U.S. DoD DSN Deployment Guide

Polycom HDX Systems, Version 2.0.5_J

This document provides the latest information about deploying Polycom HDX systems on the U.S. Department of Defense Defense Switched Network (DSN). The information in this document applies to Polycom HDX Systems running version 2.0.5_J software.

For information about specific certifications, refer to www.polycom.com/usa/en/solutions/industry_solutions/government/certification_accreditation.html.

In order to deploy Polycom HDX systems on the U.S. Department of Defense Defense Switched Network (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.

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.

December 2008
3725-28305-002/A

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

Password Settings for Room, Remote Access, and User Passwords

Setting	Restriction
Minimum Length	Set to **6**, must be at least 6
Can Contain ID or Its Reverse Form	Disabled, not configurable
Require Lower Case Letters	Set to **Off**, configurable
Require Upper Case Letters	Set to **Off**, configurable
Require Numbers	Set to **Off**, configurable
Require Special Characters	Set to **Off**, configurable
Do Not Allow Previous Passwords	Set to **10**, must be at least **5**
Minimum Password Age in Days	Set to **Off**, configurable
Maximum Password Age in Days	Set to **90**, **Off** not allowed

Setting	Restriction
Password Expiration Warning in Days	Set to 4, **Off** not allowed
Minimum Changed Characters	Set to **4**, not allowed: **Off**, **1**, **2**, or **3**
Maximum Consecutive Repeated Characters	Set to **Off**, configurable

Meeting Password Settings

Setting	Restriction
Minimum Length	Set to **Off**, must be **Off** or at least 9
Require Lower Case Letters	Set to **Off**, configurable
Require Upper Case Letters	Set to **Off**, configurable
Require Numbers	Set to **Off**, configurable
Require Special Characters	Set to **Off**, configurable
Do Not Allow Previous Passwords	Set to **10**, must be at least **5**
Minimum Password Age in Days	Set to **0**, configurable
Maximum Password Age in Days	Set to **90**, **Off** is not allowed
Password Expiration Warning in Days	Set to **4**, **Off** is not allowed
Minimum Changed Characters	Set to **Off**, configurable
Maximum Consecutive Repeated Characters	Set to **Off**, configurable

Home Screen and Other Settings

Setting	Restriction
Serial Ports: RS-232 Mode	Set to **Off**, not configurable
SIP Transport Protocol	Set to **TLS**, not configurable
Directory Servers	Disabled, not configurable
Auto Answer Point-to-Point Video	Disabled, configurable
Auto Answer Multipoint Video	Disabled, configurable
Availability Control	Enabled, not configurable
Recent Calls	Disabled, not configurable

Setting	Restriction
Last Number Dialed	Disabled, not configurable
Far Control of Near Camera	Disabled, not 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 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 Settings > Security**, and configure these settings on the **Security** screen

Setting	Description
AES Encryption	Specifies whether to encrypt calls with other sites. • **When Available —** Allows calls with all endpoints, including sites that may not support encryption. • **Required for All Calls —** Allows video calls only with sites that support encryption. ISDN voice and analog phone calls are not allowed. • **Required for Video Calls Only —** Allows video calls only with sites that support encryption. ISDN voice and analog phone calls are allowed.
Allow Access to User Settings	Specifies whether the **User Setting** screen is accessible to users via the System screen. • Enable this setting if meeting passwords are required to join multipoint calls. • Disable this setting if meeting passwords are not required for multipoint calls.

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

   Polycom HDX 9000 systems have an internal battery that allows them to keep accurate time across power outages and system restarts. Polycom HDX 4000, 7000, and 8000 systems require a connection to an NTP server in order to keep accurate time across power outages and system restarts.

   — For Polycom HDX 9000 ISDN-only deployments:

   • Go to **System > Admin Settings > General Settings > Security Settings > Security**, and disable **Connect to My LAN**.

   • Go to **System > Admin Settings > General Settings > Location** >  , and set **Time Server** to **Off** and then manually configure the time and date.

   — For Polycom HDX 9000 IP deployments and all Polycom HDX 4000, 7000, and 8000 deployments:

   • Go to **System > Admin Settings > General Settings > Security Settings > Security**, and enable **Connect to My LAN**.

   • Go to **System > Admin Settings > General Settings > Location** >  , and set **Time Server** to either **Auto** or **Manual**, as appropriate. If you choose **Manual**,you must also enter the **Time Server Address**.

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.

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

Setting	Description
IP H.323	• Disable this setting for ISDN-only deployments. • Enable this setting if H.323 calling on IP networks is required.
SIP	• Disable this setting for ISDN-only deployments. • Enable this setting if SIP calling on IP networks is required.
ISDN H.320	• Disable this setting for IP-only deployments. • Enable this setting if ISDN H.320 calling is required.

8. Go to **System > 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. This alert is mandated by the Application Security STIG (APP0420).

Configuring Your Room 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
Minimum Length	Value: 14 (recommended) This setting meets these requirements: • UNIX STIG V5R1: GEN000580 (minimum 14) • Application Security Checklist V2R19: APP0140 (minimum 8) • DSN STIG V2R3: DSN13.06 (minimum 8) • GR-815-CORE-2 R3-39 [26] (minimum 6) • DODI 8500.2: IAIA-1, IAIA-2 (minimum 8 • VTC STIG V1R1: RTS-VTC 2024.00 (minimum 6))	Value: 15
Can Contain ID or Its Reverse Form	Disable This setting meets this requirement: • GR-815-CORE-2: R3-39 [26]	Disable This setting meets these requirements: • GR-815-CORE-2: R3-39 [26]
Require Lower Case Letters	Value: 1 This setting meets these requirements: • UNIX STIG V5R1: GEN000600 • Application Security Checklist V2R19: APP0140 • DSN STIG V2R3: DSN13.06 • GR-815-CORE-2 R3-39 [26] • DODI 8500.2: IAIA-1, IAIA-2	Off
Require Upper Case Letters	Value: 1 This setting meets these requirements: • UNIX STIG V5R1: GEN000600 • Application Security Checklist V2R19: APP0140 • DSN STIG V2R3: DSN13.06 • GR-815-CORE-2 R3-39 [26] • DODI 8500.2: IAIA-1, IAIA-2	Off

Setting	Strong Passwords	Numeric-only Passwords
Require Numbers	Value: 1 This setting meets these requirements: • UNIX STIG V5R1: GEN000620 • Application Security Checklist V2R19: APP0140 • DSN STIG V2R3: DSN13.06 • GR-815-CORE-2 R3-39 [26] • DODI 8500.2: IAIA-1, IAIA-2	All
Require Special Characters	Value: 1 This setting meets these requirements: • UNIX STIG V5R1: GEN000640 • Application Security Checklist V2R19: APP0140 • DSN STIG V2R3: DSN13.06 • GR-815-CORE-2 R3-39 [26] • DODI 8500.2: IAIA-1, IAIA-2	Off

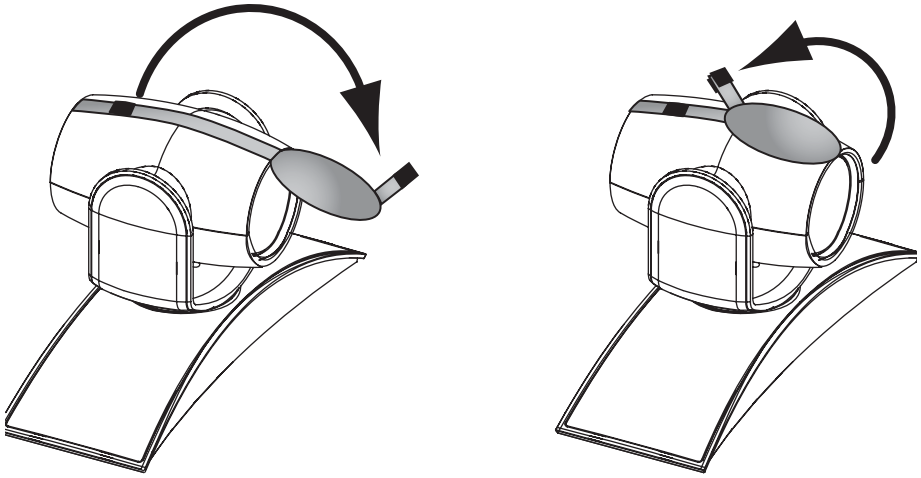
2. Select  and configure these settings:

Setting	Description
Do Not Allow Previous Passwords	Value: 10 This setting meets these requirements: • Application Security Checklist V2R19: APP0140 (requires 10) • DSN STIG V2R3: DSN13.09 (requires 8) • GR-815-CORE-2: R3-38 [25] (requires 5) • VTC STIG V1R1: RTS-VTC2040.00) (requires 8)
Minimum Password Age in Days	Value: 1 or 0ff This setting meets these requirements: • Application Security Checklist V2R19: APP0140 (minimum 1 for users, 0 for administrators) • DSN STIG V2R3: DSN13.08 (minimum 1 without IAO intervention) • GR-815-CORE-2: R3-38 [25] (minimum 20)
Maximum Password Age in Days	Value: 60 This setting meets these requirements: • UNIX STIG V5R1: GEN000700 (maximum 60) • Application Security Checklist V2R19: APP0140 (maximum 90) • DSN STIG V2R3: DSN13.07 (maximum 90) • GR-815-CORE-2: R3-33 [21] (maximum 20-90)

Setting	Description
Password Expiration Warning in Days	Value: 4 This setting meets this requirement: • GR-815-CORE-2: CR3-36 [23]
Minimum Changed Characters	Value: 4 This setting meets this requirement: • DODI 8500.2: IAIA-1, IAIA-2
Maximum Consecutive Repeated Characters	Value: 2 This setting meets this requirement: • UNIX STIG V5R1: GEN000680 (maximum 2)

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

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

Polycom® and the Polycom logo design are registered trademarks of Polycom, Inc. Polycom EagleEye™, Polycom HDX 4000™, Polycom HDX 7000™, Polycom HDX 8000™, and Polycom HDX 9000™ are trademarks of Polycom, Inc.

All other brand and product names are trademarks or registered trademarks of their respective companies.