Contents

Installation and Upgrade

How to verify the Cisco Prime Collaboration Assurance installation (for advanced and standard modes)?

If you are unable to launch Prime Collaboration Assurance, it could be because the required processes are not running on the Prime Collaboration Assurance server.

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

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

show application status cpcm

The following is sample output of the status command, for **Prime Collaboration Assurance- Advanced** 9.x or 10.0 server:

```
STAT PID USER COMMAND ELAPSED
==============================================
S<l 4337 root Decap_main 03:54:04
SNl 15925 root emsam_cdc 03:46:05
SNl 8571 root emsam_fault 03:50:27
SNl 4576 root emsam_inventory 03:53:17
SNl 4458 root emsam_mq 03:53:56
SNl 7666 root emsam_poller 03:50:47
SNl 10000 root emsam_sessionmo 03:49:57
SNl 6050 root emsam_tomcat 03:51:27
SNl 10012 root emsam_troublesh 03:49:57
SN 4438 postgres postgres 03:53:59
Process State Pid
*******    *****   ***
ESS Program started - No mgt msgs received 7505
VHMIntegrator Program started - No mgt msgs received 7534
EssMonitor Running normally 7535
InventoryCollector Program started - No mgt msgs received 7816
GpfPurgeTask Administrator has shut down this server 0
SSHD Program started - No mgt msgs received 7818
QOVRMonitor Program started - No mgt msgs received 7819
QOVRMultiProcLogger Program started - No mgt msgs received 7820
IPSLAPurgeTask Administrator has shut down this server 0
FHPurgeTask Administrator has shut down this server 0
SEGPurgeTask Administrator has shut down this server 0
IPCDiscovery Administrator has shut down this server 0
SDRPurgeTask Administrator has shut down this server 0
IVR Program started - No mgt msgs received 7834
DiagPurgeTask Administrator has shut down this server 0
IPIUDbEngine Program started - No mgt msgs received 7873
IPIUDbMonitor Running normally 8105
FHDbEngine Program started - No mgt msgs received 8106
FHDbMonitor Running normally 8240
INVDbEngine Program started - No mgt msgs received 8241
ITMDiagServer Program started - No mgt msgs received 8361
INVDbMonitor Running normally 8362
EPMDbEngine Program started - No mgt msgs received 8363
EPMDbMonitor Running normally 8514
SIRServer Program started - No mgt msgs received 8515
ITMLogServer Program started - No mgt msgs received 8658
ITMCTMStartup Administrator has shut down this server 0
DfmBroker Running normally 8660
DfmServer Running normally 8843
CSDiscovery Never started 0
DCRDevicePoll Never started 0
CSRegistryServer Running normally 8844
TomcatMonitor Running normally 8845
```

LicenseServer Program started - No mgt msgs received 8846
FDRewinder Never started 0
NameServer Program started - No mgt msgs received 8847
NameServiceMonitor Program started - No mgt msgs received 9108
EDS Running normally 9234
CmfDbEngine Program started - No mgt msgs received 9474
CmfDbMonitor Running normally 9649
EDS-GCF Running normally 9678
DCRServer Running normally 9679
CMFOGSServer Program started - No mgt msgs received 9883
TISServer Program started - No mgt msgs received 9884
EPMServer Running normally 10181
STServer Program started - No mgt msgs received 10303
AdapterServer Program started - No mgt msgs received 10304
VHMServer Program started - No mgt msgs received 10393
PIFServer Program started - No mgt msgs received 10394
IPIUDataServer Running normally 10639
SRSTServer Running normally 10640
FHServer Program started - No mgt msgs received 10641
QoVMServer Program started - No mgt msgs received 10642
QOVR Running normally 10935
IPSLAServer Program started - No mgt msgs received 10936
SEGServer Running normally 10937
ITMOGSServer Program started - No mgt msgs received 10938
NOTSServer Running normally 11087
PTMServer Running normally 11088
GPF Running normally 11198
TopoServer Program started - No mgt msgs received 11200
SMDBMonitor Program started - No mgt msgs received 11201
jrm Program started - No mgt msgs received 11202
DataPurge Administrator has shut down this server 0
diskWatcher Running normally 11349

The following is sample output of the status command, for **Prime Collaboration Assurance- Advanced** 10.5 server:

STAT PID USER COMMAND ELAPSED
==========
S<l 20235 root Decap_main 5-14:32:56
SN 20357 postgres postgres 5-14:32:55
SN 20458 primea postmaster 5-14:32:53
SN1 20490 root emsam_mq 5-14:32:51
SN1 20559 root cpc_multiproclo 5-14:32:43
SN1 20596 root emsam_inventory 5-14:32:43
SN1 21400 root emsam_perfmonen 5-14:31:18
S<l 21471 root emsam_tomcat 5-14:31:08
SN1 21560 root emsam_poller 5-14:31:04
SN1 21670 root emsam_fault 5-14:30:44
SN1 22271 root emsam_sessionmo 5-14:29:54
SN1 22310 root emsam_troublesh 5-14:29:54
SN1 22524 root cpc_datapurge 5-14:29:49
SN1 22626 root cpc_segserver 5-14:29:43
SN1 22752 root cpc_sirserver 5-14:29:39
SN1 22934 root cpc_qovmserver 5-14:29:28

How to verify the Cisco Prime Collaboration Assurance installation (for advanced and standardmodes)?

SN1 23415 root cpc_pifserver 5-14:29:13
SN1 23868 root cpc_ipiudataser 5-14:29:03
SN1 23953 root cpc_srstserver 5-14:29:00
SN1 24078 root cpc_stserver 5-14:28:55
SN1 25324 root cpc_gpf 5-14:26:26
SN1 25482 root cpc_sshd 5-14:26:21
SN1 25520 root cpc_qovr 5-14:26:19
SN1 25698 root cpc_smdbmonitor 5-14:26:17
SN1 25748 root cpc_notsserver 5-14:26:15
SN1 25816 root cpc_ipslaserver 5-14:26:13
SN1 26015 root cpc_toposerver 5-14:26:08

The following is the output of status command for **Prime Collaboration Assurance- Standard** 9.x or 10.0 server:
STAT PID USER COMMAND ELAPSED
==========
S<l 4271 root Decap_main 1-23:28:00
SNl 7622 root emsam_fault 1-23:24:15
SNl 4499 root emsam_inventory 1-23:27:14
SNl 4400 root emsam_mq 1-23:27:53
SNl 6687 root emsam_poller 1-23:24:35
SNl 9444 root emsam_sessionmo 1-23:23:44
SNl 5350 root emsam_tomcat 1-23:25:17
SNl 9532 root emsam_troublesh 1-23:23:43
SN 4363 postgres postgres 1-23:27:55

The following is the output of status command for **Prime Collaboration Assurance- Standard** 10.5 server:
STAT PID USER COMMAND ELAPSED
==========
S<l 4327 root Decap_main 3-23:24:50
SN 4422 postgres postgres 3-23:24:45
SN 4513 primea postmaster 3-23:24:42
SN1 4541 root emsam_mq 3-23:24:40
SN1 4603 root cpc_multiproclo 3-23:24:32
SN1 4635 root emsam_inventory 3-23:24:31
SN1 5434 root emsam_perfmonen 3-23:22:45
S<l 5521 root emsam_tomcat 3-23:22:35
SN1 5679 root emsam_poller 3-23:22:29
SN1 5791 root emsam_fault 3-23:22:09
S1 13090 root emsam_sessionmo 3-22:55:16
S1 13215 root emsam_troublesh 3-22:55:15
S1 15885 root cpc_datapurge 3-22:44:36
S1 15958 root cpc_segserver 3-22:44:28
S1 16272 root cpc_sirserver 3-22:44:20
S1 16331 root cpc_toposerver 3-22:44:15
S1 16475 root cpc_qovmserver 3-22:44:02
S1 16754 root cpc_pifserver 3-22:43:44
S1 16798 root cpc_ipiudataser 3-22:43:39
S1 17137 root cpc_srstserver 3-22:43:23
S1 17204 root cpc_stserver 3-22:43:15
S1 17276 root cpc_gpf 3-22:43:07
S1 17478 root cpc_sshd 3-22:42:59

How to verify the Cisco Prime Collaboration Assurance installation (for advanced and standardmodes)?

S1 17551 root cpc_qovr 3-22:42:51
S1 17649 root cpc_smdbmonitor 3-22:42:43
S1 17783 root cpc_notsserver 3-22:42:35
S1 17872 root cpc_ipslaserver 3-22:42:27

The parameters in the COMMAND column are the processes that are running on the Prime Collaboration Assurance server (standard/advanced). If you do not see all of these processes running, enter the following commands to restart the Prime Collaboration Assurance services:
<hostname>/admin#application stop cpcm
<hostname>/admin#application start cpcm

```
The application start cpcm/cpcmcontrol.sh start takes 10 to15 minutes for execution and

application stop cpcm/cpcmcontrol.sh stop takes 10 minutes.
```

3. Repeat Step 2 and check whether all of the processes are running.

If all of the required processes are still not running on the Prime Collaboration Assurance server or if you are unable to access the Prime Collaboration Assurance URL, contact the Cisco support team.

If all the processes are running, see the "Getting Started" chapter, of the Cisco Prime Collaboration 9.0 Quick Start Guide to get started with the Prime Collaboration Assurance application.

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. Log in 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 9.0 Quick Start Guide to get started with the Prime Collaboration Provisioning application.

How to upgrade Cisco Prime Collaboration Assurance deployment model?

If you need to upgrade Cisco Prime Collaboration Assurance deployment model, you must first upgrade your hardware resources, such as, vRAM, vCPU, and vDisk.

You must increase the disk size by adding a new vDisk of size equal to the required additional size. (Refer to VMware documentation to upgrade/add the hardware resources)

Note:

- Do not select existing vDisk and increase its size. Add a new vDisk.
- You can upgrade Cisco Prime Collaboration 9.0, 9.5, or 10.0 Assurance server (thick provisioned format) from small to medium, large, or very large deployment model. Prime Collaboration 10.0 Analytics is not supported on very large deployment.
- If you are using Prime Collaboration 10.5 Assurance and Prime Collaboration 10.5 Analytics, you cannot use this procedure to upgrade deployment model from large to very large.
- If you are using Prime Collaboration 10.6 Assurance and/or Prime Collaboration 10.6 Analytics, you must contact Cisco TAC team to get the root access to the Prime Collaboration Assurance server. The root access enables you to run the tuning script.

You must login as root user and upgrade the Cisco Prime Collaboration Assurance deployment model to medium, large, or very large using the following tuning script.

For Prime Collaboration Assurance version 9.0, 9.5 and 10.0

```
# /opt/emms/emsam/bin/cpcmtuning.sh
```

For Prime Collaboration Assurance version 10.5

```
# /opt/emms/emsam/bin/newcpcmtuning.sh
```

For Prime Collaboration Assurance version 10.6, root access is disabled. You must contact TAC to get the patch for root access to run the tuning script.

From the options displayed, choose the deployment model (excluding option 1) that you wish to upgrade to, and then select Y to proceed with upgrading or N to reselect the deployment model.

For information on installing Prime Collaboration Assurance, Prime Collaboration Provisioning, and system requirements, see Cisco Prime Collaboration Quick Start Guide:
http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.ht

How to upgrade Cisco Prime Collaboration 10.5 Assurance and Analytics Large to Very Large deployment model?

(Applicable to version 10.5)

```
Note:
If you need to upgrade Cisco Prime Collaboration Assurance deployment model, you must first upgrad
such as, vRAM, vCPU, and vDisk.
Also, you must increase the virtual disk size by adding a new vDisk. (Refer to VMware documentatio
```

1. Make a backup of the Prime Collaboration Analytics database server (Large model). Refer to Steps 1-4 in Performing Backup and Restore in Prime Collaboration Analytics.
2. Download the Prime Collaboration Assurance and Analytics Very Large OVA file, and deploy a remote Prime Collaboration Analytics database server. To learn how to deploy, refer to Installing Prime Collaboration Assurance.You must note the IP address of this database server, to perform the later steps.
3. On the original/main server (Large model), change the VM configuration and execute the /opt/emms/emsam/bin/newcpcmtuning.sh command to upgrade the VM.
4. Execute /opt/emms/emsam/advance_reporting/bin/enableAnalyticsWithRemoteDB.sh to point the Prime Collaboration Analytics database server to the VM (Very Large OVA) deployed in Step 2.
5. Restore Prime Collaboration Analytics data (that you have backed-up in Step 1) to this Prime Collaboration Analytics database server. Refer to Step 5 in Performing Backup and Restore in Prime Collaboration Analytics.

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 Quick Start 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 Quick Start 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
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 GigabitEthernet 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 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>';

7. Reboot the server.

How to change IP Address on the Prime Collaboration Assurance Server?

1. Login to CLI as admin and execute the following command:

```
IPAddress-Change/admin# conf t
```

2. Execute the following configuration commands, one per line, and end each of them with "control Z".
    - ♦ IPAddress-Change/admin(config)# interface GigabitEthernet 0
    - ♦ IPAddress-Change/admin(config-GigabitEthernet)# ip
    - ♦ IPAddress-Change/admin(config-GigabitEthernet)# ip address 10.64.91.177 255.255.255.0
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. IPAddress-Change/admin(config-GigabitEthernet)# exit
5. IPAddress-Change/admin(config)# exit
6. IPAddress-Change/admin# wr mem

Restart VM after IP address change and execute the script EMSAM_HOME/bin/updateJmsProps.sh

NOTE: Before you change the IP address in converged mode, the Provisioning server must be detached and browser cache must be cleared. You can then launch the server.

Prime Collaboration may fail, when installed with MAC

After you deploy the Prime Collaboration Assurance OVA, and before you Power On the virtual appliance, you must edit the virtual appliance settings.

1. Right-click the virtual appliance and choose **Edit VM Settings > Options**.
2. Under Settings, choose **Advanced > General > Configuration Parameters**.
3. Click **Add**.
4. In the Key Name field, enter keyboard.typematicMinDelay and in the Value field enter 2000000.
5. Click **OK**.

Licensing

How to find the MAC address of Prime Collaboration Assurance and/or Prime Collaboration Provisioning servers?

To find the MAC address of Prime Collaboration Assurance and 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 Assurance Information or Provisioning information link to launch the system information details for both Prime Collaboration Assurance and/or 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 Assurance or Prime Collaboration Provisioning server and run the command **ifconfig**.

Provisioning

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 the 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: depart
b. test* (this will sync those users that have the above specified property (ex: departme
c. *test* (this will sync those users that have the above specified property (ex: departm
```

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.

Video Diagnostics

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 status shows No CLI Access and does not allow to troubleshoot.

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.

General

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 Prime Collaboration 9.0 Administration Guide 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**.

What happens when Prime Collaboration Assurance server and NTP server are not synchronized?

(Applicable for Prime Collaboration 9.5)

The Oracle service fails to execute after you start the Assurance server. To resolve this issue, you must synchronize the NTP server time with the Prime Collaboration Assurance server time.

Login as root user and check for this message in the /var/log/start_emsam.log file: "Oracle failed to start. Check your system time and NTP server configuration". Synchronize the NTP server time with the PC Assurance server time. Restart the Assurance server (using start application cpcm).

Some of the hostnames are not resolved in Prime Collaboration Assurance server, Why?

(Applicable for Prime Collaboration 9.5)

The /etc/hosts file changes after the restart. After the Prime Collaboration Assurance server restarts, the file from the storedconfig folder is synchronized with (copied to) the /etc/hosts file.

To avoid this issue and for the changes to occur immediately after restart, whenever you add a new entry in /etc/host, you must also add the entry in /storedconfig/startup-config-xxx/etc/hosts file, so that the entry is retained and is not deleted if the PC server is rebooted.

This issue is also applicable if the Unified CM publisher is configured using name in the CUCM section/System Server section of Prime Collaboration Administration and the name is not resolved through DNS from the Prime Collaboration Assurance server.

Sometimes Prime Collaboration Assurance UI may become Blank

In some rare cases, you may notice that Prime Collaboration UI screen may become blank. This is a known issue noticed primarily in Version 10.0

Workaround: Refresh the page.

UC Performance Monitor goes blank due to customized layout settings change

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

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