Backing Up and Restoring Data

Last Updated: December 2, 2010

Note Setting up a backup server is part of the initial configuration process. If you have not already done this, see the Initial Configuration Tasks.

- About Backing Up and Restoring Data, page 131
- Restrictions for Backing Up and Restoring Data, page 132
- Setting Backup Parameters, page 132
- Backing Up Files, page 134
- Restoring Files, page 136
- Backup and Restore Using SFTP, page 139
- Backup Server Authentication Using a SSH Host Key, page 140
- Encrypting and Signing of Backup Content on the Server, page 143
- Configuring Scheduled Backup Jobs, page 144

About Backing Up and Restoring Data

Cisco UMG backup and restore functions use an FTP server to store and retrieve data. The backup function copies the files from the Cisco UMG module to the FTP server and the restore function copies the files from the FTP server to the Cisco UMG application. The FTP server can reside anywhere in the network as long as the backup and restore functions can access it with an IP address or hostname.

We recommend that you back up your configuration files whenever you make changes to the system or application files. Do backups regularly to preserve configuration data.

The system supports the following types of backup:

- All files (backs up configuration and data)
- Only data files (includes dynamic data such as local endpoint IDs, mailboxes, and system distribution lists)

Note We strongly discourage doing the “only data” type of backup and restore because of its potential to introduce inconsistency between configuration and data files.

- Only configuration files (includes the local messaging gateway ID, messaging gateway peers, manually configured endpoints, registration credentials, and NAT data)

Restrictions for Backing Up and Restoring Data

- Backing up and restoring both require offline mode, so we recommend performing this task when call traffic is least impacted. Offline mode terminates message forwarding and directory exchange.
- Cisco UMG does not support the following backup and restore capabilities:
  - Centralized message storage arrangement. Cisco UMG backup files cannot be used or integrated with other message stores.
  - Selective backup and restore. Only full backup and restore functions are available. Individual messages or other specific data can be neither stored nor retrieved.
- If you delete an endpoint, then do a system restore, the update will erase the information that the endpoint was deleted. You must reset it from the endpoint's primary messaging gateway.

Setting Backup Parameters

The backup parameters define the FTP server to use for storing Cisco Unified Messaging Gateway backup files and the number of backups that are stored before the system deletes the oldest one.

All Cisco Unified Messaging Gateway backup files are stored on the specified server. You can copy the backup files to other locations or servers, if necessary.

Cisco Unified Messaging Gateway automatically assigns an ID to each successful backup. Use this backup ID to restore the backup.

Prerequisites

- Verify that the backup server is configured.
- Verify that an FTP administrator or other user who can log in to the FTP server has full permission on the FTP server, such as read, write, overwrite, create, and delete permissions for files and directories.

Required Data for This Procedure

- Number of revisions to save before the oldest backup is written over
- FTP server URL
- User ID and password of the FTP server login

SUMMARY STEPS

1. **config t**
2. **backup** {**revisions** *number* | **server url** *ftp-url* **username** *ftp-username* **password** *ftp-password*}
3. **exit**

4. **show backup**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** `umg-1# config t`	Enters configuration mode.

Step 2	**backup** {**revisions** *number* | **server url** *ftp-url* **username** *ftp-username* **password** *ftp-password*}
	
	Example:
	`umg-1(config)# backup server url ftp://main/backups username "admin" password "wxyz"`
	`umg-1(config)# backup server url ftp://172.168.10.10/backups username "admin" password "wxyz"`
	`umg-1(config)# backup revisions 5`
		Sets the backup parameters.
		• **server url**—The *ftp-url* value is the URL to the network FTP server where the backup files will be stored. The *ftp-username* and *ftp-password* values are the user ID and password for the network FTP server.
		Note The backup server must be configured before the backup revisions can be configured.
		• **revisions**—The number of backup files that will be stored. When this number is reached, the system deletes the oldest stored file.
		In the example, **main** is the hostname of the FTP server and **backups** is the directory where backup files are stored.

Step 3	**exit** **Example:** `umg-1(config)# exit`	Exits configuration mode.
Step 4	**show backup** **Example:** `umg-1# show backup`	Displays the backup server configuration information, including the FTP server URL and the number of revisions.

Examples

The following example configures a backup server and displays the **show backup** output:

```
umg-1# config t
umg-1#(config)# backup server url ftp://172.16.0.0/backups username admin password voice
umg-1#(config)# backup revisions 10
umg-1#(config)# exit
umg-1#

umg-1# show backup
Server URL:                          ftp://172.16.0.0/backups
User Account on Server:              admin
Number of Backups to Retain:         10
umg-1#
```

Backing Up Files

Three types of backup requests are available: data only, configuration only, or all.

- Data—Backs up dynamic data such as local endpoint IDs, mailboxes, and system distribution lists
- Configuration—Backs up system configuration, including the local messaging gateway ID, messaging gateway peers, manually configured endpoints, registration credentials, and NAT data). Use the **show run** command to display the current running configuration.
- All—Backs up all data and configuration information.

Backups are performed only in offline mode.

Cisco Unified Messaging Gateway automatically numbers and dates the backup files and identifies the revision number in a **backupid** field.

Performing different backup types at various times causes different backup IDs for data backups and configuration backups. For example, the last data backup ID might be 3, and the last configuration backup might be 4. Performing an "all" backup might result in a backup ID of 5 for both data and configuration.

When restoring the files, refer to the backup ID for the backup file that you want to use. Use the **show backup server** command for a list of backup IDs.

Note We recommend that you back up your configuration files whenever changes are made to the system or application files. Data files, which contain voice messages, should be backed up regularly to minimize data loss, such as from a hardware failure.

SUMMARY STEPS

1. **offline**
2. **backup category** {**all** | **configuration** | **data**}
3. **continue**
4. **show backup history**
5. **show backup server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**offline** **Example:** umg-1# **offline**	Enters offline mode.
Step 2	**backup category** {**all**	**configuration**	**data**} **Example:** umg-1(offline)# **backup category all** umg-1(offline)# **backup category configuration** umg-1(offline)# **backup category data**	Specifies the type of data to be backed up and stored.

	Command or Action	Purpose
Step 3	**continue** **Example:** umg-1(offline)# **continue**	Exits offline mode and returns to EXEC mode.
Step 4	**show backup history** **Example:** umg-1# **show backup history**	Displays the backup procedures and the success or failure of those attempts.
Step 5	**show backup server** **Example:** umg-1# **show backup server**	Displays the backup files available on the backup server, the date of each backup, and the backup file ID.

Examples

The following is sample output from the **show backup history** command:

```
umg-1# show backup history

aaa# show backup history
#Start Operation
Category: Configuration
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 7
Date: Wed Feb 17 23:19:48 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

#Start Operation
Category: Data
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 7
Date: Wed Feb 17 23:19:48 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

#Start Operation
Category: Data
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 7
Date: Wed Feb 17 23:19:49 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation

#Start Operation
Category: Configuration
```

```
Backup Server: ftp://192.1.1.31/backups
Operation: Backup
Backupid: 8
Date: Fri Feb 19 14:36:33 EST 2010
Result: Success
Reason:
Version: 8.0.0.1
#End Operation
```

The following is sample output from the **show backup server** command:

```
umg-1# show backup server

Category:       Data
Details of last 5 backups
Backupid:     1
Date:         Tue Jul 22 10:55:52 PDT 2003
Description:

Backupid:     2
Date:         Tue Jul 29 18:06:33 PDT 2003
Description:

Backupid:     3
Date:         Tue Jul 29 19:10:32 PDT 2003
Description:

Category:       Configuration
Details of last 5 backups
Backupid:     1
Date:         Tue Jul 22 10:55:48 PDT 2003
Description:

Backupid:     2
Date:         Tue Jul 29 18:06:27 PDT 2003
Description:


Backupid:     3
Date:         Tue Jul 29 19:10:29 PDT 2003
Description:

umg-1#
```

Restoring Files

After the backup files are created, you can restore them when needed. Restoring is done in offline mode.

Use the **show backup server** command to locate the backup ID of the file that you want to restore.

SUMMARY STEPS

1. **show backup server**
2. **offline**
3. **restore id** *backupid* **category** {**all** | **configuration** | **data**}
4. **show restore history**
5. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show backup server** **Example:** `umg-1# show backup server`	Lists the data and configuration backup files. Look at the backup ID field for the revision number of the file that you want to restore.
Step 2	**offline** **Example:** `umg-1# offline`	Enters offline mode. All active voice-mail calls are terminated.

Step 3	**restore id** *backupid* **category** {**all** | **configuration** | **data**}
	
	Example:
	`umg-1(offline)# restore id 22 category all`
	`umg-1(offline)# restore id 8 category configuration`
	`umg-1(offline)# restore id 3 category data`
		Specifies the backup ID *backupid* value and the file type to be restored.

Step 4	**show restore history** **Example:** `umg-1# show restore history`	Displays the restore procedures and the success or failure of those attempts.
Step 5	**reload** **Example:** `umg-1(offline)# reload`	Resets the Cisco Unified Messaging Gateway module so that the restored values take effect.

Example

The following example displays the backup server:

```
umg-1# show backup server

Category:       Data
Details of last 5 backups
Backupid:     1
Date:         Tue Jul 22 10:55:52 PDT 2003
Description:

Backupid:     2
Date:         Tue Jul 29 18:06:33 PDT 2003
Description:

Backupid:     3
Date:         Tue Jul 29 19:10:32 PDT 2003
Description:

Category:       Configuration
Details of last 5 backups
Backupid:     1
Date:         Tue Jul 22 10:55:48 PDT 2003
Description:

Backupid:     2
Date:         Tue Jul 29 18:06:27 PDT 2003
Description:


Backupid:     3
Date:         Tue Jul 29 19:10:29 PDT 2003
Description:

umg-1#
```

The following example shows the restore history:

```
umg-1# show restore history


#Start Operation
Category:      Configuration
Backup Server: ftp://10.100.10.215/CUE_backup
Operation:     Restore
Backupid:      129
Restoreid:     15
Description:   CUE test backup
Date:          Sun Jun 13 12:32:48 PDT 1993
Result:        Success
Reason:
Version: 8.0.0.1
#End Operation
```

Backup and Restore Using SFTP

This section discusses the following topics:

- Overview, page 139
- Configuring Backup and Restore Using SFTP, page 139

Overview

You can transfer files from any Cisco Unified Messaging Gateway application to and from the backup server using Secure File Transfer Protocol (SFTP). SFTP provides data integrity and confidentiality that is not provided by FTP.

Because SFTP is based on Secure Shell tunnel version 2 (SSHv2), only SSHv2 servers are supported for this feature.

To run backup and restore over SFTP, you must configure the URL of the backup server in the form of sftp://*hostname*/*dir*, and also the username and password to login to the server. The backup server must have an SSH daemon running with the SFTP subsystem enabled. The SSH protocol allows various user authentication schemes.

Configuring Backup and Restore Using SFTP

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

Required Data for This Procedure

There is no data required.

SUMMARY STEPS

1. **config t**
2. **backup** {**revisions** *number* | **server url** *sftp-url* **username** *sftp-username* **password** *sftp-password*}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** `umg-1# config t`	Enters configuration mode.
Step 2	**backup** {**revisions** *number* | **server url** *sftp-url* **username** *sftp-username* **password** *sftp-password*} **Example:** `umg-1(config)# backup server url sftp://branch/vmbackups username admin password mainserver`	Performs a backup to the specified SFTP or FTP server. To use SFTP, the URL must be of the form sftp://*hostname*/*directory*.
Step 3	**end** **Example:** `umg-1(config)# end`	Returns to privileged EXEC mode.

Backup Server Authentication Using a SSH Host Key

This section discusses the following topics:

- Overview, page 139
- Configuring Backup Server Authentication Without Using the SSH Host Key, page 141
- Configuring Backup Server Authentication Using the SSH Host Key, page 142

Overview

You can authenticate the backup server using the SSH protocol before starting a backup/restore operation. The SSH protocol uses public key cryptography for server authentication.

This feature provides two methods of authenticating a server:

- Establishing a secure connection based only on the URL of a trusted backup server.
- Obtaining the fingerprint of the backup server and using it to establish a secure connection. This fingerprint is also known as the host key or private key.

The first method is easier than the second method, but it is less secure because it does not depend on you knowing the backup server's private host key. However, if you know the URL of a trusted backup server, it is generally safe. In this case, the backup server securely provides the client with its private host key.

In both cases, when server authentication is enabled, the system validates the SSH server's private host key by comparing the fingerprint of the key received from the server with a preconfigured string. If the two fingerprints do not match, the SSH handshake fails, and the backup/restore operation does not occur.

You cannot use the GUI to configure this feature; you must use the CLI.

Both methods are explained in the following sections.

Configuring Backup Server Authentication Without Using the SSH Host Key

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

Required Data for This Procedure

To enable SSH authentication of a backup server without knowing the server's fingerprint (private host key), you must know the URL of a trusted backup server.

SUMMARY STEPS

1. **config t**
2. **backup server url sftp://***url*
3. **backup server authenticate**
4. **end**
5. **show security ssh knownhost**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** `umg-1# config t`	Enters configuration mode.
Step 2	**backup server url sftp://***url* **Example:** `umg-1(config)# backup server url sftp://company.com/server22`	Establishes an initial connection with the backup server.
Step 3	**backup server authenticate** **Example:** `umg-1(config)# backup server authenticate`	Retrieves the fingerprint of the backup server's host key and establishes a secure SSH connection.
Step 4	**end** **Example:** `umg-1(config)# end`	Returns to privileged EXEC mode.
Step 5	**show security ssh knownhost** **Example:** `umg-1(config)# show security ssh knownhost`	Displays a list of configured SSH servers and their fingerprints.

Configuring Backup Server Authentication Using the SSH Host Key

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

Required Data for This Procedure

To use a backup server's fingerprint (private host key) to enable SSH authentication, you must first retrieve the fingerprint "out-of-band" by running the **ssh-keygen** routine on the backup server. This routine is included in the OpenSSH package. The following example shows the command and its output:

ssh-keygen -l -f /etc/ssh/ssh_host_dsa_key.pub

1024 4d:5c:be:1d:93:7b:7c:da:56:83:e0:02:ba:ee:37:c1 /etc/ssh/ssh_host_dsa_key.pub

SUMMARY STEPS

1. **config t**
2. **security ssh knownhost** *host* **{ssh-rsa | ssh-dsa}** *fingerprint-string*
3. **end**
4. **show security ssh knowhost**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** umg-1# config t	Enters configuration mode.
Step 2	**security ssh knownhost** *host* {**ssh-rsa** | **ssh-dsa**} *fingerprint-string* **Example:** umg-1(config)# security ssh knownhost server.cisco.com ssh-rsa a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3	Configures the MD5 fingerprint of the SSH server's host key using the following arguments and keywords: *host* — Fully qualified hostname or IP address of the SSH server. **ssh-rsa** — RSA algorithm was used to create this fingerprint for a SSH server's host key. **ssh-dsa** — DSA algorithm was used to create this fingerprint for a SSH server's host key. *fingerprint-string* — MD5 fingerprint string.

	Command or Action	Purpose
Step 3	**end** **Example:** `umg-1(config)# end`	Returns to privileged EXEC mode.
Step 4	**show security ssh knownhost** **Example:** `umg-1(config)# show security ssh knownhost`	Displays a list of configured SSH servers and their fingerprints.

Encrypting and Signing of Backup Content on the Server

This section discusses the following topics:

- Overview, page 143
- Configuring the Encryption and Signing of Backup Content on the Server, page 143

Overview

You can protect backed up configuration and data files using signing and encryption before the files are transferred to the backup server.

To enable this feature, you must configure a master key, from which the encryption and signing key (known as the session key) are derived. The backup files are encrypted and signed before they are sent to the backup server. When you restore the files, the master key is used to validate the integrity of the files and decrypt them accordingly. You can also restore the backup files to any other machine running Cisco Unified Messaging Gateway 8.0 or later versions, if you configure the same master key before you begin the restore process. To make it easier to automate a scheduled backup, the master key is stored securely on the hosting device. It is not included in the backup content.

During the restore process, if the system detects that backup content has been tampered with, the restore process aborts. The system also halts and waits for the administrator to take some action, such as restoring using a different revision.

For backward compatibility, you can allow unsigned backup files to be restored if the risk is acceptable.

Configuring the Encryption and Signing of Backup Content on the Server

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

Required Data for This Procedure

There is no data required.

SUMMARY STEPS

1. **config t**
2. **backup security key generate**
3. **backup security protected**
4. **backup security enforced**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** `umg-1# config t`	Enters configuration mode.
Step 2	**backup security key generate** **Example:** `umg-1(config)# backup security key generate`	Creates the master key used for encrypting and signing the backup files.
Step 3	**backup security protected** **Example:** `umg-1(config)# backup security protected`	Enables secure mode for backups. In secure mode, all backup files are protected using encryption and a signature.
Step 4	**backup security enforced** **Example:** `umg-1(config)# backup security enforced`	Specifies that only protected and untampered backup files are restored.
Step 5	**end** **Example:** `umg-1(config)# end`	Returns to privileged EXEC mode.

Configuring Scheduled Backup Jobs

Beginning in release 8.0, you can configure one-time or recurring backup jobs.

For recurring backup jobs, you can configure the jobs to repeat:

- Every N days at a specific time
- Every N weeks on a specific day and time
- Every N months on a specific day of the month and time
- Every N years on a specific month

You can configure up to five repetitive scheduled backup jobs and five one-time scheduled backup jobs.

Whenever a backup job (or any scheduled activity) is started and in progress, any other activities that are scheduled to start at this time, are put in queue to wait for the first activity to finish. The maximum size of the queue is nine activities.

You cannot delete individual instances of a recurring scheduled backup schedule; you can only delete the entire series of backup jobs. However, you can enable forever a given scheduled action by configuring start and end dates for the action to specify when the action is active. You can also suspend a scheduled action indefinitely by not specifying an expiration date for the action.

Immediate backup requests are always given precedence over scheduled backup jobs. If the scheduled backup is configured to start at the same time as an immediate backup, the scheduled backup job is queued and the system waits for the immediate backup to finish before it attempts to start the scheduled backup job.

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

SUMMARY STEPS

1. **backup schedul**e [*name*]
2. **repeat every** {*number* **days at** *time* |*number* **weeks on** *day* | *number* **months on day** *date* | *number* **years on month** *month*} **at** *time*

Note Instead of the **repeat every** command, you can optionally use one of the following commands:

- **repeat once at** *time*
- **repeat daily at** *time*
- **repeat monthly on day** *date* **at** *time*
- **repeat weekly on** *day* **at** *time*
- **repeat yearly on month** *month* **at** *time*

3. **start-date** *date*
4. **stop-date** *date*
5. **disabled from** *date* **to** *date*
6. **backup categories** [**all**] [**configuration**] [**data**]
7. **end**
8. **show backup schedules** or **show schedules**
9. **show backup schedule detail job** *job-name* or **show schedule detail job** *job-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**backup schedule** [*name*] **Example:** umg-1# backup schedule 22	Enters backup schedule configuration submode to enable you to configure a scheduled backup job.
Step 2	**repeat every** {*number* **days** |*number* **weeks on** *day* | *number* **months on day** *date* | *number* **years on month** *month*} **at time** *time* **Example:** umg-1(backup-schedule)# repeat every 2 days at time 10:00	Specifies how often a recurring scheduled backup occurs. To configure a one-time backup job, use the **repeat once** command. You can also optionally use one of the other **repeat** commands listed in the previous note.
Step 3	**start-date** *date* **Example:** umg-1(backup-schedule)# start-date 05/30/2009	Specifies the start date for the recurring scheduled backup to occur.
Step 4	**stop-date** *date* **Example:** umg-1(backup-schedule)# stop-date 10/20/2009	Specifies the stop date for the recurring scheduled backup to occur.
Step 5	**disabled from** *date* **to** *date* **Example:** umg-1(backup-schedule)# disabled from 10/02/2009 to 10/06/2009	Specifies a time period that the recurring scheduled backup jobs are disabled.
Step 6	**backup categories** [**all**] [**configuration**] [**data**] **Example:** umg-1(backup-schedule)# **backup categories configuration**	Specifies which categories of data to backup.
Step 7	**end** **Example:** umg-1(backup-schedule)# end	Exits to privileged EXEC mode.
Step 8	**show schedules** or **show backup schedules** **Example:** umg-1# show schedules	(Optional) Displays all recurring scheduled events or all scheduled backup jobs configured on the local system.
Step 9	**show schedule detail job** *job-name* or **show backup schedule detail job** *job-name* **Example:** umg-1# show schedule detail job job-22	(Optional) Displays the details of the specified recurring scheduled event or backup job.

Examples

The following is sample output from the **show backup schedules** command:

```
umg-1# show backup schedules

Name         Schedule                Next Run       Description   Categories
A22          NOT SET                 NEVER
backup1000   Every 1 days at 12:34   Jun 25, 2002 12:34           Data
Total: 2
```

The following is sample output from the **show schedules** command:

```
umg-1# show schedules

Name         Schedule                Next Run       Description   Categories
A22          NOT SET                 NEVER
backup1000   Every 1 days at 12:34   Jun 25, 2002 12:34           Data
Total: 2
```

The following is sample output from the **show backup schedule detail job** command:

```
umg-1# show backup schedule detail job job-8

Name          job-8
Description   main backup
Categories   Configuration Data
Schedule      Daily at 06:00
Last Run      Jan 1, 2009 at 6:00
Last Result   Success
Next Run      Jan 2, 2009 at 6:00
Active        from Jan 01, 2000 until Dec 31, 2009
```

The following is sample output from the **show schedule detail job** command:

```
umg-1# show schedule detail job job-8

Job Name     job-8
Application backup
Description main backup
Schedule    Daily at 06:00
Last Run    5 hours 59 seconds ago
Next Run    in 18 hours 1 seconds
Active          from Jun 25, 2002 until INDEFINITE
```

Disabling or Reenabling All Scheduled Backups

Beginning in Cisco Unified Messaging Gateway 8.0, you can disable or reenable all scheduled backups with a single command.

Prerequisites

Cisco Unified Messaging Gateway 8.0 or a later version

SUMMARY STEPS

1. **backup schedule disable all from** *date* **to** *date*
2. **no backup schedule disable all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**backup schedule disable all from** *date* **to** *date* **Example:** `umg-1# backup schedule disable all from 07/06/2010 to 07/08/2010`	Disables all scheduled backups for a specified period. Dates are entered in MM/DD/YYYY format.
Step 2	**no backup schedule disable all**	Reenables all the scheduled backups that were disabled with the previous command.