Migrate Cisco Prime Collaboration Assurance

This chapter is NOT applicable for 12.1 Service Pack 3 and later releases.

This section explains the following:

Overview of Data Migration Assistant

Note Migration from Cisco Prime Collaboration Assurance 11.x to Cisco Prime Collaboration Assurance 12.1 Service Pack 3 is not supported.

This chapter provides an overview of Data Migration Assistant (DMA), explains how to install and use it, and provides related information.

DMA assists in migrating Cisco Prime Collaboration Assurance data from supported versions of 11.x to Cisco Prime Collaboration Assurance 12.1.

If you want to migrate from 11.x to 12.1 for both ENT/MSP modes, the following DMA paths are supported:

Table 1: Supported Versions

Mode	11.5	11.5 SP1	11.6
ENT	No	No	Yes
MSP	Yes	No	Yes

Mandatory Migration Path for 11.x to 12.1 customers,

```
Install 12.1 FCS -> Apply 12.1 SP1 -> Perform DMA
```

Note We recommend you to perform the following before migration.

Apply 12.1 SP1 on 12.1 Fresh installation. For more information on installing 12.1 Service Pack 1, see the "Readme for Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 1".

Use the Backup RPM as mentioned in the "Readme for Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 1".

12.1 Service Pack 1 Backup RPM can be downloaded from CCO at Software Download.

Path: Downloads Home / Cloud and Systems Management / Collaboration and Unified Communications Management / Prime Collaboration / Prime Collaboration Assurance 12.1 / Prime Collaboration Patches- 12.1 Service Pack1

The reason for migration is due to the change in the underline operating system of Cisco Prime Collaboration Assurance.

Data Migration Assistant is performed in the following method:

- Data Migration Assistant Backup - Use Perform Data Migration Assistant Backup to backup your data on 11.x server.
- Data Migration Assistant Restore - Use Perform Data Migration Assistant Restore to restore the backup data on 12.x server.

Note

- We recommend you to perform DMA backup either during lean or maintenance period because Cisco Prime Collaboration Assurance Database (DB) restarts twice (once at the beginning and once at the end), as part of a few DMA configuration setup. This restart leads to inconsistent system after backup.
- Currently, the time taken to perform a DMA backup of 50 GB data from 11.x server to 12.1 is around 4 to 5 hours. For a fully loaded setup it takes a minimum of 30 hours.

Preinstallation Guidelines

Review the following guidelines and perform the appropriate steps before installing DMA:

1. If a PKCS7 or PKCS12 certificate is applied to 11.x and the Cisco Prime Collaboration Assurance is migrated to version 12.1, the certificate will not be restored. You need to regenerate the certificate for the Cisco Prime Collaboration Assurance 12.1.

Note From Cisco Prime Collaboration Assurance 11.6 onwards, only PKCS12 certificate is supported.

2. You cannot restore the purchased license of Cisco Prime Collaboration Assurance 11.x to 12.1. You must purchase the license with the same endpoint count for Cisco Prime Collaboration Assurance 12.1. Once

the DMA migration is completed successfully, the Cisco Prime Collaboration Assurance 12.1 server will be in Evaluation mode.

3. DMA backup is not supported in Cisco Prime Collaboration Assurance Release 11.x in “FIPS mode and Standard mode”.
4. DMA restore is not supported in Cisco Prime Collaboration Assurance Release 12.1 in “FIPS mode”.
5. If you have deployed in MSP mode, the Video endpoints with Public IP address(es) become Unreachable after DMA restore.

Following sFTP Servers are supported in the Cisco Prime Collaboration Assurance Data Migration Assistant.

Table 2: sFTP Servers Supported

sFTP Server
Mac OS X
Windows SolarWinds
Windows FreeFTPd
CentOS sFTP Server
Linux sFTP Server

Pre-requisites for Backup and Restore

Before you begin

Pre-requisites for Backup

1. If you want to perform data migration from 11.0 or 11.1 versions to 12.1 version then first upgrade to the supported upgrade path of either 11.5 or 11.6 versions and then perform data migration to 12.1 version. For more information, see the table on “Supported Versions” in the chapter on “Overview of Data Migration Assistant”.
2. Enable Root Access on 11.x servers before performing Data Migration Assistant (DMA). For steps to enable root access, see Enable Root Access in 11.x Server.
3. If you have created the Phone Status test in Cisco Prime Collaboration Assurance 11.6 server then it is mandatory to run the following commands. This way you can export the existing Phone Status test to a file that can be used to import tests after DMA migration.
   a. Login to the Cisco Prime Collaboration Assurance server as ***root***.
   b. Create a new text file '11.6_PhoneStatusImportFile.txt' with read and write permissions at **/opt/emms/cuom/ImportFiles**.
   c. Run the following command:

```
/opt/postgres/9.2/bin/psql -p 5433 --username=cmuser  cpcm -c "copy (select
extensionnumber, macaddress, ipaddress, saaipaddress from prphone) to '/opt/emms/cuom/
ImportFiles/11.6_PhoneStatusImportFile.txt' delimiter ':';"
```

After running the above commands, you are required to delete all the Phone Status test created in the Cisco Prime Collaboration Assurance 11.6.

4. Delete all the Batch and subsequent Synthetic tests from the Cisco Prime Collaboration Assurance 11.6.
5. Backup is created with hostname in backup path (For example, if the backup path is **/tempbackups** then the backup will be available at: **{ssh username}/tempbackups/{hostname}**).

Note The hostname of 11.x and 12.1 should be the same. If the values do not match, then DMA restore fails.

6. The expected time taken for the DMA to complete the backup process varies depending on the profile and data of the backup server.
7. **Disable CDR/CMR configuration on CUCM** Disabling CDR/CMR configuration on CUCM prevents CUCM sending bulk CDR/CMR(s). Perform the following steps:
   a. Go to **CUCM Serviceability** page of all managed CUCM publishers.
   b. Navigate to **Tools** > **CDR Management**.
   c. Select the **PCA IP address/Hostname**.
   d. On the **Billing Application Server Parameters** section, uncheck **Resend on Failure** check box and click **Update**.

Note Make sure whether the check box is already unchecked.

8. If Analytics is enabled, the Cisco Prime Collaboration Assurance and Analytics Database (DB) restarts during DMA backup.

Note Backup must be taken from 11.x server with the RPM that is provided on CCO site.

Pre-requisites for Restore

Note The system reboots after successful DMA restore.

1. The expected time taken for the DMA to complete the restore process varies depending on the profile and data of the backup server.
2. The Deleted state devices/endpoints will be purged and after the upgrade these (the devices/endpoints) will not be available.
3. DMA restore on Cisco Prime Collaboration Assurance 12.1 should be performed through Serviceability after taking a DMA backup on 11.x server.
4. The hostname of 11.x and 12.1 should be the same. If the values do not match, then DMA restore fails.

For information on preinstallation guidelines, see the section on Preinstallation Guidelines.

DMA Backup and Restore Time Period - Approximate Values

The time taken for DMA Backup and Restore varies according to the database size. **Approximate** time taken for different sizes are listed in the table below.

	Assurance DB Size	Assurance Backup Time	Assurance Restore Time	Analytics DB Size	Analytics Backup Time	Analytics Restore Time	Total Backup Time	Total Restore Time	Total Time Taken for Migration (Excluding Process Startup Time)
Small	5 GB	10 minutes	25 minutes	60 GB	50 minutes	25 minutes	1 hour	50 minutes	1 hour 50 minutes
Medium	15 GB	25 minutes	1 hour 5 minutes	150 GB	1 hour 15 minutes	1 hour	1 hour 40 minutes	2 hours 5 minutes	3 hours 45 minutes
Large	25 GB	35 minutes	1 hour 45 minutes	279 GB	2 hours 40 minutes	1 hour 40 minutes	3 hours 15 minutes	3 hours 5 minutes	6 hours 20 minutes
Very Large	39 GB	55 minutes	2 hours 40 minutes	383 GB	3 hours 5 minutes	2 hours 10 minutes	4 hours	4 hours 50 minutes	8 hours 50 minutes

Preparation for Data Migration Assistant

1. For Very Large Deployment, if Analytics is enabled, perform the following:
   a. Enable root for DBVM.
   b. Install the backup RPM in both DBVM and MainVM.
   c. Perform DMA only on the MainVM and when prompted provide password for DBVM on Cisco Prime Collaboration Assurance 12.1.

      If Analytics is disabled or if you do not require Analytics data to be migrated, then DMA has to be performed on the Application server.

2. The hostname of 11.x and 12.1 should be the same and the IP address for both these servers should also be same. If the values do not match, then DMA restore fails.

Enable Root Access in 11.x Server

Perform the following steps to enable root access in 11.5 and 11.6 servers.

Step 1 Login as admin from the Cisco Prime Collaboration Assurance VM Console.

```
admin/admin# root_enable
```

Step 2 Configure the root patch password.

```
admin/admin# root
```

Step 3 Enter the root password.

```
ade# /opt/emms/emsam/bin/enableRoot.sh
```

Step 4 Configure the actual root password.

```
ade# passwd
```

What to do next

Perform DMA (Data Migration Assistant) from Cisco Prime Collaboration Assurance Serviceability.

Perform Data Migration Assistant Backup

For Pre-requisites, see the section "Pre-requisites for Backup and Restore".

Step 1 Copy RPM (as shown in the example below) to **/opt**.

For example, CSCOpca-dma-x.x-x.x86_64.rpm.

Note For more information, see the respective Read me of Engineering Special or Service Pack release for exact RPM name to be downloaded and used.

The RPM is available on the Cisco Connection Online (CCO) postings.

Step 2 Run below commands to install RPM.

```
#cd /opt
#rpm -ivh CSCOpca-dma-x.x-x.x86_64.rpm
```

Note

- To verify whether the RPM is installed successfully, run the following command:

  ```
  rpm -qa | grep -i CSCOpca-dma
  ```

  The command with an entry is displayed as follows:

  ```
  rpm -qa | grep -i CSCOpca-dma
  Result: CSCOpca-dma-x.x-x
  ```

- If the installation of RPM fails or exists abruptly, run the following command to remove the RPM:

  ```
  rpm -e CSCOpca-dma--x.x-x
  ```

  Or

  ```
  yum remove CSCOpca-dma-x.x-x
  ```

- To verify whether the RPM is uninstalled successfully, run the following command:

  ```
  rpm -qa | grep -i CSCOpca-dma
  ```

The result of the command should not display any entry (**`CSCOpca-dma-x.x-x`**).

Note If the error continues to occur, contact the Cisco Technical Assistance Center (TAC) for assistance.

Step 3 Go to directory **/opt/emms/infra/dma/**.

Step 4 Run script **./pcandma.sh**.

Step 5 Enter the values when prompted:

a) **sFTP Server (IP Address)**: Enter sFTP server IP address to store the backup.

Choose any of the sFTP server(s) where DMA backup can be stored and later fetched during DMA restore.

b) **sFTP Port**: Enter sFTP server port number.
c) **User Name**: Enter the username.
d) **Path**: Enter sFTP server backup path.
e) **Password**: Enter the sFTP password.

Table 3: Field Names with Examples

Field Name	Example
sFTP Server (IP Address)	10.78.88.102
sFTP Port	22
UserName	Enter a name for the Username. For example, **user1** or provide any desired name.
Path	Enter the path. The DMA backup is taken in the path relative to the sFTP user home directory. If path is **/backup**, the DMA backup location will be **/user1/backup/{hostname}.**

Step 6 Verify for backup in sFTP server at the configured backup location.

If the sFTP UserName is **user1** and the configured backup path is **/backup**, then the backup resides at **/user1/backup/{hostname}**.

Here **{hostname}** is the directory created with the 11.x server's hostname.

Step 7 Backup file is generated in gpg format for Assurance and Analytics and uploads to sFTP server under the hostname folder under the configured backup location: **/user1/backup/{hostname}**.

For example, if **/backup** is the configured backup location, where the backup is available at **/user1/backup/{hostname}**, where **user1** is the sFTP user home directory and **backup** is Assurance_Backup.tar.gz, Analytics_Backup.tar.gz.

What to do next

For information on performing Data Migration Assistant Restore, see the section on Perform Data Migration Assistant Restore.

Troubleshooting

Issue: DMA backup fails.

Conditions: Following are the conditions:

- sFTP server is not reachable
- Credentials do not match
- Upload of backup file fails and so on

  Relevant messages appear on console.

Possible Solution: Following are the logs for reference -

- /var/log/pcandma.log - Provides basic information of the Cisco Prime Collaboration Assurance and Analytics DMA.
- /var/log/dma_debug.log - Provides a complete debug messages of DMA.
- /var/log/assurance_backup_dma.log - Provides detailed information of Assurance backup DMA.
- /var/log/analytics_dma.log - Provides detailed information of Analytics DMA.

Credential Verification Error Messages for DMA Backup

The credential verification error messages for DMA Backup are tabulated below.

Error Message	Conditions	Possible Solutions
Login failed, sFTP server is not reachable.	Invalid sFTP server IP address entered for backup in 11.x server.	Enter an appropriate IPaddress.
Unable to connect to the server. Session timed out.	Invalid sFTP port number entered for backup in 11.x server.	Enter an appropriate sFTP Port number.

Error Message	Conditions	Possible Solutions
Login failed, sFTP user name or password is wrong.	Invalid sFTP server credentials entered for backup in 11.x server.	Enter an appropriate sFTP server credentials.
Couldn't create directory <location> in sFTP server.	Invalid sFTP server backup path entered for backup in 11.x server.	Enter valid path and try backup again.
The data filesystem is <disk usage> % full. The threshold is 85 % . Starting a backup may result in filling up the filesystem. Warning user and aborting backup. Insufficient disk space to perform full backup.	If the disk usage is greater than 85% in backup server.	Check free space and try backup again.
Cisco Prime Collaboration Assurance is in FIPS mode.	The DMA backup process terminates, since DMA backup is not supported in FIPS mode.	Turn OFF FIPS mode in PCA to continue DMA backup and start the backup process.
Cisco Prime Collaboration Assurance in STANDARD mode.	The DMA backup process terminates, since DMA backup is not supported in STANDARD mode.	-

Perform Data Migration Assistant Restore

For Pre-requisites, see the section "Pre-requisites for Backup and Restore".

Note When DMA restore is in progress and until DMA is successful, you will not be able to access the following: Cisco Prime Collaboration Assurance User Interface, UCOD application, and all other features of Cisco Prime Collaboration Assurance Serviceability. Once DMA is successful, system reboots and launches the Cisco Prime Collaboration Assurance Serviceability (Login using 11.x password).

Step 1 Login to Cisco Prime Collaboration Assurance Serviceability.

Note For future DMA status logging purpose, enable root access from Cisco Prime Collaboration Assurance Serviceability and take a snapshot of the Virtual Machine. For information, see the chapter on “Root Access” in “Cisco Prime Collaboration Assurance Serviceability” User Guide for Release 12.1.

Step 2 Choose DMA (Data Migration Assistant) in Cisco Prime Collaboration Assurance Serviceability User Interface.

A confirmation message appears indicating whether you want to perform Data Migration.

- Click **OK** to perform Data Migration. Follow **substeps a** through **substeps e** of Step 3 for a successful data migration.
- Click **Cancel** to close.

  If you click **OK** the application loads the DMA configurations.

Note The system reboots after successful DMA restore.

In case of a 2VM setup for a Very Large Deployment, perform the following steps:

Note Ensure to enable root access for both DB VM and Main VM before performing Data Migration, to monitor all the activities during the migration. For steps to enable root access, see the chapter on "Root Access" in "Cisco Prime Collaboration Assurance Serviceability" User Guide for Release 12.1.

a. Very Large Deployment is a 2VM setup:

1. **DB VM**
   - **a.** In Cisco Prime Collaboration Assurance Serviceability User Interface of DB VM, click **DMA**

     Note Read the instructions on the screen carefully before you click OK.

   - **b.** Click **OK**.

     This configures the DB VM server for DMA restore.

2. **Main VM**
   - **a.** In Cisco Prime Collaboration Assurance Serviceability User Interface of Main VM, click **DMA**.

     Note Read the instructions on the screen carefully before you click OK.

   - **b.** Click **OK**.

     This configures the Main VM server for DMA restore.

This takes you to the DMA sFTP configuration page of the Cisco Prime Collaboration Assurance Serviceability of the Main VM.

Provide the details of the sFTP server (where the backup is stored) and proceed with DMA configuration.

Step 3 Perform the following steps:

a) 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 sFTP 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.

Parameter	Example
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.

b) 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.

c) Click **Start DMA** to perform DMA restore.

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 indicating DMA Success or Failure status.

A notification appears once DMA is completed.

d) If you have deployed in MSP mode, the Video endpoints with Public IP address(es) become Unreachable after DMA restore.

In such cases, delete the Video endpoints from Inventory Management page and add them with Public and Private IP address(es).

e) Once DMA Restore process completes, the Cisco Prime Collaboration Assurance 12.1 server reboots.

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.

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

What to do next

Import Phone Status test After Upgrade

These steps holds good only after a complete migration of 12.1.

1. Login to Cisco Prime Collaboration Assurance server as *root*.
2. Navigate to **/opt/emms/cuom/ImportFiles** and download **11.6_PhoneStatusImportFile.txt** file to local server.

3. Add respective Read community and Write community strings. For more information, see "/opt/emms/cuom/ImportFiles/PhoneStatusImportFile.txt".
4. Login to Cisco Prime Collaboration Assurance as *globaladmin*.
5. Navigate to **/Synthetic Tests/Phone Status Test** and import the Phone Status test from the file downloaded in Point 2.

Note After running the above commands, you are required to delete all the Phone Status test created in the Cisco Prime Collaboration Assurance 11.6 and re-create the Batch Test after the restore is successful.

Enable CDR/CMR on CUCM Perform the following steps after DMA Restore.

1. Go to **CUCM Serviceability** page of all managed CUCM publishers.
2. Navigate to **Tools** > **CDR Management**.
3. Select the **PCA IP address/Hostname**.
4. On the **Billing Application Server Parameters** section, check **Resend on Failure** check box and click **Update**.

Troubleshooting

Issue: DMA restore fails.

Conditions: Following are the conditions:

- sFTP server is not reachable.
- Credentials do not match.

Possible Solution: Following are the logs for reference -

- /var/log/pcandma.log - Provides basic information of the Cisco Prime Collaboration Assurance and Analytics DMA.
- /var/log/dma_debug.log - Provides a complete debug messages of DMA.
- /var/log/assurance_restore_dma.log - Provides detailed information of Assurance restore DMA.
- /var/log/analytics_upgrade.log - Provides detailed information of Analytics upgrade.
- /var/log/dma_status.log - Provides status information of the success or failure of DMA.

Credential Verification Error Messages for DMA Restore

Following are the conditions and possible solutions for test connection failure.

Conditions	Possible Solutions
Invalid sFTP server IP address entered for restore in 12.1 server.	Enter an appropriate IPaddress.

Conditions	Possible Solutions
Invalid sFTP port number entered for restore in 12.1 server.	Enter an appropriate sFTP Port number.
Invalid sFTP server credentials entered for restore in 12.1 server.	Enter an appropriate sFTP server credentials.
Invalid sFTP server restore path entered for restore in 12.1 server.	Enter valid path and try restore again.

Validate Data Migration Assistant

Consider the following steps to validate DMA restore.

Step 1 To verify if DMA is successful, then

a. Login as **Root**.

b. 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

a. Click on View DMA Status Detail link to understand the reason for failure and based on the details configure DMA accordingly.

b. Reenter the required sFTP configuration values on the DMA page. Click **Test Connection** to test the sFTP connection.

c. 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.