Maintaining the Videoscape Distribution Suite, Internet Streamer

This chapter describes how to perform common administrative tasks including updating system software, hard disk drive maintenance, and rebooting and deleting devices.

- Software Upgrade, page 9-1
- Rebooting Devices, page 9-10
- Deleting a Device, page 9-10
- Replacing a Device, page 9-13
- Backup and Recovery Procedures, page 9-16
- Disk Maintenance, page 9-27

For information about database maintenance, see the "Scheduling Database Maintenance" section on page 4-64.

Software Upgrade

- Getting a Software File from Cisco.com, page 9-1
- Finding the Software Version of the Devices, page 9-3
- Configuring the Software Image Settings, page 9-3
- Upgrading the Software, page 9-6
- Software Upgrades by Device, page 9-9

Getting a Software File from Cisco.com

To get a software file from Cisco.com, follow these steps:

Step 1 Launch your web browser and enter the following URL:

http://www.cisco.com/cisco/software/navigator.html

The Select a Product page is displayed if you have recently logged in; otherwise, the Log In page is displayed.

Step 2 Log in to Cisco.com using your designated username and password. The Video and Content Delivery page is displayed, listing the available software products.

Step 3 Choose **Products > Video and Content Delivery > Content Delivery Systems > Content Delivery Applications > Cisco Internet Streamer Application**. The Downloads page is displayed.

Step 4 Click the desired software release. The page refreshes and the software image files are displayed.

Step 5 Click the link for the software image file that you want.

- If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click **Accept**.
- If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form is not displayed again.

The Download page is displayed with the information about the software image file and a Download link.

Step 6 Click **Download Now** to download the file, or click **Add to cart** to select more image files before downloading them. The Download Cart page is displayed.

Step 7 Click **Proceed With Download**. The Cisco End User Software License Agreement is displayed.

Step 8 Read the agreement and click **Agree**. The Download Software page is displayed.

Step 9 Choose a download option, either **Download Manger Option** or **Non Java Download Option**. A new window displays the filename of the ISO image file.

Step 10 Click **Download**. The File Download dialog box is displayed.

Step 11 Click **Save**. The Save As dialog box is displayed.

Step 12 Navigate to the location where you want to save the file and click **Save**. The file downloads.

Pre-positioning a Software File

A software file is pre-positioned in the same manner as any other content item. Pre-positioning allows you to conserve bandwidth usage across the WAN and avoid congesting your network during updates. The software file is fetched one time from the origin server, replicated across your network, and stored in Service Engine caches in your LAN.

To pre-position a software file, you must complete the following tasks:

- Define a Delivery Service.
- Assign devices to the Delivery Service.
- Define the software file that you want to pre-position by using a Manifest file or the CDSM Delivery Service content page.
- Check the device replication status.

See Chapter 5, “Configuring Services” for more information.

Note Only Service Engines that are assigned to the Delivery Service can be updated using pre-positioned software files. Service Routers and CDSMs do not have pre-positioned content; therefore, you cannot use the pre-positioned method for device updates for these devices.

Sample Manifest File to Pre-position a Software File

You can use the following sample Manifest file to pre-position a software file by replacing the URL with a valid software file URL:

```
<CdnManifest>
<item src="http://your-web-server.com/folder/upgrade.bin" />
</CdnManifest>
```

The server name or IP address of the URL in the Manifest file (and in the Software File URL field in the Software File Settings page must match either the Origin Server field or the Service Router Domain Name field in the Content Origin page).

Finding the Software Version of the Devices

The CDSM Home page gives a brief summary of the software versions in use on all of the devices in the Videoscape Distribution Suite, Internet Streamer (VDS-IS) network.

To view the software version running on a particular device, choose **Devices > Devices**. The Devices Table page displays the software version for each device listed.

Clicking the **Edit** icon next to the device name in the Devices Table page displays the Devices home page, which shows the software version for that device.

Note The software version is not upgraded until a software upgrade has been successfully completed. If a software upgrade is in progress, the version number displayed is the base version, not the upgraded version number.

Configuring the Software Image Settings

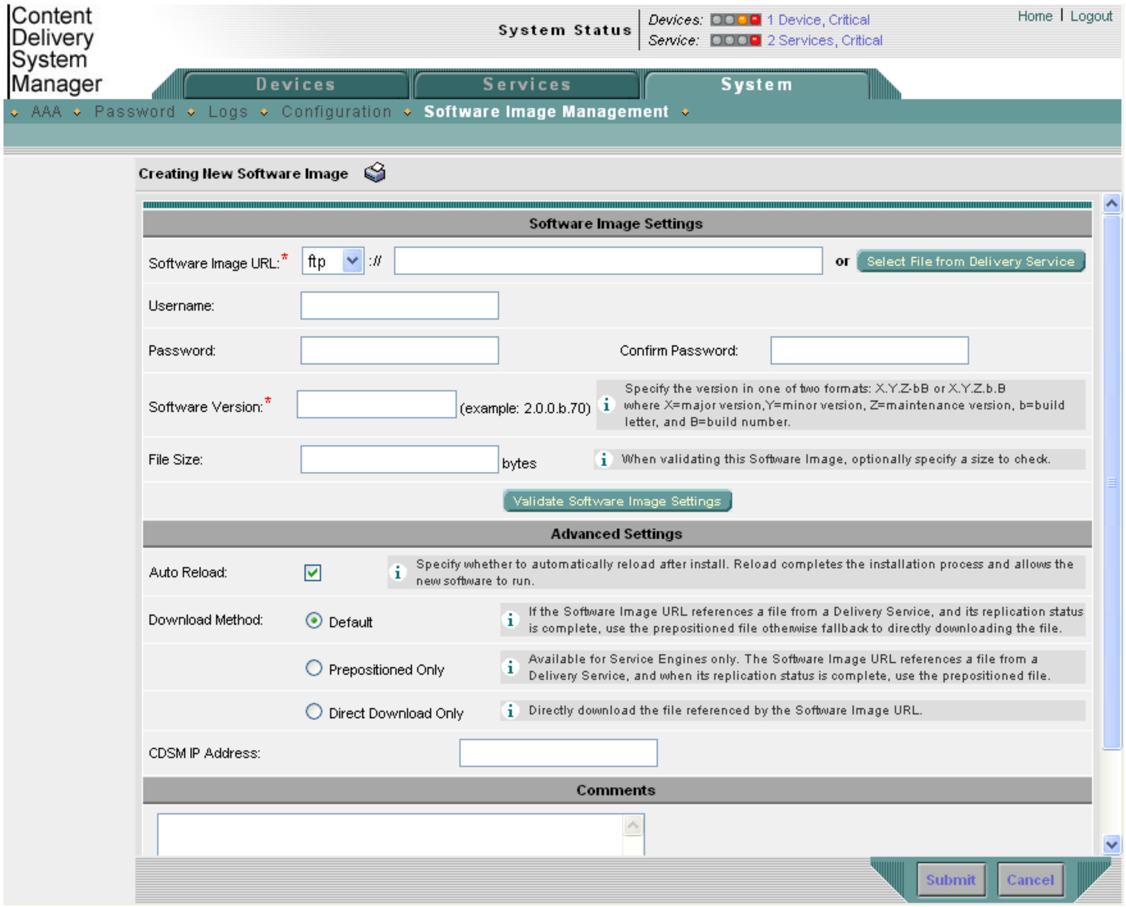
To upgrade your VDS-IS software release, you must first configure the software image settings.

To configure the software image settings, follow these steps:

Step 1 Choose **System > Software Image Management**. The Software Files Table page is displayed.

Step 2 Click the **Create New** icon in the task bar. The Software Image page is displayed (Figure 9-1).

Figure 9-1 Software Image Page


Content Delivery System Manager
System Status
Devices: 1 Device, Critical
Service: 2 Services, Critical
Home | Logout
Devices
Services
System
AAA
Password
Logs
Configuration
Software Image Management
Submit
Cancel
211837

Creating New Software Image

Software Image Settings

Software Image URL:* ftp :// or Select File from Delivery Service

Username:

Password: Confirm Password:

Software Version:* (example: 2.0.0.b.70) Specify the version in one of two formats: X.Y.Z-bB or X.Y.Z.b.B where X=major version,Y=minor version, Z=maintenance version, b=build letter, and B=build number.

File Size: bytes When validating this Software Image, optionally specify a size to check.

Validate Software Image Settings

Advanced Settings

Auto Reload: ☑ Specify whether to automatically reload after install. Reload completes the installation process and allows the new software to run.

Download Method: ● Default If the Software Image URL references a file from a Delivery Service, and its replication status is complete, use the prepositioned file otherwise fallback to directly downloading the file.

○ Prepositioned Only Available for Service Engines only. The Software Image URL references a file from a Delivery Service, and when its replication status is complete, use the prepositioned file.

○ Direct Download Only Directly download the file referenced by the Software Image URL.

CDSM IP Address:

Comments

Step 3 In the **Software Image URL** field, enter the URL for the .bin software file that you downloaded from Cisco.com.

a. Choose a protocol (**http** or **ftp**) from the drop-down list.

b. Enter the URL of the software file; for example, a valid URL might look like this:

http://internal.mysite.com/cds/*CDS-2.x.x-K9*.bin

In this URL, *CDS-2.x.x-K9* is the name of the software upgrade file. (The filename might include the version number.)

Note If you are using a pre-positioned software file and you are entering the URL manually (rather than using the **Select File from Delivery Service** option), the server name or IP address of the URL in the Software Image URL field must match either the Origin Server field or the Service Routing Domain Name field in the Content Origin page of the Delivery Service. This is not a requirement if you are downloading the software file directly from the origin server. (See the "Pre-positioning a Software File" section on page 9-2 for details.)

Alternatively, click **Select File from Delivery Service**. A separate page is displayed that allows you to choose a Delivery Service, set criteria, search the Delivery Service, and select the software file that you want to use for the software upgrade. (You must first pre-position the software file in the Delivery Service. See the "Pre-positioning a Software File" section on page 9-2.)

Step 4 If your server requires user login authentication, enter your username in the **Username** field and enter your login password in the **Password** field. Enter the same password in the **Confirm Password** field.

Step 5 Enter the software version number in the **Software Version** field. You can copy this number from the version portion of the software filename in the software file URL.

Specify the version in one of two formats: X.Y.Z-bB or X.Y.Z.b.B, where X = major version, Y = minor version, Z = maintenance version, b = build letter, and B = build number.

Step 6 If you want the size of the software file considered during validation, enter a file size (in bytes) in the **File Size** field. If you leave this field blank, the URL is checked without regard to the software file size.

Step 7 To validate the Software Image URL, Username, and Password fields, click **Validate Software Image Settings**.

When you click **Validate Software Image Settings**, the following occurs:

- The software file URL is resolved.
- The connection to the software file URL is established using the username and password, if specified.
- If a file size is specified, the actual size of the software file is obtained and compared against the value in the File Size field.
- The message is returned, indicating success or errors encountered.

Step 8 In the Advanced Settings area, check the **Auto Reload** check box to automatically reload a device when you upgrade the software.

Step 9 Choose one of three download methods:

- **Default**—Uses pre-positioned content but always falls back to direct download.
- **Prepositioned Only**—Uses the local file copy if the software file URL references pre-positioned content and its replication status is complete.
- **Direct Download Only**—Directly downloads the file using the software file URL.

Note If you choose **Prepositioned Only**, the software file settings that you define in this page cannot be used to upgrade a CDSM or an SR, because these devices do not have pre-positioned content.

Step 10 For downgrades only, specify the CDSM IP address to be used for device registration in the **CDSM IP address** field.

The CDSM IP address field is the IP address of a CDSM after the software is downgraded. (This field is optional and only applies for downgrades.) After the downgrade, the SE registers with the CDSM with the IP address specified in this field.

Step 11 Click **Submit**.

To delete a software file, click the **Delete** icon in the task bar.

Caution If your browser is configured to save the username and password for the CDSM, the browser auto-populates the Username and Password fields in the Software Image page. You must clear these fields before you click **Submit**.

The software file that you want to use is now registered with the CDSM. When you perform the software upgrade or downgrade, the URL that you just registered becomes one of the choices available in the Update Software page. (See the "Upgrading the Software" section on page 9-6.)

Upgrading the Software

When upgrading software in your VDS-IS network, begin with Service Engines and Service Routers before upgrading the CDSM. The CDSM reboots at the conclusion of the upgrade procedure, causing you to temporarily lose contact with the device and the user interface. After the CDSM has upgraded its software and rebooted, it may be unable to communicate with devices running different versions of the VDS-IS software.

Caution Primary and standby CDSMs must be running the same version of VDS-IS software. If they are not, the standby CDSM detects this and does not process any configuration updates it receives from the primary CDSM. You need to upgrade your standby CDSM first, and then upgrade your primary CDSM. We also recommend that you create a database backup for the primary CDSM and copy the database backup file to a safe place before you upgrade the software.

Caution To upgrade the software image on a server, you first need to offload a server for maintenance. Once the server has been fully offloaded, you can upgrade the software. After updating the software, uncheck the **Server Offload** check box to allow the server to receive client requests from the Service Router. See the Server Offload field in Table 4-6 on page 4-11 for more information.

Downgrading the Software

For software downgrades of systems with primary and standby CDSMs, you need to follow these steps:

1. If you are using the CDSM GUI, downgrade the standby CDSM first, followed by the primary CDSM.

   If you are using the CLI, downgrade the primary CDSM first, followed by the standby CDSM.

2. After downgrading the primary and standby CDSMs, using the CLI, log in to each CDSM and run the following commands:

```
cms database downgrade
cms enable
```

3. Downgrade the software on the Service Routers.
4. Downgrade the Content Acquirers.
5. Downgrade the middle-tier Service Engines.
6. Downgrade the edge Service Engines.

Note Before downgrading from Release 4.0 to the previous 3.x release image, you need to execute the content-mgr rollback command on the Service Engine, otherwise all the cached content will be lost after downgrade. The content-mgr rollback command evicts the cached disk content till max cached files count below 20,000,000 and max cached directories count below 950,000.

Interoperability Considerations

In general, a VDS-IS network is upgraded gradually, so that your network might consist of nodes with different software versions for the duration of time it takes to upgrade all nodes. Dissimilar software versions are not supported in the long term, and only the interoperability considerations listed below are supported until all devices are running the same software version. You can expect the following behavior during an upgrade or downgrade of your network:

- The VDS-IS network continues to operate with mixed versions up to one major or minor version difference in a deployed solution.
- New features that depend on device cooperation might not be fully functional until the VDS-IS network upgrade is complete, but no existing features are affected.
- While being upgraded, a node is unavailable for a short time.
- All nodes, other than the node being upgraded, continue to operate at full capacity. The availability of other nodes is not affected during an upgrade.
- Content is preserved during an upgrade or downgrade unless you remove a Delivery Service.
- All logs are preserved during an upgrade or downgrade, unless you change the disk configuration. Anytime disk space is reconfigured, the logs are automatically removed.

We strongly recommend that you upgrade your VDS-IS network devices in the following order:

1. Multicast sender Service Engines
2. Multicast receiver Service Engines
3. Edge Service Engines
4. Middle-tier Service Engines
5. Content Acquirers

Note When upgrading the Content Acquirers in a Delivery Service, to avoid having a critical alarm generated while the Content Acquirer is being upgraded, temporarily set the System.datafeed.pollRate field to 200 seconds or higher. When the upgrade is complete, reset the field to the original value. See the "System Properties" section on page 6-8 for more information.

6. Service Routers
7. Standby CDSMs (Upgrade before the primary CDSM when using the GUI only.)
8. Primary CDSM

Note When you upgrade CDSMs using the CLI, we recommend that you upgrade your primary CDSM first, and then upgrade your standby CDSM. Primary and standby CDSMs must be operating with exactly the same software release as each other for failover to be successful.

Upgrading Software by Device Groups

Note This procedure is for Service Engines only. Service Routers and CDSMs cannot be associated with device groups.

To upgrade your software on multiple Service Engines, follow these steps:

Step 1 Choose **Devices > Device Groups**. The Device Groups Table page is displayed.

Step 2 Click the **Edit** icon next to the name of the device group that you want to upgrade. The Device Group page is displayed.

Step 3 From the left-panel menu, choose **Software Update**. The Software Update for Device Group page is displayed.

Step 4 Choose the software file URL from the Software File URL list by clicking the radio button next to the filename.

Step 5 Click **Submit**.

To view progress on an upgrade, go to the Devices Table page (**Devices > Devices**). Software upgrade status messages are displayed in the Software Version column. These intermediate messages are also written to the system log on the Service Engines. See Table 9-1 for a description of upgrade status messages.

Table 9-1 Upgrade Status Messages

Upgrade Status Message	Condition
Pending	The request has yet to be sent from the CDSM to the device, or receipt of the request has yet to be acknowledged by the device.
Downloading	The download method for the software file is being determined.
Proceeding with Pre-positioned Download	The download method for the software file is detected as pre-positioned. Proceeding with download of a pre-positioned software file.
Proceeding with Download	The download method for the software file is detected as direct download. Proceeding with the request for direct download of the software file.
Download in Progress (Completed …)	Direct download of the software file is being processed. “Completed” indicates the number of megabytes processed.
Download Successful	The direct download of the software file has been successful.
Download Failed	The direct download of the software file cannot be processed. Further troubleshooting is required; see the device system message log.
Proceeding with Flash Write	A request has been made to write the software file to the device flash memory.
Flash Write in Progress (Completed …)	The write of the device flash memory is being processed. “Completed” indicates the number of megabytes processed.
Flash Write Successful	The flash write of the software file has been successful.

Table 9-1 Upgrade Status Messages (continued)

Upgrade Status Message	Condition
Reloading	A request to reload the device has been made to complete the software upgrade. The device may be offline for several minutes.
Reload Needed	A request to reload the device has not been made. The device must be reloaded manually to complete the software upgrade.
Canceled	The software upgrade request was interrupted, or a previous software upgrade request was bypassed from the CLI.
Update Failed	The software upgrade could not be completed. Troubleshooting is required; see the device system message log.

Software Upgrades by Device

Use this upgrade procedure for Service Routers and CDSMs. You can also use this upgrade procedure to upgrade Service Engines one at a time.

To upgrade your software on a single device, follow these steps:

Step 1 Choose **Devices > Devices**. The Devices Table page is displayed.

Step 2 Click the **Edit** icon of the device that you want to upgrade. The Devices home page is displayed.

Step 3 Verify that the device is not already running the version that you plan to upgrade to, and that the current version has an upgrade path to the version that you plan to upgrade to.

Step 4 Click **Update Software**. The Software Update page is displayed.

Step 5 Choose the software file URL from the Software Files list by clicking the radio button next to the filename.

Step 6 Click **Submit**, and then click **OK** to confirm your decision.

The Devices Table page is displayed again. You can monitor the progress of your upgrade from this page.

Software upgrade status messages are displayed in the Software Version column. These intermediate messages are also written to the system log on the Service Engines. See Table 9-1 for a description of upgrade status messages.

Note For a Service Engine with physical memory less than 32 GB, if the cached file entries is less than 16 million, the Content Manager will run with the max-cached-entries value of 16 million after upgrading the software image to 4.0. If the cached file entries is greater than 16 million, the Content Manager runs with the max-cached-entries value of 20 million after upgrading the software image to 4.0.

Rebooting Devices

You can reboot a device or device group. The CDSM performs a controlled shutdown of all devices and then restarts the operating system on each device.

To reboot an individual device, follow these steps:

Step 1 Choose **Devices > Devices**.

Step 2 Click the **Edit** icon next to the device name that you want to reboot. The Devices home page is displayed

Step 3 In the task bar, click the **Reload** icon. You are prompted to confirm your decision.

Step 4 To begin rebooting the device, click **OK**.

To reboot an entire device group, follow these steps:

Step 1 Choose **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the name of the device group that you want to reboot. The Device Group page is displayed.

Step 3 In the task bar, click the **Reboot All Devices in Device Group** icon. You are prompted to confirm your decision.

Step 4 To begin rebooting each SE in the device group, click **OK**.

Deleting a Device

You can delete a device if the device is experiencing unresolvable problems or when its network address or configuration has changed and you need to add the device back to the VDS-IS network using its new address and configuration information.

Caution If you delete the only SR in your VDS-IS network, you are removing the ability of your VDS-IS network to fill user requests.

When you delete an SE from the VDS-IS network, you are removing that device and the content it contains from the routing scheme that the VDS-IS uses to fill user requests. Although the VDS-IS routes requests around SEs that are busy, offline, or missing, removing an SE may affect the speed at which the VDS-IS network can serve user requests.

Note You cannot delete an SE if it is the only device assigned to a location that is designated as the root location (Content Acquirer) for a Delivery Service and there are other SEs associated with the Delivery Service. You can delete the Content Acquirer for a Delivery Service if the Content Acquirer is the only SE associated with that Delivery Service. However, deleting the only SE in a Delivery Service makes the Delivery Service unable to deliver content. If you receive an error message referencing the Content

Acquirer for a Delivery Service, add more SEs to that location, or change the root location by choosing an SE in a different location to be the Content Acquirer for the Delivery Service before attempting to delete the SE again.

Removing the device from the VDS-IS network involves using the CLI to shut down VDS-IS network services and deregister the node. If you are removing the device because of hardware failure and it cannot be accessed through its CLI, you can remove the device by using the CDSM; however, the device continues to store its registration information until you deregister it by using the CLI.

Before a device can be removed from the VDS-IS network, the following conditions must be met:

- The device must have been activated in the CDSM.
- The CDSM must be operating.
- The device must have the correct CDSM IP address or hostname configured.
- The CDSM IP address or hostname must be that of the primary CDSM.
- The device must not be the Content Acquirer for any Delivery Service.

Deleting a device from the VDS-IS network involves using the CLI to remove the registration information from the device itself and removing the registration record from the CDSM.

Note Do not use the CDSM to delete a device while the device is still active and registered. The CDSM delete feature removes only the device’s registration record from the CDSM; it does not deregister the device. The device retains its registration information and continues to contact the CDSM; however, the CDSM no longer recognizes the device.

If for some reason the CDSM loses the registration record of a device, use the **cms deregister force** command on the device to remove all of its registration information. Then use the **cms enable** command to reregister the device with the CDSM as though it were a new node in the VDS-IS network.

To remove and deregister a device, follow these steps:

Step 1 Open an SSH session to the device CLI.

Step 2 In global configuration mode, enter the **no cms enable** command:

```
SE# configure
SE(config)# no cms enable
```

Note Issuing the **no cms enable** command does not disable acquisition and distribution services on the device; however, issuing the **cms deregister** command does. The **cms deregister** command disables the CMS, all acquisition and distribution services, and all routing communications to and from this device.

Step 3 In EXEC mode, enter the **cms deregister** command:

```
SE(config)# exit
SE# cms deregister
```

Note The **cms deregister** command cleans up the database automatically. You do not need to use the **cms database delete** command.

If the deregistration fails, the best practice is to resolve any issues that caused the deregistration failure; for example, the Service Engine is the Content Acquirer of a Delivery Service and cannot be deleted or deactivated. In this case, assign a different SE as the Content Acquirer in each Delivery Service where this SE is assigned as the Content Acquirer and try the **cms deregister** command again.

Step 4 If for some reason the deregistration fails, you can force the deregistration by using the **cms deregister force** command:

```
SE# cms deregister force
```

Note Take note of any messages stating that the deregistration failed and make sure to resolve them before reregistering the device with the same CDSM or registering the device to another CDSM. The **cms deregister force** command forces the deregistration to continue.

Step 5 To add the device back into the VDS-IS network, reregister the device with the CDSM by using the **cms enable** command in global configuration mode:

```
SE# configure
SE(config)# cms enable
```

In case of a hardware failure, you might need to remove the device from the VDS-IS network routing scheme by using the CDSM.

Before a device can be removed from the VDS-IS network through the CDSM, the following conditions must be met:

- The device must have been activated in the CDSM.
- The CDSM must be running.
- The device must have the correct CDSM IP address or hostname configured.
- The CDSM IP address or hostname must point to the primary CDSM.
- The device must not be the Content Acquirer for any Delivery Service.

To delete a device using the CDSM, follow these steps:

Step 1 Choose **Devices** > **Devices**. The Devices Table page is displayed. The online status of the device is listed in the Status column.

Step 2 Click the **Edit** icon next to the device name that you want to delete. The Devices home page is displayed.

Step 3 In the task bar, click the **Delete Device** icon. You are prompted to confirm your decision.

Step 4 To execute your request, click **OK**. The device is removed from the CDSM.

Step 5 If possible, access the device CLI to deregister the device.

Step 6 In the CLI, enter the **cms deregister force** command.

Note You must use the **cms deregister force** command after deleting a device in the CDSM. This is because once the device has been deleted, the CDSM no longer has a record of the device.

Step 7 To add the device back in to the VDS-IS network, reregister the device with the CDSM by using the **cms enable** command in global configuration mode.

Deleting a Warm Standby CDSM

You can delete a warm standby CDSM from the VDS-IS network at any point after you have registered the device and before the device has come online as the primary CDSM. Once the device has been called into use as the primary CDSM, however, you cannot delete it by using the CDSM.

Delete a warm standby CDSM when the device is experiencing unresolvable problems or when its network address or configuration has changed and you need to add the device back to the VDS-IS network by using its new address and configuration information.

To delete a warm standby CDSM, follow these steps:

Step 1 Log in directly to the CDSM CLI, and enter the **cms deregister** command.

If, for some reason, the deregistration fails, you can force the deregistration by using the **cms deregister force** command.

Step 2 From the CDSM GUI, choose **Devices > Devices**.

The browser refreshes, listing the CDSMs on your VDS-IS network. The warm standby CDSM is identified as *Standby*.

Step 3 Click the **Edit** icon next to the name of the warm standby CDSM. The Devices home page is displayed.

Step 4 From the left-pane menu, choose **Device Activation**. The Activation page is displayed.

Step 5 In the task bar, click the **Delete** icon. You are prompted to confirm your decision.

Step 6 To execute your request, click **OK**.

Replacing a Device

The procedure to replace a device in the VDS-IS is different depending on the type of the device being replaced. This section covers the following procedures:

- Replacing a CDSM, page 9-13
- Replacing an SE or SR, page 9-14

Replacing a CDSM

To replace a CDSM in a VDS-IS, you must first add the new CDSM into the network as a standby CDSM. For procedural information, see the “Configuring Primary and Standby CDSMs” section on page 3-11.

Note The primary and standby CDSMs must be running the same version of software. You must first add the new CDSM with the same version as the existing CDSM. Once the standby CDSM has been added, you must wait at least two polling intervals (10 minutes) for the databases to synchronize before you can begin the upgrade procedure.

Note After you have activated the standby CDSM using the primary CDSM web interface and the device shows as online in the Devices Table page, wait at least two polling intervals (10 minutes) before changing roles to ensure that the standby CDSM has a record of the most recent configuration changes.

To promote the standby CDSM to primary, first stop the primary CDSM using the **cdsm role standby** command. For procedural information, see the "Changing a Standby CDSM to a Primary CDSM" section on page 3-12.

After the primary CDSM has been stopped, and the standby CDSM has taken the role of primary, wait at least two polling intervals (10 minutes) before logging in to the new primary CDSM. The new primary CDSM is accessible by entering the IP address of the CDSM with port 8443 in a web browser. For example, if the IP address of your CDSM is 192.168.0.236, enter **https://192.168.0.236:8443**.

It is now safe to deactivate the old primary CDSM in the CDSM web interface and remove it from the VDS-IS network.

Note Do not try to back up the old CDSM database and restore it on the new CDSM. This may lead to problematic issues.

Replacing an SE or SR

Note If you replace a Content Acquirer with an SE that was not previously assigned to the Delivery Service, all content is reacquired and the old content is deleted.

Note To prevent the reacquisition of content when replacing a Content Acquirer, make one of the receiver SEs in the same Delivery Service the replacement Content Acquirer. Add the new SE as a receiver SE, wait until replication is complete for the newly added SE, and then designate it as the Content Acquirer. When you replace a Content Acquirer in this manner, the SEs in the Delivery Service synchronize with the new Content Acquirer through the metadata poll. Content is not redistributed to the other SEs in the Delivery Service unless the content has changed since the last metadata poll.

To replace an SE or SR, follow these steps:

Step 1 Open an SSH session to the device being replaced.

Step 2 In global configuration mode, enter the **no cms enable** command to disable CMS on the device that needs to be replaced.

```
SE# configure
SE(config)# no cms enable
```

Step 3 From the CDSM, choose **Devices > Devices > Device Activation**. The Device Activation page is displayed.

Step 4 Uncheck the **Activate** check box and click **Submit**. The page refreshes and displays a **Replaceable** check box.

Step 5 Check the **Replaceable** check box and click **Submit**.

Step 6 Choose **System > Configuration > System Properties**. The System Properties page is displayed.

Step 7 Click the edit icon next to the **System.devivce.recovery.key** property. The Modify Config Property page is displayed.

Step 8 In the **Value** field, enter a key and click **Submit**. The default value is default.

Step 9 Follow the instructions for configuring a device using the setup utility. The instructions can be found in the *Cisco Content Delivery Engine Hardware Installation Guide* that is applicable to your device.

Note The replacement device must be the same hardware model as that of the device being replaced.

a. When prompted by the setup utility, configure the basic network settings.

b. When prompted by the setup utility for the hostname of the new device, use the same hostname of the device being replaced. For example, if the old device has a hostname of “SE1,” the new device must have a hostname of “SE1.”

c. When prompted by the setup utility for the IP address of the CDSM, enter the IP address of the CDSM.

Step 10 Open an SSH session to the new device.

Step 11 In EXEC mode, enter the **cms recover identity** command with the key parameter that you set in Step 8:

```
SE# cms recover identity <key>
```

On successful registration to the CDSM, a message similar to the following is displayed:

```
DT-7326-4#cms recover identity sr
Registering this node as Service Router...
Sending identity recovery request with key sr
Node successfully registered with id CrConfig_291
Registration complete.
```

Step 12 Register the device with the CDSM by using the **cms enable** command in global configuration mode:

```
SE# configure
SE(config)# cms enable
```

Step 13 From the CDSM, choose **Devices > Devices > Device Activation**. The Device Activation page is displayed.

Step 14 Check the **Activate** check box and click **Submit**.

After a few minutes, approximately two polling intervals, the device status appears online and all configurations (Delivery Service assignments, programs, and so on) are the same as those on the device that was replaced.

Step 15 Once the new device is up and running, as noted by the online status, the old device can be removed from the VDS-IS network.

Backup and Recovery Procedures

This section describes the CDSM database backup and VDS-IS software recovery procedures.

- Performing Backup and Restore on the CDSM Database, page 9-16
- Using the Cisco VDS-IS Software Recovery CD-ROM, page 9-17
- Recovering the System Software, page 9-19
- Recovering a Lost Administrator Password, page 9-22
- Recovering from Missing Disk-based Software, page 9-23
- Recovering VDS-IS Network Device Registration Information, page 9-25

Performing Backup and Restore on the CDSM Database

The CDSM stores VDS-IS 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 CDSM, use the **cms database backup** EXEC command.

Note The naming convention for backup files includes the timestamp.

To back up and restore the CMS database on the CDSM, follow these steps:

Step 1 Back up the CMS database to a file:

```
CDE# cms database backup
creating backup file backup-db-11-06-2007-13-10.dump
backup file local1/backup-db-11-06-2007-13-10.dump is ready.
Please use ‘copy’ 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, as shown in the following example:

```
CDE# cd /local/local1
CDE# copy disk ftp 10.86.32.82 /incoming cds-db-9-22-2002-17-36.dump
cds-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-3.0.1-18) 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 cds-db-9-22-2002-17-36.dump
```

```
Opening BINARY mode data connection for cds-db-9-22-2002-17-36.dump.
Transfer complete.
Sent 18155 bytes
```

Step 3 Delete the existing CMS database:

```
CDE# cms database delete
```

Step 4 Restore the CMS database contents from the backup file:

```
CDE# cms database restore cds-db-9-22-2002-17-36
```

Step 5 Enable CMS:

```
CDE# cms enable
```

Using the Cisco VDS-IS Software Recovery CD-ROM

A software recovery CD-ROM image (.iso file) is available for each software release. The recovery CD-ROM can be used to recover system software that must be completely reimaged. The recovery CD-ROM image contains the system software for a single software release and a single application software.

This section provides instructions for creating and 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 with a later release than the software recovery CD-ROM image file that you downloaded, using the CD-ROM software recovery images may downgrade your system.

System Software Components

Cisco VDS-IS software consists 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 the VDS-IS software to work properly.

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

- A .bin image containing disk and flash memory components

  An installation containing only the VDS-IS 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 the flash memory only, without modifying the disk contents.

Getting the Cisco VDS-IS Software Recovery File from Cisco.com

To get a software file from Cisco.com, follow these steps:

Step 1 Launch your web browser and enter the following URL:

http://www.cisco.com/kobayashi/sw-center/sw-video.shtml

The Log In page is displayed.

Step 2 Log in to Cisco.com using your designated username and password. The Video and Content Delivery page is displayed, listing the available software products.

Step 3 Click **Cisco Content Delivery Systems (CDS)**. The Downloads page is displayed.

Step 4 Click the **Cisco Content Delivery Applications** folder to expand it, and click the **Cisco Internet Streamer Application**. The page refreshes and the software releases are displayed.

Step 5 Click the link for the software recovery file that you want to download.

- If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click **Accept**.
- If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form does not display again.

The Download page is displayed with the information about the software image file and a Download link.

Step 6 Click **Download**. The Cisco End User Software License Agreement is displayed.

Step 7 Read the agreement and click **Agree**. The File Download dialog box is displayed.

Step 8 Click **Save**. The Save As dialog box is displayed.

Step 9 Navigate to the location where you want to save the file and click **Save**. The file downloads.

Step 10 Burn the software recovery image file onto a CD-ROM.

Installing the Software Using the Recovery CD-ROM

To install the system software by using the recovery CD-ROM, perform the following steps:

Step 1 Plug a USB CD-ROM drive into a USB port on the device.

Step 2 Insert the recovery software CD-ROM into the USB CD-ROM drive, and boot the device.

Step 3 When the installer menu appears, choose **2 Install all Software**.

Step 4 Wait for the process to complete.

Step 5 Before you reboot the device, remove the USB CD-ROM drive from the USB port so that the device boots from flash memory.

Step 6 Reboot the device.

Recovering the System Software

The Service Engine, Service Router, and CDSM 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.

Note The .sysimg file is located under the images folder on the Recovery CD-ROM. If you have upgraded the VDS-IS software, download the corresponding rescue CD iso image, copy to a CD and use the rescue iso image.

To install a new system image using the rescue image, follow these 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 switch.

The rescue image dialog appears. The following example demonstrates how to interact with the rescue dialog and use a port channel for the network connection (user input is denoted by entries in bold typeface). This example is for the CDE220-2G2, which has 10 Gigabit Ethernet interfaces. The CDE110 and CDE205 have 2 Gigabit Ethernet interfaces and the has 14 Gigabit Ethernet interfaces.

```
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
    - FTP server IP address
    - username/password on FTP server
- path to system image on server

System Recovery Menu:
    1. Configure Network
    2. Download and install system image
    3. Exit (and reboot)
Choice [1]: 1

Network Configuration Menu:
    1. Configure ethernet interface
    2. Configure portchannel interface
    3. Exit to main menu
Choice [1]: 2

Please enter an interface from the following list:
   0. GigabitEthernet 1/0
   1. GigabitEthernet 2/0
   2. GigabitEthernet 3/0
   3. GigabitEthernet 4/0
   4. GigabitEthernet 5/0
   5. GigabitEthernet 6/0
   6. GigabitEthernet 7/0
   7. GigabitEthernet 8/0
   8. GigabitEthernet 9/0
   9. GigabitEthernet 10/0
  10. Done
    0
Please select an interface from the list below:
   0. GigabitEthernet 1/0 [Use]
   1. GigabitEthernet 2/0
   2. GigabitEthernet 3/0
   3. GigabitEthernet 4/0
   4. GigabitEthernet 5/0
   5. GigabitEthernet 6/0
   6. GigabitEthernet 7/0
   7. GigabitEthernet 8/0
   8. GigabitEthernet 9/0
   9. GigabitEthernet 10/0
  10. Done
Choice [1]: 1

Please select an interface from the list below:
   0. GigabitEthernet 1/0 [Use]
   1. GigabitEthernet 2/0 [Use]
   2. GigabitEthernet 3/0
   3. GigabitEthernet 4/0
   4. GigabitEthernet 5/0
   5. GigabitEthernet 6/0
   6. GigabitEthernet 7/0
   7. GigabitEthernet 8/0
   8. GigabitEthernet 9/0
   9. GigabitEthernet 10/0
  10. Done
Choice [2]: 10

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

Network Configuration Menu:
    1. Configure ethernet interface
    2. Configure portchannel interface (done)
    3. Exit to main menu
Choice [3]: 3

System Recovery Menu:
    1. Configure Network (done)
    2. Download and install system image
    3. Exit (and reboot)
Choice [2]: 2

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]: CDS24.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: CDS-24.sysimg

Attempting download...
Downloaded 34234368 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.

System Recovery Menu:
    1. Configure Network (done)
    2. Download and install system image (done)
    3. Exit (and reboot)
Choice [3]: 3
Restarting system.
```

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
Content Delivery System Software (CDS)
Copyright (c) 2007 by Cisco Systems, Inc.
Content Delivery System Software Release 3.0.0 (build b460 July 5 2011)
Version: se507-2.4.0

Compiled 02:34:38 July 15 2009 by (cisco)
Compile Time Options: PP SS

System was restarted on Thu July 15 16:03:51 2009.
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 mis-configured, you need 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.

To reset the password, follow these steps:

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 CDS boot:hit RETURN to set boot flags:0009
```

Step 3 When prompted to enter bootflags, enter the **0x800** value:

```
Available boot flags (enter the sum of the desired flags):
0x0000 - exit this menu and continue booting normally
0x2000 - ignore Carrier Detect on console
0x4000 - bypass nvram config
0x8000 - disable login security

[SE 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 Service Engine Console

Username: admin
```

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

```
ServiceEngine# configure
ServiceEngine(config)# username admin password 0 password
```

You can specify that the password be either clear text or encrypted. Zero (0) means the password is displayed as a plain word; one (1) means the password is encrypted.The password strength must be a combination of alphabetic character, at least one number, at least one special character, and at least one uppercase character.

Note Do not set the user ID (uid).

Step 6 Save the configuration change by using the **write memory** command in EXEC mode:

```
ServiceEngine(config)# exit
```

```
ServiceEngine# write memory
```

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

```
ServiceEngine# 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 VDS-IS 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 both system disks is corrupt or missing.

There are two types of disk volumes in the VDS-IS: system disk volumes (which contain all of the system volumes plus the sysfs volume) and cdnfs disk volumes. A disk is either allocated as a system disk or a cdnfs disk (on some CDEs, a system disk might contain a cdnfs volume). The system volumes, contain data and applications that are critical to the system's basic functionality.

The system volumes are stored in a two-disk RAID-1 (mirrored) array. RAID-1 duplicates data between each of the disks in the array. The two-disk scheme allows for either of the drives in the system volumes array to fail without sustaining data loss or incurring system errors.

The status of the volumes can be seen through the **show disk raid-state** command, and can be in any of the following states:

- Normal—Both drives are attached, and data is mirrored between them.
- Syncing—Data is being copied between the drives to restore the volumes to a normal state. This typically happens when a new drive is added to repair degraded volumes.
- Degraded—One of the disks has failed. We highly recommend that a new disk is added to repair the volumes.
- Bad—Both disks have failed. The system has likely lost all but basic functionality.

Note If both system disks fail, a VDS-IS state of "missing disk-based software" occurs.
Normally, when a problem occurs on one system disk, a disk failure or RAID alarm is triggered. If this occurs, replace the failed disk. See the "Disk Maintenance" section on page 9-27.

The VDS-IS state of "missing disk-based software" is most likely to occur if you replaced both system disks in your Service Engine, Service Router, or CDSM. By design, the software installation on the system disks cannot be corrupted by a system failure or a power failure.

If both system disks fail or are missing, the software continues to run. However, it runs in a basic functionality mode in which HTTP proxy and related HTTP features still work, but most other features fail.

The compact flash functionality is merged on to the system disk in a non-CDE platform. If both system disks fail or are missing on a non-CDE platform, the non-CDE device can not function and needs to have the VDS-IS software reinstalled by using the Recovery CD-ROM. For more information, see the "Using the Cisco VDS-IS Software Recovery CD-ROM" section on page 9-17.

Caution This procedure should only be used as a last-resort method to recover the system software on a unit. Typically, the system automatically repairs itself across a reboot if any new disks are detected. If the volumes are degraded and a new disk is present at reboot, the new disk is added to the existing array (sync starts). If the volumes are “bad” and a new disk is present at reboot, the initial system volume is built on the disk.

To recover from this condition, follow these steps:

Step 1 Remove the Service Engine record from the CDSM.

a. Choose **Devices > Devices**.

b. Click the **Edit** icon next to the name of the Service Engine that you want to delete. The Devices home page is displayed.

c. Click the **Delete** icon. You are prompted to confirm your decision.

d. Click **OK** to execute your request. The Service Engine is removed from the CDSM.

Note The Service Engine registration record needs to be deleted from the CDSM for the Service Engine to complete reregistration after it comes back online. The CDSM does not register a device if the device already appears in the record as registered.

Step 2 Power off the device and replace the failed or missing system disks with new, blank disks.

Step 3 After the new disks are installed, power on the device.

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

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

```
Jan 21 21:55:45 (none) ruby_disk:%SE-DISK-2-200024:First disk not in standard
configuration. Run 'disk recover-system-volumes' command and re-install software.
ruby_disk:Your first disk is not in standard configuration.
ruby_disk:Run 'disk recover-system-volumes' from the CLI

********************************************
    System software is missing.
    Check whether first-disk is bad, or
    use 'disk recover-system-volumes' to recover first-disk.
********************************************
```

Step 5 Log in as **admin**:

```
Cisco Service Engine Console

Username: admin
Password:
System Initialization Finished.

SE-507 con now available

Press RETURN to get started!
```

Step 6 After logging in to a console or SSH session, enter the **copy ftp install** or **copy http install** EXEC command to download and install a new system image.

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

For example:

```
SE# copy ftp install vista /CDS/upgrades CDS-2.0.0.2-K9.bin
Enter username for remote ftp server: biff
Enter password for remote ftp server:
Initiating FTP download...
printing one # per 1MB downloaded
Reclaiming unused safe state sectors...
############################################################################
###########
############################################################################
###########
Installing phase3 bootloader...
Installing system image to flash: done
The new software will run after you reload.
#
ServiceEngine# show flash
CDS software version (disk-based code): CDS-2.0.1-b130

System image on flash:
Version: 2.0.1.2

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

Step 7 Reboot the software with the new disk and new system image by entering the **reload** EXEC command:

```
SE# reload
```

Step 8 Register the device with the CDSM by using the **cms enable** command in global configuration mode:

```
SE# configure
SE(config)# cms enable
```

Recovering VDS-IS Network Device Registration Information

Device registration information is stored both on the device itself and on the CDSM. If a device loses its registration identity or needs to be replaced because of hardware failure, the VDS-IS 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 CDSM.

a. Choose **Devices > Devices**.

b. Click the **Edit** icon next to the name of the Service Engine that you want to deactivate. The Devices home page is displayed.

c. From the left-panel menu, choose **Device Activation**.

d. Uncheck the **Activate** check box. The page 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 displays when the device is inactive.

Step 2 Configure a system device recovery key.

a. Choose **System > Configuration**.

b. Click the **Edit** icon next to the System.device.recovery.key property. The Modifying Config Property page is displayed.

c. 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.

Step 4 Open an SSH session to the device CLI and enter the **cms recover identity** *keyword* EXEC command, where *keyword* is the device recovery key that you configured in the CDSM.

When the CDSM receives the recovery request from the Service Engine, it searches its database for the Service Engine record that meets the following criteria:

- The record is inactive and replaceable.
- The record has the same hostname 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 Service Engine record, then the CDSM updates the existing record and sends the requesting Service Engine a registration response. The replaceable state is cleared so that no other device can assume the same identity. When the Service Engine receives its recovered registration information, it writes it to file, initializes its database tables, and starts.

Step 5 Return to the CDSM and activate the device.

a. Choose **Devices > Devices**.

b. Click the **Edit** icon next to the name of the Service Engine that you want to activate. The Devices home page is displayed.

c. From the left-panel menu, choose **Device Activation**. The Service Engine status should be Online.

d. Check the **Activate** check box and click **Submit**.

Note If you are replacing an old device with a different hardware model, check the following hardware-related settings and adjust them according to your needs, after the new device is online in CDSM GUI:

- IP Access List settings associated with network interfaces
- Disk quota settings of VOD-type delivery services
- Default and maximum bandwidth setting of Windows Media Streaming and Movie Streamer
- Service Monitor Disk Failure Percent Settings

Disk Maintenance

- Disk Error Handling, page 9-27
- Removing and Replacing Disk Drives, page 9-34

Disk Error Handling

When sector I/O errors on a disk exceed the Disk Error Handling Thresholds, the disk is marked as bad. The following tasks are performed when a disk is marked as bad:

- Raise a disk_failure alarm
- Forcibly unmount the disk
- Inform the CAL/UNS layer of any CDNFS partitions that are marked as bad so that they cannot be used for streaming (CDNFS partitions only)
- Intentionally invalidate the Master Boot Record (MBR) of the disk, thereby destroying any cached content. This eliminates the possibility of reusing potentially corrupt cached content. This essentially removes the disk from the CDNFS file-system.

The disk must be repaired before it can be reused by the VDS-IS system software.

For information about disk error handling thresholds, see the "Enabling Disk Error Handling" section on page 4-65.

The following sections cover detecting disk sector errors and repairing them:

- Disk Latent Sector Error Handling, page 9-27
- SMART Sector Errors, page 9-28
- disk repair Command, page 9-32

Disk Latent Sector Error Handling

Latent Sector Errors (LSEs) are when a particular disk sector cannot be read from or written to, or when there is an uncorrectable ECC error. Any data previously stored in the sector is lost. There is also a high probability that sectors in close proximity to the known bad sector have as yet undetected errors, and therefore are included in the repair process.

The syslog file shows the following disk I/O error message when there are disk sector errors:

```
Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-4-900000: end_request: I/O error, dev sdd,
sector 4660
Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-3-900000: Buffer I/O error on device sdd,
logical block 582
```

SMART Sector Errors

Typically, the indication that a hard disk drive (HDD) is bad and needs to be replaced is if the **show disk SMART-info detail** command output exceeds the values described in Table 9-2. Solid state drives (SSDs) do not report pending errored sector attributes in the **show disk SMART-info detail** command output.

Table 9-2 Output Values of show disk SMART-info detail Command Indicating Disk Replacement

Field	CDNFS and SYSTEM Drives—Threshold Raw Values
Reallocated_Sector_Ct raw_value	128
Current_Pending_Sector raw_value	30
Offline_Uncorrectable raw_value	30

A drive needs to be replaced if any of the RAW_VALUEs listed in Table 9-2 are exceeded.

The **show disk SMART-info** command (without the **detail** keyword), provides information on the overall health of each HDD or SSD. The following example of the **show disk SMART-info** command output shows that disk08 is bad:

```
# show disk SMART-info

      … etc …

=== disk08 ===
smartctl 5.40 2010-10-16 r3189 [i686-pc-linux-gnu] (local build)
Copyright (C) 2002-10 by Bruce Allen, http://smartmontools.sourceforge.net

=== START OF INFORMATION SECTION ===
Model Family:     Seagate Barracuda ES.2
Device Model:     ST3500320NS
Serial Number:    9QM92HZ0
Firmware Version: SN05
User Capacity:    500,107,862,016 bytes
Device is:        In smartctl database [for details use: -P show]
ATA Version is:   8
ATA Standard is:  ATA-8-ACS revision 4
Local Time is:    Tue Jul 19 04:42:16 2011 PDT

==> WARNING: There are known problems with these drives,
see the following Seagate web pages:
http://seagate.custkb.com/seagate/crm/selfservice/search.jsp?DocId=207931
http://seagate.custkb.com/seagate/crm/selfservice/search.jsp?DocId=207963

SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: FAILED!
Drive failure expected in less than 24 hours. SAVE ALL DATA.
Failed Attributes:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  5 Reallocated_Sector_Ct   0x0033   025   025   036    Pre-fail  Always   FAILING_NOW 1548
```

The **show disk SMART-info** command is repeated for each drive. If the overall-health assessment of a drive indicates “FAILED,” then the drive should be replaced. The output of the **show disk SMART-info** command also shows the SMART attributes that indicate drive failure (in the above example, the Reallocated_Sector_Ct attribute indicates FAILING_NOW).

If the **show disk SMART-info details** command output values for Current_Pending_Sector and Offline_Uncorrectable for an HDD are below the threshold described in Table 9-2, then monitor these values over several days. The Latent Sector Error feature attempts to repair such errored sectors in a background process by deleting (evicting) corrupted content. If after several days of monitoring the values for Current_Pending_Sector and Offline_Uncorrectable have not decreased, consider running the **disk repair** command. After the **disk repair** command completes, we recommend that you reboot the SE to ensure all VDS-IS software services are functioning correctly.

If the output values for Current_Pending_Sector and Offline_Uncorrectable for an HDD are above the threshold described in Table 9-2, then you need to replace the disk.

Note The **disk repair** command deletes all cached video content on the drive and takes approximately three hours to complete per HDD. The **disk repair** command takes approximately 30 minutes on a solid-state drive (SSD).

Table 9-3 provides an example of the last part of the output of the **show disk SMART-info detail** command. The attributes that need to be reviewed to determine if the drive needs to be replaced or repaired are highlighted in bold. A drive needs to be replaced if any of the RAW_VALUEs listed in Table 9-2 are exceeded. In this example, because the Reallocated_Sector_Ct value is greater than 128, this drive should be replaced.

Table 9-3 RMA Case—Replace HDD Example

ID#	ATTRIBUTE_NAME	FLAG	VALUE	WORST	THRESH	TYPE	UPDATED	RAW_VALUE
1	Raw_Read_Error_Rate	0x000f	072	063	044	Pre-fail	Always	59861501
3	Spin_Up_Time	0x0003	099	099	000	Pre-fail	Always	0
4	Start_Stop_Count	0x0032	100	100	020	Old_age	Always	12
5	**Reallocated_Sector_Ct**	**0x0033**	**099**	**099**	**036**	**Pre-fail**	**Always**	**130**
7	Seek_Error_Rate	0x000f	072	060	030	Pre-fail	Always	17169006
9	Power_On_Hours	0x0032	090	090	000	Old_age	Always	9010
10	Spin_Retry_Count	0x0013	100	100	097	Pre-fail	Always	0
12	Power_Cycle_Count	0x0032	100	037	020	Old_age	Always	12
184	Unknown_Attribute	0x0032	100	100	099	Old_age	Always	0
187	Reported_Uncorrect	0x0032	093	093	000	Old_age	Always	**7**
188	Unknown_Attribute	0x0032	100	100	000	Old_age	Always	0
189	High_Fly_Writes	0x003a	100	100	000	Old_age	Always	0
190	Airflow_Temperature_Cel	0x0022	071	069	045	Old_age	Always	29 (Lifetime Min/Max 28/29)
194	Temperature_Celsius	0x0022	029	040	000	Old_age	Always	29 (0 22 0 0)
195	Hardware_ECC_Recovered	0x001a	052	011	000	Old_age	Always	59861501
197	**Current_Pending_Sector**	**0x0012**	**100**	**100**	**000**	**Old_age**	**Always**	**1**

Table 9-3 RMA Case—Replace HDD Example (continued)

ID#	ATTRIBUTE_NAME	FLAG	VALUE	WORST	THRESH	TYPE	UPDATED	RAW_VALUE
198	**Offline_Uncorrectable**	**0x0010**	**100**	**100**	**000**	**Old_age**	**Offline**	**1**
199	UDMA_CRC_Error_Count	0x003e	200	200	000	Old_age	Always	0

Table 9-4 provides an example of the last part of the output of the of the **show disk SMART-info detail** command. The attributes that need to be reviewed to determine if the drive needs to be replaced or repaired are highlighted in bold. In this example, the Current_Pending_Sector and Offline_Uncorrectable each have a value greater than one, so monitor these values over several days. The Latent Sector Error feature attempts to repair such errored sectors in a background process by deleting (evicting) corrupted content. If after several days of monitoring the values for Current_Pending_Sector and Offline_Uncorrectable have not decreased, consider running the **disk repair** command.

Table 9-4 Disk Repair Case—Repair HDD Example

ID#	ATTRIBUTE_NAME	FLAG	VALUE	WORST	THRESH	TYPE	UPDATED	RAW_VALUE
1	Raw_Read_Error_Rate	0x000f	072	063	044	Pre-fail	Always	59861501
3	Spin_Up_Time	0x0003	099	099	000	Pre-fail	Always	0
4	Start_Stop_Count	0x0032	100	100	020	Old_age	Always	12
5	**Reallocated_Sector_Ct**	**0x0033**	**099**	**099**	**036**	**Pre-fail**	**Always**	**5**
7	Seek_Error_Rate	0x000f	072	060	030	Pre-fail	Always	17169006
9	Power_On_Hours	0x0032	090	090	000	Old_age	Always	9010
10	Spin_Retry_Count	0x0013	100	100	097	Pre-fail	Always	0
12	Power_Cycle_Count	0x0032	100	037	020	Old_age	Always	12
184	Unknown_Attribute	0x0032	100	100	099	Old_age	Always	0
187	Reported_Uncorrect	0x0032	093	093	000	Old_age	Always	**0**
188	Unknown_Attribute	0x0032	100	100	000	Old_age	Always	0
189	High_Fly_Writes	0x003a	100	100	000	Old_age	Always	0
190	Airflow_Temperature_Cel	0x0022	071	069	045	Old_age	Always	29 (Lifetime Min/Max 28/29)
194	Temperature_Celsius	0x0022	029	040	000	Old_age	Always	29 (0 22 0 0)
195	Hardware_ECC_Recovered	0x001a	052	011	000	Old_age	Always	59861501
197	**Current_Pending_Sector**	**0x0012**	**100**	**100**	**000**	**Old_age**	**Always**	**3**
198	**Offline_Uncorrectable**	**0x0010**	**100**	**100**	**000**	**Old_age**	**Offline**	**3**
199	UDMA_CRC_Error_Count	0x003e	200	200	000	Old_age	Always	0

Note The Latent Sector Error feature attempts to repair errored sectors in a background process by deleting (evicting) corrupted content. If after several days of monitoring the values for Current_Pending_Sector and Offline_Uncorrectable have not decreased, consider running the **disk repair** command.

The **show disk SMART-info detail** command only reports sector errors that have been detected; there may be more sectors in error adjacent to the reported bad sector. Repairing the drive also proactively repairs unreported sector errors. However, because repairing a drive is a time-consuming process, it may be easier to just replace the drive if a spare drive is available.

Table 9-5 provides detailed description of the Attribute Names that could indicate disk problems primarily applicable to HDDs.

Table 9-5 Attribute Names Descriptions—Disk Problem Indicators

ID	Attribute Name	Description
5	Reallocated Sectors Count	Count of reallocated sectors. When the hard drive finds a read/write/verification error, it marks that sector as "reallocated" and transfers data to a special reserved area (spare area). This process is also known as remapping, and reallocated sectors are called *remaps*. The raw value normally represents a count of the bad sectors that have been found and remapped; thus, the higher the attribute value, the more sectors the drive has had to reallocate. This allows a drive with bad sectors to continue operation; however, a drive that has had any reallocations at all is significantly more likely to fail in the near future. While primarily used as a metric of the life-expectancy of the drive, this number also affects performance. As the count of reallocated sectors increases, the read/write speed tends to worsen because the drive head is forced to seek to the reserved area whenever a remap is accessed. A workaround, which preserves drive speed at the expense of capacity, is to create a disk partition over the region that contains remaps and instruct the operating system to not use that partition. If the drive can repair the sector without remapping it, then the Reallocated Sectors Count is not incremented. If the drive must remap the sector, the Reallocated Sectors Count is incremented.
197	Current Pending Sector Count	Count of “unstable” sectors (waiting to be remapped, because of read errors). If an unstable sector is subsequently read successfully, this value is decreased and the sector is not remapped. Read errors on a sector do not cause a remap of the sector, because the sector might be readable later. Instead, the drive firmware remembers that the sector needs to be remapped, and remaps it the next time it is written. Running the **disk repair** command resolves these counts.
198	Uncorrectable Sector Count or Offline Uncorrectable or Off-Line Scan Uncorrectable Sector Count	The total count of uncorrectable errors when reading/writing a sector. A rise in the value of this attribute indicates defects of the disk surface, problems in the mechanical subsystem, or both. Running the **disk repair** command resolves these counts.

Other Disk-Related show Commands

Additionally, the CDSM GUI and the CLI on the SEs display information about the disk-related alarms with the **show alarms** command, and information about the disk and sector related errors with the **show disks error-handling** command and the **show disks error-handling details** command. If sector alarms have occurred, enter the **show disk SMART-info details** command on the SE to determine the state of the drive and whether the drive needs to be replaced or potentially manually repaired using the **disk repair** command.

Following is an example of the **show alarms** command output:

```
ServiceEngine# show alarms
Minor Alarms:
```

```
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- -------------------------
   1 badsector            sysmon               disk01
   2 badsector            sysmon               disk08
```

Following is an example of the **show disks error-handling** command output:

```
ServiceEngine# show disks error-handling
disk05: Total bad sectors = 1, total errors = 2
disk10: Total bad sectors = 3, total errors = 9

Total failed disks = 0
```

Following is an example of the **show disks error-handling details** command:

```
ServiceEngine# show disks error-handling details
disk05: Total bad sectors = 1, total errors = 2
        disk05: sector (LBA): 3000005      errors: 2

disk10: Total bad sectors = 3, total errors = 9
        disk10: sector (LBA): 16000        errors: 3
        disk10: sector (LBA): 170001       errors: 4
        disk10: sector (LBA): 180001       errors: 2

Total failed disks = 0
```

The **details** keyword displays the logical block address (LBA) for each bad sector along with the corresponding I/O error count.

disk repair Command

Caution The device should be offline before running the **disk repair** command. Because this command involves complex steps, we recommend that you contact Cisco Technical Support before running it.

The **disk repair** command not only repairs the bad sectors, but reformats the entire drive, so all data on the drive is lost. The difference between the **disk repair** command and the **disk reformat** command is that the **disk format** command only reinitializes the file system and does not repair bad sectors.

The **disk repair** command takes approximately three hours to complete per disk. The **disk repair** command takes approximately 30 minutes on a solid-state drive (SSD).

Running the **disk repair** command erases all content on the drive. Never run the **disk repair** command on a "live" system.

Overview

The **disk repair** command detects and repairs bad sectors across an entire drive on an SE, SR and CDSM, then reformats the drive. All data on the drive is lost, but the sectors are repaired and available for data storage again.

Usage

The **disk repair** command has the following syntax:

```
# disk repair disk_name sector sector_address_in_decimal
```

For example, the following command repairs the sector 4660 on disk02:

```
# disk repair disk02 sector 4660
```

The **sector** keyword is optional. If the **sector** keyword is omitted, the entire disk is repaired. If the **sector** keyword is specified along with the *sector_address_in_decimal*, then only a small area of the disk is repaired (approximately 2 GB on either side of the sector address specified). The **sector** keyword should only be used if the disk has a single sector error; that is, if the output of the **show disk SMART-info details** command shows 1 unrecoverable pending sector in error; otherwise, omit the **sector** keyword to repair the entire disk drive.

A minor alarm is set when an LSE is detected. After the sector is repaired with the **disk repair** command, the alarm is turned off.

```
Minor Alarms:
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- -------------------------
   1 badsector            sysmon               disk11
     May 19 20:40:38.213 UTC, Equipment Alarm, #000003, 1000:445011
     "Device: /dev/sdl, 1 Currently unreadable (pending) sectors"
```

The command is limited to repairing one disk at a time. Supplying multiple disk names to the **disk repair** command is considered invalid input, and results in the command displaying the syntax information.

Output

Following is an example of the output displayed when the **disk repair** command is running:

```
Repairing disk01 [140013/140013] (100%) rate: 51(MB/s) eta: 4(s)
Repaired LBA 286747000 (total: 1)
Repaired LBA 286747999 (total: 2)
Repairing disk01 [140014/140013] (100%) rate: 51(MB/s) eta: 4(s)
Recovery complete (2 sectors repaired)
Check syslog for more details
```

Progress Indicator

The progress indicator is frequently updated to provide the user with up-to-date statistics and progress of the repair. Following is an example of the progress indicator:

```
Repairing disk01 [140013/140013] (100%) rate: 51(MB/s) eta: 4(s)
Repairing disk01 [140013/140013] (100%) rate: 51(MB/s) eta: 4(s)
```

Note Rate and ETA fields provide approximate estimates. The rate field does not indicate the top performance of the drive.

Performance of low-level utilities can vary as much as 30 percent across different VDS-IS releases.

Repair Notice

Each time the **disk repair** command detects and repairs a sector, a simple message is displayed that describes the location of the repair as well as the cumulative total of repairs. Following is an example:

```
Repaired LBA 286747000 (total: 1)
```

Syslog

To provide a history of the repair, the **disk repair** command logs basic test information (start / stop / failures) along with the address of every sector repaired.

```
repair-disk disk01: %SE-UNKNOWN-5-899999: Starting recovery
```

```
repair-disk disk01: %SE-UNKNOWN-5-899999: Repaired LBA 286747000 (total: 1)
repair-disk disk01: %SE-UNKNOWN-5-899999: Repaired LBA 286747999 (total: 2)
repair-disk disk01: %SE-UNKNOWN-5-899999: Recovery complete (2 sectors repaired)
```

Removing and Replacing Disk Drives

In brief, the procedure for replacing a disk is simply to enter the **disk unuse** command, optionally power off the unit, remove the disk, insert the new disk, and reboot. During the reboot, the system automatically detects any new disks and seamlessly allocates their space according to a simple disk-policy heuristic.

The disk policy's design, when adding new disks, is to always favor safety. If when a new disk is added, the disk manager detects "degraded" or "bad" system volumes, the new disk is used to repair the system volumes. Thus, the disk manager always strives to have two disks allocated to the system volumes. If when a new disk is added, the system volumes are "normal" or "syncing," the new disk is added to the cdnfs volume.

For non-CDEs, the system disk cannot be easily replaced. If a system disk needs to be replaced on a non-CDE, it needs to have the VDS-IS software reinstalled by using the Recovery CD-ROM. For more information, see the "Using the Cisco VDS-IS Software Recovery CD-ROM" section on page 9-17.

The CDE250-2S6 and CDE25-2S3i have fixed bay mappings for internal drives. If the internal drives show as "degraded" or "bad" on these platforms and a new drive is inserted into one of the external slots, the disk manager allocates the disk as CDNFS, not SYSTEM. A failed internal drive requires that the CDE be replaced.

Note For the, CDE250-2S6, CDE250-2S8, CDE250-2S9, and CDE250-2S10, because the system disks are internal drives, if the system disk is "bad," the CDE should be replaced. However, it may be possible to repair the internal drive using the **disk repair** command, and let the system rebuild the SYSTEM RAID drives.

The disk numbering on the CDE250 starts on the left side at disk00, with the last disk being disk23.

Figure 9-2 shows the disk numbering on a CDE220.

Figure 9-2 Disk Numbering on a CDE220

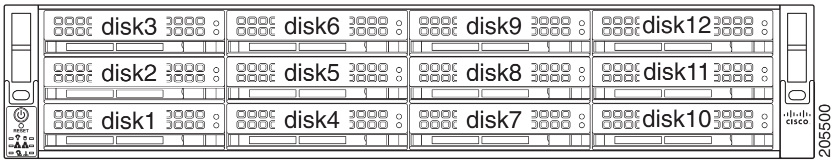
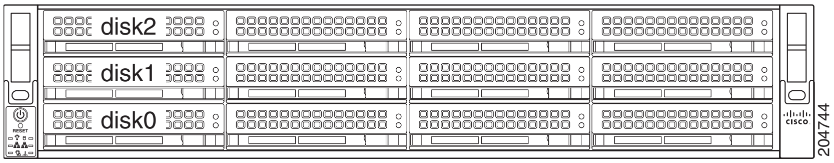


Figure 9-3 shows the disk numbering on a CDE205.

Figure 9-3 Disk Numbering on a CDE205



Replacing a Disk

When replacing a disk, the new disk is recognized and for SYSTEM drives, the RAID is rebuilt. After inserting the new disk, enter the **disk policy apply** command to force the VDS-IS software to detect the new disk and rebuild the RAID. After replacing the disk, we recommend that you reboot the SE to ensure that all VDS-IS software services are functioning correctly.

To replace a disk on a device, follow these steps:

Step 1 Offload the device. In the CDSM GUI, choose **Devices > Devices > Device Activation**, check the **Server Offload** check box, and click **Submit**.

Step 2 Enter the **show disk details** command to see if the drive is mounted. If the drive is mounted, enter the **disk unuse** command to fully unuse the drive. The **disk unuse** command safely shuts down the drive, guaranteeing all background drive activity is halted. This prevents accidental data loss when removing or power cycling the device.

Step 3 Remove the bad disk and insert the new disk.

Step 4 If the output for the **show disk details** command shows the drive bay as “bad,” enter the **disk mark** *diskname* **good** command to mark the drive bay good. For example, if you replaced disk 5 on a CDE220 (see Figure 9-2), you would enter the following command:

```
disk mark disk05 good
```

Step 5 As a precaution, run the **disk erase** *diskXX* command to place the drive in the unformatted state and reboot the device.

Step 6 Enter the **disk policy apply** command to format and mount the drive, examine all disks and RAID volumes, and make any necessary changes. If the device was rebooted after the **disk erase** command, the **disk policy apply** command is started automatically at bootup.

If new drives and system volumes are degraded or bad, the new drive is added as a SYSTEM/RAID volume; otherwise, the drive becomes a CDNFS drive.

Additionally, any detected unused drives are reused (mounted). If there are no new drives and everything is mounted, the command has no effect.

Step 7 Enter the **show disk details** command to see if the drive was added as a SYSTEM drive. If so, enter the **show disk raid** command to verify that the RAID volumes have been completely resynchronized.

Step 8 Return the device to online status. In the CDSM GUI, choose **Devices > Devices > Device Activation**, uncheck the **Server Offload** check box, and click **Submit**.

The VDS-IS software marks the drive bay as good or bad, as opposed to the disk itself. Marking the bay helps to avoid the scenario where a bad disk looks good during the next boot, which, for disks, is almost always the case. As such, simply placing a new disk into a bad bay does not automatically mark the bay good. Once more, if a bad disk is moved to a good bay, the system would not immediately recognize the disk as faulty.

Note Replacing a bad disk with a good disk from another CDE is not supported. If the disk is already in use on another CDE when it is removed and inserted into the current CDE, then the disk is used without reformatting, which creates problems.

The proper way to erase a disk after transplanting is as follows:

```
disk erase diskXX
disk policy apply diskXX
```

Note If you encounter an “unreadable sectors on the disk” condition, contact Cisco Technical Support for information on using the **disk repair** command, For more information about the **disk repair** command, see the “disk repair Command” section on page 9-32.