



# Disaster Recovery System Administration Guide Release 5.0(4)

---

The *Disaster Recovery System Administration 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 CallManager and other Cisco IP telephony applications.

This document includes the following topics:

- [What is the Disaster Recovery System?](#)
- [Quick-Reference Tables for Backup and Restore Procedures](#)
- [Supported Features and Components](#)
- [System Requirements](#)
- [How to Access the Disaster Recovery System](#)
- [Master Agent Duties and Activation](#)
- [Local Agents](#)
- [Configuring Features to Back Up](#)
- [Configuring a Storage Location](#)
- [Configuring a Backup Schedule](#)
- [Starting a Manual Backup](#)
- [Checking Backup Status](#)
- [Restoring a Backup File](#)
- [Restoring a Cluster](#)
- [Viewing the Backup and Restore History](#)
- [Trace Files](#)
- [Command Line Interface](#)
- [Error Messages](#)
- [Related Documentation](#)



---

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

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

# What is the Disaster Recovery System?

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified CallManager 5.0 Administration, provides full data backup and restore capabilities for all servers in a Cisco Unified CallManager cluster. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups. DRS supports only one backup schedule.

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

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 all the 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*.

---

# Quick-Reference Tables for Backup and Restore Procedures

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

## 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
Configure Features to Back Up—Before you can run a backup job, you must choose the features that you want to back up.	<a href="#">“Configuring Features to Back Up” section on page 6</a>
Configure a Storage Location—You must choose the physical location where you want to store the backup file.	<a href="#">“Configuring a Storage Location” section on page 7</a>
Configure a Scheduled Backup or start a Manual Backup—You can perform an immediate manual backup or configure a regularly scheduled backup for the cluster. <b>Note</b> Either a manual or a scheduled backup backs up the whole cluster.	To configure a scheduled backup, see <a href="#">“Configuring a Backup Schedule” section on page 8</a> . To start a manual backup, see <a href="#">“Starting a Manual Backup” section on page 8</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 9</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 14</a>

## Supported Features and Components

For the Cisco Unified CallManager 5.0 release, you can back up and restore the Features and Subcomponents that are shown in the following table. For each feature that you choose, the system backs up all of its subcomponents automatically.

**Table 3** Supported Features and Components

Feature	Components
CCM—Cisco Unified CallManager	Cisco Unified CallManager (version 5.0) database (CMDB)
	Platform
	Serviceability
	Music On Hold (MOH)
	Cisco Emergency Responder (CER)
	Bulk Tool (BAT)
	Preference
	Phone device files (TFTP)
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	tct (trace collection tool)

**Table 3**      **Supported Features and Components (continued)**

Feature	Components
CDR_CAR	Call Detail Records (CDR)
	CDR Analysis and Reporting (CAR)

## System Requirements

Make sure that Cisco Unified CallManager 5.0 is running on all servers in the cluster.

## How to Access the Disaster Recovery System

To access the Disaster Recovery System, choose **Disaster Recover System** from the **Navigation** menu in the upper, right corner of Cisco Unified CallManager Administration window. Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Platform Administration.



### Note

You set the Administrator username and password during Cisco Unified CallManager 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 *Cisco Unified Communications Operating System Administration Guide* for more information.

## Master Agent Duties and Activation

The system automatically activates the Master Agent on all nodes in the cluster, but only the Master Agent 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 Cisco Unified CallManager 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 scheduling backups, adding a new backup task for a specific server or a defined cluster, updating or reviewing an existing entry, displaying status of executed tasks, and performing system restoration.
- The MA stores backup sets on a locally attached tape drive or a remote network location.

# Local Agents

Each server in a Cisco Unified CallManager 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 each node in the cluster.

## Configuring Features to Back Up

Before you can schedule or start a backup job, you must configure the features that you want to back up.

**Note**

---

Changing a backup feature changes it for both manual and scheduled backups.

---

Perform the following steps to choose the features that you want to back up.

**Procedure**

- 
- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager 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 Platform Administration.
  - Step 3** Navigate to **Backup>Configure Features**.
  - Step 4** From the list of available features, choose the feature or features that you want to include in the backup and click **Save**. You must choose at least one feature.
  - Step 5** Continue with the next procedure for configuring a storage location.
-

# Configuring a Storage Location

Before using the Disaster Recover System, you must configure the location where you want the backup file to be stored. Perform the following steps to configure the storage location.

## Procedure

**Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager 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 Platform Administration.

**Step 3** Navigate to **Backup>Storage Location**. The Storage Location window displays.



**Note** You can configure the number of backup sets that are stored on a network directory.

**Step 4** Choose one of the following storage destination options and enter the appropriate field values:

- **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



**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 5** To update these settings, click **Save**.



**Note** For network directory backups, after you click the Save button, the DRS Master Agent will validate the selected SFTP server. If the user name, password, server name, or directory path is invalid, the save will fail.

**Step 6** Continue with either a manual or a scheduled backup.

## Configuring a Backup Schedule

You can schedule a backup to start at a specified date and time and configure it either to run once or at a specified frequency. The system automatically backs up the features that you chose on the **Configure Features** menu. Perform the following steps to configure a backup schedule.

### Procedure

- 
- Step 1** Navigate to the Disaster Recovery System. If you are currently in Cisco Unified CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager 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 Platform Administration.
- Step 3** Navigate to **Backup>Scheduler**. The Scheduler window displays.
- Step 4** If the Scheduler is not enabled, click **Enable Scheduler**.
- Step 5** Choose the date and time when you want the backup to begin.
- Step 6** Choose the frequency at which you want the backup to occur: 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 7** To update these settings, click **Save**.
- Step 8** 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 CallManager and are reachable through the network. Servers that are not running at the time of the scheduled backup will not be backed up.

---

## Starting a Manual Backup

You can manually start a backup of the features that you chose on the **Configure Features** menu. Perform the following steps to start a manual backup.

### Procedure

- 
- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager 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 Platform Administration.
- Step 3** Navigate to **Backup>Manual Backup**. The Manual Backup window displays.
- Step 4** Make sure the features that you want to back up are chosen. To choose other features, see the [“Configuring Features to Back Up” section on page 6](#).




---

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

---

- Step 5** To begin the manual backup, click **Start Backup**.
  - Step 6** Make sure that you have configured the backup storage location. See the [“Configuring a Storage Location” section on page 7](#).
- 

## 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 14](#).

### 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 CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager 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 Platform 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

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 11](#).



**Caution**

Before you restore Cisco Unified CallManager, ensure that the Cisco Unified CallManager version that is installed on the server matches the version of the backup file that you want to restore.

## Procedure

**Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager 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 Platform Administration.

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

**Step 4** Choose the storage location from which you want to restore the file and enter the following required information for the chosen storage location:

- **Tape Device**—Restores the backup file from a locally attached tape drive. Choose the appropriate tape device from the list.
- **Network Directory**—Restores the backup file from 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 from which you want to restore the backup file
  - **User name:** Valid username for an account on the remote system
  - **Password:** Valid password for the account on the remote system

**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**.  
You get prompted to choose the node to restore.

**Step 11** 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.

**Step 12** 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 14](#).

**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.

## Restoring a Cluster

If a major failure or a hardware upgrade occurs, you may need to restore all nodes in the cluster. To restore a whole cluster, you must first restore the publisher server and then restore the subsequent nodes. The following procedures provide the steps for the full-cluster restore process.

### Restoring the First Node

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

#### Procedure

**Step 1** Perform a fresh installation of Cisco Unified CallManager 5.0 on the first node or publisher server. For more information on installing Cisco Unified CallManager, see *Installing Cisco Unified CallManager*.



**Caution** Before you restore Cisco Unified CallManager, ensure that the Cisco Unified CallManager version that is installed on the server matches the version of the backup file to restore.

**Step 2** Navigate to the Disaster Recovery System. Log in to Cisco Unified CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

**Step 3** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Platform Administration.

**Step 4** Navigate to **Restore>Restore Wizard**. The Restore Wizard Step 1 window displays.

- Step 5** Choose the storage location from which you want to restore the file and enter the following required information for the chosen storage location:
- **Tape Device**—Restores the backup file from a locally attached tape drive. Choose the appropriate tape device from the list.
  - **Network Directory**—Restores the backup file from 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 from which you want to restore the backup file
    - **User name:** Valid username for an account on the remote system
    - **Password:** Valid password for the account on the remote system

**Step 6** Click **Next**. The Restore Wizard Step 2 window displays.

**Step 7** 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 8** Click **Next**. The Restore Wizard Step 3 window displays.

**Step 9** Choose the features that you want to restore.




---

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

---

**Step 10** Click **Next**. The Restore Wizard Step 4 window displays.

**Step 11** To start restoring the data, click **Restore**.

**Step 12** When you get prompted to choose the nodes to restore, choose only the first node (the publisher).

**Step 13** Your data gets restored on the publisher node. To view the status of the restore, see the [“Viewing the Restore Status”](#) section on page 14.




---

**Note** During the restore process, do not perform any tasks with Cisco Unified CallManager Administration or User Pages.

---

**Step 14** 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 15** After the first node restarts, continue with the [“Restoring Subsequent Cluster Nodes”](#) section on page 13.

---

## Restoring Subsequent Cluster Nodes

Follow this procedure to restore subsequent nodes in the cluster.

### Procedure

**Step 1** Perform a fresh installation of Cisco Unified CallManager 5.0 on the subsequent nodes. For more information on installing Cisco Unified CallManager, see *Installing Cisco Unified CallManager*.



#### Caution

Before you restore Cisco Unified CallManager, ensure that the Cisco Unified CallManager version that is installed on the server matches the version of the backup file to restore.

**Step 2** Navigate to the Disaster Recovery System. Log in to Cisco Unified CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager Administration window, and click **Go**.

The Disaster Recovery System Logon window displays.

**Step 3** Log in to the Disaster Recovery System by using the same Administrator username and password that you use for Platform Administration.

**Step 4** Navigate to **Restore>Restore Wizard**. The Restore Wizard Step 1 window displays.

**Step 5** Choose the storage location from which you want to restore the file and enter the following required information for the chosen storage location:

- **Tape Device**—Restores the backup file from a locally attached tape drive. Choose the appropriate tape device from the list.
- **Network Directory**—Restores the backup file from 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 from which you want to restore the backup file
  - **User name**: Valid username for an account on the remote system
  - **Password**: Valid password for the account on the remote system

**Step 6** Click **Next**. The Restore Wizard Step 2 window displays.

**Step 7** 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 8** Click **Next**. The Restore Wizard Step 3 window displays.

**Step 9** Choose the features that you want to restore.



#### Note

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

**Step 10** Click **Next**. The Restore Wizard Step 4 window displays.

**Step 11** To start restoring the data, click **Restore**.

- Step 12** When you get prompted to choose the nodes to restore, choose only the subsequent nodes.
- Step 13** Your data gets restored on the subsequent nodes. To view the status of the restore, see the [“Viewing the Restore Status” section on page 14](#).
- Step 14** 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.

---

## 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 CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager 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 Platform Administration.
- Step 3** Navigate to **Restore>Status**. The Restore Status window displays.
- 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 CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager 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 Platform 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, storage location, 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 CallManager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified CallManager 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 Platform 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, storage location, 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, the trace file is *platform/drf/trace/drfMA0\**
- For each Local Agent, the trace file is *platform/drf/trace/drfLA0\**
- For the GUI, the trace file is *platform/drf/trace/drfConfLib0\**

You can view trace files by using the command line interface. See the *Cisco Unified Communications Operating System Administration Guide* 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 *Cisco Unified Communications Operating System Administration Guide*.

**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 configure_features	Configures the features to back up.
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
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	DRF backup process encountered errors while accessing device.
CiscoDRFBackupFailure	Cisco DRF Backup process failed	DRF backup process encountered errors.
CiscoDRFBackupInProgress	Unable to start new backup while another backup is still running	DRF cannot start new backup while another backup is still running.
CiscoDRFInternalProcessFailure	DRF internal process has encountered an error.	DRF internal process encountered an error.
CiscoDRFLA2MAFailure	DRF Local Agent is not able to connect to Master Agent	DRF Local Agent cannot connect to Master Agent.
CiscoDRFLocalAgentStartFailure	DRF Local Agent was not able to start	DRF Local Agent might be down.
CiscoDRFMA2LAFailure	DRF Master Agent is not able to connect to Local Agent	DRF Master Agent cannot connect to Local Agent.
CiscoDRFMABackupComponent Failure	DRF was unable to backup at least one component.	DRF requested a component to back up its data; however, an error occurred during the backup process, and the component was not backed up.
CiscoDRFMABackupNodeDisconnect	The node being backed up disconnected from the Master Agent prior to being fully backed up.	The DRF Master Agent was running a backup operation on a Cisco Unified CallManager node, and the node disconnected before the backup operation completed.
CiscoDRFMARestoreComponent Failure	DRF was unable to restore at least one component.	DRF requested a component to restore its data; however, an error occurred during the restore process, and the component was not restored.
CiscoDRFMARestoreNodeDisconnect	The node being restored disconnected from the Master Agent prior to being fully restored.	The DRF Master Agent was running a restore operation on a Cisco Unified CallManager node, and the node disconnected before the restore operation completed.
CiscoDRFMasterAgentStartFailure	DRF Master Agent was not able to start	DRF Master Agent might be down.
CiscoDRFNoRegisteredComponent	No registered components available, backup failed	DRF backup failed because no registered components are available.
CiscoDRFNoRegisteredComponent	No feature selected for backup	No feature got selected for backup.
CiscoDRFRestoreDeviceError	DRF restore process has problems accessing device	DRF restore process cannot read from device.
CiscoDRFRestoreFailure	DRF restore process failed	DRF restore process encountered errors.
CiscoDRFSftpFailure	DRF sftp operation has errors	DRF SFTP operation has errors.

## Related Documentation

Refer to the following documentation about related Cisco IP Telephony applications and products:

- *Cisco Unified CallManager Installation Guide*
- *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Data Migration Assistant User Guide*
- *Cisco Unified Communications Operating System Administration Guide*
- Any release notes, installation/upgrade, and configuration guides for the applications that you want to integrate with Cisco Unified CallManager.

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

## Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

## Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



#### Note

Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



#### Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:  
<http://www.cisco.com/offer/subscribe>
- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:  
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:  
<http://www.cisco.com/univercd/cc/td/doc/abtunibd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

---

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0609R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

