B

Last Updated: November 17, 2010

backup

backup categories

backup category

backup schedule

backup schedule disable all

backup security enforced

backup security key

backup security protected

backup server authenticate

banner login

backup

To set the backup parameters, use the **backup** command in Cisco UMG configuration mode. To delete the number of revisions or the backup server URL, use the no form of this command.

backup {**revisions** *number* | **server url** *backup-ftp-url* **username** *backup-ftp-username* **password** *backup-ftp-password*}

no backup {**revisions** *number* | **server url** *backup-ftp-url*}

Syntax Description

revisions *number*	Number of revision files stored in the Cisco UMG database.
server url *backup-ftp-url*	URL of the FTP server to which the backup files will be saved.
username *backup-ftp-username*	Username needed to access the FTP server.
password *backup-ftp-password*	Password needed to access the FTP server.

Command Default

No backup server is set.

Command Modes

Cisco UMG configuration mode (config)

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

Set these parameters before backing up any files.

Consider the amount of storage space that each backup file requires when setting the number of files to store. When the number is reached, the next backup file overwrites the oldest stored backup file.

The system automatically numbers and dates the backup files and identifies the revision number in a backupid field. Reference this backup ID value when restoring a file.

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. See the **backup category** command for information about different backup types.

Examples

The following example sets backups to be stored on an FTP server called “ftpinfrastructure” in the “umgbackups” directory, with the username of “ftpusername” and a password of “ftppassword”.

```
umg-1# config t
umg-1(config)# backup revisions 7
umg-1(config)# backup server url ftp://ftpinfrastructure/umgbackups username ftpusername
password ftppassword
```

Related Commands

Command	Description
backup category	Specifies the type of data to be backed up and initiates the backup process.
restore id	Restores a backup file.
show backup	Displays information about the server used to store backup files.
show backup history	Displays the success or failure of backup and restore procedures.
show backup server	Displays the details of the most recent backup files.

backup categories

To specify which categories of data to backup for scheduled backups, use the **backup categories** command in Cisco UMG scheduled backup configuration mode.

backup categories [**all**] [**configuration**] [**data**]

Syntax Description

all	Backup all categories of data.
configuration	Backup configuration data.
data	Backup data.

Command Default

None.

Command Modes

Cisco UMG scheduled backup configuration (backup-schedule)

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

You can specify multiple categories of data. This command applies to scheduled backups only. To set categories for non-scheduled backups, see the **backup category** command.

Examples

The following example specifies that only configuration data will be backed up in the scheduled backup:

```
umg-1# config t
umg-1(config)# backup schedule
Your new JOB ID is 22
umg-1(backup-schedule)# backup categories configuration
```

Related Commands

Command	Description
backup schedule	Enters backup-schedule submode.
show backup schedule detail job	Shows details for the specified recurring scheduled backup job.

backup category

To specify the type of data to be backed up and initiate the backup process, use the **backup category** command in Cisco UMG offline-EXEC mode.

backup category { **all** | **configuration** | **data** }

Syntax Description

all	Backup file includes both configuration and data.
configuration	Includes the location ID of the current configuring Cisco UMG, messaging gateway peers, manually provisioned endpoints, registration credentials, and NAT settings.
data	Includes local dynamic endpoints, mailboxes, and System Distribution Lists (SDLs).

Command Default

All data is backed up.

Command Modes

Cisco UMG offline-EXEC (offline)

Command History

Cisco UMG Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command indicates the content of the backup file to be saved to the FTP server.

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

The systems assigns a backup ID to each backup, and it is this backup ID that you must reference when you restore a file. Use the **show backup history** command to locate the backup ID of the file you want to restore.

Offline mode terminates message forwarding and directory exchange. We recommend backing up at times when there is little or no messaging activity.

Cisco UMG 1.0 does not support scheduled backups. Scheduled backups are supported beginning with Cisco UMG 8.0.

Examples

The following examples illustrate the use of all three of the **backup category** commands:

```
umg-1# offline
!!!WARNING!!!: If you are going offline to do a backup, it is recommended that you save
the current running configuration using the 'write' command prior to going to the offline
state.
Putting the system offline will terminate all end user sessions.
Are you sure you want to go offline[n]? : y
```

```
umg-1(offline)# backup category all
umg-1(offline)# continue
umg-1 en
umg-1#

umg-1# offline
!!!WARNING!!!: If you are going offline to do a backup, it is recommended that you save
the current running configuration using the 'write' command prior to going to the offline
state.
Putting the system offline will terminate all end user sessions.
Are you sure you want to go offline[n]? : y
umg-1(offline)# backup category configuration
umg-1(offline)# continue
umg-1 en
umg-1#

umg-1# offline
!!!WARNING!!!: If you are going offline to do a backup, it is recommended that you save
the current running configuration using the 'write' command prior to going to the offline
state.
Putting the system offline will terminate all end user sessions.
Are you sure you want to go offline[n]? : y
umg-1(offline)# backup category data
umg-1(offline)# continue
umg-1 en
umg-1#
```

Related Commands

Command	Description
backup	Specifies the number of backup files to store and the server to which they are to be saved.
continue	Enters online mode.
offline	Enters offline mode.
restore id	Restores a backup file.
show backup history	Displays detailed information about backed-up files.
show backup server	Displays detailed information about the backup server.
write	Writes to, erases, copies, or displays the running configuration.

backup schedule

To configure a one-time or recurring scheduled backup, use the **backup schedule** command in Cisco UMG configuration mode. Use the **no** form of this command to remove the configuration of the backup job.

backup schedule [*name*]

no backup schedule *name*

Syntax Description

name	(Optional) Specifies the name used to create, modify, or delete a scheduled backup job. It can be up to three characters long and include the characters A through Z, 0 through 9, underscore, and hyphen (-).

Command Default

None.

Command Modes

Cisco UMG EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

This command enters backup-schedule mode and enables you to configure one-time or recurring backup jobs.

If you do not provide a name when you enter the command, one is automatically selected and displayed. If the maximum number of schedules reached and the system is unable to create the scheduled backup job using the specified parameters, an error message is display.

To create a one time backup job, enter the time of day and the date as input.

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

- Every N days at a specific time
- Every N weeks on 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 also configure the following parameters for backup jobs:

- start date for recurring backup jobs
- end date for recurring backup jobs

Examples

The following example configures a a scheduled backup to occur every 7 days at 11:00pm:

```
umg-1# backup schedule
Your new JOB ID is 22
umg-1(backup-schedule)# repeat every 7 days at 23:00
```

Related Commands

Command	Description
repeat every (backup-schedule)	Specifies how often a recurring scheduled backup occurs.

backup schedule disable all

To disable all scheduled backups, use the **backup schedule disable all** command in Cisco Unified Message Gateway EXEC mode. Use the **no** form of this command to reenable all scheduled backups.

backup schedule disable all from *date* **to** *date*

no backup schedule disable all

Syntax Description

from *date*	Specifies the date from which all scheduled backups are disabled. The format is MM/DD/YYYY.
until *date*	Specifies the date until which all scheduled backups are disabled. The format is MM/DD/YYYY.

Command Default

None.

Command Modes

Cisco Unified Message Gateway EXEC mode

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

The format for the date is month, day, and then year (for example: 05/302010).

Examples

The following example disables all scheduled backups from July 6, 2010 to July 8, 2010:

```
umg-1# backup schedule disable all from 07/06/2010 to 07/08/2010
```

Related Commands

Command	Description
repeat every (backup-schedule)	Specifies how often a recurring scheduled backup occurs.

backup security enforced

To specify that only protected and untampered backup files can be restored, use the **backup security enforced** command in Cisco UMG configuration mode.

backup security enforced

Syntax Description

This command has no arguments or keywords.

Command Default

All of the following types of backup files are restored:

- Unprotected (clear)
- Protected
- Untampered

Command Modes

Cisco UMG configuration

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

Before you can use this command, you must generate a backup security key by using the **backup security key generate** command.

Use the **backup security enforced** command in Cisco UMG configuration mode to specify that only protected and untampered backup files can be restored. By default, the system also restores unprotected (clear) backup files as well, as protected backup files and untampered backup files.

Examples

The following example specifies that only protected and untampered backup files can be restored:

```
umg-1# config t
umg-1(config)# backup security enforced
```

Related Commands

Command	Description
backup security key	Creates or deletes the master key used for encrypting and signing the backup files.
backup security protected	Enables secure mode for backups.

backup security key

To create or delete the master key used for encrypting and signing the backup files, use the **backup security key** command in Cisco UMG configuration mode.

backup security key {generate | delete}

Syntax Description

generate	Creates a master key.
delete	Deletes a master key.

Command Default

No key is configured.

Command Modes

Cisco UMG configuration

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

Use the **backup security key** command in Cisco UMG configuration mode to create or delete the master key used for encrypting and signing the backup files. When creating a backup security key, you are prompted to enter the password from which the key will be derived.

This command will not be saved in the startup configuration when you use the **write** command.

Examples

The following example creates a master key:

```
umg-1# config t
umg-1(config)# backup security key generate
Please enter the password from which the key will be derived: ******
```

The following example deletes a master key:

```
umg-1# config t
umg-1(config)# backup security key delete
You have a key with magic string cfbdbbee
Do you want to delete it [y/n]?:
```

Related Commands

Command	Description
backup security enforced	Specifies that only protected and untampered backup files can be restored.
backup security protected	Enables secure mode for backups.

backup security protected

To enable secure mode for backups, use the **backup security protected** command in Cisco UMG configuration mode.

backup security protected

Syntax Description

This command has no arguments or keywords.

Command Default

Backup files are stored in unprotected mode on the remote server.

Command Modes

Cisco UMG configuration

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

Before using this command, you must generate backup security key by using the **backup security key generate** command.

Use the **backup security protected** command in Cisco UMG configuration mode to enable secure mode for backups. In secure mode, all backup files are protected using encryption and a signature.

Examples

The following example enables secure mode for backups:

```
umg-1# config t
umg-1(config)# backup security protected
```

Related Commands

Command	Description
backup security enforced	Specifies that only protected and untampered backup files can be restored.
backup security key	Creates or deletes the master key used for encrypting and signing the backup files.

backup server authenticate

To retrieve the fingerprint of the backup server's host key, use the **backup server authenticate** command in Cisco UMG configuration mode.

backup server authenticate

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default value.

Command Modes

Cisco UMG configuration

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

Use the **backup server authenticate** command in Cisco UMG configuration mode to retrieve the fingerprint of the backup server's host key. Before using this command, users must configure the backup server URL and the login credential. The backup server URL must start with "sftp://." After the fingerprint is retrieved from the backup server, the system prompts the user for confirmation.

If this command is accepted, the fingerprint is stored in the form of "backup server authenticate fingerprint *fingerprint-string*" in the running configuration.This command will not be saved in the startup configuration when you use the **write** command.

Examples

The following example retrieves the fingerprint of the backup server's host key:

```
umg-1# config t
umg-1(config)# backup server authenticate
The fingerprint of host 10.30.30.100 (key type ssh-rsa) is:
  a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3
Do you want to accept it [y/n]?
```

Related Commands

Command	Description
security ssh	Configures the MD5 (Message-Digest algorithm 5) fingerprint of the SSH (Secure Shell) server's host key.
show security ssh	Displays a list of configured SSH (Secure Shell) servers and their fingerprints.

banner login

To configure the login banner, use the **banner login** command in Cisco UMG EXEC mode. Use the **no** or **default** form of the command to remove the login banner.

banner login {*delimiter-char banner-content delimiter-char* **| append}**

no banner login

default banner login

Syntax Description

delimiter-char	Character that indicates the beginning and end of the banner text.
banner-content	Text content of the banner.
append	Appends additional text to the banner.

Command Default

No login banner is configured.

Command Modes

Cisco UMG EXEC

Command History

Cisco UMG Version	Modification
8.0	This command was introduced.

Usage Guidelines

This command configures a system wide login banner that is displayed to all users when they log in. This command requires a delimiter character that signals the end of banner content input. The delimiter character can be any printable character except ? and “. The delimiter character must not occur in the banner content or the banner input will be ended prematurely. The banner contains plain text (no special formatting) and can have up to 1944 characters (including new lines). You can enter multiline input as the banner content.

The banner command is a multi-line command. The banner-content can be one or more lines. You can include the following tokens in the banner-content to represent system settings.

token	Information displayed in the banner
$(hostname)	Displays the hostname for the module.
$(domain)	Displays the domain for the module.

If you enter a banner that exceeds the allowed length, the command stops accepting input, truncates the message at the maximum length, outputs an error message, and returns to global configuration.

Examples

The following example configures the banner login to "Welcome to *hostname*:"

```
umg-1# config t
umg-1 (config)# banner login %
Enter TEXT message.  End with the character '%'.
    Welcome to $(hostname)%
umg-1 (config)# exit
```

The following example configures the banner login to "Welcome to *hostname*.somewhere.com, enjoy:"

```
umg-1# config t
umg-1 (config)# ip domain-name somewhere.com
umg-1 (config)# banner login @
Enter TEXT message.  End with the character '@'.
Welcome to $(hostname).$(domain), enjoy!
@
umg-1 (config)# exit
```

The following example configures the banner login to:

```
-----------------------------------
You have entered a restricted area.
Unauthorized access is prohibited.
-----------------------------------

umg-1# config t
umg-1 (config)# banner login 1
Enter TEXT message.  End with the character '1'.
-----------------------------------
You have entered a restricted area.
Unauthorized access is prohibited.
-----------------------------------
1
umg-1 (config)# exit
```

Related Commands

Command	Description
login pinless	Whether the console connection is subject to authentication or not.