



This software has not achieved UC APL certification.

This document provides the latest information for security-conscious users running version 3.0.3 software. The information in this document is not intended to imply that DoD or DISA certifies Polycom HDX systems.

The Polycom HDX software uses OpenSSL FIPS Object Module (Software Version: 1.2.2). This usage provides FIPS-140-approved cryptography for systems.

## Upgrading and Deploying your Polycom HDX System

When you upgrade your Polycom HDX system to version 3.0.3, the factory partition might also be automatically upgraded if it contains certain previous versions with known issues that have been corrected. Then, if you later perform a factory restore, the system returns to version 3.0.3 instead of to the software version originally installed on the system.

After you install version 3.0.3, downgrading to an earlier software version is not recommended. However, if you must install a previous software version, contact Polycom support at [www.polycom.com/support](http://www.polycom.com/support).



To mitigate certain network-based attacks, Polycom recommends that the network administrator configure port security on the switch to which Polycom devices connect. Security is enhanced by binding the device's MAC address to a specific physical port on the switch.

Refer to the *Administrator's Guide for Polycom HDX Systems* for information about configuration settings that are not included in this guide including the other Security Profile settings.

## Upgrading the Software in a Non-DHCP Environment

In the LAN properties screen, choose **Enter IP Address Manually** and continue through the next screens to finish configuring the LAN properties.

If you need to configure the system to use certificates or to customize other settings, you must access the HDX system's web interface using a computer located on the same network segment as the HDX system.

## Configuring Security Settings in a Web Browser

You can configure some of the security settings on the local HDX screens. For other security settings, however, you must use the HDX web interface.



When making a connection from a web browser to configure the HDX system, always enter the address of the 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. This includes those credentials 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.

## Using the Maximum Security Profile

The Maximum Security Profile lets you control particular fields in order to meet the highest security requirements (for example, systems used in government or military environments). The Security Profile can only be set in the setup wizard. You can run the setup wizard:

- At initial setup
- When you select **Erase System Flash Memory** during a system update
- After a system reset when system settings are deleted

After the setup wizard is complete, the Security Profile setting appears as read-only in the Admin Settings.

### To configure the Security Profile to Maximum:

- >> In the setup wizard, enable **Security Mode** and set **Security Profile** to **Maximum**.

When you choose this setting, the system automatically sets certain fields to predefined values. After you set the Security Profile to Maximum in the setup wizard, some fields are restricted or not configurable. The fields controlled by the profile are set to predefined values and may have additional restrictions applied as described in the following tables.

## Setup Wizard

Setting	Restriction
Room Password	Must be changed.
Admin ID	Must be changed.
User ID	Must be changed.
User Room Password	Must be entered.
Admin Room Password	Must be changed.
Admin Remote Password	Must be changed.

## Security Settings

Setting	Restriction
Security Profile	Set to <b>Maximum</b> , not configurable.
Security Mode	Enabled, not configurable.
Use Room Password for Remote Access	Disabled, not configurable.
Remote Admin Access (web)	Enabled, configurable.
Require Login for System Access	Enabled, not configurable.
Enable Remote Access: <ul style="list-style-type: none"> <li>• Web</li> <li>• Telnet</li> <li>• SNMP</li> </ul>	These are the restrictions: <ul style="list-style-type: none"> <li>• Enabled, configurable.</li> <li>• Disabled, not configurable.</li> <li>• Disabled, not configurable.</li> </ul>
AES Encryption	Set to <b>Required for Video Calls Only</b> , configurable.
Web Access Port	Set to <b>443</b> , not configurable.
Allow Video Display on Web	Disabled, not configurable.
Connect to my LAN	Set to <b>On</b> , configurable.
Allow Access to User Settings	Set to <b>Off</b> , configurable.

Setting	Restriction
NTLM Version	Set to <b>Auto</b> , configurable.
Enable Sessions List	Set to <b>On</b> , not configurable.
Enable Security Banner	Set to <b>DoD</b> , Off is not allowed. The Custom setting allows you to create your own banner wording, which must contain text.

## Password Settings for Room, Remote Access, and User Passwords

Setting	Restriction
Minimum Length	<ul style="list-style-type: none"> <li>Remote (Admin only): Set to <b>15</b>; range is 8 to 15.</li> <li>Room (User/Admin): Set to <b>9</b>; range is 6 to 20.</li> </ul>
Can Contain ID or Its Reverse Form	Disabled, not configurable.
Require Lowercase Letters	Set to <b>Off</b> , configurable.
Require Uppercase Letters	Set to <b>Off</b> , configurable.
Require Numbers	Set to <b>Off</b> , configurable.
Require Special Characters	<ul style="list-style-type: none"> <li>Remote (Admin only): Set to <b>1</b>; range is 1 to 2.</li> <li>Room (User/Admin): Set to <b>Off</b>; range is 1 to 2.</li> </ul>
Reject Previous Passwords	Set to <b>10</b> ; range is 8 to 16.
Minimum Password Age in Days	Set to <b>Off</b> ; range is 1 to 30.
Maximum Password Age in Days	Set to <b>60</b> ; range is 30 to 180.
Password Expiration Warning in Days	Set to <b>7</b> , Off is not allowed, range is 1 to 7.
Minimum Changed Characters	Set to <b>4</b> , range is 1 to 4.
Maximum Consecutive Repeated Characters	Set to <b>2</b> , range is 1 to 4.

## Meeting Password Settings

Setting	Restriction
Minimum Length	Set to <b>Off</b> , range is 6 to 20.
Require Lower Case Letters	Set to <b>Off</b> , configurable.
Require Upper Case Letters	Set to <b>Off</b> , configurable.
Require Numbers	Set to <b>Off</b> , configurable.
Require Special Characters	Set to <b>Off</b> , configurable.
Reject Previous Passwords	Set to <b>10</b> ; range is 8 to 16.
Minimum Password Age in Days	Set to <b>Off</b> , configurable.
Maximum Password Age in Days	Set to <b>60</b> , range is 30 to 180.
Password Expiration Warning in Days	Set to <b>7</b> , Off is not allowed, range is 1 to 7.
Minimum Changed Characters	Set to <b>Off</b> , range is 1 to 4.
Maximum Consecutive Repeated Characters	Set to <b>2</b> , range is 1 to 4.

## Account Management

Setting	Restriction
Admin: <ul style="list-style-type: none"><li>Lock Account after Failed Logins</li><li>Account Lock Duration in Minutes</li></ul>	Set to <b>3</b> , Off is not allowed. Set to <b>1</b> , configurable.
User: <ul style="list-style-type: none"><li>Lock Account after Failed Logins</li><li>Account Lock Duration in Minutes</li></ul>	Set to <b>3</b> , Off is not allowed. Set to <b>1</b> , configurable.

## Certificates, Revocation, and Whitelist

These settings can only be configured through the HDX web interface.

Setting	Restriction
Maximum Peer Certificate Chain Depth	Set to <b>2</b> , configurable.
Always Validate Peer Certificates from Browsers	Enabled, not configurable.
Always Validate Peer Certificates from Servers	Enabled, not configurable.
Revocation Method	Configurable.
Allow Incomplete Revocation Checks	Disabled, configurable.
Whitelist	Enabled, not configurable.

## Remote Access Settings

These settings apply to remote access through the RS-232 serial port and the HDX web interface. Both are considered to be access ports. The RS-232 interface is a physical port, and the HDX web interface is a virtual port.



Only someone logged onto the system as an admin can configure remote access on a system that is using the Maximum Security Profile.

Setting	Restriction
Idle Session Timeout in Minutes	Set to <b>10</b> , configurable. Off is not allowed.
Maximum Number of Active Web Sessions	Set to <b>25</b> , range is 10 to 50.
Maximum Number of Sessions per User	Set to <b>3</b> , range is 1 to 5.
Lock Port after Failed Logins	Set to <b>3</b> , configurable. Off is not allowed.
Port Lock Duration in Minutes	Set to <b>1</b> , configurable. Off is not allowed.

You can configure the period of time, in hours, in which the failed login threshold must be exceeded to lock the user's account. This command can only be changed through the command-line interface using the serial API:

`loginwindowduration`: Set to **1**, range is 1 to 24. Off is not allowed.

## External Authentication

Setting	Restriction
Enable Active Directory Authentication	Enabled, configurable.

## Home Screen and Other Settings

Setting	Restriction
Idle Session Timeout in Minutes	Set to <b>10</b> , configurable. Off is not allowed.
Lock Port after Failed Logins	Set to <b>3</b> , configurable. Off is not allowed.
Port Lock Duration in Minutes	Set to <b>1</b> , configurable. Off is not allowed.

Setting	Restriction
Serial Ports: RS-232 Mode	Set to <b>Off</b> , configurable (only Control is allowed).
SIP Transport Protocol	SIP not available.
Directory Servers	Only LDAP available.
Auto Answer Point-to-Point Video	Disabled, configurable.
Auto Answer Multipoint Video	Disabled, configurable.
Availability Control	Enabled, not configurable.
Recent Calls	Disabled, not configurable.
Last Number Dialed	Disabled, not configurable.
Far Control of Near Camera	Disabled, configurable.
Call Detail Report	Enabled, not configurable.
Exchange Calendaring	Disabled, not configurable.

## Locating Your System

The system should be placed in a secured location and on a firewall-protected network segment.

## Configuring Your Local System

This section describes how to manually configure system settings to meet the maximum security requirements.

### To configure your system for deployment in a maximum security environment:

- 1 Download and install the Polycom HDX software update. For information about installing the software, refer to the release notes for your software version.
- 2 When prompted in the setup wizard:
  - Enable Security Mode.
  - Set the Security Profile to **Maximum**.
  - Set Admin ID to a value other than **admin**.
  - Set a Room Password, a Remote Access Password, and a User Password that meet the default password policy as described in [Password Settings for Room, Remote Access, and User Passwords](#) on page 4.


You can modify the password policies after you complete the setup wizard. Refer to [Configuring Your Room and User Password Policy](#) on page 12 for more information about doing this.
  - Change the **User ID** to something other than **user**.
- 3 After you complete the setup wizard and the system restarts, log into the system using the new Admin ID and Room Password that you set.
- 4 Go to **System > Admin Settings > General Settings > Security > External Authentication** to configure the Active Directory Server (ADS) settings.
- 5 Go to **System > Admin Settings > General Settings > Security > Security Settings**.



Note that any user account information entered during the setup wizard is not valid after system restart. ADS is enabled by default in Maximum Security mode, which disables the local user account.

**6** Go to **System > Admin Settings > General Settings > Security > Security Settings** >  >  and configure the following settings.

Setting	Description
AES Encryption	Specifies whether to encrypt calls with other sites. <ul style="list-style-type: none"> <li>• Off — AES Encryption is disabled.</li> <li>• When Available — Allows calls with all endpoints, including sites that may not support encryption.</li> <li>• Default: Required for Video Calls Only — Allows video calls only with sites that support encryption. ISDN voice and analog phone calls are allowed.</li> <li>• Required for All Calls — Allows video calls only with sites that support encryption. ISDN voice and analog phone calls are not allowed.</li> </ul>
Allow Access to User Settings	Specifies whether the User Setting screen is accessible to users through the System screen. <ul style="list-style-type: none"> <li>• Enable this setting if meeting passwords are required to join multipoint calls.</li> <li>• Disable this setting if meeting passwords are not required for multipoint calls.</li> </ul>

**7** Configure the system for time and date management using the steps appropriate for your particular Polycom HDX model and deployment type.

Deployment Type	Configuration Steps
IDSN-only Deployments Polycom HDX 9000 Polycom HDX 9006 Polycom HDX 8000 Hardware Version B Polycom HDX 7000 Hardware Version B or later Polycom HDX 6000	Go to <b>System &gt; Admin Settings &gt; General Settings &gt; Location</b> >  , and set Time Server to <b>Off</b> and manually configure the time and date.

Deployment Type	Configuration Steps
IP Deployments Polycom HDX 9000 Polycom HDX 9006 Polycom HDX 8000 Hardware Version B Polycom HDX 7000 Hardware Version B or later Polycom HDX 6000 Polycom HDX 4000 Hardware Version C	Go to <b>System &gt; Admin Settings &gt; General Settings &gt; Location &gt;</b>  , and do one of the following: <ul style="list-style-type: none"> <li>• Set Time Server to <b>Off</b> and manually configure the time and date.</li> <li>• Set Time Server to <b>Auto</b>.</li> <li>• Set Time Server to <b>Manual</b>:                             <ul style="list-style-type: none"> <li>- Enter the NTP server address for the Primary Time Server.</li> <li>- Enter the NTP server address for the Secondary Time Server.</li> </ul> </li> </ul>
IP Deployments Polycom HDX 8000 Hardware Version A Polycom HDX 7000 Hardware Version A Polycom HDX 4000	Go to <b>System &gt; Admin Settings &gt; General Settings &gt; Location &gt;</b>  , and do one of the following: <ul style="list-style-type: none"> <li>• Set Time Server to <b>Auto</b>.</li> <li>• Set Time Server to <b>Manual</b> with NTP server address specified.                             <ul style="list-style-type: none"> <li>- Enter the NTP server address for the Primary Time Server.</li> <li>- Enter the NTP server address for the Secondary Time Server.</li> </ul> </li> </ul>



All Polycom HDX 4000 systems with Hardware Version A and B, and Polycom 7000 and 8000 systems with Hardware Version A require a connection to an NTP server to keep accurate time across power outages and system restarts.



Polycom HDX 6000 and 9000 series systems, Polycom HDX 7000 and 8000 systems with Hardware Version B or later, and Polycom HDX 4000 systems with Hardware Version C have an internal battery-backed real-time clock that allows them to keep accurate time across power outages and system restarts.

To verify your hardware version:

- For HDX 8000 and 7000 HD systems, you can verify the hardware version by going to **System > System Information**. If no hardware version is designated, your system has Hardware Version A.
- For HDX 7000 systems, the part number indicates the hardware revision. You can find the part number on the back of the unit.

Hardware Version A part numbers: 2201-27285-XXX and 2215-27427-XXX

Hardware Version B part numbers: 2201-28629-XXX and 2215-28632-XXX

- 8 On Polycom HDX 4000, 7000, and 8000 series systems, go to **System > Admin Settings > LAN Properties >**  **>** , and disable the **Enable PC LAN Port** setting, unless its use is required. If you change this setting, the system restarts.
- 9 Go to **System > Admin Settings > Network > Call Preference**, and configure the following settings on the Call Preference screen.

Setting	Description
IP H.323	<ul style="list-style-type: none"><li>• Disable this setting for ISDN-only deployments.</li><li>• Enable this setting if H.323 calling on IP networks is required.</li></ul>
SIP	SIP is disabled and not configurable in Maximum Security mode.
ISDN H.320	<ul style="list-style-type: none"><li>• Disable this setting for IP-only deployments.</li><li>• Enable this setting if ISDN H.320 calling is required.</li></ul>

**10** Go to **System > Admin Settings > General Settings > Security > Log Management**, and set this setting on the Log Management screen.




Setting	Description
Percent Filled Threshold	Specifies the percent filled level, which triggers a system alert. Suggested value: 70.

## Configuring Your System for Remote Access

This section describes how to configure the system to meet the maximum security requirements for remote access through the RS-232 serial port or through the HDX web interface.

When you configure the system to use the Maximum Security Profile, the system:

- Requires devices that are attempting to start a session through the serial port to provide either an Admin ID and password or a User ID and password. If you are connecting interactively using a terminal emulator program, press Enter to display a login prompt. If you are connecting by using a serial control application, send a new line character to display a login prompt.
- Requires you to set separate remote access passwords for both the User and Admin accounts. The **Use the Room Password for Remote Access** setting is automatically disabled in the Maximum Security Profile and is not configurable. You configure the remote access password initially during the setup wizard, and you can make changes later using the Admin Settings screens.
- Makes available different API commands depending on whether you log in with the Admin account or with the User account.

- Locks the serial port after a specified number of failed login attempts. The port lockout causes the HDX system to refuse further log-in attempts for a period of time, which you can configure. Each serial port has its own separate port lockout.
- Displays a Security Banner with the serial port login. You cannot set the Security Banner to Off. To configure the Security Banner, go to **System > Admin Settings > General Settings > Security > Security Settings > >**   and set a Security Banner to either Custom or DoD. 
- Automatically terminates idle sessions (a configurable setting).


## Configuring Your Room and User Password Policy

Though passwords defined as being strong are recommended for security purposes, keep in mind that strong passwords require the use of the onscreen virtual keyboard to enter letters and special characters. This requirement can make it possible for others to view a password as you enter it. You can mitigate this risk by using longer numeric-only passwords that you can enter using the remote control. This section gives the recommended settings for both configurations.

### To configure your room password policy:

- 1 Go to **System > Admin Settings > General Settings > Security > Password Settings > Admin Room Password**, and configure the following settings.

Setting	Strong Passwords	Numeric-only Passwords
Minimum Length	Value: 15 (recommended)	Value: 15
Can Contain ID or Its Reverse Form	Disable	Disable
Require Lowercase Letters	Value: 1	Off
Require Uppercase Letters	Value: 1	Off
Require Numbers	Value: 1	All
Require Special Characters	Value: 1	Off

- 2 Select  and configure the following settings.

Setting	Description
Reject Previous Passwords	Value: 10
Minimum Password Age in Days	Value: 1 or Off
Maximum Password Age in Days	Value: 60
Password Expiration Warning in Days	Value: 4
Minimum Changed Characters	Value: 4
Maximum Consecutive Repeated Characters	Value: 2

- 3 Go to **System > Admin Settings > General Settings > Security > Password Settings > User Room Password**, and enter the corresponding settings for the User Room Password.
- 4 Go to **System > Admin Settings > General Settings > Security > Password Settings > Remote Access Passwords**, and enter the corresponding settings for the Remote Access Password.

## Configuring the System to Use Certificates

The Polycom HDX system supports the use of PKI certificates for additional security. You can manage certificates and revocation only by using the Polycom HDX web interface. Make sure the appropriate certificate authority (CA) and identity certificates are available on your computer so that you can upload them. Refer to the *Administrator's Guide for Polycom HDX Systems* for more information.

## Detecting Intrusions

The Polycom HDX system logs an entry to the security log when it detects a possible network intrusion. The security log prefix identifies the type of packet detected, as shown in the following table.

Prefix	Packet Type
SECURITY: NIDS/unknown_tcp	Packet that attempts to connect or probe a closed TCP port
SECURITY: NIDS/unknown_udp	Packet that probes a closed UDP port
SECURITY: NIDS/invalid_tcp	TCP packet in an invalid state

Prefix	Packet Type
SECURITY: NIDS/invalid_icmp	ICMP or ICMPv6 packet in an invalid state
SECURITY: NIDS/unknown	Packet with an unknown protocol number in the IP header
SECURITY: NIDS/flood	Stream of ICMP or ICMPv6 ping requests or TCP connections to an opened TCP port

Following the message prefix, the security log entry includes the timestamp and the IP, TCP, UDP, ICMP, or ICMPv6 headers. For example, the following security log entry shows an “unknown\_udp” intrusion:

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

## Viewing Network Interface and System Status

### Network Interface Status

The network interface status is indicated by the lights on the network interface module.

#### Quad BRI Network Interface Status Lights

The network interface lights are located on the network interface module.

Indicator Light	Connection Status
Green and yellow lights off	Indicates one of the following situations: <ul style="list-style-type: none"> <li>• No power to the system.</li> <li>• The system is not connected to the network.</li> <li>• The system is not receiving a clock signal from the network.</li> <li>• The system is restarting.</li> </ul>

Indicator Light	Connection Status
Green light on	The system is receiving a clock signal from the network.
Yellow light on	The system is able to make a call.
Green and yellow lights on	Indicates one of the following situations: <ul style="list-style-type: none"> <li>The system is receiving a software update.</li> <li>The system is operating normally.</li> </ul>

## PRI Network Interface Status Lights

The network interface lights are located on the network interface module.

Indicator Light	Connection Status
Green and yellow lights off	No power to the system.
Red light on or blinking	Indicates one of the following situations: <ul style="list-style-type: none"> <li>The system is not connected to the ISDN network.</li> <li>There is a problem with the ISDN line.</li> </ul>
Yellow light on or blinking	There is a problem with the ISDN line.
Green light on	The system is able to make and receive calls.


## Viewing System Status

You can view the System Status screen on the local system or by using the HDX web interface. The System Status screen displays system status information, including auto answer point-to-point, remote control battery, IP network, meeting password, log threshold, and ISDN lines.



If the system detects that any of the ISDN BRI SPIDs are incorrect or that an ISDN line is connected to the wrong ISDN port on the network interface module, the System Status screen displays a red arrow for that line. If this happens, ensure the ISDN and SPID numbers are correct.

### To view the System Status on the system:

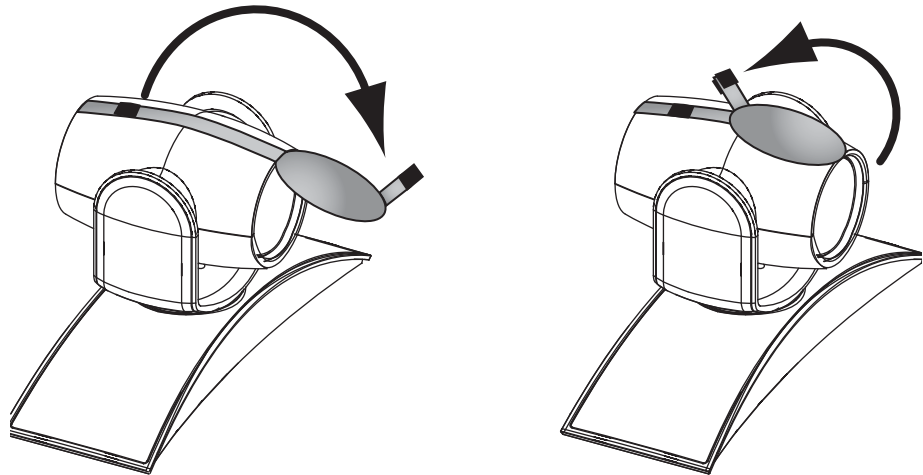
- Go to **System > Diagnostics > System Status**.
- For an explanation of any of the status items, select the item and press  on the remote control.

**To view the System Status using the Polycom HDX web interface:**

1. Open a web browser, and in the browser address line enter the system IP address, for example, `https://10.11.12.13`, to go to the Polycom HDX web interface.
2. Enter the Admin ID as the user name (default is `admin`), and enter the Admin Remote Access Password, if one is set.
3. Click **Diagnostics** from any page in the Polycom HDX web interface.
4. For an explanation of any of the status items, click the item.

## Using the Camera Privacy Cover

The Polycom EagleEye camera goes to sleep when the Polycom HDX system does. For added security Polycom now offers a privacy cover (part number 2215-28454-001) that you can attach to the camera. You can open and close the cover as needed. Contact your Polycom distributor for more information.



## Using the API with a Secure RS-232 Interface

You must log in with a password to start an RS-232 session when the system is configured with the Maximum Security Profile and if the system is configured for external authentication through Active Directory. Refer to [Configuring Your System for Remote Access](#) on [page 11](#) for more information.

## 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.