

Configure Backup and Restore from GUI in CUCM

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Backup](#)

[Restore](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the setup requirements for **Backup** and **Restore** features in **CUCM** from the **Graphic User Interface (GUI)**.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- **Cisco Unified Communications Manager**
- **Secure File Transfer Protocol (SFTP)**

Components Used

The information in this document is based on these software versions:

- **Cisco Unified Communications Manager** version 10.5.2.15900-8

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The **Disaster Recovery System (DRS)**, which can be invoked from CUCM Administration, provides full data backup and restore capabilities for all servers in the cluster. The DRS enables regularly scheduled automatic or user-invoked data backups.

DRS restores its own parameters (backup device and schedule parameters) as part of the platform backup/restore. DRS backs up and restores the `drfDevice.xml` and `drfSchedule.xml` files. When the server is restored with these files, there is no need to reconfigure DRS backup device and schedule.

The **Disaster Recovery System** includes these capabilities:

- A user interface in order to perform backup and restore tasks
- A distributed system architecture with backup and restore functions
- Scheduled backups
- Archive backups to a physical tape drive or remote SFTP server

The **Disaster Recovery System** contains two key functions, **Master Agent (MA)** and **Local Agent (LA)**.

The **Master Agent** coordinates backup and restore activity with **Local Agents**. The system automatically activates the **Master Agent** and **Local Agent** on all nodes in the cluster.

CUCM cluster (this involves the CUCM nodes and the **Cisco Instant Messaging & Presence (IM&P)** servers) must fulfil these requirements:

- **Port 22** open in order to establish the communication with SFTP server
- Validated that the **IPsec** and **Tomcat** certificates are not expired.

In order to verify the validity of the certificates, navigate to **Cisco Unified OS Administration > Security > Certificate Management**

 **Note:** In order to regenerate ipsec and Tomcat certificates, use the [Procedure to regenerate certificates in CUCM](#)

- Ensure that the Database Replication is setup completed and does not show any errors or mismatches from the CUCM Publisher and the IM&P Publisher servers.

SFTP server settings must cover these requirements:

- Login credentials are available
- It must be reachable from the CUCM server
- Files are included in the path selected when a restore is performed

Configure

Backup

The **Disaster Recovery System** performs a cluster-level backup, which means that it collects backups for all servers in a CUCM cluster to a central location and archives the backup data to physical storage device.

Step 1. To create backup devices on which data is saved; navigate to **Disaster Recovery System > Backup > Backup Device**.

Step 2. Select **Add New**; define a **Backup Device Name** and enter the SFTP values. **Save**



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Backup Device



Save



Back

Status



Status:Ready

Backup device name

Backup device name*

BackupDevice1

Select Destination*

Network Directory

Host name/IP address

10.1.89.107

Path name

/

User name

administrator

Password

Number of backups to store on Network Directory

2 ▾

Save

Back

Step 3. Create and edit backup schedules in order to back up data. Navigate to **Backup > Scheduler**.

Step 4. Define a **Schedule Name**. Select the **Device Name** and check the **Features** based on your scenario.

Backup ▾ Restore ▾ Help ▾

Scheduler

Status

① Status: Ready

Schedule Name

Schedule Name*

Select Backup Device

Device Name*

Select Features *

CDR_CAR
 UCM
 PLM

Step 5. Configure a scheduled backup based on your scenario.

Start Backup at*

Date Time Hour Minute

Frequency*

Once
 Daily
 Weekly
 Monthly






Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday
 Sunday

Step 6. Select **Save** and notice the warning as shown in the image. Select **OK** in order to move forward.


The DRS Backup archive encryption depends on the current security password. During a restore, you could be prompted to enter this security password if this password has been changed.

Step 7. Once that a **Backup Schedule** is created, select **Enable Schedule** .

Scheduler

 Save  Set Default  Disable Schedule  Enable Schedule  Back


Status

 Disabled

Schedule Name






Schedule Name*

Step 8. Wait until the status is changed to **Enabled**.


 **Disaster Recovery System**
For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Scheduler

 Save  Set Default  Disable Schedule  Enable Schedule  Back

Status

 Enabled

Schedule Name

Schedule Name*

Step 9. If a Manual backup is required, navigate to **Backup > Manual Backup**.

Step 10. Select the **Device Name** and check the **Features** based on your scenario.



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Manual Backup



Start Backup



Estimate Size



Select All



Clear All

Status



Status:Ready

Select Backup Device

Device Name*

BackupDevice1 ▾

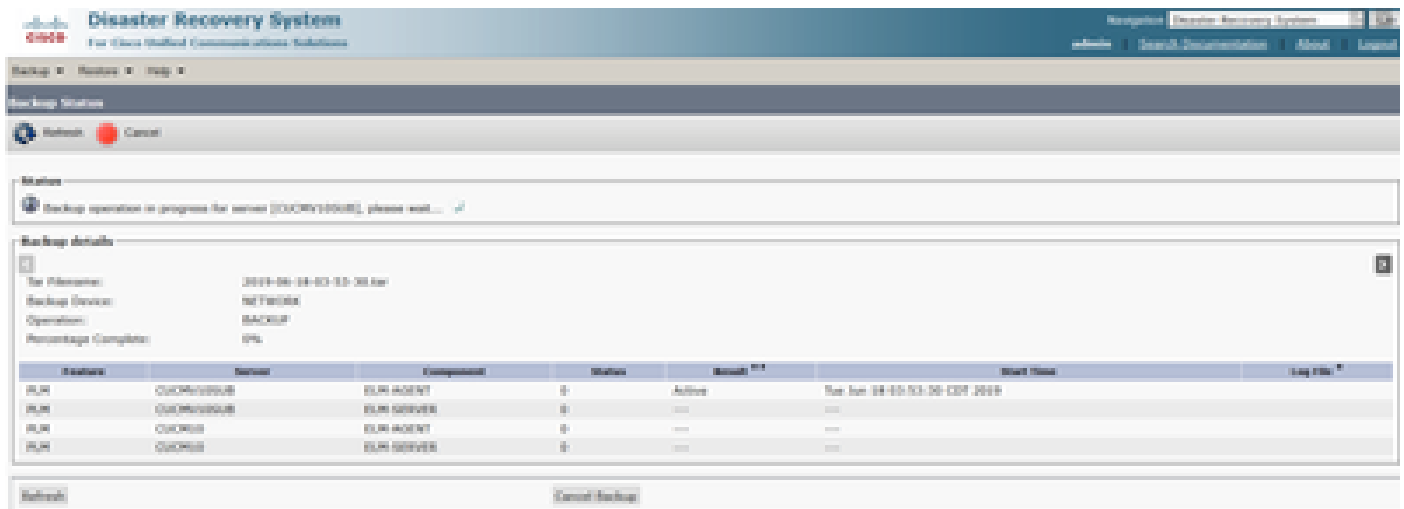
Select Features *

CDR_CAR

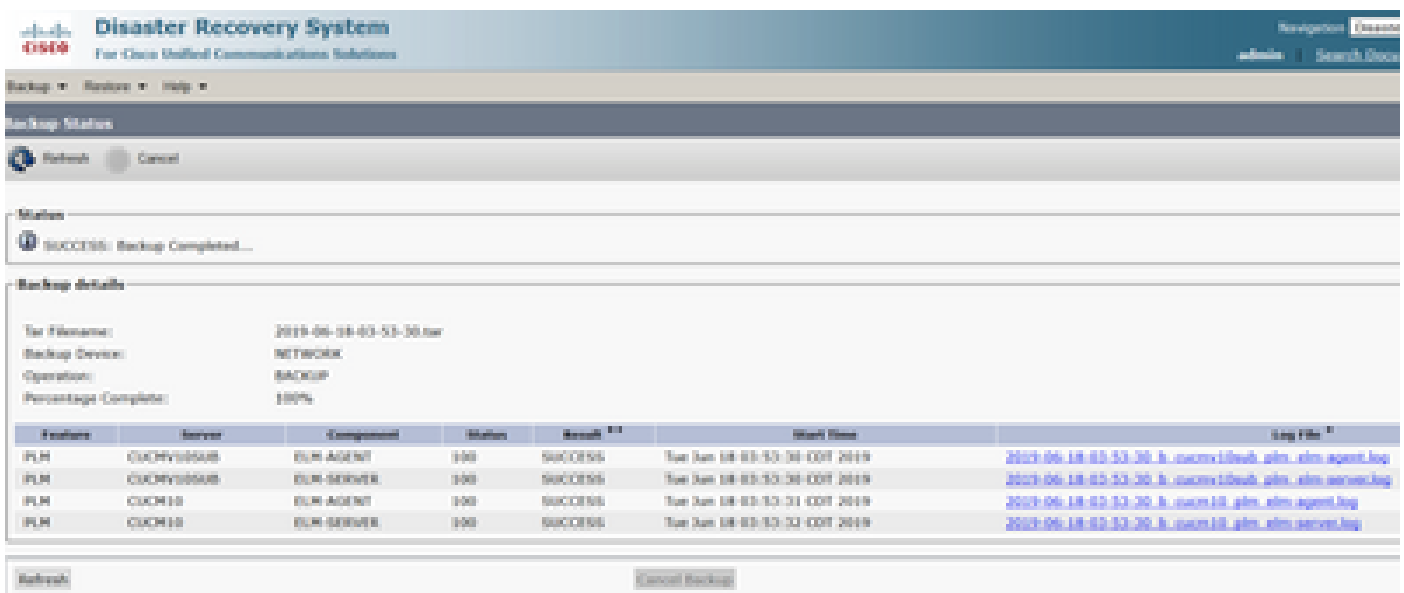
UCM

PLM

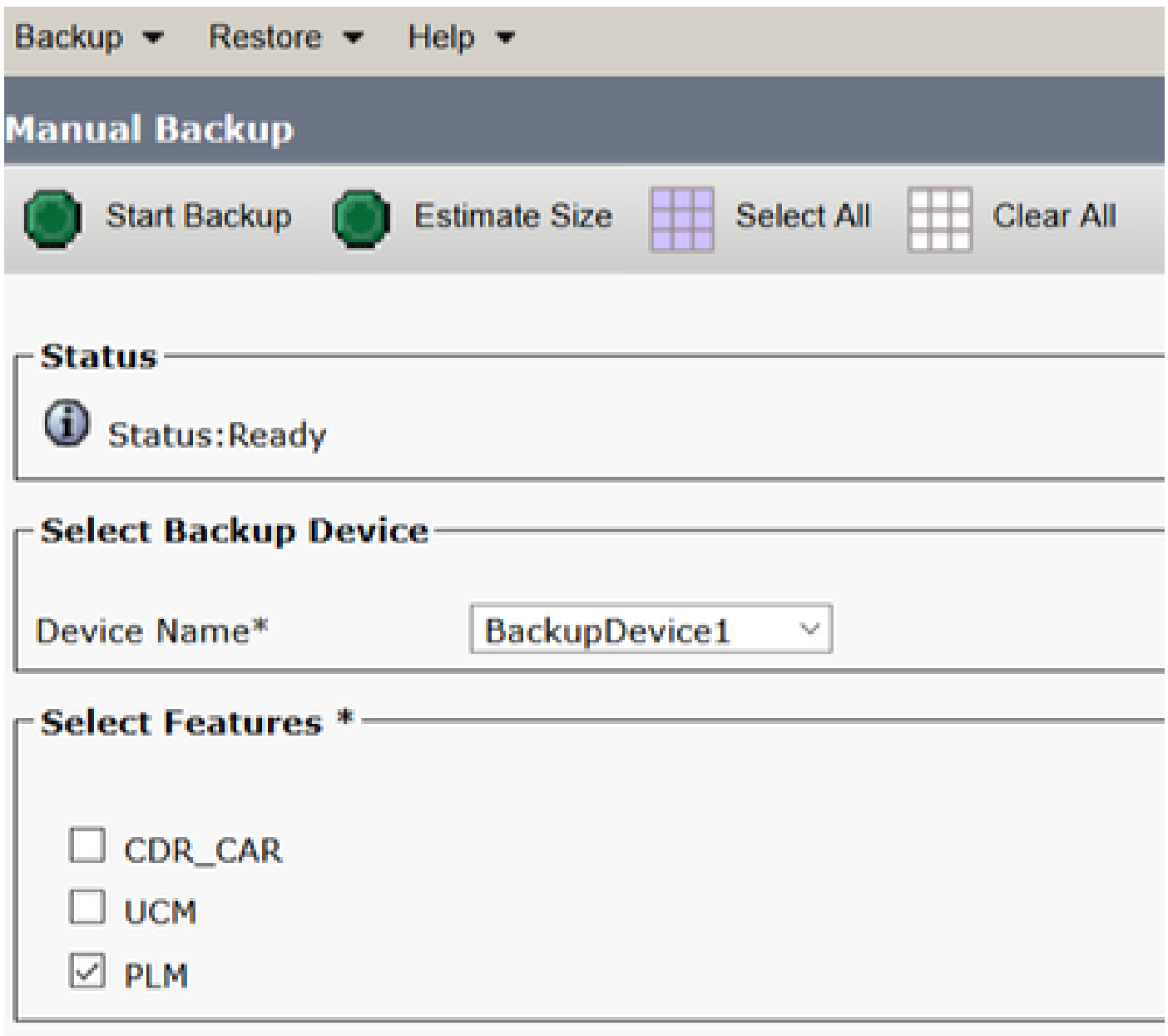
Step 11. Select **Start Backup** and operation is displayed in progress.



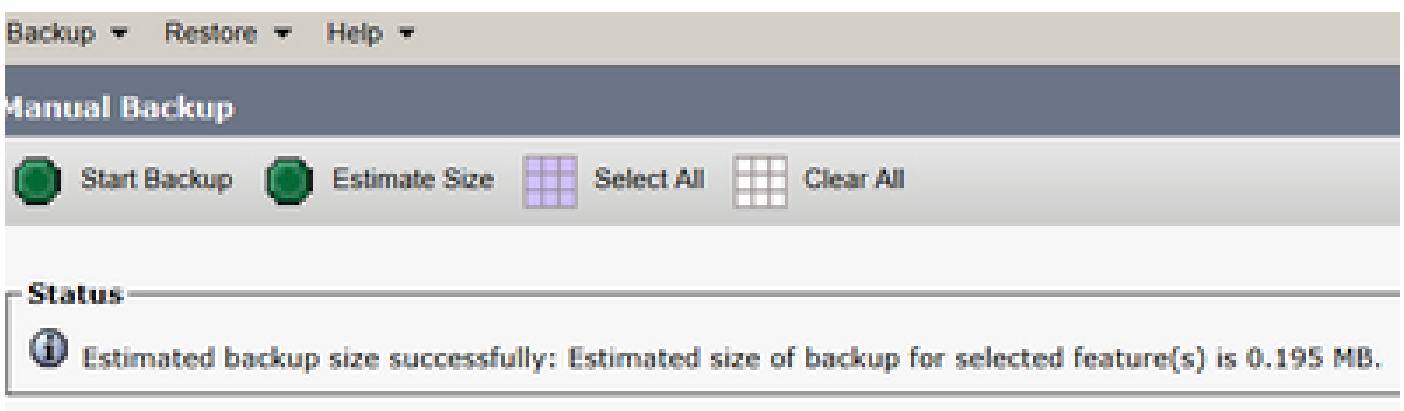
Step 12. When the manual backup is completed, the completion message is displayed.




Step 13. To estimate the size of backup tar file that SFTP device uses, select **Estimate Size**.



Step 14. Estimate size is displayed as shown in the image



 **Note:** Estimate Size function is calculated based on previous successful backups and can vary in case configuration has been changed since the last backup.

Step 15. To check the Status of the Backup while a backup runs, navigate to **Backup > Backup Status**.

Backup Status

Refresh Cancel

Status

SUCCESS: Backup Completed...

Backup Details

Tar Filename: 2019-06-18-03-53-30.tar
 Backup Device: NETWORK
 Operation: BACKUP
 Percentage Complete: 100%

Features	Server	Component	Status	Result	Start Time	Log File
PLM	EUM1000048	EUM-AGENT	100	SUCCESS	Tue Jun 18 03:53:30 CDT 2019	2019-06-18-03-53-30_h_eum1000048_plm_eum-agent.log
PLM	EUM1000048	EUM-SERVER	100	SUCCESS	Tue Jun 18 03:53:30 CDT 2019	2019-06-18-03-53-30_h_eum1000048_plm_eum-server.log
PLM	EUM11	EUM-AGENT	100	SUCCESS	Tue Jun 18 03:53:31 CDT 2019	2019-06-18-03-53-30_h_eum11_plm_eum-agent.log
PLM	EUM11	EUM-SERVER	100	SUCCESS	Tue Jun 18 03:53:32 CDT 2019	2019-06-18-03-53-30_h_eum11_plm_eum-server.log

Refresh Cancel Backup

Step 16. To consult the backup procedures performed in the system, navigate to **Backup > History**.

Backup History

Refresh

History

Tar Filename	Backup Device	Completed On	Result	Backup Type	Version	Features Backed Up	Features Backed Up Warning	Failed Features
2019-06-18-03-53-30.tar	NETWORK	Tue Jun 18 03:53:31 CDT 2019	SUCCESS	MANUAL	10.5.2.02000-0	PLM	---	---
2019-06-18-03-53-30.tar	NETWORK	Tue Jun 18 03:53:34 CDT 2019	SUCCESS	MANUAL	10.5.2.02000-0	PLM	---	---
100_06_not_created	NETWORK	Tue Jun 18 12:00:00 CDT 2019	ERROR	SCHEDULED - DailyBackup	---	---	---	---
100_06_not_created	NETWORK	Wed Jun 19 12:00:00 CDT 2019	ERROR	SCHEDULED - DailyBackup	---	---	---	---

Restore

DRS restores mainly **drfDevice.xml** and **drfSchedule.xml** files. However, when a system data restoration is performed, you can choose which nodes in the cluster require to get restored.

Note: Backup Device (SFTP server) must be already configured in order to retrieve the tar files from it and restore the system with these files.

Step 1. Navigate to **Disaster Recovery System > Restore > Restore Wizard**.

Step 2. Select the **Device Name** which stores the backup file to use for the restore. Select **Next**.



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Step1 Restore - Choose Backup device



Next



Cancel

Status



Status:Ready

Select Backup Device

Device Name*

-- Not Selected -- ▾

-- Not Selected --

SFTP_1

BackupDevice1

Next

Cancel

Step 3. Select the **Backup File** from the displayed list of available files as shown in the image. Selected backup file must include the information to restore.



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Step2 Restore - Choose the Backup Tar File

Back Next Cancel

Status

Status:Ready

Select Backup Archive**

Select Backup File*

-- Tar file list --	▾
-- Tar file list --	
2019-06-18-03-51-57	
2019-06-18-03-53-30	

Step 4. From the list of available features, select the feature to restore.

Disaster Recovery System
For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Step3 Restore - Select the type of Restore

Back Selected All Clear All Next Cancel

- Status

Status: Ready

Select Features *

FLM

Backed up components in TAB:

Feature	Server	Server
FLM	CUCM10SUB	ELM-AGENT
FLM	CUCM10SUB	ELM-SERVER
FLM	CUCM10	ELM-AGENT
FLM	CUCM10	ELM-SERVER

Step 5. Select the nodes in which to apply the restore.

Disaster Recovery System
For Cisco Unified Communications Solutions

Step4 Restore - Final Warning for Restore

Back Restore Cancel

- Status

Status: Ready

Warning

* Feature(s) FLM have been selected for restore. Select the servers on which these features need to be restored. Once the selection has been made, restore will overwrite the data on the destination server and all the existing data for the selected feature will be lost.

One-Step Restore

One-Step Restore: Perform a one-step restore of entire cluster.

File Integrity Check


Perform file integrity check using SHA1 Message Digest

Select the Servers to be restored for each feature:

FLM

CUCM10SUB CUCM10

Back Restore Cancel

 **Note:** One-Step Restore allows the restoration of the entire cluster if the Publisher has already been rebuilt or fresh installed. This option is visible ONLY if the backup file selected for restore is the backup file of the cluster and the features chosen for restore includes the feature(s) that is registered with both publisher and subscriber nodes.

Step 6. Select **Restore** to start the process and Restore status is updated.



Disaster Recovery System

For Cisco Unified Communications Solutions

Backup ▾ Restore ▾ Help ▾

Restore Status



Status

Reading backup from media

Restore details

Tar Filename: 2019-06-18-03-53-30.tar
Backup Device: NETWORK
Operation: RESTORE
Percentage Complete: 0%

Step 7. To verify the status of the restore, navigate to **Restore > Current Status**.

The screenshot shows the Disaster Recovery System interface with the following details:

- Status:** Restoring server (EUM-SERVER), please wait...
- Restore details:**
 - Tar Filename: 2019-06-18-03-53-30.tar
 - Backup Device: NETWORK
 - Operation: RESTORE
 - Percentage Complete: 50%
- Table:**

Feature	Server	Component	Status	Result	Start Time	Log File
PLM	CUCM10508	EUM-AGENT	50	SUCCESS	Thu Jun 20 03:09:51 CDT 2019	2019-06-20-03-09-29_r_cucm10508_plm_eum-agent.log
PLM	CUCM10508	EUM-SERVER	0	Active	Thu Jun 20 03:09:51 CDT 2019	

Step 8. **Restore Status** changes to **SUCCESS** when it is complete.

Disaster Recovery System
For Cisco Unified Communications Solutions

Navigation: Home | Admin | Search | Logout

Home > Restore > Help

Restore Status

Network

Status: SUCCESS: Restore Completed...

Restart Required

Please restart the server(s) [CUCMv10SUB] before performing the next restore for changes to take effect. In case of a cluster, restart the entire cluster.
 Note: If you have restored system to be in FIPS mode, please note it has been enabled, but has not taken effect yet. FIPS mode will be active only after next reboot.

Restore Details

For Filename: 2019-06-18-03-25-28.tar
 Backup Device: NETWORK
 Operation: RESTORE
 Percentage Complete: 100%

Feature	Server	Component	Status	Result **	Start Time	Log File *
RM	CUCMv10SUB	ELM-AGENT	100	SUCCESS	Thu Jun 20 03:04:14 CDT 2019	2019-06-20-03-28-29_r_cucmv10sub_plm_elm-agent.log
RM	CUCMv10SUB	ELM-SERVER	100	SUCCESS	Thu Jun 20 03:04:14 CDT 2019	2019-06-20-03-28-29_r_cucmv10sub_plm_elm-server.log

Step 9. For the changes to take effect, the system must be restarted.

```
admin:utils system restart
Do you really want to restart ?
Enter (yes/no)? yes

Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
- Service Manager shutting down services... Please Wait
Restart operation appears to be stuck

Would you like to force the Restart?
continue Restart (yes/no)?
Broadcast message from admin@CUCMv10SUB
      (unknown) at 3:19 ...

The system is going down for reboot NOW!
```

 **Tip:** Use a supported procedure in order to restart the system [Shut Down or Restart the System](#)

Step 10. In order to consult the restore procedures performed in the system, navigate to **Restore > History**.

Backup Name	Backup Type	Completed On	Status	Version	Features Backed Up	Initial Features
2017-06-08-03-13-28.tar	NETWORK	Thu Jun 08 03:13:28 CDT 2017	SUCCESS	00.0.0.1.0000-0	PLM	---


Troubleshoot

This section provides information to troubleshoot your configuration.

CUCM cluster (this involves the CUCM nodes and the Cisco Instant Messaging & Presence (IM&P) servers) must fulfil these requirements:

- Port 22 open in order to establish the communication with SFTP server
- Validated that the IPsec and Tomcat certificates are not expired.

In order to verify the validity of the certificates, navigate to **Cisco Unified OS Administration > Security > Certificate Management**

 **Note:** To regenerate ipsec and Tomcat certificates, use the [Procedure to regenerate certificates in CUCM](#)

- Ensure that the Database Replication is setup completed and does not show any errors or mismatches from the CUCM Publisher and the IM&P Publisher servers.
- Validate reachability between the servers and the SFTP Server.
- Validate that all the servers in the cluster are authenticated with the command `show network cluster`.

When Backup or Restore failures are reported and further assistance is required, this set of logs must be collected and shared with Technical Assistance Center (TAC):

- Cisco DRF Master Logs
- Cisco DRF Local Logs
- Failure logs from the DRF Current Status page
- Timestamp of the issue

Related Information

- [Supported SFTP servers](#)