



Disaster Recovery System Administration Guide for Cisco Unified Mobility Advantage

Revised Date: December 1, 2009

- [What is the Disaster Recovery System?, page 2](#)
- [Quick-Reference Tables for Backup and Restore Procedures, page 2](#)
- [System Requirements, page 3](#)
- [How to Access the Disaster Recovery System, page 4](#)
- [Master Agent Duties and Activation, page 4](#)
- [Local Agents, page 5](#)
- [Preloaded Backup Servers, page 5](#)
- [Managing Backup Devices, page 5](#)
- [Creating and Editing Backup Schedules, page 6](#)
- [Enabling, Disabling, and Deleting Schedules, page 7](#)
- [Starting a Manual Backup, page 8](#)
- [Checking Backup Status, page 8](#)
- [Restoring Cisco Unified Mobility Advantage Data From a Backup, page 9](#)
- [Viewing the Restore Status, page 10](#)
- [Viewing the Backup and Restore History, page 11](#)
- [Trace Files, page 12](#)
- [Command Line Interface, page 12](#)
- [Error Messages, page 13](#)
- [Documentation Updates and Related Documentation, page 14](#)



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

What is the Disaster Recovery System?

The Disaster Recovery System (DRS), which can be invoked from the Cisco Unified Mobility Advantage server, provides full data backup and restore capabilities. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

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 reconfigure DRS backup device and schedule.



Caution

Before you restore Cisco Unified Mobility Advantage, ensure that the Cisco Unified Mobility Advantage version that is installed on the server exactly matches the version of the backup file that you want to restore, including the release number of any service update or engineering special. The Disaster Recovery System supports only matching versions of Cisco Unified Mobility Advantage for restore. For example, the Disaster Recovery System does not allow a restore from version 7.0(1) to version 7.0(2).

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.



Caution

Schedule backups during off-peak hours to avoid 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 get restored as a part of the platform backup/restore. After the server is restored with these files, you do not need to reconfigure 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.

Table 1 *Major Steps for Performing a Backup Procedure*

Action	Reference
Create backup devices on which to back up data.	“Managing Backup Devices” section on page 5
Create and edit backup schedules to back up data on a schedule.	“Creating and Editing Backup Schedules” section on page 6
Enable and disable backup schedules to back up data.	“Enabling, Disabling, and Deleting Schedules” section on page 7
Optionally, run a manual backup.	“Starting a Manual Backup” section on page 8
Check the Status of the Backup—While a backup is running, you can check the status of the current backup job.	“Checking Backup Status” section on page 8

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.	“Restoring Cisco Unified Mobility Advantage Data From a Backup” section on page 9
Choose the Backup File—From a list of available files, choose the backup file that you want to restore.	“Restoring Cisco Unified Mobility Advantage Data From a Backup” section on page 9
Choose Features— Specify that this is a Cisco Unified Mobility Advantage data file.	“Restoring Cisco Unified Mobility Advantage Data From a Backup” section on page 9
Check the Status of the Restore—While the restore process is running, you can check the status of the current restore job.	“Viewing the Restore Status” section on page 10

System Requirements

To back up data to a remote device on the network, you must have an SFTP server that is configured. Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to <http://sshtwindows.sourceforge.net/>)
- Cygwin (refer to <http://www.cygwin.com/>)

- Titan (refer to <http://www.titanftp.com/>)



Note Note: For issues with third-party products, contact the third-party vendor for support



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.



Tip Schedule backups during periods when you expect less network traffic.

How to Access the Disaster Recovery System

To access the Disaster Recovery System, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the Cisco Unified Mobility Advantage 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 Mobility Advantage 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* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cli_ref/7_1_2/cli_ref_712.html for more information.

Master Agent Duties and Activation

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

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 an XML file. The MA updates this file when it receives updates of schedules 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 has a Local Agent to perform backup and restore functions.

Duties That Local Agents Perform

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


Preloaded Backup Servers

To speed recovery, you can preload Cisco Unified Mobility Advantage on a server and keep it offline unless it is needed. The backup server hardware must be able to support the number of users on the primary server. The software version must exactly match the version of the active installation, including any service updates and engineering specials. Install the backup server with the same hostname and IP address as the active server. Before you make the backup server active, be sure the failed server is shut down or not on the network.

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** In the Cisco Unified Mobility Advantage window, in the Navigation list, click **Disaster Recovery System**, 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 alphanumeric characters, spaces (), dashes (-) and underscores (_). Do not use any other characters.
-
- Step 7** Choose **Network Directory** as the backup destination.

You will store the backup file on a network drive that is accessed through an SFTP connection.

Step 8 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. If you are using DRS to back up other applications (such as Cisco Unified Communications Manager, Cisco Unified Presence), you must create a separate directory for each server.
- **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. Specify a value high enough to ensure that the backups you want to keep are not overwritten.



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 9 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 10 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.




Note DRS Scheduler does not automatically adjust after Daylight Saving Time (DST) changes—Neither the change to DST, nor the change back to Standard time.

For example, assume that today is the Friday before DST time takes effect. The DST time change takes place at 2 a.m. Sunday, when the time gets advanced from 2 to 3 a.m. If you schedule a backup to occur at 10 a.m. on that Sunday, the upgrade will actually occur at 11 a.m. Sunday.


Adjust the backup schedule time after every DST change by updating the scheduled start time as described in the following procedure.

Perform the following steps to manage backup schedules:

Procedure

-
- Step 1** In the Cisco Unified Mobility Advantage window, in the Navigation list, click **Disaster Recovery System**, 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 **CUMA** in the **Select Features** area.
- 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.
- Step 12** To disable the schedule, click **Disable Schedule**.
-

Enabling, Disabling, and Deleting Schedules

Procedure

-
- Step 1** In the Cisco Unified Mobility Advantage window, in the Navigation list, click **Disaster Recovery System**, 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.

Before You Begin

Make sure you have configured a location where you want your backup files to be stored. See the [“Managing Backup Devices” section on page 5](#).

Procedure

-
- Step 1** In the Cisco Unified Mobility Advantage window, in the Navigation list, click **Disaster Recovery System**, 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 **CUMA** 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 11](#).



Caution

Be aware that if the backup to the remote server is not completed within 20 hours, the backup session will time out. You will then need to begin a fresh backup.

Checking the Status of the Current Backup Job

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

Procedure

-
- Step 1** In the Cisco Unified Mobility Advantage window, in the Navigation list, click **Disaster Recovery System**, 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 completes its backup operation.

Restoring Cisco Unified Mobility Advantage Data From a Backup

Before You Begin

- An existing backup is required.
- You must restore to a server that can accommodate the number of users on your primary server. For example, you cannot restore to a Media Convergence Server 7825 series if your primary server is a 7845 series server.
- If you preloaded a backup server with Cisco Unified Mobility Advantage, make sure your failed server is shut down or not on the network.
- This server must be on the network and accessible using SFTP. The SFTP path must exist prior to the backup.
- You must configure the backup device on the new server. This backup device is the location on which your backup is located. See [Managing Backup Devices, page 5](#).

Procedure

-
- Step 1** Install on the new server the *identical* operating system and Cisco Unified Mobility Advantage version as your original Cisco Unified Mobility Advantage server, including the release number of any service update or engineering special. You must assign this server the same IP address as your original Cisco Unified Mobility Advantage server.
- Step 2** Access the Admin Portal page but do NOT sign into Cisco Unified Mobility Advantage.
- Step 3** Select **Disaster Recovery System** from the list box at the top right of the page.

- Step 4** Select **Go**.
 - Step 5** Sign in with the platform credentials you entered while installing Cisco Unified Mobility Advantage.
 - Step 6** Select **Restore > Restore Wizard**.
 - Step 7** Select the **Backup Device** you named when setting up your backups.
 - Step 8** Select **Next**.
 - Step 9** Select the date and time of the backup file from which you want to restore.
 - Step 10** Select **Next**.
 - Step 11** Select **CUMA** for Select Features.
 - Step 12** Select **Next**.
 - Step 13** Select the original server name as the server to restore.
 - Step 14** Select **Restore**.
 - Step 15** Wait until the restore status shows **Success**.
 - Step 16** Select **Cisco Unified OS Administration** from the list box at the top right of the window.
 - Step 17** Sign in to the Cisco Unified OS Administration portal.
 - Step 18** Choose **Settings > Version**.
 - Step 19** Select **Restart**.
-

Related Topics

- [Preloaded Backup Servers, page 5](#)

Viewing the Restore Status

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

Procedure

-
- Step 1** In the Cisco Unified Mobility Advantage window, in the Navigation list, click **Disaster Recovery System**, 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** In the Cisco Unified Mobility Advantage window, in the Navigation list, click **Disaster Recovery System**, 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** In the Cisco Unified Mobility Advantage window, in the Navigation list, click **Disaster Recovery System**, 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 active partition:

- For the Master Agent, find the trace file at `/common/log/taos-log-a/platform/drf/trace/drfMA0*`
- For each Local Agent, find the trace file at `/common/log/taos-log-a/platform/drf/trace/drfLA0*`
- For the GUI, find the trace file at `/common/log/taos-log-a/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* at

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cli_ref/7_1_2/cli_ref_712.html 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 3](#). For more information on these commands and on using the command line interface, see the *Command Line Interface Reference Guide for Cisco Unified Solutions* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cli_ref/7_1_2/cli_ref_712.html.

Table 3 **Disaster Recovery System Command Line Interface**

Command	Description
<code>utils disaster_recovery backup</code>	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface
<code>utils disaster_recovery restore</code>	Starts a restore and requires parameters for backup location, filename, features, and server to restore
<code>utils disaster_recovery status</code>	Displays the status of ongoing backup or restore job
<code>utils disaster_recovery show_backupfiles</code>	Displays existing backup files
<code>utils disaster_recovery cancel_backup</code>	Cancels an ongoing backup job
<code>utils disaster_recovery show_registration</code>	Displays the currently configured registration
<code>utils disaster_recovery show_tapeid</code>	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 4](#) provides a list of Cisco DRS alarms.

Table 4 *Disaster Recovery System Alarms*

Alarm Name	Description	Explanation
CiscoDRFBackupDeviceError	DRF backup process has problems accessing device.	DRS backup process encountered errors while it was accessing device.
CiscoDRFBackupFailure	Cisco DRF Backup process failed.	DRS backup process encountered errors.
CiscoDRFBackupInProgress	New backup cannot start while another backup is still running	DRS cannot start new backup while another backup is still running.
CiscoDRFInternalProcessFailure	DRF internal process encountered an error.	DRS internal process encountered an error.
CiscoDRFLA2MAFailure	DRF Local Agent cannot connect to Master Agent.	DRS Local Agent cannot connect to Master Agent.
CiscoDRFLocalAgentStartFailure	DRF Local Agent does not start.	DRS Local Agent might be down.
CiscoDRFMA2LAFailure	DRF Master Agent does not connect to Local Agent.	DRS Master Agent cannot connect to Local Agent.
CiscoDRFMABackupComponent Failure	DRF cannot back up 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 server that is being backed up disconnected from the Master Agent prior to being fully backed up.	While the DRS Master Agent was running a backup operation, the server being backed up disconnected before the backup operation completed.
CiscoDRFMARestoreComponent Failure	DRF cannot 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.
CiscoDRFMARestoreNodeDisconnect	The server that is being restored disconnected from the Master Agent prior to being fully restored.	While the DRS Master Agent was running a restore operation, the server being restored disconnected before the restore operation completed.
CiscoDRFMasterAgentStartFailure	DRF Master Agent did not start.	DRS Master Agent might be down.
CiscoDRFNoRegisteredComponent	No registered components are available, so backup failed.	DRS backup failed because no registered components are available.
CiscoDRFNoRegisteredFeature	No feature got 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.

Table 4 **Disaster Recovery System Alarms (continued)**

Alarm Name	Description	Explanation
CiscoDRFSecurityViolation	DRF system detected a malicious pattern that could result in a security violation.	The DRF Network Message contains a malicious pattern that could result in a security violation like code injection or directory traversal. DRF Network Message has been blocked.
CiscoDRFUnknownClient	DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.	The DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.

Documentation Updates and Related Documentation

For the most current version of this documentation, visit

http://www.cisco.com/en/US/products/ps7270/prod_maintenance_guides_list.html

Refer to the *Documentation Guide for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator* at

http://www.cisco.com/en/US/products/ps7270/products_documentation_roadmaps_list.html to learn about the documentation for Cisco Unified Mobility Advantage.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

Copyright © 2009 Cisco Systems, Inc. All rights reserved.

