



ADMINISTRATOR GUIDE

2.0 | May 2019 | 3725-85854-001A

Polycom® G7500



Copyright© 2019, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries.



All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

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 OpenSourceVideo@polycom.com (for video products) or OpenSourceVoice@polycom.com (for voice products).

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 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.....	6
Getting Help.....	6
The Polycom Community.....	6
Related Documentation.....	6
Documentation Feedback.....	6
Getting Started.....	7
Polycom G7500 Overview.....	7
Powering the System On and Off.....	8
Navigating the System.....	8
Access the System Web Interface.....	8
Place a Call from the System Web Interface.....	8
End a Content Session from the System Web Interface.....	9
Setting Up the System.....	10
System Back Panel Ports.....	10
LED Status Indicators for the G7500 System.....	11
Complete System Setup.....	12
Managing Peripheral Devices.....	12
Pairing IP Peripheral Devices to the System.....	12
IP Microphones.....	14
Polycom Microphone IP Adapter.....	16
Polycom Bluetooth Remote Control.....	18
Configuring General Settings.....	21
Name the System and Room.....	21
Provide Contact Information.....	21
Set the Date and Time.....	22
Set the System Location.....	22
Set the Local Interface Language.....	23
Configure Sleep Settings.....	23
Send Usage Data to Polycom.....	23
Using a Provisioning Service.....	25
Register the System with a Provisioning Service.....	25
Download a Template Configuration File.....	26

Configuring Network Settings.....	27
Configuring Wired LAN Settings.....	27
Obtain IPv4 Address Settings Automatically.....	27
Configure IPv4 Address Settings Manually.....	27
Configure DNS Settings Manually.....	28
Configure Wired LAN Options.....	28
Configure Wi-Fi Settings.....	31
Configure Network Quality Settings.....	32
Configure H.323 Settings.....	34
Configure SIP Settings.....	36
Enable Point-to-Point Call Escalation to a RealPresence DMA Conference Call.....	39
Wireless Devices.....	40
Securing the System.....	41
Managing System Access.....	41
Local Accounts.....	41
Enable External Authentication.....	44
Configure System Access Settings.....	45
Enable Command-Line API Access Over SSH.....	46
Enable Command-Line API Access Over Telnet.....	46
Disable Command-Line API Access.....	46
Configure the System Web Interface Port Lock.....	47
Configure the SSH Port Lock.....	47
Locking the Telnet Port.....	48
Configure Serial Port Settings.....	48
Disable USB 3.0 Ports.....	49
PKI Certificates.....	49
Create a Certificate Signing Request.....	50
Configure Certificate Validation Settings.....	51
Install a Certificate.....	52
View a Certificate.....	52
Delete a Certificate.....	52
Certificate Revocation.....	53
Disable the Security Code.....	54
Limit or Disable the Ability to Save Content.....	55
Encryption.....	55
Configure Call Encryption.....	55
Configure Minimum TLS.....	56
H.460 Firewall/NAT Traversal.....	56
Configure the System for H.460 Firewall/NAT Traversal.....	56

Web Proxies.....	58
View Connections to the System.....	60
Port Usage.....	61
Configuring Call Settings.....	65
Configure Call Settings.....	65
Configure Dialing Options.....	66
Set Call Answering Mode.....	67
Set Preferred Call Speeds.....	67
Configure the Recent Calls List.....	68
Clear Recent Calls.....	68
Configuring Audio Settings.....	69
Configure General Audio Settings.....	69
Audio Input.....	70
Configure IP Microphones.....	71
Configuring the Microphone Adapter.....	71
Polycom Acoustic Fence.....	71
Configure 3.5 mm and HDMI Audio Input.....	73
Audio Output.....	74
Configure Audio Output Settings.....	74
Using 3.5 mm Audio Output.....	75
Audio I/O Specifications.....	75
Configuring Video and Camera Settings.....	76
HDMI Connections.....	76
Configure Monitor Settings.....	77
Configure a Touch Monitor.....	78
Configure Camera Settings.....	79
Configure Video Input Settings.....	80
Video Codec Capabilities.....	84
H.265 High Efficiency Video Coding.....	84
H.264 Advanced Video Coding.....	85
Setting Up a Directory.....	87
Register with the Polycom Global Directory Server.....	87
Register with an LDAP Directory Server.....	87
Managing Contacts and Favorites.....	89
Registering with a Calendaring Service.....	90

Configure a Calendaring Service.....	90
Sharing Content.....	93
Customizing the Local Interface.....	94
Change the Home Screen Background Image.....	94
Restore the Default Background Image.....	94
Customize the Address Bar.....	94
Display Meetings or Favorites on the Home Screen.....	95
Configure Dual Monitor Display Settings.....	95
System Maintenance.....	97
Activating System Features.....	97
Unlock System Settings.....	98
Updating Software.....	98
Updating Software in the System Web Interface.....	99
Update Software with a USB Flash Drive.....	101
Update Polycom HDCI Cameras.....	101
Downgrading Software.....	102
Restart the System.....	102
Reset System Settings.....	103
Factory Restore the System.....	103
Factory Restore a Table Microphone.....	104
Factory Restore a Ceiling Microphone.....	104
Factory Restore a Microphone Adapter.....	106
SNMP Reporting.....	106
Configure SNMP.....	107
Download MIBs.....	109
Troubleshooting.....	110
Checking System Status.....	110
Paired IP Peripheral Device is Disconnected.....	111
View Call Statistics.....	112
LED Status Indicators for the System LAN Ports.....	112
Check Provisioning Results.....	113
Logs.....	113
Consolidated System and Peripheral Device Logs.....	113
Configure Log Preferences.....	114
Configure Log Level.....	115
Download Logs.....	115

Transfer Logs to a USB Flash Drive.....	116
Configure Remote Logging.....	116
Sample Log File.....	117
Audio Tests.....	118
Fix Polycom Acoustic Fence Issues.....	119
Issues When the System is Sleeping or Waking.....	119
Test the Call Experience.....	120
Test Connection with Another System.....	120
Run a Trace Route.....	120
LDAP Directory Server Ignores the Minimum TLS Version Setting.....	120
Checking the Web Proxy Configuration.....	121

Before You Begin

Topics:

- [Getting Help](#)

This guide helps you understand how to configure and manage your Polycom G7500 system.

This guide covers the following products:

- Polycom G7500 system (Model: P011)
- Polycom Microphone IP Adapter (Model: P012)
- Polycom IP Table Microphone (Model: P013)
- Polycom IP Ceiling Microphone (Model: P014)

Getting Help

For information about installing, configuring, using, and administering Polycom products, see **Documents & Software** at [Polycom Support](#).

The Polycom Community

The [Polycom Community](#) gives you access to the latest developer and support information.

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

Related Documentation

In addition to this guide, the following documentation further describes Polycom endpoints and peripherals used in video conferencing. The Release Notes might include known issues or limitations related to interoperability with Polycom endpoints.

For more information, see the [Polycom Documentation Library](#) or [Polycom Support](#).

- *Polycom G7500 User Guide*
- *Polycom G7500 Release Notes*
- *Polycom G7500 Configuration Parameter Reference Guide*
- *Polycom G7500 Command-Line API Reference Guide*

Documentation Feedback

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

You can email [Documentation Feedback](#) for any queries or suggestions related to this documentation.

Getting Started

Topics:

- [Polycom G7500 Overview](#)
- [Powering the System On and Off](#)
- [Navigating the System](#)

The Polycom G7500 system provides video-conferencing capabilities and collaboration tools for any size meeting space or room.

Polycom G7500 Overview

The Polycom G7500 system is an all-in-one video conferencing and content-sharing solution.

The G7500 system provides the following features and capabilities:

- Placing and joining video calls
- Viewing and joining scheduled calendar meetings
- Managing contacts, call lists, and directories
- Creating a favorites list
- Sharing content
- Collaborating by electronic whiteboarding

Related Links

[Video Codec Capabilities](#) on page 84

Administrator Features and Capabilities

The G7500 system provides the following features and capabilities:

- Scalability for various room sizes
- Remote access for managing standalone systems
- Provisioning with Polycom RealPresence Resource Manager to support single system, small business, and large multisite enterprise deployments
- SNMP reporting and remote logging
- Industry-standard security techniques, including 802.1X authentication
- Polycom platform on-premises infrastructure and management solutions
- Standards-based video conferencing
- Customizable home screen and monitor layouts

Powering the System On and Off

The G7500 system turns on when you plug it into a power source. The system doesn't have a power button, so you must unplug the power cable to turn it off.

Don't power off the system during maintenance activities (for example, while a software update is in progress).

Related Links

[Restart the System](#) on page 102

Navigating the System

You can navigate the G7500 system using the system web interface.

Access the System Web Interface

Access the G7500 system web interface to perform administrative tasks.

The system web interface enables you to do the following actions:

- Finish setting up your system.
- Remotely configure and manage your system. Unlike the local interface, you can configure every setting through the system web interface.
- Control certain user functions of the system (such as placing calls and ending content sessions).
- Manage contacts.

Procedure

1. Enter the system IP address in a browser.
When setting up your system, the onscreen instructions display the IP address to use.
2. Enter the user name (the default is `admin`).
3. Enter the password (the default is the last six characters of your system's serial number).

Related Links

[Complete System Setup](#) on page 12

Place a Call from the System Web Interface

The G7500 system web interface gives you many of the same calling features and controls that are in the local interface.

You can also place video and audio-only calls directly from the **Dashboard**.

Procedure

1. In the system web interface, go to **Place a Call**.
2. Do one of the following:
 - Select **Dial** to manually dial a number or name.
 - Select **Contacts** to search local and directory contacts to call.
 - Select **Favorites** to search contacts marked as Favorites.
 - Select **Recent** to select a number or name you've called in the past.

End a Content Session from the System Web Interface

When you end a sharing session, the system stops live content and deletes blackboards and whiteboards.

Procedure

1. In the system web interface, go to **Active Session**.
2. Select **End Session** (⊗).

A message displays informing you that the session is ending.

Related Links

[Sharing Content](#) on page 93

Setting Up the System

Topics:

- [System Back Panel Ports](#)
- [LED Status Indicators for the G7500 System](#)
- [Complete System Setup](#)
- [Managing Peripheral Devices](#)

See the *Polycom G7500 Setup Sheet* for information on connecting your G7500 system and its peripheral devices, including cameras, monitors, and microphones.

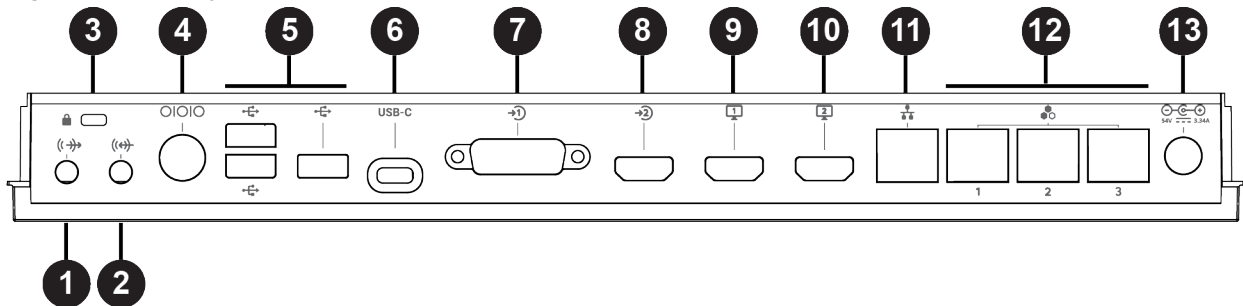
Also see the following documents for more setup information:

- *Polycom G7500 Room Preparation Guide*
- *Polycom G7500 Mounting Kit*
- *Polycom Microphone IP Adapter Setup Sheet*
- *Polycom IP Ceiling Microphone Array Setup Sheet*

System Back Panel Ports

The following illustration and table explain the ports on the back panel of your G7500 system.

Figure 1: G7500 System Back Panel Ports



G7500 System Back Panel Port Descriptions

Ref. Number	Port Description
1	3.5 mm audio line out
2	3.5 mm audio line in
3	Security lock
4	Mini-DIN/RS-232 serial port
5	USB 3.0 port (host)
6	USB-C port (dual-role port provides power only)

Ref. Number	Port Description
7	HDCI input for Polycom cameras
8	HDMI input for sharing content (for example, from a laptop)
9	HDMI output for the primary monitor
10	HDMI output for the secondary monitor
11	Primary LAN connection for the system
12	Link-local network (LLN) connections for IP-based peripheral devices
13	Power

Related Links

[HDMI Connections](#) on page 76

Related Links

[Specify the Primary and Fence Microphones](#) on page 72

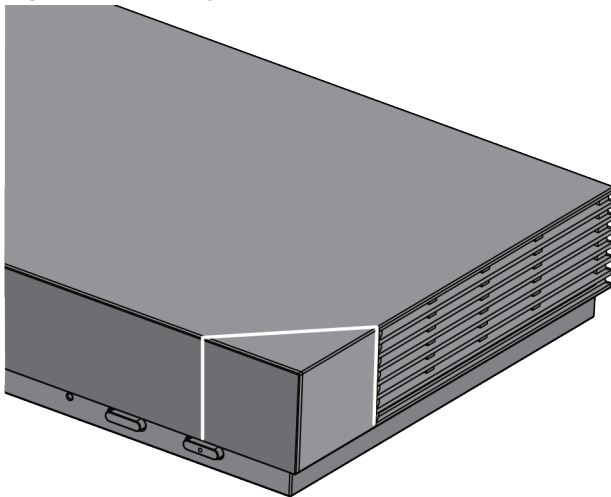
Related Links

[LED Status Indicators for the System LAN Ports](#) on page 112

LED Status Indicators for the G7500 System

Use the LED on the front right corner of the codec to get information on the state of your G7500 system.

Figure 2: G7500 System LED Location



G7500 System LED Status Indicators

Indicator	Status
Blinking white	Powering on

Indicator	Status
Solid white	Working normally
Blinking amber	Update in progress
Solid amber	Sleeping
Blinking red	Error preventing normal operation

Related Links

[Factory Restore the System](#) on page 103

Complete System Setup

You can set up your G7500 system manually or provision it.

Note: Make sure to configure your provisioning server (for example, RealPresence Resource Manager) ahead of time so that it recognizes and works with your endpoint.

Procedure

1. Log in to the system web interface.
2. Follow the onscreen instructions.

You only see these instructions when you set up your system for the first time or after you reset the system and delete all settings.

You can start using the system.

Related Links

[Using a Provisioning Service](#) on page 25

Related Links

[Access the System Web Interface](#) on page 8

Managing Peripheral Devices

You can manage and monitor the peripheral devices connected to your G7500 system in the system web interface.

Pairing IP Peripheral Devices to the System

You must pair IP peripheral devices you use with your G7500 system.

These peripheral devices include:

- Polycom IP Table Microphone
- Polycom IP Ceiling Microphone
- Polycom Microphone IP Adapter

Automatic pairing is enabled by default and recommended in most situations. You can also manually pair and unpair these peripheral devices in the system web interface.

Pair an IP Peripheral Device Automatically

IP peripheral devices automatically pair with your G7500 system by default when you connect them to the system. For example, when you connect a Polycom IP Table Microphone, it pairs automatically and is ready to use.

Procedure

- » Connect the peripheral device to an **LLN port**  on the back of your system.

If paired successfully, the device displays under **Paired Devices** with a **Connected** status. If a device shows a **Disconnected** status, this indicates that pairing wasn't successful.

Disable Automatic Pairing

You can disable automatic pairing for your G7500 system.

If you disable automatic pairing, you must connect and manually pair a peripheral device in the system web interface to use it.


Procedure

1. In the system web interface, go to **General Settings > Device Management**.
2. Clear the **Enable New Device Auto-Pairing** check box to disable automatic pairing.

Pair an IP Peripheral Device Manually

If you disable automatic pairing, you must manually pair an IP peripheral device to use it with your G7500 system.

Procedure

1. Connect the peripheral device to an **LLN port**  on the back of your system.
2. In the system web interface, go to **General Settings > Device Management**.
3. Under **Available Devices**, find the device and select **Pair**.

If paired successfully, the device displays under **Paired Devices** with a **Connected** status. If a device shows a **Disconnected** status, this indicates that pairing wasn't successful.

Unpair an IP Peripheral Device

If you don't want to use an IP peripheral device with your G7500 system anymore, unpair it in the system web interface.

Don't unpair peripheral devices you plan to use with your system again. For example, if you move your entire system to another room, just disconnect the devices and reconnect them in the new location.

Note: If you manually unpair a peripheral device, it won't automatically pair again with this system.

Procedure

1. In the system web interface, go to **General Settings > Device Management**.
2. Under **Paired Devices**, find the device and select **Unpair**.

The unpaired device moves from **Paired Devices** to **Available Devices** (which shows discovered devices you can pair with the system).

Related Links

[Move a Microphone Adapter to Another Location](#) on page 18

IP Microphones

You can use a combination of IP-based Polycom table and ceiling microphones with your G7500 system. These microphones also support Polycom Acoustic Fence technology.

You can connect up to three of the following microphones directly to your system:

- Polycom IP Table Microphone
- Polycom IP Ceiling Microphone

Related Links

[Polycom Acoustic Fence](#) on page 71

Related Links

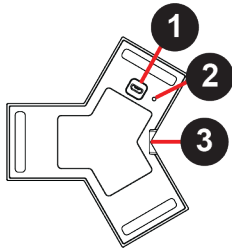
[Factory Restore a Table Microphone](#) on page 104

[Factory Restore a Ceiling Microphone](#) on page 104

Polycom IP Table Microphone Ports

The following illustration and table explain the ports on the table microphone.

Figure 3: Polycom IP Table Microphone Ports (bottom view)



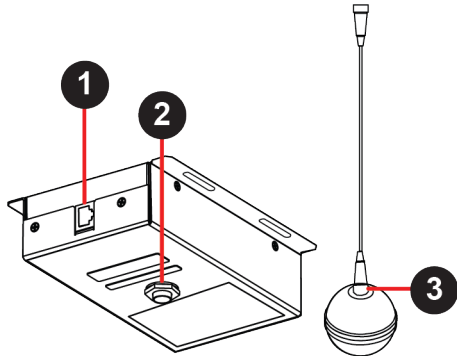
Polycom IP Table Microphone Port Descriptions

Ref. Number	Port Description
1	USB-C debugging port
2	Factory restore pinhole
3	Link-local network (LLN) connection

Polycom IP Ceiling Microphone Ports

The following illustration and table explain the ports on the ceiling microphone.

Figure 4: Polycom IP Ceiling Microphone Ports



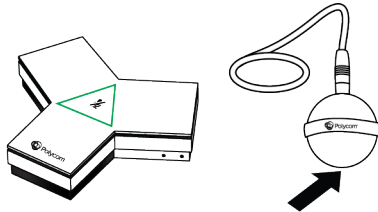
Polycom IP Table Microphone Port Descriptions

Ref. Number	Port Description
1	Link-local network (LLN) connection
2	Microphone cable connector
3	Microphone cable connector

LED Status Indicators for IP Microphones

Use the LED on the IP table and ceiling microphones to get information on the state of each device.

Figure 5: Polycom IP Table Microphone and Polycom IP Ceiling Microphone LED Locations



IP Microphone LED Status Indicators

Indicator	Status
Solid then blinking white	Powering on
Solid red	Muted microphone To avoid distraction, the ceiling microphone doesn't display red when muted.
Solid green	In a call To avoid distraction, the ceiling microphone doesn't display green in a call.

Indicator	Status
Alternating blinking and solid amber	Update in progress
Blinking amber	Factory restore in progress
Blinking blue	Ready to pair
Solid blue	Paired successfully

Polycom Microphone IP Adapter

The Polycom Microphone IP Adapter lets you connect non-IP Polycom audio devices with your G7500 system. For example, if your Polycom microphone uses a Walta-Walta cable, you can connect it to your system through the microphone adapter.

You can use the following non-IP microphones and audio accessories with your G7500 system:

- Polycom table microphones
- Polycom ceiling microphones
- Polycom SoundStructure accessory

Note: You can't use the microphone adapter with IP microphones connected to your system.

Related Links

[Configuring the Microphone Adapter](#) on page 71

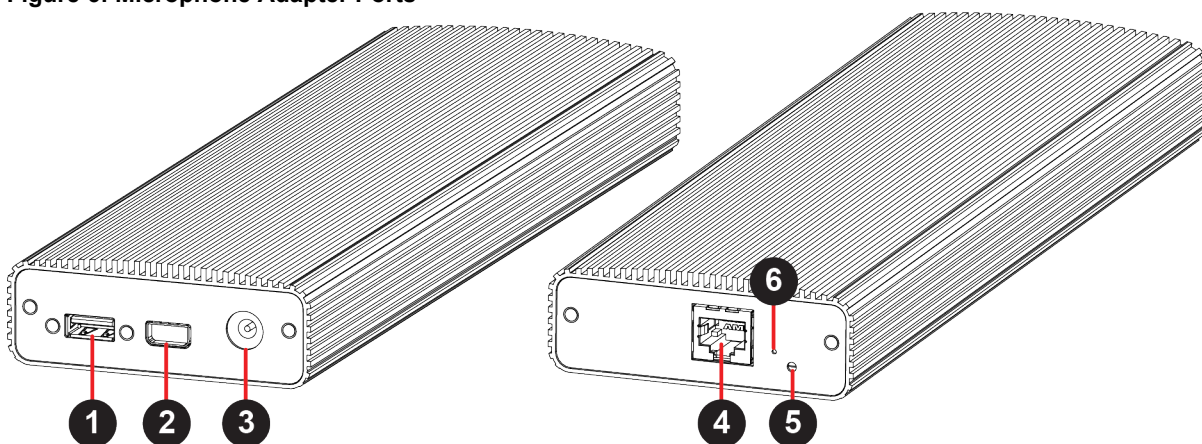
Related Links

[Factory Restore a Microphone Adapter](#) on page 106

Microphone Adapter Ports

The following illustration and table explain the ports on the microphone adapter.

Figure 6: Microphone Adapter Ports



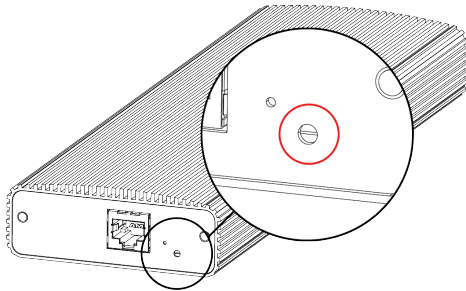
Microphone Adapter Port Descriptions

Ref. Number	Port Description
1	USB 2.0 debugging port
2	Polycom microphone Walta-Walta connector
3	Power
4	Link-local network (LLN) connection
5	LED status indicator
6	Factory reset pinhole

LED Status Indicators for the Microphone Adapter

Use the LED to get information on the state of your microphone adapter.

Figure 7: Polycom Microphone IP Adapter LED Location



Microphone Adapter LED Status Indicators

Indicator	Status
Blinking white	Powering on
Solid white	On
Blinking blue	Ready to pair
Solid blue	Paired successfully
Blinking green and blue	Update in progress Factory restore in progress

Powering the Microphone Adapter On and Off

When plugged in to a power source, the microphone adapter is on. The system doesn't have a power button, so you must unplug the power cable to turn it off.

Don't power off the system during maintenance activities (for example, while a software update is in progress).

Connecting Microphones to the Microphone Adapter

To connect a non-IP Polycom microphone to the microphone adapter, use a RealPresence Group Series microphone array Walta-Walta cable. You can then daisy chain up to three more microphones to the one directly connected to the adapter.

For more information, see the *Polycom Microphone IP Adapter Setup Sheet*.

Move a Microphone Adapter to Another Location

You might need to move your microphone adapter from a G7500 system in one room to a G7500 system in another room.

Procedure

1. In the system web interface, unpair the microphone adapter from the system.
2. Move the microphone adapter to the new location.
3. Use the system web interface to pair the microphone adapter to the new system.

Related Links

[Unpair an IP Peripheral Device](#) on page 13

Polycom Bluetooth Remote Control

Your Polycom Bluetooth Remote Control is ready to use with your G7500 system without any extra setup.

Use the system web interface to do the following:

- Configure a remote control's button behavior
- Pair and unpair a remote control
- View the remote control name, pairing status, and battery level

Related Links

[Disable Wireless Options](#) on page 40

Configure Remote Control Behavior

You can customize how the remote control paired to your G7500 system behaves.

Procedure

1. In the system web interface, go to **General Settings > System Settings**.
2. Configure the following settings:

Setting	Description
Keypad Audio Confirmation	Specifies whether to play a voice confirmation of numbers selected with the remote control or keypad.
Numeric Keypad Function while in a Call	Specifies whether pressing number buttons on the remote control or keypad moves the camera to presets or generates touch tones (DTMF tones). If you set this option to Presets , you can generate DTMF tones by pressing the # key on the remote control while in a call.

Setting	Description
#/@ Button function	<p>Specifies the behavior of the # button on the remote control.</p> <ul style="list-style-type: none"> ▪ #, then @: Pressing the # button once displays the hash symbol. Pressing the # button twice quickly displays the @ symbol. ▪ @, then #: Pressing the # button once displays the @ symbol. Pressing the # button twice quickly displays the # symbol.
*./ Button function	<p>Specifies the behavior of the * button on the remote control:</p> <ul style="list-style-type: none"> ▪ * then .: Pressing the * button once displays the * symbol. Pressing the * button twice quickly displays a period. ▪ . then *: Pressing the * button once displays a period. Pressing the * button twice quickly displays the * symbol.

3. Select **Save**.

Unpair a Remote Control

You can unpair a remote control if you no longer want to use it with your G7500 system.

Procedure

1. In the system web interface, go to **Remote Control**.
2. Select **Unpair Remote**.


The remote control unpairs.

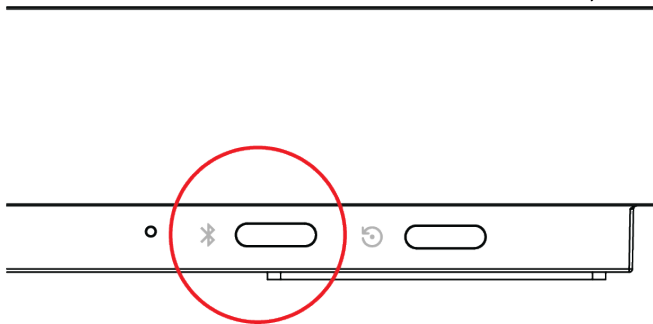
Pair a Remote Control

Out of the box, your remote control is paired with the G7500 system, so no setup is required. To use a different remote control, you must pair it with the system.

The system doesn't support multiple remote controls. You can pair only one at a time.

Procedure

1. Do one of the following:
 - On the front of the system, press the **Bluetooth**  button.



- In the system web interface, go to **General Settings > Remote Control** and select **Start Discovery Mode**.
2. Follow the instructions on the pairing screen.
The screen displays either a successful or unsuccessful pairing notification.
 3. Depending on the pairing result, do one of the following:
 - **Successful pairing:** The remote control is ready to use. You can view the remote control name, battery level, and status of the device in the system web interface.
 - **Unsuccessful pairing:** Try the following solutions:
 - Remove the batteries from the remote control and reinsert after five seconds.
 - Move your remote control closer to the system than other remote controls and try to pair again.

Configuring General Settings

Topics:

- [Name the System and Room](#)
- [Provide Contact Information](#)
- [Set the Date and Time](#)
- [Set the System Location](#)
- [Set the Local Interface Language](#)
- [Configure Sleep Settings](#)
- [Send Usage Data to Polycom](#)

General settings include your G7500 system name, location, language, and sleep preferences.

Name the System and Room

Name your G7500 system and assign it a room name.

The room name displays on call participants' screens.

Procedure

1. In the system web interface, go to **General Settings > System Settings**.
2. Enter the **Device Name**, **Room Name**, or both.
The system supports double-byte characters.
3. Select **Save**.

Provide Contact Information

Enter contact information for your G7500 system so that users know whom to call when they need assistance.

Procedure

1. In the system web interface, go to **General Settings > My Information**.
2. Go to **Contact Information**.
3. Configure the following settings:
 - **Contact Person**
 - **Contact Number**
 - **Contact Email**
 - **Contact Fax**
 - **Tech Support:** Specifies a second contact in case someone needs additional support.
 - **City**
 - **State/Province**

- **Country**
4. Select **Save**.

Set the Date and Time

Change the date and time settings in the G7500 system web interface.

Procedure

1. In the system web interface, go to **General Settings**.
2. Select **Date and Time**.
3. Configure the following settings (your changes save automatically):

Setting	Description
Date Format	Specifies how the date displays.
Time Format	Specifies how the time displays.
Auto Adjust for Daylight Saving Time	When enabled, the system clock automatically adjusts for daylight saving time.
Time Zone	Specifies the time difference between GMT and your location.
Time Server	Specifies if you want to automatically or manually configure the system to use a time server. You can also select Off to manually enter the date and time.
Primary Time Server Address	Specifies the address of the primary time server your system uses when you set Time Server to Manual .
Secondary Time Server Address	Specifies the address of the time server your system uses when the Primary Time Server Address doesn't respond. This is an optional field.
Current Date and Current Time	If you set Time Server to Manual or Auto , the system doesn't display these settings. If you set Time Server to Off , you can configure Current Date and Current Time .

Set the System Location

Specify the country and country code where the G7500 system is located.

Procedure

1. In the system web interface, go to **General Settings > My Information**.
2. Go to **Location**.
3. Configure the following settings (your changes save automatically):

Setting	Description
Country	Specifies the country where the system is located. Changing the country automatically adjusts the country code associated with your system.
Country Code	Displays the country code associated with the system location.

Set the Local Interface Language

Change the language that users see on the G7500 system local interface.

Procedure

1. In the system web interface, go to **General Settings**.
2. Select **System Language** and choose a language.

Configure Sleep Settings

Configure when you want your device to go to sleep after a period of inactivity. Sleep mode can help prevent monitor burn-in.

Procedure

1. In the system web interface, go to **General Settings > System Settings**.
2. For **Display**, select whether you want to display a black screen or no signal message.
3. For **Time Before System Goes to Sleep**, select how long the device can be idle before it goes to sleep.
4. Select the **Enable Mic Mute in Sleep Mode** check box to mute your microphones while the system is asleep.
5. Select **Save**.

Related Links

[Issues When the System is Sleeping or Waking](#) on page 119

[Configure General Audio Settings](#) on page 69

[Configure Camera Settings](#) on page 79

Send Usage Data to Polycom

You can help Polycom improve its products and services by allowing the collection of usage data from your G7500 system.

With your agreement, the system sends the following information to Polycom Cloud Services and the Device Analytics service:

- Basic device information, including hardware and software versions
- Basic device configuration data
- Data and statistics related to device or feature usage
- Device health data, including CPU and memory usage

Procedure

1. In the system web interface, go to **Servers > Cloud > Preferences**.
2. Click the link to read the “Terms and Conditions”.
3. Select the check box to agree to the data collection.

Using a Provisioning Service

Topics:

- [Register the System with a Provisioning Service](#)
- [Download a Template Configuration File](#)

You can use a provisioning service, such as Polycom RealPresence Resource Manager, to perform the following actions with your G7500 system:

- Automatically provision settings
- Automatically update software

Remember the following when you register your system to a provisioning service:

- Provisioned settings are read-only in the system web interface. Settings that are dependent on provisioned values are read-only or unavailable.
- The system automatically checks for and runs software updates every time it restarts and at an interval set by the service.
- If a registered system fails to detect the service when it restarts or checks for updates, an alert displays on **System Status**.
- If the system loses registration with the service, it continues to use the most recent configuration it received.

Note: To maintain call connection, you can't configure provisioning settings during a call.

For a list of configuration parameters, see the [Polycom G7500 Configuration Parameters Reference Guide](#).

Related Links

[Updating Software](#) on page 98

[PKI Certificates](#) on page 49

Related Links

[Complete System Setup](#) on page 12

[Choose How to Get Software Updates](#) on page 99

Register the System with a Provisioning Service

Before you can provision a G7500 system, you must manually register it with a provisioning service.

Note: Make sure to configure your provisioning server (for example, RealPresence Resource Manager) ahead of time so that it recognizes and works with your endpoint.

Procedure

1. In the system web interface, go to **Servers > Provisioning Server**.
2. Select **Enable Provisioning**.
3. Select **Load Discovered Information**.

The registration fields update automatically if your system detects a provisioning server.

- Optional: If your system didn't detect a provisioning server, complete the following fields (contact your network administrator for help):

Setting	Description
Server Type	Specifies the type of provisioning service (for example, RealPresence Resource Manager).
Server Address	Address of the system running the provisioning service.
Domain Name	Domain for registering with the provisioning service.
User Name	User ID for registering with the provisioning service.
Password	Password for registering with the provisioning service.

- Select **Save**.
- Verify that **Registration Status** changes from **Pending** to **Registered**.

It might take a minute or two for the status to change.

For information on how to provision your system with RealPresence Resource Manager, see the [Polycom RealPresence Resource Manager System Operations Guide](#).

Related Links

[Check Provisioning Results](#) on page 113

Download a Template Configuration File

Template configuration files show how parameters are set on your G7500 system. You can use this template to modify parameters and import the changes to your provisioning server.

If you're provisioning your system with a RealPresence Resource Manager system, you can use the template to create a UC endpoint configuration profile to associate with your system(s). For more information, see the [Polycom RealPresence Resource Manager System Operations Guide](#).

Note: Not all parameters that you can provision to your system are in the downloaded template. For example, you don't see password-related parameters due to security reasons.

Procedure

- In the system web interface, go to **Servers > Provisioning Server**.
- Select **Download Profile Template**.

The template saves to your local device as a `.cfg` file.

Configuring Network Settings

Topics:

- [Configuring Wired LAN Settings](#)
- [Configure Wi-Fi Settings](#)
- [Configure Network Quality Settings](#)
- [Configure H.323 Settings](#)
- [Configure SIP Settings](#)
- [Enable Point-to-Point Call Escalation to a RealPresence DMA Conference Call](#)
- [Wireless Devices](#)

Network settings include the G7500 system primary (wired LAN) and secondary (Wi-Fi) network configurations. You also can register your system with SIP and H.323 for calling.

Configuring Wired LAN Settings

You can set the wired LAN properties for your G7500 system.

Related Links

[LED Status Indicators for the System LAN Ports](#) on page 112

Obtain IPv4 Address Settings Automatically

You can configure the G7500 system to obtain its IPv4 addresses automatically.

You must have a DHCP server deployed in your environment.

Procedure

1. In the system web interface, go to **Network > Primary Network > IP Addresses**.
2. For **IP Address**, select **Obtain IP address automatically**.
Some of your IP address settings populate automatically and are read-only.
3. Select **Save**.

Configure IPv4 Address Settings Manually

You can configure the IPv4 settings for your G7500 system.

Procedure

1. In the system web interface, go to **Network > Primary Network > IP Addresses**.
2. For **IP Address**, select **Enter IP address manually**.
3. Configure the following settings:

Setting	Description
Your IP Address is	Specifies the system IP address.

Setting	Description
Subnet Mask	Specifies the subnet mask assigned to your system.
Default Gateway	Specifies the default gateway assigned to your system.

4. Select **Save**.

Configure DNS Settings Manually

You can manually configure the DNS server settings for your G7500 system.

If your system gets its IP address automatically, you can't configure these settings. They display as read-only.

Procedure

1. In the system web interface, go to **Network > DNS**.
2. Enter your DNS server address (you can enter up to four addresses).
3. Select **Save**.

Configure Wired LAN Options

You can configure LAN properties for your G7500 system in the local interface or the system web interface.

Procedure

1. In the system web interface, go to **Network > Primary Network > LAN Options**.
2. Configure the following settings:

Setting	Description
Host Name	Indicates your system name. If the system discovers a valid name during setup or a software installation, the system automatically creates the host name. However, if the system finds an invalid system name, such as a name with a space, the system creates a host name using the following format: <code>SystemType-xxxxxxx</code> , where <code>xxxxxxx</code> is a set of random alphanumeric characters. IPv4 networks: The system sends the host name to the DHCP server to attempt to register the name with the local DNS server or look up the domain where the system is registered (if supported).
Domain Name	Identifies the domain your system belongs to. If the system doesn't automatically obtain a domain name, enter one here.

Setting	Description
Autonegotiation (under General Settings in the local interface)	<p>Specifies whether the system should automatically negotiate the LAN speed and duplex mode per IEEE 802.3 autonegotiation procedures. If you enable this setting, the system sets LAN Speed and Duplex Mode to read-only.</p> <p>Polycom recommends that you use autonegotiation to avoid network issues.</p>
LAN Speed (under General Settings in the local interface)	<p>Specifies whether to use 10 Mbps, 100 Mbps, or 1000 Mbps for the LAN speed. Note that the switch must support the speed you choose. If you enable the Autonegotiation setting, this setting is read-only.</p>
Duplex Mode (under General Settings in the local interface)	<p>Specifies the duplex mode to use. Note that the switch must support the speed you choose. If you enable the Autonegotiation setting, this setting is read-only.</p>
Ignore Redirect Messages	<p>Enables the system to ignore ICMP redirect messages.</p> <p>Polycom recommends that you enable this setting in most circumstances.</p>
ICMP Transmission Rate Limit (millisec)	<p>Specifies the minimum number of milliseconds between transmitted packets. Enter a number between 0 and 60000. The default value of 1000 means the system sends 1 packet per second. If you enter 0, the system disables the transmission rate limit.</p> <p>This setting applies only to “error” ICMP packets. This setting has no effect on “informational” ICMP packets, such as echo requests and replies.</p>
Generate Destination Unreachable Messages	<p>Generates an ICMP <i>Destination Unreachable</i> message if the system can’t deliver a packet to its destination for reasons other than network congestion.</p>
Respond to Broadcast and Multicast Echo Requests	<p>When enabled, your system sends an ICMP <i>Echo Reply</i> message in response to a broadcast or multicast Echo Request that isn’t specifically addressed to the system.</p>
Enable LLDP (under General Settings in the local interface)	<p>Specifies if you want the system to advertise itself on the network using the Link Layer Discovery Protocol (LLDP). Enable if you want your system to operate on a virtual LAN (VLAN).</p>

Setting	Description
Enable EAP/802.1X (under EAP 802.1X in the local interface)	Enables EAP/802.1X network access. The system supports the following authentication protocols: <ul style="list-style-type: none"> ▪ EAP-MD5 ▪ EAP-PEAPv0 (MSCHAPv2) ▪ EAP-TTLS ▪ EAP-TLS
EAP/802.1X Identity (under EAP 802.1X in the local interface)	Specifies the identity the system uses for 802.1X authentication. This setting is available only when you enable EAP/802.1X. You can't leave this field blank.
EAP/802.1X Password (under EAP 802.1X in the local interface)	Specifies the password the system uses for 802.1X authentication. This setting is required when you use EAP-MD5, EAP-PEAPv0, or EAP-TTLS.
Enable 802.1p/Q (under 802.1p/Q in the local interface)	Enable if you want to configure your system with a virtual LAN (VLAN) and set link layer priorities.
VLAN ID	Identifies the VLAN you want your system to operate on. This setting is available only when you enable 802.1p/Q. You can use any value from 1 to 4094.
Video Priority	Sets the link layer priority of video traffic on the wired LAN. Video traffic is RTP traffic consisting of video data and associated RTCP traffic. This setting is available only when you enable 802.1p/Q. You can use any value from 0 to 7, although Polycom recommends not using 6 and 7.
Audio Priority	Sets the link layer priority of audio traffic on the wired LAN. Audio traffic is RTP traffic consisting of audio data and associated RTCP traffic. This setting is available only when you enable 802.1p/Q. You can use any value from 0 to 7, although Polycom recommends not using 6 and 7.
Control Priority	Sets the link layer priority of control traffic on the wired LAN. Control traffic consists of control information associated with a call: <ul style="list-style-type: none"> ▪ H.323: H.225.0 Call Signaling, H.225.0 RAS, H.245, Far-End Camera Control (FECC) ▪ SIP: SIP Signaling, FECC, Binary Floor Control Protocol (BFCP) This setting is available only when you enable 802.1p/Q. You can use any value from 0 to 7, although Polycom recommends not using 6 and 7.

3. Select **Save**.

Configure Wi-Fi Settings

In addition to a LAN, you can also connect your G7500 system to a Wi-Fi network for additional user access. For example, this enables guests to share content to the system.

Procedure

1. In the system web interface, go to **Network > Wi-Fi Network**.
2. For **Choose Network Type**, select **Wi-Fi**.
3. Select **Enable Administrator Access to This Network** to enable administrators to access the system web interface on the Wi-Fi network.

For higher security, you can disable this option to limit access to the system web interface through LAN connections only.

4. Do one of the following:
 - Select a network from **Available Wi-Fi Networks**. (The system lists networks in order of signal strength.)
 - Enter the network name in the **SSID** field.

Selecting a new SSID erases the previous SSID and relevant Wi-Fi settings from the system.

5. Configure the following settings:

Available settings vary with your selections.

Setting	Description
Security	Specifies the encryption protocol: <ul style="list-style-type: none"> ▪ None ▪ WEP ▪ WPA/WPA2-PSK ▪ 802.1xEAP
Key (Passphrase/PSK)	Specifies an encryption passphrase (like a password) for the Wi-Fi network. You must enter the passphrase to connect to the Wi-Fi network.
EAP Method	Specifies the extensible authentication protocol (EAP) for WPA-Enterprise (802.1xEAP): <ul style="list-style-type: none"> ▪ PEAP ▪ TLS ▪ TTLS ▪ PWD
Phase 2 Authentication	Specifies the Phase 2 authentication method: <ul style="list-style-type: none"> ▪ None ▪ MSCHAPV2 ▪ GTC

Setting	Description
Username	Specifies the login user name for WPA-Enterprise (802.1xEAP).
Password	Specifies the login password for WPA-Enterprise (802.1xEAP).
IP Address	Select one of the following to set your system Wi-Fi network IP address: <ul style="list-style-type: none"> ▪ Obtain IP address automatically (You must have a DHCP server in your environment to use this option.) ▪ Enter IP address manually
Your IP Address Is	Specifies the IP address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
Subnet Mask	Specifies the subnet mask address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
Default Gateway	Specifies the IP gateway for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
DNS Server	Specifies the DNS server address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
DNS Alternate Server	Specifies the alternate DNS server address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.

When you connect, you receive a `Successfully connected to <your network's SSID name>` message.

Configure Network Quality Settings

You can specify how your G7500 system responds to network quality issues by controlling how your network handles packets during video calls.

Procedure

1. In the system web interface, go to **Network > Primary Network > Network Quality**.
2. Configure the following settings:

Setting	Description
Quality Preference	<p>Specifies which video stream has precedence when attempting to compensate for network loss:</p> <ul style="list-style-type: none"> ▪ Both people and content streams ▪ People streams ▪ Content streams <p>The stream option you select experiences less quality degradation during network loss compensation than the other. Choosing Both means each stream experiences roughly equal degradation.</p> <p>This setting is not available if you enable Automatically Adjust People/Content Bandwidth.</p>
Type of Service	<p>Specifies the type of service (ToS), which lets you prioritize packets sent to your system for video, audio, Far End Camera Control (FECC), and OA&M:</p> <ul style="list-style-type: none"> ▪ IP Precedence: Represents a priority level between 0 and 7. ▪ DiffServ: Represents a priority level between 0 and 63.
Video	<p>Specifies the IP Precedence or DiffServ priority level for video RTP and associated RTCP traffic.</p>
Audio	<p>Specifies the IP Precedence or DiffServ priority level for audio RTP and associated RTCP traffic.</p>
Control	<p>Specifies the IP Precedence or Diffserv priority level for control traffic on the following channels:</p> <ul style="list-style-type: none"> ▪ H.323: H.225.0 Call Signaling, H.225.0 RAS, H.245, and FECC ▪ SIP: SIP Signaling, FECC, and Binary Floor Control Protocol (BFCP) <p>(The system enables FECC by Allow Other Participants in a Call to Control Your Camera.)</p>
OA&M	<p>Specifies the IP Precedence or Diffserv value for traffic unrelated to video, audio, or FECC.</p>
Maximum Transmission Unit Size	<p>Specifies whether to use the default Maximum Transmission Unit (MTU) size for IP calls or let you select it.</p>

Setting	Description
Maximum Transmission Unit Size Bytes	Specifies the MTU size (in bytes) used in calls. <ul style="list-style-type: none"> If video quality is poor or you experience network errors, packets might be too large. Decrease the MTU. If the network is burdened with unnecessary overhead, packets might be too small. Increase the MTU.
Enable Lost Packet Recovery	If you enable this setting, the system uses the Lost Packet Recovery (LPR) protocol to help compensate for packet loss if it occurs.
Enable RSVP	If you enable this setting, the system can use the Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. (To use this feature, the near and far site must support RSVP.)
Dynamic Bandwidth	Enable this setting if you want the system to automatically determine the optimal call rate.
MRC Bandwidth Allocation	Adjusts media bit stream bandwidth, reducing packet loss.
Maximum Transmit Bandwidth	Specifies the maximum transmit call rate between 64 kbps and the system's maximum line rate. Use this setting when the system connects to the network using an access method with different transmit and receive bandwidths.
Maximum Receive Bandwidth	Specifies the maximum receive call rate between 64 kbps and the system's maximum line rate. Use this setting when the system connects to the network using an access method with different transmit and receive bandwidths.

3. Select **Save**.

Configure H.323 Settings

If your network uses a gatekeeper, the G7500 system can automatically register its H.323 name and extension. This enables others to call the system by entering the H.323 name or extension instead of the IP address.

Procedure

1. In the system web interface, go to **Call Configuration > H.323**.
2. Configure the following settings:

Setting	Description
Enable IP H.323	Enables the system to display H.323 settings and configuration options.
Registration Status	Read-only setting shows if your system is registered with an H.323 gatekeeper.
H.323 Name	<p>How gatekeepers and gateways identify your system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper.</p> <p>The H.323 Name is the same as the device name unless you change it.</p> <p>Your organization's dial plan might define the name you can use.</p>
H.323 Extension (E.164)	<p>You can place point-to-point calls using this extension if both systems are registered with a gatekeeper. Gatekeepers and gateways also use the extension to identify your system.</p> <p>Your organization's dial plan might define the extensions you can use.</p>
Use Gatekeeper	<p>Specifies if you want to use a gatekeeper for H.323 services.</p> <ul style="list-style-type: none"> ▪ Off: Calls don't use a gatekeeper. ▪ Auto: System tries to automatically find an available gatekeeper. ▪ Specify: Calls use the specified gatekeeper. You must select this setting to enable H.235 Annex D Authentication. <p>If you don't configure this setting to Off, a registration status displays.</p>
Require Authentication	<p>Enables support for H.235 Annex D Authentication.</p> <p>When you enable H.235 Annex D Authentication, the H.323 gatekeeper ensures that only trusted H.323 endpoints can access the gatekeeper.</p> <p>This setting is available when you set Use Gatekeeper to Specify.</p>
Username	Specifies a user name if the gatekeeper requires authentication for registration.
Password	Specifies a password if the gatekeeper requires authentication for registration.

Setting	Description
Current Gatekeeper IP Address	<p>Displays the IP address that the gatekeeper is using.</p> <p>If you select Off for the Use Gatekeeper field, the Current Gatekeeper IP Address field doesn't display.</p>
Primary Gatekeeper IP Address	<p>The gatekeeper IPv4 address the system registers with. As part of the registration process, the gatekeeper might return alternate gatekeepers. If your system loses communication with the primary gatekeeper, your system registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system re-establishes communication with the primary gatekeeper, it unregisters from the alternate gatekeeper.</p> <ul style="list-style-type: none"> ▪ If you set the Use Gatekeeper field to Off, the Primary Gatekeeper IP Address field doesn't display. ▪ If you use an automatically selected gatekeeper, this area displays the gatekeeper's IP address. ▪ If you specify a gatekeeper, enter the gatekeeper IP address or name (for example, 10.11.12.13 or gatekeeper.companyname.usa.com).

3. Select **Save**.

Related Links

[Configuring Call Settings](#) on page 65

Related Links

[Configure SIP Settings](#) on page 36

Configure SIP Settings

If your network supports SIP, you can use it to connect calls on your G7500 system.

Procedure

1. In the system web interface, go to **Call Configuration > SIP**.
2. Configure the following settings:

Setting	Description
Enable SIP	Enables the system to make and receive SIP calls.
Registration Status	Read-only setting shows if your system is registered to a SIP server.

Setting	Description
SIP Server Configuration	<p>Specifies whether to automatically or manually set the SIP server's IP address.</p> <p>If you select Auto, you can't edit the Transport Protocol, Registrar Server, and Proxy Server settings. If you select Specify, you can edit these settings.</p>
Transport Protocol	<p>Sets the protocol your system uses for SIP signaling (your SIP network determines which protocol is required).</p> <ul style="list-style-type: none"> ▪ Auto: Enables automatic negotiation of protocols in the following order: TLS, TCP, and UDP. Polycom recommends this setting for most environments. ▪ TLS: Provides secure SIP signaling. TLS is available only when you register your system with a SIP server that supports it. If you set this option, your system ignores TCP/UDP port 5060. ▪ TCP: Provides reliable transport via TCP. ▪ UDP: Provides best-effort transport via UDP.
Force Connection Reuse	<p>Disabled by default (recommended).</p> <p>When disabled, the system uses an ephemeral source port for outgoing SIP messages. When enabled, the system uses the active SIP listening port as the source port (5060 or 5061, depending on the negotiated SIP transport protocol in use).</p> <p>You can use this setting to establish correct operation with remote SIP peer devices, which require that the source port match the contact port in SIP messages.</p>

Setting	Description
BFCP Transport Preference	<p>Controls content sharing negotiation behavior. When you use the Binary Floor Control Protocol (BFCP), a relationship is established between the floor control server and its clients. What you set here determines how network traffic flows between the server and clients.</p> <p>Note: TCP is typically slightly slower but more reliable than UDP. Some deployments don't support it, such as with session border controllers (SBCs).</p> <ul style="list-style-type: none"> ▪ Prefer UDP: (Default) Starts resource sharing using UDP but falls back to TCP if needed. ▪ Prefer TCP: Starts resource sharing using TCP but falls back to UDP if needed. ▪ UDP Only: Shares resources only using UDP. If UDP is unavailable, your system can't share content in a separate video stream. ▪ TCP Only: Shares resources only through TCP. If TCP is unavailable, your system can't share content in a separate video stream.
Sign-in Address	<p>The SIP address or name of the system (for example, <code>mary.smith@department.company.com</code>). If you leave this blank, the system IP address is used for authentication.</p>
User Name	<p>The user name for authenticating your system with a SIP registrar server (for example, <code>marySmith</code>). If the SIP proxy requires authentication, you can't leave the user name and password blank.</p>
Password	<p>The password associated with the user name for authenticating your system with a SIP registrar server.</p>
Registrar Server	<p>The IP address or FQDN of the SIP registrar server. If you register a remote system with an edge server, use that server's FQDN.</p> <p>By default, the system sends SIP signaling to ports 5060 (TCP) and 5061 (TLS) on the registrar server.</p> <p>Enter the address and port using the following format: <code><IP_Address>:<Port></code>.</p> <p>The <code><IP_Address></code> can be an IPv4 address or an FQDN such as <code>servername.company.com:5060</code>.</p>

Setting	Description
Proxy Server	<p>The IP address or FQDN of the SIP proxy server. If you leave this field blank, the system uses the registrar server address. If you also leave the SIP registrar server field blank, there is no SIP proxy server to configure.</p> <p>By default, the system sends SIP signaling to ports 5060 (TCP) and 5061 (TLS) on the proxy server.</p> <p>The syntax for this setting is the same as the registrar server.</p>
Registrar Server Type	Specifies the type of SIP registrar server you're using.

3. Select **Save**.

Related Links

[Configuring Call Settings](#) on page 65

Related Links

[Configure H.323 Settings](#) on page 34

Enable Point-to-Point Call Escalation to a RealPresence DMA Conference Call

When you register your G7500 system with a Polycom RealPresence DMA system, you can enable a point-to-point call on your system to escalate to an impromptu conference call on an external Polycom MCU.

You must configure your system's SIP settings to register with your RealPresence DMA system.

For information about working with a RealPresence DMA system, specifically SIP conference factories, see the [Polycom RealPresence DMA Operations Guide](#).

Procedure

1. In the system web interface, go to **Call Configuration > SIP**.
2. Go to **Adhoc Call Escalation**.
3. Select the **Enable automatic call escalation of point-to-point to an external MCU** check box.
4. For the **Conference Factory ID**, enter the ID associated with the SIP conference factory on your RealPresence DMA system.

Note: The conference factory ID must come from the same RealPresence DMA system your video conferencing system uses for SIP registration. Calls don't escalate if your RealPresence DMA system doesn't recognize the ID you provide.

5. Select **Save**.

Calls converted through a RealPresence DMA system gateway (H.323 to SIP or vice versa) don't join an impromptu conference call.

Wireless Devices

The G7500 system includes Wi-Fi and Bluetooth wireless communication options so your users can discover the system on the network with the Polycom Content App or their AirPlay- or Miracast-certified device. Your remote control also connects to the system using Bluetooth.

You can enable or disable these features as needed.

Wireless Band for Miracast-Certified Devices

Miracast-certified devices must use the 5 GHz band to connect with the G7500 system (using 802.11 channel 44 by default).

Note: If you enable Wi-Fi, the system uses the same 802.11 channel for Miracast-certified device connections.

Disable Wireless Options

You can disable the wireless features on your G7500 system. Wireless features are enabled by default.

Remember the following when disabling wireless features:

- Disabling wireless connectivity turns off screen mirroring with Miracast-certified devices and prevents the system from using Wi-Fi to connect to a secondary network.
- Disabling Bluetooth turns off screen mirroring with AirPlay-certified devices and prevents those devices and the Polycom Content App from automatically discovering your G7500 system. (You can still connect with the Polycom Content App using the system IP address.)
- Disabling Bluetooth also disables your remote control.

Procedure

1. In the system web interface, go to **Security > Wireless Security**.
2. Do one of the following:
 - Clear the **Enable Wireless Connectivity** check box.
 - Clear the **Enable Bluetooth** check box.

Related Links

[Default Options for Sharing Content](#) on page 93

[Polycom Bluetooth Remote Control](#) on page 18

Securing the System

Topics:

- [Managing System Access](#)
- [PKI Certificates](#)
- [Disable the Security Code](#)
- [Limit or Disable the Ability to Save Content](#)
- [Encryption](#)
- [H.460 Firewall/NAT Traversal](#)
- [Web Proxies](#)
- [View Connections to the System](#)
- [Port Usage](#)

Your G7500 system includes features and settings to help you meet security requirements.

Managing System Access

You can control how users and administrators access the G7500 system.

You can set up local and external authentication for the following system interfaces:

- Local interface
- System web interface
- Command-line API (external authentication is available only when accessing the API using SSH)

Local Accounts

The system stores local account IDs and passwords.

Configure Password Policies

You can specify requirements for administrator, remote access, and SNMP passwords for your G7500 system.

Polycom strongly recommends that you create an administrator password for your system.

Procedure

1. In the system web interface, go to **Security > Password Requirements**.
2. Configure the following settings for the **Admin Room**, **Remote Access**, or **SNMP** passwords:
Not all settings apply to SNMP.

Setting	Description
Minimum Length	The minimum number of characters required for a valid password.
Require Lowercase Letters	The minimum number of lowercase letters required for a valid password.
Require Uppercase Letters	The minimum number of uppercase letters required for a valid password.
Require Numbers	The minimum number of numerals required for a valid password.
Require Special Characters	The minimum number of special characters required for a valid password. Supported characters include: @ - _ ! ; \$, \ / & . # *
Reject Previous Passwords	The number of most recent passwords that you can't reuse. If you set this to Off , all previous passwords are valid.
Minimum Password Age in Days	The minimum number of days before the password can change.
Maximum Password Age in Days	The maximum number of days before the password must change.
Minimum Changed Characters	The number of characters that must be different or change position in a new password. For example, if you set this to 3, 123abc can change to 345cde but not to 234bcd.
Maximum Consecutive Repeated Characters	The maximum number of consecutive repeated characters allowed in a password. For example, if you set this to 3, aaa123 is a valid password but aaaa123 is not.
Password Expiration Warning	Specifies how many days in advance a warning displays indicating that the password expires soon (if you set a maximum password age).
Can Contain ID or Its Reverse Form	Specifies whether the associated ID or its reverse can be part of a password. If you enable this setting and the ID is admin, passwords admin and nimda are allowed.

3. Select **Save**.

Changes to most password policy settings don't take effect until the next time the password is changed. Changes take effect immediately for **Minimum Password Age in Days**, **Maximum Password Age in Days**, and **Password Expiration Warning**.

Create Local Administrator Credentials

You can require local administrator credentials for in-room and remote access to the G7500 system.

Passwords for logging in to the system are case sensitive and can't contain more than 40 characters.

Procedure

1. In the system web interface, go to **Security > Local Accounts**.
2. Configure the following settings:

Setting	Description
Admin ID	The local administrator account name (default is <code>admin</code>).
Room Password	If you set this option, you must enter this password to change administrator settings in the local interface. The default password is the last six characters of the serial number listed in System Details and on the back of the device.
Remote Access Password	If you set this option, you must enter this password to access the system through the system web interface or command-line API (SSH or telnet). This password lets you perform device management tasks, such as updating the system's software.

3. Optional: Do one of the following:
 - To use the local administrator **Room Password** for remote logins, leave the **Use Room Password for Remote Access** option enabled.
 - If you don't want to use the local administrator **Room Password** for remote logins, disable the **Use Room Password for Remote Access** option.

This setting specifies that the system uses the local administrator **Room Password** for remote logins. This setting is enabled by default.

4. Select **Save**.

Configure Account Lockout Settings

You can specify account lockout controls to prevent unauthorized access to your G7500 system.

Procedure

1. In the system web interface, go to **Security > Local Accounts**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Lock Admin Account after Failed Logins	Specifies the number of failed login attempts allowed before the system locks the account. You can turn this setting Off .
Admin Account Lock Duration	Specifies the amount of time an account is locked because of failed login attempts. After this period expires, the system resets the failed login attempts counter to zero, and users can again log in with that account.

Setting	Description
Reset Admin Account Lock Counter After	<p>Determines how many hours the failed login window lasts. The window is a period of time starting with the first failed login attempt and during which the system counts subsequent failed attempts against the number allowed.</p> <p>The counter resets to zero at the end of the window (if the account is not locked because of failed attempts) and after a successful login.</p>

Enable External Authentication

You can set up external authentication through Active Directory for your G7500 system. When enabled, you can access the system with an Active Directory account or the system's local administrator credentials.

Before you begin, make sure that you configure the **Domain Name** setting on the **Network > Primary Network > LAN Options** page with your Active Directory domain.

The system can map only one Active Directory group to a given role.

Procedure

1. In the system web interface, go to **Security > Global Security**.
2. Go to **Authentication**.
3. Configure the following settings:

Setting	Description
Enable Active Directory External Authentication	<p>Specifies whether to authenticate users with the Active Directory server. When you enable Active Directory authentication, users can log in to the system with their network credentials using this format: <code>domain\user</code>. With this format, users can have accounts on multiple domains.</p>
Active Directory Server Address	<p>Specifies the Active Directory server's FQDN or IP address. If you are using subdomains, append port number 3268 as follows: <code>ad.domain.com:3268</code>.</p> <p>You can alternatively use RealPresence Resource Manager as an Active Directory server and enter its address here.</p> <p>If you enable Always Validate Peer Certificates from Server on the Certificates page, make sure this value matches what is in the Active Directory server certificate. For example, if you enter the Active Directory server IP address here, but the certificate only has the server's FQDN, external authentication fails.</p>

Setting	Description
Active Directory Admin Group	Specifies the Active Directory group whose members should have administrator access to the system. This name must exactly match the name in the Active Directory server for successful authentication.
Active Directory User Group	Specifies the Active Directory group whose members should have user access to the system. This name must exactly match the name in the Active Directory server for successful authentication.

4. Select **Save**.

Configure System Access Settings

You can configure how you access your G7500 system.

Procedure

1. In the system web interface, go to **Security > Access**.
2. Configure the following settings:

Setting	Description
Enable Network Intrusion Detection System (NIDS)	When you enable this setting, the system creates security log entries when it detects a possible network intrusion.
Enable Web Access	Specifies whether you can access the system using the system web interface.
Allow Access to User Settings	Specifies whether users can access the User Settings screen through the local interface.
Restrict to HTTPS	Specifies that you can access the system web interface only over port 443. Enabling this setting closes access through port 80 (HTTP).
Web Access Port (HTTP)	Specifies the port to use when accessing the system web interface over HTTP. If you change the default (port 80), specify port 1025 or higher and make sure it is not already in use. You must include the port number with the IP address when you use the system web interface to access the system. (This setting is unavailable if Restrict to HTTPS is enabled.)
Enable Diagnostics Port Idle Session Timeout	Specifies whether to allow the diagnostics port to time out at the configured time interval or not. You set the timeout at Idle Session Timeout in Minutes .

Setting	Description
Enable API Port Idle Session Timeout	Specifies whether to allow the API port to time out at the configured time interval or not. You set the timeout at Idle Session Timeout in Minutes .
Enable SNMP Access	Specifies whether to allow SNMP access.
Idle Session Timeout in Minutes	Specifies the number of minutes a session can be idle before it times out.
Maximum Number of Active Sessions	Specifies the maximum number of users logged in through the system web interface or command-line API (SSH or telnet).

3. Select **Save**.

Enable Command-Line API Access Over SSH

Use SSH on port 22 if you want encrypted access to the G7500 system command-line API.

Procedure

1. In the system web interface, go to **Security > Access**.
2. Select the **Enable Legacy API Over SSH** check box if it's cleared.
3. Select the **Enable Telnet Access** check box.

Enable Command-Line API Access Over Telnet

Use port 24 or 23 to access the G7500 system command-line API using telnet.

Procedure

1. In the system web interface, go to **Security > Access**.
2. Select the **Enable Telnet Access** check box.
3. Choose an **API Port** for telnet connections: **24** (default) or **23**.

Disable Command-Line API Access

To disable command-line API access to your G7500 system, close network ports 22, 23, and 24 and the RS-232 serial port.

Procedure

1. In the system web interface, go to **Security > Access**.
2. Clear the **Enable Telnet Access** check box.
Network ports 22, 23, and 24 on your system are closed.
3. In the system web interface, go to **General Settings > Serial Ports**.
4. For **RS-232 Mode**, select **Off**.
The serial port is closed.

Command-line API access to your system is disabled.

Configure the System Web Interface Port Lock

You can limit the number of failed login attempts to the G7500 system web interface to protect against brute-force attacks.

Procedure

1. In the system web interface, go to **Security > Access**.
2. Configure the following settings:

Setting	Description
Lock Port after Failed Logins	The number of failed login attempts allowed before the web interface locks. You can set this to Off .
Port Lock Duration	Specifies the amount of time that the web interface remains locked due to failed login attempts. When this period expires, the failed login attempts counter resets and you can try to log in again.
Reset Port Lock Counter After	Specifies the number of hours, starting with the first failed login attempt, during which subsequent failed login attempts are counted against the maximum number allowed (Lock Port After Failed Logins). The counter resets when the set period of time expires or a user successfully logs in.

3. Select **Save**.

Configure the SSH Port Lock

You can limit the number of failed SSH login attempts to your G7500 system command-line API to protect against brute-force attacks.

Procedure

1. In the system web interface, go to **Security > Access**.
2. Configure the following settings:

Setting	Description
Lock SSH Port After Failed Logins	Specifies the number of failed login attempts allowed before the system locks SSH access to the API.
SSH Port Lock Duration	Specifies the amount of time that SSH access to the API remains locked due to failed login attempts. After this period expires, the system resets the failed login attempts counter, and you can again try to log in again.

Setting	Description
Reset SSH Port Lock Counter After	<p>Specifies the number of hours, starting with the first failed login attempt, during which subsequent failed login attempts are counted against the maximum number allowed (Lock SSH Port after Failed Logins).</p> <p>The counter resets when the set period of time expires or a user successfully logs in.</p>

3. Select **Save**.

Locking the Telnet Port

Other than disabling telnet access to the G7500 system command-line API, you can't restrict telnet access in other ways, such as locking its port for too many failed login attempts (like you can with web or SSH access).

Note: Remember the following about telnet access: A telnet session disconnects after three failed login attempts. If you start a new session, the system allows another three attempts.

Configure Serial Port Settings

You can configure RS-232 serial port settings in the G7500 system web interface.

Procedure

1. In the system web interface, go to **General Settings > Serial Ports**.
2. Configure the following settings:

Setting	Description
RS-232 Mode	<p>Specifies the mode used for the RS-232 serial port.</p> <ul style="list-style-type: none"> • Off: Disables the serial port. • Control: Receives control signals from a touch-panel control. Allows any device connected to the RS-232 port to control the system using API commands.
Baud Rate Parity Stop Bits	Set these options to the same values configured on the serial device.
Data Bits	This setting is read-only.
RS-232 Flow Control	Specifies if you want to use hardware flow control between the connected device and your system.

Setting	Description
Login Mode	<p>Specifies the credentials necessary for a control system to connect to the RS-232 port.</p> <ul style="list-style-type: none"> • Admin password only: (Default) Requires the administrator password (if you set one) when the control system connects. • Username/Password: Requires the user name and administrator password (if you set one) when the control system connects. • None: The system doesn't require a user name or password when the control system connects. <p>Note: This setting only displays when you set RS-232 Mode to Control.</p>

3. Select **Save**.

Disable USB 3.0 Ports

You can configure your G7500 system so no one can use its USB 3.0 ports.

Note: You can't turn off the USB-C port, which only provides power.

Procedure

1. In the system web interface, go to **Security > Access**.
2. Select **Disable All USB Ports**.

PKI Certificates

If your organization uses a public key infrastructure (PKI) for securing network connections, Polycom recommends that you have a strong understanding of certificate management and how it applies to your G7500 system.

PKI certificates authenticate secure network connections to and from the G7500 system. The system uses standard PKI techniques to configure and manage certificates and certificate signing requests (CSRs). ANSI X.509 standards regulate the certificate characteristics.

Your system can generate CSRs to send to a certificate authority (CA), a trusted entity that validates and officially issues, or signs, PKI certificates. Your system uses those certificates for client and server authentication.

If your system is in an environment without PKI, you don't need a CA-signed certificate; the system comes with a self-signed certificate for its TLS connections. When you deploy PKI, however, self-signed certificates aren't trusted and you must use CA-signed certificates.

Here are some examples of how you use PKI certificates:

- If your environment uses the 802.1X authentication framework for wired connections, create a CSR and install the resulting CA-signed certificate on your system so it's trusted on the network.
- If you want to navigate with a browser over a secure connection to your system web interface, create a CSR and install the resulting CA certificate chain on your system to replace its factory-installed certificate, which is not trusted.

- Provisioning your system using RealPresence Resource Manager in a secure environment.

Note: Your system must have a **Host Name** in this situation.

Related Links

[Using a Provisioning Service](#) on page 25

Create a Certificate Signing Request

If you deploy a PKI in your environment, create a CSR to make sure your G7500 system is trusted by its network peers.

Note: Only a single CSR can exist at a time. After a CSR is generated, get it signed and installed on your system before creating another. For example, if you generate a CSR and generate another prior to having the first one signed and installed, the system discards the previous CSR.

Procedure

1. In the system web interface, go to **Security > Certificates**.
2. Select **Create Certificate Signing Request (CSR)**.
3. In the **Certificate Details** form, complete the following fields:

CSR Information	Description
Hash Algorithm	Specifies the hash algorithm for the CSR: SHA-256 (recommended) or SHA-1 (not recommended).
Common Name (CN)	Specifies the system name. Polycom recommends the following guidelines for this field: <ul style="list-style-type: none"> ▪ For systems registered in DNS, use the system's fully qualified domain name (FQDN). ▪ For systems not registered in DNS, use the system's IP address. Maximum characters: 64 (truncated if necessary). Default is blank.
Organizational Unit (OU)	Specifies the business group defined by your organization. Default is blank. Maximum characters: 64. Note: The system supports only one OU field. If you want the CA-signed certificate to include more than one OU, download and manually edit the CSR.
Organization (O)	Specifies your organization's name. Default is blank. Maximum characters: 64.
City or Locality (L)	Specifies the city where your organization is located. Default is blank. Maximum characters: 128.
State or Province (ST)	Specifies the state or province where your organization is located. Default is blank. Maximum characters: 128.
Country (C)	Displays the country selected in the setup wizard. Cannot be changed here.

CSR Information	Description
SAN: FQDN	Specifies the FQDN assigned to the system. It is the same as the Common Name (CN) but not truncated. Default is blank. Maximum characters: 253.
SAN: Additional Name	Specifies an additional system name. Default is blank. Maximum characters: 253.
SAN: IPv4 Address	Default is the system's IPv4 address. Maximum characters: 15
User Principal Name (UPN)	Specifies the user and domain name to log in to a Windows domain (for example, <code>UserName@YourDomain.com</code>). This is the <code>userPrincipalName</code> attribute of the account object in Active Directory. Relate this setting to the 802.1X identity and password you specified on the Network > LAN Options page. Default is blank.

4. Select **Create**.
5. If the CSR was created successfully, select **CSR Available for Download** to download the CSR file to send to a CA, which issues your signed certificate.

Configure Certificate Validation Settings

The G7500 system can automatically validate user-installed certificates when establishing an authenticated network connection.

To perform this validation, you must install certificates from the CAs that are part of the trust chain on the G7500 system.

Note: These settings are used only for 802.1X authentication.

Procedure

1. In the system web interface, go to **Security > Certificates**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Maximum Peer Certificate Chain Depth	Specifies how many links a certificate chain can have. The term <i>peer certificate</i> refers to any certificate sent by the far-end host when a network connection is being established between the two systems.
Always Validate Peer Certificates from Server	Determines whether your system requires a remote server to present a valid certificate when connecting to it for services, such as provisioning.

Install a Certificate

Once you receive a signed certificate from the CA that processed your CSR, you can install it on your G7500 system.

This option isn't available if your certificate is provisioned to the system.

Procedure

1. In the system web interface, go to **Security > Certificates**.
2. Select **Install Certificate** to browse for the CA-signed certificate you want to install and select **Open**.

Your system accepts the following certificate file formats: `.pem`, `.der`, and PKCS #7 (which typically has a `.p7b` filename extension).


The system checks the certificate data and, if the upload is successful, adds it to the page.

With your CA-signed certificate installed, your system is trusted by its network peers (provided that a root certificate has established a chain of trust). This allows you to navigate with your browser over a secure connection to the system web interface and perform administrative tasks.

View a Certificate

The G7500 system lists user-installed certificates in the system web interface, where you also can view the contents of those certificates.

Procedure

1. In the system web interface, go to **Security > Certificates**.
The **Certificates** page lists your user-installed certificates. It includes information about which entity a certificate is issued to, who issued it, when it expires, and the certificate type (server, client, or CA).
2. To view the contents of a certificate, select **Visibility**  in the same row as the certificate.

The certificate contents display in plain text.


Delete a Certificate

You can remove user-installed certificates through the G7500 system web interface.

When you delete all user-installed certificates, your system reverts to using the factory-installed certificate. This option isn't available if your certificate is provisioned to the system.

Note: Deleting system settings by default retains your user-installed certificates, but performing a factory reset removes these certificates.

Procedure

1. In the system web interface, go to **Security > Certificates**.
2. Locate the certificate you want to delete and select **Trash**  in the same row as the certificate.

You can't undo this action.

3. Confirm by selecting **Delete**.

A message indicates that the system deleted the certificate.

Certificate Revocation

During certificate validation, your G7500 system checks whether certificates used for secure communications are revoked by their issuing CAs.

Your system can check certificate revocation status with one of the following standard methods:

- **Certificate Revocation List (CRL):** File containing a list of certificates revoked by their issuing CA. You must manually upload CRLs to your system.
- **Online Certificate Status Protocol (OCSP):** Your system contacts an OCSP responder, a web server that provides revocation status through a query/response exchange.

Manually Upload a CRL

You can use CRLs to perform certificate revocation checks on your G7500 system.

Uploading a CRL fails unless you install all of the certificates in the issuing CA's chain of trust for that CRL.

This option is not available if your CRL is provisioned to the system.

Procedure

1. In the system web interface, go to **Security > Certificates**.
2. Configure the following settings:

Setting	Description
Revocation Method	To use the CRL revocation method, select CRL .
Allow Incomplete Revocation Checks	When enabled, a certificate in the chain of trust validates without a revocation check if no corresponding CRL from the issuing CA is installed.

3. Select **Save**.
4. Select **Upload CRL File** to add a CRL.

You aren't limited to how many CRLs you can install, but you can only upload 10 at a time.

Successfully-uploaded CRLs display on the page and include information about the issuing CA, when the CRL was updated, and when it's scheduled to update again.

Delete a CRL

You can remove CRLs that were previously uploaded on the G7500 system.

This option is not available if your CRL is provisioned to the system.

Procedure

1. In the system web interface, go to **Security > Certificates**.
2. Under **Revocation**, select **Trash**  next to the CRL you want to delete.

Configure the OCSP Method

You can use the OCSP method to perform certificate revocation checks on your G7500 system.

Procedure

1. In the system web interface, go to **Security > Certificates**.
2. Configure the following settings:

Setting	Description
Revocation Method	To use the OCSP revocation method, select OCSP .
Allow Incomplete Revocation Checks	<p>When enabled, your system considers a revocation check successful if there is no response or the OCSP responder indicates a certificate's status is unknown.</p> <p>Regardless of how you configure this setting, the following statements apply:</p> <ul style="list-style-type: none"> • If the OCSP responder indicates a known revoked status, your system treats it as a revocation check failure and doesn't allow the connection. • If the OCSP responder indicates a known good status, your system treats it as a successful revocation check and allows the connection.
Global Responder Address	Specifies the URI of the OCSP responder (for example, <code>http://responder.example.com/ocsp</code>). The responder is used when Use Responder Specified in Certificate is disabled and sometimes even when it's enabled. Polycom recommends that you always include a URI in this field regardless of how you configure Use Responder Specified in Certificate .
Use Responder Specified in Certificate	<p>Some certificates include the OCSP responder address. When you enable this setting, your system attempts to use this address (when present) instead of the Global Responder Address you specified.</p> <p>Note: Only HTTP URLs in a certificate's AIA field are supported.</p>

3. Select **Save**.

Disable the Security Code

By default, you must enter a security code to connect to the G7500 system to share or save content, but you can disable it.

Procedure

- » In the system web interface, go to **Security > Security Code** and clear the **Enable Security Code** check box.

Related Links

[Sharing Content](#) on page 93

Limit or Disable the Ability to Save Content

You can block users, depending on their network connection, from saving content using the Polycom Content App.

For example, you may not want someone connected to your G7500 system through the Wi-Fi network to save content. However, users can still save content when connected through the primary network (LAN).

Procedure

1. In the system web interface, go to **Security > Content**.
2. Select or clear one of the following check boxes:
 - **Allow users to save content from Primary Network**
 - **Allow users to save content from Wi-Fi Network**

Related Links

[Sharing Content](#) on page 93

Encryption

AES is standard on G7500 systems. When enabled, your system automatically encrypts calls with other systems using AES.

A locked padlock icon displays on the connected monitor(s) when a call is encrypted. If a call is unencrypted, you see an unlocked padlock. The padlock may not accurately indicate encryption status if the call is cascaded or includes an audio-only endpoint. To avoid security ambiguity, participants can verbally communicate the state of their padlock icon at the beginning of a call.

The following AES cryptographic algorithms ensure flexibility when negotiating secure media transport:

- H.323 (per H.235.6)
 - AES-CBC-128 / DH-1024
 - AES-CBC-256 / DH-2048
- SIP (per RFCs 3711, 4568, 6188)
 - AES_CM_128_HMAC_SHA1_32
 - AES_CM_128_HMAC_SHA1_80
 - AES_CM_256_HMAC_SHA1_32
 - AES_CM_256_HMAC_SHA1_80

Configure Call Encryption

You can encrypt calls on your G7500 system.

Procedure

1. In the system web interface, go to **Security > Global Security**.
2. For the **Require AES Encryption for Calls** setting, choose how you want to encrypt calls:
 - **Off:** AES encryption is disabled.
 - **When Available:** AES encryption is used with systems that support it, but the system also allows unencrypted calls.

- **Required for Video Calls Only:** AES encryption is used in all video calls. Calls with systems that don't support it fail.
- **Required for All Calls:** AES encryption is used in all types of calls. Calls with systems that don't support it fail.

Configure Minimum TLS

You can restrict your G7500 system from using earlier versions of TLS for secure communications.

For example, if you set your minimum TLS version to 1.1, you're disabling TLS 1.0.

Procedure

1. In the system web interface, go to **Security > Global Security**.
2. Choose one of the following options for **Minimum TLS Version**:
 - **TLS 1.2**
 - **TLS 1.1**
 - **TLS 1.0**
3. Select **Save**.

Related Links

[Register with an LDAP Directory Server](#) on page 87

[LDAP Directory Server Ignores the Minimum TLS Version Setting](#) on page 120

H.460 Firewall/NAT Traversal

You can configure your G7500 system for firewall or network address translation (NAT) traversal using the H.460.18 and H.460.19 standards. This includes environments with session border controllers (SBCs).

For example, an endpoint outside your network that's initiating a SIP call connects to an SBC as a remote endpoint. The incoming SIP traffic then traverses a firewall before connecting to the endpoint it's calling inside your network.

Real-time media streams often use UDP for their speeds. If your system is behind a firewall that restricts access to UDP ports, however, you can configure your system for only TCP connections.

Caution: Systems deployed outside a firewall are potentially vulnerable to unauthorized access. Visit the Polycom Security section of the Knowledge Base at [Polycom Support](#) for timely security information. You can also register to receive periodic updates and advisories.

Configure the System for H.460 Firewall/NAT Traversal

You can configure your G7500 system for H.460 firewall/NAT traversal. Enable firewall traversal if you're using a cloud-based conferencing service or if your system is outside a corporate network (for example, a home office).

Make sure you register your system with a network device that supports H.460.18 and H.460.19 standards (for example, a RealPresence Access Director system or a Polycom VBP device).

Procedure

1. In the system web interface, go to **Network > Primary Network**.
2. Go to **Firewall**.

3. Select **Enable H.460 Firewall Traversal**.
4. Verify the firewalls that you traverse allow your system to use outbound TCP and UDP connections.
 - Firewalls with a stricter rule set must allow the system to use at least the following outbound TCP and UDP ports: 1720 (TCP), 14085-15084 (TCP), 1719 (UDP), and 16386-25386 (UDP).
 - Firewalls must allow inbound traffic to the TCP and UDP ports used for outbound traffic.
5. Configure the following settings:

Setting	Description
Fixed Ports	<p>Defines which TCP and UDP ports your system uses for firewall traversal.</p> <p>Enable this option if your firewall isn't H.323 compatible. The system assigns a port range starting with the TCP and UDP ports you specify (port 3230 is where the range begins by default).</p> <p>Note: For the fixed ports you configure, you must open the corresponding ports on your firewall. For H.323, open TCP port 1720. For SIP, open UDP port 5060, TCP 5060, or TCP 5061 depending on if you're using UDP, TCP, or TLS, respectively, as the SIP transport protocol.</p> <p>Disable this option if your firewall is H.323 compatible or the system isn't behind a firewall.</p>
TCP Ports UDP Ports	<p>The starting value for the range of TCP and UDP ports the system uses. The system automatically configures the range based on the beginning value you set here.</p> <p>To allow H.323 traffic, you need two TCP and eight UDP ports per connection. You must also open TCP port 1720 on the firewall.</p> <p>To allow SIP traffic, you need TCP port 5060 and eight UDP ports per connection.</p> <p>UDP port range: Because systems support ICE, the range of fixed UDP ports is 32. The system cycles through the available ports from call to call.</p> <p>Fixed ports range and filters: You might notice that the source port of a SIP signaling message is not in the fixed ports range. When your firewall is filtering on source ports, in the system web interface, go to the SIP page and enable Force Connection Reuse. When enabled, the system uses port 5060 and 5061 for the source and destination port (these must be open on the firewall).</p>

Setting	Description
NAT Configuration	<p>Specifies if the system automatically determines the NAT public (WAN) address.</p> <ul style="list-style-type: none"> ▪ If the system isn't behind a NAT or is connected to the network through a VPN, set this option to Off. ▪ If the system is behind a NAT that allows HTTP traffic, set this option to Auto. ▪ If the system is behind a NAT that doesn't allow HTTP traffic, set this option to Manual.
NAT Public (WAN) Address	<p>The address callers from outside the LAN use to call your system. If you configured the NAT manually, enter the NAT public address here.</p> <p>You can configure this option only when you set NAT Configuration to Manual.</p>
NAT is H.323 Compatible	<p>Identifies whether the system is behind a NAT that can translate H.323 traffic.</p> <p>This option is available only when you set NAT Configuration to Auto or Manual.</p>
Address Displayed in Global Directory	<p>Choose whether to display the system's public or private address in the global directory.</p> <p>This option is available only when you set NAT Configuration to Auto or Manual.</p>
Enable SIP Keep-Alive Messages	<p>Specifies whether to regularly transmit keep-alive messages on the SIP signaling channel and on RTP sessions part of SIP calls. Keep-alive messages maintain connections through firewall/NAT devices that are often used at network edges.</p> <p>If your system is in an Avaya SIP environment, Polycom recommends that you disable this setting to enable calls to fully connect.</p>

6. Select **Save**.

Web Proxies

A web proxy can help your G7500 system communicate outside your network securely and with increased performance. For example, you can direct your system's outbound requests through an enterprise proxy.

You can configure your system to use a proxy one of the following ways:

- **Automatic:** You specify only the proxy credentials (if needed). Using DHCP, your system obtains a URL to automatically download a proxy auto-configuration (PAC) file.

- **Semi-automatic:** You specify the proxy credentials and URL for automatically downloading a PAC file.
- **Manual:** You specify the proxy address, port, and credentials. (This method lets you configure your system with only one proxy.)

If your configuration includes automatically downloading a PAC file, there must be an expiration associated with the file so the system knows when to download a new one. Make sure your PAC file server includes an `Expires` header in its HTTP response (for example, `Expires: Wed, 30 Oct 2016 09:30:00 GMT`).

Your system can authenticate with a proxy using the following methods:

- Digest authentication (with either MD-5 or SHA-256 digest)
- NTLM authentication (only NTLMv2 is supported)
- Basic authentication (this insecure method is disabled by default)
- No authentication (or null authentication, meaning the proxy server doesn't require credentials)

Your system supports the following services when configured to use a web proxy:

- Directory servers
- Provisioning service
- Calendaring service
- Software updates

Related Links

[Checking the Web Proxy Configuration](#) on page 121

Enable the System to Use a Web Proxy

By default, your G7500 system configuration doesn't use web proxies.

Procedure

1. In the system web interface, go to **Network > Primary Network > Web Proxy Settings**.
2. Select **Enable Web Proxy**.

Set Up Automatic Web Proxy Configuration

With automatic web proxy configuration, your G7500 system obtains a URL for downloading a proxy auto-configuration (PAC) file through DHCP option 252.

Procedure

1. In the system web interface, go to **Network > Primary Network > Web Proxy Settings**.
2. Select **Automatic Configuration**.
3. Select **Enable WPAD**.
This option enables the web proxy auto-discovery protocol (WPAD), which helps your system automatically download the PAC file on your network using DHCP option 252.
4. Enter the **Proxy Username** and **Proxy Password**.
5. Select **Save**.

Your system automatically downloads and reads the PAC file specifying the proxy rules. The system also automatically downloads subsequent files before the current file expires.

Set Up Semi-Automatic Web Proxy Configuration

With semi-automatic web proxy configuration, you must specify the URL your G7500 system uses to download a proxy auto-configuration (PAC) file.

Procedure

1. In the system web interface, go to **Network > Primary Network > Web Proxy Settings**.
2. Select **Automatic Configuration**.
3. If checked, clear the **Enable WPAD** check box.
4. Enter the **Proxy Username** and **Proxy Password**.
5. Enter the **PAC URL** from which your system downloads the PAC file.
6. Select **Save**.

Your system automatically downloads and reads the PAC file specifying the proxy rules. The system also automatically downloads subsequent files before the current file expires.

Manually Update the PAC File on the System

Even if you set up your G7500 system for automatic or semi-automatic web proxy configuration, you can still manually download a new PAC file from the server.

The PAC file may update on the server much sooner than its expiration date. In this situation, you don't have to wait for the system to automatically download the latest version.

Procedure

1. In the system web interface, go to **Network > Primary Network > Web Proxy Settings**.
2. Select **Update PAC File** to fetch the latest version of the file from the server.

Manually Configure a Web Proxy

You can manually configure your G7500 system to communicate with a web proxy by providing a proxy address, port, and credentials (if required).

This method lets you configure your system with only one proxy.

Procedure

1. In the system web interface, go to **Network > Primary Network > Web Proxy Settings**.
2. If checked, clear the **Automatic Configuration** check box.
3. Enter the **Proxy Address** and **Proxy Port**.
4. Enter the **Proxy Username** and **Proxy Password**.
5. Select **Save**.

View Connections to the System

You can see a list of current connections to your G7500 system.

You can find the following information in the list:

- Type of connection (for example, web)
- ID associated with the session (for example, admin or user)
- Remote address (IP addresses of the hosts accessing your system)

This list doesn't show details related to sharing content. For example, if someone shares a video from an AirPlay-certified device or HDMI-connected laptop, you don't see that those devices are connected to the system.

Procedure

1. In the system web interface, go to **Diagnostics**.
2. Go to **Sessions**.

Port Usage

The following table lists the inbound, outbound, and bidirectional ports used by the G7500 system.

G7500 System Port Usage

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
22	Inbound	Static	SSH	Comand-line API access over SSH	No	No
23	Inbound	Static	TCP	Comand-line API access over telnet	No	No
24	Inbound	Static	TCP	Comand-line API access over telnet	No	No
53	Outbound	Static	UDP	DNS	Yes	No
80	Inbound	Static	TCP	HTTP web server listener that provides access to the web interface. Redirects all sessions to HTTPS on port 443 and is used by AirPlay.	Yes	Yes
123	Outbound	Static	UDP	NTP (automatic time synchronization)	Yes	No
161	Inbound	Static	UDP	SNMP reporting	No	Yes

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
443	Bidirectional	Static	TCP/SCTP	Static TCP HTTPS web server listener that provides TLS access to the web interface. AirPlay Microsoft Exchange Server Provisioning (for example, RealPresence Resource Manager) REST API Polycom Content App	Yes	No
514	Outbound	Static	UDP	Remote logging	No	Yes
554	Inbound	Static	TCP, UDP	AirPlay (Real-Time Streaming Protocol [RTSP])	No	No
601	Outbound	Static	TCP	Remote logging	No	Yes
1718	Outbound	Static	UDP	H.255.0 gatekeeper discovery	No	No
1719	Bidirectional	Static	UDP	H.255.0 RAS signaling	No	Yes (outbound) No (inbound)
1720	Bidirectional	Static	TCP	H.255.0 call signaling	Yes	No
1900	Inbound	Static	UDP	AirPlay/Bonjour (Simple Service Discovery Protocol [SSDP])	Yes	No
3689	Inbound	Static	TCP	iTunes Music Sharing/AirPlay (Digital Audio Access Protocol [DAAP])	Yes	No

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
4100–4115	Bidirectional	Static	TCP	AirPlay (audio control)	Yes	No
4100–4115	Inbound	Static	UDP	AirPlay (audio data)	Yes	No
4443	Bidirectional	Static	TCP/TLS	Web server for peripheral device software downloads and log uploads	Yes	No
5001	Inbound	Static	TCP/TLS	Polycom Content App	Yes	No
5060	Bidirectional	Static	TCP or UDP, depending the on configuration	SIP	Yes	No
5061	Bidirectional	Static	TLS	SIP	Yes	No
5127	Outbound	Static	TCP	Polycom usage data collection	No	No
5297	Inbound	Static	TCP	Bonjour	Yes	No
5298	Inbound	Static	TCP	Bonjour	Yes	No
5353	Inbound	Static	UDP	Bonjour/AirPlay (multicast Domain Name System [mDNS])	Yes	No
6514	Outbound	Static	TLS	Remote logging	No	Yes
7000	Inbound	Static	TCP	AirPlay standard services	Yes	No
7080	Inbound	Static	TCP	Web services	Yes	No
7081	Inbound	Static	TCP	Web services	Yes	No
7100	Inbound	Static	TCP	AirPlay mirroring services	Yes	No
7236	Inbound	Static	TCP	Miracast services	Yes	No
16384–32764	Bidirectional	Dynamic	UDP	RTP/RTCP (video and audio streams)	Yes	Yes
44444	Inbound	Static	TCP	Content stream	Yes	No

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
47000	Inbound	Static	TCP	AirPlay casting services	Yes	No
49152–65535	Bidirectional	Dynamic	TCP	H.245	Yes	Yes
49159	Inbound	Static	UDP	Bonjour/AirPlay (mDNS [Windows])	Yes	No
49163	Inbound	Static	UDP	Bonjour/AirPlay (mDNS [Windows])	Yes	No

Configuring Call Settings

Topics:

- [Configure Call Settings](#)
- [Configure Dialing Options](#)
- [Set Call Answering Mode](#)
- [Set Preferred Call Speeds](#)
- [Configure the Recent Calls List](#)
- [Clear Recent Calls](#)

Specify how you want your G7500 system to handle and manage calls.

Related Links

[Configure H.323 Settings](#) on page 34

[Configure SIP Settings](#) on page 36

Configure Call Settings

You can configure call settings in the G7500 system web interface.

Procedure

1. In the system web interface, go to **Call Configuration > Call Settings**.
2. Configure the following settings:

Setting	Description
Maximum Time in Call	<p>Sets the maximum number of hours allowed for a call.</p> <p>When the maximum time expires, the system prompts the user to hang up. If the user doesn't answer within one minute, the call automatically ends. If the user chooses to stay in the call, the system doesn't prompt the user again.</p>
Auto Answer Point-to-Point Call	<p>Specifies whether the system answers an incoming call when not in a call. Choose one of the following options:</p> <ul style="list-style-type: none">▪ Yes: The system automatically answers incoming point-to-point calls.▪ No: Users must answer incoming calls manually.▪ Do Not Disturb: The system rejects incoming calls without notification.

Setting	Description
Display Icons in a Call	Specifies whether to display onscreen graphics, including icons and help text, during calls.
Enable Flashing Incoming Call Notification	Specifies whether you see an incoming call notification.
Preferred 'Place a Call' Navigation	Specifies the default options that display on the local interface Place a Call screen. Choose one of the following options: <ul style="list-style-type: none"> ▪ Keypad: Displays recently-dialed numbers and a dialpad. ▪ Contacts: Displays a screen for searching a directory. The multitiered directory (LDAP) root entry displays at the top of the Contacts list, which combines your search results and favorites. ▪ Recent Calls: Lists previous calls in chronological order.

3. Select **Save**.

Related Links

[Configure General Audio Settings](#) on page 69

Configure Dialing Options

You can specify video and audio dialing preferences for your G7500 system.

Procedure

1. In the system web interface, go to **Call Configuration > Dialing Preference**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Scalable Video Coding Preference (H.264)	This read-only setting indicates your system uses only AVC conferencing. Note: Scalable video coding (SVC) conferencing isn't supported.
Enable H.239	Enables the use of a standards-based specification for parallel video streams (people and content). Enable this setting if you know call participants support H.239.
Enable Audio-Only Calls	Enables you to place audio-only calls on the system.

Setting	Description
Call Type Order	Specifies an order preference for video or voice calls. Select either Video then Phone , or Phone then Video . This setting is read-only if the video system has no phone connections.
Video Dialing Order Preferences	<p>Specifies how the system places video calls to directory entries with more than one type of number.</p> <p>Select one of the following protocols for each preference:</p> <ul style="list-style-type: none"> ▪ IP H.323 ▪ SIP <p>This setting also determines how the system places video calls from the Place a Call screen when you set the call protocol to Auto or if it's unavailable. For example, if a call doesn't connect with H.323, the system tries using SIP.</p>
Audio Dialing Order Preferences	<p>Specifies how the system places audio calls to directory entries with more than one type of number.</p> <p>Select one of the following protocols for each preference:</p> <ul style="list-style-type: none"> ▪ H.323 ▪ SIP

Set Call Answering Mode

You can configure how users answer calls on the G7500 system.

Procedure

1. In the system web interface, go to **Call Configuration > Call Settings**.
2. Select one of the following for **Auto Answer Point-to-Point Call**:
 - **Yes**: The system automatically answers incoming calls.
 - **No**: Users must answer incoming calls manually.
 - **Do Not Disturb**: The system rejects incoming calls without notification.

Set Preferred Call Speeds

You can configure call speeds in the G7500 system web interface.

Procedure

1. In the system web interface, go to **Call Configuration > Dialing Preference**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Preferred Speed for Placed Calls	<p>Determines the IP call speed your system uses when either of the following occurs:</p> <ul style="list-style-type: none"> ▪ A user sets the call speed to Auto on the Place a Call screen. ▪ A user places a call from the directory. <p>If the far-site system doesn't support the selected speed, the system automatically negotiates a lower speed.</p>
Maximum Speed for Received Calls	The system doesn't receive calls at a higher rate than the speed you set here.

Configure the Recent Calls List

You can display recent calls on the **Place a Call** page in the G7500 system web interface.

The recent calls list includes the following information:

- Name or number
- If the system placed or received the call
- Date and time

Procedure

1. In the system web interface, go to **Call Configuration > Recent Calls**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Call Detail Report	Call detail records (CDRs) are in the system logs. When disabled, the system doesn't write call information.
Enable Recent Calls	Specifies whether to show recent calls on the local interface and the system web interface.
Maximum Number to Display	The maximum number of calls the system displays in the recent calls list.

Clear Recent Calls

You can clear the recent calls list from the G7500 system web interface.

Procedure

1. In the system web interface, go to **Call Configuration > Recent Calls**.
2. For **Clear Recent Calls**, select **Clear** and confirm your choice.

Configuring Audio Settings

Topics:

- [Configure General Audio Settings](#)
- [Audio Input](#)
- [Audio Output](#)
- [Audio I/O Specifications](#)

You can configure audio settings in the G7500 system web interface.

Configure General Audio Settings

You can specify general audio settings for your G7500 system.

If you are in a call with a far site that is sending audio in stereo mode, you can receive in stereo. In calls where some sites can send and receive stereo but some can't, any site set up to send or receive stereo can do so.

Note: Some audio settings are unavailable when you connect a SoundStructure digital mixer to your system.

Procedure

1. In the system web interface, go to **Audio/Video > Audio > General Audio Settings**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Polycom StereoSurround	Enables Polycom StereoSurround software for all calls. To use StereoSurround, make sure you correctly configure your system's stereo settings. Note: Enabling this setting disables Polycom Acoustic Fence technology and vice versa.
Sound Effects Volume	Sets the volume level of the ringtone and user alert tones.
Ringtone	Specifies the ringtone for incoming calls.
User Alert Tones	Specifies the tone for user alerts.
Audio Mute Auto-Answered Calls	Specifies whether to automatically mute incoming calls. Note: You must first enable Auto Answer Point-to-Point Video in Call Settings to use this feature.

Setting	Description
Enable M-Mode	<p>Specifies whether the system transmits audio using a configuration that best reproduces interactive and live performance music picked up by microphones. This feature provides the highest-possible bandwidth for audio.</p> <p>When you enable M-Mode, even the faintest musical notes come through clearly.</p>
Enable Keyboard Noise Reduction and Polycom NoiseBlock	<p>Specifies whether the system microphones mute when the system detects keyboard typing or other extraneous noises but no one is talking. NoiseBlock unmutes the system when it detects speech, regardless if there's background noise or not.</p> <p>Note: This setting is disabled when you enable M-Mode. If you use an external echo canceller, keyboard noise reduction is not available.</p>
Enable Join and Leave Tones	The system plays a tone when someone joins or leaves a conference call.
Transmission Audio Gain (dB)	Specifies the audio level (in decibels) that the system transmits sound. Unless otherwise advised, Polycom recommends setting this value to 0 dB.
Enable Audio Mute Reminder	Specifies if the system displays a notification that the microphones are muted when it detects someone speaking.

Related Links

[Configure Sleep Settings](#) on page 23

[Configure Call Settings](#) on page 65

[Test Speakers](#) on page 118

[Test Polycom StereoSurround](#) on page 118

Audio Input

You have several options to input audio for your G7500 system.

Your system supports the following audio inputs:

- IP-based Polycom audio peripheral devices:
 - **Polycom IP Table Microphone**
 - **Polycom IP Ceiling Microphone**
 - **Polycom Microphone IP Adapter**
- **3.5 mm:** 3.5 mm line-level stereo input used to share audio from a device or line-in microphone. Depending on your setup, you can specify if sound from this input plays in the room and at far sites or just at far sites.
- **HDMI:** Used to share audio (along with content) from a device. Sound from this input plays in the room and at far sites.

Configure IP Microphones

You can configure IP table and ceiling microphone settings for your G7500 system.

Procedure

1. In the system web interface, go to **Audio/Video > Audio > Audio Input**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Stereo Mode	Positions the audio input within the left and right channels. Left sends all of the audio to the left channel. Right sends all of the audio to the right channel. For Polycom table microphone and ceiling microphones, Left+Right sends audio from one microphone element to the left channel and audio from a second element to the right channel.
Autorotation	Specifies whether the system uses autorotation for Polycom microphones. If you enable this feature, the system automatically assigns left and right channels for the microphone based on the sound it senses from the left and right speakers.
Audio Meter (dB)	Shows you the peak input signal level for Polycom microphones.

Configuring the Microphone Adapter

Your G7500 system automatically configures the microphone adapter when you connect it.

Note the following when using the microphone adapter:

- Polycom StereoSurround software isn't available when using the microphone adapter.
- You can see the audio input level (single channel meter) in the local interface and the system web interface.

Related Links

[Polycom Microphone IP Adapter](#) on page 16

Polycom Acoustic Fence

Polycom Acoustic Fence technology uses standard Polycom microphones to build a virtual audio boundary around one or several people.

This feature works in mono mode only. Enabling Polycom Acoustic Fence disables Polycom StereoSurround.

Polycom Acoustic Fence technology provides the following features:

- Mutes sounds outside the fence when no one is speaking inside it
- Lowers sounds outside the fence by 12 dB when someone is speaking inside it.
- Mutes speakers when they leave the fenced area

In addition to the primary microphone, you need at least one more microphone to create the fence. You can connect up to three IP microphones directly to your G7500 system.

The boundary radius can be from two to several feet around the following Polycom peripheral devices:

- Table microphone
- Ceiling microphone

Note: Microphones connected to a Polycom Microphone IP Adapter currently don't support Polycom Acoustic Fence technology.

For more details on Polycom Acoustic Fence technology, search the [Polycom Knowledge Base](#) for *acoustic fence*.

Related Links

[IP Microphones](#) on page 14

Related Links

[Fix Polycom Acoustic Fence Issues](#) on page 119

Configure Polycom Acoustic Fence

You can configure your G7500 system to use Polycom Acoustic Fence technology.

Note: This option isn't available if you enable **Polycom StereoSurround**.

Procedure

1. In the system web interface, go to **Audio/Video > Audio > General Audio Settings**.
2. Select the **Enable Acoustic Fence** check box.
3. Set **Acoustic Fence Sensitivity** from 0 to 10, where 0 is the minimum microphone sensitivity and 10 is the maximum.

Higher values increase the radius of the fence area around the primary microphone.

Specify the Primary and Fence Microphones

To use Polycom Acoustic Fence technology with your G7500 system, you need a primary microphone to pick up audio and one or more fence microphones to define the audio boundary.

The system considers the first microphone you pair to be the primary microphone. By default, a microphone pairs to the system when you connect it (unless you've disabled automatic pairing).

Note: If you use a mix of table and ceiling microphones, the primary microphone must be a table microphone. The primary microphone can be a ceiling microphone if you use only that type of microphone.

Procedure

1. Connect the primary microphone to an **LLN port**  on the back of your system.

Caution: When using Polycom Acoustic Fence technology, remember which microphone is the primary one. If you disconnect this microphone, Polycom Acoustic Fence no longer works and you have to reconnect all microphones (starting with the primary microphone) for it to work again.

2. Connect the other microphone(s).

Related Links


[System Back Panel Ports](#) on page 10

Specify a Different Primary Microphone

If you want to change the primary microphone you're using for Polycom Acoustic Fence technology, you must first disconnect all the microphones from your G7500 system.

Note: If you use a mix of table and ceiling microphones, the primary microphone must be a table microphone. The primary microphone can be a ceiling microphone if you use only that type of microphone.

Procedure

1. Disconnect all microphones from the **LLN ports**  on the back of your system.
2. Reconnect the microphone you want to be the primary.
Your primary microphone is set up.
3. Connect the other microphone(s).

Your system is ready to use Polycom Acoustic Fence with a new primary microphone.

Configure 3.5 mm and HDMI Audio Input

You can configure the audio input settings for your G7500 system.

Procedure

1. In the system web interface, go to **Audio/Video > Audio > Audio Input**.
2. Configure the following settings (your changes save automatically):
Settings vary depending on the audio input source.

Setting	Description
Audio Input Level	Sets levels for the left and right channels. Choose a value from 0 to 10.

Setting	Description
Playback Options	<p>(3.5 mm only) Specifies how the system routes and controls audio from the 3.5 mm stereo audio input.</p> <ul style="list-style-type: none"> ▪ Playback to All Locations (Default): <ul style="list-style-type: none"> ◦ The 3.5 mm stereo audio input is heard on the system's speakers and at far sites. ◦ Mute control and echo cancellation aren't available. ◦ Select this option if you're sharing audio from a device. ▪ Playback to Far Sites, Mute Controlled, Echo Cancelled: <ul style="list-style-type: none"> ◦ The 3.5 mm stereo audio input is heard at far sites but not on the system's speakers. ◦ You can mute all audio and echo cancellation is enabled. ◦ Select this option if you're using a line-in microphone.
Audio Meter (dB)	Displays the audio level of the input (left and right channels).

Audio Output

You have different options to play audio on your G7500 system to fit your setup: You can use the primary monitor's built-in speakers, or you can connect an external speaker system (such as the Polycom StereoSurround kit) to provide more volume and comprehensive sound in large rooms.

See your system setup sheet for connection details. Make sure that you power off the system before connecting anything to it.

Configure Audio Output Settings

You can configure the audio output settings for your G7500 system.

Procedure

1. In the system web interface, go to **Audio/Video > Audio > Audio Output**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Master Audio Volume	Sets the main audio output volume level going to the speakers.
Bass	Sets the volume level for low frequencies without changing the master audio volume.

Setting	Description
Treble	Sets the volume level for high frequencies without changing the master audio volume.
Output Mode	Specifies how the system configures the volume for a device connected to the line out port. <ul style="list-style-type: none"> ▪ Variable: Enables users to set the volume with the remote control. ▪ Fixed: Sets the volume to the audio level configured for the system.
Audio Meter (dB)	Displays the audio level of the output (left and right channels).

Using 3.5 mm Audio Output

If you want to use the 3.5 mm stereo line output to hear audio in the room, make sure you mute the monitor(s) connected to your G7500 system through HDMI.

Audio I/O Specifications

The following table provides audio input and output specifications for your G7500 system.

G7500 Audio I/O Specifications

Characteristic	Value
Maximum input level, line input	+6 dBV (2.0 V _{RMS}), ± 1 dB
Input impedance, line input	45 kΩ, ± 5 %
Maximum output level, line output (≥ 600 Ω load)	+6 dBV (2.0 V _{RMS}), ± 1 dB
Output impedance, line output	150 Ω, ± 5 %
Signal-to-noise ratio: Line input routed to line output	>85 dB, A-weighted
Signal-to-noise ratio: HDMI input routed to either HDMI output	>95 dB, A-weighted
Dynamic range: Line input routed to line output	>85 dB, A-weighted
Dynamic range: HDMI input routed to either HDMI output	>95 dB, A-weighted
Crosstalk and feed-through (any input or output channel to any other channel)	≤-80 dB, 20 Hz to 20 kHz
Frequency response (any input to any output, relative to 997 Hz)	+1, -3 dB, 50 Hz to 20 kHz
Total harmonic distortion + noise vs. frequency	Better than -75 dB, 50 Hz to 20 kHz

Configuring Video and Camera Settings

Topics:

- [HDMI Connections](#)
- [Configure Monitor Settings](#)
- [Configure a Touch Monitor](#)
- [Configure Camera Settings](#)
- [Configure Video Input Settings](#)
- [Video Codec Capabilities](#)

You can configure video settings for your G7500 system, including monitors and cameras.

Use the HDMI input resolutions and video codec capabilities to further enhance your video experience, based on your deployment requirements.

HDMI Connections

Your G7500 system has three HDMI ports so you can have dual monitors and an HDMI content source.

Your system has the following HDMI connections:

- Output for connecting the primary system monitor (Monitor 1)
- Output for connecting the secondary system monitor (Monitor 2)
- Input for content sharing, including audio streaming

The system supports only HDMI-to-HDMI connections and doesn't support display conversions, such as VGA-to-HDMI or HDMI-to-DVI cable converters.

Note: Polycom claims no responsibility or liability for the quality, performance, or reliability of third-party HDMI cables, HDMI splitters, or HDMI USB adapters. Contact your Polycom distributor or representative to order parts that meet the appropriate manufacturing tolerances, quality, and performance parameters for your deployment.

Related Links

[System Back Panel Ports](#) on page 10

Supported HDMI Output Resolutions for Single-Monitor Setups

Your G7500 system supports the following HDMI output resolutions and frame rates when using one monitor.

Supported HDMI Output Resolutions and Frame Rates for Single-Monitor Setups

Output	Resolution	Frame Rates (fps)
UHD (4K)	3840 × 2160p	25, 30, 50, 60

Output	Resolution	Frame Rates (fps)
FHD	1920 × 1080p	50, 60

Supported HDMI Output Resolutions for Dual-Monitor Setups

Your G7500 system supports the following HDMI output resolutions and frame rates when using two monitors.

Note: 4K resolution (3840 × 2160p) isn't supported when you configure your system for dual monitors. If you want to use 4K, set Monitor 2 to **Off** in the system web interface.

Supported HDMI Output Resolutions and Frame Rates for Dual-Monitor Setups

Output	Resolution	Frame Rates (fps)
FHD	1920 × 1080p	50, 60

Supported HDMI Input Resolutions

Your G7500 system supports the following monitor resolutions for HDMI input.

Supported HDMI Input Resolutions and Frame Rates

Input	Resolution	Frame Rates (fps)
UHD (4K)	3840 × 2160p	24, 25, 30
FHD	1920 × 1080p	50, 60
HD	1280 × 720p	50, 60

Configure Monitor Settings

You can optimize your G7500 system video output for single- and dual-monitor setups.

Interlaced modes aren't supported.

Procedure

1. In the system web interface, go to **Audio/Video > Monitors**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Configure Monitor	<p>Specifies monitor settings.</p> <ul style="list-style-type: none"> ▪ Automatic: (Default) Detects the highest-supported resolution of the connected monitors. When you select this option, the Resolution setting is disabled. ▪ Manual: You can choose the monitor Resolution. ▪ Off: Disable this monitor (not available for Monitor 1). <p>Note: To use 4K resolution, make sure you set Monitor 2 to Off.</p>
Resolution	<p>Specifies the monitor resolution. This setting is unavailable when you select Automatic for the Configure Monitor setting.</p> <p>Note: The system uses the resolution you select even if the monitor doesn't support it. There is no dynamic resolution adjustment in this situation.</p>

Related Links

[Configure a Touch Monitor](#) on page 78


[Configure Dual Monitor Display Settings](#) on page 95

Configure a Touch Monitor

In a dual-monitor setup, you must configure the touch monitors to work with your G7500 system.

Note: Touch monitors in single-monitor setups don't require configuration.

Procedure

1. Do one of the following:
 - In a call: Go to **Menu** ≡ > **More ...** > **Settings** ⚙ > **Diagnostics** > **Touch Configuration**.
 - Out of a call: Go to **Menu** ≡ > **Settings** ⚙ > **Diagnostics** > **Touch Configuration**.
2. On each screen, tap the **Hand**  icon.
3. Tap **Finish Configuration**.

Related Links

[Configure Monitor Settings](#) on page 77

[Configure Dual Monitor Display Settings](#) on page 95

Configure Camera Settings

You can configure settings for cameras connected to your G7500 system. When you connect a supported camera, the system automatically discovers it and displays the available camera settings in the system web interface.

See the latest release notes for specific information about the cameras you can use with your G7500.

Note: If you connect an unsupported camera, the system still attempts to show video. Polycom can't guarantee that the results are optimal or that the available settings are the same as a supported camera.

Procedure

1. In the system web interface, go to **Audio/Video > Video Inputs**.
2. Go to **General Camera Settings**.
3. Configure the following settings:

Setting	Description
Allow Other Participants In a Call to Control Your Camera	Specifies whether the far site can pan, tilt, or zoom the near-site camera. When you enable this setting, a user at the far site can control the framing and angle of the camera for the best view of the near site. This is also called Far End Camera Control (FECC).
Power Frequency	Specifies the power-line frequency for your system. Your system typically defaults to the correct power-line frequency based on the video standard used in the country where it's located. This setting helps you adapt the system to areas where the frequency doesn't match the video standard. You might also need to change this setting to avoid flicker from fluorescent lights in the room.
Enable Camera Preset Snapshot Icons	Enables the use of snapshot icons that represent camera presets. To see a preset icon, you must enable this setting before configuring the preset.

Setting	Description
Camera Sleep Mode	<p>Specifies a sleep mode for your camera.</p> <p>Fast Wake Up: The camera provides an image as soon as the monitor wakes. While asleep, the camera faces forward.</p> <ul style="list-style-type: none"> When you set sleep Display to Black, an image more quickly displays, but be aware that this uses maximum power. When you set sleep Display to No Signal, the display synchronizes with the system. This can take a few seconds but may conserve energy depending on the monitor. <p>Save Energy: Puts the camera into standby mode to save power (the camera spins to the rear and faces down).</p> <ul style="list-style-type: none"> When you set sleep Display to Black, it takes a few seconds for the camera to send an image. When you set sleep Display to No Signal, the camera is already sending an image by the time the display synchronizes with the system.

4. Select **Save**.

Related Links

[Update Polycom HDCI Cameras](#) on page 101

[Configure Sleep Settings](#) on page 23

Configure Video Input Settings

You can customize your video input settings, such as enabling connected cameras, adjusting camera orientation, or specifying whether people or content display on connected monitors.

Note: The system doesn't display settings that don't apply to your camera. For example, you don't see tracking options if your connected camera doesn't support tracking.

Procedure

1. In the system web interface, go to **Audio/Video > Video Inputs**.
2. Do one of the following:
 - Go to **Input 1** to configure a **People** source.
 - Go to **Input 2** to configure a **Content** source.

Each source has different settings. For example, a **People** source has pan, tilt, zoom, and near/far camera control settings, while a **Content** source has different settings.

3. Configure the following settings:

Setting	Description
Model	Displays the type of device connected to the system.
Name	Displays the default name of the connected device. You also can enter a name for the device.
Input format	Specifies the source type of the device. This setting is read-only unless the system doesn't detect the device.
Orientation	Specifies whether the display is oriented normally or inverted (upside down).
Optimized for	<p>Specifies optimization preferences for the video input.</p> <ul style="list-style-type: none"> ▪ Sharpness: Gives preference to resolution over frames per second. With this setting, moderate-to-heavy motion at low call rates can cause some frames to drop. ▪ Motion: Gives preference to frames per second over resolution.
Backlight Compensation	Specifies if the camera automatically adjusts for a bright background. Backlight compensation is best used in situations where the subject appears darker than the background.

Setting	Description
White Balance	<p>Specifies how the camera compensates for light source variations in the room. Select Auto, Manual, or a color temperature value.</p> <ul style="list-style-type: none"> ▪ Auto: Polycom recommends this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room. ▪ Manual: Use this setting for rooms where the Auto and fixed values don't provide acceptable color reproduction. <p>When you set this option to Manual, fill the camera's field of view with a flat white object, such as a piece of paper. For best results, the object should be uniformly illuminated with light that is representative of the room lighting used in the conference, rather than light from a display, another area, or a shadow. After the object is in place, select Calibrate.</p> <ul style="list-style-type: none"> ▪ Color Temperature Value: The color temperature values, measured in degrees Kelvin, correspond to the color of ambient light in a room. Because the available color temperature values vary by camera, this list is a sampling of some of the values you might see in the interface: <ul style="list-style-type: none"> ◦ 3200K (warm office fluorescent) ◦ 3680K (tungsten bulb) ◦ 4160K (cool office fluorescent) ◦ 5120K (neutral daylight) ◦ 5600K (cool daylight)
Brightness	Adjusts the video brightness.
Color Saturation	Adjusts the color saturation.

Setting	Description
Tracking Mode	<p>Specifies the camera tracking mode.</p> <ul style="list-style-type: none"> ▪ Frame Speaker: Enables the camera to automatically locate and frame the active speaker. When someone else starts speaking, the camera switches that person. <p>Note: When you mute the local microphone, the camera tracking mode automatically switches to Frame Group.</p> <ul style="list-style-type: none"> ▪ Frame Group: Enables the camera to automatically locate and frame participants in the room without moving the camera. ▪ Frame Group with Transition: (EagleEye Producer camera only) Enables the camera to automatically locate and frame participants in the room while moving the camera. For example, if someone enters the room, you might see the camera pan until that person is in view. ▪ Off: Disables automatic tracking. You must handle all camera control manually.
Tracking Speed	<p>Determines how quickly the camera finds and switches to the new speaker. The room environment can influence how fast the camera locates new speakers.</p>
Framing Size	<p>Specifies the framing view.</p> <ul style="list-style-type: none"> ▪ Wide: Establishes a wide view of meeting participants. ▪ Medium: (Default group framing view) Establishes a medium view of meeting participants. ▪ Tight: Establishes a close-up view of meeting participants
Picture in Picture	<p>When enabled, a picture-in-picture window displays showing a wide angle of the room in addition to the main window showing the primary speaker(s).</p> <p>This setting is available when using a camera with tracking features, such as the EagleEye Director II.</p>

4. Select **Save**.

Video Codec Capabilities

The G7500 system supports H.265 High Efficiency Video Coding (HEVC), H.264 Advanced Video Coding (AVC), and H.263 codec standards.

Related Links

[Polycom G7500 Overview](#) on page 7

[Default Options for Sharing Content](#) on page 93

H.265 High Efficiency Video Coding

From a video call quality standpoint, H.265 gives you up to 1080p at 60 fps for people streams and 4K at 15 fps for content streams.

Note: H.265 is supported only during a point-to-point SIP call with another G7500 system.

Supported H.265 People Stream Resolutions During Calls

The following table includes the H.265 resolutions and frame rates for people streams observed in SIP calls between two G7500 systems.

Resolutions and frame rates are based on the call speed and the **Optimized for** setting of your video input. (For example, **Motion** or **Sharpness**.)

Due to the complexities of system capabilities and the call types and scenarios in your environment, it isn't possible to provide the resolutions and frame rates for calls between a G7500 system and a different type of endpoint. The systems attempt to provide the highest resolutions and the best frame rates in all types of calls.

The information in the following table is based on a camera source capable of 1080p at 60fps.

Supported H.265 People Stream Resolutions During Calls

Call Speed (kbps)	Motion/Sharpness	Resolution	Max Frame Rate (fps)
370–479	Motion	1024 × 576	60
480–1009	Motion	1280 × 720	60
≥1010	Motion	1920 × 1080	60
300–600	Sharpness	1280 × 720	30
600–1199	Sharpness	1920 × 1080	30
≥1200	Sharpness	1920 × 1080	60

Supported H.265 Content Stream Resolutions During Calls

The following table includes the H.265 resolutions and frame rates for content streams observed in SIP calls between two G7500 systems.

Resolutions and frame rates are based on the call speed and the **Optimized for** setting of your video input. (For example, **Motion** or **Sharpness**.)

Due to the complexities of system capabilities and the call types and scenarios in your environment, it isn't possible to provide the resolutions and frame rates for calls between a G7500 system and a different type of endpoint. The systems attempt to provide the highest resolutions and the best frame rates in all types of calls.

Supported H.265 Content Stream Resolutions During Calls

Resolution	Sharpness Max Frame Rate (fps)	Motion Max Frame Rate (fps)
1920 × 1080	30	30
2560 × 1440	30	30
2880 × 1620	15	15
3200 × 1800	15	15
3840 × 2160	15	15

H.264 Advanced Video Coding

Your G7500 system supports H.264 during H.323 and SIP calls.

Supported H.264 People Stream Resolutions During Calls

The following table includes the H.264 resolutions and frame rates for people streams observed in H.323 calls between two G7500 systems.

Resolutions and frame rates are based on the call speed and the **Optimized for** setting of your video input. (For example, **Motion** or **Sharpness**.)

Due to the complexities of system capabilities and the call types and scenarios in your environment, it isn't possible to provide the resolutions and frame rates for calls between a G7500 system and a different type of endpoint. The systems attempt to provide the highest resolutions and the best frame rates in all types of calls.

The information in the following table is based on a camera source capable of 1080p at 60fps.

Supported H.264 People Stream Resolutions During Calls

Call Speed (kbps)	Motion/Sharpness	Resolution	Max Frame Rate (fps)
<160	Motion	512 × 288	60
160–511	Motion	640 × 368	60
512–831	Motion	848 × 480	60
832–895	Motion	720 × 832	60
896–1727	Motion	1280 × 720	60
≥1728	Motion	1920 × 1080	60
<128	Sharpness	640 × 368	30

Call Speed (kbps)	Motion/Sharpness	Resolution	Max Frame Rate (fps)
128–511	Sharpness	1024 × 576	30
512–1023	Sharpness	1280 × 720	30
≥1024	Sharpness	1920 × 1080	30

Supported H.264 Content Stream Resolutions During Calls

The following table includes the H.264 resolutions and frame rates for content streams observed in H.323 calls between two G7500 systems.

Resolutions and frame rates are based on the call speed and the **Optimized for** setting of your video input. (For example, **Motion** or **Sharpness**.)

Due to the complexities of system capabilities and the call types and scenarios in your environment, it isn't possible to provide the resolutions and frame rates for calls between a G7500 system and a different type of endpoint. The systems attempt to provide the highest resolutions and the best frame rates in all types of calls.

Supported H.264 Content Stream Resolutions During Calls

Resolution	Sharpness Max Frame Rate (fps)	Motion Max Frame Rate (fps)
800 × 600	30	60
1024 × 768	30	60
1280 × 720	30	60
1280 × 1024	30	60
1920 × 1080	30	60

Setting Up a Directory

Topics:

- [Register with the Polycom Global Directory Server](#)
- [Register with an LDAP Directory Server](#)
- [Managing Contacts and Favorites](#)

You can register your G7500 system with a directory to call contacts in your organization.

The system supports the following directory features:

- Up to 2,000 Favorites
- Up to 200 Favorites groups
- Global groups (local groups aren't supported)
- Up to 4,000 contacts from a Polycom GDS server

Register with the Polycom Global Directory Server

You can register your G7500 system with the Polycom Global Directory Server (GDS).

Enable H.323 on your system before you register it with this directory server.

Procedure

1. In the system web interface, go to **Servers > Directory Servers**.
2. In the **Server Type** field, select **Polycom GDS**.
3. Configure the following settings:

Setting	Description
Server Address	Specifies the IP or DNS address of the Polycom GDS.
Password	The Polycom GDS password, if one exists.

4. Select **Save**.

Register with an LDAP Directory Server

You can register your G7500 system with an LDAP directory server.

Procedure

1. In the system web interface, go to **Servers > Directory Servers**.
2. In the **Server Type** field, select **LDAP**.
3. Configure the following settings:

Setting	Description
Server Address	Specifies the address of the LDAP directory server. When provisioned, this setting is read-only.
Server Port	Specifies the port for connecting with the LDAP server. When provisioned, this setting is read-only.
Base DN (Distinguished Name)	Specifies the top level of the LDAP directory where searches begin. When provisioned, this setting is read-only. To avoid LDAP registration issues, make sure the base DN is at least one level deeper than your domain. For example, enter <code>ou=users,dc=example,dc=com</code> instead of <code>dc=example,dc=com</code> .
Multitiered Directory Default Group DN	Specifies the top-level group of the LDAP directory required to access its hierarchical structure. When provisioned, this setting is read-only.
Authentication Type	Specifies the protocol for authenticating with the LDAP server: NTLM , Basic , or Anonymous .
Bind DN (Distinguished Name)	Specifies the bind DN when using basic authentication. Available only when you set Authentication Type to Basic . When provisioned, this setting is read-only.
Use SSL (Secure Socket Layer)	When enabled, encrypts data to and from the LDAP server.
Domain Name	Specifies the domain name for registering with the LDAP server.
User Name	Specifies the user name for registering with LDAP server.
Password	Specifies the password for registering with the LDAP server.

4. Select **Save**.

Related Links

[Configure Minimum TLS](#) on page 56

[LDAP Directory Server Ignores the Minimum TLS Version Setting](#) on page 120


Managing Contacts and Favorites

You can create local contacts and designate favorites for your G7500 system.

Manage Contacts

You can add contacts individually or in bulk in the G7500 system web interface.

Procedure

1. Do one of the following:
 - Go to **Dashboard > Contacts**.
 - Go to **Place a Call > Contacts**.
2. Select **More**  and choose one of the following options:
 - **New Contact**: Create a single contact.
 - **Import**: Upload contacts in bulk using an XML file (can't exceed 3 MB).
 - **Export**: Download local contacts to an XML file (doesn't include contacts available through a directory server).

Types of Favorites

The G7500 system web interface displays several types of favorites.

Directory Server Registration	Types of Contacts
Polycom GDS	<ul style="list-style-type: none"> ▪ Directory entries created locally by the user. ▪ References to Polycom GDS entries added to Favorites by the user. <p>These entries are available only if you successfully register the system with Polycom GDS. Users can delete these entries from Favorites, but they can't edit these entries. Users can copy these entries to other Favorites and remove them from those groups.</p>
LDAP with H.350	<ul style="list-style-type: none"> ▪ Directory entries created locally by the user. ▪ References to LDAP directory entries added to Favorites by the user. <p>These entries are available only if the system can successfully access the LDAP server. Users can delete these entries from Favorites, but they can't edit these entries. Users can copy these entries to other Favorites and remove them from those groups.</p>

Registering with a Calendaring Service

Topics:

- [Configure a Calendaring Service](#)

Your G7500 system can display calendar details linked to a Microsoft Outlook or Office 365 account.

The system retrieves this information from Microsoft Exchange Server with credentials you provide or through automatic discovery using an associated email or SIP server address.

Your system performs the following actions when you configure it to use a calendaring service:

- Displays the day's scheduled meetings, including details about each
- Lets users join a meeting with one click or touch
- Hides details about meetings marked private (depending on how you configure the system)
- Displays a meeting reminder and plays a reminder tone before the next scheduled meeting

Configure a Calendaring Service

You must configure your G7500 system to use a calendaring service so users can see scheduled meetings on the local interface.

Procedure

1. In the system web interface, go to **Servers > Calendaring Service**.
2. Select the **Enable Calendaring Service** check box.
3. Configure the following settings:

Setting	Description
Email	Specifies the email address used when scheduling the system for a meeting (for instance, you can use your system as a mechanism to reserve a meeting space). This email address must match the Primary SMTP Address for the account on Microsoft Exchange Server, which displays as the value of the mail attribute in the account properties.
Domain	Specifies the domain to register to the Microsoft Exchange Server in NETBIOS or DNS notation (for example, <code>company.local</code> or <code>COMPANY</code>). If you are using the Auto Discover Using setting in the system web interface, don't provide a value here.

Setting	Description
<p>User Name</p>	<p>Specifies the user name to register to the Microsoft Exchange Server. This can be the name of the system or an individual (for example, <code>username@company.com</code>).</p> <p>If you want to use the calendar associated with an Office 365 account, enter the user name for that account here.</p>
<p>Password</p>	<p>Specifies the system password to register to the Microsoft Exchange Server. This can be the system's or an individual's password.</p> <p>If you want to use the calendar associated with an Office 365 account, enter the password for that account here.</p>
<p>Auto Discover Using</p>	<p>Specifies how the system obtains the Microsoft Exchange Server address. If you select Email Address, the system uses the value provided in the Email field. If you select SIP Server, the system uses the registered SIP server domain name configured for the system.</p> <p>With either option, you must complete the Email, User Name, and Password fields that correspond to the account you want the system to use for the calendaring service. The system may prompt you to confirm the password.</p> <p>Note: This feature is unavailable if the Microsoft Exchange Server address is provisioned.</p> <p>If after configuring the calendaring service a message displays that the system is unable to discover the service, verify that the information you provided is correct.</p> <p>You can also use an API command to automatically discover the Microsoft Exchange Server address. For more information, go to Polycom Support.</p>
<p>Microsoft Exchange Server</p>	<p>Specifies the FQDN of the Microsoft Exchange Client Access server. If your organization has multiple servers behind a network load balancer, this is the FQDN of the server's virtual IP address. If required, you can use an IP address instead of an FQDN, but Polycom recommends using the same FQDN for Outlook clients.</p> <p>Provide a value here only if you want to manually provide connection information to the Microsoft Exchange Server. Otherwise, use the Auto Discover Using setting to automatically populate this field.</p>

Setting	Description
Meeting Reminder Time in Minutes	Specifies the number of minutes before the meeting that a reminder displays on the system.
Play Reminder Tone When Not in a Call	Specifies whether to play a sound along with the text reminder (when the system is not in a call).
Show Information for Meetings Set to Private	Specifies whether to display details about meetings marked private.

4. Select **Save**.

After you register your system to the calendaring service, users can join scheduled meetings from the **Home** and **Calendar** screens on the local interface.

Sharing Content

Topics:

- [Default Options for Sharing Content](#)
- [Disable Screen Mirroring Options](#)

Your G7500 system provides several ways to share and annotate content.

Related Links

[End a Content Session from the System Web Interface](#) on page 9

[Disable the Security Code](#) on page 54

[Limit or Disable the Ability to Save Content](#) on page 55

Default Options for Sharing Content

Once your G7500 system is running and configured for your environment, users can share content from their personal devices with no additional setup using the following methods:

- **Wireless screen mirroring:**
 - A Miracast-certified device screen is mirrored onto the system display.
 - An AirPlay-certified device screen and any accompanying audio is mirrored onto the system display.

You can disable these options in the system web interface.

- **Wired input:** A laptop or desktop connected through HDMI on the back of the system.
- **Polycom Content App:** Installed on a Microsoft Windows or Apple Mac system for wireless screen or application sharing.

Related Links

[Video Codec Capabilities](#) on page 84

Related Links

[Disable Wireless Options](#) on page 40

Disable Screen Mirroring Options

You can disable content sharing with Miracast- or AirPlay-certified devices (screen mirroring) without turning off wireless connectivity or Bluetooth on your G7500 system. Screen mirroring options are enabled by default.

Procedure

1. In the system web interface, go to **Security > Wireless Security**.
2. Do one of the following:
 - Clear the **Enable AirPlay** check box to disable screen mirroring with AirPlay-certified devices.
 - Clear the **Enable Miracast** check box to disable screen mirroring with Miracast-certified devices.

Customizing the Local Interface

Topics:

- [Change the Home Screen Background Image](#)
- [Restore the Default Background Image](#)
- [Customize the Address Bar](#)
- [Display Meetings or Favorites on the Home Screen](#)
- [Configure Dual Monitor Display Settings](#)

You can configure some of the G7500 system local interface settings according to your preferences.

Change the Home Screen Background Image

You can upload a custom background image to display on your G7500 system monitor(s).

The image must have a 16:9 resolution between 1280 × 720 and 3840 × 2160 (Polycom recommends 1920 × 1080, 2560 × 1440, or 3840 × 2160). The system supports JPEG and PNG formats with a file size of less than 10 MB.

Note: This option is unavailable if your image is provisioned to the system.

Procedure

1. In the system web interface, go to **General Settings > Home Screen**.
2. Select **Choose File**, navigate to the image file, then select **Upload**.

The custom image displays on your monitor(s).

Restore the Default Background Image

You can switch back to the default background image to display on your G7500 system monitor(s).

Procedure

1. In the system web interface, go to **General Settings > Home Screen**.
2. Select **Use Default Background**.

Customize the Address Bar

You can customize what displays in the address bar of the G7500 system local interface home screen.

The address bar is under the room name. You can list two of the following details:

- Primary IP Address
- Guest Wi-Fi IP Address
- H.323 Extension
- SIP Address

- None

Procedure

1. In the system web interface, go to **General Settings > Home Screen**.
2. Choose options for **Primary Element** and **Secondary Element** (your changes save automatically).

Display Meetings or Favorites on the Home Screen

You can display meeting information or favorite contacts on the home screen of the G7500 system local interface.

Procedure

1. In the system web interface, go to **General Settings > Home Screen**.
2. Configure the following settings (your changes save automatically):

Setting	Description
None	Hides the home screen widget.
Calendar	Displays meeting information on the home screen.
Favorites	Displays favorites on the home screen.

Configure Dual Monitor Display Settings

You can choose your Self View and content display preferences when you connect two monitors to your G7500 system.

Even if your system has only one monitor, you can still configure second monitor settings. These settings take effect once you connect a second monitor.

Procedure

1. In the system web interface, go to **Audio/Video > Monitors**.
2. Configure the following settings (your changes save automatically):

Setting	Description
Self View Size	<p>Specifies how the self view window displays when others join a call.</p> <ul style="list-style-type: none"> ▪ Corner: Displays Self View in the corner of Monitor 2. ▪ Full Screen: Displays Self View on the entire screen of Monitor 2.

Setting	Description
Content Display	Specifies whether to display content on one or two monitors. <ul style="list-style-type: none">▪ Single: Display content on Monitor 2 and people on Monitor 1.▪ Dual: Display people and content on Monitor 1 and content only on Monitor 2.

Related Links

[Configure Monitor Settings](#) on page 77

[Configure a Touch Monitor](#) on page 78

System Maintenance

Topics:

- [Activating System Features](#)
- [Unlock System Settings](#)
- [Updating Software](#)
- [Downgrading Software](#)
- [Restart the System](#)
- [Reset System Settings](#)
- [Factory Restore the System](#)
- [Factory Restore a Table Microphone](#)
- [Factory Restore a Ceiling Microphone](#)
- [Factory Restore a Microphone Adapter](#)
- [SNMP Reporting](#)

You can perform several functions to keep your G7500 system running properly.

Activating System Features

The G7500 system uses keys to identify the features and software updates you ordered.

Obtain a Feature Activation or Software Version Key

To activate features or update software, you must obtain a key that's valid only with your system. If you don't have a support agreement, contact an authorized Polycom dealer to get a key.

A *key* is a number that unlocks certain features or gives you the ability to update your G7500 system.

You can obtain one of the following key types:

- **Feature activation key** makes new system features available and is valid for all software releases.

Note: Software version 2.0 enables all available G7500 system features by default. With this version, you don't need to enter a feature activation key.

- **Software version key** is valid for the update you want to install and any future feature, maintenance, or patch releases.

Procedure

1. Go to **Licensing & Product Registration > Activation/Upgrade** at [Polycom Support](#).
2. Select the product name in the prompted list.
3. Do one of the following:
 - Log in with your email address and password.
 - Register as a new user.

4. Do one of the following:
 - To update one system, select **Site & Single Activation/Upgrade**. Follow the onscreen instructions to enter your system serial number and license. Go to the **Upgrade** tab to confirm the version upgrade key code.
 - To update multiple systems that are covered by a software service agreement, select **Batch Upgrade** and then select your product. Follow the onscreen instructions to upload the text file that contains your system license and serial numbers (or serial numbers only).

The **Batch Activation** option isn't available for version 2.0.

Activate Features

To activate certain features for your G7500 system, you must enter a feature activation key.

Procedure

1. In the system web interface, go to **General Settings > License**.
2. Enter the **Feature Activation Key** you obtained for your system.
3. Select **Save**.

Get the Latest Software

To update your G7500 system, you must first enter a software version key.

Procedure

1. In the system web interface, go to **General Settings > License**.
2. Enter the **Software Version Key** you obtained for your system.
3. Select **Save**.

Unlock System Settings

Some settings in the local interface are locked by default. You can unlock these settings with your G7500 system's local administrator credentials.

Procedure

1. Do one of the following:
 - In a call, select **Menu** ≡ > **More ...** > **Settings** ⚙️.
 - Out of a call, select **Menu** ≡ **Settings** ⚙️.
2. Select a setting with a **Lock** 🔒.
3. Enter your local administrator credentials to unlock the setting.

Note: Settings lock again if you exit the **Settings** screen, restart the system, or power off the system.

Updating Software

You can update your G7500 system software a few different ways.

Use one of the following methods to update system software:

- Polycom download server
- Custom server URL
- Software package you obtain from [Polycom Support](#) and upload with a USB flash drive
- Provisioning service (for example, RealPresence Resource Manager)

When you update your system, you also update some of its connected peripheral devices (if those devices have a new version available). Depending on your setup, these devices might include:

- Polycom IP Table Microphone
- Polycom IP Ceiling Microphone
- Polycom Microphone IP Adapter

Related Links

[Using a Provisioning Service](#) on page 25

Updating Software in the System Web Interface

You can manually update software or set up automatic updates in the G7500 system web interface.

Choose How to Get Software Updates

You may have several options to update your G7500 system software, depending on your environment.

Note: If you provision your system, it can only get updates from the provisioning server. For example, if you want updates from a custom server URL, you must disable provisioning.

Procedure

1. In the system web interface, go to **General Settings > Device Management**.
2. Select one of the following options in the **Download Update From** field:

Software Update Method	Description
Polycom Support Site	A software server hosted by Polycom.
Custom Server URL	<p>A server on your network that supports HTTP or HTTPS downloads.</p> <p>The URL is the path to the latest software build folder (for example, <code>https://<system_build_folder></code>). It includes update packages for your connected peripheral devices (for example, a table microphone) and the system. To successfully update the system and its connected peripheral devices, you must have this exact folder structure:</p> <ul style="list-style-type: none"> ▪ <code><device_type_1_update_folder></code> <ul style="list-style-type: none"> ◦ <code>Config</code> ◦ <code>image.zip</code> ◦ <code>version</code> ▪ <code><device_type_2_update_folder></code>

Software Update Method	Description
	<ul style="list-style-type: none"> ◦ Config ◦ image.zip ◦ version ▪ <system_update_folder> <ul style="list-style-type: none"> ◦ Config ◦ poly-video-<version>.zip ◦ poly-<system_b>-<version>.json ◦ poly-<system_b>-<version>.zip ◦ release.json ◦ version ▪ softwareupdate.cfg
Provisioning Server	Receive updates from a provisioning service, such as RealPresence Resource Manager.

3. If you choose to download software from a **Custom Server URL**, enter the path to the software build folder on your network in the **Update Server Address** field.

Once you select from where to download software updates, you can manually or automatically update the system.

Related Links

[Using a Provisioning Service](#) on page 25

Update Software Manually

You can manually update the software of your G7500 system and its connected peripheral devices.

Procedure

1. In the system web interface, go to **General Settings > Device Management**.
2. Select **Check for Updates**.
3. If the system finds updates, select **Update All**.

Your system and its connected peripheral devices update.

Update Software Automatically

You can automatically update the software of your G7500 system and its connected peripheral devices.

Procedure

1. In the system web interface, go to **General Settings > Device Management**.
2. Select **Enable Automatic Updates**.
 - Unless you specify a maintenance window, your system tries to update a minute after you enable this setting. If an update isn't available at the time, the system tries again every four hours.
3. Optional: Select **Only Check for Updates During Maintenance Hours** to specify a range of time to automatically update the software.
4. Optional: Choose times for **Maintenance Hours Begin** and **Maintenance Hours End**.
 - The system calculates a random time within the defined maintenance window to check for updates.

Note: If these settings are provisioned, the provisioning profile defines the polling interval. The default interval is one hour.

Update Software with a USB Flash Drive

You can update the software of your G7500 system and some of its connected peripheral devices with a USB flash drive.

Note: Polycom recommends formatting your USB flash drive with the FAT32 file system.

Procedure

1. Get the software package you want to install from [Polycom Support](#).
2. Save the package to the root directory of a USB flash drive and unzip the file.

To successfully update the system and its connected peripheral devices, you must have this exact folder structure:

- <device_type_1_update_folder>
 - Config
 - image.zip
 - version
- <device_type_2_update_folder>
 - Config
 - image.zip
 - version
- <system_update_folder>
 - Config
 - poly-video-<version>.zip
 - poly-<system_b>-<version>.json
 - poly-<system_b>-<version>.zip
 - release.json
 - version
- softwareupdate.cfg

3. Connect the USB flash drive to a USB port on the back of the system.

If the system detects the USB flash drive, a prompt displays on the monitor to confirm that you want to update the software.

4. Follow the onscreen instructions to complete the update.

Update Polycom HDCI Cameras

You can automatically update an HDCI-connected Polycom camera, but not in the same way you update the G7500 system and other connected peripheral devices (such as IP microphones).

Procedure

1. In the system web interface, go to **Audio/Video > Video Inputs**.

2. Select **Enable Camera Update**.

If the system detects a newer software version than what the camera is currently running, the camera updates automatically when the system isn't in a call. However, if during a call you connect a camera that isn't running the latest software, the call ends and the camera software update starts.

Related Links

[Configure Camera Settings](#) on page 79

Downgrading Software

You can downgrade your G7500 system software and the software of some of its connected peripheral devices.

Install an older software version to downgrade your G7500 system and peripheral devices with either of the following methods:

- On the **General Settings > Device Management** page, manually update to an older version located on your download server.
- Download an older version to a USB flash drive and connect it to your system.


Note: Before you downgrade, Polycom recommends doing the following:

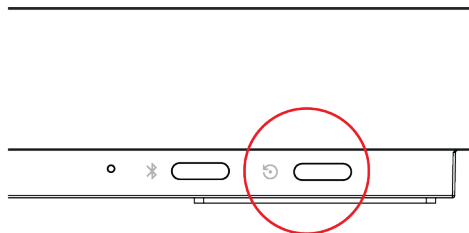
- Check the version you are running. You can find the version on the system web interface **Dashboard**.
 - Make sure automatic updates are disabled on the **General Settings > Device Management** page.
-

Restart the System

If you encounter issues, you can try restarting your G7500 system.

Procedure

- » Do one of the following:
 - On the front of the system, press and hold the **Restart**  button for five seconds.



- In the system web interface, go to **Diagnostics > System Reset** and select **Restart**.

Related Links

[Powering the System On and Off](#) on page 8

Reset System Settings

You can reset your G7500 system to its default configuration settings.

You may need to perform a system reset for a variety of reasons, for example, when moving a device to a new location.

Resetting your system deletes all but the following data:

- Current software version
- User-installed PKI certificates
- Local directory entries
- Logs
- Call detail reports (CDRs)

You also can choose not to retain some of this data after the system resets.

Procedure

1. In the system web interface, go to **Diagnostics**.
2. Go to **System Reset**.
3. Select **Reset All System Configurations**.
4. Optional: Clear any of the following check boxes for data you want to delete as part of the reset:
 - **Keep installed certificates.**
 - **Keep the directory entries.**
 - **Keep the system logs.**
 - **Keep the system call detail reports.**
5. Select **Restart**.

Factory Restore the System

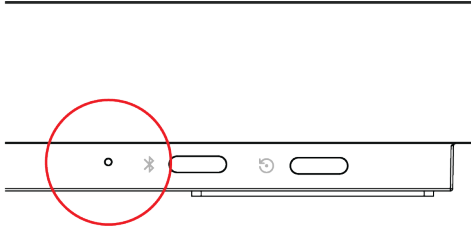
A factory restore completely erases the G7500 system's flash memory and restores it to the latest major software version (x.0).

The system doesn't save the following data with a factory reset:

- Current software version
- Logs
- User-installed PKI certificates
- Local directory entries
- Call detail reports (CDRs)

Procedure

1. Disconnect the power supply to turn off the system.
2. On the front of the system, insert a straightened paper clip through the restore button pinhole.



3. While continuing to hold the restore button, reconnect the power supply to turn the system on.
4. When the system LED indicator light blinks amber, stop pressing the restore button.

Related Links

[LED Status Indicators for the G7500 System](#) on page 11

Factory Restore a Table Microphone

You can restore a microphone to its default settings. This process refreshes the microphone by deleting its configurations except the current version of software.

Procedure

1. Ensure that the microphone is powered on.
2. Insert a straightened paper clip through the restore button pinhole.
3. Press and hold the reset button for 5 seconds, then release it when the microphone LED blinks amber.

Note: Don't power off the microphone during this process. It restarts when complete.

Related Links

[IP Microphones](#) on page 14

Related Links

[Factory Restore a Ceiling Microphone](#) on page 104

Factory Restore a Ceiling Microphone

You can restore a microphone to its default settings. This process refreshes the microphone by deleting its configurations except the current version of software.

Factory restoring the ceiling microphone requires the following tools:

- A small, thin block N45 magnet (for example, 76.2 mm [3 in.] × 12.7 mm [1/2 in.] × 3.18 mm [1/8 in.])
- Yardstick or adjustable floor-to-ceiling pole (so you don't have to use a ladder)
- Duct tape

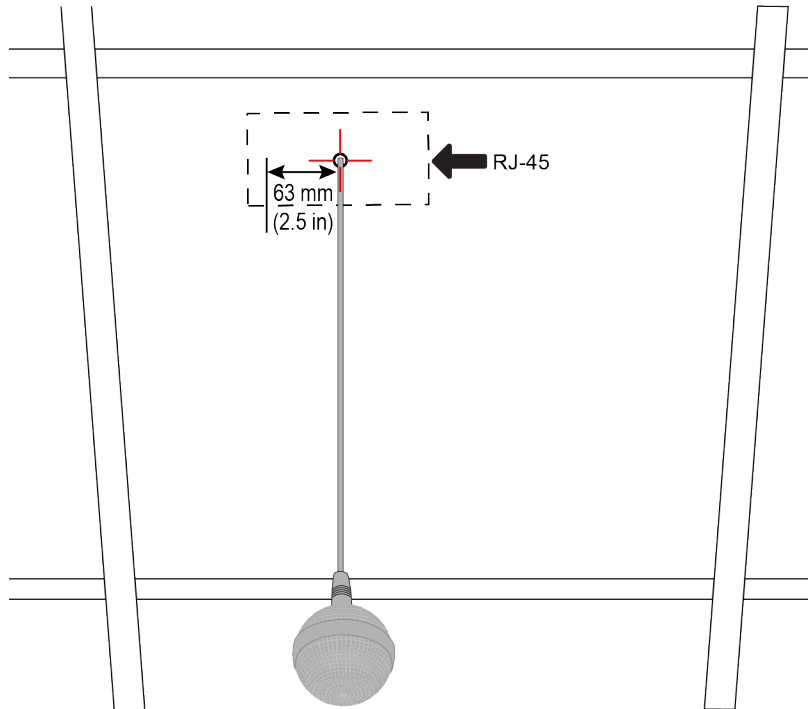
Procedure

1. Tape the magnet to one end of the pole with one of the 3.18 mm (1/8 in.) edges facing up.

Caution: If you have a suspended ceiling, tape the magnet securely to avoid it coming loose and sticking to a ceiling support grid.

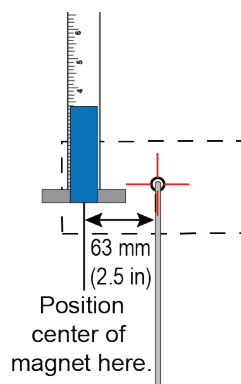
2. Ensure that the microphone is powered on.
3. Locate the factory reset sensor.

Looking at the bottom edge of the microphone connector along a longer side of the electronics enclosure, the sensor is approximately 63.5 mm (2.5 in.) towards the end opposite to the enclosure's RJ-45 connector.



If you can't see the RJ-45 connector, look for the small black button on the microphone cable. Facing that button at the 12 o'clock position, the sensor is located toward the 9 o'clock position.

4. Line up the center of the magnet with the sensor and hold it no more than 19 mm (3/4 in.) away from the enclosure for approximately 7 seconds.



The microphone LED blinks amber during a factory restore.

Note: Don't power off the microphone during this process. It restarts when complete.

Related Links

[IP Microphones](#) on page 14

Related Links

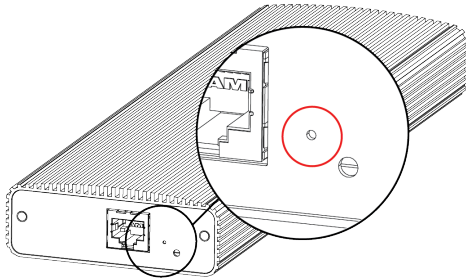
[Factory Restore a Table Microphone](#) on page 104

Factory Restore a Microphone Adapter

If your microphone adapter isn't functioning correctly, you might need to factory restore it. A factory restore completely erases the microphone adapter's flash memory and restores it to the latest major software version (x.0).

The restore button is on the side of the microphone adapter.

Figure 8: Microphone Adapter Restore Button Location

**Procedure**

1. Disconnect the power supply to turn off the microphone adapter.
2. **Optional for USB flash drive method:** Download the software package you want to install from Polycom Support and save the package to the root directory of a USB flash drive. Insert the USB flash drive into a USB port.

Note: Polycom recommends formatting your USB flash drive with the FAT32 file system.

3. Insert a straightened paper clip through the restore button pinhole.
4. While continuing to hold the restore button, reconnect the power supply to turn the microphone adapter on.
5. Hold the restore button for 10 more seconds, then release it.

The microphone adapter LED blinks green and blue during a factory restore.

Note: Don't power off the microphone adapter during this process. It restarts when complete.

Related Links

[Polycom Microphone IP Adapter](#) on page 16

SNMP Reporting

G7500 systems support SNMP versions 1, 2c, and 3.

SNMP can provide the following event information about your system:

- Alert conditions located on the system alert screen
- Details of jitter, latency, and packet loss

- Low battery power in the remote control
- System power on
- Successful or unsuccessful administrator login
- Call fail for a reason other than a busy line
- User help request
- Video or audio call connection or disconnection

Note: Polycom doesn't support SNMP write operations for configuring or provisioning systems.

SNMPv3 does the following:

- Provides secure connections between the SNMP manager and agent
- Supports IPv4 networks
- Logs all configuration change events
- Supports a user-based security model
- Supports trap destination addresses

Configure SNMP

You can monitor your G7500 system remotely with SNMP.

Procedure

1. In the system web interface, go to **Servers > SNMP**.
2. Configure the following settings:

Setting	Description
Enable SNMP	Enables administrators to monitor the system remotely using SNMP.
Enable Notifications	Enables MIB notifications.
Version1	Enables your system to use the SNMPv1 protocol. Due to security issues, Polycom recommends that you don't enable this setting.
Version2c	Enables your system to use the SNMPv2c protocol. Due to security issues, Polycom recommends that you don't enable this setting.
Version3	Enables your system to use the SNMPv3 protocol. Enabled by default, you can't configure other SNMPv3 settings unless this is on.

Setting	Description
Read-Only Community	<p>Specifies the SNMP community string for your system. For security reasons, don't use the default community string (<code>public</code>).</p> <p>Note: Polycom doesn't support SNMP write operations for configuring or provisioning systems. The community string is for read operations and outgoing SNMP traps.</p>
Contact Name	Specifies the name of the person responsible for remotely managing the system.
Location Name	Specifies the system location.
System Description	Provides details about the system.
User Name	Specifies the User Security Model (USM) account name for SNMPv3 message transactions. The maximum length is 64 characters.
Authentication Algorithm	<p>Specifies the type of SNMPv3 authentication algorithm used.</p> <ul style="list-style-type: none"> ▪ SHA ▪ MD5
Authentication Password	Specifies the SNMPv3 authentication password. The maximum length is 48 characters.
Privacy Algorithm	<p>Specifies the cryptographic privacy algorithm for SNMPv3 packets.</p> <ul style="list-style-type: none"> ▪ CFB-AES128 ▪ CBC-DES
Privacy Password	Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.
Engine ID	<p>Specifies the unique ID of the SNMPv3 engine. You might need this information to match the configuration of an SNMP console application. The ID is automatically generated, but you can create your own as long as it is between 10 and 32 hexadecimal digits. You can separate each group of two hex digits by a colon (:) to form a full 8-bit value. A single hex digit delimited on each side with a colon is equivalent to the same hex digit with a leading zero (for example, <code>:F:</code> is equivalent to <code>:0F:</code>).</p> <p>The ID can't be all zeros or Fs.</p>
Listening Port	Specifies the port SNMP uses to listen for system messages (the default is port 161).

Setting	Description
Transport Protocol	Specifies the transport protocol used. <ul style="list-style-type: none"> ▪ TCP ▪ UDP
Destination Address1 Destination Address2 Destination Address3	Specifies the IP addresses of SNMP managers where SNMP traps are sent. Each address has four settings: <ul style="list-style-type: none"> ▪ Server address (accepts IPv4 addresses, hostnames, and FQDNs) ▪ Message type (TRAP or INFORM) ▪ Protocol (SNMP v1, v2c, or v3) ▪ Port where SNMP traps are sent (default is 162)

3. Select **Save**.

Download MIBs

You can download MIB data for your G7500 system.

A MIB helps your SNMP management console resolve SNMP traps and provide human-readable descriptions of those traps.

Procedure

1. In the system web interface, go to **Servers > SNMP**.
2. Select **Download MIB**.

Troubleshooting

Topics:

- [Checking System Status](#)
- [Paired IP Peripheral Device is Disconnected](#)
- [View Call Statistics](#)
- [LED Status Indicators for the System LAN Ports](#)
- [Check Provisioning Results](#)
- [Logs](#)
- [Audio Tests](#)
- [Fix Polycom Acoustic Fence Issues](#)
- [Issues When the System is Sleeping or Waking](#)
- [Test the Call Experience](#)
- [Test Connection with Another System](#)
- [Run a Trace Route](#)
- [LDAP Directory Server Ignores the Minimum TLS Version Setting](#)
- [Checking the Web Proxy Configuration](#)

Refer to the following topics to help you diagnose and fix issues with your G7500 system.

Checking System Status

You can verify the status of your G7500 system in the local and system web interfaces. Status information also include details about connected peripheral devices and system services.

The system displays statuses using three colors:

- Green indicates the device or service is working or registered
- Red indicates an alert
- Gray indicates the device or service is unavailable or unregistered

Some statuses are available only after you connect the corresponding device, such as a camera, to the system.


Check Status in the Local Interface


Verify your G7500 system status in the local interface.

Procedure

1. Do one of the following:
 - In a call: **Menu** ≡ > **More ...** > **Settings** ⚙ > **Status**.
 - Out of a call: **Menu** ≡ > **Settings** ⚙ > **Status**.

2. View a system status page:

You must enter the system’s local administrator credentials to access status pages displaying a **Lock** .

Setting	Description
Active Alerts	Displays the status of any device or service with an error status. If there’s an alert, an Alert  displays next to the system time.
Call Control	Displays status of the Auto-Answer Point-to-Point Video setting.
LAN Properties	Displays network connection status.
Servers	<ul style="list-style-type: none"> ▪ Displays the gatekeeper and SIP registrar server status. ▪ Displays the active global directory server or LDAP server status. ▪ Displays the provisioning or calendaring service status (if enabled).
Peripheral Devices	Connection status of peripheral devices.

Check Status in the System Web Interface

Verify your G7500 system status in the web interface.

Procedure

1. In the system web interface, go to **Diagnostics > System Status**.
2. Optional: Select **Details** next to each device or service for more information.
3. Optional: Select **Adjust <Feature> Settings** to access to the corresponding settings page.

Paired IP Peripheral Device is Disconnected

Symptom:

You paired an IP peripheral device with your G7500 system but can’t use it. On the web interface **Device Management** page, you see that the device is **Disconnected**.

Problem:

A paired device must have a **Connected** status to use. A **Disconnected** status may mean there’s a physical connection issue or your device or system is malfunctioning.

Workaround:

Reconnect cables or factory restore your hardware. Follow each step until you’ve fixed the issue.

1. Check the device LED. If it isn’t blinking blue, reconnect the LAN cable to the device and system.
2. If the device is a Polycom Microphone IP Adapter, also reconnect its power supply cables.

3. Perform a factory restore on the device.
4. Perform a factory restore on the system.

View Call Statistics

You can look at in-call data to help you troubleshoot system issues or problems experienced by call participants.

Procedure

1. In the system web interface, go to **Diagnostics**.
2. Go to **Call Statistics**.

If you're in a call, a link to call statistics is also available on the **Dashboard** and **Active Call** page.

A list of participants displays, including their names, numbers, and the quality of their connections.

3. Select the arrow next to the **Details** of the participant you want more information about.

The following additional details about the participant display:

- System or application the participant is using
- Call type
- Call speed
- AES Encryption status
- Call streams (for your system and the participant)

Depending on the nature of your call, you may also see the transmitted and received streams of audio, video, and content.

4. Optional: Select the arrow next to a call stream for additional information.

The following additional details about the stream display:

- Stream type
- Stream quality
- Protocol used
- Format (may not display on some mobile devices)
- Rate used
- Frame rate
- Packets lost
- Packet loss percentage
- Jitter
- Error concealment

LED Status Indicators for the System LAN Ports

You can verify network connectivity by looking at the LAN port LEDs on the back of your G7500 system.

There are four LAN ports: one for the system's network connection (farthest left) and three link-local network (LLN) connections for peripheral devices.

Each LAN port has two LEDs: The left LED indicates network connectivity and traffic, while the right LED indicates Power over Ethernet (PoE) status for connected devices.

LED Status Indicators for the G7500 System LAN Ports

Indicator	Left LED Status (Network Traffic)	Right LED Status (Power)*
Off	No connection	No device connected
Solid green	Connected with no traffic	Connected and functioning normally
Blinking green	Connected with traffic	N/A
Solid orange	N/A	Connected but malfunctioning

* - The right LED is not used on the primary network connection port (farthest left on the back of the system).

Related Links

[Configuring Wired LAN Settings](#) on page 27

Related Links

[System Back Panel Ports](#) on page 10

Check Provisioning Results

To verify your settings are provisioned the way you want, you can see if the configuration parameters were applied successfully to your G7500 system.

Make sure your system is registered with a provisioning service, such as RealPresence Resource Manager.

Procedure

1. In the system web interface, go to **Servers > Provisioning Server**.
2. Select **Show Results** to verify that the configuration parameters applied successfully the last time you provisioned your system.

If provisioning failed for a parameter, there are details in the **Error Message** column to help you fix the issue.

Related Links

[Register the System with a Provisioning Service](#) on page 25

Logs

Logs contain information about G7500 system activities and configurations to help you troubleshoot issues.

Consolidated System and Peripheral Device Logs

Logs include details about your G7500 system and some of its connected peripheral devices.

These peripheral devices include the following:

- Polycom IP Table Microphone
- Polycom IP Ceiling Microphone

- Polycom Microphone IP Adapter

Configure Log Preferences

You can manage some basic aspects of your G7500 system logs, including how logs are transferred to a USB flash drive.

Your system has limited storage space for logs. If you want logs to be overwritten less frequently, attach a USB flash drive to the system.

When the G7500 system log fills past your configured threshold, the system triggers the following actions:

- Transfers the log to a USB flash drive if you set **Transfer Frequency** to **Auto At Threshold**.
- Creates a log entry indicating that the system reached the threshold.

Procedure

1. In the system web interface, go to **Diagnostics > Logs**.
2. Go to **Log Management**.
3. Configure the following settings and select **Save**.

Setting	Description
Current Percent Filled	Displays as a percentage how full the logs are. When the logs are full, system deletes the oldest entries.
Percent Filled Threshold	Reaching the threshold you configure here creates a log entry and automatically transfers logs if you set Transfer Frequency to Auto At Threshold .
Folder Name	Specifies the folder name for log transfers. Select one of the following: <ul style="list-style-type: none"> • System Name and Timestamp—Folder name is the system name and the timestamp of the log transfer. For example, if the system name is <i>Marketing</i>, the folder name might be <i>marketing_<date_and_time></i>. • Timestamp—Folder name is the timestamp of the log transfer (e.g., <i><yyyyMMddhhmmssSSS></i>). • Custom—Lets you specify a folder name for manual log transfers.
Storage Type	Specifies the type of storage device used for log file transfers.

Setting	Description
Transfer Frequency	<p>Specifies when the system transfers logs:</p> <ul style="list-style-type: none"> • Manual—The transfer starts when you select the Start button, which is visible only in the local interface. If the log fills before you transfer, new events overwrite the oldest events. • Auto at Threshold—The transfer starts automatically when the system reaches the Percent Filled Threshold.

Configure Log Level

You can determine how much detail you want in your G7500 system logs.

Procedure

1. In the system web interface, go to **Diagnostics > Logs**.
2. Go to **System Log Settings**.
3. Configure the following settings and select **Save**.

Setting	Description
Log Level	<p>Sets the minimum log level of messages stored in the system's flash memory.</p> <p>DEBUG logs all messages, while WARNING logs the fewest number of messages.</p> <p>Polycom recommends that you use the default value DEBUG.</p> <p>When you enable Enable Remote Logging, the log level is the same for both remote and local logging.</p>
Enable H.323 Trace	Logs additional H.323 connectivity information.
Enable SIP Trace	Logs additional SIP connectivity information.

Download Logs

You can retrieve the logs associated with your G7500 system and some of its peripheral devices.

Procedure

1. In the system web interface, go to **Diagnostics > Logs**.
2. Select **Download System Logs**.

The log package, which includes call detail record (CDR) information, downloads as a `.tgz` file. The date and time of the log entries display in GMT.

Transfer Logs to a USB Flash Drive

You can transfer logs to a USB flash drive to free up space on your G7500 system.

Note: Polycom recommends formatting your USB flash drive with the FAT32 file system.

Procedure

1. In the local interface, go to **Menu** ≡ > **Settings** ⚙ > **Diagnostics**.
2. Select **Log Management** and enter the system's local administrator credentials.
3. Select **Start**.

Note: Wait until the system displays a message that the log transfer has completed successfully before you remove the USB flash drive.

The system saves a file in the USB flash drive named according to the settings in the system web interface.

Configure Remote Logging

In addition to downloading logs locally, you can also configure your G7500 system to send the event details it collects to a remote logging server (using Syslog or a similar mechanism).

Remember the following about remote logging with your system:

- The system sends logs to remote logging servers over a secure TLS connection.
- You can use more than one remote logging server.
- Logs can be consumed by an intrusion detection system (IDS) and a security information and event management (SIEM) system.

Procedure

1. In the system web interface, go to **Diagnostics** > **Logs**.
2. Configure the following settings and select **Save**.

Setting	Description
Enable Remote Logging	<p>Specifies whether remote logging is enabled. Enabling this setting causes the system to send each log message to the specified server in addition to logging it locally.</p> <p>The system immediately begins forwarding its log messages after you click Save.</p> <p>The system supports remote logging encryption using TLS. If you use UDP or TCP transport, Polycom recommends remote logging only on secure, local networks.</p>

Setting	Description
Remote Log Server Address	<p>Specifies the server address and port. If you don't specify the port, the system uses a default destination port. The system determines the default port by how you configure Remote Log Server Transport Protocol:</p> <ul style="list-style-type: none"> • UDP: 514 • TCP: 601 • TLS: 6514 <p>You can specify the address and port in the following formats:</p> <ul style="list-style-type: none"> • IPv4 address: 192.0.2.0:<port>, where <port> is the elective destination port number in the 1-65535 range. • FQDN: logserverhost.company.com:<port>, where <port> is the elective destination port number in the 1-65535 range.
Remote Log Server Transport Protocol	<p>Specifies the transport protocol for sending logs to a remote server:</p> <ul style="list-style-type: none"> • UDP • TCP • TLS (secure connection)

Sample Log File

The following code block is a sample G7500 system log file:

```

2018-10-19 13:53:08 Kernel.Debug 10.223.73.18 1
2018-10-19T18:53:08.626000+00:00 DeviceName ProductName - - [NXLOG@14506
EventReceivedTime="2018-10-19 18:53:08" SourceModuleName="plcmlog"
SourceModuleType="im_file"] CEng: RouteProc[0]: RouteReceived - VID
videoroute set 0 mon1 1920 1080 HDMI 60 Progressive vout1 0 0 1920 1080 0
none 0 0 0 0
2018-10-19 13:53:08 Kernel.Info 10.223.73.18 1
2018-10-19T18:53:08.626000+00:00 DeviceName ProductName - - [NXLOG@14506
EventReceivedTime="2018-10-19 18:53:08" SourceModuleName="plcmlog"
SourceModuleType="im_file"] SMan: SrcMan: IncallMuteStateCmdUpdate set
incall = 0
2018-10-19 13:53:08 Kernel.Debug 10.223.73.18 1
2018-10-19T18:53:08.626000+00:00 DeviceName ProductName - - [NXLOG@14506
EventReceivedTime="2018-10-19 18:53:08" SourceModuleName="plcmlog"
SourceModuleType="im_file"] CEng: RouteTrans[0]: RouteTrans people camera
source id 1, width 1920, height 1080 vinp->mon1

```

Audio Tests

You can test your G7500 system speakers, audio levels, and Polycom StereoSurround setup.

Test Speakers

You can verify that you correctly connected the speakers to your G7500 system.

You must enable Polycom StereoSurround to test both speakers at once.

Procedure

1. In the system web interface, go to **Diagnostics > Audio Test**.
2. Do one of the following to start a speaker test:
 - Select **Start**.
 - Select **Left**, **Both**, or **Right** to test individual or both speakers. (The **Both** test is available only if you've enabled Polycom StereoSurround.)

If you run a test during a call, people on the far site also hear the test tone.

A 473 Hz tone indicates that the local audio connections are correct.

Related Links

[Configure General Audio Settings](#) on page 69

[Test Polycom StereoSurround](#) on page 118

Test Audio Levels

Audio meters show you real-time audio input and output signals for your G7500 system, including microphones, far-site audio, and other connected audio devices.

Procedure

1. Do one of the following:
 - In the system web interface, go to **Diagnostics > Audio Tests > Audio Meter**.
 - In the local interface, go to **Settings > System Information > Diagnostics > Audio Meter**.
2. To test the audio levels, do one of the following:
 - To check the near-site audio, speak into your microphones.
 - To check the far-site audio, ask a call participant to speak or call a phone in the far-site room to hear it ring.

Occasional peaks of +12 dB to +16 dB with loud transient noises are acceptable. If you see +20 on the audio meter, the audio signal is 0 dBFS and the audio might be distorted. A meter reading of +20dB corresponds to 0dBFS in the room system audio. A signal at this level is likely clipping the audio system.

Test Polycom StereoSurround

After you configure the G7500 system to use Polycom StereoSurround, you can place a test call to see if it works.

Make sure the microphones are positioned correctly.

Procedure

1. In the system web interface, go to **Audio/Video > Audio > Audio Input**.

2. Gently blow on the left and right leg of each Polycom microphone while watching the audio meters to identify the left and right inputs.
3. Test the speakers to check volume and verify that audio cables are connected.
If the system is in a call, the far site hears the tone.
4. Optional: Exchange the right and left speakers if they are reversed.
5. Adjust the volume control on your external audio amplifier so that the test tone sounds as loud as a person speaking in the room. If you use a Sound Pressure Level (SPL) meter, it should measure approximately 80 to 90 dBA in the middle of the room.
6. Repeat these steps for **Audio Output**.

Related Links


[Configure General Audio Settings](#) on page 69

[Test Speakers](#) on page 118

Fix Polycom Acoustic Fence Issues

If you're using Polycom Acoustic Fence technology with your G7500 system and notice it isn't working, you may have to reconnect your microphones.

Procedure

1. Disconnect all microphones from the **LLN ports**  on the back of your system.
2. Reconnect the microphones (connect the primary microphone first).

Related Links

[Polycom Acoustic Fence](#) on page 71

Issues When the System is Sleeping or Waking

Symptom:

Your G7500 system sometimes restarts while sleeping or waking up.

Problem:

This is caused by manipulating the connected HDMI output while your system is asleep.

Workaround:

While your system is asleep, don't change the HDMI source on your monitor, switch out HDMI cables, or turn off your monitor.

If your sleep **Display** setting is configured to **No Signal**, try the following to avoid these issues:

- Turn off the input auto-select feature on your monitor.
- Set the sleep **Display** setting to **Black**.
- Disable sleep mode on your system by setting **Time Before System Goes to Sleep** to **Off**.

Related Links

[Configure Sleep Settings](#) on page 23

Test the Call Experience

Run a near end loop test to verify what others see and hear in a call with your G7500 system.

This test isn't available in a call.

Procedure

1. In the local interface, go to **Menu** ≡ > **Settings** ⚙ > **Diagnostics**.
2. Go to **Near End Loop**.
3. Select **Start**.

Monitor 1 displays the video and plays the audio sent to a far site during a call.

Test Connection with Another System

With a ping test, you can check if your G7500 system can call another system.

Procedure

1. In the local interface, go to **Menu** ≡ > **Settings** ⚙ > **Diagnostics**.
2. Go to **Ping**.
3. Enter the IP address or URL of the system you want to call.
4. Select **Start**.

If the test is successful, an abbreviated Internet Control Message Protocol (ICMP) message displays. You see H.323 or SIP information depending on how the far-site system is configured.

Run a Trace Route

You can run a trace route to identify network connectivity issues with your G7500 system.

Procedure

1. In the local interface, go to **Menu** ≡ > **Settings** ⚙ > **Diagnostics**.
2. Go to **Trace Route**.
3. Enter the IP address or URL with which to run the trace route.
4. Select **Start**.

If the test is successful, the hops between your system and the specified destination display.

LDAP Directory Server Ignores the Minimum TLS Version Setting

Symptom:

You've changed your G7500 system configuration to use TLS version 1.1 at minimum, but the system still connects to your LDAP directory server with TLS 1.0.

Workaround:

Restart your system after configuring the **Minimum TLS Version** setting.

Related Links

[Register with an LDAP Directory Server](#) on page 87

[Configure Minimum TLS](#) on page 56

Checking the Web Proxy Configuration

If you experience issues with your automatic or semi-automatic web proxy configuration, check the status and contents of your proxy auto-configuration (PAC) file.

For manual configurations, verify that the information you used to connect your system to the proxy is accurate.

Related Links

[Web Proxies](#) on page 58

PAC File Status Messages

Your G7500 system displays messages indicating the status of the proxy auto-configuration (PAC) file used for web proxy communication. Refer to the following table for more information about these messages, which you see on the **Web Proxy Settings** page of the system web interface.

PAC File Status Messages

Status Messages	Description
Success	File successfully downloaded to your system.
In Progress	File is downloading to your system.
WPAD Failed	File download URL was not discovered using DHCP option 252.
Download Failed	File did not download.
Expired	File is expired.

Verify the PAC File on the System

You can check the contents of the PAC file on your G7500 system.

Procedure

1. In the system web interface, go to **Network > Primary Network > Web Proxy Settings**.
2. Select **Download PAC File**.

This option isn't available if the **PAC File Status** doesn't indicate **Success**.