Cisco Prime Collaboration Assurance Serviceability, 12.1

First Published: 2017-12-19

Last Modified: 2018-01-17

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PART I Cisco Prime Collaboration Assurance Serviceability 1

CHAPTER 1 Getting Started with Cisco Prime Collaboration Assurance Serviceability 3

- Introduction to Cisco Prime Collaboration Assurance Serviceability 3
- Accessing Cisco Prime Collaboration Assurance Serviceability 4
- User Interface 4
- Dashboard 5

CHAPTER 2 Maintenance 7

- Software Update 7
  - Add from sFTP Server 8
  - Add from Local Machine 8
- Backup 9
- Restore 9

CHAPTER 3 Root Access 13

- Root Access 13

CHAPTER 4 System History 15

- System History Dashboard 15
  - System Update Log 15
  - Backup / Restore Log 15

CHAPTER 5 System Parameters 17

- Update System Parameters 17

CHAPTER 6 Show System Information 19

- Show System Information 19

CHAPTER 7 **Reset Password** 21

Reset Password 21

CHAPTER 8 **DMA** 23

Overview of Data Migration Assistant 23

Setting Up Data Migration Assistant 23

Validate Data Migration Assistant 25

CHAPTER 9 **Reboot** 27

Reboot 27

PART I

Cisco Prime Collaboration Assurance Serviceability

- Getting Started with Cisco Prime Collaboration Assurance Serviceability, page 3
- Maintenance, page 7
- Root Access, page 13
- System History, page 15
- System Parameters, page 17
- Show System Information, page 19
- Reset Password, page 21
- DMA, page 23
- Reboot, page 27

CHAPTER 1

Getting Started with Cisco Prime Collaboration Assurance Serviceability

This document provides information on Cisco Prime Collaboration Assurance Serviceability for 12.1 release.

- Introduction to Cisco Prime Collaboration Assurance Serviceability, page 3
- Accessing Cisco Prime Collaboration Assurance Serviceability, page 4
- User Interface, page 4
- Dashboard, page 5

Introduction to Cisco Prime Collaboration Assurance Serviceability

Cisco Prime Collaboration Assurance Serviceability User Interface in 12.1 is an addition to the Command Line Interface (CLI) used in 11.x Cisco Prime Collaboration Assurance.

Serviceability User Interface helps you perform the following:

- Start/stop the process
- View the process status
- Perform software update
- Restore backed up data
- Enable Root Access
- Check system information
- View system history log
- Data Migration Assistant
- Change system parameters like IP address, DNS, and so on.
- Reset globaladmin password
- Reboot

Serviceability User Interface runs on the jetty web server.

Accessing Cisco Prime Collaboration Assurance Serviceability

Step 1 Open a browser session using a supported web browser, like Internet Explorer, Chrome.

Step 2 Go to https://<Cisco Prime Collaboration Assurance Serviceability server IP address>:<port number>/serviceability/.

Note Ensure to configure your web browser to enable/allow pop-up blocker for Cisco Prime Collaboration Assurance IP address before launching Cisco Prime Collaboration Assurance Serviceability. The Allow pop-up window/blocker for Cisco Prime Collaboration Assurance must be configured for all the supported web browsers.

Step 3 Enter an username as **globaladmin** and password credentials, and select **Login**. Only the user globaladmin is allowed to access the user interface.
Logging on to Cisco Prime Collaboration Assurance Serviceability provides access to all the menus.

Note The below note must be performed during the first login after fresh installation.

First invocation of Cisco Prime Collaboration Assurance Serviceability requires you to change the default *globaladmin* password. To login, enter the username as *globaladmin* with default password *Cisco123!*. For more information, see the section on "Log in to Cisco Prime Collaboration Assurance", chapter "Get Started after New Installation" in the topic "New Installation" in "Cisco Prime Collaboration Assurance and Analytics Install and Upgrade User Guide".

User Interface

Cisco Prime Collaboration Assurance Serviceability gives you a simplified user experience. The left pane displays vertical expandable Navigation tab, Index tab, Favorites tab, and Search menu fields.

Note To launch Cisco Prime Collaboration Assurance, the default password is *Cisco123!*. You have to change the default password during the first login after a fresh installation. For detailed steps, see Cisco Prime Collaboration Assurance Serviceability User Guide.

Click the **Navigation** icon ( ) on the Cisco Prime Collaboration Assurance Serviceability page to view a list of dashlets. You can click the pin icon at the top left to hide or display the left pane.

The following table describes the Cisco Prime Collaboration Assurance Serviceability dashboard.

Table 1: List of Dashboards

Dashboard	Description
Dashboard (Dashboard)	Allows you to view all the processes along with their status and System Update History. You can Start and Stop all the processes.
Software Update (Maintenance > Software Update)	Allows you to install a software bundle. This can be either a patch or an upgrade bundle.

Dashboard	Description
Backup (Maintenance > Backup)	Allows you to take data backup for both Assurance and Analytics from the user interface.
Restore (Maintenance > Restore)	Allows you to restore the backup data for both Assurance and Analytics from the user interface.
Root Access (Root Access)	Allows you to configure root access.
System Update Log (System History > System Update Log)	Allows you to view the system update log.
Backup/Restore Log (System History > Backup/Restore Log)	Allows you to view the backup and restore log.
Update System Parameters (System Parameters > Update System Parameters)	Allows you to update system parameters.
Show System Information (Show System Information)	Allows you to view system related information in a quick view.
Reset Password (Reset Password)	Allows you to reset the Cisco Prime Collaboration Assurance Serviceability globaladmin password.
DMA	Allows you to perform DMA Restore.
Reboot	Allows you to Reboot.

Dashboard

Choose **Dashboard** to view the following:

1. The header "Cisco Prime Collaboration Assurance" provides information on Version, License Type, and OVA Type. Click on the cross launch Click here to open PC Assurance to navigate between Cisco Prime Collaboration Assurance and Cisco Prime Collaboration Assurance Serviceability.
2. **Process Status:** You can view the Cisco Prime Collaboration Assurance Serviceability processes that are running on the server. You can start or stop the processes apart from viewing the server. The table displays the following information:
    1. **Process Name:** Name of the process.
    2. **Pid:** Process ID.
    3. **Status:** Status of the processes, either Running or Stopped.
    4. **Elapsed:** Duration for which the process has been running.
    5. **Description:** Description of the process.

Note You cannot start or stop an individual process. You can either Start or Stop all processes.

1. **Start All Process** button appears only when all processes are stopped.
2. **Stop All Process** button appears when all/some processes are running.

A notification also appears once the processes are started or stopped.

Note The View Process Status Detail link appears only when the processes is being started or stopped.

The process status dashboard automatically refreshes every 6 seconds.

3. **System Update History:** Lists all the installed software patches along with their date of installation.
   1. **Software:** Provides a list of installed software.
   2. **Installed Date:** Displays the date of installation.
   3. **Description:** Description of the installed software package.

CHAPTER 2

Maintenance

This chapter provides information on Maintenance Dashboard and the menus involved.

- Software Update, page 7
- Backup, page 9
- Restore, page 9

Software Update

Before You Begin

- You can install a software bundle. This can be either a patch or an upgrade bundle.
- The software bundle has to be in a tar.gz format. This should be uploaded first into Cisco Prime Collaboration Assurance Server.

You can upload the software bundle from any one of the following locations:

- sFTP Server
- Local Machine

Note The system reboots after successful Cisco Prime Collaboration Assurance software update.

What to Do Next

For information on how to add from sFTP Server and add from Local Machine, see the steps on "Add from sFTP Server" and "Add from Local Machine".

Add from sFTP Server

sFTP Server is mostly preferred for uploading upgrade bundle.

Step 1 Choose **Maintenance** > **Software Update**.

Step 2 Select **sFTP Server** and provide the sFTP credentials of the server and the complete path (including the filename) of the bundle where it resides.
You must provide the relative path (excluding the logged in user home directory).

Step 3 Click **Test Connection** to check the connectivity to the sFTP Server.

Step 4 Upon successful connection, click **Upload**. During this process, a progress bar appears indicating the progress of update. A notification also appears once the update is completed successfully.
Depending on the size of the bundle the time taken to upload will vary.

Step 5 Select a row and click **Start Update** to proceed with the upgrade.
A message indicating "After successful Software Update, system reboot will be performed. Do you want to continue?" appears.

- Click **OK** to perform Cisco Prime Collaboration Assurance software update.
- Click **Cancel** to exit the Cisco Prime Collaboration Assurance software update process.

Add from Local Machine

Local Machine is mostly preferred for uploading small patches. The bundle can exist on a local desktop/server where the Serviceability User Interface client is invoked.

Step 1 Choose **Maintenance** > **Software Update**.

Step 2 Select **Local Machine**.

Step 3 Click **Browse** to select the location of the file (tar.gz format) and click **Upload**.
During this process, a progress bar appears indicating the progress of update. A notification also appears once the update is completed successfully.

Step 4 Select a row and click **Start Update** to proceed with the update.
A message indicating "After successful Software Update, system reboot will be performed. Do you want to continue?" appears.

- Click **OK** to perform Cisco Prime Collaboration Assurance software update.
- Click **Cancel** to exit the Cisco Prime Collaboration Assurance software update process.

Backup

Choose **Maintenance** > **Backup**.

This cross launches to **Backup Settings** under **System Administration** in Cisco Prime Collaboration Assurance.

Restore

You can execute restore for both Assurance and Analytics from the user interface. Backup is performed in Cisco Prime Collaboration Assurance User Interface through **Backup Management**. The backup data can be restored using the Cisco Prime Collaboration Assurance Serviceability.

Note

- The system reboots after successful Cisco Prime Collaboration Assurance restore.
- Restore might fail in the following conditions -
  1. When connection to the remote server fails.
  2. If Analytics fails to stop.
  3. If the server does not have enough space for backup.

To start restore

Step 1 Choose **Maintenance** > **Restore**.

Step 2 Select the **Restore Category** from the drop-down list. You have two options to restore:

- **Assurance & Analytics –** You can restore files for Assurance and Analytics.
- **Assurance –** You can restore files only for Assurance.

Step 3 In the **Assurance Connection Settings** pane, enter the following details.
You can use sFTP or local connection to restore.

Assurance backup data resides in the local PC server or in the remote sFTP server.

Step 4 From **Restore Connection**,

a) If you select **sFTP**, enter the following details:

1. **IP Address** of the server where the backup file resides.
2. **Path** to the restore location.

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.

Field	Description
Path	Enter a name for the path. For example, the path that you provide should be **/backup/assurance_backup/{backup filename}**. Where, • /backup can be any desired name. This is the path given while taking a backup. • /assurance_backup - folder should be in this format.

3 **Port**

4 **Username**

5 **Password**

Click **Test Connection** to test the sFTP connection using the credentials.

b) If you select **Local**, enter the following details:

1 Specify the location or **Restore Path** including the filename. This is the location where the backup resides on the local machine.

2 You can specify the number of restore files to be saved, using the **Restore History** drop-down list.

Step 5 **Note** The **Analytics Connection Settings** pane is available only if you have enabled Cisco Prime Collaboration Analytics.

In the **Analytics Connection Settings** pane, enter the following details.
You can use only a remote server to restore the Analytics data using SSH configuration. The credentials used is only related to SSH and not sFTP.

Analytics backup data always resides only in a remote server and in order to download the data from the remote server, you MUST provide SSH details of the remote server.

1 **Remote IP Address** of the remote server where Analytics backup data resides.

2 **Path** in the remote sever where the Analytics backup data resides. You must provide the relative path.

For restore, provide the path excluding the logged in user home directory. For example,

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.

Field	Description
Path	Enter a name for the path. For example, the path that you provide should be **/backup/pg_basebackup** (followed by the timestamp (for example, pg_basebackup_201707201255)). Where, • /backup can be any desired name. This is the path given while taking a backup. • /pg_basebackup - folder should be in this format.

3 **SSH Port** of the remote server.

4 **SSH Username** of the remote server.

5 **SSH Password** of the remote server.

Click **Test Connection** to test the connection using the credentials.

Step 6 Click **Start Restore**.
A message indicating "After successful PCA Restore, system reboot will be performed. Do you want to continue?" appears.

- Click **OK** to perform Cisco Prime Collaboration Assurance restore.
- Click **Cancel** to exit the Cisco Prime Collaboration Assurance restore process.

Note Time taken for restoration is based on the file size.

CHAPTER 3

Root Access

This chapter provides information on Root Access Dashboard and the options involved.

- Root Access, page 13

Root Access

To Configure Root Access

Step 1 Choose **Root Access**.

Note Make sure that you do not lose the root password as there is no official Cisco supported method to retrieve the password.

Step 2 Click the **Root Access** drop-down list. You can select any one of the following options to configure root access:

1. Enable
2. Disable

Note Root access is disabled in Cisco Prime Collaboration Assurance 12.1 by default. To enable the root access, login to Cisco Prime Collaboration Assurance Serviceability User Interface to activate it.

Step 3 From Root Access,

a) If you select **Enable**, enter the following details:

1. **New Password**: Enter the New Password.
2. **Confirm New Password**: Enter the new password to confirm.

Note
- If the Root Access is already enabled then choose a different password.
- Resetting the password terminates the current active sessions.
- For Password policy, see the section on "Password Rules for globaladmin/root" in "Cisco Prime Collaboration Assurance and Analytics Install and Upgrade User Guide".

b) Select **Disable** to deactivate root access.

Note Disabling the Root terminates the current active sessions.

Step 4 Click **Submit**.

CHAPTER 4

System History

This chapter provides information on System History Dashboard and the menus involved.

- System History Dashboard, page 15

System History Dashboard

The **System History** Dashboard provides information on various logs generated during System Update and Backup / Restore.

System Update Log

Choose **System History** > **System Update Log** to view the system update log. You can hover on each row in the **Description** column to view complete information.

The following table describes the information displayed in the System Update Log dashboard.

Information	Description
Installation/Updates history	View the installation/update history of installed packages.
Restart/Shutdown history	View the process restart/shutdown date and time.
Reboot history	View the last rebooted date and time.

Backup / Restore Log

Choose **System History** > **Backup / Restore Log** to view the system update log.

The following table describes the information displayed in the System Update Log dashboard.

Information	Description
Backup history	Displays the Cisco Prime Collaboration Assurance backup history.

Information	Description
Restore history	Displays the Cisco Prime Collaboration Assurance restore history.

CHAPTER 5

System Parameters

This chapter provides information on System Parameters Dashboard and the menus involved.

- Update System Parameters, page 17

Update System Parameters

System Parameters menu refers to a specific system setting.

Use this menu to update system parameters. It has the provision of entering or changing the IP address, Time Zone, Host Name, DNS Domain, Name Server, and Configure IPv6 Address.

Step 1 Choose **System Parameters** > **Update System Parameters**.

Step 2 Click **Select to update** drop-down list. You can select any one of the following system parameters to update:

Note
- An **IP Address** update requires a system Reboot.
- A **Time Zone** update requires a restart of all the processes.
- 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.

- 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

Step 3 Enter the details in the required fields.

Step 4 Click **Update**. It updates the entire Cisco Prime Collaboration Assurance server.

CHAPTER 6

Show System Information

This chapter provides information on System Information Dashboard and the menus involved.

- Show System Information, page 19

Show System Information

To View System Information

Choose **Show System Information** to view the following system information details in a quick view. You can view the following Cisco Prime Collaboration Technical Support Debug Information:

1. OS Version
2. System Uptime
3. Clock
4. Memory Usage(KB): Displays the real-time memory and CPU usage.
5. Top output
6. swapon -s
7. swap usage per pid
8. status of CPCM processes
9. processes (ps ax --forest)
10. Disk Space: Displays information about disk usage on the node.
11. /proc/cpuinfo
12. netstat -i
13. netstat -a
14. netstat -rn

The following buttons are available on the right side of the page:

1. Click the **Download** button to either open or save the **show_system_info.log** file.
2. Click the **Refresh** button to load the page with the latest information.

CHAPTER 7

Reset Password

This chapter provides information on Reset Password Dashboard.

- Reset Password, page 21

Reset Password

You can reset the Cisco Prime Collaboration Assurance and Cisco Prime Collaboration Assurance Serviceability globaladmin password using the following procedure.

During installation, the product is installed with a default password. The system will redirect you to this page during the first time installation routine. It is mandatory to change the default password.

To reset the Cisco Prime Collaboration Assurance and Cisco Prime Collaboration Assurance Serviceability globaladmin password

Step 1 Choose **Reset Password**.

Step 2 Enter the **Current** globaladmin **Password**

Step 3 Enter a **New Password** for the globaladmin.

Step 4 Re-enter the new **Password** for the globaladmin to confirm.

Step 5 Click **Save**. A message notifies that the globaladmin passwords is successfully reset.

CHAPTER 8

DMA

This chapter provides information on DMA (Data Migration Assistant) and the procedure to set it up.

- Overview of Data Migration Assistant, page 23

Overview of Data Migration Assistant

Data Migration Assistant (DMA) assists you with the first step in migrating Cisco Prime Collaboration Assurance Serviceability data from earlier versions (11.5 or 11.6) by exporting this data in a format that Cisco Prime Collaboration Assurance Serviceability can read.

Whenever you migrate from 11.1 to another version it will be on the same Cisco Prime Collaboration Assurance server. For example, you have 11.5 and want to upgrade to 11.6. This means, in the Cisco Prime Collaboration Assurance equipment with the 11.5 version, the command to migrate to the latest versions is executed. So, migration happens in the same Cisco Prime Collaboration Assurance.

In version 12.1, the operating system is changed to CentOS. Hence, during migration, you must execute the backup utility in 11.x. Consequently, you must download the backup utility from CCO, execute it on the Cisco Prime Assurance server with 11.x. This action will generate a target (tar) file and upload it onto a sFTP remote server.

DMA is meant for moving data from 11.x to 12.1.

In 12.1 - To perform DMA, click DMA. Provide sFTP details and start the migration process. It downloads backup file from sFTP server and migrates the database. It is a one-time activity. On successful DMA migration, the data from 11.x server is available in 12.1 server. The login password remain unchanged (will be the 12.1 password).

Setting Up Data Migration Assistant

Choose **DMA**.

A confirmation message appears indicating whether you want to perform data migration.

- Click **OK** to perform data migration.
- Click **Cancel** to close.

Note The system reboots after successful DMA restore.

Step 1 Enter the following values on the **DMA** page.

1. **sFTP Server (IP Address)**: Enter sFTP server IP address where the backup resides.
2. **sFTP Port**: Enter sFTP server port number.
3. **Path**: Enter sFTP server backup path.
4. **User Name**: Enter the username.
5. **Password**: Enter the password.

Parameter	Example
sFTP Server IP address	10.78.88.102
sFTP Port number	22
User Name	Enter a name for the User Name. For example, user1 or provide any desired name.
sFTP server backup path	Enter the path (relative to the sFTP user home directory). For example, /backup if the backup resides in /user1/backup/{hostname}. Here {hostname} is the directory with the 11.x server's hostname.

Step 2 Click **Test Connection** to test the sFTP connection.

Note In case of test connection failure, possible are the reasons:

- sFTP IP address invalid or not reachable.
- sFTP port number invalid.
- sFTP path invalid.
- sFTP user name or password wrong.

Step 3 Click **Start DMA** to perform DMA restore.

Step 4 During this process, a progress bar appears indicating the progress of data migration. You can also click on View DMA Status Detail link to view the DMA status detail log.
A notification also appears once DMA is completed.

Step 5 If DMA is successful, you are redirected to the dashboard.

Login to Cisco Prime Collaboration Serviceability and Cisco Prime Collaboration Assurance using the 11.x password. Logging on to Cisco Prime Collaboration Assurance Serviceability provides access to all the menus.

Consider the following methods to validate DMA. For information, see Validate Data Migration Assistant.

Step 6 If DMA fails, you can view the failure log. The login to Cisco Prime Collaboration Assurance Serviceability User Interface mandates DMA to perform again.

Validate Data Migration Assistant

Consider the following steps to validate DMA restore.

Step 1 To verify if DMA is successful, then

1. Login as **Root**.
2. Check the status in **/var/log/dma_status.log**.

   You can view the status information in the log file.

Step 2 If DMA fails, then

1. Click on View DMA Status Detail link to understand the reason for failure and based on the details configure DMA accordingly.
2. Reenter the required sFTP configuration values on the DMA page. Click **Test Connection** to test the sFTP connection.
3. Click **Start DMA**.

   During this process, a progress bar appears indicating the progress of data migration.

   Note
   - If DMA is successful, a success notification popup appears on the right side bottom of the screen.
   - If you have missed to view the popup,
     1. Login to Root.
     2. Check for the "Success" or "Failure" status message in **/var/log/dma_status.log** file.

CHAPTER 9

Reboot

This chapter provides information on Reboot Dashboard and the procedure involved.

- Reboot, page 27

Reboot

This option reboots the Cisco Prime Collaboration Assurance server box.

To Reboot Cisco Prime Collaboration Assurance server box

Step 1 Choose **Reboot**. A confirmation message notifies that the server will take a few minutes to reboot. You might have to close your browser and relaunch it after a few minutes.

Step 2 Click **OK** to reboot. The system process reboots. or Click **Cancel** to exit the reboot process.