

# U.S. DoD DSN Deployment Guide

Polycom HDX Systems, Version 2.5.0.7\_G



This document provides the latest information about deploying Polycom HDX systems on the U.S. Department of Defense (DoD) Defense Switched Network (DSN). The information in this document applies to Polycom HDX Systems running version 2.5.0.7\_G software.

When you upgrade your Polycom HDX system to version 2.5.0.7\_G, both the main system and factory partition are upgraded to version 2.5.0.7\_G. If you later perform a factory restore, the system returns to version 2.5.0.7\_G instead of to the software version originally installed on the system.

After you install version 2.5.0.7\_G, downgrading to an earlier UC APL-certified 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).

For information about specific certifications, refer to [www.polycom.com/usa/en/solutions/industry\\_solutions/government/certification\\_accreditation.html](http://www.polycom.com/usa/en/solutions/industry_solutions/government/certification_accreditation.html).

In order to deploy Polycom HDX systems on the DoD DSN, you must configure certain system settings and define your password policy. This document describes how to perform these tasks.

If a setting is mandated by a Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirement, the specific STIG reference is listed along with the setting.



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.

## Using the DoD DSN Security Profile

The DoD DSN Security Profile setting lets you control particular fields in order to meet DoD DSN requirements. The Security Profile can only be set in the setup wizard, which you can access only during initial setup, when the system flash memory is deleted as part of a system update, or after a system reset with system settings deleted. After the setup wizard is complete, the Security Profile setting appears as read-only in the Admin Settings.

**To configure the Security Profile:**

- In the setup wizard, enable **Security Mode** and set **Security Profile** to **DoD DSN**.

This setting automatically sets and controls particular fields in order to meet DoD DSN requirements. The fields controlled by the profile are set to pre-defined 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 Password	Must be entered

**Security Settings**

Setting	Restriction
<b>Security Mode</b>	Enabled, not configurable
<b>Security Profile</b>	Set to <b>DoD DSN</b> , not configurable
<b>Require Login for System Access</b>	Enabled, not configurable
<b>Enable Remote Access: Web</b>	Disabled, not configurable
<b>Allow Video Display on Web</b>	Disabled, not configurable
<b>Security Banner</b>	Set to DoD, <b>Off</b> is not allowed
<b>Lock Account after Failed Logins</b>	Set to 3, <b>Off</b> is not allowed
<b>Account Lock Duration</b>	Set to 1, configurable
<b>AES Mode</b>	Set to <b>Required for Video Calls Only</b> , configurable

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

Setting	Restriction
Minimum Length	Set to <b>6</b> , must be at least 6
Can Contain ID or Its Reverse Form	Disabled, not configurable
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
Do Not Allow Previous Passwords	Set to <b>10</b> , must be at least <b>5</b>
Minimum Password Age in Days	Set to <b>Off</b> , configurable
Maximum Password Age in Days	Set to <b>90</b> , must be at least 5
Password Expiration Warning in Days	Set to 4, <b>Off</b> not allowed
Minimum Changed Characters	Set to <b>4</b> , not allowed: <b>Off</b> , <b>1</b> , <b>2</b> , or <b>3</b>
Maximum Consecutive Repeated Characters	Set to <b>Off</b> , configurable

### Meeting Password Settings

Setting	Restriction
Minimum Length	Set to <b>Off</b> , must be <b>Off</b> or at least 9
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
Do Not Allow Previous Passwords	Set to <b>10</b> , must be at least <b>5</b>
Minimum Password Age in Days	Set to <b>Off</b> , configurable
Maximum Password Age in Days	Set to <b>90</b> , must be at least <b>5</b>
Password Expiration Warning in Days	Set to <b>4</b> , <b>Off</b> is not allowed
Minimum Changed Characters	Set to <b>Off</b> , configurable
Maximum Consecutive Repeated Characters	Set to <b>Off</b> , configurable

## Home Screen and Other Settings

Setting	Restriction
Serial Ports: RS-232 Mode	Set to <b>Off</b> , not configurable
SIP Transport Protocol	Set to <b>TLS</b> , not configurable
Directory Servers	Not 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

## Configuring Your System



This section describes how to manually configure system settings to meet DSN Deployment requirements.

### To configure your system for DSN deployment:

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 **DoD DSN**.
  - Set **Admin ID** to a value other than **admin**.
  - Set a **Room Password** that meets the default password policy as described in [Password Settings for Room, Remote Access, and User Passwords](#).


You can modify the password policies after you complete the setup wizard. See [Configuring Your Room and User Password Policy](#) for more information about doing this.



- Change the **User ID** to something other than **user**.

- Set a **User Password** that meets the default password policy as described in [Password Settings for Room, Remote Access, and User Passwords](#).
3. After you complete the setup wizard and the system restarts, log into the system using the Admin ID and Room Password.
  4. Go to **System > Admin Settings > General Settings > Security > Security Settings** >  >  and configure these settings:

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

5. 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
<b>ISDN-only Deployments</b> Polycom HDX 9000 Polycom HDX 8000 Version B Polycom HDX 7000 Version B or later Polycom HDX 6000	Go to <b>System &gt; Admin Settings &gt; General Settings &gt; Location</b> >  , and set <b>Time Server</b> to <b>Off</b> and manually configure the time and date.

Deployment Type	Configuration Steps
<b>IP Deployments</b> Polycom HDX 9000 Polycom HDX 8000 Version B Polycom HDX 7000 Version B or later Polycom HDX 6000	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 <b>Time Server</b> to <b>Off</b> and manually configure the time and date.</li> <li>• Set <b>Time Server</b> to <b>Auto</b>.</li> <li>• Set <b>Time Server</b> to <b>Manual with NTP server address specified</b>.</li> </ul>
<b>IP Deployments</b> Polycom HDX 8000 Version A Polycom HDX 7000 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 <b>Time Server</b> to <b>Auto</b>.</li> <li>• Set <b>Time Server</b> to <b>Manual with NTP server address specified</b>.</li> </ul>





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

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

**To check your hardware version:**

- For HDX 8000 and 7000 HD systems, you can check 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

6. 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.
7. Go to **System > Admin Settings > Network > Call Preference**, and configure these settings on the **Call Preference** screen:

Setting	Description
<b>IP H.323</b>	<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>
<b>SIP</b>	<ul style="list-style-type: none"> <li>• Disable this setting for ISDN-only deployments.</li> <li>• Enable this setting if SIP calling on IP networks is required.</li> </ul>
<b>ISDN H.320</b>	<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>

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

Setting	Description
<b>Percent Filled Threshold</b>	<p>Specifies the percent filled level which triggers a system alert. Suggested value: 70.</p> <p>This alert is mandated by the Application Security STIG (APP0420).</p>

## Configuring Your Room and User Password Policy

Though “strong passwords” are recommended for security purposes, keep in mind that strong passwords require use of the onscreen keyboard to enter letters and special characters. This can make it possible for others to view a password as it is entered. This risk can be mitigated by using longer numeric-only passwords which can be entered 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 > Room Password**, and configure these settings:

Setting	Strong Passwords	Numeric-only Passwords
<b>Minimum Length</b>	Value: 15 (recommended) This setting meets these requirements: <ul style="list-style-type: none"> <li>• UNIX STIG V5R1: GEN000580 (minimum 14)</li> <li>• Application Security Checklist V2R19: APP0140 (minimum 8)</li> <li>• DSN STIG V2R3: DSN13.06 (minimum 8)</li> <li>• GR-815-CORE-2 R3-39 [26] (minimum 6)</li> <li>• DODI 8500.2: IAIA-1, IAIA-2 (minimum 8)</li> <li>• VTC STIG V1R1: RTS-VTC 2024.00 (minimum 6)</li> </ul>	Value: 15
<b>Can Contain ID or Its Reverse Form</b>	Disable This setting meets this requirement: <ul style="list-style-type: none"> <li>• GR-815-CORE-2: R3-39 [26]</li> </ul>	Disable This setting meets these requirements: <ul style="list-style-type: none"> <li>• GR-815-CORE-2: R3-39 [26]</li> </ul>
<b>Require Lower Case Letters</b>	Value: 1 This setting meets these requirements: <ul style="list-style-type: none"> <li>• UNIX STIG V5R1: GEN000600</li> <li>• Application Security Checklist V2R19: APP0140</li> <li>• DSN STIG V2R3: DSN13.06</li> <li>• GR-815-CORE-2 R3-39 [26]</li> <li>• DODI 8500.2: IAIA-1, IAIA-2</li> </ul>	Off
<b>Require Upper Case Letters</b>	Value: 1 This setting meets these requirements: <ul style="list-style-type: none"> <li>• UNIX STIG V5R1: GEN000600</li> <li>• Application Security Checklist V2R19: APP0140</li> <li>• DSN STIG V2R3: DSN13.06</li> <li>• GR-815-CORE-2 R3-39 [26]</li> <li>• DODI 8500.2: IAIA-1, IAIA-2</li> </ul>	Off



Setting	Strong Passwords	Numeric-only Passwords
<b>Require Numbers</b>	Value: 1 This setting meets these requirements: <ul style="list-style-type: none"> <li>• UNIX STIG V5R1: GEN000620</li> <li>• Application Security Checklist V2R19: APP0140</li> <li>• DSN STIG V2R3: DSN13.06</li> <li>• GR-815-CORE-2 R3-39 [26]</li> <li>• DODI 8500.2: IAIA-1, IAIA-2</li> </ul>	All
<b>Require Special Characters</b>	Value: 1 This setting meets these requirements: <ul style="list-style-type: none"> <li>• UNIX STIG V5R1: GEN000640</li> <li>• Application Security Checklist V2R19: APP0140</li> <li>• DSN STIG V2R3: DSN13.06</li> <li>• GR-815-CORE-2 R3-39 [26]</li> <li>• DODI 8500.2: IAIA-1, IAIA-2</li> </ul>	Off

Select  and configure these settings:

Setting	Description
<b>Do Not Allow Previous Passwords</b>	Value: 10 This setting meets these requirements: <ul style="list-style-type: none"> <li>• Application Security Checklist V2R19: APP0140 (requires 10)</li> <li>• DSN STIG V2R3: DSN13.09 (requires 8)</li> <li>• GR-815-CORE-2: R3-38 [25] (requires 5)</li> <li>• VTC STIG V1R1: RTS-VTC2040.00) (requires 8)</li> </ul>
<b>Minimum Password Age in Days</b>	Value: 1 or Off This setting meets these requirements: <ul style="list-style-type: none"> <li>• Application Security Checklist V2R19: APP0140 (minimum 1 for users, 0 for administrators)</li> <li>• DSN STIG V2R3: DSN13.08 (minimum 1 without IAO intervention)</li> <li>• GR-815-CORE-2: R3-38 [25] (minimum 20)</li> </ul>
<b>Maximum Password Age in Days</b>	Value: 60 This setting meets these requirements: <ul style="list-style-type: none"> <li>• UNIX STIG V5R1: GEN000700 (maximum 60)</li> <li>• Application Security Checklist V2R19: APP0140 (maximum 90)</li> <li>• DSN STIG V2R3: DSN13.07 (maximum 90)</li> <li>• GR-815-CORE-2: R3-33 [21] (maximum 20-90)</li> </ul>

Setting	Description
<b>Password Expiration Warning in Days</b>	Value: 4 This setting meets this requirement: <ul style="list-style-type: none"> <li>GR-815-CORE-2: CR3-36 [23]</li> </ul>
<b>Minimum Changed Characters</b>	Value: 4 This setting meets this requirement: <ul style="list-style-type: none"> <li>DODI 8500.2: IAIA-1, IAIA-2</li> </ul>
<b>Maximum Consecutive Repeated Characters</b>	Value: 2 This setting meets this requirement: <ul style="list-style-type: none"> <li>UNIX STIG V5R1: GEN000680 (maximum 2)</li> </ul>

Go to **System > Admin Settings > General Settings > Security > Password Settings > User Password**, and enter the corresponding settings for the User Password.

## 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: <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: <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: <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. 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:

Go to System > Diagnostics > System Status.

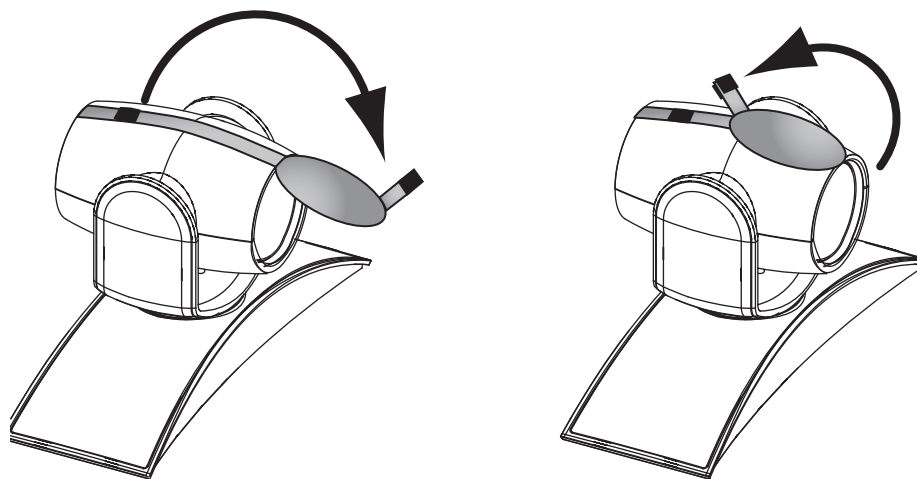
For an explanation of any of the status items, select the item and press



on the remote control.

## Using the Camera Privacy Cover

The Polycom EagleEye™ camera goes to sleep when the Polycom HDX system does. But 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.



## Copyright Information

© 2010 Polycom, Inc. All rights reserved.

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.

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.

## Disclaimer

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and fitness for purpose.

## Trademark Information

© 2010, Polycom, Inc. All rights reserved. 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 property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

