# Backing Up and Restoring the Cisco EGW 2200 Software

This section describes the procedures for backing up and restoring the Cisco EGW 2200 software. Backup and restore procedures use scripts that support secure (**scp**) and non-secure (**ftp**) file transfers to a remote host. You can back up and restore all your data, and when you restore data, you can resume system operation with no further input.

**Note** Call information is not backed up.

Cisco recommends backing up your system at least once a week. You should back up your system data:

- As part of routine system maintenance
- Before performing system maintenance
- Before upgrading
- Before system reboots

**Note** Before starting the backup process, you must identify the remote host where you will transfer your files.

## Backing Up the Cisco EGW 2200 Software

**Step 1** Log in to the Platform Administration GUI and select **Backup and Restore** > **Setup** from the left navigation pane.

**Step 2** Enter the required information. See Table 1 for details on the various fields and default values.

**Step 3** Select either **Secure** or **Non-secure**.

**Step 4** Click **Backup**.

The Cisco EGW 2200 backup script transfers the file to the remote host.

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

# Restoring the Cisco EGW 2200

The Cisco EGW 2200 Restore utility transfers the file from the remote host, uncompresses and un-tars the backup file to extract the backup files, then restores these files.

**Note** The backup of a previous software release will not restore to another software release.

**Step 1** Log in to the Platform Administration GUI and select **Backup and Restore** > **Setup** from the left navigation pane.

**Step 2** Enter the required information. See Table 1 for details on the various fields and default values.

**Note** When restoring the Cisco EGW 2200, you must specify the backup file name.

**Step 3** Select either **Secure** or **Non-secure**.

**Step 4** Click **Restore**.

The Cisco EGW 2200 restore script restores the file from the remote host.

# Verifying Backup and Restore

There are two ways to verify if your backup has been successful:

- Verifying Backup from the GUI
- Verifying Backup from the Home Directory

### Verifying Backup from the Platform Administration GUI

**Step 1** From the Platform Administration GUI, select **Software Upgrade** > **Check Component Info**.

**Step 2** Click **Backup**.

**Step 3** Click **Retrieve**.

A screen showing whether the backup has been successful appears.

### Verifying Backup From the Home Directory

Go to the home directory of the user ID used for backup. Use the OS file checker to verify the Cisco EGW 2200 backup file. (For example, use the command **ls-l** for Linux.)

If the backup and restore is successful, text containing the name of the Cisco EGW 2200 backup file, hour, and date appears.

Example:

```
-rw-r--r--  1 wagnerm  lsi     1072554 Apr 15 10:38 egwbackup_20040415_103753.tar.Z
```

In this example:

- **wagnerm** is the user ID that you used to create the file.
- **egwbackup** is the file name that you entered.

If this is your first time to do a backup and restore, and the process did not work, no text is displayed.

If you have backed up your data before, but the backup process did not work at this time, you will get the date of the last successful backup and restore. Contact Cisco TAC for assistance.

***Table 1 Backup and Restore Fields***

| Field | Description |
|---|---|
| Host ID | The name or IP address of the server on which the backed up data will be stored.<br>This is the name as configured on the backup server. |
| User ID | The ID of a user already configured on the backup server. |
| Password | The user's password already configured on the backup server. |
| Filename | The name of the file (containing the backed up data) on the remote server, from which data will be restored.<br>**Note** This field is required only for Restore.<br>Example: egwbackup_20040420_141110.tar.Z |
| Secure | Select this option to use the secure file transfer protocol (**sftp**).<br>**Note** You can select secure of non-secure depending on what type of transfer is allowed by the destination host. |
| Non-Secure | Select this option to use the file transfer protocol (**ftp**).<br>**Note** You can select secure of non-secure depending on what type of transfer is allowed by the destination host. |