Maintaining the Server

Managing Log Files

Cisco Prime Collaboration Provisioning writes application log files for the Service Enabling Platform (SEP) module (sep.log), the Network Interface and Configuration Engine (NICE) service (nice.01.log), Unified CM AXL responses and requests, Unity Connection SQL queries, and Presence AXL information.

As an administrator, you can manage the log files using:

- Cisco Prime Collaboration Provisioning user interface, where the log files can be viewed and downloaded by navigating through **Administration** > **Logging and ShowTech**.

You cannot disable logging. However, you can:

- Collect more data when needed by increasing the logging level
- Return to the default logging level (NORMAL)

Following are the available logging levels:

- DETAIL
- NORMAL

- HIGH

The log files are backed up every hour, or when they reach their maximum log size limit. The default size limit is 20 Mb (see Changing the Maximum Log File Size). The files are saved in the format sep.log.date stamp timestamp.

The log files are deleted from the Cisco Prime Collaboration Provisioning server when their size exceeds 5000 MB or the number of log files in the logs folder exceeds 500. If you want to change these levels, see Changing the Log Purging Level.

Changing the Log Level (GUI)

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration** > **Logging and ShowTech**.

Step 2 In the **View and Set Logging Levels** pane, you can view the existing logging levels and change them to the desired level.

Following are the available logging levels:

- DETAIL (provides detailed log information and uses more disk space)
- NORMAL (provides the basic information)
- HIGH (provides high-level log information only)

Note By default, the log level is set to NORMAL. To view the Unified CM AXL responses and requests logs, the logging level must be set to Normal or Detail.

Step 3 Click **Save Settings**.

Changing the Maximum Log File Size

Procedure

Step 1 On the Cisco Prime Collaboration Provisioning system, go to the `opt/cupm/sep` folder.

If you accepted the default location during installation, the installation location is /opt/cupm.

Step 2 Open the dfc.properties file and change the dfc.log.maxsize property to the desired size (default is 20 Mb).

Step 3 Save the changes and restart the Provisioning services as your changes will not take effect until Cisco Prime Collaboration Provisioning is restarted. To restart:

a) Log into the server using SSH.
b) Go to /opt/cupm folder and execute the ./cupm-app-service.sh stop command.

c) Check whether the services are down by executing the following command:

```
ps -aef | grep standalone
```

If there are any processes running, kill those services by using the following command:

```
kill -9 <processID1> <processId2>
ps -aef | grep nice
```

If there are any processes running, kill those services by using the following command:

```
kill -9 <processID1> <processId2>
```

d) Check if the port 8009 is free (used by JBoss):

```
netstat -a | grep 8009
```

If this port is in use, wait till it gets free.

Step 4 Start the application services:

```
execute ./cupm-app-service.sh start
```

Wait for the services to start.

Changing the Log Purging Level

Procedure

Step 1 On the Cisco Prime Collaboration Provisioning system, go to the `/opt/cupm/sep` folder. If you accepted the default location during installation, the installation location is /opt/cupm.

Step 2 Open the ipt.properties file, and do one or both of the following:

- To change the maximum file size level, update the dfc.purgelog.maxused_mb property to the desired level.
- To change the maximum number of log files level, update the dfc.purgelog.maxlogsaved property to the desired level.

Step 3 Save the changes, and restart the Cisco Prime Collaboration Provisioning services, as your changes will not take effect until Cisco Prime Collaboration Provisioning is restarted.

a) Log into the server using SSH.
b) Go to /opt/cupm folder and execute the ./cupm-app-service.sh stop command.
c) Check whether the services are down by executing the following commands:

```
ps -aef | grep standalone
```

If there are any processes running, kill those services by using the following command:

```
kill -9 <processID1> <processId2>
ps -aef | grep nice
```

If there are any processes running, kill those services by using the following command:

```
kill -9 <processID1> <processId2>
```

d) Check if the port 8009 is free (used by JBoss):

```
netstat -a | grep 8009
```

If this port is in use, wait till it gets free.

Step 4 Start the application services:

```
execute ./cupm-app-service.sh start
```

Wait for the services to start.

Generating and Downloading Showtech Files

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration** > **Logging and ShowTech** .

Step 2 Click **Generate ShowTech**. The **Collect ShowTech** window opens.

Step 3 Enter the following information:

- File Name—Enter the file name as it is mandatory. By default, it is auto-populated as ShowTech-2014-12-01-012705.
- Duration—Select the duration
  - Range—By default, the date range is the server-installed date. You can modify this date but make sure the From date is greater than the server-installed date and the To date is lesser or equal to the current server time.
  - Last—You can select a relative duration with this option.
- Select Components—Select the required components. By default, all components are selected.

Step 4 Click **Start Collection** to collect the showtech information for the selected duration. Once the showtech collection is complete, you can see the showtech zip file generated in the table.

Step 5 Unzip the file to view the showtech information.

Browsing Logs

Cisco Prime Collaboration Provisioning allows you to launch and view the following logs for online troubleshooting:

- Application and NICE logs

Note By default, user name during login is case sensitive. If "Login user name is case-insensitive" setting is enabled, Cisco Prime Collaboration Provisioning will perform case insensitive authentication.

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration** > **Logging and ShowTech**.

Step 2 In the **Browse Logs** pane, click the Application and NICE Logs link. The logs are fetched from the server and you can view them on the browser for troubleshooting.

Step 3 (Optional) To download a log file:

a) In the Application and NICE Logs page, click the download icon for that file.

b) In the popup window, select the **Save File** option and click **OK**.

The log file is downloaded to your local machine.

Troubleshooting Account

For Cisco Prime Collaboration Provisioning 12.5 and later

When you log in to the Troubleshooting Account User login page for the second time, it displays the successful date and time of the previous login.

This feature enables you, as a user with full access, to create a troubleshooting account (**Administration > Logging and ShowTech**) from Cisco Prime Collaboration Provisioning to debug and monitor issues. In addition, you can use a troubleshooting user interface to debug and monitor the Cisco Prime Collaboration Provisioning server. The troubleshooting user interface displays details of logs, process management, DB Restore, memory usage, disk usage, and so on.

To create a troubleshooting account and launch the troubleshooting UI:

Before you begin

- The option to create a troubleshooting account is only available to a user with full access.
- As a troubleshooting user, you cannot delete your account.
- As a troubleshooting user, you cannot change your password.

- Only one troubleshooting account is valid per Cisco Prime Collaboration Provisioning server.

Note Only a privileged user can restart the three services (JBoss, NICE and Trouble shooting Service) and a user can be assigned privilege to restart only one service at any point of time.

Procedure

Step 1 Choose **Administration > Logging and ShowTech > Troubleshooting Account**.

Step 2 Enter the User ID with which you can login to the troubleshooting account. Valid values are alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), space ( ), apostrophe, and at sign (@).

Step 3 Choose the number of hours the account should be active from the **Expires in** drop-down.

Step 4 Click **Create Account**.

Step 5 Click **Click to create email** to pass the account details to TAC to generate the password for the troubleshooting account that has been created.

Step 6 Once the account is created you can launch the Troubleshooting UI in two ways:

- Click **Go to Log In** and enter the credentials to login. You are redirected to **Cisco Prime Collaboration Provisioning - Troubleshooting** page where **Logs** menu is displayed by default.
- Through the **https://pcp-server-ip-address:28080/index** URL syntax. This option checks if the troubleshooting account already exists or not. If the account exists, you are redirected to the login page, and using troubleshooting user credentials you can access the menus. If the troubleshooting account does not exist, you are redirected to create an account.

Note Once you login into Cisco Prime Collaboration Provisioning as a troubleshooting user (choose **Troubleshooting** menu), you can either click **Launch** to launch the Troubleshooting UI or **SEP Admin** to launch the sep admin page.

You can also delete the troubleshooting account (**Delete Account**).

Managing System Settings

Cisco Prime Collaboration Provisioning allows you to manage various system settings through the Provisioning interface. It provides you the options to select or unselect the following feature settings:

- Analog Endpoint Support—This setting allows analog endpoints to be provisioned.
- Maintenance Mode Popup Notification—This setting, when enabled, gives a message to all logged in users when the system falls to maintenance mode.
- Allow orders in progress to be stopped after—This setting allow you to schedule time interval to stop the processing orders.
- **For Cisco Prime Collaboration Release 11.6 and later**

Disable 'globaladmin' account—This checkbox (**Administration > Settings > General**) is used to disable globaladmin user account.

Note This checkbox will be available only for users with full access. Once globaladmin account is disabled, you cannot undo and the checkbox is replaced with a green tick mark.

- Password Policy Settings—These settings allow you to manage your user passwords. Refer Managing User Passwords section for more information on password settings.
- Self-Care Feature Access Settings—These settings allow you to have access to all self-care features when you log into the self-care account. It is recommended not to disable these settings.
- **For Cisco Prime Collaboration Release 11.5 and later**

  Federal Information Processing Standard (FIPS)—This setting allows you to enable or disable FIPS. Refer Configure FIPS, on page 9 for more information on FIPS settings.

- **For Cisco Prime Collaboration Release 11.6 and later**

  Banner and Login Message—The **Administration > Settings > Banner and Login Message** setting enables you, as a user with Full Access privilege, to customize a banner on the login page, all pages of Cisco Prime Collaboration Provisioning, and self-care portal. You can define the classification text to be added for the reports or documents generated out of Cisco Prime Collaboration Provisioning.

  - The banner screen contains **Show Banner Message**, **Show Banner for Exported Reports** and **Show Login Message** checkboxes, which are disabled by default. When you select a checkbox, the appropriate banner is displayed.
  - You can customize the banner message using the appropriate **Color Scheme** and **Text Size** drop-down list.
  - You can classify any data using the banner, such as classifying the output of reports generated from Cisco Prime Collaboration Provisioning, classifying the output for sample batch files, and classifying the output for all log files. The following table lists the reports that are considered for classification.

Report	Report Type
Service Area	Print
Resource Configuration	Print
Service Configuration	Print
Directory Number Inventory	Print
Directory Number Block	Print
Endpoint Inventory	Export
Endpoint Line Mismatch	Export
Audit Trail	Export
Custom Reports	Export

Report	Report Type
Access Control	Export
Export Endpoints without associated users	Export

- You can customize your own messages, such as information of maintenance mode or application upgrade.

- **For Cisco Prime Collaboration Release 12.1 and later**

  Read-only and Security Changes—This feature enables you to list application users in Cisco Prime Collaboration Provisioning and supports Service Provisioning for the application users, mainly endpoint and line services. In addition, this feature enables you to add Controlled Devices to the application users.

  Check **Manage CUCM Application Users as Provisioning User** checkbox in Cisco Prime Collaboration Provisioning (**Administration > Settings**) to manage the application users. If the setting is enabled, the application user in Cisco Unified CM is synchronized in Cisco Prime Collaboration Provisioning and displayed on the **User Provisioning** page as a normal user. The devices associated to the application user in Cisco Unified CM are displayed in the customer record page

  Disable write access for North Bound API (Read-Only Allowed)—This checkbox (**Administration > Settings > General**) is used to disable write access for North Bound API and allows only get and list requests.

- **For Cisco Prime Collaboration Release 12.3 and later**

  Number of failed login attempts before locking account-- This setting allows the user to set the limits for the number of failed login attempts. The user can select the number from the drop-down list.

  Lock the user account-- This setting allows the user to select the time period for which the account will be locked after the number of failed login attempts exceeds the set limit. Temporarily and Permanently are the two options available.Temporarily is the default option. For upgraded system, the default option is Permanently.

  All user accounts will be unlocked after--- This setting allows the user to set a time period after which the account will be unlocked. In case of the Temporarily option, the user can select a value from the drop-down list. In case of the Permanently option, all the user accounts need to be unlocked manually. However, for globaladmin and the users of the Administration Group, the user can set the time period after which the account will be unlocked using the drop-down list.

Note By default, all system settings are enabled.

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration > Settings**.

Step 2 In the System Settings pane, check or uncheck the required check boxes and click **Update**.

Custom Settings

Custom settings are intended for debugging.

Note Restart the application, if a setting is removed.

Warning Do not try to configure any values in the Custom Settings text box as it is recommended only for Cisco Support. Setting an inappropriate value may cause the application to stop functioning.

Configure FIPS

For Cisco Prime Collaboration Release 11.5 and later

Cisco Prime Collaboration Provisioning supports the Federal Information Processing Standards (FIPS). The **Federal Information Processing Standard (FIPS)** option under **System Administration** > **Settings** is accessible only to the users with administrator privileges.

FIPS are U.S. government computer-security standards. The FIPS-140 series of standards specifies requirements for cryptography modules. For more information, see http://www.nist.gov/itl/fips.cfm.

Note By default, FIPS is disabled in Cisco Prime Collaboration Provisioning. The administrator can configure FIPS in the Cisco Prime Collaboration Provisioning server. Once the changes are updated, the system restarts automatically.

Before you proceed to enable or disable FIPS, ensure that:

- No active orders are in progress.
- No active batch projects are in progress.
- No synchronization in progress.
- The third-party CA signed certificates meet the FIPS approved encryption algorithm requirements.

You can perform the following actions:

To perform this action:	Do the following:
Enable FIPS	1. Choose **Administration** > **Settings**. 2. Click **Federal Information Processing Standard (FIPS)**, and check the **Federal Information Processing Standard (FIPS)** check box. 3. Click **Update**. 4. Click **Yes** in the confirmation message box to continue, otherwise click **No** to return to the Settings page.
Disable FIPS	1. Choose **Administration** > **Settings**. 2. Click **Federal Information Processing Standard (FIPS)**, and uncheck the **Federal Information Processing Standard (FIPS)** check box. 3. Click **Update**. 4. Click **Yes** in the confirmation message box to continue, otherwise click **No** to return to the Settings page.
Check FIPS status	1. Choose **Administration** > **Settings**. 2. Click **Federal Information Processing Standard (FIPS)**, If the **Federal Information Processing Standard (FIPS)** check box is checked, FIPS is enabled otherwise it is disabled.

Process Management

For Cisco Prime Collaboration Release 11.1 and later

The **Process Management** menu enables you to restart the Cisco Prime Collaboration Provisioning application services from the user interface. This feature eliminates the need to log in as a root user into the system and restart the services.

Navigate to **Administration > Process Management** to view the **Process Management** page.

On the **Process Management** page, you can view the current state of the processes such as PostgreSQL, Apache, JBOSS, and NICE.

Also, you can restart individual or all the processes as follows:

- Restart All Processes—To restart all the processes such as Apache, JBOSS, PostgreSQL, and NICE, click **Restart All Processes**.
- Restart Individual Processes—To restart specific processes click the **Restart** against the respective process name. You can restart the process such as Apache, JBOSS, PostgreSQL, and NICE.
- Reboot Server—To reboot the Linux server and restart PCP Application, click **Reboot Server**.

In a distributed environment, you can reboot the Application server and restart services such as Apache, JBOSS, and NICE. The Reboot option is not available for the Database Server. However, you can restart PostgreSQL on the Database Server.

The **Process Management History** displays the restart history details such as the user who initiated the restart operation, process name, restart date, and reason for restart. Using restart history, you can analyze when, why, and who restarted the service. For services which are restarted automatically, the user is displayed as **System** and the reason is displayed as **Service restarted automatically**.

Note

- The **Process Management** page provides only static or snap-shot information about the processes. Refresh the **Process Management** page to know the status of the process. Click the refresh icon in the top left corner of the page to refresh the page.
- For all the operation except NICE restart, you are redirected to **Application Unavailable** page. On completion of the restart or reboot operation, you are redirected to the application **Login** page and the details are updated in the restart history table.
- For NICE, when you restart the process, instead of redirecting to the **Application Unavailable** page, the **Restart** button is disabled. The **Restart** button gets enabled automatically on completion of the restart operation and the details are updated in the restart history table.

Managing Localization Languages

As an administrator, you can upload a new language file or modify an existing language file and manage localization directly from the Cisco Prime Collaboration Provisioning interface.

To upload a new language file:

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration > Updates**. The Application Software Updates page shows a table with the list of supported languages for localization.

Step 2 Click **Add**. In the **Add a Language Pack** dialog box, choose a new language file and click **Upload**. If there is a new language pack for the existing language, you have an option to overwrite the same.
A popup appears saying that the new language pack is successfully uploaded.

Step 3 Change your browser settings to select a preferred language.

Step 4 Refresh the browser to see the changes to the Cisco Prime Collaboration Provisioning interface in your preferred language.

Certificates Supported in Cisco Prime Collaboration Provisioning

There are two types of certificates supported in Cisco Prime Collaboration Provisioning:

- LDAP certificates
- Provisioning application server certificates

LDAP certificates

LDAP certificate is the certificate from an external directory server to be used in Cisco Prime Collaboration Provisioning for secured communication. This certificate is imported into the Provisioning key store located in

`/opt/cupm/sep/dfc.keystore`

Provisioning application server certificates

Provisioning application server certificates provides an identity of the Cisco Prime Collaboration Provisioning server. The types are:

- Self-Signed—The identity certificate of the Cisco Prime Collaboration Provisioning server.
- CA-Signed—To obtain a CA–signed certificate, you must:
  1. Create a Certificate Signing Request (CSR)—A CSR is a block of encrypted text that is generated on the Cisco Prime Collaboration Provisioning server. It contains information such as your organization name, common name (domain name), locality, and country.
  2. Submit it to a Certificate Authority.
  3. Obtain the signed certificate
  4. Import the CA certificates from **Administration > Updates**.

Managing SSL Certificate

For Cisco Prime Collaboration Release 11.1 and later

Cisco Prime Collaboration Provisioning enables the administrator to generate and download SSL (Secure Socket Layer) certificates. Using these certificates you can eliminate browser security warnings and secure your internet communication.

To view the existing SSL certificates, navigate to **Administrator > Updates**. In the **SSL Certificate** pane, you can view the list of existing certificates along with its type, expiry date, and usage (LDAP or Provisioning Web Access) details. The expiry date is displayed only for signed certificates.

In addition, you can perform the following operations in the **SSL Certificate** pane:

Note You must have the administrator privilege to perform these tasks.

- Generate CSR(Certificate Signing Request)—For steps to generate a CSR, refer Generate CSR, on page 13. You can have only one CSR in the system. So, when you generate a CSR, it overwrites the old CSR.
- Upload certificate—You must get the generated CSR signed from the CA (Certificate Authority) and upload the signed certificate. You can also upload LDAP certificate. For steps to upload the SSL certificate, refer Upload SSL Certificate, on page 16.
- View certificate—To view the certificate contents, click the required certificate name and click **View**.
- Download—To download the certificate, click the required certificate name and click **Download CSR**.
- Delete—To delete a certificate, click the required certificate name and click **Delete**. You can delete only LDAP certificate.

Generate CSR

To generate a CSR :

Before you begin

You must have administrator privilege to perform this task.

Note The CSR generated from the Cisco Prime Collaboration Provisioning user interface does not include alternate names. To generate a CSR with alternate names using CLI, refer to Generate CSR with Alternate Names, on page 14.

Procedure

Step 1 Choose **Administration** > **Updates**.

Step 2 In the SSL certificate pane, click **Generate CSR**.

Step 3 Enter the required details in the **Generate Certificate Signing Request** window. An asterisk next to a field indicates a mandatory field. Refer Table 1: Generate CSR Fields, on page 14 for field description.

Step 4 Click **Generate** to generate the CSR. The generated CSR is added to the top of the table.

Note Generated CSR overwrites any existing CSR.

- The default value for Key Length is 2048 bits.
- The default value for Hash Algorithm is SHA256.

Table 1: Generate CSR Fields

Field	Description
Certificate Name	Name of the certificate.
Country Name	Two-letter ISO abbreviation of your country.
State or Province	State or Province where the organization is located.
Locality Name	City where the organization is located.
Organization Name	Name of the organization.
Organization Unit Name	Section of the organization.
Common Name	Fully qualified domain name.
Email Address(Optional)	Email address to contact the organization.

Generate CSR with Alternate Names

Perform the following steps to create a Certificate Signing Request (CSR) with alternate names. The CSR with alternate names allows you to access Cisco Prime Collaboration Provisioning with multiple Domain Name Server (DNS) entries using the same certificate.

Before you begin

Obtain the following:

- Certified Authority (CA) signed Cisco Prime Collaboration Provisioning certificate.
- Root access to the Cisco Prime Collaboration Provisioning CLI.

Note For Cisco Prime Collaboration Provisioning 12.x and above:

- Contact TAC for CLI access.
- Prefix all the commands that are executed as a console account user with **Sudo**.

Procedure

Step 1 Log in to PCP as the root user.

Step 2 Enter the command, **cd /opt/cupm/httpd/** to navigate to the httpd folder.

Step 3 Enter the command, **vi san.cnf** to create a new blank file, **san.cnf**.

Step 4 Press the I key to edit the san.cnf file.

Step 5 Copy and paste the following text in the file:

```
[req]
default_bits         = 2048
distinguished_name   = req_distinguished_name
req_extensions       = req_ext
[req_distinguished_name]
countryName          = Country Name (2 letter code)
stateOrProvinceName  = State or Province Name (full name)
localityName         = Locality Name (eg, city)
organizationName     = Organization Name (eg, company)
commonName           = Common Name (e.g. server FQDN or YOUR name)
[req_ext]
subjectAltName       = @alt_names
[alt_names]
DNS.1 = pcptest23.cisco.ab.edu
DNS.2 = pcptest.gov.cisco.ca
```

Where:

- DNS.1 = Primary DNS
- DNS.2 = Secondary DNS

You can access the PCP using either of these DNS entries.

Step 6 Enter the commands, **esc** followed by **:wq!** to save the file.

Step 7 Restart all the services for the config file:

a. Enter the command, **/opt/cupm/bin/cpcmcontrol.sh stop** to stop the services.

b. Enter the command, **/opt/cupm/bin/cpcmcontrol.sh status** to verify that all the services have stopped.

c. Enter the command, **/opt/cupm/bin/cpcmcontrol.sh start** to restart all the services.

Step 8 Enter the command, **pwd** to verify that your current directory is **/opt/cupm/httpd/**.

Step 9 Enter the following command to generate the Private key and CSR:

openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout PCPSAN.key -config san.cnf

```
[root@ryPCP11-5 httpd]# openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout
private.key -config san.cnf
Generating a 2048 bit RSA private key
.........+++
.........+++
writing new private key to 'private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields, but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:TX
Locality Name (eg, city) []:RCDN
Organization Name (eg, company) []:CISCO
Common Name (e.g. server FQDN or YOUR name) []:doctest.cisco.com
[root@ryPCP11-5 httpd]#
```

Step 10 Enter the following command to verify if the CSR contains the correct alternate names:

openssl req -noout -text -in PCPSAN.csr | grep DNS

```
[root@ryPCP11-5 httpd]# openssl req -noout -text -in PCPSAN.csr | grep DNS
DNS:pcptest23.cisco.ab.edu,
DNS:pcptest.gov.cisco.ca [root@ryPCP11-5 httpd]#
```

Step 11 Move the .csr from the PCP server to your desktop.

Step 12 Use an FTP client to connect to PCP as the root user and navigate to the `/opt/cupm/httpd/` directory.

Step 13 Sign the CSR with your CA using a windows server or online.

Step 14 Log in to the PCP server and navigate to **Administration** > **Updates** > **SSL Certificates** to install the PCP Certificate.

Step 15 Install the required browser certificate. Clear the cache and close the browser window.

Step 16 Log in to the PCP server to verify that the security error is not displayed.

Upload SSL Certificate

You can upload either LDAP or provisioning SSL certificate.

To upload SSL certificate:

Before you begin

You must have administrator privilege to perform this task.

Procedure

Step 1 Choose **Administration > Updates** .

Step 2 In the **SSL Certificate** pane, click **Upload** and choose **LDAP** or **Provisioning Certificate**.

Step 3 In the **Upload LDAP/Provisioning Certificate** dialog box, browse through the local file system and choose the required file.

Note The valid certificate file formats are .crt and .cer for provisioning certificate and .cer for LDAP certificate.

Step 4 Click **Upload**. The uploaded certificate is added to the top of the table.

After uploading the certificate, you must restart the server to activate the certificate.

Based on the type of the uploaded certificate, restart the server as follows:

- LDAP certificate—restart provisioning server.
- Provisioning certificate:
  - restart apache server.
  - from Troubleshooting UI "Restart all processes" must be done to apply the certificate for Troubleshooting UI.

Note To upload TLS 1.2 certificates, follow the same steps as above.

Cisco Prime Collaboration Provisioning does not support chained certificates.

Note A certificate chain is a sequence of certificates, where each certificate in the chain is signed by the subsequent certificate. The purpose of a certificate chain is to establish a chain of trust from a peer certificate to a trusted CA certificate.

Managing Endpoints

Using Cisco Prime Collaboration Provisioning , you can upload new and existing endpoints through the user interface. You can add or update endpoints by uploading the endpoint files (valid zip file containing list of supported endpoints). The endpoint bundle eliminates the need to login as root into the system and restart services. The details about endpoints are automatically updated in the table based on the endpoints added to Cisco Prime Collaboration Provisioning. The Endpoint Bundles pane displays a table with the list of endpoints that are available in the system and its supported Cisco Unified Communications Manager versions. To manage endpoints:

Note The endpoint zip files are available on Cisco.com.

Before you begin

You must have Administrator privileges to perform this task.

Procedure

Step 1 Choose **Administration** > **Updates**. The **Endpoint Bundles** pane displays a table with the list of endpoints that are available in the system and its supported Cisco Unified CM versions.

Unified Communications Manager versions are automatically updated in the table based on the endpoints added to Provisioning.

Step 2 Click **Add** and in the **Add Endpoint Bundles** dialog box, browse for the appropriate zip file and click **Upload**.

A warning message appears with the details of number of endpoints that are to be added to the endpoint bundle table.

Step 3 To proceed with the process, click **Continue**. The new/updated endpoints are included to the system and the user can be provisioned with the new endpoints immediately without a restart.

Note When you update the existing endpoints, a warning message is displayed stating how many endpoints and what endpoints are going to be updated.

Enabling Data Purging for Provisioning

You can configure Cisco Prime Collaboration Provisioning to purge data at a scheduled interval.

Cisco Prime Collaboration Provisioning retains the following types of data:

- Order—When an order is placed for any product provisioning (for example: endpoint, line, voicemail or any bundle), an order data object is created and stored in the system.
- ServiceAction—Objects that are created when the application is communicating with the device during product provisioning. By default, purging of Service Action data is enabled.
- Task—Scheduling of infrastructure configuration updates. Through Infrastructure Configuration you can save configurations locally. The saved configurations can then be bundled in a Task and pushed to the device.
- Workflow—After an order is placed for a product, it goes through a workflow (approval, shipping, and receiving) before going to the service activator.
- Audit Trail—An audit entry is created for every PIN or Password change, PIN or Password reset, PIN or Password change on next login, unlock voice mail of a user in a Unity or Unity Connection device, login management, user management, pin or password management, changes in access control group and user roles, self-care, system settings, and synchronization. By default, purging of Audit Trail data is enabled.

Note Data is purged when the retention time or retention count criterion is met. For example, if the data is older than the retention time it will be removed. Also, if the data amount exceeds the retention count, it will be removed.

Procedure

Step 1 Choose **Administration > Data Maintenance** . (See Table 1 for navigation in the Cisco Prime Collaboration Provisioning application.)

Step 2 Check the check box in the row for the data you want to schedule for purging.

Step 3 In the **Retention Time in Days** column, change the number of days for which you want to retain the data (default is seven days except for Audit Trail and ServiceAction, which is 30 days).

Step 4 In the **Retention Count** column, select the amount of data that you want to retain.

Note Retention count is the number of objects that you want Provisioning to keep and not purge. For example, if there are 1000 total orders and the retention count is 200, Provisioning will purge 800 orders and keep the last 200 orders.

The default settings for the Retention Count are:

- Orders—latest 100 orders
- ServiceAction—Unlimited
- Task—50
- Workflow—50
- **(For Cisco Prime Collaboration Release 11.2 and earlier)** Audit Trail—50
- **(For Cisco Prime Collaboration Release 11.5 and later)** Audit Trail—100,000

  Note 1000K is the maximum retention count that can be set for the audit trail.

Step 5 (Optional) To export the purged data to a file before it is removed, in the Export Before Purge field select **Yes**. .

Only Orders and Workflow data is exported. Service action data cannot be exported.

Step 6 Select a purge interval (the default is 24 hours), and click **Update.**

The Purging Information pane displays the time of the next scheduled purge and the last purge.

To purge Provisioning data, choose **Administration > Data Maintenance** (In the Cisco Prime Collaboration Provisioning application, choose **Administration > Data Maintenance**). You can provide the data in the Data Maintenance Configuration page.

Note During 12.1 migration, the purged data is not copied to the 12.1 server automatically. If 11.x server purged data is required, then these files must be copied manually.

Maintenance Mode

You can put Cisco Prime Collaboration Provisioning into maintenance mode to perform user-impacting actions that are not available in normal mode, such as deleting Domains, processors, and Service Areas.

Any user other than administrator will be able to access all non Provisioning pages as per the roles assigned to him. Though Provisioning links are available, when user tries to access these pages, a message appears indicating that the application is currently in Maintenance mode.

Note The user needs to log off from the application mode, and re-login to the maintenance mode, for the maintenance mode rules to be applicable.

Procedure

Step 1 Choose **Administration** > **Maintenance Mode** .

The Application Mode Management page appears with the following message:

Exiting Maintenance mode will restore access to all users. Delete operations on processors (Call Processors, Unified Message Processors), LDAP and ACS Servers, Domains, and Service Areas will no longer be available.

Step 2 Select a time delay from the **Delay Before Maintenance Mode Begins (mins)** drop-down list. You can select a time delay between 1 minute to 60 minutes. To put Cisco Prime Collaboration Provisioning to maintenance mode immediately, select **Immediately.**

Step 3 In **Message to Display to Logged-in Users**, enter a message. This message will appear on the screens of the logged-in users. You can enter a maximum of 200 characters.

Step 4 Click **Enter Maintenance Mode**, and then click **Yes** to confirm.

A warning appears on the login page, notifying users that the system use is limited to users with administrative privileges. Maintenance options that are not available in normal mode, such as deleting Domains, become available.

Step 5 Perform any maintenance activities, such as deleting a Domain.

Step 6 When you have completed the maintenance activities, select **Maintenance Mode**.

Step 7 Click **Exit Maintenance Mode**.

The warning on the login page is removed and users can now log in as usual. Maintenance options such as deleting Domains are no longer available.

An email notification will be sent to all the administrators when Cisco Prime Collaboration Provisioning is going into maintenance mode. The following notification event must be enabled to send an email notification:

When system enters or exits Maintenance Mode (email will be sent to the logged in administrators)

To configure notification settings, see Configuring System Notifications

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 21).

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 21.

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.

Schedule Backup Using the Provisioning User Interface

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

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.

Before performing the upgrade, ensure to take a snapshot of the existing setup.

Procedure

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:

a. Create a console account from the troubleshooting web application.

b. Log in to console and delete the content of the /opt/backup folder and then the backup folder.

c. 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.

Back Up Provisioning Database from Console CLI — 11.x and below

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

Procedure

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
```