# Contents

Before You Begin ............................................................................................................................. 5
  Get Help....................................................................................................................................... 5

Getting Started................................................................................................................................. 6
  Features and Capabilities................................................................................................................. 6
    Hardware Features....................................................................................................................... 6
  System Indicator Lights.................................................................................................................... 8
  Powering On and Off....................................................................................................................... 8
    Power On the Device.................................................................................................................... 8
    Power Off the Device................................................................................................................... 9
  Managing the System....................................................................................................................... 9
    Access the System Web Interface.............................................................................................. 9
    Access the Polycom Cloud Service Administration Portal from the System Web Interface........ 10
    Access the Polycom Cloud Service Administration Portal from an Assigned URL.................. 10

System Hardware.............................................................................................................................. 11
  Connect a Touch-Capable Monitor................................................................................................. 11
  Connect a Non-Touch Monitor....................................................................................................... 11
  Positioning the System.................................................................................................................. 12
    Mount the System on a Wall......................................................................................................... 12
    Mount the System on a Monitor.................................................................................................. 13

Setup Wizard..................................................................................................................................... 15
  Modes of Operation...................................................................................................................... 15
  Change System Default Credentials........................................................................................... 15
  Set Up System Manually.............................................................................................................. 16
  Provision the System.................................................................................................................... 16

General Settings............................................................................................................................... 17
  Set the Local Interface Language................................................................................................. 17
  Set the System Web Interface Language.................................................................................... 17
  Set the Date and Time................................................................................................................... 17
  Set Device and Room Names...................................................................................................... 18
  Register with Polycom Cloud Service.......................................................................................... 18
Content Sharing............................................................................................ 41
  Content Sharing Options........................................................................... 41

System Maintenance............................................................................... 43
  Resetting the System........................................................................... 43
  Perform a Factory Reset....................................................................... 43
  Delete System Settings....................................................................... 44
  Updating System Software................................................................... 45
    Choose Software Update Location in System Web Interface............... 45
    Manually Update Software.................................................................. 45
    Automatically Update Software....................................................... 46
    Update Software from a USB Storage Device................................... 46
  Downingrading System Software....................................................... 47

Polycom Cloud Service........................................................................... 48
  Polycom Cloud Service Administration Account Activation Process...... 48
    Activate a Polycom Cloud Service Administration Account.............. 49
    Complete Account Activation.......................................................... 49
  Sign in with Your Administration Account........................................... 50
  Integrate with Microsoft Office 365.................................................... 50
  Authentication Providers...................................................................... 52
    Enable or Disable a Built-In Authentication Provider.................... 52
    Add Office 365 as a Custom Authentication Provider.................... 53
    Add ADFS as a Custom Authentication Provider............................ 54
    Edit or Delete a Custom Authentication Provider............................ 55
  Document Services............................................................................... 55
    Add Office 365 OneDrive for Business as a Document Service........ 55
    Edit or Delete the Integrated Document Service.............................. 56
  Device Management............................................................................. 56
    Edit or Delete a Registered Device.................................................. 57
  User Management................................................................................. 58
    Polycom Cloud Service Enterprise Administrator.......................... 59
    Add an Administration Account....................................................... 59
    Edit or Delete an Administration Account...................................... 60
    Change User Interface Language...................................................... 61
  User Password..................................................................................... 61
  Sign Out............................................................................................... 62

Integrating with a Polycom Video System............................................. 63
Supported Polycom Video Systems.................................................................63
Connecting a Polycom Video System Using Two Monitors............................64
  Direct Connection Setup..................................................................................64
  HDMI Splitter Setup.......................................................................................65
  HDMI USB Adapter Setup..................................................................................67
  Complete the Two-Monitor Setup (HDMI Splitter or HDMI USB Adapter)......69
Connecting a Polycom Video System Using Three Monitors............................71
  Complete the Three-Monitor Setup...............................................................72
Test Content Sharing.........................................................................................74
Unpair a Polycom Video System.........................................................................75

Troubleshooting.................................................................................................76
  Retrieve Log Files............................................................................................76
  Contact Polycom Support..................................................................................76
Before You Begin

Topics:

- Get Help

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

The following related documents are available at Polycom Support:

- Polycom Pano User Guide, which provides instructions about how to use the Pano device
- Setup sheets for your hardware
- Release notes
- Polycom Pano Safety and Regulatory Notices, which describes safety and legal considerations with using the Pano device

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 Polycom products, refer to Polycom Support.
Getting Started

Topics:

- **Features and Capabilities**
- **System Indicator Lights**
- **Powering On and Off**
- **Managing the System**

**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® Pano™ App, and HDMI connections.
- Integration with supported Polycom video systems.
- Integrated toolbar with high-performance annotation capabilities.
- Cloud connectivity for content sharing and 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.

**Hardware Features**

Polycom designed the Pano device system to be always connected and powered. The system includes limited cable connections to simplify setup, and its compact design fits most space requirements.
### Front and Side Feature Descriptions

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Feature</th>
<th><img src="image.png" alt="Image" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LED indicator of system status and button to initiate factory reset</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Security cable lock slot on the side</td>
<td></td>
</tr>
</tbody>
</table>

### Back Panel Feature Descriptions

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HDMI input port</td>
</tr>
<tr>
<td>2</td>
<td>Analog audio output</td>
</tr>
<tr>
<td>3</td>
<td>HDMI output port</td>
</tr>
<tr>
<td>4</td>
<td>USB 3.0 host port</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>5</td>
<td>USB 2.0 host port</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>6</td>
<td>10/100/1000 Ethernet port</td>
</tr>
<tr>
<td></td>
<td>The device ships with this Ethernet port covered. This port is reserved for future use.</td>
</tr>
<tr>
<td>7</td>
<td>10/100/1000 Ethernet port powered with PoE+ PD</td>
</tr>
<tr>
<td></td>
<td>This port supports IEEE 1588 for time synchronization with devices in a room.</td>
</tr>
<tr>
<td>8</td>
<td>2.0 mm jack for optional external 54 V DC power adapter</td>
</tr>
</tbody>
</table>
### System Indicator Lights

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

<table>
<thead>
<tr>
<th>Indicator Light</th>
<th>System Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off or blinking red light</td>
<td>System is disconnected, cannot initialize, or has encountered a severe malfunction</td>
</tr>
<tr>
<td>Steady white light</td>
<td>System is initializing</td>
</tr>
<tr>
<td>Steady blue light</td>
<td>System is running</td>
</tr>
<tr>
<td>Alternating blue and amber lights</td>
<td>System is in software update or factory restore mode</td>
</tr>
</tbody>
</table>

### Powering On and Off

The Pano device remains in an awake state. It does not have a power button or power-saving or monitor sleep modes.

You can power the Pano 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**

1. 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**

Using a supported browser with cookies enabled, you can access the Pano system web interface.

**Procedure**

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

   **Note:** The HTTPS protocol ensures that login information is transmitted using an encrypted channel, including usernames and passwords for communicating with third-party systems on your network. Using HTTPS severely limits the ability of anyone on the network to discover these credentials. For this reason, attempts to use the system web interface via HTTP are redirected to the HTTPS interface.

2. Enter your administrator credentials.

   The default Admin ID is `admin`, and the default admin password is the last six digits of the Pano device serial number. You can find the serial number on a sticker on the back of the device, on the shipping container, or on the Dashboard screen of the system web interface.

3. Select Login.

**Related Links**

*General Settings* on page 17
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 10
System Hardware

Topics:
- Connect a Touch-Capable Monitor
- Connect a Non-Touch Monitor
- Positioning the System

The Pano system needs to be connected to a monitor and can be mounted on table, wall, or monitor.

Note: To prevent the Pano system from overheating, make sure there is at least 1 in. of space on top and 2 in. on the sides with the ventilation openings (this does not apply to the sides with the input/output ports, mounting plate, or prominently displayed Polycom logo).

Connect a Touch-Capable Monitor

The Pano system automatically detects when a touch-capable monitor or USB pointing device (e.g., a USB mouse) is connected.

Procedure
1. Connect the HDMI cable from the system to the monitor.
2. Connect the USB cable to the bottom USB port for touch capability.
3. Connect the LAN cable to the system for network connectivity or to power it with PoE+.
4. Optional: Connect a power adapter to the system.

Connect a Non-Touch Monitor

The Pano system automatically detects when a touch-capable monitor or USB pointing device (e.g., a USB mouse) is not connected.

The non-touch experience has the following characteristics during a content-sharing session:
- The Toolbar, content tray, and panel bar are unavailable.
- Content is displayed in full-screen mode and according to the aspect ratio of the connected device.
- Users end sessions by disconnecting their devices.

Procedure
1. Connect the HDMI cable from the system to the monitor.
2. Connect the LAN cable to the system for network connectivity or to power it with PoE+.
3. Optional: Connect a power adapter to the system.
Positioning the System

You can mount the Pano system on a table, wall, or monitor.

If you mount the system on a tabletop, desk, or shelf, position the cables away from foot traffic to prevent accidental disconnections or damage.

Mount the System on a Wall

You can mount the Pano system on a wall.

Before you begin, make sure all cables are disconnected from the system.
Procedure

1. Attach the two shoulder screws from the mounting kit to the bottom of the system.

2. Draw a horizontal line on the wall to indicate the location of the mounting plate.
   The line must be level to ensure the system is properly installed. Use a level, if necessary.

3. Add the screws:
   a. Drill four 4.8 mm holes in the desired location on the wall where you want to position the system. These holes should be horizontal and vertical in alignment with the holes on the mounting plate. Insert expanding tubes into the four holes.
   b. Using a #2 Phillips screwdriver and the screws in the mounting kit, screw the mounting plate to the wall.

4. With the back panel facing up, insert the heads of the two shoulder screws on the system into the corresponding holes on the mounting plate. Then, gently push the device down until you hear a lock that indicates the system is secure.

5. Connect the cables, making sure to position them so that they are kept neatly in place and away from heavy foot traffic to prevent accidental cable disconnections or damage.

Mount the System on a Monitor

You can mount the Pano system on the back of a monitor.

Before you begin, make sure all cables are disconnected from the system.

The Pano system mounting kit includes a mounting plate with 50 mm, 75 mm, and 100 mm VESA Mounting Interface Standard (MIS) hole patterns. If your monitor has a different VESA hole pattern, you may be able use a VESA adapter plate (refer to the manufacturer’s documentation).
Procedure

1. Attach the two shoulder screws from the mounting kit to the bottom of the system.

2. Using the four 4.5 mm screws included in the mounting kit, attach the mounting plate to the back of the monitor.

3. With the back panel facing up, insert the heads of the two shoulder screws on the system into the corresponding holes on the mounting plate. Then, gently push the system down until you hear a lock that indicates the device is secure.

4. Connect the cables and position them away from foot traffic to prevent accidental disconnections or damage.
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 18

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 18

**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 18
General Settings

Topics:

- Set the Local Interface Language
- Set the System Web Interface Language
- Set the Date and Time
- Set Device and Room Names
- Register with Polycom Cloud Service
- Enable Screen Mirroring
- Disable Screen Mirroring

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 9

Set the Local Interface Language
You can change the language that users see on the Pano device 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

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

Set the Date and Time
You can change the time settings in the Pano system web interface.

Procedure

1. In the system web interface, go to General Settings > Date Time.
2. Configure the following settings:
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Format</strong></td>
<td>Specifies how the time displays in the interface.</td>
</tr>
<tr>
<td><strong>Auto Adjust for Daylight Saving Time</strong></td>
<td>Specifies the daylight saving time setting. When you enable this setting, the system clock automatically changes for daylight saving time.</td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
<td>Specifies the time difference between GMT and your location.</td>
</tr>
<tr>
<td><strong>Time Server</strong></td>
<td>Specifies whether the connection to a time server is automatic or manual for system time settings. You can also select Off to manually enter the date and time.</td>
</tr>
<tr>
<td><strong>Primary Time Server Address</strong></td>
<td>Specifies the address of the primary time server to use when Time Server is set to Manual.</td>
</tr>
<tr>
<td><strong>Secondary Time Server Address</strong></td>
<td>Specifies the address of the time server to use when the Primary Time Server Address does not respond. This is an optional field.</td>
</tr>
<tr>
<td><strong>Current Date and Current Time</strong></td>
<td>If Time Server is set to Manual or Auto, the system doesn’t display these settings. If Time Server is set to Off, Current Date and Current Time are configurable.</td>
</tr>
</tbody>
</table>

---

### 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 or Room Name 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 Pano 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 16
Provision the System on page 16
Provisioning Service on page 21
Choose Software Update Location in System Web Interface on page 45
Modes of Operation on page 15

Enable Screen Mirroring

By default, screen mirroring is enabled for AirPlay- and Miracast-certified devices. Screen mirroring lets users connect and share content from their personal devices.

Note: The system does not automatically allow screen mirroring when you enable the wireless settings.

Procedure

1. In the system web interface, go to General Settings > Screen Mirroring.

2. Select the screen mirroring options that you want available for sharing content.

   The Pano system updates, and the screen mirroring options available to users display in the home screen animation.

Related Links
Enable Wireless Settings on page 34

Disable Screen Mirroring

You can turn off screen mirroring options for AirPlay- and Miracast-certified devices.
**Note:** The system automatically turns off screen mirroring when you disable the wireless settings.

**Procedure**

1. In the system web interface, go to **General Settings > Screen Mirroring**.
2. Deselect the screen mirroring options that you want to disable.

The Pano system updates, and the screen mirroring options you disabled do not display in the home screen animation.
Provisioning Service

Topics:

- Enable a Provisioning Service
- Configure a Provisioning Service
- Disable a Provisioning Service

If your organization has Polycom® RealPresence® Resource Manager, you can use it to do the following with your Pano systems:

- 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 your systems.

Remember the following about using RealPresence Resource Manager with the Pano system:

- Configuration settings that are provisioned or dependent on provisioned values are read-only on the system.
- 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 appears on the System Status screen.
- If the system loses registration with the service, it continues to operate with the most recent configuration it received.

Related Links

Access the System Web Interface on page 9
Choose Software Update Location in System Web Interface on page 45
Register with Polycom Cloud Service on page 18

Enable a Provisioning Service

You can register your Pano system with RealPresence Resource Manager in one of the following ways:

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

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

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

Configure a Provisioning Service

After enabling the service, you must register your Pano system for provisioning.

Procedure

1. In the system web interface, go to General Settings > Provisioning Server.
2. Select Load Discovered Information.
   The registration fields complete automatically if your Pano system detects a provisioning server.
3. If your system did not detect a provisioning server, complete the following fields with information from your network administrator:

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

4. Select Save to register with the provisioning service.
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:

- LAN Status Lights
- Configure IP Address Settings
- Configure DNS Settings
- Configure LAN Options

Once you have connected the Pano device to the LAN, you can begin configuring its network settings.

Note: Not all network types are available in every country.

Related Links
Access the System Web Interface on page 9

LAN Status Lights

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

<table>
<thead>
<tr>
<th>Indicator Light</th>
<th>Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both lights off</td>
<td>No 10/100/1000 Base-T connection and no network traffic</td>
</tr>
<tr>
<td>Green and yellow lights on</td>
<td>10/100/1000 Base-T connection</td>
</tr>
<tr>
<td>Green light on and blinking yellow light</td>
<td>10/100/1000 Base-T connection with network traffic</td>
</tr>
</tbody>
</table>

Configure IP Address Settings

You can configure IPv4 and IPv6 settings for the Pano system.

Procedure

1. In the system web interface, go to Network > IP Addresses.
2. Select one of the following options to specify how the Pano system gets its IP address:
   - Obtain IP address automatically
   - Enter IP address manually
3. Configure the following IPv4 settings as needed:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your IP Address</td>
<td>Displays the system IP address. If you need to create a static address, enter it here. This field is disabled if you set the IP Address field to <em>Obtain IP Address automatically</em>.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Displays the gateway currently assigned to the system. If you need to create a static address, enter it here. This field is disabled if you set the IP Address field to <em>Obtain IP Address automatically</em>.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Displays the subnet mask currently assigned to the system. If you need to create a static address, enter it here. This field is disabled if you set the IP Address field to <em>Obtain IP Address automatically</em>.</td>
</tr>
</tbody>
</table>

4. Configure the following IPv6 settings as needed:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IPv6</td>
<td>Enables the IPv6 network stack and makes the IPv6 settings available.</td>
</tr>
<tr>
<td>Enable SLAAC</td>
<td>Specifies whether to use stateless address autoconfiguration (SLAAC) instead of DHCP to automatically obtain an IP address.</td>
</tr>
<tr>
<td>Link-Local</td>
<td>Displays the IPv6 address used for local communication within a subnet. This setting is configurable only when you select <em>Enter IP address manually</em>.</td>
</tr>
<tr>
<td>Site-Local</td>
<td>Displays the IPv6 address used for communication within the site or organization. This setting is configurable only when you select <em>Enter IP address manually</em>.</td>
</tr>
<tr>
<td>Global Address</td>
<td>Displays the IPv6 Internet address. This setting is configurable only when you select <em>Enter IP address manually</em>.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Displays the gateway currently assigned to the system.</td>
</tr>
</tbody>
</table>
5. Select Save.

**Configure DNS Settings**

You can configure the DNS settings for the Pano system.

**Procedure**

1. In the system web interface, go to **Network > DNS**.
2. If the system does not automatically obtain a DNS server address, enter one on this page (up to four are allowed).
3. 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 Options**.
2. Configure the following settings as needed:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Indicates the system name</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The domain name assigned to the system. If the system does not automatically obtain a domain name, enter one here.</td>
</tr>
<tr>
<td>Autonegotiation</td>
<td>Specifies whether the system should automatically negotiate the <strong>LAN Speed</strong> and <strong>Duplex Mode</strong> per IEEE 802.3 autonegotiation procedures. If enabled, those settings become read-only. Polycom recommends that you use autonegotiation to avoid network issues.</td>
</tr>
<tr>
<td>LAN Speed</td>
<td>Specifies whether to use <strong>10 Mbps</strong>, <strong>100 Mbps</strong>, or <strong>1000 Mbps</strong> for the LAN speed. The duplex</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Specifies the duplex mode to use. The duplex mode you choose must be supported by the switch.</td>
</tr>
<tr>
<td>Ignore Redirection Messages</td>
<td>Enables the system to ignore ICMP redirect messages.</td>
</tr>
<tr>
<td>ICMP Transmission Rate Limit (millisec)</td>
<td>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 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.</td>
</tr>
<tr>
<td>Enable EAP/802.1X</td>
<td>Specifies whether 802.1X authentication is enabled. The following authentication protocols are supported:</td>
</tr>
<tr>
<td></td>
<td>▪ EAP-MD5</td>
</tr>
<tr>
<td></td>
<td>▪ EAP-PEAPv0 (MSCHAPv2)</td>
</tr>
<tr>
<td></td>
<td>▪ EAP-TTLS</td>
</tr>
<tr>
<td></td>
<td>▪ EAP-TLS</td>
</tr>
<tr>
<td>EAP/802.1X Identity</td>
<td>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.</td>
</tr>
<tr>
<td>EAP/802.1X Password</td>
<td>Specifies the system's password for 802.1X authentication. This setting is required when EAP-MD5, EAP-PEAPv0, and EAP-TTLS are used.</td>
</tr>
</tbody>
</table>
Monitor Settings

Topics:

- HDMI Interfaces
- 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 9

HDMI Interfaces

The Pano device includes two HDMI interfaces: an input for wired content sharing, including audio streaming, and an output for the local interface monitor connection.

The device supports only HDMI-to-HDMI connections and not display conversions such as VGA-to-HDMI cable converters.

Supported HDMI Input Resolutions

The Pano device supports a variety of input resolutions for wired content sharing.

**Supported HDMI Input Resolutions and Frame Rates**

<table>
<thead>
<tr>
<th>Input</th>
<th>Resolution</th>
<th>Frame Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>UHD</td>
<td>3840×2160p</td>
<td>24, 25, 30</td>
</tr>
<tr>
<td>QHD</td>
<td>2560×1440p</td>
<td>50, 60</td>
</tr>
<tr>
<td>FHD</td>
<td>1920×1080p</td>
<td>50, 60</td>
</tr>
<tr>
<td>WSXGA+</td>
<td>1680×1050</td>
<td>60</td>
</tr>
<tr>
<td>UXGA</td>
<td>1600×1200</td>
<td>60</td>
</tr>
<tr>
<td>SXGA</td>
<td>1280×1024</td>
<td>60</td>
</tr>
<tr>
<td>HD</td>
<td>1280×720p</td>
<td>50, 60</td>
</tr>
<tr>
<td>XGA</td>
<td>1024×768</td>
<td>60</td>
</tr>
<tr>
<td>SVGA</td>
<td>800×600</td>
<td>60</td>
</tr>
</tbody>
</table>
Supported HDMI Output Resolutions
The Pano device supports the following output resolutions for the local interface monitor connection.

Supported HDMI Output Resolutions and Frame Rates

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Frame Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>2160p</td>
<td>25, 30, 50, 60</td>
</tr>
<tr>
<td>1080p</td>
<td>25, 30, 50, 60</td>
</tr>
<tr>
<td>720p</td>
<td>25, 30, 50, 60</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Size (inches)</th>
<th>Touch Technology</th>
<th>Brand</th>
<th>Model/Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Capacitive</td>
<td>Elo®</td>
<td>E497001</td>
</tr>
<tr>
<td>46</td>
<td>Capacitive</td>
<td>Elo®</td>
<td>ET4602L</td>
</tr>
<tr>
<td>55</td>
<td>InGlass™</td>
<td>Dell</td>
<td>C5518QT (black)</td>
</tr>
<tr>
<td>65</td>
<td>InGlass</td>
<td>Volanti</td>
<td>VD-6500-0B0C-1100 (black)</td>
</tr>
<tr>
<td>65</td>
<td>InGlass</td>
<td>Volanti</td>
<td>VD-6500-0Q0C-16P3 (white)</td>
</tr>
<tr>
<td>70</td>
<td>IR</td>
<td>Sharp</td>
<td>PN-L703B (black)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Monitor</td>
<td>Specifies the monitor setting:</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Automatic</strong> The default setting specifies that the <strong>Resolution</strong> setting is automatically detected.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Manual</strong> Lets you select the <strong>Resolution</strong> setting.</td>
</tr>
<tr>
<td>Resolution</td>
<td>Specifies the monitor resolution.</td>
</tr>
<tr>
<td></td>
<td>This setting is unavailable when you select <strong>Automatic</strong> for the <strong>Configure Monitor</strong> setting.</td>
</tr>
</tbody>
</table>

Your changes save automatically.
Security

Topics:

▪ PKI Certificates
▪ Change Local Account Credentials
▪ Disable the Security Code
▪ Wireless Communication Options
▪ Port Usage
▪ Encryption

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

Related Links
Access the System Web Interface on page 9

PKI Certificates

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

How PKI Certificates Are Used

PKI certificates authenticate secure network connections to and from the Pano system. Standard PKI techniques are used to configure and manage certificates and certificate signing requests (CSRs). ANSI X.509 standards regulate the certificate characteristics.

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

If your system is in an environment without a PKI, you do not need a CA-signed certificate; the system comes with a self-signed certificate for its TLS connections. When a PKI is deployed, however, self-signed certificates are not trusted and CA-signed certificates are needed.

Here are some examples of how you would use PKI certificates:

▪ If your environment uses the 802.1X authentication framework for wired connections, you would need to create a CSR and install the resulting CA-signed certificate on your system so it is trusted on the network.
▪ If you want to navigate with your browser over a secure connection to the Pano system web interface, you would need to 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.
Create a Certificate Signing Request

If a PKI is deployed in your environment, creating a CSR is the first step in making sure your Pano system is trusted by its network peers.

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 and select **Create**.

<table>
<thead>
<tr>
<th>CSR Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Algorithm</td>
<td>Specifies the hash algorithm for the CSR: SHA-256 (recommended) or SHA-1 (not recommended).</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>Specifies the system name. Polycom recommends the following guidelines for this field:</td>
</tr>
<tr>
<td></td>
<td>- For systems registered in DNS, use the system’s fully qualified domain name (FQDN).</td>
</tr>
<tr>
<td></td>
<td>- For systems not registered in DNS, use the system's IP address.</td>
</tr>
<tr>
<td></td>
<td>Maximum characters: 64 (truncated if necessary). Default is blank.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Specifies the business group defined by your organization. Default is blank. Maximum characters: 64.</td>
</tr>
<tr>
<td></td>
<td>Note: The system supports only one OU field. If you want the CA-signed certificate to include more than one OU, download and manually edit the CSR.</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Specifies your organization's name. Default is blank. Maximum characters: 64.</td>
</tr>
<tr>
<td>City or Locality (L)</td>
<td>Specifies the city where your organization is located. Default is blank. Maximum characters: 128.</td>
</tr>
<tr>
<td>State or Province (ST)</td>
<td>Specifies the state or province where your organization is located. Default is blank. Maximum characters: 128.</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Displays the country selected in the setup wizard. Cannot be changed here.</td>
</tr>
<tr>
<td>SAN: FQDN</td>
<td>Specifies the FQDN assigned to the system. It is the same as the Common Name (CN) but not truncated. Default is blank. Maximum characters: 253.</td>
</tr>
<tr>
<td>SAN: Additional Name</td>
<td>Specifies an additional system name. Default is blank. Maximum characters: 253.</td>
</tr>
<tr>
<td>SAN: IPv4 Address</td>
<td>Default is the system’s IPv4 address. Maximum characters: 15.</td>
</tr>
</tbody>
</table>
CSR Information | Description
---|---
User Principal Name (UPN) | Specifies the user and domain name for logging in to a Windows domain (e.g., UserName@YourDomain.com). (This is the userPrincipalName attribute of the account object in Active Directory.) It should be related to the 802.1X identity and password you specified on the Network > LAN Options page. Default is blank.

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

**Note:** Only a single CSR can exist at a time. After a CSR is generated, you should get it signed and installed on your system before creating another. For example, if you generate a CSR and, prior to having it signed and installed, generate another, the previous CSR is discarded and invalidated.

**Configure Certificate Validation Settings**

User-installed certificates can be automatically validated when establishing an authenticated network connection.

To perform this validation, the Pano system must have certificates installed for the CAs that are part of the trust chain.

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

**Procedure**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Peer Certificate Chain Depth</td>
<td>Specifies how many links a certificate chain can have. The term peer certificate refers to any certificate sent by the far-end host when a network connection is being established between the two systems.</td>
</tr>
<tr>
<td>Always Validate Peer Certificates from Server</td>
<td>Controls whether the system requires the remote server to present a valid certificate when connecting to it for services, such as provisioning.</td>
</tr>
</tbody>
</table>

**Install Certificates**

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

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

2. Select **Install Certificate** to browse for the CA-signed certificate you want to install and select **Open**.

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

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

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

View Certificates

User-installed certificates are listed in the Pano 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 the 🕵️ eye icon in the same row.

   The certificate contents display in plain text.

Delete Certificates

You can remove user-installed certificates on your Pano system from the web interface.

When all these certificates are deleted, your system reverts to using the factory-installed certificate. (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 the 🗑️ trash icon in the same row.

   Deleting user-installed certificates cannot be undone.

3. Confirm by selecting **Delete**.

   A message indicates that the certificate was deleted.

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

The security code on the Pano system home screen is enabled by default.

The way you can disable the code varies depending on the system setup. For example, if the system is registered and connected to the Polycom Cloud Service, the option to disable the security code is read-only in the system web interface.

Procedure

1. Do one of the following to disable the security code:
   - In the system web interface, go to Security > Security Code and select Enable Security Code to clear the checkbox.
   - Edit the system settings in the Polycom Cloud Service Administration portal.
   - Update the provisioning profile for the system in RealPresence Resource Manager.

Wireless Communication Options

The Pano system Wi-Fi and Bluetooth wireless communication hardware allow the Pano App and AirPlay- and Miracast-certified devices to detect Pano systems on the network. 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.

Note: The Pano system does not support wireless LAN (WLAN). It cannot make direct Wi-Fi connections to external access points.

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) that do not overlap. Once a connection is established, a device that supports the 5 GHz band could choose that frequency instead to avoid interference.

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 feature does not automatically turn it on. You must also enable screen mirroring.
Procedure

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

2. Do one or more of the following:
   - Select the **Enable Wi-Fi** option to enable screen mirroring for Miracast-certified devices.
   - Select the **Enable Bluetooth** option to enable screen mirroring for AirPlay-certified devices.

Related Links

Enable Screen Mirroring on page 19

Disable Wireless Settings

By default, the wireless communication features are enabled and can be disabled as needed.

Remember the following when disabling the wireless features:

- Disabling Wi-Fi turns off screen mirroring with Miracast-certified devices.
- Disabling Bluetooth turns off screen mirroring with AirPlay-certified devices and prevents those devices and the Pano App from automatically discovering a Pano system. (The Pano App can still connect with the system IP address.)

Procedure

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

2. Specify your preferences:
   - Select the **Enable Wi-Fi** option to clear the checkbox and disable screen mirroring for Miracast-certified devices.
   - Select the **Enable Bluetooth** option to clear the checkbox and disable screen mirroring for AirPlay-certified devices.

   Your preferences automatically update.

Port Usage

The Pano system uses a range of ports to handle communication with other systems, devices, and network services.

---

**Note:** Your network must allow bidirectional communication between personal devices and the Pano system.

---

Port Connections

The following table lists the inbound, outbound, and bidirectional ports used by the Pano system.
## Port Connections

<table>
<thead>
<tr>
<th>Port</th>
<th>Direction</th>
<th>Type</th>
<th>Protocol</th>
<th>Application Protocol</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>Outbound</td>
<td>Static</td>
<td>UDP</td>
<td>DNS</td>
<td>Dynamic IP assignment</td>
</tr>
<tr>
<td>80</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td>HTTP</td>
<td>HTTP web server listener that redirects all sessions to HTTPS on port 443. Also used by AirPlay.</td>
</tr>
<tr>
<td>123</td>
<td>Outbound</td>
<td>Static</td>
<td>UDP</td>
<td>NTP</td>
<td>Automatic time synchronization</td>
</tr>
<tr>
<td>443</td>
<td>Bidirectional</td>
<td>Static</td>
<td>TCP/SCTP</td>
<td>SSL/HTTPS</td>
<td>Static TCP HTTPS web server listener that provides TLS access to the Pano system web interface. Also used by AirPlay. Required for integrating with the Polycom Cloud Service.</td>
</tr>
<tr>
<td>554</td>
<td>Inbound</td>
<td>Static</td>
<td>UDP/TCP</td>
<td>Real Time Streaming Protocol (RTSP)</td>
<td>AirPlay</td>
</tr>
<tr>
<td>1900</td>
<td>Inbound</td>
<td>Static</td>
<td>UDP</td>
<td>Simple Service Discovery Protocol (SSDP)</td>
<td>Bonjour</td>
</tr>
<tr>
<td>3689</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td>Digital Audio Access Protocol (DAAP)</td>
<td>iTunes Music Sharing/AirPlay</td>
</tr>
<tr>
<td>5001</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP/UDP</td>
<td>IPIPC</td>
<td>The Pano App for content sharing.</td>
</tr>
<tr>
<td>5297</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td></td>
<td>Bonjour</td>
</tr>
<tr>
<td>5298</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td></td>
<td>Bonjour</td>
</tr>
<tr>
<td>5353</td>
<td>Inbound</td>
<td>Static</td>
<td>UDP</td>
<td>multicast Domain Name System (mDNS)</td>
<td>Bonjour/AirPlay</td>
</tr>
<tr>
<td>7000</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td>AirPlay</td>
<td>AirPlay standard services</td>
</tr>
<tr>
<td>7100</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td>AirPlay</td>
<td>AirPlay mirroring services</td>
</tr>
<tr>
<td>Port</td>
<td>Direction</td>
<td>Type</td>
<td>Protocol</td>
<td>Application Protocol</td>
<td>Function</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>--------</td>
<td>----------</td>
<td>----------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>47000</td>
<td>Inbound</td>
<td>Static</td>
<td>TCP</td>
<td>AirPlay</td>
<td>AirPlay casting services</td>
</tr>
<tr>
<td>49152-65535</td>
<td>Bidirectional</td>
<td>Dynamic</td>
<td>TCP/UDP</td>
<td></td>
<td>For applications that use a dynamic, random, or configurable port. If a default port is already in use, the application will use another available port in this range.</td>
</tr>
<tr>
<td>49159</td>
<td>Inbound</td>
<td>Static</td>
<td>UDP</td>
<td>mDNS (Windows)</td>
<td>Bonjour/AirPlay</td>
</tr>
<tr>
<td>49163</td>
<td>Inbound</td>
<td>Static</td>
<td>UDP</td>
<td>mDNS (Windows)</td>
<td>Bonjour/AirPlay</td>
</tr>
</tbody>
</table>

### Encryption

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

<table>
<thead>
<tr>
<th>Application</th>
<th>Encryption Function</th>
<th>Description</th>
<th>Protocol Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Boot</td>
<td>Authentication</td>
<td>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.</td>
<td>PKCS #1</td>
</tr>
<tr>
<td>Application</td>
<td>Encryption Function</td>
<td>Description</td>
<td>Protocol Used</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Software signing (OTA)</td>
<td>Authentication</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td>PKCS #8 (RFC 5208)</td>
</tr>
<tr>
<td>AirPlay</td>
<td>Confidentiality</td>
<td>Encrypted content casting protocol for sending media from an AirPlay-certified device to the Pano device’s Ethernet network interface.</td>
<td>This protocol requires an IP network connection from an AirPlay-certified device to the Pano device Ethernet NIC. It does not use a private, short-range wireless network connection to the Pano device.</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td>RSN (WPA2/IEEE 802.11i)</td>
</tr>
<tr>
<td>Miracast</td>
<td>Confidentiality</td>
<td>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.</td>
<td>RSN (WPA2/IEEE 802.11i)</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Proxy Client</td>
<td>Authentication</td>
<td>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.</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Encryption Function</td>
<td>Description</td>
<td>Protocol Used</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Cluster Control Service Client</td>
<td>Authentication</td>
<td>Allows the Pano device to retrieve PIN codes from the Polycom Cloud Service for the room device cluster.</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RealPresence Group Series Pairing Client</td>
<td>Authentication</td>
<td>Allows pairing with a RealPresence Group Series system so that it can control the content-sharing functions of the Pano device.</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Document Service Authentication</td>
<td>Authentication</td>
<td>Allows the Pano device to authenticate to the cloud document service for functions such as document sharing over an encrypted TLS connection.</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Document Session Manager WebSocket</td>
<td>Authentication</td>
<td>Allows the Pano device to connect to a cloud document sharing session over a WSS connection.</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTViewer Client</td>
<td>Authentication</td>
<td>An Android application that facilitates receiving a rendered document from the cloud casting server over a WSS connection.</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics Client</td>
<td>Authentication</td>
<td>Allows the Pano device to send analytic information to the Polycom Cloud Service.</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Update Client</td>
<td>Authentication</td>
<td>Allows the Pano device to check for and get software update images from a configured software update server over an encrypted channel.</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pano App Screen/App Share Media Server</td>
<td>Confidentiality</td>
<td>Media connection from a device using the Pano App to the Pano device.</td>
<td>Proprietary session-layer protocol over UDP</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Encryption Function</td>
<td>Description</td>
<td>Protocol Used</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Pano App Screen/App Share Signaling Server</td>
<td>Confidentiality</td>
<td>Used by the Pano App to set up the screen and application sharing sessions</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td>(Port 5001)</td>
<td>Integrity</td>
<td>with the Pano device (no media flows over this connection; there is only</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>signaling).</td>
<td></td>
</tr>
<tr>
<td>Management API Server</td>
<td>Authentication</td>
<td>Provides a local management interface over HTTPS. It is used for the</td>
<td>TLS 1.1 and 1.2</td>
</tr>
<tr>
<td>(Port 443)</td>
<td>Integrity</td>
<td>system web interface and REST API, which retrieves saved snapshot images</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>from the Pano device.</td>
<td></td>
</tr>
</tbody>
</table>
Content Sharing

Topics:

- Content Sharing Options

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

Content Sharing Options

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

- **Wireless screen mirroring**  Users connect to the Pano device using an AirPlay- or Miracast-certified device. The screen of the personal device is mirrored onto the Pano device monitor, and any accompanying audio is also shared. You can enable or disable one or more of these options in the system web interface. The connection animation on the home screen lets users know which options are available.

- **Wired input**  Using the HDMI interface located on the back panel of the Pano device, users can connect a personal laptop or desktop to share local content.

- **Pano App**  Users can install the application on a Microsoft® Windows® or Apple® Mac® system that is not wired to the Pano device. Users can share their screen, a running application, or content...
from a Microsoft OneDrive for Business account (the latter option requires a Polycom Cloud Service account).

**Note:** Polycom Cloud Service Content Sharing is a Polycom Labs feature. For more information, see the *Polycom Pano Release Notes.*
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 9

Resetting the System

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

Perform a Factory Reset

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

The following data is not saved with a factory reset:

- Software updates
- Logs
- User-installed PKI certificates

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.

Delete System 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 > System Reset.
2. Select Reset All System Configurations.
3. If you have user-installed PKI certificates that you do not want to retain, deselect the **Keep installed certificates after system reset** checkbox.

4. Select **Restart**.
   After about 15 seconds, the system restarts and displays the setup wizard.

---

### Updating System Software

You can use the following methods to update the software of your Pano system:

- Online server at the Polycom Support Site
- Custom server URL
- Provisioning service (e.g., RealPresence Resource Manager)
- Polycom Cloud Service
- Software file obtained from [http://support.polycom.com](http://support.polycom.com) and uploaded to the system web interface using a USB storage device.

---

### Choose Software Update Location in System Web Interface

You may have several options for updating 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):

<table>
<thead>
<tr>
<th>Software Update Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Support Site</td>
<td>An online software server hosted by Polycom.</td>
</tr>
<tr>
<td>Custom Server URL</td>
<td>A server on your network that supports HTTP or HTTPS downloads.</td>
</tr>
<tr>
<td></td>
<td>The URL is the path to the latest software build folder (e.g., <code>https://pano-build-folder</code>). The folder should contain the following files:</td>
</tr>
<tr>
<td></td>
<td>• release.json</td>
</tr>
<tr>
<td></td>
<td>• polycom-pano-&lt;version&gt;.json</td>
</tr>
<tr>
<td></td>
<td>• polycom-pano-&lt;version&gt;.zip</td>
</tr>
<tr>
<td>Provisioning Server</td>
<td>Receive updates from a provisioning service, such as RealPresence Resource Manager.</td>
</tr>
<tr>
<td>Polycom Cloud Service</td>
<td>Receive updates from the service if your device is registered to it.</td>
</tr>
</tbody>
</table>

3. If you chose to download from a **Custom Server URL**, enter the path to the software build folder on your network in the **Update Server Address** field.

---

Polycom, Inc.
Once you have selected where to download software updates from, you can manually or automatically update the system.

**Related Links**
- [Provisioning Service](#) on page 21
- [Register with Polycom Cloud Service](#) on page 18

**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.
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.

Your changes automatically save.

**Update Software from a USB Storage Device**
You can update the software with a USB storage device by connecting it to the back of the Pano device.

**Procedure**
1. Obtain the software package you want to install from Polycom Support.
2. Save the package to the root directory of a USB storage device.
3. Connect the storage device to the USB 2.0 port on the back of the Pano device (i.e., the top USB port).
   The device detects the USB storage device and displays a prompt on the monitor to confirm that you want to update the software.
4. Select **OK** and 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 the system software, Polycom recommends doing the following:

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

Topics:

▪ Polycom Cloud Service Administration Account Activation Process
▪ Integrate with Microsoft Office 365
▪ Authentication Providers
▪ Document Services
▪ Device Management
▪ User Management

The Polycom Cloud Service is an offering that enables users in an organization to securely share content with a registered Pano system from the Microsoft® OneDrive® for Business enterprise document storage service, using a locally installed copy of Polycom Pano App.

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 Pano App uses standard HTTPS connections to communicate with the Polycom Cloud Service. Polycom Pano 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 Pano App. This allows users to sign in directly to Office 365 without the Polycom Pano App or the Polycom Cloud Service ever having access to user credentials.

▪ Documents shared from the Polycom Cloud Service are rendered to Polycom Pano App and a Polycom Pano system over encrypted WebSocket Secure (WSS) connections, which keeps the information secure during transit.

▪ When a document is shared from the Polycom Cloud Service, the actual document is not sent or made available to either the Polycom Pano or the Polycom Pano App. Instead, a web view of the document is created in the cloud and rendered into a compressed video stream that is then sent to both Polycom Pano and Polycom Pano App. This keeps the document safe in the cloud, unaltered and inaccessible to those viewing it.

▪ When a content sharing session ends, the shared content is deleted from the Polycom Cloud Service and Polycom Pano App. The content remains in its original state on the OneDrive for Business system.

Related Links
Access the Polycom Cloud Service Administration Portal from the System Web Interface on page 10
Access the Polycom Cloud Service Administration Portal from an Assigned URL on page 10

Polycom Cloud Service Administration Account Activation Process

Your company’s initial Polycom Cloud Service administration account is created as part of the purchase of a Polycom product or associated cloud service.
The initial Polycom Cloud Service administrative user can create additional Polycom Cloud Service administration accounts for other administrative users in your company, assigning them each specific user roles to match the level of access required. The administrative users whose accounts are assigned with the UserAdmin user role can also create and manage Polycom Cloud Service administration accounts.

As a new Polycom Cloud Service administrative user, you receive a “Welcome to Polycom Cloud Service Administration” email message. This welcome email message contains an activation link that guides you through the steps of activating your administration account.

**Important:** If an email address for the initial Polycom Cloud Service Administration account was not included with your purchase order, or your Polycom system is shipped to China, Mexico, Brazil, or Argentina, you must activate your Polycom system maintenance service on the Polycom Support Center and provide an email address before your Polycom Cloud Service administration account can be created.

If you have not received the “Welcome to Polycom Cloud Service Administration” email, please contact Polycom Global Services at 1-800-POLYCOM (1-800-765-9266).

### Activate a Polycom Cloud Service Administration Account

You can activate a Polycom Cloud Service administration account.

**Procedure**

1. In the “Welcome to Polycom Cloud Service Administration” email you received, click **Activate Your Account**.
   
   The link is active for two hours.

### Complete Account Activation

When you receive your account activation link email, you can set up your password and finalize your account activation from the **Activate Account** screen.

**Procedure**

1. In the “Polycom Cloud Service Account Activation” email you received, click **Complete Account Activation**.
   
   You are redirected to the **Activate Account** screen.

2. Create a password in the **Set Password** field.

   **Note:** Password must be between 8 and 32 characters in length and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

3. Re-enter the password in the **Confirm Password** field.

4. Click **Submit**.

You are redirected to the Polycom Cloud Service Administration **Sign In** screen where you can sign in using your email address and the password you just configured for your account.
You also receive a “Polycom Cloud Service Administration Account Activated” email containing additional information about your Polycom Cloud Service Administration account. Be sure to save this email for future reference.

**Sign in with Your Administration Account**

The Polycom Cloud Administration portal URL is in your “Polycom Cloud Service Administration Account Activated” email message.

**Procedure**

1. You can sign into your account at any time in the Polycom Cloud Service Administration portal at [https://console.plcm.cloud](https://console.plcm.cloud).
2. Enter your email address in the **Email Address** field and click **Continue**.
3. When the **Sign In** screen reappears, do one of the following:
   - Enter your password in the **Password** field and click **Sign in**.
   - Click a listed authentication provider and sign in with it.

**Integrate with Microsoft Office 365**

To allow users sign in using their enterprise credentials to share documents from their Microsoft OneDrive for Business folders, the Polycom Cloud Service supports integration with your Microsoft Office 365 service.

Integration with your Microsoft Office 365 service consists of three basic steps:

1. Retrieving some information from your Polycom Cloud Service administration account required for the integration (Redirect URLs for the Authentication and Document Service provider).
2. With the assistance of your company’s Microsoft Azure Active Directory administrator, registering the Polycom Cloud Service as a trusted web application that allows users to sign in and access their OneDrive for Business folders and files.
3. Using information returned from this registration, configuring the Authentication and Document Service provider in your Polycom Cloud Service administration account.

You can use the following detailed steps to complete the integration:

**Procedure**

1. Sign in to the Polycom Cloud Service Administration portal.
2. You need to get the authentication provider redirect URL to use.
   a. Go to **Authentication Provider**.
   b. Click **(Inactive)**.
   c. In the configuration section once it displays, click the **Copy to Clipboard** icon at the end of the **Redirect URL** field and paste it in a secure location and save it for future use.
   d. Click **Cancel**.
3. You need to get the Document Services redirect URL to use.
a. Go to Document Services.

b. Click (Inactive)

c. In the configuration section once it displays, click the Copy to Clipboard icon at the end of the Redirect URL field and paste it in a secure location and save it for future use.

d. Click Cancel.

4. Once you have saved the Redirect URLs, provide them to your Microsoft Azure Active Directory administrator. Ask the Active Directory administrator to perform an App registration of the Polycom Cloud Service within your company’s Microsoft Azure Active Directory. Your Active Directory administrator can use the Redirect URLs by referring to the following mapping table (The app registration can be performed via the Microsoft Azure portal https://portal.azure.com).

<table>
<thead>
<tr>
<th>Polycom Cloud Service URLs</th>
<th>Microsoft Azure Active Directory URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Provider&gt;Redirect URL</td>
<td>App registration &gt; Sign-on URL</td>
</tr>
<tr>
<td>Document Services &gt; Redirect URL</td>
<td>App registration &gt; Settings &gt; GENERAL &gt; Reply URLs</td>
</tr>
</tbody>
</table>

As part of the App registration, ask your Microsoft Azure Active Directory administrator to add following APIs and grant listed permissions to the APIs:

<table>
<thead>
<tr>
<th>Add API</th>
<th>DELEGATED PERMISSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SharePoint</td>
<td>• Read user files&lt;br&gt; • Read and write user files</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Sign in and read user profile</td>
</tr>
</tbody>
</table>

5. Collect the following Microsoft Azure Active Directory settings from your Microsoft Azure Active Directory administrator.

<table>
<thead>
<tr>
<th>Microsoft Azure Active Directory Settings</th>
<th>Polycom Cloud Service Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>App registration &gt; Settings &gt; Essentials &gt; Application ID</td>
<td>Client ID</td>
</tr>
<tr>
<td>App registration &gt; Settings&gt; API Access &gt; Keys</td>
<td>Client Secret</td>
</tr>
<tr>
<td>Properties &gt; Directory ID</td>
<td>Tenant ID</td>
</tr>
<tr>
<td>Default Azure Active Directory Domain Name (Example: &lt;company&gt;.onmicrosoft.com)</td>
<td>Tenant</td>
</tr>
</tbody>
</table>

6. Return to the Polycom Cloud Service Administration portal and finish the rest of the authentication provider configurations.

   a. Go to Authentication Provider.
b. Click (Inactive).

c. Enter a Name for your authentication provider.

   **Note:** Your users see this name when they sign in using the Polycom Pano App.

d. Paste the **Client ID, Client Secret, Tenant ID** values according to the mapping table in **Step 5**.

7. Finish the rest of the document service configurations.

   a. Go to **Document Services**.

   b. Click (Inactive)

   c. Enter a **Name** for your document service.

   d. Paste the **Client ID, Client Secret, Tenant ID, Tenant** values according to the mapping table in **Step 5**.

### Authentication Providers

Authentication Providers allow users to sign in to the Polycom Cloud Service using their user account credentials from an enterprise user authentication service such as Microsoft Office 365 (Microsoft Azure Active Directory) or an on-premises Microsoft Active Directory service (federated for cloud service access via ADFS).

Pano App users sign in using their Microsoft Office 365 user account credentials to access files in their OneDrive for Business folders; Polycom Cloud Service Administration users can sign into the Polycom Cloud Service Administration portal using their enterprise account credentials or their local account credentials.

You can connect the Polycom Cloud Service to any of the following custom and built-in authentication providers:

- **Built-in Office 365**: Polycom pre-configured Microsoft Azure Active Directory that you can only enable or disable it in the Polycom Cloud Service Administration portal.

- **Custom Office 365**: Your enterprise customized Microsoft Azure Active Directory that you need to add it to the Polycom Cloud Service Administration portal.

- **Custom ADFS**: Your enterprise customized Microsoft Active Directory Federation Services 3.0 that you need to add it to the Polycom Cloud Service Administration portal.

Both custom providers use the **OAuth 2.0** authorization framework to access the external authentication service. This ensures reliable and secure use of the provider’s identity management services.

For the vast majority of Office 365 integrations, the **Office 365** provider will be used.

**Related Links**

[Integrate with Microsoft Office 365](#) on page 50

### Enable or Disable a Built-In Authentication Provider

You can enable or disable the Polycom pre-configured built-in Office 365.
### Procedure

1. In the Polycom Cloud Service Administration portal, go to Authentication Providers.

2. In the Built-in Authentication Providers section, enable or disable the built-in Office 365:
   - To enable it, click ![Inactive] (Inactive), then click **Enable**.
   - To disable it, click ![Active] (Active), then click **Disable**.

**Note:** If enabled, Polycom Cloud Service Administration users can sign in with it instead of entering user credentials and Polycom Cloud Service is granted the permission to access user profile in the Microsoft Office 365.

### Add Office 365 as a Custom Authentication Provider

You can add any custom authentication providers from Authentication Providers.

### Procedure

1. In the Polycom Cloud Service Administration portal, go to Authentication Providers.

2. In the Custom Authentication Providers section, click ![Inactive] (Inactive).

3. Register the Polycom Cloud Service as an OAuth 2.0 client. Your Active Directory administrator should register the service using the Redirect URL (see table below).

4. Configure the required fields for the authentication provider.

**Office 365**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Authentication provider name</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Your users see this name when they sign in using the Polycom Pano App.</td>
</tr>
<tr>
<td>Client ID</td>
<td><em>Application ID created for the Polycom Cloud Service as part of registering it within Microsoft Azure Active Directory</em></td>
</tr>
<tr>
<td>Client Secret</td>
<td><em>API Access Key created for the Polycom Cloud Service as part of registering it within Microsoft Azure Active Directory</em></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure you save the Client Secret in a secure location. Once you entered the Client Secret, you cannot retrieve it from the Polycom Cloud Service Administration portal.</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>Microsoft Azure Directory ID</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>This is a read-only field. Supply the Redirect URL to your Microsoft Azure Active Directory administrator as it is required for registering the Polycom Cloud Service within Microsoft Azure Active Directory.</td>
</tr>
</tbody>
</table>

5. Click **Save**.
Add ADFS as a Custom Authentication Provider

You can add any custom authentication providers from Authentication Providers.

Procedure

1. In the Polycom Cloud Service Administration portal, go to Authentication Providers.
2. In the Custom Authentication Providers section, click ADFS (Inactive).
3. Register the Polycom Cloud Service as an OAuth 2.0 client. Your Active Directory administrator should register the service using the Callback URL (see table below).
4. Configure the required fields for the authentication provider.

**ADFS**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Authentication provider name</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Your users see this name when they sign in using the Polycom Pano App.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Client Application ID is used to register the Polycom Cloud Service as an ADFS OAuth 2.0 client.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Your Active Directory administrator will create this as part of performing the registration. It is a Globally Unique Identifier (GUID), so any GUID generator can be used to create it.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>OAuth 2.0 client secret that is created as part of registering the Polycom Cloud Service as an ADFS OAuth 2.0 client. Your Active Directory administrator will provide this to you.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Make sure you save the Client Secret in a secure location. Once you entered the Client Secret, you cannot retrieve it from Polycom Cloud Service Administration portal.</td>
</tr>
<tr>
<td>Callback URL</td>
<td>This is a read-only field. Supply the Callback URL to your Active Directory administrator as it is required for registering the Polycom Cloud Service as an ADFS OAuth 2.0 client.</td>
</tr>
<tr>
<td>Authorization URL</td>
<td>Your Active Directory administrator will provide this to you. It is typically in the form of https://&lt;company-adfs-domain&gt;/adfs/oauth2/authorize</td>
</tr>
<tr>
<td>Token URL</td>
<td>Your Active Directory administrator will provide this to you. It is typically in the form of https://&lt;company-adfs-domain&gt;/adfs/oauth2/token</td>
</tr>
<tr>
<td>Logout Redirect URL</td>
<td>Your Active Directory administrator will provide this to you. It is typically in the form of https://&lt;company-adfs-domain&gt;/adfs/oauth2/authorize</td>
</tr>
</tbody>
</table>

Polycom Cloud Service
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Your Active Directory administrator will provide this to you. It is registered as the &quot;Identifier&quot; parameter of the Relying Party Trust in ADFS, for example, https://&lt;myapplication&gt;</td>
</tr>
</tbody>
</table>

5. Click Save.

**Edit or Delete a Custom Authentication Provider**

You can edit or delete a custom authentication provider from Authentication Providers.

**Procedure**

1. In the Polycom Cloud Service Administration portal, go to Authentication Providers.
2. In the Custom Authentication Providers section, click Office 365 (Active) or ADFS (Active).
3. In the authentication provider configuration section, configure the required fields for the authentication provider, and do one of the following:
   - Click Save to save the changes, then click to close the configuration tab.
   - Click Cancel to cancel the changes.
4. To delete an authentication provider, click Delete.

**Document Services**

Document Services is where you can integrate the Polycom Cloud Service with the document service provider.

The Polycom Cloud Service supports a single document service provider: Microsoft Office 365 OneDrive for Business.

**Note:** Polycom Cloud Service Content Sharing is a Polycom Labs feature. For more information, see the Polycom Pano Release Notes.

**Related Links**

Integrate with Microsoft Office 365 on page 50

**Add Office 365 OneDrive for Business as a Document Service**

You can add Microsoft Office 365 OneDrive for Business as a document service from Document Services.

**Procedure**

1. In the Polycom Cloud Service Administration portal, go to Document Services.
2. Click Office 365 (Inactive).
3. In the document service configuration section, configure the required fields for the document service.
Office 365

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Document service name</td>
</tr>
<tr>
<td>Client ID</td>
<td><em>Application ID</em> created for the Polycom Cloud Service as part of registering it within Microsoft Azure Active Directory</td>
</tr>
<tr>
<td>Client Secret</td>
<td><em>API Access Key</em> created for the Polycom Cloud Service as part of registering it within Microsoft Azure Active Directory</td>
</tr>
<tr>
<td>Note</td>
<td>Make sure you save the Client Secret in a secure location. Once you entered the Client Secret, you cannot retrieve it from the Polycom Cloud Service Administration portal.</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>Microsoft Azure Active <em>Directory ID</em></td>
</tr>
<tr>
<td>Tenant</td>
<td>Your default Microsoft Azure Active Directory domain name in the form of <code>&lt;company&gt;.onmicrosoft.com</code></td>
</tr>
<tr>
<td>Redirect URL</td>
<td>This is a read-only field. Supply the Redirect URL to your Microsoft Azure Active Directory administrator as it is required for registering the Polycom Cloud Service within Microsoft Azure Active Directory.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

**Edit or Delete the Integrated Document Service**

You can edit or delete an integrated document service from **Document Services**.

**Procedure**

1. In the Polycom Cloud Service Administration portal, go to **Document Services**.
2. Click **Office 365** (Active).
3. In the document service configuration section, configure the required fields for the document service, and do one of the following:
   • Click **Save** to save the changes, then click **>** to close the configuration tab.
   • Click **Cancel** to cancel the changes.
4. To delete the document service, click **Delete**.

**Device Management**

Device Management is where you can monitor and edit your registered Polycom Pano devices.

The system lists each registered device in a table with the following information:
Registered Device Information

<table>
<thead>
<tr>
<th>Device Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Icon that indicates the registration status of the device:</td>
</tr>
<tr>
<td>▪ (●) (Online)</td>
<td>Indicates that the device is currently connected to the Polycom Cloud Service</td>
</tr>
<tr>
<td>▪ (○) (Offline)</td>
<td>Indicates that the device has been disconnected from the Polycom Cloud Service</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Device type</td>
</tr>
<tr>
<td>▪ Pano</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Device IPv4 address</th>
</tr>
</thead>
</table>

**Tip:** Clicking on the address of the Polycom Pano device establishes a web UI session (a separate tab in your browser) to the Polycom Pano device.

<table>
<thead>
<tr>
<th>Room Name</th>
<th>Room name of the Polycom Pano device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Version</td>
<td>Device software version</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Device serial number</td>
</tr>
</tbody>
</table>

You can click Refresh to refresh all the device information manually.

**Edit or Delete a Registered Device**

You can edit or delete a registered device from Device Management.

**Procedure**

1. In the Polycom Cloud Service Administration portal, go to **Device Management**.
2. Click the device name that you want to edit.

When you click the device name, additional device information displays in a configuration tab and you can edit part of the properties.

**Editable Device Properties**

<table>
<thead>
<tr>
<th>Properties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Can contain any Unicode string up to 40 characters</td>
</tr>
<tr>
<td>Room</td>
<td>Can contain any Unicode string up to 40 characters</td>
</tr>
<tr>
<td>Security Code</td>
<td>Controls whether a security code is required to connect to the Polycom Pano device</td>
</tr>
<tr>
<td>Required</td>
<td></td>
</tr>
</tbody>
</table>
### Read-only Device Properties

<table>
<thead>
<tr>
<th>Properties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Device ID</td>
</tr>
<tr>
<td>Status</td>
<td>Device status</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Device MAC address</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Device Serial Number</td>
</tr>
<tr>
<td>IPv4</td>
<td>Device IPv4 IP address</td>
</tr>
<tr>
<td>IPv6</td>
<td>Device IPv6 IP address</td>
</tr>
<tr>
<td>Software Version</td>
<td>Device software version</td>
</tr>
<tr>
<td>Hardware Version</td>
<td>Device hardware version</td>
</tr>
</tbody>
</table>

3. Modify the editable device properties and do one of the following:
   - Click **Save** to save the changes, then click ➔ to close the configuration tab.
   - Click **Cancel** to cancel the changes.

4. To delete a registered device, click **Delete**.

### User Management

User Management is where you can create and manage Polycom Cloud Service Administration user credentials used to access the Polycom Cloud Service Administration portal.

These accounts have different permissions depending on the User Role and Sign In Account that you select for them.

Each user is listed in a table with the following information:

#### User Information

<table>
<thead>
<tr>
<th>User Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>User' name</td>
</tr>
<tr>
<td>Notification Language</td>
<td>Language of notification email messages</td>
</tr>
<tr>
<td>Sign In Account</td>
<td>User credentials that user can use for signing in the Polycom Cloud Service Administration portal.</td>
</tr>
<tr>
<td>User Role</td>
<td>User roles that associate with different access permissions in the Polycom Cloud Service Administration portal.</td>
</tr>
</tbody>
</table>
Polycom Cloud Service Enterprise Administrator

Polycom assigns the name “Enterprise Administrator” to the initial Polycom Cloud Service Administration user. The Enterprise Administrator has an active local administration account associated with all available user roles. With these initial settings, the Enterprise Administrator has full access to the Polycom Cloud Service Administration portal without activating and configuring the administration account.

Add an Administration Account

You can add an administration account using the user’s email address.

Procedure

1. In the Polycom Cloud Service Administration portal, go to **User Management**.
2. Click **Add**.
3. Enter the following user account information:
   
<table>
<thead>
<tr>
<th>User Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Can contain any Unicode string of up to 64 characters.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Can contain any Unicode string of up to 64 characters.</td>
</tr>
<tr>
<td>Email Address</td>
<td>User’s email address</td>
</tr>
</tbody>
</table>

   **Note:** The email address you enter must be from the same email domain as the one associated with the initial Polycom Cloud Service administration account.

4. In the **User Role** field, select one or more predefined user roles for the new account:
   
<table>
<thead>
<tr>
<th>User Role</th>
<th>Permission Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserAdmin</td>
<td>Provides access to the <strong>User Management</strong> functions</td>
</tr>
<tr>
<td>EnterpriseAdmin</td>
<td>Provides access to the <strong>Authentication Providers</strong> and <strong>Document Services</strong> functions</td>
</tr>
<tr>
<td>DeviceAdmin</td>
<td>Provides access to the <strong>Device Management</strong> functions</td>
</tr>
</tbody>
</table>

5. In the **Notification Language** field, select a language from the drop-down list that the system uses to send email notification messages to the user.

6. In the **Sign In Account** field, select one of the following account types:
### Account Type

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise and Local</td>
<td>Allows users to sign in either using their Polycom Cloud Service administration account credentials or their enterprise account credentials from any of the configured authentication providers. Select this option if you didn’t configure additional authentication providers or if additional authentication providers are unreachable within your organization. The “additional authentication providers” refer to other authentication provider types that you can’t add them to the Polycom Cloud Service Administration portal.</td>
</tr>
<tr>
<td>Enterprise Only</td>
<td>Allows users to sign in using their enterprise account credentials from any of the configured authentication providers. Select this option if at least one additional authentication provider is available.</td>
</tr>
</tbody>
</table>

7. Click **Save**.

   The new user receives different welcome email messages depending on your selected account type:

   - If you selected **Enterprise and Local** in the **Sign In Account** field, the user receives a welcome email message with an activation link to begin activating the Polycom Cloud Service administration account.
   - If you selected **Enterprise Only** in the **Sign In Account** field, the user receives a welcome email message. The email message notifies the user has been added as an administrative user and instructs the user to use the enterprise account credentials to sign in.

**Related Links**

[Activate a Polycom Cloud Service Administration Account](#) on page 49

**Edit or Delete an Administration Account**

You can edit the properties of an administration account or delete it.

**Procedure**

1. In the Polycom Cloud Service Administration portal, go to **User Management**.
2. Click the user’s name that you want to edit.
3. In the user account configuration section, configure the required fields for the user, and do one of the following:
   - Click **Save** to save the changes, then click [close the configuration tab.](#)
   - Click **Cancel** to cancel the changes.

   The user receives different notification email messages depending on the **Sign In Account** type changes as follows:
   - If you changed the account type to **Enterprise and Local**, the user receives a welcome email with an activation link to begin activating the Polycom Cloud Service administration account.
   - If you changed the account type to **Enterprise Only**, the user receives a deactivation email indicating the Polycom Cloud Service administration account has been deactivated.

4. To delete the user account, click **Delete**.
Deleting a user account removes the user’s ability to sign into the Polycom Cloud Service Administration portal. When you delete a user account, the user receives an email notification of the account deletion.

**Related Links**

[Activate a Polycom Cloud Service Administration Account](#) on page 49

### Change User Interface Language

You can change the user interface language to one of the supported languages from different screens.

**Procedure**

- Change the user interface language in the top right corner of the **Sign In** screen.
- Change the user interface language in the bottom right corner of all the configuration screens.

### User Password

You can reset your password on the Polycom Cloud Service Administration **Sign In** screen; you can change your password from the account menu.

### Reset Your Password

If you forget your password, you can reset it from the **Sign In** screen.

**Procedure**

1. On the Polycom Cloud Service Administration **Sign In** screen, enter your email address in the **Email Address** field and click **Continue**.
2. When the **Sign In** screen reappears, click **Forgot Password**.
3. On the **Forgot Password** screen, ensure that your correct email address is shown in the **Enter your email address** field and then click **Submit**.
   A “Reset Password Request” email message is then sent to your email address.
4. Open the email and click **Set a New Password**.
   You are redirected to the **Reset Password** screen.
5. Create a password in the **Set Password** field.

**Note:** Password must be between 8 and 32 characters in length and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

6. Re-enter the password in the **Confirm Password** field.
7. Click **Submit**.

When the password is successfully reset, you are redirected to the **Sign In** screen, and a “Password Changed” email message is sent to you confirming that your password was changed.

### Change Your Password

You can change your password from the account menu.
Procedure

1. In the Polycom Cloud Service Administration portal, click the account menu (a drop-down list labeled with your name, found in the top right corner of the screen).

2. Select Change Password.

3. Enter your current password and new password.

4. Click Update.

Sign Out

You can sign out your account from the account menu.

Procedure

1. In the Polycom Cloud Service Administration portal, click the account menu (a drop-down list labeled with your name, found in the top right corner of the screen).

2. Select Sign Out.
Integrating with a Polycom Video System

Topics:

- Supported Polycom Video Systems
- Connecting a Polycom Video System Using Two Monitors
- Connecting a Polycom Video System Using Three Monitors
- Test Content Sharing
- Unpair a Polycom Video System

The Pano system can send content to a Polycom video system. Once your preferred setup is complete, content sharing is enabled; the Pano system detects when content is available and automatically presents it to the Polycom video system.

You can pair a Pano system with a Polycom video system using two or three monitors:

- **Two Monitors**  Configure the Pano system and Polycom video system to present content on the second monitor.
- **Three Monitors**  Integrate the Pano system with the Polycom video system and configure the Pano system to present content on the third monitor. For this setup, the Pano system content displays on two monitors.

Remember the following when enabling content on a Polycom video system:

- The Pano system must be used to share content during a meeting.
- Far-end annotations on content from the Pano system are not supported.
- Make sure you disable the VisualBoard application in the system web interface.
- The maximum resolution for content shared through a Polycom® RealPresence® Group Series system is 720p.

Polycom recommends the following when integrating your Pano system with a Polycom video system:

- Create a printout with the Pano system connection information (device name, security code, and enabled connection methods) for users who want to connect their device. Alternatively, you can go to the Polycom video system web interface and select the Content, then Near monitor profile to view the Pano system.
- Do not display the IP address on the Polycom video system local interface. This prevents users with personal devices from using that IP address to connect to the Pano system.

**Supported Polycom Video Systems**

The Pano system can pair with the following Polycom video systems:

- Polycom® RealPresence® Group Series 310, 500, 550, and 700 systems with software version 6.0 or later.
- Polycom® RealPresence Centro™ systems with software version 6.0 or later.
Connecting a Polycom Video System Using Two Monitors

You can pair a Pano system with a Polycom video system using two monitors.

Direct Connection Setup

You can directly connect your Pano system to a Polycom video system using two monitors.

Remember the following about this setup:

▪ Monitor 1 shows near and far video.
▪ Monitor 2 shows near and far content (only if the Pano system is in a session).
▪ Annotations made to far content cannot be seen by far-end participants.
▪ Users can connect their device (such as a laptop) to the Pano system using HDMI to share content.

The following diagram illustrates how the components for this setup are connected:

Direct Connection with Two Monitors Setup

Complete the Two-Monitor Setup (Direct Connection)

The following instructions describe how to directly connect your Pano system, Polycom video system, and two monitors.

Procedure

1. Make sure that the Pano system is running the latest software.
2. Connect one end of an HDMI cable to the HDMI Input port on the Pano system monitor.

3. Connect the other end of the HDMI cable to an HDMI Output port on the Polycom video system.

4. Connect one end of an HDMI cable to the HDMI Input port on the Polycom video system.

5. Connect the other end of the HDMI cable to the HDMI Output port on the Pano system, as shown in the following figure:

![Image of Pano System HDMI Out]

6. Configure your monitor profiles for your Polycom video system monitor:
   a. Open a browser and enter the IP address of the Polycom video system.
   b. Go to Admin Settings > Audio/Video > Monitors.
   c. For Monitor 1 at Monitor Profile, select Far, then Near.
   d. For Monitor 2 at Monitor Profile, select Content, then Far.

   The Pano system starts presenting content on the Polycom video system once the setup is complete. You must continue with the following steps to pair the systems and complete the setup.

7. Open a browser and enter the IP address of the Pano system.

8. Go to General Settings > Pairing.

9. Enter the IP Address, Admin User Name, and Admin User Password that are associated with the Polycom video system. (If no password is set, leave the password field blank.)

10. Select Connect, then select Pair.
    The Pair button displays only when the connection in the previous step is successful.

11. Optional: Modify the Pano system name, then select Update.

12. Test that content sharing functions properly.

Related Links
Test Content Sharing on page 74

HDMI Splitter Setup
With an HDMI splitter, you can connect a Pano system to a Polycom video system using two monitors. Remember the following with this setup:

- Monitor 1 shows far and near video.
- Monitor 2 shows near and far content (only if the Pano system is in a session).
• Annotations made to far content can be seen by all participants.
• Users cannot directly connect their device to the Pano system using HDMI.
• To share content during a meeting, you must first place a call on the Polycom video system and then start content.
• You need three HDMI cables and a 4K HDMI splitter for this setup.

Polycom has tested and recommends an HDMI splitter by CSRET with the following specifications:
• 1x2 HDMI Splitter Amplifier version 2.0
• Certified for 4Kx2K (60Hz) and 3D 1080p
• Supports 1 in 2 out signal distribution

You can use a different 4K splitter. If you do, make sure the specifications are comparable to those of the CSRET product.

The following diagram illustrates how the components for this setup are connected:

HDMI Splitter with Two Monitors Setup

Begin the HDMI Splitter Setup
There are some initial steps you must complete that are specific to connecting your Pano system and Polycom video system with an HDMI splitter.

Procedure
1. Make sure your Pano system is running the latest software.
2. Set the HDMI splitter to Scaler.
3. Connect one end of an HDMI cable to the splitter.
4. Connect the other end of the HDMI cable to the HDMI Output port on the Pano system, shown in the following figure:

![Pano System HDMI Out](image)

5. Connect one end of an HDMI cable to HDMI 1 on the splitter.

6. Connect the other end of the HDMI cable to the HDMI Input port on the Pano system monitor.

7. Complete the rest of the setup.

**Related Links**

*Complete the Two-Monitor Setup (HDMI Splitter or HDMI USB Adapter)* on page 69

**HDMI USB Adapter Setup**

With an HDMI USB adapter, you can connect a Pano system to a Polycom video system using two monitors.

Remember the following about this setup:

- Monitor 1 shows near and far video.
- Monitor 2 shows near and far content (only if the Pano system is in a session).
- Annotations made to far content can be seen by all participants.
- Users cannot directly connect their device to the Pano system using HDMI.
- To share content during a meeting, you must first place a call on the Polycom video system and then start content.
- You need two HDMI cables and an HDMI USB adapter.

The following diagram illustrates how the components for this setup are connected:
HDMI USB Adapter with Two Monitors Setup

Begin the HDMI USB Adapter Setup

There are some initial steps you must complete that are specific to connecting your Pano system and Polycom video system with an HDMI USB adapter.

Procedure

1. Make sure your Pano system is running the latest software.
2. Connect the adapter USB cable to the USB 3.0 port on the Pano system, shown in the following figure:

3. Complete the rest of the setup.

Related Links
Complete the Two-Monitor Setup (HDMI Splitter or HDMI USB Adapter) on page 69
Complete the Two-Monitor Setup (HDMI Splitter or HDMI USB Adapter)

Once you have connected your Pano system, Polycom video system, and two monitors (using an HDMI splitter or HDMI USB adapter), you can finish the setup.

You must connect the splitter or adapter (depending on your setup method) before you can complete the following steps.

Procedure

1. Configure your Pano system monitor settings:
   - a. Open a browser and enter the IP address of the Pano system.
   - b. Go to General Settings > Monitor.
   - c. Select Automatic for the Configure Monitor option.

   **Note:** If you instead choose to manually configure your monitor, make sure it supports your selected resolution. An unsupported resolution can cause display issues.

   Your changes automatically save, and the monitor adjusts to the configured resolution.

2. Configure the monitor profile for your Polycom video system monitor:
   - a. Open a browser and enter the IP address of the Polycom video system.
   - b. Go to Admin Settings > Audio/Video > Monitors.
   - c. For Monitor 1 at Monitor Profile, select Content, then Far, then Near.

3. Restart the Polycom video system.

4. Connect one end of an HDMI cable to the Polycom video system HDMI Input port (see images below for port location). (For RealPresence Group 700 systems, you must connect the HDMI cable to Input port 3.)
5. Connect the other end of the HDMI cable to an output port on the splitter or adapter, depending on your setup method.

6. Open a browser and enter the IP address of the Pano system.

7. Go to General Settings > Pairing.

8. Enter the IP Address, Admin User Name, and Admin User Password that are associated with the Polycom video system. (If no password is set, leave the password field blank.)

9. Select Connect, then select Pair.

   The Pair button displays only when the connection is successful.

10. In the Pair with RealPresence Group Series panel, do the following and select Update to save your settings:

   a. Optional: Change the name of the video input.

   b. Select the RealPresence Group Series HDMI Out is Connected to Pano checkbox if you have connected the Polycom video system.

      If you see an error message indicating that the Pano system Input port is not connected, ignore it for now.

11. Connect one end of an HDMI cable to the Monitor 2 port on the Polycom video system.

12. Connect the other end of the HDMI cable to the Pano system HDMI Input port.

13. Test that content sharing functions properly.
Note: If you disconnect and reconnect a cable from an HDMI USB adapter, the systems are no longer paired. To fix this issue, go to the Pano system web interface, unpair your Polycom video system, and pair it again.

Related Links
Test Content Sharing on page 74
Begin the HDMI Splitter Setup on page 66
Begin the HDMI USB Adapter Setup on page 68

Connecting a Polycom Video System Using Three Monitors

You can pair a Pano system with a Polycom video system using a three-monitor setup that lets you display far video, far and near content, and Pano system content during a meeting.

Remember the following about this setup:

▪ The monitor that is connected to the Pano system must be touch-capable.
▪ You need three HDMI cables and a 4K HDMI splitter for this setup.

Polycom has tested and recommends an HDMI splitter by CSRET with the following specifications:

▪ 1x2 HDMI Splitter Amplifier version 2.0
▪ Certified for 4Kx2K (60Hz) and 3D 1080p
▪ Supports 1 in 2 out signal distribution

You can use a different 4K splitter. If you do, make sure the specifications are comparable to those of the CSRET product.

Three-Monitor Setup
Room Setup with Three Monitors

Group Series Monitor 1

Group Series Monitor 2

Pano Monitor 3

Complete the Three-Monitor Setup
The following instructions describe how to connect your Pano system, Polycom video system, and three monitors.

Procedure

1. Make sure the Pano system is running the latest software.
2. Set the HDMI splitter to Scaler.
3. Connect one end of an HDMI cable to the splitter.
4. Connect the other end of the HDMI cable to the HDMI Output port on the Pano system, shown in the following figure:
5. Connect one end of an HDMI cable to HDMI 1 on the splitter.

6. Connect the other end of the HDMI cable to the HDMI Input port on the Pano system monitor.

7. Configure your Pano system monitor settings:
   a. Open a browser and enter the IP address of the Pano system.
   b. Go to General Settings > Monitor.
   c. Select Automatic for the Configure Monitor option.

   **Note:** If you instead choose to manually configure your monitor, make sure it supports your selected resolution. An unsupported resolution can cause display issues.

   Your changes automatically save and the monitor adjusts to the configured resolution.

8. Connect one end of an HDMI cable to the Polycom video system HDMI Input port (see images below for port location). (For RealPresence Group 700 systems, you must connect the HDMI cable to Input port 3.)
9. Connect the other end of the HDMI cable to an output port on the splitter
   The Pano system starts presenting on the Polycom video system once the systems and monitors
   are connected. You must continue with the following steps to pair the systems and complete the
   setup process.

10. In the system web interface, go to General Settings > Pairing.

11. Enter the IP Address, Admin User Name, and Admin User Password that are associated with
    the Polycom video system. (If no password is set, leave the password field blank.)

12. Select Connect, then Pair.
    The Pair button displays only when the connection in the previous step is successful.

13. Test that content sharing functions properly.

Related Links
Test Content Sharing on page 74

**Test Content Sharing**

You can perform a test to confirm that content sent from a Pano system is displaying on a Polycom video
system and vice versa. This is helpful when you are pairing systems from a remote location.

**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, go to General Settings > Pairing.

3. Select Start Content for one or both of the following tests depending on your setup:
   - Test Content to RealPresence Group Series: Checks if the Pano system HDMI Output port is properly connected to the Polycom video system HDMI Input port. You can tell the test is successful without simulating a call if the Polycom video system enters a preview state.
   - Test Content to Pano: Checks if the Polycom video system Monitor 2 port is properly connected to the Pano system HDMI Input port. You can tell the test is successful without simulating a call if the Pano system screen displays content from the Polycom video system. If unsuccessful, an error message displays on the Pano system web interface indicating that no content is detected.

4. When a test completes without errors, select Stop Content.

Related Links
Complete the Two-Monitor Setup (HDMI Splitter or HDMI USB Adapter) on page 69
Complete the Three-Monitor Setup on page 72
Complete the Two-Monitor Setup (Direct Connection) on page 64

Unpair a Polycom Video System

You can unpair a Polycom video system from a Pano system when you no longer want to pair with it, such as to pair a different system.

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, go to General Settings > Pairing.
3. Select Unpair.
Troubleshooting

Topics:

- Retrieve Log Files
- Contact Polycom Support

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

Retrieve Log Files

You can download log files from the Pano system web interface.

**Note:** The date and time of the log entries display in GMT.

**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, go to **Diagnostics > Logs**.
3. Select **Download system logs**.
   A dialog 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 and 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.