POLYCOM®

Polycom® DMA™ 7000 System Deployment Guide for Maximum Security Environments

v. 2.1.1J | February 2012 | 3725-76304-001A

Trademark Information

Patent Information

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

End User License Agreement

Use of this software constitutes acceptance of the terms and conditions of the Polycom DMA 7000 system end-user license agreement (EULA).

The EULA is included in the release notes document for your version, which is available on the Polycom Support page for the Polycom DMA 7000 system.

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

Contents

1

Before You Begin

The Polycom® Distributed Media Application™ (DMA™) 7000 system v. 2.1.1J release provides the special features and functionality required to deploy the system into a maximum security environment. This deployment guide describes the recommended procedure for doing so.

This chapter provides important information that you should review before proceeding. In particular, be sure you fully understand the information in "The Consequences of Enabling Maximum Security Mode" on page 2.

It's important to note that the Polycom DMA system v. 2.1.1J release is not a maximum-security-only release. During initial setup, it can be configured for a lower security level (the **High security** or out-of-the-box default **Custom security** settings). You can switch the system to **Maximum security** at any time after initial installation.

This flexibility allows you to, for instance, install certificates and then switch to **High security** in order to "test drive" their operation before you make the irreversible switch to **Maximum security**.

This guide assumes that you intend to enable **Maximum security** as part of the system deployment process. But this step is one of several in configuring the system for a maximum security environment, and it's most conveniently done after several other steps have been completed.

Assumptions

This guide is written for a technical audience. You will be:

- Installing and configuring the system servers.
- Configuring networking, signaling, and system security.
- Installing certificates.
- Integrating with your enterprise directory server.

This guide assumes that you're starting with a new two-server Polycom DMA system that's being installed for the first time.

Documentation Resources

In addition to this guide, the available documentation that describes the Polycom DMA system includes:

- *Polycom DMA System Quick Start Guide*
- *Polycom DMA System Release Notes*
- *Polycom DMA System Operations Guide*
- Online help. In the management interface, select **Help > Help Contents** to access the entire help system, or click  on any page or the **Help** button in any dialog box to see the specific help topic for that location.

For more information about partner product interoperability, refer to the partner deployment guides.

For information about specific certifications, refer to:

`www.polycom.com/usa/en/solutions/industry_solutions/government/certification_accreditation.html`

The Consequences of Enabling Maximum Security Mode

Enabling the **Maximum security** setting is irreversible and has the following significant consequences:

- All unencrypted protocols and unsecured access methods are disabled.
- The boot order is changed so that the servers can't be booted from the optical drive or a USB device.
- A BIOS password is set.
- The port 443 redirect is removed, and the system can only be accessed by the full URL (`https://<IP>:8443/dma7000`, where *<IP>* is one of the system's management IP addresses or a host name that resolves to one of those IP addresses).
- For all server-to-server connections, the system requires the remote party to present a valid X.509 certificate. Either the Common Name (CN) or Subject Alternate Name (SAN) field of that certificate must contain the address or host name specified for the server in the Polycom DMA system.

  Polycom RMX MCUs don't include their management IP address in the SAN field of the CSR (Certificate Signing Request), so their certificates identify them only by the CN. Therefore, in the Polycom DMA system, an RMX MCU's management interface must be identified by the host name or FQDN specified in the CN field, not by IP address.

  Similarly, an Active Directory server certificate often specifies only the FQDN. Therefore, in the Polycom DMA system, the enterprise directory must be identified by FQDN, not by IP address.

- SIP signaling is not supported.
- Superclustering is not supported.
- Juniper SRC integration is not supported.
- **Calendaring service** can't be enabled, and the Polycom DMA 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.
- On the **Tools** menu, **Top** is removed.
- In the **Add User** and **Edit User** dialog boxes, conference and chairperson passwords are obscured.
- After **Maximum security** is enabled, users must change their passwords.
- 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 15-30 characters (default is 15).
  - 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.
- Software build information is not displayed anywhere in the interface.
- You can't restore a backup made before **Maximum security** was enabled.
- File uploads may fail when using the Mozilla Firefox browser unless the proper steps have been taken. See below.

Enabling File Uploads in Maximum Security with Mozilla Firefox

The Mozilla Firefox browser uses its own certificate database instead of the certificate database of the OS. If you use only that browser to access the Polycom DMA system, the certificate(s) needed to securely connect to the system may be only in the Firefox certificate database and not in the Windows certificate store. This causes a problem for file uploads.

File upload via the Polycom DMA system's Flash-based interface bypasses the browser and creates the TLS/SSL connection itself. Because of that, it uses the Windows certificate store, not the Firefox certificate database. If the certificate(s) establishing trust aren't there, the file upload silently fails.

To avoid this problem, after the Polycom DMA system's certificates are installed, you must import the needed certificates into Internet Explorer (and thus into the Windows certificate store). And, when accessing the system with Firefox, you must use its fully qualified host name.

First, start Internet Explorer and point it to the Polycom DMA system. If you don't receive a security warning, the needed certificates are already in the Windows certificate store.

If you receive a warning, import the needed certificates. The details for doing so depend on the version of Internet Explorer and on your enterprise's implementation of certificates.

In Internet Explorer 7, elect to continue to the site. Then click **Certificate Error** to the right of the address bar and click **View Certificates** to open the **Certificate** dialog box. From there, you can access the Certificate Import Wizard.

The entire trust chain must be imported (the system's signed certificate, intermediate certificates, if any, and the root CA's certificate). When importing a certificate, let Internet Explorer automatically select a certificate store.

Intrusion Detection Systems

The Polycom DMA system has both HIDS (Host Intrusion Detection System) and NIDS (Network Intrusion Detection System) enabled at all times, regardless of security settings.

HIDS

The Polycom DMA system uses the Linux kernel's iNotify file/directory change notification system to monitor the enire file system for change events, with the exclusion of a short list of files and directories that are expected to change (logs, temporary files, etc.).

Any change to one of the monitored files or directories (including attribute change, write, delete, move, and create) is recorded in `/var/logs/nids.log`.

NIDS

The Polycom DMA system uses iptables for access control. For each different kind of packet processing, there is a table containing chained rules for the treatment of packets. Every network packet arriving at or leaving from the computer must pass the rules applicable to it.

Depending on the nature of the suspect packets, the rules may reject, drop, or limit their arrival rate (dropping the rest)..

The system adds a `hosts.deny` file when Linux console access is disallowed (as is the case when **Maximum security** is enabled).

Details of each blocked access attempt are recorded in `/var/logs/nids.log`.

2

Polycom® DMA™ System Initial Server Setup

This chapter describes the steps required to perform the installation and initial setup of a Polycom® Distributed Media Application™ (DMA™) two-node server cluster.

The servers in a two-node cluster must be co-located. If possible, use the provided 18" crossover cable to connect them to each other.

At the end of this chapter, you will have successfully logged into the Polycom DMA system, completed the network and time server configuration, and be ready to finish configuring the system, including configuring it for a maximum security environment.

Collect Necessary Materials

Before you install a Polycom DMA system, collect these materials:

- *Polycom DMA System Release Notes*
- Polycom DMA system server shipment
- Completed First-Time Setup Worksheet (see page 8)
- PC running Microsoft® Windows® (XP Pro, Vista, or 7) with:
  - Ethernet port
  - Java™ 1.6 or newer
  - Microsoft Internet Explorer® 7 or newer, or Mozilla Firefox® 3 or newer
  - Adobe® Flash® Player 9.0.124 or newer

Complete the First-Time Setup Worksheet

Before you begin system setup, fill out the **My System Values** column of this worksheet.

First-Time Setup Worksheet

System Configuration Information	My System Values	Description
One node or two?		Always two for this version of the system.
Split management and signaling interfaces or combined?		If the same network will be used for both management (administrative access) and signaling, skip the signaling IP addresses and the Shared Signaling Network Settings section below.
IPv4, IPv6, or both?		Complete the appropriate address fields below for your choice. Note: Some system features are not supported or not fully tested in an IPv6 environment, including embedded DNS, site topology, and Juniper Networks SRC integration.
Node 1		
Management host name		Local host name of the first Polycom DMA system server's management (or combined) interface. Must be a valid host name: the letters a - z (case-insensitive), digits 0 - 9, and internal hyphens are allowed.
Management IPv4		Static, physical IP address(es) for the first server's management (or combined) interface.
Management IPv6		
Signaling IPv4		Static, physical IP address(es) for the first server's signaling interface.
Signaling IPv6		
Node 2		
Management host name		Local host name of the second server's management (or combined) interface. Must be a valid host name: the letters a - z (case-insensitive), digits 0 - 9, and internal hyphens are allowed.
Management IPv4		Static, physical IP address(es) for the second server's management (or combined) interface.
Management IPv6		

System Configuration Information	My System Values	Description
Signaling IPv4		Static, physical IP address(es) for the second server's signaling interface.
Signaling IPv6		
Shared Management Network Settings		Used for both management and signaling in a combined network configuration.
Virtual management host name		Local host name of the virtual management host.
Virtual management IPv4		IP address(es) of the virtual management host.
Virtual management IPv6		
Subnet mask		Network mask that defines the subnetwork of the system's management interface.
IPv6 prefix length		IPv6 CIDR value.
IPv4 gateway		IP address of the gateway server used to route network traffic outside the subnet.
Auto-negotiation		Yes or no. If no, indicate speed and full or half duplex.
Shared Signaling Network Settings		Needed only if signaling network is separate.
Virtual signaling host name		Local host name of the virtual signaling host.
Virtual signaling IPv4		IP address(es) of the virtual signaling host.
Virtual signaling IPv6		
Subnet mask		Network mask that defines the subnetwork of the system's signaling interface.
IPv6 prefix length		IPv6 CIDR value.
IPv4 gateway		IP address of the gateway server used to route network traffic outside the subnet.
Auto-negotiation		Yes or no. If no, indicate speed and full or half duplex.

System Configuration Information	My System Values	Description
General System Network Settings		
DNS search domains		Space- or comma-separated list of fully qualified domain names to query on the DNS servers to resolve host names (optional). The system domain is added automatically; you don't need to enter it.
DNS 1		IP address of the primary Domain Name System server. Optional, but strongly recommended. At least one DNS server is required in order to import global groups from an enterprise directory and for CMA integration.
DNS 2		IP address of a second DNS server (optional).
DNS 3		IP address of a third DNS server (optional).
Domain		Fully qualified domain name for the system (optional).
Signaling DSCP		The DSCP value is used to classify packets for quality of service (QoS) purposes. If you're not sure what value to use, leave the default of 0.
Default IPv6 gateway		The interface to use for accessing the IPv6 gateway, generally eth0. Optionally, the gateway's address and the interface, specified as: <*IPv6_address*>%eth0
Default IPv4 gateway		In split network configuration, select which of the two networks' gateway servers is the default. Your choice depends on your network configuration and routing. Typically, unless all the endpoints, MCUs, and other devices that communicate with the system are on the same subnet, you'd select the signaling network. **Caution:** When initially configuring the servers, set this to Management to ensure that you can log into the management interface after the system reboots. You can change the setting to Signaling later.

System Configuration Information	My System Values	Description
System Time		
Time zone		Time zone in which the system resides.
NTP server #1		IP address of the primary NTP time server (optional, but strongly recommended).
NTP server #2		IP address of a second NTP time server (optional).
NTP server #3		IP address of a third NTP time server (optional).
Routing Configuration		If you know you need to set up a special network routing rule or rules, specify the information below for each rule. In a split network configuration, routing rules are necessary for proper routing of network traffic.
Destination		The destination network mask for this route.
Length		The destination CIDR subnet.
Interface		In split network configuration, specify the interface for this route.
Via		IP address of router for this route. Optional, and only needed for non-default routers.

Unpack and Install the Hardware Components

The Polycom DMA system uses either one or two Polycom-branded Dell servers. Unpack and install the servers as described in the *Polycom DMA System Quick Start Guide* included in the shipment, but don't connect the Polycom DMA servers to the network (step 8) if you're installing in a secure environment.

If the *Quick Start Guide* isn't readily available, follow the procedure below.

To unpack and install the hardware

1 If you purchased Polycom RMX conference platforms (MCUs) with your Polycom DMA system servers, unpack, install, and securely deploy them as described in the *Polycom RMX 2000/4000 Deployment Guide for Maximum Security Environments*.

2 Examine the Polycom DMA system shipping containers for damage. Polycom is not responsible for damage sustained during shipment of this product.

3 Open and review the container packing slips.

4 Open the containers and examine the contents. A two-node Polycom DMA system shipment includes two containers each holding:

- 1 Polycom DMA system server
- 2 power cords
- 1 rack-mount kit (four-post)
- 1 bezel key
- 1 server documentation set
- 1 copy of the *Polycom DMA System Quick Start Guide*
- 1 Polycom DMA system installation disk
- 2 crossover Ethernet cables, short and long
- Your license documents

If you ordered the optional 2-post rack mounting kit, it's in a separate box.

5 Examine the contents for damage.

If you find damage, file a claim with the delivery carrier. Polycom is not responsible for damage sustained during shipment.

6 Remove all of the components from their containers.

7 Install the Polycom DMA servers according to the server documentation. To rack-mount a server, refer to the *Rack Installation Guide* and use the brackets provided.

Do not connect the servers to the enterprise network or turn them on at this time.

8 Remove the bezel(s) from the servers.

Secure the Polycom DMA System Servers

When you switch to maximum security mode (page 20), the servers' BIOS settings are changed to prevent them from being booted from the DVD drive or a USB device. In addition, a BIOS password is set (if not already present) to prevent unauthorized persons from reversing these BIOS changes.

But occasionally, a BIOS change fails to be implemented on reboot. To make absolutely certain that the servers are secure, we recommend manually securing them by performing the procedure below on each server.

To secure a Polycom DMA system server

1. Attach a USB keyboard and monitor to the server and start it.
2. During the boot sequence, press **F2** to enter the **System Setup** menu.

   The system displays an **Entering Setup** message.

- To view the **System Setup** help file, press **<F1>** .
- For most of the options, the changes that you make are recorded but don't take effect until you restart the system.

3. Use the arrow keys to navigate to the **Boot Settings** sub-menu and press **ENTER** to select it. Then navigate to **Boot Sequence** and press **ENTER**.
4. Disable the **SATA Optical Drive** and **Embedded NIC 1**.
5. Return to the main **System Setup** menu, select **Integrated Devices**, and make the following changes:
   - Set **User Accessible USB Ports** to **All Ports Off**.
   - Set **Internal USB Port** to **Off**.
6. Return to the main **System Setup** menu, select **System Security**, and make the following changes:
   - Set **System Password** to **Not Enabled**.
   - Select **Setup Password** and enter and confirm a system setup password that meets your site password requirements.
   - Set **Password Status** to **Locked**.
7. Return to the main **System Setup** menu, select **Serial Communication**, and set **Serial Communication** to **Off**.
8. Exit and save the changes.

   The server reboots.
9. Turn the server off.

Configure the Polycom DMA System servers

The normal configuration procedure uses the Polycom DMA USB Configuration Utility on the USB memory stick shipped with the system. In an environment where USB storage devices aren't permitted, the following procedure enables you to complete the initial setup using only a laptop PC and an Ethernet cable.

This is possible because Polycom DMA system servers are shipped with default network settings that you can use to connect to the system. The settings are:

IP address: `192.168.1.101`

Subnet mask: `255.255.255.0`

Default gateway: `192.168.1.1`

To configure the Polycom DMA system servers using a laptop PC

1. Follow the unpack and install procedure (page 11) and the procedure for manually securing the servers (page 13). ***Do not*** connect the servers to the enterprise network.
2. Start the first server (the one you want configured as Node 1).

   The server boots, which takes several minutes. When it's finished, the front panel LCD displays **DMA Installed**. This indicates that the system software is installed, but its network and time settings aren't configured.
3. Configure the network settings on your laptop to put it on the same network segment as the Polycom DMA system servers (see the server's default settings above). For instance, you can use the following settings:

   IP address: `192.168.1.20`

   Subnet mask: `255.255.255.0`

   Default gateway: `192.168.1.1`
4. Connect an Ethernet cable between your laptop and the GB 1 interface of the first server (the one you want configured as Node 1).

   You can use the cable that will later connect the server to the switch (enterprise network). Be sure you connect to the server's GB 1 interface, not the GB 2 or GB 3 interface.
5. On the laptop, point your browser to `http://192.168.1.101` (if a security certificate warning appears, ignore it) and log in with user ID **`admin`** and password **`admin`**.

   The Polycom DMA system's management interface appears, displaying the **Dashboard**.
6. Go to **Configuration > System > Network** and enter the network values from the First-Time Setup Worksheet.

7 If you need to set up a special network routing rule or rules, click **Routing Configuration**, create the rule(s), and click **OK**.

In a split network configuration, routing rules are necessary for proper routing of network traffic. If you aren't sure what rule or rules you need, consult the appropriate IT staff or network administrator for your organization.

Depending on your organization's policies, you may also need to configure your network infrastructure so that access to the system's management interface is limited to authorized IP addresses. Typically, this is handled via Access Control Lists (ACLs) in network routers.

8 Click **Update**. When asked to confirm restarting the system, click **Yes**.

The system begins to reboot.

9 While the server is rebooting, do the following:

a Disconnect the Ethernet cable from the laptop and connect the server's GB 1 Ethernet port to the enterprise network to be used for management (or combined) traffic.

This is the eth0 network interface, which must be used for this purpose.

b For a split network configuration, connect the GB 3 Ethernet port to the network to be used for signaling traffic.

This is the eth2 network interface, which must be used for this purpose.

The reboot process takes several minutes. When it's finished, the front panel LCD displays **DMA Ready**.

10 From a PC with network access to the Polycom DMA system, point your browser to the system's virtual IP address and log in with user ID **admin** and password **admin**.

11 Go to **Configuration > System > System Time** and do the following:

a Select the correct **System time zone** for your location.

We strongly recommend selecting the best location-specific setting, not one of the generic GMT offset settings.

b Leave **Auto Adjust For Daylight Savings** checked (deselecting this may cause problems, especially with NTP servers).

c Under **NTP servers**, enter the IP addresses (or domain names) for the time servers from the First-Time Setup Worksheet.

We strongly recommend specifying at least one and preferably three time servers. Use NTP stratum 3 quality time servers, if possible.

d Click **Update**. When asked to confirm restarting the system, click **Yes**.

The system reboots, which takes several minutes. When it's finished, the front panel LCD displays **DMA Ready**.

12 Verify that Node 2 is off and do the following:

a Connect the GB 1 Ethernet port of the second server (Node 2) to the enterprise network to be used for management (or combined) traffic. For a split network configuration, connect the GB 3 port to the network to be used for signaling traffic.

b Connect one of the provided crossover cables between the GB 2 ports of the two servers.

c Verify that the first server (Node 1) is running and its front panel LCD displays **DMA Ready**.

d Turn on the second server (Node 2).

The second server boots, detects and gets its configuration settings from Node 1, and joins the cluster. When done, both servers' LCDs display **DMA Clustered**.

13 Log back into the system and complete your system setup and security configuration as described in the following chapter.

3

Polycom® DMA™ System Maximum Security Deployment

This chapter describes the tasks required to complete the deployment of a Polycom® DMA™ v. 2.1.1J system in a maximum security environment. It assumes you've completed the physical installation and initial setup tasks in the preceding chapter.

The task descriptions refer you to the following information resources that provide more detailed descriptions and procedures:

- Once you're logged into the system, the online help provides access to all the additional information you need. Click on any page or the **Help** button in any dialog box to see the specific help topic for that location.
- Alternatively, the *Polycom DMA System Operations Guide* (pdf) contains the same information as the online help in a printable format.

Completing the system configuration, including properly securing the system, involves the following tasks:

- Add DNS records for the system to your DNS servers. (This can be done at any time prior to or during system installation and configuration.)
- Create a proper local user account with the system administrator user role, log in as that user, and then delete the default admin user.
- License the system.
- Configure signaling.
- Install security certificates.
- Set the system's **Security Configuration** to **Maximum security**.
- Change the single local administrator's password.
- Configure virus scans and virus signature file updates.
- Review and modify, if necessary, various security-related settings.
- Integrate with Active Directory, log into the system using the AD service account, and assign system roles to the appropriate AD users.
- Add Polycom RMX MCUs to the system.

- Verify system functionality.
- Enable, if necessary, certificate validation for user login sessions.

Add DNS Records for the Polycom DMA System

In order to access your Polycom DMA system by its host names instead of by IP addresses, you must create A (*alias*) records (for IPv4) and/or AAAA records (for IPv6) on your DNS server.

A two-server system has three host names and IP addresses (one virtual and two physical) for the management or combined interface, and three more for the signaling interface in a split network configuration. We recommend that you create an alias record for each. See "Add Required DNS Records for the Polycom DMA System" in the online help or *Polycom DMA Operations Guide*.

Create Local System Administrator Account

In maximum security mode, if the Polycom DMA system is integrated with Active Directory, only one local user is permitted, and that user must have the Administrator role. If you're configuring the system in this manner, presumably this local administrator login will serve only as a safety mechanism, and you have procedures for securing the credentials for that user.

Whether that's the case or not, perform the procedure below as soon as possible after installing your system to eliminate a serious security risk.

To remove the default admin account and create a more secure local account with administrative privileges

1. Log in as admin and go to **Operations > Users**.

   The **Users** page appears.

2. Create a local user account with the Administrator role. See "Users Procedures" in the online help or *Polycom DMA Operations Guide*.
3. Log out and log back in using the new local account.
4. Go to **Operations > Users** and delete the default admin account. See "Users Procedures" in the online help or *Polycom DMA Operations Guide*.

License the System

To license the system

1 Go to **Configuration > System > License**.

The **License** page appears.

2 Follow the procedures for requesting software activation key codes and entering them, described in "Add Licenses" in the online help or *Polycom DMA Operations Guide*.

Configure Signaling

In maximum security mode, the Polycom DMA system supports only H.323 signaling, not SIP.

To configure H.323 signaling

1 Go to **Configuration > System > Signaling Configuration**.

The **Signaling Configuration** page appears.

2 Enable H.323 signaling and optionally register to (or neighbor with) a gatekeeper, following the procedure described in "Configure Signaling" in the online help or *Polycom DMA Operations Guide*.

Install Security Certificates and Enable OCSP

The steps for installing the necessary security certificate(s) depend on the certificate procedures used at your organization. For instance, if your certificate authority (CA) doesn't provide a full certificate chain in response to a certificate signing request (CSR), you need to install the CA's certificate(s) into the Polycom DMA system prior to adding the system's signed certificate.

If you're installing the Polycom DMA system into a highly secure environment, presumably you're knowledgeable about X.509 certificates and their use (or have access to someone who is). Nevertheless, we suggest that you review "Management and Security Overview" in the online help or *Polycom DMA Operations Guide* to familiarize yourself with the forms of certificates that can be installed in the Polycom DMA system and how the system uses certificates.

See "Certificate Procedures" in the online help or *Polycom DMA Operations Guide* for step-by-step instructions for the following tasks:

- Install your CA's public certificate (and any intermediate certificates).

- Create a CSR to submit to the CA.
- Install the public certificate signed by the CA that identifies the Polycom DMA system.

The CSR generated by the system automatically includes all the host names and IP addresses (virtual and physical) by which the system can be accessed, using the Subject Alternate Name (SAN) field. If your organization's procedure for creating a certificate doesn't use the system-generated CSR, be sure to specify the SAN entries so that the certificate is valid regardless of which address is used to access the system.

See "Certificate Management" in the online help or *Polycom DMA Operations Guide* for information about enabling the Online Certificate Status Protocol (OCSP). Typically, you only need to select **Enable OCSP** (on the **Certificate Management** page) and click **Store OCSP configuration**.

If your organization uses a specific OCSP responder instead of the responder in the certificate's AuthorityInfoAccess (AIA) field, specify that responder in the **OCSP responder URL** field. **OCSP certificate** lets you select a certificate to be used to authenticate the response messages.

With OCSP enabled, the Polycom DMA system attempts to verify the status of all certificates presented to it. If it's unable to connect to the OCSP responder or doesn't receive a response indicating that the certificate is good, the system rejects the certificate and refuses the connection.

Set Security Configuration to Maximum Security

Once certificates are in place (and assuming that all devices with which the Polycom DMA system communicates also have valid certificates signed by a CA that the Polycom DMA system trusts), you're ready to switch the system into maximum security mode.

Enabling **Maximum security** is ***irreversible*** and has significant consequences (see "The Consequences of Enabling Maximum Security Mode" on page 2). Don't choose this setting unless you're certain that you're ready to proceed.

You may wish to "test drive" secure communications first by switching to **High security**, which is reversible. In that mode, you can confirm that all server connections work and that there are no certificate or communications protocol problems before performing the irreversible procedure below.

To switch to maximum security mode

1. Go to **Configuration > System > Security Configuration**.
2. Click **Maximum security**.

   We recommend leaving **Skip certificate validation for user login sessions** enabled for now. If your environment requires user certificates, this setting can be turned off later, after verifying the functionality of the system.
3. Click **Update**.

   A dialog box informs you that only one local administrator is permitted in maximum security mode and prompts you to confirm. Another dialog box informs you that the change is irreversible, lists some of the consequences, and prompts you to confirm again.
4. Confirm at both prompts.

   The system reboots, which takes several minutes. When you log back in, you're prompted to change your password.
5. Change your login password.

If there is no existing BIOS password on the servers when the system is placed into maximum security mode, doing so sets a default BIOS password (`B1O5pa55wOrd`). If you performed the recommended procedure to manually secure the servers (page 13), a BIOS password already exists, and it remains unchanged.

To manually change the BIOS password on a Polycom DMA server

1. Attach a USB keyboard and monitor to the server and restart it.
2. During the boot sequence, press **F2** to enter the **System Setup** menu.
3. If prompted to **Enter Setup Password**, enter your current BIOS password (if you don't remember it, contact Polycom Global Services for instructions on how to access the **System Setup** menu).
4. Use the arrow keys to navigate to the **System Security** sub-menu and press **ENTER**. Then navigate to **Setup Password** and press **ENTER**.
5. Enter the same value in the **Enter Password** and **Confirm Password** fields (to remove the BIOS password, press **ENTER** without typing a new password value for both fields).
6. Save your changes and exit BIOS setup.

   The system reboots.

Configure Anti-virus Protection

On the **Anti-virus Protection** page, the anti-virus service is enabled, but you must configure scans and updates. Schedule anti-virus scans and signature file updates in accordance with your site policies.

> **Note**
>
> Anti-virus scans impose a significant burden on the system that could impact system performance. Schedule system scans for times when the system is in maintenance mode or when little or no conferencing activity is anticipated.

To configure anti-virus scans:

1. Go to **Configuration > System > Anti-virus**.
2. Verify that the McAfee® anti-virus service is enabled and **Enable scan of uploaded files** is selected.
3. Select **Enable scheduled system scans**.
4. Click **Schedule** and set the system scanning schedule.
5. Click **Update**.

Scan results are logged in the server logs. If a virus is detected, an alert appears in the management interface.

To configure anti-virus signature file updates:

1. To manually update using a signature file on your PC, click **Upload signature update file** and select the file to upload.

> **Note**
>
> Since the McAfee site doesn't support HTTPS connections, updating directly from the McAfee site isn't possible when **Maximum security** is enabled.

2. To schedule automatic updates from a secure local mirror, do the following:
   a. Use a program such as Wget to mirror the McAfee site (`http://update.nai.com/Products/CommonUpdater/`) on your mirror server.

      The mirror server must have a web server.

   b. Use a scheduled script or cron job to update the mirror at the interval you wish.

   c. On the **Anti-virus Protection** page, select **Update automatically from a local mirror** and specify the mirrored location's URL and login credentials.

d Click **Schedule** and set the update schedule.

3 Click **Update**.

Review and Modify (If Necessary) Security-Related Settings

Review the settings on the following **Configuration > System** pages and make any necessary changes (see the online help or *Polycom DMA Operations Guide* topic for each page for details about the settings):

- **Local Password Requirements**
- **Local Account Configuration**
- **Session Configuration**
- **Login Banner**

The settings after switching to maximum security mode are the defaults for that mode, unless you previously chose a more stringent setting.

Integrate with Active Directory

Review the information in the "Connect to an Enterprise Directory" topic of the online help or *Polycom DMA Operations Guide*, and then integrate the system with your Active Directory as described in "Enterprise Directory Integration Procedure."

In step 4a, you can only use an IP address if your AD server's certificate has the IP address entries in the SAN field. Otherwise, you must specify the host name or FQDN in the CN field, or use the **Auto-discover from FQDN** option. We strongly recommend using the auto-discover option.

At the end of the integration procedure, you should have completed the following:

- Successfully connected the system to your Active Directory and retrieved directory data.
- Successfully generated conference room IDs (virtual meeting rooms, or VMRs) for the enterprise users, if you elected to do so.
- Given Administrator privileges to your named enterprise account.
- Secured the service account.
- Verified that the results of the integration are satisfactory.

At this time, you can give access to the Polycom DMA system's management and operations interface (via the Administrator, Auditor, or Provisioner role) to the appropriate enterprise accounts. See "Users" and its subtopics in the online help or *Polycom DMA Operations Guide*.

You may wish to use enterprise groups to manage these role assignments. For instance, you can create a "Polycom DMA Administrators" group in Active Directory, which automatically confers the Administrator role on its members. See "Groups" and its subtopics in the online help or *Polycom DMA Operations Guide*.

In maximum security mode, a user may only have one of the three roles. Thus, a group you create for this purpose can only have one role. If an enterprise user is a member of more than one group conferring a role, only the lowest-ranking role (Administrator > Auditor > Provisioner) applies.

Add Polycom RMX MCUs to the System

If you haven't already done so, deploy your Polycom RMX MCUs as described in the *Polycom RMX 2000/4000 Deployment Guide for Maximum Security Environments*.

Then, add the MCUs to the Polycom DMA system. See "MCUs" and its subtopics in the online help or *Polycom DMA Operations Guide*.

A Polycom RMX MCU doesn't include its management IP address in the SAN field of its CSR, so the Polycom DMA system can only connect to it using the host name or FQDN specified in the CN field of the MCU's certificate.

For a maximum security environment, the administrative user ID with which the Polycom DMA system can log into the MCU must be a machine account created on the RMX MCU.

Note that the RMX MCU uses case-sensitive machine names (and thus FQDNs) when creating machine accounts.

Verify System Functionality

See "Test the System" in the online help or *Polycom DMA Operations Guide* for suggestions on verifying that the system is correctly configured and functioning properly. In particular, check that:

- All communications to and from the system are working and there are no certificate problems or other security issues either on the Polycom DMA system or on the systems to which it connects.
- Calls can reach the Polycom DMA system's physical signaling interface address(es).

- You can log into the management interface using any of the management interface addresses — physical or virtual, IPs or FQDNs.

If you receive a security warning from your browser, you need to install into your OS and/or browser certificate database the public certificate of the CA that signed the Polycom DMA system's certificate. If you use only the Mozilla Firefox browser, be sure to read "Enabling File Uploads in Maximum Security with Mozilla Firefox" on page 4.

Enable User Certificate Validation

If your environment requires user certificates for accessing the management interface, enable certificate validation for user login sessions.

To enable user certificate validation

1. Go to **Configuration > System > Security Configuration**.
2. Clear the **Skip certificate validation for user login sessions** check box and click **Update**.

   A dialog box notifies you that if you don't log back in within five minutes, the setting will be automatically turned back on.
3. Click **Yes**.

   The system logs you out and restarts, which takes a minute or so.
4. Log back into the system with a valid user certificate signed by a CA that the system trusts.

   If you can't log back in, there is a problem with the certificate your browser is presenting. After five minutes, the system turns **Skip certificate validation for user login sessions** back on. Resolve the problem and repeat this procedure.