Polycom® CMA® System Patch Release Notes

Patch ID #:	CMA-GeneralPatch_2.0.0.0-116791.bin
Affected version:	**Polycom CMA System v5.x.x systems** **Apply this patch to CMA v5.x.x systems only.** **Use CMA-GeneralPatch_1.0.0.0-116370.bin patch for CMA v6.x.x systems**
Release date:	May 12, 2013

About This Patch

After 00:00 on May 7, 2013, Polycom CMA Desktop clients could no longer log into their associated Polycom CMA systems. The login process stopped at “Initializing Call Stack”.

This issue occurs for all versions of the Polycom CMA system and it occurs because the third-party “Openfire” XMPP component within in the CMA system uses a certificate that expired at 00:00 on May 7, 2013. After this date and time, the CMA Desktop client refused to establish a TLS connection for XMPP services due to the invalid certificate.

This patch replaces the certificate “keystore” file on the Polycom CMA system with a new certificate file that has an expiration date extended to year 2024

Important Prerequisites and Configuration Considerations

- Apply this patch to CMA v5.x.x systems only. Do not install this patch on CMA v6.x.x systems.
- If after installing this patch, you upgrade the CMA system software to a later version, you will be required to apply an XMPP keystore patch to that newer version.
- In order to ensure that you can upgrade your CMA system to a later version, this patch does not write patch information to the CMA system database. Therefore, this patch does not appear in the **Past Upgrades** page.

Installation on a Non-Redundant CMA System

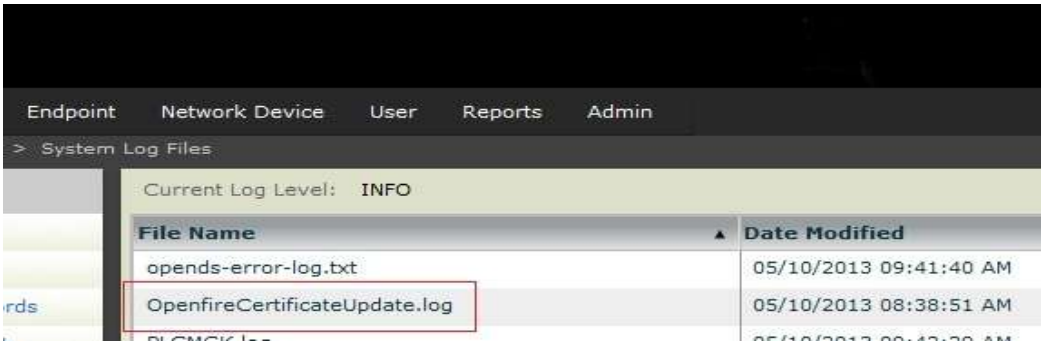
To install this patch on a non-redundant CMA system:

1. Backup the CMA system. See the *Polycom CMA System Operations Guide* for more information on backing up your system.

2. Download the patch and save it to a local disk.
3. From the CMA system user interface, go to **Admin > Management Security > Server Software Upgrade.**
4. Click **Upload upgrade file to Server** and browse to and select the patch file you downloaded in step 2.

5. When prompted, click **OK** to finish the patch upload.
6. Click **Upgrade** to have the system begin the patch installation.

   Installation will take less than 1 minute, then the CMA system will reboot automatically. Note that the interface connection will be lost during system reboot.
7. After the CMA system reboots completely, log into the system again and go to **Report > System Log Files**
8. Select the *OpenfireCertificateUpdate.log* file and click **Open**.



9. If the patch installed successfully, the following log entry will be found in the file

   "Thu May 09 18:38:51 MDT 2013 XMPP keystore is updated successfully, it will take effect after restarting CMA"

Installation on a Redundant CMA System

IMPORTANT: This procedure requires that someone have physical access to the CMA system servers so they can be powered down and up as needed.

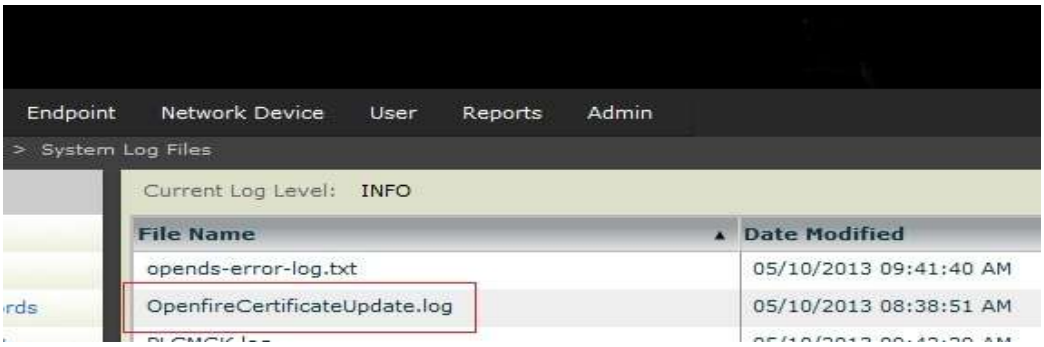
To install this patch on a redundant CMA system:

1. Backup the CMA system. See the *Polycom CMA System Operations Guide* for more information on backing up your system.
2. Download the patch and save it to a local disk.
3. Access the CMA system by its virtual IP address, and go to **Admin > Dashboard** and click **Shutdown**.
4. Wait for the standby CMA system to become the active CMA system.
5. Access the currently active CMA system server user interface by its real IP (not virtual) and then go to **Admin > Management Security > Server Software Upgrade.**
6. Click **Upload upgrade file to Server** and browse to and select the patch file you downloaded in step 2.

7. When prompted, click **OK** to finish the patch upload.
8. Click **Upgrade** to have the system begin the patch installation.

   Installation will take less than 1 minute, then the CMA system will reboot automatically. Note that the interface connection will be lost during system reboot.
9. After the CMA system reboots completely, log into the system again and go to **Report > System Log Files.**

10. Select the *OpenfireCertificateUpdate.log* file and click **Open**.



11. If the patch installed successfully, the following log entry will be found in the file

    "Thu May 09 18:38:51 MDT 2013 XMPP keystore is updated successfully, it will take effect after restarting CMA"

12. Physically power on the standby CMA system server and when it is ready, go to **Admin > Dashboard** and click **Shutdown**.
13. Wait for the standby CMA system to become the active CMA system.
14. Access the active CMA system server user interface by its real IP (not virtual) and then go to **Admin > Management Security > Server Software Upgrade.**
15. Repeat steps 5 through 11 of this procedure on the active CMA system server.
16. Power on the standby CMA system server.