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.