Troubleshooting

Changing the SSL Port

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

Procedure

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:

Procedure

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.

Note After attaching the Provisioning server to Assurance, the Assurance time zone settings are displayed in the converged server. However, the Provisioning dashboards will display Provisioning time zone only.

In the Provisioning standalone server, you can also change the time zone by selecting the Time Zone icon from the top right corner of the Provisioning home page. In the Time Zone Settings (UTC Offset) page, enter the New UTC offset and Location details and click Apply.

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.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.

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 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 standalone
ps -aef | grep nice
kill -9 <standalone 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/standalone/configuration/standalone-full.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 4.

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.

Procedure

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.

Procedure

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:

Procedure

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.

Procedure

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.

How to verify the Cisco Prime Collaboration Provisioning Installation (for advanced/standard mode)?

After you install Prime Collaboration Provisioning, verify if it has been properly installed.

1. In a browser, specify the IP address of the server on which Prime Collaboration Provisioning (standard/advanced) has been installed.

The login page is displayed. Login with globaladmin credentials.

2. Log in to the Provisioning server using the SSH service and with the CLI admin that you created during OVA configuration. By default, this username is admin.

3. Enter the following command to display the processes that are running:

```
show application status cpcm
bash: no job control in this shell
httpd denotes httpd service.
nice.sh denotes Nice service.
startcupm.sh denotes Jboss service.
postmaster/su denotes Postgres service.
STAT PID USER COMMAND ELAPSED
===============================================
Ss 629 root httpd 02:11:38
S 613 root nice.sh 02:11:38
S 610 root startcupm.sh 02:11:38
S 608 root su 02:11:38
```

The parameters in the COMMAND column are the processes that are running on the Prime Collaboration Provisioning server (standard/advanced). If you do not see the processes running, enter the following commands to restart the Prime Collaboration Provisioning services:

```
admin#application stop cpcm
         admin#application start cpcm
```

The above commands take one or two minutes to stop or start the Prime Collaboration Provisioning services.

You can verify if the installation is complete and successful, by checking if the JBoss service is running.

In the SSH terminal, run the following command as a root user to know if the JBoss service is running :

```
ps - aef|grep startcupm
```

You can also check at what time the JBoss service was started, in the following location (in the last line of the log file) :

```
/opt/cupm/sep/logs/jboss.log
```

If the JBoss service is running, see the **Getting Started** chapter, of the Cisco Prime Collaboration Provisioning Guide - Standard and Advanced to get started with the Prime Collaboration Provisioning application.

How to upgrade Cisco Prime Collaboration Provisioning from small to medium deployment model?

After you manually upgrade the system requirements (vRAM, vCPU, vDISK and such), you must run the following scripts as a root user:

1. Execute the memorymodel.sh file under /opt/cupm:

```
./memorymodel.sh medium "-Xms512m -Xmx1024m -XX:MaxPermSize=256m -server" "-Xms512m
-Xmx1024m -XX:MaxPermSize=256m" simple all
```

2. Execute cpcmdiskutil.sh under /opt/cupm:

```
. /cpcmdiskutil.sh /dev/sda
```

3. Restart the server(vmware instance)

How to upgrade Cisco Prime Collaboration Provisioning server from small/medium to large deployment model?

1. Backup the database from the Prime Collaboration Provisioning application by following the procedures provided in Cisco Prime Collaboration Provisioning Guide.
2. Deploy large OVA as a database server (say, “server1”) by following the procedure provided in the Cisco Prime Collaboration Provisioning Install and Upgrade Guide. During the deployment, ensure that the globaladmin password is same as the password provided during deployment.
3. Deploy large OVA as an application server (say, “server2”) by following the procedure provided in the Cisco Prime Collaboration Provisioning Install and Upgrade Guide. During the deployment, ensure that the globaladmin password is same as the password provided during deployment.
   - **a.** Copy the licenses from the old server to the new server2.
   - **b.** If you make use of the MAC address of the existing Prime Collaboration Provisioning server, then you must update the MAC address using the VMware client for this VMWare instance.
   - **c.** If you make use of a new MAC address for server2, then the licenses in the /opt/cupm/license directory must be rehosted to match the new server2 VM.
4. Stop provisioning services in the application server (“server2”).
   - **a.** `Go to /opt/cupm folder.`

     Execute `./cupm-app-service.sh stop`
   - **b.** Ensure that Apache, JBoss and NICE Services are stopped using the following commands:

     ```
     ps -aef | grep startcupm
      ps -aef | grep nice
     ```
   - **c.** If there are any process running, use the following commands to stop their execution:

     ```
     kill -9 <startcupm process id>
          kill -9 <nice process id>
     ```
   - **d.** To check whether the nice process is still holding on the postgres connection, enter the following command: `ps -aef`

     Look for the process:

     ```
     /opt/cupm/jvm/bin/java -server -classpath /opt/cupm/sep/lib/dom.jar:
     ```

     If the process is running, enter the following command:

     ```
     kill -9 <Process-Id found earlier>.
     ```
   - **e.** Wait for a minute to make the resources, such as ports, to become free.
5. Restore database in the database server (“server1”) using the backed up database file taken from step 1. For details, see the section “Restoring Database in the database server” in the Cisco Prime Collaboration Provisioning Guide - Standard and Advanced.

6. Stop and then start the provisioning services in database server (“server1”).
   a. cd /opt/cupm folder.

      ```
      ./cupm-db-service.sh stop.
      ```

   b. Wait for 30 seconds before starting the db services.
   c. To start the db services:

      ```
      cd /opt/cupm
      ./cupm-db-service.sh start.
      ```

7. Copy the following files from the original Prime Collaboration Provisioning server to the newly deployed application server (“server2”)
   a. `/opt/cupm/sep/dfc.properties`
   b. `/opt/cupm/sep/dfc.keystore`
   c. `/opt/cupm/jboss/server/cupm/conf/login-config.xml`
8. Change directory to /opt/cupm/sep and edit the dfc.properties file using the “vi” editor
   a. `cd /opt/cupm/sep`
   b. `vi dfc.properties`
   c. Change the property dfc.memory.model=medium to dfc.memory.model=large
   d. Change the property dfc.postgres.host=localhost to dfc.postgres.host=<IP of server Database>
   e. Save changes and exit the editor
9. Start application services in the application server (“server2”).
   a. Change directory to /opt/cupm folder to start the application services
   b.
      ```
      cd /opt/cupm.
      ./cupm-app-service.sh start.
      ```

The system is now ready to be used.

How to downgrade Cisco Prime Collaboration deployment model?

Prime Collaboration does not support downgrade of deployment model; that is you cannot downgrade from Prime Collaboration Large deployment to Small.

How to configure a second NIC for Prime Collaboration?

A second NIC can be added to the Prime Collaboration as follows:

- Use vSphere Client (**Edit virtual machine settings** option) to add a second virtual Network Adapter to the virtual machine.
- Login to the Prime Collaboration admin CLI to configure the IP address for the second interface.
- Configure the ip route gateways for the two interfaces (with the same CLI access).

Login as admin user and execute the following CLI commands:

```
admin# configure
admin (config)# interface GigabitEthernet 1 (Note that the first interface is Giga-bitEthernet
 0)
admin (config-GigabitEthernet)# ip address <ip address> <net mask>
admin (config-GigabitEthernet)# exit
```

To configure the ip routes to the two different gateways:

```
admin (config)# ip route <network addr> <net mask> <route-specific gateway1>
admin (config)# ip route <network addr> <net mask> <route-specific gateway2>
```

Change the default route (0.0.0.0 0.0.0.0) to the appropriate gateway if needed.

How to change the IP Address on the Provisioning server (for a Distributed Setup)?

The following procedure is applicable for Cisco Prime Collaboration Provisioning 10.0 and 10.5. For Provisioning 9.0 and 9.5, see the Setting Up the Server chapter in *Cisco Prime Collaboration Provisioning Guide*.

1. Stop the application services using the following command:

   ```
   execute ./cupm-full-service.sh stop
   ```

2. Login to the database server as admin through SSH and execute the following commands:

   ```
   admin# conf t
            admin(config)# interface GigabitEthernet 0
            admin(config-GigabitEthernet)# ip address <ipaddress> <subnet mask>
   ```

3. Specify "y" when the following message is displayed: Changing the IP may result in undesired side effects on any installed application(s). Are you sure you want to proceed? [y/n] y.

4. Login to the database server as admin with the new IP address and execute the following configuration commands:

   ```
   admin(config)# ip default-gateway <a.b.c.d>
            admin(config)# ip domain-name <new_domain>
            admin(config)# ip name-server <a.b.c.d>
            admin(config)# hostname <new_name>
            admin(config)# exit
            admin# write memory
   ```

5. Login to the database server as root with the new IP address.

6. Update the Nice system record in postgres:

   - Login to postgres
   - `cd /opt/postgres/9.0/bin`

- `./psql -Upmadmin -d cupm`
- `Select * from nicesyseng;`
- Check if there are any entries that contain your old IP address (in the "host" column). If there are any entries, delete them by executing the following query: delete from nicesyseng where host='<old_ip_address>';

7. In the /opt/postgres/9.0/data/pg_hba.conf file, replace the line: host all all <ip>/32 trust with host all all <changed app-server ip>/32 trust.

8. Login to the application server as admin through SSH and execute the following commands:

```
admin# conf t
         admin(config)# interface GigabitEthernet 0
         admin(config-GigabitEthernet)# ip address <ipaddress> <subnet mask>
```

9. Specify "y" when the following message is displayed: Changing the IP may result in undesired side effects on any installed application(s). Are you sure you want to proceed? [y/n] y.

10. Login to the application server as admin with the new IP address and execute the following configuration commands:

```
admin(config)# ip default-gateway <a.b.c.d>
         admin(config)# ip domain-name <new_domain>
         admin(config)# ip name-server <a.b.c.d>
         admin(config)# hostname <new_name>
         admin(config)# exit
         admin# write memory
```

11. Login to the application server as root with the new IP address.

12. Update the following line in the /opt/cupm/sep/dfc.properties file:

```
dfc.postgres.host=<database-server-new-ip-address>
```

13. Update the following line in the /opt/cupm/jboss/server/cupm/deploy/dfc-ds.xml:

```
<connection-url>jdbc:postgresql://<database-server-new-ip-address>:5432/cupm</connection-url>
```

14. Reboot the database server. After this is completed, reboot the application server.

How to change the IP Address on the Provisioning Server (Single Setup)?

The following procedure is applicable for Cisco Prime Collaboration Provisioning 10.0 and 10.5. For Provisioning 9.0 and 9.5, see the Setting Up the Server chapter in *Cisco Prime Collaboration Provisioning Guide*.

1. Log in to the server as admin through SSH and execute the following commands:

```
admin# conf t
         admin(config)# interface GigabitEthernet 0
         admin(config-GigabitEthernet)# ip address <ipaddress> <subnet mask>
```

2. Specify "y" when the following message is displayed: Changing the IP may result in undesired side effects on any installed application(s). Are you sure you want to proceed? [y/n] y.

3. Login as admin with the new IP address and execute the following configuration commands:

```
admin(config)# ip default-gateway <a.b.c.d>
         admin(config)# ip domain-name <new_domain>
         admin(config)# ip name-server <a.b.c.d>
         admin(config)# hostname <new_name>
         admin(config)# exit
         admin# write memory
```

4. Login as root with the new IP address.

5. Update the Nice system record in postgres:

    - Login to postgres
    - `cd /opt/postgres/9.0/bin`
    - `./psql -Upmadmin -d cupm`
    - `Select * from nicesyseng;`
    - In the console output, check if there are any entries that contain your old IP address (in the "host" column). If there are any entries, delete them by executing the following query: delete from nicesyseng where host='<old_ip_address>';

6. Reboot the server.

How to find the MAC address of Prime Collaboration Provisioning Servers?

To find the MAC address of Prime Collaboration Provisioning 10.0,

1. Click the About icon at the top right corner of the user interface.
2. In the About page, click the Provisioning information link to launch the system information details for both Prime Collaboration Provisioning.

For all the other versions of Prime Collaboration, you can check the MAC address through the vSphere client. You can also log in as root to the Prime Collaboration Provisioning server and run the command **ifconfig**.

How to configure Prime Collaboration Provisioning to synchronize a subset of subscribers from Cisco Unified Communications Manager?

The option to synchronize a subset of subscribers from Cisco Unified Communications Manager is disabled by default. To enable this feature, add the properties mentioned below in $CUPM\sep\ipt.properties file.

- `dfc.ipt.sync.users.filter.attribute.name: department`
- `dfc.ipt.sync.users.filter.attribute.value: *`

Names and Values to be set in ipt.properties file

1. Specify the following parameters for the property dfc.ipt.sync.users.filter.attribute.name:
    a. department
    b. userid
    c. firstname
    d. lastname
2. Specify the following values for the property dfc.ipt.sync.users.filter.attribute.value
    a. (this will sync only those users that have the above specified property (ex: department) value as not empty)
    b. test* (this will sync those users that have the above specified property (ex: department) value that starts with 'test')
    c. *test* (this will sync those users that have the above specified property (ex: department) value that contains 'test')

How to set Throttling Values for Cisco Unified Communications Managers?

The throttling values set in Provisioning must be equal to or less than the values set in Cisco Unified Communications Manager. If you change the throttling settings in Cisco Unified Communications Manager, you must also change the same settings in Provisioning.

The throttling settings in Provisioning are set in the ipt.properties file (located at /opt/cupm/sep folder).

Note The default location for the installation directory is /opt/cupm.

The following properties (in the ipt.properties file) are used to control the write request sent to Cisco Unified Communications Manager:

- `dfc.ipt.axl.soap.MaxAXLWritesPerMinute: 20`

  This property specifies the default number of write requests per minute. Its value is used if there is no version or device specific value specified.

- `dfc.ipt.axl.soap.MaxAXLWritesPerMinute.ccm501: 50`

  This property specifies the number of write requests per minute for Cisco Unified Communications Manager version 5.0(1). Its value is used if there is no device specific value specified.

- `dfc.ipt.axl.soap.MaxAXLWritesPerMinute.<IP address>: 20`

  This property specifies the number of write requests per minute for a specific Cisco Unified Communications Manager indicated by the IP address.

For example, dfc.ipt.axl.soap.MaxAXLWritesPerMinute.1.2.3.4: 20 sets the value to 20 for Cisco Unified Communications Manager with the IP address of 1.2.3.4.

While performing the troubleshooting workflow between endpoints, I am seeing these issues:

- Troubleshooting status shows Errored and log tab shows Pathtrace Discovery could not be completed because of an internal error.
- Some network nodes are missing in the path topology.

If you are seeing any one of the above issues, you can check whether:

- "utils network mtr" runs successfully between the source endpoint and destination device; where the source endpoint is a Cisco TelePresence System (CTS 500, 1000 and or 3000).
- "systemtools network traceroute" runs successfully between the source endpoint and destination device; where the source endpoint is a Cisco C and/or EX series system.

  Traceroute runs successfully between the first hop router or layer 3 switch and destination device. The first hop router or layer 3 switch is connected to either a Cisco Video Phone (89xx/99xx) Cisco Cius, Cisco Jabber video, Polycom, and/or E20.

  In addition, you must ensure that traceroute command from Prime Collaboration server to the source device works successfully where the source device is Cisco Jabber Video, Polycom, E20.
- "systemtools network traceroute" runs successfully between the source endpoint and destination device; where the source endpoint is a Cisco MXP.

The first hop router or layer 3 switch must have the CLI Access Level RW (Prime Collaboration server > Operate > Device Work Center > Current Inventory table).

The troubleshooting shows no CLI Access and does not allow troubleshooting

Check whether the source device has CLI Access Level as RW (Prime Collaboration server > Operate > Device Work Center > Current Inventory table).

Why the mediatrace or IP SLA statistics is not displayed in the troubleshooting result page?

In the troubleshooting workflow, if both the endpoints do not support five-tuple configuration, the mediatrace statistics is not displayed. In the troubleshooting workflow, if one of the endpoints support five-tuple, the mediatrace statistics is displayed.

The E20, MXP, Cisco Jabber Video, and Polycom devices does not support five-tuple configuration.

For running IPSLA VO diagnostics, you must ensure that traceroute command from source switch or router to destination switch or router runs successfully.

How to remove the SSL certificate warning?

- Windows Internet Explorer—You can permanently remove the SSL certificate warning by installing the Prime Collaboration self-signed certificate.
- Mozilla Firefox—You can remove the SSL certificate warning only by adding an exception.

In Windows Internet Explorer, to remove the SSL certificate warning:

1. Choose **Continue to this website (not recommended)**.
2. Choose **Tools** > **Internet Options**.
3. In the **Internet Options** dialog box, click the **Security** tab, choose **Trusted sites**, and then click **Sites**.
4. Confirm that the URL that appears in the field and matches the application URL, and then click **Add**.
5. Close all dialog boxes and refresh the browser.
6. Choose **Certificate Error** to the right of the address bar, and then click **View certificates**.
7. In the **Certificate** dialog box, click **Install Certificate**.
8. In the **Certificate Import Wizard** dialog box, click Next.
9. Click the **Place all certificates in the following store** radio button, and then click **Browse**.
10. In the **Select Certificate Store** dialog box, choose **Trusted Root Certification Authorities**, and then click **OK**.
11. Click **Next** > **Finish**.
12. In the **Security Warning** message box, click **Yes**.
13. In the **Certificate Import Wizard** message box, click **OK**.
14. In the **Certificate** dialog box, click **OK**.
15. Repeat Step 2 and Step 3.
16. Select the URL in the **Websites** section, and then click **Remove**.
17. Close all dialog boxes, restart the browser, and invoke Prime Collaboration. See the "Getting Started" chapter of Cisco Prime Collaboration Provisioning Guide - Standard and Advanced for information about invoking Prime

    Collaboration.

If you have a safe URL implemented, do the following:

1. Choose **Tools** > **Internet Options**.
2. In the **Internet Options** dialog box, click the **Advanced** tab.
3. In the **Security** section, uncheck the **Warn about certificate address mismatch** check box.

In Mozilla Firefox, to remove the SSL certificate warning:

1. Click **I Understand the Risks** >**Add Exception**.
2. In the the **Add Security Exception** dialog box, click **Confirm Security Exception**.

UC Performance Monitor goes blank due to customized layout settings change

1. Launch Home -> UC Performance Monitor
2. Select some clusters and view the dashboards.
3. Now change the Dashlet layout or do any such customization.
4. Again, launch the UC performance monitor. It shows blank page.

   Workaround: Reset the customized settings and the launch the UC Performance Monitor.