Maintenance Icon Tasks

This chapter describes the Chassis Manager maintenance icon tasks and contains these sections:

Configuring Basic System Information

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

Viewing System Information

To view basic system information, perform the following steps:

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

Step 2 Click the **System Information** branch. The System Information display appears in the View frame. Table 4-1 lists and describes the fields in this table.

Table 4-1 System Information Elements

Element	Description
Description field	Description of the chassis and the image that runs on the chassis.
System Uptime field	Amount of time that the chassis has run since the last boot.
Last Change Made At field	Date and time that a user last changed the running configuration.
Last Config Saved At field	Date and time that a user last saved the running configuration as the startup configuration.
System Name field	Configurable name for your Server Switch.
Location field	Configurable location of your Server Switch.
Support Contact field	Configurable support information for your Server Switch.
Apply button	Applies changes that you make in configurable fields to your Server Switch.
Refresh button	Refreshes the System Information display.
Rack Locator UID field (select chassis only)	Unique rack-locator ID.
System Operation Mode field	Provides a Normal radio button for non-VFrame environment and a VFrameManaged radio button for VFrame environments.

Naming Your InfiniBand Switch

To assign a hostname to your device, perform the following steps:

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

Step 2 Click 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 the **Apply** button.

Defining Device Location

To add a physical device location description to your switch, perform the following steps:

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

Step 2 Click 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 the **Apply** button.

Defining Technical Support Resource

The technical support email address that you define appears in the System frame when you refresh or restart Chassis Manager. To define a technical support resource, perform the following steps:

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

Step 2 Click the **System Information** branch. The System Information display appears in the View frame.

Step 3 In the Support Contact field, type the email address of your technical support provider, and then click the **Apply** button.

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.

Configuring Date and Time

To configure the date and time of the internal clock on your device, perform the following steps:

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

Step 2 Click 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 the **Apply** button.

Assigning NTP Servers

To configure your device to use an NTP server to synchronize your Server Switch with the network, perform the following steps:

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

Step 2 Click 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 in the event that 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 in the event that your switch cannot access the primary or secondary NTP servers.

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

Viewing Files in the File System

To view files, such as image files, log files, and configuration files, that reside on your device, perform the following steps:

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

Step 2 Click the **File Management** branch. The File Management table appears in the View frame. Table 4-2 lists and 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 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 3 (Optional) Click the **Refresh** button 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, perform the following steps:

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

Step 2 Click the **File Management** branch. The File Management table appears in the View frame.

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

Installing Software Images

To install an image file, perform the following steps:

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

Step 2 Click 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, refer to "Importing Configuration Files and Image Files with FTP" section on page 4-5.

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

Note 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

To import files to your Server Switch from remote devices, perform the following steps:

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

Step 2 Click the **File Management** branch. The File Management table appears in the View frame.

Step 3 Click the **Import** button. The Import File window opens.

Step 4 Select a file type (**Image** or **Configuration**) from the File Type pulldown menu.

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

Step 6 Enter the IP address of the server that holds the file that you want to import in the Remote IP Address field.

Step 7 Enter the user ID that logs you in to the server in the Remote User Name field.

Step 8 Enter the password logs you in to the server in the Remote Password field.

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.

Step 11 Click the **Import** button. A status bar appears to display the progress of the file transfer.

Exporting Configuration Files and Log Files with FTP

To export files from your Server Switch to remote devices, perform the following steps:

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

Step 2 Click 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 the **Export** button. The Export File window opens and the name of the file that you chose to export appears in the File Name on System field.

Step 5 Select **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 the user ID that logs you in to the server, in the Remote User Name field.

Step 8 Enter the password that logs you in to the server, in the Remote Password field.

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

Step 10 Click the **Export** button. A status bar appears to display the progress of the file transfer.

Customizing the Boot Configuration

Customize the boot configuration to do the following:

- 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.

To customize the boot configuration, perform the following steps:

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

Step 2 Click the **Boot Configuration** branch. The Boot Configuration display appears in the View frame.

Step 3 (Optional) From the Image Source For Next Reboot pulldown menu, select the image that you want the Server Switch to boot when it reboots.

Step 4 (Optional) Click the **Overwrite startup configuration with** radio button, and then select a configuration from the pulldown menu to replace the current startup configuration with another configuration file.

Note To overwrite your startup configuration with your running configuration, refer to the "Backiung Up the Running Configuration File" section on page 4-7.

Step 5 (Optional) Click the **Delete startup configuration** radio button to configure your Server Switch to use the factory default startup configuration.

Step 6 Click the **Apply** button.

Backiung Up the Running Configuration File

To save your running configuration file, perform the following steps:

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

Step 2 Click 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 will save your running configuration in the config directory with the name 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 the **Save** button. Optionally, click the **File Management** branch to verify that your file appears in the file system.

Saving Configuration File

To back up your running configuration as your startup configuration (and to the standby controller on your chassis in dual-controller chassis), perform the following steps:

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

Step 2 Click the **Save Config** branch. The Save Config display appears in the View frame.

Step 3 Click the **Save Config** button.

Rebooting the Device

When you reboot your device, Element Manager gives you the option to reboot without saving your configuration or to save your configuration, and then reboot. If you choose to reboot but not save, any differences between your running configuration file and startup configuration file do not persist after the reboot.

To reboot your Server Switch with Chassis Manager, perform the following steps:

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

Step 2 Click the **Reboot** branch. The Reboot display appears in the View frame.

Step 3 Click the **Reboot** button.

Configuring Basic Services

Configure basic services to facilitate remote access to your device.

Assigning a DNS Server

To assign a DNS server to your device, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click 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 that you want 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 the **Apply** button.

Enabling or Disabling the FTP Access

To enable FTP transfers to and from your device, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click the **General** branch. The System Services display appears in the View frame.

Step 4 In the FTP Server field, check (enable) or uncheck (disable) the **Enable** checkbox, and then click the **Apply** button.

Enabling or Disabling the Telnet Access

To enable telnet access to your device, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click 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** checkbox, and then click the **Apply** button.

Assigning a SYSLOG Server

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

To assign a SYSLOG server to store logs from your device, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click the **General** branch. The System Services display appears in the View frame.

Step 4 In the Remote Syslog Server field, enter the IP address of the remote server to accept messages from your device, and then click the **Apply** button.

Assigning an Authentication Method

To assign an authentication method to your device, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click 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 select a method, and then click the **Apply** button. Table 4-3 lists and describes the radio buttons that you can choose.

Table 4-3 Authentication Methods

Button	Description
local	Authenticates user logins with the local CLI user database only.
localThenRadius	Authenticates user logins with the local CLI user database; upon failure, authenticates with the RADIUS server.
radiusThenLocal	Authenticates user logins with the RADIUS server; upon failure, authenticates with the local CLI user database.

Configuring HTTP and HTTPS

To configure HTTP and HTTPS services, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click the **HTTP** branch. The System HTTP display appears in the View frame.

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

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

Step 6 Click the **Apply** button.

Viewing RADIUS Servers

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

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click the **Radius Servers** branch. The Radius Servers display appears in the View frame. Table 4-4 lists and 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.
UDP Port	UDP authentication port of the RADIUS server.
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 update the RADIUS servers that you have configured your device to use to authenticate CLI logins, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click 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 the **Properties** button. The Radius Server Properties window opens. Table 4-5 lists and describes the elements in the Radius Server Properties window.

Table 4-5 Radius Server Properties Window Elements

Element	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 the **Apply** button 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 field	Authentication key that the client and RADIUS server use. Enter a value and click the **Apply** button 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 field	Amount of time, in seconds, in which the server must authenticate a login before the login fails. Edit this value and click the **Apply** button 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.
Max Retries field	Number of sequential logins that a user may perform before the server denies access to the username altogether. Edit this value and click the **Apply** button 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.
Access Requests field	Number of authentication requests that the server has received from your device since your device booted.
Access Accepts field	Number of logins to your device that the server authenticated since your device booted.
Access Rejects field	Number of logins to your device that the server denied since your device booted.
Server Timeout field	Number of authentications that timed out on the server since your device booted.
Apply button	Applies the changes that you make in the Radius Server Properties window.
Reset button	Resets the fields in the window to match the server configuration.
Close button	Closes the Radius Server Properties window. If you close the window before you apply changes, Chassis Manager makes no changes to the configuration.
Help button	Opens online help.

Adding RADIUS Servers

To configure a new RADIUS server on your device, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click the **Radius Servers** branch. The Radius Servers table appears in the View frame.

Step 4 Click the **Add** button. The Add Radius Server window opens.

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

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 the **Apply** button.

Deleting RADIUS Servers

To remove a RADIUS server from your configuration, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click 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 the **Delete** button.

Viewing Authentication Failures

To view a log of authentication failures for your Server Switch, perform the following steps:

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

Step 2 Expand the **Services** sub-icon in the Tree frame.

Step 3 Click the **Authentication Failures** branch. The Authentication Failures display appears in the View frame. Table 4-6 lists and describes the fields in this display.

Table 4-6 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.

Viewing POST Test Results

To view POST test results, perform the following steps:

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

Step 2 Expand the **Diagnostics** sub-icon in the Tree frame.

Step 3 Click the **POST** branch. The POST Status table appears in the View frame. Table 4-7 lists and describes the fields in the table.

Table 4-7 POST Status Field Descriptions

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

Viewing FRU Errors

To view FRU test results, perform the following steps:

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

Step 2 Expand the **Diagnostics** sub-icon in the Tree frame.

Step 3 Click the **Fru Error** branch. The Fru Error display appears in the View frame. The display lists each FRU and any error messages that apply to the FRU.