Backup and Restore Cisco Prime Collaboration Provisioning

Perform Backup and Restore

Cisco Prime Collaboration Provisioning allows you to backup your data and restore it. You can schedule periodic backups using the Provisioning UI (Schedule Backup Using the Provisioning User Interface, on page 3).

Note **For upgrading Cisco Prime Collaboration Provisioning 12.4 and later releases**

In Cisco Prime Collaboration Provisioning 12.4, backup and restore requires a mandatory password for enhanced security. Hence, after the upgrade to 12.4, all scheduled backup jobs from 12.x fail. Once upgrade from 12.x to 12.4 is complete, you can cancel all the previously scheduled and saved jobs. The admin has to either reset the password and schedule the backup again or delete the scheduled backup job and reschedule it on 12.4. You can view the upgrade logs for the appropriate message.

There are two backup and restore scenarios; select the set of procedures that matches your scenario:

- Backup and restore with the same installation or a new installation. For this scenario, see Schedule Backup Using the Provisioning User Interface, on page 3.

Note When backing up files, place the files on a different file server. Also, burn the backup data onto a CD.

Cisco Prime Collaboration Provisioning allows you to back up system data and restore it on a different system in the event of total system failure. To restore the backup from another system, the following prerequisites must be met:

- Ensure that the server to which data is restored has the same MAC address as that of the system that was backed up (the IP address and the hostname can be different).
- If you are unable to assign the MAC address of the original system (the one that was backed up) to another system, contact the Engineering Team for information on a new license file (for a new MAC address).
- The procedure to backup and restore data on a different system is the same as the procedure to backup and restore data on the same system.

Back Up Provisioning Database from Console CLI

This procedure requires that you have administrator level access to the Provisioning database (the PostgreSQL database).

Step 1 Login as troubleshooting user using SSH with port 22

Step 2 Navigate to the **/opt/cupm** folder and enter the following command:

```
sudo ./cupm-app-service.sh stop
```

Step 3 Stop Apache, JBoss, and NICE Services using the following commands:

```
ps -aef | grep startcupm
ps -aef | grep nice
kill -9 <startcupm process ID>
kill -9 <nice process ID>
```

Step 4 Go to the directory using the command:

```
cd /opt/postgres/pghome/bin
```

Step 5 Run the following command:

```
sudo ./pg_dumpall -o -Upmadmin > /<backup_directory_name>/<backup_file_name>
```

where,

- *pmadmin*—postgres user id
- *backup_directory_name*— For sudo user, the directory name is **/home/<sudo User directory>**. For Example: If sudo user is 'testuser' , directory name will be /home/testuser/
- *backup_file_name*—Backup will be created with this file name.

Step 6 In a backup folder, make copies of the following files and directories:

- /opt/cupm/sep/dfc.properties
- /opt/cupm/sep/ipt.properties
- /opt/cupm/sep/dfc.keystore
- /opt/cupm/jboss/server/cupm/conf/login-config.xml
- /opt/cupm/jboss/server/cupm/deploy/dfc-ds.xml

- /opt/cupm/sep/ipt/.system/.pcprandom.key

Step 7 Start Apache, JBoss, and NICE Services using the following commands:

```
cd /opt/cupm
sudo ./cupm-app-service.sh start
```

Schedule Backup Using the Provisioning User Interface

You can create periodic backups of Provisioning database using the Provisioning User Interface. You must be logged in as an administrator to perform backup. To create a backup of the Provisioning database:

Before you begin

The prerequisites for a successful SFTP backup for a non-root user are as follows:

- The backup folder is manually created in advance
- The backup folder has the group or owner as root
- The backup folder has the correct read and write permissions

Step 1 Choose **Administration > Backup Management**.

Step 2 In the Backup Management page, click **New.**

Step 3 Enter a backup title in the Create New Backup page.

Step 4 From the Backup Connection drop-down list, select SFTP, FTP, or Local to save your backup files.

a) If you select SFTP or FTP, provide the following details:

- IP address of the server where the backup files need to be saved.
- Path to the backup location and port details (for SFTP only).

  Note The backup location is relative to the specified SSH user home directory. The relative path must contain directory details (for example DIRNAME or DIRNAME 1 / DIRNAME 2), to avoid backup in root directory.

- Username and password information. Testing the SFTP or FTP password is optional.

Note Taking backup through SFTP on another PCP server in FIPS mode is not supported.

b) If you select Local, the backup files are saved to the CUPM local directory.

Note Ensure that the destination path for SFTP, FTP, or Local is not given as “opt/backup”

Note If backup fails, verify whether the temporary backup folder "**backup**" is present at /opt. If present, delete it:

1. Create a console account from the troubleshooting web application.
2. Log in to console and delete the content of the /opt/backup folder and then the backup folder.
3. Trigger the backup again.

Step 5 For a local backup, select the number of backup files you want to save on your local machine from the Backup History drop-down list.

The default value is 2. By default, you can save two recent backup files. You can save up to 9 recent backup files.

Step 6 Enter the scheduling details to schedule a backup.

The time displayed is the server browser time. The default recurrence type for a new backup job is None. After a backup job is created with default settings, the backup will start immediately.

Step 7 Enter email address to receive status notification for the scheduled backup. You can enter multiple email addresses separated with a comma.

Step 8 Click Save. The scheduled backup appears in the Backups table on the Backup Management page.

Step 9 Click Run Now, to run a backup immediately.

Prime Collaboration Provisioning enters maintenance mode before backup starts. A notification will be displayed for all logged-in users stating that the users will be logged out of Prime Collaboration Provisioning 10 minutes before the scheduled backup starts. Users must save their work and log out before the backup starts, else they will be logged out automatically, and will not be able to access Prime Collaboration Provisioning.

The backup table provides information on the status and history of each backup job. The Next Run Time option provides details on the next periodic schedule.

The Last Run Status column shows the status of the last run backup job. The status of a backup job can be Scheduled, In Progress, Success or Failed.

When a backup job reaches the scheduled time, the last run status changes to Scheduled. After entering into maintenance mode, that is after 10 minutes, the status will change from Scheduled to In Progress.

After the backup job is complete, the status is either Success or Failure.

To know about the history of any backup job, click **Run History Count**, and open the dialog box. You can view the start time, end time, status and file size of the backup. You can delete the run history logs. The backed up files are not deleted when the backup logs are deleted.

Managing Backup Jobs

With the scheduled jobs, you can:

- Edit and Delete: The Edit and Delete options are disabled during Scheduled and In Progress states. You cannot edit or delete a backup job when the backup is in Scheduled or In Progress state. You can edit only one backup job at a time.
- Cancel: You can cancel a running backup job which is in Scheduled or In Progress state only.