



## Backup and Recovery Procedures

---

This chapter provides Content Distribution Manager database backup and ACNS software recovery procedures. It contains the following sections:

- [Performing Backup and Restore Operations for the Content Distribution Manager Centralized Management System Database, page 19-1](#)
- [Using the Cisco ACNS Software Recovery CD-ROM, page 19-2](#)
- [Recovering the System Software, page 19-4](#)
- [Recovering a Lost Administrator Password, page 19-6](#)
- [Recovering from Missing Disk-Based Software, page 19-8](#)
- [Replacing a Failed Disk Drive, page 19-10](#)
- [Recovering ACNS Network Device Registration Information, page 19-10](#)

### Performing Backup and Restore Operations for the Content Distribution Manager Centralized Management System Database

The Content Distribution Manager stores ACNS network-wide device configuration information in its Centralized Management System (CMS) database. You can manually back up the CMS embedded database contents for greater system reliability.

To back up the CMS database for the Content Distribution Manager, use the **cms database backup EXEC** command. For database backups, you need to specify the following items:

- Location, password, and user ID
- Dump format in PostgreSQL plain text syntax



**Note**

---

The naming convention for backup files includes the time stamp.

---

To back up and restore the CMS database on the Content Distribution Manager, follow these steps:

---

**Step 1** Back up the CMS database to a file.

```
CDM# cms database backup  
creating backup file with label \Qbackup'
```

backup file local1/acns-db-9-22-2002-17-36.dump is ready. use \Qcopy' commands to move the backup file to a remote host.

- Step 2** Save the file to a remote server by using the **copy disk ftp** command. This command copies the file from the local disk to a remote FTP server. For example:

```
CDM# cd /local1
CDM# copy disk ftp 10.86.32.82 /incoming acns-db-9-22-2002-17-36.dump
acns-db-9-22-2002-17-36.dump
```

```
Enter username for remote ftp server:ftp
Enter password for remote ftp server:*****
Initiating FTP upload...
Sending:USER ftp
10.86.32.82 FTP server (Version wu-2.6.1-18) ready.
Password required for ftp.
Sending:PASS *****
User ftp logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (10,86,32,82,112,221)
Sending:CWD /incoming
CWD command successful.
Sending PASV
Entering Passive Mode (10,86,32,82,203,135)
Sending:STOR acns-db-9-22-2002-17-36.dump
Opening BINARY mode data connection for acns-db-9-22-2002-17-36.dump.
Transfer complete.
Sent 18155 bytes
```

- Step 3** Delete the existing CMS database.

```
CDM# cms database delete
```

- Step 4** Restore the CMS database contents from the backup file. For example:

```
CDM# cms database restore acns-db-9-22-2002-17-36
```

- Step 5** Enable CMS.

```
CDM# cms enable
```

## Using the Cisco ACNS Software Recovery CD-ROM

A software recovery CD-ROM ships with Content Engine 500 series and 7300 series models. This section contains instructions for using the software recovery CD-ROM to reinstall your system software, if for some reason the software that is installed has failed.



### Caution

If you upgraded your software after you received your software recovery CD-ROM, using the CD-ROM software images may downgrade your system.

Cisco ACNS software consist of three basic components:

- Disk-based software
- Flash-based software
- Hardware platform cookie (stored in flash memory)

All of these components must be correctly installed for Cisco ACNS software to work properly.

The software is contained in two types of software images provided by Cisco Systems:

- A .bin image containing disk and flash memory components

An installation containing only the ACNS flash memory-based software, without the corresponding disk-based software, boots and operates in a limited mode, allowing for further disk configuration before completing a full installation.

- A .sysimg image containing a flash memory component only

The .sysimg component is provided for recovery purposes, and allows for repair of flash memory only, without modifying the disk contents.

The following options are available from the software recovery CD-ROM installer menu.

## Option 1: Configure Network

If the .bin image to install is located on the network instead of the CD-ROM (which may be the case when an older CD-ROM is used to install new software), then you must choose this option to configure the network before attempting to install the .bin image.

This option is automatically performed if you install a .sysimg file from the network.

## Option 2: Manufacture Flash

The flash memory is verified and, if invalid, is automatically reformatted to contain a Cisco standard layout. If reformatting is required, a new cookie is automatically installed.

This option is automatically performed as part of a .bin or .sysimg installation.

## Option 3: Install Flash Cookie

A hardware-specific platform cookie is generated and installed in flash memory. This option only needs to be performed if there has been a change in the hardware components, such as replacing the motherboard, or moving a flash memory card between systems.

This option is automatically performed during the flash manufacturing process, if needed, as part of a .bin or .sysimg installation.

## Option 4: Install Flash Image from Network and Option 5: Install Flash Image from CD-ROM

These options allow installation of the flash memory .sysimg only, and do not modify disk contents. They may be used when a new chassis has been provided and populated with the customer's old disks that need to be preserved.

These options automatically perform flash verification and hardware cookie installation, if required. When installing from the network, you are prompted to configure the network if you have not already done so.

## Option 6: Install Flash Image from Disk

This option is reserved for future expansion and is not available.

## Option 7: Wipe Out Disks and Install .bin Image



### Caution

---

Option 7 erases the content from all disk drives in your device.

---

This is the preferred procedure for installing the Cisco ACNS software. This option performs the following steps:

1. Checks that flash memory is formatted to Cisco specifications.  
If yes, continues to number 2.  
If no, the following takes place:
  - a. Reformats the flash memory, which installs the Cisco file system.
  - b. Generates and installs a platform-specific cookie for the hardware.
2. Erases data from all drives.
3. Remanufactures the default Cisco file system layout on the disk.
4. Installs the flash memory component from the .bin image.
5. Installs the disk component from the .bin image.

## Option 8: Exit and Reboot

Reboots the device. Remove the CD-ROM before rebooting in order to boot from flash memory.

# Recovering the System Software

The Content Engine, Content Router, and Content Distribution Manager have a resident rescue system image that is invoked should the image in flash memory be corrupted. A corrupted system image can result from a power failure that occurs while a system image is being written to flash memory. The rescue image can download a system image to the main memory of the device and write it to flash memory.

To install a new system image using the rescue image, perform the following steps:

- 
- Step 1** Download the system image file (\*.sysimg) to a host that is running an FTP server.
  - Step 2** Establish a console connection to the device and open a terminal session.
  - Step 3** Reboot the device by toggling the power on/off switch.

The rescue image dialog appears. The following example demonstrates how to interact with the rescue dialog (user input is denoted by entries in bold typeface):

```
This is the rescue image. The purpose of this software is to let
you download and install a new system image onto your system's
boot flash device. This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.
```

```
To download an image, this software will request the following
information from you:
```

- which network interface to use
- IP address and netmask for the selected interface
- default gateway IP address
- server IP address
- which protocol to use to connect to server
- username/password (if applicable)
- path to system image on server

```
Please enter an interface from the following list:
```

```
0: FastEthernet 0/0
1: FastEthernet 0/1
```

```
0
```

```
Using interface FastEthernet 0/0
```

```
Please enter the local IP address to use for this interface:
```

```
[Enter IP Address]: 172.16.22.22
```

```
Please enter the netmask for this interface:
```

```
[Enter Netmask]: 255.255.255.224
```

```
Please enter the IP address for the default gateway:
```

```
[Enter Gateway IP Address]: 172.16.22.1
```

```
Please enter the IP address for the FTP server where you wish
to obtain the new system image:
```

```
[Enter Server IP Address]: 172.16.10.10
```

```
Please enter your username on the FTP server (or 'anonymous'):
```

```
[Enter Username on server (e.g. anonymous)]: anonymous
```

```
Please enter the password for username 'anonymous' on FTP server (an email address):
```

```
Please enter the directory containing the image file on the FTP server:
```

```
[Enter Directory on server (e.g. /)]: /
```

```
Please enter the file name of the system image file on the FTP server:
```

```
[Enter Filename on server]: ACNS-5.2.0-K9.sysimg
```

```
Here is the configuration you have entered:
```

```
Current config:
```

```
IP Address: 172.16.22.22
Netmask: 255.255.255.224
Gateway Address: 172.16.22.1
Server Address: 172.16.10.10
Username: anonymous
Password:
Image directory: /
Image filename: ACNS-5.0.0-K9.sysimg
```

```
Attempting download...
```

```
Downloaded 10711040 byte image file
```

```
A new system image has been downloaded.
```

```

You should write it to flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no')]: yes
Ok, writing new image to flash
.....Finished
writing image to flash.
Enter 'reboot' to reboot, or 'again' to download and install a new image:
[Enter reboot confirmation ('reboot' or 'again')]: reboot
Restarting system.
Initializing memory. Please wait.

```

- Step 4** Log in to the device as username **admin**. Verify that you are running the correct version by entering the **show version** command.

```

Username: admin
Password:

Console> enable
Console# show version
Application and Content Networking System Software (ACNS)
Copyright (c) 1999-2004 by Cisco Systems, Inc.
Application and Content Networking System Software Release 5.2.0 (build b360 Aug
 5 2004)
Version: ce507-5.2.0

Compiled 02:34:38 Aug  5 2004 by (cisco)
Compile Time Options: PP SS

System was restarted on Thu Aug  5 16:03:51 2004.
The system has been up for 4 weeks, 1 day, 6 hours, 7 minutes, 23 seconds.

```

## Recovering a Lost Administrator Password

If an administrator password is forgotten, lost, or misconfigured, perform the following steps to reset the password on the device.



### Note

There is no way to restore a lost administrator password. You must reset the password to a new one, as described in this procedure.

- Step 1** Establish a console connection to the device and open a terminal session.
- Step 2** Reboot the device. While the device is rebooting, watch for the following prompt and press **Enter** when you see it:

```
Cisco ACNS boot:hit RETURN to set boot flags:0009
```

- Step 3** When prompted to enter bootflags, enter this value:

```
0x8000
```

For example:

```

Available boot flags (enter the sum of the desired flags):
0x4000 - bypass nvram config
0x8000 - disable login security

```

```
[CE boot - enter bootflags]:0x8000
You have entered boot flags = 0x8000
Boot with these flags? [yes]:yes
```

[Display output omitted]  
Setting the configuration flags to **0x8000** lets you into the system, bypassing all security. Setting the configuration flags field to **0x4000** lets you bypass the NVRAM configuration.

- Step 4** When the device completes the boot sequence, you are prompted to enter the username to access the CLI. Enter the default administrator username (**admin**):

```
Cisco Content Engine Console
```

```
Username: admin
```

- Step 5** Once you see the CLI prompt, set the password for the user using the **username password** command in global configuration mode.

The following example shows the different options and parameters for the **username** command. You can specify that the password be either clear text or encrypted. The user in the example chose to have an encrypted password.

```
ContentEngine# configure
ContentEngine(config)# username ?
WORD User name
ContentEngine(config)# username biff ?
password Specify the password for the user
privilege Set user privilege level
samba-password Set user's Windows sharing password
ContentEngine(config)# username biff password ?
0 Specifies clear-text password (default)
1 Specifies type 1 encrypted password
WORD User password (clear text)
ContentEngine(config)# username biff password 0 ?
WORD User password (encrypted)
ContentEngine(config)# username biff password 0 mypassword ?
uid User Id
<cr>
ContentEngine(config)# username biff password 0 mypassword uid ?
<2001-65535> User Id
ContentEngine(config)# username biff password 0 mypassword uid 2001 ?
<cr>
ContentEngine(config)#
```

- Step 6** Use the **write memory** command in EXEC mode to save the configuration change.

```
ContentEngine(config)# exit
ContentEngine# write memory
```

- Step 7** Optionally, reboot your device by using the **reload** command.

```
ContentEngine# reload
```

Rebooting is optional; however, you might want to reboot to ensure that the boot flags are reset, and to ensure that subsequent console administrator logins do not bypass the password check.



**Note** In ACNS software, the bootflags are reset to 0x0 on every reboot.

# Recovering from Missing Disk-Based Software

This section describes the recovery procedures to use if for some reason the software installation on the first disk drive (disk00) is corrupt or missing.

This situation is most likely to occur only if you replaced disk00 in your Content Engine, Content Router, or Content Distribution Manager. By design, the software installation on disk00 cannot be corrupted by a system crash or a power failure.

If the system disk (disk00) fails or is missing, the software continues to run; however, it runs in a degraded mode in which HTTP proxy and related HTTP features still work, but most other features fail.

To recover from this condition, follow these steps:

- 
- Step 1** Remove the Content Engine record from the Content Distribution Manager GUI.
- From the Content Distribution Manager GUI, choose **Devices > Devices**.
  - Click the **Edit** icon next to the name of the Content Engine that you wish to delete. The browser window refreshes, displaying the Modifying a Content Engine window.
  - Click the **Trash** icon. You are prompted to confirm your decision.
  - Click **OK** to execute your request. The Content Engine is removed from the Content Distribution Manager GUI.




---

**Note** The Content Engine registration record needs to be deleted from the Content Distribution Manager in order for the Content Engine to complete reregistration after it comes back online. The Content Distribution Manager will not register a device if the device already appears in the record as registered.

---

**Step 2** Power down the device and replace the failed or missing disk00 with a new, blank disk.

**Step 3** After the new disk is installed, power up the device.

**Step 4** From a console or through a Telnet session, check the startup messages that appear on your screen.

If there is a problem with disk00 or the disk-based software, a message similar to the following appears:

```
*****
Your first disk is not in standard configuration.
You might need to run 'disk recover' from the CLI.
*****
```

**Step 5** Log in as **admin**.

```
Cisco Content Engine Console

Username: admin
Password:
System Initialization Finished.

CE-507 con now available

Press RETURN to get started!
```

- Step 6** Enter the **disk recover** EXEC command to create the file systems on disk00 that are for internal system use.

```
CE-507# disk recover
This will erase everything on disk00. Are you sure? [no]yes
System filesystems appear to have been installed.
Please verify your software installation with 'show flash'
and install a new image if necessary.
CE-507#
CE-507# show flash
/diamond/bin/exec_show_flash: could not open /swstore/manifest: No such file or directory
Your software installation is damaged.
Please run 'copy ftp install' to install a new image.
```

- Step 7** Enter the **copy ftp install** EXEC command to download and install a new system image.

```
ContentEngine# copy ftp install ftp-server remotefiledir remotefilename
```

For example:

```
CE# copy ftp install vista /users2/biff/bfc/boot ce507-ACNS-5.0.0-K9.bin
Enter username for remote ftp server: biff
Enter password for remote ftp server:
Initiating FTP download...
printing one # per 1MB downloaded
Sending: USER biff
vista.cisco.com FTP server (Version wu-2.6.0(1) Mon Feb 24 10:30:36 EST 2003) ready.
Password required for biff.
Sending: PASS *****
User biff logged in.
Sending: TYPE I
Type set to I.
Sending: PASV
Entering Passive Mode (128,107,193,244,173,205)
Sending: CWD /users2/biff/bfc/boot
CWD command successful.
Sending PASV
Entering Passive Mode (128,107,193,244,173,205)
Sending: RETR ruby.bin
Opening BINARY mode data connection for ruby.bin (102794344 bytes).
#####
Installing phase3 bootloader...
Installing system image to flash: image on flash identical to new image, no work required
The new software will run after you reload.
#
ContentEngine# show flash
ACNS software version (disk-based code): ACNS-5.0.0-b130

System image on flash:
Version: 5.0.0

System flash directory:
System image: 98 sectors
Bootloader, rescue image, and other reserved areas: 26 sectors
128 sectors total, 4 sectors free.
```

- Step 8** Enter the **disk config** EXEC command to define file system space allocations on disk00. For example:

```
ContentEngine# disk config sysfs 10% cfs 20% mediafs 20% cdnfs 50%
```



**Note** Disk allocation percentages or values should reflect the anticipated usage for each file type.

Alternatively, you can run the **disk config** command after you reboot the software.

- Step 9** Use the **reload EXEC** command to reboot the software with the new disk and new system image running.

```
ContentEngine# reload
```

- Step 10** Register the device with the Content Distribution Manager by using the **cms enable** command in global configuration mode.

```
CE-507# configure
CE-507(config)# cms enable
```

## Replacing a Failed Disk Drive

When adding or replacing a disk drive other than disk00, you need to use the **disk add EXEC** command to make the system aware of the additional disk space and to reallocate the file systems, if necessary.



### Note

In ACNS 5.x software, the **disk add** command does not support disk00 but supports disk01 or higher, when the drive in the slot is a blank new replacement disk. Use the **disk recover EXEC** command rather than the **disk add** command to add disk00.

## Recovering ACNS Network Device Registration Information

Device registration information is stored both on the device itself and on the Content Distribution Manager. If a device loses its registration identity or needs to be replaced because of hardware failure, the ACNS network administrator can issue a CLI command to recover the lost information, or in the case of adding a new device, assume the identity of the failed device.

To recover lost registration information, or to replace a failed node with a new one having the same registration information, follow these steps:

- Step 1** Mark the failed device as “Inactive” and “Replaceable” in the Content Distribution Manager GUI.
- a. From the Content Distribution Manager GUI, choose **Devices > Devices**.
  - b. Click the **Edit** icon next to the name of the Content Engine that you want to deactivate. The Content Engine Device Home window appears.
  - c. In the Contents pane, choose **Device Activation**.
  - d. Uncheck the **Activate** check box. The window refreshes, displaying a check box for marking the device as replaceable.
  - e. Check the **Replaceable** check box and click **Submit**.



### Note

This check box only appears in the GUI when the device is inactive.

- Step 2** Configure a system device recovery key.
- From the Content Distribution Manager GUI, choose **System > Configuration**.
  - Click the **Edit** icon next to the `System.device.recovery.key` property. The Modifying Config Property window appears.
  - Enter a password in the Value field and click **Submit**. The default password is **default**.
- Step 3** Configure the basic network settings for the new device. (See Chapter 3, “Getting Started.”)
- Step 4** Open a Telnet session to the device CLI and execute the `cms recover identity keyword EXEC` command, where *keyword* is the device recovery key that you configured in the Content Distribution Manager GUI.
- When the Content Distribution Manager receives the recovery request from the Content Engine, it searches its database for the Content Engine record that meets the following criteria:
- The record is inactive and replaceable.
  - The record has the same host name as given in the recovery request.
  - The device is the same hardware model as the device in the existing record.
  - The file system allocations for the device are the same as or greater than the device in the existing record.
- If the recovery request matches the Content Engine record, then the Content Distribution Manager updates the existing record and sends the requesting Content Engine a registration response. The replaceable state is cleared so that no other device can assume the same identity. When the Content Engine receives its recovered registration information, it writes it to file, initializes its database tables, and starts.
- Step 5** Return to the Content Distribution Manager GUI and activate the device.
- From the Content Distribution Manager GUI, choose **Devices > Devices**.
  - Click the **Edit** icon next to the name of the Content Engine that you want to activate. The Content Engine Device Home window appears.
  - In the Contents pane, choose **Device Activation**. The Content Engine status should be Online.
  - Check the **Activate** check box and click **Submit**.
-

