Cisco Unified Communications Manager
RSA Version-3 keys COP file

Release Notes Version 4
March 6, 2015

Introduction:

To improve software integrity protection, new RSA keys are being used to sign Cisco Unified Communications Manager releases and any of their associated updates such as Phone Firmware, Device Packages, DST Updates, Locales, Dialplans, or any other update that can be applied to the system.

Who needs this fix:

If you are already running CUCM release 10.x or higher you already have this fix and do ***not*** need to install this Cisco Options Package (COP) file.

If you are running an Engineering Special (ES) or Service Update (SU) that already contains CSCua88701 you do ***not*** need to install this COP file. CSCua88701 is included in:

- 8.5.1.17123-1 and higher
- 8.6.2.24122-1 and higher
- 9.1.2.11018-1 and higher

Follow the link to the CDETS for additional details.

If you are running an ES or SU less than the builds listed in the previous bullet, you need to install this COP file if:

- You are upgrading to CUCM Release 10.5(1), or later.

- You are installing Phone Firmware, or any other update or COP file that has been signed with an RSA v3 key. RSA v3 files will contain the k3 designation seen in the following example and will start appearing on CCO mid 2015.

  ciscocm.free_common_space_v1.1.**k3**.cop.sgn

If you still aren't sure if you need to apply this COP file, you can install or even reinstall it without issue.

Note: Before you install this COP file, Cisco recommends that you review the *Important Notes* section for information about issues that may affect your system.

Updates in This Release

This patch will provide the following fix:

New Updates

CSCua88701	RSA keys used to sign images needs updating

Products Impacted:

The following products might require this Key:

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco IM and Presence
- Cisco Emergency Responder

Important Notes:

When upgrading to a new release of Cisco Unified Communications Manager, make sure that the updates in this release are included in the version you are upgrading to. If an ES or SU is installed after this update that does not also contain the fixes referenced in "*Updates in This Release"* then this update will need to be reapplied after the ES or SU is installed.

Determining the Software Versions:

You can determine the System Version of your Cisco Unified Communications Manager software that is running on your server by accessing Cisco Unified Operating System Administration.

The following information displays:

- System version: xxxxx
- VMware Installation: xxxxx

Installation Instructions:

As with any installation or upgrade, it is recommended that you apply this Update during off peak hours.

This update must be installed on all machines in the cluster, starting with the Publisher

This package will install on the following System Versions:

- 8.5.1.10000-26 or any higher version starting with 8.5.1.xxxxx
- 8.6.2.10000-12 or any higher version starting with 8.6.2.xxxxx
- 9.1.2.10000-28 or any higher version starting with 9.1.2.xxxxx

You can install a patch or upgrade version from a DVD (local source) or from a computer (remote source) that the server being upgraded can access.

Note: Be sure to back up your system data before starting the software upgrade process. For more information, see the Disaster Recovery System Administration Guide

From Local Source:

Step 1: Download *ciscocm.version3-keys.cop*

Step 2: Copy the upgrade file above to a writeable CD or DVD.

Step 3: Insert the new CD or DVD into the disc drive on the local server that is to be upgraded.

Step 4: Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

http://server-name/cmplatform

where server-name is the host name or IP address of the admin server.

Step 5: Enter your OS Administrator username and password.

Step 6: Choose Software Upgrades > Install/Upgrade.

Step 7: For the software location source, choose DVD/CD.

Step 8: If you burned the patch file to a subdirectory on the CD or DVD, enter the path in the Directory field.

Step 9: To continue the upgrade process, click Next.

Step 10: Choose "*ciscocm.version3-keys.cop.sgn*" and click Next.

Step 11: In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

When the download completes, the Checksum window displays.

Step 12: Verify the checksum value:

95a676f969777f72bfe82fa0ffd896fa

Step 13: After determining that the cheksums match, click Next to proceed with the software upgrade.

A Warning window displays the selected option.

Step 14: Click Install.

The Install Status window displays the Install log.

Step 15: When the installation completes, click Finish

Step 16: Verify the COP file version using this command from the CLI:

admin:show version active

Active Master Version: 8.6.2.xxxxx-xx <-- *Note: 8.6.2 is shown for example only; your version may vary*

Active Version Installed Software Options:

cmterm-9971.9-0-3ES-1.cop <-- *Note: Other COP files such as this may or may not already be present on your system*

ciscocm.version3-keys.cop

From Remote Source:

Step 1: Download *ciscocm.version3-keys.cop.sgn*

Step 2: Copy the upgrade to an ftp or sftp server.

Step 3: Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

http://server-name/cmplatform

where server-name is the host name or IP address of the admin server.

Step 4: Enter your OS Administrator username and password.

Step 5: Choose Software Upgrades > Install/Upgrade.

Step 6: For the software location source, choose Remote File System.

Step 7: Enter the directory name for the software upgrade, if required.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter /patches.

If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.

Step 8: Enter the required upgrade information as described in the following table:

Remote Server: Host name or IP address of the remote server from which software will be downloaded.

Remote User: Name of a user who is configured on the remote server.

Remote Password: Password that is configured for this user on the remote server.

Download Protocol: Choose sftp or ftp.

Step 9: To continue the upgrade process, click Next.

Step 10: Choose "*ciscocm.version3-keys.cop.sgn*" and click Next.

Step 11: In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

When the download completes, the Checksum window displays.

Step 12: Verify the checksum value:

95a676f969777f72bfe82fa0ffd896fa

Step 13: After determining that the checksums match, click Next to proceed with the software upgrade.

A Warning window displays the selected option.

Step 14: Click Install.

The Install Status window displays and displays the install log.

Step 15: When the installation completes, click Finish

Step 16: Verify the COP file version using this command from the CLI:

```
admin:show version active
   Active Master Version: 8.6.2.xxxxx-xx <-- Note: 8.6.2 is shown for example only; your version may vary

   Active Version Installed Software Options:

   cmterm-9971.9-0-3ES-1.cop   <-- Note: Other COP files such as this may or may not already be present on your system

   ciscocm.version3-keys.cop
```