

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 (CUCM)
- 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 fulfill 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 setup is 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:

- Log in 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**.

The screenshot shows the Cisco Disaster Recovery System configuration interface for a Backup Device. The page title is "Disaster Recovery System For Cisco Unified Communications Solutions". The navigation menu includes "Backup", "Restore", and "Help". The main heading is "Backup Device". Below the heading are "Save" and "Back" buttons. The "Status" section shows "Status: Ready". The "Backup device name" field contains "BackupDevice1". The "Select Destination*" section includes a "Network Directory" table with the following fields: "Host name/IP address" (10.1.89.107), "Path name" (/), "User name" (administrator), and "Password" (masked with dots). Below this table is a "Number of backups to store on Network Directory" dropdown menu set to "2". At the bottom of the form are "Save" and "Back" buttons.

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.

Disaster Recovery System
For Cisco Unified Communications Solutions

Navigation: Disaster Rec
admin | Search Documents

Backup ▾ Restore ▾ Help ▾

Scheduler

Save Set Default Disable Schedule Enable Schedule Back

Status
Status: Ready

Schedule Name
Schedule Name* DailyBackUp

Select Backup Device
Device Name* BackupDevice1

Select Features *
 CDR_CAR UCM PLM

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

Start Backup at *

Date 2019 Jun 18 Time 00 Hour 00 Minute

Frequency *
 Once
 Daily
 Weekly
 Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday
 Monthly

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

OK

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

Scheduler

Save Set Default Disable Schedule Enable Schedule Back

Status
Disabled

Schedule Name
Schedule Name* DailyBackUp

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

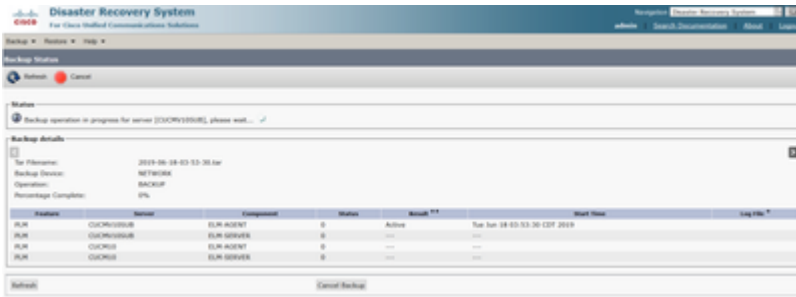


Step 9. If a Manual backup is required, navigate to **Backup > Manual Backup**.

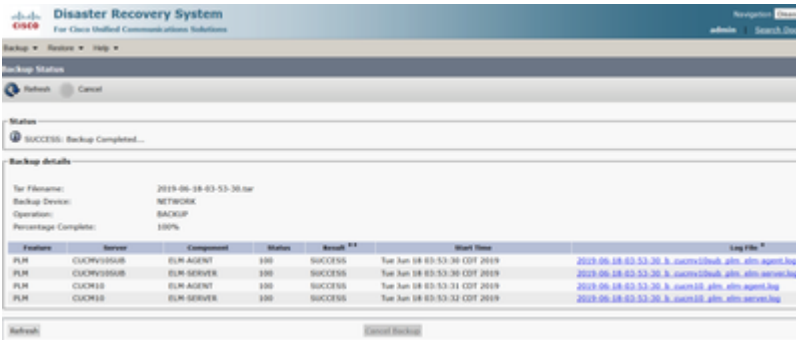
Step 10. Select the **Device Name** and check the **Features** based on your scenario.



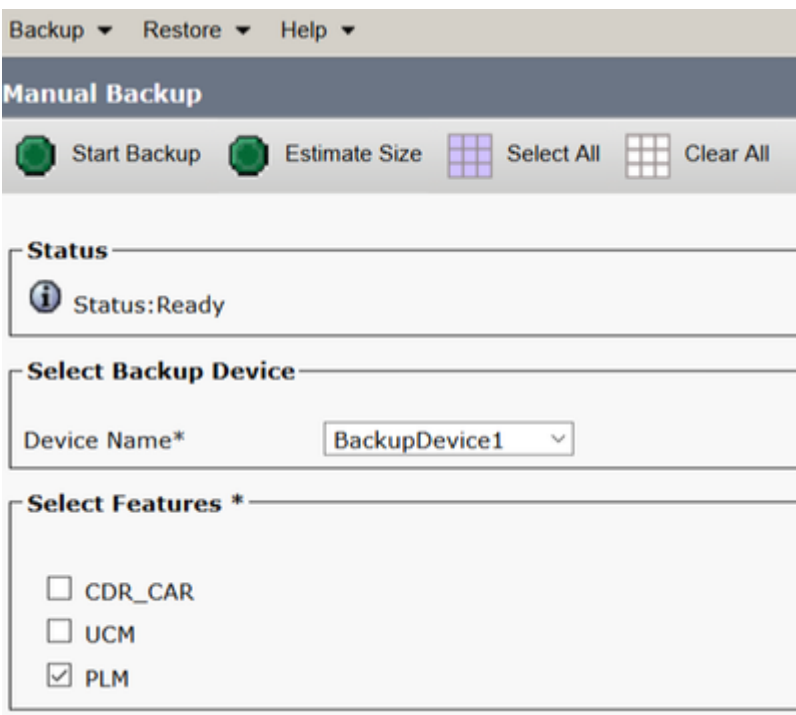
Step 11. Select **Start Backup** and the operation is displayed in progress.



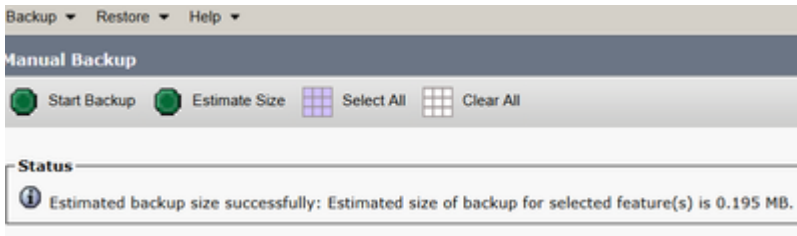
Step 12. When the manual backup is completed, the completion message is displayed.




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

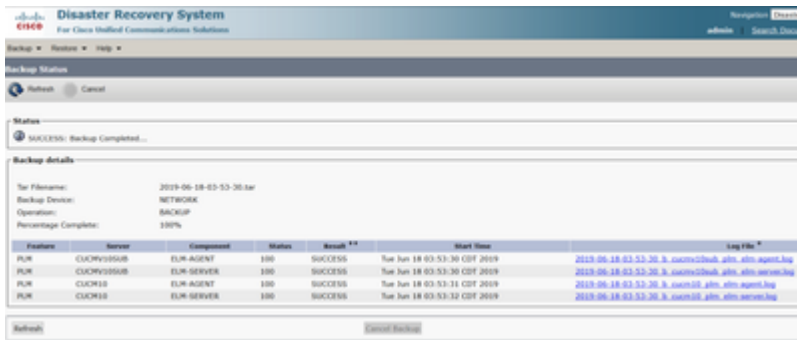


Step 14. Estimate size is displayed as shown in the image

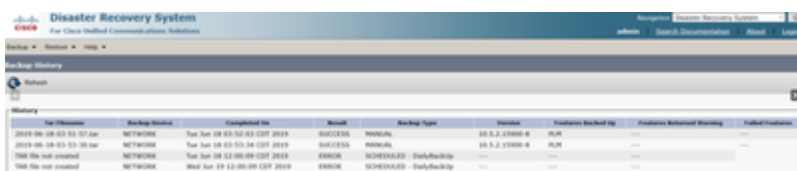


 **Note:** Estimate Size function is calculated based on previous successful backups and can vary in case configuration has been changed since the last backup.

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




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



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.

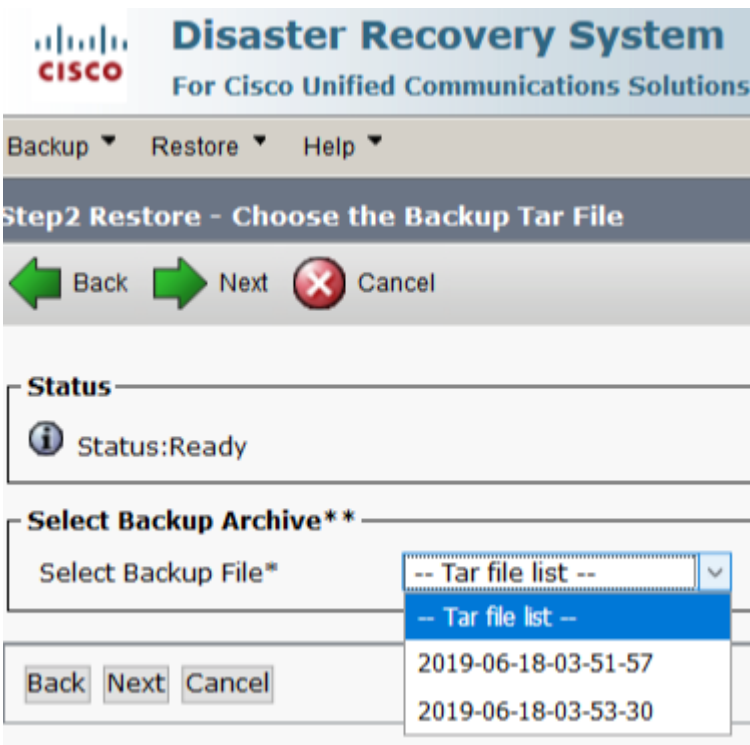
 **Note:** Backup Device (SFTP server) must already be configured in order to retrieve the tar files from it and restore the system with these files.

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**.



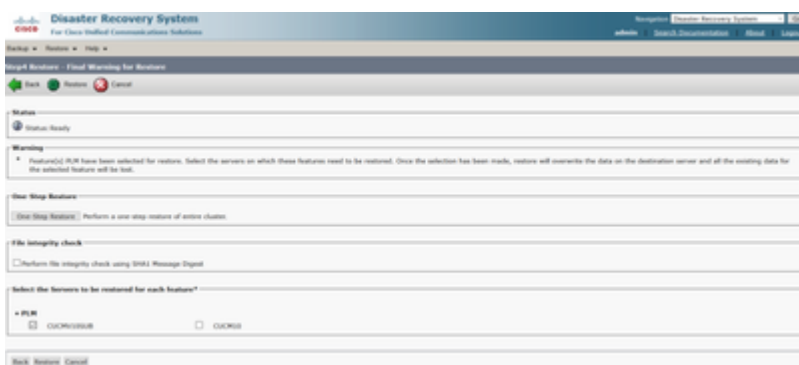
Step 3. Select the **Backup File** from the displayed list of available files as shown in the image. Selected backup file must include the information to restore.




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



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

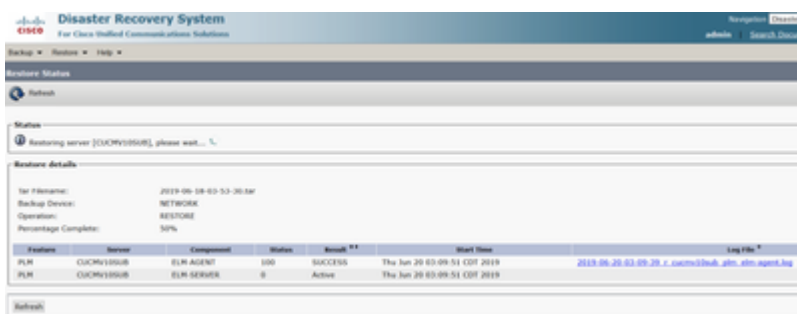


 **Note:** One-Step Restore allows the restoration of the entire cluster if the Publisher has already been rebuilt or fresh installed. This option is visible **ONLY** if the backup file selected for restore is the backup file of the cluster and the features chosen for restore includes the feature(s) that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

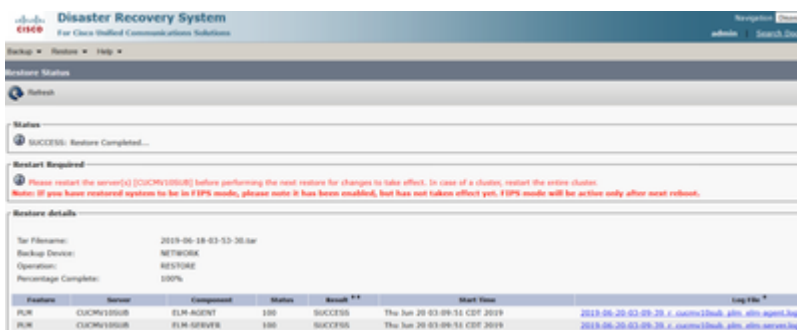
Step 6. Select **Restore** to start the process and Restore status is updated.



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



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



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**.



Troubleshoot

This section provides information to troubleshoot your configuration.

CUCM cluster (this involves the CUCM nodes and the Cisco Instant Messaging & Presence servers) must fulfill 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 setup is 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](#)