



# Disaster Recovery System Administration Guide for Cisco Unified Communications Manager Release 7.0(1)

---

This guide provides an overview of the Disaster Recovery System, describes how to use the Disaster Recovery System, and provides procedures for completing various backup-related tasks and restore-related tasks. This guide serves as a reference and procedural guide that is intended for users of Cisco Unified Communications Manager and other Cisco IP telephony applications.

This document includes the following topics:

- [What is the Disaster Recovery System?, page 2](#)
- [Quick-Reference Tables for Backup and Restore Procedures, page 3](#)
- [Supported Features and Components, page 4](#)
- [System Requirements, page 5](#)
- [How to Access the Disaster Recovery System, page 5](#)
- [Master Agent Duties and Activation, page 5](#)
- [Local Agents, page 6](#)
- [Managing Backup Devices, page 6](#)
- [Creating and Editing Backup Schedules, page 7](#)
- [Enabling, Disabling, and Deleting Schedules, page 9](#)
- [Starting a Manual Backup, page 9](#)
- [Checking Backup Status, page 10](#)
- [Restoring a Backup File, page 10](#)
- [Restoring a Cluster, page 12](#)
- [Viewing the Restore Status, page 15](#)
- [Viewing the Backup and Restore History, page 16](#)
- [Trace Files, page 17](#)
- [Command Line Interface, page 17](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2008 Cisco Systems, Inc. All rights reserved.

- [Error Messages, page 18](#)
- [Related Documentation, page 19](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 19](#)

## What is the Disaster Recovery System?

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Communications Manager Administration, provides full data backup and restore capabilities for all servers in a Cisco Unified Communications Manager cluster. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

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

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to re-configure DRS backup device and schedule.



**Caution**

Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore. For example, the Disaster Recovery System does not allow a restore from version 6.1.(1).1000-1 to version 6.1(2).1000-1, or from version 6.1.(2).1000-1 to version 6.1(2).1000-2.

When performing a system data restoration, you can choose which nodes in the cluster you want to restore.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing 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 both the Master Agent and the Local Agent on all nodes in the cluster.



**Note**

The Disaster Recovery System does not migrate data from Windows to Linux or from Linux to Linux. A restore must run on the same product version as the backup. For information on data migration from a Windows-based platform to a Linux-based platform, refer to the *Data Migration Assistant User Guide*.



**Caution**

Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

# Quick-Reference Tables for Backup and Restore Procedures

The following tables provide a quick reference for the backup and restore procedures.


**Note**

DRS backs up and restores the drfDevice.xml and drfSchedule.xml files. These backup device settings and schedule settings are restored as a part of the platform backup/restore. Once the server is restored with these files, you do not need to re-configure DRS backup device and schedule.

## Backup Quick Reference

[Table 1](#) provides a quick, high-level reference to the major steps, in chronological order, that you must perform to do a backup procedure by using the Disaster Recovery System.


**Note**

The Disaster Recovery System does not migrate data from Windows to Linux or from Linux to Linux. A restore must run on the same product version as the backup. For information on data migration from a Windows-based platform to a Linux-based platform, refer to the *Data Migration Assistant User Guide* before following the steps in [Table 1](#).

**Table 1** Major Steps for Performing a Backup Procedure

Action	Reference
Create backup devices on which to back up data.	<a href="#">“Managing Backup Devices” section on page 6</a>
Create and edit backup schedules to back up data on a schedule. <b>Note</b> Either a manual or a scheduled backup backs up the whole cluster.	<a href="#">“Creating and Editing Backup Schedules” section on page 7</a>
Enable and disable backup schedules to back up data.	<a href="#">“Enabling, Disabling, and Deleting Schedules” section on page 9</a>
Optionally, run a manual backup.	<a href="#">“Starting a Manual Backup” section on page 9</a>
Check the Status of the Backup—While a backup is running, you can check the status of the current backup job.	<a href="#">“Checking Backup Status” section on page 10</a>

## Restore Quick Reference

[Table 2](#) provides a quick, high-level reference to the major steps, in chronological order, that you must perform to do a restore procedure by using the Disaster Recovery System.

**Table 2** Major Steps for Performing a Restore Procedure

Action	Reference
Choose Storage Location—You must first choose the storage location from which you want to restore a backup file.	<a href="#">“Restoring a Backup File” section on page 10</a>
Choose the Backup File—From a list of available files, choose the backup file that you want to restore.	<a href="#">“Restoring a Backup File” section on page 10</a>
Choose Features—From the list of available features, choose the features that you want to restore.	<a href="#">“Restoring a Backup File” section on page 10</a>
Choose Nodes—If the feature was backed up from multiple nodes, you must choose the nodes that you want to restore.	<a href="#">“Restoring a Backup File” section on page 10</a>
Check the Status of the Restore—While the restore process is running, you can check the status of the current restore job.	<a href="#">“Viewing the Restore Status” section on page 15</a>

## Supported Features and Components

Disaster Recovery System can back up and restore the features and components that are shown in [table Table 3](#). For each feature that you choose, the system backs up all of its components automatically.

**Table 3** Supported Features and Components

Feature	Components
CCM—Cisco Unified Communications Manager	Cisco Unified Communications Manager database (CMDB)
	Platform
	Serviceability
	Music On Hold (MOH)
	Bulk Tool (BAT)
	Preference
	Phone device files (TFTP)
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	tct (trace collection tool)
	Call Detail Records (CDR)
	CDR Analysis and Reporting (CAR)

## System Requirements

To back up data to a remote device on the network, you must have an SFTP server configured. Cisco tests and recommends the following SFTP servers, but you may use any SFTP server:




---

**Note** Cisco does not support third-party software. Contact the SFTP vendor for support issues.

---

- Open SSH (for Unix systems)
- Cygwin (refer to <http://sshhwindows.sourceforge.net/>)
- freeFTPD (refer to <http://www.freeftpd.com/?ctt=download>)
- Titan (<http://www.titanftp.com/>)



**Note**

---

While a backup or restore is running you cannot perform any OS Administration tasks because Disaster Recovery System blocks all OS Administration requests by locking the platform API. However, this does not block most CLI commands as only the CLI based upgrade commands use the Platform API locking package.

---

## How to Access the Disaster Recovery System

To access the Disaster Recovery System, choose **Disaster Recover System** from the **Navigation** drop-down list box in the upper, right corner of Cisco Unified Communications Manager Administration window. Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.



**Note**

---

You set the Administrator username and password during Cisco Unified Communications Manager installation, and you can change the Administrator password or set up a new Administrator account by using the Command Line Interface (CLI). Refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions* for more information.

---

## Master Agent Duties and Activation

The system automatically activates the Master Agent (MA) on the server.

In a cluster, the MA ia automatically activated on all nodes in the cluster, but only the MA running on the publisher server is fully active.

## Duties That the Master Agent Performs

The Master Agent (MA) performs the following duties:

- The MA stores systemwide component registration information.
- The MA maintains a complete set of scheduled tasks in the database. When it receives updates from the user interface, the MA sends executable tasks to the applicable Local Agents, as scheduled. (Local Agents execute immediate-backup tasks without delay.)

- You access the MA through the Disaster Recovery System user interface to perform activities such as configuring backup devices, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying status of executed schedules, and performing system restoration.
- The MA stores backup data on a locally attached tape drive or a remote network location.

## Local Agents

The server also has a Local Agent to perform backup and restore functions.

Each server in a Cisco Unified Communications Manager cluster, including the server that contains the Master Agent, must have its own Local Agent to perform backup and restore functions for its server.



**Note**

---

By default, a Local Agent automatically gets activated on each node of the cluster.

---

## Duties That Local Agents Perform

The Local Agent runs backup and restore scripts on the server.

In a cluster, the Local Agent runs backup and restore scripts on each node in the cluster.

## Managing Backup Devices

Before using the Disaster Recovery System, you must configure the locations where you want the backup files to be stored. You can configure up to 10 backup devices. Perform the following steps to configure backup devices.

### Procedure

- 
- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
- The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Backup>Backup Device**. The Backup Device List window displays.
- Step 4** To configure a new backup device, click **Add New**.
- Step 5** To edit a backup device, select it in the Backup Device list, then click **Edit Selected**.
- The Backup Device window displays.
- Step 6** Enter the backup device name in the **Backup device name** field.



**Note** The backup device name may contain only alpha numeric characters, spaces ( ), dashes (-) and underscores (\_). No other characters are allowed.

**Step 7** Choose one of the following backup devices and enter the appropriate field values in the Select Destination area:

- **Tape Device**—Stores the backup file on a locally attached tape drive. Choose the appropriate tape device from the list.



**Note** You cannot span tapes or store more than one backup per tape.

- **Network Directory**—Stores the backup file on a networked drive that is accessed through an SFTP connection. Enter the following required information:
  - **Server name:** Name or IP address of the network server
  - **Path name:** Path name for the directory where you want to store the backup file
  - **User name:** Valid username for an account on the remote system
  - **Password:** Valid password for the account on the remote system
  - **Number of backups to store on Network Directory:** The number of backups to store on this network directory.



**Note** You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. The account that is used to access the SFTP server must have write permission for the selected path.

**Step 8** To update these settings, click **Save**.



**Note** After you click the **Save** button, the DRS Master Agent validates the selected backup device. If the user name, password, server name, or directory path is invalid, the save will fail.

**Step 9** To delete a backup device, select it in the Backup Device list, then click **Delete Selected**.



**Note** You cannot delete a backup device that is configured as the backup device in a backup schedule.

## Creating and Editing Backup Schedules

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.



**Caution**

Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

Perform the following steps to manage backup schedules:

**Procedure**

**Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

**Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

**Step 3** Navigate to **Backup>Scheduler**.

The Schedule List window displays.

**Step 4** Do one of the following steps to add a new schedule or edit an existing schedule

- a. To create a new schedule, click **Add New**.
- b. To configure an existing schedule, click its name in the **Schedule List** column.

The scheduler window displays.

**Step 5** Enter a schedule name in the **Schedule Name** field.



**Note** You cannot change the name of the default schedule.

**Step 6** Select the backup device in the **Select Backup Device** area.

**Step 7** Select the features to back up in the **Select Features** area. You must choose at least one feature.

**Step 8** Choose the date and time when you want the backup to begin in the **Start Backup at** area.

**Step 9** Choose the frequency at which you want the backup to occur in the **Frequency** area: Once, Daily, Weekly, or Monthly. If you choose Weekly, you can also choose the days of the week when the backup will occur.



**Tip** To set the backup frequency to Weekly, occurring Tuesday through Saturday, click **Set Default**.

**Step 10** To update these settings, click **Save**.

**Step 11** To enable the schedule, click **Enable Schedule**.

The next backup occurs automatically at the time that you set.



**Note** Ensure that all servers in the cluster are running the same version of Cisco Unified Communications Manager and are reachable through the network. Servers that are not running at the time of the scheduled backup will not be backed up.

**Step 12** To disable the schedule, click **Disable Schedule**.

# Enabling, Disabling, and Deleting Schedules

## Procedure

- 
- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
- The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Backup>Scheduler**.
- The Schedule List window displays.
- Step 4** Check the check boxes next to the schedules that you want to modify.
- To select all schedules, click **Select All**.
  - To clear all check boxes, click **Clear All**.
- Step 5** To enable the selected schedules, click **Enable Selected Schedules**.
- Step 6** To disable the selected schedules, click **Disable Selected Schedules**.
- Step 7** To delete the selected schedules, click **Delete Selected**.
- 

# Starting a Manual Backup

Follow this procedure to start a manual backup.

## Procedure

- 
- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
- The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Backup>Manual Backup**. The Manual Backup window displays.
- Step 4** Select a backup device in the **Select Backup Device** area.
- Step 5** Select the features to back up in the **Select Features** area.
- Step 6** To start the manual backup, click **Start Backup**.
-

## Checking Backup Status

You can check the status of the current backup job and cancel the current backup job. To view the backup history, see the [“Viewing the Backup and Restore History”](#) section on page 16.

### Checking the Status of the Current Backup Job

Perform the following steps to check the status of the current backup job.

#### Procedure

- 
- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.  
The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Backup>Current Status**. The Backup Status window displays.
- Step 4** To view the backup log file, click the log filename link.
- Step 5** To cancel the current backup, click **Cancel Backup**.




---

**Note** The backup cancels after the current component has completed its backup operation.

---

## Restoring a Backup File

Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco Unified Communications Manager.



#### Caution

---

Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore. For example, the Disaster Recovery System does not allow a restore from version 6.1.(1).1000-1 to version 6.1(2).1000-1, or from version 6.1(2).1000-1 to version 6.1(2).1000-2.

---

In essence, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful Cisco Unified Communications Manager database restore.

The Restore Wizard walks you through the steps that are required to restore a backup file. To perform a restore, use the procedure that follows.



#### Tip

---

To restore all servers in a cluster, see the [“Restoring a Cluster”](#) section on page 12.

---

## Procedure

**Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

**Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

**Step 3** Navigate to **Restore>Restore Wizard**. The Restore Wizard Step 1 window displays.

**Step 4** Choose the backup device from which to restore in the **Select Backup Device** area, then click **Next**.

The Restore Wizard Step 2 window displays.

**Step 5** Choose the backup file that you want to restore.



**Note** The backup filename indicates the date and time that the system created the backup file.

**Step 6** Click **Next**. The Restore Wizard Step 3 window displays.

**Step 7** Choose the features that you want to restore.



**Note** Only the features that were backed up to the file that you chose display.

**Step 8** Click **Next**. The Restore Wizard Step 4 window displays.

**Step 9** To start restoring the data, click **Restore**.

You get prompted to choose the node to restore.

**Step 10** Choose the appropriate node.



**Caution** After you choose the node to which you want the data restored, any existing data on that server gets overwritten.



**Note** If you choose the first node to restore the data, DRS automatically restores the Cisco Unified Communications Manager database on the subsequent nodes.

**Step 11** Your data gets restored on the nodes that you chose. To view the status of the restore, see the [“Viewing the Restore Status”](#) section on page 15.

**Step 12** Restart the server. For more information on restarting, see the *Cisco Unified Communications Operating System Administration Guide*.



**Note** Cisco recommends that you do not restart the first node until the subsequent nodes are restored and restarted. See Steps 15 through 17 of the [“Restoring Subsequent Cluster Nodes”](#) section on page 14 for details.



**Note** Even if you are restoring only to the first node, you must restart all nodes in the cluster. Make sure that you restart the subsequent nodes before you restart the first node.



**Note** Depending on the size of your database and the components that you choose to restore, the system can require one hour or more to restore.

## Restoring a Cluster

If a major failure or a hardware upgrade occurs, or if you want to restore your configuration and database to a last known working state, you may need to restore all nodes in the cluster. Follow these steps to restore an entire cluster:



**Note** Before you restore a cluster, make sure that all nodes in the cluster are up and communicating with the first node. You must carry out a fresh install for the nodes that are down or not communicating with first node at the time of the restore.

**Step 1** Restore the first cluster node.

See the [“Restoring the First Node” section on page 12](#).



**Note** Restoring the first node restores the whole cluster database. This may take up to several hours based on number of nodes and size of database being restored.



**Note** If a subsequent node is down or not connected to the cluster during the cluster restore, the database component restore will skip that node and proceed with the next one. You must carry out a fresh install of Cisco Unified Communications Manager on these subsequent nodes.

The following sections provide the procedures for restoring cluster nodes:

- [“Restoring the First Node” section on page 12](#)
- [“Restoring Subsequent Cluster Nodes” section on page 14](#)



**Note** You can restore the whole cluster as a single operation. The first node and the subsequent nodes do not necessarily need to be restored in two separate operations.

## Restoring the First Node

Follow this procedure to restore the first node or publisher server in the cluster.

## Procedure



### Note

Cisco recommends that you perform a fresh installation of Cisco Unified Communications Manager on the first node. For more information on installing Cisco Unified Communications Manager, see *Installing Cisco Unified Communications Manager*.



### Caution

Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore. For example, the Disaster Recovery System does not allow a restore from version 6.1.(1).1000-1 to version 6.1.(2).1000-1, or from version 6.1.(2).1000-1 to version 6.1.(2).1000-2.

- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
- The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Restore>Restore Wizard**. The Restore Wizard Step 1 window displays.
- Step 4** In the **Select Backup Device** area, choose the backup device from which to restore.
- Step 5** Click **Next**. The Restore Wizard Step 2 window displays.
- Step 6** Choose the backup file that you want to restore.



### Note

The backup filename indicates the date and time that the system created the backup file.

- Step 7** Click **Next**. The Restore Wizard Step 3 window displays.
- Step 8** Choose the features that you want to restore.



### Note

Only the features that were backed up to the file that you chose display.

- Step 9** Click **Next**. The Restore Wizard Step 4 window displays.
- Step 10** To start restoring the data, click **Restore**.
- Step 11** When you get prompted to choose the nodes to restore, choose only the first node (the publisher).
- Step 12** Your data gets restored on the publisher node. To view the status of the restore, see the [“Viewing the Restore Status” section on page 15](#).



### Note

During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Pages.




---

**Note** Restoring the first node restores the whole Cisco Unified Communications Manager database to the cluster. This may take up to several hours based on number of nodes and size of database being restored.

---

**Step 13** When the restore status indicates 100 percent, continue with the [“Restoring Subsequent Cluster Nodes” section on page 14.](#)




---

**Note** Depending on the size of your database and the components that you choose to restore, the system can require one hour or more to restore.

---

## Restoring Subsequent Cluster Nodes

Follow this procedure to restore subsequent nodes in the cluster.

### Procedure



#### Caution

---

Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco Unified Communications Manager for restore. For example, the Disaster Recovery System does not allow a restore from version 6.1.(1).1000-1 to version 6.1(2).1000-1, or from version 6.1(2).1000-1 to version 6.1(2).1000-2.

---

**Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

**Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

**Step 3** Navigate to **Restore>Restore Wizard**. The Restore Wizard Step 1 window displays.

**Step 4** In the **Select Backup Device** area, choose the backup device from which to restore.

**Step 5** Click **Next**. The Restore Wizard Step 2 window displays.

**Step 6** Choose the backup file that you want to restore.



#### Caution

---

To restore subsequent nodes in the cluster, you must choose the same backup file that you used to restore the first node.

---

**Step 7** Click **Next**. The Restore Wizard Step 3 window displays.

**Step 8** Choose the features that you want to restore.




---

**Note** Only the features that were backed up to the file that you chose display.

---

- Step 9** Click **Next**. The Restore Wizard Step 4 window displays.
- Step 10** To start restoring the data, click **Restore**.
- Step 11** When you get prompted to choose the nodes to restore, choose only the subsequent nodes.
- Step 12** Your data gets restored on the subsequent nodes. To view the status of the restore, see the [“Viewing the Restore Status” section on page 15](#).
- Step 13** Restart the server. For more information on restarting, see the *Cisco Unified Communications Operating System Administration Guide*.




---

**Note** Depending on the size of your database and the components that you choose to restore, the system can require one hour or more to restore.

---

- Step 14** When the restoration completes and the Percentage Complete field on the Restore Status window in the Disaster Recovery System shows 100 percent, begin rebooting the subsequent nodes in the cluster.
- Step 15** When all the subsequent nodes have rebooted and are running the restored version of Cisco Unified Communications Manager, reboot the first node.




---

**Note** Database replication on the subsequent nodes may take an hour or more to complete after the publisher reboots, depending on the size of the cluster.

---

- Step 16** Check the Replication Status value on all nodes by using the `utils dbreplication status` CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Solutions*. The value on each node should equal two.




---

**Tip** If replication does not set up properly, use the `utils dbreplication reset` CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

---

## Viewing the Restore Status

To check the status of the current restore job, perform the following steps:

### Procedure

- 
- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
- The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

- Step 3** Navigate to **Restore>Status**. The Restore Status window displays.
- The Status column in the Restore Status window shows the status of the restoration in progress, including the percentage of completion of the restore procedure.
- Step 4** To view the restore log file, click the log filename link.
- 

## Viewing the Backup and Restore History

Using the following procedures, you can see the last 20 backup and restore jobs:

- [Backup History](#)
- [Restore History](#)

### Backup History

Perform the following steps to view the backup history.

#### Procedure

- 
- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
- The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Backup>History**. The Backup History window displays.
- Step 4** From the Backup History window, you can view the backups that you have performed, including filename, backup device, completion date, result, and features that are backed up.




---

**Note** The Backup History window displays only the last 20 backup jobs.

---

### Restore History

Perform the following steps to view the restore history.

### Procedure

- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
- The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Restore>History**. The Restore History window displays.
- Step 4** From the Restore History window, you can view the restores that you have performed, including filename, backup device, completion date, result, and the features that were restored.



**Note** The Restore History window displays only the last 20 restore jobs.

## Trace Files

In this release of the Disaster Recovery System, trace files for the Master Agent, the GUI, and each Local Agent get written to the following locations:

- For the Master Agent, find the trace file at *platform/drf/trace/drfMA0\**
- For each Local Agent, find the trace file at *platform/drf/trace/drfLA0\**
- For the GUI, find the trace file at *platform/drf/trace/drfConfLib0\**

You can view trace files by using the command line interface. See the *Command Line Interface Reference Guide for Cisco Unified Solutions* for more information.

## Command Line Interface

The Disaster Recovery System also provides command-line access to a subset of backup and restore functions, as shown in [Table 4](#). For more information on these commands and on using the command line interface, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

**Table 4** *Disaster Recovery System Command Line Interface*

Command	Description
utils disaster_recovery backup	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, features, and nodes to restore
utils disaster_recovery status	Displays the status of ongoing backup or restore job
utils disaster_recovery show_backupfiles	Displays existing backup files

**Table 4** *Disaster Recovery System Command Line Interface (continued)*

Command	Description
utils disaster_recovery cancel_backup	Cancels an ongoing backup job
utils disaster_recovery show_registration	Displays the currently configured registration
utils disaster_recovery show_tapeid	Displays the tape identification information

## Error Messages

The Disaster Recovery System (DRS) issues alarms for various errors that could occur during a backup or restore procedure. [Table 5](#) provides a list of Cisco DRS alarms.

**Table 5** *Disaster Recovery System Alarms*

Alarm Name	Description	Explanation
CiscoDRFBackupDeviceError	DRF backup process has problems accessing device	DRS backup process encountered errors while accessing device.
CiscoDRFBackupFailure	Cisco DRF Backup process failed	DRS backup process encountered errors.
CiscoDRFBackupInProgress	Unable to start new backup while another backup is still running	DRS cannot start new backup while another backup is still running.
CiscoDRFInternalProcessFailure	DRF internal process has encountered an error.	DRS internal process encountered an error.
CiscoDRFLA2MAFailure	DRF Local Agent is not able to connect to Master Agent	DRS Local Agent cannot connect to Master Agent.
CiscoDRFLocalAgentStartFailure	DRF Local Agent was not able to start	DRS Local Agent might be down.
CiscoDRFMA2LAFailure	DRF Master Agent is not able to connect to Local Agent	DRS Master Agent cannot connect to Local Agent.
CiscoDRFMABackupComponent Failure	DRF was unable to backup at least one component.	DRS requested a component to back up its data; however, an error occurred during the backup process, and the component did not get backed up.
CiscoDRFMABackupNodeDisconnect	The node being backed up disconnected from the Master Agent prior to being fully backed up.	While the DRS Master Agent was running a backup operation on a Cisco Unified Communications Manager node, the node disconnected before the backup operation completed.
CiscoDRFMARestoreComponent Failure	DRF was unable to restore at least one component.	DRS requested a component to restore its data; however, an error occurred during the restore process, and the component did not get restored.

**Table 5** *Disaster Recovery System Alarms (continued)*

Alarm Name	Description	Explanation
CiscoDRFMARestoreNodeDisconnect	The node being restored disconnected from the Master Agent prior to being fully restored.	While the DRS Master Agent was running a restore operation on a Cisco Unified Communications Manager node, the node disconnected before the restore operation completed.
CiscoDRFMasterAgentStartFailure	DRF Master Agent was not able to start	DRS Master Agent might be down.
CiscoDRFNoRegisteredComponent	No registered components available, backup failed	DRS backup failed because no registered components are available.
CiscoDRFNoRegisteredFeature	No feature selected for backup	No feature got selected for backup.
CiscoDRFRestoreDeviceError	DRF restore process has problems accessing device	DRS restore process cannot read from device.
CiscoDRFRestoreFailure	DRF restore process failed	DRS restore process encountered errors.
CiscoDRFSftpFailure	DRF sftp operation has errors	Errors exist in DRS SFTP operation.

## Related Documentation

Refer to the *Cisco Unified Communications Manager Documentation Guide* to learn about the documentation for Cisco Unified Communications Manager.

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

## Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at [http://www.access.gpo.gov/bis/ear/ear\\_data.html](http://www.access.gpo.gov/bis/ear/ear_data.html).

---

CCDE, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0803R)

Copyright © 2008.Cisco Systems, Inc. All rights reserved.