



▶ Polycom® CMA™ System  
Upgrade Guide

---

## 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.

© 2012 Polycom, Inc. All rights reserved.

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

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

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

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

# Contents

<b>1</b>	<b>Prepare for Polycom® CMA™ System Upgrade</b>	<b>1</b>
	Complete the First-Time Setup Worksheet	1
	Request or Locate Current Recovery DVD	2
	Request Certificates (Optional)	3
	Request a Software Upgrade Key Code	3
	Request the CMA System v6.0 Software and Patch	4
	Download Endpoint and Peripheral Software Updates	4
	Connect to the Polycom CMA System Server	5
<b>2</b>	<b>Upgrading a Non-Redundant Polycom CMA System</b>	<b>7</b>
	Save a Backup of the Polycom CMA System Databases	8
	Install the CMA System Pre-upgrade Patch	9
	Back Up the CMA System	10
	Re-image the CMA System with v6.0	10
	Perform the First-Time Setup	11
	Restore the System Backup	13
	Integrate the CMA System to the External Database	14
	Enter the Software Upgrade Key Code	15
	Verify the Upgrade	15
	Provision SIP Settings for Microsoft Lync or Microsoft Office Communications Server Integration	15
	Upload Endpoint and Peripheral Software Updates	16
	Set Up Certificates	17
<b>3</b>	<b>Upgrading a Redundant Polycom CMA System</b>	<b>19</b>
	Request Software Upgrade Key Codes	21
	Shut Down the Redundant Standby Server	21
	Save a Back Up of the Polycom CMA System Databases	22
	Download and Install the CMA System Pre-upgrade Patch	22
	Back Up the CMA System on the Primary Server	23
	Re-image the Primary CMA System Server with v6.0	24
	Perform the First-Time Setup on the Primary System Server	24
	Re-image the Redundant CMA Server with v6.0	26
	Perform the First-Time Setup on the Redundant Server	27
	Integrate Both CMA System Servers to the External Database	27

Enter the Software Upgrade Key Codes .....	28
Verify the Upgrade .....	29
Provision SIP Settings for Microsoft Lync or Microsoft Office Communications Server Integration .....	29
Upload Endpoint and Peripheral Software Updates .....	30
Set Up Certificates .....	31

# Prepare for Polycom<sup>®</sup> CMA<sup>™</sup> System Upgrade

This chapter describes the tasks you should do in advance of upgrading the Polycom<sup>®</sup> Converged Management Application<sup>™</sup> (CMA<sup>™</sup>) system including:

- [Complete the First-Time Setup Worksheet](#)
- [Request or Locate Current Recovery DVD](#)
- [Request Certificates \(Optional\)](#)
- [Download Endpoint and Peripheral Software Updates](#)
- [Connect to the Polycom CMA System Server](#)

## Complete the First-Time Setup Worksheet

Before you begin the upgrade, fill out the **My System Values** column of this worksheet. If you have the worksheet from your initial installation, you can use it instead.

You should have all of the required settings and accounts already set up, but you will need to re-enter this information during the upgrade process.

Item	My System Values	Factory-Set Default Values	Description
<b>Security Mode Setting</b>			
Set Standard Mode			Required setting.
<b>System Network Settings (from Admin &gt; Server Settings &gt; Network)</b>			
System Name		POLYCOM- <7-random-ASCII- characters> For example, POLYCOM-1 DT9R5W	NetBIOS name of the CMA system server. The name must be between 6 and 15 characters and can include dashes and underscores.

Item	My System Values	Factory-Set Default Values	Description
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 pol ycom. com, not the fully qualified path of <hostname>. pol ycom. com.
Preferred DNS Server			IP address of the domain name server.
Alternate DNS Server			IP address of an alternate domain name server. Must be in the same IP address format as the preferred DNS server.
<b>System Time Information (from Admin &gt; Server Settings &gt; System Time)</b>			
System Time Zone			
Current Date			
Current Time			
External NTP Server			IP address of external NTP time server (optional).
<b>Information Required for Polycom Customer Support (from Admin &gt; Server Settings &gt; Licenses)</b>			
Serial number			
License number			

## Request or Locate Current Recovery DVD

This new version of the CMA system includes some important new features. To support those new features, the CMA system upgrade process is more complex than usual. Please be sure to carefully follow the documented procedures for the upgrade to ensure success. As with any upgrade, we recommend that the person performing the upgrade has the recovery DVD for the currently installed CMA system version available during the upgrade.

process. With the recovery DVD, you can re-image the system back to its original state and restore the original system data. If needed, contact Polycom Global Services to request a recovery DVD.

## 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.

## Request a Software Upgrade Key Code

### To request a software upgrade key code

- 1 Locate and record the CMA system server serial number. To locate the serial number:
  - a Log in to the CMA system as an administrator.
  - b Choose **Admin > Server Settings > Licenses**.

The serial number appears at the top of the **Licenses** page.

- 2 Using a web browser, go to <http://support.polycom.com>.
- 3 On the Polycom Support page, go to **Licensing & Product Registration > Activation/Upgrade**.
- 4 Click **SITE & Single Activation/Upgrade**.
- 5 Follow the onscreen instructions to request the key code. Make a note of this number for use during installation. Use the Activation Assistant if you need help.
- 6 Record the U-Key code returned by the system.

## Request the CMA System v6.0 Software and Patch

Only CMA systems running v5.5.0 patched with the Pre-Upgrade Patch can be upgraded to version 6.0.0. If your system is not currently at v5.5.0, you must upgrade to v5.5.0 before applying the Pre-Upgrade Patch and upgrading to v6.0.0. Here are the upgrade scenarios that you may need to consider and apply:

**Table 1-1** Staged Software Upgrade Paths

Starting CMA System Version	Upgrade to...
CMA v5.0	CMA v5.3
CMA v5.3 or v5.4	CMA v5.5
CMA v5.5	Apply Pre-Upgrade Patch
CMA v5.5 with Pre-Upgrade Patch	CMA v6.0

### To request the CMA system v6.0 software and Pre-Upgrade Patch

- 1 Go to the Polycom support site ([support.polycom.com](http://support.polycom.com)) and select **Request CMA System v6.0 Software**.
- 2 Complete and submit the request form.

Polycom will send the software (the CMA System v6.0 Recovery DVD) to you along with instructions on how to obtain the Pre-Upgrade Patch.

## Download Endpoint and Peripheral Software Updates

If you have endpoint or peripheral software updates that have been uploaded to your CMA system (**Admin > Automatic Updates > Automatic Software Updates**), the upgrade process will not retain those updates. If you need those



software updates after the upgrade to CMA v6.0, you should review the updates that you have there, download the files from <http://support.polycom.com>, and store them on another system.

After the upgrade, you can upload them to the CMA system server.

## 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:
  - Using a crossover cable, connect the CMA system server (via the GB1 port) directly to an ethernet port on a computer that has a monitor, keyboard and mouse .
  - Using ethernet cables, connect the CMA system server (via the GB1 port) and a computer with a monitor, keyboard and mouse to the same ethernet switch or hub.
- 2 Power on the computer and the CMA system server.



# Upgrading a Non-Redundant Polycom CMA System

This chapter provides instructions for upgrading a non-redundant Polycom CMA system. See [Chapter 3](#) for instructions on upgrading a redundant Polycom CMA system.

See the *Polycom CMA System Release Notes* for the version to which you are upgrading for information about valid upgrade paths.



## IMPORTANT

- Give yourself plenty of time for the system upgrade process. It will take some time, depending on the environment. At some steps you are instructed to wait. **MAKE SURE YOU WAIT UNTIL THE PROCESS IS COMPLETE.** Interrupting the upgrade can corrupt the system.
- During most of the upgrade process, the CMA system is offline and all services are unavailable. In addition, the serial console appears inactive; nevertheless, do not power off the system unless instructed to do so.
- If you have an external database, make sure to close all external database connections before performing this upgrade.

**To upgrade to the CMA system v6.0 software, complete the following tasks**

- 1 [Save a Backup of the Polycom CMA System Databases.](#)
- 2 [Save a Backup of the Polycom CMA System Databases.](#)
- 3 [Install the CMA System Pre-upgrade Patch.](#)
- 4 [Back Up the CMA System.](#)
- 5 [Re-image the CMA System with v6.0.](#)
- 6 [Perform the First-Time Setup.](#)
- 7 [Restore the System Backup.](#)

Only required if you are using the internal database.

- 8 [Integrate the CMA System to the External Database](#) (optional)

- 9 [Enter the Software Upgrade Key Code.](#)
- 10 [Verify the Upgrade.](#)
- 11 [Provision SIP Settings for Microsoft Lync or Microsoft Office Communications Server Integration.](#)
- 12 (Optional) [Upload Endpoint and Peripheral Software Updates.](#)
- 13 (Optional) [Set Up Certificates.](#)

## Save a Backup of the Polycom CMA System Databases

This process gives you an additional safeguard for your CMA system databases. You will back up all system data in a later step and use that backup to restore your data after installing the CMA 6.0 software.

This section describes backing up the internal databases. If your system uses an external database, ask your database administrator to back up the external CMA system databases according to Microsoft SQL Server Management Studio procedures or your company's backup procedures.

### To back up the internal CMA system databases

- 1 Log into the CMA system.
- 2 Go to **Admin > Troubleshooting Utilities**.
- 3 Click **Backup Databases**.  
This creates up-to-the-minute backups of the internal databases.
- 4 To save each backup file to another location, go to **Admin > Database Backup Files**.
- 5 When the **Database Backup Files** list appears, left click on the latest **Readi Manager\_<yyyymmddhhhh>.bak** file, click **Save**, and save the file to a location on your local system.
- 6 Left click on the latest **Logger\_<yyyymmddhhhh>.bak** and select **Save**, and save the file to a location on your local system.
- 7 Left click on the latest **XMPP\_<yyyymmddhhhh>.bak** and select **Save**, and save the file to a location on your local system.
- 8 Attach a USB memory drive to a port on your local system and copy the three database files to the drive.

## Install the CMA System Pre-upgrade Patch

Only CMA systems running v5.5.0 patched with the Pre-Upgrade Patch can be upgraded to version 6.0.0. If your system is not currently at v5.5.0, you must upgrade to v5.5.0 before applying the Pre-Upgrade Patch and upgrading to v6.0.0. For more information, see [“Request the CMA System v6.0 Software and Patch”](#) on page 4.

The Pre-Upgrade Patch adds a full system backup function to your v5.5.0 system. After installing the patch, you will use this function to back up your complete CMA system. You must install the patch regardless of whether you are using internal or external databases.



### Notes

- After installing the patch, you must continue with the upgrade process. The CMA system will not operate properly until the upgrade process is complete.
- The Pre-Upgrade Patch is not required if you are not migrating system data from an earlier software version.

### To install the patch

- 1 On a local PC, create a directory to which to save the Pre-Upgrade Patch.
- 2 Download the Pre-Upgrade Patch to the directory.
  - a Follow the directions for obtaining the Pre-Upgrade Patch from the FTP site. You will receive these directions when you [“Complete and submit the request form.”](#) as described on [page 4](#).
  - b When the **Save As** dialog box appears, browse to the directory created in step 1 and click **Save** to save the .bin file to your local system.
- 3 Log into the CMA system.
- 4 Go to **Admin > Management and Security > Server Software Upgrade**.
- 5 From the **Server Software Upgrade** page, click **Upload upgrade file to server** and browse to the location of the patch file.
- 6 Select the .bin file and click **Open**.  
The .bin file uploads to the system.



### Note

The system cannot be upgraded while in HTTPS mode if using Mozilla Firefox. You must either switch the CMA system to HTTP or do the upgrade using Microsoft Internet Explorer.

- 7 When the system indicates the **File Upload is Complete**, click **OK**.

**8 Click Upgrade.**

When the status messages on the upgrade screen start changing ("Stopping services", "applying upgrade", etc.), the upgrade process has started. When the upgrade process is complete, the system reboots.

## Back Up the CMA System

After you install the Pre-Upgrade Patch, you must back up the entire system. This process creates a backup archive of the CMA system. This is a new function that also adds to your system database. Once this archive is created, you must immediately continue on to ["Re-image the CMA System with v6.0"](#) on page 10.

If you are using the internal database, you can use this backup archive to restore the system after installing the new version. You must create the backup archive regardless of whether you are using internal or external databases.

### To backup the CMA system

- 1 From the CMA system web interface, go to **Admin > Backup System Settings**.



**Note**

If you do not see the **Backup System Settings** option, clear your browser cache, and retry. This option is added by the Pre-Upgrade Patch.

- 2 When the **Backup System Settings** page appears, click **Create and Download a Backup Archive**.
- 3 In the **Select location for download** dialog box, enter a unique **File name**, browse to a location on your system and click **Save**.



**Note**

Be sure to select a drive that is not on the server used for the CMA system. All data on the CMA system drive will be deleted during the upgrade process.

A **File Download** dialog box displays the progress of the download operation.

- 4 When the operation is completed, click **OK**.
- 5 Browse to the location specified in step 3 and verify the file download.

## Re-image the CMA System with v6.0

The upgrade to CMA system v6.0 requires that you re-image the system from the CMA System v6.0 Recovery Disc. This installs a whole new version of the system on your server.

This procedure requires a keyboard and monitor.

### To re-image the CMA system with v6.0

- 1 Insert the Recovery Disc into the DVD drive on the CMA system server.
- 2 Log into the system as admin and from the Dashboard, select Restart.
- 3 During the reboot, press F11 on the keyboard connected to the CMA server. F11 will display the BIOS Boot Manager. Once the screen appears, select Optical CD drive.
- 4 When the system prompts you to, press any key to restart the server from the disc.

The system restarts, re-images with v6.0, and ejects the disc when the process is complete. The process takes approximately 20 minutes on a CMA 4000 system and approximately 10 minutes on a CMA 5000 system.

## Perform the First-Time Setup

You must now complete most of the first-time setup of the CMA system v6.0 software. Use the information you recorded in [“Complete the First-Time Setup Worksheet”](#) on page 1.

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.

### To step through the First-Time Setup Wizard

- 1 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 5.
- 2 Open a browser window and in the **Address** field enter the CMA system IP address or host name.

- 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 adm i n/admi n.
- 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.
- Security Mode** 7 When you are prompted to select a security mode, select **Set Standard Mode**.  
The **Administrative User** page appears.
- Administrator Password** 8 When the **Change Administrator Password** page appears, enter the **Old Password**.  
9 For the **New Password**, enter a new password with a length of at least eight characters.  
10 **Confirm the New Password** and click **Next**.  
The **Network** page appears.
- Network Settings** 11 Enter the **Network Settings** information and click **Next**.  
The **Certificates** page appears. By default the system is configured to use a default self-signed certificate.
- Certificate Management** 12 Click **Next**.  
We recommend configuring certificates after completing the first-time setup and after restoring the system.
- System Reboot** 13 When prompted to reboot, click **Commit the Settings and Reboot**.  
The system displays a confirmation message.  
14 Click **Yes**.  
The system reboots.  
15 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** 16 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.



#### Note

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.

#### 17 Click **Next**.

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

#### 18 Click **Next**. For ease of setup, we recommend setting up the external database after you've finished first-time setup.

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

#### 19 Click **Next**. Do not enter the information on **Enterprise Directory** page. The restore process or the integration with your external database will include all of your previous enterprise directory settings.

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

#### 20 Click **Next**. Do not enter the information on **Directory Setup** page. The restore process or the integration with your external database will include all of your previous directory settings

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 system **Dashboard**.

## Restore the System Backup

After you install the new version, you can restore all of your system data from the backup. You only need to restore the back archive if you are using the internal database.

If you are using an external database, skip to “[Integrate the CMA System to the External Database](#)” on page 14.

### To restore the backup archive

- 1 Go to **Admin > Backup System Settings**.
- 2 In the **Select Archive File** section of the **Backup System Settings** page, click **...**.
- 3 In the **Select file to upload** dialog box, select the backup archive that you created earlier and click **Open**.
- 4 Click **Restore from Backup Archive**.  
A warning appears about the restore process.
- 5 Click **Yes**.  
A message displays that the file upload is complete.
- 6 Click **OK**.  
The system uses the archive file to restore the CMA system to the state of the backup files. This process could take some time, depending on the size of your database.
- 7 Log in to the CMA system.  
The system will have a System Alert that says the CMA version is out of sync with the database version and the system has been forced to use an internal database. This alert is normal one time after the upgrade.
- 8 Click **System Alerts** to view the alert, then click **Clear** to remove the alert.

## Integrate the CMA System to the External Database

If you are using an Microsoft SQL database server, you must now integrate the external database.

### To integrate the CMA system to the external database

- 1 Verify that your Microsoft SQL Server meets the CMA system requirements. Refer to the *Polycom CMA System Release Notes*.
- 2 Go to **Admin > Server Settings > Database**.

- 3 Select the **Use an external SQL Server database** check box.
- 4 Enter the **Database Server IP Address or DNS Name** and change the **Database Server Port** number as needed.
- 5 Click **Update**.  
The system will guide you through formatting or upgrading the external database, as necessary.
- 6 Click **Finish**.

## Enter the Software Upgrade Key Code

To enter the CMA system software upgrade key code

- 1 Go to **Admin > Server Settings > Licenses**.
- 2 Enter the software upgrade key code for the primary server into the **Add New License > Activation Key** field and click **Add**.

The **Active License** section of the **Licenses** page is updated.

## Verify the Upgrade

To verify that the upgrade was successful:

- 1 On the login screen, verify that the system displays the version number of software to which you are upgrading.
- 2 Verify that your endpoints are registered to the Gatekeeper and Global Address Book, as required.
- 3 Verify that you can schedule and start a conference.
- 4 Verify that you can monitor a conference.
- 5 Verify that you can terminate a conference.
- 6 Review the CDR for the test conference and verify the record is accurate.

## Provision SIP Settings for Microsoft Lync or Microsoft Office Communications Server Integration

If your system is integrated with Microsoft® Lync™ Server 2010 or Microsoft® Office Communications Server 2007, you must configure the new SIP settings to enable the integration.

By default, SIP is disabled in site provisioning. This procedure describes how to change the existing site provisioning settings so that they provision integration with one of these unified communications servers.

### To provision SIP for integration with Microsoft Lync or Office Communications Server

- 1 Go to **Admin > Dial Plan and Sites > Sites**.
- 2 In the **Sites** page, select the site of interest and click **Edit Site Provisioning Details**.
- 3 In the **Edit Site Provisioning Details** dialog box, click **SIP Settings** and select these options. Settings not listed below are optional, based on your systems configuration.

Fields	Description
Enable SIP	Select to enable SIP.
Transport Protocol	Specifies the transport protocol for communications with the unified communications server. Possible values are: <b>Auto</b> —The communication protocol will be auto-negotiated. <b>TCP</b> —This protocol has error-recovery services, message delivery is assured, and messages are delivered in the order they were sent. <b>UDP</b> —This protocol does not provide error-recovery services, message delivery is not assured, and messages are not necessarily delivered in the order they were sent. <b>TLS</b> —This protocol transfers communications over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection.
SIP Server Type	Select Microsoft.

Fields	Description
Use Enterprise Credentials	<p>Select this option. With the option selected, CMA system will provision the following to dynamically managed endpoints:</p> <ul style="list-style-type: none"> <li>• For the unified communications server, each endpoint system will be provisioned with the same credentials it used to access the CMA system.</li> <li>• For its domain username, each endpoint system will be provisioned with the domain username initially provided to it. This username must be pre-configured for the endpoint system on the unified communications server.</li> </ul>

4 Click **OK**.

## Upload Endpoint and Peripheral Software Updates

If your system had endpoint or peripheral software updates stored on it, you must upload those updates. They were not retained in the system backup.

If you stored them in another location in preparation for the upgrade, you can use that location as the source. If you did not, you can upload them from <http://support.polycom.com>.

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

## Set Up Certificates

If you are using certificates, you can set them up. This setup was not retained in the system backup.

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



# Upgrading a Redundant Polycom CMA System

This chapter provides instructions for upgrading a redundant CMA system. See [Chapter 2](#) for instructions on upgrading a non-redundant CMA system.

See the *Polycom CMA System Release Notes* for the version to which you are upgrading for information about valid upgrade paths.



## IMPORTANT

- Give yourself plenty of time for the system upgrade process. It will take some time, depending on the environment. At some steps you are instructed to wait. **MAKE SURE YOU WAIT UNTIL THE PROCESS IS COMPLETE.** Interrupting the upgrade can corrupt the system.
- During most of the upgrade process, the CMA system is offline and all services are unavailable. In addition, the serial console appears inactive; nevertheless, do not power off the system unless instructed to do so.
- If you have an external database, make sure to close all external database connections before performing this upgrade.
- During this process only one of the two CMA system servers is powered on at any given time. Be sure to follow these procedures carefully and refer to the IP addresses you recorded in step 1 if you need help determining which is your primary or redundant server.

## About Redundancy and Upgrading a Redundant CMA system

A redundant CMA system configuration has two CMA system servers and three IP addresses on the same network—one physical IP address for each of the servers and one virtual IP address dedicated to endpoint registration.

Take note of the following terminology:

- In a redundant configuration, one server is licensed as the *primary server* and the other server is licensed as the *redundant server*. That means that the primary server is always the primary server and the redundant server is always the redundant server.

- In a redundant configuration, there is only one *active server*. The active server is the server managing the system. That means when the redundant server is managing the system, it is the active server. This distinction is important when performing this upgrade.
- In a redundant configuration, there is only one *standby server*. The standby server is the server that is not managing the system. If at anytime you receive a **Cannot find server** error when you try to log into a server, check to see if it is the standby server.

Also note that in a properly configured and fully operational redundant configuration, you can log into the virtual IP address for the redundant system. When you do so, the **Redundant Configuration** page shows:

- The **Virtual IP** field is populated.
- The primary server is identified as the active server and the redundant server is identified as the inactive server.

A redundant system is also fully operational when the redundant server is the active server and the primary server is the inactive server. However, for licensing purposes, the primary server should be the active server when both servers are functional.

- Both servers have a **Machine Status** of ON.

When upgrading a redundant CMA system, you will be instructed when to disable redundancy between the primary and redundant servers and when to re-enable redundancy. During these procedure only one of the two CMA system servers is powered on at any given time. Be sure to follow these procedures carefully.

**To upgrade a redundant CMA system to the v6.0 software, complete the following tasks**

- 1 [Request Software Upgrade Key Codes.](#)
- 2 [Shut Down the Redundant Standby Server.](#)
- 3 [Save a Back Up of the Polycom CMA System Databases.](#)
- 4 [Download and Install the CMA System Pre-upgrade Patch.](#)
- 5 [Back Up the CMA System on the Primary Server.](#)
- 6 [Re-image the Primary CMA System Server with v6.0.](#)
- 7 [Perform the First-Time Setup on the Primary System Server.](#)
- 8 [Re-image the Redundant CMA Server with v6.0.](#)
- 9 [Perform the First-Time Setup on the Redundant Server.](#)
- 10 [Integrate Both CMA System Servers to the External Database.](#)
- 11 [Enter the Software Upgrade Key Codes.](#)
- 12 [Verify the Upgrade.](#)



- 13 [Provision SIP Settings for Microsoft Lync or Microsoft Office Communications Server Integration.](#)
- 14 (Optional) [Upload Endpoint and Peripheral Software Updates.](#) (primary server)
- 15 (Optional) [Set Up Certificates.](#)

## Request Software Upgrade Key Codes

You will need a software upgrade key code for both servers in a redundant Polycom CMA system configuration.


### To request a software upgrade key code

- 1 On the primary server, locate and record the CMA system server serial number. To locate the serial number:
  - a Log in to the CMA system as an administrator.
  - b Choose **Admin > Server Settings > Licenses.**  
The serial number appears at the top of the **Licenses** page.
- 2 Using a web browser, go to <http://support.polycom.com>.
- 3 On the Polycom Support page, go to **Licensing & Product Registration > Activation/Upgrade.**
- 4 Click **SITE & Single Activation/Upgrade.**
- 5 Follow the onscreen instructions to request the key code. Make a note of this number for use during installation. Use the Activation Assistant if you need help.
- 6 Record the U-Key code returned by the system.
- 7 Repeat this procedure for the redundant server.

## Shut Down the Redundant Server

You must shut down the redundant server while you upgrade the primary server.

### To shut down the redundant server

- 1 Log into the *IP address of the redundant server.*
- 2 Go to **Admin > Dashboard** and click **Shutdown** .

## Save a Back Up of the Polycom CMA System Databases

You must save a back up of your CMA system external databases. Ask your database administrator to backup the external CMA system databases according to Microsoft SQL Server Management Studio procedures or your company's backup procedures.

## Install the CMA System Pre-Upgrade Patch

Only CMA systems running v5.5.0 patched with the Pre-Upgrade Patch can be upgraded to version 6.0.0. If your system is not currently at v5.5.0, you must upgrade to v5.5.0 before applying the Pre-Upgrade Patch and upgrading to v6.0.0. For more information, see [“Request the CMA System v6.0 Software and Patch”](#) on page 4.

The Pre-Upgrade Patch adds a full system backup function to your v5.5.0 system. After installing the patch, you will use this function to back up your complete CMA system. You must install the patch regardless of whether you are using internal or external databases.



### Notes

- After installing the patch, you must continue with the upgrade process. The CMA system will not operate properly until the upgrade process is complete.
- The Pre-Upgrade Patch is not required if you are not migrating system data from an earlier software version.

### To install the patch

- 1 On a local PC, create a directory to which to save the Pre-Upgrade Patch.
- 2 Download the Pre-Upgrade Patch to the directory.
  - a Follow the directions for obtaining the Pre-Upgrade Patch from the FTP site. You will receive these directions when you [“Complete and submit the request form.”](#) as described on [page 4](#).
  - b When the **Save As** dialog box appears, browse to the directory created in step 1 and click **Save** to save the . bin file to your local system.
- 3 Log in to the CMA system using the *IP address of the primary server*.
- 4 Go to **Admin > Management and Security > Server Software Upgrade**.
- 5 From the **Server Software Upgrade** page, click **Upload upgrade file to server** and browse to the location of the patch file.
- 6 Select the . bin file and click **Open**.  
The . bin file uploads to the system.

**Note**

The system cannot be upgraded while in HTTPS mode if using Mozilla Firefox. You must either switch the CMA system to HTTP or do the upgrade using Microsoft Internet Explorer.

7 When the system indicates the **File Upload** is **Complete**, click **OK**.

8 Click **Upgrade**.

When the status messages on the upgrade screen start changing ("Stopping services", "applying upgrade", etc.), the upgrade process has started. When the upgrade process is complete, the system reboots.

## Back Up the CMA System on the Primary Server

After you install the patch, you must back up the entire system. This process creates a backup archive of the CMA system.

You must create the backup archive from the primary server even though you are using an external databases.

### To backup the CMA system

- 1 Log in to the CMA system using the *IP address of the primary server*.
- 2 From the CMA system web interface, go to **Admin > Backup System Settings**.
- 3 When the **Backup System Settings** page appears, click **Create and Download a Backup Archive**.
- 4 In the **Select location for download** dialog box, enter a unique **File name**, browse to a location on your system and click **Save**.

**Note**

Be sure to select a drive that is not on the server used for the CMA system. All data on the CMA system drive will be deleted during the upgrade process.

A **File Download** dialog box displays the progress of the download operation.

5 When the operation is completed, click **OK**.

6 Browse to the location specified in step 3 and verify the file download.

## Re-image the Primary CMA System Server with v6.0

The upgrade to CMA system v6.0 requires that you re-image the primary system server from the new v6.0 Recovery Disc. This installs a whole new image of the system software on the server.

### To re-image the primary CMA system server with v6.0

- 1 Insert the Recovery Disc into the DVD drive on the primary CMA system server.
- 2 When the system prompts you, press any key to restart the server from the disc.

The system restarts, re-images with v6.0, and ejects the disc when the process is complete. The process takes approximately 20 minutes on a CMA 4000 system and approximately 10 minutes on a CMA 5000 system.

## Perform the First-Time Setup on the Primary System Server

You must now complete most of the first-time setup of the CMA system v6.0 software on the primary system server. Use the information you recorded in [“Complete the First-Time Setup Worksheet”](#) on page 1.

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.

### To step through the First-Time Setup Wizard

- 1 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 5. To step through the First-Time Setup Wizard
- 2 Open a browser window and in the **Address** field enter the CMA system *physical IP address* of the primary server.
- 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.
- Security Mode** **7** When you are prompted to select a security mode, select **Set Standard Mode**.
- The **Administrative User** page appears.
- Administrator Password** **8** When the **Change Administrator Password** page appears, enter the **Old Password**.
- 9** For the **New Password**, enter a new password with a length of at least eight characters.
- 10** **Confirm the New Password** and click **Next**.
- The **Network** page appears.
- Network Settings** **11** Enter the **Network Settings** information and click **Next**.
- The **Certificates** page appears. By default the system is configured to use a default self-signed certificate.
- Certificate Management** **12** Click **Next**.
- We recommend configuring certificates after completing the first-time setup and after restoring the system.
- System Reboot** **13** When prompted to reboot, click **Commit the Settings and Reboot**.
- The system displays a confirmation message.
- 14** Click **Yes**.
- The system reboots.
- 15** 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** **16** Configure these settings on the **System Time** page, as necessary.

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

Field	Description
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.



**Note**

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.

**17 Click Next.**

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

**18 Click Next.** Leave the system configured to use the internal database. You will point them to an external database later.

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

**19 Click Next.** Do not enter the information on **Enterprise Directory** page. The restore process or the integration with your external database will include all of your previous enterprise directory settings.

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

**20 Click Next.** Do not enter the information on **Directory Setup** page. The restore process or the integration with your external database will include all of your previous directory settings

**21 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**.

## Re-image the Redundant CMA Server with v6.0

The upgrade to CMA system v6.0 requires that you re-image the redundant server from the new v6.0 Recovery Disc. This installs a whole new version of the system on your server.

**To re-image the redundant CMA server with v6.0**

- 1 Insert the Recovery Disc into the redundant CMA server.
- 2 When the system prompts you, press any key to restart the server from the disc.

The system restarts, re-images with v6.0, and ejects the disc when the process is complete. The process takes approximately 20 minutes on a CMA 4000 and approximately 10 minutes on a CMA 5000.

## Perform the First-Time Setup on the Redundant Server

You must now complete most of the first-time setup of the CMA v6.0 software on the redundant server. Use the information you recorded in [“Complete the First-Time Setup Worksheet”](#) on page 1.

Follow the same procedure as described in [“Perform the First-Time Setup on the Primary System Server”](#) on page 24.

## Integrate Both CMA System Servers to the External Database

You must now integrate each server to the external database.

**To integrate both CMA system servers to the external database:**

- 1 Log in to the *physical IP address* of the redundant server.
- 2 Go to **Admin > Server Settings > Database**.
- 3 On the **Database** screen, select the **Use an external SQL Server database** check box, re-enter the external database settings you recorded in step 3b on page 20, and click **Update**.
- 4 Click **Yes** to confirm the change and reboot the redundant system.
- 5 As the redundant server is rebooting, log in to the *physical IP address* of the primary server.
- 6 Go to **Admin > Server Settings > Database**.
- 7 On the **Database** screen, select the **Use an external SQL Server database** check box, re-enter the external database settings you recorded in step 3b on page 20, and click **Update**.
- 8 Click **Yes** to confirm the change and reboot the redundant system.
- 9 As the primary server is rebooting, on the redundant server go to **Admin > Server Settings > Redundant Configuration** and verify that the system is configured for redundancy. At this time, the redundant server will be the active server.

- 10 When the primary server is up, on the redundant server go to **Admin > Server Settings > Redundant Configuration** page and click **Switch Server Roles**.

The primary system server becomes the active server. The redundant system server becomes the standby server again.

## Enter the Software Upgrade Key Codes

### To enter the CMA system software upgrade key codes

- 1 To enter the CMA system software upgrade key code for the primary server:
  - a Log in to the system's *virtual IP address*.
  - b Go to **Admin > Server Settings > Redundant Configuration** and verify that the primary server is the active server.
  - c Go to **Admin > Server Settings > Licenses**.
  - d Enter the software upgrade key code for the primary server into the **Add New License > Activation Key** field and click **Add**.  
The **Active License** section of the **Licenses** page is updated.
  - e Go to **Admin > Server Settings > Redundant Configuration** and click **Switch Server Role**.
  - f Verify that the redundant server becomes the active server.
- 2 To enter the CMA system software upgrade key code for the redundant server:
  - a Log in to the system's *virtual IP address*.
  - b Go to **Admin > Server Settings > Redundant Configuration** and verify that the redundant server is the active server.
  - c Go to **Admin > Server Settings > Licenses**.
  - d Enter the software upgrade key code for the redundant server into the **Add New License > Activation Key** field and click **Add**.  
The **Active License** section of the **Licenses** page is updated.
  - e Go to **Admin > Server Settings > Redundant Configuration** and click **Switch Server Role**.
  - f Verify that the primary server becomes the active server.



## Verify the Upgrade

### To verify that the upgrade was successful:

- 1 On the login screen, verify that the system displays the version number of software to which you are upgrading.
- 2 Verify that your endpoints are registered to the Gatekeeper and Global Address Book, as required.
- 3 Verify that you can schedule and start a conference.
- 4 Verify that you can monitor a conference.
- 5 Verify that you can terminate a conference.
- 6 Review the CDR for the test conference and verify the record is accurate.

## Provision SIP Settings for Microsoft Lync or Microsoft Office Communications Server Integration

If your system is integrated with Microsoft® Lync™ Server 2010 or Microsoft® Office Communications Server 2007, you must configure the new SIP settings to enable the integration.

By default, SIP is disabled in site provisioning. This procedure describes how to change the existing site provisioning settings so that they provision integration with one of these unified communications servers.

### To provision SIP for integration with Microsoft Lync or Office Communications Server

- 1 Go to **Admin > Dial Plan and Sites > Sites**.
- 2 In the **Sites** page, select the site of interest and click **Edit Site Provisioning Details**.
- 3 In the **Edit Site Provisioning Details** dialog box, click **SIP Settings** and select these options.

Settings not listed below are optional, based on the configuration of your systems.

Fields	Description
Enable SIP	Select to enable SIP.

Fields	Description
Transport Protocol	<p>Specifies the transport protocol for communications with the unified communications server. Possible values are:</p> <p><b>Auto</b>—The communication protocol will be auto-negotiated.</p> <p><b>TCP</b>—This protocol has error-recovery services, message delivery is assured, and messages are delivered in the order they were sent.</p> <p><b>UDP</b>—This protocol does not provide error-recovery services, message delivery is not assured, and messages are not necessarily delivered in the order they were sent.</p> <p><b>TLS</b>—This protocol transfers communications over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection.</p>
SIP Server Type	Select Microsoft.
Use Enterprise Credentials	<p>Select this option. With the option selected, CMA system will provision the following to dynamically managed endpoints:</p> <ul style="list-style-type: none"> <li>• For the unified communications server, each endpoint system will be provisioned with the same credentials it used to access the CMA system.</li> <li>• For its domain username, each endpoint system will be provisioned with the domain username initially provided to it. This username must be pre-configured for the endpoint system on the unified communications server.</li> </ul>

4 Click **OK**.

## Upload Endpoint and Peripheral Software Updates

If your system had endpoint or peripheral software updates stored on it, you must upload those updates. They were not retained in the system backup.

If you stored them in another location in preparation for the upgrade, you can use that location as the source. If you did not, you can upload them from <http://support.polycom.com>.

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

## Set Up Certificates

If you are using certificates, you can set them up. This setup was not retained in the system backup.

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

