POLYCOM®

Polycom® CMA™ System Getting Started Guide

6.0.0 | October 2011 | 3725-77612-001E

Trademark Information

Polycom®, the Polycom "Triangles" logo, and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

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

Patent Information

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

End User License Agreement

Use of this software constitutes acceptance of the terms and conditions of the Polycom CMA 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 CMA system.

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

Contents

About This Guide

This guide provides the first-time setup information you need to configure a Polycom® Converged Management Application™ (CMA™) scheduling and management system. Once you've completed first-time setup, see Chapter 2 of the *Polycom CMA System Operations Guide* for additional configuration and customizing tasks you can perform.

Documentation Resources

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

- *Polycom CMA System Release Notes*

  Provides the information users need to know about the specific release of the CMA system you're implementing.

- *Polycom CMA System Quick Start Guide*

  Describes how to unpack and install a CMA system.

- *Polycom CMA System Operations Guide*

  Provides more detailed and specialized configuration information users needs to know to implement and customize the CMA system.

- *Polycom CMA System Web Scheduling Guide*

  Gives schedulers detailed information on scheduling and monitoring conferences.

The CMA system also has online help available through the user interface.

Assumptions

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

This guide assumes that you are starting with a CMA system that has never been previously configured.

1

Prepare for Polycom® CMA™ System Installation

This chapter describes the tasks you should do in advance of installing the Polycom® Converged Management Application™ (CMA™) system including:

- Collect Necessary Materials
- Complete the First Time Setup Worksheet
- Request Certificates (Optional)
- Unpack and Install the Hardware Components
- Pre-stage a Computer Account
- Connect to the Polycom CMA System Server

If you are installing a redundant Polycom CMA system configuration, perform all of the procedures in this chapter on both system servers unless instructed otherwise.

Collect Necessary Materials

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

- *Polycom CMA System Release Notes*
- Polycom CMA system server shipment
- Completed site survey or project toolkit
- Computer with a serial or ethernet port

Complete the First Time Setup Worksheet

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

In redundant system configurations, complete a **First Time Setup Worksheet** for each CMA system server.

Item	My System Values	Factory-Set Default Values	Description
Security Mode Setting			
Set Standard Mode			Recommended setting.
Set Maximum Security Mode			No recommended except for those businesses that must adhere to the most stringent security protocols. This selection is irreversible and has significant consequences, as many CMA system features aren't supported in this mode.
System Network Settings (from Admin > Server Settings > Network)			
System Name		POLYCOM-<7-random-ASCII-characters> For example, `POLYCOM-IDT9R5W`	NetBIOS name of the CMA system server. The name must be between 6 and 15 characters and can include dashes and underscores.
IPv4 Address		192.168.1.254	Static, physical IP address for the CMA system server on an IPv4 network.
Virtual IP Address			For redundant CMA 5000 system configurations only.
IPv4 Subnet Mask		255.255.255.0	Network subnet mask of the system server. For IPv4 networks only.
IPv4 Default Gateway		192.168.1.1	IP address of the gateway server/router. For IPv4 networks only.
DNS Domain			This is the DNS domain name suffix, for the network in which the domain name server and CMA system server reside. For example `polycom.com`, not the fully qualified path of `<hostname>.polycom.com`.
Preferred DNS Server			IP address of the domain name server.

Item	My System Values	Factory-Set Default Values	Description
Alternate DNS Server			IP address of an alternate domain name server. Must be in the same IP address format as the preferred DNS server.
System Time Information (from Admin > Server Settings > System Time)			
System Time Zone			
Current Date			
Current Time			
External NTP Server			IP address of external NTP time server (optional).
Information Required for Polycom Customer Support (from Admin > Server Settings > Licenses)			
Serial number			
License number			

Request Certificates (Optional)

If you are using certificates, you should use the same certificates that you used for the initial installation of the CMA system. If that information is not available, use the information below to set them up.

Certificates and certificate chains are a security technology that allows networked computers to determine whether to trust each other.

By default, to support encrypted communications and establish a minimal level of trust, the CMA system includes a default key and self-signed certificate. However, to implement a full certificate chain to a root certificate authority (CA), a CMA system requires both a root CA certificate and a identity server certificate signed by the root CA. Therefore, at some time you must request these certificates from your CA. The question is when.

You must install the root CA certificate during first-time setup, therefore we recommend you request it from your CA before beginning first-time setup. However, with regard to the identity server certificate you have three options:

- The CMA system First-Time Setup Wizard supports the function of creating a certificate signing request (CSR). Therefore, you may choose to create the CSR for the identity server certificate during first-time setup and suspend the process while you wait for your CA to provide the certificate.
- You can also choose to install the identity server certificate after first-time setup, because you can complete first-time setup with just the root CA certificate and the CMA system default certificate information.

- You also have the third option of requesting the identity server certificate in advance of first-time setup, but to do this you must have extensive knowledge of certificates, certificate templates, and CSR structures.

1 If you are using Active Directory in Server 2000 mixed mode, edit the properties of the computer account and on the **General** tab, select **Trust computer for delegation**.

Unpack and Install the Hardware Components

The Polycom CMA system uses a Polycom-branded Dell PowerEdge R610 server. To unpack and install the CMA system hardware, follow this procedure.

To unpack and install the hardware:

1 Examine the Polycom CMA system shipping container for damage.

2 Open and review the container packing slips.

3 Open the containers and 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 of this product.

Besides this *Polycom CMA System Getting Started Guide*, the Polycom CMA system server package includes these items:

- Polycom CMA system server
- Power cord and power cord retention brackets
- Rack-mount kit
- Serial cable
- Dell PowerEdge R610 server documentation set

4 Unpack your system and identify each item. Keep all shipping materials in case you need them later.

5 Read the "Safety Instructions" in the*Rack Installation Guide* and then use the brackets provided to install the system in the rack.

6 Assemble the rails and install the system in the rack following the safety instructions and the rack installation instructions provided with your system.

7 Connect the system's power cable(s) to the system and, if a monitor is used, connect the monitor's power cable to the monitor..

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

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

10 Press the power button on the system and the monitor. The power indicators should light.

11 (Optional) Install the bezel.

Pre-stage a Computer Account

To enable the **Use Single Signon** option, which allows endpoint users who are included in the Active Directory to securely log into their dynamically-managed endpoint without typing in credentials, an Active Directory administrator must first pre-stage an Active Directory computer account for the Polycom CMA system. Only one account is required for a redundant Polycom CMA system.

This procedure can be done at any time before running **First Time Setup**.

To pre-stage a computer account

1 On the Active Directory system, use the Microsoft **Active Directory Users and Computers** MMC snap-in to create a computer account for the Polycom CMA system. Create the computer account in any desired organizational unit (OU). The computer account object must have **Reset Password** and **Write Account Restrictions** permissions.

For more information on the **Active Directory Users and Computers** MMC snap-in, see Microsoft Technet.

2 From a command window on the Domain Controller, type:
`net user <computer account name>$ <Password> /domain`

Where <***computer account name***> is the name of the computer account created in step 1 on page 5, <***Password***> is the desired password, and **`/domain`** is literally **`/domain`** (i.e., do not substitute with a domain name). For more information on the `net user` command, see the Microsoft Knowledge Base.

You have now created a computer account that you can use for integrated Windows authentication.

Connect to the Polycom CMA System Server

You configure the CMA system server through a ethernet port.

To connect to the CMA system through an ethernet port

1. Do one of the following:
   - Connect the CMA system server (via the GB1 port) directly to an ethernet port on a computer through a crossover cable.
   - Use ethernet cables to connect the CMA system server (via the GB1 port) and a computer to the same ethernet switch or hub.
2. Power on the computer and the CMA system server.

2

Polycom® CMA™ System Software Setup in Standard Security Mode

This chapter describes the Polycom® Converged Management Application™ (CMA™) system software first-time setup for systems being configured in standard security mode.

If you are installing a redundant CMA system configuration, perform all of the procedures in this chapter on both system servers unless instructed otherwise.

First-Time Setup Wizard

When you log into a CMA system that has not been configured, the First-Time Setup Wizard automatically steps you through a series of ordered configuration pages. You cannot use the system until you've completed the steps in the first-time setup.

Note that changing configuration settings on some pages of the First-Time Setup Wizard, such as the **System Information** and **Database** pages, will cause the system to reboot. When you log into a system after one of these reboots, the next page in the ordered configuration pages appears.

Log in to the CMA system from the computer you connected to the Polycom CMA system sever as described in "Connect to the Polycom CMA System Server" on page 6. To log into the CMA system web interface, you need:

- Microsoft Internet Explorer® 6.0, 7.0 or 8.0, Mozilla FireFox® 3.5 or 3.6, or Apple Safari 3.2, 4.0 or 5.0.
- Adobe® Flash® Player 9.x or 10.x
- The IP address or host name of the CMA system server and your username, password, and domain.

The CMA system user interface is best viewed with an SXGA display resolution of at least 1280x1024 pixels. The minimum support display resolution is XGA 1024x768 pixels.

Generally, you get three opportunities to enter the correct password. After three failed attempts, the system returns an error message.

To step through the First-Time Setup Wizard

1 Open a browser window and in the **Address** field enter the CMA system IP address or host name.

2 When the CMA system login screen appears, if necessary select a different **Language** or **Domain**.

3 Enter the administrator **Username** and **Password**.

The factory default is `admin/admin`.

4 Click **Login**.

Because the CMA system has not been previously configured, the **Licensing** page of the setup wizard appears.

EULA License Agreement

5 Read the license agreement and click **Accept** to accept the terms and continue.

Security Mode

6 When you are prompted to select a security mode, select **Set Standard Mode**.

The **Administrative User** page appears.

Administrator Password

7 When the **Change Administrator Password** page appears, enter the **Old Password.**

8 For the **New Password**, enter a new password with a length of at least eight characters.

9 **Confirm the New Password** and click **Next**.

The **Network** page appears.

Network Settings

10 Enter the **Network Settings** information recorded in "Complete the First Time Setup Worksheet" on page 2 and click **Next**.

The **Certificates** page appears. By default the system is configured to use a default self-signed certificate.

Certificate Management

11 To continue the First Time Setup Wizard using the CMA system self-signed certificate, go to step 15.

12 To add the root CA certificate:

a Click **Install Certificate** and in the **Install Certificates** dialog box, do one of the following:

» If you have a certificate file, click **Upload certificate**, enter the password (if any) for the file, and browse to the file or enter the path and file name.

» If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box.

You should only import certificates obtained from trusted sources. Importing an altered or unreliable certificate could compromise the security of any system component that uses the imported certificate.

b Click **OK** and verify that the certificate appears in the list as a *Trusted Root CA*.

13 To create a certificate signing request for the CMA system identity certificate:

a Click **Create Certificate Signing Request**.

b Enter this information in the **Certificate Information** dialog box and then click **OK**.

Field	Description
Common name (CN)	Set to the virtual host name of the system, as defined in the network settings.
Domain	Set to the domain name, as defined in the network settings.
Organizational unit (OU)	Subdivision of organization. Optional.
Organization (O)	Optional.
City or locality (L)	Optional.
State (ST)	Optional.
Country (C)	Two-character country code.

The **Certificate Signing Request** dialog box displays the encoded request.

c Copy the entire contents of the **Encoded Request** field (including the text -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----) and submit it to your certificate authority.

d Click **OK** to close the dialog box.

e Submit the CSR as required by your CA. This is usually by E-mail or by pasting it into a web page.

14 To suspend the First-Time Setup Wizard until your certificate authority has processed your request:

a Wait until you receive the signed identity server certificate for your CMA system and the CA's certificate revocation list. You may also received intermediate certificates. Depending on the certificate authority, these files may be communicated as mail text, mail attachments, or on a secure web page.

b Click **Upload Certificate** and in the **Install Certificates** dialog box, do one of the following:

» If you have a certificate file, click **Upload certificate**, enter the password (if any) for the file, and browse to the file or enter the path and file name.

» If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box.

c To upload the associated certificate revocation list:

» Go to click **Upload Certificate Revocation List**.

» In the **Select file** dialog box, browse to the location of the CRL and select the file.

» Click **Open**.

d Click **OK** and verify the following appears in the certificate list:

» A *CMA Server Identity*

» A Trusted root CA with an associated CRL

15 Click **Next**.

System Reboot

16 When prompted to reboot, click **Commit the Settings and Reboot**.

The system displays a confirmation message.

17 Click **Yes**.

The system reboots.

18 As needed, wait 5 minutes for the system to completely reboot and then log into the CMA system again using the administrator password you created earlier.

The **System Time** page appears.

System Time

19 Configure these settings on the **System Time** page, as necessary.

Field	Description
System Time Zone	The time zone in which the CMA server resides.

Field	Description
Auto Adjust for Daylight Saving?	Select this checkbox to adjust the clock automatically for daylight savings time.
Use Current Time	Select this checkbox to input the current date and time.
Current Date	The system date for the CMA system.
Current Time	The system time for the CMA system.
Use External NTP Server Time Synchronization	(Recommended) Select this checkbox to synchronize the CMA system date and time with an external NTP server.
IP address or DNS resolved names separated by commas	The IP address or fully qualified domain name (ASCII only) of the NTP server.

If you set the system to use an external NTP server without first setting the current date and time, the system time may be wrong until the system's first synchronization.

20 Click **Next**.

The **Database** page appears. By default, the CMA system internal database is used.

Integration with an external Microsoft SQL Server database is required for redundant CMA 5000 systems or for CMA 5000 systems supporting more than 400 concurrently registered endpoints and 240 concurrent calls. However, for ease of setup, you may wish to leave the system pointed to its internal database and integrate with the external database later.

If you are installing a redundant CMA 5000 system configuration, *leave both servers configured to use the internal database*. You will point them to an external database later when you perform the redundancy configuration tasks in Chapter 2 of the *Polycom CMA System Operation Guide*.

21 To continue to use the default internal database during first-time setup, click **Next** and skip to Enterprise Directory Server Configuration on page 12. You can set up the external database after you've finished first-time setup.

Database Configuration

22 To use an external Microsoft SQL database server:

a Verify that your Microsoft SQL Server meets the CMA system requirements. Refer to the *Polycom CMA System Release Notes*.

b Select the **Use an external SQL Server database** check box.

c Enter the **Database Server IP Address** and change the database port number as needed.

d Click **Next**.

e When prompted to reboot, click **Yes**.

The system reboots.

The **Database Maintenance** dialog box appears.

f As needed, enter the User ID and Password for the Microsoft SQL server.

» If you use Microsoft Windows authentication, be sure the login ID has administrator privileges on the SQL server.

» If you use Microsoft SQL authentication, be sure the login ID is a member of the `sysadmin` role.

g (Optional) Click **Reformat/Install Database**.

You do not have to click **Reformat/Install Database**. The database is set up after the last reboot.

The system connects to the server and installs the databases.

h When the installation is complete, click **Close**.

The system reboots.

i Wait 5 minutes and when the system completely reboots, log into the CMA system again.

The **Enterprise Directory** page appears. By default, the CMA system accesses an internal user database.

23 To continue using the local directory during first-time setup, skip to "Directory Configuration" on page 14. You can set up the integration with an enterprise Active Directory after you've finished first-time setup.

Enterprise Directory Server Configuration

24 To integrate the CMA system with an enterprise Active Directory server so that users can include enterprise groups, users, and rooms in their conferences:

a On the **Enterprise Directory** page, select **Integrate with Enterprise Directory Server**.

b To have the system auto-discover the enterprise directory server by querying the DNS, enable **Auto-discover** in the **Integrate with Enterprise Directory server** section; otherwise, enter the Enterprise Directory **IP Address** or **DNS Name**.

c As needed, configure these settings on the **Enterprise Directory** page.

Setting	Description
Domain\Enterprise Directory User ID	Domain and Enterprise Directory User ID for an account that the CMA system can use to access the enterprise directory server and retrieve group, user, and room information. This Enterprise Directory User ID must have read permissions so it can search the entire forest on the enterprise directory server. This Enterprise Directory User ID is automatically associated with the CMA system administrator role.
Enterprise Directory User Password	The password for the enterprise directory user account.
Security Level	The level of security on the connection between the CMA system and the Active Directory server. Possible values include: • **Plain**—No security on the connection • **LDAPS**—The connection is secured over outbound port 3269 using LDAP-S in a manner similar to `https`. If the “Domain Controller: LDAP Server signing requirements” setting on the Active Directory server is set to “Require Signing”, then you must use LDAPS to secure the connection. • **StartTLS**—The connection is secured over outbound port 3268 (the same port as **Plain**), but it then negotiates security once the socket is opened. Some enterprise directory servers reject any unsecured transactions, so the first command is the `StartTLS` negotiation command.
Ignore Disabled Enterprise Directory Users	Enable this option to have the CMA system ignore disabled enterprise users. Do not enable this option if your enterprise conference rooms are set up as disabled enterprise users.
Enterprise Directory Exclusion Filter	If necessary and you understand enterprise directory filter syntax, specify other types of user accounts to exclude. Don’t edit these expressions unless you understand enterprise directory filter syntax. For more information, see “Understanding Exclusion Filters” in the *Polycom CMA System Operations Guide*.

Setting	Description
Enterprise Directory Search BaseDN	If necessary and you understand enterprise directory filter syntax, specify the top level of the enterprise directory tree (referred to as the base DN) to search. Don't edit these expressions unless you understand enterprise directory filter syntax. For more information, see "Understanding Base DN" in the *Polycom CMA System Operations Guide*.

Allow Delegated Authentication to Enterprise Directory Server

25 To integrate the CMA system with an Active Directory domain controller for single sign-on authentication:

a On the **Enterprise Directory** page, select **Allow Delegated Authentication to Enterprise Directory Server**.

The CMA system can auto-discover the closest logical domain controller and Active Directory servers, but to do this the network DNS server must have a DNS SRV record for these servers

b If your network DNS server has a DNS SRV record for the domain controller, in the **Domain controller name** section enable **Auto-discover**; otherwise, enter the **Fully Qualified Host Name** of the domain controller (for example, `dc1.mydomain.com`). The pre-staged computer account must be within this domain as well.

c In the **Computer Account Credentials** section, enter the **Domain\Comuter Name** and **Password** for the pre-staged computer account created in step "Pre-stage a Computer Account" on page 5.

26 Click **Next**.

The CMA system **Directory Setup** page appears.

Directory Configuration

27 On the **Directory Setup** page:

a To exclude users with dynamically-managed devices from the Global Address Book, clear the **Include dynamically-managed devices in the Global Address Book** option.

b To exclude guestbook entries from the enterprise directory, clear the **Show Guestbook Entries in the Directory** option.

c If your video network includes LifeSize endpoints, select the **Modify Directory Listings for LifeSize® Endpoint Support** option.

28 Click **Next**.

The CMA system displays the message that you have completed first-time setup. You have the option of logging out of the application or going to the application **Dashboard**.

Complete the Setup

Once you've finished first-time setup, you may need to perform these configuration tasks:

- Using the Microsoft SQL Server Configuration Manager, change the SQL Server keep alive checks (typically, **SQL Server 2005 Network Configuration > Protocols for MSSQLSERVER > TCP/IP > KeepAlive**) to 3,600,000 milliseconds.
- If you're installing redundant CMA 5000 system servers, complete the procedures for configuring redundancy. This includes setting up the external database, entering the virtual IP address, and testing failover.
- As needed, integrate the CMA system with an external Microsoft SQL database.
- As needed, integrate the CMA system with a Microsoft Active Directory enterprise directory.
- Add licenses to your system.
- Set up users, rooms, and devices.
- Associate devices with users and rooms.
- Schedule a test conference.
- Set up client computers with Microsoft Internet Explorer and the Polycom CMA Desktop application, as required.
- Download and distribute the Polycom Scheduling Plugins for Microsoft® Outlook® and/or IBM® Lotus® Notes®.

For more information on these tasks, refer to the *Polycom CMA System Operation Guide*.

3

Polycom® CMA™ System Software Setup in Maximum Security Mode

This chapter describes the Polycom® Converged Management Application™ (CMA™) system software first-time setup tasks when setting the system up in a maximum security environment. It includes these topics:

- Secure the Polycom CMA System Server
- First Time Setup Wizard
- Complete the Setup

Before setting a CMA system up in maximum security mode, make sure you completely understand the significant outcomes from selecting **Set Maximum Security Mode**.

- The capabilities of the system are restricted.
- To return to standard security mode, you must erase the system configuration and restart first-time setup.
- Other Polycom products must be in maximum security mode.

If you decide to set the system up in standard security mode, go to "Polycom® CMA™ System Software Setup in Standard Security Mode" on page 7.

Secure the Polycom CMA System Server

When installing a CMA system in a maximum security environment, secure the CMA system server before entering the **First Time Setup** wizard. To do this, interrupt the CMA system server boot process and secure the system by changing the system server Bios as described in the following procedure.

To secure the CMA system server

1 Power on the computer and the CMA system server.

2 Press **<F2>** to interrupt the system reboot using the keyboard attached to the system server.

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

3 From the main **System Setup** menu, select **System Time**.

— Set the system's internal clock to UTC (coordinated universal time).

- If you're unsure how to navigate through the **System Setup** menu, press **<F1>** to view the **System Setup** program help file.
- For most of the options, any changes that you make are recorded but do not take effect until you restart the system.

4 Return to the main **System Setup** menu and select **Boot Settings** and then **Boot Sequence**.

— Disable the **SATA Optical Drive** and **Embedded NIC 1**.

5 Return to the main **System Setup** menu and select **Integrated Devices**.

— Set **User Accessible USB Ports** to **All Ports Off**.

— Set **Internal USB Port** to **Off**.

— Set **Embedded NIC 3 and NIC 4** to **Disable**.

6 Return to the main **System Setup** menu and select **System Security**.

— 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**.

— Set **Power Button** to **Disabled**.

7 Return to the main **System Setup** menu and select **Serial Communications**.

— Set **Serial Communications** to **Off**.

8 Exit and save the changes.

The system reboots.

First Time Setup Wizard

When you log into a CMA system that has not been previously configured, the first-time setup wizard automatically steps you through a series of ordered configuration pages. You cannot use the system until you've completed the steps in the first-time setup wizard.

Note that changing configuration settings on some pages of the First-Time Setup Wizard, such as the **System Information** and **Database** pages, will cause the system to reboot. When you log into a system after one of these reboots, the next page in the ordered configuration pages appears.

To log into the CMA system web interface, you need:

- Microsoft Internet Explorer® 7.0 or 8.0 (If your system is operating in maximum security mode, you may use only Microsoft Internet Explorer.)
- Adobe® Flash® Player 9.x or 10.x
- The IP address or host name of the CMA system server and your username, password, and domain.

The CMA system user interface is best viewed with an SXGA display resolution of at least 1280x1024 pixels. The minimum support display resolution is XGA 1024x768 pixels.

Generally, you get three opportunities to enter the correct password. After three failed attempts, the system returns an error message.

To step through the First-Time Setup Wizard

1. Open a browser window and in the **Address** field enter the CMA system IP address or host name.
2. When the CMA system login screen appears, if necessary select a different **Language** or **Domain**.
3. Enter the administrator **Username** and **Password**. The factory default is `admin/admin`.
4. Click **Login**.

   Because the CMA system has not been previously configured, the **Licensing** page of the setup wizard appears.

EULA License Agreement

5. Read the license agreement and click **Accept** to accept the terms and continue.

Security Mode

6. When you are prompted to select a security mode, select **Set Standard Mode** unless you completely understand the significant outcomes from selecting **Set Maximum Security Mode**.
   - The capabilities of the system are restricted.

- To return to standard security mode, you must erase the system configuration and restart first-time setup.
- Other Polycom products must be in maximum security mode.

Administrator User Name and Password

7 Change the default local administrator **User Name**. If the system will be integrated with a Microsoft Active Directory, we recommend using a user name that does not exist in the enterprise directory. CMA system user names must be unique across all users in all domains.

8 Change the default local administrator **Password**. Since this is the first login to the system, the password must comply with the default password requirements including:

- Minimum length of 15 characters
- Minimum of 2 lowercase letters, 2 uppercase letters, 2 numbers, and 2 special characters. Special characters are the 32 standard ASCII keyboard characters:

  ~ ! @ # $ % ^ & * ( ) _ + ‘ - = { } | [ ] \ : ” ; ’ < > ? , . /

9 **Confirm the New Password** and click **Next**.

The **Login Banner** page appears.

Login Banner

10 To create a customized login banner for your business, enable **Use Custom Banner** and enter a new login banner into the **Custom Banner** field.

11 To keep the default login banner, enable **Use Default Banner**.

12 Click Next.

The **Network** page appears.

Network Settings

13 Enter the **Network Settings** information recorded in “Complete the First Time Setup Worksheet” on page 2 and click **Next**.

The **Certificates** page appears. By default the system is configured to use a default self-signed certificate.

Certificate Management

14 To add the root CA certificate:

a Click **Add Certificate** and in the **Add Certificates** dialog box, do one of the following:

» If you have a certificate file, click **Upload certificate**, enter the password (if any) for the file, and browse to the file or enter the path and file name.

» If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box.

You should only import certificates obtained from trusted sources. Importing an altered or unreliable certificate could compromise the security of any system component that uses the imported certificate.

b Click **OK** and verify that the certificate appears in the list as a *Trusted Root CA*.

15 To create a certificate signing request for the CMA system identity certificate:

a Click **Create Certificate Signing Request**

b Enter this information in the **Certificate Information** dialog box and then click **OK**.

Field	Description
Common name (CN)	Set to the virtual host name of the system, as defined in the network settings.
Domain	Set to the domain name, as defined in the network settings.
Organizational unit (OU)	Subdivision of organization. Optional.
Organization (O)	Optional.
City or locality (L)	Optional.
State (ST)	Optional.
Country (C)	Two-character country code.

The **Certificate Signing Request** dialog box displays the encoded request.

c Copy the entire contents of the **Encoded Request** field (including the text -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----) and submit it to your certificate authority.

d Click **OK** to close the dialog box.

e Submit the CSR as required by your CA. This is usually by E-mail or by pasting it into a web page.

16 To continue the First Time Setup Wizard using the CMA system self-signed certificate, go to step 18.

17 To suspend the First Time Setup Wizard until your certificate authority has processed your request:

a Wait until you receive the signed identity server certificate for your CMA system and the CA's certificate revocation list. You may also received intermediate certificates. Depending on the certificate authority, these files may be communicated as mail text, mail attachments, or on a secure web page.

b Click **Upload Certificate** and in the **Install Certificates** dialog box, do one of the following:

» If you have a certificate file, click **Upload certificate**, enter the password (if any) for the file, and browse to the file or enter the path and file name.

» If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box.

c To upload the associated certificate revocation list:

» Go to click **Upload Certificate Revocation List**.

» In the **Select file** dialog box, browse to the location of the CRL and select the file.

» Click **Open**.

d Click **OK** and verify the following appears in the certificate list:

» A *CMA Server Identity*

» A Trusted root CA with an associated CRL

18 Click **Next**.

System Reboot

19 When prompted to reboot, click **Reboot**.

The system reboots.

20 As needed, wait 5 minutes for the system to completely reboot and then log into the CMA system again using the new administrator user name and password you created earlier.

The **System Time** page appears.

System Time

21 Configure these settings on the **System Time** page, as necessary.

Field	Description
System Time Zone	The time zone in which the CMA system server resides.
Auto Adjust for Daylight Saving?	Select this check box to adjust the clock automatically for daylight savings time.
Use Current Time	Select this check box to input the current date and time.
Current Date	The system date for the CMA system.
Current Time	The system time for the CMA system.

Field	Description
Use External NTP Server Time Synchronization	(Recommended) Select this check box to synchronize the CMA system date and time with an external NTP server.
IP address or DNS resolved names	The IP address or fully qualified domain name (ASCII only) of the NTP server.
Minutes between synchronization attempts	Input how often the CMA system should synchronize with the NTP server. The default is 60 minutes.

22 Click **Next**.

The **Enterprise Directory** page appears. By default, the CMA system accesses an internal account directory.

23 To continue using the local directory for now, skip to step 25 on page 24. You can integrate with an enterprise Active Directory after you've finished First Time Setup.

Enterprise Directory Server Configuration

24 To integrate the CMA system with an enterprise Active Directory server so that users can include enterprise groups, users, and rooms in their conferences:

a On the **Enterprise Directory** page, select **Integrate with Enterprise Directory Server**.

b To have the system auto-discover the enterprise directory server by querying the DNS, enable **Auto-discover** in the **Integrate with Enterprise Directory Server** section; otherwise, enter the enterprise directory server **DNS Name**.

c As needed, configure these settings on the **Enterprise Directory Server** page.

Setting	Description
Domain\Enterprise Directory User ID	Domain and User ID for an account that the CMA system can use to access the enterprise directory server and retrieve group, user, and room information. This User ID must have read permissions so it can search the entire forest on the enterprise directory server. This User ID is automatically associated with the CMA system administrator role.
Enterprise Directory User Password	The password for the enterprise directory user account.

Setting	Description
Security Level	The level of security on the connection between the CMA system and the Active Directory server. The only possible value for a CMA system set to Maximum Security is: • **StartTLS**—The connection is secured over outbound port 3268 (the same port as **Plain**), but it then negotiates security once the socket is opened. Some enterprise directory servers reject any unsecured transactions, so the first command is the `StartTLS` negotiation command.
Ignore Disabled AD users	Enable this option to have the CMA system ignore disabled enterprise users. Do not enable this option if your enterprise conference rooms are set up as disabled enterprise users.
Enterprise Directory Exclusion Filter	If necessary and you understand filter syntax, specify other types of user accounts to exclude. Don't edit these expressions unless you understand filter syntax. For more information, see "Understanding Exclusion Filters" in the *Polycom CMA System Administrator's Guide*.
Enterprise Directory Search BaseDN	If necessary and you understand filter syntax, specify the top level of the directory tree (referred to as the base DN) to search. Don't edit these expressions unless you understand filter syntax. For more information, see "Understanding Base DN" in the *Polycom CMA System Administrator's Guide*.

Delegated Authentication

25 To integrate the CMA system with an enterprise directory domain controller for authentication:

a On the **Enterprise Directory Server** page, select **Allow delegated authentication to enterprise directory server**.

The CMA system can auto-discover the closest logical domain controller and enterprise directory servers, but to do this the network DNS server must have a DNS SRV record for these servers.

b If your network DNS server has a DNS SRV record for the domain controller, in the **Domain controller name** section enable **Auto-discover**; otherwise, enter the fully qualified hostname of the domain controller (for example, `dc1.mydomain.com`). The pre-staged computer account must be within this domain as well.

c In the **Computer Account Credentials** section, enter the **Domain\Computer Name** and **Password** for the pre-staged

computer account created in "Pre-stage a Computer Account" on page 5.

26 Click **Next**.

The CMA system displays the message that you have completed First Time Setup. You have the option of logging out of the system or being redirected to the system **Dashboard**.

27 Click **Next** to go to the system **Dashboard**.

Reset the System Passwords

28 Go to **Admin > Management and Security Settings > Reset Sysem Passwords**.

29 Click **Reset Passwords and Restart**.

30 Click **Reset Passwords and Restart** to confirm the change.

The system resets the service passwords and restarts. It may take the CMA system up to 10 minutes to shutdown and then restart all server processes.

Complete the Setup

Once you've finished First Time Setup, you may need to perform these configuration tasks:

- As needed, integrate the CMA system with a Microsoft Active Directory enterprise directory.
- Add licenses to your system.
- Set up your site topology.
- As necessary, configure Areas.
- Associate users with roles.
- Associate users and rooms with endpoints.
- Add machine accounts for all managed HDX systems.
- Associate endpoints with users and rooms.
- Add MCUs.
- Schedule a test conference.

For more information on these taskes, refer to the *Polycom CMA System Operation Guide*.