Troubleshooting

This appendix provides CLI-related information for TAC.

Note For CLI access, contact Cisco TAC.

Changing the SSL Port

To change the port used by Cisco Prime Collaboration Provisioning for SSL:

Step 1 In the Cisco Prime Collaboration Provisioning system, open the ssl.conf file located at /opt/cupm/httpd/conf.

Step 2 Change the port number in the following lines:

```
Listen 443

VirtualHost_default_:443

ServerName www.example.com:443

RewriteRule ^/?(.*) https://%{SERVER_NAME}:443/$1 [R,L]
```

Note After you change the port number, you must enter the new port number when you access Cisco Prime Collaboration Provisioning.

Step 3 Save the changes and close the file.

Step 4 Open the httpd.conf file located at /opt/cupm/httpd/conf.

Step 5 Change the port number in the following line:

```
RewriteRule ^/?(.*) https://%{SERVER_NAME}:443/$1 [R,L]
```

Step 6 Save the changes and close the file.

Step 7 Restart the Apache server by using the following commands:

```
/opt/cupm/httpd/bin# ./apachectl -k stop
/opt/cupm/httpd/bin# ./apachectl -k start -DSSL
```

Configuring Cisco Prime Collaboration Provisioning Server Time Zone

You can provide Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT), updated with leap seconds.

To change the time zone in the Provisioning server:

Step 1 Log into the Cisco Prime Collaboration Provisioning server with the Console User Login account.

Step 2 Enter the following command to check the configured timezone:

```
user $ timedatectl
```

Step 3 Enter the following command to see the list of supported time zones:

```
user $ timedatectl list-timezones
```

Step 4 Enter the following commands to set the time zone for the Cisco Prime Collaboration Provisioning server:

```
user $ timedatectl set-timezone Asia/Kolkata
```

Step 5 Navigate to **cd /opt/cupm/sep**.

Step 6 Update the following property in the dfc.properties file to update the offset:

```
dfc.gui.utc_offset=<applicable offset for your geographic location>
```

For example, if you are in IST time zone, you must enter: `dfc.gui.utc_offset=+0530`

Step 7 Restart the services

```
sudo /opt/cupm/bin/cpcmcontrol.sh stop
sudo /opt/cupm/bin/cpcmcontrol.sh start
```

Note You can also restart the services from Cisco Prime Collaboration Provisioning >Process Management Page.

Synchronizing Special Directory Numbers

Prior to the Cisco Prime Collaboration Provisioning 9.5 release, Cisco Prime Collaboration Provisioning only synchronizes those Directory Numbers (DN) whose endpoints are managed by Cisco Prime Collaboration Provisioning and will not have a complete knowledge of the DNs configured by Cisco Unified Communications Manager. There might be instances of few special DNs configured on Cisco Unified Communications Manager.

Special Directory Numbers:

- The DN features which are present in Cisco Unified Communications Manager but not managed by Cisco Prime Collaboration Provisioning. For example, Intercom DN.
- The DN attached to endpoints which are not managed by Cisco Prime Collaboration Provisioning.

Note Provisioning has a limited support of endpoints and does not support all the endpoints available in Cisco Unified Communications Manager.

From Cisco Prime Collaboration Provisioning 10.0 and above versions, you can synchronize all special DNs as part of user synchronization. This feature will be disabled by default. To enable this feature, you must add the following property to /opt/cupm/sep/ipt.properties file:

```
dfc.ipt.cisco.ccm.sync.orphanDN=true
```

By enabling this property, Cisco Prime Collaboration Provisioning synchronizes more DN's and takes additional time to complete the user synchronization process. Time taken depends on the number of special DN's configured in Cisco Unified CM.

Note After updating the ipt.properties file, you must restart the cupm services for the changes to take effect.

When this feature is enabled, the provisioning orders are validated from Provisioning, rather than submitting it to Cisco Unified Communications Manager which results in failure.

Provisioning and Special DN conditions:

Any provisioning activity carried out from Cisco Prime Collaboration Provisioning, which tries to re-use such special DNs, can result in provisioning failure.

- When the provisioning line is auto-assigned, line will not be provisioned if the DN is already used.
- When the provisioning line is chosen manually, Cisco Prime Collaboration Provisioning will throw an error during provisioning.

Restore the Single-Machine Provisioning Database

Before you begin

If you are restoring to a new installation, have the system with the new installation up and running before beginning this procedure. This procedure requires that you have administrator level access to the Provisioning database (the PostgreSQL database).

If you are restoring the database on a new system, you must verifying that the following ports are not being used by another application:

- dfc.jboss.port=46008
- dfc.postgres.port=5432
- dfc.nice.rmi.registry.internal.port=46001

- dfc.webport=80

If a port is being used by another application, you must change the port number to a vacant port. These settings are defined in the /opt/cupm/sep/dfc.properties file. If you accepted the default location during installation, the installation directory is /opt/cupm.

Step 1 Login as troubleshooting user using SSH with port 22.

Step 2 Navigate to the **/opt/cupm** folder and enter the following command to stop the application services like Apache, JBoss and NICE:

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

Step 3 Ensure whether the application services are stopped by using the following command:

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

a) To check whether the nice process is still holding on the postgres connection, enter the following command:

```
ps -aef
```

b) Look for the process: /opt/cupm/jvm/bin/java -server -classpath /opt/cupm/sep/lib/dom.jar:/opt/cupm/sep/lib/jaxbapi.jar:/opt/cupm/sep/lib/jaxb-impl.jar

If the process is running then enter the following command:

```
kill -9 <Process-Id found earlier>
```

Step 4 If you are restoring to the same installation, then proceed to the next step, if you are restoring to a new installation, paste the backed-up file (bak) into /mnt folder

Step 5 Go to the directory using the command:

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

Step 6 Run the following command to restore the database:

```
sudo ./CUPM-restore.sh <username> <password> <backup_file_name with Absolute Path>
```

where, username is the username of the PostgreSQL administrator. The default administrator username is pmadmin; the password is same as you entered for globaladmin.

If you are getting the following error:

```
"dropdb: database removal failed: ERROR:  database "cupm" is being accessed by other users"
```

Do the following:

a) Check whether the nice process is still holding on the postgres connection by using the following command:

```
ps -aef
```

b) Look for the process: /opt/cupm/jvm/bin/java -server -classpath /opt/cupm/sep/lib/dom.jar:/opt/cupm/sep/lib/jaxbapi.jar:/opt/cupm/sep/lib/jaxb-impl.jar

If the process is running then enter the following command:

```
kill -9 <Process-Id found earlier>
```

c) Run the restore command again (./CUPM-restore.sh <username> <password> /mnt/<backup_file_name>).

Step 7 If you are restoring to the same installation, proceed to next step. If you are restoring to a new installation, copy back the following backed-up files. To copy the file using ssh, copy the files at **/home/<sudo user directory>** , and then copy using **sudo cp <file_name> <Absoulte_Patch_file_name_to _ be_copied>**. For example: If sudo user id is 'testuser', and file to be copied is 'dfc.properties' file at /home/testuser/, Using ssh, copy dfc.properties file at /home/testuser/ and then, copy the file again to mentioned directory using the command sudo cp /home/testuser/dfc.properties /opt/cupm/sep/dfc.properties

- /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/custom.properties
- /opt/cupm/sep/passwordpolicy.properties

Note To restore the random key, refer Restore the Single-Machine Provisioning Database, on page 3.

Step 8 Start Apache, JBoss, and NICE Services using the following commands:

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

Restoring Random Key

The backup compressed file created by Backup Management (**Administration > Backup Management**) includes a copy of random key file.

Step 1 Copy the backed up directory to the server. Navigate to /opt/cupm/sep/ipt/.

Step 2 Create a directory .system (if it does not exist) using the mkdir command, else move to step 3.

Step 3 Navigate to /opt/cupm/sep/ipt/.system.

Step 4 Copy the following from backed up directory:

```
cp <BACK UP DIR>/pcprandom.key .pcprandom.key
cp .pcprandom.key .pcprandom.key.bkp
touch .pcprandomconfigured
```

Restore the Database from the Provisioning User Interface

For Cisco Prime Collaboration Provisioning 12.2 and later

The user can restore the database from the PCP user interface.

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

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

Step 3 In Database Restore page, select the required restore options:

- **Automatic**: If you select **Automatic**, and click **Find Backups**. It displays the list of the available backups, select the required backup, and click **Restore**. A warning is displayed stating, Database backups, Backup yyyy-mm-dd hh:mm:ss, will now be restored. Current system data will be lost. The application will not be accessible. Do you wish to continue? click **Yes** to continue.
- **SFTP** or **FTP**

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

  - IP address of the server where the backup files is saved.
  - Provide the port details.
  - Path to the backup location.
  - Username and password information.
  - Click**Find Backups** . It displays the list of the available backups, select the required backup, and click **Restore**. A warning is displayed stating, Database backups, Backup yyyy-mm-dd hh:mm:ss, will now be restored. Current system data will be lost. The application will not be accessible. Do you wish to continue? click **Yes** to continue.

- **Local Disk**

  If you select Local, provide the following details:

  - Path to the backup location.
  - Click**Find Backups** . It displays the list of the available backups, select the required backup, and click **Restore**. A warning is displayed stating, Database backups, Backup yyyy-mm-dd hh:mm:ss, will now be restored. Current system data will be lost. The application will not be accessible. Do you wish to continue? click **Yes** to continue.

  Once the restore process begins in Cisco Prime Collaboration Provisioning, it directs you to a static page, where the logs can be viewed, and after the completion of restore process, you are directed to the Cisco Prime Collaboration Provisioning login screen.

  Note In troubleshooting UI, once the restore process begins, it directs you the restore progress screen, where the logs can be viewed and the Start another DB Restore button is available. Click **Start another DB Restore** to start another restore process.

  Note This functionality is also available in Troubleshooting UI, which can be used when the PCP/JBOSS are down.

  Note Currently, restore from Cisco Prime Collaboration Provisioning user interface is not supported in case of backed up database having a different password than the server on which it is being restored. For such cases, the user needs to restore the database from CLI.

Self-Care User Migration Script

The SelfCareMigrationUtility can be invoked during the migration, or from the CLI, after migration. The tool processes all the users in the domains that have CreateSelfCareAccounts rule and DefaultCUPMPassword rule set.

This tool can be run through CLI from /opt/cupm/sep/ipt/bin. It can be run either globally (means for all domains) or for a single domain.

To run script:

Step 1 Go to /opt/cupm/sep/ipt/bin.

Step 2 Run: `./SelfCareMigrationUtility.sh ALL ENABLE`

- ALL—Indicates all domains.
- ENABLE—Enables selfcare for all users in the domain specified.

Tto disable selfcare option, run:

```
./SelfCareMigraionUtility.sh ALL DISABLE
```

The script can be run at the domain level also. To do this, run:

./SelfCareMigrationUtility.sh *DOMAIN NAME* [ENABLE | DISABLE]

For more information on migration, see the Cisco Prime Collaboration Upgrade and Migration Guide.

Retaining User Information During System Reboot

For Cisco Prime Collaboration Release 11.5 and later

This method of creating new user helps to retain the user information that is lost during system reboot.

Step 1 Log in to CLI as root.

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

```
useradd <username>
passwd <username>
```

Step 3 Enter the password.

Step 4 To retain the user data, enter the following command:

```
cp /etc/shadow /storedconfig/startup-config-*/etc/shadow
```

Step 5 Enter **Yes** to continue.

Step 6 Enter the following command:

```
cp /etc/passwd /storedconfig/startup-config-*/etc/passwd
```

Step 7 Enter **Yes** to continue.