ADMINISTRATOR GUIDE

1.2.4 | August 2021 | 3725-42460-006A1

Polycom® Pano™

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

Limitation of Liability Poly and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Poly and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Poly has been advised of the possibility of such damages.

Disclaimer While Poly uses reasonable efforts to include accurate and up-to-date information in this document, Poly makes no warranties or representations as to its accuracy. Poly assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@poly.com.

Support Visit the Poly Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

Before You Begin

Topics:

- Get Help

This information is for administrators who need to configure, manage, customize, and troubleshoot Polycom® Pano™ devices.

Polycom recommends that you record your device's serial number and have it available for setup and troubleshooting. The serial number is printed on the device and the shipping box labels. It also is listed on the **Dashboard** of the system web interface.

Get Help

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

Getting Started

Topics:

Features and Capabilities

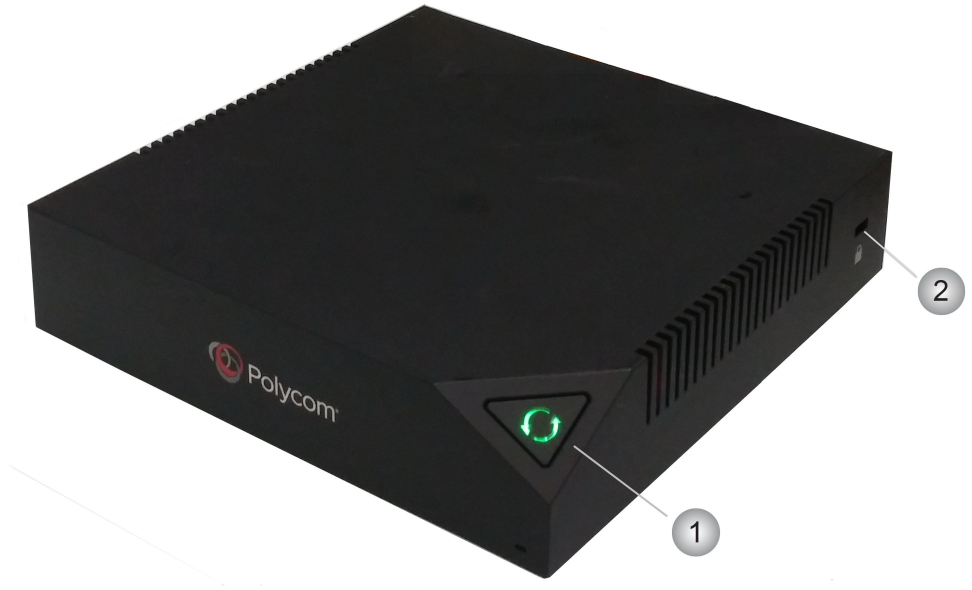
The Pano device provides real-time collaboration with the following features:

- Up to full 4K performance for sending content streams to high-definition monitors with or without touch capabilities. Meeting participants simultaneously stream content onto the monitor or interactively annotate and control content.
- Support for multiple content streams from AirPlay®- and Miracast®-certified devices, the Polycom® Content™ App, and HDMI connections.
- Integration with supported Polycom video systems.
- Integrated toolbar with high-performance annotation capabilities.
- Cloud connectivity for remote administrator access.
- System security with 802.1X authentication for wired connections and PKI certificates.
- Device management with Polycom® RealPresence™ Resource Manager.
- Remote administrator access for managing standalone devices.

Note: Audio transmission in Miracast mirroring is best-effort. For Windows 10 or Android devices, Miracast audio-video synchronization isn't guaranteed.

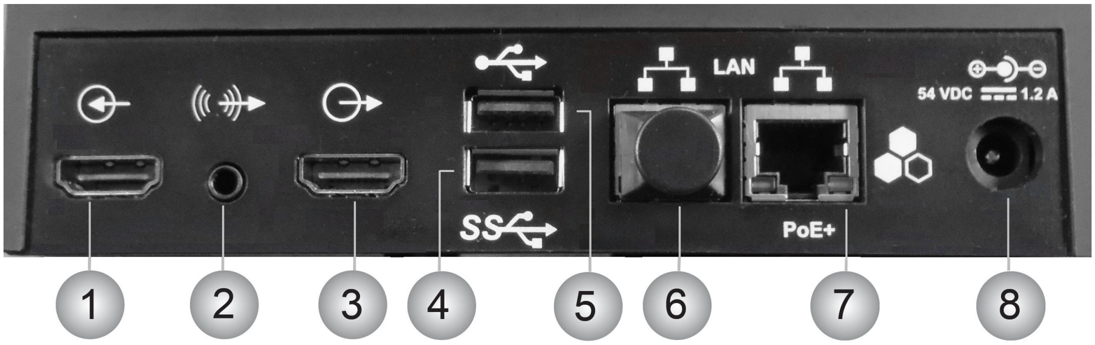
Hardware Features

Polycom designed the Pano device system to be always connected and powered. The system includes limited cable and Wi-Fi connections to simplify setup, and its compact design fits most space requirements.



Front and Side Feature Descriptions

Reference Number	Feature
1	LED indicator of system status and button to initiate factory reset
2	Security cable lock slot on the side



Back Panel Feature Descriptions

Reference Number	Feature
1	HDMI input port
2	Analog audio output
3	HDMI output port

Reference Number	Feature
4	USB 3.0 host port If you plug a dongle for a wireless pointing device into the USB 2.0 port and connect a USB flash drive to the USB 3.0 port, the wireless pointing device may not function properly.
5	USB 2.0 host port If you plug a dongle for a wireless pointing device into the USB 2.0 port and connect a USB flash drive to the USB 3.0 port, the wireless pointing device may not function properly.
6	10/100/1000 Ethernet port The device ships with this Ethernet port covered. This port is reserved for future use.
7	10/100/1000 Ethernet port powered with PoE+ PD This port supports IEEE 1588 for time synchronization with devices in a room.
8	2.0 mm jack for optional external 54 V DC power adapter

System Indicator Lights

The LED on the front of the Pano device system provides the following information.

Indicator Light	System Status
Off or blinking red light	System is disconnected, cannot initialize, or has encountered a severe malfunction
Steady white light	System is initializing
Steady blue light	System is running
Alternating blue and amber lights	System is in software update or factory restore mode

Powering On and Off

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

You can power the device with the following:

- Power over Ethernet+ (PoE+) IEEE 802.3at Type 2 (Link Layer Discovery Protocol [LLDP] negotiation is supported for switches that require it)
- 2.0 mm power adapter

Remember the following when powering the Pano device:

- When you connect both a PoE+ source and power adapter, the power adapter takes precedence.

- The device reboots when you connect or disconnect the power adapter.
- The Pano device supports only PoE 2-event classification mode. Depending on the model, you may need to configure your switch to support the 2-event classification mode before the system is able to receive proper power from the component. If necessary, check the switch user manual for instructions to activate this feature.
- Powering a Consumer Electronics Control (CEC)-enabled monitor off and on disrupts how the Pano device functions and requires you to restart the device. To avoid these issues, Polycom recommends disabling the monitor's CEC setting. (Note: CEC may have a different name depending on the monitor manufacturer.)

Power On the Device

You need to connect all of the related equipment that you intend to use before connecting the power source to the Pano device.

Procedure

1. Connect the Pano device to the monitor using an HDMI cable.
2. Optional: Connect the touch-capable monitor to the bottom USB port.
3. Connect the LAN cable.

   Note: You might experience a low signal strength when connecting the device with a LAN cable longer than 30 m (100 ft). Polycom recommends that you use an externally powered Ethernet hub or PoE switch to limit the LAN cable length to shorter than 30 m (100 ft).

4. Connect the power source.

   The device is considered on.

Power Off the Device

Powering off your Pano device depends on how you have it connected.

Procedure

» Choose one of the following options to power off your device.

- Disconnect the power adapter.
- Disconnect the LAN cable if your device is using PoE+.

If your setup includes both connections, you must disconnect both cables.

Managing the System

After you run the setup wizard, you can configure, manage, and monitor your Pano device using its web interface.

Access the System Web Interface

You can access the Pano system web interface.

- You must use a supported web browser with cookies enabled to access the system web interface.

Note: If you try to access the system with a web browser with cookies disabled, the system displays a notification. However, this message doesn't appear with Microsoft Edge web browsers.

- During initial setup, you must have a DHCP server in your environment to ensure the system gets an IP address. To access the system web interface for the first time, you must use the IP address assigned to the system by the DHCP server.

  The system IP addresses display on its home screen by default.

If you enable the Secondary network (Wi-Fi) by selecting the **Enable Administrator Access to This Network** option, you can also access the system web interface using the Wi-Fi network IP address.

Note: You can always access the system web interface using the Primary network (LAN) IP address.

The system IP addresses display on its home screen by default.

Procedure

1. Open a browser and enter the system IP address using the format `https://10.11.12.13`.

   Note: HTTPS severely limits the ability of anyone on the network to discover login information or credentials. For this reason, the system redirects attempts to use the system web interface via HTTP to the HTTPS interface.

2. Enter your administrator credentials.

   The default Administrator user name is `admin`, and the default admin password is the last six digits of the Pano device serial number. You can find the serial number in one of these locations:

   - A sticker on the back of the device
   - The shipping container
   - The **Dashboard** screen of the system web interface

3. Select **Login**.

Related Links

General Settings on page 13

Provisioning Service on page 18

Monitor Settings on page 27

Security on page 30

System Maintenance on page 43

Configure Wi-Fi Settings on page 23

Access the Polycom Cloud Service Administration Portal from the System Web Interface

If your organization has activated a Polycom Cloud Service account, you can access the service's administration portal to manage registered devices and configure cloud capabilities.

You can access the portal from the system web interface of a Pano device that is registered to the Polycom Cloud Service.

Procedure

1. Open a browser and enter the system IP address using the format `https://10.11.12.13`.

2. In the system web interface, to **General Settings** > **Cloud**.
3. Select **Launch the Polycom Cloud Service Portal**.
4. Enter your **Email ID** and **Password** and select **Sign In**.

Related Links

Polycom Cloud Service on page 48
Access the Polycom Cloud Service Administration Portal from an Assigned URL on page 10

Access the Polycom Cloud Service Administration Portal from an Assigned URL

If your organization has activated a Polycom Cloud Service account, you can access the service's administration portal to manage registered devices and configure cloud capabilities.

Procedure

1. Access the Polycom Cloud Service Administration portal by copying and pasting the URL you received in the Polycom Cloud Service Administration Account Activation email into a browser.
2. Enter your email address in the **Email Address** field and click **Continue**.
3. Enter your password in the **Password** field and select **Sign in**.

Related Links

Polycom Cloud Service on page 48
Access the Polycom Cloud Service Administration Portal from the System Web Interface on page 9

Setup Wizard

Topics:

- Modes of Operation
- Change System Default Credentials
- Set Up System Manually
- Provision the System

The setup wizard, also known as the out-of-box (OOB) state, walks you through the initial steps of configuring your Pano system. It is available during initial setup, after a system reset with settings deleted, and after a factory reset.

Note: Make sure you complete the entire setup process. A timeout occurs after 10 minutes and the system returns to the sign-in page.

Modes of Operation

When you run the Pano system setup wizard, you have the following options:

- **Manual Setup** You bypass registering with the provisioning service and configure a standalone system. In this mode, you can control system operations manually.
- **Provision** You register your system with a provisioning service (e.g., Polycom® RealPresence® Resource Manager). In this mode, some system operations (such as configuration settings and software updates) are automatically controlled.

During either setup, you also can register your system to the Polycom Cloud Service to automatically control some system operations (such as software updates). (Registration requires that your organization first complete the Polycom Cloud Service activation process.)

Related Links

Register with Polycom Cloud Service on page 16

Change System Default Credentials

When you run the setup wizard, you are required to change your system's default password.

Before you begin, make sure that the monitor and network cables are connected and the power source is plugged in. A URL displays on the monitor once the Pano system is on.

Procedure

1. Open a browser and enter the system IP address using the format `https://10.11.12.13`.
2. Change your system's default password.

   A new password is required to limit access to the system administrator settings. The default password, which is case sensitive, is the last six characters of your Pano system serial number.

If you forget your administrator password, you must reset the system and run the setup wizard again to reset the password.

3. Optional: Select the **Change username** checkbox to create a new username.

   The default username is **admin**.

Set Up System Manually

You can finish setting up your system manually after you change your default password.

Procedure

1. On the welcome screen, select **Manual Setup**.
2. Select a language for the system.
3. Select the country where the system is located.
4. Do one of the following on the Polycom Cloud Service registration page:
   - Select **Sign In** to register your system with the Polycom Cloud Service.
   - Select **Skip** to set up a standalone system.
5. If you chose **Sign In**, complete the Polycom Cloud Service registration.
6. Select **Finish** when prompted.

Related Links

Register with Polycom Cloud Service on page 16

Provision the System

You can register your system with a provisioning service after you change your default password.

Procedure

1. On the welcome screen, select **Provision**.

   The system searches for a provisioning service.
2. Complete the required fields for registering with the provisioning service and select **Register**.

   If your system detects a provisioning service on the network, all the fields except **Username** and **Password** are automatically completed. If a service is not detected, you must enter all the fields manually.
3. If the Polycom Cloud Service registration page displays, select **Sign In** to register your system or **Skip**.

   You see this page only if your provisioning service allows your system to also register with the Polycom Cloud Service.
4. Select **Finish** when prompted.

Related Links

Register with Polycom Cloud Service on page 16

General Settings

Topics:

The **General Settings** tab in the system web interface lets you configure basic features of your Pano device, such as its language and if you want to allow screen mirroring.

Related Links

Access the System Web Interface on page 8

Set the Local Interface Language

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

Procedure

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

Set the System Web Interface Language

You can change the language that administrators see in the Pano system web interface.

Procedure

» In system web interface title bar, select the language you want from the dropdown list.

Customizing Your Home Screen

You can change the background image of the home screen.

Customize Your Home Page Image

You can change the background image of the Pano home page.

The background image must be in JPEG or PNG format, less than 10 MB, with a 16:9 resolution of at least 1280 × 720. Polycom recommends one of the following resolutions:

- 3840 × 2160

- 2560 × 1440
- 1920 × 1080

Changing the background image deletes the old one from the system, unless it's the default Polycom background image. You can always revert to the default background image.

Procedure

1. Select **General Settings** > **Home Screen Settings**.
2. Select **Choose File** and then select an image from your local disk.
3. Select **Upload**.

   The system prompts you when the image successfully loads.

Revert to the Default Home Screen Background

You can revert the home screen background to the default picture.

Procedure

1. Select **General Settings** > **Home Screen Settings**.
2. Select **Use Default Background**.
3. In the **Are you sure?** dialog box, select **Apply Default**.

   The system deletes your current background image and replaces it with the default.

Disable Your Home Screen Instructions

You can disable the default **Home** screen content sharing instructions.

When you disable the instructions, the **Home** screen displays only the background image.

Procedure

1. Select **General Settings** > **Home Screen**.
2. Disable **Enable Content Sharing Instructions on Home Screen** the option.

Change Network Name

You can give a descriptive name to your networks so users can identify them easily.

Procedure

1. Select **General Settings** > **System Status Bar**.
2. Type a name to the right of the desired network.

   The maximum name length is 16 characters.

Configure 4K HDMI Content Input

You can enable or disable 4K HDMI content input.

`

Procedure

1. Go to **General Settings** > **Homescreen**.
2. Select **Enable 4K HDMI Content Input**.

   Changing this setting causes the system to restart.

Customizing Your System Status Bar

You can set whether to display the Primary network (LAN) or Secondary network (Wi-Fi) IP addresses on the system status bar. You can also change the network names.

Display IP Addresses on System Status Bar

You can display the Pano system IP addresses in the system status bar.

Content App users can find and connect to the Pano system using the Pano IP addresses shown on the system status bar.

Procedure

1. Select **General Settings** > **System Status Bar**.
2. Select **Display on system status bar:** under the desired network.

Related Links

Configure Monitor Settings on page 29

Change Network Name

You can give a descriptive name to your networks so users can identify them easily.

Procedure

1. Select **General Settings** > **System Status Bar**.
2. Type a name to the right of the desired network.

   The maximum name length is 16 characters.

Set the Date and Time

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

Procedure

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

Setting	Description
Date Format	Specifies how the date displays.
Time Format	Specifies how the time displays.
Auto Adjust for Daylight Saving Time	When enabled, the system clock automatically adjusts for daylight saving time.
Time Zone	Specifies the time difference between GMT and your location.

Setting	Description
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 Device and Room Names

You can set the device and room names associated with a standalone Pano system using the system web interface.

You must use the Polycom Cloud Service Administration portal to change the names of a system that is registered with the Polycom Cloud Service.

Procedure

1. In the system web interface, go to **General Settings** > **Device and Room Name**.
2. Enter the **Device Name**, **Room Name**, or both and select **Save**.

Register with Polycom Cloud Service

You can register your system to the Polycom Cloud Service through the setup wizard or in the system web interface.

Besides the first step, the following instructions are the same whether you chose to register during initial setup or later in the system web interface.

Procedure

1. In the system web interface, go to **General Settings** > **Cloud**. (Skip this step if you are running the setup wizard.)
2. Select **Sign In**.
3. Enter your **Email ID** and **Password**.

   The **Email ID** was activated through the Polycom Cloud Service Administration portal and enables the system to locate your account.
4. Enter a **Room Name**.

   A **Room Name** is how users identify a Pano system they want to connect to from a device or the Content App. Polycom recommends that you use a name that is associated with the system's location (e.g., a conference room).

5. Optional: Deselect the **Enable Security Code** checkbox if you do not want users to enter a code to connect their device to the Pano system.
6. Keep the automatically generated **Device Name** or enter a new one.

   This name identifies the Pano device in the Polycom Cloud Service portal dashboard.
7. Select **Finish** when prompted.

Related Links

Set Up System Manually on page 12

Provision the System on page 12

Provisioning Service on page 18

Choose a Software Update Method on page 45

Modes of Operation on page 11

Provisioning Service

Topics:

- Enable a Provisioning Service
- Register with a Provisioning Service
- Disable a Provisioning Service

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

- Automatically provision settings, including Room Name, Device Name, and whether a security code is required for connecting to the system.
- Automatically update software
- Allow your systems to register with the Polycom Cloud Service.
- Monitor health and status

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.
- The provisioning service can determine whether the system can register with and receive software updates from the Polycom Cloud Service.
- With administrative permissions, you can change a system's settings after a bundle is applied (a new bundle also overwrites manual settings).
- 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.

Related Links

Access the System Web Interface on page 8

Choose a Software Update Method on page 45

Register with Polycom Cloud Service on page 16

Enable a Provisioning Service

You can register your Pano system with a provisioning service in one of the following ways:

- Entering the required information in the **General Settings** of the system web interface.
- Running the setup wizard, which indicates if your system detects a provisioning service on the network.

  The setup wizard is available during initial setup, after a system reset when you delete system settings, or when you factory reset the system.. For information about configuring the RealPresence Resource Manager system so that Polycom systems detect and register with it, see the *Polycom RealPresence Resource Manager System Operations Guide*.

Procedure

1. In the system web interface, go to **General Settings** > **Provisioning Server**.
2. Select **Enable Provisioning**.

Register with a Provisioning Service

After enabling provisioning, you can register your Pano system with a provisioning service.

Procedure

1. In the system web interface, go to **General Settings** > **Provisioning Server**.
2. Select **Load Discovered Information**.

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

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

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

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

Disable a Provisioning Service

You can disable a provisioning service on the Pano system web interface.

Procedure

1. In the system web interface, go to **General Settings** > **Provisioning Server**.
2. Disable the **Enable Provisioning** setting.

Network Settings

Topics:

- Configuring the Primary Network (LAN) Settings
- Configuring the Secondary Network (Wi-Fi) Settings

You can configure a Primary network (LAN) or a Secondary network (Wi-Fi) for users to connect to and share content on the Pano system.

Note: Throughout this document, the term ‘Primary network’ stands for the wired LAN network; while ‘Secondary network’ stands for the Wi-Fi network. Even if you use Wi-Fi as your only network connection, it’s still referred as the ‘Secondary network’.

Configuring the Primary Network (LAN) Settings

You can configure IPv4, IPv6, DNS, and LAN options for the Primary Network (LAN).

LAN Status Lights

The LAN connector on the Pano device has two lights to indicate connection status and traffic.

Indicator Light	Connection Status
Both lights off	No 10/100/1000 Base-T connection and no network traffic
Green and yellow lights on	10/100/1000 Base-T connection
Green light on and blinking yellow light	10/100/1000 Base-T connection with network traffic

Obtain IP Addresses Automatically

You can configure the Pano system to obtain its IPv4 and IPv6 addresses automatically.

You must have a DHCP server deployed in your environment.

Procedure

1. In the system web interface, go to **Network** > **LAN Network**.
2. Under the **Primary Network** section, select **Obtain IP address automatically** for **IP Address**.

   Some of your **IP Address (IPv4)** and **IP Address (IPv6)** settings populate automatically. You can’t change these settings manually.
3. Select **Save**.

Configure IPv4 Settings

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

Procedure

1. In the system web interface, go to **Network** > **LAN Network**.
2. Under the **Primary Network** section, select **Enter IP address manually** for the **IP Address** option.
3. Configure the settings under **IP Address (IPv4)** as needed.

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

4. Select **Save**.

Configure IPv6 Settings

You can configure the IPv6 settings for your Pano system.

Procedure

1. In the system web interface, go to **Network** > **LAN Network**.
2. Under the **Primary Network** section, select **Enter IP address manually** for the **IP Address** option.
3. Configure the settings under **IP Address (IPv6)** as needed.

Setting	Description
Enable IPv6	Enables the IPv6 network stack and makes the IPv6 settings available.
Enable SLAAC	Specifies whether to use stateless address autoconfiguration (SLAAC) instead of DHCP to automatically obtain an IP address.
Link-Local	Displays the IPv6 address used for local communication within a subnet.
Site-Local	Displays the IPv6 address used for communication within the site or organization.
Global Address	Displays the IPv6 internet address.
Default Gateway	Displays the default gateway assigned to the system. If your system doesn’t automatically obtain a gateway IP address, enter one here.

4. Select **Save**.

Configure DNS Settings

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

DNS settings apply to both the Primary network (LAN) and Secondary network (Wi-Fi).

Procedure

1. In the system web interface, go to **Network** > **LAN Network**.
2. In the system web interface, go to **Network** > **DNS**.
3. If the system does not automatically obtain a DNS server address, enter one on this page (up to four are allowed).
4. Select **Save**.

Configure LAN Options

There are several options for configuring the LAN in your Pano system web interface.

Procedure

1. In the system web interface, go to **Network** > **LAN Network**.
2. Under the **LAN Options** section, configure the following settings as needed:

Setting	Description
Host Name	Indicates the system name
Domain Name	The domain name assigned to the system. If the system does not automatically obtain a domain name, enter one here.
Autonegotiation	Specifies whether the system should automatically negotiate the **LAN Speed** and **Duplex Mode** per IEEE 802.3 autonegotiation procedures. If enabled, those settings become read-only. Polycom recommends that you use autonegotiation to avoid network issues.
LAN Speed	Specifies whether to use **10 Mbps**, **100 Mbps**, or **1000 Mbps** for the LAN speed. The duplex mode you choose must be supported by the switch.
Duplex Mode	Specifies the duplex mode to use. The duplex mode you choose must be supported by the switch.
Ignore Redirection Messages	Enables the system to ignore ICMP redirect messages.
ICMP Transmission Rate Limit (millisec)	Enter a number between 0 and 1000 to specify the minimum number of milliseconds between transmitted packets. The default value of 1000 signifies that the system sends

Setting	Description
	1 packet per second. If you enter 0, the transmission rate limit is disabled. This setting applies only to “error” ICMP packets and has no effect on “informational” ICMP packets, such as echo requests and replies.
Enable EAP/802.1X	Specifies whether 802.1X authentication is enabled. The following authentication protocols are supported: ▪ EAP-MD5 ▪ EAP-PEAPv0 (MSCHAPv2) ▪ EAP-TTLS ▪ EAP-TLS
EAP/802.1X Identity	Specifies the system's identity for 802.1X authentication. This setting is available only when EAP/802.1X is enabled. The field cannot be blank.
EAP/802.1X Password	Specifies the system's password for 802.1X authentication. This setting is required when EAP-MD5, EAP-PEAPv0, and EAP-TTLS are used.

Configuring the Secondary Network (Wi-Fi) Settings

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

Configure Wi-Fi Settings

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

Note: Note the following:

- When you select a non-default operating channel for Miracast, the secondary network is disabled to avoid frequency conflict with Miracast connections. If you don't use the secondary network, you can select a non-default operating channel which works best in your Wi-Fi environment.
- When you enable the secondary network, the **Miracast Operating Channel** option is disabled to ensure Miracast and the secondary network use the same channel. However, if the secondary network is connected to a Wi-Fi Access Point (AP) working on a Dynamic Frequency Selection (DFS) channel, Miracast may not work properly. This is because some Wi-Fi drivers don’t support DFS channels well.

Procedure

1. In the system web interface, go to **Network** > **Secondary Network**.
2. In the system web interface, go to **Network** > **Wi-Fi Network**.
3. From the **Choose Network Type** drop-down menu, select **Wi-Fi**.
4.
5. Select **Enable Administrator Access to This Network** to enable administrators to access the system web interface on the Wi-Fi network.

   For higher security, you can disable this option to limit access to the system web interface through LAN connections only.
6. Do one of the following:
   - Select a network from **Available Wi-Fi Networks**. (The system lists networks in order of signal strength.)
   - Enter the network name in the **SSID** field.

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

   Available settings vary with your selections.

Setting	Description
Security	Specifies the encryption protocol: ▪ **None** ▪ **WEP** ▪ **WPA/WPA2-PSK** ▪ **802.1xEAP**
Key (Passphrase/PSK)	Specifies an encryption passphrase (like a password) for the Wi-Fi network. You must enter the passphrase to connect to the Wi-Fi network. The maximum length of the passphrase or PSK is 48 characters.
EAP Method	Specifies the extensible authentication protocol (EAP) for WPA-Enterprise (802.1xEAP): ▪ **PEAP** ▪ **TLS** ▪ **TTLS** ▪ **PWD**
Phase 2 Authentication	Specifies the Phase 2 authentication method: ▪ **MSCHAPV2** ▪ **GTC**
Username	Specifies the login user name for WPA-Enterprise (802.1xEAP).
Password	Specifies the login password for WPA-Enterprise (802.1xEAP).

Setting	Description
IP Address	Select one of the following to set your system Wi-Fi network IP address: ▪ **Obtain IP address automatically** (You must have a DHCP server in your environment to use this option.) ▪ **Enter IP address manually**
Your IP Address Is	Specifies the IP address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
Subnet Mask	Specifies the subnet mask address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
Default Gateway	Specifies the IP gateway for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.
DNS Server	Specifics 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	Specifics the alternate DNS server address for the Wi-Fi network. This setting is read-only if your system gets its IP address automatically.

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

Related Links

Access the System Web Interface on page 8

Select the Miracast Operating Channel on page 36

Enable DFS on page 25

Enable DFS

You can enable Dynamic Frequency Selection (DFS) for Miracast and the secondary network on Pano.

Some Miracast-certified devices may not work as expected when connected to a DFS channel. In such cases, disable the **Allow DFS Channels** option. This forces the secondary network to select an available non-DFS channel to avoid signal interference.

DFS is disabled by default.

Procedure

1. Select **Network** > **Secondary Network**.
2. In the **Choose Network Type** option, select **Wi-Fi**.
3. Enable **Allow DFS Channels**.

Related Links

Select the Miracast Operating Channel on page 36

Enable DFS on page 25

Configure Wi-Fi Settings on page 23

Connect to a Hidden Wi-Fi Network on page 26

Connect to a Hidden Wi-Fi Network

Some Wi-Fi networks don't broadcast their SSID thus hide their presence for better security. You can enable Pano active scanning to find these networks.

To connect to a hidden network, you must know its SSID and password.

Procedure

1. In the system web interface, go to **Network** > **Secondary Network**.
2. Go to the **Choose Network Type** option and select **Wi-Fi**.
3. Select **Hidden Network**.

   To connect to a hidden Wi-Fi network, enter its SSID and password and then select **Connect**.

Related Links

Select the Miracast Operating Channel on page 36
Enable DFS on page 25

Disable the Secondary Network (Wi-Fi)

You can disable the Wi-Fi network.

Procedure

1. Select **Network** > **Secondary Network**.
2. For the **Choose Network Type:** option, select **No Secondary Network**.
3. Select **Save**.

Monitor Settings

Topics:

- HDMI I/O
- Supported Displays
- Configure Monitor Settings

The Pano device supports a variety of resolutions on touch-capable and non-touch monitors.

Note: The Pano device monitor must support a minimum of 1280×720 resolution.

Related Links
Access the System Web Interface on page 8

HDMI I/O

Your Pano system has HDMI input and output ports.

Your system has the following HDMI connections:

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

Note the following:

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

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 Input Resolutions

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

Supported HDMI Input Resolutions and Frame Rates

Input	Resolution	Frame Rate(s)
UHD	3840 x 2160p	24, 25, 30
QHD	2560 x 1440p	50, 60
FHD	1920 x 1080p	50, 60
WSXGA+	1680 x 1050	60
UXGA	1600 x 1200	60
SXGA	1280 x 1024	60
HD	1280 x 720p	50, 60
XGA	1024 x 768	60
SVGA	800 x 600	60

Supported HDMI Output Resolutions and Frame Rates

The Pano system supports the following output resolutions for local interface monitor connections.

Supported HDMI Output Resolutions and Frame Rates

Resolution	Frame Rates
2160p	25, 30, 50, 60
1080p	25, 30, 50, 60
720p	25, 30, 50, 60

Supported Displays

The Pano device can present content streams on user-supplied non-touch and touch displays that support up to 4K (UHD) 60 fps RGB444 output over HDMI 2.0.

Polycom recommends that you use a display that supports the same input and visual output.

Tested Touch-Capable Monitors

The Pano device supports single- and multi-touch input from a HID-compliant device.

The following touch-capable monitors have been tested with the device and provide an optimal touch experience.

Tested Touch-Capable Monitors

Size (inches)	Touch Technology	Brand	Model/Part Number
23	Capacitive	Acer	T232HL
22	Capacitive	Elo®	E497001
46	Capacitive	Elo®	ET4602L
55	InGlass™	Dell	C5518QT (black)
65	InGlass™	Volanti	VD-6500-0B0C-1100 (black)
65	InGlass™	Volanti	VD-6500-0Q0C-16P3 (white)
65	InGlass™	Avocor	AVF-6550
70	IR	Sharp	PN-L703B (black)
75	InGlass™	Dell	C7520QT
86	InGlass™	Dell	C8618Q7

Configure Monitor Settings

You can configure the Pano system monitor settings to optimize the video output.

Procedure

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

Setting	Description
Configure Monitor	Specifies the monitor setting: ▪ **Automatic** The default setting specifies that the **Resolution** setting is automatically detected. ▪ **Manual** Lets you select the **Resolution** setting.
Resolution	Specifies the monitor resolution. This setting is unavailable when you select **Automatic** for the **Configure Monitor** setting.

Your changes save automatically.

Related Links

Display IP Addresses on System Status Bar on page 15

Security

Topics:

For detailed information about configuring security settings, see the following topics.

Related Links

Access the System Web Interface on page 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 Pano system.

PKI certificates authenticate secure network connections to and from the Pano 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 RealPresence Resource Manager in a secure environment.

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

How the System Uses PKI Certificates

PKI certificates authenticate secure network connections to and from the Pano 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 a PKI, you don’t need a CA-signed certificate; the system comes with a self-signed certificate for its TLS connections. When you deploy a 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 web browser over a secure connection to your system web interface, create a CSR and install the resulting CA certificate chain on your system to replace its factory-installed certificate, which is not trusted.
- If you want to provision your system using RealPresence Resource 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 Pano system or device is trusted by its network peers.

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

Procedure

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

CSR Information	Description
Hash Algorithm	Specifies the hash algorithm for the CSR: SHA-256 (recommended) or SHA-1 (not recommended).
Common Name (CN)	Specifies the system name. This is a required field. Maximum characters: 64 (truncated if necessary). Poly recommends the following guidelines for this field: ▪ For systems registered in DNS, use the system's FQDN. ▪ For systems not registered in DNS, use the system's IP address.

CSR Information	Description
Organizational Unit (OU)	Specifies the unit of business defined by your organization. Default is blank. Maximum characters: 64. **Note:** The system supports only one OU field. If you want the signed certificate to include more than one OU field, you must download and edit the CSR manually.
Organization (O)	Specifies your organization's name. Default is blank. Maximum characters: 64.
City or Locality (L)	Specifies the city where your organization is located. Default is blank. Maximum characters: 128.
State or Province (ST)	Specifies the state or province where your organization is located. Default is blank. Maximum characters: 128.
Country (C)	Displays the country selected in the setup wizard. You can't change this setting here.
SAN: FQDN	Specifies the FQDN assigned to the system. This is the same as the **Common Name (CN)**, but it isn't truncated. Default is blank. Maximum characters: 253.
SAN: Additional Name	Specifies an additional name. Default is blank. Maximum characters: 253.
SAN: IPv4 Address	Default is the IPv4 address of the system. Maximum characters: 15.
User Principle Name (UPN)	Specifies the user and domain name to log in to a Windows domain (for example, `UserName@YourDomain.com`). This is the `userPrincipalName` attribute of the account object in Active Directory. Relate this setting to the 802.1X identity and password you specified on the **Network** > **LAN Options** page. Default is blank.

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

Configure Certificate Validation Options

The Pano 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 Pano system.

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

Procedure

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

Setting	Description
Maximum Peer Certificate Chain Depth	Specifies how many links a certificate chain can have. The term *peer certificate* refers to any certificate sent by the far-end host when a network connection is being established between the two systems.
Always Validate Peer Certificates From Server	Determines whether your system requires a remote server to present a valid certificate when connecting to it for services, such as provisioning.
Always Validate Peer Certificates From Browser	Determines whether your system requires a web browser to present a valid certificate when connecting to it. **Note:** If you are using private PKI certificates in your environment and want HTTPS software downloads to work, you must install the trusted root certificate from your internal certificate authority (CA) on the system since certificate validation is always performed.
Disable Preinstalled Certificates	Disables preinstalled root certificate CA chains.

Install a Certificate

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

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

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

Procedure

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

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

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

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

View a Certificate

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

Procedure

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

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

   The certificate contents display in plain text.

Delete a Certificate

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

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

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

Procedure

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

   Caution: You can't undo this action.
3. Confirm by selecting **Delete**.

   A message indicates that the system deleted the certificate.

Change Local Account Credentials

The Pano system administrator ID and password you created while running the setup wizard can be changed.

Procedure

1. In the system web interface, go to **Security** > **Local Accounts**.
2. Change your credentials (username or password) and select **Save**.

Disable the Security Code

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

Procedure

» Disable the security code in one of the following ways, depending on your setup:

- In the system web interface, go to **Security** > **Security Code** and clear the **Enable Security Code** check box. This setting is read-only if your system is registered to the Polycom Cloud Service.
- Edit the system settings in the Polycom Cloud Service Administration portal.
- Update the system’s provisioning profile in RealPresence Resource Manager.

Related Links

Enforce Security Code for Every Connections on page 37

Wireless and Screen Mirroring Options

The Pano system includes Wi-Fi and Bluetooth wireless communication options so your users can discover the system on the network with the Polycom Content App or their AirPlay- or Miracast-certified device. You can enable or disable these features as needed.

The animations that display on the Pano system home screen correspond to the system settings for wireless communication and screen mirroring.

Audio transmission in Miracast mirroring is best-effort. For Windows 10 or Android devices, Miracast audio-video synchronization isn’t guaranteed.

Polycom Miracast implementation uses peer-to-peer Wi-Fi connections and is subject to the same environmental factors as typical Wi-Fi connections are. Multiple factors can impact Miracast performance. For example, your OS version, Wi-Fi or video card driver versions, and your computer performance level.

Wireless Bands for Miracast-Certified Devices

Miracast-certified devices require the 2.4 GHz band for negotiating a connection to the Pano system, using one of three 802.11 channels (1, 6, or 11).

Once a connection is established, a device that supports the 5 GHz band can choose that frequency instead of the 2.4 GHz band to avoid interference.

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

Enable Wireless Settings

You can enable the wireless communication features so users can share content from Miracast- and AirPlay-certified devices.

Note: Enabling a wireless communication option doesn’t automatically allow content sharing. You must also allow screen mirroring.

Procedure

1. In the system web interface, go to **Security** > **Wireless and Screen Mirroring**.
2. Select **Menu** ≡.
   - Select the **Enable Wi-Fi** option to enable Wi-Fi hardware. You must turn on Wi-Fi before you can enable screen mirroring for Miracast-certified devices.
   - Select the **Enable Bluetooth** option to enable Bluetooth hardware. You must turn on Bluetooth before you can enable screen mirroring for AirPlay-certified devices.

- Select **Enable AirPlay** to enable screen mirroring for AirPlay-certified devices.
- Select **Enable Miracast** to enable screen mirroring for Miracast-certified devices.

Notes on Miracast

Note the following information when you use Miracast.

- The secondary network can impact the Miracast screen mirroring quality. For best results, disable the secondary network when using Miracast.
- If the Wi-Fi network is enabled, the same 802.11 channel is also used for the Miracast connections.
- When you disable Miracast, both the **Require PIN Every Connection** and **Operating Channel** options are reset to their default values.

Miracast Operating Channel

Pano system uses the operating channel to transmit Miracast mirroring content.

Notes on Default Operating Channel

Pano selects the **DEFAULT** channel automatically so the system can support both Miracast and the secondary network at the same time.

When you enable the secondary network, the **Miracast Operating Channel** option is disabled to ensure Miracast and the secondary network use the same channel. However, if the secondary network is connected to a Wi-Fi Access Point (AP) working on a Dynamic Frequency Selection (DFS) channel, Miracast may not work properly. This is because some Wi-Fi drivers don't support DFS channels well.

Notes on Selecting a Non-default Operating Channel

If you don't use a secondary network, you can select a non-default Miracast operating channel to provide the best performance in your environment.

Note the following when you choose a non-default channel:

- Select a channel with less channel saturation in your Wi-Fi environment. Channel saturation impacts the quality of the mirrored content.
- Select the same channel as the Wi-Fi Access Point (AP). This reduces channel switching from the Miracast clients. Channel switching leads to latency in your mirrored content.

Note: When you disable Miracast screen mirroring, the operating channel resets to its default value.

Select the Miracast Operating Channel

You can specify the Miracast operating channel for better content quality.

Make sure you're not in a content mirroring session. You can't change the operating channel during an ongoing content mirroring session.

Procedure

1. In the system web interface, go to **Security** > **Wireless and Screen Mirroring**.
2. Select the **Enable Miracast** option to enable screen mirroring for Miracast-certified devices.
3. Select an **Operating Channel**.

Related Links

Configure Wi-Fi Settings on page 23

Enable DFS on page 25

Connect to a Hidden Wi-Fi Network on page 26

Miracast over Infrastructure

Miracast over Infrastructure allows your Windows devices to send a Miracast stream to Pano over a local network rather than over a direct wireless link.

Pano automatically detects the availability of the local network and switches the video stream over this path if applicable.

Miracast over Infrastructure is not a replacement for standard Miracast. Instead, the functionality is complementary, and provides an advantage to users who are part of the enterprise network. Users who are guests to a particular location and don't have access to the enterprise network will continue to connect using the Wi-Fi Direct connection method.

Enable Miracast over Infrastructure

This feature enables your Windows–based devices to send a Miracast stream to Pano over a local network rather than over a direct wireless link.

- Only Windows 10 devices with build 1703 or later support this feature.
- The Windows 10 firewall automatically allows inbound TCP ports 7250 and 7236. If a third-party firewall application blocks these ports, you may need to add these two inbound ports.
- Pano and the Miracast casting source device must be on the same enterprise network via Ethernet or a secure Wi-Fi connection.
- The Miracast casting source can automatically resolve the Pano IP address via mDNS. The mDNS multicast must be received by the Windows client.

Note: Pano doesn't ask for PIN if a device connects to Pano using Miracast over Infrastructure.

Procedure

1. In the system web interface, go to **Security** > **Wireless and Screen Mirroring**.
2. Under **Miracast**, select **Miracast over Infrastructure**.

Enforce Security Code for Every Connections

For enhanced security, you can require Windows Miracast users to enter a security code each time before they can connect to Pano.

Note the following:

- You must enable Pano's **Security Code** feature before you can use this feature.
- This feature applies only to version 1709 and above on Windows 10.
- You can't change the **Require PIN Every Connection** option during an ongoing content mirroring session.
- Updates to the **Require PIN Every Connection** setting takes about one to five minutes to take effect. During that time, you can't connect to Pano through Miracast.
- When you disable Miracast, the **Require PIN Every Connection** option is reset to its default value.

Procedure

1. In the system web interface, go to **Security** > **Wireless and Screen Mirroring**.
2. Select the **Enable Miracast** option to enable screen mirroring for Miracast-certified devices.
3. Select **Require PIN Every Connection**.

It takes about one two five minutes for this change to take effect. During that time, you can't connect to Pano through Miracast.

Related Links

Disable the Security Code on page 34

Disable Wireless Settings

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

Remember the following when disabling wireless features:

- Disabling Wi-Fi turns off the Wi-Fi network functionality and screen mirroring with Miracast-certified devices.
- Disabling Bluetooth turns off screen mirroring with AirPlay-certified devices and prevents those devices and the Polycom Content App from automatically discovering your Pano system. (You can still connect with the Polycom Content App using the system IP address.)

Procedure

1. In the system web interface, go to **Security** > **Wireless and Screen Mirroring**.
2. Specify your preferences:
   - Clear the **Enable Wireless Connectivity** check box.
   - Clear the **Enable Bluetooth** check box.

   Your preferences automatically update.

Encryption

The following table lists the product capabilities that are supported but not necessarily required. Requirements vary based on the customer environment.

Note: More detailed information is available under NDA in the form of Product Encryption Data Sheets. Please contact your Polycom representative for more details.

Application	Encryption Function	Description	Protocol Used
Secure Boot	Authentication Integrity	Procedure to verify that basic software assets are not compromised (i.e., replaced or modified by hackers). During system bootup, the Pano device verifies that only a valid bootloader and Boot Configuration Table (BCT) images can execute.	PKCS #1

Application	Encryption Function	Description	Protocol Used
Software signing (OTA)	Authentication Integrity	Software signing process that ensures hackers do not create a fake OTA file for a software upgrade package to replace the software images on the Pano device. This verification is done during the software update process when the OTA signature is compared with a locally stored certificate before allowing the Android system to continue the procedure.	PKCS #8 (RFC 5208)
AirPlay	Confidentiality Integrity	A proprietary Wi-Fi streaming protocol for sending media from an AirPlay-certified device to the Pano device.	Apple AirPlay
Miracast	Confidentiality Integrity	Encrypted content casting protocol for sending media from a Miracast-certified device to the Pano device using a dedicated, short-range wireless 802.11 network connection.	RSN (WPA2/IEEE 802.11i)
Device Proxy Client	Authentication Integrity Confidentiality	Allows the Pano device to communicate with the Polycom Cloud Service to discover its tenant ID and register with that tenant's cloud services. The connections are signaling only; no media is passed. Connections are made to the Global Directory Service, Device Discovery Service, Tenant Directory Service, Device Authentication Service, Polycom Cloud Service Device Authentication Service, and Device Proxy and Registry.	TLS 1.1 and 1.2

Application	Encryption Function	Description	Protocol Used
Cluster Control Service Client	Authentication Integrity Confidentiality	Allows the Pano device to retrieve PIN codes from the Polycom Cloud Service for the room device cluster.	TLS 1.1 and 1.2
RealPresence Group Series Pairing Client	Authentication Integrity Confidentiality	Allows pairing with a RealPresence Group Series system so that it can control the content-sharing functions of the Pano device.	TLS 1.1 and 1.2
Analytics Client	Authentication Integrity Confidentiality	Allows the Pano device to send analytic information to the Polycom Cloud Service.	TLS 1.1 and 1.2
Software Update Client	Authentication Integrity Confidentiality	Allows the Pano device to check for and get software update images from a configured software update server over an encrypted channel.	TLS 1.1 and 1.2
Content App Screen/App Share Media Server	Confidentiality Integrity	Media connection from a device using the Content App to the Pano device.	Proprietary session-layer protocol over UDP
Content App Screen/App Share Signaling Server (Port 5001)	Confidentiality Integrity	Used by the Content App to set up the screen and application sharing sessions with the Pano device (no media flows over this connection; there is only signaling).	TLS 1.1 and 1.2
Management API Server (Port 443)	Authentication Integrity Confidentiality	Provides a local management interface over HTTPS. It is used for the system web interface and REST API, which retrieves saved snapshot images from the Pano device.	TLS 1.1 and 1.2

Enable or Disable Content Saving

Enable or disable content saving from the Pano App for users who connect to the primary or secondary network.

Procedure

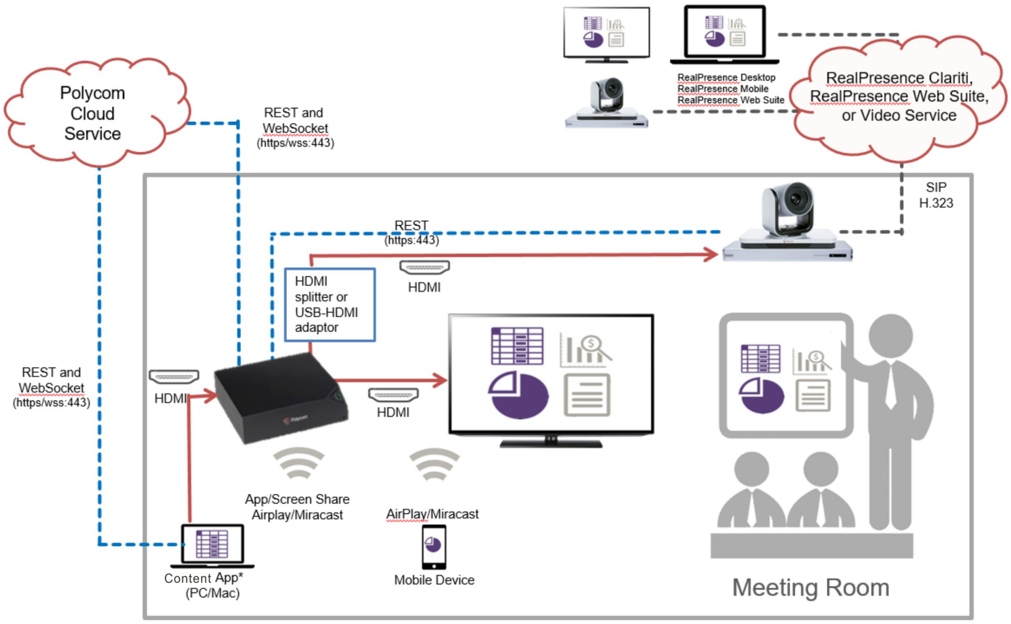
1. In the system web interface, go to **Security** > **Content**.
2. Select or deselect **Allow users to save content from Primary Network** and **Allow users to save content from Wi-Fi Network**.

Content Sharing

Topics:

- Content Sharing Options

The Pano device lets users connect and share content from personal smartphones, tablets, laptops, and desktop systems.


RealPresence Desktop
RealPresence Mobile
RealPresence Web Suite
RealPresence Clariti, RealPresence Web Suite, or Video Service
Polycom Cloud Service
REST and WebSocket (https/wss:443)
SIP H.323
REST (https:443)
HDMI splitter or USB-HDMI adaptor
HDMI
REST and WebSocket (https/wss:443)
HDMI
HDMI
App/Screen Share Airplay/Miracast
AirPlay/Miracast
Content App* (PC/Mac)
Mobile Device
Meeting Room

Content Sharing Options

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

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

  You can disable these options in the system web interface.
- **Wired input**: A laptop or desktop connected to the system through HDMI.
- **Polycom Content App**: Installed on a Microsoft Windows or Apple Mac system for wireless screen or application sharing.

System Maintenance

Topics:

- Resetting the System
- Updating System Software
- Downgrading System Software

Providing maintenance to your Pano system includes resetting it and upgrading the software.

Related Links
Access the System Web Interface on page 8

Resetting the System

If your Pano system is not functioning correctly, you can reset it to its default configuration or factory settings.

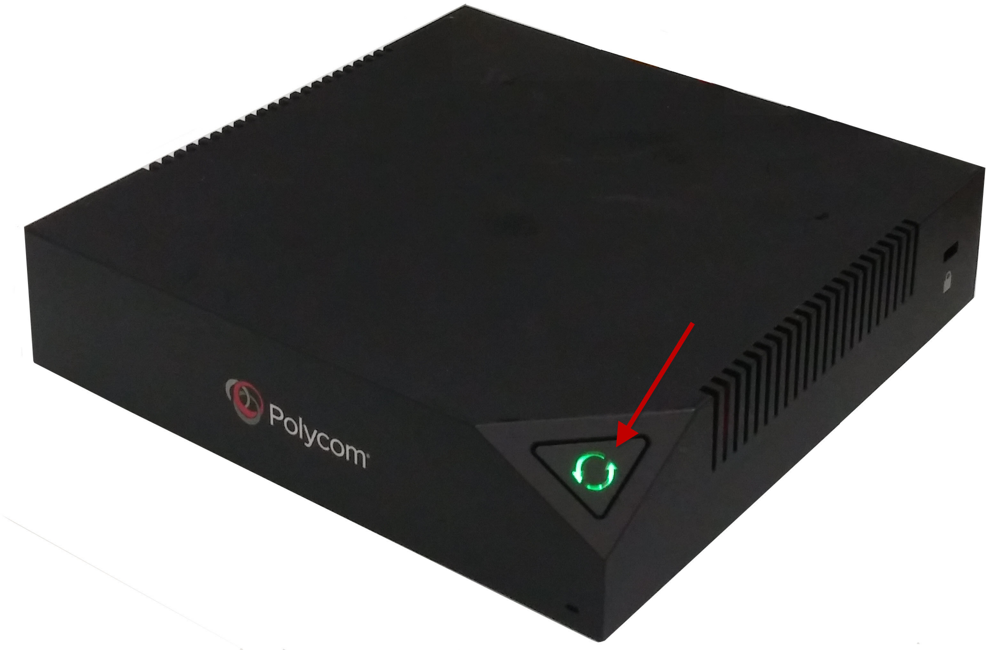
Perform a Factory Reset

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

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

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

The Pano system reset button that you use to initiate the factory reset process is located on the front of the device, displayed in the following figure:



Procedure

1. Do one of the following to restart the system:
   - In the system web interface, go to **Diagnostics** > **System Reset** and select **Restart**.
   - Disconnect and reconnect the power adapter cable and network cable (if the system is powered by PoE+).
2. When the LED on the reset button turns white, immediately press and hold it for ten seconds (make sure your finger fully covers the button).

   This interrupts the system startup and initiates the factory reset process. The LED alternates blue and amber lights during this time.

   If the LED blinks a blue light after you press the reset button, an interruption of the system startup did not occur.
3. If the interruption did not occur, wait for the startup to complete and repeat the process.

The system restarts automatically when the factory reset process is complete.

Reset System Settings

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

Resetting your system deletes all but the following data:

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

Procedure

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

4. Optional: If you have user-installed PKI certificates that you do not want to retain, deselect the **Keep installed certificates** checkbox.
5. Select **Restart**.

   After about 15 seconds, the system restarts and displays the setup wizard.

Updating System Software

Use one of the following methods to update system software:

- Poly download server
- Custom server URL
- Provisioning service (for example, RealPresence Resource Manager)
- Polycom Cloud Service
- Software package you obtain from the Poly Online Support Center and upload with a USB flash drive

Choose a Software Update Method

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

Procedure

1. In the system web interface, go to **General Settings** > **Software Update**.
2. Select one of the following in the **Download Update From** field (some options may not be available based on how your system is configured):

Software Update Location	Description
Poly Online Support Center	A software server hosted by Poly.
Custom Server URL	A server on your network that supports HTTP or HTTPS downloads. The URL is the path to the latest software build folder (for example, `https://`*`<system_build_folder>`*). The folder should contain the following: ▪ `release.json` ▪ *`<system>`*`-`*`<version>`*`.json` ▪ *`<system>`*`-`*`<version>`*`.zip`
Provisioning Server	Receive updates from a provisioning service, such as RealPresence Resource Manager.
Polycom Cloud Service	Receive updates from the service if your device is registered to it.

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 have selected where to download software updates from, you can manually or automatically update the system and its paired devices.

Related Links

Provisioning Service on page 18

Register with Polycom Cloud Service on page 16

Manually Update Software

You can manually update the Pano system software.

Procedure

1. In the system web interface, go to **General Settings** > **Software Update**.
2. Select **Check for Updates**.
3. If updates are found, select **Update**.

Automatically Update Software

You can automatically update the Pano system software.

Note: Automatic software updates are enabled by default when your system is registered to the Polycom Cloud Service.

Procedure

1. In the system web interface, go to **General Settings** > **Software Update**.
2. Select **Enable Automatic Updates**.

   Unless you specify a maintenance window, your system tries to update 1 minute after you enable this setting. If an update isn't available at the time, the system tries again every 4 hours.
3. Optional: Select **Only Check for Updates During Maintenance Hours** to specify a range of time to automatically update the software.
4. Optional: Choose times for **Maintenance Hours Begin** and **Maintenance Hours End**.

   The system calculates a random time within the defined maintenance window to check for updates.

   Note: If these settings are provisioned, the provisioning profile defines the polling interval. The default interval is 1 hour.

Your changes save automatically.

Update System Software from a USB Flash Drive

You can place the firmware files for your system and any paired devices onto a flash drive and use the flash drive to update your system.

Procedure

1. Obtain the software package from the Poly Online Support Center.
2. Save the software upgrade package to the root directory of a USB flash drive.
3. Connect the USB flash drive to the USB 2.0 port on the back of the device. This is the top USB port.

   The device detects the USB flash drive and displays a prompt on the monitor for you to confirm that you want to update the software.
4. Select **OK**.

5. Follow the setup wizard instructions to complete the update.

Downgrading System Software

You can downgrade the software on your Pano system to an earlier version using any of the supported software update methods.

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

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

Polycom Cloud Service

Topics:

- The Poly Cloud Services Portal
- Polycom Cloud Service Administration Guide

The Polycom Cloud Service is an offering that provides connection authentication and pushes software updates for Content App and Pano users.

Keep the following in mind about the Polycom Cloud Service:

- Polycom Pano systems use standard HTTPS connections to communicate with the Polycom Cloud Service. The Polycom Cloud Service authenticates each Polycom Pano device prior to accepting connections from it; similarly, Polycom Pano systems authenticate the Polycom Cloud Service's identity before completing a connection to it.
- Polycom Content App uses standard HTTPS connections to communicate with the Polycom Cloud Service. Polycom Content App authenticates the identity of the Polycom Cloud Service prior to connecting to it. The Polycom Cloud Service uses the industry-standard OAuth 2.0 protocol to enable access to your enterprise Office 365 services via the Polycom Content App. This allows users to sign in directly to Office 365 without the Polycom Content App or the Polycom Cloud Service ever having access to user credentials.

Related Links

Access the Polycom Cloud Service Administration Portal from the System Web Interface on page 9

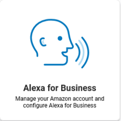
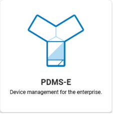
Access the Polycom Cloud Service Administration Portal from an Assigned URL on page 10

The Poly Cloud Services Portal

The Poly Cloud Services portal is the central point where you can set up and use Poly Cloud Services.

The Poly Cloud Services portal includes the following features:

Poly Cloud Services

Portlet Name	Description
Alexa for Business  Alexa for Business Manage your Amazon account and configure Alexa for Business	Manage your Amazon account and configure Alexa for Business.
PDMS-E  PDMS-E Device management for the enterprise.	Device Management Service for your Enterprise.

Portlet Name	Description
Register Devices Register Devices Connect devices to the cloud.	Connect devices to the cloud.
Administration Administration Manage services and users across cloud applications.	Manage services and users across cloud applications.

Polycom Cloud Service Administration Guide

For more information about Polycom Cloud Service Administration Portal, refer to Polycom Cloud Service Administration Guide.

Troubleshooting

Topics:

- Blurry Miracast Video
- Retrieve Log Files
- Contact Polycom Support

There are ways to troubleshoot if you experience issues with your Pano system.

Blurry Miracast Video

When you cast content using Miracast mirroring, the content may be blurry on the far end due to limitations on your Miracast device.

There are two possible causes for this problem.

Cause 1:

The Miracast device lacks resources to encode the mirrored content.

This may happen when your device screen refreshes too quickly. For example, when you browse a dense Excel sheet.

Workaround :

Lower your device screen resolution, or close unnecessary applications or processes.

Cause 2:

The Miracast device can't send the mirrored content out. This may happen when the Pano **Operating Channel** and the WLAN Access Point (AP) channel that your Miracast device uses to access the internet are working on different frequency bands.

Workaround:

Set the Pano **Operating Channel** and the WLAN Access Point (AP) channel that your Miracast device uses to access the internet are working on to the same channel. For example, if your device accesses the internet from a WLAN AP using 5 GHz channel ID 36, then set your Pano **Operating Channel** to the same channel.

Retrieve Log Files

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

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

Procedure

1. Access the web interface by opening a web browser and entering the IP address of the Polycom Pano 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.

Contact Polycom Support

If you are not able to share content successfully and you have verified that the equipment is installed and set up correctly, contact Polycom Support. Be prepared to provide the Pano system logs an details about the issue you are experiencing.

Procedure

1. Make notes of any active alerts generated by the system, and any troubleshooting steps that you have already tried.
2. Go to the Polycom Support site and create a Problem Report ticket that includes the downloaded system logs and a description of the problem.