyToForward	Generic Base Profile (default) – 1 Lync Base Profile (default) – 0 0 - The dial plan applies to forwarded calls for this line. 1 - The dial plan applies to forwarded calls for this line.	No
site.cfg	dialplan.x.applyToTelUriDial	0 1 (default)	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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	Generic Base Profile (default) – 0 Lync Base Profile (default) – 4	Yes
site.cfg	dialplan.x.digitmap	Generic Base Profile (default) - Null Lync Base Profile (default) - 4 string - max number of characters 100	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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

Local Contact Directory File Size Parameters

The following table lists the parameters you can configure to set the size of the 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. 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 the option to use the phone's volatile RAM and set the maximum file size.

Local Contact Directory File Size Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
debug.cfg	dir.local.nonVolatile.maxSize	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 phone uses non-volatile memory for the local contact directory. 1 - Enables the use of volatile memory for the local contact directory.	No
debug.cfg	dir.local.volatile.maxSize	Sets the maximum file size of the local contact directory stored on the phone's volatile memory. VVX1500 = 200KB (default) 1 - 200KB	No

Parameter Elements for the Local Contact Directory

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	The contact's first name.	UTF-8 encoded string of up to 40 bytes1
ln	The contact's last name.	UTF-8 encoded string of up to 40 bytes1

Element	Definition	Permitted Values
ct	Contact, Used by the phone to address a remote party in the same way that a string of digits or a SIP URL are dialed manually by the user. This element is also used to associate incoming callers with a particular directory entry. The maximum field length is 128 characters. Note: This field cannot be null or duplicated	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL
sd	Speed Dial Index, Associates a particular entry with a speed dial key for one-touch dialing or dialing.	VVX=Null, 1 to 9999 Polycom Trio=20
lb	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.	UTF-8 encoded string of up to 40 bytes1
pt	Protocol, The protocol to use when placing a call to this contact.	SIP or Unspecified
rt	Ring Tone, When incoming calls match a directory entry, this field specifies the ringtone to be used.	Null, 1 to 21

Element	Definition	Permitted Values
dc	Divert Contact, The address to forward calls to if the Auto Divert feature is enabled.	UTF-8 encoded string containing digits (the user part of a SIP URL) or a string that constitutes a valid SIP URL
ad	Auto Divert, 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.	0 or 1
ar	Auto Reject, 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.	0 or 1
bw	Buddy Watching, If set to 1, this contact is added to the list of watched phones.	0 or 1
bb	Buddy Block, If set to 1, this contact is blocked from watching this phone.	0 or 1

Feature Activation/Deactivation Parameters

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.callCenterCallInformation.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.callCenterStatus.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.enhancedCallDisplay.enabled	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
features.cfg	feature.flexibleLineKey.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.ringDownload.enabled	1 (default) - The phone downloads ringtones when starting up. 0 - The phone does not download ringtones when starting up.	Yes
features.cfg	feature.uniqueCallLabeling.enabled	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.urlDialing.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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
features.cfg	reg.x.urlDialing.enabled	1 (default) - Enable dialing by URL for SIP registrations. 0 - Disable dialing by URL for SIP registrations.	
features.cfg	feature.usb.device.enabled	The USB device port enables you to use Polycom Trio 8800 and 8500 system as an audio device for your laptop. 1 (default) - Enable the USB device port. 0 - Disable the USB device port. When you disable the Polycom Trio system's USB device port using the parameter feature.usb.device.enabled, the USB Connections settings do not display on the phone menu at Settings > Advanced > Administration Settings > USB Computer Connections.	No
features.cfg	feature.usb.host.enabled	1 (default) Enable the USB host port on the Polycom Trio 8800 and 8500 system. 0 - Disable the USB host port on the Polycom Trio 8800 and 8500 system. Use the host port for memory sticks, mouse, keyboards, and charging your devices.	No

HTTPD Web Server Parameters

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
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

Home Screen Parameters

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
	homeScreen.diagnostics.enable	0 (default) - A Diagnostics icon does not show on the Home screen. 1 - A Diagnostics icon shows on the Home screen to provide quick access to the Diagnostics menu.	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
features.cfg	homeScreen.doNotDisturb.enable	1 (default) - VVX 0 (default) - Polycom 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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
	homeScreen.present.enable	Control whether the Content icon displays on the Polycom Trio system Home screen when Content Sharing is enabled and the system is paired with Polycom Trio Visual+. 1 (default) 0	No
features.cfg	homeScreen.redial.enable	1 (default) - VVX 0 (default) - Polycom 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
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

Feature License Parameters

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

Chord Parameters

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	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
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

Message Waiting Parameters

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-interop.cfg	msg.bypassInstantMessage	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-interop.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

Ethernet Interface MTU Parameters

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 Polycom 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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

Presence Parameters

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
debug.cfg	pres.idleTimeoutoffHours.period	The number of minutes to wait while the phone is idle during off hours before showing the Away presence status. 15 (default) 1 - 600	
features.cfg	pres.idleTimeout.officeHours.enabled	1 (default) - Enables the office hours idle timeout feature 0 - Disables the office hours idle timeout feature	No
debug.cfg	pres.idleTimeout.officeHours.periods	The number of minutes to wait while the phone is idle during office hours before showing the Away presence status 15 (default) 1 - 600	

Provisioning Parameters

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.eula.accepted	0 (default) - Accept manually the product EULA agreement on Polycom Trio 8800 system at the initial startup. 1 - The EULA agreement is automatically accepted Polycom Trio 8800 system at the initial startup.	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

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

Configuration Request Parameters

The parameters listed in the following table configure the phone's behavior when a request for restart or reconfiguration is received.

Configuration Request Parameters

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

General Security Parameters

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

SRTP Parameters

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.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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

DHCP Parameters

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

Domain Name System (DNS) Parameters

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

Template	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

TCP Keep-Alive Parameters

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	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

File Transfer Parameters

Allows you to configure file transfers from the phone to the provisioning server.

File Transfer Parameters

Template	Parameter	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

User Preferences Parameters

Sets phone user preferences.

User Preferences Parameters

Template	Parameter	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

Template	Parameter	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 whether **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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
	up.formatPhoneNumbers	Enable or disable automatic number formatting. 1 (Default) 0	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.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
sip-interop.cfg	up.idleTimeout	Set the number of seconds that the phone is idle for before automatically leaving a menu and showing the idle display. During a call, the phone returns to the Call screen after the idle timeout. 40 seconds (default) 0 to 65535 seconds	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
features.cfg	up.numOfDisplayColumns	Sets the maximum number of columns the VVX 500/501, 600/601, or Polycom 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) Polycom Trio=3 (Default) 0 - Phones display one column.	Yes
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

Template	Parameter	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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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
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.	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

Upgrade Parameters

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

Template	Parameter	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 Parameters

The parameters in the table are supported on the VVX 500/501, VVX 600/601, and VVX 1500, and Polycom Trio solution.

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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.conf.profile	Sets the video resolution to large window in all layouts. 540p (default) 1080p 720p 360p 240p 180p	
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.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.mute.sendCannedVideo	1 (default) - The Polycom Trio system sends a custom image to the far end when you press Stop my video. 0 - The Polycom Trio system does not send a video to the far end when you press Stop my video and displays a no video graphic, by default.	

Video Codec Preference Parameters

The following table lists video codec parameters and specifies the video codec preferences for the Polycom Trio solution.

To disable codecs, set the value to 0. A value of 1 indicates the codec is the most preferred and has highest priority.

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
video.cfg	video.codecPref.H264.packetizationMode0	Sets the H.264 payload type when packetization mode is set to 0. 5 (default) 0 - 8	
video.cfg	video.codecPref.H264HP	Sets the H.264 High Profile video codec preference priority. 2 (default) 0 - 8	
video.cfg	video.codecPref.H264HP.packetizationMode0	Sets the H.264 high profile payload type when packetization mode is set to 0. 3 (default) 0 - 8	
	video.codecPref.H264SVC		No

Template	Parameter	Permitted Value	Change Causes Restart or Reboot
video.cfg	video.codecPref.Xdata	Sets the Remote Desktop Protocol (RDP) codec preference priority. 7 (default) 0 - 8 1 - Codec has highest priority.	
video.cfg	video.codecPref.XH264UC	Sets the Microsoft H.264 UC video codec preference priority. 1 (default) 0 - 8	
video.cfg	video.codecPref.XUlpFecUC	Sets the forward error correction (FEC) codec priority. 8 (default) 0 - 8	

Video Profile Parameters

These settings include 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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.H261.jitterBufferMax	The largest jitter buffer depth to be supported (in milliseconds). 2000ms (default) (video.profile.H261.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.H261.jitterBufferMin	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.cfg	video.profile.H261.jitterBufferShrink	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.payloadType	Specifies the RTP payload format type for H261 MIME type. 31 (default) 0 -127	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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.jitterBufferMax	The largest supported jitter buffer depth (in milliseconds). 2000ms (default) (video.profile.H263.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.H263.jitterBufferMin	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.H263.jitterBufferShrink	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.payloadType	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.cfg	video.profile.H2631998.annexF	0 (default) - Enables Annex F when negotiating video calls. 1 - Disables Annex F when negotiating video calls.	Yes
video.cfg	video.profile.H2631998.annexI	0 (default) - Enables Annex I when negotiating video calls. 1 - Disables Annex I when negotiating video calls.	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.H2631998.annexJ	0 (default) - Enables Annex J when negotiating video calls. 1 - Disables Annex J when negotiating video calls.	Yes
video.cfg	video.profile.H2631998.annexK	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.annexN	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.annexT	0 (default) - Enables Annex T when negotiating video calls. 1 - Disables Annex T when negotiating video calls.	Yes
video.cfg	video.profile.H2631998.CifMpi	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.cfg	video.profile.H2631998.jitterBufferMax	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.H2631998.jitterBufferMin	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.jitterBufferShrink	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.payloadType	Specifies the RTP payload format type for H263-1998/90000 MIME type. 96 (default) 96 to 127	Yes
video.cfg	video.profile.H2631998.QcifMpi	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.H2631998.SqcifMpi	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.jitterBufferMax	The largest jitter buffer depth to be supported (in milliseconds). 2000ms (default) (video.profile.H264.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.H264.jitterBufferMin	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.cfg	video.profile.H264.jitterBufferShrink	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.H264.payloadType	Specifies the RTP payload format type for H264/90000 MIME type. 109 (default) 96 to 127	Yes
video.cfg	video.profile.H264.payloadType.packetizationMode0	Sets the H.264 payload type when packetization mode is set to 0. 99 (default) 0 - 127	
video.cfg	video.profile.H264.payloadType.packetizationMode1	Sets the H.264 payload type when packetization mode is set to 1. 109 (default) 0 - 127	
video.cfg	video.profile.H264.profileLevel	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
video.cfg	video.profile.H264HP.jitterBufferMax	The largest jitter buffer depth to be supported (in milliseconds). 2000 (default) 533 - 2500 milliseconds This parameter should be set to the smallest possible value that supports the expected network jitter. Jitter above this size always causes packet loss.	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.H264HP.jitterBufferMin	The smallest jitter buffer depth (in milliseconds) that must be achieved before play out begins for the first time. 150 milliseconds (default) 33 - 1000 milliseconds 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.	
video.cfg	video.profile.H264HP.jitterBufferShrink	The absolute minimum duration time (in milliseconds) of RTP packet Rx with no packet loss between jitter buffer size shrinks. 70 milliseconds (default) 33 - 1000 milliseconds Use smaller values (33 ms) to minimize the delay from trusted networks. Use larger values (1000ms) to minimize packet loss on networks with large jitter (3000 ms).	
video.cfg	video.profile.H264HP.payloadType	Specifies the RTP payload format type for H264/90000 MIME type. 100 (default) 0 - 127	
video.cfg	video.profile.H264HP.payloadType.packetizationMode1	Sets the H.264 high profile payload type when packetization mode is set to 1. 100 (default) 0 - 127	
video.cfg	video.profile.H264HP.profileLevel	Specifies the highest profile level within the baseline profile supported in video calls. 4.1 (default) String (1 - 5 characters)	
video.cfg	video.profile.H264M.payloadType.packetizationMode0	Sets the H.264 high profile payload type when packetization mode is set to 0. 113 (default) 0 - 127	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.Xdata.payloadType	Specifies the payload type to use in SDP negotiations of the payload used for Skype for Business desktop content sharing. 127 (default) 0 - 127	
video.cfg	video.profile.XH264UC.jitterBufferMax	The largest supported jitter buffer depth. 2000 (default) 533 - 2500 milliseconds Jitter above 2500ms always causes packet loss. This parameter should be set to the smallest possible value that supports the network jitter.	
video.cfg	video.profile.XH264UC.jitterBufferMin	The smallest jitter buffer depth that must be achieved before playout begins for the first time. 150 (default) 33 - 1000 milliseconds 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.	
video.cfg	video.profile.XH264UC.jitterBufferShrink	Specifies the minimum duration in milliseconds of Real-time Transport Protocol (RTP) packet Rx, with no packet loss to trigger jitter buffer size shrinks. 70 (default) 33 - 1000 Use smaller values (1000 ms) to minimize the delay on known good networks.	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.XH264UC.mstMode	Specifies the multi-session transmission packetization mode. NI-TC (default) String The value of NI-TC identifies non-interleaved combined timestamp and CS-DON mode. This value should not be modified for interoperation with other Skype for Business devices.	
video.cfg	video.profile.XH264UC.payloadType	Specifies the RTP payload format type for H.264 MIME type. 122 (default) 0 - 127	No
video.cfg	video.profile.XUlpFecUC.alwaysOn	1 (default) - Enable Forward Error Correction during video calls even when it is not needed. 0 - Disable Forward Error Correction.	No
video.cfg	video.profile.XUlpFecUC.debug.rxDropBurst	1 (default) 1 - 100	
video.cfg	video.profile.XUlpFecUC.debug.rxDropOnlyLayer0	1 (default) 0 or 1	
video.cfg	video.profile.XUlpFecUC.debug.rxDropRate	0 (default) 0 - 40000	
video.cfg	video.profile.XUlpFecUC.debug.txDropBurst	1 (default) 1 - 100	
video.cfg	video.profile.XUlpFecUC.debug.txDropRate	0 (default) 0 - 40000	

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
video.cfg	video.profile.XUlpFecUC.noLossTurnOffTimeout	300 (default) 10 - 7200	
video.cfg	video.profile.XUlpFecUC.payloadType	123 (default) 0 - 127	
video.cfg	video.profile.XUlpFecUC.rxEnabled	1 (default) 0 or 1	
video.cfg	video.profile.XUlpFecUC.txEnabled	1 (default) 0 or 1	
video.cfg	video.simpleJB.enable	1 (default) 0 or 1	
video.cfg	video.simpleJB.lipSyncDelayMs	0 (default) 0 -250 ms	
video.cfg	video.simpleJB.timeoutMs	100 ms (default) 0 - 250 ms	
video.cfg	video.rtcpbandwidthdetect.enable	0 (default) 1 - Polycom Trio 8800 uses an estimated bandwidth value from the RTCP message to control Tx/Rx video bps.	

Voice Parameters

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

Acoustic Echo Suppression (AES) Parameters

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
techsupport.cfg	voice.aes.hs.enable	1 (default) - Enables the handset AES function. 0 - Disables the handset AES function.	No

Comfort Noise Parameters

Use these parameters to configure the addition and volume of comfort noise during conferences.

Comfort Noise Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
debug.cfg	voice.cn.hf.enable	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.attn	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
debug.cfg	voice.cn.hd.attn	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.enable	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.cn.hs.attn	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
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

Voice Jitter Buffer Parameters

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
site.cfg	voice.rxQos.mr.avgJitter	Specify the average expected jitter for audio streams in miliiseconds (ms). Value must be a multiple of 10ms. 10 ms (default) 0 - 200 ms	Yes
site.cfg	voice.rxQos.mr.maxJitter	Specify the maximum expected jitter for audio streams in milliseconds (ms). Value must be at least twice the value of voice.rxQos.mr.avgJitter and a multiple of 10 ms. 30 ms (default) 20 - 500 ms	Yes

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
site.cfg	voice.rxQoS.ptt.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.ptt.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.jitterBuffer.* 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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
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

Session Description Protocol (SDP) Parameters

This table describes Session Description Protocol configuration parameters.

Session Description Protocol (SDP) Parameters

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SDP.answer.useLocalPreferences	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.	No
	voIpProt.SDP.answer.useLocalPreferences.video	Allows you to reset the parameter voIpProt.SDP.answer.useLocalPreferences to the default 0 for audio only. 1(default) - The phone uses its own preference list instead of the preference list in the offer when deciding which video codec to use. 0 - The phone's use of its own preference list is disabled.	No
sip-interop.cfg	voIpProt.SDP.early.answerOrOffer	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

Template	Parameter	Permitted Values	Change Causes Restart or Reboot
sip-interop.cfg	voIpProt.SDP.offer.iLBC.13_33kbps.includeMode	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.	No
	voIpProt.SDP.useLegacyPayloadTypeNegotiation	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-interop.cfg	voIpProt.SDP.offer.rtcpVideoCodecControl	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 I-Frames section. 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

Web Configuration Utility Parameters

The parameters listed 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.cfg	**webutility.language.plcmServerUrl**	Specifies the download location of the translated language files for the Web Configuration Utility. http://downloads.polycom.com/voice/software/languages/ (default) URL	No

XML Streaming Protocol Parameters

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