Poly Studio V52 Administrator Guide

SUMMARY

This guide provides administrators with information about configuring, maintaining, and troubleshooting the featured product.

Legal information

Copyright and license

Trademark credits

All third-party trademarks are the property of their respective owners.

Privacy policy

HP complies with applicable data privacy and protection laws and regulations. HP products and services process customer data in a manner consistent with the HP Privacy Policy. Please refer to HP Privacy Statement.

Open source software used in this product

This product contains open source software. You may receive the open source software from HP up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to HP of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact HP by email at ipgoopensourceinfo@hp.com.

Table of contents

1 About this guide 1

Audience, purpose, and required skills 1

Icons used in Poly documentation 1

2 Getting Started 2

Poly Studio V52 Features and Capabilities 2

Poly Studio V52 Hardware 2

Poly Studio V52 System Ports 3

Poly Studio V52 Privacy Cover 3

Setting up the Studio V52 4

Setting Up the System 4

Set Up Your Studio V52 4

Powering the System On and Off 4

Navigating the System 5

Access the System Web Interface 5

Locate the system IP address using a monitor 5

Change Administrator Credentials 5

LED Status Indicators for the Studio V52 System 6

3 Configuring General Settings 7

Name the System 7

Provide Contact Information 7

Set the Date and Time 8

Set the System Location 8

Set the Local Interface Language 9

Change LED Bar Brightness 9

System Usage Data Collected by Poly 9

Send Usage Data to Poly 9

4 Using a Provisioning Service 11

Register the System with the Poly Lens Provisioning Service 11

De-register the System from the Poly Lens Provisioning Service 12

Register the System with Poly Clariti Manager Provisioning Service 12

Download a Provisioning Template Configuration File 13

Register the System Using DHCP Auto Discovery 13

5 Configuring Network Settings 14

Configuring Wired LAN Settings 14

Automatically Obtain IPv4 Address Settings 14

Manually Configure IPv4 Address Settings 14
Automatically Obtain IPv6 Address Settings 14
Manually Configure IPv6 Address Settings 15
Manually Assign a Host Name and Domain Name 15
Manually Configure DNS Settings 16
Configure System VLAN Settings 16
Configure System 802.1X Settings 16
Configure Wired LAN Options 17
LLDP and LLDP-MED Support 18
LLMP-MED Information Discovery 18
Behavior When LLDP is Enabled 19
Enable LLDP 19
Configure Wi-Fi as the Primary Network 19
Configure Wi-Fi Settings 20
6 Configuring Audio Settings 22
Configure General Audio Settings 22
Connect a USB Audio Device to the System 22
Live Microphone Switching 22
Polycom Acoustic Fence 23
Configure Polycom Acoustic Fence 23
Sound Reflection Reduction 23
Enable Sound Reflection Reduction 24
Configure Audio Output Settings 24
7 Configuring Video and Camera Settings 25
HDMI Ports 25
Supported HDMI Output Resolutions for Single-Monitor Setups 25
Monitors with CEC 25
Disable CEC 26
Enable CEC 26
Configure General Camera Settings 26
Poly DirectorAI Perimeter 27
Define the DirectorAI Perimeter 27
Reset Camera Settings to Defaults 27
Configuring Video Input Settings 27
Configure General Video Input Settings 28
Adjust the White Balance 28
Configure Camera Tracking Settings for Poly Studio V52 Systems 28
8 System Maintenance 30
Locate the System Serial Number 30
Updating Software 30
Updating Software in the System Web Interface 30
Choose How to Get Software Updates 30

Update Software Using a USB Flash Drive 31
Update the Poly Bluetooth Remote Control Firmware 31
Downgrading Software 31
Manually Downgrade Software in the System Web Interface 32
Downgrade Software with a USB Flash Drive 32
Scheduled Auto Restart 32
Configure Scheduled Auto Restart 32
Restart the System 32
Reset System Settings 33
Factory Restore the Studio V52 33
9 Troubleshooting 35
Studio V52 Doesn't Receive an IP Address When Connected to a Netgear Smart Switch 1G Port 35
10 Securing the System 36
Managing System Access 36
Local Accounts 36
Configure Password Policies 36
Create Local Administrator Credentials 37
Change Administrator Credentials 37
Configure Account Lockout Settings 38
Enable External Authentication 38
Configure System Access Settings 39
Command-Line API Access 40
Enable Command-Line API Access Over SSH 40
Configure the SSH Port Lock 40
Enable Command-Line API Access Over Telnet 40
Disable the Telnet Password 41
Locking the Telnet Port 41
Disable Command-Line API Access 41
Configure the System Web Interface Port Lock 41
Disable USB-A Port 42
Detecting Intrusions 42
PKI Certificates 42
Create a Certificate Signing Request 43
Configure Certificate Validation Options 44
Install a Certificate 45
View a Certificate 45
Delete a Certificate 45
Certificate Revocation 46
Manually Upload a CRL 46
Delete a CRL 46
System Allow List 47
Add IP Addresses to the Allow List 47
Delete IP Addresses from the Allow List 47
IPv4 Address Formats 47
IPv6 Address Formats 48

Set Up a Security Banner 48
Simple Certificate Enrollment Protocol (SCEP) 48
Install a SCEP Certificate 48
Configuring Simple Certificate Enrollment Protocol (SCEP) 49
Web Proxies 49
Enable the System to Use a Web Proxy 50
Set Up Automatic Web Proxy Configuration 50
Set Up Semi-Automatic Web Proxy Configuration 51
Manually Update the PAC File on the System 51
Manually Configure a Web Proxy 51
Sample PAC File 51
View Connections to the System 52
System Port Usage 52
11 Diagnostic Functions 54
Check Provisioning Results 54
Checking System Status 54
Check Status in the Local Interface 55
Checking the Web Proxy Configuration 55
PAC File Status 55
Verify the PAC File Contents 55
Logs 56
Consolidated System and Peripheral Device Logs 56
Configure Log Preferences 56
Configure Log Level 57
Retrieve Log Files 58
Transfer Logs to a USB Flash Drive 58
Configure Remote Logging 59
Configure Logging to System Internal Storage 60
Sample Log File 60
Run a Trace Route 61
SNMP Reporting 62
Configure SNMP 62
Download MIBs 64
Verify Poly Lens Registration Status 64
12 Poly Studio V52 accessibility features 65
13 Getting help 66
HP Inc. addresses 66
Document information 66

1 About this guide

This section provides clarifying information about this guide.

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

Icons used in Poly documentation

This section describes the icons used in Poly Documentation and what they mean.

WARNING! Indicates a hazardous situation that, if not avoided, **could** result in serious injury or death.

CAUTION: Indicates a hazardous situation that, if not avoided, **could** result in minor or moderate injury.

IMPORTANT: Indicates information considered important but not hazard-related (for example, messages related to property damage). Warns the user that failure to follow a procedure exactly as described could result in loss of data or in damage to hardware or software. Also contains essential information to explain a concept or to complete a task.

NOTE: Contains additional information to emphasize or supplement important points of the main text.

TIP: Provides helpful hints for completing a task.

2 Getting Started

The Poly Studio V52 systems provide a premium USB video bar with advanced features for the most immersive hybrid meetings in medium rooms.

Poly Studio V52 Features and Capabilities

Studio V52 systems support the following features:

- A premium USB video bar with advanced features for the most immersive hybrid meetings in medium rooms
- Sharp 4K, 20MP camera with 95-degree horizontal field of view
- Camera tracking technology that automatically frames the group of people in the room
- Hi-fidelity, built-in stereo microphones that pick up sound within 6.09 m (20 ft) and use spatial audio for life-like presence and clarity
- Poly NoiseBlockAI, which eliminates background and extraneous sound in common working environments
- Dual stereo speakers
- Simple to set up, manage, and use with Poly Lens

Poly Studio V52 Mounting Orientation

You can mount the Studio V52 above or below a display. The Studio V52 doesn't support inverted mounting. For information on mounting the Studio V52, see the *Poly Studio V52 Quick Start Guide*.

Poly Studio V52 Hardware

The following figure displays the hardware features on the Poly Studio V52 system. The table lists each feature numbered in the figure.

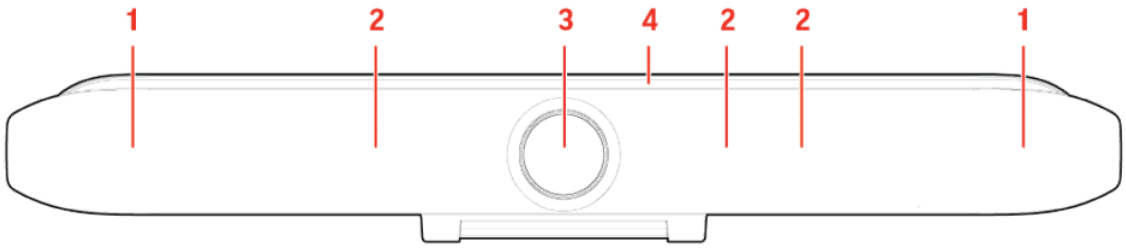


Table 2-1 Poly Studio V52 Feature Descriptions

Ref. Number	Feature	Feature Description
1	Speaker	Stereo audio output

Table 2-1 Poly Studio V52 Feature Descriptions (continued)

Ref. Number	Feature	Feature Description
2	Microphone array	Microphone array that captures audio
3	Camera	Camera with a privacy cover that enables or disables the video input as you choose
4	LED indicators	Indicates the system status and information on the tracked speaker

Poly Studio V52 System Ports

The following illustration and table explain the ports on your Poly Studio V52 system.

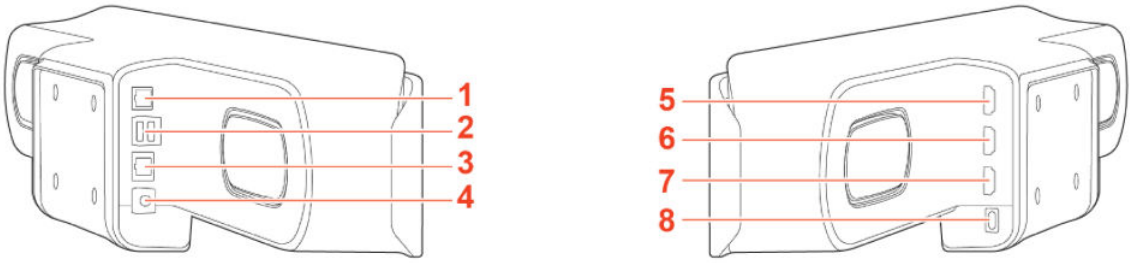
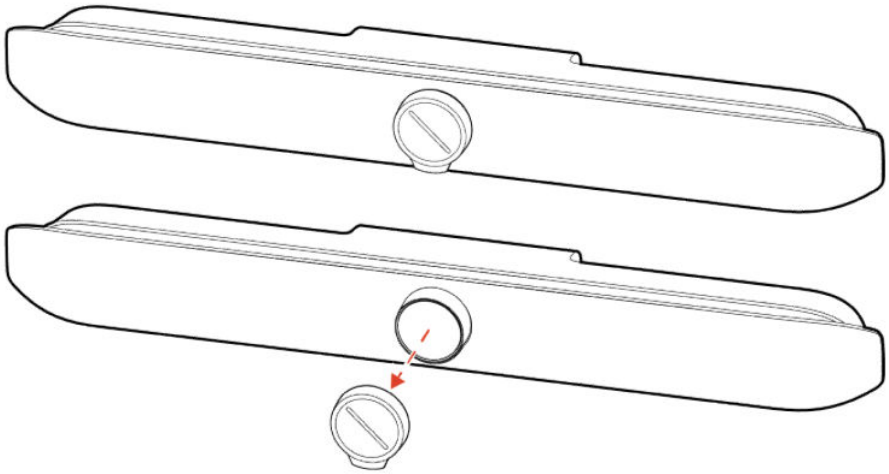


Table 2-2 Poly Studio V52 System Port Descriptions

Ref. Number	Port Description
1	RJ-11 port for external microphone
2	USB-A port. Disabled by default, but configurable to enable.
3	RJ45 Ethernet port
4	Power port
5	HDMI output port 2 (for provisioning support only)
6	HDMI output port 1 (for provisioning support only)
7	Not supported
8	USB-C port

Poly Studio V52 Privacy Cover

The Poly Studio V52 system provides a physical cover that you can place over the camera lens to protect your privacy.



Setting up the Studio V52

The Studio V52 includes a 1.83m (6ft) HDMI cable, a 4.57m (15ft) LAN cable, and a USB-C cable to connect your computer to the Studio V52.

Connect all cables before powering on the system.

You can use your Studio V52 as an external video device on your computer or connect it to a conferencing system that supports USB cameras.

Setting Up the System

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

Set Up Your Studio V52

You can connect your Studio V52 to your computer only using the supplied USB cable. You can also connect Studio V52 to your network and to an external monitor.

NOTE: Before powering on your system, connect the system to your network and connect an optional monitor.

1. Connect the supplied USB cable from the USB-C port on the Studio V52 to your computer.
2. Optional: To view your system IP address, connect a monitor to an HDMI output port of your Poly Studio V52 using the supplied HDMI cable.
3. Optional: Connect the system Ethernet port to your network using the supplied Ethernet cable.
4. Plug the system in to a power source using the supplied power supply cable.

   The system powers on when you plug it in to a power source. If you have a monitor connected to the system, the system IP address displays on the monitor.

Powering the System On and Off

The system powers on when you plug it in to a power source.

Poly recommends the following when powering off or restarting your system:

- Don't restart or power off the system during maintenance activities (for example, while a software update is in progress).
- If a system restart is necessary, use the system web interface, RestAPI, Telnet, or SSH. If possible, avoid using the power cable to restart the system.

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. Local interface is intended only for the initial setup.

1. Open a web browser and enter the system IP address.

   To view the system IP address, connect a monitor to an HDMI output port of your system. The system IP address displays on the monitor.
2. Enter the username (the default is `admin`).
3. Enter the password (the default is the last six characters of your system's serial number).

   The password is case sensitive.

Locate the system IP address using a monitor

Connect your Poly Studio V52 to a monitor and the IP address for Ethernet displays by default.

- Connect a monitor to an HDMI output port of your Poly Studio V52 using the supplied HDMI cable.

  The Poly Studio V52 IP address for the Ethernet displays on the monitor.

Change Administrator Credentials

You can change the administrator username and password to access the system web interface and administrator sections of the local interface.

The default username is `admin` and the default password is the last six characters of the system's serial number.

1. In the system web interface, go to **Security** > **Local Accounts**.
2. Enter the new administrator username in the **Admin ID** field.
3. Select **Change Password**.
4. Enter the current password and then the new password.

   Entering an incorrect current password too many times causes the system to automatically log out and close the session.

5. Select **Save**.

LED Status Indicators for the Studio V52 System

Use the LED on the right side of the system to help you understand the system's behaviors.

Table 2-3 Basic Studio V52 LED Indicators and Status

Indicator	Status
Off	System powered off
Solid white	System is idle and standing by
Pulsing white	Boot initiation in progress
Pulsing amber	Firmware update or factor restore in progress
Blinking blue and white	Bluetooth pairing with a remote control
Solid blue for 3 seconds	Bluetooth paired with a remote control
Solid green	Camera or microphone in use
Solid red	Audio is muted

3 Configuring General Settings

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

Name the System

You can give your system a name.

1. In the system web interface, go to **General Settings** > **System Settings**.
2. Edit the **Device Name**.

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

3. Select **Save**.

Provide Contact Information

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

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

Set the Date and Time

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

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

Table 3-1 Date and time settings

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

Set the System Location

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

NOTE: To avoid power frequency issues with your system, choose a location.

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 3-2 Location settings

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

Set the Local Interface Language

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

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

Change LED Bar Brightness

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

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

System Usage Data Collected by Poly

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

For information about the data that Poly collects, see the system privacy guide.

Send Usage Data to Poly

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

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

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

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

4 Using a Provisioning Service

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

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

- Automatically configure settings
- Automatically update software

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

- Provisioned settings are read-only in the system web interface. Settings that are dependent on provisioned values are read-only or unavailable.
- The system automatically checks for and runs software updates every time it restarts and at an interval set by the service.
- If a registered system fails to detect the service when it restarts or checks for updates, an alert displays on **System Status**.
- If the system loses registration with the service, it continues to use the most recent configuration it received.
- The system looks for provisioning options during initial system setup in the following order: Zero Touch Onboarding, Poly Lens, then DHCP. If the system doesn't find provisioning information for an option, it automatically goes to the next one.

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

Register the System with the Poly Lens Provisioning Service

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

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

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

Setting	Description
Server Address	Address of the system running the provisioning service.
User Name	User ID for registering with the provisioning service.

Setting	Description
Password	Password for registering with the provisioning service.

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

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

De-register the System from the Poly Lens Provisioning Service

Delete your device from the Poly Lens inventory to de-register it. .

For more information see the Poly Lens Help Documentation.

Register the System with Poly Clariti Manager Provisioning Service

Before you can provision a Poly Studio V52 system, you must register it with a provisioning service.

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

For information on how to provision your system with Poly Clariti Manager, see the Poly Clariti Manager Administrator Guide.

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

   The registration fields update automatically if your system detects a provisioning server.
4. **Optional:** If your system didn't detect a provisioning server, complete the following fields (contact your network administrator for help):

Setting	Description
Authentication Type	The type of authentication the system uses to connect to the provisioning server.
Server Address	Address of the system running the provisioning service. The format is `https://<server>/ucservice`. For example, `https://video.myrpp.poly.com/ucservice`.
Domain Name	Domain for registering with the provisioning service. This option doesn't display if you select **Basic** as the authentication type.
User Name	User ID for registering with the provisioning service.
Password	Password for registering with the provisioning service.

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

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

Download a Provisioning Template Configuration File

Template configuration files show how parameters are set on your Poly Studio V52 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 Poly Clariti Manager system, you can use the template to create a UC endpoint configuration profile to associate with your systems. For more information, see the Poly Clariti Manager Administrator Guide.

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.

Register the System Using DHCP Auto Discovery

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

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

- Configure your DHCP server to send the username, password, and URL of your provisioning service in the following format:
  - For Poly Clariti Manager use `https://<shareduserID>:<sharedpassword>@<server>/ucservice`
    For example, `https://mySharedID:mySharedPW@video.example.com/ucservice`
  - For Poly Lens use `https://<ServerUser>:<ServerPassword>@<ServerAddressURL>`
    For example, `https://ServerUser:ServerPassword@txxxx.dm.lens.poly.com`, where xxxx are numeric values from 1 to 9.

5 Configuring Network Settings

Network settings include the Poly Studio V52 system primary (wired LAN) and secondary (Wi-Fi) network configurations.

Configuring Wired LAN Settings

You can set the wired LAN properties for your Poly Studio V52 system.

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.

1. In the system web interface, go to **Network** > **LAN Network** > **IP Addresses**.
2. For **IP Address**, select **Obtain IP address automatically**.

   Some of your IP address settings populate automatically and are read-only.
3. Select **Save**.

Manually Configure IPv4 Address Settings

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

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

   Table 5-1 IP settings

Setting	Description
Your IP Address is	Specifies the system IP address.
Subnet Mask	Specifies the subnet mask assigned to your system.
Default Gateway	Specifies the default gateway assigned to your system.

4. Select **Save**.

Automatically Obtain IPv6 Address Settings

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

You must have a DHCP server deployed in your environment.

⚠ **WARNING!** If your network environment only supports IPv6, you must manually configure a static IPv4 address. For example, manually configure the IPv4 IP address to 192.168.0.4.

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

Manually Configure IPv6 Address Settings

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

⚠ **WARNING!** If your network environment only supports IPv6, you must manually configure a static IPv4 address. For example, manually configure the IPv4 IP address to 192.168.0.4.

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

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

5. Select **Save**.

Manually Assign a Host Name and Domain Name

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

1. In the system web interface, go to **Network** > **LAN Network** > **LAN Options**.
2. Enter or modify the system **Host Name**.

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

   IPv4 networks: The system sends the host name to the DHCP server to attempt to register the name with the local DNS server or look up the domain where the system is registered (if supported).
3. **Optional:** Enter or modify the **Domain Name** that the system belongs to.

4. Select **Save**.

Manually Configure DNS Settings

You can manually configure the DNS server settings for your Poly Studio V52 system.

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

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

Configure System VLAN Settings

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

NOTE: VLAN isn't supported in IPv6 environments.

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

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

   You can use values from `1` to `4094`.
4. Enter a **Video Priority** to set the link layer priority of video traffic on the wired LAN.

   Video traffic is RTP traffic consisting of video data and associated RTCP traffic. You can use any value from `0` to `7`, although Poly recommends not using `6` and `7`.
5. Enter an **Audio Priority** to set the link layer priority of audio traffic on the wired LAN.

   Audio traffic is RTP traffic consisting of audio data and associated RTCP traffic. You can use any value from `0` to `7`, although Poly recommends not using `6` and `7`.
6. Select **Save**.

Configure System 802.1X Settings

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

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

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

The system supports the following authentication protocols:

- EAP-MD5
- EAP-TLS

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

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

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

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

Configure Wired LAN Options

You can configure other LAN properties for your Poly Studio V52 system in the local interface or the system web interface.

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

Setting	Description
Autonegotiation (under **General Settings** in the local interface)	Specifies whether the system should automatically negotiate the LAN speed and duplex mode per IEEE 802.3 autonegotiation procedures. If you enable this setting, the system sets **LAN Speed** and **Duplex Mode** to read-only. Poly recommends that you use autonegotiation to avoid network issues.
LAN Speed (under **General Settings** in the local interface)	Specifies whether to use **10 Mbps**, **100 Mbps**, or **1000 Mbps** for the LAN speed. Note that the switch must support the speed you choose. If you enable the **Autonegotiation** setting, this setting is read-only.

Setting	Description
Duplex Mode (under **General Settings** in the local interface)	Specifies the duplex mode to use. Note that the switch must support the speed you choose. If you enable the **Autonegotiation** setting, this setting is read-only.
Ignore Redirect Messages	Enables the system to ignore ICMP redirect messages. Poly recommends that you enable this setting in most circumstances.
ICMP Transmission Rate Limit (millisec)	Specifies the minimum number of milliseconds between transmitted packets. Enter a number between `0` and `60000`. The default value of `1000` means the system sends 1 packet per second. If you enter `0`, the system disables the transmission rate limit. This setting applies only to "error" ICMP packets. This setting has no effect on "informational" ICMP packets, such as echo requests and replies.
Generate Destination Unreachable Messages	Generates an ICMP **Destination Unreachable** message if the system can't deliver a packet to its destination for reasons other than network congestion.
Respond to Broadcast and Multicast Echo Requests	When enabled, your system sends an ICMP **Echo Reply** message in response to a broadcast or multicast Echo Request that isn't specifically addressed to the system.

3. Select **Save**.

LLDP and LLDP-MED Support

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

Examples of applications that use information discovered by LLDP include:

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

LLMP-MED Information Discovery

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

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

Behavior When LLDP is Enabled

When LLDP is enabled on a Poly Studio V52 system, it discovers VLANs advertised by the network switch and automatically configures the system for one of the VLANs.

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

- Video Conferencing VLAN
- Voice VLAN
- Voice Signaling VLAN

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

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

Enable LLDP

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

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

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

Configure Wi-Fi as the Primary Network

Configure Wi-Fi on your Poly Studio V52. You must use WEP, WPA, or WPA2 Wi-Fi protocols on the 2.4 GHz and 5 GHz spectrums.

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

- Web proxy
- Provisioning
- 802.1x authentication

1. In the system web interface, go to **Network** > **Wi-Fi Network**.
2. From the **Choose Network Type** drop-down menu, select **Wi-Fi**.

3. Do one of the following:

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

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

4. Configure the following settings:

NOTE: Available settings vary with your selections.

Setting	Description
Security	Specifies the encryption protocol: • None • WEP • WPA/WPA2-PSK • 802.1x EAP NOTE: Although 802.1x EAP is listed in the drop-down menu, it isn't supported when using Wi-Fi as the primary network.
Key (Passphrase/PSK)	Specifies an encryption passphrase (like a password) for the Wi-Fi network. You must enter the passphrase to connect to the Wi-Fi network.
IP Address	Specifies the IP address of the network.
Your IP Address is	Specifies the IP address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
Subnet Mask	Specifies the network mask address for the network.
Default Gateway	Specifies the IP gateway for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
DNS Server	Specifies the DNS server address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
DNS Alternate Server	Specifies the alternate DNS server address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.

5. Select **Connect**.

Configure Wi-Fi Settings

In addition to a LAN, you can also connect your system to a Wi-Fi network.

6 Configuring Audio Settings

You can configure audio settings in the system web interface.

Configure General Audio Settings

You can specify general audio settings for your system.

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

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

Setting	Description
Enable M-Mode	Specifies whether the system transmits audio using a configuration that best reproduces interactive and live performance music picked up by microphones. This feature provides the highest-possible bandwidth for audio. When you enable M-Mode, even the faintest musical notes come through clearly.
Enable NoiseBlockAI	Enables Poly NoiseBlockAI, which eliminates background and extraneous sounds in common working environments. **NOTE:** This setting is disabled when you enable M-Mode. If you use an external echo canceller, keyboard noise reduction isn't available.
Transmission Audio Gain (dB)	Specifies the audio level (in decibels) that the system transmits sound. Unless otherwise advised, you should set this value to 0 dB.

Connect a USB Audio Device to the System

To use a USB audio device with the system, enable USB audio.

NOTE: USB Audio

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

Live Microphone Switching

Configure your system to automatically toggle the microphone input between the system's built-in microphones and a Poly Studio table microphone (formerly know as RealPresence Debut expansion microphone).

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

Polycom Acoustic Fence

Polycom Acoustic Fence technology creates a virtual *audio fence* that blocks sounds from outside the fence.

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

Configure Polycom Acoustic Fence

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

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.
   - Higher values increase the width of the audio fence beam. Use `1` for the narrowest beam (12 degrees) or `10` for the widest beam (120 degrees). The total angles is the setting number multiplied by 12.
   - If **Acoustic Fence Sensitivity** is set to 0, the system mutes the built in microphone and any supported echo canceling external microphone connected to the system. Setting the sensitivity level to 0 doesn't mute the USB audio in input.

Sound Reflection Reduction

Sound Reflection Reduction is a NoiseBlockAI option that reduces audible reverberations caused by environmental factors, including tables and glass walls. Audible reverberations result in reduced audio quality for audio transmitted to the far side.

NOTE: The addition of Sound Reflection Reduction as a NoiseBlockAI option changes the NoiseBlockAI parameter from `voice.noiseSuppression.enable` to `audio.noiseblockaioptions`.

If you hear echo or reverb with **NoiseblockAI** enabled, Poly recommends using **Sound Reflection Reduction**.

Sound Reflection Reduction supported configurations

NOTE: Disable noise reduction on your DSP when using Sound Reflection Reduction or NoiseBlockAI options.

Sound Reflection Reduction is supported in the following configurations:

- When Polycom StereoSurround is disabled. If you enable Polycom StereoSurround the system uses NoiseblockAI.
- On Poly Studio V52 systems using:
  - Built in microphones
  - Poly expansion microphone
  - USB audio DSP

Enable Sound Reflection Reduction

Eliminate echoes heard on the far end due to room conditions and materials by enabling Sound Reflection Reduction.

1. In the system web interface, go to **Audio / Video** > **Audio** > **NoiseBlockAI Options**.
2. In the drop-down menu, select **Sound Reflection Reduction**.

Configure Audio Output Settings

You can configure the audio output settings for your system.

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

Table 6-1 Audio input settings

Setting	Description
Primary Audio Volume	Sets the main audio output volume level going to the speakers.
Bass	Sets the volume level for low frequencies without changing the primary audio volume.
Treble	Sets the volume level for high frequencies without changing the primary audio volume.

7 Configuring Video and Camera Settings

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

HDMI Ports

Your system has two HDMI output ports. Use either of them for the system initial setup.

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 Poly 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.

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

Poly 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.

Table 7-1 Supported HDMI Output Resolutions and Frame Rates for Single-Monitor Setups

Output	Resolution	Frame Rates (fps)
UHD (4K)	3840 × 2160p	25, 30, 50, 60
FHD	1920 × 1080p	50, 60

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:

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

Disable CEC in the system web interface.

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

Enable CEC

Enable CEC in the system web interface.

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

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 Poly Studio V52 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.

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

Setting	Description
Power Frequency	NOTE: To avoid power frequency issues with your system, choose a location. 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.

3. Select **Save**.

Poly DirectorAI Perimeter

Define the area used by your video system to track meeting participants when a tracking mode is enabled.

NOTE: In this release, DirectorAI Perimeter is a preview feature.

In some environments, it's possible that the width defined in the system may not exactly match the area you're defining. When using this feature, Poly recommends testing and adjusting the perimeter settings as necessary.

You can provide feedback on the DirectorAI Perimeter feature by visiting the Poly Lens Feedback Portal.

Your Poly system uses the area visible by the camera to locate and track meeting participants in a conference room. In situations such as a conference room with glass walls, the area visible by the camera may extend beyond the conference room.

Using DirectorAI Perimeter, you can ensure that the camera only tracks participants within the defined conference room area.

If a participant moves out of the perimeter, the camera no longer tracks their movement.

Define the DirectorAI Perimeter

Define the area used by your system to track participants in a conference room.

1. In the system web interface, go to **Audio/Video** > **Video Inputs**.
2. Select **Enable DirectorAI Perimeter**.
3. Using the drop down, choose to use either **Metric** or **Feet** to define the tracking area.
4. Enter a tracking width, tracking depth, and the front exclusion depth.
5. Select **Save**.

Reset Camera Settings to Defaults

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

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

   Camera settings reset to the default configuration.

Configuring Video Input Settings

Customize your video input settings, such as Tracking Mode, White Balance, Brightness, and DirectorAI Perimeter.

Camera settings aren't available to users during a meeting. Poly recommends adjusting these settings as part of setting up and configuring the video system in your environment.

You can adjust the camera settings in the system web interface.

Configure General Video Input Settings

Customize your video input settings to provide the best meeting experience with your cameras.

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

   Table 7-2

Settings	Description
Model	Displays the type of device connected to the system.
Brightness	Adjusts the video brightness.
Maximum Digital Zoom Factor	Specifies the maximum digital zoom factor for the camera.
Enable DirectorAI Perimeter	Defines the area used by your system to track participants in a conference room.

3. Select **Save**.

Adjust the White Balance

Use white balance to compensate for light source variations in the room.

Poly cameras automatically adjust the white balance when set to **Auto**.

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

   - **Auto**: Recommended for most situations. It calculates the best white balance setting based on lighting conditions in the room.
   - **Manual**: Use this setting for rooms where the **Auto** and fixed values don't provide acceptable color reproduction.
     When you set to **Manual**, fill the camera's field of view with a flat white object, such as a piece of paper. For best results, the object should be uniformly illuminated with light that is representative of the room lighting used in the conference, rather than light from a display, another area, or a shadow. After the object is in place, select **Calibrate**.
   - **Color Temperature Value**: The color temperature values, measured in degrees Kelvin, correspond to the color of ambient light in a room. Use lower values for warmer lighting and higher values for cooler lighting.
   - **Color Temperature Term**: Some cameras, includingPoly Studio V52, provide text descriptions of available color temperatures. For example, **Fluorescent** or **Shade** .
   - **Off**

3. Select **Save**.

Configure Camera Tracking Settings for Poly Studio V52 Systems

With Poly Studio V52 systems, Poly camera tracking technology can automatically frame groups of people and follow conversations in meeting rooms.

NOTE: If you select a framing option, it automatically enables tracking on the Poly Studio V52 systems.

NOTE: People framing is a preview feature. Preview features are fully tested and supported features that Poly continues to develop in alignment with customer feedback.To provide feedback, go to the **Poly Lens Feedback Portal** and fill out the questionnaire.

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

     NOTE: If **Speaker Tracking** is selected, when you mute your microphone, the camera tracking mode automatically switches to **Frame Group**.
   - **People Framing (Preview)**: The camera tracks up to six individuals placing them in individual frames. If the camera detects more than six people, the camera places all participants in a single frame.
   - **Off**: Disables automatic tracking. You control the camera manually.
3. Set **Tracking Enabled** to **On** or **Off**.

   When you set **Tracking Enabled** to off, camera tracking is immediately disabled.
4. Select **Save**.

8 System Maintenance

You can perform several functions to keep your Poly Studio V52 system running properly.

Locate the System Serial Number

Use the system serial number to help technical support troubleshoot issues with your system.

The last 6-digits of the system serial number is the default system password.

- Do one of the following:
  - In the system web interface, go to **Dashboard** > **System Detail**.
  - Locate the printed serial number on the bottom or rear of your system.

Updating Software

You can update your Poly Studio V52 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 the Poly Lens Software Versions page and upload with a USB flash drive
- Provisioning service (for example, Poly Lens or Poly Clariti Manager)

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 Poly Studio V52 system software, depending on your environment.

NOTE: If you provision your system, the software update methods in the system web interface are unavailable. You must configure the software update method using your chosen provisioning method.

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

Software Update Method	Description
Poly Online Support Center	A software server hosted by Poly.

Software Update Method	Description
Custom Server URL	Manually downloaded software from https://lens.poly.com/manage/software-versions. 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>`). **NOTE:** If you are using private PKI certificates in your environment and want HTTPS software downloads to work, you must install the trusted root certificate from your internal certificate authority (CA) on the system since certificate validation is always performed.
Provisioning Server	Receive updates from a provisioning service, such as Poly Clariti Manager.

3. If you 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.

Update Software Using a USB Flash Drive

Update the software for your system and some of its paired devices using a USB flash drive.

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

1. Get the software package you want to install from the Poly Lens Software Versions page.
2. Open the ZIP file and extract the tar.gz file.
3. Save the package to the root directory of a USB flash drive and unzip the file.
4. 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. If there's no input to the system, it automatically starts the update after a short delay.

Update the Poly Bluetooth Remote Control Firmware

A system update may include new firmware for your Poly Bluetooth Remote Control.

You must be actively using the remote control for an available update to take effect. After 30 seconds of inactivity, the remote control disconnects from the system until you pick it up or press a button.

1. Update your system software.
2. Pick up the remote control or press a button.

The remote control automatically updates if it detects a new firmware version.

Downgrading Software

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

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

Manually Downgrade Software in the System Web Interface

You can downgrade your Poly Studio V52 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**.

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 Poly Studio V52 system software 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**.

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

Scheduled Auto Restart

You can configure your system to automatically restart on a weekly or daily interval.

When **Scheduled Auto Restart** is enabled, the system restarts at the designated time.

Configure Scheduled Auto Restart

Configure a weekly or daily system auto restart.

1. In the system web interface, go to **General Settings** > **System Settings**.
2. Enable **Enable Scheduled Auto Restart**.
3. Select **Daily** or **Weekly**.

   For **Weekly**, choose a day of the week.
4. Select the time each day or week that the system auto restarts.
5. Select **Save**.

Restart the System

If you encounter issues, you can try restarting your Poly V52 system.

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

Reset System Settings

You can reset your Poly Studio V52 system to its default configuration settings.

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

Resetting your system deletes all but the following data:

- Current software version
- User-installed PKI certificates
- Logs

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

NOTE: A system reset restores your system to its original mode of operation.

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**.

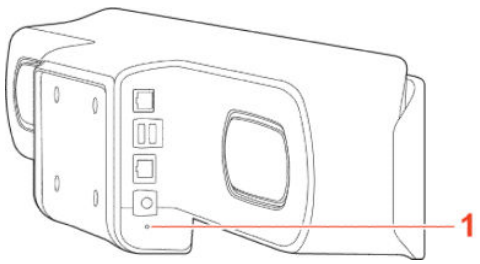
Factory Restore the Studio V52

A factory restore reset the system to its factory settings.

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

- Current software version
- Logs
- User-installed PKI certificates

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



3. While pressing the factory restore pinhole button, connect the power adapter to power on the system.
4. Continue pressing the factory pinhole reset button until the Studio V52 LED flashes.

9 Troubleshooting

Use the following topics to troubleshoot your system.

Studio V52 Doesn't Receive an IP Address When Connected to a Netgear Smart Switch 1G Port

In some cases, connecting a Studio V52 to a Netgear Smart Switch 1G port may result in no IP address received by the system.

If Power Back Off (PBO) is enabled on a Netgear 1G Smart Switch port, the Studio V52 will fail to connect to the network. The PBO feature isn't supported on 1G ports and if enabled can cause this issue.

Connect the Studio V52 to a 2.5G port on the switch.

Once the system receives an IP address, setup continue. You don't need to manually restart the system.

10 Securing the System

Your Poly Studio V52 system includes features and settings to help you meet security requirements.

Managing System Access

An administrator can configure systems to grant access using network accounts that are authenticated through an Active Directory (AD) server such as the Microsoft Active Directory server.

An administrator can configure Poly Studio V52 systems to grant access using network accounts that are authenticated through an Active Directory (AD) server such as the Microsoft Active Directory server. In this case, the account information is stored on the AD server and not on the room system. The AD administrator assigns accounts to AD groups, one for the room system admin access and one for user access. For this reason, external authentication is also referred to as Active Directory authentication.

The room system administrator configures the external authentication settings on the system to specify the address of an AD Server for authenticating user logins, AD group for user access, and AD group for admin access on the room system. The system can map only one Active Directory group to a given role.

Users can enter their network account credentials to access the system on the following interfaces:

- Web interface (admin access only)
- Local interface (`user` and `admin` role accounts when **Require Login for System Access** is enabled; `admin` accounts when admin-only areas of the local interface are accessed)

When External Authentication is enabled in PKI environments where Always Validate Peer Certificates from Server is enabled on the system, configure the Active Directory Server Address on the system using the address information that is in the Active Directory Server identity certificate. This allows the system to validate the identity certificate. As an example, if the Active Directory Server identity certificate contains its DNS name only, and no specific IP address, configuring the Active Directory Server Address on the system using the server's IP address results in certificate validation failure, and consequently authentication failure. The system configuration would have to specify the server by DNS name, in this case, to successfully match the server certificate data.

The system local user account is disabled when **Enable Active Directory External Authentication** is enabled. The admin account is active and usable, however.

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 Poly Studio V52 system.

Poly strongly recommends that you create an administrator password for your system. Administrators set password policies and minimum requirements.

1. In the system web interface, go to **Security** > **Password Requirements**.

2. Configure the following settings for the **Admin Room** , **Remote Access**, or **SNMP** passwords:

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

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.

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

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

3. **Optional:** Do one of the following:

   - To use the local administrator **Room Password** for remote logins, leave the **Use Room Password for Remote Access** option enabled.

   > **NOTE:** Password requirements for the local administrator password and remote access password must be configured separately.

   - If you don't want to use the local administrator **Room Password** for remote logins, disable the **Use Room Password for Remote Access** option.

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

4. Select **Save**.

Change Administrator Credentials

You can change the administrator username and password to access the system web interface and administrator sections of the local interface.

The default username is `admin` and the default password is the last six characters of the system's serial number.

1. In the system web interface, go to **Security** > **Local Accounts**.
2. Enter the new administrator username in the **Admin ID** field.
3. Select **Change Password**.
4. Enter the current password and then the new password.

   Entering an incorrect current password too many times causes the system to automatically log out and close the session.
5. Select **Save**.

Configure Account Lockout Settings

Account lockout controls prevent unauthorized access to your Poly Studio V52 system.

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

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

Set up external authentication through Active Directory for your Poly Studio V52 system. You can then access the system with an Active Directory account or the system's local administrator credentials.

Configure the **Domain Name** setting on the **Network** > **LAN Network** > **LAN Options** page with your Active Directory domain.

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

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

Setting	Description
Enable Active Directory External Authentication	Specifies whether to authenticate users with the Active Directory server. When you enable Active Directory authentication, users can log in to the system with their network credentials using this format: `domain\user`. With this format, users can have accounts on multiple domains.

Setting	Description
Active Directory Server Address	Specifies the Active Directory server's FQDN or IP address. If you are using subdomains, append port number 3268 as follows: `ad.domain.com:3268`. You can alternatively use Poly Clariti Manager as an Active Directory server and enter its address here. If you enable **Always Validate Peer Certificates from Server** on the **Certificates** page, make sure this value matches what is in the Active Directory server certificate. For example, if you enter the Active Directory server IP address here, but the certificate only has the server's FQDN, external authentication fails.
Active Directory Admin Group	Specifies the Active Directory group whose members should have administrator access to the system. This name must exactly match the name in the Active Directory server for successful authentication.
Active Directory User Group	Specifies the Active Directory group whose members should have user access to the system. This name must exactly match the name in the Active Directory server for successful authentication.

3. Select **Save**.

Configure System Access Settings

Configure how you and others access the system.

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

Setting	Description
Enable Network Intrusion Detection System (NIDS)	When you enable this setting, the system creates security log entries when it detects a possible network intrusion.
Enable Web Access	Specifies whether you can access the system using the system web interface.
Enable Diagnostics Port Idle Session Timeout	Specifies whether to allow the diagnostics port to time out and close the active session at the configured time interval of no activity or not. You set the timeout at **Idle Session Timeout in Minutes**.
Enable API Port Idle Session Timeout	Specifies whether to allow the API port to time out and close the active session at the configured time interval of no activity or not. You set the timeout at **Idle Session Timeout in Minutes**.
Enable SNMP Access	Specifies whether to allow SNMP access.
Idle Session Timeout in Minutes	Specifies the number of minutes a session can be idle before it times out.
Maximum Number of Active Sessions	Specifies the maximum number of users logged in through the system web interface or command-line API (SSH or telnet).
Max Session Timeout in Minutes	Specifies the maximum number of minutes a session can be open before it times out, regardless of session activity.

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

3. Select **Save**.

Command-Line API Access

You can access your system's command-line API over SSH, telnet, or through a serial port connection.

Enable Command-Line API Access Over SSH

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

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

Configure the SSH Port Lock

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

Enable command-line API access over SSH to access these settings.

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

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

3. Select **Save**.

Enable Command-Line API Access Over Telnet

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

1. In the system web interface, go to **Security** > **Access**.
2. Select the **Enable Telnet Access** check box.

3. Choose an **API Port** for telnet connections: **24** (default) or **23**.

Disable the Telnet Password

By default, you must enter a password to connect to the command-line API using telnet. You can disable it.

1. In the system web interface, go to **Security** > **Access**.
2. Clear the **Telnet Authentication** check box.

Locking the Telnet Port

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

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

Disable Command-Line API Access

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

1. In the system web interface, go to **Security** > **Access**.
2. Clear the **Enable Telnet Access** check box.

   Network ports 22, 23, and 24 on your system are closed.
3. In the system web interface, go to **General Settings** > **Serial Ports**.
4. For **RS-232 Mode**, select **Off**.

   The serial port is closed.

Command-line API access to your system is disabled.

Configure the System Web Interface Port Lock

You can limit the number of failed login attempts to the Poly Studio V52 system web interface to protect against brute-force attacks.

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

Setting	Description
Lock Port after Failed Logins	The number of failed login attempts allowed before the web interface locks. You can set this to **Off**.
Port Lock Duration	Specifies the amount of time that the web interface remains locked due to failed login attempts. When this period expires, the failed login attempts counter resets and you can try to log in again.

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

3. Select **Save**.

Disable USB-A Port

You can configure your system to disable the use of the system USB-A port.

1. In the system web interface, go to **Security** > **Access**.
2. Select **Disable USB-A Port**.

   The system reboots and disables the USB-A port.

Detecting Intrusions

When the Poly Studio V52 system detects a possible network intrusion, it logs an entry to the security log.

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

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

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

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

PKI Certificates

If your organization uses a public key infrastructure (PKI) for securing network connections, Poly recommends that you have a strong understanding of certificate management and how it applies to your Poly Studio V52 system.

PKI certificates authenticate secure network connections to and from the Poly Studio V52 system. The system uses standard PKI techniques to configure and manage certificates and certificate signing requests (CSRs). ANSI X.509 standards regulate the certificate characteristics.

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

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

Here are some examples of how you use PKI certificates:

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

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

Create a Certificate Signing Request

If you deploy a PKI in your environment, create a CSR to make sure your Poly Studio V52 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.

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:

Table 10-1 CSR Settings

CSR Information	Description
Hash Algorithm	Specifies the hash algorithm for the CSR: SHA-256 (recommended) or SHA-1 (not recommended).
Common Name (CN)	Specifies the system name. This is a required field. Maximum characters: 64 (truncated if necessary). Poly recommends the following guidelines for this field: • For systems registered in DNS, use the system's FQDN. • For systems not registered in DNS, use the system's IP address.
Organizational Unit (OU)	Specifies the unit of business defined by your organization. Default is blank. Maximum characters: 64. **NOTE:** The system supports only one OU field. If you want the signed certificate to include more than one OU field, you must download and edit the CSR manually.

Table 10-1 CSR Settings (continued)

CSR Information	Description
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 Principal 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.

Configure Certificate Validation Options

The Poly Studio V52 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 Poly Studio V52 system.

For a full list of preinstalled certificates on your system, see the *Poly VideoOS Certificates Update* on the HP Support Site.

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

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

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

Install a Certificate

Once you receive a signed certificate from the CA that processed your CSR, you can install it on your Poly Studio V52 system.

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

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

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

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

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

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

View a Certificate

The Poly Studio V52 system lists user-installed certificates in the system web interface, where you also can view the contents of those certificates.

1. In the system web interface, go to **Security** > **Certificates**.

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

2. To view the contents of a certificate, select **Visibility** in the same row as the certificate.

   The certificate contents display in plain text.

Delete a Certificate

You can remove user-installed certificates through the Poly Studio V52 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.

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

   CAUTION: You can't undo this action.

3. Confirm by selecting **Delete**.

   A message indicates that the system deleted the certificate.

Certificate Revocation

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

Your system can check certificate revocation status with the following standard method:

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

Manually Upload a CRL

You can use CRLs to perform certificate revocation checks on your Poly Studio V52 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.

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

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

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

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

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

Delete a CRL

You can remove CRLs that were previously uploaded on the Poly Studio V52 system.

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

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

System Allow List

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

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

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

Add IP Addresses to the Allow List

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

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

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

Delete IP Addresses from the Allow List

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

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

IPv4 Address Formats

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

The following are valid IPv4 formats for your Poly Studio V52 system:

- 10.12.128.7

- 172.26.16.0/24

IPv6 Address Formats

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

The following are valid IPv6 formats for your Poly Studio V52 system:

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

Set Up a Security Banner

You can create a security banner, which is a message that displays before users log in to the Poly Studio V52 system remotely.

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

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

Simple Certificate Enrollment Protocol (SCEP)

VideoOS Lite 1.0 supports SCEP on Poly Studio V52.

Install a SCEP Certificate

If you already have an SCEP certificate installed in your system, you don't have to disable EAP/802.1x authentication before you install SCEP. Verify your system's certificate settings before you install the service.

NOTE: If installing a SCEP certificate fails at any point during the process, a system reboot is required to bring the system back to a good state.

1. From the system web interface, go to **Admin Settings** > **Network** > **LAN Properties** > **LAN Options**.

2. Clear the **Enable EAP/802.1x** check box.
3. Restart the system.
4. Update your system with new software that includes SCEP.
5. Verify the SCEP certificate is installed into the system.
6. Enable EAP/802.1x authentication.

Configuring Simple Certificate Enrollment Protocol (SCEP)

Configure SCEP properties for your Poly system in the system web interface.

1. In the system web interface, go to **Admin Settings** > **Security** > **Certificates**.
2. Click **View and Update**.
3. Select **Enable SCEP** and configure the following settings:

Settings	Description
SCEP URL	The URL of the SCEP server
SCEP Challenge Password	Password configured in the SCEP server to generate a certificate.
Automatic Renewal	The automatic renewal period before certificates expire. You can choose the period based on the number of days or percentage of time left.
Days	The amount of days left before expiration to renew the certificate.
Percentage	The percentage of time left before expiration to renew the certificate.
Renewal Retry Attempts	The number of times a certificate tries to renew.
Enrollment Retry Attempts	The time interval that a certificate tries to renew.
CA Profile	The profile in the server set by the administrator.
Common Name	The system accepts an email as a common name.
Organizational Unit	The unit of business defined by your organization.
Organization	Your organization's name.
City or Locality	Your organization's city.
State or Province	Your organization's state or province.
Country	Your organization's country.

4. Select **Save**.

Web Proxies

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

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

- **Automatic**: Specify only the proxy credentials (if needed). Using DHCP, your system obtains a URL to automatically download a proxy auto-configuration (PAC) file.
- **Semi-automatic**: Specify the proxy credentials and URL for automatically downloading a PAC file.
- **Manual**: Specify the proxy address, port, and credentials. (This method lets you configure your system with only one proxy.)

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

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

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

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

- Provisioning service
- Software updates

Enable the System to Use a Web Proxy

By default, your Poly Studio V52 system configuration doesn't use web proxies.

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

Set Up Automatic Web Proxy Configuration

With automatic web proxy configuration, your Poly Studio V52 system obtains a URL for downloading a proxy auto-configuration (PAC) file through DHCP option 252.

1. In the system web interface, go to **Network** > **LAN Network** > **Web Proxy Settings**.
2. Select **Automatic Configuration**.
3. Select **Enable WPAD**.

   This option enables the web proxy auto-discovery protocol (WPAD), which helps your system automatically download the PAC file on your network using DHCP option 252.
4. Enter the **Proxy User Name** and **Proxy Password**.
5. Select **Save**.

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

Set Up Semi-Automatic Web Proxy Configuration

With semiautomatic web proxy configuration, you must specify the URL your Poly Studio V52 system uses to download a proxy auto-configuration (PAC) file.

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

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

Manually Update the PAC File on the System

Even if you set up your Poly Studio V52 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.

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

Manually Configure a Web Proxy

You can manually configure your Poly Studio V52 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.

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

Sample PAC File

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

The following code shows a sample PAC file.

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

```
6) == "https:" ){return "PROXY 10.221.77.3:8080; PROXY
10.221.76.7:8080;DIRECT";}else{return "DIRECT";} }
```

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

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

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

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

PAC file limitations:

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

View Connections to the System

Access a list of current connections to your Poly Studio V52 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)

- 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 Poly Studio V52 system.

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
22	Inbound	Static	SSH	Command-line API access over SSH	No	No
23	Inbound	Static	TCP	Command-line API access over telnet	No	No
24	Inbound	Static	TCP	Command-line API access over telnet	No	No

Port	Direction	Type	Protocol	Function	Open by Default?	Configurable Port?
53	Outbound	Static	UDP	DNS	Yes	No
80	Inbound	Static	TCP	HTTP web server listener that provides access to the web interface. Redirects all sessions to HTTPS on port 443.	Yes	Yes
123	Outbound	Static	UDP	NTP (automatic time synchronization)	Yes	No
161	Inbound	Static	UDP	SNMP reporting	No	Yes
443	Bidirectional	Static	TCP/SCTP	Static TCP HTTPS web server listener that provides TLS access to the web interface. Provisioning (for example, Poly Clariti Manager) REST API Poly Lens Poly software download URL `downloads.polycom.com` (3.13.1 and prior) `swupdate.lens.poly.com` (3.14.0 and later)	Yes	No
514	Outbound	Static	UDP	Remote logging	No	Yes
601	Outbound	Static	TCP	Remote logging	No	Yes
4443	Bidirectional	Static	TCP/TLS	Web server for peripheral device software downloads and log uploads	Yes	No
6514	Outbound	Static	TLS	Remote logging	No	Yes
7080	Inbound	Static	TCP	Web services	Yes	No
7081	Inbound	Static	TCP	Web services	Yes	No

11 Diagnostic Functions

Poly Studio V52 systems provide multiple diagnostic features for testing audio, networking, and collecting logs.

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 Poly Lens or Poly Clariti Manager.

NOTE: Provisioning results are available only if Poly Lens or is directly provisioned to a service via network connection. The results are unavailable if Poly Lens or is provisioned through a USB connection to Poly Lens Room or Poly Lens Desktop.

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 Lite Configuration Parameters Reference Guide.

Checking System Status

You can verify the status of your Poly Studio V52 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 the Local Interface

Verify your Poly Studio V52 system status in the local interface.

1. Go to **Menu** > **Settings** > **Status**.
2. View a system status page:

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

Setting	Description
Active Alerts	Displays the status of any device or service with an error status. If there's an alert, an **Alert** displays next to the system time.
LAN Properties	Displays network connection status.
Peripheral Devices	Connection status of peripheral devices.

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.

PAC File Status

Your Poly Studio V52 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 11-1 PAC File Status

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

Verify the PAC File Contents

You can check the contents of the PAC file on your Poly Studio V52 system.

1. In the system web interface, go to **Network** > **LAN Network** > **Web Proxy Settings**.

2. Select **Download PAC File**.

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

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)

Configure Log Preferences

You can manage some basic aspects of your Poly Studio V52 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 Poly Studio V52 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.

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

Table 11-2 Log settings

Setting	Description
Current Percent Filled	Displays as a percentage how full the logs are. When the logs are full, system deletes the oldest entries.
Percent Filled Threshold	Reaching the threshold you configure here creates a log entry and automatically transfers logs if you set **Transfer Frequency** to **Auto At Threshold**.

Table 11-2 Log settings (continued)

Setting	Description
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 Poly Studio V52 system logs.

1. In the system web interface, go to **Diagnostics** > **Logs** > **System Log Settings**.

2. Configure the following settings:

Table 11-3 Log Level Settings

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

3. Select **Save**.

Retrieve Log Files

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

Wake the system before retrieving log files.

NOTE: The date and time of the system log entries for Poly Studio V52 devices are shown in GMT.

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

Transfer Logs to a USB Flash Drive

You can transfer logs to a USB flash drive to free up space on your Poly Studio V52 system.

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

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

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

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

Configure Remote Logging

You can configure your Poly Studio V52 system to send the event details it collects to a remote logging server (using syslog or a similar mechanism).

Remember the following about remote logging with your system:

- The system sends logs to remote logging servers over a secure TLS connection. Your system may use a version of TLS that you configured your system not to use. This happens because your system sends logs using the TLS version configured on your remote logging server. This doesn't affect the use of the configured TLS version for other parts of your system. For example, if you set your system's minimum version of TLS to 1.2, but the server only uses 1.0, it still receives the logs.
- You can use more than one remote logging server.
- Logs can be consumed by an intrusion detection system (IDS) and a security information and event management (SIEM) system.

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

Table 11-4 Log settings

Setting	Description
Enable Remote Logging	Specifies whether remote logging is enabled. Enabling this setting causes the system to send each log message to the specified server. The system immediately begins forwarding its log messages after you click **Save**. The system supports remote logging encryption using TLS. If you use UDP or TCP transport, Poly recommends remote logging only on secure, local networks.
Remote Log Server Address	Specifies the server address and port. If you don't specify the port, the system uses a default destination port. The system determines the default port by how you configure **Remote Log Server Transport Protocol**: • UDP: 514 • TCP: 601 • TLS: 6514 You can specify the address and port in the following formats: • IPv4 address: `192.0.2.0:<port>` , where *<port>* is the elective destination port number in the 1-65535 range. • FQDN: `logserverhost.company.com:<port>` , where *<port>* is the elective destination port number in the 1-65535 range.

Table 11-4 Log settings (continued)

Setting	Description
Remote Log Server Transport Protocol	Specifies the transport protocol for sending logs to a remote server: • UDP • TCP • TLS (secure connection)

3. Select **Save**.

Configure Logging to System Internal Storage

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

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

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

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

3. Select **Save**.

Sample Log File

The following code shows examples from a system log file.

```
Login:2020-05-07 19:06:36.526 DEBUG SecurityService: SecurityService:
securityserviceproto.cpp SecurityServiceCreateSessionRequest
clienttype: 3 location: 192.168.137.1 clientName: Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/81.0.4044.129 Safari/537.36 request: clienttype:
kWeb2020-05-07 19:06:36.526 DEBUG SecurityService: SecurityService:
createSession ClientType is 3 location: 192.168.137.1 name:Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/81.0.4044.129 Safari/537.362020-05-07 19:06:36.526
DEBUG SecurityService: SecurityService: In createSession
sessionId=PSLgZBGvGw7I2020-05-07 19:06:36.526 DEBUG SecurityService:
SecurityService: createSession The password is not empty, setting
the user as anonymous2020-05-07 19:06:36.526 DEBUG SecurityService:
SecurityService: updateSessionCount: Increment session count for
client type '3' to 12020-05-07 19:06:36.526 DEBUG SecurityService:
SecurityService: SessionAddNtfy: len 2682020-05-07 19:06:36.526 DEBUG
SecurityService: SecurityService: SecurityServiceSendNotification():
finished sending the notification, msg_sendnotification() returned
02020-05-07 19:06:36.533 DEBUG SecurityService: SecurityService:
SecurityServiceLoginRequest(): username: admin2020-05-07 19:06:36.533
```

```
DEBUG SecurityService: SecurityService: login2020-05-07 19:06:36.533
DEBUG SecurityService: SecurityService: LocalAuthenticator::login,
role 3 loginSuccess 12020-05-07 19:06:36.535 DEBUG SecurityService:
SecurityService: SessionStateNtfy: len 692020-05-07 19:06:36.535 DEBUG
SecurityService: SecurityService: SecurityServiceSendNotification():
finished sending the notification, msg_sendnotification()
returned 02020-05-07 19:06:36.535 DEBUG SecurityService:
SecurityService: getPwdStatusAux password can not expire node
security.authentication.accounts.adminremote.passwordpolicy2020-05-07
19:06:36.535 DEBUG SecurityService: SecurityService: login
login, pwStatus 22020-05-07 19:06:36.535 DEBUG SecurityService:
SecurityService: setCurrentLoginInfo set login status: lastLoginTime
1588877728, lastClientType 3, lastClient 192.168.137.1,
failedLogins 02020-05-07 19:06:36.536 DEBUG SecurityService:
SecurityService: setSuccessfulLoginInfoToConfig successful login,
current time 15888783962020-05-07 19:06:36.537 DEBUG SecurityService:
SecurityService: LoginNtfy: len 302020-05-07 19:06:36.537 DEBUG
SecurityService: SecurityService: SecurityServiceSendNotification():
finished sending the notification, msg_sendnotification() returned
02020-05-07 19:06:36.537 DEBUG SecurityService: SecurityService:
securityserviceproto.cpp SecurityIFLoginStatusPackLogout:2020-05-07
19:17:29.313 DEBUG SecurityService: AuthenticationManager:
AuthenticationManager::logout(): username: admin2020-05-07
19:17:29.313 DEBUG SecurityService: SecurityService: LogoutNtfy: len
212020-05-07 19:17:29.313 DEBUG SecurityService: SecurityService:
SecurityServiceSendNotification(): finished sending the notification,
msg_sendnotification() returned 02020-05-07 19:17:29.313 DEBUG
SecurityService: SessionManager: deleteItem(): deleting the
session PSllKtLtRoFp2020-05-07 19:17:29.313 DEBUG SecurityService:
SecurityService: updateSessionCount: Decrement session count
for client type '3' to 02020-05-07 19:17:29.313
DEBUG SecurityService: SecurityService: SessionDeleteNtfy: len
522020-05-07 19:17:29.313 DEBUG SecurityService: SecurityService:
SecurityServiceSendNotification(): finished sending the notification,
msg_sendnotification() returned 02020-05-07 19:17:29.313
DEBUG SecurityService: SecurityService: securityserviceproto.cpp
errorResponsePack
```

Run a Trace Route

You can run a trace route to identify network connectivity issues with your Poly Studio V52 system.

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

1. Go to **Trace Route**.
2. Enter the IP address or URL with which to run the trace route.
3. Select **Start**.

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

SNMP Reporting

The Poly Studio V52 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
- System power on
- Successful or unsuccessful administrator login
- User help request

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

Configure SNMP

You can monitor your Poly Studio V52 system remotely with SNMP.

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

Table 11-5 SNMP settings

Setting	Description
Enable SNMP	Enables administrators to monitor the system remotely using SNMP.
Enable Notifications	Enables MIB notifications.
Version1	Enables your system to use the SNMPv1 protocol. Due to security issues, Poly recommends that you don't enable this setting.
Version2c	Enables your system to use the SNMPv2c protocol. Due to security issues, Poly recommends that you don't enable this setting.

Table 11-5 SNMP settings (continued)

Setting	Description
Version3	Enables your system to use the SNMPv3 protocol. Enabled by default, you can't configure other SNMPv3 settings unless this is on.
Read-Only Community	Specifies the SNMP community string for your system. For security reasons, don't use the default community string (`public`). **NOTE:** Poly doesn't support SNMP write operations for configuring or provisioning systems. The community string is for read operations and outgoing SNMP traps. **NOTE:** For SNMPv3, if your SNMP utility prompts for a context name, enter the Read-Only Community name.
Contact Name	Specifies the name of the person responsible for remotely managing the system.
Location Name	Specifies the system location.
System Description	Provides details about the system.
User Name	Specifies the User Security Model (USM) account name for SNMPv3 message transactions. The maximum length is 64 characters.
Authentication Algorithm	Specifies the type of SNMPv3 authentication algorithm used. • **SHA** • **MD5**
Authentication Password	Specifies the SNMPv3 authentication password. The maximum length is 48 characters.
Privacy Algorithm	Specifies the cryptographic privacy algorithm for SNMPv3 packets. • **CFB-AES128** • **CBC-DES**
Privacy Password	Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.

Table 11-5 SNMP settings (continued)

Setting	Description
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 Destination Address2 Destination Address3	Specifies the IP addresses of SNMP managers where SNMP traps are sent. Each address has four settings: • Server address (accepts IPv4 addresses, hostnames, and FQDNs) • Message type (**Trap** or **Inform**) • Protocol (SNMP **v1**, **v2c**, or **v3**) • Port where SNMP traps are sent (default is **162**)

3. Select **Save**.

Download MIBs

You can download MIB data for your Poly Studio V52 system.

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

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

Verify Poly Lens Registration Status

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

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

12 Poly Studio V52 accessibility features

Poly Studio V52 includes a number of features to accommodate users with disabilities.

Table 12-1 Poly Studio V52 accessibility features

Accessibility feature	Description
Visual notifications	LED indicators let you know when status changes and functions work.
95-degree field of view	The wide view captures your movements without needing to adjust the camera.
Tactile buttons	The mechanical buttons on the optional remote control provide visual contrast to enable you to control the system.

13 Getting help

Poly is now a part of HP. The joining of Poly and HP paves the way for us to create the hybrid work experiences of the future. Information about Poly products is now transitioning from the Poly Support site to the HP Support site.

The Poly Documentation Library is continuing to host the installation, configuration/administration, and user guides for Poly products in HTML and PDF format. In addition, the Poly Documentation Library provides Poly customers with up-to-date status information about the transition of Poly content from Poly Support to HP Support.

The HP Community provides additional tips and solutions from other HP product users.

HP Inc. addresses

HP US
HP Inc.
1501 Page Mill Road
Palo Alto 94304, U.S.A.
650-857-1501

HP Germany
HP Deutschland GmbH
HP HQ-TRE
71025 Boeblingen, Germany

HP UK
HP Inc UK Ltd
Regulatory Enquiries, Earley West
300 Thames Valley Park Drive
Reading, RG6 1PT
United Kingdom

Document information

Model ID: Poly Studio V52 (model: P033,P033NR)

Document part number: P01287-001

Last update: April 2024

Email us at documentation.feedback@hp.com with queries or suggestions related to this document.