ADMINISTRATOR GUIDE

3.5.0 | June 2021 | 3725-86561-009A

Poly Partner Mode (G7500, Studio X50, and Studio X30)

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

© 2021 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.

PLANTRONICS + POLYCOM. NOW TOGETHER AS poly

Contents

Before You Begin.....6

Audience, Purpose, and Required Skills.....6
Related Poly and Partner Resources.....6

Getting Started..... 8

Poly Partner Mode Overview..... 8
Product Overview of Poly Video Systems.....8
Administrator Features and Capabilities..... 10
Powering the System On and Off.....10
Navigating the System..... 10
Access the System Web Interface.....10

Setting Up the System..... 11

Overview of Poly G7500, Studio X50, and Studio X30 Hardware.....11
Poly G7500 System Ports.....11
Poly Studio X50 System Ports..... 12
Poly Studio X30 System Ports..... 13
LED Status Indicators..... 14
LED Status Indicators for the G7500 System.....14
LED Status Indicators for the Studio X50 and Studio X30 Systems..... 15
Completing Initial System Setup..... 16
Registering the System with Poly Lens.....17
Complete Setup with the System Web Interface.....17
Complete Setup with Provisioning.....18
Managing Peripheral Devices..... 18
Pairing IP Devices on the Link-Local Network (LLN)..... 18
Pairing IP Devices on the Local Area Network (LAN)..... 19
Unpair an IP Device..... 21
Connect a USB Device.....21
Poly Bluetooth Remote Control.....21
IP Microphones..... 23
Poly Microphone IP Adapter.....25

Configuring General Settings..... 28

Name the System and Room.....28
Provide Contact Information.....28
Set the Date and Time..... 29

Set the System Location..... 30
Set the Local Interface Language..... 30
Configure Sleep Settings..... 30
Configure Out of Office Settings..... 31
Change Studio X50 and Studio X30 LED Bar Brightness..... 31
Disable Poly Device Mode..... 31
System Usage Data Collected by Poly..... 32
Send Usage Data to Polycom..... 32

Using a Provisioning Service..... 33
Register the System with RealPresence Resource Manager Provisioning Service..... 34
Download a Provisioning Template Configuration File..... 35
Register the System with the Poly Lens Provisioning Service..... 35
Register the System Using DHCP Auto Discovery..... 36

Configuring Network Settings..... 37
Configuring Wired LAN Settings..... 37
Automatically Obtain IPv4 Address Settings..... 37
Manually Configure IPv4 Address Settings..... 37
Automatically Obtain IPv6 Address Settings..... 38
Manually Configure IPv6 Address Settings..... 38
Manually Assign a Host Name and Domain Name..... 39
Manually Configure DNS Settings..... 39
Configure System VLAN Settings..... 39
Configure System 802.1X Settings..... 40
Configure Wired LAN Options..... 41
LLDP and LLDP-MED Support..... 42
LLMP-MED Information Discovery..... 42
Behavior When LLDP is Enabled..... 42
Enable LLDP 43
Configure Wi-Fi as the Primary Network..... 43

Securing the System..... 46
Managing System Access..... 46
Local Accounts..... 46
Configure System Access Settings..... 49
Configure the System Web Interface Port Lock..... 50
Disable USB Ports..... 50
Detecting Intrusions..... 51
PKI Certificates..... 51

Create a Certificate Signing Request....52
Create a TC8 Certificate Signing Request....53
Configure Certificate Validation Options....55
Install a Certificate....55
View a Certificate....56
View a TC8 Certificate....56
Delete a Certificate....56
Certificate Revocation....57
Disable the Polycom Content App Port....58
System Allow List....58
Add IP Addresses to the Allow List....58
Delete IP Addresses from the Allow List....59
IPv4 Address Formats....59
IPv6 Address Formats....59
Call Encryption....59
Set Up a Security Banner....59
Web Proxies....60
Sample PAC File....62
View Connections to the System....63
System Port Usage....63

Configuring Audio Settings....66

Configure General Audio Settings....66
Audio Input....67
Configure IP Microphones....68
Polycom Acoustic Fence....68
Live Microphone Switching on Studio X50....70
Configure HDMI Audio Input....71
Configure 3.5 mm Audio Input....71
Using Poly Trio Microphones....72
Configuring the Microphone Adapter....73
Audio Output....73
Configure Audio Output Settings....73
Using Poly Trio Speakers....74
Configure 3.5 mm Audio Output....75
USB Audio....75
Using USB and Bluetooth Headsets....75
Using the Shure IntelliMix P300....75
Using the EagleEye Cube USB Camera Microphone....76
Enable USB Audio....76

Configuring Video and Camera Settings.....77
HDMI I/O.....77
Supported HDCI Input Resolutions.....79
Configure Monitor Settings.....79
Configure a Touch Monitor.....80
Monitors with CEC.....80
Disable CEC.....81
Enable CEC.....81
Configure General Camera Settings.....81
Reset Camera Settings to Defaults.....82
Calibrate EagleEye Producer Group Framing.....82
Supported USB Cameras.....83
Selecting the Primary Camera.....83
Camera Priority.....83
Maximum Number of Supported Camera Connections.....84
Configuring Video Input Settings.....84
Configure General Video Input Settings.....84
Adjust the White Balance.....86
Configure Camera Tracking Settings for Studio X50 or Studio X30.....86
Configure Camera Tracking Settings for G7500.....87
Presenter Mode.....88

Sharing Content.....89
Default Option for Sharing Content.....89

Customizing the Local Interface.....90
Configure Dual Monitor Display Settings.....90

System Maintenance.....91
Unlock System Settings.....91
Updating Software.....91
Updating Paired Devices.....92
Updating Software in the G7500 System Web Interface.....92
Update System Software from a USB Flash Drive.....95
Update Poly HDCI Cameras.....96
Downgrading Software.....96
Manually Downgrade Software in the System Web Interface.....97
Downgrade Software with a USB Flash Drive.....97
Restart the System.....97

Change the Conferencing Partner Application....98
Set the Conferencing Provider to Device Mode....98
Reset System Settings....98
Factory Restore the System....99
Factory Restore a Table Microphone....100
Factory Restore a Ceiling Microphone....100
Factory Restore a Microphone Adapter....102

Troubleshooting....103

Logs....103
Consolidated System and Peripheral Device Logs....103
Configure Log Preferences....104
Configure Log Level....105
Retrieve Log Files....106
Transfer Logs to a USB Flash Drive....106
Configure Remote Logging....106
Configure Logging to System Internal Storage....108
Sample Log File....108
SNMP Reporting....109
Configure SNMP....110
Download MIBs....112
Checking System Status....112
Check Status in Local Interface....112
Check Provisioning Results....113
Paired IP Devices....114
Audio Tests....114
LED Status Indicators for the System LAN Ports....115
Fix Polycom Acoustic Fence Issues with G7500....116
Test Connection with Another System....116
Run a Trace Route....116
Checking the Web Proxy Configuration....117
Verify Poly Lens Registration Status....117
Poly Trio Audio Meter Not Displaying in System Web Interface....118
A Portion of the EagleEye Cube USB Camera Name Is Cut Off....118
Monitor Loses Signal After Monitor Swap....118

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
- OpenSIP networks and VoIP endpoint environments

Related Poly and Partner Resources

See the following sites for information related to this product.

- The Poly Online Support Center is the entry point to online product, service, and solution support information including Video Tutorials, Documents & Software, Knowledge Base, Community Discussions, Poly University, and additional services.
- The Poly 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 Poly 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 Poly Partner Network is a program where resellers, distributors, solutions providers, and unified communications providers deliver high-value business solutions that meet critical customer needs, making it easy for you to communicate face-to-face using the applications and devices you use every day.
- The Poly 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 Rooms**: https://support.zoom.us/hc/en-us
- **Microsoft Teams Rooms**: https://support.office.com/en-us/teams
  - For network preparation information, see Prepare your environment for Microsoft Teams Rooms
  - For account configuration information, see Configure Accounts for Microsoft Teams Rooms
- **GoToRoom by LogMeIn**: https://support.goto.com/products
- **StarLeaf**: https://support.starleaf.com/
- **RingCentral Rooms (RCV Rooms)**: https://support.ringcentral.com/
- **Dialpad**: https://help.dialpad.com/

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.

Note: Exact features and capabilities can vary between partner applications. See the application's documentation for information.

Poly G7500 System Features and Capabilities

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 the paired camera and system configuration)
- Poly NoiseBlockAI, which eliminates background and extraneous sound during calls in common working environments
- Polycom Acoustic Fence technology, which enables video conferencing in open workspaces by capturing only the voices in a defined area
- HDMI: Single input and dual output
- Using a wired or wireless USB mouse as an input device

Poly Studio X50 Features and Capabilities

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
- Hi-fidelity, built-in stereo microphones that pick up sound within 7.62 m (25 ft) and use spatial audio for life-like presence and clarity
- Poly NoiseBlockAI, which eliminates background and extraneous sound during calls in common working environments
- Dual stereo speakers
- HDMI: Single input and dual output
- Using a wired or wireless USB mouse as an input device

Poly Studio X30 Features and Capabilities

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 4.57 m (15 ft) and use spatial audio for life-like presence and clarity
- Poly NoiseBlockAI, which eliminates background and extraneous sound during calls in common working environments
- Single mono speaker
- HDMI: Single input and output
- Using a wired or wireless USB mouse as an input device

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 97

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 username (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 17

Setting Up the System

Topics:

- Overview of Poly G7500, Studio X50, and Studio X30 Hardware
- LED Status Indicators
- Completing Initial System Setup
- Managing Peripheral Devices

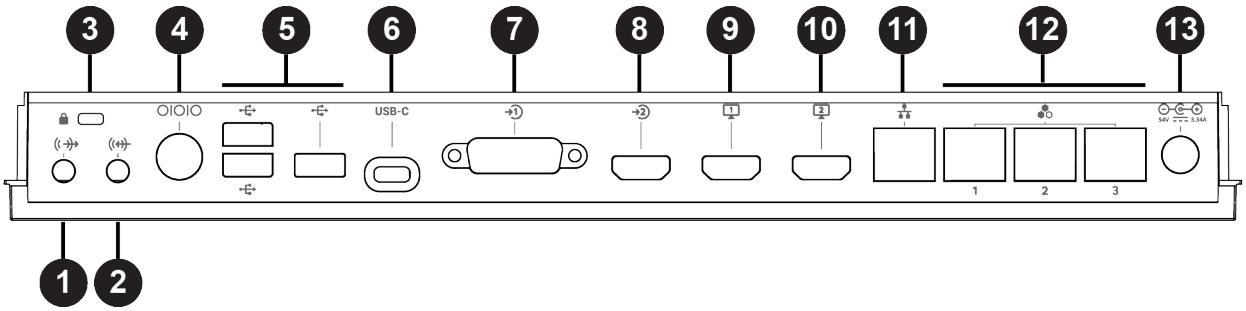
See the setup sheets applicable to your video system and its peripheral devices, including cameras, monitors, microphones, and controllers.

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

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

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
5	USB 3.0 port (host)
6	USB-C port
7	HDCI input for Polycom cameras

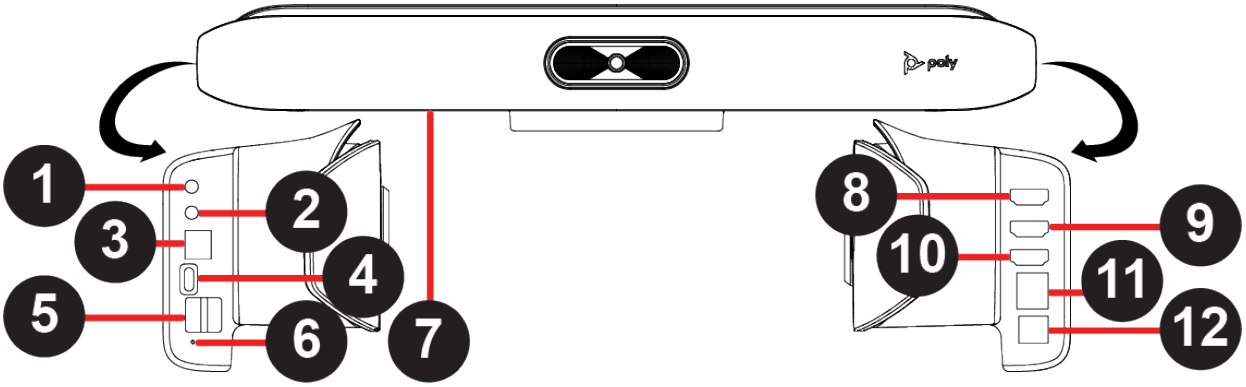
Ref. Number	Port Description
8	HDMI input for sharing content (for example, from a laptop)
9	HDMI output for the primary monitor
10	HDMI output for the secondary monitor
11	LAN connection for the system
12	Link-local network (LLN) connections for IP-based peripheral devices
13	Power cord port

Related Links

Specify the Primary and Fence Microphones on page 69
LED Status Indicators for the System LAN Ports on page 115

Poly Studio X50 System Ports

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



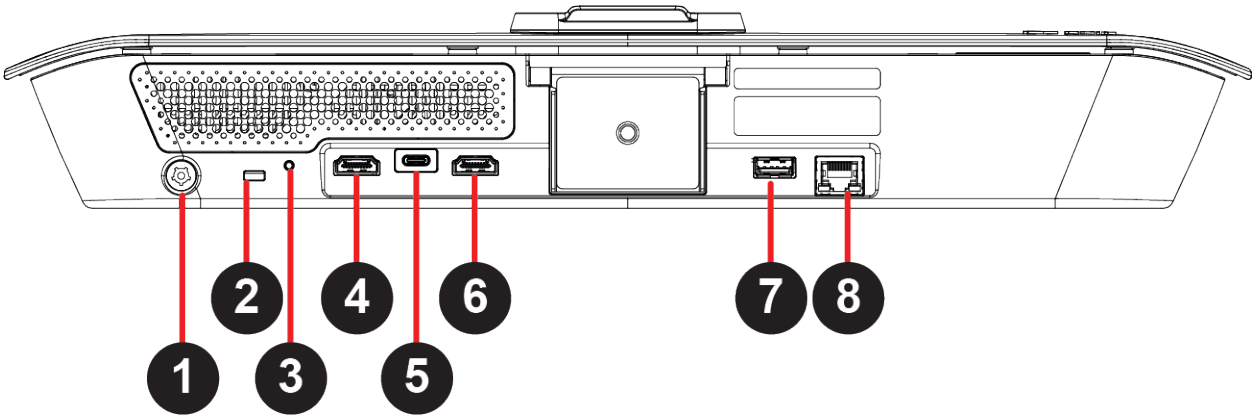
Poly Studio X50 System Port Descriptions

Ref. Number	Port Description
1	3.5 mm audio line in
2	3.5 mm audio line out
3	Polycom RealPresence Debut expansion microphone connection
4	USB-C port
5	USB ports
6	Factory restore pinhole
7	Security lock (on the back flat section of the system)
8	HDMI output for the secondary monitor

Ref. Number	Port Description
9	HDMI output for the primary monitor
10	HDMI input for sharing content (for example, from a laptop)
11	LAN connection for the system
12	Power cord port

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 cord port
2	Security lock
3	Factory restore pinhole
4	HDMI output for the primary monitor
5	USB-C port
6	HDMI input for sharing content (for example, from a laptop)
7	USB port
8	LAN connection for the system

LED Status Indicators

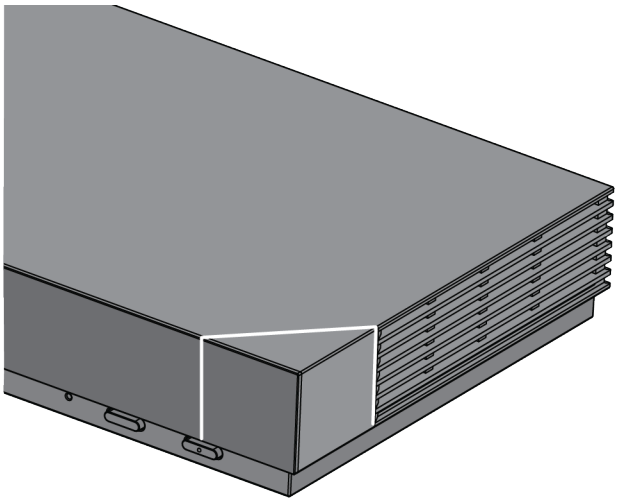
The following figures display the LEDs on your systems. The tables list each LED indicator and its associated status.

Related Links

Factory Restore the System on page 99

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
Solid green	In a call
Blinking amber	Update in progress
Solid amber	Sleeping
Blinking red	Error preventing normal operation
Solid red	Muted microphone

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
Solid white	All	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	All	Outgoing call
Solid green	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 in the following cases: ▪ Tracking people in group framing and speaker tracking mode ▪ Indicating the direction of the camera that you customize in pan-tilt-zoom (PTZ) mode
Solid amber	Twelve in the middle	Standing by The system is in sleep mode with no active video output.
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
Solid red	Four in the middle	Muted camera. The muted microphone LEDs take precedence and cover the camera mute LEDs.
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.

Indicator	Position	Status
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 Mode or Partner Mode.

Note the following requirements:

- 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, web proxy, or both so that the system can communicate with the following services on port 443:
  - ZTO (`zto.poly.com`)
  - Poly Lens (`lens.poly.com`)
  - Software download site (`downloads.polycom.com`)
- 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.

If the system isn't connected to a valid network at startup, it prompts you to connect to Ethernet or configure Wi-Fi.

Note: Only Zoom Rooms and Microsoft Teams support a Wi-Fi connection as the primary network. If you change to an unsupported conferencing application, a message displays indicating you must connect to the Ethernet.

After initial network setup, the system boots directly into a conferencing application. If the ZTO specified conferencing application isn't available in the current software, the system performs a software update. If the specified conferencing application isn't available after the update, the system defaults to Poly Video Mode. To change the conferencing application, go to the system web interface **Provider** section and select an option.

Required Steps Following Initial System Setup

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).

Registering the System with Poly Lens

Poly Lens provides cloud-based management and insights for your system.

You can register your system with Poly Lens during system setup or on the Poly Lens registration page. For more information, see Poly Lens Help.

Register During System Setup

You can register with Poly Lens during system setup.

Procedure

1. When prompted to register with Poly Lens, do one of the following:
   - Scan the registration QR code with your mobile device.
   - Enter the registration URL in a browser.
   - Select the registration link in the system web interface.
2. Follow the instructions to finish registering your system.

Your system remains registered with Poly Lens even after a reset or factory restore.

Related Links

Register Later on page 17
Verify Poly Lens Registration Status on page 117

Register Later

If you don’t register during setup, you can do so on the Poly Lens registration page.

Procedure

1. Go to https://lens.poly.com/go.
2. Follow the instructions to register your system.

Related Links

Register During System Setup on page 17
Verify Poly Lens Registration Status on page 117

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 (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 10
Create Local Administrator Credentials on page 47
Set the System Location on page 30
Set the Date and Time on page 29

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 *Poly VideoOS Parameter Reference Guide* on the Poly 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 RealPresence Resource Manager Provisioning Service on page 34
Download a Provisioning Template Configuration File on page 35

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 (LLN)

IP devices automatically pair with your 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 a system LLN port. For example, when you plug in a Polycom 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.

Pairing IP Devices on the Local Area Network (LAN)

Supported IP devices can pair to your video system over your primary local area network (LAN).

Pairing a Poly Trio

You can use a Poly Trio system as a controller and audio device with a Poly Studio X50, Studio X30, or G7500 video system. See your system's latest *Release Notes* for supported Poly Trio models.

Zoom Rooms is the only third-party conferencing application supported in this setup.

You pair the phone as an IP device over your primary network. When paired, from the video system web interface you can configure audio to play from the phone speakers, Studio X50 or Studio X30 system speakers, or monitors connected to the video system. The Poly Trio microphones are always on.

Related Links

Using Poly Trio Microphones on page 72
Choose Speakers When Paired with Poly Trio on page 74
Updating a Paired Poly Trio on page 92

Configure a Poly Trio for Pairing

To pair with a video system, you must configure your Poly Trio system's base profile and device role.

Procedure

1. On the phone's local interface, go to **Settings** > **Advanced** > **Administration Settings** > **Network Configuration**.
2. Set the **Base Profile** to **Generic**.
3. After the phone restarts, go to **Settings** > **Advanced** > **Networked Devices**.
4. Set **Networked Device Role** to **Device**.

   The system automatically restarts.

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 TC 8 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 components must be unblocked:

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

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

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).

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

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**.
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, the configuration of your device, and the 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.

Procedure

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

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

Related Links

Move a Microphone Adapter to Another Location on page 27

Connect a USB Device

You can use some devices, such as a Windows or Mac laptop, with a USB connection to your video system. See the latest *Release Notes* for supported USB devices.

Procedure

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

Poly Bluetooth Remote Control

You can use the Poly Bluetooth Remote Control with your system.

Use the system web interface to perform the following tasks:

- Configure a remote control's button behavior.
- Pair and unpair a remote control.

  Note: The remote control included with your G7500 system purchase is paired and ready to use without any extra setup.
- View the remote control name, pairing status, and battery level.

Configure Remote Control Behavior

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

Procedure

1. In the system web interface, go to **General Settings** > **System Settings**.

2. Configure the following settings:

Setting	Description
Keypad Audio Confirmation	Specifies whether to play a voice confirmation of numbers selected with the remote control or keypad.
Numeric Keypad Function While In a Call	Specifies whether pressing number buttons on the remote control or keypad moves the camera to presets or generates touch tones (DTMF tones). If you set this option to **Presets**, you can generate DTMF tones by pressing the # key on the remote control while in a call.
#/@ Button function	Specifies the behavior of the **#** button on the remote control. ▪ **#, then @**: Pressing the # button once displays the hash symbol. Pressing the # button twice quickly displays the @ symbol. ▪ **@, then #**: Pressing the # button once displays the @ symbol. Pressing the # button twice quickly displays the # symbol.
*/. Button function	Specifies the behavior of the ***** button on the remote control: ▪ *** then .**: Pressing the * button once displays the * symbol. Pressing the * button twice quickly displays a period. ▪ **. then ***: Pressing the * button once displays a period. Pressing the * button twice quickly displays the * symbol.

3. Select **Save**.

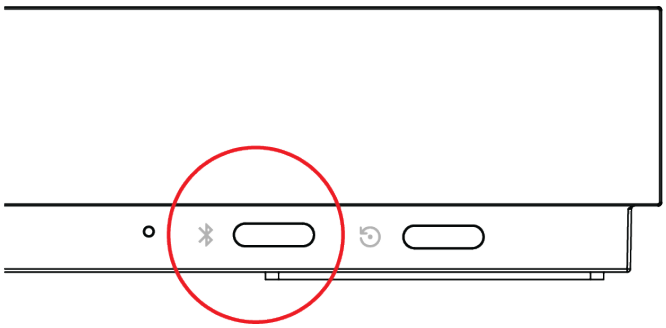
Pair a Remote Control

In most cases, you must pair the remote control after setting up your system. To use a different remote control, you must pair it with the system.

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

Procedure

1. Depending on your system, do one of the following:
   - (All systems) In the system web interface, go to **General Settings** > **Remote Control** and select **Start Discovery Mode**.
   - (G7500 systems only) On the front of the system, press the **Bluetooth** button.



2. On your remote control, press **Mute** for seven seconds.

   In Poly Video Mode, the screen displays either a successful or unsuccessful pairing notification. In Partner Mode, the blue LED indicator stops blinking blue and returns to white.
3. Depending on the pairing result, do one of the following:
   - **Successful pairing**: The remote control is ready to use. You can view the remote control name, battery level, and status of the device in the system web interface.
   - **Unsuccessful pairing**: Try the following solutions:
     - Remove the batteries from the remote control and reinsert after 5 seconds.
     - Move your remote control closer to the system than other remote controls and try to pair again.

Unpair a Remote Control

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

Procedure

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

   The remote control unpairs.

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:

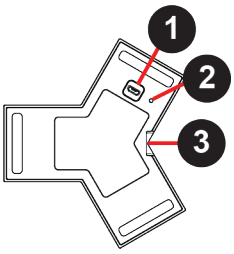
- Poly IP Table Microphone
- Poly IP Ceiling Microphone

Related Links

Polycom Acoustic Fence on page 68
Factory Restore a Table Microphone on page 100

Poly IP Table Microphone Ports

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

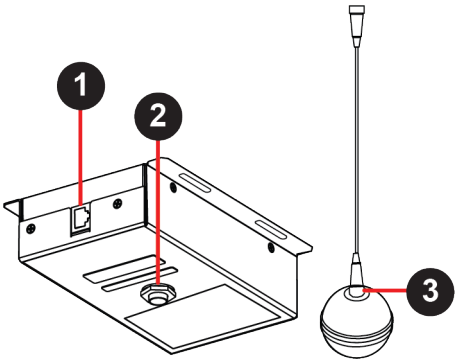


Poly IP Table Microphone Port Descriptions

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.

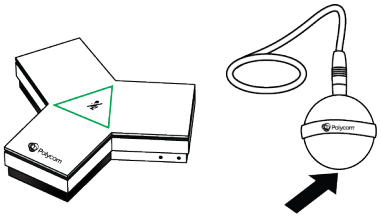


Poly IP Table Microphone Port Descriptions

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
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.
LED is off	Out of a call and microphone not muted
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.

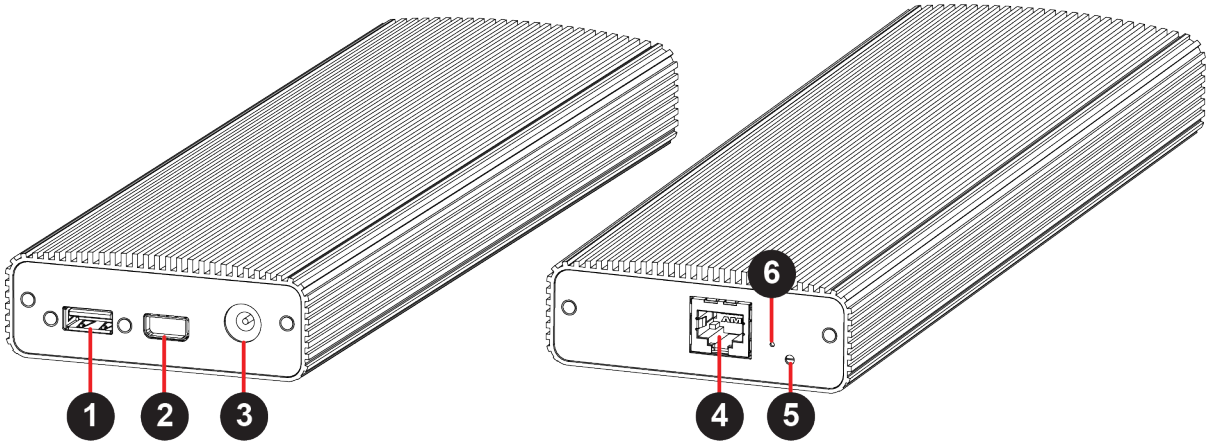
Note: You can't use the microphone adapter with IP microphones connected to your system.

Related Links

Factory Restore a Microphone Adapter on page 102
Configuring the Microphone Adapter on page 73

Microphone Adapter Ports

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

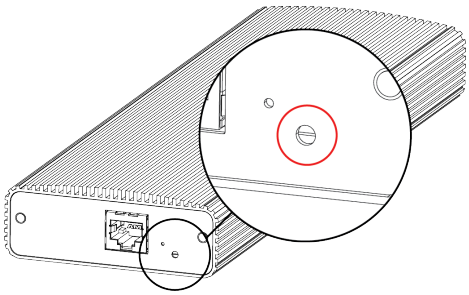


Microphone Adapter Port Descriptions

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

Indicator	Status
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 21

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
- Configure Out of Office Settings
- Change Studio X50 and Studio X30 LED Bar Brightness
- Disable Poly Device Mode
- System Usage Data Collected by Poly

General settings include your system name, location, and language 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. Edit the **Device Name**, **Room Name**, or both.

   The system supports double-byte characters. The **Device Name** field accepts all alphanumeric and special character formats (including foreign language characters) and has a maximum limit of 40 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 17

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 17

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. Configure the following settings:

Setting	Description
Display	Choose if the system displays a black screen or a no signal message.
Time Before System Goes to Sleep	▪ Select how long the device can be idle before it goes to sleep. ▪ Select **Off** to disable system sleep mode.

Setting	Description
Enable Mic Mute in Sleep Mode	Select the check box to mute your microphones while the system is asleep.

3. Select **Save**.

Configure Out of Office Settings

Configure when your system goes to sleep after normal office hours. The system goes to sleep 3 minutes after out of office hours begin.

Putting the system to sleep prevents screen burn-in and excess power consumption.

Procedure

1. In the system web interface, go to **General Settings** > **System Settings**.
2. Select the **Out of Office Hours** check box and configure the following settings:

Setting	Description
Start Time	When out of office hours begin
End Time	When out of office hours end

3. Select **Save**.

Change Studio X50 and Studio X30 LED Bar Brightness

If you’re sitting close to the system and monitor, bright LEDs can affect the video white balance, causing odd coloration of the video output.

To correct issues such as this, adjust your system's LED bar brightness.

Procedure

1. In the system web interface, go to **General Settings** > **System Settings**.
2. Slide the **LED Bar Brightness** slider to the left to lower the brightness and to the right to increase the brightness.
3. Select **Save**.

Disable Poly Device Mode

Disable Device Mode to stop the system from being used as an external camera, microphone, and speaker for a USB-connected laptop.

Disabling Device Mode requires a system restart.

Procedure

1. In the system web interface, go to **General Settings** > **System Settings** > **Collaboration Tools**.
2. Clear the **Enable Device Mode** check box and select **Save**.

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*.

Send Usage Data to Polycom

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

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

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

Procedure

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

Using a Provisioning Service

Topics:

- Register the System with RealPresence Resource Manager Provisioning Service
- Download a Provisioning Template Configuration File
- Register the System with the Poly Lens Provisioning Service
- Register the System Using DHCP Auto Discovery

Provisioning services, such as Poly Lens or Polycom RealPresence Resource Manager, enable you to deploy enterprise-wide configurations to your systems.

You can use a provisioning service to perform the following actions with your system and some of its paired devices:

- 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.
- The system looks for provisioning options during initial system setup in the following order: Zero Touch Onboarding, Poly Lens, then DHCP. If the system doesn’t find provisioning information for an option, it automatically goes to the next one.

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* on the Poly Documentation Library.

Related Links

Updating Software on page 91
PKI Certificates on page 51
Choose How to Get Software Updates on page 93

Register the System with RealPresence Resource Manager 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
Authentication Type	The type of authentication the system uses to connect to the provisioning server.
Server Address	Address of the system running the provisioning service. The format is `https://<server>/ucservice`. For example, `https://video.myrpp.poly.com/ucservice`.
Domain Name	Domain for registering with the provisioning service. This option doesn't display if you select **Basic** as the authentication type.
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 113
Complete Setup with Provisioning on page 18
Downgrading Software on page 96

Download a Provisioning 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.

Related Links

Complete Setup with Provisioning on page 18

Register the System with the Poly Lens Provisioning Service

Provision your system with Poly Lens to easily configure and manage your systems.

For information on how to provision your system with Poly Lens, see the *Poly Lens Help Documentation*.

Procedure

1. In the system web interface, go to **Servers** > **Provisioning Server**.
2. Select **Enable Provisioning**.
3. In the **Authentication Type** field, select **Basic**.
4. Optional: If your system didn't detect a provisioning server, complete the following fields (contact your network administrator for help):

Setting	Description
Server Address	Address of the system running 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 113

Register the System Using DHCP Auto Discovery

You can use DHCP to automatically register your system to a provisioning service before initial system setup or after a system reset.

The system looks for option number 160 and 66 (in that order) in the response received from the DHCP server. The DHCP server should send address information that matches one of the address formats.

Procedure

- **»** Configure your DHCP server to send the username, password, and URL of your provisioning service in the following format:
  - For Polycom RealPresence Resource Manager use `https://<shareduserID>:<sharedpassword>@<server>/ucservice`

    For example, `https://mySharedID:mySharedPW@video.example.com/ucservice`
  - For Poly Lens use `https://<ServerUser>:<ServerPassword>@<ServerAddressURL>`

    For example, `https://ServerUser:ServerPassword@yourprovisioningsubdomain.lens.poly.com`

Configuring Network Settings

Topics:

- Configuring Wired LAN Settings
- LLDP and LLDP-MED Support
- Configure Wi-Fi as the Primary Network

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

Configuring Wired LAN Settings

You can set the wired LAN properties for your system.

Related Links

LED Status Indicators for the System LAN Ports on page 115

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** > **LAN 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** > **LAN 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.

Setting	Description
Default Gateway	Specifies the default gateway assigned to your system.

4. Select **Save**.

Automatically Obtain IPv6 Address Settings

You can enable your system to use IPv6 addresses and get IP address information automatically.

You must have a DHCP server deployed in your environment.

Warning: If your network environment only supports IPv6, you must manually configure a static IPv4 address. For example, manually configure the IPv4 IP address to 192.168.0.4.

Procedure

1. In the system web interface, go to **Network** > **LAN Network** > **IP Addresses**.
2. Select the **Enable IPV6** checkbox.
3. For **IP Address**, select **Obtain IP address automatically**.
4. Optional: Select the **Enable SLAAC** checkbox to enable the system to use stateless address autoconfiguration (SLAAC) to automatically obtain IP address.

Manually Configure IPv6 Address Settings

You can manually configure the system's IPv6 address settings.

Warning: If your network environment only supports IPv6, you must manually configure a static IPv4 address. For example, manually configure the IPv4 IP address to 192.168.0.4.

Procedure

1. In the system web interface, go to **Network** > **LAN Network** > **IP Addresses**.
2. Select the **Enable IPV6** checkbox.
3. For **IP Address**, select **Enter IP address manually**.
4. Configure the following settings:

Setting	Description
Link-Local	Specifies the IPv6 address to use for local communication within the subnet.
Site-Local	Specifies the IPv6 address to use for communication within the site or organization.
Global Address	Specifies the IPv6 internet address.
Default Gateway	Specifies the default gateway assigned to your system.

5. 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. In the system web interface, go to **Network** > **LAN Network** > **LAN Options**.
2. 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-xxxxxx`, where `xxxxxx` 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).
3. Optional: Enter or modify the **Domain Name** that the system belongs to.
4. 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 System VLAN Settings

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

Note: VLAN isn't supported in IPv6 environments.

Procedure

1. In the system web interface, go to **Network** > **LAN Network** > **LAN Options**.
2. Optional: Select the **Enable LLDP** check box so that the system can advertise itself on the network using Link Layer Discovery Protocol (LLDP).

   If you enable LLDP and then enter a VLAN ID, the VLAN ID you enter supersedes the auto-discovered VLAN ID from LLDP.
3. Select the **802.1p/Q** check box 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**.

Related Links

LLDP and LLDP-MED Support on page 42

Configure System 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.

Note: 802.1X isn't supported in IPv6 environments.

The system supports the following authentication protocols:

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

Procedure

1. In the system web interface, go to **Network** > **LAN Network** > **LAN Options**.
2. Select the **Enable EAP/802.1X** check box.
3. Select an EAP/802.1X authentication method.
4. Optional: For EAP-TTLS or EAP-PEAPv0, choose an **EAP/802.1X Phase 2 Authentication**.
5. Enter an **EAP/802.1X Identity** for your system.

   You can't leave this field blank.
6. Enter an **EAP/802.1X Password** for your system.

   This setting is required when you use EAP-MD5, EAP-PEAPv0, or EAP-TTLS.
7. Select **Save**.

Related Links

PKI Certificates on page 51

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** > **LAN 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.
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 `Destination Unreachable` message if the system can’t deliver a packet to its destination for reasons other than network congestion.

Setting	Description
Respond to Broadcast and Multicast Echo Requests	When enabled, your system sends an ICMP `Echo Reply` message in response to a broadcast or multicast Echo Request that isn't specifically addressed to the system.

3. Select **Save**.

LLDP and LLDP-MED Support

Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) are supported on your systems. LLDP is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices to advertise their identity and capabilities on an IEEE 802 local area network (LAN). This protocol runs over the data-link layer only, allowing connected systems running different network layer protocols to discover information about each other. LLDP-MED is an extension of LLDP.

Examples of applications that use information discovered by LLDP include:

- Network topology - A network management system (NMS) can accurately represent a map of the network topology.
- Inventory - A management system can query a switch to learn about all the devices connected to that switch. The LLDP protocol is formally specified in standards document IEEE 802.1AB.

Related Links

Configure System VLAN Settings on page 39

LLMP-MED Information Discovery

LLDP-MED enables the following information discovery for your systems:

- Auto discovery of LAN policies enabling plug and play networking
- Inventory management, which allows network administrators to track their network devices.

Behavior When LLDP is Enabled

When LLDP is enabled on a system, it discovers VLANs advertised by the network switch and automatically configures the system for one of the VLANs. If the room system discovers any of the following VLAN types in LLDP data from the network switch, the system automatically configures itself for one of them. The chosen VLAN type is based on the order of precedence, as follows:

- Video Conferencing VLAN
- Voice VLAN
- Voice Signaling VLAN

If none of the above VLAN types are found, the room system configures itself for the default or native LAN of the switch port to which it is connected.

LLDP packets are transmitted regularly so that the network switch (and the neighboring endpoints) are aware of the system presence on the network.

Enable LLDP

Enable Link Layer Discovery Protocol (LLDP) to automatically configure your system to a VLAN with data received from your network switch.

Procedure

1. In the system web interface, go to **Network** > **LAN Network** > **LAN Options**.
2. Select the **Enable LLDP** check box so that the system can advertise itself on the network using LLDP.

   If you enable LLDP and then enter a VLAN ID, the VLAN ID you enter supersedes the autodiscovered VLAN ID from LLDP.
3. Select **Save**.

Configure Wi-Fi as the Primary Network

You can configure Wi-Fi as your primary network if you're using Zoom Rooms or Microsoft Teams Rooms as your conferencing provider. You must use WEP, WPA, or WPA2 Wi-Fi protocols on the 2.4 GHz and 5 GHz spectrums.

Note: The quality of your calls is dependent on the quality of your Wi-Fi signal.

The system doesn't support Wi-Fi as a primary network for the following conferencing providers or modes:

- Poly Video Mode
- GoToRoom
- StarLeaf
- RingCentral Rooms
- Dialpad

The system doesn't support the following options if you configure Wi-Fi as your primary network:

- Web proxy
- Provisioning
- 802.1x authentication

Note: You can pair a TC8 to a system that's using Wi-Fi as the primary network. To pair a TC8 over Wi-Fi, the TC8 must be on the same subnet as the video system.

Procedure

1. In the system web interface, go to **Network** > **Wi-Fi Network**.
2. From the **Choose Network Type** drop-down menu, select **Wi-Fi**.
3. Do one of the following:
   - Select a network from **Available Wi-Fi Networks**. (The system lists networks in order of signal strength.)
   - Enter the network name in the **SSID** field.

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

4. Configure the following settings:

Note: Available settings vary with your selections.

Setting	Description
Security	Specifies the encryption protocol: ▪ None ▪ WEP ▪ WPA/WPA2-PSK ▪ 802.1x EAP **Note:** Although 802.1x EAP is listed in the drop-down menu, it isn't supported when using Wi-Fi as the primary network.
Key (Passphrase/PSK)	Specifies an encryption passphrase (like a password) for the Wi-Fi network. You must enter the passphrase to connect to the Wi-Fi network.
IP Address	▪ To set your system Wi-Fi network IP address, select **Obtain IP address automatically**. (You must have a DHCP server in your environment to use this option.) ▪ To enter a specific Wi-Fi network IP address, select **Enter IP address manually**.
Your IP Address is	Specifies the IP address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
Subnet Mask	Specifies the subnet mask address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
Default Gateway	Specifies the IP gateway for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
DNS Server	Specifies the DNS server address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.

Setting	Description
DNS Alternate Server	Specifies the alternate DNS server address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.

5. Select **Connect**.

If you’re using Microsoft Team Rooms as a provider, reboot the system.

Securing the System

Topics:

- Managing System Access
- Detecting Intrusions
- PKI Certificates
- Disable the Polycom Content App Port
- System Allow List
- Call Encryption
- Set Up a Security Banner
- 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 109

Managing System Access

You can control how users and administrators access the system.

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. Administrators set password policies and minimum requirements.

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:

Note: You must configure the **Admin Room** and **Remote Access** password settings separately.

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

3. Select **Save**.

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

Create Local Administrator Credentials

You can require local administrator credentials for in-room and remote access to the 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 `admin`).
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 17

Configure Account Lockout Settings

Account lockout controls 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	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. 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.

Configure System Access Settings

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.
Enable Diagnostics Port Idle Session Timeout	Specifies whether to allow the diagnostics port to time out and close the active session at the configured time interval of no activity or not. You set the timeout at **Idle Session Timeout in Minutes**.
Enable API Port Idle Session Timeout	Specifies whether to allow the API port to time out and close the active session at the configured time interval of no activity or not. You set the timeout at **Idle Session Timeout in Minutes**.
Enable SNMP Access	Specifies whether to allow SNMP access.
Idle Session Timeout in Minutes	Specifies the number of minutes a session can be idle before it times out.
Maximum Number of Active Sessions	Specifies the maximum number of users logged in through the system web interface or command-line API (SSH or telnet).
Max Session Timeout in Minutes	Specifies the maximum number of minutes a session can be open before it times out, regardless of session activity.

Setting	Description
Minimum TLS Version	Specifies the system minimum TLS version. You can restrict your system from using earlier versions of TLS for secure communications. For example, if you set your minimum TLS version to 1.1, you're disabling TLS 1.0.

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 completely turn off the USB-C port; it still provides power.

If you disable the system's USB ports, you can't use the system as an external camera, microphone, and speaker accessory (i.e., Poly Device Mode).

Procedure

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

Detecting Intrusions

When the system detects a possible network intrusion, it logs an entry to the security log.

The Enable Network Intrusion Detection System (NIDS) setting controls the logging behavior. The security log prefix identifies the type of packet detected, as shown in the following table:

Prefix	Packet Type
SECURITY: NIDS/unknown_tcp	Packet that attempts to connect or probe a closed TCP port
SECURITY: NIDS/unknown_udp	Packet that probes a closed UDP port
SECURITY: NIDS/invalid_tcp	TCP packet in an invalid state
SECURITY: NIDS/invalid_icmp	ICMP or ICMPv6 packet in an invalid state
SECURITY: NIDS/unknown	Packet with an unknown protocol number in the IP header
SECURITY: NIDS/flood	Stream of ICMP or ICMPv6 ping requests or TCP connections to an opened TCP port

Following the message prefix, the security log entry includes the time stamp and the IP, TCP, UDP, ICMP, or ICMPv6 headers. For example, the following security log entry shows an `unknown_udp` intrusion:

```
2009-05-08 21:32:52 WARNING kernel: SECURITY: NIDS/unknown_udp IN=eth0
OUT= MAC=00:e0:db:08:9a:ff:00:19:aa:da:11:c3:08:00 SRC=172.18.1.80
DST=172.18.1.170 LEN=28 TOS=0x00 PREC=0x00 TTL=63 ID=22458 PROTO=UDP
SPT=1450 DPT=7788 LEN=8
```

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.

Root certificates installed on your system automatically transfer to a paired TC8 device. If you delete root certificates from the system, they're automatically deleted from the TC8. System certificates are unique to each system and don't transfer to paired devices.

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 isn't 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 33
Configure System 802.1X Settings on page 40

Create a Certificate Signing Request

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

Note: Only one CSR can exist at a time. After a CSR is generated, get it signed and installed on your system before creating another. If you generate a CSR and generate a second CSR before you install the first one, the device discards the previous one.

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. This is a required field. Maximum characters: 64 (truncated if necessary). Poly recommends the following guidelines for this field: ▪ For systems registered in DNS, use the system's FQDN. ▪ For systems not registered in DNS, use the system's IP address.

CSR Information	Description
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. You can't change this setting 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, `UserName@YourDomain.com`). This is the `userPrincipalName` 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.

Create a TC8 Certificate Signing Request

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

Only one CSR can exist on your device at a time. After you generate a CSR, get it signed and install it on your device before generating another. If you generate a second CSR before you install the first one, the device discards the previous CSR.

Procedure

1. In the system web interface, go to **Security** > **Certificates**.
2. Select **Poly TC8** > **Create and Download 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. This is a required field. Maximum characters: 64 (truncated if necessary). Poly recommends the following guidelines for this field: ▪ For systems registered in DNS, use the system's FQDN. ▪ For systems not registered in DNS, use the system's IP address.
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. You can't change this setting 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, `UserName@YourDomain.com`). This is the `userPrincipalName` 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**.

   If the system successfully creates the CSR, it automatically downloads the file.
5. Send the CSR file to a CA, which issues your signed certificate.

Configure Certificate Validation Options

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.

For a full list of preinstalled certificates on your system, see the *Poly VideoOS and TC8 Certificates Update* on the Poly Online Support Center.

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 *peer certificate* 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.
Always Validate Peer Certificates From Browser	Determines whether your system requires a web browser to present a valid certificate when connecting to it. **Note:** If you are using private PKI certificates in your environment and want HTTPS software downloads to work, you must install the trusted root certificate from your internal certificate authority (CA) on the system since certificate validation is always performed.
Disable Preinstalled Certificates	Disables preinstalled root certificate CA chains.

Install a Certificate

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

Note: System certificates must be created on the Poly system and signed by an external CA before installation. Externally created device certificates won't work properly.

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 the **System** tab or **Connected Device** tab.
3. 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` file name 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 web 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.

View a TC8 Certificate

The system lists user-installed TC8 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**.
2. Select the connected device tab.

   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).

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 the following standard method:

- **Certificate Revocation List (CRL)**: File containing a list of certificates revoked by their issuing CA. You must manually upload CRLs to your system.

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.

Disable the Polycom Content App Port

To prevent the Content App from connecting to your system and providing a video and audio content stream, disable the content sharing application in the system web interface.

This option stops TCP/TLS traffic on port 5001.

Procedure

1. In the system web interface, go to **General Settings** > **System Settings**.
2. Clear the **Enable Poly Content App Sharing** check box.
3. Select **Save**.

System Allow List

The allow list enables access to your system web interface and SNMP ports only to IP addresses you specify.

An allow list supports up to 30 addresses (including IPv4 and IPv6 formats) and can only be configured in the system web interface.

Note: If your IP addresses are dynamically assigned, make sure the allow list is updated so those hosts can connect to your system.

Add IP Addresses to the Allow List

You can add and edit specific IP addresses to an allow list for your system.

Warning: Once you save the IP allow list, you can access the system web interface of only those devices on the list. If your current device isn't on the list, you can't access the system web interface for that device. You may have to factory restore the system to regain access.

Procedure

1. In the system web interface, go to **Security** > **Access**.
2. Select **Enable Allow List**, then **Edit Allow List**.
3. Select address type **IPv4** or **IPv6**.
4. In the **IP Address** field, enter the address of the system you want to add to the allow list.
5. Select **Add**.
6. Optional: Repeat steps 4 and 5 for the other IP addresses you want to add to the allow list.
7. Select **Save**.

Delete IP Addresses from the Allow List

You can delete specific IP addresses from the allot list for your system.

Procedure

1. In the system web interface, go to **Security** > **Access**.
2. Select **Edit Allow List**.
3. Select the check box next to any IP address you want to delete and select **Remove**.

IPv4 Address Formats

The configuration requires a single IP address, a range of addresses, or an IP and netmask. (The netmask represents the number of valid bits of the IPv4 address to use.)

The following are valid IPv4 formats for your system:

- 10.12.128.7
- 172.26.16.0/24

IPv6 Address Formats

For IPv6 addresses, you can use a Classless Inter-Domain Routing (CIDR) notation to represent a range of IP addresses.

The following are valid IPv6 formats for your system:

- ::1
- 2001:db8:abc:def:10.242.12.23
- 2001:db8::/48
- 2001:db8:abcd:0012::0/64
- 2001:0db8:85a3:0000:0000:1234:0abc:cdef

Call Encryption

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

Set Up a Security Banner

You can create a security banner, which is a message that displays before users log in to the system remotely.

Procedure

1. In the system web interface, go to **Security** > **Security Banner**.
2. Select **Enable Security Banner**.
3. Configure the following settings and select **Save**.

Setting	Description
Banner Text	▪ **Custom**: Enter any text for the banner. ▪ **DoD**: A default U.S. Department of Defense security banner. You can't change this text.
Remote Access Banner Text	The security banner that displays on the system web interface and command-line API (SSH or telnet). Enter up to 2408 single-byte or 1024 double-byte characters. The text wraps to the next line as you type, but you can press **Enter** anywhere to force a line break.

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.

Configure your system to use a proxy one of the following ways:

- **Automatic**: 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**: Specify the proxy credentials and URL for automatically downloading a PAC file.
- **Manual**: 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 117
Manually Configure a Web Proxy on page 62

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** > **LAN 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** > **LAN 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 User Name** 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** > **LAN Network** > **Web Proxy Settings**.
2. Select **Automatic Configuration**.
3. If checked, clear the **Enable WPAD** check box.
4. Enter the **Proxy User Name** 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** > **LAN Network** > **Web Proxy Settings**.
2. Select **Update PAC File** to fetch the latest version of the file from the server.

Related Links

Manually Configure a Web Proxy on page 62

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** > **LAN 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 User Name** and **Proxy Password**.
5. Select **Save**.

Related Links

Manually Update the PAC File on the System on page 61
Web Proxies on page 60

Sample PAC File

A proxy auto-configuration (PAC) file is a text file that instructs your system to forward traffic to a proxy server.

The following code shows a sample PAC file.

```
function FindProxyForURL(url, host)
{
if ( url.substring (0, 5) == "http:" )
{return "PROXY 10.221.77.3:8080; PROXY 10.221.76.7:8080;DIRECT";}
else if ( url.substring (0, 6) == "https:" )
{return "PROXY 10.221.77.3:8080; PROXY 10.221.76.7:8080;DIRECT";}
else
{return "DIRECT";}
}
```

The Function "`function FindProxyForURL(url, host)`" returns a string with one or more access method specifications. These specifications cause your system to use a particular proxy server or connect directly.

This function instructs your system to retrieve information for http / https protocols using the first proxy, that is "PROXY 10.221.77.3:8080".

If "PROXY 10.221.77.3:8080" is unreachable/unresponsive, then your system tries the second proxy, that is "PROXY 10.221.76.7:8080".

For more examples on PAC syntax, refer to Proxy Auto-Configuration (PAC) file.

PAC file limitations:

- If the first specified proxy is reachable and the authentication is unsuccessful, your system doesn't try a different proxy path.
- The PAC file must contain pure JavaScript.
- Poly recommends your PAC files use the `.pac` or `.proxy` extension.
- Poly supports PAC JavaScript functions that return "`PROXY host:port`" and "`DIRECT`". Poly doesn't support return values of "`SOCKS`", "`HTTP host:port`", or "`HTTPS host:port`".

View Connections to the System

Access 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 application'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
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

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
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 a Poly TC8 device Video system control using a Poly Trio system 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
5001	Inbound	Static	TCP/TLS	Polycom Content App	Yes	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
16384–32764	Bidirectional	Dynamic	UDP	RTP/RTCP (video and audio streams)	Yes	Yes
18888	Inbound	Static	TCP	Modular room messaging	Yes	No

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
44444	Inbound	Static	TCP	Content stream	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
- USB Audio

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. **Note:** Enabling this setting disables Polycom Acoustic Fence technology and vice versa. This feature isn't available on the Studio X30 system. It also isn't available when using a Poly Microphone IP Adapter or Poly Trio microphones with your system.
Sound Effects Volume	Sets the volume level of the ringtone.
Ringtone	Specifies the ringtone for incoming calls.

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 NoiseBlockAI	Enables Poly NoiseBlockAI, which during a call eliminates background and extraneous sounds in common working environments. **Note:** This setting is disabled when you enable M-Mode. If you use an external echo canceller, keyboard noise reduction isn't 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 set 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

Test Speakers on page 114

Audio Input

You can connect several types of microphones to your system.

The following audio inputs are supported:

- IP-based Poly microphone peripherals (for the G7500 system only):
  - **Poly IP Table Microphone**
  - **Poly IP Ceiling Microphone**
  - **Poly Microphone IP Adapter**
- **X50 Microphones** and **X30 Microphones**: The built-in microphones that come with the Studio X50 and Studio X30 systems.
- **Polycom RealPresence Debut Expansion Microphone** (for the Studio X50 system only)
- **3.5 mm** (not available on Studio X30 system): 3.5 mm stereo input used to share audio from a device or 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.
- **Trio Microphones**: Available when paired with a Poly Trio system.

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.

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.

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

For Studio X50 and Studio X30 Systems:

Once you enable Polycom Acoustic Fence on your Studio X50 or Studio X30 system, you can also adjust the width of the audio fence beam so that the system’s built-in microphones pick up sound in the area you want.

For G7500 Systems:

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 23
Fix Polycom Acoustic Fence Issues with G7500 on page 116

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

Procedure

1. In the system web interface, go to **Audio/Video** > **Audio** > **General Audio Settings**.
2. Select the **Enable Acoustic Fence** check box.
3. Set **Acoustic Fence Sensitivity** to adjust the width of the audio fence beam.
   - **For Studio X50 and Studio X30 systems**: Higher values increase the width of the audio fence beam. Use `1` for the narrowest beam (12 degrees) or `10` for the widest beam (120 degrees). If **Acoustic Fence Sensitivity** is set to `0`, the system mutes the microphone(s). The total angles is the setting number multiplied by 12.
   - **For G7500 systems**: Higher values increase the width of the audio fence beam between the primary and fence microphone(s). Use `0` for the narrowest beam (20 degrees) or `10` for the widest beam (120 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 11

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.

Live Microphone Switching on Studio X50

Configure your system to automatically toggle the microphone input between the system's built-in microphones and a RealPresence Debut expansion microphone.

The system detects which microphone is picking up the strongest audio input from the speaker and automatically changes to that microphone. For example, if you frequently walk behind your unit you can place the RealPresence Debut expansion microphone behind your system to catch your voice as you walk around.

Configure Studio X50 Microphone

You can enable the ability to switch between a built-in microphone that comes with the Studio X50 and a RealPresence Debut expansion microphone.

Procedure

1. In the system web interface, go to **Audio/Video** > **Audio** > **General Audio Settings**.
2. Select the **Enable Auto Mic Switching** check box (your changes save automatically).

Configure HDMI Audio Input

You can specify the audio input level for your system's HDMI connections (for example, audio from an HDMI-connected laptop).

Procedure

1. In the system web interface, go to **Audio/Video** > **Audio** > **Audio Input** > **HDMI**.
2. For **Audio Input Level**, set the left and right channel levels by choosing a value from `0` to `10`.

   The audio meters display the input's left and right channel levels.

Configure 3.5 mm Audio Input

You can specify how the system routes and controls audio from the 3.5 mm stereo input.

The Studio X30 doesn't support 3.5 mm audio input.

Procedure

1. In the system web interface, go to **Audio/Video** > **Audio** > **Audio Input** > **3.5 mm**.
2. For **Audio Input Level**, set the left and right channel levels by choosing a value from `0` to `10`.

   The audio meters display the input's left and right channel levels.
3. Choose one of the following **Playback Options**:

Playback Options

Option	Description	Result
Playback to All Locations	Select this option if you're sending audio from a device.	▪ Near and far sites hear the 3.5 mm stereo input. ▪ You can't mute audio or control echo cancellation.
Playback to All Locations	Select this option if you're using an external digital signal processor (DSP), such as Polycom SoundStructure, which provides mute controls and echo cancellation.	▪ Only far sites hear the 3.5 mm stereo input (there is no associated video content). ▪ You can't mute audio or control echo cancellation through the system.

Option	Description	Result
Playback to Far Sites, Mute Controlled	Select this option if you want to perform activities like sharing music from a mobile phone to call participants.	▪ Only far sites hear the 3.5 mm stereo input (there is no associated video content). ▪ You can mute audio but can't control echo cancellation.
Playback to Far Sites, Mute Controlled, Echo Cancelled	Select this option if you're using a line-level microphone. **Note:** The microphone must provide the line-level signal to work.	▪ Only far sites hear the 3.5 mm stereo input (there is no associated video content). ▪ You can mute audio and control echo cancellation. ▪ Mic-level inputs aren't supported.

Using Poly Trio Microphones

The video system automatically configures Poly Trio microphones when you pair the phone.

Note: Poly Trio microphones are disabled by default if your system is using Microsoft Teams.

You can only use the following microphones in addition to the Poly Trio microphones:

- Poly Trio Expansion Microphones
- Studio X50 and Studio X30 built-in microphones (speaker locating only)

Also note the following when using Poly Trio microphones with your video system:

- You can't use Poly IP audio devices, including table and ceiling microphones and the microphone adapter.
- Polycom Acoustic Fence technology isn't available.
- Polycom StereoSurround isn't available.
- The audio input level (mono channel meter) displays in the local interface and system web interface.
- You can only pair a single Trio with your system.

Related Links

Pairing a Poly Trio on page 19
Updating a Paired Poly Trio on page 92

Enable Poly Trio Microphones When Using Microsoft Teams Rooms

Poly Trio microphones are disabled by default when the system is using Microsoft Teams Rooms. Enabling the phone's mics requires a system restart.

Procedure

1. In the system web interface, go to **Audio/Video** > **Audio** > **General Audio Settings**.
2. Select the **Enable Poly Trio Audio (Speakers and Microphones)** check box, then **Continue** to confirm the restart.

Configure NoiseBlockAI When Paired with Poly Trio

To use Poly NoiseBlockAI when paired with a Poly Trio, enable the setting on your video system. There's nothing to configure on the phone.

Procedure

1. In the system web interface, go to **Audio/Video** > **Audio** > **General Audio Settings**.
2. Select the **Enable Keyboard Noise Reduction and NoiseBlock** check box.

Configuring the Microphone Adapter

The video system automatically configures Poly Microphone IP Adapter when you pair it.

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

Note the following when using the microphone adapter:

- You can't use Poly IP table and ceiling microphones.
- Polycom StereoSurround isn't available.
- The audio input level (mono channel meter) displays in the local interface and system web interface.
- Polycom Acoustic Fence technology isn't supported.
- The RealPresence Group Series microphone array configuration uses stereo audio by default, but the microphone adapter supports only mono mode.

Related Links

Poly Microphone IP Adapter on page 25

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
Primary Audio Volume	Sets the main audio output volume level going to the speakers.

Setting	Description
Bass	Sets the volume level for low frequencies without changing the primary audio volume.
Treble	Sets the volume level for high frequencies without changing the primary audio volume.
Speaker Options	Specifies the speaker output. ▪ **TV Speakers**: Use only the speakers on your connected monitors. ▪ **System Speakers**: Use only the built-in speakers on a Studio X50 or Studio X30 system.

Using Poly Trio Speakers

When you pair a Poly Trio system with your video system, you can use the phone's speakers as the audio output for the room.

Enable Poly Trio Speakers When Using Microsoft Teams Rooms

Poly Trio speakers are disabled by default when the system is using Microsoft Teams Rooms. Enabling the phone's speakers requires a system restart.

Procedure

1. In the system web interface, go to **Audio/Video** > **Audio** > **General Audio Settings**.
2. Select the **Enable Poly Trio Audio (Speakers and Microphones)** check box, then **Continue** to confirm the restart.

Choose Speakers When Paired with Poly Trio

In or out of a call, you can toggle whether you want to use Poly Trio, connected monitor, or video system speakers.

Procedure

1. In the system web interface, go to **Audio/Video** > **Audio** > **Audio Output**.
2. Choose one of the following **Speaker Options**:
   - **Phone Speakers**: Use only your Poly Trio system speakers.
   - **TV Speakers**: Use only the speakers on your connected monitors.
   - **System Speakers**: Use only the built-in speakers on a Studio X50 or Studio X30 system.

Related Links

Pairing a Poly Trio on page 19
Updating a Paired Poly Trio on page 92

Configure 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 X30 doesn't support 3.5 mm audio output.

Procedure

1. In the system web interface, go to **Audio/Video** > **Audio** > **Line Out**.
2. To specify how volume is controlled for a device connected to the line out port, choose one of the following **Output Mode** options:
   - **Variable**: Enables users to change the volume.
   - **Fixed**: Sets the volume to the audio level configured for the system.

USB Audio

Your system supports audio input and output sources through USB connections. When enabled, non-USB audio connections aren't supported.

Using USB and Bluetooth Headsets

You can use USB and Bluetooth headsets with your system (Bluetooth headsets require a USB adapter).

When connected, you can control your headset audio but not the system audio (such as mute or volume control).

Only headsets with the following specifications are supported:

- 48 kHz sample rate
- Dual channels
- 16-bit pulse-code modulation (PCM)

Using the Shure IntelliMix P300

You can connect a Shure IntelliMix P300 audio conferencing processor to your G7500 or Studio X50 system using a USB-A port (USB-C isn't supported).

Note the following when using this audio processor:

- Once connected to the system, the processor handles all audio.
- You can't use speakers and microphones that aren't connected to the processor.
- The video system automatically disables its internal echo cancellation processing.

Using the EagleEye Cube USB Camera Microphone

With a G7500 system, you can use the Poly EagleEye Cube USB camera as a microphone if you don’t connect other microphones to the system.

Enable USB Audio

USB audio connections (for example, a USB headset) don’t work by default.

Procedure

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

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
- Reset Camera Settings to Defaults
- Calibrate EagleEye Producer Group Framing
- Supported USB Cameras
- Selecting the Primary Camera
- Configuring 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.

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

The content sharing HDMI interface supports audio streaming. Sharing content from personal computing devices refers to sharing content using a computer with an HDMI connection. The system supports a variety of resolutions.

Supported HDMI Input Resolutions and Frame Rates

Input	Resolution	Frame Rate(s)
UHD	3840 x 2160p	24, 25, 30
QHD	2560 x 1440p	50, 60
FHD	1920 x 1080p	50, 60
WSXGA+	1680 x 1050	60
UXGA	1600 x 1200	60
SXGA	1280 x 1024	60

Input	Resolution	Frame Rate(s)
HD	1280 x 720p	50, 60
XGA	1024 x 768	60
SVGA	800 x 600	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	Specifies monitor settings. ▪ **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). **Note:** To use 4K resolution, make sure you set Monitor 2 to **Off**.

Setting	Description
Resolution	Specifies the monitor resolution. This setting is unavailable when you select **Automatic** for the **Configure Monitor** setting. **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.

Related Links

Configure Dual Monitor Display Settings on page 90

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).

Setting	Description
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.
Camera Sleep Mode	**Note:** Don't configure sleep settings in Partner Mode.
Current People Camera	Select the camera or HDMI input to be used for conferencing.
Enable User Camera Selection	Allow the user to select primary camera from the TC8 or the local interface.

3. Select **Save**.

Related Links

Update Poly HDCI Cameras on page 96

Reset Camera Settings to Defaults

After changing camera settings, you can quickly reset all camera settings to the default configuration.

Procedure

1. In the system web interface, go to **Audio/Video** > **Video Inputs**.
2. Select **Reset to Defaults**.
3. Select **Continue**.

   Camera settings reset to the default configuration.

Calibrate EagleEye Producer Group Framing

Calibrate your EagleEye Producer camera to align with your EagleEye camera using the RealPresence Group Series remote (the RealPresence Group Series remote is different from the remote that came with your system). Calibrating the cameras ensures the best view of the room for group framing.

Verify that the EagleEye camera is properly attached to the EagleEye Producer as described in the *Polycom EagleEye Producer Setup Sheet*.

The EagleEye Producer camera must align with the EagleEye IV camera. If the alignment changes, group framing isn't accurate.

Procedure

1. In the local interface, go to **Menu** > **Camera** > **Select Camera**.

2. Select **EagleEye Producer** as the primary camera.
3. On the RealPresence Group Series remote, press the **Home** button for five seconds.

   The EagleEye Producer LED changes to a fast blue blink.
4. Using the video preview on your monitor, press the **Up** and **Down** arrow buttons on the RealPresence Group Series remote control to align the EagleEye Producer camera with the EagleEye camera.

   Note: Use the video preview on your monitor to show the best room view when group framing.
5. Do one of the following:
   - On the RealPresence Group Series remote, press the **Home** button to exit calibration mode.
   - Don’t press any buttons 5 seconds to automatically exit calibration mode.

Supported USB Cameras

You can connect a supported USB camera to your G7500 or Studio X50 system when the system is in Zoom Rooms mode to use as a primary or secondary camera.

Poly supports the following USB cameras:

- Poly EagleEye Cube USB camera
- Polycom EagleEye IV USB camera
- Vaddio ConferenceSHOT AV
- Huddly IQ Conference Camera
- Logitech Rally Ultra HD PTZ Camera

Poly supports the INOGENI 4K2USB3 4K HDMI to USB 3.0 Capture Device.

Note: The INOGENI 4K2USB3 defaults to a 4K output resolution. Poly recommends updating the device to firmware release 8.39 or higher, and using the INOGENI Control App v2.81 or higher. Configure the maximum resolution to match the HDMI input source you intend to connect to the INOGENI 4K2USB3. For example, if the HDMI input source to be connected to the INOGENI 4K2USB3 is outputting 1920x1080, the INOGENI 4K2USB3 must be configured with a maximum resolution of 1920x1080. A mismatch between the HDMI input resolution of the source connected to the INOGENI 4K2USB3 and the device's maximum resolution results in no video.

Selecting the Primary Camera

In Poly Video Mode and Zoom Rooms, if you have more than one camera attached to the system, you can select the primary camera in or out of a call.

Camera Priority

When you connect or disconnect a camera, camera priority determines the primary or active camera.

- When you attach a camera to a system that’s powered on, it automatically becomes the current people camera.
- If you attach a camera during a call, it automatically becomes the current people camera.

- If you disconnect the current people camera, the system falls back to the next priority camera.

The system observes the following camera type priority:

1. Embedded camera
2. HDCI camera
3. USB camera
4. HDMI source set to display as people

Maximum Number of Supported Camera Connections

Your systems support a limited number of cameras for use in and out of calls.

This is only available when the system is in Poly Video Mode or Zoom Rooms.

Each system supports the following number of cameras:

Maximum Number of Connected Cameras

System	Cameras
G7500	Supports a maximum of two connected cameras at a time. ▪ One USB-A camera ▪ One HDCI camera
Studio X50	Supports a maximum of one connected camera at a time. ▪ One USB-A camera ▪ Built-in camera
Studio X30	Doesn't support multicamera connections.

Configuring 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.

Your system supports two video inputs. For example, a **People** source has pan, tilt, zoom, and near/far camera control settings, while a **Content** source doesn’t.

Configure General Video Input Settings

Available settings vary depending on your video input sources.

Procedure

1. In the system web interface, go to **Audio/Video** > **Video Inputs**.
2. Go to the input of a connected camera.
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.
Optimized for	Specifies optimization preferences for the video input. ▪ **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.
Orientation	Specifies whether to invert the camera display for a Studio X30 system that's mounted below a monitor.
Backlight Compensation	Specifies if the camera automatically adjusts for a bright background. Use backlight compensation when the subject appears darker than the background.
Skin Enhancement	Enables or disables natural skin color enhancements for participants.
Wide Dynamic Range	Enables or disables re-exposure according to the framed area instead of full view.
Framing Size	Specifies the framing view. ▪ **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.
Maximum Digital Zoom Factor	Specifies the maximum digital zoom factor for the camera.

4. Select **Save**.

Adjust the White Balance

The white balance setting specifies how the camera compensates for light source variations in the room.

Procedure

1. In the system web interface, go to **Audio/Video** > **Video Inputs**.
2. Choose one of the following options for the **White Balance** setting (available options depend on the camera you're using):
   - **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.

     When you set 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**.
   - **Color Temperature Value**: The color temperature values, measured in degrees Kelvin, correspond to the color of ambient light in a room. Use lower values for warmer lighting and higher values for cooler lighting.
   - **Color Temperature Term**: Some cameras provide text descriptions of available color temperatures (for example, **Fluorescent** or **Shade**).
   - **Off**
3. Select **Save**.

Configure Camera Tracking Settings for Studio X50 or Studio X30

With Studio X50 and Studio X30 systems, Poly camera tracking technology can automatically frame groups of people and follow conversations in small and medium rooms.

Tracking options and behavior depend on your connected camera. For example, if you use a standalone EagleEye IV camera with your system, you won't see tracking options.

Note: If you select a framing option, it automatically enables tracking on Studio X50 and Studio X30 systems.

Procedure

1. In the system web interface, go to **Audio/Video** > **Video Inputs**.
2. Go to the camera's settings and specify a **Tracking Mode**.
   - **Frame Group**: The camera automatically locates and frames all the people in the room.
   - **Frame Speaker**: The camera includes everyone in the current conversation. For example:
     - The camera focuses on people actively talking.
     - When someone is talking for a prolonged period of time, the camera assumes that this person is presenting and only focuses on them.
     - If there's a period in which no one has said anything or the far side is doing most of the talking, the camera frames everyone in the room.

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

- **Presenter Mode**: The camera tracks an active speaker who's talking and moving. Presenter mode is a preview feature on the Studio X30 that may be removed or changed in a future release.
- **Off**: Disables automatic tracking. You must control the camera manually.

3. Select **Save**.

Related Links

Presenter Mode on page 88

Configure Camera Tracking Settings for G7500

With a G7500 system, Poly camera tracking technology can automatically frame groups of people or the active speaker in medium and large rooms.

Tracking options and behavior depend on your connected camera. For example, if you use a standalone EagleEye IV camera with your system, you won't see tracking options.

Procedure

1. In the system web interface, go to **Audio/Video** > **Video Inputs**.
2. Go to the camera's settings and specify a **Tracking Mode**.
   - **Frame Group**: The camera automatically locates and frames all the people in the room.
   - **Frame Group with Transition**: The camera automatically locates and frames people 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 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 your microphone, the camera tracking mode automatically switches to **Frame Group**.

   - **Off**: Disables automatic tracking. You must control the camera manually.
3. Optional: Turn on the **Picture in Picture** setting.

   This setting is available only with the 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).
4. Select **Save**.

Related Links

Presenter Mode on page 88

Presenter Mode

Presenter mode frames the main speaker in your meeting room and follows the speaker when the speaker moves.

You can enable presenter mode for meetings where one person is the primary presenter or for distance learning so the camera always shows the instructor. When using presenter mode, you need to talk for 3 to 5 seconds before the camera starts tracking your movement.

Presenter mode ends automatically in the following situations:

- The presenter stops talking for a while.
- The presenter walks off camera.

To ensure the best performance of presenter mode, do the following:

- Place the device within 3 m (10 ft) of the speaker.
- Position the device so the camera is level with the speaker's upper chest instead of eye level. This enables the camera to capture most of the speaker's body along with the presentation background.

  If you position the camera at the speaker's eye level, the device may be positioned too high to capture all the content on the screen. If you position the camera lower than the speaker's upper chest, the speaker's head may not appear in the camera view.
- If other people are in camera view, ensure they're not speaking and minimize background noises.
- Provide sufficient lighting on the presenter while avoiding excessive backlighting or glare from ceiling lights or windows.
- The system can track the presenter when they're facing away from the camera, but tracking works best when the presenter faces the camera.
- The system can track presenters wearing face coverings or glasses.
- If the camera tracking isn't functioning as expected, try turning presenter mode tracking off and back on again.

Related Links

Configure Camera Tracking Settings for Studio X50 or Studio X30 on page 86
Configure Camera Tracking Settings for G7500 on page 87

Sharing Content

Topics:

- Default Option for Sharing Content

Your system provides a single way to share content through a wired connection. The conferencing provider may provide other ways of sharing content. Refer to partner documentation for information on their content sharing capabilities.

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	Specifies how the self view window displays when others join a call. ▪ **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	Specifies whether to display content on one or two monitors. ▪ **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 79

System Maintenance

Topics:

- Unlock System Settings
- Updating Software
- Downgrading Software
- Restart the System
- Change the Conferencing Partner Application
- Set the Conferencing Provider to Device Mode
- 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.

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
- Microsoft Teams Device Management (Microsoft Teams Rooms only)
- Zoom Rooms Administrator Portal (Zoom Rooms only)

- Software package you obtain from the Poly Online Support Center and upload with a USB flash drive
- Provisioning service (for example, Poly Lens or RealPresence Resource Manager)

Related Links

Using a Provisioning Service on page 33

Updating Paired Devices

When you update your system, you also update some of its paired 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

Updating a Paired Poly Trio

You can update a Poly Trio system that's supposed to work with a video system in various ways.

See the Poly Trio administrator documentation for information on updating the phone using the following methods.

Automatic Updates

Provision your phone with Poly UC Software. This method works when the phone is paired with the video system.

Manual Updates

Upgrade the phone with a USB flash drive. You must first set the phone to **Hub** mode before you can update.

Note: Unlike some other peripherals, you can't update a paired Poly Trio from the **Device Management** page in the system web interface.

Related Links

Pairing a Poly Trio on page 19
Using Poly Trio Microphones on page 72
Choose Speakers When Paired with Poly Trio on page 74

Updating Software in the G7500 System Web Interface

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

Note: The Studio E70 camera does not have a separate web user interface. All management of the camera is performed via the G7500 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, the software update methods in the system web interface are unavailable. You must configure the software update method using your chosen provisioning method.

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
Poly Online Support Center	A software server hosted by Poly.

Software Update Method	Description
Custom Server URL	A server on your network that supports HTTP or HTTPS downloads. The URL is the path to the latest software build folder (for example, `https://<system_build_folder>`). 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: ▪ `eecube` ◦ `Config` ◦ `image.zip` ◦ `version` ▪ `videocodec` ◦ `Config` ◦ `poly-video-<version>.zip` ◦ `release.json` ◦ `version` ▪ `ipmic` ◦ `Config` ◦ `image.zip` ◦ `version` ▪ `micadapter` ◦ `Config` ◦ `image.zip` ◦ `version` ▪ `touchctrl` ◦ `Config` ◦ `poly-tc8-<version>.zip` ◦ `version` ◦ `release.json` ▪ `softwareupdate.cfg` **Note:** If you are using private PKI certificates in your environment and want HTTPS software downloads to work, you must install the trusted root certificate from your internal certificate authority (CA) on the system since certificate validation is always performed.

Software Update Method	Description
Microsoft Teams Device Management	For systems using the Microsoft Teams Rooms application. Selecting this disables other update controls on the page.
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 33

Manually Update Software

You can manually update the software of your system and some of its paired 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**.

Automatically Update Software

You can automatically update the software of your system and some of its paired 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 System Software from a USB Flash Drive

Procedure

1. Obtain the software package from the Poly Online Support Center.
2. Save the software upgrade package to the root directory of a USB flash drive.

3. Connect the USB flash drive to the USB 2.0 port on the back of the device. This is the top USB port. The device detects the USB flash drive and displays a prompt on the monitor for you to confirm that you want to update the software.
4. Select **OK**. Follow the setup wizard 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 81

Downgrading Software

Manually downgrade software using a USB flash drive or the system web interface if your system doesn't use a provisioning server.

Make sure that system supports the selected provider in the version you're downgrading to.

Warning: When downgrading software to versions earlier than 3.3.2, use the system's dashboard to check that the hardware version meets the requirement for the software version. If you attempt to downgrade to an unsupported software version the downgrade fails.

Supported Hardware Versions

System	Poly VideoOS 3.3.1 and Earlier	Poly VideoOS 3.3.2 and Later
Poly Studio X50	1	All
Poly Studio X50 No Radio	20	All
Poly G7500	1 to 7	All
Poly G7500 No Radio	20	All

Note: Poly Studio X30 has no restrictions on downgrading.

Related Links

Register the System with RealPresence Resource Manager Provisioning Service on page 34

Manually Downgrade Software in the System Web Interface

You can downgrade your system software and the software of some of its paired 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 some of its paired devices (not a TC8 device) 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.

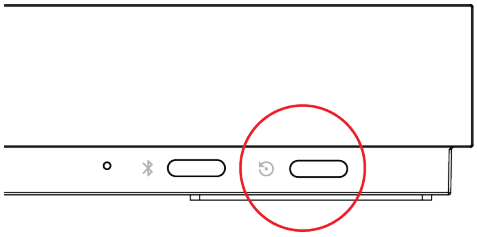
Restart the System

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 10

Change the Conferencing Partner Application

Change your conferencing partner to use the partner's native conferencing app on your system to make and receive calls.

When you change the conferencing provider, the system retains previously configured settings. It also updates the provider setting for the Zero Touch Onboarding (ZTO) profile associated with your system.

Procedure

1. In the system web interface, go to **General Settings** > **Provider**.
2. Select the provider you want to change to.
3. Select **Save**, then select **Restart**.

   The system restarts and launches the selected conferencing provider application.

Set the Conferencing Provider to Device Mode

Choosing Device Mode as your provider locks your system in Poly Device Mode. When you set the conferencing provider to Device Mode, the local interface displays only the Device Mode interface.

Connect the system to your network using an Ethernet cable, and complete the initial system setup. The system requires an active network connection after switching your provider to Device Mode.

Changing the provider to Device Mode disables Airplay and Miracast in the system web interface.

Procedure

1. In the system web interface, go to **General Settings** > **Provider**.
2. In the **Provider** drop-down menu, choose **Device Mode**.
3. Select **Save**, then select **Restart**.

The system restarts and launches Device Mode. Connect a computer to the system to join meetings or place calls using the system as an audio and video peripheral.

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: A system reset restores your system to its original mode of operation (for example, 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 system logs.**
4. Select **Reset**.

Factory Restore the System

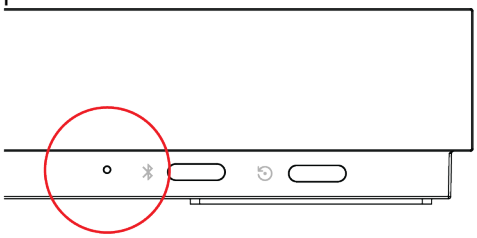
A factory restore completely erases the system's flash memory and restores it to a stable software version. See the *Poly VideoOS Release Notes*, Version History section for the current factory restore version.

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

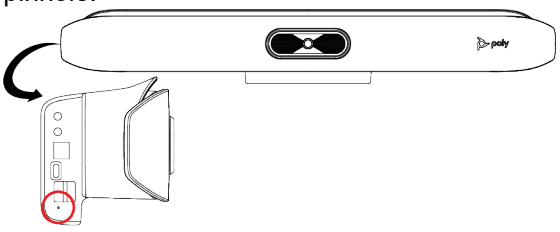
- Current software version
- Logs
- User-installed PKI certificates
- Local directory entries
- Call detail record (CDR)

Procedure

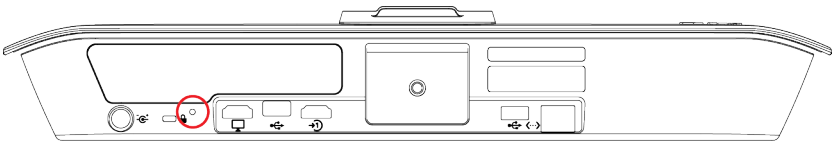
1. Disconnect the power supply to turn off the system.
2. Do one of the following:
   - On the front of the G7500, insert a straightened paper clip through the factory restore pinhole.



   - 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 straightened 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 turns amber, stop pressing the restore button.

   You can only see the restore progress on a display connected to the secondary monitor HDMI output port.

Note: You can't see the restore progress for a Studio X30 system because it has only one monitor connection.

Related Links

LED Status Indicators on page 14

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 23

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

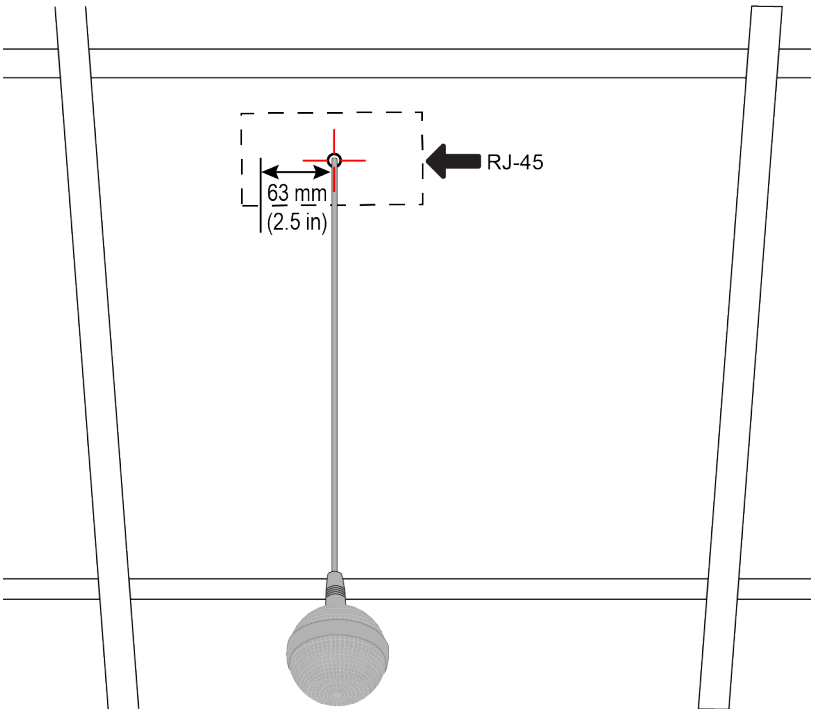
Procedure

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.

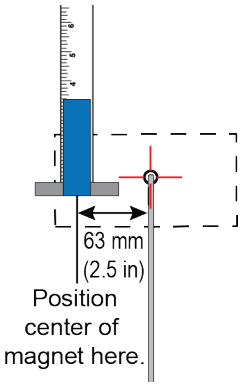
2. Ensure that the microphone is powered on.
3. Locate the factory reset sensor.

   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.



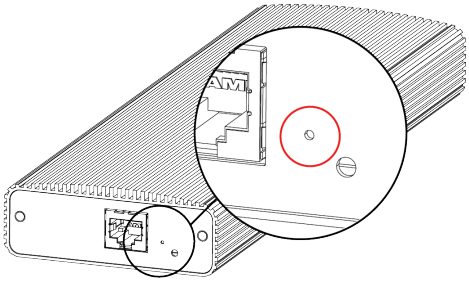
The microphone LED blinks amber during a factory restore.

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 25

Troubleshooting

Topics:

- Logs
- SNMP Reporting
- Checking System Status
- Check Provisioning Results
- Paired IP Devices
- Audio Tests
- LED Status Indicators for the System LAN Ports
- Fix Polycom Acoustic Fence Issues with G7500
- Test Connection with Another System
- Run a Trace Route
- Checking the Web Proxy Configuration
- Verify Poly Lens Registration Status
- Poly Trio Audio Meter Not Displaying in System Web Interface
- A Portion of the EagleEye Cube USB Camera Name Is Cut Off
- Monitor Loses Signal After Monitor Swap

Refer to the following topics to help you diagnose and fix problems while using your system.

Logs

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

Note: If your system experiences a sudden loss of power, your system loses all logs since the last system reboot or log download.

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:

- Cameras (see your video system's latest *Release Notes* for supported models)
- Poly TC8 device
- Poly Trio system (see your video system's latest *Release Notes* for supported models)
- 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: • **System Name and Timestamp**: Folder name is the system name and the timestamp of the log transfer. For example, if the system name is `Marketing`, the folder name might be `marketing_<date_and_time>`. • **Timestamp**: Folder name is the timestamp of the log transfer (for example, `<yyyyMMddhhmmssSSS>`). • **Custom**: Lets you specify a folder name for manual log transfers.
Storage Type	Specifies the type of storage device used for log file transfers.

Setting	Description
Transfer Frequency	Specifies when the system transfers logs: • **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	Sets the minimum log level of messages stored in the system's flash memory. Poly recommends that you use the default value. When you enable remote logging, the log level is the same for both remote and local logging. Set one of the following log levels. Poly recommends that you enable automatic transfer of logs to a USB flash drive when using one of these setting. • **Debug**: Logs all messages. • **Info** • **Warning** • **Critical**: Logs the fewest number of messages
Enable H.323 Trace	Logs additional H.323 connectivity information. Poly recommends that you enable automatic transfer of logs to a USB flash drive when using this setting.
Enable SIP Trace	Logs additional SIP connectivity information. Poly recommends that you enable automatic transfer of logs to a USB flash drive when using this setting.

3. Select **Save**.

Retrieve Log Files

You can use the web interface to download log files to a location on your computer.

Note: The date and time of the system log entries for devices are shown in GMT.

Procedure

1. Access the web interface by opening a web browser and entering the IP address of the system using the format https://IPaddress (for example, https://10.11.12.13), and go to **Diagnostics > Logs**.
2. Select **Download system logs**. A dialog window opens for you to specify how you want to open or save the .tgz file.

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

You can 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. Your system may use a version of TLS that you configured your system not to use. This happens because your system sends logs using the TLS version configured on your remote logging server. This doesn't affect the use of the configured TLS version for other parts of your system. For example, if you set your system's minimum version of TLS to 1.2, but the server only uses 1.0, it still receives the logs.
- 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	Specifies whether remote logging is enabled. Enabling this setting causes the system to send each log message to the specified server. The system immediately begins forwarding its log messages after you click **Save**. The system supports remote logging encryption using TLS. If you use UDP or TCP transport, Poly recommends remote logging only on secure, local networks.
Remote Log Server Address	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**: • UDP: 514 • TCP: 601 • TLS: 6514 You can specify the address and port in the following formats: • IPv4 address: `192.0.2.0:<port>`, where <*port*> is the elective destination port number in the 1-65535 range. • FQDN: `logserverhost.company.com:<port>`, where <*port*> is the elective destination port number in the 1-65535 range.
Remote Log Server Transport Protocol	Specifies the transport protocol for sending logs to a remote server: • UDP • TCP • TLS (secure connection)

3. Select **Save**.

Configure Logging to System Internal Storage

Enable logging to the system's internal storage to help troubleshoot critical issues that are causing normal logging operations to fail.

Caution: Poly recommends logging to the system's internal storage only when tracking critical issues. Enabling for extended periods of time causes wear on the system's storage and may cause the system to fail.

Procedure

1. In the system web interface, go to **Diagnostics** > **Logs** > **System Log Settings**.
2. Select the **Save Logs to Internal Storage** check box.

   Note: The system saves logs to the internal storage for 2 weeks. After 2 weeks, the system reverts to the previously configured logging method and deletes the logs in the internal storage. Download the logs before the time expires.

3. Select **Save**.

Sample Log File

The following code shows examples from a system log file.

```
Login:
2020-05-07 19:06:36.526 DEBUG    SecurityService: SecurityService:
securityserviceproto.cpp SecurityServiceCreateSessionRequest clienttype: 3
location: 192.168.137.1 clientName: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/
537.36 request: clienttype: kWeb
2020-05-07 19:06:36.526 DEBUG    SecurityService: SecurityService:
createSession ClientType is 3 location: 192.168.137.1  name:Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/81.0.4044.129 Safari/537.36
2020-05-07 19:06:36.526 DEBUG    SecurityService: SecurityService: In
createSession sessionId=PSLgZBGvGw7I
2020-05-07 19:06:36.526 DEBUG    SecurityService: SecurityService:
createSession The password is not empty, setting the user as anonymous
2020-05-07 19:06:36.526 DEBUG    SecurityService: SecurityService:
updateSessionCount: Increment session count for client type '3' to 1
2020-05-07 19:06:36.526 DEBUG    SecurityService: SecurityService:
SessionAddNtfy: len 268
2020-05-07 19:06:36.526 DEBUG    SecurityService: SecurityService:
SecurityServiceSendNotification(): finished sending the notification,
msg_sendnotification() returned 0
2020-05-07 19:06:36.533 DEBUG    SecurityService: SecurityService:
SecurityServiceLoginRequest(): username: admin
2020-05-07 19:06:36.533 DEBUG    SecurityService: SecurityService: login
2020-05-07 19:06:36.533 DEBUG    SecurityService: SecurityService:
LocalAuthenticator::login, role 3 loginSuccess 1
2020-05-07 19:06:36.535 DEBUG    SecurityService: SecurityService:
SessionStateNtfy: len 69
2020-05-07 19:06:36.535 DEBUG    SecurityService: SecurityService:
SecurityServiceSendNotification(): finished sending the notification,
msg_sendnotification() returned 0
2020-05-07 19:06:36.535 DEBUG    SecurityService: SecurityService:
```

```
getPwdStatusAux password can not expire node
security.authentication.accounts.adminremote.passwordpolicy
2020-05-07 19:06:36.535 DEBUG    SecurityService: SecurityService: login
login, pwStatus 2
2020-05-07 19:06:36.535 DEBUG    SecurityService: SecurityService:
setCurrentLoginInfo set login status: lastLoginTime 1588877728,
lastClientType 3, lastClient 192.168.137.1, failedLogins 0
2020-05-07 19:06:36.536 DEBUG    SecurityService: SecurityService:
setSuccessfulLoginInfoToConfig successful login, current time 1588878396
2020-05-07 19:06:36.537 DEBUG    SecurityService: SecurityService:
LoginNtfy: len 30
2020-05-07 19:06:36.537 DEBUG    SecurityService: SecurityService:
SecurityServiceSendNotification(): finished sending the notification,
msg_sendnotification() returned 0
2020-05-07 19:06:36.537 DEBUG    SecurityService: SecurityService:
securityserviceproto.cpp SecurityIFLoginStatusPack

Logout:

2020-05-07 19:17:29.313 DEBUG    SecurityService: AuthenticationManager:
AuthenticationManager::logout(): username: admin
2020-05-07 19:17:29.313 DEBUG    SecurityService: SecurityService:
LogoutNtfy: len 21
2020-05-07 19:17:29.313 DEBUG    SecurityService: SecurityService:
SecurityServiceSendNotification(): finished sending the notification,
msg_sendnotification() returned 0
2020-05-07 19:17:29.313 DEBUG    SecurityService: SessionManager:
deleteItem(): deleting the session PSllKtLtRoFp
2020-05-07 19:17:29.313 DEBUG    SecurityService: SecurityService:
updateSessionCount: Decrement session count for client type '3' to 0
2020-05-07 19:17:29.313 DEBUG    SecurityService: SecurityService:
SessionDeleteNtfy: len 52
2020-05-07 19:17:29.313 DEBUG    SecurityService: SecurityService:
SecurityServiceSendNotification(): finished sending the notification,
msg_sendnotification() returned 0
2020-05-07 19:17:29.313 DEBUG    SecurityService: SecurityService:
securityserviceproto.cpp errorResponsePack
```

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 46

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 (`public`). **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.

Setting	Description
Location Name	Specifies the system location.
System Description	Provides details about the system.
User Name	Specifies the User Security Model (USM) account name for SNMPv3 message transactions. The maximum length is 64 characters.
Authentication Algorithm	Specifies the type of SNMPv3 authentication algorithm used. ▪ **SHA** ▪ **MD5**
Authentication Password	Specifies the SNMPv3 authentication password. The maximum length is 48 characters.
Privacy Algorithm	Specifies the cryptographic privacy algorithm for SNMPv3 packets. ▪ **CFB-AES128** ▪ **CBC-DES**
Privacy Password	Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.
Engine ID	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:`). The ID can’t be all zeros or Fs.
Listening Port	Specifies the port SNMP uses to listen for system messages (the default is port 161).
Transport Protocol	Specifies the transport protocol used. ▪ **TCP** ▪ **UDP**

Setting	Description
Destination Address1 Destination Address2 Destination Address3	Specifies the IP addresses of SNMP managers where SNMP traps are sent. Each address has four settings: ▪ 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.
LAN	Displays network connection status.
Servers	▪ 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 RealPresence Resource Manager Provisioning Service on page 34

Register the System with the Poly Lens Provisioning Service on page 35

Paired IP Devices

Use the following information to troubleshoot issues with paired IP devices.

Audio Tests

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

Test Speakers

Verify that you correctly connected the speakers to your system.

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

The following setups don't support stereo audio:

- Standalone Studio X30 systems
- G7500, Studio X50, and Studio X30 systems paired with Poly Trio systems

Procedure

1. In the system web interface, go to **Diagnostics** > **Audio Test**.
2. Do one of the following:
   - Select **Start**.
   - Select **Left** to test the left speaker.
   - Select **Right** to test the right speaker.
   - Select **Both** to test both speakers (if you enable 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 66

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 following setups don't support stereo audio:

- Standalone Studio X30 systems
- G7500, Studio X50, and Studio X30 systems paired with Poly Trio systems

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**.

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 37
Poly G7500 System Ports on page 11

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 68

Test Connection with Another System

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

This test isn't available on the TC8 device and the system web interface.

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.

This test isn't available on the TC8 device and the system web interface.

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 60

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** > **LAN Network** > **Web Proxy Settings**.
2. Select **Download PAC File**.

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

Verify Poly Lens Registration Status

You can check if your system is registered with Poly Lens.

Procedure

» In the system web interface, go to **Servers** > **Cloud** to check the **Registration Status**.

Related Links
Register During System Setup on page 17
Register Later on page 17

Poly Trio Audio Meter Not Displaying in System Web Interface

You can't see the audio meter for paired Poly Trio microphones in the system web interface. However, you can still see the audio meter in the local interface.

Procedure

» Reset the system and pair the Poly Trio.

A Portion of the EagleEye Cube USB Camera Name Is Cut Off

Names created using the Polycom Companion app can be up to 60 characters long, but your system cuts off the name after 32 characters.

Procedure

» Use a camera name that isn't longer than 32 characters.

Monitor Loses Signal After Monitor Swap

Swapping a 4K monitor for a 1080p monitor while your system is asleep results in losing the monitor signal.

Procedure

» Do one of the following:

- Swap the monitor while your system isn’t sleeping.
- Restart the system after you lose signal.