



Military Unique Deployment Guide

v. 6.0.1 | January 2014 | 3725-76304-001B1

Polycom[®] DMA[®] 7000 System Deployment Guide for Maximum Security Environments



Trademark Information



POLYCOM® 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.



Java is a registered trademark of Oracle America, Inc., and/or its affiliates.

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.

Support Information

For support on your Polycom systems, contact Polycom Global Services at 1-888-248-4143 or go to the [Polycom Support Contact](http://support.polycom.com/PolycomService/support/us/support/Contact_Us.html) page (http://support.polycom.com/PolycomService/support/us/support/Contact_Us.html).

Documentation Feedback

Polycom appreciates your help as we work to improve its product documentation. Send your comments to videoinformationdesign@polycom.com.

© 2011-2014 Polycom, Inc. All rights reserved.

Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Contents

1	Before You Begin	1
	End User License Agreement	2
	Assumptions	2
	Documentation Resources	2
	Document Change History	3
	The Consequences of Enabling Maximum Security Mode	3
	Intrusion Detection Systems	6
2	Polycom® DMA® System Initial Server Setup	7
	Conditions of Fielding	8
	Complete the First-Time Setup Worksheet	8
	Collect the Necessary Materials	16
	Unpack and Install the Hardware Components	17
	Configure the Polycom DMA System Server(s)	19
	Secure the Polycom DMA System Servers	23
3	Polycom® DMA® System Maximum Security Deployment	25
	Add DNS Records for the Polycom DMA System	26
	Create Local System Administrator Account	26
	License the System	27
	Configure Signaling	27
	Install Security Certificates and Enable OCSP	27
	Configure Secure SIP or AS-SIP Connections	28
	Integrate the DMA System With a Local Session Controller (LSC)	29
	Configure Default AS-SIP Resource Priority Values for Dial-Out Conferencing	30
	Configure Encryption for Conference Templates	30
	Enable Secure Inbound SIP or AS-SIP VMR Connections	31
	Configure VMRs for Users	31
	Set Security Configuration to Maximum Security	32
	Review and Modify (If Necessary) Security-Related Settings	33
	Integrate with Active Directory	34

Add Polycom MCUs to the System	36
Verify System Functionality	36
Enable User Certificate Validation	37

Before You Begin

The Polycom® Distributed Media Application™ (DMA®) 7000 system 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 software, when configured per the guidance provided in this guide, is designed to meet the latest U.S. Department of Defense (DoD) security requirements for listing on the Unified Capabilities (UC) Approved Products List (APL) as maintained by the Defense Information Systems Agency (DISA) Unified Capabilities Connection Office (UCCO).

For more information about the UC APL process, please visit the [UCCO website](#).

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 3.

It’s important to note that this version of the Polycom DMA system 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.

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 at support.polycom.com.

Assumptions


This document is written for a technical audience. You must know the following:

- Basic computer and network system administration skills
- Physical installation and cabling of servers
- Network configuration, including IP addressing, subnets, gateways, domains, DNS, time servers, and possibly network routing
- The deployment plan for the Polycom DMA system being installed and the video conferencing/collaboration network of which it will be a part

If necessary, obtain the assistance of the appropriate IT or network administration personnel before proceeding.

Documentation Resources

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

- *Polycom DMA 7000 System Quick Start Guide*
- *Polycom DMA 7000 System Release Notes*
- *Polycom DMA 7000 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

Document Change History

This information is required for listing on the US Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL):

Doc Version	Release Date	Description
1.0	August 2011	Initial approved release
2.0	January 2014	Second release

To request information or submit comments about this document, please contact Polycom Global Services.

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 RealPresence® Collaboration Server and 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, a Polycom MCU's management interface must be identified by the 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.

- 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 to a Polycom RealPresence Resource Manager or CMA system is not supported.



A Polycom RealPresence Resource Manager system can be integrated to the DMA system, providing it with access to the DMA API and the ability to use the DMA system's pool of MCUs for scheduling and "Anytime" conferences.

But the reverse connection, integrating the DMA system to the RealPresence Resource Manager or CMA system for the purpose of obtaining site topology and user-to-device association data, is not supported.

- On the **Banner** page, **Enable login banner** is selected and can't be disabled.
- On the **Login Sessions** page, the **Terminate Session** action is not available.
- On the **Troubleshooting Utilities** 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 entire 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*.

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[®]) 7000 video collaboration infrastructure server or two-server cluster.



If your enterprise ordered two Polycom DMA servers, it's imperative that you know whether the intent is to set up a single co-located two-server DMA cluster or to set up two separate single-server DMA systems. Once you've configured two DMA servers as a two-server cluster, reconfiguring the servers as separate single-server DMA systems requires re-imaging the servers.

Before you start, we strongly suggest that you read "Introduction to the Polycom DMA System" in Chapter 1 and all of Chapter 2 of the *Polycom DMA 7000 System Operations Guide*, available for download from support.polycom.com.



The servers in a two-server cluster must be co-located, preferably in the same rack. If possible, use one of the Ethernet cables included in the server shipment to connect them to each other.

If you have a Polycom CMA system, be aware that a two-server DMA cluster is not functionally the same as a CMA system with a redundancy server, and the proper procedure for installation is not the same. We strongly recommend installing and configuring both servers of a two-server cluster as a single system, as described in this document.

If you have an existing fully configured and operational single-server system that you want to expand into a two-server cluster, use the procedure described in the "Adding a Second Server" section of the online help or *Polycom DMA 7000 System Operations Guide*, not this document.

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.

Conditions of Fielding

When the system is deployed into an operational environment, the following security measures (at a minimum) must be implemented to ensure an acceptable level of risk for the sites' Designated Approving Authority:

- a** The system must be incorporated in the site's PKI. If PKI is not incorporated, the following findings will be included in the site's architecture:
 - » APP3280 for DMA 7000 Rel. 6.0.1J
 - » APP3290 for DMA 7000 Rel. 6.0.1J
 - » APP3300 for DMA 7000 Rel. 6.0.1J
 - » APP3305 for DMA 7000 Rel. 6.0.1J
 - » NET0445 for DMA 7000 Rel. 6.0.1J
- b** The system must be integrated into the site's AD environment for authentication and authorization requirements.
- c** The site must be a STIG-compliant, PK-enabled workstation for management of the solution.
- d** The configuration must be in compliance with the Polycom DMA 7000 Rel. 6.0.1J military-unique features deployment guide.
- e** The site must register the system in the Systems Networks Approval Process Database (<https://snap.dod.mil/index.cfm>) as directed by the DSAWG and Program Management Office.

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
System IP type		Specify whether the system should support IPv4, IPv6, or both. If both, complete all the IP address information below. If only IPv4 or IPv6, complete only the corresponding fields below.
System server configuration		Specify whether you're installing a single-server system or a two-server system. For a single-server system, the Server 2 section below is not used. If you received two servers, be sure you've read and understood the cautions on page 7 and know whether you're setting up a co-located two-server DMA cluster or two separate single-server DMA systems.
System split network setting		Specify whether to combine or split the management and signaling interfaces. If the same network will be used for both management (administrative access) and signaling, the signaling IP addresses and Shared Signaling Network Settings section below are not used.

Caution: Choose split networking *only* if you need to restrict access to the management interface and SNMP to users on an isolated “non-public” network.

In most network environments, users accessing the management interface are on the same network as endpoints and other devices communicating with the DMA system, and they use the same physical and virtual IP addresses and the same network interface.

To split the network configuration, you must use different gateways and subnets for management and signaling, and separate physical connections for the management and signaling networks (eth0 for management, eth2 for signaling). In a split network configuration, routing rules are necessary for proper routing of network traffic.

If management and signaling traffic are combined on the same network (subnet), both use the same physical and virtual IP addresses and the same network interface.

If you aren't sure whether split networking is appropriate, possible, or necessary for this installation, consult the appropriate IT staff or network administrator for your organization.

System Configuration Information	My System Values	Description
Server 1		
Management host name		Local host name of the first (or only) Polycom DMA server's management (or combined) interface. Host names may contain only letters, numbers, and internal dashes (hyphens), and may not include a domain. The reserved values appserv* and dmamgk-* may not be used for host names.
Management IPv4		Static, physical IP address(es) for the first (or only) server's management (or combined) interface.
Management IPv6		
Signaling IPv4		Static, physical IP address(es) for the first (or only) server's signaling interface (if networking is split).
Signaling IPv6		
Server 2		
Management host name		Local host name of the second server's management (or combined) interface. Host names may contain only letters, numbers, and internal dashes (hyphens), and may not include a domain. The reserved values appserv* and dmamgk-* may not be used for host names.
Management IPv4		Static, physical IP address(es) for the second server's management (or combined) interface.
Management IPv6		
Signaling IPv4		Static, physical IP address(es) for the second server's signaling interface (if networking is split).
Signaling IPv6		

System Configuration Information	My System Values	Description
Shared Management Network Settings		In the combined network configuration (most network environments), users accessing the management interface are on the same network as endpoints and other devices communicating with the DMA system, and these settings are used for both management and signaling.
Virtual host name		Virtual host name and IP address(es) for the system's management (or combined) network interface. For a one-server configuration, these fields are disabled. (Exception: If only IPv6 is enabled, the system must have two addresses, so a single-server system must still have a virtual host name and IP address.) Host names may contain only letters, numbers, and internal dashes (hyphens), and may not include a domain. The reserved values appserv* and dmamgk-* may not be used for host names.
Virtual IPv4		
Virtual IPv6		
Subnet mask		IPv4 network mask that defines the subnetwork of the system's management or combined interface.
IPv6 prefix length		IPv6 CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask) that defines the subnetwork of the system's management or combined interface.
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. Note: Auto-negotiation is required if your network is 1000Base-T.
LAN Security Settings Caution: In a network that requires 802.1x authentication for servers (this is rarely the case), incorrect settings in this section and, if applicable, lack of the proper certificate(s) can make the system unreachable. Recovering from this situation requires connecting a laptop to the system using a crossover cable in order to access it.		
Enable 802.1x		Enables the system to authenticate this network interface to the LAN. Depending on the authentication method, the access credentials required may be either a user name and password (specified below) or a security certificate.

System Configuration Information	My System Values	Description
User name		The user name with which the system authenticates this interface.
Password		The password for the user name entered above.
EAP method		The Extensible Authentication Protocol method used to establish trust with the authentication server (this is also known as the outer authentication protocol).
Protocol		When a TLS tunnel is established with the authentication server, the protocol used within the tunnel (this is also known as the inner authentication protocol).
Shared Signaling Network Settings		Needed only if signaling network is separate (this is rarely the case; see the description for “System split network setting” on page 9). In that case, required even for single-server installation.
Virtual signaling host name		Virtual host name and IP address(es) for the system’s signaling network interface.
Virtual signaling IPv4		For a one-server configuration, these fields are disabled. (Exception: If only IPv6 is enabled, the system must have two addresses, so a single-server system must still have a virtual host name and IP address.) Host names may contain only letters, numbers, and internal dashes (hyphens), and may not include a domain. The reserved values appserv* and dmamgk-* may not be used for host names.
Virtual signaling IPv6		
Subnet mask		IPv4 network mask that defines the subnetwork of the system’s signaling interface.
IPv6 prefix length		IPv6 CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bits in the routing prefix mask) that defines the subnetwork of the system’s signaling interface.
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. Note: Auto-negotiation is required if your network is 1000Base-T.

System Configuration Information	My System Values	Description
LAN Security Settings Caution: In a network that requires 802.1x authentication for servers (this is rarely the case), incorrect settings in this section and, if applicable, lack of the proper certificate(s) can make the system unreachable. Recovering from this situation requires connecting a laptop to the system using a crossover cable in order to access it.		
Enable 802.1x		Enables the system to authenticate this network interface to the LAN. Depending on the authentication method, the access credentials required may be either a user name and password (specified below) or a security certificate.
User name		The user name with which the system authenticates this interface.
Password		The password for the user name entered above.
EAP method		The Extensible Authentication Protocol method used to establish trust with the authentication server (this is also known as the outer authentication protocol).
Protocol		When a TLS tunnel is established with the authentication server, the protocol used within the tunnel (this is also known as the inner authentication protocol).
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 addresses of up to three domain name servers. At least one DNS server is required. Your Polycom DMA system must be accessible by its host name(s), not just its IP address(es), so you (or your DNS administrator) must create A (address) resource records (RRs) for IPv4 and/or AAAA records for IPv6 on your DNS server(s). A/AAAA records that map each physical host name to the corresponding physical IP address and each virtual host name to the corresponding virtual IP address are mandatory.
DNS 2		
DNS 3		
Domain		Fully qualified domain name of the site to which the system belongs.

System Configuration Information	My System Values	Description
Signaling DSCP		<p>The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers on outbound packets associated with signaling traffic.</p> <p>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.</p>
Management DSCP		<p>The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers on outbound packets associated with management traffic.</p> <p>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.</p>
Default IPv6 gateway		<p>The IPv6 gateway's address and the interface used to access it, generally eth0, specified as: <code><IPv6_address>%eth0</code></p>
Default IPv4 gateway		<p>If management and signaling traffic are on separate networks, select which of the two networks' gateway servers is the default.</p> <p>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 and use the appropriate routing rules to enable access to the management interface.</p> <p>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.</p>

System Configuration Information	My System Values	Description
System Time		
Time zone		<p>Time zone in which the system is located. We strongly recommend selecting the time zone of a specific geographic location (such as America/Denver), not one of the generic GMT offsets (such as GMT+7).</p> <p>If you really want to use a generic GMT offset (for instance, to prevent automatic daylight saving time adjustments), note that they use the Linux/Posix convention of specifying how many hours ahead of or behind local time GMT is. Thus, the generic equivalent of America/Denver (UTC-07:00) is GMT+07, not GMT-07.</p>
NTP server #1		<p>IP address of the primary NTP time server. Use of time servers is strongly recommended. All the devices in your video conferencing deployment should use the same time servers to avoid potential problems caused by time differences among devices.</p>
NTP server #2		<p>IP address of a second NTP time server (optional, but strongly recommended).</p>
NTP server #3		<p>IP address of a third NTP time server (optional, but strongly recommended).</p>
<p>Routing Configuration</p> <p>Caution: In split network configuration, the management network and signaling network <i>must</i> use different gateways and subnets.</p>		<p>In a combined network configuration (the most common setup), where users accessing the management interface are on the same network as endpoints and other devices communicating with the DMA system, the operating system's underlying routing configuration is likely sufficient and special routing rules usually aren't needed.</p> <p>In a split network configuration, routing rules are necessary for proper routing of network traffic. If you know you need to set up a network routing rule or rules, specify the information below for each rule.</p> <p>If you aren't sure, consult the appropriate IT staff or network administrator for your organization.</p>
Destination host/network		<p>The IP address of the destination network host or segment.</p>

System Configuration Information	My System Values	Description
Prefix length		The CIDR (Classless Inter-Domain Routing) value that, together with the destination host/network address, defines the subnet for this route. For IPv4, a prefix length of 24 is equivalent to specifying a subnet mask of 255.255.255.0. A prefix length of 16 is equivalent to specifying a subnet mask of 255.255.0.0.
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.

Collect the Necessary Materials

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

- *Polycom DMA 7000 System Release Notes*
- Polycom DMA system server shipment
- Completed First-Time Setup Worksheet (see [page 8](#))
- PC running Microsoft® Windows® (XP Pro, Vista, or Windows 7) with:
 - 1280x1024 (SXGA) minimum display resolution; 1680x1050 (WSXGA+) or greater recommended
 - USB and Ethernet ports
 - Java™ 1.6 or newer
 - Microsoft Internet Explorer® 7 or newer, Mozilla Firefox® 3 or newer, or Google Chrome 11 or newer
 - Adobe® Flash® Player 9.0.124 or newer



The Polycom DMA system's Flex-based management interface requires Adobe Flash Player. For stability and security reasons, we recommend always using the latest version of Flash Player.

Even so, be aware that your browser's Flash plugin may hang or crash from time to time. Your browser should alert you when this happens and enable you to reload the plugin. In some cases, you may need to close and restart your browser.

In the Google Chrome browser, use the Adobe Flash plugin, not the built-in Flash support.

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 RealPresence® Collaboration Server or RMX conference platforms (MCUs) with your Polycom DMA system servers, unpack, install, and securely deploy them as described in the documentation for the model you purchased.
- 2 Examine the shipping containers for damage. If you find damage, file a claim with the delivery carrier. 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 single-server Polycom DMA system shipment includes:
 - 1 Polycom DMA system server
 - 1 copy of the *Polycom DMA 7000 System Quick Start Guide* (which contains this procedure)
 - 2 power cords
 - 1 rack-mount kit
 - 1 bezel assembly and key
 - 1 server documentation set
 - 1 Polycom DMA system recovery disk (included for recovery purposes; the software on the disk is already installed on the server)



If the system recovery disk is inserted into a PC that can boot from the optical drive and that PC is rebooted, the PC boots from the DMA system recovery disk, which performs a full disk wipe and a clean installation of the DMA system OS and software, destroying all existing data on the PC.

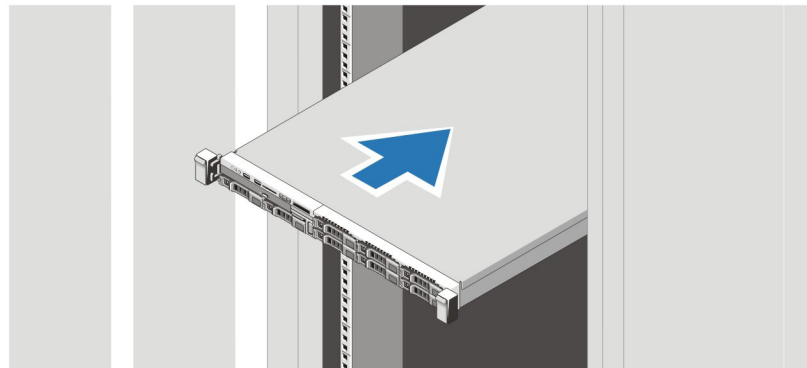
- 1 blank USB memory stick that, in an environment where it's permitted, can be used for the Polycom DMA USB Configuration Utility (available in the `/usb-gui` directory of the system recovery disk and at support.polycom.com)
- 1 USB memory stick with server diagnostic utilities (to be used only under the direction of Polycom Global Services)

- 1 server *Product Information Guide*
- 2 Ethernet cables, short and long (not used for a single-server system)

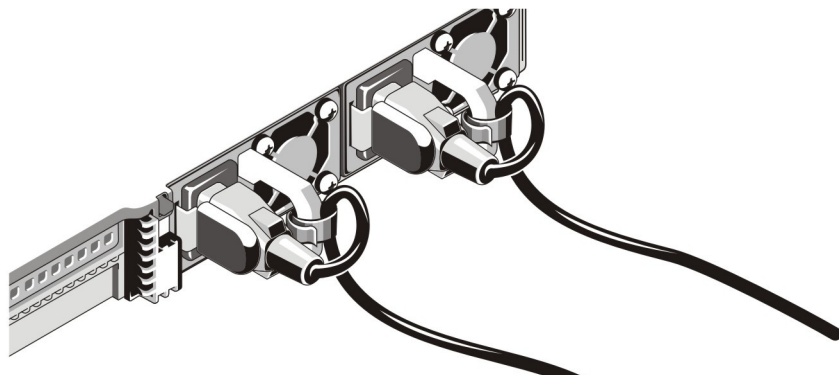
If you ordered the optional 2-post rack mounting kit, it's in a separate box.

A two-server system shipment contains a second set of the above items.

- 5** Examine the contents for damage. Again, if you find damage, file a claim with the delivery carrier.
- 6** Unpack your system and identify each item. Keep all shipping materials in case you need them later.
- 7** Assemble the rails and install the server(s) in the rack. To rack-mount a server, see the *Rack Installation Guide* (available at <http://support.dell.com/support/edocs/systems/peR620/en/index.htm>).



- 8** Connect the power cable(s) to the server(s).
- 9** (Optional) Attach the power cord retention bracket on the right bend of the power supply handle. Bend the power cable into a loop and attach to the bracket's cable clasp. Repeat for the second power supply.



- 10** Plug the other end of the cable into a grounded electrical outlet or separate power source such as an uninterruptible power supply (UPS) or a power distribution unit (PDU).



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

- 11 Remove the bezel(s) from the server(s).

Configure the Polycom DMA System Server(s)

The normal configuration procedure (documented in the *Polycom DMA 7000 System Getting Started Guide*) 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*



The Polycom DMA system software is already installed on the server(s), so the system recovery disk isn't needed to set up a new system. Using it overwrites the same software already on the server and needlessly lengthens the setup process. Put the disk away in a safe place in case it's ever needed to restore the system.

Exception: Your server shipment box contains two disks. One contains the software installed on the server and the other contains the official UC APL version, which was added before shipment but not installed on the server. If you are in a high-security environment that requires the UC APL version, use the UC APL software DVD to install that version of the software (on both servers of a two-server system).

To configure the Polycom DMA system server(s) using a laptop PC

- 1 Follow the unpack and install procedure ([page 17](#)) and the procedure for manually securing the servers ([page 23](#)). **Do not** connect the servers to the enterprise network.
- 2 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*

- 3 Connect an Ethernet cable between your laptop and the GB 1 interface of the first server.

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.

- 4 If you're replacing the system software on the server(s) with the official UC APL version (see the note on [page 19](#)), do the following:

- a Turn on the first (or only) server and insert the UC APL system recovery disk.

- b Reboot the first (or only) server. Leave the second server off.

The server boots from the DVD, and the installation commences. About 15-20 minutes later, the DVD ejects and the server reboots. 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.



If the LCD displays anything else or nothing, stop. Contact Polycom Global Services for assistance.

- c Go to step 6.

- 5 If you're not replacing the system software, start the first (or only) server.

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.



If the LCD displays anything else or nothing, stop. Contact Polycom Global Services for assistance.

- 6 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**.

- 7 Go to **Admin > Local Cluster > Network Settings** and select the **System IP type**, **System server configuration**, and **System split network setting** that you specified on the [First-Time Setup Worksheet](#).

Be sure you've read and understood the cautions on pages 7 and 9.



The settings you make for these three items determine which of the remaining network value fields are enabled. For instance, if you specify a single-server configuration, the Server 2 fields are disabled (grayed out).

- 8 Enter the network values from the [First-Time Setup Worksheet](#).



If the network into which you're installing the system requires 802.1x authentication for servers (this is rarely the case), incorrect settings in the **LAN Security Settings** section can make the system unreachable. Recovering from this situation requires disconnecting the system from the network and connecting a laptop directly to the system in order to access it. Make certain these settings are correct if needed.

- 9 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. In the much more common combined network configuration, this is rarely the case. 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.

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

The system begins to reboot.

- 11 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**.



If the LCD displays anything else or nothing, stop. Contact Polycom Global Services for assistance.

- 12** From a PC with network access to the Polycom DMA system, point your browser to the system's virtual host name or IP address (if installing a two-server system) or physical host name or IP address (if installing a single-server system) and log in with user ID **admin** and password **admin**.
- 13** Go to **Admin > Local Cluster > Time Settings** 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. If you really want to use a generic GMT offset, note that they use the Linux/Posix convention of specifying how many hours ahead of or behind local time GMT is. Thus, the generic equivalent of America/Denver (UTC-07:00) is GMT+07, not GMT-07.
 - b** 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.
 - c** 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**.
 - d** If you're installing a single-server system, skip to step 15.
- 14** If you're installing a two-server cluster, do the following:



If you're not sure whether you're installing a two-server cluster, please re-read [page 7](#).

Both servers in the cluster must be running the same version of the software, so if you installed a different version on the first server, you **must** do so on the second.

- a** If you replaced the system software on the first server with the official UC APL version, turn on the second server, insert the system recovery disk for the UC APL version, and reboot it.

The server boots from the DVD, and the installation commences. About 15-20 minutes later, the DVD ejects and the server reboots. 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.



If the LCD displays anything else or nothing, stop. Contact Polycom Global Services for assistance.

- b** Connect the GB 1 Ethernet port of the second server 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.

- c Connect one of the Ethernet cables included in the server shipment between the GB 2 ports of the two servers.
- d Verify that the first server is running and its front panel LCD displays **DMA Ready**. Then turn on (or reboot) the second server.

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



If the LCDs aren't displaying **DMA Clustered**, stop. Contact Polycom Global Services for assistance.

- 15 Optionally (but strongly recommended), manually secure the system servers as described in the next section.
- 16 Log back into the system and complete your system setup and security configuration as described in the following chapter.



Don't turn off a Polycom DMA system server by simply unplugging it or otherwise removing power, especially if it's going to remain off for some time. If a server loses power without being properly shut down, the RAID controller fails to shut down, eventually depleting its battery. If that happens, the server can't be restarted without user input, requiring a keyboard and monitor.

Secure the Polycom DMA System Servers

When you switch to maximum security mode ([page 32](#)), 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 strongly 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.

Polycom® DMA® System Maximum Security Deployment

This chapter describes the tasks required to complete the deployment of a Polycom® DMA® 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 7000 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.
- 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 RealPresence® Collaboration Server or 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/AAAA records that map each physical host name to the corresponding physical IP address and each virtual host name to the corresponding virtual IP address are mandatory.

A two-server system has three host names and IP addresses (one virtual and two physical) for the management or combined interface, and in a split network configuration, three more for the signaling interface. See “Add Required DNS Records for the Polycom DMA System” in the online help or *Polycom DMA 7000 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 **User > 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 7000 Operations Guide*.
- 3 Log out and log back in using the new local account.
- 4 Go to **User > Users** and delete the default admin account. See “Users Procedures” in the online help or *Polycom DMA 7000 Operations Guide*.

License the System

To license the system

- 1 Go to **Admin > Local Cluster > Licenses**.
The **Licenses** 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 7000 Operations Guide*.

Configure Signaling

To configure signaling

- 1 Go to **Admin > Local Cluster > Signaling Settings**.
The **Signaling Settings** page appears.
- 2 Enable H.323 and/or SIP signaling, following the procedure described in “Configure Signaling” in the online help or *Polycom DMA 7000 Operations Guide*. Optionally, do any of the following:
 - Configure H.323 device authentication, SIP digest authentication, or both.
 - If SIP signaling is enabled, turn on ANAT support if AS-SIP is in use, require certificate validation for TLS, and/or configure untrusted call handling.



If H.323 is enabled, we strongly recommend putting the DMA system into routed mode (especially if the DMA system is being neighbored with another H.323 gatekeeper) so that it proxies all H.323 signaling messages. Go to **Admin > Call Server > Call Server Settings** and under **H.323 Settings**, change **Gatekeeper call mode** to **Routed call mode**.

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 7000 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 7000 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.

Configure Secure SIP or AS-SIP Connections

If you are deploying the DMA system in a secure SIP or AS-SIP environment, you can configure the system to take advantage of encrypted SIP or AS-SIP communication paths as described in this topic.

Integrate the DMA System With a Local Session Controller (LSC)

If necessary in your environment, enable secure outbound connections to a Local Session Controller from DMA system VMRs. For more information and instructions for individual steps below, refer to the online help or the *Polycom DMA 7000 Operations Guide*.

To integrate the DMA system with the LSC

- 1 Go to **Network > External SIP Peer**.
- 2 Click **Add**.
- 3 Enter the following information:
 - **Name** for the LSC
 - **Description** for the LSC
 - IP address of the LSC as the **Next hop address**
 - **Port** of 5061
- 4 If the LSC requires the DMA system to provide SIP digest authentication, add the credentials in the **Authentication** tab.
- 5 Ensure that the **Transport type** field is set to **TLS**.



The DMA system must trust the LSC security certificate. If necessary, import the LSC certificate into the DMA system's certificate repository, or ensure that the DMA system's certificate and the LSC certificate are signed by the same Certificate Authority. See the "Certificate Procedures" topic in the online help or *Polycom DMA 7000 Operations Guide* for more information about working with certificates.

- 6 Go to **Admin > Call Server > Dial Rules**.
- 7 Click **Add** to create a new dial rule for authorized calls that will route calls to the newly defined SIP peer.
- 8 Enter a **Description** for the rule.
- 9 Choose an **Action of Resolve to external SIP peer**.
- 10 In the list of **Available SIP peers**, select the SIP peer you defined earlier and use the right arrow button to move it to the list of **Selected SIP peers**.
- 11 When finished, click **OK**.
- 12 Select the new rule in the list and use **Move Up** and **Move Down** to order the rule after any rules that route calls to local resources, such as VMRs, Virtual Entry Queues (VEQs), direct dial VEQs, and registered H.323 endpoints.

Ensure that the rule is ordered after any rules that route to external devices (such as neighbored H.323 gatekeepers or H.323 -> ISDN gateways) that should be applied before routing a call to the external SIP call server.

- 13** If H.323 is enabled on the DMA system, add the following preliminary script to each H.323-only dial rule. The preliminary script will ensure that the dial rule is skipped if the dial string begins with “sip” or “sips”:

```
if (DIAL_STRING.match(/sip/i))
{
    return NEXT_RULE;
}
```

Configure Default AS-SIP Resource Priority Values for Dial-Out Conferencing

If you are deploying the DMA system on an AS-SIP network and will be using VMR dial-out functionality, you need to configure the default resource priority values to use when placing these calls. If you won't be using the VMR dial-out feature, it's not necessary to configure these settings.

To configure default AS-SIP resource priority values for dial-out conferencing

- 1 Go to **Admin > Conference Manager > Conference Settings**.
- 2 Set the **Resource priority namespace** and **Resource priority value** fields to appropriate values for your environment.

See the online help or the *Polycom DMA 7000 Operations Guide* for more information about these settings.
- 3 Click **Update**.

Configure Encryption for Conference Templates

To configure encryption for conference templates

- 1 Go to **Admin > Conference Manager > Conference Templates**.
- 2 Click **Add** to add a new conference template, or select an existing conference template from the list and click **Edit**.
- 3 Select the **RMX General Settings** tab.
- 4 Under **Advanced Settings**, ensure the **Encryption** field is set to **Encrypt all**.

To ensure a secure connection with endpoints, the MCU conference profile you use must have AES encryption enabled, as must any endpoints joining calls on this system.
- 5 If you are deploying the DMA system in an AS-SIP environment:
 - a Select the **RMX Video Quality** tab.

- b** Ensure that the **AS SIP content** check box is selected.
- 6** Click **OK**.

Enable Secure Inbound SIP or AS-SIP VMR Connections

To enable secure inbound SIP or AS-SIP connections to a VMR

- 1** Go to **Admin > Call Server > Device Authentication**.
- 2** Click the **Shared Outbound Authentication** tab.
- 3** Click **Add**.

If the external call server requires the DMA system to provide authentication credentials when connecting, you need to configure the credentials that the DMA system will provide.
- 4** Add any required authentication credentials for authenticating the DMA system with the external call server as described in the “Device Authentication” topic of the online help or the *Polycom DMA 7000 Operations Guide*.
- 5** Add an MCU to the DMA system if none have been added, or ensure the existing MCUs have a secure connection to the DMA system.
- 6** Add the MCU to a pool, and the pool to a pool order. See “[Add Polycom MCUs to the System](#)” on page 36 for more information.
- 7** If necessary, create a secure SIP trunk or routing rule on the external call server to route inbound VMR calls to the DMA system. Refer to the external call server’s documentation for more information.

Configure VMRs for Users

Once you’ve configured the system to use secure connections for SIP and AS-SIP calls, you can configure virtual meeting rooms (VMRs) to take advantage of this configuration.

To configure VMRs for users

- 1** Go to **User > Users**.
- 2** Select a user from the list.
- 3** Click **Manage Conf Rooms**.
- 4** Click **Add** to create a DMA VMR for the selected user.

- 5 Configure the VMR to use the conference template you created or modified in [“Configure Encryption for Conference Templates”](#) on page 30 and the MCU pool order that you configured in [“Enable Secure Inbound SIP or AS-SIP VMR Connections”](#) on page 31.

See the online help or the *Polycom DMA 7000 Operations Guide* for more information on creating VMRs and working with MCU pools and pool orders.

- 6 If necessary, change the resource priority values for this VMR.



When you deploy the DMA system in an AS-SIP environment, you can configure each VMR to use specific, non-default resource priority values for outbound calls. For example, some users may require all outbound calls to be placed with a higher priority than the system-wide default.

When creating VMRs for users, configure the resource priority values for those VMRs if required in your environment. Refer to the online help or *Polycom DMA 7000 Operations Guide* for more information.

- 7 Click **OK**.
- 8 Repeat steps 4 through 7 to add more VMRs.

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 3). 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 **Admin > Local Cluster > Security Settings**.
- 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 you performed the recommended procedure to manually secure the servers (page 23), a BIOS password already exists, and it remains unchanged.



Occasionally, a BIOS change fails to be implemented on reboot. That's why, to make absolutely certain that the servers are secure, we recommend manually securing them by performing the procedure on page 23 on each server.

Otherwise when the system enters maximum security mode, it attempts to set a default BIOS password (*B105pa55w0rd*). In that case, follow the procedure below to change the default BIOS password to something more secure.

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.

Review and Modify (If Necessary) Security-Related Settings

Review the settings on the following pages and make any necessary changes (see the online help or *Polycom DMA 7000 Operations Guide* topic for each page for details about the settings):

- **Admin > Login Policy Settings > Local Password**
- **Admin > Login Policy Settings > Local User Account**
- **Admin > Login Policy Settings > Session**
- **Admin > Login Policy Settings > Banner**
- **Admin > Login Policy Settings > Access Policy Settings**



The **Access Policy Settings** page lets you restrict management access to a whitelist of authorized IP addresses or address ranges. If you choose to do so, make sure that you've correctly added the IP address of the workstation from which you logged into the system and all other IP addresses or address ranges authorized for management access.

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 7000 Operations Guide*, and then integrate the system with your Active Directory as described in “Active 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 7000 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 7000 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 MCUs to the System

If you haven't already done so, deploy your Polycom RealPresence Collaboration Server or RMX MCUs as described in the documentation for the model you purchased.

Then, add the MCUs to the Polycom DMA system. See "MCUs" and its subtopics in the online help or *Polycom DMA 7000 Operations Guide*.



A Polycom 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 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 MCU. When the connection between the DMA system and the MCU is encrypted, the "Connected securely" lock icon will appear next to the MCU name in the list of MCUs.

Note that Polycom MCUs use 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 7000 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 5.

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 **Admin > Local Cluster > Security Settings**.
- 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.

