B

Last Updated: June 30, 2007

backup

backup category

backup security key

backup security enforced

backup security protected

backup server authenticate

backup

To set the backup parameters, use the **backup** command in Cisco Unity Express 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** *ftp-url* **username** *ftp-username* **password** *ftp-password*}

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

Syntax Description

revisions *number*	Number of revision files stored in the Cisco Unity Express database.
server url *ftp-url*	URL to the FTP (or secure FTP) server where the backup files will be stored.
username *ftp-username*	User ID needed to access the FTP (or secure FTP) server.
password *ftp-password*	Password needed to access the FTP (or secure FTP) server.

Command Modes

Cisco Unity Express configuration

Command History

Cisco Unity Express Version	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.
3.0	This command was modified to allow you to use a backup server that supports SFTP.

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.

For secure FTP, the URL is of the form sftp://...

Examples

The following example sets 7 revisions on FTP server /branch/vmbackups.

```
se-10-0-0-0> enable
se-10-0-0-0# config t
se-10-0-0-0(config)# backup revisions 7
se-10-0-0-0(config)# backup server url ftp://branch/vmbackups username admin password
mainserver
```

The following example sets 5 revisions on a secure FTP server /vmbackups.

```
se-10-0-0-0> enable
se-10-0-0-0# config t
se-10-0-0-0(config)# backup revisions 7
se-10-0-0-0(config)# backup server url sftp://vmbackups username admin password mainserver
```

Related Commands

Command	Description
backup category	Specifies the type of data to be backed up.
show backup history	Displays statistics for backed-up files.
show backup server	Displays the FTP server designated to store backup files.

backup category

To specify the type of data to be backed up, use the **backup category** command in Cisco Unity Express offline mode.

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

Syntax Description

all	Backs up all data.
configuration	Backs up only system and application settings.
data	Backs up only voice-mail messages and application data.

Defaults

All data is backed up.

Command Modes

Cisco Unity Express offline

Command History

Cisco Unity Express Release	Modification
1.0	This command was introduced on the Cisco Unity Express network module and in Cisco Unified Communications Manager Express 3.0.
1.1	This command was implemented on the advanced integration module (AIM) and in Cisco Unified Communications Manager 3.3(3).
1.1.2	This command was implemented on the Cisco 2800 series and Cisco 3800 series routers.

Usage Guidelines

This command indicates the type of Cisco Unity Express data to be backed up to the FTP server.

When the backup procedure begins, all active calls are terminated. In Release 1.0, Cisco Unity Express does not support scheduled restores. Consider doing the backup procedure when the telephones are least active.

Examples

The following examples illustrate all the backup categories:

```
se-10-0-0-0> enable
se-10-0-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-0-0-0(offline)# backup category all
se-10-0-0-0(offline)# continue
se-10-0-0-0#
```

```
se-10-0-0-0> enable
se-10-0-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
```

```
Do you wish to continue[n]? : y
se-10-0-0-0(offline)# backup category configuration
se-10-0-0-0(offline)# continue
se-10-0-0-0#

se-10-0-0-0> enable
se-10-0-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-0-0-0(offline)# backup category data
se-10-0-0-0(offline)# continue
se-10-0-0-0#
```

Related Commands

Command	Description
continue	Activates the backup or restore process.
offline	Initiates Cisco Unity Express offline mode.
show backup history	Displays details about backed-up files.
show backup server	Displays details about the backup server.

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 Unity Express 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 Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Use the **backup security key** command in Cisco Unity Express 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:

```
se-10-0-0-0# config t
se-10-0-0-0(config)# backup security key generate
Please enter the password from which the key will be derived: ******
```

The following example deletes a master key:

```
se-10-0-0-0# config t
se-10-0-0-0(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 enforced

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

Command History

Cisco Unity Express Version	Modification
3.0	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 Unity Express 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:

```
se-10-0-0-0# config t
se-10-0-0-0(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 protected

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

Command History

Cisco Unity Express Version	Modification
3.0	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 Unity Express 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:

```
se-10-0-0-0# config t
se-10-0-0-0(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 Unity Express 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 Unity Express configuration

Command History

Cisco Unity Express Version	Modification
3.0	This command was introduced.

Usage Guidelines

Use the **backup server authenticate** command in Cisco Unity Express 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:

```
se-10-0-0-0# config t
se-10-0-0-0(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.