



ADMINISTRATOR GUIDE

3.0.0 | December 2019 | 3725-86561-001A

Poly Partner Mode

Getting Help

For more information about installing, configuring, and administering Poly/Polycom products or services, go to Polycom Support.

Plantronics, Inc. (Poly — formerly Plantronics and Polycom)
345 Encinal Street
Santa Cruz, California
95060

© 2019 Plantronics, Inc. All rights reserved. Poly, the propeller design, and the Poly logo are trademarks of Plantronics, Inc. All other trademarks are the property of their respective owners.

Contents

- Before You Begin.....5**
 - Audience, Purpose, and Required Skills.....5
 - Related Poly and Partner Resources.....5

- Getting Started..... 7**
 - Poly Partner Mode Overview..... 7
 - Product Overview of Poly Video Systems.....7
 - Administrator Features and Capabilities..... 8
 - Powering the System On and Off.....9
 - Navigating the System..... 9
 - Access the System Web Interface.....9

- Setting Up the System..... 10**
 - Overview of Poly G7500, Studio X50, and Studio X30 Hardware..... 10
 - Poly G7500 System Ports..... 10
 - Poly Studio X50 System Ports.....11
 - Poly Studio X30 System Ports..... 12
 - LED Status Indicators..... 13
 - LED Status Indicators for the G7500 System.....13
 - LED Status Indicators for the Studio X50 and Studio X30 Systems..... 14
 - Completing Initial System Setup..... 15
 - Complete Setup with the System Web Interface..... 15
 - Complete Setup with Provisioning.....16
 - Change Conferencing Partner..... 16
 - Managing Peripheral Devices..... 16
 - Pairing IP Devices on the Link-Local Network..... 16
 - Pair an IP Device on the Primary Network..... 18
 - Connect a USB Device.....19
 - IP Microphones..... 19
 - Poly Microphone IP Adapter.....21

- Configuring General Settings..... 24**
 - Name the System and Room.....24
 - Provide Contact Information.....24
 - Set the Date and Time..... 25
 - Set the System Location..... 25
 - Set the Local Interface Language..... 26

Configure Sleep Settings.....	26
System Usage Data Collected by Poly.....	26
Turn Off System Usage Data Collection.....	27
Using a Provisioning Service.....	28
Register the System with a Provisioning Service.....	28
Download a Template Configuration File.....	29
Managing Conferencing Applications.....	30
Update Third-Party Conferencing Software Manually in the System Web Interface.....	30
Configuring Network Settings.....	31
Configuring Wired LAN Settings.....	31
Automatically Obtain IPv4 Address Settings.....	31
Manually Configure IPv4 Address Settings.....	31
Manually Assign a Host Name and Domain Name.....	32
Manually Configure DNS Settings.....	32
Configure VLAN Settings.....	32
Configure 802.1X Settings.....	33
Configure Wired LAN Options.....	33
Configure Wi-Fi Settings.....	34
Configure Network Quality Settings.....	34
Securing the System.....	37
Managing System Access.....	37
Local Accounts.....	37
Configure System Access Settings.....	40
Configure the System Web Interface Port Lock.....	41
Disable USB Ports.....	41
PKI Certificates.....	42
Create a Certificate Signing Request.....	42
Configure Certificate Validation Settings.....	44
Install a Certificate.....	44
View a Certificate.....	45
Delete a Certificate.....	45
Certificate Revocation.....	45
Call Encryption.....	47
H.460 Firewall/NAT Traversal.....	47
Configure the System for H.460 Firewall/NAT Traversal.....	48
Web Proxies.....	50

View Connections to the System.....	52
System Port Usage.....	52
Configuring Audio Settings.....	55
Configure General Audio Settings.....	55
Audio Input.....	56
Configure IP Microphones.....	57
Configuring the Microphone Adapter.....	57
Polycom Acoustic Fence.....	57
Configure 3.5 mm and HDMI Audio Input.....	59
Audio Output.....	60
Configure Audio Output Settings.....	60
Using 3.5 mm Audio Output.....	61
Configuring Video and Camera Settings.....	62
HDMI I/O.....	62
Supported HDCI Input Resolutions.....	64
Configure Monitor Settings.....	64
Configure a Touch Monitor.....	65
Monitors with CEC.....	65
Disable CEC.....	65
Enable CEC.....	65
Configure General Camera Settings.....	66
Configure Camera Tracking Settings.....	67
Configure Video Input Settings.....	68
Sharing Content.....	71
Default Option for Sharing Content.....	71
Customizing the Local Interface.....	72
Configure Dual Monitor Display Settings.....	72
System Maintenance.....	73
Activating System Features.....	73
Unlock System Settings.....	74
Updating Software.....	75
Updating Software in the System Web Interface.....	75
Update Software with a USB Flash Drive.....	77
Update Poly HDCI Cameras.....	77

Manually Downgrade Software in the System Web Interface.....	78
Downgrade Software with a USB Flash Drive.....	78
Restart the System.....	78
Reset System Settings.....	79
Factory Restore the System.....	79
Factory Restore a Table Microphone.....	80
Factory Restore a Ceiling Microphone.....	81
Factory Restore a Microphone Adapter.....	82
Troubleshooting.....	84
Logs.....	84
Consolidated System and Peripheral Device Logs.....	84
Configure Log Preferences.....	85
Configure Log Level.....	86
Download Logs.....	86
Transfer Logs to a USB Flash Drive.....	86
Configure Remote Logging.....	87
Sample Log File.....	88
SNMP Reporting.....	88
Configure SNMP.....	89
Download MIBs.....	91
Checking System Status.....	91
Check Status in Local Interface.....	91
Check Provisioning Results.....	92
Paired IP Audio Device is Disconnected from G7500.....	93
Poly TC8.....	93
Poly TC8 Can't Pair to the Video System.....	93
Poly TC8 Doesn't Display On the Available Devices List.....	93
Paired Poly TC8 is Disconnected.....	94
Poly TC8 Paired to Inaccessible Video System.....	95
Can't Wake the System by Touching the Monitor.....	95
LED Status Indicators for the System LAN Ports.....	96
Audio Tests.....	96
Fix Polycom Acoustic Fence Issues with G7500.....	98
Test the Call Experience.....	98
Test Connection with Another System.....	98
Run a Trace Route.....	99
Checking the Web Proxy Configuration.....	99
Zero Touch Onboarding Connection Fails During Initial Setup or After Reset.....	100

Before You Begin

Topics:

- [Audience, Purpose, and Required Skills](#)
- [Related Poly and Partner Resources](#)

This guide contains overview information, procedures, and references you can use to perform tasks with your video system.

The information in this guide applies to all the following Poly video systems and peripherals except where noted:

- Poly Bluetooth Remote Control (model: P010)
- Poly G7500 (model: P011)
- Poly Microphone IP Adapter (model: P012)
- Poly IP Table Microphone (model: P013)
- Poly IP Ceiling Microphone (model: P014)
- Poly Studio X50 (model: P017)
- Poly Studio X30 (model: P018)
- Poly TC8 (model: P020)

Audience, Purpose, and Required Skills

This guide is written for a technical audience.

You must be familiar with the following concepts before beginning:

- Current telecommunications practices, protocols, and principles
- Telecommunication basics, video teleconferencing, and voice or data equipment

Related Poly and Partner Resources

See the following sites for information related to this product.

- The [Polycom Support Site](#) is the entry point to online product, service, and solution support information including **Licensing & Product Registration**, **Self-Service**, **Account Management**, **Product-Related Legal Notices**, and **Documents & Software** downloads.
- The [Polycom Document Library](#) provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The [Polycom Community](#) provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.

- The [Polycom Partner Network](#) are industry leaders who natively integrate the Poly standards-based RealPresence Platform with their customers' current UC infrastructures, making it easy for you to communicate face-to-face with the applications and devices you use every day.
- The [Polycom Collaboration Services](#) help your business succeed and get the most out of your investment through the benefits of collaboration.

Getting Started

Topics:

- [Poly Partner Mode Overview](#)
- [Product Overview of Poly Video Systems](#)
- [Powering the System On and Off](#)
- [Navigating the System](#)

The Poly G7500, Studio X50, and Studio X30 systems provide video conferencing capabilities and collaboration tools for any size meeting space or room.

Poly Partner Mode Overview

Poly Partner Mode allows you to run third-party conferencing applications on supported Poly video systems. For example, after powering on your system for the first time, you can select Zoom Rooms to place Zoom calls.

Refer to the supported partner documentation for information on using third-party applications:

- **Zoom:** <https://support.zoom.us/hc/en-us>

Product Overview of Poly Video Systems

Poly G7500, Studio X50, and Studio X30 systems in Partner Mode can seamlessly join meetings using third-party conferencing applications.

Poly G7500 System Features and Capabilities

The G7500 systems support the following features:

- Peripheral cameras and microphones make the system scalable for medium rooms and up to large integrated rooms
- Placing and joining video calls
- Sharing wireless and wired content
- Camera tracking technology that can automatically zoom in on the person talking or frame the group of people in the room (depending on how you configure the system)
- Poly NoiseBlockAI, which during calls eliminates background and extraneous sound from being heard in common working environments when no one is talking
- Polycom Acoustic Fence technology, which allows video conferencing in open workspaces by capturing only the voices in a defined area
- HDMI: Single input and dual output

Poly Studio X50 Features and Capabilities

The Studio X50 systems support the following features:

- All-in-one collaboration system for huddle rooms and small-to-medium rooms

- No need for a separate PC, laptop, or codec to run video-conferencing software
- Placing and joining video calls
- Sharing wireless and wired content
- Built-in 4K camera with ultra-wide 120-degree field of view
- Camera tracking technology that automatically frames the group of people in the room
- High-fidelity, built-in stereo microphones that pick up sound within 3.66 m (12 ft) and use spatial audio for life-like presence and clarity
- Poly NoiseBlockAI, which during calls eliminates background and extraneous sound from being heard in common working environments when no one is talking
- Dual stereo speakers
- HDMI: Single input and dual output

Poly Studio X30 Features and Capabilities

The Studio X30 systems support the following features:

- All-in-one collaboration system for huddle rooms and small-to-medium rooms
- No need for a separate PC, laptop, or codec to run video-conferencing software
- Placing and joining video calls
- Sharing wireless and wired content
- Built-in 4K camera with ultra-wide 120-degree field of view
- Camera tracking technology that automatically frames the group of people in the room
- High-fidelity, built-in stereo microphones that pick up sound within 3.66 m (12 ft) and use spatial audio for life-like presence and clarity
- Poly NoiseBlockAI, which during calls eliminates background and extraneous sound from being heard in common working environments when no one is talking
- Single mono speaker
- HDMI: Single input and output

Administrator Features and Capabilities

The G7500, Studio X50, and Studio X30 systems provide features for administrators to deploy, manage, and access systems.

These systems provide the following features and capabilities:

- 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

Powering the System On and Off

The 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 power it off.

Note: 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 78

Navigating the System

You can navigate the system using the system web interface.

Access the System Web Interface

Access the 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.

Procedure

1. Open a web browser and enter the system IP address.
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 Setup with the System Web Interface](#) on page 15

Setting Up the System

Topics:

- [Overview of Poly G7500, Studio X50, and Studio X30 Hardware](#)
- [LED Status Indicators](#)
- [Completing Initial System Setup](#)
- [Change Conferencing Partner](#)
- [Managing Peripheral Devices](#)

See the setup sheets applicable to your video system and its peripheral devices, including cameras, monitors, microphones, and controllers.

Overview of Poly G7500, Studio X50, and Studio X30 Hardware

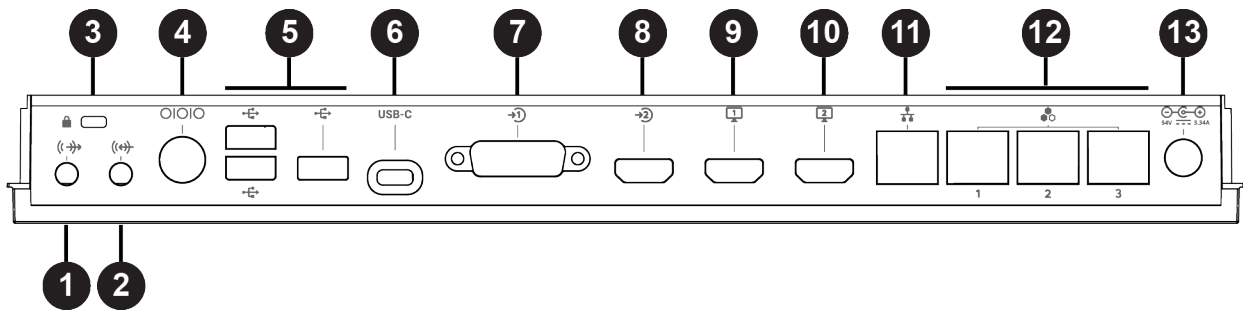
The following figures and tables provide information about hardware features available on your system.

Related Links

[HDMI I/O](#) on page 62

Poly G7500 System Ports

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



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

Ref. Number	Port Description
5	USB 3.0 port (host)
6	USB-C port (dual-role port provides power only)
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	LAN connection for the system
12	Link-local network (LLN) connections for IP-based peripheral devices
13	Power

Related Links

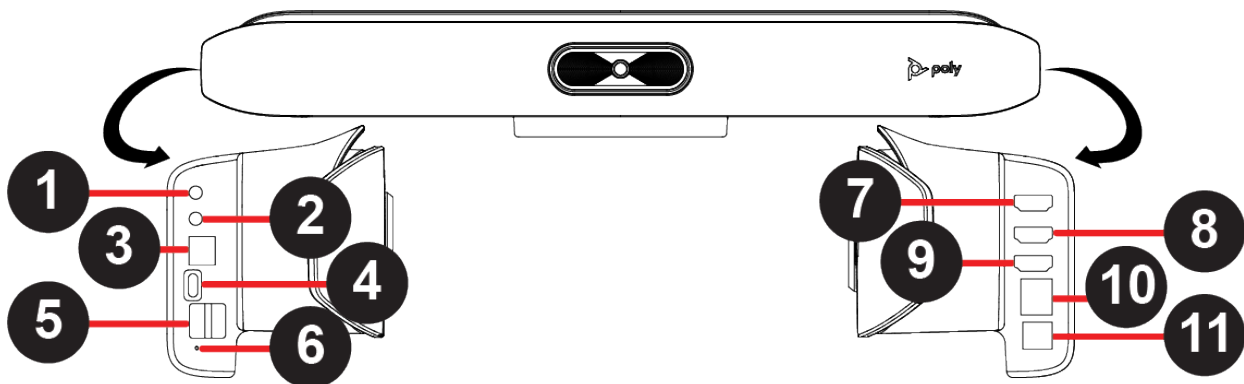
[Specify the Primary and Fence Microphones](#) on page 58

Related Links

[LED Status Indicators for the System LAN Ports](#) on page 96

Poly Studio X50 System Ports

The following illustration and table explain the ports on your Poly Studio X50 system.



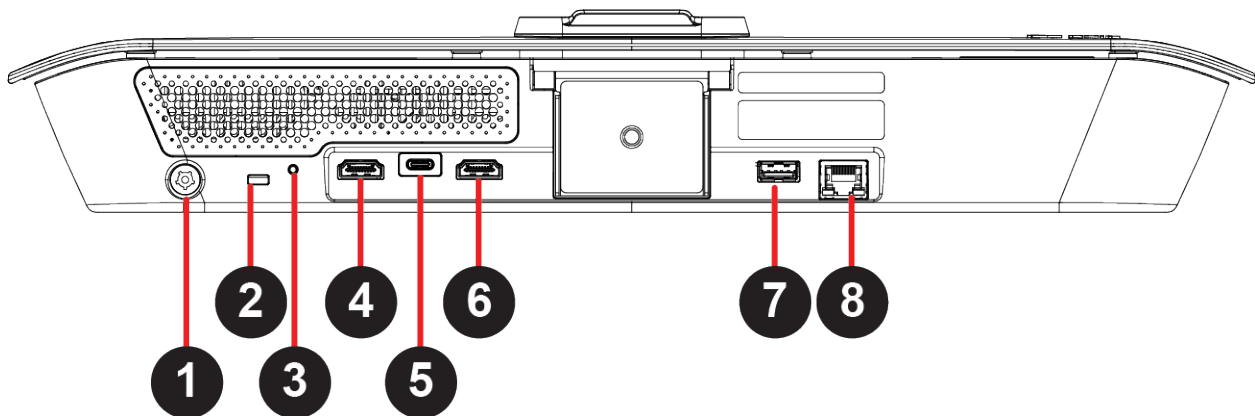
Poly Studio X50 System Port Descriptions

Ref. Number	Port Description
1	3.5 mm audio line in (reserved for future use)
2	3.5 mm audio line out (reserved for future use)
3	Polycom RealPresence Debut expansion microphone connection (reserved for future use)

Ref. Number	Port Description
4	USB-C port (dual-role port provides power only)
5	USB ports
6	Factory restore pinhole
7	HDMI output for the secondary monitor
8	HDMI output for the primary monitor
9	HDMI input for sharing content (for example, from a laptop)
10	LAN connection for the system
11	Power

Poly Studio X30 System Ports

The following illustration and table explain the ports on your Poly Studio X30 system.



Poly Studio X30 System Port Descriptions

Ref. Number	Port Description
1	Power
2	Security lock
3	Factory restore pinhole
4	HDMI output for the primary monitor
5	USB-C port (dual-role port provides power only)
6	HDMI input for sharing content (for example, from a laptop)
7	USB port

Ref. Number	Port Description
8	LAN connection for the system

LED Status Indicators

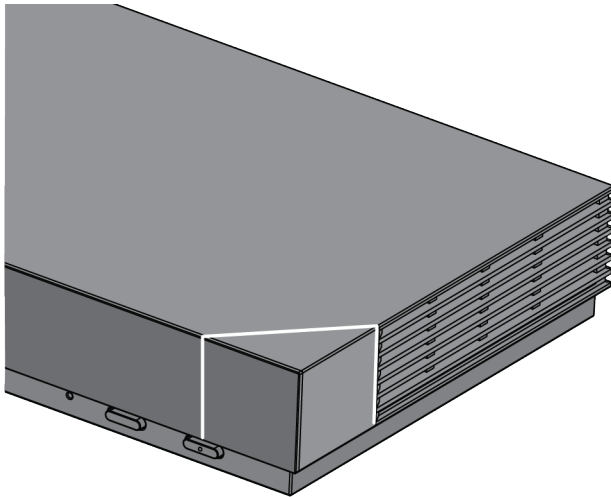
The following figures display the LEDs on your systems. The tables list each LED indicator and its associated status.

Related Links

[Factory Restore the System](#) on page 79

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 system.



G7500 System LED Status Indicators

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

LED Status Indicators for the Studio X50 and Studio X30 Systems

The system provides an LED light bar above the camera to help you understand the system's behaviors.

Basic Studio X50 and Studio X30 LED Indicators and Status

Indicator	Position	Status
Chasing white	All while alternating	Boot initialization in progress
Blinking blue	Twelve in the middle	Bluetooth in discovery
Solid blue for 3 seconds	All	Bluetooth paired
Blinking green	All	Incoming call
Solid green	Two in the middle	Outgoing call
Solid green or white	Four to eight (when in the middle), indicating the tracked speaker or the direction of the camera	Working The lights are green with supported applications, with the following cases: <ul style="list-style-type: none"> Tracking people in the group framing and speaker tracking mode. Indicating the direction of the camera that you customize in the pan-tilt-zoom (PTZ) mode.
Pulsing red	Twelve in the middle	Call on hold
Pulsing green	Twelve in the middle	Call on hold (by far site)
Solid white for 3 seconds	Twelve in the middle	Saving a preset
Solid red	All	Muted microphone
Pulsing amber	All	Firmware update in progress
Blinking red	All	Error preventing normal operation
Blinking amber	Twelve alternating	In a POST sequence, at least one test resulted in a warning error. The system continues to blink amber, but initializes after the sequence is complete if no severe errors occur.
Blinking red	Twelve alternating	In a POST sequence, at least one test resulted in a severe error. The system continues to blink red and doesn't start up.

Completing Initial System Setup

When you power on the system for the first time (or after a system reset or factory restore), you must complete the system setup process.

This process involves the system contacting the Poly Zero Touch Onboarding (ZTO) server to determine its mode of operation: Poly Video or Partner mode.

Before you begin:

- During initial setup, you must have a DHCP server in your environment to ensure the system gets an IP address. (You can configure the system with a static IP address later if needed.)
- Configure your firewall and/or web proxy so that the system can communicate with the ZTO service (zto.poly.com) on port 443.
- You must have an NTP server on your network for the system to connect with the ZTO service.
- Your conferencing application may require a separate license or subscription for call-related features. Contact your conferencing partner for information.

Depending on how your system was purchased, the system either boots directly into a conferencing application or to a screen where you choose the application. Once up and running, you can switch to a different application in the system web interface.

After going through the system setup process, you also must manually configure or provision the following system settings for an optimal deployment and user experience:

- **Local administrator password:** For security reasons, don't use the default password.
- **Country:** If you use the default country setting, the system's Wi-Fi settings may not be optimal for your country or region.
- **Timezone:** Depending on the system location, using the default timezone setting may display the incorrect time on the system (including for scheduled calendar events).

Complete Setup with the System Web Interface

To finish setting up your system, manually configure the system's local administrator password, country, and timezone.

Procedure

1. Power on the system and follow the onscreen instructions.
2. Log in to the system web interface.
3. Go to **Security > Local Accounts** to change the local administrator password from the default value (which is the last six characters of your system's serial number).
4. Go to **General Settings > My Information > Location** to specify the country where your system is located.
5. Go to **General Settings > Date and Time** to set the timezone for your system.

Initial system setup is complete. You can start using the system.

Related Links

[Access the System Web Interface](#) on page 9

[Create Local Administrator Credentials](#) on page 38

[Set the System Location](#) on page 25

[Set the Date and Time](#) on page 25

Complete Setup with Provisioning

To finish setting up your system, provision the system's local administrator password, country, and timezone.

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. Power on the system and follow the onscreen instructions.
2. Log in to the system web interface and go to **Servers > Provisioning Server** to register the system with your provisioning service.
3. In your provisioning template configuration file, set the following parameters:
See the [Polycom Documentation Library](#) for detailed descriptions about configuration parameters and their permitted values.
 - `sec.auth.admin.password`
 - `device.local.country`
 - `device.local.timezone`

The provisioning service automatically configures these settings on your system.

Initial system setup is complete. You can start using the system.

Related Links

[Register the System with a Provisioning Service](#) on page 28

Change Conferencing Partner

You can switch the conferencing partner application your system uses (for example, Poly or Zoom Rooms).

Note: The system retains previously configured settings after making this change.

Procedure

1. In the system web interface, go to **General Settings > Provider**.
2. Select a conferencing application from **Choose a Provider**.

The system automatically restarts.

Managing Peripheral Devices

You can pair, monitor, and unpair the devices connected to your system in the system web interface.

Pairing IP Devices on the Link-Local Network

IP devices automatically pair with your G7500 system when connected to either of the system's three link-local network (LLN) ports.

The Studio X50 and Studio X30 don't support LLN connections.

You can pair the following devices to your G7500 system with an LLN connection:

- Poly IP Table Microphone
- Poly IP Ceiling Microphone
- Poly Microphone IP Adapter

While not recommended, you can turn off automatic pairing and manually pair devices using the system web interface.

Automatically Pair an IP Device

By default, IP devices automatically pair when connected to one of the system's link-local network (LLN) ports. For example, when you plug in a Poly IP Table Microphone to the back of the system, it's ready to use.

Procedure

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

If paired successfully, the device displays under **Connected 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 with your system's link-local network (LLN) connections.

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

Procedure


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

Manually Pair an IP Device

If you turn off automatic pairing of link-local network (LLN) connections, you must manually pair an IP device to use it with your system.

Know the MAC address of the device you're pairing.

Procedure

1. Connect the 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 by its MAC address (for example, **00e0db4cf0be**) and select **Pair**.

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

Pair an IP Device on the Primary Network

Some devices connected to your primary network can pair with your video system. For example, this feature enables you to pair a Poly TC8 device without a physical connection to the video system.

Note: Pairing IP audio devices and cameras over the primary network isn't supported.

To pair, the device must be on the same subnet as the video system and the following network address and ports must be unblocked:

- Multicast address 224.0.0.200
- UDP port 2000
- TCP port 18888

Know the MAC address of the device you're pairing. You may see multiple devices you can pair with on your video system's **Device Management** page. Knowing the MAC address makes sure you're pairing with the device you want (for example, the device in the room you're setting up).

A device may pair automatically after connecting to the network. However, you may need to manually pair a device in the following situations:

- The device doesn't automatically pair during setup with the system you purchased.
- You want to pair the device with a different system.
- You want to pair multiple similar devices (for example, to control the system with more than one Poly TC8 device).

Procedure

1. Connect the device you want to pair to an Ethernet port in the room.
2. In the system web interface, go to **General Settings > Device Management**.

Note: The **Enable New Device Auto-Pairing** setting applies only to link-local network (LLN) devices, not devices connected to the primary network.

3. Under **Available Devices**, find the device by its MAC address (for example, **00e0db4cf0be**) and select **Pair**.

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

If pairing isn't successful, check the network connection and the configuration of your device and system you're pairing with.

Unpair an IP Device

You must unpair an IP device if you no longer want to use it with a particular video system.

Don't unpair devices if you plan to use them with the same system. For example, if you move your video-conferencing equipment to another room, just disconnect and reconnect the devices in the new location.

Note: If you unpair a link-local network (LLN) device, it won't automatically pair again with the same system. (The Studio X50 and Studio X30 don't support LLN connections.)

Procedure

1. In the system web interface, go to **General Settings > Device Management**.
2. Under **Available Devices**, find the device by its MAC address (for example, **00e0db4cf0be**) and select **Pair**.

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

Related Links

[Move a Microphone Adapter to Another Location](#) on page 23

Connect a USB Device

You can use some USB devices with your system. See the latest *Release Notes* for supported USB devices.

You can only connect a USB device to a G7500 system.

Procedure

- » Connect the device to a **USB**  port on the back of your system.

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.

The Studio X50 and Studio X30 don't support IP microphones.

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

- Poly IP Table Microphone
- Poly IP Ceiling Microphone

Related Links

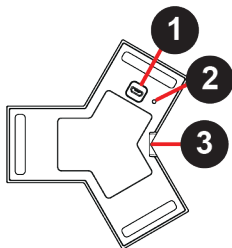
[Polycom Acoustic Fence](#) on page 57

Related Links

[Factory Restore a Table Microphone](#) on page 80

Poly IP Table Microphone Ports

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

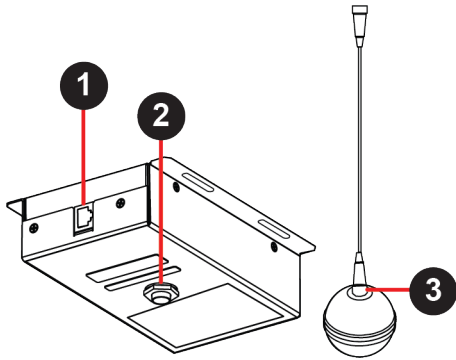


Poly IP Table Microphone Port Descriptions

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

Poly IP Ceiling Microphone Ports

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

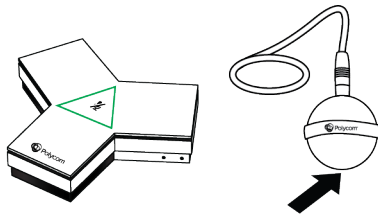


Poly IP Table Microphone Port Descriptions

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.



IP Microphone LED Status Indicators

Indicator	Status
Solid then blinking white	Powering on

Indicator	Status
Solid red	Muted microphone To avoid distraction, the ceiling microphone doesn't display red when muted.
Solid green	In a call and microphone not muted To avoid distraction, the ceiling microphone doesn't display green in a call.
Alternating blinking and solid amber	Update in progress
Blinking amber	Factory restore in progress
Blinking blue	Ready to pair
Solid blue	Paired successfully

Poly Microphone IP Adapter

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

The Studio X50 and Studio X30 don't support the microphone adapter.

See the latest video system *Release Notes* for which audio devices work with the microphone adapter.

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

Related Links

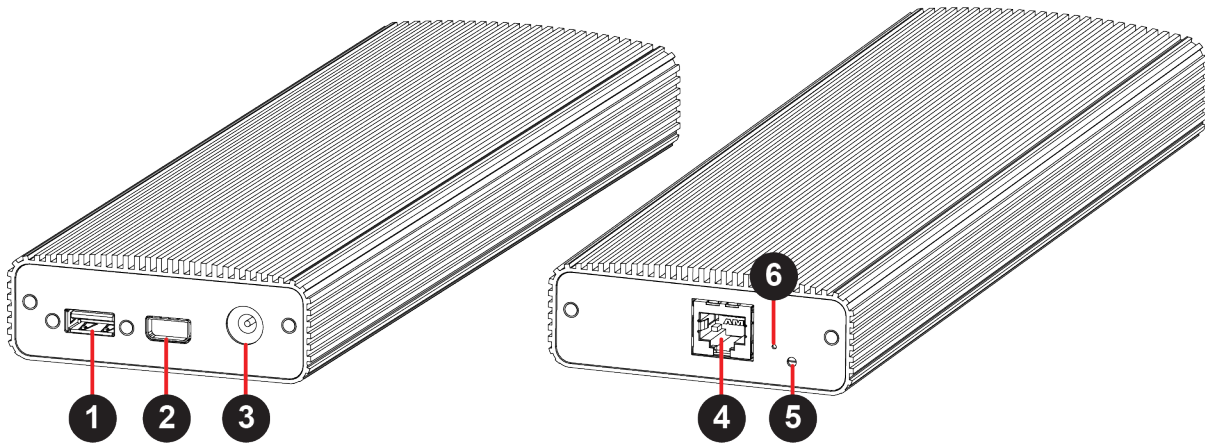
[Configuring the Microphone Adapter](#) on page 57

Related Links

[Factory Restore a Microphone Adapter](#) on page 82

Microphone Adapter Ports

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

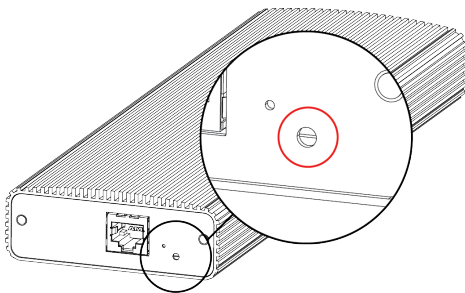


Microphone Adapter Port Descriptions

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 restore pinhole

LED Status Indicators for the Microphone Adapter

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



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 power 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 system in one room to a 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 Device](#) on page 18

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](#)
- [System Usage Data Collected by Poly](#)

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

Name the System and Room

Name your system and assign it a room name.

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 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.
 - **Site**
 - **Organization**
 - **City**

- **State/Province**
 - **Country**
4. Select **Save**.

Set the Date and Time

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

Procedure

1. In the system web interface, go to **General Settings > Date and Time**.
2. 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 .

Related Links

[Complete Setup with the System Web Interface](#) on page 15

Set the System Location

Specify the country and country code where the 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.

Related Links

[Complete Setup with the System Web Interface](#) on page 15

Set the Local Interface Language

Change the language that users see on the 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

[Configure General Audio Settings](#) on page 55

[Configure General Camera Settings](#) on page 66

System Usage Data Collected by Poly

By default, your system sends usage data to Poly to help improve its products and services.

For information about the data that Poly collects, see the system [Privacy Guide](#).

Turn Off System Usage Data Collection

You can stop your system from sending usage data to Poly.

Procedure

1. In the system web interface, go to **Servers > Cloud > Preferences**.
2. Clear the check box to stop the data collection.

Using a Provisioning Service

Topics:

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

Use a provisioning service to deploy enterprise-wide configurations to your systems.

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

- Automatically configure 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 [Poly VideoOS Configuration Parameters Reference Guide](#).

Related Links

[Updating Software](#) on page 75

[PKI Certificates](#) on page 42

Related Links

[Choose How to Get Software Updates](#) on page 75

Register the System with a Provisioning Service

Before you can provision a system, you must 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.

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

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.
4. 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.

5. Select **Save**.
6. Verify that **Registration Status** changes from **Pending** to **Registered**.
It might take a minute or two for the status to change.

Related Links

[Check Provisioning Results](#) on page 92

[Complete Setup with Provisioning](#) on page 16

Download a Template Configuration File

Template configuration files show how parameters are set on your 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 systems. For more information, see the [Polycom RealPresence Resource Manager System Operations Guide](#).

Procedure

1. In the system web interface, go to **Servers > Provisioning Server**.
2. Select **Download Profile Template**.
The template saves to your local device as a `.cfg` file.

Managing Conferencing Applications

Topics:

- [Update Third-Party Conferencing Software Manually in the System Web Interface](#)

You can manage conferencing applications installed on your system.

Update Third-Party Conferencing Software Manually in the System Web Interface

You can manually update the third-party conferencing software on your system.

Download the update file from your conferencing provider's website and save it on your computer.

Procedure

1. In the system web interface, select **Application Management**.
2. Select the conferencing application you want to update.
3. Select **Choose File**, navigate to the update file on your computer, and select **Open**.

Your system installs the update and automatically restarts.

Configuring Network Settings

Topics:

- [Configuring Wired LAN Settings](#)
- [Configure Wi-Fi Settings](#)
- [Configure Network Quality Settings](#)

Network settings include the system primary (wired LAN) and secondary (Wi-Fi) network configurations.

Configuring Wired LAN Settings

You can set the wired LAN properties for your system.

Related Links

[LED Status Indicators for the System LAN Ports](#) on page 96

Automatically Obtain IPv4 Address Settings

Your system by default gets its IP address information automatically. If this behavior is turned off, you can turn it back on.

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**.

Manually Configure IPv4 Address Settings

You can manually specify the system's IPv4 address settings.

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

4. Select **Save**.

Manually Assign a Host Name and Domain Name

You can manually enter the host name and domain name for your system. You also can modify these settings even if your network automatically assigns them.

Procedure

1. Enter or modify the system **Host Name**.

Indicates your system name. If the system discovers a valid name during setup or a software update, the system automatically creates the host name. However, if an invalid name is found, such as a name with a space, the system creates a host name using the following format: `SystemType-xxxxxxx`, where `xxxxxxx` 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).

2. Optional: Enter or modify the **Domain Name** that the system belongs to.
3. Select **Save**.

Manually Configure DNS Settings

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

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

Procedure

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

Configure VLAN Settings

You can configure your system's virtual LAN (VLAN) settings.

Procedure

1. In the system web interface, go to **Network > Primary Network > LAN Options**.
2. Turn the **Enable LLDP** setting on so that the system can advertise itself on the network using the Link Layer Discovery Protocol (LLDP).
3. Turn the **802.1p/Q** setting on and enter a **VLAN ID**.
You can use values from 1 to 4094.
4. Enter a **Video Priority** to set the link layer priority of video traffic on the wired LAN.
Video traffic is RTP traffic consisting of video data and associated RTCP traffic. You can use any value from 0 to 7, although Poly recommends not using 6 and 7.
5. Enter an **Audio Priority** to set the link layer priority of audio traffic on the wired LAN.
Audio traffic is RTP traffic consisting of audio data and associated RTCP traffic. You can use any value from 0 to 7, although Poly recommends not using 6 and 7.
6. Enter a **Control Priority** to set the link layer priority of control traffic on the wired LAN.

Control traffic consists of control information associated with a call:

- **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)

You can use any value from 0 to 7, although Poly recommends not using 6 and 7.

7. Select **Save**.

Configure 802.1X Settings

You can configure your system to use 802.1X authentication when connecting to the wired LAN.

Install the PKI certificates on your system required for authenticating with your network.

The system supports the following authentication protocols:

- EAP-MD5
- EAP-PEAPv0 (MSCHAPv2)
- EAP-TTLS
- EAP-TLS

Procedure

1. In the system web interface, go to **Network > Primary Network > LAN Options**.
2. Turn on the **Enable EAP/802.1X** setting.
3. Enter a **EAP/802.1X Identity** for your system.
You can't leave this field blank.
4. Enter a **EAP/802.1X Password** for your system.
This setting is required when you use EAP-MD5, EAP-PEAPv0, or EAP-TTLS.
5. Select **Save**.

Related Links

[PKI Certificates](#) on page 42

Configure Wired LAN Options

You can configure other LAN properties for your 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
Autonegotiation (under General Settings in the local interface)	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. Poly recommends that you use autonegotiation to avoid network issues.

Setting	Description
LAN Speed (under General Settings in the local interface)	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.
Duplex Mode (under General Settings in the local interface)	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.
Ignore Redirect Messages	Enables the system to ignore ICMP redirect messages. Polycom recommends that you enable this setting in most circumstances.
ICMP Transmission Rate Limit (millisec)	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. This setting applies only to “error” ICMP packets. This setting has no effect on “informational” ICMP packets, such as echo requests and replies.
Generate Destination Unreachable Messages	Generates an ICMP <code>Destination Unreachable</code> message if the system can’t deliver a packet to its destination for reasons other than network congestion.
Respond to Broadcast and Multicast Echo Requests	When enabled, your system sends an ICMP <code>Echo Reply</code> message in response to a broadcast or multicast Echo Request that isn’t specifically addressed to the system.

3. Select **Save**.

Configure Wi-Fi Settings

In addition to a LAN, you can also connect your system to a Wi-Fi network so that guests can share content to the system using an AirPlay-certified device or the Polycom Content App.

Caution: Disable the secondary Wi-Fi network in Partner Mode.

Configure Network Quality Settings

You can specify how your 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	<p>Specifies the MTU size (in bytes) used in calls.</p> <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	<p>If you enable this setting, the system uses the Lost Packet Recovery (LPR) protocol to help compensate for packet loss if it occurs.</p>
Enable RSVP	<p>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.)</p>
Dynamic Bandwidth	<p>Enable this setting if you want the system to automatically determine the optimal call rate.</p>
Maximum Transmit Bandwidth	<p>Specifies the maximum transmit call rate between 64 kbps and the system's maximum line rate.</p> <p>Use this setting when the system connects to the network using an access method with different transmit and receive bandwidths.</p>
Maximum Receive Bandwidth	<p>Specifies the maximum receive call rate between 64 kbps and the system's maximum line rate.</p> <p>Use this setting when the system connects to the network using an access method with different transmit and receive bandwidths.</p>

3. Select **Save.**

Securing the System

Topics:

- [Managing System Access](#)
- [PKI Certificates](#)
- [Call Encryption](#)
- [H.460 Firewall/NAT Traversal](#)
- [Web Proxies](#)
- [View Connections to the System](#)
- [System Port Usage](#)

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

Related Links

[SNMP Reporting](#) on page 88

Managing System Access

You can control how users and administrators access the system.

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

- Local interface
- System web interface

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 system.

Poly 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.

Setting	Description
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 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	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 disable Use Room Password for Remote Access , you must enter this password to access the system web interface. This password lets you perform device management tasks, such as updating the system's software.
Use Room Password for Remote Access	Enable this option to also use the room password for remote logins. Disable this option to require a separate password for remote logins.

3. Select **Save**.

Related Links

[Complete Setup with the System Web Interface](#) on page 15

Configure Account Lockout Settings

You can specify account lockout controls to prevent unauthorized access to your 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>

Configure System Access Settings

You can configure how you and others access the 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.
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)	<p>Specifies the port to use when accessing the system web interface over HTTP.</p> <p>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.</p> <p>(This setting is unavailable if Restrict to HTTPS is enabled.)</p>
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 .
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.

Setting	Description
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**.

Configure the System Web Interface Port Lock

You can limit the number of failed login attempts to the 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**.

Disable USB Ports

You can configure your system so no one can use its USB 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, Poly recommends that you have a strong understanding of certificate management and how it applies to your system.

PKI certificates authenticate secure network connections to and from the 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 28

Related Links

[Configure 802.1X Settings](#) on page 33

Create a Certificate Signing Request

If you deploy a PKI in your environment, create a CSR to make sure your 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. Poly 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 unit of business defined by your organization. Default is blank. Maximum Characters: 64 Note: The system supports only one OU field. If you want the signed certificate to include more than one OU field, you must download and edit the CSR manually.
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.
SAN: FQDN	Specifies the FQDN assigned to the system. This is the same as the Common Name (CN) , but it isn't truncated. Default is blank. Maximum Characters: 253
SAN: Additional Name	Specifies an additional name. Default is blank. Maximum Characters: 253
SAN: IPv4 Address	Default is the IPv4 address of the system. Maximum Characters: 15
User Principle 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 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 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 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 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 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 **Delete**  in the same row as the certificate.

Caution: 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 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 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 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 **Delete**  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 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 .

Setting	Description
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	<p>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. It's recommended that you always include a URI in this field regardless of how you configure Use Responder Specified in Certificate.</p>
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**.

Call Encryption

Check your conferencing application documentation for information about how calls are encrypted.

H.460 Firewall/NAT Traversal

You can configure your 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

H.460 firewall/NAT traversal can be necessary if you're calling with a cloud-based conferencing service or 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. Make sure that the **Enable H.460 Firewall Traversal** check box is selected.
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>

Setting	Description
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>
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>

Setting	Description
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, it's recommended that you disable this setting to enable calls to fully connect.</p>

6. Select **Save**.

Web Proxies

A web proxy can help your 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:

- Provisioning service
- Software updates

Related Links

[Checking the Web Proxy Configuration](#) on page 99

Enable the System to Use a Web Proxy

By default, your 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 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 semiautomatic web proxy configuration, you must specify the URL your 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 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 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 system.

The list provides the following information:

- 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 HDMI-connected laptop, you don't see that this device is connected to the system.

Procedure

- » In the system web interface, go to **Diagnostics > Sessions**.

System Port Usage

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

Note: Check your conferencing partner's documentation for firewall settings specific to their service.

G7500, Studio X50, and Studio X30 System Port Usage

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
53	Outbound	Static	UDP	DNS	Yes	No

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
80	Inbound	Static	TCP	HTTP web server listener that provides access to the web interface. Redirects all sessions to HTTPS on port 443.	Yes	Yes
123	Outbound	Static	UDP	NTP (automatic time synchronization)	Yes	No
161	Inbound	Static	UDP	SNMP reporting	No	Yes
443	Bidirectional	Static	TCP/SCTP	Static TCP HTTPS web server listener that provides TLS access to the web interface. Zero Touch Onboarding Provisioning (for example, RealPresence Resource Manager) Video system control using the Poly TC8 device REST API	Yes	No
514	Outbound	Static	UDP	Remote logging	No	Yes
601	Outbound	Static	TCP	Remote logging	No	Yes
2000	Inbound	Static	UDP	Multicast pairing	Yes	No
4443	Bidirectional	Static	TCP/TLS	Web server for peripheral device software downloads and log uploads	Yes	No

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
5127	Outbound	Static	TCP	Poly usage data collection	No	No
6514	Outbound	Static	TLS	Remote logging	No	Yes
7080	Inbound	Static	TCP	Web services	Yes	No
7081	Inbound	Static	TCP	Web services	Yes	No
18888	Inbound	Static	TCP	Modular room messaging	Yes	No
Various	Other ports may be used depending on the conferencing application you've selected. See the partner's relevant documentation for more information.					

Configuring Audio Settings

Topics:

- [Configure General Audio Settings](#)
- [Audio Input](#)
- [Audio Output](#)

You can configure audio settings in the system web interface.

Configure General Audio Settings

You can specify general audio settings for your 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. This feature isn't available on the Studio X30 system. 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.

Setting	Description
Enable M-Mode	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. When you enable M-Mode, even the faintest musical notes come through clearly.
Enable Keyboard Noise Reduction and NoiseBlock	Enables Poly NoiseBlockAI, which during calls eliminates background and extraneous sounds in common working environments when no one is talking. Note: This setting is disabled when you enable M-Mode. If you use an external echo canceller, keyboard noise reduction is not available.
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, you should 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 26

[Test Speakers](#) on page 96

Audio Input

You have several options to input audio for your system.

Your system supports the following audio inputs:

- IP-based Poly audio peripheral devices (for the G7500 system only):
 - **Poly IP Table Microphone**
 - **Poly IP Ceiling Microphone**
 - **Poly Microphone IP Adapter**
- **3.5 mm** (for the G7500 system only): 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 system.

The Studio X50 and Studio X30 don't support IP microphones.

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 Poly 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 Poly 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 meter)	Shows you the peak input signal level for Poly microphones.

Configuring the Microphone Adapter

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

The Studio X50 and Studio X30 don't support microphone adapters.

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

[Poly Microphone IP Adapter](#) on page 21

Polycom Acoustic Fence

Polycom Acoustic Fence technology creates a virtual *audio fence* that blocks sounds from outside the fence. It suppresses background noise during calls to enhance audio quality for call participants.

Note: This feature is only available on the G7500 system.

Polycom Acoustic Fence works in mono mode only and disables Polycom StereoSurround when enabled.

Polycom Acoustic Fence technology provides the following:

- 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 someone leaves the fenced area
- Enables you to adjust the width of the audio fence *beam* to define the area where sounds are picked up

Once you enable Polycom Acoustic Fence, you must set up additional hardware to use this feature with your G7500 system. You need a primary microphone and at least one more microphone to create the fence.

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

- Table microphone
- Ceiling microphone

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

Once you set up the microphones, you can adjust the width of the audio fence beam to limit or expand where sounds are picked up inside the fence.

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

Related Links

[IP Microphones](#) on page 19

Related Links

[Fix Polycom Acoustic Fence Issues with G7500](#) on page 98

Configure Polycom Acoustic Fence

You can enable and configure the Polycom Acoustic Fence feature to help define the *audio fence* around the system.

Note: This feature is only available on the G7500 system.

Procedure

1. In the system web interface, go to **Audio/Video > Audio > General Audio Settings**.
2. Select the **Enable Acoustic Fence** check box.

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

3. Set **Acoustic Fence Sensitivity** to adjust the width of the audio fence beam.

Higher values increase the width of the audio fence beam between the primary and fence microphone(s). Use 0 for the narrowest beam (+/- 10 degrees) or 10 for the widest beam (+/- 60 degrees).


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 as the primary microphone. By default, a microphone pairs to the system when you connect it (unless you've disabled automatic pairing). You can connect up to three microphones directly to your 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. Connect the primary microphone to an **LLN**  port on the back of your system.

Important: 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 must reconnect all microphones (starting with the primary microphone) for it to work again.

2. Connect the other microphone(s).

Related Links


[Poly G7500 System 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 system.

The Studio X50 and Studio X30 don't support 3.5 mm audio input.

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.
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 system to fit your setup.

You can use the primary monitor's built-in speakers, the Studio X50 and Studio X30 systems' built-in speakers, or you can connect an external speaker system (such as Polycom StereoSurround kit) to the G7500 system 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 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.
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 change the volume. ▪ 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 system through HDMI.

The Studio X50 and Studio X30 don't support 3.5 mm audio output.

Configuring Video and Camera Settings

Topics:

- [HDMI I/O](#)
- [Supported HDCI Input Resolutions](#)
- [Configure Monitor Settings](#)
- [Configure a Touch Monitor](#)
- [Monitors with CEC](#)
- [Configure General Camera Settings](#)
- [Configure Camera Tracking Settings](#)
- [Configure Video Input Settings](#)

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

Use the information about supported HDMI I/O resolutions and codec capabilities to optimize your video experience based on your deployment requirements.

HDMI I/O

Your system has HDMI input and output ports.

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)
The Studio X30 system doesn't have a second HDMI output.
- Input for content sharing, including audio streaming

Note the following:

- 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.
- The HDMI specifications don't provide maximum cable length definitions. The requirements defined in the specification implicitly give rise to length limitations that are based on the cable's construction.
- As with other Polycom hardware, the HDMI ports on your system meet HDMI specification requirements. HDMI signal quality is dependent on every cable and connector in the HDMI path. Passive HDMI extenders, female-female couplers, and wall plates are potential points of failure and signal loss.
- A high-quality passive cable of minimum length provides the most repeatable solution. As the power level of HDMI output devices can vary greatly, keep the distance from the HDMI source to the system input as short as possible.

Polycom claims no responsibility or liability for the quality, performance, or reliability of third-party HDMI cables, HDMI splitters, or HDMI USB adapters.

Polycom recommends working with your A/V integrator or partner who understands the unique requirements in your environment.

Related Links

[Overview of Poly G7500, Studio X50, and Studio X30 Hardware](#) on page 10

Supported HDMI Output Resolutions for Single-Monitor Setups

Your 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
FHD	1920 × 1080p	50, 60

Supported HDMI Output Resolutions for Dual-Monitor Setups

The G7500 and Studio X50 systems support 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 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

Supported HDCI Input Resolutions

The HDCI input resolution is fixed based on the supported Poly camera.

HDCI input applies only to the G7500 system.

Configure Monitor Settings

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

The Studio X30 system doesn't support dual monitors.

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 Monitor Settings](#) on page 64

[Configure Dual Monitor Display Settings](#) on page 72

Configure a Touch Monitor

In a dual-monitor setup, you must configure the touch monitors to work in the system local interface.

Note: Touch monitors in single-monitor setups don't require configuration. For example, there's no additional touch monitor configuration required if you have a Studio X30 system.

Procedure

1. From the right border of your screen, swipe left.
2. Go to **Settings > Diagnostics > Touch Configuration**.
3. On each screen, select the **Hand** icon.
4. Select **Finish Configuration**.

Monitors with CEC

You can use some Consumer Electronics Control (CEC) features with HDMI-connected monitors that support the CEC protocol.

Your system supports the following CEC commands:

- **System Standby:** When the system goes to sleep, connected monitors switch to standby mode to save power.

Remember the following when enabling CEC on your system:

- If you connect a monitor with an HDMI splitter, the splitter must support CEC. Due to HDMI splitter limitations, monitors behind a 1xM (one-input multiple-output) splitter might not switch to the correct input when waking up.
- The system doesn't respond to CEC commands from a monitor remote control.
- If a monitor is connected to two endpoints, the monitor displays the active endpoint when the other is sleeping.

Disable CEC

You can disable CEC in the system web interface.

Procedure

1. In the system web interface, go to **Audio/Video > Monitors**.
2. Clear the **Enable Consumer Electronics Control** check box.

Enable CEC

You can enable CEC in the system web interface.

Make sure your monitor's CEC settings are configured correctly (see your monitor's documentation).

Procedure

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

2. Select the **Enable Consumer Electronics Control** check box.

Configure General Camera Settings

You can configure settings for cameras connected to your system. The system automatically discovers your camera model and displays the relevant settings in the system web interface.

See the latest *Release Notes* for specific information about the cameras you can use with your system.

Note: If you connect an unsupported camera, the system still attempts to show video. Poly 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 > General Camera Settings**.
2. 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.

3. Select **Save**.

Related Links

[Update Poly HDCI Cameras](#) on page 77

[Configure Sleep Settings](#) on page 26

Configure Camera Tracking Settings

Poly camera tracking technology provides automatic speaker and group framing in the room.

Tracking options and behavior depend on your system model and camera. For example:

- The **Frame Speaker** camera tracking option isn't available on the Studio X50 or Studio X30 systems.
- If you use a standalone EagleEye IV camera with a G7500 system, you won't see tracking options.

Procedure

- In the system web interface, go to **Audio/Video > Video Inputs**.
- Go to **Input 1** and specify a camera **Tracking Mode**.
 - Frame Group**
 - For G7500 systems:** The camera automatically locates and frames participants in the room without moving the camera.
 - For Studio X50 and Studio X30 systems:** The camera automatically locates and frames participants in a small or medium room.
 - Frame Group with Transition:** The camera automatically locates and frames 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. This option is available only with a G7500 system using an EagleEye Producer camera.

- **Frame Speaker:** The camera automatically locates and frames the active speaker. When someone else starts speaking, the camera switches to that person.

Note: When you mute the local microphone, the camera tracking mode automatically switches to **Frame Group**.

- **Off:** Disables automatic tracking. You must handle all camera control manually.
3. Select a **Tracking Speed**, which determines how quickly the camera frames new speakers and participants.
The room environment can influence the tracking speed.
 4. Optional: Turn on the **Picture in Picture** setting.
This setting is available only with G7500 systems using an EagleEye Director II camera. 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).
 5. Select **Save**.

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.

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 doesn't.

3. Configure the following settings:

Setting	Description
Input format	Specifies the source type of the device. This setting is read-only unless the system doesn't detect the device.
Name	Enter a name for the camera or device.
Model	Displays the type of device connected to the system.
Orientation	Specifies whether the display is oriented normally or inverted (upside down).

Setting	Description
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	<p>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.</p>
Skin Enhancement	<p>Enables or disables natural skin color enhancements for participants.</p>
Wide Dynamic Range	<p>Enables or disables re-exposure according to the framed area instead of full view.</p>
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: Recommended 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> ▪ 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)

Setting	Description
Framing Size	Specifies the framing view. <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
Sharpness	Adjusts the video's overall clarity.
Brightness	Adjusts the video brightness.
Color Saturation	Adjusts the color saturation.

4. Select **Save**.

Sharing Content

Topics:

- [Default Option for Sharing Content](#)

Your system provides several ways to share and annotate content.

Default Option for Sharing Content

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

- **Wired input:** A laptop or desktop connected to the system through HDMI.

Customizing the Local Interface

Topics:

- [Configure Dual Monitor Display Settings](#)

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

Configure Dual Monitor Display Settings

You can choose your self view and content display preferences when you connect two monitors to your 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.

The Studio X30 system supports only one 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 the self view in the corner of Monitor 2.▪ Full Screen: Displays the self view on the entire screen of Monitor 2.
Content Display	<p>Specifies whether to display content on one or two monitors.</p> <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 64

System Maintenance

Topics:

- [Activating System Features](#)
- [Unlock System Settings](#)
- [Updating 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](#)

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

Activating System Features

The 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 Poly dealer to get a key.

Note: Software version 3.0 enables all available Poly system features by default. With this version, you don't need a feature activation or software version key.

Your conferencing application may require a separate license or subscription for call-related features. Contact your conferencing partner for information.

A *key* is a number that unlocks certain features or gives you the ability to update your 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.
- **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 activate features for multiple systems covered by a software service agreement, select **Batch Activation**. Follow the onscreen instructions to upload the text file that contains your system license numbers and serial numbers (or serial numbers only). You are sent a text file containing the requested keys for each system.
 - To update multiple systems that are covered by a software service agreement, select **Batch Upgrade** and choose your product. Follow the onscreen instructions to upload the text file that contains your system license and serial numbers (or serial numbers only).

Activate Features

To activate certain features for your 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 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 setting with your system's local administrator credentials.

Procedure

1. From the far right border of the screen, swipe left and select **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 system software a few different ways.

Use one of the following methods to update system software:

- Poly 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 devices (if those devices have a new version available). Depending on your setup, these devices might include:

- Poly IP Table Microphone
- Poly IP Ceiling Microphone
- Poly Microphone IP Adapter
- Poly EagleEye Cube USB camera
- Poly TC8 device

Related Links

[Using a Provisioning Service](#) on page 28

Updating Software in the System Web Interface

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

Choose How to Get Software Updates

You may have several options to update your 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.

Software Update Method	Description
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 some of your connected devices (for example, a TC8 device) and the video system. To successfully update everything, you must have this exact folder structure:</p> <ul style="list-style-type: none"> ▪ eecube <ul style="list-style-type: none"> ◦ Config ◦ image.zip ◦ version ▪ g7500 <ul style="list-style-type: none"> ◦ Config ◦ poly-video-<version>.zip ◦ release.json ◦ version ▪ ipmic <ul style="list-style-type: none"> ◦ Config ◦ image.zip ◦ version ▪ micadapter <ul style="list-style-type: none"> ◦ Config ◦ image.zip ◦ version ▪ touchctrl <ul style="list-style-type: none"> ◦ Config ◦ poly-tc8-<version>.zip ◦ version ◦ release.json ▪ 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 28

Manually Update Software

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

Automatically Update Software

You can automatically update the software of your system and its connected 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 system with a USB flash drive.

Note: Poly 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.
3. 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 Poly HDCI Cameras

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

HDCI cameras only apply to the G7500 system.

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 General Camera Settings](#) on page 66

Manually Downgrade Software in the System Web Interface

You can downgrade your system software and the software of some of its connected peripheral devices from a custom download server.

Before you downgrade, Poly recommends doing the following:

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

Procedure

1. Go to **General Settings > Device Management**.
2. Manually downgrade your software to an older version located on your download server.

Downgrade Software with a USB Flash Drive

You can downgrade your system software and the software of some of its connected peripheral devices using a USB flash drive.

Before you downgrade, Poly recommends doing the following:

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


Procedure

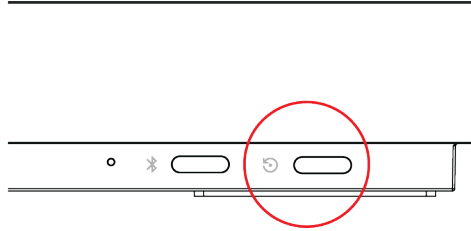
1. Download an older software version to a USB flash drive.
2. Connect the USB flash drive to your system.

Restart the System

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

Procedure

- » Do one of the following:
 - (G7500 only) On the front of the system, press and hold the **Restart**  button for five seconds.



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

Related Links

[Powering the System On and Off](#) on page 9

Reset System Settings

You can reset your 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
- Logs

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

Note: System resets restores your system to its original mode of operation (e.g., Poly Video Mode or Poly Partner Mode).

Procedure

1. In the system web interface, go to **Diagnostics > System Reset**.
2. Select **Reset All System Configurations**.
3. 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.**
4. Select **Reset**.

Factory Restore the System

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

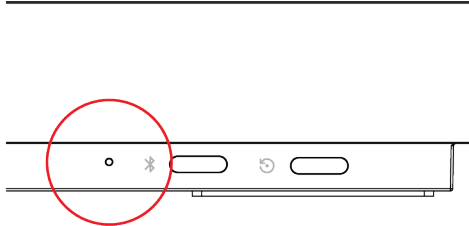
The system doesn't save the following data with a factory restore:

- Current software version
- Logs

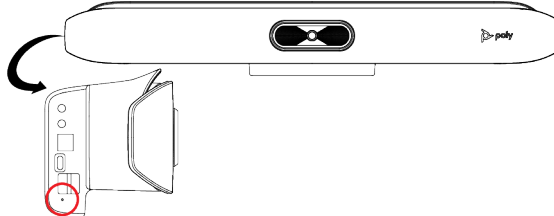
- User-installed PKI certificates
- Local directory entries
- Call detail record (CDR)

Procedure

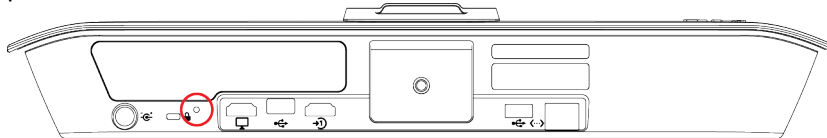
1. Disconnect the power supply to turn off the system.
2. Do one of the following:
 - On the front of the G7500 insert a straightened paper clip through the factory restore pinhole.



- On the side of the Studio X50 insert a straightened paper clip through the factory restore pinhole.



- On the bottom of the Studio X30 insert a strained paper clip through the factory restore 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](#) on page 13

Factory Restore a Table Microphone

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

Procedure

1. Ensure that the microphone is powered on.
2. On the back of the table microphone insert a straightened paper clip through the factory restore pinhole.

3. Press and hold the restore 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 19

Factory Restore a Ceiling Microphone

You can restore a microphone to its default settings. This process refreshes the device 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

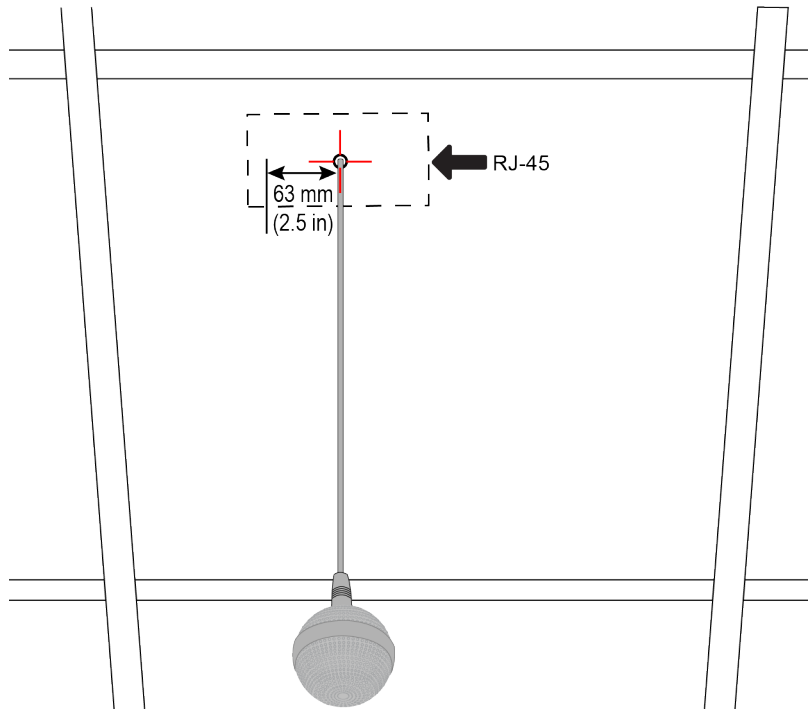
Procedure

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.

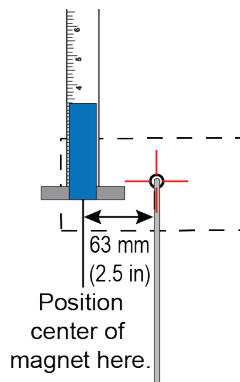
2. Ensure that the microphone is powered on.
3. Locate the factory reset sensor.

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.



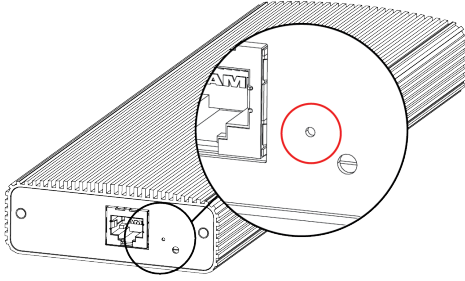
The microphone LED blinks amber during a factory restore.

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

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



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

3. Insert a straightened paper clip through the factory 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

[Poly Microphone IP Adapter](#) on page 21

Troubleshooting

Topics:

- [Logs](#)
- [SNMP Reporting](#)
- [Checking System Status](#)
- [Check Provisioning Results](#)
- [Paired IP Audio Device is Disconnected from G7500](#)
- [Poly TC8](#)
- [Can't Wake the System by Touching the Monitor](#)
- [LED Status Indicators for the System LAN Ports](#)
- [Audio Tests](#)
- [Fix Polycom Acoustic Fence Issues with G7500](#)
- [Test the Call Experience](#)
- [Test Connection with Another System](#)
- [Run a Trace Route](#)
- [Checking the Web Proxy Configuration](#)
- [Zero Touch Onboarding Connection Fails During Initial Setup or After Reset](#)

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

Logs

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

Consolidated System and Peripheral Device Logs

Event information about your system and some of its connected devices are available in a single log package.

The system log package includes details about the following devices:

- Supported cameras (see the latest *Release Notes* for your system)
- Poly TC8 device
- Poly IP Table Microphone (G7500 only)
- Poly IP Ceiling Microphone (G7500 only)
- Poly Microphone IP Adapter (G7500 only)

Configure Log Preferences

You can manage some basic aspects of your 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 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 > Log Management**.
2. Configure the following settings:

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 <code>marketing_<date_and_time></code>. • Timestamp: Folder name is the timestamp of the log transfer (for example, <code><yyyyMMddhhmmssSSS></code>). • Custom: Lets you specify a folder name for manual log transfers.
Storage Type	Specifies the type of storage device used for log file transfers.
Transfer Frequency	Specifies when the system transfers logs: <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.

3. Select **Save**.

Configure Log Level

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

Procedure

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

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>It's recommended 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>

3. Select **Save**.

Download Logs

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

Procedure

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

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

Procedure

1. Connect the USB flash drive to a USB port on the back of the system
2. In the local interface, from the right border of your screen, swipe left.
3. Go to **Settings > Diagnostics > Log Management**.
4. Enter the system's local administrator credentials.
5. 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 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:

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, Poly recommends remote logging only on secure, local networks.</p>
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: <code>192.0.2.0:<port></code>, where <code><port></code> is the elective destination port number in the 1-65535 range. • FQDN: <code>logserverhost.company.com:<port></code>, where <code><port></code> is the elective destination port number in the 1-65535 range.

Setting	Description
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)

3. Select **Save**.

Sample Log File

The following code shows an example of a 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

```

SNMP Reporting

The system supports 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
- 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: Poly 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

Related Links

[Securing the System](#) on page 37

Configure SNMP

You can monitor your 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, Poly recommends that you don't enable this setting.
Version2c	Enables your system to use the SNMPv2c protocol. Due to security issues, Poly 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.
Read-Only Community	Specifies the SNMP community string for your system. For security reasons, don't use the default community string (<code>public</code>). Note: Poly doesn't support SNMP write operations for configuring or provisioning systems. The community string is for read operations and outgoing SNMP traps.
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.

Setting	Description
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, :F: is equivalent to :0F:).</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).
Transport Protocol	<p>Specifies the transport protocol used.</p> <ul style="list-style-type: none"> ▪ TCP ▪ UDP
Destination Address1 Destination Address2 Destination Address3	<p>Specifies the IP addresses of SNMP managers where SNMP traps are sent.</p> <p>Each address has four settings:</p> <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 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**.

Checking System Status

You can verify the status of your system in the local and system web interfaces. Status information also include details about connected 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 Local Interface

Verify your system status in the local interface.

Procedure

1. From the right border of your screen, swipe left.
2. Go to **Settings > Status**.
3. 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  icon 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.

Setting	Description
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 system status in the system 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 the corresponding settings page.

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 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** and verify if parameters applied successfully the last time you provisioned your system.

The **Result** column displays one of the following statuses:

- **SUCCESS:** The parameter was applied.
- **IGNORED:** The parameter didn't apply because a configuration that controls this feature is disabled, not applicable, or wasn't provisioned.
- **FAILURE:** If you see this, the **Error Message** column can help you identify the issue.

For a list of available system parameters and their permitted values, see the [Poly VideoOS Configuration Parameters Reference Guide](#).

Related Links

[Register the System with a Provisioning Service](#) on page 28

Paired IP Audio Device is Disconnected from G7500

Symptom:

You paired an IP audio device with your G7500 system but can't use it. On the system 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. Complete each step until you've fixed the issue.

Procedure

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 Poly 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.

Poly TC8

Use the following information to troubleshoot issues with a Poly TC8 device.

Poly TC8 Can't Pair to the Video System

Symptom:

After powering on the device, it doesn't automatically pair with the video system. You also can't manually pair the device from the **Available Devices** list in the video system web interface.

Problem:

Network traffic on TCP port 18888 is blocked.

Workaround:

Procedure

- » Allow traffic on TCP port 18888.

Poly TC8 Doesn't Display On the Available Devices List

Symptom:

Even though the device you want to pair is connected to the network, you don't see it under **Available Devices** in the video system web interface.

Problem:


There are a few possible causes for this issue:

- The device and video system aren't on the same subnet.
- The network switch isn't allowing UDP broadcast traffic forwarded to multicast address 224.0.0.200 on port 2000.
- The device is paired with another video system.

Workaround:

Complete each step until you see the device on the **Available Devices** list:

Procedure

1. Make sure the device and video system are on the same subnet.
If needed, work with your network administrator.
2. Allow traffic to 224.0.0.200 on UDP port 2000.
3. Make sure the device isn't paired with another video system. If it is, unpair the device.
4. In the device interface, go to **Settings**  > **Reset** and select **Reset**.
Your device resets to its default configuration settings, which unpairs it from the video system.

Paired Poly TC8 is Disconnected

Symptom:

You paired a device with your video system but can't use it. On the system 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:

Complete each step until you've fixed the issue.

Procedure

1. Check the device's LAN cable connection.
2. Restart the device.
3. Restart the video system.
4. Make sure network traffic on TCP port 18888 is unblocked.
5. Perform a factory restore on the device.
6. Perform a factory restore on the system.

Poly TC8 Paired to Inaccessible Video System

Symptom:

Your device was paired with a video system you can no longer access (for example, the video system lost its network connection or was moved to another location). Whatever the situation, the device screen now indicates it's waiting to pair.

Problem:

The device is still paired to the video system but can't connect to it.


Workaround:

When this happens, there's a reset button in the device **Settings** menu to unpair the device from the video system.

If you can eventually access the video system it was paired with, you also should unpair the device from the **Device Management** page. Otherwise, the device continues to display in the **Connected Devices** list but is `Unavailable`.

Once unpaired, you can pair the device with the same video system or another video system.

Procedure

1. In the device interface, go to **Settings**  > **Reset** and select **Reset**.
Your device resets to its default configuration settings, which unpairs it from the video system.
2. In the system web interface, go to **General Settings** > **Device Management**.
3. Under **Connected Devices**, find the device by its MAC address (for example, `00e0db4cf0be`) and select **Unpair**.

The device you're unpairing should have an `Unavailable` status.

Can't Wake the System by Touching the Monitor

Symptom:

Touching the monitor doesn't wake your system.

Problem:

If your system's **Display** setting is on **No Signal**, your monitor may be powering down its USB ports when the system goes to sleep and disabling its touch capabilities.

Workaround:

1. Configure your monitor to wake when touched.
2. If your monitor doesn't have this kind of setting, switch your system's **Display** setting to **Black**.

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 system.

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.

The G7500 system has four LAN ports: one for the system's network connection (farthest left) and three link-local network (LLN) connections for peripheral devices.

LED Status Indicators for the 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 31

Related Links

[Poly G7500 System Ports](#) on page 10

Audio Tests

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

Test Speakers

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

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

The Studio X30 system doesn't support stereo audio.

Procedure

1. In the system web interface, go to **Diagnostics > Audio Test**.
2. Do one of the following:
 - 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 55

Test Audio Levels

Audio meters show you real-time audio input and output signals for your 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 Meters**.
 - In the local interface, from the right border of your screen swipe left, and go to **Settings > 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 system to use Polycom StereoSurround, you can place a test call to see if it works.

Make sure the microphones are positioned correctly.

The Studio X30 system doesn't support stereo audio.


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 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**.

Fix Polycom Acoustic Fence Issues with G7500

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 57

Test the Call Experience

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

This test isn't available in a call.

Procedure

1. In the local interface, from the right border of your screen, swipe left.
2. Go to **Settings > Diagnostics**.
3. Go to **Near End Loop**.
4. 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 system can call another system.

Procedure

1. In the local interface, from the right border of your screen, swipe left.
2. Go to **Settings > Diagnostics**.
3. Go to **Ping**.
4. Enter the IP address or URL of the system you want to call.
5. 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 system.

Procedure

1. In the local interface, from the right border of your screen, swipe left.
2. Go to **Settings > Diagnostics**.
3. Go to **Trace Route**.
4. Enter the IP address or URL with which to run the trace route.
5. Select **Start**.

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

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 50

PAC File Status

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

PAC File Status

Status	Description
Success	File successfully downloaded to your system.
In Progress	File is downloading to your system.
WPAD Failed	File download URL wasn't discovered using DHCP option 252.
Download Failed	File didn't download.
Expired	File is expired.

Verify the PAC File Contents

You can check the contents of the PAC file on your 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**.

Zero Touch Onboarding Connection Fails During Initial Setup or After Reset

Symptom:

The system fails to connect to the Zero Touch Onboarding (ZTO) service during initial setup or after a system reset.

Problem:

The system can't communicate with the ZTO service because of a firewall and/or web proxy setting.

Workaround:

Configure your firewall and/or web proxy so that the system can communicate with the ZTO service (`zto.poly.com`) on port 443.