POLYCOM®

Polycom Unified Communications Deployment Guide for Maximum Security Environments

Wave 3 | August 2011 | 3725-00030-001A

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 product is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

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

Contents

About This Guide

This guide describes how to securely deploy the Polycom® unified communications experience—specifically the Polycom products that enable the experience.

Polycom unified communications solution for maximum security environments is enabled by an integrated suite of Polycom hardware devices and software applications that allow you to securely integrate high-quality video and audio conferencing.

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 a high-level overview of the deployment process for maximum security environments. Please refer to the product documentation for the appropriate Polycom product for detailed instructions. You can find Polycom product documentation online at http://www.polycom.com/support.

Required Skills

Deploying a secure video conferencing system requires planning and elementary knowledge of video conferencing and video conferencing administration.

This guide is written for a technical audience. You will be configuring system security, networking, and security certificates as well as integrating with a time server, directory server, and database server.

This guide assumes that you are starting with a Polycom devices that have not been previously configured.

Also, deploying Polycom unified communications also requires knowledge of the following third-party products:

- An external domain name server
- An external Microsoft Active Directory server

- An NTP (network time protocol) server
- A certificate authority server, as well as knowledge of security certificates
- An OCSP (Online Certificate Status Protocol) server

This document assumes that these infrastructure systems are already deployed and that the administrators for these applications are available to aide the administrator deploying Polycom video conferencing products.

Polycom Solution Support Services

Please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative for more information.

1

Secure Polycom Unified Communications

Polycom unified communications for maximum security environments is enabled by an integrated suite of Polycom hardware devices and software applications that allow you to securely integrate high-quality video and audio conferencing.

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 information for security-conscious using the listed products.

Polycom Products

The following Polycom product versions are part of the Wave 3 solution of integrated products designed to deliver a scalable, easily managed video conferencing solution for maximum security environments.

Product	Version	Description
Systems		
Polycom RMX 1500, 2000 or 4000 system	v7.5.0J	Provides MCU conferencing resources.
Polycom DMA 7000 system	v2.1.0J	Virtualizes MCU conferencing resources. Highly recommended for deployments that include two or more Polycom RMX systems.
Polycom CMA 4000 or 5000 system	v5.2.0J	Enables automatic provisioning of Polycom HDX endpoint systems. Recommended for remote management of endpoints.
Endpoints		
Polycom HDX system	v2.7.0_J	High-definition video endpoint systems.

2

Securing Your Environment

Before you deploy your secure video conferencing system, your IT environment must meet security requirements that are outside the scope of this guide.

Polycom unified communications components require certain network infrastructure components in order to meet maximum security requirements.

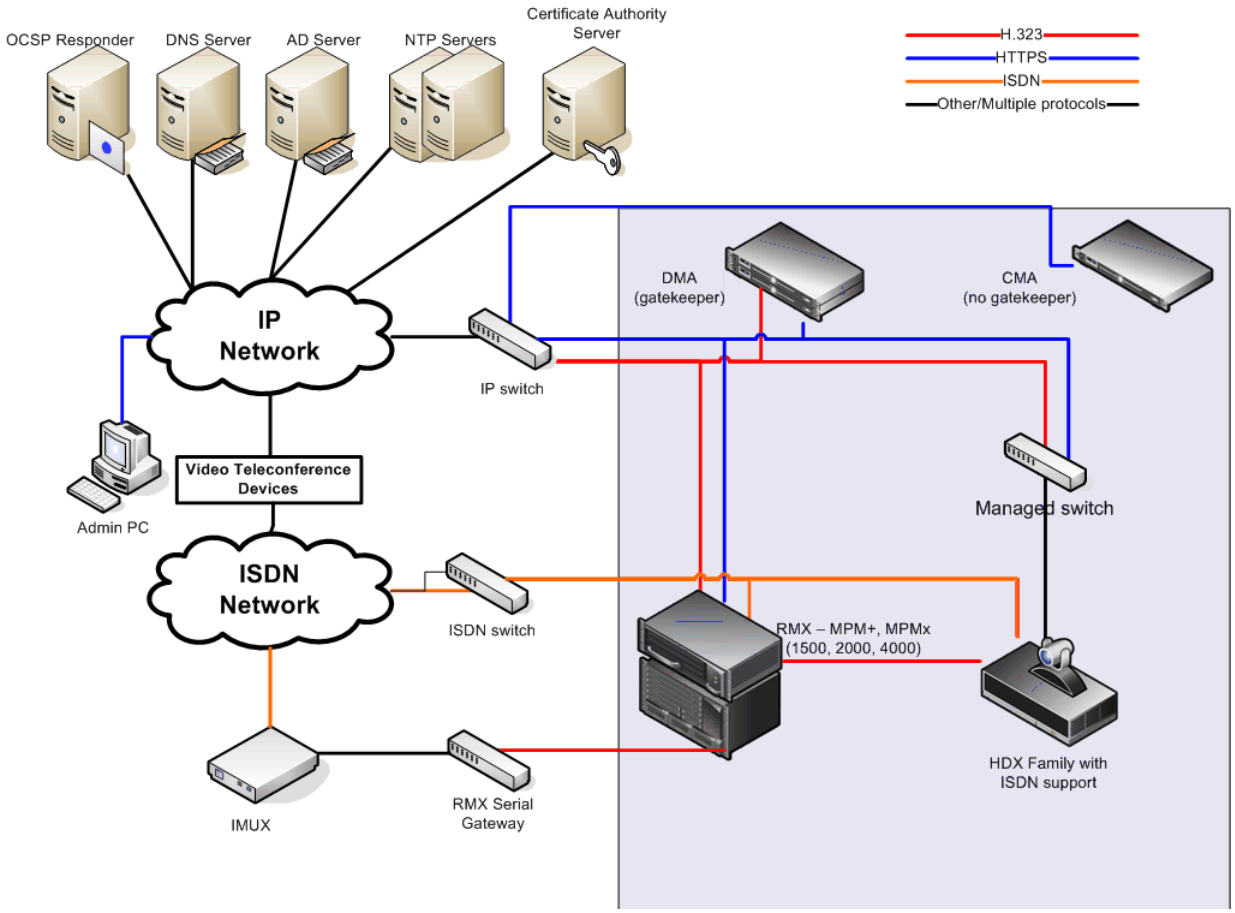
This chapter discusses network security components and provides details of the Polycom-specific uses for each.

This chapter includes the following sections:

Reference Architecture

A typical deployment of a secure audio and video conferencing system is represented in Figure 2-1.

Figure 2-1 *Reference Architecture for maximum security audio and video conferencing.*



Required IT Infrastructure

The following IT infrastructure components are required and used to secure the Polycom audio and video solution.

- An external domain name server (DNS)
- An network time protocol (NTP) server
- A certificate authority server, as well as knowledge of security certificates
- An OCSP (Online Certificate Status Protocol) server

DNS

All systems that are part of the secure solution, either IT infrastructure or Polycom devices, must be configured to resolve all other Polycom and IT infrastructure device host names on the network.

This also includes any PC used to access Polycom management consoles.

The easiest way to do this is to use a DNS server to ensure that each machine in your deployment can be identified by a host name or FQDN (Fully Qualified Domain Name).

- Machines must have FQDNs to use security certificates.
- In dual stack network configurations that support both IPv4 and IPv6, you should include both IP addresses in the DNS configuration.
- For the CMA system, both primary and alternate DNS servers must use the same IP addressing protocol, either IPv4 OR IPv6.
- When connecting to machines within your IT infrastructure from Polycom devices, you should use the FQDN of the respective machine.

The Polycom DMA system, Polycom CMA system and Polycom HDX systems include SANs (subject alternative names) in their certificate requests which means that the IP address is automatically included with the identifying information in the security certificate.

Certificate Authority Server

A certificate authority (CA) server is used to issue and manage security credentials. A CA server is an integral part of a PKI (public key infrastructure) security system and is required within a maximum security environment.

- Polycom products must be able to resolve the CA server using its fully qualified domain name.
- All machines within your environment must have a valid certificate or certificate chain and a certificate revocation method in place.
- However, the NTP server does not require a security certificate.

- Certificates issued for Polycom devices within a secure environment must meet specific requirements. See "Certificate Configuration and Management" on page 10.
- Each machine that uses security certificates must also have a certificate revocation policy in place. Machines can either use an OCSP responder or CRLs. See"Configure Certificate Management" on page 11.

OCSP Responder

You can configure a Polycom DMA system and Polycom HDX systems to use an OCSP (Online Certificate Status Protocol) server to manage certificate revocation.

When a machine submits a certificate for access to a network host, the host sends an OCSP request for certificate status to a responder. The responder sends back a status of "good", "revoked", or "unknown." The network host denies or allows access based on the certificate status returned by the responder.

OCSP responders eliminate the need to distribute, install, and update revocation lists across all PKI-enabled hosts, because the revocation status is maintained and updated centrally on the OCSP responder.

Polycom CMA systems and Polycom RMX systems require CRLs. See "Certificate Revocation Lists (CRL)" on page 11.

NTP Servers

In order to meet maximum security requirements, a secure audio and video conferencing environment must include at least two NTP servers.

Some Polycom devices must use an IP address to connect to respective NTP servers. See individual product documentation for details.

Security certificates are not required for NTP servers.

Microsoft Active Directory

You can connect to Microsoft Active Directory to allow users to connect to Polycom products with their network credentials.

When connecting your Polycom product to your Active Directory server, Polycom recommends that you use the FQDN. This means that the Active Directory server must also be included in DNS configuration.

Administration PCs

Polycom components are often administered and managed by using a web console accessed through a PC. Each PC used to administer Polycom components needs to meet maximum security requirements.

- When deploying in government environments, the administration PC needs to have the Army Golden Master (Gold Disk) installed. The Polycom solution was tested with following Gold Disk version
  - Vista 9.0.0 Desktop Final with the Vista 9.0.0 April Update and the Vista 9.0.0 September Update.
- Needs to have certificates for complete CA chain.
- When deploying in government environments, only Internet Explorer 8 is supported.
- The Polycom maximum security environment only supports TLS 1.0.

Certificate Configuration and Management

When using Polycom devices in a maximum security environment, Polycom devices require security certificates.

You must also configure certificate management. See "Configure Certificate Management" on page 11.

Certificate Template Requirements

Polycom devices in maximum security environments have specific security certificate requirements.

You may need to modify the certificate template used by your CA server to meet Polycom requirements. See Table 2-2 for a list of requirements.

Table 2-1 *Certificate Requirements for Polycom devices.*

Polycom Product	Template Requirements
Polycom RMX System	• Support 2048-bit encryption keys. • Support EKU (extended key usage) and include both client and server authentication purposes.
Polycom DMA system	• Support 2048-bit encryption keys. • Support EKU (extended key usage) extensions and include both client and server authentication purposes. • Support SANs.
Polycom CMA system	• Support 2048-bit encryption keys. • Support EKU (extended key usage) and include both client and server authentication purposes.
Polycom HDX system	• Support 2048-bit encryption keys. • Support EKU (extended key usage) and include both client and server authentication purposes. • Support SANs.

Certificate Requirements Per Polycom Devices

Each Polycom device must have certificates for the entire certificate chain.

Table 2-2 *Certificate Requirements for Polycom devices.*

Polycom Product	Certificates Required
Polycom RMX system	• Applicable certificates for CA identity chain. • Public certificate identifying the RMX system.
Polycom DMA system	• Applicable certificates for CA identity chain. • Public certificate identifying the DMA system.
Polycom CMA system	• Applicable certificates for CA identity chain. • Public certificate identifying the CMA system.
Polycom HDX system	• Applicable certificates for CA identity chain. • Public certificate identifying the HDX system.

Configure Certificate Management

Within a PKI environment, certificate revocation policies are used to ensure that certificates are still valid. Certificates can become expired or revoked for various reasons.

Polycom devices use one of two methods to manage certificate revocations:

- Certificate Revocation Lists (CRL)
- OCSP Responder

The type of management method you can use depends on the Polycom product and the availability of each method in your PKI environment.

Certificate Revocation Lists (CRL)

A CRL is a text file that lists all revoked certificates along with the reason(s) for their revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next CRL release. When a user submits a certificate for access to a network host, the host allows or denies access based on the certificate revocation status according to the CRL.

When using CRLs to maintain certificate authenticity, you must ensure that the CRL itself is always up-to-date.

Each CA issuer certificate in your certificate chain must have a corresponding CRL.

Polycom Products that Use CRLs

- Polycom RMX systems
- Polycom CMA systems

OCSP Responder

In some environments, the certificate authority (CA) embeds the address of the OCSP responder in a certificate at the time the certificate is issued. In other cases, the certificate does not carry this information and you must configure the Polycom DMA system or Polycom HDX system to use a particular OCSP responder for certificate verification.

Polycom Products that can use an OCSP Responder

- Polycom DMA systems
- Polycom HDX systems

Antivirus Software

Some Polycom products ship with antivirus software. Antivirus software is required for maximum security environments. Schedule anti-virus scans and signature file updates in accordance with your site policies.

Virus scans can impede system performance. Polycom recommends running antivirus scans during off hours.

Intrusion Detection Software

In maximum security environments, Polycom products support detection of network-based intrusion attempts. See individual product documentation to find out more about how detections are logged.

IPv6 Support

Polycom products in maximum security environments support both IPv4 and IPv6 addressing protocols.

You can support IPv4-only, IPv6-only, or both protocols at once (dual stack).

3

Securing Polycom Products

This chapter provides an overview of the process of securing your Polycom conferencing infrastructure and includes the following sections:

Securing Polycom Products

The following Polycom product versions are part of the Wave 3 solution of integrated products designed to deliver a scalable, easily managed video conferencing solution for maximum security environments.

Product	Version	Description
Systems		
Polycom RMX 1500, 2000 or 4000 system	v7.5.0J	Provides MCU conferencing resources.
Polycom DMA 7000 system	v2.1.0J	Virtualizes MCU conferencing resources. Highly recommended for deployments that include two or more Polycom RMX systems.
Polycom CMA 4000 or 5000 system	v5.2.0J	Enables automatic provisioning of Polycom HDX endpoint systems. Recommended for remote management of endpoints.
Endpoints		
Polycom HDX system	v2.7.0_J	High-definition video endpoint systems.

Install and Configuration Order

When deploying Polycom unified communications, it is important to ensure that each device is properly configured. Many settings cannot be modified once the device has been set to a level of maximum security.

Because of this, Polycom recommends configuring the devices in your Polycom solution in the following order:

1. The Polycom RMX system. See "Configuring the Polycom RMX System" on page 14.
2. The Polycom CMA system. See "Configuring the CMA System" on page 15.
3. The Polycom DMA system. See"Configuring the Polycom DMA System" on page 16.
4. The Polycom HDX system. See "Configuring the Polycom HDX System" on page 16.

Configuring the Polycom RMX System

To configure the RMX system:

1. Set up your Polycom RMX system.

   Follow the instructions in the *Polycom RMX™ Deployment Guide for the Maximum Security Environments*.

2. Configure DMA machine accounts in the RMX system.

   After you have set up your Polycom RMX system, you need to configure DMA machine account for the DMA system that routes calls to your RMX system. See "Using Machine Accounts" on page 17.

3. Configure CMA machine accounts in the RMX system.

   After you have set up your Polycom RMX system, you need to configure a CMA machine account for each CMA system that will monitor or schedule calls on your RMX system. See "Using Machine Accounts" on page 17.

Polycom RMX System Deployment Considerations

- The RMX system administrator must create a DMA machine account for the DMA system that will route calls to your RMX system. The DMA machine account must be created before bringing the DMA system online. See "Using Machine Accounts" on page 17.
- The RMX administrator must create a CMA machine account for the CMA system that will be monitoring or scheduling calls for your RMX system. The CMA machine account must be created before bringing the CMA system online. See "Using Machine Accounts" on page 17.

- RMX systems for maximum security environments include only some of the functionality found in the more commercial but less secure RMX system releases, and there are many operational differences, see "Restricted Polycom Functionality in Maximum Security Environments" on page 21.

Related Documentation

For detailed instruction on configuring the Polycom RMX system, consult the Polycom RMX system documentation:

- *Polycom RMX System Release Notes*
- *Polycom RMX System Deployment Guide for Maximum Security Environments*
- *Polycom RMX Administrator's Guide for Maximum Security Environments*

Configuring the CMA System

When your deployment includes a Polycom CMA system, you should configure and secure the Polycom CMA system before bringing any managed endpoints online.

1. Set up your Polycom CMA system.

   Follow the instructions in the *Polycom CMA System Getting Started Guide*.

2. Create HDX machine accounts in the CMA system.

   The CMA system administrator needs to create HDX machine accounts for each HDX system that the CMA system will manage, see "Considerations for HDX Machine Accounts" on page 17

Polycom CMA system Deployment Considerations

- The CMA system does not support provisioning an IPv6 address for a gatekeeper. If you want to use a gatekeeper, it must be IPv4.
- The CMA system does not support a dual stack address
- You must use dynamic device management to manage endpoints. The CMA system does not support other methods of device management.
- You must create an HDX machine account for each HDX endpoint that the CMA system will manage. The HDX machine account must be created before bringing the endpoint online, see "Using Machine Accounts" on page 17.
- CMA systems for maximum security environments include only some of the functionality found in the more commercial but less secure CMA system releases, and there are many operational differences, see "Restricted Polycom Functionality in Maximum Security Environments" on page 21.

Related Documentation

For detailed documentation on configuring the Polycom CMA system, consult the Polycom DMA documentation:

- *Polycom CMA System Release Notes*
- *Polycom CMA System Getting Started Guide*
- *Polycom CMA System Deployment Guide for Maximum Security Environments*

Configuring the Polycom DMA System

1 Set up your Polycom DMA system.

Follow the instructions in the *Polycom DMA™ Deployment Guide for the Maximum Security Environments*.

Polycom DMA system Deployment Considerations

- DMA systems for maximum security environments include only some of the functionality found in the more commercial but less secure DMA system releases, and there are many operational differences, see "Restricted Polycom Functionality in Maximum Security Environments" on page 21.
- The DMA system gatekeeper only supports IPv4.

Related Documentation

- *Polycom DMA System Release Notes*
- *Polycom DMA System Getting Started Guide*
- *Polycom DMA System Deployment Guide for Maximum Security Environments*
- *Polycom DMA System Operations Guide*

Configuring the Polycom HDX System

1 Set up your Polycom HDX system.

Refer to the *Polycom HDX System Deployment Guide for Maximum Security Environments* for instructions on how to secure a Polycom HDX system.

Polycom HDX system Deployment Considerations

- IPv6 calls do not support a gatekeeper. If your network includes support for IPv6, you cannot provision the HDX system with a gatekeeper or it will not be able to connect to an IPv6 network.

- If an HDX system is provisioned with an IPv4 gatekeeper address, it cannot make calls to an IPv6 network.
- When registering an HDX system with the CMA provisioning service, you must use the HDX machine account that was created in the CMA system, see "Using Machine Accounts" on page 17.
- HDX systems for maximum security environments include only some of the functionality found in the more commercial but less secure DMA system releases, and there are many operational differences, see "Restricted Polycom Functionality in Maximum Security Environments" on page 21.

Related Documentation

For detailed instruction on configuring the Polycom HDX system, consult the Polycom HDX system documentation:

- *Polycom HDX System Release Notes*
- *Polycom HDX System Deployment Guide for Maximum Security Environments*
- *Polycom HDX System Administration Guide*

Using Machine Accounts

Machine accounts are dedicated local accounts associated with specific Polycom devices that allow Polycom systems to communicate with each other without using a specific user's network credentials.

Within maximum security environments, the Polycom unified communications solution uses machine accounts in the following ways:

- The CMA system administrator must create an HDX machine account for each HDX system that it manages.
- The HDX system must login to the CMA system using the HDX machine account that was created in the CMA system for it to use.
- The RMX system administrator must create a DMA machine account for each DMA system that it communicates with.
- The DMA system must login to the RMX system using the DMA machine account that was created in the RMX system for it to use.

Considerations for HDX Machine Accounts

Polycom CMA system administrators need to create an HDX machine account for each HDX that the CMA system will manage. HDX machine accounts are maintained on the Polycom CMA system.

HDX machine accounts should be named after the corresponding device. For example, if the machine name of the HDX system is **machinename2**, the administrator for the CMA system should create a HDX machine account called **machinename2**.

Considerations for DMA and CMA Machine Accounts

Polycom RMX system administrators need to create machine accounts for each DMA or CMA system that will work with the RMX system. CMA and DMA machine accounts are maintained on the Polycom RMX system.

Respective machine accounts are used to authenticate the DMA system or CMA system with the RMX system.

Machine accounts should be named after the corresponding device. For example, if the machine name of the DMA system is **machinename3**, the administrator for the RMX system should create a DMA machine account called **machinename3**.

This machine account must include a fully-qualified domain name (FQDN) for the CMA and/or DMA system. This FQDN field on the RMX system is case-sensitive, so it must match the name in the CMA system or DMA system certificate (including case) exactly.

Verify Your Secure Polycom Environment

1. Perform first-time setup for the Polycom CMA system.
   a. Configure the CMA system for both IPv4 and IPv6 if necessary for your environment.
   b. Add HDX machine account for each endpoint (HDX system) that the Polycom CMA system will manage.
2. Place your HDX systems into Maximum Security Mode.
   a. Configure the HDX system for both IPv4 and IPv6 if necessary for your environment.
3. Use the CMA system to provision each HDX system.
4. Place an HDX to HDX call on each network protocol in your environment (IPv4 and IPv6 if applicable).
5. Place your Polycom RMX system into Ultra Secure mode.
   a. Configure the RMX system for both IPv4 and IPv6 if necessary for your environment.
   b. Configure the RMX system for network separation if necessary for your environment.
6. Configure the CMA system to monitor the RMX system(s).
7. Have two HDX systems call into the RMX system for a multi-point call.
   a. Test both network protocols (IPv4 and IPv6) if necessary for your environment.
8. Review CMA system monitoring of RMX system.
9. Place the Polycom DMA system into Maximum Security Mode.
   a. Configure the DMA system for both IPv4 and IPv6 if necessary for your environment.
   b. Configure the DMA system for network separation if necessary for your environment.
10. Have two HDX systems make a multi-point call using the DMA system.
    a. Test both network protocols (IPv4 and IPv6) if necessary for your environment.
11. Review the CMA system monitoring of system.

A

Restricted Polycom Functionality in Maximum Security Environments

Polycom disables or restricts various functionality when running a product in a maximum security environment. In some cases, administrators and users will see disabled menus or fields; while in other cases, entire sections of functionality is unavailable.

This chapter provides a reference to functionality that is restricted or disabled when running in a maximum security environment.

This chapter includes the following sections:

Polycom CMA System

This Polycom CMA system v5.2.0J release includes only some of the functionality found in the more commercial but less secure CMA system releases, and there are many operational differences.

For complete documentation, see the *Polycom CMA System Deployment Guide for Maximum Security Environments.*

Unsupported Features

Polycom CMA system v5.2.0J release does not include support for:

- Operation on Polycom CMA 4000 hardware
- Gatekeeper functionality
- Redundant configurations

- An external database
- ISDN scheduling
- Global Address Book
- Standard (scheduled) management and monitoring of endpoints
- Presence
- SNMP
- Remote desktop
- Integration with Microsoft Exchange for calendaring
- Integration with Microsoft Office Communications Server
- Polycom CMA Desktop clients
- Polycom Scheduling Plugins for Microsoft Outlook and IBM Lotus Notes
- Least Cost Routing

Supported Polycom Integrations

Polycom CMA system v5.2.0J release does include support for:

- Polycom HDX endpoints running version 2.7.0_J operating in dynamic management mode and configured at Maximum Security level.
- Multipoint conferencing on Polycom RMX 1500/2000/4000 conferencing platforms running version 7.5.0J and configured at Maximum Security level.

Polycom HDX System

When running Polycom HDX software version 2.7.0_J and set to the Maximum Security level, these 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
- Restrictions for some dialing features, such as last number dialed, and recent calls, which cannot 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

For complete documentation, see the *Polycom HDX System Deployment Guide for Maximum Security Environments.*

Polycom RMX System

When running Polycom RMX software version 7.5.0.J and set to the Maximum Security level, these features are disabled, restricted, or unavailable:

- Connection to Alternate Management Network via LAN3 port
- SUPPORT user
- Auditor user
- Chairperson user
- Connections to External Databases
- IP Sec security protocols
- ISDN Cascade
- Serial connection
- Modem connection
- MPM cards
- SIP signalling is not supported.
- SIP security (Digest)
- SIP TLS
- QoS with IPv6
- Recording link
- SNMP
- SSH server.
- USB key configuration
- Web link (Hyperlink in Participant Properties dialog box)

For complete documentation, see the *Polycom RMX System Deployment Guide for Maximum Security Environments.*

Polycom DMA System

When running Polycom DMA system set to the Maximum Security level, these features are disabled, restricted, or unavailable:

- The DMA system H.323 gatekeeper only supports IPv4.
- All unencrypted protocols and unsecured access methods are disabled.
- For all server-to-server connections, the system requires the remote party to present a valid X.509 certificate, and it presents its certificate for the remote party to validate.
- SIP signaling is not supported.
- **Calendaring service** can't be enabled, and the Polycom CMA system doesn't support virtual meeting rooms (VMRs) created by the Polycom Conferencing Add-in for Microsoft Outlook.
- Integration with a Polycom CMA system is not supported.
- On the **Login Banner** page, **Enable login banner** is selected and can't be disabled.
- On the **Sessions** page, the **Terminate Session** action is not available.
- If the system is integrated with an enterprise directory, only one local user can have the Administrator role, and no local users can have the Provisioner or Auditor role.

  If there are multiple local administrators when you enable **Maximum security**, the system prompts you to choose one local user to retain the Administrator role. All other local users, if any, become conferencing users only and can't log into the management interface.
- If the system is not integrated with an enterprise directory, each local user can have only one assigned role (Administrator, Provisioner, or Auditor).

  If some local users have multiple roles when you enable **Maximum security**, they retain only the highest-ranking role (Administrator > Auditor > Provisioner).
- Local user passwords have stricter limits and constraints (each is set to the noted default if below that level when you enable **Maximum security**):
  - Minimum length is 8-15 characters (default is 9).
  - Must contain 1 or 2 (default is 2) of each character type: uppercase alpha, lowercase alpha, numeric, and non-alphanumeric (special).
  - Maximum number of consecutive repeated characters is 1-4 (default is 2).
  - Number of previous passwords that a user may not re-use is 8-16 (default is 10).
  - Minimum number of characters that must be changed from the previous password is 1-4 (default is 4).

  - Password may not contain the user name or its reverse.
  - Maximum password age is 30-180 days (default is 60).
  - Minimum password age is 1-30 days (default is 1).
- Other configuration settings have stricter limits and constraints (each is set to the noted default if below that level when you enable **Maximum security**):
  - Session configuration limits:
    - Sessions per system is 8-80 (default is 40).
    - Sessions per user is 1-10 (default is 5).
    - Session timeout is 5-60 minutes (default is 10).
  - Local account configuration limits:
    - Local user account is locked after 2-10 failed logins (default is 3) due to invalid password within 1-24 hours (default is 1).
    - Locked account remains locked either until unlocked by an administrator (the default) or for a duration of 1-480 minutes.

For complete documentation, see the *Polycom DMA System Deployment Guide for Maximum Security Environments.*