CHAPTER 4

Maintenance Tasks

These topics describe the Chassis Manager maintenance tasks:

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 basic system information:

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.

Viewing System Information

To view basic system information, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Information** branch.

The System Information display appears in the View frame. Table 4-1 describes the fields in this table.

Table 4-1 System Information 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 ID (select chassis)	No longer used.
System Sync State	Synchronization state between the primary controller card and the hot standby controller card. (Cisco SFS 7008 and Cisco SFS 7008P Server Switches only.)

Naming Your InfiniBand Switch

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Information** branch.

The System Information display appears in the View frame.

Step 3 In the System Name field, type the name that you want to assign to the device, and then click **Apply**.

Defining a Device Location

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Information** branch.

The System Information display appears in the View frame.

Step 3 In the Location field, type the name location of your device, and then click **Apply**.

Defining a Cisco TAC Resource

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Information** branch.

The System Information display appears in the View frame.

Step 3 In the Support Contact field, type the e-mail address of Cisco TAC, and then click **Apply**.

Configuring System Global Settings

Global configuration includes the system operating mode and the InfiniBand counter reset.

These topics describe how to configure system global settings:

Configuring System Operation Mode

To configure your server switch to deny changes to SRP configuration and preserve VFrame-authorized configurations, set the system operating mode to VFrame Managed. To change the system operation mode, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Global Settings** branch.

The System Global Settings display appears in the View frame.

Step 3 In the System Operation Mode field, choose either the **Normal** or **VFrame Managed** radio button.

Step 4 Click **Apply**.

Enabling or Disabling InfiniBand Counter Reset

Counters are accumulated by the port_agent when performance monitoring is enabled (by default, it is disabled). To enable or disable automatic clearing of the counters by the port_agent, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Global Settings** branch.

The System Global Settings display appears in the View frame.

Step 3 In the Enable Counter Reset field, to enable the counter reset function check the **Enable** check box. To disable the counter reset function, uncheck the **Enable** check box.

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 4-4
- Assigning NTP Servers, page 4-5

Configuring the Date and Time

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Time** branch.

The Date and Time Properties display appears in the View frame.

Step 3 In the Date field, enter the date in the *MM*/*DD*/*YY* format.

Step 4 In the Time field, enter the time in *HH*:*MM*:*SS* format, and then click **Apply**.

Assigning NTP Servers

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Time** branch.

The Date and Time Properties display appears in the View frame.

Step 3 In the NTP Server 1 field, enter the IP address of the NTP server that you want your switch to use.

Step 4 (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 5 (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.

Note We recommend that you configure all three NTP servers to maintain time synchronization if a server becomes unreachable.

Configuring the Local Time Zone and Daylight Savings Time

These topics describe how to configure the time zone and daylight savings time on your server switch:

- Setting a Time Zone and Daylight Savings Time, page 4-5
- Resetting the Time Zone and Daylight Savings Time, page 4-6

Note This feature is not available on server switches running the 2.9 version of the operating system.

Setting a Time Zone and Daylight Savings Time

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

Step 1 Expand **Maintenance** in the Tree frame.

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

The Time Zone and Daylight Savings Time Properties window appears.

Step 3 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).

The format for this field is *hh*:*mm*.

For Pacific Standard Time, for example, enter **-08:00**.

Step 4 Leave the Daylight Saving Time section blank if you do not want to configure daylight savings time. Otherwise, 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.

The format for this field is *hh*:*mm*.

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**.

Resetting the Time Zone and Daylight Savings Time

To reset the time zone, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

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

The Time Zone and Daylight Savings Time Properties window appears.

Step 3 In the Time Zone area, delete the information in all fields.

Step 4 In the Daylight Saving Time area, delete the information in all fields.

Step 5 Click **Apply**.

Viewing or Deleting Files in the File System

These topics describe how to view or delete files in the file system:

Viewing Files in the File System

To view device files, such as image files, log files, and configuration files, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame. Table 4-2 describes the fields in this table.

Table 4-2 File Management Table Field Descriptions

Field	Description
Slot ID	Slot of the controller card on which the file resides.
Name	Name of the file.
Type	Type of file. The following appear for selection: • 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 3 (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 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame.

Step 3 Click the radio button next to the file to delete, and then click **Delete**.

A Delete ? confirmation dialog box appears.

Step 4 Click **Yes** in the Delete ? dialog box to delete the file.

Installing Software Images

To install an image file, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame.

Note If you have not already imported the image file to your file system, see the "Importing Configuration Files and Image Files with FTP or SCP" section on page 4-8.

Step 3 Click the radio button next to the image file to install, and then click **Install**.

A dialog box appears to verify that you want to proceed.

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.

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

Step 4 Click **OK** to install the image.

A status bar appears to display the status of the installation.

Importing Configuration Files and Image Files with FTP or SCP

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame.

Step 3 Click **Import**.

The Import File window opens.

Step 4 Choose **FTP** or **SCP** from the Remote Server Type field.

Step 5 Choose a file type (**Image** or **Configuration**) from the File Type drop-down menu.

Step 6 Enter the IP address of the server that holds the file (to be imported) in the Remote IP Address field.

Step 7 Enter your user ID in the Remote User Name field to log into the server.

Step 8 Enter your password in the Remote Password field to log into the server.

Step 9 Enter the directory path and name of the file on the server in the Remote File Path and Name field.

Step 10 Enter the name that the file will take on your chassis in the File Name on System field.

Image files must be saved with an .img extension; otherwise, you will not be able to install these files.

Step 11 Click **Import**.

A status bar appears to display the progress of the file transfer.

Exporting Configuration Files and Log Files with FTP or SCP

Note You cannot export image files.

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame.

Step 3 Click the radio button of the file that you want to export.

Step 4 Click **Export**.

The Export File window opens with the name of the file to export in the File Name on System field.

Step 5 Choose **FTP** or **SCP** from the Remote Server Type field.

Step 6 Enter the IP address of the server to which you want to export the file in the Remote IP Address field.

Step 7 Enter your user ID in the Remote User Name field to log into the server.

Step 8 Enter your password in the Remote Password field to log into the server.

Step 9 Enter the directory path and filename for the file on the server in the Remote File Path and Name field.

Step 10 Click **Export**.

A status bar appears to display the progress of the file transfer.

Customizing the Boot Configuration

To customize the boot configuration, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Boot Configuration** branch.

The Boot Configuration display appears in the View frame.

Step 3 (Optional) 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 4 Click **Apply**.

Deleting or Overwriting the Startup Configuration

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Boot Configuration** branch.

The Boot Configuration display appears in the View frame.

Step 3 Click the **Overwrite startup configuration with** radio button, and then choose a configuration from the drop-down menu to replace the current startup configuration file.

Note To overwrite your startup configuration with your running configuration, see the "Backing Up the Running Configuration File" section on page 4-10.

Step 4 (Optional) Click the **Delete startup configuration** radio button to configure your server switch to use the factory-default startup configuration.

Step 5 Click **Apply**.

Backing Up the Running Configuration File

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Backup Configuration** branch.

The Backup Configuration display appears in the View frame.

Step 3 Enter a filename in the Save Configuration As field.

Chassis Manager saves running configurations 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.

Step 4 Click **Save**.

Step 5 (Optional) Click the **File Management** branch to verify that your file appears in the file system.

Saving a Configuration File

To back up your running configuration as your startup configuration (and to the standby controller on your chassis with a dual-controller chassis), follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Save Config** branch.

The Save Config display appears in the View frame.

Step 3 Click **Save Config**.

Rebooting the Device

When you reboot your device, Chassis Manager gives you the option to reboot either with or without saving your configuration. If you choose to reboot but not save, any differences between your running configuration file and startup configuration file are not saved after the reboot.

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Reboot** branch.

The Reboot display appears in the View frame.

Step 3 To save the system configuration and reboot, click **Save-Reboot**. To reboot without saving the system configuration, click **Reboot-Only**.

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 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame.

Step 4 In the Server 1 field, enter the IP address of the primary DNS server that you want to use.

Step 5 (Optional) In the Server 2 field, enter the IP address of the DNS server to use if your device cannot access the primary DNS server.

Step 6 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 FTP transfers to and from your device, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame.

Step 4 In the FTP Server field, check to enable or uncheck to disable the **Enable** check box, and then click **Apply**.

Enabling or Disabling the Telnet Access

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame.

Step 4 In the Telnet Server field, check (enable) or uncheck (disable) the **Enable** check box, 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 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame. You can use either one or two servers.

Step 4 In the Remote Syslog Server field, enter the IP address of the remote server(s). The sever switch will send messages to this device.

Step 5 Click **Apply**.

Assigning an Authentication Method

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame.

Step 4 In the Authentication Method field (under the Radius heading), click a radio button to choose a method, and then click **Apply**. Table 4-3 describes the radio buttons that you can choose.

Table 4-3 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.

Configuring HTTP and HTTPS

To configure HTTP and HTTPS services, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **HTTP** branch.

The System HTTP display appears in the View frame.

Step 4 (Optional) Check or uncheck the **Enable** check box in the Polling field to enable or disable automatic polling.

Step 5 (Optional) Click a radio button in the Secure Cert Common Name field of the identifier that you want to use for security certification.

Step 6 Click **Apply**.

Viewing and Managing RADIUS Servers

These topics describe how to view and manage RADIUS servers:

Viewing RADIUS Servers

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Radius Servers** branch.

The Radius Servers display appears in the View frame. Table 4-4 describes the fields in the Radius Servers table.

Table 4-4 Radius Servers Table Field Descriptions

Field	Description
Address	Displays the IP address of the RADIUS server.
Priority	Sequence number designating the order in which the authentication process accesses Radius servers. Priority is assigned in the order in which you configure Radius servers.
UDP Port	UDP authentication port of the RADIUS server.

Table 4-4 Radius Servers Table Field Descriptions (continued)

Field	Description
Encryption Key	Authentication key that the client and RADIUS server use.
Timeout	Amount of time, in seconds, in which the server must authenticate a login before the login fails.
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username altogether.

Viewing and Configuring RADIUS Server Properties

To view and configure RADIUS servers to authenticate CLI logins, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Radius Servers** branch.

The Radius Servers table appears in the View frame.

Step 4 Click the radio button to the left of the server whose properties you want to view or configure, and then click **Properties**.

The Radius Server Properties window opens. Table 4-5 describes the fields in the Radius Server Properties window.

Table 4-5 Radius Server Properties Window Fields

Field	Description
Address field	Displays the IP address of the RADIUS server.
UDP Port field	UDP 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 of integer values that this field supports.
Encryption Key	Authentication key that the client and RADIUS server use. 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 of integer values that this field supports.
Timeout	Amount of time, in seconds, in which the server must authenticate a login before the login fails. 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 of integer values that this field supports.

Table 4-5 Radius Server Properties Window Fields (continued)

Field	Description
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username. 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 of integer values that this field supports.
Priority	Server priority for use.
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 configure a new RADIUS server on your device, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Radius Servers** branch.

The Radius Servers table appears in the View frame.

Step 4 Click **Add**.

The Add 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 5 In the Address field, enter the IP address of the server.

Step 6 (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 7 (Optional) Enter an encryption key in the Encryption Key field.

Step 8 (Optional) Edit the Timeout field. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 9 (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 10 Click **Apply**.

Deleting RADIUS Servers

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Radius Servers** branch.

The Radius Servers table appears in the View frame.

Step 4 Click the radio button to the left of the server that you want to delete.

Note Chassis Manager will not prompt you to be sure that you want to delete this server.

Step 5 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 Chassis Manager logins, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Tacacs Servers** branch.

The Tacacs Servers display appears in the View frame. Table 4-6 describes the fields in the Tacacs Servers table.

Table 4-6 Tacacs Servers Table Field Descriptions

Field	Description
Address	Displays the IP address of the TACACS server.
Priority	Server priority for use.
UDP Port	UDP authentication port of the TACACS server.
Encryption Key	Authentication key that the client and TACACS server use.

Table 4-6 Tacacs Servers Table Field Descriptions (continued)

Field	Description
Timeout	Amount of time, in seconds, in which the server must authenticate a login before the login fails.
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username.

Viewing and Configuring TACACS Server Properties

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Tacacs Servers** branch.

The Tacacs Servers table appears in the View frame.

Step 4 Click the radio button to the left of the server whose properties you want to view or configure, and then click **Properties**.

The Tacacs Server Properties window opens. Table 4-7 describes the fields in the Tacacs Server Properties window.

Table 4-7 Tacacs Server Properties Window Fields

Fields	Description
Address	Displays the IP address of the TACACS server.
Priority	Server priority for use.
UDP Port	UDP 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.
Encryption Key	Authentication key that the client and TACACS server use. 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 of integer values that this field supports.
Timeout	Amount of time, in seconds, in which the server must authenticate a login before the login fails. 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 of integer values that this field supports.

Table 4-7 Tacacs Server Properties Window Fields (continued)

Fields	Description
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username. 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 TACACS Servers

To configure a new TACACS server on your device, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Tacacs Servers** branch.

The Tacacs Servers table appears in the View frame.

Step 4 Click **Add**.

The Add Tacacs 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 5 In the Address field, enter the IP address of the server.

Step 6 (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 7 (Optional) Enter an encryption key in the Encryption Key field.

Step 8 (Optional) Edit the Timeout field. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 9 (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 10 Click **Apply**.

Deleting TACACS Servers

To remove a TACACS server from your configuration, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Tacacs Servers** branch.

The Tacacs Servers table appears in the View frame.

Step 4 Click the radio button to the left of the server that you want to delete.

Step 5 Click **Delete**.

Viewing Authentication Failures

To view a log of authentication failures for your server switch, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Authentication Failures** branch.

The Authentication Failures display appears in the View frame. Table 4-8 describes the fields in this display.

Table 4-8 Authentication Failures Field Descriptions

Field	Description
CLI Access Violation Count	Cumulative number of failed CLI logins since the server switch booted.
CLI Last Violation Time	Time of the most recent failed CLI login.
SNMP Access Violation Count	Cumulative number of failed SNMP logins since the server switch booted.
SNMP Last Violation Time	Time of the most recent failed SNMP login.
HTTP Access Violation Count	Cumulative number of failed HTTP logins since the server switch booted.
HTTP Last Violation Time	Time of the most recent failed HTTP login.

Viewing Diagnostic Test Results

Available test results vary by hardware platform.

These topics describe how to view diagnostic test results:

Viewing Card POST Test Results

To view power-on self-test results for a card, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **POST** branch.

The POST Status table appears in the View frame. Table 4-9 describes the fields in the table.

Table 4-9 Card POST Test Status Field Descriptions

Field	Description
Card	Card on which the power-on self-test ran.
Post Status	Status of the test.
Error Code	Applicable error codes that resulted from the test.

Viewing Fan POST Test Results

To view power-on self-test results for a fan, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **POST** branch.

The POST Status table appears in the View frame. Table 4-10 describes the fields in the table.

Table 4-10 Fan POST Test Status Field Descriptions

Field	Description
Fan	Fan on which the power-on self-test ran.
Post Status	Status of the test.
Error Code	Applicable error codes that resulted from the test.

Viewing Power Supply POST Test Results

To view power-on self-test results for a power supply, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **POST** branch.

The POST Status table appears in the View frame. Table 4-11 describes the fields in the table.

Table 4-11 Power Supply POST Test Status Field Descriptions

Field	Description
Power Supply	Power supply on which the POST test ran.
Post Status	Status of the test.
Error Code	Applicable error codes that resulted from the test.

Viewing Card FRU Errors

Note This procedure displays runtime errors that are not caught by POST. POST errors are also displayed using this procedure.

To view card FRU errors, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **Fru Error** branch.

The Fru Error display appears in the View frame. Table 4-12 describes the fields shown in the Card portion of the display.

Table 4-12 Card FRU Field Descriptions

Field	Description
Card	Slot number of the card.
Error Code	Shows the last hardware error (if any) detected on this card. The information provided in this field is read from the vital product data of the device.

Viewing Fan FRU Errors

Note This procedure displays runtime errors that are not caught by POST. POST errors are also displayed using this procedure.

To view fan FRU errors, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **Fru Error** branch.

The Fru Error display appears in the View frame. Table 4-12 describes the fields shown in the Fan portion of the display.

Table 4-13 Fan FRU Field Descriptions

Field	Description
Fan	Fan number.
Error Code	Shows the last hardware error (if any) detected on this fan. The information provided in this field is read from the vital product data of the device.

Viewing Power Supply FRU Errors

Note This procedure displays runtime errors that are not caught by POST. POST errors are also displayed using this procedure.

To view power supply FRU errors, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **Fru Error** branch.

The Fru Error display appears in the View frame. Table 4-12 describes the fields shown in the Card portion of the display.

Table 4-14 Power Supply FRU Field Descriptions

Field	Description
Power Supply	Power supply number.
Error Code	Shows the last hardware error (if any) detected on this power supply. The information provided in this field is read from the vital product data of the device.