CHAPTER 5

Maintenance Tasks

These topics describe the Maintenance tasks of Element Manager:

Note The Maintenance menu provides opportunities to monitor your server switch and configure fundamental behavior.

Viewing Basic System Information

Basic system information includes the name and the location of your device and support resources.

To view basic system information, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens. Table 5-1 describes the fields in the window.

Table 5-1 System Info Fields

Field	Description
Description	Description of the chassis and the image that runs on the chassis.
System Uptime	Amount of time that the chassis has run since the last boot.
Last Change Made At	Date and time that a user last changed the running configuration.
Last Config Saved At	Date and time that a user last saved the running configuration as the startup configuration.
System Name	Configurable name for your server switch.
Location	Configurable location of your server switch.
Support Contact	Configurable support information for your server switch.
Rack Locator UID (select chassis)	No longer used.
SystemSyncState	Displays system synchronization state information for the Cisco SFS 7008 only.

Step 2 Click the **Backplane** tab to display the serial number, PCA serial number, PCA assembly number, FRU number, base MAC address, and chassis ID.

Step 3 Click the **Global Setting** tab to display the Global Settings.

Table 5-2 describes the fields in the Global Settings window.

Table 5-2 Global Settings Window Fields

Element	Description
Enable Ib Counter Reset	When checked, resets the Enable Ib counter.
System Operation Mode field	Choose the **Normal** radio button for non-VFrame systems and the **VFrameManaged** radio button for systems in a VFrame environment. For more information, see the VFrame documentation.

Configuring Basic System Information

Basic system information includes the name of your device, the location of your device, and support resources. These topics describe how to configure this information:

Naming Your InfiniBand Switch

To assign a hostname to your device, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens.

Step 2 In the System Name field, type the name that you want to assign to the device, and then click **Apply**.

Defining Device Location

To add a physical device location description to your switch, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens.

Step 2 In the Location field, type the name location of your device, and then click **Apply**.

Defining a Technical Support Resource

The technical support e-mail address that you define appears in the System frame when you refresh or restart Element Manager. To define a technical support resource, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens.

Step 2 In the Support Contact field, type the e-mail address of your technical support provider, and then click **Apply**.

Configuring SystemOperMode

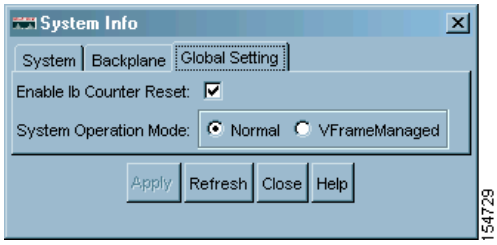
Configure SystemOperMode status to alter the behavior of the server switch to respond appropriately to a VFrame environment or a non-VFrame environment. To configure SystemOperMode, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens.

Step 2 Click the **Global Setting** tab shown in Figure 5-1.

Figure 5-1 Global Settings



Step 3 In the SystemOperMode field, click one of the following radio buttons:

- Click **Normal** to configure the server switch for a non-VFrame environment.
- Click **VFrameManaged** to configure the server switch for a VFrame-managed environment.

Step 4 Click **Apply**.

Configuring Date and Time Properties

An internal clock runs on your device, but we recommend that you configure your device to access a Network Time Protocol (NTP) server to synchronize your device with your network.

These topics describe how to configure date and time properties:

- Configuring the Date and Time, page 5-4
- Assigning NTP Servers, page 5-5

Configuring the Date and Time

To configure the date and time of the internal clock on your device, follow these steps:

Step 1 From the Maintenance menu, choose **Time**.

The Date and Time Properties window opens. The Date and Time tab appears by default.

Step 2 In the Date field, enter the date in the *MM*/*DD*/*YY* format.

Step 3 In the Time field, enter the time in *HH*:*MM*:*SS* format, and then click **Apply**.

Step 4 Click **Apply** in the Date and Time partition.

Assigning NTP Servers

To assign an NTP server to synchronize your server switch with the network, follow these steps:

Step 1 From the Maintenance menu, choose **Time**.

The Date and Time Properties window opens.

Step 2 In the NTP Server 1 field, enter the IP address of the NTP server that you want your server switch to use.

Step 3 (Optional) In the NTP Server 2 field, enter the IP address of the NTP server that you want your switch to use if your switch cannot access the primary NTP server.

Step 4 (Optional) In the NTP Server 3 field, enter the IP address of the NTP server that you want your switch to use if your switch cannot access the primary or secondary NTP servers.

Step 5 Click **Apply** in the NTP Servers partition.

Note When your device cannot access a NTP server, it defaults to the onboard clock.

Configuring the Local Time Zone and Daylight Savings Time

You can configure the time zone and daylight savings time either by selecting from a pre-configured list of time zones, or you can name and configure the details the of the time zone manually. These topics describe how to perform these tasks:

- Configuring a Time zone and Daylight Savings Time Manually, page 5-5
- Configuring a Time Zone and Daylight Savings Time from a Pre-Configured List, page 5-6

Configuring a Time zone and Daylight Savings Time Manually

To configure the time zone or daylight savings time manually, follow these steps:

Step 1 From the Maintenance menu, choose **Time ...**.

The Date and Time Properties window appears.

Step 2 Click the **Time Zone** tab.

Step 3 To configure the time zone, in the Time Zone section, enter the following information:

a. In the Name field, enter the name of a time zone.

For example, if your server switch is located in the Pacific time zone, enter **PST**. This string appears in subsequent messages that display the time.

b. In the Offset from UTC field, enter the number of hours that your time zone is offset from Coordinated Universal Time (UTC).

For Pacific Standard Time, for example, enter **- 8**.

Step 4 To configure daylight savings time, in the Daylight Saving Time section, enter the following information:

a. In the Name field, enter a name for the daylight savings time.

For example, in the Pacific time zone, enter PDT. For the period for which daylight savings time is active, this string appears in messages that display the time.

b. In the Offset from Local Time field, enter the number of hours and minutes to advance the clock while daylight savings time is active.

c. In the Start Date field, enter the date on which daylight savings time begins.

The format for the date is *mm*/*dd*/*yyyy*.

d. In the End Date field, enter the date on which daylight savings time ends.

The format for the date is *mm*/*dd*/*yyyy*.

e. In the Start Time field, enter the time of day at which daylight savings time begins.

The format for the time is *hh*:*mm* on a 24-hour clock.

f. In the End Time field, enter the time of day at which daylight savings time ends.

The format for the time is *hh*:*mm* on a 24-hour clock.

Step 5 Click **Apply**.

Configuring a Time Zone and Daylight Savings Time from a Pre-Configured List

To configure the time zone or daylight savings time from a pre-configured list, follow these steps:

Step 1 From the Maintenance menu, choose **Time ...**.

The Date and Time Properties window appears.

Step 2 Click the **Time Zone** tab.

Step 3 Click the **Select TZ** button.

The Time Zones window appears.

Step 4 From the drop-down menu, select the time zone.

Step 5 Click the **Details** button to preview the time zone information.

Step 6 Click **OK** to populate the Time Zone tab of the Data and Time window with the data for the selected time zone.

Step 7 Click **Apply**.

Configuring Basic Services

These topics describe how to configure basic services to facilitate remote access to your device:

Assigning a DNS Server

To assign a DNS server to your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **DNS** tab.

Step 3 In the Server 1 field, enter the IP address of the primary DNS server that you want to use.

Step 4 (Optional) In the Server 2 field, enter the IP address of the DNS server that you want to use if your device cannot access the primary DNS server.

Step 5 In the Domain field, enter the domain to which you want your switch to belong, and then click **Apply**.

Enabling or Disabling the FTP Access

To enable or disable FTP access to and from your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **FTP** tab.

Step 3 Check (to enable) or uncheck (to disable) the **Enable FTP Server** check box, and then click **Apply**.

Enabling or Disabling the Telnet Access

To enable or disable Telnet access to your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Telnet** tab.

Step 3 Check (to enable) or uncheck (to disable) the **Enable Telnet Server** check boxes, and then click **Apply**.

Assigning a Syslog Server

Note This task assumes that you have already configured the host and connected it to the InfiniBand fabric.

To assign a syslog server to store logs from your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Syslog** tab.

Step 3 In the Remote Syslog Server One field, enter the IP address of a remote server to accept messages from your device, and then click **Apply**.

Repeat this step to add a second server to Remote Syslog Server Two.

Assigning an Authentication Method

Note SFS Server Switch product configurations with TopspinOS release 2.3.x and higher use a 128-bit MD5-based hashing scheme to store passwords.

To assign an authentication method to your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Authentication** tab.

Step 3 In the Authentication Method field, click a radio button to choose a method, and then click **Apply**.

Table 5-3 describes the radio buttons that you can choose.

Table 5-3 Authentication Methods

Radio Button	Description
local	Authenticates user logins against the chassis database.
localThenRadius	Authenticates user logins against the chassis database. Upon failure, authenticates with up to three configured RADIUS servers. Upon failure to authenticate the user or failure to reach any configured RADIUS server, the user is denied access.
radiusThenLocal	Authenticates user logins with up to three configured RADIUS servers. Upon failure to authenticate the user or failure to access any configured RADIUS server, authenticates against the chassis database. If authentication against the chassis database fails, then the user is denied access.
localThenTacacs	Authenticates user logins against the chassis database. Upon failure, authenticates with up to three configured TACACS+ servers. Upon failure to authenticate the user or failure to access any configured TACACS+ server, the user is denied access.
tacacsThenLocal	Authenticates user logins with up to three configured TACACS+ servers. Upon failure to authenticate the user or failure to access any configured TACACS+ server, authenticates against the chassis database. If authentication against the chassis database fails, then the user is denied access.
radius	Authenticates user logins with up to three configured RADIUS servers. Upon failure to authenticate the user, the user is denied access. The authentication process checks against the chassis database only if it cannot access any RADIUS server.
tacacs	Authenticates user logins with up to three configured TACACS+ servers. Upon failure to authenticate the user, the user is denied access. The authentication process checks against the chassis database only if it cannot access any TACACS+ server.

Viewing and Managing RADIUS Servers

These topics describe how to view and manage RADIUS servers:

- Viewing RADIUS Servers, page 5-10
- Adding RADIUS Servers, page 5-11
- Editing a RADIUS Server Configuration, page 5-11
- Deleting RADIUS Servers, page 5-12

Viewing RADIUS Servers

To view the RADIUS servers that you have configured your device to use to authenticate CLI and Element Manager logins, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Radius Servers** tab.

Table 5-4 describes the fields in the Radius Servers table.

Table 5-4 Radius Server Properties Window Fields

Field	Description
Address	IP address of the RADIUS server.
Priority	Value used to configure priority of this entry. This value is not writable. The first added server gets the highest priority which is priority 1. If multiple RADIUS servers are specified the server with a higher priority is used before a server with a lower priority. No two radius servers can have the same priority.
Udp Port	Authentication port of the RADIUS server. Edit this value, and click **Apply** to configure the UDP port of the RADIUS server. The numbers to the right of the field indicate the range that this field supports.
Encryption Key	Encryption key used by the radius server and client. Enter a value, and click **Apply** to configure the encryption key of the RADIUS server. The numbers to the right of the field indicate the range that this field supports.
Timeout	Timeout: timeout period for any outstanding request to the server. Edit this value, and click **Apply** to configure the timeout value of the RADIUS server. The numbers to the right of the field indicate the range that this field supports.
Max Retries	Maximum number of retries that the same request can be sent to the server before the request times out. Edit this value, and click **Apply** to configure the maximum number of retries that the RADIUS server permits. The numbers to the right of the field indicate the range that this field supports.
Access Requests	Number of authentication requests that the server has received from your device since your device booted.
Access Accepts	Number of logins to your device that the server authenticated since your device booted.
Access Rejects	Number of logins to your device that the server denied since your device booted.
Server Timeout	Number of authentications that timed out on the server since your device booted.

Adding RADIUS Servers

To add a new RADIUS server on your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Radius Servers** tab.

Step 3 Click **Insert**.

The Insert Radius Server window opens.

Note Click **Close** at any time to abort this process with no changes to your device. Configurations apply only after you click **Apply**.

Step 4 In the Address field, enter the IP address of the server.

Step 5 (Optional) Edit the UDP Port field.

The numbers to the right of the field indicate the range of integer values that this field supports.

Step 6 (Optional) In the Encryption Key field, enter an encryption key.

Step 7 (Optional) Edit the Timeout field.

The numbers to the right of the field indicate the range of integer values that this field supports.

Step 8 (Optional) Edit the Max Retries field.

The numbers to the right of the field indicate the range of integer values that this field supports.

Step 9 Click **Insert**.

Editing a RADIUS Server Configuration

To edit a RADIUS server in your configuration, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Radius Servers** tab.

Step 3 Identify the row of the RADIUS server that you want to reconfigure, and then double-click the cell that you want to edit.

Note You can only edit cells that have a white background.

Step 4 Edit the content of the cell.

Step 5 Click **Apply**.

Deleting RADIUS Servers

To delete a RADIUS server from your configuration, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Radius Servers** tab.

Step 3 Click the row entry of the RADIUS server that you want to delete.

Step 4 Click **Delete**.

Viewing and Managing TACACS+ Servers

These topics describe how to view and manage TACACS+ servers:

Viewing TACACS+ Servers

To view the TACACS+ servers that you have configured your device to use to authenticate CLI and Element Manager logins, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Tacacs Servers** tab.

Table 5-5 describes the fields in the TACACS+ Servers table.

Table 5-5 TACACS+ Server Properties Window Elements

Field	Description
Address	Displays the IP address of the TACACS+ server.
Priority	Value used to configure the priority of this entry. This value is not writable. The first added server gets the highest priority which is priority 1. If multiple TACACS+ servers are specified, the server with a higher priority is used before a server with a lower priority. No two TACACS+ servers can have the same priority.
Udp Port	Authentication port of the TACACS+ server. Edit this value, and click **Apply** to configure the UDP port of the TACACS+ server. The numbers to the right of the field indicate the range of integer values that this field supports.

Table 5-5 TACACS+ Server Properties Window Elements (continued)

Field	Description
Encryption Key	Encryption key used by the TACACS+ client and server. Enter a value, and click **Apply** to configure the encryption key of the TACACS+ server. The numbers to the right of the field indicate the range that this field supports.
Timeout	Timeout period for any outstanding request to the server. Edit this value, and click **Apply** to configure the timeout value of the TACACS+ server. The numbers to the right of the field indicate the range that this field supports.
Max Retries	Maximum number of retries that the same request can be sent to the server when the request times out. Edit this value, and click **Apply** to configure the maximum number of retries that the TACACS+ server permits. The numbers to the right of the field indicate the range of integer values that this field supports.
Access Requests	Number of authentication requests that the server has received from your device since your device booted.
Access Accepts	Number of logins to your device that the server authenticated since your device booted.
Access Rejects	Number of logins to your device that the server denied since your device booted.
Server Timeout	Number of authentications that timed out on the server since your device booted.

Adding a TACACS+ Server

To add a TACACS+ server to your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Tacacs Servers** tab.

Step 3 Click **Insert**.

Step 4 Provide an IP address for the server.

Step 5 (Optional) Change the UDP port from the default. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 6 (Optional) Provide an encryption key.

Step 7 (Optional) Change the timeout from the default. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 8 (Optional) Change the maximum retries from the default. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 9 Click **Insert**.

Editing a TACACS+ Server Configuration

To edit a TACACS+ server, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Tacacs Servers** tab.

Step 3 Identify the row of the server that you want to reconfigure, and then double-click the cell to edit.

Note You can only edit cells that have a white background.

Step 4 Edit the content of the cell.

Step 5 Click **Apply**.

Deleting a TACACS+ Server

To delete a TACACS+ server from your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Tacacs Servers** tab.

Step 3 Select a server.

Step 4 Click **Delete**.

Enabling HTTP Services

To configure HTTP services, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **HTTP** tab.

Step 3 Check the **Enable HTTP Server** check box.

Step 4 (Optional) Assign a port in the HTTP Port field.

Step 5 (Optional) Check the **Enable HTTP Polling** check box.

Step 6 (Optional) Check the **Enable HTTPS Server** check box.

Step 7 (Optional) Assign a port in the HTTPS Port field.

Step 8 Choose a security method from the Secure Cert Common Name field.

Step 9 Click **Apply**.

Configuring Cisco Discovery Protocol

Cisco Discovery Protocol discovers information on neighbors and status. To configure CDC services, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Discovery** tab.

Step 3 Check the **Run Discovery** check box to enable discovery.

Step 4 (Optional) Change the message interval by clicking the current value and typing a new one between 5 and 254 seconds.

Step 5 (Optional) Change the hold time by clicking the current value and typing a new one between 10 and 255 seconds.

Step 6 Click **Apply**.

Viewing the Discovery Cache

To view the discovery cache, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Discovery Cache** tab.

Customizing the Boot Configuration

To customize the boot configuration follow these steps:

- View the image that the switch will boot during the next reboot.
- Delete the startup configuration.
- Overwrite the startup configuration with another configuration file in your file system.

These topics describe how to perform the following tasks:

- Configuring Reboot Image, page 5-16
- Deleting or Overwriting the Startup Configuration, page 5-16

Configuring Reboot Image

To choose the image that the server switch loads when it reboots, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Boot Config**.

The Boot Configuration window opens.

Step 2 From the Image Source For Next Reboot drop-down menu, choose the image that you want the server switch to boot when it reboots.

Step 3 Click **Apply** in the Software Images partition.

Deleting or Overwriting the Startup Configuration

To delete or overwrite the startup configuration, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Boot Config**.

The Boot Configuration window opens.

Step 2 (Optional) Click the **Overwrite startup configuration with** radio button, and choose a configuration from the drop-down menu to replace the current startup configuration with another configuration file.

Note To overwrite your startup configuration with your running configuration, see the "Backing Up the Running Configuration File" section on page 5-16.

Step 3 (Optional) Click the **Delete startup configuration** radio button to configure your server switch to use the factory-default startup configuration.

Step 4 Click **Apply** in the Startup Configuration partition.

Backing Up the Running Configuration File

To back up your running configuration file, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Backup Config**.

The Backup Configuration window opens.

Step 2 Enter a filename in the Save Configuration As field.

Element Manager saves the running configuration in the configuration directory that you specify.

Note Enter **startup-config** in this field if you want to save the running configuration as the startup configuration. This process overwrites the existing startup configuration file.

Step 3 Click **Save**.

Viewing and Deleting Files in the File System

These topics describe file system tasks and concepts:

Viewing Files in the File System

To view files, such as image files, log files, and configuration files, that reside on your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens. Table 5-6 describes the fields in the Current Files on System table in this window.

Table 5-6 Current Files on System Table Field Descriptions

Field	Description
Slot ID	Slot of the controller card on which the file resides.
File Name	Name of the file.
File Type	Type of file. The following types may appear: • config • log • image
Size	Size of the file, in bytes.
Date	Most recent date and time that your device or a user updated the file.

Step 2 (Optional) Click **Refresh** to poll your switch and update your display to reflect the most current inventory of your file system.

Deleting Files in the File System

To delete files from your file system, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click the line in the **Current Files on System** table that lists the file that you want to delete, and then click **Delete**.

A Delete File window opens.

Step 3 Click **Yes**.

Understanding Configuration Files

A configuration file is a text file that stores a list of CLI commands. These topics describe specific instances of configuration files:

- startup-config File, page 5-18
- running-config File, page 5-18

startup-config File

The main configuration file is called startup-config. This file stores all of the CLI commands necessary to completely configure a box from a factory-default state. This configuration file can be copied, backed up, and modified.

running-config File

Whenever configuration changes are made through the GUI or CLI, a CLI command is temporarily saved in a virtual configuration file called running-config. If you want to save these changes permanently, this file is copied into the startup-config file.

Any number of configuration files can be stored. For convenience and rapid configuration, files can also maintain a partial list of CLI commands. These files can also be copied into running-config for immediate use or startup-config for persistent use across reboots.

Understanding Log Files

Log files are text files that record activity, including configuration changes. Depending on their size, log files are rotated and compressed. Log files can also be exported from the system by using the **copy** command. These topics provide details about log files:

- File Management and Storage of Log Files, page 5-19
- Log Message Types, page 5-19

File Management and Storage of Log Files

The management of log files is performed automatically, but you can configure log files. Log files are stored separately from other file types, but all files share the 128 MB of flash memory. Log files are stored in syslog files.

The system checks the size of the active log file hourly, and when it exceeds 1 MB, the active log file, ts_log, is closed, compressed, and renamed ts_log.1.gz. Other ts_log.x.gz files are incremented by 1. These files can be downloaded through the Log Viewer GUI, which can create filters for troubleshooting and auditing purposes.

Log Message Types

The following levels of logging are captured:

- CONF—configuration changes; no user action is required.
- INFO—general information; no user action is required.
- WARN— abnormal condition; user intervention may be required.
- ERROR— abnormal condition; user intervention is required.
- FATAL—abnormal condition; user must reboot.
- DEBUG—occurs only after enabling tracing. See the **trace** command documentation in the *Cisco SFS Product Family Command Reference*.

Installing Software Images

Note To proceed to the software installation instructions, see the "Installing a Software Image" section on page 5-22. The sections that follow provide context and details about installing images.

The Image data that is used to configure the software is being continuously updated and enhanced. Use the latest system image data to ensure the most efficient usage of your system.

See the user's support portal at support.cisco.com for the latest upgrades.

These topics describe concepts and procedures related to installing a system image:

System Image

A system image is an unpacked and installed image file. An image file is the source from which to install a system image and it has an .img extension.

When an image file is installed, the image file is expanded into a system image. The system image is what the user will see in order to specify what the system should use to boot up each card in the system.

Image File

Image files are stored in flash memory as a single complete file with an .img extension. Each image file contains all the operating software (application software and firmware/microcode) needed by the various cards that can be installed into the system.

The system cannot use an image file directly to boot up the system. The image file must first be installed. The installation process automatically unbundles the image file and distributes the software components to each card in the system. Users do not have to be aware of individual software components. The user enters one CLI command to install an image file. See the **install** command in the *Cisco SFS Product Family Command Reference*.

The server switch operating system stores up to three images on a disk: the uninstalled image, the current system (or installed) image, and the recovery image.

The system has only enough flash memory to store:

- One system image file (active)
- One image file (inactive/uninstalled)
- One recovery image

Occasionally, you need to manually delete an image file from the InfiniBand system to make room for a new version. See the "Deleting Files in the File System" section on page 5-18.

These topics describe image concepts:

- Inactive Image, page 5-20
- Active Image, page 5-20
- Recovery Image, page 5-20
- Version Numbers, page 5-21

Inactive Image

An inactive image is an image that has been downloaded but has not been installed. It is not the active or system image.

The operating system can store only one inactive image. Delete inactive images through the CLI (see the "Deleting Files in the File System" section on page 5-18), or by clicking **delete** in the Element Manager.

Active Image

An active image is the current system image. An installed or active image has gone through the entire upgrade process. The system image usually has a slash (/) in its name. Do not modify or delete the installed system image.

Recovery Image

The recovery image is a default image that comes installed on the system. The recovery image can be used to quickly restore operation to the system if an image upgrade should fail.

Version Numbers

The operating system and installed system image running on the InfiniBand system determine the supported software features.

Two types of system-images are provided:

- An image for the HCA card
- An image for the Cisco SFS 7000D, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 7008P, or Cisco IB Server Switch Module.

Before configuring the InfiniBand system, check the version of the installed system image used to boot the chassis. Use this information to ensure that you upgrade to the correct software.

Copying/Downloading the Image

Upgrading the server switch operating system requires several steps, which are described in the following sections. Note that one step is to copy the image before installing it.

Table 5-7 describes several options for copying the image into the system.

Table 5-7 Copying/Downloading Image Options

Through the CLI	Through the GUI
FTP	Remote FTP Server
TFTP	Local File
SCP	Remote Secure Server

Card Status Requirements

Only cards with an oper-status of up are updated. If a card is down when you run install or a card is added after running install, follow these steps:

Step 1 Bring up the card.

Step 2 Run the installation again.

Step 3 Specify the same image file.

If the image is already installed on a card, installation skips that card.

Step 4 Be sure to specify the boot-config again so that all cards know to boot from the same system image.

Upgrading a System

The system upgrade process is summarized in the following steps:

Step 1 Set up the hardware connection for the upgrade.

Step 2 Verify the installed system image version number.

Step 3 Download an image file from a network-accessible FTP server, or download an image file remotely from a TFTP server.

Step 4 Install the new system image.

Step 5 Configure the CLI and Element Manager to use the appropriate configuration file the next time that they reboot.

Step 6 Reboot the system.

Installing a Software Image

Note Alert other users that you plan to install a new image to your server switch.

To install a software image file, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Note If you have not already imported an image file to your file system, see the "Importing Configuration Files and Image Files" section on page 5-22.

Step 2 Click the line in the Current Files on System table that lists the file that you want to install, and then click **Install**.

A verification window opens.

Note Before you install an image, verify that you have brought up all of the cards on the chassis that you want to run the new image. Cards that run a different image from the chassis cannot pass traffic.

Step 3 Click **Yes** to install the image.

Importing Configuration Files and Image Files

These topics describe how to import files to your server switch from your local host or a remote FTP server:

Importing from a Remote Server

To import files to your server switch from remote devices, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click **Import**.

The Import File window opens.

Step 3 From the File Type drop-down menu, choose the type of file to import (**image** or **configuration**).

Step 4 Click the **Remote FTP Server** radio button or the **Remote SCP Server** radio button.

Step 5 In the Server Name or IP Address field, enter the DNS name or IP address of the FTP server that holds the file that you want to import.

Step 6 In the User Name field, enter the user ID that logs you in to the FTP server.

Step 7 In the Password field, enter the password that logs you in to the FTP server.

Step 8 Enter the directory path and name of the file on the FTP server in the File Path and Name field.

Step 9 In the File Name on System field, enter the name that the file will take on your server switch.

Step 10 Click **Copy**.

Importing from Your Local Host

To import files to your server switch from your local host, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click **Import**.

The Import File window opens.

Step 3 Choose **image** or **configuration** from the File Type drop-down menu (type of file to import).

Step 4 Click the **Local File** radio button.

Step 5 Click **Choose** and navigate to the file that you want to import.

Step 6 Select the file that you want to import, and then click **OK**.

Step 7 In the File Name on System field, enter the name that the file will take on your server switch.

Step 8 Click **Copy**.

Exporting Configuration Files and Log Files

These topics describe how to export files from your server switch to your local host or a remote FTP server:

Exporting to a Remote Server

To export files from your server switch to a remote server, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click the file that you want to export.

The Export button becomes active.

Step 3 Click **Export**.

The Export File window opens.

Step 4 Click either the **Remote FTP Server** or the **Remote SCP Server** radio button.

Step 5 In the Server Name or IP Address field, enter the DNS name or IP address of the FTP server that will receive the file that you export.

Step 6 In the User Name field, enter the user ID that logs you in to the FTP server.

Step 7 In the Password field, enter the password that logs you in to the FTP server.

Step 8 In the File Path and Name field, enter the path on your remote host to copy the exported file, and the name for the file.

```
/root/files/old-config.cfg
```

Step 9 Click **Copy**.

Exporting to Your Local Host

To export files from your server switch to your local host, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click the file that you want to export.

The Export button becomes active.

Step 3 Click **Export**.

The Export File window opens.

Step 4 Click the **Local File** radio button.

Step 5 Click **Choose**.

Step 6 Navigate to the directory where you want to copy the file, and then click **OK**.

Step 7 Click **Copy**.

Saving a Configuration File

To back up your running configuration to the standby controller on your chassis, click the **Maintenance** menu, and choose **Save Config**.

Note If you make configuration changes to the master image and then save the configuration, verify that the master and backup have synchronized, and then save the configuration on the backup as well. For more information, see the "Configuring Database Synchronization" section on page 8-11.

Rebooting the Server Switch with Element Manager

To reboot your server switch with Element Manager, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Reboot**.

Step 2 Click **OK**.

Running General Diagnostics

These topics describe how to run chassis, card, and port diagnostics:

Running Chassis Diagnostics

To run chassis diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **General**.

Step 2 Click the **Chassis** tab.

Step 3 In the Module Type field, click the radio button of the type of the element that you want to diagnose.

Step 4 In the Module Number field, enter the index number of the element that you want to diagnose.

Step 5 In the Test field, click the radio button of the type of test that you want to run.

Step 6 Enter the number of times that you want the test to run in the Iterations field.

Step 7 In the Action field, click the **start** radio button to begin a test or the **stop** radio button to end a test.

Step 8 In the Option field, click the error condition that you want to apply.

Step 9 Click **Apply** to execute the configuration and start or stop the test.

Running Card Diagnostics

To run card diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **General**.

Step 2 Click the **Card** tab.

Step 3 Click **Insert**.

The diagnostic Insert Card window opens.

Step 4 Click the **Card** drop-down menu, and choose the card that you want to test.

Step 5 In the Test field, click the type of test that you want to execute.

Step 6 In the Iterations field, click the number of test iterations that you want to run.

Step 7 From the Action field, choose an action:

- Click the **start** radio button if you want the test to run when you click **Insert**.
- Click the **stop** radio button if you want the test to appear in the table but not execute. To run the test later, see the "Running Configured Diagnostic Tests" section on page 5-28.

Step 8 Click **Insert**.

Deleting a Card Test Entry

To delete a card test entry, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **General**.

Step 2 Click the **Card** tab.

Step 3 Click the row of the entry that you want to delete, and then click **Delete**.

Running Port Diagnostics

To run port diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **General**.

Step 2 Click the **Port** tab.

Step 3 Click **Insert**.

The Diagnostic Insert Port window opens.

Step 4 Enter a port in the Port field, or click the **...** button, choose ports, and then click **OK**.

Step 5 In the Test field, click the radio button of the test that you want to execute.

Step 6 (Optional) Check the **Data Validation** check box to validate data.

Step 7 In the Data Size field, enter the size, in bits, of the data packet that you want to send.

Step 8 In the test in the Data Pattern field, enter the data pattern that you want to iterate.

Step 9 In the Iterations field, enter the number of iterations that you want to execute.

Step 10 In the Source ID field, enter a source local ID.

Step 11 In the Target ID field, enter a destination local ID.

Step 12 From the Action field, choose an action:

- Click the **start** radio button if you want the test to execute when you click **Insert**.
- Click the **stop** radio button if you want the test to appear in the table but not execute. To execute the test later, see the "Running Configured Diagnostic Tests" section on page 5-28.

Step 13 Click **Insert**.

Deleting a Port Test Entry

To delete a port test entry, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **General**.

Step 2 Click the **Port** tab.

Step 3 Click the row of the entry that you want to delete, and then click **Delete**.

Running Configured Diagnostic Tests

To run a diagnostic test that you have already added to the Diagnostics window, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **General**.

Step 2 Click the appropriate tab for the test that you want to run.

Step 3 Identify the entry of the test that you want to run.

Step 4 Click the cell in the Action column of that entry and choose **start** from the drop-down menu.

Note The cell must display **stop** for this process to work. If the cell displays **start**, choose **stop** from the drop-down menu, and click **Apply** before performing this step.

Step 5 Click **Apply**, and then repeatedly click **Refresh** to track the progress of the test.

Viewing POST Diagnostics

These topics describe how to view power-on self-test diagnostics for cards, power supplies, and fans:

- Viewing Card POST Diagnostics, page 5-28
- Viewing Power Supply POST Diagnostics, page 5-29
- Viewing Fan POST Diagnostics, page 5-29

Viewing Card POST Diagnostics

To view card power-on self-test diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **POST**.

Step 2 Click the **Card** tab.

Table 5-8 describes the fields that appear.

Table 5-8 Card POST Field Descriptions

Field	Description
Slot ID	Slot number.
POST Status	Indicates the result of the power-on-self-test: • unknown • passed • failed
PostErrorCodes	Show error(s) detected during the power-on self-test.

Viewing Power Supply POST Diagnostics

To view power supply power-on self-test diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **POST**.

Step 2 Click the **Power Supply** tab.

Table 5-9 describes the power supply POST fields that appear.

Table 5-9 Power Supply POST Field Descriptions

Field	Description
PS ID	Power supply number.
POST Status	Indicates the result of power-on-self-test: • unknown • passed • failed
PostErrorCodes	Show error(s) detected during the power-on-self-test.

Viewing Fan POST Diagnostics

To view fan power-on self-test diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **POST**.

Step 2 Click the **Fan** tab.

Table 5-10 describes the fan POST fields that appear.

Table 5-10 Fan POST Field Descriptions

Field	Description
Fan ID	Fan number.
POST Status	Indicates the result of the power-on self-test: • unknown • passed • failed
PostErrorCodes	Show error(s) detected during the power-on self-test.

Viewing FRU Diagnostics

These topics describe how to view field-replaceable unit diagnostics for cards, power supplies, and fans:

- Viewing Card FRU Diagnostics, page 5-30
- Viewing Power Supply FRU Diagnostics, page 5-31
- Viewing Fan FRU Diagnostics, page 5-31

Viewing Card FRU Diagnostics

To view card field-replaceable unit diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **FRU Error**.

Step 2 Click the **Card** tab.

Table 5-11 describes the card FRU fields that appear.

Table 5-11 Card FRU Field Descriptions

Field	Description
Slot ID	Slot number.
FruError	Shows the last hardware error (if any) detected on this field-replaceable unit. The information returned in this variable is read from the device's vital product data.

Viewing Power Supply FRU Diagnostics

To view power supply field-replaceable unit diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **FRU Error**.

Step 2 Click the **Power Supply** tab.

Table 5-12 describes the power supply FRU fields that appear.

Table 5-12 Power Supply FRU Field Descriptions

Field	Description
PS ID	Power supply number.
FruError	Shows the last hardware error (if any) detected on this field-replaceable unit. The information returned in this variable is read from the vital product data of the device.

Viewing Fan FRU Diagnostics

To view fan field-replaceable unit diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **FRU Error**.

Step 2 Click the **Fan** tab.

Table 5-13 describes the fan FRU fields that appear.

Table 5-13 Fan FRU Field Descriptions

Field	Description
Fan ID	Fan number.
FruError	Shows the last hardware error (if any) detected on this field-replaceable unit. The information returned in this variable is read from the vital product data of the device.