POLYCOM®

Polycom® CMA™ System Deployment Guide for Maximum Security Environments

5.2.0J | September 2011 | 3725-77620-001A1

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 latest information for security-conscious businesses implementing CMA system version 5.2.0J.

This software meets the latest U.S. Department of Defense network requirements for listing on the Defense Switched Network (DSN) Approved Products List (APL), as maintained by the Joint Interoperability Test Command (JITC).

Documentation Resources

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

- *Polycom CMA System Release Notes*
- *Polycom CMA System Getting Started Guide*
- *Polycom CMA System Administrator's Guide*
- *Polycom CMA System Auditor's Guide*
- *Polycom CMA System Web Scheduling Guide*

1

Polycom® CMA™ System Server Setup

This chapter describes the steps required to set up a Polycom® Converged Management Application™ (CMA™) system server and connect it to the network. It includes these topics:

Collect Necessary Materials

Before you install a CMA system, collect these materials:

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

To connect to the CMA system server through an ethernet port, make sure you also have:

- A crossover cable OR
- A hub or a switch and two ethernet cables

Unpack and Install the Hardware Components

The CMA system uses a Polycom-branded Dell PowerEdge R610 server.

To unpack and install the hardware:

1. Examine the 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 CMA system server package includes these items:

   - 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.

2

Prepare for Polycom® CMA™ System Setup

This chapter describes the tasks you can do in advance of installing the Polycom® Converged Management Application™ (CMA™) system to make the process run more smoothly, including:

- Complete the First-Time Setup Worksheet
- Set up DNS Host and Service Records
- Request Certificates
- Pre-stage a Computer Account
- Prepare Client Systems

Complete the First-Time Setup Worksheet

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

Table 2-1 *First-Time Setup Worksheet*

Item	My System Values	Factory-Set Default Values	Description
System Network Settings			
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.
System IPv6 address			Static, physical IP address for the CMA system server on an IPv6 network.

Table 2-1 *First-Time Setup Worksheet (continued)*

Item	My System Values	Factory-Set Default Values	Description
System IPv4 address		192.168.1.254	Static, physical IP address for the CMA system server on an IPv4 network.
System virtual IP address			For redundant Polycom CMA 5000 system configurations only
System subnet mask		255.255.255.0	Network subnet mask of the system server. For IPv4 networks only.
IP address of the default gateway/router IP address		192.168.1.1	IP address of the gateway server. For IPv4 networks only.
IP address of the DNS server			IP address of the domain name server.
IP address of an alternate DNS server			IP address of an alternate domain name server.
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`.
System Time Information			
Current date			
Current time			
Time zone			
IP address of NTP time server (optional)			
External Database Integration (Optional)			
IP address or host name of database server			IP address of the database server
Port			Port number of the Microsoft SQL database instance
User ID and password			Credentials for database administration account with privileges to create databases and accounts.

Table 2-1 *First-Time Setup Worksheet (continued)*

Item	My System Values	Factory-Set Default Values	Description
Enterprise Directory (LDAP) Integration (Optional)			
IP address or DNS name of enterprise directory server			Fully qualified hostname of the enterprise directory server (for example, `dc1.mydomain.com`). The CMA system can auto-discover the enterprise directory server using standard Microsoft services.
Domain, user ID, and password			Credentials for read-only service account that the CMA system uses to perform queries against the Active Directory Global Catalog.
Delegated Authenticaion (Optional)			
Domain controller name			Fully qualified hostname of the domain controller for integrated enterprise directory server (for example, `dc1.mydomain.com`) The CMA system can auto-discover the domain controller using standard services.
Domain, pre-staged computer account name, and password			Credentials for pre-staged computer account used to enable communications with the enterprise directory. See "Pre-stage a Computer Account" on page 7.
Information Required for Polycom Customer Support			
Serial number			
License number			

Set up DNS Host and Service Records

Before installing a CMA system, you should consider configuring your DNS servers to:

- Resolve queries for the CMA system by host name
- Resolve reverse lookup queries for the CMA system
- Identify the CMA system as a service on the network.

The first function requires a DNS host record and optionally a reverse lookup pointer record. The second function requires a DNS service record.

The DNS should also have entries for your Active Directory server, external database server, mail server, and gatekeeper.

For reference information about DNS, DNS records, and how DNS works, see Microsoft Technet (http://technet.microsoft.com/en-us/library/cc772774(WS.10).aspx).

DNS Host Record

To allow your DNS servers to resolve queries for the CMA system by host name, you must enter a DNS host record in your DNS file. The format of this record depends on the format of your network addressing.

- If you use IPv4 addressing, enter a DNS A record in the required format.
- If you use IPv6 addressing, enter a DNS AAAA record in the required format.

To allow your DNS servers to resolve queries for the CMA system by reverse lookup, you must enter a DNS pointer (PTR) record in your DNS file.

Request Certificates

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.

Pre-stage a Computer Account

Before installing a CMA system, an Active Directory administrator must pre-stage an Active Directory computer account for the 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 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 7, <***Password***> is the desired password, and **`/domain`** is literally **`/domain`** (that is, 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.

3. 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**.

Prepare Client Systems

To log into the CMA system for the first time, you need a client system with the following applications.

- Microsoft Internet Explorer® 7.0 or 8.0
- Adobe® Flash® Player 10.0.x.

If you will be working in a closed network environment, make sure these applications are installed on the client system before beginning First Time Setup.

3

Polycom® CMA™ System Software Setup

This chapter describes the Polycom® Converged Management Application™ (CMA™) system software first-time setup tasks. It includes these topics:

Connect to the Polycom CMA System Server

You configure the CMA system server through an ethernet port connection.

To connect to the CMA system through an ethernet port

1. Choose one of the following procedures:
   - 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. Attach a USB keyboard to CMA system server.

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.

Run the First Time Setup Wizard

To log into the CMA system for the first time, you need:

- Microsoft Internet Explorer® 7.0 or 8.0
- Adobe® Flash® Player 9.x or 10.0.x.
- The IP address or host name of the CMA system server.
- A completed first-time setup worksheet. See Table 2-1 on page 3.

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.

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.

To run through the first-time setup wizard

1. Open a browser window and in the **Address** field enter the CMA system default server IP address: 192.168.1.254.
   - If you receive a **Security Alert**, click **Yes**.

     When you successfully complete First Time Setup and certificates are installed, this alert disappears.
2. When the default system **Login Banner** appears, read the banner and click **Accept** to accept the terms and continue.
3. When the CMA system login screen appears, if necessary select a different **Language** or **Domain**.
4. Enter the administrator **Username** and **Password**. The factory default is `admin/admin`.
5. Click **Login**.

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

EULA License Agreement

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

   The **Administrative User** page appears.

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 Table 2-1 on page 3 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 process using the CMA system self-signed certificate, go to step 18.

17 To suspend the First Time Setup process 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 **Secure the System and 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 in steps 7 and 8.

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.
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**.

Enterprise Directory Server Configuration

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 16. You can integrate with an enterprise Active Directory after you've finished First Time Setup.

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.
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.

Setting	Description
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 "Connect to the Polycom CMA System Server" on page 9.

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.

4

Working with a Polycom CMA System at Maximum Security Level

This document provides the latest information for security-conscious businesses implementing CMA system version 5.2.0J. It has the following sections:

- Log Into the Polycom CMA System
- Polycom CMA System Site Map
- Roles, Permissions, and Functions
- Polycom CMA System Functionality
  - Conference Scheduling
  - Endpoint Management
  - Network Device Management
  - User Management
  - Group Management
  - Reporting
  - Device Administration
  - System Administration
  - Restore from a Backup Archive
  - Troubleshooting

IMPORTANT

A CMA system running v5.2.0J operates at Maximum Security level, the level required in a strict security networks, and this security level cannot be changed.

Log Into the Polycom CMA System

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

- Microsoft Internet Explorer® 7.0 or 8.0
- Adobe® Flash® Player 10.x
- The IP address or, preferably, host name of the CMA system and your user name, password, and domain.A certificate installed in your browser that has a root Certificate Authority (CA) that matches the root CA installed on the CMA system

By default, the system gives you three opportunities to enter a correct password. (A user assigned the **Administrator** role can change this option.) After three failed attempts, the system returns an error message.

To log into a CMA system

1. Open a browser window and in the **Address** field enter the CMA system server IP address.
   - If you cannot connect, there are likely certificate issues.
   - If you receive a **Security Alert**, click **Yes**.
   - If prompted to install the Adobe Flash Player, click **OK** and follow the installation instructions. If you have access to the Internet, the preferred method is to install the latest version from Adobe.
2. When the default system **Login Banner** appears, read the banner and click **Accept** to accept the terms and continue.
3. When the CMA system login screen appears, enter your **Username** and **Password**.
4. If necessary, select a different **Language** or **Domain** and click **Login**.

   Because the CMA system is a role-based system, users see only the pages and functions available to their role.

Polycom CMA System Site Map

The following figure shows the site map for a CMA system running v5.2.0J. It illustrates the organization of the system interface and the pages available to each of the pre-defined CMA system roles.

ADMINISTRATOR

- Endpoint
  - Monitor View
- Network Device
  - Monitor View
  - MCUs
- User
  - Users
  - Groups
  - Guest Book
- Reports
  - Endpoint Usage Report
  - Conference Type Report
  - System Log Files
  - Audit Log Files
- Admin
  - Dashboard
  - Conference Templates
  - Conference Settings
  - Provisioning Profiles
    - Automatic Provisioning Profiles
  - Software Updates
    - Automatic Software Updates
  - Rooms
  - Areas
  - Server Settings
    - Network
    - System Time
    - Enterprise Directory
    - Licenses
    - Custom Logo
    - Directory Setup
- Admin (continued)
  - Management and Security
    - Server Software Upgrade
    - Certificate Management
    - Session Management
    - Banner Configuration
    - Local User Account Configuration
    - Local Password Requirements
    - Anti-virus Protection
    - Reset System Passwords
  - Dial Plan and Sites
    - Site Topology
    - Sites
    - Site-Links
    - Site-to-Site Exclusions
    - Network Clouds
    - Territories
    - Dial Rules
  - Backup System Settings
  - Database Backup Files
  - Troubleshooting Utilities
  - Report Administration

DEVICE ADMINISTRATOR

- Endpoint
  - Monitor View
  - Automatic Provisioning
  - Automatic Software Update
- Network Device
  - Monitor View
  - MCU
- Admin
  - Dashboard
  - Rooms
  - Management and Security
    - Machine Accounts

OPERATOR

- Conference
  - Future
  - Ongoing
- Endpoint
  - Monitor View
- Network Device
  - MCUs
- User
  - Guest Book
  - Favorites
- Reports
  - Conference Usage Report

SCHEDULER/ADVANCED SCHEDULER

- Conference
  - Future
  - Ongoing
- User
  - Guest Book

VIEW-ONLY SCHEDULER

- Conference
  - Future

AUDITOR

- Reports
  - Endpoint Usage Report
  - System Log Files
  - Audit Log Files

Roles, Permissions, and Functions

The following sections identify the pre-defined roles for a CMA system running v5.2.0J and the permissions with which they are associated.

> **Note**
>
> The role names (for example, **Administrator**, **Operator**, and **Scheduler**) are stored in the system database and are not localized into other languages.

No Predefined Role

This role is new to the CMA system running v5.2.0J. By default, when new local users are added to the system, they are assigned **No Predefined Role**. By default, when the CMA system is integrated to an enterprise directory server, all enterprise users are assigned **No Predefined Role**.

Users who have **No Predefined Role** cannot access the system; they have no permissions or functions available to them until they are explicitly assigned a role by a user assigned the **Administrator** role.

Administrator

When users who are assigned the **Administrator** role log into the CMA system, they see the **Endpoint**, **Network Device**, **User**, **Reports,** and **Admin** menus and the system **Dashboard** is displayed. They have access to all CMA system functionality except that associated with auditing the system and scheduling, monitoring, or managing conferences or devices.

If a CMA system has areas defined, administrators can only monitor devices within their designated area or areas.

Device Administrator

This role is new to the CMA system running v5.2.0J. When users who are assigned the **Device Administrator** role log into the CMA system, they see the **Endpoint**, **Network Device**, and **Admin** menus and the system **Dashboard** is displayed. They can perform device-related functions including adding, editing, and deleting endpoints and MCUs and monitoring endpoints including provisioning and software update operations.

If a CMA system has areas defined, device administrators can only manage devices within their designated area or areas.

Auditor

This role is new to the CMA system running v5.2.0J. When users who are assigned the **Auditor** role log into the CMA system, they see the **Reports** menu and the system **Audit Log Files** page is displayed. They can run specific

system reports that document security-related events, such as successful and unsuccessful login attempts, gathered from the CMA system. They can also backup, archive, and then delete audit logs.

Operator

When users who are assigned the **Operator** role log into the CMA system, they see the **Conference**, **Endpoint**, **Network Device**, **User**, and **Reports** menus and the **Ongoing** conference page is displayed. They can monitor and manage all ongoing CMA system conferences; monitor all devices; delete entries from the system **Guest Book**; and view some system reports.

Scheduler

When users who are assigned the **Scheduler** role log into the CMA system, they see the **Conference** and **User** menus and the **Future** conference page is displayed. They can schedule, monitor, and manage their own conferences. They can also delete entries from the system **Guest Book**. They cannot see conferences that they did not create.

Advanced Scheduler

When users who are assigned the **Advanced Scheduler** role log into the CMA system, they see the **Conference** and **User** menus and the **Future** conference page is displayed. They can schedule, monitor, and manage their own conferences. They can also edit some conference settings for their scheduled conferences and delete entries from the system **Guest Book**. They cannot see conferences that they did not create.

View Only Scheduler

When users who are assigned the **View Only Scheduler** role log into the CMA system, they see the **Conference** and **User** menus and the **Future** conference page is displayed. They can monitor all ongoing CMA system conferences within the areas to which they are associated.

Polycom CMA System Functionality

This CMA system v5.2.0J release supports a different set of features than the more commercial but less secure CMA system releases, and there are many operational differences.

- This release includes support for the following new features:
  - Software updates in a maintenance window
  - Monitoring HDX systems through an XML API
  - Secure `https`
  - Encrypted passwords
  - IPv6
  - User account management
  - Session management
  - Certificate management
  - Areas
  - Multiple time servers
  - Multiple DNS servers
  - Standard and customized login banner
  - Backup and restore of system settings
- This release include support for the following devices:
  - Polycom HDX endpoints running version 2.7.0J operating in dynamic management mode and configured at Maximum Security level.
  - Multipoint conferencing on Polycom RMX 1500/2000/4000 conferencing platforms running version 7.0.1J and configured at Maximum Security level.
- This release does not include support for the following features:
  - Operation on CMA 4000 hardware
  - CMA system gatekeeper functionality
  - Redundant configurations
  - External databases
  - ISDN scheduling
  - Global Address Book
  - Standard (scheduled) management and monitoring of endpoints
  - Presence
  - SNMP
  - Remote desktop

- Integration with Microsoft Exchange for calendaring
- Integration with Microsoft Office Communications Server
- Polycom CMA Desktop clients
- Polycom Scheduling Plug-ins for Microsoft Outlook and IBM Lotus Notes
- Least Cost Routing
- Audio only conferences
- Online Help

The following sections describe in detail the operational differences for a CMA system running v5.2.0J.

Conference Scheduling

Conference scheduling functionality is available to users assigned the basic scheduler, advanced scheduler, and operator roles. The conference scheduling workflow on a CMA system running v5.2.0J has not changed. However, because all conferences must be hosted on RMX conferencing systems, the **MCU Settings** for all **Conference Templates** has changed in the following ways:

- The **Supported MCUs** section lists only **RMX** systems.
- The **Always Use MCU** option on the **Conference Template** page is not available (grayed-out); it is always enabled and cannot be changed.

Endpoint Management

Endpoint management functionality is available to users assigned the device administrator role. Users assigned the standard administrator role may only monitor endpoints.

The endpoint management workflow on a CMA system running v5.2.0J has changed in that a CMA system running v5.2.0J only supports HDX system endpoints operating in dynamic management mode. The system changes made to support this workflow change include:

- The **Scheduled Provisioning** and **Scheduled Software Update** pages and the **ACTIONS** associated with them are not available.
- Only HDX system endpoints that are automatically provisioned by the CMA system are displayed in the endpoint list.

- The **ACTIONS** on the **Endpoint > Monitor View** page changes as follows:

Command	Use this command to...
Add 	Not available in this release. Endpoints can only be added to the system during automatic provisioning.
Search Devices	Not available in this release.

- The **Device Summary** section of the **Endpoint > Monitor View** page does not change.
- The **Device Status** section of the **Endpoint > Monitor View** page changes as follows:

Field	Description
Gatekeeper Registration	The status of the device's registration with the gatekeeper service always indicates  **Unknown**.
Directory Registration	The status of the device's registration with the Global Directory Service always indicates  **Not Registered**.
Presence Registration	Not displayed in this release.
Exchange Registration	Not displayed in this release.
SIP Registration	Not displayed in this release.
Device Managed	Indicates **Heartbeat Timeout**.
Gatekeeper Address	New field. The IP address of the gatekeeper to which the device is registered.
Last GK Registration	Field blank in this release.
ISDN Line Status Type	Field blank in this release.
ISDN Assignment Type	How the ISDN type was assigned to the device. This always indicates **Undefined**.
Device ISDN Type	Field blank in this release.

- The **Call Info** section of the **Endpoint > Monitor View** page does not change.

- The **Device Alerts** section of the **Endpoint > Monitor View** page changes as follows:

Field	Description
Errors	Device error message text always shows **Gatekeeper Unregistered**.

- The **Provisioning Details** section of the **Endpoint > Monitor View** page does not change.

Network Device Management

Network device management functionality is available to users assigned the device administrator role. Users assigned the standard administrator role may only monitor network devices.

The network device management workflow on a CMA system running v5.2.0J has changed in that a CMA system running v5.2.0J supports only RMX conferencing systems. The system changes required for this workflow change include:

- The **VBPs** and **DMAs** pages and the **ACTIONS** associated with them are not available.
- The **ACTIONS** on the **MCU > Monitor View** page do not change.
- The **Add New Device** dialog box for the RMX MCU does not change. Note that in a maximum security environment, the **Admin ID** for an MCU is the CMA machine account created on the RMX system just for this purpose and the **Password** is the password designated for this CMA machine account.

User Management

User management functionality is divided among different roles: scheduler, operator, and administrator.

Scheduler

Users assigned the basic scheduler and advanced scheduler role can add guest participants to the **Guest Book**.

The **Guest Book** workflow for schedulers on a CMA system running v5.2.0J has not changed.

Operator

Users assigned the operator role can add, edit, and delete guest participants from the **Guest Book** as well as add, edit, and delete their own **Favorites** lists.

The **Guest Book** and **Favorites** workflow for operators on a CMA system running v5.2.0J have not changed.

Administrator

The administrator's user management functionality and workflow has changed significantly on a CMA system running v5.2.0J.

When integrated with an enterprise directory (Microsoft Active Directory), the CMA system can have only one local account—the default administrator account used to access and administer the system. This account cannot be deleted in any circumstances.

When integrated with an enterprise directory, this local administrator can perform the following user management functions:

- Integrate the CMA system with Active Directory. Note that when you integrate the CMA system with an Active Directory, all local users other than the default local administrator are removed from the system.
- Edit a subset of enterprise user attributes, such as their role, area, or endpoint associations. This allows the local administrator to assign the administrator role to enterprise users.
- Troubleshoot and administrate the system if the Active Directory connection to the system is lost.

When not integrated with an enterprise directory, this local administrator can perform the following user management functions:

- Add and edit local user attributes including their contact information and other user attributes such as their role, area, or endpoint associations.
- Delete local users.

As a best practice, use this local administrator account for user management tasks on the CMA system. Do not use it to log into managed devices.

The user management workflow on a CMA system running v5.2.0J has changed in the following ways:

- Once integrated with an enterprise directory, the local administrator see enterprise users as well as associate them to endpoints, roles, and areas (when applicable).

- Administrators can no longer create custom roles with a custom set of permissions. The system has only pre-defined roles and associated permissions as described in "Roles, Permissions, and Functions" on page 22.

  The system changes required to support this workflow change are:

  – The **User Roles** page and the **ACTIONS** associated with it are not available.

  – The **ACTIONS** on the **User > Users** page includes a new command, so that you can view the permissions that come with the role a user has been assigned.

Command	Use this command to...
View Permissions	New field. Display the set of permissions that come with the user's assigned role.

- Administrators can no longer assign users more than one role.

  The system change required to support this workflow change is:
  The user interface for assigning roles (**Add/Edit User > Associated Roles**) has changed to a radio button list from which you can assign only one role from a set of mutually exclusive, predefined options.

- Via the **Edit** function, local administrators can now enable and disable local users rather than permanently deleting their user accounts. This function is only available for local users. Enterprise users must be enabled and disabled in Active Directory.

Disabled local users (when not integrated with an enterprise directory) still appear in the CMA system **Users** list. However, disabled enterprise users (when integrated with an enterprise directory) won't appear in the CMA system **User** list if the **Ignore Disabled Enterprise Directory Users** option on the **Enterprise Directory** page is enabled.

  The system change required to support this workflow change is:
  The **General Info** tab of the **Edit User** dialog box now has an **Enable User** option. By default, when a local user is created, this option is selected.

- Via the **Edit** function, administrators can unlock user accounts that become locked when a user reaches the **Failed login threshold**.

Administrators cannot lock user accounts. This functionality is triggered only when the failed login threshold is met.

The system change required to support this workflow change is:
The **General Info** tab of the **Edit User** dialog box now has an **Unlock User** option. By default, when a local user is created, this option is not selected. However, when a local user reaches the **Failed login threshold**, the administrator can reset the lock by enabling the **Unlock User** option.

- Users can no longer be associated with an alert profile because a CMA system running v5.2.0J does not include remote alerts.

  The system change required to support this workflow change is:
  The **Add/Edit User > Associated Alert Profile** tab has been removed from the user interface.

A CMA system running v5.2.0J also includes new password requirements, local user account configuration requirements, and session management requirements that affect local users and local user accounts. For more information about these requirements, see "Management and Security" on page 36.

Group Management

Group management functionality is available to users assigned the administrator role.

The group management workflow on a CMA system running v5.2.0J has not changed except that users can no longer inherit roles from groups.

When not integrated with an enterprise directory, local administrators can add local groups with local users. When integrated with an enterprise directory, the single local administrator and any enterprise users assigned the administrator role can **Add** local groups, **Import Enterprise Groups**, and **Synchronize Groups** with Active Directory.

Reporting

Reporting functionality is divided among different roles: administrator, operator, and auditor.

Administrator

The administrator's reporting functionality and workflow has changed on a CMA system running v5.2.0J. Users assigned the administrator role can access the following system reports:

- Endpoint Usage Report
- Conference Type Report
- System Log Files
- Audit Log Files (New)

Users assigned the administrator role can no longer access the following system reports, since these reports have been removed from the system:

- Site Statistics
- Site-link Statistics
- IP Call Detail Records
- Conference Usage Report
- Gatekeeper Message Log

For more information on these reports, see the *Polycom CMA System Administrator's Guide*.

Operator

The operator's reporting functionality and workflow has changed somewhat on a CMA system running v5.2.0J. Users assigned the operator role can only access the following system report:

- Conference Usage Report

Users assigned the operator role can no longer access the following system reports:

- IP Call Detail Records
- Endpoint Usage Report
- Gatekeeper Message Log

For more information on these reports, see the *Polycom CMA System Administrator's Guide*.

Auditor

Users assigned the auditor role can access the following system reports:

- Endpoint Usage Report
- System Log Files
- Audit Log Files

For more information on these reports, see the *Polycom CMA System Administrator's Guide*.

The auditor role is new. The auditor workflow on a CMA system running v5.2.0J allows the auditor to:

- View online the **Endpoint Usage Report** for selected endpoints.

  The system change required to support this workflow change is:
  The **Endpoint Usage Report** menu option and page is available from the **Reports** menu, but the **Generate Report** and **Download All CDRs** options are not available to the auditor.

- Download the **System Log Files**.

  The system changes required to support this workflow change are:

  — The **System Log Files** menu option and page is available from the **Reports** menu.

  — The **Download ALL** command is available from the list of **ACTIONS**.

- **Backup and Delete** audit log files.

  The system changes required to support this workflow change are:

  — The **Audit Log Files** menu option and page is available from the **Reports** menu.

  — The **Backup and Delete** command is available from the list of **ACTIONS**. This option allows an auditor to backup and delete selected audit logs. During this process, the CMA system requires that the auditor download and run a verification utility that performs a checksum operation to make certain that the downloaded audit log is complete and uncorrupted before the audit log is deleted from the CMA system.

- Change the audit log **Alert Level**.

  The system change required to support this workflow change is:
  The **Change Settings** command is available from the list of **ACTIONS**. By default the audit log **Alert Level** is set to 70% of the **Max File Size Usage**, which is 2 gigabytes.

Device Administration

Only users assigned the new device administrator role can perform device administration tasks.

The device administrator role is new. In addition to the tasks described in the Endpoint Management section, the device administrator workflow on a CMA system running v5.2.0J allows the device administrator to:

- See the system **Dashboard**.
- Add, edit, and delete machine accounts for endpoint systems.

  The system change required to support this workflow change are:

  — The **Machine Accounts** menu option and page is available from the **Admin > Management and Security** menu. This option is new. Before the CMA system can dynamically manage a HDX system, a device administrator must add a machine account for the HDX system. This is the same username that the HDX system administrator should enter on the HDX system for the provisioning service. This allows the HDX and CMA systems to authenticate and communicate without using a specific user's account.

About Machine Accounts

Before the CMA system can dynamically manage HDX systems in a maximum security environment, a user assigned the **Device Administrator** role must create an HDX machine account for each HDX that the CMA system will manage. The machine account allows the endpoint to connect and authenticate with the CMA system for dynamic management purposes without using the endpoint user's account.

The **Add Machine Account** dialog box includes the following information.

Field	Description
Enable Machine Account	Select or clear this option to enable and disable (respectively) the machine account you create for the endpoint.
Unlock Machine Account	Select this option to unlock machine accounts that become locked when they exceed the Failed login threshold. This will only happen when the password expires.
User ID	Enter a unique name for the machine account. As a best practice, name the machine account in a way that associates it with the corresponding device. For example, if your company names endpoint systems for the system user or room (for example, `bsmith_HDX` or `Evergreen_Room`), then give the machine account an associated **User ID** (`bsmith_HDX_machine` or `evergreen_room_machine`).
Password/ Confirm Password	Enter a password for the machine account user ID. This password must meet the **Local Password Requirements**. This password expires in 365 days.
Description	Enter a meaningful description for the endpoint.
Associate with an existing user or room	Select this option to associate the endpoint system with a specific user or room. This may be a local or enterprise user or room.
Associate with a new room (created automatically)	Select this option to associate the endpoint system with a system-generated room name.

Once you have created this machine account on the CMA system, provide this information to the appropriate HDX system administrator. They should enter this **User ID** and **Password** as the **User Name** and **Password** on the HDX **Provisioning Service** page.

Note that the machine account password expires after one year. After the expiration, the HDX login will fail. After three failed login attempts, the system locks the machine account. You can reset the password and unlock the machine account by editing it and assigning a new password.

System Administration

Only users assigned the administrator role can perform general CMA system administration functions. The CMA system administration functionality and workflow has changed on a CMA system running v5.2.0J. The following sections describe the areas of functionality and how they have changed.

Users assigned the administrator role can see the system **Dashboard**, the **Admin** menu, and the pages and **ACTIONS** associated with it.

Admin Menu

The **Admin** menu in this release has changed in the following ways:

- The **Global Address Book**, **SNMP Settings**, **Gatekeeper Settings**, and **Alert Settings** menu options and their associated functionality have been removed.
- Removing the gatekeeper functionality in this release resulted in the following system changes:
  - The system cannot display bandwidth usage. Bandwidth usage is for sites, subnets, or site limits is always 0.
  - Site exclusions cannot be enforced.
  - Dial rules are required for ISDN calling in translating numbers, but have no affect for IP calls.
  - The system is not the gatekeeper, so it cannot perform address resolution.
  - E164 aliases assigned by the CMA system are not communicated to the gatekeeper, so they cannot be resolved.
  - Dialing rules can be configured on the CMA system, but they are not communicated to the gatekeeper, so they cannot be implemented.
  - Threshhold alarms and hardware alarms are always 0.
  - Site topology cannot provide a graphical representation of status (color) .
  - The CMA system has no knowledge of external gatekeeper or its rules

Conference Templates

As was noted before, because all conferences scheduled on a CMA system running v5.2.0J must be hosted on a RMX conferencing system, the **MCU Settings** for all **Conference Templates** has changed in the following ways:

- The **Supported MCUs** section lists only **RMX**.
- The **Always Use MCU** option on the **Conference Template** page is not available (grayed-out); it is always enabled and cannot be changed.

Conference Settings

On a CMA system running v5.2.0J, a new setting is available on the **Conference Setting** page. The **Conference and chairperson password length** field allows an administrator to designate the required length of the system-generated conference password and chairperson password. The acceptable length for both of these passwords is six to 16 characters. By default, the required length for both of these passwords is set to 15 characters.

Note

Depending on the system settings, the scheduler may be allowed to change the Conference Password or Chairperson Password. However, the password length requirement still applies.

Other than this requirement, the conference settings, conference password, and chairperson password workflows have not changed.

Provisioning Profiles

Because a CMA system running v5.2.0J supports only HDX endpoints running version 2.7.0J operating in dynamic management mode, the **Scheduled Provisioning Profiles** page and the **ACTIONS** associated with it are not available.

The **Automatic Provisioning Profiles** page and the **ACTIONS** associated with it has not changed on a CMA system running v5.2.0J

Software Updates

Because a CMA system running v5.2.0J supports only HDX endpoints running version 2.7.0J operating in dynamic management mode, the **Scheduled Software Update** page and the **ACTIONS** associated with it are not available.

The **Automatic Software Update** page and the **ACTIONS** associated with it has not changed on a CMA system running v5.2.0J.

Server Settings

The **Server Settings** menu for a CMA system running v5.2.0J has changed significantly. The following options have been removed:

- Database
- Calendaring Management
- Microsoft Lync or Office Communications Server Integration
- Redundant Configuration
- Remote Alert Setup
- E-mail

In addition, you will also note the following changes and additions:

- The **Network** settings page now includes the ability to enable IPv6 and to include a preferred and alternate DNS server.
- The **System Time** page does not include the **Minutes Between Synchronization** option when using an NTP server.
- What was formerly titled the **LDAP** page is now titled the E**nterprise Directory** page.
- On the **Enterprise Directory** page:
  - You must identify the enterprise directory by **DNS Name**. You can no longer identify the enterprise directory server by IP address.
  - The **Security Level** defaults to StartTLS and cannot be modified.
- The **Reclaim Inactive CMA Desktop Licenses** option has been removed from the **Licenses** page.
- The **CMA Desktop Logo** option has been removed from the **Custom Logo** page.
- The **Include dynamically-managed devices in the Global Address Book** option has been removed from the **Directory Setup** page.

Management and Security

A CMA system running v5.2.0J offers a new **Management and Security** workflow. The following sections describe the changes.

Server Software Upgrade

The **Server Software Upgrade** workflow on a CMA system running v5.2.0J has not changed.

Certificate Management

Because a CMA system running v5.2.0J always operates in encrypted mode, the **Use HTTPS** is not an option on the Certificate Management page.

By default, to support encrypted communications and establish a minimum 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. However, you can complete First Time Setup with just the root CA certificate and the CMA system default self-signed certificate. Then you can use the Certificate Management page to finish certificate set up.

Session Management

The **Session Management** page, which is new in this release, allows an administrator to change but not disable the following settings:

Field	Description
CMA user interface timeout	By default the CMA system user interface times out after 10 minutes of inactivity. Use this procedure to change the timeout value for the user interface inactivity timer. Possible value is 5 to 60 minutes.
Maximum number of sessions per user	The number of simultaneous login sessions per user ID. Possible value is 1 to 10 sessions.
Maximum number of sessions per system	The number of simultaneous login sessions by all users. Possible value is 2 to 50 sessions. **Note** If this limit is reached, but none of the logged-in users is an Administrator, the first Administrator user to arrive is granted access, and the system terminates the non-Administrator session that's been idle the longest.

Banner Configuration

The **Banner Configuration** page allows users assigned the **Administrator** role to customize (but not disable) the long and short login banners.

A log in banner is the message that appears when users attempt to access the system. Users must acknowledge the message before they can log in.

By default, the long banner field on the **Banner Configuration** page displays the required Standard Mandatory Notice and Consent Provision for systems operating in a maximum security environment. The short banner field displays a shortened version of this same notice.

The long banner is used for the CMA system log in banner. It is also provisioned to HDX systems that the CMA system manages. The short banner is provisioned to HDX systems that the CMA system manages for those situations in which the long banner length exceeds the available display area.

The CMA system provides several sample long banners. You can use these banners as is or edit them to create a custom long banner. The CMA system provides a single short banner, which you can also customize. If you customize the banners, remember that the long banner message may contain up to 5000 characters. The short banner message may contain up to 1315 characters.

Local User Account Management

The **Local User Account Management** page, which is new in this release, allows an administrator to change but not disable the following local user account settings:

Field	Description
Account Lockout	
Failed login threshold	Specify how many consecutive login failures cause the system to lock an account. Possible value is 2 to 10.
Failed login window (hours)	Specify the time span within which the consecutive failures must occur in order to lock the account. Possible value is 1 to 24.
Customized user account lockout duration (minutes)	Specify how long the user's account remains locked. Possible value is 1 to 480.
Account Inactivity	
Customize account inactivity threshold (days)	Specify the inactivity threshold that triggers disabling of inactive accounts. Possible value is 30 to 180.

Local Password Requirements

The **Local Password Requirements** page, which is new in this release, allows an administrator to change but not disable password security requirements by specifying password age, length, and complexity.

Field	Description
Password Management	
Maximum password age (days)	Specify at what age a password expires. Possible value is 30 to 180.
Minimum password age (days)	Specify how frequently a password can be changed. Possible value is 1 to 30.
Password warning interval (days)	Specify when users start to see a warning about their password expiration. Possible value is 1 to 7.
Minimum length	Specify the number of characters a password must contain. Possible value is 8 to 18.
Minimum changed characters	Specify the number of characters that must be different from the previous password. Possible value is 1 to 4.

Field	Description
Reject previous passwords	Specify how many of the user's previous passwords the system remembers and won't permit to be reused. Possible value is 8 to 16.
Password Complexity	
Lowercase letters	Specify the number of lowercase letters (a-z) that a password must contain. Possible value is 1 or 2.
Uppercase letters	Specify the number of uppercase letters (A-Z) that a password must contain. Possible value is 1 or 2.
Numbers	Specify the number of digit characters (0-9) that a password must contain. Possible value is 1 or 2.
Special characters	Specify the number of non-alphanumeric keyboard characters that a password must contain. Possible value is 1 or 2.
Maximum consecutive repeated characters	Specify how many sequential characters may be the same. Possible value is 1 to 4.

Anti-virus Protection

The **Anti-virus Protection** page, which is a new option on the **Dashboard** and **Admin** menu (**Admin >Management and Security > Anti-virus Protection)** in this release, allows an administrator to enable a McAfee anti-virus software scan. It offers the following functionality:

Field	Description
Enable anti-virus service	Turns on the McAfee® scan engine service. This service is always enabled.
Protection Status	
Scan engine	Version of the anti-virus scan engine.
Signature info	Version of the signature file.
Signature date	Date of the signature file.
Last signature update	Date the signature file was last updated manually.
Last automatic update	Date the signature file was last updated automatically.
Last system scan	Date the system was last scanned.

Field	Description
Daily Scanning	
Run at ____ every	Configures the anti-virus service to scan the file system at the specified time. Enter the time and select one or more days to run the scan.
Abort if not completed within____ minutes	Select this option if you want to ensure the scan does not take longer than the specified amount of time. Enter the number of minutes the scan should not exceed. Scans may take well over 60 minutes. Be sure to give the scan enough time to complete.
Cancel Scan	Click to cancel the currently running scan.
Manual Updates	
Upload signature update file	Click to upload an updated virus signature file that you have downloaded from the McAfee® signature server or other server where the signature file is available.
Automatic Updates	
Run at	Enter the time for the automatic update.
Signature file URL	Configures the anti-virus service to retrieve updated virus signature files from the McAfee site at the scheduled time.

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

IMPORTANT

- Schedule anti-virus scans and signature file updates in accordance with your site policies.
- Anti-virus scans impose a significant burden on the system that could impact system performance. Schedule system scans for times when the system is in maintenance mode or when little or no conferencing activity is anticipated.

Reset System Passwords

The CMA system has several underlying service passwords. The **Reset System Passwords** page, which is new in this release, allows an administrator to reset these underlying service passwords. When you select this option, all of these underlying service passwords will be changed to the same obscured system-generated value.

Dial Plan and Sites

The **Dial Plan and Sites** workflow on a CMA system running v5.2.0J has changed. The **Least Cost Routing** and **Services** menu options and their associated functionality have been removed. Also because the CMA system is not the gatekeepr, the CMA system **Site Topology** display is less informative. It used data provided to it by the gatekeeper functionality.

Backup System Settings

A CMA system running v5.2.0J offers the new **Backup System Settings** feature, which allows an administrator to create an archive that includes not only a backup of the CMA system databases but also all CMA system configuration settings.

The process for backing up the CMA system settings is:

1 Generate Database Backup Files.

2 Create and Download a Backup Archive.

To restore a system from a backup archive

1 **Restore the system to its factory default configuration**. You will need the **Restore to Factory Default DVD** that shipped with the CMA system server. This DVD has the base image of the CMA system server software.

WARNING

- This is a last resort, so never do this without being instructed to do so by PGS support.
- This process will wipe out your system database and all other system data.
- The **Restore to Factory Default DVD** is specific to the CMA system server type and version.

2 **Perform First Time Setup**. For more information about First Time Setup, see the *Polycom CMA System Getting Started Guide* for this release.

3 **Restore the system configuration** using the last archived configuration. The archived configuration will overwrite the configuration that resulted from First Time Setup. The only CMA system configuration settings not included in the archive and thus not overwritten are the network settings and the security certificates required for an operational system.

In cases when the CMA system is functional, but the configuration or database is corrupted, the backup archive can also be used to return a CMA system back to its last known good archive. As long as the network settings and security certificates are operational, the last known good archive will return the CMA system to its former functional state.

Restore from a Backup Archive

A user with the **Administrator** role can restore the CMA system using a backup archive.

To restore a backup archive

1. Go to **Admin > Backup System Settings**.
2. In the Select Archive File in the **Backup System Settings** page, click ....
3. In the **Select file to upload** dialog box, select the archive file to upload and click **Open**.
4. Click **Restore from Backup Archive**.

   The system uses the archive file to restore the CMA system to the state of the backup files.

Database Backup Files

There is no change in the **Database Backup Files** functionality.

Network Intrusion Detection

The CMA system detects network intrusions by processing the Microsoft Windows Firewall logs, inserting dropped packet information into a temporary system database table, and identifying certain patterns in the data.

The CMA system detects the following types of instrusions: a fast port scan, a slow port scan, a denial of service (DoS) attack, and a flood attack. These are currently defined as:

- Fast port scan:
  10 connections in a 5-second time period from the same source IP.
- Slow port scan:
  100 connections in a 1-hour time period from the same source IP.
- DoS attack:
  100 connections in a 5-second time period to the same destination port.
- Flood attack:
  100 connections in a 5-minute window to any destination port from any source IP.

If the CMA system detects an intrusion, it displays a system alert on the user interface. The alert text will indicate the type of intrusion detected, such as:

- Port scan detected. See audit log for details.
- DoS attack detected. See audit log for details.
- Flood attack detected. See audit log for details.

Troubleshooting

Troubleshooting Utilities

A CMA system running v5.2.0J has most of the same troubleshooting utilities of the standard commercial CMA system; however the **Traces** functionality has changed and new functionality has been added. The following sections describe the troubleshooting utilities.

Windows Event Logs

There is no change in the **Windows Event Logs** function.

CMA System Logs

There is no change in the **CMA System Logs** function.

Database Backup

There is no change in the **Database Backup** function.

Test Network Connect

The **Test Network Connect** function, which is new in this release, allows you to perform a **Traceroute** or **Ping** operation. **Traceroute** allows you to investigate the route path and transit times of packets as they travel across an IP network. **Ping** allows you to test the availability of a host on an IP network.

Synchronize Certificate Stores

The **Synchronize Certificate Stores** function, which is new in this release, allows you to reset all certificate stores with the currently uploaded certificates and certificate revocation lists (CRLs).

Systems

The **Systems** pane displays summary information about the devices that access the CMA system. For a CMA system running v5.2.0J, systems are limited to **Endpoints**, **MCUs**, and **Rooms**.

CMA Configuration

The **CMA Configuration** pane displays information about the configuration of the CMA system. For a CMA system running v5.2.0J, configuration items are limited to **Software Version**, **Hardware Version**, **Enterprise Directory**, **Database**, **Time Source**, and **Enterprise Directory DC** (Domain Controller).

CMA Info

The **CMA Info** pane displays general information about the CMA system. For a CMA system running v5.2.0J, this includes the following:

- Standard information:
  CPU Utilization, Paging File Utilization, Last Hard Start/Reboot, Provisioning Operations in Progress operations, Software Update Operations in Progress, Hardware Alarms, Threshold Alarms, Temperature, Power Supply Status, Battery Status, and Cooling Fan Status.
- New information:
  Total Memory, Free Memory, and Partition States.

CMA Licenses

There is no change in the **CMA Licenses** function.

Users Logged-In

The **Users Logged In** pane displays the type and number of users that are currently logged into the system. For a CMA system running v5.2.0J, this includes a new user role of **Auditor**.

Services

The **Services** pane displays information about the CMA system services, including the running services and the stopped services. For a CMA system running v5.2.0J, there are 8 services rather than the 14 services in a commercial CMA system. The following table lists the services, their purpose, and whether or not they are essential to the health of a CMA system running v5.2.0J.

Service	Manages the system's...	Comment
Apache2	Web processes	Essential
MSSQLSERVER	Database processes	Essential
OpenDS	Site topology database	Essential
openfire	Presence/XMPP processes	Not available
Polycom Cascader	Cascaded conferencing processes	Required for cascading conferences
Polycom Conference Scheduling Service	Conference scheduling processes	Essential
Polycom Device Manager	Device management processes	Not Available
Polycom DialRuleService	Dial rule management processes	Essential
Polycom Gatekeeper	Gatekeeper processes	Not Available

Service	Manages the system's...	Comment
Polycom JServer	Java processes including LDAP, SNMP, device management, Site Topology, and dynamically-managed device logins and provisioning.	Essential
Polycom Master Service	Basic operation processes	Essential
Polycom Serial COM	Serial port management processes	Not Available
Polycom Service Monitor	Redundancy monitoring processes	Not Available
Polycom Global Address Book	Global Address Book management processes	Not Available

Report Administration

The only **Report Administration** function supported on a CMA system running v5.2.0J is the **Days to keep Conference and Endpoint CDRs**. All other **Report Administration** functions including creating and storing a weekly archive of the CDRs is not available in this release.