



# Troubleshooting Cisco Prime Collaboration Assurance

Published On: March 19, 2018

Modified On: August 09, 2018

## Installation and Upgrade

### How to verify the Cisco Prime Collaboration Assurance installation (for Advanced mode)?

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

Log in to the Cisco Prime Collaboration Assurance Serviceability User Interface with the Username as *glob-admin*.

The Dashboard page appears. You can view the Information on the Header, Process Status, and System Update History.

If not all of the required processes are still running on the Cisco Prime Collaboration Assurance server or if you are unable to access the Cisco 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 Cisco Prime Collaboration Assurance 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 12.1 Assurance server (thick provisioned format) from small to medium, large, or very large deployment model.

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 Cisco Prime Collaboration Assurance version 12.1

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

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 Cisco Prime Collaboration Assurance, Cisco 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.html>

## 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 upgrade your hardware resources, such as, vRAM, vCPU, and vDisk. Also, you must increase the virtual disk size by adding a new vDisk. (Refer to VMware documentation to upgrade the hardware resources.)

1. Download the Cisco Prime Collaboration Analytics Very Large OVA file, and deploy a remote Cisco 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.
2. Make a backup of the Cisco Prime Collaboration Analytics database server (Large model). Refer to Steps 1-4 in [Performing Backup and Restore in Prime Collaboration Analytics](#).
3. On the original/main server (Large model), change the VM configuration and execute the `/opt/emms/emsam/bin/newcpmtuning.sh` command to upgrade the VM.
4. When the Cisco Prime Collaboration Assurance Server is up, go to the Cisco Prime Collaboration Assurance User Interface and enable Analytics.
5. Go to System Administration > License Management. Under the Analytics section, click Enable Analytics and configure the cisco Prime Collaboration Analytics DB Server IP Address.

6. Restore Cisco Prime Collaboration Analytics data (that you have backed-up in Step 1) to this Cisco Prime Collaboration Analytics database server. Refer to Step 5 in [Performing Backup and Restore in Prime Collaboration Analytics](#).

## How to downgrade Cisco Prime Collaboration deployment model?

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

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

1. Login to Cisco Prime Collaboration Assurance Serviceability User Interface.
2. Choose System Parameters > System Update Parameters.
3. Click Select to update drop-down list. You can select any one of the following system parameters to update:

- IP Address

You can enter only the New IP Address. The current status is not editable.

- Time Zone
- Host Name
- DNS Domain
- Name Server
- NTP Server
- Configure IPv6 address

Note:

1. An IP Address update requires a system Reboot.
  2. A Time Zone update requires a restart of all the processes.
  3. An update of other system parameters like Host Name, DNS Domain, Name Server, NTP Server, and Configure IPv6 address do not need a restart of all the processes.
4. Enter the details in the required fields.
  5. Click Update. It updates the entire Cisco Prime Collaboration Assurance server.

**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.

## Licensing

### How to find the MAC address of Cisco Prime Collaboration Assurance servers?

To find the MAC address of Cisco Prime Collaboration Assurance,

1. Login to Cisco Prime Collaboration Assurance.
2. To launch the About page in Enterprise mode, click globaladmin - Enterprise > About at the top right corner of the User Interface.

**Note:** To launch the About page in MSP mode, click globaladmin - All Customers > About at the top right corner of the User Interface.

3. Click Licensing link to open the License Management page.  
In the System Information section, you can view the MAC Address.

### 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 Cisco 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 Cisco Prime Collaboration. See the "Getting Started" chapter of [Prime Collaboration 9.0 Administration Guide](#) for information about invoking Cisco 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 Add Security Exception dialog box, click Confirm Security Exception.