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

© 2020 Plantronics, Inc. All rights reserved. Poly, the propeller design, and the Poly logo are trademarks of Plantronics, Inc. All other trademarks are the property of their respective owners.
Contents

Before You Begin...............................................................................................................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.....................................................................9
  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............................14
  Completing Initial System Setup...................................................................................16
    Registering the System with Poly Lens......................................................................16
    Complete Setup with the System Web Interface.......................................................17
    Complete Setup with Provisioning............................................................................17
  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....................................................................................................20
    Connect a USB Device...............................................................................................21
    IP Microphones..........................................................................................................21
    Poly Microphone IP Adapter....................................................................................23

Configuring General Settings........................................................................................26
  Name the System and Room..........................................................................................26
  Provide Contact Information.........................................................................................26
  Set the Date and Time...................................................................................................27
  Set the System Location...............................................................................................28
<table>
<thead>
<tr>
<th>Audio Tests</th>
<th>97</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can’t Wake the System by Touching the Monitor</td>
<td>98</td>
</tr>
<tr>
<td>LED Status Indicators for the System LAN Ports</td>
<td>98</td>
</tr>
<tr>
<td>Fix Polycom Acoustic Fence Issues with G7500</td>
<td>99</td>
</tr>
<tr>
<td>Test Connection with Another System</td>
<td>99</td>
</tr>
<tr>
<td>Run a Trace Route</td>
<td>100</td>
</tr>
<tr>
<td>Checking the Web Proxy Configuration</td>
<td>100</td>
</tr>
<tr>
<td>Zero Touch Onboarding Connection Fails During Initial Setup or After Reset</td>
<td>101</td>
</tr>
<tr>
<td>Verify Poly Lens Registration Status</td>
<td>101</td>
</tr>
<tr>
<td>Lighting Conditions Impact Picture Quality</td>
<td>101</td>
</tr>
</tbody>
</table>
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
- Open SIP networks and VoIP endpoint environments

**Related Poly and Partner Resources**

See the following sites for information related to this product.

- The Polycom Support Site is the entry point to online product, service, and solution support information including Licensing & Product Registration, Self-Service, Account Management, Product-Related Legal Notices, and Documents & Software downloads.
- The Polycom Document Library provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The Polycom Community provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
• The Polycom Partner Network are industry leaders who natively integrate the Poly standards-based RealPresence Platform with their customers' current UC infrastructures, making it easy for you to communicate face-to-face with the applications and devices you use every day.

• The Polycom Collaboration Services help your business succeed and get the most out of your investment through the benefits of collaboration.
Getting Started

Topics:

- Poly Partner Mode Overview
- Product Overview of Poly Video Systems
- Powering the System On and Off
- Navigating the System

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

Poly Partner Mode Overview

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

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

- Zoom: https://support.zoom.us/hc/en-us
- GoToRoom by LogMeIn: https://support.goto.com/products
- 8x8: https://support.8x8.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 how you configure the system)
- Poly NoiseBlockAI, which eliminates background and extraneous sound during calls in common working environments when no one is talking
• 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

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
• High-fidelity, built-in stereo microphones that pick up sound within 3.66 m (12 ft) and use spatial audio for life-like presence and clarity
• Poly NoiseBlockAI, which eliminates background and extraneous sound during calls in common working environments when no one is talking
• Dual stereo speakers
• HDMI: Single input and dual output

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 3.66 m (12 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 when no one is talking
• Single mono speaker
• HDMI: Single input and output

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

These systems provide the following features and capabilities:
• Remote access for managing standalone systems
• Provisioning with Polycom RealPresence Resource Manager to support single system, small business, and large multisite enterprise deployments
• SNMP reporting and remote logging
• Industry-standard security techniques, including 802.1X authentication

Powering the System On and Off
The system turns on when you plug it into a power source. The system doesn’t have a power button, so you must unplug the power cable to power it off.

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

Related Links
Restart the System on page 79

Navigating the System
You can navigate the system using the system web interface.

Access the System Web Interface
Access the system web interface to perform administrative tasks.
The system web interface enables you to do the following actions:
• Finish setting up your system.
• Remotely configure and manage your system. Unlike the local interface, you can configure every setting through the system web interface.

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

Related Links
Complete Setup with the System Web Interface on page 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

<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3.5 mm audio line out</td>
</tr>
<tr>
<td>2</td>
<td>3.5 mm audio line in</td>
</tr>
<tr>
<td>3</td>
<td>Security lock</td>
</tr>
<tr>
<td>4</td>
<td>Mini-DIN/RS-232 serial port</td>
</tr>
<tr>
<td>5</td>
<td>USB 3.0 port (host)</td>
</tr>
<tr>
<td>6</td>
<td>USB-C port</td>
</tr>
<tr>
<td>7</td>
<td>HDCI input for Polycom cameras</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3.5 mm audio line in (reserved for future use)</td>
</tr>
<tr>
<td>2</td>
<td>3.5 mm audio line out (reserved for future use)</td>
</tr>
<tr>
<td>3</td>
<td>Polycom RealPresence Debut expansion microphone connection</td>
</tr>
<tr>
<td>4</td>
<td>USB-C port</td>
</tr>
<tr>
<td>5</td>
<td>USB ports</td>
</tr>
<tr>
<td>6</td>
<td>Factory restore pinhole</td>
</tr>
<tr>
<td>7</td>
<td>HDMI output for the secondary monitor</td>
</tr>
<tr>
<td>8</td>
<td>HDMI output for the primary monitor</td>
</tr>
</tbody>
</table>

### Related Links

- Specify the Primary and Fence Microphones on page 57
- LED Status Indicators for the System LAN Ports on page 98
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

<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power</td>
</tr>
<tr>
<td>2</td>
<td>Security lock</td>
</tr>
<tr>
<td>3</td>
<td>Factory restore pinhole</td>
</tr>
<tr>
<td>4</td>
<td>HDMI output for the primary monitor</td>
</tr>
<tr>
<td>5</td>
<td>USB-C port</td>
</tr>
<tr>
<td>6</td>
<td>HDMI input for sharing content (for example, from a laptop)</td>
</tr>
<tr>
<td>7</td>
<td>USB port</td>
</tr>
<tr>
<td>8</td>
<td>LAN connection for the system</td>
</tr>
</tbody>
</table>
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 80

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

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking white</td>
<td>Powering on</td>
</tr>
<tr>
<td>Solid white</td>
<td>Working normally</td>
</tr>
<tr>
<td>Blinking amber</td>
<td>Update in progress</td>
</tr>
<tr>
<td>Solid amber</td>
<td>Sleeping</td>
</tr>
<tr>
<td>Blinking red</td>
<td>Error preventing normal operation</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Position</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid white</td>
<td>All</td>
<td>Boot initialization in progress</td>
</tr>
<tr>
<td>Indicator</td>
<td>Position</td>
<td>Status</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Blinking blue</td>
<td>Twelve in the middle</td>
<td>Bluetooth in discovery</td>
</tr>
<tr>
<td>Solid blue for 3 seconds</td>
<td>All</td>
<td>Bluetooth paired</td>
</tr>
<tr>
<td>Blinking green</td>
<td>All</td>
<td>Incoming call</td>
</tr>
<tr>
<td>Solid green</td>
<td>All</td>
<td>Outgoing call</td>
</tr>
<tr>
<td>Solid green</td>
<td>Four to eight (when in the middle), indicating the tracked speaker or the direction of the camera</td>
<td>Working The lights are green with supported applications, with the following cases: • Tracking people in the group framing and speaker tracking mode. • Indicating the direction of the camera that you customize in the pan-tilt-zoom (PTZ) mode.</td>
</tr>
<tr>
<td>Solid amber</td>
<td>Twelve in the middle</td>
<td>Standing by The system is in sleep mode with no active video output.</td>
</tr>
<tr>
<td>Pulsing red</td>
<td>Twelve in the middle</td>
<td>Call on hold</td>
</tr>
<tr>
<td>Pulsing green</td>
<td>Twelve in the middle</td>
<td>Call on hold (by far site)</td>
</tr>
<tr>
<td>Solid white for 3 seconds</td>
<td>Twelve in the middle</td>
<td>Saving a preset</td>
</tr>
<tr>
<td>Solid red</td>
<td>All</td>
<td>Muted microphone</td>
</tr>
<tr>
<td>Pulsing amber</td>
<td>All</td>
<td>Firmware update in progress</td>
</tr>
<tr>
<td>Blinking red</td>
<td>All</td>
<td>Error preventing normal operation</td>
</tr>
<tr>
<td>Blinking amber</td>
<td>Twelve alternating</td>
<td>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.</td>
</tr>
<tr>
<td>Blinking red</td>
<td>Twelve alternating</td>
<td>In a POST sequence, at least one test resulted in a severe error. The system continues to blink red and doesn't start up.</td>
</tr>
</tbody>
</table>
Completing Initial System Setup

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

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

Before you begin:

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

Depending on how you purchased your system, it either boots directly into a conferencing application or to a screen where you choose the application.

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. Learn more [here](#).

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

Procedure
2. Follow the instructions to register your system.

Related Links
Register During System Setup on page 16
Verify Poly Lens Registration Status on page 101

Complete Setup with the System Web Interface
To finish setting up your system, manually configure the system’s local administrator password, country, and timezone.

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

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

Related Links
Access the System Web Interface on page 10
Create Local Administrator Credentials on page 38
Set the System Location on page 28
Set the Date and Time on page 27

Complete Setup with Provisioning
To finish setting up your system, provision the system’s local administrator password, country, and timezone.

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

Procedure
1. Power on the system and follow the onscreen instructions.
2. Log in to the system web interface and go to Servers > Provisioning Server to register the system with your provisioning service.
3. In your provisioning template configuration file, set the following parameters:
   - See the Polycom Documentation Library for detailed descriptions about configuration parameters and their permitted values.
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 G7500 system when connected to either of the system’s three link-local network (LLN) ports.

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

You can pair the following devices to your G7500 system with an LLN connection:
- Poly IP Table Microphone
- Poly IP Ceiling Microphone
- Poly Microphone IP Adapter

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

### Automatically Pair an IP Device

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

**Procedure**

1. 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 the 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 59
- Choose Speakers When Paired with Poly Trio on page 61
- Updating a Paired Poly Trio on page 75

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 LAN

Some devices connected to your primary network can pair with your video system. This feature enables you to pair a Poly TC8 device or Poly Trio system without a physical connection to the video system.

Note: You can’t pair Poly IP microphones, the Poly Microphone IP Adapter, and IP cameras over the primary network.

To pair, the device must be on the same subnet as the video system and the following network address and you must unblock traffic on the following addresses and ports:

- Multicast address 224.0.0.200
- UDP port 2000
- TCP port 18888
- UDP ports 16384–32764
- Multicast on UDP ports 319 and 320

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

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

- The device doesn’t automatically pair during setup with the system you purchased.
- You want to pair the device with a different system.
- You want to pair additional similar devices (for example, to control the video system with more than one TC8).
- You want to pair a Poly Trio system (you can pair only one at a time).

Procedure

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

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

3. Under Available Devices, find the device by its MAC address (for example, 00e0db4cf0be) and select Pair.
   
   If paired successfully, the device displays under Connected Devices with a Connected status. If a device shows a Disconnected status, this indicates that pairing wasn’t successful.

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

Unpair an IP Device

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

Don’t unpair devices if you plan to use them with the same system. For example, if you move your video-conferencing equipment to another room, just disconnect and reconnect the devices in the new location.
Note: If you unpair a link-local network (LLN) device, it doesn’t automatically pair again with the same system. (The Studio X50 and Studio X30 don’t support LLN connections.)

Procedure
1. In the system web interface, go to General Settings > Device Management.
2. Under 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 25

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 ℹ️ port on the back of your system.

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

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

You can connect up to three of the following microphones directly to your system:
- Poly IP Table Microphone
- Poly IP Ceiling Microphone

Related Links
Polycom Acoustic Fence on page 56
Factory Restore a Table Microphone on page 81

Poly IP Table Microphone Ports
The following illustration and table explain the ports on the table microphone.
Poly IP Table Microphone Port Descriptions

<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Micro-USB debugging port</td>
</tr>
<tr>
<td>2</td>
<td>Factory restore pinhole</td>
</tr>
<tr>
<td>3</td>
<td>Link-local network (LLN) connection</td>
</tr>
</tbody>
</table>

Poly IP Ceiling Microphone Ports

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

Poly IP Table Microphone Port Descriptions

<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Link-local network (LLN) connection</td>
</tr>
<tr>
<td>2</td>
<td>Microphone cable connector</td>
</tr>
<tr>
<td>3</td>
<td>Microphone cable connector</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid then blinking white</td>
<td>Powering on</td>
</tr>
</tbody>
</table>
### 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 83
- *Configuring the Microphone Adapter* on page 60

#### Microphone Adapter Ports

The following illustration and table explain the ports on the microphone adapter.
Microphone Adapter Port Descriptions

<table>
<thead>
<tr>
<th>Ref. Number</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>USB 2.0 debugging port</td>
</tr>
<tr>
<td>2</td>
<td>Polycom microphone Walta-Walta connector</td>
</tr>
<tr>
<td>3</td>
<td>Power</td>
</tr>
<tr>
<td>4</td>
<td>Link-local network (LLN) connection</td>
</tr>
<tr>
<td>5</td>
<td>LED status indicator</td>
</tr>
<tr>
<td>6</td>
<td>Factory restore pinhole</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking white</td>
<td>Powering on</td>
</tr>
<tr>
<td>Solid white</td>
<td>On</td>
</tr>
<tr>
<td>Blinking blue</td>
<td>Ready to pair</td>
</tr>
<tr>
<td>Solid blue</td>
<td>Paired successfully</td>
</tr>
<tr>
<td>Blinking green and blue</td>
<td>Update in progress</td>
</tr>
<tr>
<td></td>
<td>Factory restore in progress</td>
</tr>
</tbody>
</table>

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 20
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
- System Usage Data Collected by Poly

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

Name the System and Room

Name your system and assign it a room name.

Procedure

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

Provide Contact Information

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

Procedure

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

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

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):

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Specifies the country where the system is located. Changing the country automatically adjusts the country code associated with your system.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Displays the country code associated with the system location.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Choose if the system displays a black screen or a no signal message.</td>
</tr>
<tr>
<td>Time Before System Goes to Sleep</td>
<td>• Select how long the device can be idle before it goes to sleep.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Off</strong> to disable system sleep mode.</td>
</tr>
</tbody>
</table>
### 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.

Disable system sleep mode before configuring out of office settings.

**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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Specifies the time when out of office hours begin.</td>
</tr>
<tr>
<td>End Time</td>
<td>Specifies the time when out of office hours end.</td>
</tr>
</tbody>
</table>

3. 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**.

### Turn Off System Usage Data Collection

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

**Procedure**

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

Topics:

- Register the System with a Provisioning Service
- Download a Template Configuration File

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

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

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

For a list of configuration parameters, see the Poly VideoOS Configuration Parameters Reference Guide.

Related Links
- Updating Software on page 74
- PKI Certificates on page 42
- Choose How to Get Software Updates on page 75

Register the System with a Provisioning Service

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

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

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

Procedure

1. In the system web interface, go to Servers > Provisioning Server.
2. Select Enable Provisioning.
3. Select **Load Discovered Information**.
   The registration fields update automatically if your system detects a provisioning server.

4. **Optional**: If your system didn’t detect a provisioning server, complete the following fields (contact your network administrator for help):

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Type</td>
<td>Specifies the type of provisioning service (for example, <strong>RealPresence Resource Manager</strong>).</td>
</tr>
<tr>
<td>Server Address</td>
<td>Address of the system running the provisioning service.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Domain for registering with the provisioning service.</td>
</tr>
<tr>
<td>User Name</td>
<td>User ID for registering with the provisioning service.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for registering with the provisioning service.</td>
</tr>
</tbody>
</table>

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 93
- [Complete Setup with Provisioning](#) on page 17

**Download a Template Configuration File**

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

If you’re provisioning your system with a RealPresence Resource Manager system, you can use the template to create a UC endpoint configuration profile to associate with your systems. For more information, see the **Polycom RealPresence Resource Manager System Operations Guide**.

**Procedure**

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

Topics:

- Configuring Wired LAN Settings
- Configure Wi-Fi Settings

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 98

Automatically Obtain IPv4 Address Settings

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

You must have a DHCP server deployed in your environment.

Procedure

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

Manually Configure IPv4 Address Settings

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

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your IP Address is</td>
<td>Specifies the system IP address.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specifies the subnet mask assigned to your system.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Specifies the default gateway assigned to your system.</td>
</tr>
</tbody>
</table>

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.

**Procedure**

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

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local</td>
<td>Specifies the IPv6 address to use for local communication within the subnet.</td>
</tr>
<tr>
<td>Site-Local</td>
<td>Specifies the IPv6 address to use for communication within the site or organization.</td>
</tr>
<tr>
<td>Global Address</td>
<td>Specifies the IPv6 internet address.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Specifies the default gateway assigned to your system.</td>
</tr>
</tbody>
</table>

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

Manually Configure DNS Settings
You can manually configure the DNS server settings for your system. If your system gets its IP address automatically using DHCP, you can’t configure these settings. They display as read-only.

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

Configure VLAN Settings
You can configure your system’s virtual LAN (VLAN) settings.

Procedure
1. In the system web interface, go to Network > Primary Network > LAN Options.
2. Turn the Enable LLDP setting on so that the system can advertise itself on the network using the Link Layer Discovery Protocol (LLDP).
3. Turn the 802.1p/Q setting on and enter a VLAN ID.
   You can use values from 1 to 4094.
4. Select Save.

Configure 802.1X Settings
You can configure your system to use 802.1X authentication when connecting to the wired LAN.
Install the PKI certificates on your system required for authenticating with your network.
The system supports the following authentication protocols:
- EAP-MD5
- EAP-PEAPv0 (MSCHAPv2)
- EAP-TTLS
- EAP-TLS

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

Related Links
PKI Certificates on page 42

**Configure Wired LAN Options**
You can configure other LAN properties for your system in the local interface or the system web interface.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonegotiation (under <strong>General Settings</strong> in the local interface)</td>
<td>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 <strong>LAN Speed</strong> and <strong>Duplex Mode</strong> to read-only. Poly recommends that you use autonegotiation to avoid network issues.</td>
</tr>
<tr>
<td>LAN Speed (under <strong>General Settings</strong> in the local interface)</td>
<td>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 <strong>Autonegotiation</strong> setting, this setting is read-only.</td>
</tr>
<tr>
<td>Duplex Mode (under <strong>General Settings</strong> in the local interface)</td>
<td>Specifies the duplex mode to use. Note that the switch must support the speed you choose. If you enable the <strong>Autonegotiation</strong> setting, this setting is read-only.</td>
</tr>
<tr>
<td>Ignore Redirect Messages</td>
<td>Enables the system to ignore ICMP redirect messages. Polycom recommends that you enable this setting in most circumstances.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ICMP Transmission Rate Limit (millisec)</td>
<td>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.</td>
</tr>
<tr>
<td>Generate Destination Unreachable Messages</td>
<td>Generates an ICMP Destination Unreachable message if the system can’t deliver a packet to its destination for reasons other than network congestion.</td>
</tr>
<tr>
<td>Respond to Broadcast and Multicast Echo Requests</td>
<td>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.</td>
</tr>
</tbody>
</table>

3. Select Save.

**Configure Wi-Fi Settings**

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

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

Topics:

- Managing System Access
- PKI Certificates
- 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 89

Managing System Access

You can control how users and administrators access the system.

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

- Local interface
- System web interface

Local Accounts

The system stores local account IDs and passwords.

Configure Password Policies

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

Poly strongly recommends that you create an administrator password for your system. Administrators should 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:
   Not all settings apply to SNMP.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>The minimum number of characters required for a valid password.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Require Lowercase Letters</td>
<td>The minimum number of lowercase letters required for a valid password.</td>
</tr>
<tr>
<td>Require Uppercase Letters</td>
<td>The minimum number of uppercase letters required for a valid password.</td>
</tr>
<tr>
<td>Require Numbers</td>
<td>The minimum number of numerals required for a valid password.</td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>The minimum number of special characters required for a valid password. Supported characters include: @ - _ ! ; , \ / &amp; . # *</td>
</tr>
<tr>
<td>Reject Previous Passwords</td>
<td>The number of most recent passwords that you can’t reuse. If you set this to Off, all previous passwords are valid.</td>
</tr>
<tr>
<td>Minimum Password Age in Days</td>
<td>The minimum number of days before the password can change.</td>
</tr>
<tr>
<td>Maximum Password Age in Days</td>
<td>The maximum number of days before the password must change.</td>
</tr>
<tr>
<td>Minimum Changed Characters</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Consecutive Repeated Characters</td>
<td>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.</td>
</tr>
<tr>
<td>Password Expiration Warning</td>
<td>Specifies how many days in advance a warning displays indicating that the password expires soon (if you set a maximum password age).</td>
</tr>
<tr>
<td>Can Contain ID or Its Reverse Form</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin ID</td>
<td>The local administrator account name (default is admin).</td>
</tr>
<tr>
<td>Room Password</td>
<td>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 <strong>System Details</strong> and on the back of the device.</td>
</tr>
<tr>
<td>Remote Access Password</td>
<td>If you disable <strong>Use Room Password for Remote Access</strong>, 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.</td>
</tr>
<tr>
<td>Use Room Password for Remote Access</td>
<td>Enable this option to also use the room password for remote logins. Disable this option to require a separate password for remote logins.</td>
</tr>
</tbody>
</table>

3. Select **Save**.

Related Links

*Complete Setup with the System Web Interface* on page 17

Configure Account Lockout Settings

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

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Admin Account after Failed Logins</td>
<td>Specifies the number of failed login attempts allowed before the system locks the account. You can turn this setting <strong>Off</strong>.</td>
</tr>
<tr>
<td>Admin Account Lock Duration</td>
<td>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.</td>
</tr>
</tbody>
</table>
Configure System Access Settings

You can configure how you and others access the system.

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.            |
| Enable Network Intrusion Detection System (NIDS) | When you enable this setting, the system creates security log entries when it detects a possible network intrusion.                           |
| Enable Web Access                            | Specifies whether you can access the system using the system web interface.                                                                   |
| Restrict to HTTPS                            | Specifies that you can access the system web interface only over port 443. Enabling this setting closes access through port 80 (HTTP).          |
| Web Access Port (HTTP)                       | Specifies the port to use when accessing the system web interface over HTTP.  
 |                                              | If you change the default (port 80), specify port 1025 or higher and make sure it is not already in use. You must include the port number with the IP address when you use the system web interface to access the system.  
 |                                              | (This setting is unavailable if **Restrict to HTTPS** is enabled.)                                                                          |
| Enable Diagnostics Port Idle Session Timeout | Specifies whether to allow the diagnostics port to time out at the configured time interval or not. You set the timeout at **Idle Session Timeout in Minutes**. |
| Enable SNMP Access                           | Specifies whether to allow SNMP access.                                                                                                       |
| Idle Session Timeout in Minutes              | Specifies the number of minutes a session can be idle before it times out.                                                                    |
### Setting Overview

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Number of Active Sessions</td>
<td>Specifies the maximum number of users logged in through the system web interface or command-line API (SSH or telnet).</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Port after Failed Logins</td>
<td>The number of failed login attempts allowed before the web interface locks. You can set this to <strong>Off</strong>.</td>
</tr>
<tr>
<td>Port Lock Duration</td>
<td>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.</td>
</tr>
<tr>
<td>Reset Port Lock Counter After</td>
<td>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 (<strong>Lock Port After Failed Logins</strong>). The counter resets when the set period of time expires or a user successfully logs in.</td>
</tr>
</tbody>
</table>

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**.
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 30
Configure 802.1X Settings on page 34

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

<table>
<thead>
<tr>
<th><strong>CSR Information</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hash Algorithm</strong></td>
<td>Specifies the hash algorithm for the CSR: SHA-256 (recommended) or SHA-1 (not recommended).</td>
</tr>
</tbody>
</table>
| **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 fully qualified domain name (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**.

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:

<table>
<thead>
<tr>
<th>CSR Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Algorithm</td>
<td>Specifies the hash algorithm for the CSR: SHA-256 (recommended) or SHA-1 (not recommended).</td>
</tr>
</tbody>
</table>
| 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 fully qualified domain name (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 Settings

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

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

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

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Peer Certificate Chain Depth</td>
<td>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.</td>
</tr>
<tr>
<td>Always Validate Peer Certificates From Server</td>
<td>Determines whether your system requires a remote server to present a valid certificate when connecting to it for services, such as provisioning.</td>
</tr>
</tbody>
</table>

### Install a Certificate

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

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

**Procedure**

1. In the system web interface, go to Security > Certificates.
2. Select 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 filename extension).

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

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

**View a Certificate**

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

**Procedure**

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

2. To view the contents of a certificate, select **Visibility ☰** in the same row as the certificate.
   
   The certificate contents display in plain text.

**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 one of the following standard methods:

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

- **Online Certificate Status Protocol (OCSP):** Your system contacts an OCSP responder, a web server that provides revocation status through a query/response exchange.

Manually Upload a CRL

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

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

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

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revocation Method</td>
<td>To use the CRL revocation method, select CRL.</td>
</tr>
<tr>
<td>Allow Incomplete Revocation Checks</td>
<td>When enabled, a certificate in the chain of trust validates without a revocation check if no corresponding CRL from the issuing CA is installed.</td>
</tr>
</tbody>
</table>

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

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

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

Delete a CRL

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

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

**Procedure**

1. In the system web interface, go to Security > Certificates.
2. Under **Revocation**, select **Delete** next to the CRL you want to delete.
Configure the OCSP Method
You can use the OCSP method to perform certificate revocation checks on your system.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revocation Method</td>
<td>To use the OCSP revocation method, select <strong>OCSP</strong>.</td>
</tr>
</tbody>
</table>
| Allow Incomplete Revocation Checks   | When enabled, your system considers a revocation check successful if there is no response or the OCSP responder indicates a certificate's status is unknown. Regardless of how you configure this setting, the following statements apply:  
• If the OCSP responder indicates a known revoked status, your system treats it as a revocation check failure and doesn't allow the connection.  
• If the OCSP responder indicates a known good status, your system treats it as a successful revocation check and allows the connection. |
| Global Responder Address             | Specifies the URI of the OCSP responder (for example, http://responder.example.com/ocsp). The responder is used when Use Responder Specified in Certificate is disabled and sometimes even when it's enabled. It's recommended that you always include a URI in this field regardless of how you configure Use Responder Specified in Certificate. |
| Use Responder Specified in Certificate | Some certificates include the OCSP responder address. When you enable this setting, your system attempts to use this address (when present) instead of the Global Responder Address you specified.  
**Note:** Only HTTP URLs in a certificate's AIA field are supported. |

3. Select **Save**.
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banner Text</td>
<td>• Custom: Enter any text for the banner.</td>
</tr>
<tr>
<td></td>
<td>• DoD: A default U.S. Department of Defense security banner. You can’t change this text.</td>
</tr>
<tr>
<td>Remote Access Banner Text</td>
<td>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.</td>
</tr>
</tbody>
</table>

Web Proxies

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

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

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

• **Semi-automatic**: You specify the proxy credentials and URL for automatically downloading a PAC file.

• **Manual**: You specify the proxy address, port, and credentials. (This method lets you configure your system with only one proxy.)

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

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

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

Your system supports the following services when configured to use a web proxy:
- Provisioning service
- Software updates

**Related Links**
[Checking the Web Proxy Configuration on page 100](#)

**Enable the System to Use a Web Proxy**

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

**Procedure**

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

**Set Up Automatic Web Proxy Configuration**

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

**Procedure**

1. In the system web interface, go to **Network > Primary Network > Web Proxy Settings**.
2. Select **Automatic Configuration**.
3. Select **Enable WPAD**.
   - This option enables the web proxy auto-discovery protocol (WPAD), which helps your system automatically download the PAC file on your network using DHCP option 252.
4. Enter the **Proxy 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 > Primary 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 > Primary Network > Web Proxy Settings**.
2. Select **Update PAC File** to fetch the latest version of the file from the server.

**Manually Configure a Web Proxy**

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

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

**Procedure**

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

**View Connections to the System**

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

The list provides the following information:

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

This list doesn’t show details related to sharing content. For example, if someone shares a video from an HDMI-connected laptop, you don’t see that this device is connected to the system.

**Procedure**

   » In the system web interface, go to **Diagnostics > Sessions**.
## System Port Usage

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

**Note:** Check your conferencing application’s documentation for firewall settings specific to their service.

### G7500, Studio X50, and Studio X30 System Port Usage

<table>
<thead>
<tr>
<th>Port</th>
<th>Direction</th>
<th>Type</th>
<th>Protocol</th>
<th>Function</th>
<th>Open by Default?</th>
<th>Configurable Port?</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>Outbound</td>
<td>Static</td>
<td>UDP</td>
<td>DNS</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>80</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td>HTTP web server listener that provides access to the web interface. Redirects all sessions to HTTPS on port 443.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>123</td>
<td>Outbound</td>
<td>Static</td>
<td>UDP</td>
<td>NTP (automatic time synchronization)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>161</td>
<td>Inbound</td>
<td>Static</td>
<td>UDP</td>
<td>SNMP reporting</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>443</td>
<td>Bidirectional</td>
<td>Static</td>
<td>TCP/SCTP</td>
<td>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</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Port</td>
<td>Direction</td>
<td>Type</td>
<td>Protocol</td>
<td>Function</td>
<td>Open by Default?</td>
<td>Configurable Port?</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>--------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>514</td>
<td>Outbound</td>
<td>Static</td>
<td>UDP</td>
<td>Remote logging</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>601</td>
<td>Outbound</td>
<td>Static</td>
<td>TCP</td>
<td>Remote logging</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2000</td>
<td>Inbound</td>
<td>Static</td>
<td>UDP</td>
<td>Multicast pairing</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>4443</td>
<td>Bidirectional</td>
<td>Static</td>
<td>TCP/TLS</td>
<td>Web server for peripheral device software downloads and log uploads</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>5127</td>
<td>Outbound</td>
<td>Static</td>
<td>TCP</td>
<td>Poly usage data collection</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6514</td>
<td>Outbound</td>
<td>Static</td>
<td>TLS</td>
<td>Remote logging</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>7080</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td>Web services</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>7081</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td>Web services</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>16384–32764</td>
<td>Bidirectional</td>
<td>Dynamic</td>
<td>UDP</td>
<td>RTP/RTCP (video and audio streams)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>18888</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td>Modular room messaging</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Various 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):

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom StereoSurround</td>
<td>Enables Polycom StereoSurround software for all calls.</td>
</tr>
<tr>
<td></td>
<td>Note: Enabling this setting disables Polycom Acoustic Fence technology and vice versa.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Sound Effects Volume</td>
<td>Sets the volume level of the ringtone and user alert tones.</td>
</tr>
<tr>
<td>Ringtone</td>
<td>Specifies the ringtone for incoming calls.</td>
</tr>
<tr>
<td>User Alert Tones</td>
<td>Specifies the tone for user alerts.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audio Mute Auto-Answered Calls</td>
<td>Specifies whether to automatically mute incoming calls.</td>
</tr>
<tr>
<td>Note:</td>
<td>You must first enable Auto Answer Point-to-Point Video in Call Settings to use this feature.</td>
</tr>
<tr>
<td>Enable M-Mode</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Keyboard Noise Reduction and NoiseBlock</td>
<td>Enables Poly NoiseBlockAI, which during calls eliminates background and extraneous sounds in common working environments when no one is talking. Note: This setting is disabled when you enable M-Mode. If you use an external echo canceller, keyboard noise reduction is not available.</td>
</tr>
<tr>
<td>Enable Join and Leave Tones</td>
<td>The system plays a tone when someone joins or leaves a conference call.</td>
</tr>
<tr>
<td>Transmission Audio Gain (dB)</td>
<td>Specifies the audio level (in decibels) that the system transmits sound. Unless otherwise advised, you should set this value to 0 dB.</td>
</tr>
<tr>
<td>Enable Audio Mute Reminder</td>
<td>Specifies if the system displays a notification that the microphones are muted when it detects someone speaking.</td>
</tr>
</tbody>
</table>

Related Links
Configure Sleep Settings on page 28
Test Speakers on page 97

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.
  - **3.5 mm** (for the G7500 system only): 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):

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stereo Mode</td>
<td>Positions the audio input within the left and right channels. <strong>Left</strong> sends all of the audio to the left channel. <strong>Right</strong> sends all of the audio to the right channel. For Poly table microphone and ceiling microphones, <strong>Left+Right</strong> sends audio from one microphone element to the left channel and audio from a second element to the right channel.</td>
</tr>
<tr>
<td>Autorotation</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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 0.6 m (2 ft) to 2 m (6.5 ft) 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 21
Fix Polycom Acoustic Fence Issues with G7500 on page 99

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

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 0 for the narrowest beam (+/- 12 degrees) or 10 for the widest beam (+/- 60 degrees).
   - 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 (+/- 10 degrees) or 10 for the widest beam (+/- 60 degrees).

Specify the Primary and Fence Microphones
To use Polycom Acoustic Fence technology with your G7500 system, you need a primary microphone to pick up audio and one or more fence microphones to define the audio boundary.
The system considers the first microphone you pair as the primary microphone. By default, a microphone pairs to the system when you connect it (unless you’ve disabled automatic pairing). You can connect up to three microphones directly to your system.

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

**Procedure**

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

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

   2. Connect the other microphone(s).

**Related Links**

Poly G7500 System Ports on page 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.

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

Procedure

1. In the system web interface, go to Audio/Video > Audio > Audio Input > 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 from **Playback Options**.
   - **Playback to All Locations** (Default): Select this option if you’re sending audio from a device.
     - The 3.5 mm stereo input is heard on the system's speakers and at far sites.
     - Mute control and echo cancellation aren’t available.
   - **Playback to Far Sites**: Select this option if you’re using an external digital signal processor (DSP), such as Polycom SoundStructure, which provides mute controls and echo cancellation.
     - The 3.5 mm stereo input is heard at far sites only when the system is in a call (there is no video content association).
     - Mute control and echo cancellation aren’t available through the system.
   - **Playback to Far Sites, Mute Controlled**: Select this option if you want to, for example, share music from a mobile phone to call participants.
     - The 3.5 mm stereo input is heard only at far sites (there is no associated video content).
     - You can mute audio but echo cancellation isn’t available.
   - **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.)
     - The 3.5 mm stereo input is heard at far sites but not on the system’s speakers.
     - You can mute audio and echo cancellation is enabled.
     - Mic-level inputs aren’t supported.

Using Poly Trio Microphones

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

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

- Studio X50 and Studio X30 built-in microphones
- Poly Trio Expansion Microphones

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 StereoSurround software isn’t available.
- The audio input level (mono channel meter) displays in the local interface and system web interface.
Related Links

Pairing a Poly Trio on page 19
Updating a Paired Poly Trio on page 75

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 software isn’t available.
▪ The audio input level (mono channel meter) displays in the local interface and system web interface.

Related Links
Poly Microphone IP Adapter on page 23

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Audio Volume</td>
<td>Sets the main audio output volume level going to the speakers.</td>
</tr>
<tr>
<td>Bass</td>
<td>Sets the volume level for low frequencies without changing the master audio volume.</td>
</tr>
<tr>
<td>Treble</td>
<td>Sets the volume level for high frequencies without changing the master audio volume.</td>
</tr>
</tbody>
</table>

**Choose Speakers When Paired with Poly Trio**

When you pair a Poly Trio system with your video system, you can choose the Poly Trio system as an audio output option for the room.

**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.

   You can toggle this setting while in a call.

**Related Links**
- [Pairing a Poly Trio](#) on page 19
- [Updating a Paired Poly Trio](#) on page 75

**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 X50 and Studio X30 don'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 port (except USB-C).

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 when no other microphones are connected 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
- Configure Camera Tracking Settings for Studio X50 or Studio X30
- Configure Camera Tracking Settings for G7500
- Configure Video Input Settings

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

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

HDMI I/O

Your system has HDMI input and output ports.

Your system has the following HDMI connections:

- Output for connecting the primary system monitor (Monitor 1)
- Output for connecting the secondary system monitor (Monitor 2)
  The Studio X30 system doesn't have a second HDMI output.
- Input for content sharing, including audio streaming

Note the following:

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

Polycom claims no responsibility or liability for the quality, performance, or reliability of third-party HDMI cables, HDMI splitters, or HDMI USB adapters.
Polycom recommends working with your A/V integrator or partner who understands the unique requirements in your environment.

**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**

<table>
<thead>
<tr>
<th>Output</th>
<th>Resolution</th>
<th>Frame Rates (fps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UHD (4K)</td>
<td>3840 × 2160p</td>
<td>25, 30, 50, 60</td>
</tr>
<tr>
<td>FHD</td>
<td>1920 × 1080p</td>
<td>50, 60</td>
</tr>
</tbody>
</table>

**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.

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

<table>
<thead>
<tr>
<th>Output</th>
<th>Resolution</th>
<th>Frame Rates (fps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FHD</td>
<td>1920 × 1080p</td>
<td>50, 60</td>
</tr>
</tbody>
</table>

**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 Input Resolutions**

Your system supports the following monitor resolutions for HDMI input.

**Supported HDMI Input Resolutions and Frame Rates**

<table>
<thead>
<tr>
<th>Input</th>
<th>Resolution</th>
<th>Frame Rates (fps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UHD (4K)</td>
<td>3840 × 2160p</td>
<td>24, 25, 30</td>
</tr>
<tr>
<td>FHD</td>
<td>1920 × 1080p</td>
<td>50, 60</td>
</tr>
<tr>
<td>HD</td>
<td>1280 × 720p</td>
<td>50, 60</td>
</tr>
</tbody>
</table>

**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):

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Monitor</td>
<td>Specifies monitor settings.</td>
</tr>
<tr>
<td></td>
<td>• Automatic: (Default) Detects the highest-supported resolution of the connected monitors. When you select this option, the Resolution setting is disabled.</td>
</tr>
<tr>
<td></td>
<td>• Manual: You can choose the monitor Resolution.</td>
</tr>
<tr>
<td></td>
<td>• Off: Disable this monitor (not available for Monitor 1).</td>
</tr>
<tr>
<td>Note:</td>
<td>To use 4K resolution, make sure you set Monitor 2 to Off.</td>
</tr>
</tbody>
</table>

| 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 73

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Other Participants In a Call to Control Your Camera</td>
<td>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).</td>
</tr>
<tr>
<td>Power Frequency</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Camera Preset Snapshot Icons</td>
<td>Enables the use of snapshot icons that represent camera presets. To see a preset icon, you must enable this setting before configuring the preset.</td>
</tr>
</tbody>
</table>
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera Sleep Mode</td>
<td>Specifies a sleep mode for your camera.</td>
</tr>
<tr>
<td><strong>Fast Wake Up</strong></td>
<td>The camera provides an image as soon as the monitor wakes. While asleep, the camera faces forward.</td>
</tr>
<tr>
<td>▪ When you set sleep <strong>Display to Black</strong>, an image more quickly displays, but be aware that this uses maximum power.</td>
<td></td>
</tr>
<tr>
<td>▪ When you set sleep <strong>Display to No Signal</strong>, the display synchronizes with the system. This can take a few seconds but may conserve energy depending on the monitor.</td>
<td></td>
</tr>
<tr>
<td><strong>Save Energy</strong></td>
<td>Puts the camera into standby mode to save power (the camera spins to the rear and faces down).</td>
</tr>
<tr>
<td>▪ When you set sleep <strong>Display to Black</strong>, it takes a few seconds for the camera to send an image.</td>
<td></td>
</tr>
<tr>
<td>▪ When you set sleep <strong>Display to No Signal</strong>, the camera is already sending an image by the time the display synchronizes with the system.</td>
<td></td>
</tr>
</tbody>
</table>

3. Select **Save**.

**Related Links**
- [Update Poly HD CI Cameras](#) on page 78
- [Configure Sleep Settings](#) on page 28

---

**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.

**Procedure**

1. In the system web interface, go to **Audio/Video > Video Inputs**.
2. Go to **Input 1** and specify a camera **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 to each other.
     ◦ 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.
Configuring Video and Camera Settings

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 Input 1 and specify a camera 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 handle all camera control 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.

Configure Video Input Settings

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

Note: The system doesn’t display settings that don’t apply to your camera.

Procedure

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

Each source has different settings. For example, a **People** source has pan, tilt, zoom, and near/far camera control settings, while a **Content** source doesn’t.

3. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input format</td>
<td>Specifies the source type of the device. This setting is read-only unless the system doesn’t detect the device.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for the camera or device.</td>
</tr>
<tr>
<td>Model</td>
<td>Displays the type of device connected to the system.</td>
</tr>
<tr>
<td>Optimized for</td>
<td>Specifies optimization preferences for the video input.</td>
</tr>
<tr>
<td>▪ Sharpness</td>
<td>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.</td>
</tr>
<tr>
<td>▪ Motion</td>
<td>Gives preference to frames per second over resolution.</td>
</tr>
<tr>
<td>Orientation</td>
<td>Specifies whether to invert the camera display for a Studio X30 system that’s mounted below a monitor.</td>
</tr>
<tr>
<td>Backlight Compensation</td>
<td>Specifies if the camera automatically adjusts for a bright background. Backlight compensation is best used in situations where the subject appears darker than the background.</td>
</tr>
<tr>
<td>Skin Enhancement</td>
<td>Enables or disables natural skin color enhancements for participants.</td>
</tr>
<tr>
<td>Wide Dynamic Range</td>
<td>Enables or disables re-exposure according to the framed area instead of full view.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>White Balance</td>
<td>Specifies how the camera compensates for light source variations in the room. Select <strong>Auto</strong>, <strong>Manual</strong>, or a color temperature value.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Auto</strong>: Recommended for most situations. It calculates the best white balance setting based on lighting conditions in the room.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Manual</strong>: Use this setting for rooms where the <strong>Auto</strong> and fixed values don't provide acceptable color reproduction.</td>
</tr>
<tr>
<td></td>
<td>When you set this option to <strong>Manual</strong>, fill the camera’s field of view with a flat white object, such as a piece of paper. For best results, the</td>
</tr>
<tr>
<td></td>
<td>object should be uniformly illuminated with light that is representative of the room lighting used in the conference, rather than light from a</td>
</tr>
<tr>
<td></td>
<td>display, another area, or a shadow. After the object is in place, select <strong>Calibrate</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Color Temperature Value</strong>: The color temperature values, measured in degrees Kelvin, correspond to the color of ambient light in a room.</td>
</tr>
<tr>
<td></td>
<td>Because the available color temperature values vary by camera, this list is a sampling of some of the values you might see in the interface:</td>
</tr>
<tr>
<td></td>
<td>- 3200K (warm office fluorescent)</td>
</tr>
<tr>
<td></td>
<td>- 3680K (tungsten bulb)</td>
</tr>
<tr>
<td></td>
<td>- 4160K (cool office fluorescent)</td>
</tr>
<tr>
<td></td>
<td>- 5120K (neutral daylight)</td>
</tr>
<tr>
<td></td>
<td>- 5600K (cool daylight)</td>
</tr>
<tr>
<td>Framing Size</td>
<td>Specifies the framing view.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Wide</strong>: Establishes a wide view of meeting participants.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Medium</strong>: (Default group framing view) Establishes a medium view of meeting participants.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Tight</strong>: Establishes a close-up view of meeting participants.</td>
</tr>
<tr>
<td>Sharpness</td>
<td>Adjusts the video’s overall clarity.</td>
</tr>
<tr>
<td>Brightness</td>
<td>Adjusts the video brightness.</td>
</tr>
<tr>
<td>Color Saturation</td>
<td>Adjusts the color saturation.</td>
</tr>
</tbody>
</table>

4. Select **Save**.
Sharing Content

Topics:

- Default Option for Sharing Content

Your system provides several ways to share and annotate content.

Default Option for Sharing Content

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

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

Topics:

- Configure Dual Monitor Display Settings

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

Configure Dual Monitor Display Settings

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

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

The Studio X30 system supports only one monitor.

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self View Size</td>
<td>Specifies how the self view window displays when others join a call.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Corner</strong>: Displays the self view in the corner of Monitor 2.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Full Screen</strong>: Displays the self view on the entire screen of Monitor 2.</td>
</tr>
<tr>
<td>Content Display</td>
<td>Specifies whether to display content on one or two monitors.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Single</strong>: Display content on Monitor 2 and people on Monitor 1.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dual</strong>: Display people and content on Monitor 1 and content only on Monitor 2.</td>
</tr>
</tbody>
</table>

Related Links

Configure Monitor Settings on page 65
System Maintenance

Topics:

- Unlock System Settings
- Updating Software
- Restart the System
- Change Conferencing Partner
- 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
- Software package you obtain from Polycom Support and upload with a USB flash drive
- Provisioning service (for example, RealPresence Resource Manager)

**Related Links**
[Using a Provisioning Service](#) on page 30
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.

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.

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

Related Links

Pairing a Poly Trio on page 19
Using Poly Trio Microphones on page 59
Choose Speakers When Paired with Poly Trio on page 61

Updating Software in the System Web Interface

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

Choose How to Get Software Updates

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

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

Procedure

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

<table>
<thead>
<tr>
<th>Software Update Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Support Site</td>
<td>A software server hosted by Polycom.</td>
</tr>
<tr>
<td>Software Update Method</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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
  - g7500
    - 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 |

| 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 30

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 Software with a USB Flash Drive
You can update the software of your system and some of its paired devices (not a TC8 device) with a USB flash drive.

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

Procedure
1. Get the software package you want to install from Polycom Support.
2. Save the package to the root directory of a USB flash drive and unzip the file.
   To successfully update everything, you must have this exact folder structure:
   * eecube
     * Config
     * image.zip
     * version
   * g7500
Connect the USB flash drive to a USB port on the back of the system. If the system detects the USB flash drive, a prompt displays on the monitor to confirm that you want to update the software.

Follow the onscreen instructions to complete the update.

Update Poly HDCI Cameras

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

HDCI cameras only apply to the G7500 system.

Procedure

1. In the system web interface, go to Audio/Video > Video Inputs.
2. Select Enable Camera Update.

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

Related Links
Configure General Camera Settings on page 66

Manually Downgrade Software in the System Web Interface

You can downgrade your system software and the software of some of its 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 Conferencing Partner**

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

Poly strongly recommends you perform a system reset instead to change your conferencing provider as this is an experimental feature. After system resets, select a new conferencing provider during setup.

**Note:** The system doesn’t retain previously configured settings after making this change.
Procedure
1. In the system web interface, go to General Settings > Provider.
2. Select a conferencing application from Choose a Provider.
   The system automatically restarts.

Reset System Settings
You can reset your system to its default configuration settings.

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

Resetting your system deletes all but the following data:
- Current software version
- User-installed PKI certificates
- Logs

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

Note: System resets restore 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 the latest major software version (x.0).

The system doesn’t save the following data with a factory restore:
- Current software version
- Logs
- User-installed PKI certificates
- Local directory entries
- Call detail record (CDR)

Procedure
1. Disconnect the power supply to turn off the system.
2. Do one of the following:
3. While continuing to hold the restore button, reconnect the power supply to turn the system on.
4. When the system LED indicator light blinks amber, stop pressing the restore button.

**Related Links**

LED Status Indicators on page 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 21
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.

   ![Diagram of microphone and sensor location]

   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 23
Troubleshooting

Topics:

- Logs
- SNMP Reporting
- Checking System Status
- Check Provisioning Results
- Paired IP Devices
- Audio Tests
- Can't Wake the System by Touching the Monitor
- 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
- Zero Touch Onboarding Connection Fails During Initial Setup or After Reset
- Verify Poly Lens Registration Status
- Lighting Conditions Impact Picture Quality

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.

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Percent Filled</td>
<td>Displays as a percentage how full the logs are. When the logs are full, system deletes the oldest entries.</td>
</tr>
<tr>
<td>Percent Filled Threshold</td>
<td>Reaching the threshold you configure here creates a log entry and automatically transfers logs if you set Transfer Frequency to Auto At Threshold.</td>
</tr>
</tbody>
</table>
| 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.  
| 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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Level</td>
<td>Sets the minimum log level of messages stored in the system’s flash memory.</td>
</tr>
<tr>
<td></td>
<td><strong>Debug</strong> logs all messages, while <strong>Warning</strong> logs the fewest number of messages.</td>
</tr>
<tr>
<td></td>
<td>It's recommended that you use the default value <strong>Debug</strong>.</td>
</tr>
<tr>
<td></td>
<td>When you enable <strong>Enable Remote Logging</strong>, the log level is the same for both remote and local logging.</td>
</tr>
</tbody>
</table>

3. Select Save.

Download Logs

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

Procedure

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

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

Configure Remote Logging

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

Remember the following about remote logging with your system:

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

Procedure

1. In the system web interface, go to Diagnostics > Logs.
2. Configure the following settings:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Remote Logging</td>
<td>Specifies whether remote logging is enabled. Enabling this setting causes the system to send each log message to the specified server in addition to logging it locally. The system immediately begins forwarding its log messages after you click <strong>Save</strong>. The system supports remote logging encryption using TLS. If you use UDP or TCP transport, Poly recommends remote logging only on secure, local networks.</td>
</tr>
<tr>
<td>Remote Log Server Address</td>
<td>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 <strong>Remote Log Server Transport Protocol</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Remote Log Server Transport Protocol:</strong></td>
</tr>
<tr>
<td></td>
<td>• UDP: 514</td>
</tr>
<tr>
<td></td>
<td>• TCP: 601</td>
</tr>
<tr>
<td></td>
<td>• TLS: 6514</td>
</tr>
<tr>
<td></td>
<td>You can specify the address and port in the following formats:</td>
</tr>
<tr>
<td></td>
<td>• IPv4 address: 192.0.2.0:&lt;port&gt;, where &lt;port&gt; is the elective destination port number in the 1-65535 range.</td>
</tr>
<tr>
<td></td>
<td>• FQDN: logserverhost.company.com:&lt;port&gt;, where &lt;port&gt; is the elective destination port number in the 1-65535 range.</td>
</tr>
<tr>
<td>Remote Log Server Transport Protocol</td>
<td>Specifies the transport protocol for sending logs to a remote server:</td>
</tr>
<tr>
<td></td>
<td>• UDP</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td>• TLS (secure connection)</td>
</tr>
</tbody>
</table>

3. Select **Save**.

**Sample Log File**

The following code shows an example of a system log file.

```plaintext
2018-10-19 13:53:08 Kernel.Debug 10.223.73.18 1
2018-10-19T18:53:08.626000+00:00 DeviceName ProductName -- [NXLOG@14506 EventReceivedTime="2018-10-19 18:53:08" SourceModuleName="plcmlog" SourceModuleType="im_file"] CEng: RouteProc[0]: RouteReceived - VID videoroute set 0 monI 1920 1080 HDMI 60 Progressive vout1 0 0 1920 1080 0 none 0 0 0 0
2018-10-19 13:53:08 Kernel.Info 10.223.73.18 1
```
SNMP Reporting

The system supports SNMP versions 1, 2c, and 3.

SNMP can provide the following event information about your system:

- Alert conditions located on the system alert screen
- Details of jitter, latency, and packet loss
- System power on
- Successful or unsuccessful administrator login
- Call fail for a reason other than a busy line
- User help request
- Video or audio call connection or disconnection

**Note:** Poly doesn’t support SNMP write operations for configuring or provisioning systems.

SNMPv3 does the following:

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

Related Links

[Securing the System](#) on page 37

Configure SNMP

You can monitor your system remotely with SNMP.

**Procedure**

1. In the system web interface, go to **Servers > SNMP**.
2. Configure the following settings:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SNMP</td>
<td>Enables administrators to monitor the system remotely using SNMP.</td>
</tr>
<tr>
<td>Enable Notifications</td>
<td>Enables MIB notifications.</td>
</tr>
<tr>
<td>Version1</td>
<td>Enables your system to use the SNMPv1 protocol. Due to security issues, Poly recommends that you don’t enable this setting.</td>
</tr>
<tr>
<td>Version2c</td>
<td>Enables your system to use the SNMPv2c protocol. Due to security issues, Poly recommends that you don’t enable this setting.</td>
</tr>
<tr>
<td>Version3</td>
<td>Enables your system to use the SNMPv3 protocol. Enabled by default, you can’t configure other SNMPv3 settings unless this is on.</td>
</tr>
<tr>
<td>Read-Only Community</td>
<td>Specifies the SNMP community string for your system. For security reasons, don’t use the default community string (public).</td>
</tr>
<tr>
<td>Note:</td>
<td>Poly doesn’t support SNMP write operations for configuring or provisioning systems. The community string is for read operations and outgoing SNMP traps.</td>
</tr>
<tr>
<td>Contact Name</td>
<td>Specifies the name of the person responsible for remotely managing the system.</td>
</tr>
<tr>
<td>Location Name</td>
<td>Specifies the system location.</td>
</tr>
<tr>
<td>System Description</td>
<td>Provides details about the system.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the User Security Model (USM) account name for SNMPv3 message transactions. The maximum length is 64 characters.</td>
</tr>
<tr>
<td>Authentication Algorithm</td>
<td>Specifies the type of SNMPv3 authentication algorithm used.</td>
</tr>
<tr>
<td></td>
<td>• SHA</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Specifies the SNMPv3 authentication password. The maximum length is 48 characters.</td>
</tr>
<tr>
<td>Privacy Algorithm</td>
<td>Specifies the cryptographic privacy algorithm for SNMPv3 packets.</td>
</tr>
<tr>
<td></td>
<td>• CFB-AES128</td>
</tr>
<tr>
<td></td>
<td>• CBC-DES</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.</td>
</tr>
</tbody>
</table>
| 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                                                                       |
| Destination Address1      | Specifies the IP addresses of SNMP managers where SNMP traps are sent.      |
| Destination Address2      | Each address has four settings:                                             |
| Destination Address3      | • 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Alerts</td>
<td>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.</td>
</tr>
<tr>
<td>Call Control</td>
<td>Displays status of the Auto-Answer Point-to-Point Video setting.</td>
</tr>
<tr>
<td>LAN Properties</td>
<td>Displays network connection status.</td>
</tr>
<tr>
<td>Servers</td>
<td>• Displays the gatekeeper and SIP registrar server status.</td>
</tr>
<tr>
<td></td>
<td>• Displays the active global directory server or LDAP server status.</td>
</tr>
<tr>
<td></td>
<td>• Displays the provisioning or calendaring service status (if enabled).</td>
</tr>
<tr>
<td>Peripheral Devices</td>
<td>Connection status of peripheral devices.</td>
</tr>
</tbody>
</table>
Check Status in the System Web Interface

Verify your system status in the system web interface.

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

Check Provisioning Results

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

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

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

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

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

Related Links
Register the System with a Provisioning Service on page 30

Paired IP Devices

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

IP Device Can’t Pair to the Video System

Symptom:
You may notice one or both of the following depending on the device:
- After powering on the TC8 device, it doesn’t automatically pair with the video system.
- You can’t manually pair the device from the Available Devices list in the video system web interface.

Problem:
Network traffic on TCP port 18888 is blocked.
IWorkaround:

Procedure
   » Allow traffic on TCP port 18888.

**IP Device Doesn’t Display On the Available Devices List**

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

**Problem:**
The are a few possible causes for this issue:
   ▪ The device and video system aren’t on the same subnet.
   ▪ The network switch isn’t allowing UDP broadcast traffic forwarded to multicast address 224.0.0.200 on port 2000.
   ▪ The device is paired with another video system.

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

**Procedure**
1. Make sure the device and video system are on the same subnet.
   If needed, work with your network administrator.
2. Allow traffic to 224.0.0.200 on UDP port 2000.
3. Make sure the device isn’t paired with another video system. If it is, unpair the device.
4. In the TC8 device interface, go to **Settings > Reset** and select **Reset**.
   Your device resets to its default configuration settings, which unpairs it from the video system.

**Paired IP Device is Disconnected**

**Symptom:**
You paired a device with your video system but can’t use it. On the system web interface **Device Management** page, you see that the device is **Disconnected**.

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

Workaround:
Complete each step until you fix the issue.

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

**IP Device Paired to Inaccessible Video System**

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

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

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

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

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

**Procedure**
1. In the TC8 device interface, go to **Settings** > **Reset** and select **Reset**.
   Your device resets to its default configuration settings, which unpairs it from the video system.
2. In the system web interface, go to **General Settings** > **Device Management**.
3. Under **Connected Devices**, find the device by its MAC address (for example, **00e0db4cf0be**) and select **Unpair**.
   The device you're unpairing should have **Unavailable** status.

**Degraded Audio with Paired Poly Trio**

**Symptom:**
In setups that include a paired Poly Trio, the audio seems out of sync or occasionally drops.

**Problem:**
If multicast traffic of Precision Time Protocol (PTP) packets is blocked on your network, audio quality between the paired video system and phone degrades over time.

**Workaround:**

**Procedure**
» Allow multicast on UDP ports 319 and 320.
No Audio on Paired Poly Trio

Symptom:
You may notice one or both of the following with a Poly Trio that’s paired to a video system:
- You can’t hear anything coming from the phone speakers.
- Far-site call participants either can’t hear or have trouble hearing audio.

Problem:
If you’re hearing audio from the video system or monitor speakers, try changing your speaker settings. If the Poly Trio speakers and microphones aren’t working, make sure network traffic on UDP ports 16384-32764 isn’t blocked. Audio to and from the phone doesn’t work if these ports aren’t open.

Workaround:
Complete each step until you’ve fixed the issue.

Procedure
1. In the system web interface, go to **Audio/Video** > **Audio** > **Audio Output**.
2. For **Speaker Options**, select **Phone Speakers**.
3. Allow traffic on UDP ports 16384-32764.

IP Audio Device is Disconnected from G7500

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

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

Workaround:
Reconnect cables or factory restore your hardware. Complete each step until you fix the issue.

Procedure
1. Check the device LED. If it isn’t blinking blue, reconnect the LAN cable to the device and system.
2. If the device is a Poly Microphone IP Adapter, also reconnect its power supply cables.
3. Perform a factory restore on the device.
4. Perform a factory restore on the system.
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 54

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.

Can’t Wake the System by Touching the Monitor

Symptom:
Touching the monitor doesn’t wake your system.

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

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

LED Status Indicators for the System LAN Ports

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

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

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

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

* - 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 32
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 \( \circ \) ports on the back of your system.
2. Reconnect the microphones (connect the primary microphone first).

Related Links
Polycom Acoustic Fence on page 56

Test Connection with Another System

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

Procedure

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

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

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

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

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

Checking the Web Proxy Configuration

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

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

Related Links
Web Proxies on page 49

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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>File successfully downloaded to your system.</td>
</tr>
<tr>
<td>In Progress</td>
<td>File is downloading to your system.</td>
</tr>
<tr>
<td>WPAD Failed</td>
<td>File download URL wasn’t discovered using DHCP option 252.</td>
</tr>
<tr>
<td>Download Failed</td>
<td>File didn’t download.</td>
</tr>
<tr>
<td>Expired</td>
<td>File is expired.</td>
</tr>
</tbody>
</table>

Verify the PAC File Contents

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

Procedure
1. In the system web interface, go to Network > Primary Network > Web Proxy Settings.
2. Select Download PAC File.
   This option isn’t available if the PAC File Status doesn’t indicate Success.

Zero Touch Onboarding Connection Fails During Initial Setup or After Reset

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

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

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

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 16
Register Later on page 17

Lighting Conditions Impact Picture Quality

Symptom:
When using the system in a personal environment, where lighting may not be optimal, the picture quality is impacted.

Problem:
The default video input settings are tuned for well-lit office environments.

Workaround:
Adjust the camera settings in the system web interface. Each environment differs; the amount you adjust the brightness and sharpness depends on your unique lighting and placement situations.
Procedure

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

2. Adjust the Brightness slider.
   Increase brightness in low light environments and decrease brightness in environments with strong single sources of light.

   **Note:** Increasing and decreasing brightness may cause you to lose fine detail in areas with excess lighting or shadows.

3. Adjust the Sharpness slider.
   Increasing the sharpness provides more detail.

4. Adjust the Color Saturation slider.
   Increasing color saturation can correct washed out colors in low light situations.

5. Select Save.