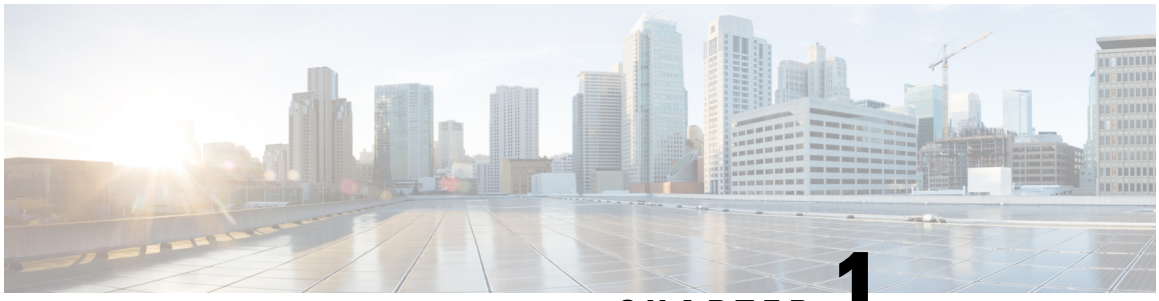
Cisco Contact Center SIP Proxy (CCCSP) Upgrade Guide

First Published: 2025-11-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

ISO Upgrade on VOS

Introduction

This document provides a step-by-step procedure to upgrade the Cisco Contact Center SIP Proxy (CCCSP) system using the Command Line Interface (CLI).

The process includes the following:

- Preparation steps
- Upgrade initiation
- Verification
- Post-upgrade validation

Prerequisites

Ensure the following before starting the upgrade process:

- The **OS admin user credentials** are available (created during installation).
- A valid upgrade image file is available on an **SFTP-enabled server**.
- The upgrade image is **incremental** compared to the currently installed version.
- Network connectivity is established between the CCCSP server and the SFTP server.

Pre-Upgrade Checks

Procedure

Step 1 Log in to the system using the **OS Admin user** credentials via SSH or terminal access.

Step 2 Check the current installed version. Run the **admin:show version active** command.

This command displays the currently active version of the system.

Step 3 Check inactive version (if any). Run the **admin:show version inactive** command.

If the system isn't upgraded before, the inactive version section will be empty.

Initiate the Upgrade

Procedure

Step 1 Run the **admin:utils system upgrade initiate** command to begin the upgrade.

Warning
Do not close this window without first canceling the upgrade.

This version only accepts COP files ending in .cop.sha512 and ISO files ending in .sha512.iso

Step 2 When prompted, choose the source where the upgrade file is saved:

- Remote filesystem via SFTP or FTP—You will be prompted to enter the server details and credentials.
- Local DVD/CD—The local CD or DVD only.
- Local image—This option is available only if you initiated an upgrade earlier and did not complete the upgrade.

Step 3 (Optional) Enter 1-4, if you choose filesystem via SFTP. Provide the image path and server details:

- **Image path**: Full directory path where the upgrade image is stored.
- **SFTP Server IP**: The IP address or hostname of the SFTP server.
- **Username and Password**: SFTP server login credentials.

Step 4 (Optional) You can specify an SMTP address for notification (for example, your Cisco ID), else skip if not required.

Step 5 When prompted, enter whether to proceed with the upgrade automatically after the upgrade file downloads.

- **Yes**—The upgrade commences once the file downloads to the system.
- **No**—The upgrade file gets saved as a Local Image. You can restart the upgrade later.

Step 6 When prompted, enter whether to switch versions automatically after the upgrade:

- **Yes**—After the upgrade, the cluster switches to the new version and reboots automatically.
- **No**—The upgrade saves to the Inactive Partition. You can switch versions manually later.

Step 7 When prompted, enter the required option for the valid upgrade file.

Step 8 When prompted to start the installation, enter **Yes**.

If you chose to switch versions automatically after the upgrade, the system reboots to the upgraded version after the upgrade. Otherwise, the upgrade saves to the inactive partition and you can switch versions manually later.

Once all information is provided:

- The system validates the upgraded image.
- Image is downloaded from the SFTP server.
- The upgrade process begins automatically.

Note The entire upgrade process typically takes around 20 minutes.

Switch Version Manually

If you did not switch versions automatically as a part of the upgrade, you can use this procedure to switch versions manually using the CLI.

Procedure

Run the **admin:utils system switch-version** command to switch to the newer version.

This command restarts the system and the system boots with the upgraded version. This process usually takes 2-3 minutes.

Post-Upgrade Validation

Procedure

Step 1 Log in again using the **OS Admin** user and verify the active and inactive version.

Step 2 Run the following commands to display the newly upgraded version:

admin:show version active

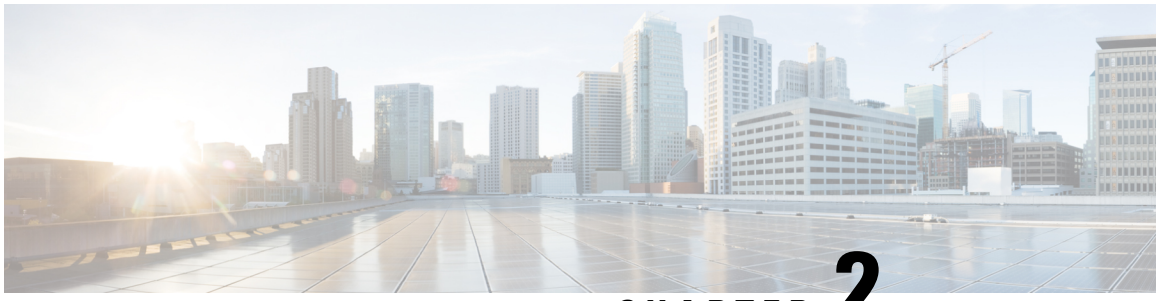
admin:show version inactive

Step 3 The system can also be accessed using the CCCSP administrator login via the web browser with its IP or hostname.

Troubleshoot and Logs

- To debug upgrade failures, check the system-history and install logs. Use the **admin:file view install** *system-history.log* and **admin:file view install** *install.log* commands.
- This log file contains detailed upgrade process and error messages (if any).

  Use the **file get install** *log file name* command to download the log file via SFTP.



CHAPTER 2

Patch Upgrade Framework for CCCSP

Patch upgrade framework that is being used is mainly from the VOS framework and the logic to apply patch or libraries are leveraged from CUSP 10.x (EOL) projects.

Patch upgrade to a CUSP project is done using Cisco Options Package (COP) files, which provides mechanism to upgrade or patch existing software in Linux environments. A few more points about COP files are as follows:

- COP file is a tar ball with .cop extension
- COP file name must start with ciscoime* and end with .cop.
- COP file must be a signed file in official release (Out of scope for this document)
- COP file provides mechanism to verify and apply patch, Error handling during patching and also roll back.

COP File Contents

COP file for CCCSP projects are maintained in repo: https://github5.cisco.com/Ecdysis/CUSP/tree/cusp_su3_15. Typical contents of a COP file are:

- actions.txt: Used by VOS patch upgrade framework (especially if reboot is needed post patching).

  Sample contents of actions.txt file:

```
reboot=no

dbinstall=no
```

- DO_NOT_RUN_INSTALLDB: Used by VOS patch upgrade framework, an empty file.
- copstart.sh: A script that is called by the framework, which does the patching activity (Sample attached, this doesn't do any patching other initiating the patch API).
- Patch files / libraries / configuration files / scripts etc: This can none or more than 1 file, which are utilized by the copstart.sh while patching.

Differences in CUSP 10.x and CCCSP 15.x patches

The following lists the differences between CUSP 10.x and CCCSP-15.0(1) patches:

Sl no.	CUSP 10.x	CCCSP-15.0(1)
1	For applying patch there's a change in sysdb version	No version change in sysdb. Applied patch information is displayed in the **show version active** command output.
2	RPM installation is possible during patch upgrade	Not recommended in VOS. However, by replacing the files similar installation can be achieved.
3	A list of patch names are maintained in the xml file.	List of patch file names are maintained in VOS. Each patch file requires install and to revert cop files.

Create, Sign, and Download COP Files

Create COP Files

COP file includes two parts, one to install the patch and the other to revert the patch. COP files are always exclusive for a release and is specific to the release. The following is the procedure to create cop files:

- The Makefile controls the naming and all the characteristics to build the COP file.

Sign the COP Files

Follow the below steps to sign the COP file:

1. Signing the COP files is done via CITG ticket. Raise a ticket here https://ctgbuild.cisco.com/cerebro7/#!
2. Once logged in create a new ticket.
   - From the **CTGBuild Ticket System** drop down list, select **Create a new Ticket**.
   - To select the project, follow the order mentioned:

     CUSP > **Cisco Contact Center SIP Proxy** > **Action Request** > **General Request** > **Enter brief Subject** > **Finish**
3. Once ticket is created, CITG team processes the case and signs the cop files. The location to download the signed COP files is shared.

Note If ticket is created during IST working hours turnaround time is 1-3 hrs. Else, time may extend.

4. Download the COP files from the shared location.
5. Change the file extension from **.cop** to **.cop.sha512** and use it during CCCSP patch upgrade.

Download COP Files

COP installation is done via CLI using the admin user on CUSP. Admin user can access the cop files in two ways for patch upgrade—via SFTP, this is done with another CUSP deployment running with SFTP service running and sharing the COP file, or manually place files in CUSP deployment in */common/download* dir. The patch upgrade procedure focuses on manual placement of cop files.

Install COP Files

Procedure

Step 1 To install COP file using CLI session:

- Start a CLI session.
- Use SSH to connect securely to the Cisco Operating System.
- In your SSH client, log in using **OS Admin user** credentials.

Step 2 Enter **utils system upgrade initiate** command for patch upgrade on VOS framework.

Multiple COP file options are displayed. The COP file that is placed in */common/download* directory is visible in Local image option.

Step 3 When prompted to choose the source for the upgrade file:

a. Remote filesystem via SFTP—You will be prompted to enter the server details and credentials.

b. Remote filesystem via FTP—You will be prompted to enter the server details and credentials.

c. Local DVD/CD—The local CD or DVD only.

d. Local image—This option includes the COP file required for the upgrade.

Step 4 Enter **4** to choose local image cop file.

Step 5 (Optional) You can specify an SMTP address for notification (for example, your Cisco ID), else skip if not required.

Step 6 When prompted, enter whether to proceed with the upgrade automatically after the upgrade file downloads.

- **Yes**—The upgrade commences once the file downloads to the system.
- **No**—The upgrade file gets saved as a Local Image. You can restart the upgrade later.

Step 7 When prompted, enter whether to switch versions automatically after the upgrade:

- **Yes**—After the upgrade, the cluster switches to the new version and reboots automatically.
- **No**—The upgrade saves to the Inactive Partition. You can switch versions manually later.

Step 8 When prompted, enter the required option for the valid upgrade file.

COP file download and the upgrade process is initiated automatically.

Step 9 System reboot is not required for installation using a COP file for the changes to take effect.

Step 10 After successful upgrade installation using COP file, patches are applied.

The complete log can be found at */common/log/install/install_log_<date>.log*

Step 11 To verify the installed patches:

- Log in again using the **OS Admin user** credentials.
- Run the **admin:show version active** command to verify the installed patches.

Revert Patch Changes using COP File

Procedure

Step 1 To revert the patch changes, install a **revert cop file**.

Step 2 Follow the steps as discussed in the patch upgrade section. When prompted to select a COP file for installation, choose the revert cop file.

Note
After every cop installation the files under */common/download* directory are cleared. Copying the cop files is necessary else use the FTP.

Add a new COP file for patching a different issue

Create Install COP file

Follow the steps to populate the COP scripts to the working directory (steps from README.txt)

1. Update the **apply_patch()** API completely in **copstart.sh** files according to the patches to be applied.
2. Make sure that the API update takes care of patching and reverting in case of failures, logging exact messages, restart the services as needed.
3. More functions or supporting scripts can be added for **copstart.sh** to be used.

Note No need to update the Makefile.

4. Edit **CUSP/setenv.sh** and **cop.mk** for patch name and files to be modified.
5. Once code update is complete, follow steps in *Sign and Install the COP Files*.

Create Revert COP file

Follow the below steps to populate the cop scripts to the working directory (steps from README.txt)

1. Move **copstart_revert.sh** to **copstart.sh**.
2. Update the **revert_patch()** API in **copstart.sh** file according to revert the patches to be applied.
3. Make sure that the API update takes care of patching and reverting in case of failures, logging exact messages, restart the services as needed.
4. More functions or supporting scripts can be added for **copstart.sh** to be used.

Note No need to update the Makefile.

5. Edit **CUSP/setenv.sh** and **cop.mk** for patch name and files to be modified.
6. Once code update is complete, follow the steps in *Sign and Install the COP Files*.

FAQs

1. Q. What happens if the cop files are run multiple times

   A. copstart.sh file checks if the patch is already applied or not and then apply the patch
2. Q. How to restart CCCSP after applying changes

   A. Update `reboot=no` to `reboot=yes` in actions.txt file.
3. Q. How to restart a service after applying changes to a service or a config file

   A. copstart.sh file reboots the service after successful patch upgrade.
4. Q. Where to find the patch upgrade run logs

   A. /common/log/install/install_log_<date>.log