

Release Notes

Polycom® HDX® Systems, Version 2.7.1_J



Polycom announces the latest release of Polycom® HDX® software. This document provides the latest information about the Polycom HDX systems and version 2.7.1_J software.



This software meets the latest U.S. Department of Defense network requirements for listing on the Defense Switched Network (DSN) Approved Products List (APL), as maintained by the Joint Interoperability Test Command (JITC).

This document provides the latest information for security-conscious users running version 2.7.1_J software. The information in this document is not intended to imply that DoD or DISA certifies Polycom HDX systems. In order to use Polycom HDX systems in a DoD environment, the software version must have achieved UC APL certification. For a listing of certified software versions, refer to

<http://www.polycom.com/solutions/industry/index.html>

This version of the software is set to use the Maximum Security profile.

For more information about using the features described in this document, refer to the product documentation available at

www.polycom.com/videodocumentation.



When making a connection from a web browser to configure the Polycom HDX system, always enter the address of the Polycom HDX system in one of the following formats: `https://hostname` or `https://10.11.12.13`.

Using the HTTPS protocol ensures that the configuration of all login credentials (such as user names and passwords) are transmitted using an encrypted channel, including those user names and passwords used to communicate with third-party systems on your network. Using the HTTPS protocol severely limits the ability of anyone on the network to discover these credentials.

Software Version History

| Software Version | Description |
|------------------|------------------------------------|
| 2.7.1_J | Support for IPv6 gatekeepers. |
| 2.7.0_J | Support for new security features. |

Installing Version 2.7.1_J

Before You Install



Points to note about Software Update:

Because of changes in software functionality and the user interface, some settings might be lost when you upgrade to version 2.7.1_J or reinstall an older version after upgrading. Polycom recommends that you store your system settings using profiles and download your system directory before updating your system software to version 2.7.1_J. Do not manually edit locally saved profile and directory files. Refer to the *Administrator's Guide for Polycom HDX Systems* for more information.

Systems perform an internal restart before running Software Update. If you are updating a Polycom HDX system using a web browser, the internal restart is not visible from the web interface. This process improves the reliability of the update process by freeing up memory before performing the update.

Updating the Software from Versions Earlier than 2.7.0_J

Polycom recommends that you upgrade from software versions earlier than 2.7.0_J to 2.7.1_J by performing a USB software update. The features added or changed between these two releases could lead to unpredictable behavior if you use the Software Update feature in the HDX web interface. Using this recommended procedure deletes all of the settings on your HDX system, so be sure to keep notes about the customizations you have made. Customers upgrading Polycom HDX systems from version 2.6.x or earlier to version 2.7.1_J must have an upgrade key.

Follow these steps to perform a USB software update:

- 1 Power off the HDX system by holding down the **Power** button for 3-5 seconds.
- 2 Save one software package (.pup) file and one key code (.txt) file to the root of a USB storage device.
Refer to "[Running Software Update](#)" on page 3 for information about locating these files.
- 3 Insert the USB storage device into the USB port on the system.
- 4 While the system is powered off, press and hold the restore button to erase the system's flash memory.

The restore button is the very small hole located next to the **Power** button. Press the restore button by inserting the end of a straightened paperclip into the hole.
- 5 While holding the restore button, press the **Power** button once.
- 6 Hold the restore button for another 5 seconds and then release it to install the 2.7.1_J software update.

- 7 Use the remote control or keypad to step through the setup screens on your HDX system, being sure to select the **Maximum** security profile when you get to the Security screen.

Running Software Update

To update your system software from version 2.7.0_J to 2.7.1_J, use the Software Update feature in the Polycom HDX web interface. You do not need an upgrade key to install version 2.7.1_J on systems running version 2.7.0_J or later software.

To access Software Update:

- 1 For DoD Unified Capabilities Approved Product List (UC APL) software releases, go to www.polycom.com/solutions/industry/federal_government/certification_accreditation.html. For non-UC APL software releases, go to support.polycom.com and navigate to your product page.
- 2 Download the Polycom software update package for your system.
- 3 In the browser address line of Internet Explorer 6.x, 7.x, or 8.x, enter the system's IP address, for example, `http://10.11.12.13`, to access its web interface.

If Security Mode is enabled on the system, you must use secure HTTPS access (for example, `https://10.11.12.13`). Click **Yes** in the security dialog boxes that appear.
- 4 Enter the Admin ID as the user name (default is `admin`), and enter the Admin remote access password, if one is set.
- 5 Go to **Admin Settings > General Settings > Software Update** and follow the instructions on the screen.

For additional information about updating your software, refer to *Installing Software and Options for Polycom® HDX® Systems and Accessories*.

Installing on a Polycom HDX System Under Warranty or a Service Plan

If you are installing software on a Polycom HDX system that is under warranty or a service plan, you need an upgrade key to activate the installation. You can get that key by logging in to support.polycom.com and requesting the upgrade key. You need the Polycom HDX system's serial number to get the key.



Before upgrading from version 2.6.x or earlier to version 2.7.1_J, you must request the upgrade key for version 3.0 or later on the support website. The upgrade key for version 3.0 or later also works with all versions of software earlier than 3.0.

If the Polycom HDX system is not under warranty or a service plan, you need to get a license and then activate the license on support.polycom.com to obtain an upgrade key.

For more detailed information about installing Polycom software, refer to *Installing Polycom HDX Software and Options* on the webpage where you download the software.

Installing an Older Version after Upgrading to Version 2.7.1_J

If you reinstall an older version of software after upgrading to version 2.7.1_J, which is also known as downgrading, Polycom recommends performing a **Custom** installation and selecting **Erase System Flash Memory**. This option is available when you use Software Update in the HDX web interface.

What's New in Version 2.7.1_J

IPv6 Gatekeeper Support

This feature adds support for HDX systems to register and use H.323 gatekeepers on an IPv6 network. Most gatekeeper services currently supported on IPv4 networks are now available on IPv6 networks, including the following:

- Direct and routed call methods
- H.323 Annex O dialing

The following restrictions exist:

- Avaya Gatekeepers currently support only IPv4 networks.
- Firewall traversal is not supported in gatekeeper environments on IPv6 networks.
- Conference on Demand is not available on IPv6 networks.
- Registering with an alternate Gatekeeper is not supported on IPv6 networks.

Refer to the *Administrator's Guide for Polycom HDX Systems* for more information about IPv6 networks. All gatekeeper IP address fields now accept IPv6 addresses.

IPv6 Duplicate Address Detection (DAD) Control

You can now specify the number of Duplicate Address Detection (DAD) messages to transmit before acquiring an IPv6 address. The HDX system sends DAD messages to determine whether the address it is requesting is already in use.

Refer to the *Administrator's Guide for Polycom HDX Systems* for more information about DAD.

What's New in Version 2.7.0_J

New Polycom HDX 4000™ HD System

The new Polycom HDX 4000 HD system with Hardware Version C adds the following features:

- Ability to send and receive H.264 High Profile video, which preserves video quality and reduces the required network bandwidth
- Ability to receive 720p people video at 60 fps
- Ability to receive 1080p people video
- Ability to send and receive 720p content at 30 fps in these conditions:
 - Far end is capable of 60 fps
 - Call rate is 832 kbps or higher
- Ability to send and receive 1080p content at up to 15 fps in these conditions:
 - Far end is capable of 60 fps
 - Call rate is 832 kbps or higher
 - Video Quality is set to **Sharpness**

To find out which hardware version you have, go to **System > System Information**. For information about configuring this system, refer to the *Administrator's Guide for Polycom HDX Systems*.

Feature Restrictions in Maximum Security

When running Polycom HDX software version 2.7.0_J using the Maximum Security Profile, the following features are disabled, restricted, or unavailable:

- Polycom Global Directory Server
- All SIP functionality

- Integration with Microsoft Exchange calendaring service and Microsoft global directory
- Access to Microsoft Office Communication Server (OCS) Directory Server
- All presence features
- Traditional management mode (replaced by dynamic management mode)
- H.460 over IPv6
- Restrictions for some dialing features (for example, last number dialed) and recent calls, which can no longer be viewed from the menu
- Remote access through SNMP and telnet
- Remote control, remote monitoring, and links to product documentation and site map on the web interface
- Some serial port functionality
- People+Content IP™ (PPCIP)
- Access to utilities functions on the local and web interfaces, with the exception of the local calendar
- Support for languages other than English

Login Notification

When you log in to use the system, the pop-up message showing the time of the last successful login and the time of the last unsuccessful login also shows the number of unsuccessful login attempts to the HDX system that have been made from any source since the last login.

Certificates and Revocation

If your organization requires a secure environment, Polycom recommends that you have a strong understanding of certificate management before you implement these features.

Polycom HDX systems can generate and use certificates to authenticate network connections to and from the Polycom HDX system. Other web applications can also generate certificates, as you might notice when you navigate the Internet. The HDX system uses configuration and management techniques typical of public-key infrastructure (PKI) to manage certificates, certificate signing requests (CSRs, sometimes also called unsigned certificates), and revocation lists. ANSI X.509 standards regulate the characteristics of certificates and revocation.

The certificate authority (CA) is the trusted entity that issues, or signs, digital certificates for others, as well as the certificates associated with the CA itself. You can manage certificates and revocation only through the Polycom HDX web interface.

Polycom encourages you to check your system logs daily to ensure that your installed certificates are current.

To go to the web interface:

- >> Open a web browser and, in the browser address line, enter the system's secure host name or IP address (for example, <https://10.11.12.13>). Click **Yes** in the security dialog boxes that appear.

Certificates

Certificates are authorized externally when they are signed by the CA. The certificates can be automatically validated when they are used to establish an authenticated network connection, that is, the certificate is validated when it is used.

If the HDX system generates a certificate, the certificate is authorized externally after the CA signs it. Certificates can be automatically validated when you use them to establish an authenticated network connection. Therefore, even if a certificate is authorized, it is not considered to be valid until you use it.

A certificate exchange is between a server and a client, both of which are peers. When you are using an HDX system, the HDX system is a web server and the web browser is the client application. In other situations, such as when the HDX system needs access to LDAP directory services or provisioning, the system is the client that communicates with the LDAP or provisioning server.

You must restart the HDX system for certificate and revocation changes to take effect.

To configure certificate usage through the web interface:

- 1 Go to **Admin Settings > General Settings > Security > Certificates**.

2 Configure the following settings on the Certificates page.

| Setting | Description |
|--|---|
| Maximum Peer Certificate Chain Depth | Specifies how many links a certificate chain can have. The term <i>peer certificate</i> refers to any certificate sent by the far-end host to the HDX system when a network connection is being established between the two systems. |
| Always Validate Peer Certificates from Servers | Enables certificate validation by specifying whether the HDX system requires the server to present a valid certificate when the server makes secure connections for services such as provisioning, directory search, and session initiation protocol (SIP) calling. For some security profiles, this setting is always enabled. |
| Always Validate Peer Certificates from Browsers | Enables certificate validation by specifying whether the HDX system requires a browser to present a valid certificate when it tries to connect to the HDX web interface. For some security profiles, this setting is always enabled. |

To add a certificate on the Certificates screen:

- 1 Click **Choose File** and select a certificate.
- 2 Click **Add**.

The system checks the certificate data and adds it to the list. If you don't see the certificate in the list, the system was unable to recognize the certificate.

You can select a certificate in the list to view its contents. You can also remove a certificate from the list by clicking **Remove**.

When you add a CA certificate to the HDX system, the certificate becomes trusted for the purpose of validating peer certificates.

Certificate Signing Requests (CSRs)

The HDX system allows you to install one client and one server certificate for identification of the HDX system to network peers. Whether you need these client-type or server-type identity certificates depends on which HDX features and services you intend to use, and whether your network environment supports certificate-based authentication for those services.

For example, if your HDX system is configured to use the following features, you might need to create a client-type CSR and add the resulting certificate approved by the CA:

- Provisioning
- Polycom CMA® Monitoring
- Directory
- Presence
- Calendaring
- SIP
- 802.1X

Only the HDX web server uses the server-type CSR and resulting certificate. That is, the server certificate does not validate the client identity on the HDX system, but it does identify the HDX system to the browser. You need the server certificate if, as the browser user, you want to be certain about the identity of the HDX system you're connecting to. Settings in the web browser typically validate the server certificate but you can also validate the certificate manually. For example, if you use Internet Explorer, you can click the SSL padlock icon in the browser and examine the certificate that way.

The following applications are either disabled in Security Mode, or do not use digital certificates:

- Telnet
- H.323
- Global Management System™

If your HDX system uses features that require certificates and does not have the certificates installed, you must first create a CSR. You can create one client and one server CSR and submit each to the appropriate CA for signing. After the CSR is signed by a CA, it becomes a certificate you can add to the HDX system. If you create additional client or server CSRs on the HDX system, they replace the existing CSR of the same type.

If browsing to the HDX system by using DNS names results in a certificate error, please regenerate the CSRs and certificates.

To create a CSR on the web interface:

- 1 Go to **Admin Settings > General Settings > Security > Certificates**.
- 2 Click **Create** for the type of CSR you want to create. The procedure is the same for server and client CSRs.
- 3 Configure the following settings on the Create Certificate Signing Request (CSR) page.

| Setting | Description |
|------------------|---|
| Type | Creates either a Client or Server CSR. |
| Common Name (CN) | Displays the name that the system assigns to the CSR. |

| Setting | Description |
|---------------------------------|--|
| Organizational Unit (OU) | Specifies the unit of business defined by your organization. |
| Organization (O) | Specifies your organization's name. |
| City or Locality (L) | Specifies the city where your organization is located. |
| State or Province (ST) | Specifies the state or province where your organization is located. |
| Country (C) | Displays the country selected in Admin Settings > General Settings > Location . |



The HDX system supports only one OU field. If you want the signed certificate to include more than one OU field, you must download and edit the CSR manually.

Certificate Validity

When certificate validation is enabled (refer to page 7), the HDX system tries to validate the peer certificate chain on secure connection attempts for the applicable network services.

The **Always Validate Peer Certificates from Browsers** setting controls how the HDX web server behaves. Enabling this setting has an effect only if Security Mode is also enabled on the HDX system, because if Security Mode is not enabled, browsers can connect to the HDX web server through an unsecured IP address. If you don't use a secure address (HTTPS), certificates are not exchanged. With validation enabled, the HDX webserver rejects connection attempts from browsers that don't present a valid certificate.

The **Always Validate Peer Certificates from Servers** setting controls how all of the other SSL-enabled applications on HDX system, such as LDAP or provisioning behave. When this setting is enabled, these applications will try to validate the server certificate when they connect via SSL/TLS to a server. The connection will be rejected if the server does not present a valid certificate.

Validation might fail for other reasons, such as certificate expiration or revocation. The HDX system can check revocation status by using certificate revocation lists (CRLs) or the online certificate status protocol (OCSP). A CRL is a list of certificates that have been revoked by the CA. An OCSP responder is a network server that provides real-time certificate status through a query/response message exchange.

Configure the HDX system to use the same method that is used by the CA. You must get CRL data files from the CA.



If you use OCSP, you might need to install one or more additional CA certificates on the HDX system, for validation of the OCSP response messages.
The Polycom HDX system supports HTTP-based OCSP transactions.

To add CRLs on the web interface:

- 1 Go to **Admin Settings > General Settings > Security > Revocation**.
- 2 Configure the following settings on the Revocation page.

| Setting | Description |
|--|--|
| Revocation Method | Specifies whether to use CRL or OSCP for revocation. |
| Allow Incomplete Revocation Checks | When this field is enabled, specifies whether a certificate in the chain is verified without a revocation status check if no corresponding CRL is installed. The HDX system assumes that the lack of a CRL means the certificate is not revoked. If all required CRLs are installed, the system performs revocation checks when validating the certificate. |
| Add a Certificate Revocation List (CRL) | <ol style="list-style-type: none">1 Click Choose File to search for and select a CRL.2 Click Add to add the CRL to the list. |

You can also remove a CRL from the list by clicking **Remove**.

To configure OCSP on the web interface:

- 1 Go to **Admin Settings > General Settings > Security > Revocation**.

2 Configure the following settings on the Revocation page.

| Setting | Description |
|---|--|
| Revocation Method | Specifies whether to use CRL or OSCP for revocation. |
| Allow Incomplete Revocation Checks | When this field is enabled, the HDX system requests the revocation status from the OSCP responder. <ul style="list-style-type: none">• If the OSCP responds that the status is <i>unknown</i> or if no response is received for any certificate in the chain, the system continues checking and accepts the connection if no other validation errors occur.• If the OSCP responder indicates a known <i>revoked</i> status, the HDX system does not allow the connection.• If the OSCP responder indicates a known <i>good</i> status, the HDX system allows the connection. |
| Global Responder Address | Specifies the URI of the responder that services OSCP requests (for example, <code>http://responder.example.com/ocsp</code>). This responder is used for all OSCP validation. |
| Use Responder Specified in Certificate | In some cases, the certificate itself includes the responder address. When this field is enabled, the HDX system uses the address in the certificate (when present) instead of the Global Responder Address specified in the previous field. |

Delete Certificates and CRLs

In some cases, expired certificates or CRLs might prevent you from accessing the web interface. You can use the local interface to reset your system without certificates, to restore access to the web interface.

To delete all certificates and CRLs the HDX system is using:

- 1 On the local interface, go to **System > Diagnostics > Reset System**.
- 2 Enter your system's **Serial Number**.
- 3 Enable the **Delete Certificates** field.
- 4 Select **Reset System**.

The HDX system restarts after deleting all installed certificates and CRLs.

You can also use the API command `resetsystem deletecertificates` to reset your system without certificates.

Whitelist

When a whitelist is enabled, the Polycom HDX system allows access to its web interface only by those systems with an IP address that matches a pattern using regular expression notation that is specified by this setting. You can use this feature only through the web interface.

With regular expression notation, addresses are matched by pattern, which means that you must take care to form your regular expressions to allow only systems you mean to allow. In particular, regular expression notation treats the period (.) character as a single wildcard (*) character. This results in interpreting what looks like a normal IP address as a wildcard expression. For example, if you entered an IP address of 15.1.2.111, all of the following results would match:

- 15.1.2.111
- 15.182.1.11
- 15.1.252.111

In order to prevent the wildcard treatment of the period (.) character, you must use a backslash (\) character immediately preceding the period (.) character. This escapes the period (.) character so that it is treated as a period. Using this mechanism, the IP address 15.1.2.111 is correctly represented in regular expression notation as 15\.1\.2\.111

If you want to allow a range of IP addresses, use the wildcard (*). The following examples use the wildcard (*) to allow a range of IP addresses:

- Enter 10\.11\.*\.* to allow all IP addresses that begin with 10.11.
- To allow the IP address 1.2.3.4, any address in the 10.11.*.* subnet and any address in the 20.10.1x.* subnet, enter:
 - » 1\.2\.3\.4
 - » 10\.11\.*\.*
 - » 20\.10\.1\.*

To use a whitelist on the web interface:

- 1** Go to **Admin Settings > General Settings > Security > Whitelist**.
- 2** Select **Enable Whitelist**.
- 3** In the **Add IP Address** field, use regular expression notation to enter the IP address of the system you want to allow, then click **Add**.

Repeat this step for all the IP addresses you want to add.



If you entered an address in error, you can highlight it in the list and click **Remove**.

Sessions List

You can use the sessions list to see information about everyone logged in to an HDX system including:

- Type of connection:
 - **Web**, when users are logged in through the web interface
 - **Serial**, when users are logged in through the RS-232 port
 - **Local**, when users are logged in to the local interface
- User ID
- Remote IP address (that is, the addresses of people logged in to the HDX system from their computers)
- Session duration in hours, minutes, and seconds for each user currently logged into the HDX system
- How long the system has been idle, in seconds

To enable the Sessions List:

>> Go to **System > Admin Settings > General Settings > Security > Security Settings >  >  >** and set **Enable Sessions List**.

To view the Sessions List:

>> Go to **System > Diagnostics > Sessions**.

Remote Access Settings

Remote access means using a Polycom HDX system in some way other than through the local interface, such as by using the web, a serial port, or telnet. Refer to “[Sessions List](#)” on page 14 for information about the sessions mentioned in the table.

To configure remote access settings:

- 1 Go to **System > Admin Settings > General Settings > Security > Remote Access Settings**.

2 Configure the following settings on the Remote Access Settings page.

| Setting | Description |
|--|--|
| Idle Session Timeout in Minutes | When sessions are enabled, specifies the number of minutes your system can be idle before the web or serial API session times out. |
| Maximum Number of Active Web Sessions | When sessions are enabled, specifies the number of users who can be logged in to your system from the web at the same time. |
| Maximum Number of Sessions Per User | When sessions are enabled, specifies the maximum number of times a single user can be logged in to your system at the same time (regardless of which interface is used). |

The **Lock Port after Failed Logins** and **Port Lock Duration in Minutes** settings are discussed in “[Port Lockout](#)” on page 20.

Security Banner

In earlier HDX software versions, you could set a security banner only through the local interface. You can still do this, but Version 2.7.0_J adds the ability to create banners on the web interface.

To set a security banner on the web interface:

- 1 Go to **Admin Settings > General Settings > Security > Security Banner**.
- 2 Configure these settings on the Security Banner Settings page.

| Setting | Description |
|-------------------------------|--|
| Enable Security Banner | <p>Specifies the security banner to display.</p> <ul style="list-style-type: none">• Off — Disables the security banner.• Custom — Allows you to enter text to use for the banner.• DoD — Specifies that the system displays a default U.S. Department of Defense security banner. <p>Banners are displayed on the Login screen and the web’s Security Banner window.</p> <p>The following is an example of banner text:</p> <p>This machine is the property of Polycom, Inc., and its use is governed by company guidelines. You have NO right of privacy when using this machine.</p> |

| Setting | Description |
|----------------------------------|---|
| Local System Banner Text | If you enable the security banner on the web interface, enter up to ten lines of text, each of which can contain up to 128 single-byte characters. The lines of text run together in paragraph format when they appear on the local system. If you enable the security banner on the local interface, the ten lines where you enter text are displayed below the Enable Security Banner field. The local interface does not have a Local System Banner Text field. |
| Remote Access Banner Text | This field is visible only when you use the web interface. You can type or paste a maximum of 1,600 characters. |

Log Management

In earlier HDX software versions, you could use log management to set up and manage logs from the local interface. You can still do this, but Version 2.7.0_J adds the ability to set up and manage logs from the web interface. However, to transfer logs manually, you must still use the local interface. Refer to the *Administrator's Guide for Polycom HDX Systems* for information about setting up log management.

Security Profiles

Version 2.7.0_J uses five security profiles, which determine how administrators and users can use the Polycom HDX system. You can use these profiles to set various security levels for your environment according to the needs of your organization. The settings you can change after setup depend on which Security Profile you choose.

The following table describes the Security Profile levels.

| Setting | Description |
|----------------|---|
| Maximum | Restricts most settings. This profile is set during system setup and can be changed with the setup wizard only. With this profile, for example, some login settings are enabled with limited configurability to prevent security breaches. This profile is typically used for very high-level security, for example by some government agencies, and is the same as the former DoD/DSN setting. |
| High | Restricts certain settings, but you can change them at any time. This setting might be used by government agencies who need a high level of security, but not the maximum level, and who want more flexibility with how users' access is configured. |
| Medium | Restricts some settings and allows for more user actions. Most settings are configurable. This setting might be useful for system administrators who have a moderate concern for security. |

| Setting | Description |
|----------------|---|
| Low | Restricts very few settings. This setting might be useful for system administrators who want to require a password for remote access. |
| Minimum | Limitations are minimal. All settings are configurable. This setting might be useful for system administrators who require the lowest level of security in their environment. |

You set the Security Profile in the setup wizard during system setup. After the system is up and running, you can change the Security Profile setting only by returning to the setup wizard in instances such as these:

- After a software update with system settings deleted
- When you reset the system with system settings deleted
- By using the restore button

Prior to version 2.7.0_J, you enabled Security Mode to configure the HDX system to operate in a highly secure environment. Now, however, you can configure the system for the security level you need by choosing a Security Profile during the setup wizard. The Security Mode setting is configurable for some security profiles. If you choose the Maximum security profile, Security Mode is enabled by default and cannot be disabled.

To view the configuration settings for your Security Profile:

>> Go to **System > Admin Settings > General Settings > Security > Security Settings**.

External Authentication

Polycom HDX systems support two roles for accessing the system, an admin role and a user role. Admins can perform administrator activities such as changing configuration, as well as user activities such as placing and answering calls. Users can perform only user-type activities.

Polycom HDX systems provide two local accounts, one for the user role (by default named `user`) and one with for the admin role (by default named `admin`). The IDs and passwords for these local accounts are stored on the HDX system itself.

With version 2.7.0_J, an administrator can also configure HDX systems to grant access using network accounts that are authenticated through an Active Directory (AD) server. In this case, the account information is stored on the AD server and not on the HDX system. The AD administrator assigns accounts to AD groups, one for HDX system admin access and one for user access.

The HDX system administrator configures the external authentication settings on the HDX system to specify the AD group for user access and the AD group for admin access on the HDX system. The HDX system can map only one

Active Directory group to a given role. After the HDX system administrator selects **Enable Active Directory Authentication** and **Require Login for System Access**, users must enter their network name and password when the local HDX system interface prompts them to log in. Admins can enter either their local or network login information.

Software version 2.7.0_J supports Active Directory on Microsoft Windows Server version 2003 and Microsoft Windows Server 2008.



The HDX system user account is disabled when **Enable Active Directory Authentication** and **Require Login for System Access** are enabled.

To enable external authentication:


- 1 Go to **System > Admin Settings > General Settings > Security > External Authentication**.
- 2 Configure the following settings on the External Authentication screen.

| Setting | Description |
|---|--|
| Enable Active Directory Authentication | Specifies whether to authenticate users through the Active Directory server. When Active Directory authentication is enabled, login is required to access the Admin Settings on the HDX system. |
| Active Directory Server Address | Specifies the DNS or IP address of the Active Directory server. |
| Active Directory Admin Group | Specifies the Active Directory group whose members should have access to the Admin settings on the HDX system. This name must exactly match the name in the Active Directory server for authentication to succeed. |
| Active Directory User Group | Specifies the Active Directory group whose members should have access to the User settings on the HDX system. This name must exactly match the name in the Active Directory server for authentication to succeed. |

If your HDX system operates with the **Maximum** Security Profile enabled, the **Enable Active Directory Authentication** setting is enabled by default. Enabling the **Enable Active Directory Authentication** setting is the same thing as enabling external authentication.

When external authentication is enabled **and** login is required for system access, *administrators* can log in to the local interface by using the admin login configured on the HDX system or the login ID and password configured for

them on the Active Directory server. However, *users* can log in to the local interface only by using the ID and password configured for them on the Active Directory server.

To require login, go to **System > Admin Settings > General Settings > Security > Security Settings**, , and enable the **Require Login for System Access** setting.

Maintenance Window

Version 2.7.0_J supports the new maintenance window feature that is available in Polycom CMA system version 5.2J. This feature allows Polycom CMA system administrators to restrict automatic software updates for Polycom HDX systems to windows of time outside normal system use. An HDX system that has been configured this way will poll the CMA system for automatic updates only during that specified time window.

H.323 over IPv6

Polycom HDX systems now support using H.323 over IPv6 as well as IPv4. DNS entries can be resolved using IPv4, IPv6, or both.

The following settings are available only on the web interface. They apply to IPv4 and IPv6 configurations. Changing any of these settings causes the system to restart.

To use the new IPv4 and IPv6 settings on the web interface:

>> Go to **Admin Settings > LAN Properties** and configure the following settings on the LAN Properties screen.

| Setting | Description |
|--|--|
| Ignore Redirect Messages | Select to enable the HDX system to ignore redirect messages from network routers. A redirect message tells the endpoint to use a different router from the one it is using. |
| ICMP Transmission Rate Limit (millisec) | Enter a number between 0 and 60000 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 turned off. This setting applies only to "error" ICMP packets. This setting has no effect on "informational" ICMP packets, such as echo requests and replies. |

| Setting | Description |
|---|--|
| Generate Destination Unreachable Messages | Select to generate a Destination Unreachable message if a packet cannot be delivered to its destination for reasons other than network congestion. |
| Respond to Broadcast and Multicast Echo Requests | Select to send an Echo Reply message in response to a broadcast or multicast Echo Request, which is not specifically addressed to the HDX system. |

Setting Account and Port Lockouts

One of the Active Directory feature settings also controls how the account and port lockout features work. You enable and disable the Active Directory by using the **Enable Active Directory Authentication** setting on the External Authentication screen. Refer to “[External Authentication](#)” on page 17 for more information.

Account Lockout

When the Active Directory is enabled, the settings on the Account Management screen control both local and web interface login attempts.

For example, if you select **3** for the **Lock Account after Failed Logins** setting, a user who fails to log in properly twice on the web interface and twice on the local interface is locked out on the fourth attempt. When a user’s total number of incorrect login attempts from the local or the web interface reaches a number greater than what you set here, the user is unable to log in for the amount of time specified in the **Account Lock Duration in Minutes** setting.

If the Active Directory server is disabled, the account lockout feature controls lockouts from the local interface only.

Port Lockout

The port lockout feature has also been affected by the introduction of the external authentication feature. As stated in the previous section, when the Active Directory authentication is *enabled*, remote access through the web interface is controlled by account lockout. When the Active Directory server is *disabled*, remote access through all ports is controlled by the port lockout feature.

For example, if you select **3** for the **Lock Port after Failed Logins** setting, a user who fails to log in properly twice through the web interface and twice through the serial port is unable to log in for the amount of time specified in the **Port Lock Duration in Minutes** setting. However, the user can still log in through the local interface.

Receiving and Sending 1080p Content

The following systems now achieve a maximum frame rate of 15 fps for content in 1080p:

- Polycom HDX 4000 HD with Hardware Version C
- Polycom HDX 7000 HD with Hardware Version C
- Polycom HDX 8000 HD with Hardware Version B
- Polycom HDX 9006

New API Commands

The following API commands are new in version 2.7.0_J. These commands are fully described in the latest version of the *Integrator's Reference Manual for Polycom HDX Systems*.

| Command | Description |
|---------------------------|---|
| clientvalidatepeer | Sets or gets the requirement that HDX client applications validate server certificates such as for provisioning servers, directory services, and SIP calls. |
| destunreachable | Sets or gets the system's ability to generate a Destination Unreachable ICMP message in response to a packet that cannot be delivered to its destination for reasons other than congestion. |
| echoreply | Sets or gets the system's ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast/anycast address. |
| icmpoutpacketr | Sets or gets the minimum number of milliseconds between packets to limit the ICMP packet transmission rate. |
| ignoreredirect | Sets or gets the ability of the system to redirect messages, which may come from a router as part of the IPv6 Neighbor Discovery protocol. |
| incompleterevocationcheck | Sets or gets the ability to use or reject a certificate if revocation checking is incomplete. |
| ipv6addrmode | Sets or gets the ability for the system to act as a client and receive an address, specify an address manually, or completely disable IPv6. |
| ipv6defaultgateway | Sets or gets the IPv6 default gateway. |
| ipv6globaladdress | Sets or gets the IPv6 link global address. |
| ipv6linklocal | Sets or gets the IPv6 link local address. |
| ipv6sitelocal | Sets or gets the ipv6 site local address. |

| Command | Description |
|---|--|
| loginwindowduration | Specifies the period of time, in hours, in which the failed login threshold must be exceeded to lock the user's account. This command can be changed only through the command-line interface using the serial API. |
| ntpsecondaryserver | Sets or gets a secondary Network Time Protocol (NTP) server using the IP address or DNS name of the server. |
| sessionsenabled | Sets or gets the ability to monitor for and terminate inactive Polycom HDX web sessions. |
| servervalidatepeerpercent | Sets or gets the certificate presentation requirement for web clients connecting to the Polycom HDX web. |
| sslverificationdepth | Specifies how many links a certificate chain can have. |
| whitelistenabled Note: A restart is no longer required. | Sets or gets the ability to restrict a system's access to those systems with IP addresses that match one of the addresses or patterns specified in the whitelist. |

Changed API Commands

The following API commands have been modified in version 2.7.0_J.

| Command | Description |
|---|--|
| dial | Added pots, isdn_phone, and sip_speakerphone parameters. |
| remotecontrol Note: The remotecontrol command is not available when using the Maximum security profile. | Removed intercept parameter |
| resetsystem | Removed deleteall parameter. |

The following API commands have been removed in version 2.7.0_J:

- callencryption
- exportdirectory
- exportprofile
- gmscopy
- gmscontactemail
- gmscontactfax
- gmscontactnumber
- gmscontactperson
- gmscountry
- gmsstate
- gmstechsupport
- gmsurl
- importdirectory
- importprofile
- remotemonenable
- requireacctnumdial
- validateacctnum

Secure RS-232 Interface API Permissions

You must log in with a password in order to start an RS-232 session if the system is configured with the Maximum Security Profile, or if the system is configured for external authentication through Active Directory.

You can log in with either the Admin ID and Admin Room Password or the User ID and User Room Password. The available API commands depend on which type of ID you use to start the session. The complete version of the table listing the secure RS-232 interface API permissions is in the *Integrator's Reference Manual for Polycom HDX Systems*, but the following table identifies which commands are different for version 2.7.0_J.

| API Command | Parameter | User ID | Admin ID |
|--|---|---------|----------|
| autoshowcontent | on | | ✓ |
| | off | | ✓ |
| defaultgateway Note: set is not allowed while in a call. | get | | ✓ |
| | set "xxx.xxx.xxx.xxx" | | ✓ |
| farcontrolnearcamera | get | ✓ | ✓ |
| | yes | | ✓ |
| | no | | ✓ |
| ipaddress Note: set is not allowed while in a call. | get | ✓ | ✓ |
| | set "xxx.xxx.xxx.xxx" | | ✓ |
| isdnum Note: set is not allowed while in a call. | get 1b1 1b2 2b1 2b2 3b1 3b2 4b1 4b2 | ✓ | ✓ |
| | set 1b1 1b2 2b1 2b2 3b1 3b2 4b1 4b2 | | ✓ |
| isdnswitch Note: set is not allowed while in a call. | get | ✓ | ✓ |
| | pt-to-pt_at&t_5_ess multipoint_at&t_5_ess ni-1 nortel_dms-100 standard_etsi_euro-isdn ts-031 ntt_ins-64 | | ✓ |
| lanport Note: set is not allowed while in a call. | get | ✓ | ✓ |
| | 10, 10hdx, 10fdx, 100, 100hdx, 100fdx | | ✓ |
| ldapauthenticationtype | get | | ✓ |
| | set | | ✓ |
| | anonymous | | ✓ |
| | basic | | ✓ |
| | ntlm | | ✓ |

| API Command | Parameter | User ID | Admin ID |
|--|-------------------------------|----------|----------|
| ldapbasedn | get | | ✓ |
| | set "base dn" | | ✓ |
| ldapbinddn | get | | ✓ |
| | set "bind dn" | | ✓ |
| ldapdirectory | get | ✓ | ✓ |
| | yes | | ✓ |
| | no | | ✓ |
| ldapntlm domain | get | | ✓ |
| | set "domain" | | ✓ |
| ldappassword | set <ntlm basic> ["password"] | disabled | disabled |
| ldapsrveraddress | get | | ✓ |
| | set "address" | | ✓ |
| ldapsrverport | get | | ✓ |
| | set | | ✓ |
| ldapsrlenabled | get | | ✓ |
| | set [on, off] | | ✓ |
| ldapusername | get | | ✓ |
| | set "user name" | | ✓ |
| loginwindowduration | get | | ✓ |
| | set | | ✓ |
| | off | | ✓ |
| popupinfo | register | | ✓ |
| | unregister | | ✓ |
| | get | | ✓ |
| remotemonenable | get | ✓ | ✓ |
| Note: The remotemonenable command is not available when using the Maximum security profile. | | | |

| API Command | Parameter | User ID | Admin ID |
|---|---|---------|----------|
| requireacctnumtodial Note: The requireacctnumtodial command is not available when using the Maximum security profile. | get | ✓ | ✓ |
| | yes | | ✓ |
| | no | | ✓ |
| setaccountnumber Note: The setaccountnumber command is not available when using the Maximum security profile. | "account number" | | ✓ |
| spidnum Note: set is not allowed while in a call. | get <all 1b1 1b2 2b1 2b2 3b1 3b2 4b1 4b2> | | ✓ |
| | set <1b1 1b2 2b1 2b2 3b1 3b2 4b1 4b2> ["spid number"] | | ✓ |
| subnetmask Note: set is not allowed while in a call. | get | | ✓ |
| | set "xxx.xxx.xxx.xxx" | | ✓ |
| tcpports Note: set is not allowed while in a call. | get | | ✓ |
| | set | | ✓ |
| telnetechoeol | get | ✓ | ✓ |
| | crnl | | ✓ |
| | nldr | | ✓ |
| udpports Note: set is not allowed while in a call. | get | | ✓ |
| | set [{1024..49150}] | | ✓ |
| useroompassword | get | | ✓ |
| | no | | ✓ |
| | yes | | ✓ |
| v35num Note: set is not allowed while in a call. | get <1b1 1b2> | | ✓ |
| | set <1b1 1b2> ["v35 number"] | | ✓ |
| webport | get | | ✓ |
| | set Note: The set parameter is not available when using the Maximum security profile. | | ✓ |

Corrected Issues in 2.7.1_J

The following table lists issues corrected in version 2.7.1_J.

| Issue | Jira ID | Description |
|------------------------|-------------|--|
| Automatic Provisioning | VIDEO-91052 | When Polycom CMA systems provisioned HDX systems in a maximum security environment, users were required to ensure that sites were provisioned with the Enable Enterprise Directory Global Directory field enabled. This issue has been corrected. |

Corrected Issues in 2.7.0_J

The following table lists issues corrected in version 2.7.0_J.

| Issue | Jira ID | Description |
|---------|-------------|--|
| Audio | VIDEO-84517 | If more than three endpoints are connected to a Polycom HDX system hosting a multipoint call, and one of the endpoints plays audio content, and that endpoint is not the last endpoint connected to the call, audio is no longer garbled. |
| | VIDEO-84718 | Polycom HDX 9001 systems no longer experience distorted audio when the following sequence of events occurs: <ol style="list-style-type: none"> 1. The Polycom HDX 9001 system places a POTS call. 2. The Polycom HDX 9001 system places a video call to an endpoint that supports stereo. 3. The Polycom HDX 9001 system places a video call to an endpoint that does not support stereo. |
| Calling | VIDEO-84592 | A Polycom HDX system now connects a SIP call when an IPv6 address is used and SIP Transport Protocol is set to UDP . |
| | VIDEO-83607 | Video is no longer delayed on a Polycom HDX 9001 system when in a multipoint call with a Polycom HDX 8000 system with Hardware Version B that is hosting the multipoint call and sending content. |
| Content | VIDEO-85285 | Polycom HDX 8000 systems with Hardware Version B or a Polycom HDX 9006 system with Hardware Version B no longer restart when hosting a call. |
| | VIDEO-85286 | Polycom HDX systems can now send content when in a call with a Polycom RMX system when content resolution is configured for 800x600. |

| Issue | Jira ID | Description |
|--|-------------|--|
| Interoperability Microsoft | VIDEO-84367 | When a Polycom HDX system hosting a multipoint call is in a Office Communications Server SIP call with three Office Communicator clients, connecting to another Polycom HDX system via SIP no longer results in degraded video on the Polycom HDX system that joined the call. |
| | VIDEO-83905 | When a Microsoft Office Communicator client is in an audio-only call with a Polycom HDX system that is already in a point-to-point call with another Polycom HDX system, the Office Communicator client can now connect to the Polycom HDX system by video. |
| Interoperability Polycom RMX® | VIDEO-81370 | Occasionally, when a 1080p-capable Polycom HDX system places a SIP call to a Polycom RMX system configured for continuous presence at 1920 kbps or greater, the Interactive Voice Response (IVR) slide was not displayed. This issue was corrected in Polycom RMX system version 6.0. |
| Interoperability Polycom Video Border Proxy™ (VBP™) | VIDEO-84719 | Polycom HDX systems no longer restart after approximately 90 minutes when all of the following conditions are true: <ul style="list-style-type: none"> the Polycom HDX system is in an H.323 call the H.323 call is routed through a Polycom VBP system the Polycom HDX system has SIP enabled, and the SIP proxy server specified is incorrect |
| Interoperability Polycom VSX Systems | VIDEO-82744 | When a Polycom HDX 8006 system is in a mixed call with a Polycom VSX system connected over H.323 and a Polycom HDX 9001 system connected over ISDN, the Polycom HDX 9001 system no longer shows video latency in the PIP window when content is stopped and started among the different endpoints. |
| Interoperability Polycom VVX 1500 | VIDEO-84464 | Audio can now be heard from any site when a Polycom HDX system hosting a multipoint call connects via SIP to a Polycom VVX1500 phone and a TANDBERG E20 system. |
| Interoperability TANDBERG | VIDEO-74376 | In SIP calls greater than 2 Mbps with a TANDBERG MXP or Codian MCU, the call connected at 1920 kbps. This issue was corrected in TANDBERG 6000 MXP F9.0. |
| Monitors | VIDEO-70164 | You can now configure both Monitor 1 and Monitor 2 to display far-end video. |
| | VIDEO-84366 | Endpoints in a point-to-point SIP call receiving content no longer display frozen video if the system sending content switches from sending content from Camera 4 to Camera 2 without first stopping content on Camera 4. |
| Multipoint | VIDEO-83800 | When a Polycom HDX system hosting a multipoint call has Multipoint Mode set to Full Screen and is in a conference with three or more endpoints, the name of one site no longer displays while displaying the video from a different site. |

| Issue | Jira ID | Description |
|-------------------|-------------|--|
| Multipoint | VIDEO-84593 | In 4-way calls between Polycom HDX systems with stereo enabled, the last endpoint no longer connects with mono instead of stereo. |
| People+Content IP | VIDEO-81288 | When using People+Content IP to send content, residual artifacts might have been observed in areas with chroma-only changes. This issue was corrected in Polycom People+Content IP version 1.2.3. |
| People on Content | VIDEO-83850 | When a Polycom HDX system hosting a multipoint call has People On Content configured and is in a multipoint SIP call, the far endpoints no longer display black video. This issue occurred when the Polycom HDX system hosting the multipoint call stops sending content via People+Content IP and begins sending content via People On Content. |
| Power | VIDEO-83487 | Polycom HDX 6000 systems no longer restart when receiving a call after the content input resolution is changed from 10x7 to 720p. |
| Remote Control | VIDEO-84516 | Polycom HDX systems no longer become non-responsive when using the <code>remotecontrol intercept</code> API command because the <code>intercept</code> parameter has been removed from the <code>remotecontrol</code> command. |

Feature Limitations

The following table lists the known feature limitations for the version 2.7.1_J release. If a workaround is available, it is noted in the table.

| Category | Issue ID | Found in Release | Description | Workaround |
|-------------------------|-------------|------------------|---|--|
| Active Directory server | VIDEO-85246 | 2.7.0_J | Setting the Security Profile to Maximum during the Setup Wizard causes External Authentication to be enabled. Although administrators can create local user IDs and passwords, local users will not be able to access the HDX system as long as External Authentication is enabled. | After you complete the Setup Wizard, go to System > Admin Settings > General Settings > Security > External Authentication and disable the Enable Active Directory Authentication setting to allow local users to access the system. |
| Analog Phone | VIDEO-80791 | 2.6 | Incoming calls from analog phones do not display on the Recent Calls screen. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|--------------|-------------|------------------|---|---|
| Analog Phone | VIDEO-73949 | 2.5.0.4 | Do not use the analog phone connector if you are using a Polycom HDX 9000 series system in Hong Kong or South Africa. If your Polycom HDX 9000 series system came with a telephone adapter, refer to the accompanying telephone adapter setup sheet for information on whether the adapter is needed in your area. | None |
| API | VIDEO-51280 | 1.0 | The <code>remotecontrol enable all</code> command does not work after disabling the remote. Use <code>remotecontrol disable none</code> to enable the remote control buttons. | None |
| API | VIDEO-55286 | 1.0.2 | <pre>state[ALLOCATED] cs: call[38] chan[0] dialstr[172.26.48.42] state[RINGING] cs: call[38] chan[0] dialstr[172.26.48.42] state[BONDING] cs: call[38] chan[0] dialstr[172.26.48.42] state[COMPLETE] active: call[38] speed[512]</pre> <p>The notification in boldface is not applicable to calls made to/received from IP end points.</p> | None |
| API | VIDEO-80854 | 2.5.0.6 | In Polycom HDX software version 2.5.0.6, the end of line (EOL) characters on port 24 for the API echo command changed from <code><CR><CR><LF></code> to <code><CR><LF></code> . | You can now configure the EOL using the <code>te1netechoeol</code> command. Refer to the <i>Integrator's Reference Manual for Polycom HDX Systems</i> for more information. |
| API | VIDEO-83150 | 2.6 | The <code>camera register</code> command does not return local camera movements if the camera is moved using the remote control or the web interface. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|-------------|------------------|---|------------|
| Audio | VIDEO-55634 | 1.0.1 | If you establish multiple calls between the two systems, you may experience audio feedback. | None |
| Audio | VIDEO-60669 | 2.0 | Incoming voice calls do not work in a password-protected conference. | None |
| Audio | VIDEO-70543 | 2.5 | When you plug a headset into the Polycom HDX 4000 series panel, the system's built-in microphones and any attached microphones are automatically muted even though the Enable Polycom Microphones and Enable Built-In Microphones configuration settings remain selected. | None |
| Audio | VIDEO-69705 | 2.5 | Starting with the release 2.5, Polycom HDX systems do not play music while restarting. Polycom HDX systems running software version 2.6 play an announcement tone once the system has been successfully restarted. | None |
| Audio | VIDEO-69796 | 2.5 | You cannot enable or disable Stereo while in a call. | None |
| Audio | VIDEO-69797 | 2.5 | Do not connect or disconnect a Polycom SoundStation IP 7000 conference phone or Polycom HDX digital microphones while in a call. Doing so may result in some anomalous behavior such as audio coming out both the conference phone and Polycom HDX system. To restore normal operation, hang up the call. | None |
| Audio | VIDEO-71505 | 2.5.0.1 | Volume changes made during the setup wizard are lost when the system restarts. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|------------------------|-------------|------------------|--|---|
| Automatic Provisioning | VIDEO-80706 | 2.6 | The Polycom HDX Gateway Country Code value is not provisioned when the Polycom CMA® Administrator has created a scheduled provisioning profile with a value for the Gateway Country code. | Update the Gateway Country Code value manually on the Polycom HDX system via the local system interface or web interface. |
| Automatic Provisioning | VIDEO-67861 | 2.5 | If the Polycom HDX system is not connected to the IP network at startup, it may not check for provisioning changes until the next scheduled polling interval. | To make the system check for provisioning changes immediately, restart the system. |
| Automatic Provisioning | VIDEO-71385 | 2.5.0.1 | If Polycom HDX systems operating with automatic provisioning are unable to reach the presence service for an extended period of time (for example, due to a server problem or network outage), they will not reregister to the server once it becomes available. | If this occurs, restart the system. |
| Automatic Provisioning | VIDEO-82959 | 2.6.1 | Occasionally, when a Polycom HDX system is configured for dynamic management mode with a CMA server, the Polycom HDX system is not provisioned with the correct user name based on the provisioned User ID. | None |
| Automatic Provisioning | VIDEO-71305 | 2.5.0.1 | Polycom HDX systems operating with automatic provisioning check for software updates at an interval specified by the administrator. If an update is required, Polycom HDX 4000 systems perform the update even if they are currently being used as PC displays. | None |
| Automatic Provisioning | VIDEO-71440 | 2.5.0.1 | Polycom HDX systems sold in Russia do not operate with automatic provisioning. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|------------------------|-------------|------------------|--|---|
| Automatic Provisioning | VIDEO-76674 | 2.5.0.6 | When a Polycom HDX system in dynamic management mode is configured with a static IP address, presence information will not be displayed correctly. To resolve this issue, configure the Polycom HDX system for DHCP. | Do not use CMA to dynamically manage a Polycom HDX system located behind the VBP-ST Access proxy. |
| Automatic Provisioning | VIDEO-81291 | 2.5.0.5 | Occasionally, when a Polycom HDX system is being managed by Polycom CMA in dynamic management mode, the Polycom HDX system will not indicate that the Presence Server is down on the System Status screen when an invalid password is entered via the provisioning page on the web interface (the Provisioning Server will show a red down arrow). Restarting the Polycom HDX system results in the Presence Service status displaying the correct status. | None |
| Calling | VIDEO-78158 | 2.6 | Meeting passwords are not supported in SIP calls. | Use H.323 for calls that require meeting passwords. |
| Calling | VIDEO-51286 | 1.0 | Calls dialed using analog voice lines will not roll over to other call types if the call is busy or otherwise fails. | None |
| Calling | VIDEO-51323 | 1.0 | Do not mix unrestricted (speeds that are a multiple of 64 kbps) and restricted (multiple of 56 kbps) participants in an internal multipoint conference. | None |
| Calling | VIDEO-70792 | 2.5 | Do not use H.323 names that include a comma. | None |
| Calling | VIDEO-76492 | 2.5.0.6 | Calls do not connect if the Polycom HDX system is not restarted after changing ISDN settings. To avoid this issue, restart the Polycom HDX system any time an ISDN parameter is changed. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|-------------|------------------|--|---|
| Calling | VIDEO-80193 | 2.6 | When a Polycom HDX system hosting a multipoint call is connected to the maximum number of video endpoints, the Place A Call screen displays Add Video Call instead of Add Audio Call. The Polycom HDX system will be able to connect to an additional audio endpoint, but will not be able to connect to another video endpoint. | None |
| Calling | VIDEO-84627 | 2.6.1 | Occasionally, a Polycom HDX 4000 system configured for an analog POTS line will not be able to place or receive a POTS call. | Restart the Polycom HDX system and place or receive the call again. |
| Calling | VIDEO-81983 | 2.6 | Calls will not connect when a Polycom HDX system is registered to a Siemens OpenScape SIP server and the transport protocol is configured for TLS. | Use the TCP transport protocol. |
| Calling | VIDEO-87941 | 2.6.1 | In some environments, HDX systems with an analog phone interface to a PBX might be able to receive voice calls from internal, but not external, callers. | None |
| Calling | VIDEO-88199 | 2.7.0_J | HDX systems using call rates of 2x56 kbps or 2x64 kbps might fail to connect V.35 calls. | Use a call rate of 1x112 kbps or 1x128 kbps. |
| Cameras | VIDEO-80258 | 2.6 | The only supported camera for the Polycom HDX 4000 system is part of the video screen that is shipped with the Polycom HDX 4000 system. If a different camera is connected to the Polycom HDX 4000 system, the Polycom HDX 4000 will turn off (if powered on) or will not power on if in an powered off state. | To work around this issue, remove the unsupported camera and reconnect the video screen that was shipped with the Polycom HDX 4000 base system. |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|----------------------------|------------------|--|--|
| Cameras | VIDEO-80077 | 2.5 | The Polycom HDX system allows you to select a 4:3 aspect ratio when a Polycom EagleEye camera is selected, even though it is not a supported aspect ratio. The Polycom HDX system will automatically default to the supported 16:9 aspect ratio without informing the user that the 4:3 aspect ratio was not a supported resolution. | None |
| Cameras | VIDEO-80256 | 2.6 | On the Polycom HDX 4000 system, you do not receive notification that the preset is stored. | You can confirm the preset was stored by adjusting the camera video away from the preset position and then pressing the preset number on the remote. The camera video will display the preset correctly. |
| Cameras | VIDEO-80255 | 2.6 | When a Polycom HDX 4000 system is in a call, pressing the 0 button does not move the Polycom HDX 4000 camera to the default camera preset 0. | Manually adjust the camera to the desired position. |
| Cameras | VIDEO-80582 | 2.6 | Far-end camera control is not supported when in a multipoint call. | None |
| Cameras | VIDEO-51830 VIDEO-52304 | 1.0 | You may see blue video for a few seconds while the Polycom HDX camera wakes up. The camera may also take a few seconds to focus after waking up. | None |
| Cameras | VIDEO-59339 | 2.0 | If you downgrade the software from version 2.0 to an earlier version, you may need to reconfigure white balance on the Polycom EagleEye HD camera. | Select the detect camera command in the user interface or web interface, and then configure the white balance. |
| Cameras | VIDEO-69172 | 2.5 | Polycom HDX 4000, Polycom HDX 7000, and Polycom HDX 8000 series systems do not provide support for calibrating VGA input. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|-------------|------------------|--|---|
| Cameras | VIDEO-69794 | 2.5 | Do not configure a Polycom EagleEye camera for 4:3 aspect ratio. | None |
| Cameras | VIDEO-71003 | 2.5 | If you have an external power supply attached to a camera and you want to move that camera from one port to another, you must follow these steps: 1 Power off the camera. 2 Connect the camera to the new port. 3 Power on the camera. 4 Select Detect Camera in the system's user interface. | None |
| Cameras | VIDEO-81290 | 2.5 | When a Polycom EagleEye 1080 camera is attached to a Polycom HDX system, you can select a 4:3 aspect ratio, which will result in video stretched vertically with black bars on the side of the video. | Select an aspect ratio of 16:9. |
| Cameras | VIDEO-82105 | 2.6 | Occasionally, when the Detect Camera operation is performed for a camera that has been configured, the camera will no longer respond to camera pan, tilt, or zoom from the remote control. | Perform the Detect Camera action again. |
| Cameras | VIDEO-82747 | 2.5.0.4 | The camera name can be modified only with Roman-based characters. If you modify the camera name using non-Roman-based characters, a message displays instructing you to use valid characters on the keyboard. Trying to modify the camera name with non-Roman-based character results in the camera name disappearing. | Use Roman-based characters only when modifying the camera name. |

| Category | Issue ID | Found in Release | Description | Workaround |
|---------------|-------------|------------------|---|---|
| Cameras | VIDEO-84040 | 2.6.1 | When a Polycom EagleEye View camera is connected to a Polycom HDX system, the Power Frequency drop-down menu is shown on the Cameras Settings page. The Power Frequency drop-down menu is not applicable for the EagleEye View camera. | None |
| Cameras | VIDEO-84272 | 2.6.1 | The Backlight Compensation setting is not applicable when a Polycom EagleEye 1080 camera is connected as the main camera and the Power Frequency setting is set to 50Hz, even though the Backlight Compensation check box is not grayed out. | None |
| Cameras | VIDEO-84274 | 2.6.1 | When a Polycom EagleEye View camera is connected to a Polycom HDX system, the Camera Settings page displays the Backlight Compensation setting. As backlight compensation is not applicable to a Polycom EagleEye View camera, this setting should not be displayed. | None |
| Certificates | VIDEO-86500 | 2.7.0_J | If certificates are installed, you might get a Page Cannot Be Displayed message after manually changing the date or time. | Restart your HDX system after you manually change the date or time. |
| Certificates | VIDEO-94290 | 2.7.1_J | Attempts to add certificates that have spaces or parentheses in the file name fail. | Add certificates and create CSRs with file names that do not contain spaces or parentheses. |
| Chair Control | VIDEO-80897 | 2.6 | When a system acting as chair control selects the Disconnect Site icon to disconnect an endpoint from a conference, the web interface returns a status of denied, even though the endpoint was disconnected from the conference. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|-----------------|-------------|------------------|--|---|
| Chair Control | VIDEO-80896 | 2.6 | When a system acting as chair control selects an endpoint and selects the View Site icon, the endpoint's video will be shown but the web interface will provide a status of denied. | None |
| Chair Control | VIDEO-80895 | 2.6 | When a system acting as chair control selects an endpoint and selects the View Site icon, the endpoint's video will be shown. When the system with chair control selects the Stop Viewing Site icon, the web interface provides a status of denied but the endpoints video is no longer displayed. | None |
| Chair Control | VIDEO-80897 | 2.6 | When a system acting as chair control selects the Disconnect Site icon to disconnect an endpoint from a conference, the web interface returns a status of denied, even though the endpoint was disconnected from the conference. | None |
| Chair Control | VIDEO-74353 | 2.5.0.4 | When selecting a system to have chair control, the endpoint does not stay highlighted as being the chair control. To release chair control, highlight all the participants in the Meeting Participants window and select Release Chair . | None |
| Chair Control | VIDEO-83802 | 2.6.1 | Chair control is not supported when a SIP endpoint is in the call. | Connect all endpoints via H.323 or H.320. |
| Closed Captions | VIDEO-59615 | 2.0 | When providing closed captions over a serial connection, you must manually go to near video before entering text. | None |
| Closed Captions | VIDEO-60912 | 2.0 | Closed captioning (sent via either the serial port or the web interface) is limited to 31 characters per line. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|-------------|------------------|---|--|
| Contacts | VIDEO-70317 | 2.5 | Polycom HDX systems can share presence information with up to 200 Contacts. If a remote site attempts to invite the Polycom HDX system as a Contact after it has reached its limit of 200 Contacts, the Polycom HDX system rejects the invitation but does not display a warning message to the local user. | None |
| Contacts | VIDEO-68749 | 2.5 | You cannot delete Contacts using the web interface. Instead, delete them in the system's local interface. | None |
| Contacts | VIDEO-68748 | 2.5 | You cannot add Contacts that support presence using the web interface. Instead, add them in the system's local interface. | None |
| Contacts | VIDEO-70531 | 2.5 | With Allow Directory Changes provisioned to disabled, you can add Contacts, but you can't delete them. | Log into Polycom CMA Desktop with the same credentials used on your Polycom HDX system and delete the Contacts in Polycom CMA Desktop. |
| Content | VIDEO-79181 | 2.5.0.5 | A laptop connected to a Polycom HDX 9000 system as a content source might not be able to display content when the laptop resolution is configured for 1280x720. | Choose a different resolution for the laptop. |
| Content | VIDEO-51633 | 1.0 | Some DVI video sources (such as certain laptops) do not correctly support the hot plug detect pin (HPD). This can result in the source sending video in the wrong format for Polycom HDX video input ports 4 and 5. Please consult your equipment manuals to find out the behavior of the HPD pin. | None |
| Content | VIDEO-55041 | 1.0.2 | Presets support switching from one People source to another. Presets do not support switching from a People source to a Content source or from one Content source to another. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|-------------|------------------|--|---------------------|
| Content | VIDEO-58577 | 2.0.5.4 | Content at a resolution of 1280 x 1024 is scaled and sent to the far site in 1024 x 768 format unless the far site can display it at 1280 x 1024. | None |
| Content | VIDEO-59132 | 2.0 | You cannot send content from a Polycom HDX 4000 system using the Content button on a Polycom HDX remote control. You must use the built-in keypad button. | None |
| Content | VIDEO-61500 | 2.0.1 | If you have a computer connected to the Polycom HDX 4000 monitor when you install the People+Content option key, the Camera 2 setting does not change from People to Content. In this case you must go to the Cameras screen for Camera 2 and set Source to Content in order to send dual streams. | None |
| Content | VIDEO-70799 | 2.5 | When hosting a multipoint call, Polycom HDX systems typically stop showing content when a new participant joins the call. It may fail to do so when the fourth participant joins. | None |
| Content | VIDEO-81293 | 2.5.0.5 | If the Quality Preference setting on the Cameras screen is configured for content and a call is placed at 6 Mbps, the allocated bandwidth for content is only 1.5 Mbps. | None |
| Content | VIDEO-70793 | 2.5.0.5 | Polycom HDX systems do not support using 1080 sources for content. If a user attempts to send a 1080 source as content, the Polycom HDX system will not send it and will prevent future uses of that port for content, even if the source is switched to one that is supported. | Restart the system. |

| Category | Issue ID | Found in Release | Description | Workaround |
|-----------|-------------|------------------|--|---------------------------------|
| Content | VIDEO-71508 | 2.5.0.1 | When using a content source other than the VCR ports, audio associated with the content source may stop playing when people sources switch. The VCR content port does not have this problem. | None |
| Content | VIDEO-75994 | 2.5.0.6 | Occasionally, a Polycom HDX 9000 system will not show content when a computer connected directly to the Polycom HDX system is coming out of sleep mode. | Stop the content and resend it. |
| Directory | VIDEO-54360 | 1.0.2 | When the directory does not have enough entries, starting at the letter specified, to fill the screen, it shows earlier entries as well to fill the screen. | None |
| Directory | VIDEO-59898 | 2.0 | When navigating through entries in the directory, you may see both a solid yellow highlight and an outlined yellow highlight. | None |
| Directory | VIDEO-60603 | 2.0 | Directory entries do not successfully connect calls to sites dialed over ISDN voice. | Add voice sites manually. |
| Directory | VIDEO-61245 | 2.0.1.1 | When a directory entry has both an ISDN and IP address, calls placed as IP connect at the designated call rate for ISDN. | None |
| Directory | VIDEO-65729 | 2.0.5_J | An entry in a custom directory group may be removed from the group if you edit the entry. The entry is still available in the Contacts group. | None |
| Directory | VIDEO-70647 | 2.5 | From time to time a directory query may not return a full list of matching entries. | Reissue the request. |
| Directory | VIDEO-72682 | 2.5.0.1 | Only directory groups from the initial upgrade will be retained. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|------------|-------------|------------------|--|--|
| Directory | VIDEO-76896 | 2.5.0.7 | Directory groups created in earlier versions are retained when the Polycom HDX system is upgraded to 2.5.0.x and later. However, if the system is then downgraded to an earlier version and new directory groups are created, the newer groups will not be retained in subsequent upgrades. Local directory entries are deleted when a Polycom HDX system is reconfigured using the reset function under System > Diagnostics > Reset System , even when only the Delete System Settings check box is enabled. | None |
| Directory | VIDEO-83485 | 2.6.1 | If a Polycom HDX system is registered to a Global Directory Server (GDS) that contains more than 2,000 entries, and the Polycom HDX system is restarted, it can take approximately five additional seconds before you can place a call or go to the Directory screen. | None |
| Directory | VIDEO-83189 | 2.6.1 | If the Polycom HDX system is registered to a Global Directory Server (GDS) and the GDS has more than 1,000 entries, the Polycom HDX system occasionally will not be populated with the directory entries after the Polycom HDX system powers on. The Polycom HDX system updates from the GDS at the next polling interval (~ 20 minutes). | None |
| Encryption | VIDEO-77204 | 2.5.0.7 | When an unencrypted Polycom HDX system calls into an encrypted call between a TANDBERG MXP system and a Sony PCS-G50 system, the Polycom HDX system will connect but the Sony system will hear loud, distorted audio. | Enable encryption on the Polycom HDX system. |

| Category | Issue ID | Found in Release | Description | Workaround |
|--------------------------|-------------|------------------|---|---|
| Factory Restore | VIDEO-80175 | 2.6 | When performing a factory restore on an Polycom HDX 9000 series system, green video is displayed for a few seconds before the system restarts. This is normal behavior and the system will boot to the setup wizard. | None |
| Gatekeepers | VIDEO-60344 | 2.0 | Registering to a gatekeeper may change the dialing order configured on the system. | None |
| Global Management System | VIDEO-60340 | 2.0 | Global Management System shows Polycom HDX systems as being active even if they are powered off. | None |
| Global Management System | VIDEO-60339 | 2.0 | The Netstats page on the Global Management System reports the wrong call type for Polycom HDX systems. | None |
| Global Management System | VIDEO-74779 | 2.5.0.4 | Global Management System cannot add a Polycom HDX endpoint to its System Management page if the system has an administrator password configured. | Disable the administrator password. |
| Global Management System | VIDEO-75457 | 2.5.0.5 | When performing a Polycom HDX software update using Global Management System version 7.1.8, the Polycom HDX system files are not removed even when the Global Management System Polycom HDX software update page is configured to remove the files. | Update the Polycom HDX system from the Polycom HDX web interface. |
| Global Management System | VIDEO-76092 | 2.5.0.6 | When provisioning the Polycom global directory service server from Global Management System, Polycom HDX systems 2.5 or higher must have Polycom GDS enabled before the provisioning attempt is made. To register with the Polycom GDS directory server, go to System > Admin Settings > Global Services > Directory Services . | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------------------------|-------------|------------------|--|-------------------------------------|
| Hardware | VIDEO-80075 | 2.5.0.5 | Polycom HDX systems with a QBRI card installed do not issue an SNMP alert when the QBRI card is replaced with a PRI card. | None |
| Hardware | VIDEO-80072 | 2.5.0.5 | Polycom HDX systems do not issue an SNMP alert when a V.35 card is installed or uninstalled | None |
| Hardware | VIDEO-82738 | 2.6 | Polycom HDX systems restart when the CLink2 cable is connected incorrectly. | Connect the CLink2 cable correctly. |
| ICMP | VIDEO-86436 | 2.7.0_J | The ICMP Transmission Rate Setting on the LAN Properties screen applies only to "error" ICMP packets. This setting has no effect on "informational" ICMP packets, such as echo requests/replies. | None |
| Interoperability ADTRAN | VIDEO-70540 | 2.5 | The first call attempt after adjusting the call rate on an ADTRAN TSU 100 fails, but subsequent calls connect without a problem. | None |
| Interoperability Aethra | VIDEO-56589 | 1.0.2 | Polycom HDX systems are not able to send HD video to the Aethra X7 M11.1.4 HD unit. | None |
| Interoperability Aethra | VIDEO-73486 | 2.5.0.4 | Polycom HDX systems are unable to receive dual stream content from an Aethra X7 (software version 12.1.7) in a SIP call. The Polycom HDX system is able to send content to the Aethra X7 system. | None |
| Interoperability Aethra | VIDEO-73485 | 2.5.0.4 | When a Polycom HDX system stops sending content in a SIP call with an Aethra X7 (software version 12.1.7) system, the Aethra system displays frozen content. | None |
| Interoperability Aethra | VIDEO-73482 | 2.5.0.4 | Polycom HDX systems do not receive video from an Aethra X7 (software version 12.1.7) when a SIP call is made at 768 kbps or 1024 kbps. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------------------------|-------------|-----------------------|--|---|
| Interoperability Aethra | VIDEO-76238 | 2.5.0.4 | In high bandwidth calls, the Polycom HDX 6000 system will not connect with 720p video in a SIP call with an Aethra X7. | None |
| Interoperability Avaya | AVA-1064 | Aura 6.0, 1-XC 6.0 | When an HDX system, one-X communicator (1-XC), or Avaya 1000 Series video endpoints are registered to an Avaya Aura 6.0 platform and in a SIP call, DTMF tones are not sent to a far-end connection. This situation prevents DTMF from being sent to a device such as a Polycom RMX® server, which prevents the use of entry queues and in-conference functions. | None |
| Interoperability Avaya | AVA-1063 | 2.6.1 | If multiple HDX systems running version 2.6.1 software are registered to the Avaya Aura 6.0 platform, The HDX system can initiate calls but the calls are not completed. | Contact your Avaya Authorized service provider. |
| Interoperability Avaya | AVA-1062 | 2.6.1 | When registering an HDX system running version 2.6.1 to Avaya Aura 6.0, the registration for the HDX system is rejected with a message of "Missing/Invalid Header." | None |
| Interoperability Avaya | VIDEO-25528 | 1.0 | AES Encryption is not supported while registered to the Avaya Communication Manager. | None |
| Interoperability Avaya | VIDEO-25523 | 1.0 | When a Polycom HDX system attempts to call another Polycom system through Avaya Communication Manager, the near-site system continues to ring if the far site rejects the call. | None |
| Interoperability Avaya | VIDEO-25521 | 1.0 | NAT is not supported for systems registered to the Avaya Communication Manager. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|---------------------------|----------------------------|------------------|---|------------|
| Interoperability Avaya | VIDEO-25520 | 1.0 | While connected to the Avaya Communication Manager, telephony features are not supported to systems behind a neighboring gatekeeper. | None |
| Interoperability Avaya | VIDEO-25517 VIDEO-25526 | 1.0 | The Avaya Communication Manager version 4 supports wideband audio over trunk calls. However, Avaya Communication Manager version 4 will not support wideband audio over a trunk to Polycom PathNavigator. | None |
| Interoperability Avaya | VIDEO-25516 | 1.0 | Cisco PIX does not pass through Annex H, which is required by the Avaya Communication Manager. Polycom HDX systems will not connect calls across a firewall that does not pass Annex H. | None |
| Interoperability Avaya | VIDEO-25522 | 1.0 | Avaya's IP Softphone (IPSP) with video set to manual will not negotiate video with endpoints registered to a neighboring gatekeeper. | None |
| Interoperability Avaya | VIDEO-25519 | 1.0 | In calls placed from a Polycom HDX system, the far-site system name may show a neighboring gatekeeper, such as PathNavigator, instead of the actual system name. | None |
| Interoperability Avaya | VIDEO-25515 | 1.0 | G728 k and G722.1-16 k audio codecs are not available when registered to the Avaya Communication Manager. | None |
| Interoperability Avaya | IP338 VS2277 | 1.0 | Internal MCU calls from a Polycom iPower™ system to an Avaya IP Softphone (IPSP) or Polycom HDX system do not connect. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|---|----------------------------|------------------|---|---|
| Interoperability Avaya | VIDEO-25478 VIDEO-48111 | 1.0.2 | Avaya Communication Manager Telephony features and IPSP video mute are not supported with Polycom HDX, V500™, Polycom VSX, iPower, or Polycom ViewStation FX systems behind PathNavigator. iPower IMCU calls to Polycom HDX systems using Avaya do not connect. | None |
| Interoperability Avaya | — | | The Avaya Communication Manager does not support Polycom Siren™ 22 audio or Siren 22 stereo. | None |
| Interoperability Avaya | VIDEO-63595 | 2.0.2 | If you set the Gatekeeper field to Specify with PIN , you will see an additional field Outbound Call Route . Ignore this field. | None |
| Interoperability Avaya | VIDEO-66117 | 2.0.5_J | When configuring the Polycom HDX system gatekeeper setting to Specify with PIN , you may see an extraneous field called PathNavigator for Multipoint Calls . Ignore this field. | None |
| Interoperability Avaya | VIDEO-86609 | 2.6 | When a Polycom HDX system running software version 2.6.1 sends content over SIP, the Avaya 1000 Series video endpoints display the content on the primary video channel. The Avaya 1000 Series video endpoints do not support the Binary Floor Control Protocol (BFCP) SIP content. | None |
| Interoperability Avaya | VIDEO-88118 | 2.7.0_J | Avaya 1XC clients that use the Microsoft VX-6000 camera as a video source might transmit distorted video to the HDX system. | Use the Microsoft VX-5000 camera instead. |
| Interoperability BroadSoft BroadWorks | VIDEO-84589 | 2.6.1 | Occasionally, the Polycom HDX system displays black video when in a SIP point to point call with a VVX 1500 phone when using the BroadSoft BroadWorks platform. | Place the call again. |

| Category | Issue ID | Found in Release | Description | Workaround |
|---|----------------------------|------------------|--|--|
| Interoperability BroadSoft BroadWorks | VIDEO-88124 | 2.7.0_J | Clink-to-dial calls in a Broadworks environment do not work when the HDX system is configured to use UDP as its transport protocol. | Configure the HDX system to use a transport protocol other than UDP. |
| Interoperability BroadSoft BroadWorks | VIDEO-88123 | 2.7.0_J | Attended Transfer SIP calls in a Broadworks environment do not work when the HDX system is configured to use UDP as its transport protocol. | Configure the HDX system to use a transport protocol other than UDP. |
| Interoperability Cisco | VIDEO-50658 VIDEO-50623 | 1.0 | Cisco PIX does not support H.239. Disable H.239 on the endpoints. | None |
| Interoperability Cisco | VIDEO-69803 | 2.0.2 | Far-end camera control does not work in calls that go through a Cisco Catalyst 6509 with Firewall Service Module version 3.1(1). | None |
| Interoperability Cisco | VIDEO-78448 | 2.5.0.7 | When a Polycom HDX system connects to a Cisco device with 2SIF/2CIF resolution, the Cisco device displays the HDX system video as black video. | Place the call again at a higher rate to connect with a higher resolution, or call with a lower rate to connect with lower resolution. |
| Interoperability Cisco | VIDEO-79110 | 2.5.0.6 | Polycom HDX calls experience degraded video if a Cisco PIX firewall is used in H.323 Fixup mode. | Disabling H.323 Fixup Mode on the Cisco PIX firewall corrects the issue. |
| Interoperability Cisco | VIDEO-84363 | 2.6.1 | A Polycom HDX system may experience pixilation or watercolor-like effects in darker environments when in a multipoint call hosted by a Cisco/RADVISION system. This issue may occur on Polycom HDX 7000 series systems, Polycom HDX 8000 series systems, and Polycom HDX 9006 systems with Hardware Version B or later. | This issue has been identified and corrected the following Cisco software below. <ul style="list-style-type: none"> • RADVISION Scopia Classic version 5.7.1.0.11 • Cisco MCU 3515/3545 Series version 5.7.0.0.8 Please contact Cisco support for more assistance with this issue. |

| Category | Issue ID | Found in Release | Description | Workaround |
|------------------------------|-------------|------------------|---|--|
| Interoperability iPower | VIDEO-51282 | 1.0 | Polycom HDX systems transmit and receive H.263 content rather than H.264 content in calls with iPower 9000 systems running 6.2.0. | None |
| Interoperability LifeSize | VIDEO-56734 | 1.0.2 | In SIP calls between Polycom HDX and LifeSize 2.6 systems, Polycom HDX systems do not receive 720HD. | None |
| Interoperability LifeSize | VIDEO-56733 | 1.0.2 | In SIP calls between Polycom HDX and LifeSize 2.6 systems, neither system has far-site camera control. | None |
| Interoperability LifeSize | VIDEO-56732 | 1.0.2 | In SIP calls between Polycom HDX and LifeSize systems, Polycom HDX systems send 711u audio. | None |
| Interoperability LifeSize | VIDEO-60350 | 2.0 | In a SIP multipoint HD call with a Polycom HDX 9004 system as the host, you cannot dial out to the second HD endpoint when LifeSize is connected as the first endpoint in the call. | None |
| Interoperability LifeSize | VIDEO-61014 | 2.0 | LifeSize systems may experience poor audio in SIP calls with Polycom HDX systems. | None |
| Interoperability LifeSize | VIDEO-71453 | 2.5.0.1 | LifeSize Express systems running 4.0.6(7) software transmit video at 15 frames per second in HD calls with Polycom HDX systems. | None |
| Interoperability LifeSize | VIDEO-77465 | 2.5.0.7 | A Polycom HDX system cannot send content when it is in a SIP call with a LifeSize Room system and H.239 is enabled. | To work around this issue, place the call using H.323. |
| Interoperability LifeSize | VIDEO-84509 | 2.6.1 | When a Polycom HDX system is in an H.323 point-to-point call with a LifeSize Room or LifeSize Room 200 system, the LifeSize system cannot control the Polycom HDX system's camera if the Polycom HDX system has far end camera control enabled. | Place the call as a SIP call. |

| Category | Issue ID | Found in Release | Description | Workaround |
|-------------------------------|-------------|------------------|---|---|
| Interoperability LifeSize | VIDEO-86789 | 2.7.0_J | Calls between Polycom HDX systems and Lifesize Room Systems over IPv6 do not connect when both systems are configured for maximum security. | None. |
| Interoperability LifeSize | VIDEO-88116 | 2.7.0_J | H.323 calls with Lifesize Team 220/4.6.1.5 systems might not receive audio from Lifesize. | Configure HDX for Basic mode. Note: Basic Mode severely limits the features available in a call. Among other things, Basic Mode disables content, far end camera control, and encryption. |
| Interoperability Microsoft | | | Users might have trouble using Internet Explorer to access the web interface, but have no such trouble when using Mozilla Firefox. | In Internet Explorer, go to Tools > Internet Options and click the Advanced tab. Under the Security section, make sure that Use SSL 3.0 is the only SSL choice selected. |
| Interoperability Microsoft | VIDEO-80679 | 2.6 | When a Polycom HDX system is configured for integration with Microsoft Office Communications Server and is in a point-to-point 2M SIP call, the call disconnects after approximately 10 hours. | Place the call again. |
| Interoperability Microsoft | VIDEO-61286 | 2.0.1 | When People Video Adjustment is set to Stretch on a Polycom HDX 8000 HD system in a call with Microsoft Office Communicator, Office Communicator displays black video. | None |
| Interoperability Microsoft | VIDEO-81020 | 2.6 | The Office Communications Server should be configured to allow no more than 200 contacts (this is the default setting). If the Office Communications Server allows more than 200 contacts and more than 200 contacts are in the directory, the Polycom HDX system may show up to 200 contacts, or none. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|-------------------------------|-------------|------------------|--|---|
| Interoperability Microsoft | VIDEO-82848 | 2.6.1 | If there is a meeting password configured for a multipoint meeting hosted on a Polycom HDX system, Microsoft Office Communicator clients cannot join the meeting. | None |
| Interoperability Microsoft | VIDEO-84365 | 2.6.1 | Occasionally, if three Office Communicator clients simultaneously call a Polycom HDX system hosting a multipoint call, the Polycom HDX system restarts. | None |
| Interoperability Microsoft | VIDEO-83849 | 2.6.1 | The user interface of a Polycom HDX system hosting a multipoint call may experience reduced response when in a high-bandwidth, 5-way federated Interactive Connectivity Establishment (ICE) call. | Reduce the call bandwidth used to place the call, or use a Polycom RMX to host the multipoint call. |
| Interoperability Microsoft | VIDEO-84732 | 2.6.1 | Polycom HDX systems do not support presence in federated ICE calls. | None |
| Interoperability Microsoft | VIDEO-84717 | 2.6.1 | During a federated Interactive Connectivity Establishment (ICE) call between an Office Communicator client and a Polycom HDX system, the Office Communicator client disconnects from the Polycom HDX system after approximately three hours. | Place the call again, or place the call between two Polycom HDX systems. |
| Interoperability Microsoft | VIDEO-84628 | 2.6.1 | A Polycom HDX system hosting a multipoint call with five or more endpoints may restart if the call is encrypted and using ICE. | Do one of the following: <ul style="list-style-type: none"> Use a Polycom RMX system to host the multipoint call. Place the calls to the Polycom HDX system hosting the multipoint call at 384 kbps or lower. |

| Category | Issue ID | Found in Release | Description | Workaround |
|-----------------------------------|-------------|------------------|--|---|
| Interoperability Microsoft | VIDEO-85242 | 2.6.1 | <p>If you experience connectivity issues with federated voice or video, check the Polycom web site for updates and notifications, and verify that you have the latest software version.</p> <p>Polycom continues to run tests between various Office Communications Server federated environments. These environments are highly complex and customized with different firewall software, settings, and versions.</p> <p>Polycom is committed to updating support for new environments in future releases.</p> | None |
| Interoperability Microsoft | VIDEO-86180 | 2.7.0_J | <p>Internet Explorer version 8 shares cookies among all active sessions. If you manage multiple HDX systems within the same Internet Explorer 8 browser session, you might encounter unexpected behavior.</p> | <p>When using Internet Explorer 8, do one of the following:</p> <ul style="list-style-type: none"> • Manage only one HDX system at a time. • Use the -noframemerging option in each new instance of Internet Explorer for each system. |
| Interoperability Microsoft | VIDEO-88084 | 2.7.0_J | <p>Polycom HDX version 2.7.0_J has not been qualified with Microsoft Office Communications Server.</p> | None |
| Interoperability PathNavigator | VIDEO-53371 | 1.0 | <p>Multipoint directory entries with speed configured for Auto will be placed at the maximum rate supported by the calling system. In some cases, this may be greater than the rate supported by the network.</p> | <p>Do one of the following:</p> <ul style="list-style-type: none"> • Configure the directory entry for the desired speed, rather than leaving it as Auto. • Configure your gatekeeper to downspeed call requests to a rate that the network supports. |

| Category | Issue ID | Found in Release | Description | Workaround |
|---|-------------|------------------|---|--|
| Interoperability PathNavigator | VIDEO-60656 | 2.0 | Set Use PathNavigator for Multipoint Calls to Always if you want to automatically use the Polycom PathNavigator Conference on Demand to place multipoint calls. | None |
| Interoperability PathNavigator | VIDEO-60602 | 2.0 | When using PathNavigator Conference on Demand to place multipoint calls to Polycom VSX systems using ISDN, the conference may connect with audio only. Polycom MGC 9.0 resolves this issue. | None |
| Interoperability Polycom Converged Management Application™ (CMA®) Desktop (CMAD) | VIDEO-80757 | 2.6 | Polycom CMAD displays confusing information when a Polycom HDX system has been added as a buddy, Polycom CMAD is configured with no camera, and Enable Call without a Camera is disabled. The Polycom CMAD displays the correct presence status (for Polycom CMAD) -- the Polycom HDX system is unavailable. But when you select the Polycom HDX contact and view its details, Polycom CMAD shows the Polycom HDX contact is online and call capable. This could be misleading to the Polycom CMAD user because, although Polycom CMAD cannot place a video call, the Polycom HDX contact is capable of receiving a video call. | None |
| Interoperability Polycom MGC | VIDEO-80753 | 2.6 | When a Polycom HDX 6000 system calls into a Polycom MGC conference, the Polycom MGC sends 4:3 video to the Polycom HDX 6000 system. | Place the call again using a Polycom RMX system. |
| Interoperability Polycom MGC | VIDEO-75997 | 2.5.0.6 | Polycom HDX systems occasionally display video updates when content is sent during a MGC50+, 1920 kbps, encrypted, H.239-enabled video switched conference. | Set the conference call rate at a rate lower than 1920 kbps. |

| Category | Issue ID | Found in Release | Description | Workaround |
|---------------------------------|-------------|------------------|--|--|
| Interoperability Polycom MGC | VIDEO-81365 | 2.6 | Polycom HDX systems do not connect with audio or video when placing a SIP call to a Polycom MGC. | Place the call as an H.323 call. |
| Interoperability Polycom MGC | VIDEO-51962 | 1.0 | Polycom HDX systems in high-speed, video-switched conferences with Polycom Pro-Motion on Polycom MGC may experience video artifacts when sending content. | Polycom MGC 8.0.0.26 resolves this issue. |
| Interoperability Polycom MGC | VIDEO-51969 | 1.0 | Polycom HDX 9004 systems connect as audio only in H.320 Pro-Motion conferences on Polycom MGC-100 v7.5.1.6. | None |
| Interoperability Polycom MGC | VIDEO-52306 | 1.0 | Configure Polycom HDX system video content sources for motion when connecting with a video-switched sharpness conference on Polycom MGC v7.5. | None |
| Interoperability Polycom MGC | VIDEO-52496 | 1.0 | Enable H.239 on Polycom HDX systems when connecting into a Polycom MGC conference configured for H.239. | None |
| Interoperability Polycom MGC | VIDEO-53388 | 1.0 | If you are using Conference on Demand with a Polycom HDX system, configure this feature to use Continuous Presence or Transcoding instead of Video Switched . | None |
| Interoperability Polycom MGC | VIDEO-58840 | 1.0.1 | When People Video Adjustment is set to zoom, Polycom HDX systems may crop some messages sent by Polycom MGC. | None |
| Interoperability Polycom MGC | VIDEO-60343 | 2.0 | Polycom HDX systems with H.323 that do not have H.239 enabled on them do not receive content in video switching and continuous presence H.239/People+Content conferences with Polycom MGC version 9.0.1.5. | To address this issue, enable H.239 on the Polycom HDX system. |

| Category | Issue ID | Found in Release | Description | Workaround |
|--|-------------|------------------|---|---|
| Interoperability Polycom MGC | VIDEO-88398 | 2.7.0_J | Encrypted H.239 conferences between HDX systems and MGC100 9.0.4.3 might fail to connect. | Disable H.239 or Encryption. |
| Interoperability Polycom PVX™ | VIDEO-51274 | 1.0 | When H.239 is disabled, Polycom HDX systems transmit and receive H.263 content (instead of H.264 content) in calls with Polycom PVX. | Enable H.239. |
| Interoperability Polycom RMX | VIDEO-71383 | 2.5 | In an HDCP call hosted by Polycom RMX 1000™ systems, layout changes that move Polycom HDX systems from a small window to a large window (and vice versa) may take several seconds. | None |
| Interoperability Polycom RMX | VIDEO-74330 | 2.5.0.4 | Content is sent as H.263 content when in an H.320/ISDN call with the Polycom RMX system (which is configured for H.264 content). | None |
| Interoperability Polycom RMX | VIDEO-82335 | 2.6 | Occasionally, when a Polycom HDX system is in a bridge call with a 5.0.1 Polycom RMX system and a large amount of packet loss occurs, video artifacts will be displayed. | Disconnect the call and place it again at less than 5% packet loss. |
| Interoperability Polycom RMX | VIDEO-82746 | 2.5.0.2 | When a Polycom HDX system is in a call with a Polycom RMX 1000, the Polycom HDX video freezes momentarily and returns to live video only when the RMX conference video layout configuration is changed. | None |
| Interoperability Polycom RMX | VIDEO-86864 | 2.7.0_J | Calls hosted on an RMX 7.0.x might occasionally experience distorted video. | Disconnect the call and place it again. |
| Interoperability Polycom RSS™ 2000 | VIDEO-49888 | 1.0 | Polycom RSS 2000 supports a maximum call speed of 1024 kbps. To record a conference in HD using Polycom RSS 2000, make sure that the Polycom HDX system is configured for sharpness. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|--|---|------------------|--|--|
| Interoperability Polycom RSS™ 2000 | VIDEO-51952 | 1.0 | Polycom HDX systems display blocky, gray video for a few seconds after leaving the Polycom RSS 2000 menu. | None |
| Interoperability Polycom RSS™ 2000 | VIDEO-57005 | 2.0 | In calls using a Polycom RSS 2000, audio is transmitted using G.722.1 Annex C. | None |
| Interoperability Polycom VSX Systems | VIDEO-71451 | 2.5.0.1 | Calls between Polycom HDX and Polycom VSX systems configured for Pro-Motion may experience poor video (interlacing artifacts). | Disable Pro-Motion on the Polycom VSX system. |
| Interoperability Polycom VSX Systems | VIDEO-74778 | 2.5.0.4 | When a Polycom VSX system running version 9.0.5 makes a SIP connection to an existing point-to-point H.323 call between two Polycom HDX endpoints, the Polycom HDX system hosting the multipoint call appears unresponsive and the call statistics indicate no transmit or receive video on any of the endpoints. On occasion, the Polycom VSX SIP system will restart. The above-described call scenario will work if the Polycom VSX system is upgraded to version 9.0.5.1. | None |
| Interoperability Polycom VVX 1500 | VIDEO-76858 | 2.5.0.7 | Occasionally, when a Polycom HDX system is placed on hold and then taken off hold while in a call with a Polycom VVX 1500 phone, content and video are not displayed. This issue occurs only when content is being sent using People+Content IP. | Stop and then restart content. |
| Interoperability Polycom VVX 1500 | Interoperability Polycom VVX 1500 | VIDEO-84464 | Audio will not be heard from any site when a Polycom HDX system hosting a multipoint call connects via SIP to a Polycom VVX1500 phone and a TANDBERG E20 system. | Enable transcoding on the Polycom HDX system and place the call again. |

| Category | Issue ID | Found in Release | Description | Workaround |
|---|-------------|------------------|--|--|
| Interoperability Polycom V500 | VIDEO-77720 | 2.5.0.7 | When a Polycom HDX system that is hosting a multipoint call is in the call with a Polycom V500 and call downspeeding is required, black video or frozen video is displayed. | Make the call with a non-V500 system or place a call that does not require downspeeding. |
| Interoperability RADVISION | VIDEO-51298 | 1.0 | In calls using a RADVISION via IP gateway, Polycom HDX 9004 H.323 systems report packet loss on the transmit side, even though such packet loss might not exist. | None |
| Interoperability RADVISION | VIDEO-54999 | 1.0.2 | Polycom HDX 9004 systems cannot send dual streams to a Polycom HDX 9001 system in IP-to-ISDN calls made through the RADVISION via IP gateway. | None |
| Interoperability RADVISION | VIDEO-84363 | 2.6.1 | A Polycom HDX system may experience pixilation or watercolor-like effects in darker environments when in a multipoint call hosted by a Cisco/RADVISION system. This issue may occur on Polycom HDX 7000 series systems, Polycom HDX 8000 series systems, and Polycom HDX 9006 systems with Hardware Version B or later. | This issue has been identified and corrected the following Cisco software below. <ul style="list-style-type: none"> • RADVISION Scopia Classic version 5.7.1.0.11 • Cisco MCU 3515/3545 Series version 5.7.0.0.8 Please contact Cisco support for more assistance with this issue. |
| Interoperability ReadiManager SE200 | VIDEO-59959 | 2.0 | ReadiManager SE200 version 3.0.6 software supports all Polycom HDX software versions through version 2.5. ReadiManager SE200 versions earlier than 3.0.6 do not support the new software update method required for Polycom HDX version 2.5 or later software. | None |
| Interoperability ReadiManager SE200 | VIDEO-61512 | 2.0 | ReadiManager SE200 does not support account validation. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|---|-------------|------------------|--|--|
| Interoperability ReadiManager SE200 | VIDEO-70225 | 2.5 | If a Polycom HDX system becomes unresponsive after a software update from ReadiManager SE200, restart the system. | None |
| Interoperability Sony | VIDEO-51276 | 1.0 | H.323 encrypted calls between a Polycom HDX system and Sony PCS-1 produce a constant audio screeching. | Disable AES encryption. |
| Interoperability Sony | VIDEO-56588 | 1.0.2 | Polycom HDX systems are not able to receive video in an AES HD call from HG90. | None |
| Interoperability Sony | — | | Content sent from Sony PCS-1 or PCS-G50 systems to Polycom HDX systems may display video artifacts. | None |
| Interoperability Sony | VIDEO-61208 | 2.0.1 | Content received on a Sony PCS-1 is not legible if Content Video Adjustment is set to Stretch on the Polycom HDX system. | Set Content Video Adjustment to None . |
| Interoperability Sony | VIDEO-70510 | 2.0.1 | Calls between Polycom HDX systems and Sony PCS-HG90 systems may result in video divergence on the Sony system and freezing video on the Polycom system. | None |
| Interoperability Sony | VIDEO-69687 | 2.5 | Polycom HDX systems can receive but not place SIP calls with Sony PCS-1, PCS-G50, or G70 systems. | None |
| Interoperability Sony | VIDEO-69181 | 2.0.2 | Sony PCS-G70, PCS-G50, and PCS-1 systems receive distorted audio in point-to-point SIP calls with Polycom HDX systems at call rates of 192 kbps and below. | None |
| Interoperability Sony | VIDEO-68009 | 2.0.3.1 | A Sony PCS-HG90 HD system generates continuous fast updates in a call with Polycom HDX systems. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|---|-------------|------------------|--|---|
| Interoperability Sony | VIDEO-73200 | 2.5.0.4 | In an H.320 call when H.239 is enabled (System > Admin Settings > Network > Call Preference), a Sony PCS-1600 and VS-1 with version 3.33 are unable to connect to a Polycom HDX system. | Disable H.239 on the Polycom HDX system. |
| Interoperability Sony | VIDEO-74245 | 2.5.0.4 | If a Polycom HDX system is sending content to a Sony XG80 in an H.323 call, the Sony XG80 will not be able to send content. | Do not simultaneously send content between a Polycom HDX system and a Sony XG80. |
| Interoperability Sony | VIDEO-74244 | 2.5.0.4 | A Sony PCS-1 system is not able to receive content from a Polycom HDX system when in a restricted line rate H.320 call. | Place the call at an unrestricted call rate solves the issue. |
| Interoperability Sony | VIDEO-76241 | 2.5.0.6 | When a Sony PCS-XG80 is hosting a multipoint call, and two Polycom HDX systems connect to it via H.323, the second Polycom HDX system to connect will display distorted video during the conference. | Use a Polycom VSX system as the second system to connect. |
| Interoperability Sony | VIDEO-81373 | 2.5.0.1 | Occasionally, a Sony XG80 system does not receive video when in an H.320 call with a HDX system. | Place the call as an H.323 call. |
| Interoperability Sony | VIDEO-81306 | 2.5.0.4 | When a Sony XG80 system is hosting a multipoint call, and in a call greater than H.323 128 kbps with two Polycom HDX systems, the second Polycom HDX system that joins the call transmits distorted video. | Place the call at 128 kbps or use a Polycom HDX system as the system hosting the multipoint call. |
| Interoperability SoundStation IP 7000 | VIDEO-69799 | 2.5 | Audio calls to a Polycom HDX system integrated with a Polycom SoundStation IP 7000 automatically join the conference when they connect. By contrast, a standalone SoundStation IP 7000 will place the conference on hold when connecting the new call. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|---|-------------|------------------|---|---|
| Interoperability SoundStation IP 7000 | VIDEO-69959 | 2.5 | If a Polycom HDX system integrated with a SoundStation IP 7000 phone receives multiple incoming calls, answer or ignore them in the order received. | None |
| Interoperability SoundStation IP 7000 | VIDEO-71384 | 2.5.0.1 | When answering calls to add sites to a multipoint conference, use the down arrow on the IP 7000 keypad to go to the next user interface screen to Answer or Reject the calls. | None |
| Interoperability SoundStation IP 7000 | VIDEO-75763 | 2.5.0.6 | When using a SoundStation IP 7000 keypad to place a call on a Polycom HDX system, the asterisk (*) character is automatically converted to a dot. | To enter an asterisk, press the Video button and then press the * button on the SoundStation IP 7000 keypad three times. |
| Interoperability SoundStation IP 7000 | VIDEO-80858 | 2.5.0.6 | Occasionally, the SoundStation IP 7000 loses the dial tone when connected to a Polycom HDX system. | Restart the Polycom HDX system. |
| Interoperability SoundStation IP 7000 | VIDEO-81369 | 2.6 | When a SoundStation IP 7000 is connected to a Polycom HDX system, configuring the SoundStation IP 7000 to Do Not Disturb will only apply to calls received on the IP 7000 directly. The SoundStation IP 7000 Do Not Disturb setting does not apply to calls made to the Polycom HDX system via H.323, H.320, or PSTN. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|---|-------------|------------------|--|--|
| Interoperability SoundStation IP 7000 | VIDEO-81368 | 2.6 | <p>When a SoundStation IP7000 phone is attached to a Polycom HDX system and the SoundStation IP 7000 system is used to place an audio call to another SoundStation IP 7000, the called SoundStation IP 7000 is placed on hold instead of being added to the multipoint call when the Polycom HDX system places a H.323 call to another Polycom HDX system via the Polycom HDX system's user interface.</p> <p>The called SoundStation IP 7000 system will be automatically added to the video call if the video participant is called using the SoundStation IP 7000 touchpad of the SoundStation IP 7000 connected to the Polycom HDX system.</p> | None |
| Interoperability SoundStation IP 7000 | VIDEO-80469 | 2.6 | <p>When a Polycom HDX system with a SoundStation IP 7000 attached makes a 4-way call, the SoundStation IP 7000 becomes idle if the last endpoint called is an ISDN endpoint. To end the call, use the Polycom HDX remote instead of hanging up from the SoundStation IP 7000.</p> | Make all endpoints H.323 or make a three-way call using an ISDN endpoint as the last endpoint. |
| Interoperability SoundStation IP 7000 | VIDEO-80467 | 2.0.3 | <p>When a Polycom HDX system is ISDN-capable but has disabled ISDN Voice and has a SoundStation IP 7000 attached, the SoundStation IP 7000 registers a missed call when an endpoint attempts to dial the ISDN number as a voice call.</p> | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|---|-------------|------------------|--|--|
| Interoperability SoundStation IP 7000 | VIDEO-80466 | 2.5 | When a Polycom HDX system configured with a SoundStation IP 7000 makes an audio call between the SoundStation IP 7000 and another SoundStation IP 7000, the far end SoundStation IP 7000 does not receive the audio when the Polycom HDX system switches to camera 3 connected to a DVD or VCR playing audio. | Place the audio call from the Polycom HDX system using a POTS line instead of using the SoundStation IP 7000. |
| Interoperability SoundStation IP 7000 | VIDEO-80176 | 2.6 | When a Polycom HDX system is in a call, do not disconnect and then reconnect a SoundStation IP 7000 to the Polycom HDX system. If a SoundStation IP 7000 is disconnected and then reconnected while the Polycom HDX is in a call, end the call to allow the Polycom HDX and the SoundStation IP 7000 to synch back up. | None |
| Interoperability SoundStation IP 7000 | VIDEO-81353 | 2.6 | Occasionally, when a Sound Station IP 7000 is attached to a Polycom HDX system, the SoundStation IP 7000 makes faint audio popping sounds. | Restart the SoundStation IP 7000 and Polycom HDX system. The audio popping goes away when a call is placed but may be heard again once the call has been disconnected. |
| Interoperability SoundStructure | VIDEO-81510 | 2.5.0.2 | When a Polycom SoundStructure system is connected to a Polycom HDX system, the microphones attached to the SoundStructure system will not be displayed on the Polycom HDX system's Audio Meter page. This issue occurs in the user and web interfaces. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|------------------------------|-------------|------------------|---|---|
| Interoperability TANDBERG | VIDEO-94158 | 2.7.1 | When one Polycom HDX system is registered to a gatekeeper on a DMA system that is neighbored to a gatekeeper on a Cisco TelePresence Video Communication Server (Cisco VCS) and another HDX system is registered to a Cisco VCS, calls between the two systems dialed by e.164 (extension) and H.323 ID do not connect. | Do one of the following: <ul style="list-style-type: none"> • Configure the DMA GK in routed mode. • Dial the call by IP address. |
| Interoperability TANDBERG | VIDEO-56587 | 1.0.2 | Polycom HDX systems are not able to send HD video to TANDBERG 6000 MXP systems. | None |
| Interoperability TANDBERG | VIDEO-51835 | 1.0 | In a multipoint H.320 call with a TANDBERG MXP F5.0, a Polycom HDX system stops receiving people video when the Polycom HDX system sends content. | None |
| Interoperability TANDBERG | VIDEO-55635 | 1.0.2 | TANDBERG and Polycom products use different techniques to generate the AES checksum shown on the Statistics screen. As a result, these numbers will not agree in calls between TANDBERG and Polycom systems. | None |
| Interoperability TANDBERG | VIDEO-58833 | 2.0 | In H.323 calls at 512 kbps and higher, TANDBERG MXP systems receive video artifacts from Polycom HDX systems. TANDBERG version F6.2 corrects this issue. | None |
| Interoperability TANDBERG | VIDEO-65939 | 2.0.2 | When registered to a TANDBERG gatekeeper, calls do not connect properly if you enter the gatekeeper address in the address field and the far-end extension (E.164 address) in the extension field. | Enter <ip address>##<extension> in the address field. |
| Interoperability TANDBERG | VIDEO-69706 | 2.5 | Content does not work in SIP calls between Polycom HDX systems and TANDBERG MXP systems. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|------------------------------|-------------|------------------|--|---|
| Interoperability TANDBERG | VIDEO-81374 | 2.5 | A Polycom HDX system cannot receive H.239 content when in a SIP call with a Tandberg MXP system. | Place the call as an H.323 call. |
| Interoperability TANDBERG | VIDEO-82286 | 2.6 | A Polycom HDX system transmits content at 15 fps when in a point-to-point H.323 call with a TANDBERG 6000 MXP system. | None |
| Interoperability TANDBERG | VIDEO-76239 | 2.5.0.6 | When a second Polycom HDX system connects to a TANDBERG MXP in an H.323 or H.320 conference, the Polycom HDX video appears elongated. | Place the call using H.323. |
| Interoperability TANDBERG | VIDEO-76889 | 2.5.0.7 | Polycom HDX systems cannot send content when H.239 is enabled and is in a SIP call with a TANDBERG C20 system. | None |
| Interoperability TANDBERG | VIDEO-77681 | 2.5.0.7 | A Polycom HDX system will not receive content from a TANDBERG C20 system if the Polycom HDX system sends content before the TANDBERG C20 system sends content. | Stop sending content from the Polycom HDX system before sending content from the TANDBERG C20 system. |
| Interoperability TANDBERG | VIDEO-80872 | 2.5.0.8 | Polycom HDX systems connect at 15 fps when in a 768 kbps H.320 call with a TANDBERG 6000 MXP system. | To obtain 30 fps, place the call as an H.323 call. |
| Interoperability TANDBERG | VIDEO-82102 | 2.6 | A TANDBERG C20 system cannot receive content from a Polycom HDX 9006 system on the first attempt when in a 720p call. | Send content again or place the call as a 1080p call. |
| Interoperability TANDBERG | VIDEO-83606 | 2.5.0.8 | When a TANDBERG system in a multiway call with another TANDBERG system initiates a call to a Polycom HDX system, the Polycom HDX system will restart. | None |
| Interoperability TANDBERG | VIDEO-87667 | 2.7.0_J | Encrypted calls between HDX and Tandberg systems using 2x56 K ISDN have poor audio and video quality. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|---------------------------------|-------------|------------------|---|---|
| Interoperability VCON | VIDEO-56729 | 1.0.1 | The Polycom HDX 9001 system does not negotiate H.264 video with the VCON HD3000 system if H.239 is enabled in the call. H.263 video is negotiated instead. | None |
| Interoperability VCON | VIDEO-51304 | 1.0 | VCON HD3000 systems may display poor video in calls with a Polycom HDX system. | None |
| Interoperability VCON | VIDEO-70393 | 2.5 | In calls between VCON HD3000 and Polycom HDX systems, the VCON system sends content to the Polycom system in a single stream instead of dual streams. | None |
| Interoperability ViewStation | VIDEO-71797 | 2.5.0.4 | In an H.323 point-to-point call between a Polycom HDX system and a ViewStation (version 7.5.4), the mute status of the Polycom HDX system is not shown on the ViewStation but the ViewStation's mute status is shown on the Polycom HDX system. | None |
| Interoperability ViewStation | VIDEO-51292 | 1.0 | In calls between Polycom HDX systems and ViewStation systems with Basic Mode enabled, the ViewStation system does not receive video. | Turn off Basic Mode. |
| Interoperability ViewStation | VIDEO-51223 | 1.0 | ViewStation EX/FX v6.0.5 does not support People+Content in calls with Polycom HDX systems. | Update to ViewStation EX/FX version 6.0.5.20. |
| Interoperability ViewStation | VIDEO-52027 | 1.0 | Polycom HDX systems do not receive graphics from ViewStation systems. | None |
| Interoperability ViewStation | VIDEO-53153 | 1.0 | In four-way H.320 calls that include ViewStation as a far site, sending content from a Polycom HDX system may cause ViewStation to display frozen video. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------------------------------|-------------|------------------|--|--|
| Interoperability ViewStation | VIDEO-81285 | 2.6 | When a Polycom HDX 9004 system is in a 1472 kbps H.323 call with a ViewStation FX system, the ViewStation FX audio will sound distorted if both sites send audio at the same time. | None |
| Interoperability Westinghouse | VIDEO-60490 | 2.0 | When using a Polycom remote control with the default channel ID of 3, the remote control signal can interfere with a Westinghouse LCD HD monitor. | To work around this issue, change the channel ID of the remote control and Polycom HDX system. |
| IPv6 | VIDEO-88499 | 2.7.0_J | The ping tool for IPv6 works correctly with ICMP. However, H.323 and SIP are not reachable when using the ping tool for IPv6. | None |
| IPv6 | VIDEO-88913 | 2.7.0_J | You might see unexpected behavior on an HDX system when you manually configure IPv6 on a network that does not support Multicast Listener Discovery (MLD). | None |
| Localization | VIDEO-71091 | 2.5 | Limit names of localized directory entries to 31 or fewer characters. | None |
| Localization | VIDEO-71092 | 2.5 | Directory entries with localized names longer than 21 characters are truncated on the Edit Entry screen. | Limit localized names to 20 or fewer characters on the Edit Entry screen. |
| Localization | VIDEO-70798 | 2.5 | Localized system names longer than 13 characters are truncated on some of the system's local interface screens. | Limit localized system names to 13 or fewer characters. |
| Localization | VIDEO-70797 | 2.5 | Localized meeting names longer than 14 characters are truncated on some of the system's local interface screens. | Limit localized meetings names to 14 or fewer characters. |
| Localization | VIDEO-70796 | 2.5 | Localized Names in the directory longer than 17 characters are truncated on some of the system's local interface screens. | Limit localized names in the directory to 17 or fewer characters. |

| Category | Issue ID | Found in Release | Description | Workaround |
|--------------|-------------|------------------|---|---|
| Localization | VIDEO-80894 | 2.6 | The tilde “~” and minus “-” symbols display as a box on the Calendar and Meeting Details screen when a user is using a Japanese version of Outlook running on the Japanese version of Windows and the Polycom HDX language is configured for Japanese. | None |
| Logging | VIDEO-66818 | 2.0.5_J | By default, both system and error logs downloaded from a Polycom HDX system are named log.txt. | When downloading multiple logs, rename the logs to have unique names. |
| Monitors | VIDEO-51308 | 1.0 | User interface distortion might occur if a monitor is configured with a 4:3 aspect ratio for a resolution of 1280 x 720. | None |
| Monitors | VIDEO-53390 | 1.0 | Distorted video may occur in a multipoint call between PAL and NTSC systems if Zoom People Video to Fit Screen is enabled. | None |
| Monitors | VIDEO-53960 | 1.0.1 | Borders are clipped when using Discussion mode in a multipoint call with a DVI monitor set to 1280 x 720 resolution. | None |
| Monitors | VIDEO-58841 | 2.0 | When Dual Monitor Emulation is enabled, the composite video in multipoint calls with five or more sites is clipped on the left and right sides. | None |
| Monitors | VIDEO-82953 | 2.6 | The only supported display for the Polycom HDX 4000 system is the Polycom display. If a third party display is connected to the Polycom HDX 4000 system, the Polycom HDX 4000 system will turn off if already powered on, or will not power on if in a powered off state. | None. |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|-------------|------------------|---|--|
| Monitors | VIDEO-59578 | 2.0 | A Polycom HDX system provides the option to output black video or no signal when the system goes to sleep. Select the setting that works best for the system. Note that you may also need to adjust the monitor's configuration to achieve optimal results. For more information, refer to the <i>Administrator's Guide for Polycom HDX Systems</i> . | None |
| Monitors | VIDEO-60148 | 2.0 | If Monitor 1 is connected to the Polycom HDX system using a different format than what is configured in the user interface, you may get a blank screen. | Press and hold the Display button on the remote control, then select the appropriate format in the remote control window. Or change the monitor format using the web interface. |
| Monitors | VIDEO-77493 | 2.6 | If a VGA monitor is connected to a Polycom HDX 9004 system, a Polycom HDX 9001 system, or a Polycom HDX 9002 system, the U-Boot splash screen is tinted green. | None |
| Monitors | VIDEO-77493 | 2.6 | If a monitor does not support the timing mode selected by U-Boot for its splash screen, the video artifact will depend on the monitor. | None |
| Monitors | VIDEO-61097 | 2.0.1 | Video from some computers may be slightly clipped on the left side when viewed on a Polycom HDX 4000 series display. | None |
| Monitors | VIDEO-70791 | 2.5 | Some monitors may fail to correctly center video and user interface screens from a Polycom HDX system. If this occurs, use your monitor's horizontal adjustment feature to center the video. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|------------|-------------|------------------|--|---|
| Monitors | VIDEO-77975 | 2.5.0.7 | If a computer is connected to a Polycom HDX system, and the computer's monitor is configured to turn off after a period of inactivity, the monitor will automatically send content when the monitor wakes if Send Content When PC Connects is enabled. Send Content When PC Connects is enabled by default. | To avoid this issue, go to System > Admin Settings > Cameras > Camera Settings and disable Send Content When PC Connects . |
| Monitors | VIDEO-77717 | 2.5.0.7 | When a Polycom HDX system wakes up, Monitor 3 displays distorted video if: <ul style="list-style-type: none"> The VCR/DVD Record Source value for Monitor 3 is Monitor 2 Monitor 2 has the following settings: <ul style="list-style-type: none"> - Video Format: Component YPbPr - Resolution: 1080p - Output Upon Screen Saver Activation: No Signal | To work around this issue, change the monitor settings or turn Monitor 2 off and then on. |
| Monitors | VIDEO-84273 | 2.6.1 | If monitor resolution is set to 1920 x 1080, Elapsed time in call information overlaps a part of the Far Site Name when the far site name is in 15 double byte characters or more. | To prevent this problem, limit number of double-byte characters in the near end Site Name to 14 characters. |
| Multipoint | VIDEO-71679 | 2.5.0.1 | PAL Polycom HDX 8006 systems (HDX 8000 HD with Hardware Version B) do not support HD continuous presence in multipoint calls. | None |
| Multipoint | VIDEO-71756 | 2.5.0.4 | A multipoint H.331 broadcast mode call is not supported. | None |
| Multipoint | VIDEO-74435 | 2.5.0.4 | When a Polycom HDX system is hosting a multipoint call and is set to Auto Answer Multipoint Video and has a meeting password set, a Polycom CMAD or PVX system will not be able to join the call unless it is the first endpoint to connect to the Polycom HDX system. | Set Auto Answer Multipoint Video to No on the endpoint that is hosting the call. |

| Category | Issue ID | Found in Release | Description | Workaround |
|------------|-------------|------------------|---|--|
| Multipoint | VIDEO-75829 | 2.5.0.5 | If a system hosting a multipoint call is configured for a meeting password and the Auto Answer Multipoint Video setting is set to Yes , some meeting password prompts do not display. Specifically, when the second endpoint to call in dials into the web interface, the meeting password prompt is displayed on the second endpoint's local system interface but not on the web interface. | Do one of the following: <ul style="list-style-type: none"> • Before dialing, enter the meeting password in the Meeting Password field on the Place a Call screen in the web interface. • Enter the meeting password using the local system interface |
| Multipoint | VIDEO-76240 | 2.5.0.6 | Video from an iPower system is not visible when a Polycom HDX system is hosting a multipoint call. | Place a point-to-point call or have each endpoint call into a video bridge. |
| Multipoint | VIDEO-78352 | 2.6 | When a Polycom HDX system uses the Conference on Demand (COD) functionality, a seven-way call is the largest conference that will connect. | Use a Polycom RMX to host the multipoint call if more than seven participants is required. |
| Multipoint | VIDEO-76695 | 2.5.0.6 | Occasionally, a Polycom HDX 9004 system acting as a Multipoint Control Unit (MCU) crashes when sending content in the following scenario: <ul style="list-style-type: none"> • Eight endpoints are in the call • Transcoding is set to OFF • Monitor 1 has Far, Near, Content, and DME enabled • Monitor 2 is set to OFF • MCU is sending content at 10x7 • All three Picture-in-Picture windows are displayed on Monitor 1 | To work around this problem, turn off the DME or reduce the number of endpoints in the call to less than eight. |
| Multipoint | VIDEO-88455 | 2.7.0_J | Do not use the HDX system's internal multipoint feature with direct connect calls. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|--------------------|-------------|------------------|---|------------|
| Network | VIDEO-51811 | 1.0 | Starting a Polycom HDX system without a LAN connection and subsequently connecting the LAN may cause the LAN interface to fail to come up. If this occurs, restart the system with the LAN connected. | None |
| Network | VIDEO-66300 | 2.0.5_J | You must provide an 802.1 password when configuring a system for 802.1X authentication. If you do not provide a password, the system will not activate 802.1X. | None |
| Network | — | — | When you change the network interface attached to a Polycom HDX system from PRI to QBI, make sure to uncheck the box Calling Endpoint Uses the Original ISDN Number before disconnecting the PRI interface. To do this, go to System > Admin Settings > Network > ISDN . | None |
| People+ Content | VIDEO-69798 | 2.0.5_J | You cannot enable or disable H.239 while in a call. | None |
| People+ Content IP | | | People+Content IP is unavailable when your security profile is set to Maximum . | |
| People+ Content IP | VIDEO-75903 | 2.5.0.6 | During installation, InstallShield might display an incorrect version number for People+Content IP. | None |
| People on Content™ | VIDEO-65397 | 2.0.3 | When using Polycom People on Content on a Polycom HDX 4000 system, do not preview camera 2 before activating People on Content. | None |
| People on Content™ | VIDEO-79760 | 2.6 | People on Content displays video artifacts if the content source is not enabled. This issue does not happen when two active sources are enabled and People on Content is started. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|--------------------|----------------------------|------------------|---|-------------------------|
| People on Content™ | VIDEO-81147 | 2.5 | When sending content with People+Content IP, the content image is displayed with black bars on the side when the PC has been configured for a 16:9 aspect ratio. | Use a 4:3 aspect ratio. |
| People on Content™ | VIDEO-83803 | 2.6.1 | Occasionally, when a Polycom HDX system hosting a multipoint call has People On Content enabled, any Polycom HDX system in the multipoint call with two monitors will have content displayed on Monitor 2 momentarily and then the video will become frozen. | None |
| Power | VIDEO-72288 VIDEO-74189 | 2.5.0.4 | To avoid corrupting the file system, always power off a Polycom HDX system using the power button on the system or the remote control. After turning the power off in this way, wait at least 15 seconds before you disconnect the system from its power source. This helps ensure that the system powers off correctly. | None |
| Power | VIDEO-80751 | 2.6 | If a Polycom HDX system does not have an internal battery and is configured to use a time server, the Polycom HDX system will go to sleep shortly after restarting if idle. This is due to the Polycom HDX time being set to the year 1970 until successful connection to the time server. Once the connection to the time server is made, the screen saver wait time is exceeded and the Polycom HDX goes to sleep. This is normal behavior. | None |
| Power | VIDEO-80602 | 2.5.0.7 | Polycom HDX 4000 systems restart when the user changes the Country selection (while not in the setup wizard) from U.S. to Peru. This is normal behavior. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|--------------|-------------|------------------|---|---|
| Power | VIDEO-78532 | 2.5.0.6 | A Polycom HDX system will restart after approximately 10 minutes when a broadcast storm is created by having two Polycom HDX systems connect to a hub and a cable connecting two ports of the hub together. | Connect a Polycom HDX system to a switch or dedicated LAN port. |
| Power | VIDEO-78531 | 2.5.0.7 | When four Polycom HDX systems are connected to a LAN through the same 10M hub, a Polycom HDX system restarts if two Polycom HDX systems are in a 4M call with the other two Polycom HDX systems. | Use a switch or dedicated LAN port instead of a hub. |
| Presence | VIDEO-80195 | 2.6 | When a Polycom HDX system is configured to a directory server that supports presence (LDAP, Office Communications Server), presence status is not displayed when a directory search is performed. Presence will be displayed once the directory entry is added to Favorites. | None |
| Profiles | VIDEO-51310 | 1.0 | Profiles do not save Monitor 2 settings. | None |
| Profiles | VIDEO-54970 | 1.0.2 | If the profile you upload to a Polycom HDX system includes registration with multiple Global Management System servers, only the first server is registered after the system restarts. | Manually register with the other servers. |
| Provisioning | VIDEO-80708 | 2.5.0.7 | If a Polycom HDX system is configured by the Polycom CMA server to disable Security Mode , the user will be prompted with a log in when attempting to navigate to the Polycom HDX web interface. The log in window will reappear even if the user enters the log in information. | Close the web browser session and navigate to the Polycom HDX system's web interface. |

| Category | Issue ID | Found in Release | Description | Workaround |
|--------------|-------------|------------------|--|--|
| Provisioning | VIDEO-83273 | 2.6.1 | Occasionally, when a Polycom HDX system is being managed by Polycom CMA 5.0, the CMA CDR records for the Polycom HDX endpoint may not list all the calls the Polycom HDX system has placed. | Use the CDR file saved locally on the Polycom HDX system endpoint. |
| Provisioning | VIDEO-80756 | 2.5.0.1 | Polycom HDX systems cannot have the remote access password provisioned when being managed by Polycom CMA in traditional management mode. | Go the web interface and configure the remote access password manually. |
| Provisioning | VIDEO-80755 | 2.5.0.5 | Polycom HDX systems do not successfully register to the CMA provisioning server if the user name contains a dash. | Use a user name that does not contain a dash. |
| Provisioning | VIDEO-80754 | 2.5.0.5 | A HDX user will not be able to authenticate to the CMA server when going through the setup wizard if the user name is duplicated across multiple domains. | Use a unique user name. |
| Provisioning | VIDEO-75458 | 2.5.0.5 | If a Polycom HDX system is configured for provisioning from the Polycom CMA server, you will be unable to log in if Secure Mode in the Polycom CMA site provisioning profile is enabled. | Disable Secure Mode in the Polycom CMA site provisioning profile. Reconfigure the Polycom HDX system with the new profile settings. |
| Provisioning | VIDEO-80710 | 2.5.0.6 | When the Polycom CMA provisions the Polycom HDX system with a scheduled provisioned profile that includes the password for a Global Directory (GDS), the Polycom HDX system is updated with the password. However, the user interface screen will show that the password has been provisioned, but the web interface will not. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------------|-------------|------------------|--|--|
| Provisioning | VIDEO-80707 | 2.6 | The ISDN Gateway check box is not enabled or disabled on the Polycom HDX system when the Polycom CMA Administrator has pushed a scheduled provisioning profile that includes provisioning values on pages of the Polycom CMA scheduled provisioning pages other than the Video Network > IP Network > H.323 Settings page. | Provision the Polycom HDX system with values only on the Video Network > IP Network > H.323 Settings page or manually update the Polycom HDX system via the local system interface or web interface. |
| Provisioning | VIDEO-75459 | 2.5.0.5 | If a Polycom HDX system is configured for provisioning from the Polycom CMA server, you will be unable to log into the system if the following conditions are met: <ul style="list-style-type: none"> • Secure Mode in the Polycom CMA site provisioning profile is enabled • the DoD DSN Security Profile is configured | To work around this issue, delete the system settings by pressing and holding the restore button on the Polycom HDX system for 15 seconds while the Polycom HDX system powers on. Disable Secure Mode in the Polycom CMA site provisioning profile. |
| Provisioning | VIDEO-86491 | 2.6.1 | In some environments, the Recent Calls button might disappear from the HDX system's Home screen after CMA v5 configures a system using scheduled provisioning. | Use automatic provisioning and then configure the Home screen using the HDX system's web interface. |
| Remote Control | VIDEO-56317 | 2.0 | When the Display button is held down, the Polycom HDX remote control displays some video output formats that are not available for Polycom HDX 4000 and Polycom 8000 HDX systems. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------------|-------------|------------------|--|---|
| Remote Control | VIDEO-82739 | 2.6 | <p>A document will occasionally fail to print when an ISDN call is made and either endpoint performs an action with the remote control. This print failure will occur when two Polycom HDX systems have the following settings:</p> <ul style="list-style-type: none"> • PC and printer attached • serial port mode set to pass through • baud rate set to 115200 • flow control to None | Set the baud rate to 57600. |
| Remote Control | VIDEO-84364 | 2.6.1 | Occasionally, pressing a button on the remote control causes the cursor to move ahead two positions instead of one. | None |
| Sample Sites | — | — | Polycom provides sample numbers in the Polycom HDX directory, as well as video test numbers that you can use to test your Polycom HDX system. Please be aware that these numbers may occasionally be unavailable. | None |
| Security | VIDEO-93757 | | When a Polycom HDX system does not use an external active directory (AD) server for authentication, changes to the remote access Idle Session Timeout setting do not take effect. | If your HDX system does not use an external AD server, restart the system after changing the Idle Session Timeout setting. |
| Security | VIDEO-51330 | 1.0 | The Security page in both the local and web interface does not correctly report Telnet, SNMP, or Web connections. | None |
| Security | VIDEO-51954 | 1.0 | When Security Mode is enabled on a Polycom HDX system, attempting to enable or disable Telnet access from the Security page causes the system to restart. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|-------------|------------------|--|--|
| Security | VIDEO-52300 | 1.0 | Polycom HDX systems do not issue an SNMP alert for failed or successful attempts to log in via Telnet. | None |
| Security | VIDEO-61292 | 2.0 | When a Meeting Password is set on a Polycom HDX 8000 HD system and multiple sites call it and enter the password in rapid succession, the Polycom HDX 8000 HD system displays blue video. | Press Home then Near on the remote control. |
| Security | VIDEO-70377 | 2.5 | If your system is in Security Mode and you use the web interface, your browser may display warning messages stating that The security certificate for the web site "Polycom" cannot be verified. | Click Yes, I want to accept the certificate to continue normal operation. |
| Security | VIDEO-68750 | 2.5 | Do not set a meeting password if multipoint calls will include SIP endpoints. | None |
| Security | VIDEO-67094 | 2.0.5_J | If you attempt to configure an invalid User ID on a system (one that does not meet the system's security policy), you may get an error message that mentions the Admin ID rather than the User ID. | None |
| Security | VIDEO-67093 | 2.0.5_J | If you attempt to configure an invalid Admin ID on a system (one that does not meet the system's security policy), you may get the error message You must specify an Admin ID rather than one stating that the ID was invalid. | None |
| Security | VIDEO-71560 | 2.5.0.1 | When you change password creation policies, the changes apply to newly created/changed passwords but do not apply to the passwords that existed before the policy change. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|-------------|------------------|---|------------------------|
| Security | — | — | The user interface changes related to password management do not apply to Polycom HDX systems sold in Russia. | None |
| Security | VIDEO-76242 | 2.5.0.6 | In an encrypted point-to-point or multipoint SIP call, the local system interface displays the correct encryption status, but the web interface displays -- 9 . | None |
| Security | VIDEO-76708 | 2.5.0.6 | Polycom HDX systems may crash when Security Mode is enabled on the Polycom HDX system and the Polycom HDX system is in dynamic management mode. Security Mode is not supported when the Polycom HDX system is in dynamic management mode. | Disable Security Mode. |
| Security | VIDEO-52314 | 1.0 | When a Polycom HDX 9004 system is hosting a multipoint call with a meeting password set, other systems are allowed to call in and be heard and seen before entering the correct meeting password. They cannot hear or see the other participants until they enter the password. | None |
| Security | VIDEO-82737 | 2.6 | When the Polycom HDX system has Security Mode enabled, you cannot access the system via telnet port 23 or 24. However, the Security Settings screen will still show a green check mark next to Telnet: | None |
| Security | VIDEO-86932 | 2.7.0_J | Because Internet Explorer version 8 shares cookies between all active sessions, you might experience unexpected behavior when managing multiple machines within the same instance of Internet Explorer. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------|-------------|------------------|---|--|
| Security | VIDEO-85889 | 2.7.0_J | If you select the Maximum Security Profile during the setup wizard, any user account information you enter during the setup wizard is not valid after system restart. Active Directory authentication is enabled by default in the Maximum profile, which disables the local user account configured on the HDX system. | None |
| Security | VIDEO-84571 | 2.7.0_J | Polycom's Web UI does not enforce session timeouts if you connect using a Chrome browser. Also, if you log out of a Web UI session and subsequently navigate back to the Web UI, the Chrome browser will "remember" the previous login and will not require you to log in again. | None |
| Security | VIDEO-88401 | 2.7.0_J | When configuring the Maximum Security Profile during the setup wizard, ensure that Require Login for System Access is selected. | None |
| Security | VIDEO-88589 | 2.7.0_J | If you change the host name or domain name during the setup wizard, complete the setup wizard and reboot the system before generating Certificate Signing Requests. | None |
| Security | VIDEO-88706 | 2.7.0_J | When configuring the Maximum Security Profile during the setup wizard, ensure that mutual certificate authentication is selected on the Certificates page. | None |
| Security | VIDEO-88708 | 2.7.0_J | Immediately after installing a certificate revocation list on the Revocation page of the HDX system's web interface, the restart button on that page has no affect. | Navigate away from the page and then back to it to use the restart button. |

| Category | Issue ID | Found in Release | Description | Workaround |
|-----------------|-------------|------------------|---|---|
| Security | VIDEO-88709 | 2.7.0_J | If you have configured the HDX system with a security profile other than maximum and have required that users log in to access the system, non-administrative users will be unable to use the system if they attempt to access a page that requires administrator credentials. | If possible, enter the admin ID and password. |
| SIP | VIDEO-51333 | 1.0 | SIP conferences do not support a meeting password. | None |
| SIP | VIDEO-71148 | 2.5 | SIP calls across firewalls may fail to connect fully. If a Polycom HDX system restarts when attempting a SIP call across a firewall, disable H.239. | None |
| SNMP | VIDEO-60341 | 2.0 | The Main Camera Up trap is not sent when a Polycom HDX system starts up. | None |
| SNMP | VIDEO-76856 | 2.5.0.7 | Polycom HDX systems do not issue an SNMP alert for excessive Jitter or Latency in a call. | None |
| Software Update | VIDEO-51312 | 1.0 | Polycom HDX systems do not time out in software update mode if they are waiting for user response. | None |
| Software Update | VIDEO-65480 | 2.0.3 | The Polycom HDX system retains its directory entries after you use the hardware restore button to restore the system's configuration to its default values. | None |
| Software Update | VIDEO-65263 | 2.0.2 | You may observe black video when performing software update on a Polycom HDX 9000 system configured for DVI 1280 x 720 50 Hz. Allow the software update to complete normally. Do not power off the system during the software update process. If the upgrade is interrupted, the system could become unusable. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|-----------------|-------------|------------------|---|---|
| Software Update | VIDEO-51950 | 1.0 | When running a software update, you may see video artifacts on secondary monitors. The primary monitor will display the Software Update status screen. | None |
| Software Update | VIDEO-52368 | 1.0 | Use the local user interface or web interface to change monitor settings rather than the configuration screens provided with Software Update. | None |
| Software Update | VIDEO-53198 | 1.0 | When updating a Polycom HDX system that is behind a Linksys router, the update stalls unless the computer you are using to run the update is configured as host on the network. | None |
| Software Update | VIDEO-60253 | 2.0 | When updating a Polycom HDX system using the USB port, the root of the USB stick should have a single .pup file and single .txt file. | None |
| Software Update | VIDEO-60317 | 2.0 | If the Software Update page does not load after a few seconds, click the browser's Refresh button. | None |
| Software Update | VIDEO-60301 | 2.0 | While a software update is in progress, additional browser sessions that attempt to connect to the system may fail to do so, even though the update is proceeding normally. | None |
| Software Update | VIDEO-60655 | 2.0 | Disable security mode before downgrading the system software from 2.0 to 1.0.x. | None |
| Software Update | VIDEO-78889 | 2.6 | Occasionally, when upgrading from software version 2.0.3.1 to 2.6, the Polycom HDX system hangs at the hour glass screen. | Restart the Polycom HDX system and perform the upgrade again. |

| Category | Issue ID | Found in Release | Description | Workaround |
|-----------------|-------------|------------------|---|---|
| Software Update | VIDEO-67352 | 2.5 | Polycom HDX 7000 series or Polycom HDX 8000 series systems customers in a PAL environment will switch to Component monitor output after a Software Update is run with Erase System Flash Memory selected. After the update, hold down the remote control Display button and change the monitor output type. | None |
| Software Update | VIDEO-71246 | 2.5 | Downgrading Polycom HDX software from version 2.5 (or later) to 2.0.x (or earlier) erases the system's local directory and CDR file. | To preserve this information, use the system's web interface to download it to your computer before the update. |
| Software Update | VIDEO-72148 | 2.5.0.2 | If the Polycom HDX 4000 series monitor cables are not properly connected, Software Update displays an error message and stops the update. | Connect the monitor cables and retry the Software Update. |
| Software Update | VIDEO-72721 | 2.5.0.2 | Polycom HDX 9000 series systems occasionally display a shifted or split progress screen during a software update. Allow the software update to complete normally. Do not power off the system during the software upgrade process. If the upgrade is interrupted, the system could become unusable. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|-----------------|-------------|------------------|--|---|
| Software Update | VIDEO-75808 | 2.5.0.6 | <p>If you perform a software update on a Polycom HDX system using Microsoft Internet Explorer 8.0, you cannot type in some text fields. Instead, you must use the Browse button. This limitation applies to the following fields:</p> <ul style="list-style-type: none"> • Utilities > Profile Center > Retrieve Settings • Utilities > Import/Export Directory > PC->HDX 7000 HD (Polycom HDX series number will vary based on your system) • Utilities > Screen Saver > Next > Screen Saver Image | None |
| Software Update | VIDEO-76323 | 2.5.0.6 | <p>If you select a static IP address in the setup wizard, the following message appears: loadXMLDoc: Something is wrong "Access is denied."</p> | <p>To regain access to the software update in the web interface, click OK on the message and then type the new IP address into the Address field of the web browser.</p> |
| Software Update | VIDEO-83958 | 2.6.1 | <p>When downgrading from version 2.6.1, downgrade first to version 2.6.0.1, then to the desired software release.</p> <p>When using the Software Update feature to downgrade from version 2.6.1 to a version between 2.5.0.4 and 2.6 (inclusively), a failure might occur. This failure can be identified by the failed to update gennum flash message displayed on the HDX web interface. If this message displays during a downgrade, repeat the downgrade to successfully update the system.</p> <p>The first repetition of the software update might not be sufficient to correct the problem. Repeat the process several times until it completes successfully.</p> | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|-----------------|-------------|------------------|--|---|
| Software Update | VIDEO-88036 | 2.7.0_J | The Software Update feature might occasionally fail to upload an update package successfully. | Refresh the browser page. When the option to select an update package appears, reselect the update package. |
| Software Update | VIDEO-86401 | 2.7.0_J | Polycom GMS, Polycom <i>ReadiManager</i> SE-200, and Polycom CMA using scheduled provisioning cannot manage HDX systems that have session lists enabled. | Disable session lists on the HDX system's security settings. |
| Software Update | VIDEO-88037 | 2.7.0_J | If you upgrade the HDX software by using a USB stick while you are logged in to the HDX system through the web interface, you might still see pages from the older version of HDX software after the upgrade. | Refresh the browser. |
| Transcoding | VIDEO-61407 | 2.0.1 | Due to the increased functionality of the Polycom HDX multipoint software, transcoding is now enabled by default. | None |
| Transcoding | VIDEO-81287 | 2.6 | If a Polycom HDX system hosting a multipoint call has been configured to display content on Monitor 2, content will be displayed on Monitor 1 if a far-end system sends content under the following circumstances: <ul style="list-style-type: none"> • Transcoding is set to OFF • a multipoint mixed call (IP, ISDN, SIP) is placed • downspeeding occurs | Enable Transcoding. |
| User Interface | VIDEO-54356 | 1.0.2 | When the trace route diagnostic screen lists more than one line in the results, use the Back button on the remote control to exit the screen. | None |
| User Interface | VIDEO-65396 | 2.0.3 | The first character of a system name should be either a letter or a digit. System names can't start with the \$ or the _ characters. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------------|---|----------------------|--|--|
| User Interface | VIDEO-64776 | 2.0.3 | Camera icons and names may be improperly transferred to the far end system. | None |
| User Interface | VIDEO-55049 | 1.0.2 | No warning appears in the user interface when changing the settings for content display in the web interface. | None |
| User Interface | VIDEO-60004 | 2.0 | On the Call Statistics screen, the video rate used may appear to exceed the negotiated video rate. This is a statistics issue only and does not reflect what is actually happening on the network. | None |
| User Interface | VIDEO-58845 | 2.0 | If a Polycom HDX 4000 series system, a Polycom HDX 7000 series system, or a Polycom HDX 8000 HD system with Hardware Version A is not configured to use a time server, the time must be set manually whenever the system restarts. | None |
| User Interface | VIDEO-61209 | 2.0 | It may take several minutes for the LAN status indicator to update after the LAN has been reactivated. | None |
| User Interface | VIDEO-61293 VIDEO-65440 VIDEO-63086 | 2.0.1, 2.0, 2.0.2 | The user interface could redraw improperly after repeated changes to the configuration of Monitor 1. | Navigate to another user interface screen, then return to the original screen. If this does not resolve the issue, restart the system. |
| User Interface | VIDEO-62867 | 2.0.0_J | When a system is configured for Basic Mode , it does not report far-site information correctly. | None |
| User Interface | VIDEO-81342 | 2.5.0.5 | On page 3 of the Security Settings screens you cannot place the yellow cursor on Allow Video Display on Web when navigating from the top to the bottom and moving downward. | To work around this issue, place the cursor at the bottom of the screen and scroll up. |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------------|-------------|------------------|--|---|
| User Interface | VIDEO-81340 | 2.5.0.5 | On the Country screen of the setup wizard, you cannot use the Down arrow key on the remote control to access the Country drop down box. | To work around this issue, use the Up arrow key on the remote control or complete the setup wizard using the web interface. |
| User Interface | VIDEO-82741 | 2.5.0.6 | Setting the Time Server to Auto sets ntp.polycom.com as the time server. | To manually set the HDX system to a different time server, set Time Server to Manual . |
| User Interface | VIDEO-81300 | 2.5.0.5 | If a Polycom HDX system is connected to a LAN port with EAP enabled, but EAP is not enabled on the Polycom HDX system, the Polycom HDX system will report IP network connectivity is up (indicated by a green arrow) when it should show IP connectivity is down (indicated by a red arrow). | Enable EAP/802.1X on the LAN Properties page or move the Polycom HDX system to a LAN port that does not have EAP enabled. |
| User Interface | VIDEO-81297 | 2.6 | When in a call, pressing the Camera button on the remote control and selecting Camera 1 (assuming it is already selected) changes the view from far video to near video or vice versa. However, the Camera 1 icon displayed will be the default or configured camera icon and not the icon that indicates that the video can be switched between near and far. | None |
| User Interface | VIDEO-69792 | 2.5 | The statistics for receive content show the maximum that might be received rather than the rate currently being received. | None |
| User Interface | VIDEO-69620 | 2.5 | When you add Polycom HDX microphones one at a time, the Diagnostics screen may list the version of the first microphone as None. If multiple microphones are connected and you restart the system, they are all correctly displayed. | None |
| User Interface | VIDEO-65940 | 2.0.5_J | Selecting the space bar in the onscreen keyboard toggles between upper-case and lower-case letters. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|----------------|-------------|------------------|---|------------|
| User Interface | VIDEO-70650 | 2.5 | Do not add more than six entries to the Speed Dial or Sites list displayed on the Place a Call screen. | None |
| User Interface | VIDEO-80600 | 2.5.0.7 | Polycom HDX 6000, 7000, and 8000 systems do not show the IPv6 addresses on the System Information screen when connected to an IPv6 network. This information is displayed in the web user interface under Diagnostics > System Information . | None |
| User Interface | VIDEO-80412 | 2.5.0.5 | The Polycom HDX system displays an IP address of 0.0.0.0 on the LAN Properties screen when the LAN cable is disconnected, even if a static IP address was configured on the Polycom HDX system. | None |
| User Interface | VIDEO-64776 | 2.0.3 | Camera icons and names can be improperly transferred to the far end system. | None |
| User Interface | VIDEO-72275 | 2.5.0.1 | Pagination of the alert System Status screens indicates that three screens exist. However, only the first two pages are accessible. The third page does not display. | None |
| Video | VIDEO-80580 | 2.6 | Occasionally, when a 6M point-to-point SIP call is made between two Polycom HDX systems, the called endpoint displays green video at the bottom of the screen for a couple of seconds when the call initially connects, then displays normal video. | None |
| Video | VIDEO-80196 | 2.5.0.7 | Blue video is displayed for approximately four seconds when the Polycom HDX camera wakes up after being asleep due to the screen saver wait time. The Polycom HDX is operating normally and near video is displayed after the brief moment of blue video. | None |

| Category | Issue ID | Found in Release | Description | Workaround |
|---------------|-------------|------------------|---|---|
| Video | VIDEO-85838 | 2.7.0_J | Making rapid changes to the selected video source by using API commands might cause the HDX system to display frozen video from one of the sources. To prevent this situation from occurring, allow sufficient time between API commands. | Restart the HDX system. |
| Video | VIDEO-87018 | 2.7.0_J | You might occasionally notice brief video artifacts when cycling through layouts when using dual monitor emulation. The system will automatically correct these within a couple of seconds. | None |
| Video | VIDEO-85839 | 2.7.0_J | If you use a computer as a People video source, the video on your HDX system might be slightly clipped. | None |
| Web Interface | VIDEO-80675 | 2.6 | A Polycom HDX system with a BRI card installed and configured for NI-1/NI-2 Switch Protocol does not have the Auto BRI Configuration option in the web interface. The local system interface does have the Auto BRI Configuration option. | None |
| Web Interface | VIDEO-80674 | 2.6 | When a Polycom HDX system is configured to automatically answer point-to-point video calls, the web interface does not display a message for an incoming POTS or ISDN voice call for the user to answer the call. The message asking you to accept the call is displayed on the local system interface. | Set Auto Answer Video calls to No . The pop-up message will then be displayed on the web interface. |
| Web Interface | VIDEO-80605 | 2.6 | In the web interface, Ctrl+Z does not delete text entered into a text field. | Use the Delete key to delete text from a text field. |

| Category | Issue ID | Found in Release | Description | Workaround |
|---------------|-------------|------------------|--|--|
| Web Interface | VIDEO-80194 | 2.6 | The web interface does not display the hardware version for revision A of the Polycom HDX 7000 and 8000 products under Tools > System Information . Hardware Version A is displayed on the System Information screen in the local system interface. The web Interface does display the hardware version for later hardware versions. | None |
| Web Interface | VIDEO-80603 | 2.5.0.4 | Searching the Directory via the web user interface takes up to 45 seconds to retrieve entries if Directory searches are happening on more than 4 simultaneous web interface sessions. | Ensure that only one user at a time performs a directory search. |
| Web Interface | VIDEO-80106 | 2.6 | Polycom HDX systems generate an SNMP alert for each web interface request. | None |
| Web Interface | VIDEO-80092 | 2.6 | Occasionally, when configuring the Calendaring Service from the web interface, the green registration check mark is not displayed after selecting the Update page. | Refresh the browser page or configure the Calendaring Service from the local system interface. |
| Web Interface | VIDEO-80074 | 2.5.0.5 | Polycom HDX systems with a V.35 card installed do not issue an SNMP alert when H.320 is enabled or disabled via the web interface. | None |
| Web Interface | VIDEO-80073 | 2.5.0.5 | Polycom HDX systems with a PRI card installed do not issue an SNMP alert when H.320 is enabled or disabled via the web interface. | None |
| Web Interface | VIDEO-79759 | 2.6 | Directory group names do not display correctly in the web interface when using Internet Explorer 7 with either Simplified Chinese, Traditional Chinese, or Korean languages. | Use Internet Explorer 6 or Internet Explorer 8. |

| Category | Issue ID | Found in Release | Description | Workaround |
|---------------|-------------|------------------|---|------------|
| Web Interface | VIDEO-77721 | 2.5.0.6 | After performing a system reset on a Polycom HDX 9004 or Polycom HDX 6000, the Wake System button on the Camera Settings web interface page might be missing when the system goes to sleep for the first time. The Wake System button is displayed on the web interface after the system is awakened by the remote control. | None |
| Web Interface | VIDEO-84031 | 2.6.1 | The Admin Settings > Network > IP Network > H.323 Settings > Current IP Address field in the web interface appears to be editable, but it is not. | None |

Software Requirements

To use the web interface, you need Microsoft Internet Explorer 6.x, 7.x., or 8.x.

Interoperability

The following PTZ cameras are supported for use with Polycom HDX systems:

- Polycom EagleEye View (requires HDX software 2.6 or later)
- Polycom EagleEye HD
- Polycom EagleEye 1080 (requires HDX software 2.5 or later)
- Polycom EagleEye II (requires HDX software 2.6.1 or later)
- Polycom PowerCam™ Plus (SD camera)
- Polycom PowerCam (SD camera))
- Sony EVI-D30/31 (SD camera)
- Sony EVI-D70 / Vaddio WallVIEW 70 (SD camera)
- Sony EVI-D100 / Vaddio WallVIEW 100 (SD camera)
- Sony BRC-300 / Vaddio WallVIEW 300 (SD camera)
- Elmo PTC-100S/110R/150S/160R (SD camera)

- Canon VC-C50i/Vaddio WallVIEW 50i (SD camera)
- Sony BRC-H700
- Sony EVI-HD1

The following keyboards have been qualified for use with HDX systems:



Polycom implemented USB keyboard support only to help you enter complex login information such as user IDs and passwords when you use the HDX system. You could see unexpected results if you use the keyboard for other system operations.

- Dell SK-3106 (with CAC reader)
- SIIG AXR1020X
- Gear Head KB2500U (some older versions of this keyboard might not work with the HDX system)
- Sanrio MID#0010510
- Lenovo SK-8825 (L)
- Dell SK-8135
- Dynex wired keyboard -Model DX-WKBD
- Lenovo wired- Model SK-8815

Polycom HDX systems are tested extensively with a wide range of products. The following list is not a complete inventory of compatible equipment. It simply indicates the products that have been tested for compatibility with this release.

Video conferencing systems use a variety of algorithms to compress audio and video. In a call between two systems, each end transmits audio and video using algorithms supported by the other end. In some cases, a system may transmit a different algorithm than it receives. This process occurs because each system independently selects the optimum algorithms for a particular call, and different products may make different selections. This process should not affect the quality of the call.

| Product | Version |
|------------------------------------|---------|
| Polycom HDX Series systems | 2.7.1_J |
| Polycom CMA 5000 | 5.2.0J |
| Polycom RMX 1500/RMX 2000/RMX 4000 | 7.5.1.J |
| Polycom DMA 7000 | 2.1.1J |
| Polycom PathNavigator | 7.0.14 |
| Cisco VCS | X6.1 |
| TANDBERG MXP Family | F7.3.1 |
| TANDBERG C-Series | TC3.5.0 |

| Product | Version |
|-------------------|---|
| LifeSize VTC Room | SW Rel. 4.2.10(5) and Networker with SW Rel. 3.1.1(4) |
| LifeSize Express | SW Rel. 4.7.9(2) and Networker with SW Rel. 3.1.1(4) |

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)."

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS

OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Copyright Information

© 2011 Polycom, Inc. All rights reserved.

Polycom, Inc.
4750 Willow Road
Pleasanton, CA 94588-2708
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Trademark Information

Polycom®, the Polycom “Triangles” logo, and the names and marks associated with Polycom’s products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

Patent Information

The accompanying products may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.