CHAPTER 6

Health Tasks

These topics describe the Health tasks for Element Manager:

Note The Health menu provides options that let you verify the status of your server switch. With Health menu options, you can view the operational status of server switch and view logs of server switch events.

Viewing the Health Summary

To view a summary of the health of your server switch, follow these steps:

Step 1 From the Health menu, choose **Status**.

The Health Status window opens.

Step 2 Click the **Summary** tab.

Table 6-1 describes the Summary tab fields.

Table 6-1 Summary Tab Field Descriptions

Field	Description
Up Time	Amount of time that the switch has been up since the last reboot.
Power	Displays a green check if all power supplies function successfully. Displays a red X if a power supply experiences a problem.
Fans	Displays a green check if all fans function successfully. Displays a red X if a fan experiences a problem.
Sensors	Displays a green check if all temperature sensors function successfully. Displays a red X if a temperature sensor experiences a problem or if the temperature exceeds the safe threshold.

Viewing Power Supply Status

To view the status of the power supplies on your server switch, follow these steps:

Step 1 From the Health menu, choose **Status**.

The Health Status window opens.

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

Table 6-2 describes the Power Supplies tab fields.

Table 6-2 Power Supplies Tab Field Descriptions

Field	Description
PS ID	Numeric identifier of the power supply. For more information about the power supplies in your device, see your hardware documentation.
Type	Type of power (AC or DC).
Admin Status	Displays the status to which a user has configured the power supply.
Oper Status	Displays up to indicate that your power supply functions and currently supplies power to your device. Displays down for faulty power supplies.
Utilization	Percentage of total power supply resources in use.
Voltage	Voltage of the power supply.
Product Serial Number	Factory-assigned product serial number.
PCA Serial Number	Printed circuit assembly (PCA) serial number.
PCA Assembly Number	Printed circuit assembly (PCA) assembly number.
FRU Number	Field-replaceable unit (FRU) number.

Viewing Fan Status

To view the status of the fans on your server switch, follow these steps:

Step 1 From the Health menu, choose **Status**.

The Health Status window opens.

Step 2 Click the **Fans** tab.

Table 6-3 describes the Fans tab fields.

Table 6-3 Fans Tab Field Descriptions

Field	Description
FanId	Numeric identifier of the fan. For more information about the fans in your device, see your hardware documentation.
OperStatus	Displays up if the fan functions properly; otherwise, displays down.
Speed	Speed of the fan as a percentage of maximum speed.
ProductSerialNum	Factory-assigned product serial number.
PcaSerialNum	Printed circuit assembly (PCA) serial number.
PcaAssemblyNum	Printed circuit assembly (PCA) assembly number.
FruNum	Field-replaceable unit (FRU) number.

Viewing Sensor Status

To view the status of the temperature sensors on your server switch, follow these steps:

Step 1 From the Health menu, choose **Status**.

The Health Status window opens.

Step 2 Click the **Sensors** tab.

Table 6-4 describes the Sensors tab fields.

Table 6-4 Sensors Tab Field Descriptions

Field	Description
Slot ID	Numeric identifier of the slot in which the temperature sensor resides. For more information about the slots in your device, see your hardware documentation.
Sensor ID	Numeric identifier of the temperature sensor.
Oper Status	Operational code of the sensor. The values are normal, tempAlert, currAlert, or voltAlert.
Oper Code	Temperature of the slot.
Current Temp	Current temperature of the chassis.
Alarm Temp	Chassis temperature that triggers an alarm.
Shutdown Temp	Chassis temperature that triggers a shutdown.

Viewing and Managing Server Switch Events

These topics describe how to view and manage server switch events:

Viewing Server Switch Events

When you configure your local host to receive server switch events, you can then view a log of the events. Before you view server switch events, see the "Configuring Your Host as a Trap Receiver" section on page 6-8.

To view server switch events on a host that you have configured to receive events, follow these steps:

Step 1 From the Health menu, choose **Event Viewer**.

The Event Viewer window opens. Table 6-5 describes the fields in the window.

Step 2 (Optional) Click the **Node** column header to organize the Event Viewer table by node. Click the header a second time to reverse the order (from top to bottom) of the display.

Step 3 (Optional) Click the **Time** column header to organize the Event Viewer table by node. Click the header a second time to reverse the order (from top to bottom) of the display.

Step 4 (Optional) Click the **Type** column header to organize the Event Viewer table by node. Click the header a second time to reverse the order (from top to bottom) of the display.

Step 5 (Optional) Click the **Description** column header to organize the Event Viewer table by node. Click the header a second time to reverse the order (from top to bottom) of the display.

Table 6-5 Event Viewer Field Descriptions

Field	Description
Node	IP address of the server switch on which the event took place.
Time	Time that the event took place.
Type	Type of event that took place.
Description	Description of the event.

Exporting Event Logs to a Text File

To export an event log, follow these steps:

Step 1 From the Health menu, choose **Event Viewer**.

The Event Viewer window opens.

Step 2 Click **Export**.

The Save window opens.

Step 3 Navigate to the directory on your local host on which you want to store the event log.

Step 4 In the File Name field, enter a filename for the log, and then click **Save**.

Element Manager creates a text file with the contents of the event log on your host.

Clearing Event Entries by Category

To clear event entries from the Event Viewer table, follow these steps:

Step 1 From the Health menu, choose **Event Viewer**.

The Event Viewer window opens.

Step 2 Click **Clear**, and then click the type of entry that you want to remove from the table.

All entries of that type disappear from the display.

Clearing All Event Entries

To clear all event entries from the Event Viewer table, follow these steps:

Step 1 From the Health menu, choose **Event Viewer**.

The Event Viewer window opens.

Step 2 Click **Clear**, and then click **All**.

All event entries disappear from the display.

Configuring Trap Receivers

These topics describe how to configure your host as a trap receiver:

Verifying Your Host as a Trap Receiver

You must configure your host to receive traps in order to view events. If no other application on your local host controls port 162, Element Manager automatically registers your local host as a trap receiver. To verify that Element Manager registered your host, follow these steps:

Step 1 From the Health menu, choose **Trap Receivers**.

The Trap Receivers window opens.

Step 2 Verify that the IP address of your host appears in the Address column.

Step 3 If it appears, verify that **true** appears in the Receive Events column.

Note If your local host has multiple IP addresses (for instance, one from a LAN and one from a wireless connection), disable all IP addresses other than the LAN address, and then close Element Manager and open it again. Verify that only the LAN address appears in the Trap Receivers window. If it appears, you can enable your other addresses.

Configuring Your Host as a Trap Receiver

If you have an application (other than Element Manager) that takes over port 162 to receive and manage SNMP traps, you must add your host to the server switch configuration with Element Manager so that the application receives server switch traps. To add your host as a trap receiver, follow these steps:

Step 1 From the Health menu, choose **Trap Receivers**.

The Trap Receivers window opens.

Step 2 Click **Insert**.

The Insert Trap Receivers window opens.

Step 3 In the Address field, enter the IP address of your host.

Step 4 In the Community field, enter the SNMP community of your host.

Step 5 Check the **Receive Events** check box, and then click **Insert**.

Deleting Your Host as a Trap Receiver

If you manually configured your host as a trap receiver, you must manually remove your host to de-register. To delete your host as a trap receiver, follow these steps:

Step 1 From the Health menu, choose **Trap Receivers**.

The Trap Receivers window opens.

Step 2 Click your host in the Trap Receivers table, and then click **Delete**.

Step 3 Click **Close**.

Viewing Authentication Failures and Enabling Authentication Traps

These topics describe how to view authentication failures and enable authentication traps:

- Viewing Authentication Failures, page 6-9
- Enabling Authentication Traps, page 6-10

Viewing Authentication Failures

To view authentication failures, from the Health menu, choose **Authentication**.

The Authentication window opens. Table 6-6 describes the fields in this window.

Table 6-6 Authentication Field Descriptions

Field	Description
Enable Authentication Traps	Radio buttons enable and disable authentication traps.
CLI Access Violation Count	Number of CLI access violation counts.
CLI Last Violation Time	Time of the most recent CLI access violations.
SNMP Access Violation Count	Number of SNMP access violation counts.
SNMP Last Violation Time	Time of the most recent SNMP access violations.
HTTP Access Violation Count	Number of HTTP access violation counts.
HTTP Last Violation Time	Time of the most recent HTTP access violations.

Enabling Authentication Traps

To enable authentication traps, follow these steps:

Step 1 From the Health menu, choose **Authentication**.

The Authentication window opens.

Step 2 Click the **enabled** radio button, and then click **Apply**.

Viewing and Filtering Logs

These topics describe how to view and filter logs:

- Viewing Logs, page 6-10
- Applying Filters to ts_log Displays, page 6-10

Viewing Logs

To view one of the logs in the file system on your server switch, follow these steps:

Step 1 From the Health menu, choose **Log Viewer**.

The Log Viewer window opens.

Step 2 Click **Download**.

The Download Log Files window opens.

Step 3 In the Available log files table, click the log that you want to view, and then click **Download**.

The Save As window opens.

Step 4 Navigate to the directory in which you want to save the log file, and then click **Save**.

A Download Complete window opens and displays an Open File check box.

Step 5 Check the **Open File** check box, and then click **OK**.

The log opens in the Log Viewer window.

Applying Filters to ts_log Displays

When you configure and apply filters, Element Manager removes from the display all entries that do not match the filter criteria. To filter particular entries from log displays, follow these steps:

Step 1 From the Health menu, choose **Log Viewer**.

The Log Viewer window opens.

Step 2 Open a ts_log file. For detailed instructions, see the "Viewing and Filtering Logs" section on page 6-10.

Step 3 Click **Filter**.

The Log Filter window opens.

Step 4 Select the filter attributes that you want to apply:

- All filter options are cumulative. If you choose slot 1 and WARN, the log viewer displays only logs that apply to slot 1 *and* are of the WARN type. Any WARN type messages that do not apply to slot 1 do not appear. Any slot 1 messages of other types do not appear.
- Click **Show Advanced** to reveal application options that you can add to the filter. Click an application to apply it to the filter. Press the **Ctrl** key, and click additional applications to apply multiple applications to the filter.

Step 5 Click **Apply**.

All entries that do not match the filter disappear from the display.