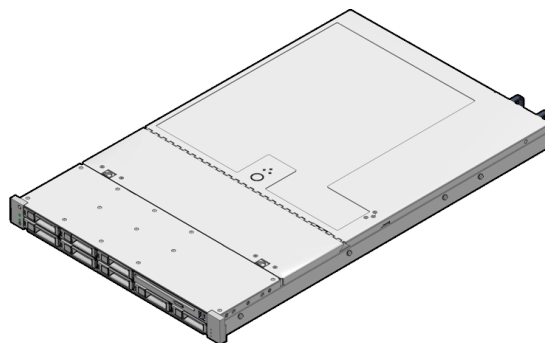


# Embedded Lights Out Manager Administration Guide

---

for the Sun Fire™ X4150 and X4450 Servers



Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

Part No. 820-1855-13  
April 2008, Revision A

Submit comments about this document at: <http://www.sun.com/hwdocs/feedback>

Copyright © 2007 - 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

THIS PRODUCT CONTAINS CONFIDENTIAL INFORMATION AND TRADE SECRETS OF SUN MICROSYSTEMS, INC. USE, DISCLOSURE OR REPRODUCTION IS PROHIBITED WITHOUT THE PRIOR EXPRESS WRITTEN PERMISSION OF SUN MICROSYSTEMS, INC.

This distribution may include materials developed by third parties. Sun, Sun Microsystems, the Sun logo, Java, Netra, Solaris, StarOffice, Sun Ray, Sun Fire and the SunSpectrum Pac (Sunburst design) logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries. Intel Inside is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

This product is covered and controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

Use of any spare or replacement CPUs is limited to repair or one-for-one replacement of CPUs in products exported in compliance with U.S. export laws. Use of CPUs as product upgrades unless authorized by the U.S. Government is strictly prohibited.

---

Copyright © 2007 - 2008 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

CE PRODUIT CONTIENT DES INFORMATIONS CONFIDENTIELLES ET DES SECRETS COMMERCIAUX DE SUN MICROSYSTEMS, INC. SON UTILISATION, SA DIVULGATION ET SA REPRODUCTION SONT INTERDITES SANS L'AUTORISATION EXPRESSE, ECRITE ET PREALABLE DE SUN MICROSYSTEMS, INC.

Cette distribution peut des éléments développés par des tiers. Sun, Sun Microsystems, le logo Sun, Java, Netra, Solaris, StarOffice, Sun Ray, Sun Fire et le logo SunSpectrum Pac (Sunburst design) sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Intel est une marque de fabrique ou une marque déposée de Intel Corporation ou de sa filiale aux Etats-Unis et dans d'autres pays. Intel Inside est une marque de fabrique ou une marque déposée de Intel Corporation ou de sa filiale aux Etats-Unis et dans d'autres pays.

Ce produit est soumis à la législation américaine sur le contrôle des exportations et peut être soumis à la réglementation en vigueur dans d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou reexportations vers les pays sous embargo américain, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exhaustive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine sur le contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

L'utilisation de pièces détachées ou d'unités centrales de remplacement est limitée aux réparations ou à l'échange standard d'unités centrales pour les produits exportés, conformément à la législation américaine en matière d'exportation. Sauf autorisation par les autorités des Etats-Unis, l'utilisation d'unités centrales pour procéder à des mises à jour de produits est rigoureusement interdite.



Adobe PostScript

# Contents

---

<b>Preface</b>	<b>xiii</b>
<b>1. Embedded Lights Out Manager Overview</b>	<b>1</b>
ELOM Features	2
ELOM Common Tasks	2
Server Default Settings	3
About the Preconfigured Administrator Account	3
About the Indicator and Fault LEDs	4
<b>2. Connecting to the ELOM</b>	<b>5</b>
About Connection Tasks	6
Connecting Using a Serial Connection	6
▼ To Connect Using a Serial Connection	6
Connecting Using Ethernet	7
<b>3. Monitoring the Server System Using the Web GUI</b>	<b>11</b>
Using the Web GUI	11
Browser and Software Requirements	12
Users and Privileges	12
Web GUI Tasks	12
Accessing the ELOM Using a Web Browser	13

- ▼ To Access the ELOM Using a Web Browser 13
- Viewing the System From the Web Browser 14
- Viewing System and Component Information 16
  - ▼ To View System Information 16
  - Viewing SP Version Information 16
  - ▼ To View SP Version Information 16
  - Viewing Server Board Information 17
  - ▼ To View Server Board Information 17
  - Viewing Component Information 17
  - ▼ To View CPU Information 17
  - Viewing Memory Information 18
  - ▼ To View Memory Information 18
- Monitoring the System Sensors 19
  - ▼ To Monitor the System Sensors 19
  - Reading Sensors 19
  - ▼ To Read Sensors 19
  - Viewing a Sensor Summary 20
  - ▼ To View a Sensor Summary 20
- Monitoring Fans 22
  - ▼ To Monitor Fans 22
- Monitoring Temperatures 22
  - ▼ To Monitor Temperatures 22
- Monitoring Voltages 23
  - ▼ To Monitor Voltage 23
- Viewing and Managing the Event Log 23
  - ▼ To Display the Event Log 24
  - ▼ To View the Event Logs 24
  - ▼ To Save the Event Log 24

- ▼ To Clear the Event Log 25
- 4. Configuring, Managing and Maintaining the Server Using the Web GUI 27**
  - Configuring the System 28
    - ▼ To Configure the System 29
  - Configuring Network Settings 30
    - ▼ To Configure the Network Settings 30
  - Configuring E-mail Notification 30
    - ▼ To Configure E-mail Notification 30
  - Configuring Platform Event Filters 30
    - ▼ To Configure a Platform Event Filter 31
  - Configuring System Management Access 33
    - ▼ To access the System Management Access Submenus 33
  - Configuring the SSL Certificate 34
    - ▼ To Configure the SSL Certificate 34
  - Configuring SNMP 34
    - ▼ To Configure SNMP 35
    - ▼ To Add an SNMP Community 35
    - ▼ To Delete an SNMP Community 36
    - ▼ To Modify an SNMP Community 36
    - ▼ To Add an SNMP User 36
    - ▼ To Delete an SNMP User 37
    - ▼ To Edit an SNMP User 37
  - Configuring Active Directory Service 37
    - ▼ To Configure Active Directory Service 38
- Managing and Maintaining the System 46
  - Managing Users and Accounts 46
    - ▼ To Add a User 49
    - ▼ To Change a User Password or Privilege 51

- ▼ To Delete a User Account 51
- ▼ To Disable or Enable a User 51
- Managing the State of the System Locator Indicator LED 52
- ▼ To Manage the State of the System Locator Indicator LED 52
- Managing the Front Panel and On-Board Fault LEDs 52
- ▼ To View the State of the Fault LEDs 53
- ▼ To Turn the Fault LEDs Off 53
- Setting Power Control 54
- ▼ To Set Power Control 54
- Resetting the Service Processor 54
- ▼ To Reset the Service Processor 54
- Updating the Firmware 55
- Updating the firmware using the Tools and Drivers CD 55
- ▼ To Update the firmware Using the Tools an Drivers CD 55
- Updating the Firmware Using a Web Browser 56
- ▼ To Update the Firmware Using a Web Browser 56
- Managing Session Timeout 57
- ▼ To Set the Session Timeout 57
- ▼ To Disable the Session Timeout 57
- Setting the Time 58
- ▼ To Set the Time 58
- Changing the Administrator Password Using the BIOS Setup Utility 58
- ▼ To Change the Administrator Password using the BIOS Setup Utility 58
- Recovering from a Corrupt SP 59

## **5. Using the Remote Console Application 61**

Accessing the Remote Console 61

Requirements 61

CD and Diskette Redirection Operational Model 62

Starting the Remote Console Application	64
▼ To Start the Remote Console Application	64
Setting Parameters for the Remote Console	65
▼ To Set Parameters for the Remote Console	65
Redirecting Keyboard, Video, Mouse, or Storage Devices	66
▼ To Redirect Keyboard and Mouse Devices	66
▼ To Redirect Storage Devices	67
Redirection and Mount Workarounds for RHEL	68
Installing an Operating System on a Remote Server	72
▼ To Install an OS on a Remote Server Using a Virtual CD-ROM	72
Other Remote Options	73
<b>6. Using IPMI</b>	<b>75</b>
About IPMI	75
IPMItool	76
Sensors	76
Supported IPMI 2.0 Commands	77
<b>7. Using the Command-Line Interface</b>	<b>83</b>
Logging In to the CLI	83
Command Syntax	84
Managing the Host	86
Managing the Host State	86
Managing the Host Console	87
Viewing Host Sensors	87
Managing ELOM Network Settings	88
▼ To Display Network Settings	88
▼ To Configure Network Settings	88
Managing Local User Accounts With the CLI	89

Adding a User Account Using the CLI	90
▼ To Add a User Account Using the CLI	90
To Delete a User Account Using the CLI	90
▼ To Display User Accounts Using the CLI	90
Configuring User Accounts	91
Managing Alerts	92
Displaying Alerts	92
▼ To Display Alerts	92
Displaying PET Target Properties	93
▼ To Display PET Target Properties	93
Configuring Alerts	94
Configuring the PET IP Address	94
▼ To Configure the PET IP Address	94
Configuring the PEF Global Controls	95
▼ To Configure the PEF Global Controls	95
Configuring the Event Filter Tables	96
▼ To Configure the Event Filter Tables	97
Displaying Version Information	99
To Display the Current SP Version Information	99
Updating the Firmware	100
▼ To Update the Firmware	100
<b>8. Using Simple Network Management Protocol</b>	<b>103</b>
About SNMP	103
How SNMP Works	103
SNMP MIB Files	104
MIBs Integration	104
SNMP Messages	105
Configuring SNMP on the ELOM	106



Adding Your Server to Your SNMP Environment	106
Configuring Receipt of SNMP Traps	106
Managing SNMP User Accounts	106
Adding a User Account	106
Deleting a User Account	107
Configuring User Accounts	107
<b>A. Command-Line Interface Reference</b>	<b>109</b>
CLI Command Quick Reference	109
CLI Command Reference	113
Properties and Values for Targets	122
<b>Index</b>	<b>135</b>



# Figures

---

FIGURE 3-1	ELOM System Information Screen	14
FIGURE 3-2	An Excerpt of the View Event Logs Screen	24
FIGURE 4-1	The Configuration Screen	29
FIGURE 4-2	The Platform Event Filter Screen	32
FIGURE 4-3	Windows Components Screen	38
FIGURE 4-4	CA Type Windows Components Wizard Screen	39
FIGURE 4-5	Public and Private Key Pair Windows Components Wizard Screen	39
FIGURE 4-6	CA Identifying Information Windows Components Wizard Screen	40
FIGURE 4-7	Certificate Database Settings Windows Components Wizard Screen	41
FIGURE 4-8	The Certificate Information Screen	42
FIGURE 4-9	The Certificate Details Screen	43
FIGURE 4-10	The Certificate Export Wizard Screen	43
FIGURE 4-11	The Export File Format	44
FIGURE 4-12	The File to Export Screen	45
FIGURE 4-13	The User Management Screen	50
FIGURE 4-14	The Fault LED Screen	53
FIGURE 5-1	Keyboard, Video, and Mouse Selections	67
FIGURE 8-1	Sun Server MIB Tree	105



# Preface

---

The *Embedded Lights Out Manager Administration Guide for the Sun Fire X4150 and X4450 Servers* provides instructions for managing Sun servers using the Embedded Lights Out Manager (ELOM) with the service processor.

---

## How This Document Is Organized

**Chapter 1** provides an overview of the ELOM and indicates tasks that can be accomplished with the management software.

**Chapter 2** details the physical connections and how to communicate with your Sun Fire server.

**Chapter 3** describes how to use the web GUI to monitor your server with the embedded system management software.

**Chapter 4** provides information about configuring, managing and maintaining the server system with a web browser.

**Chapter 5** describes how to use the remote console through the web GUI.

**Chapter 6** describes the Intelligent Platform Interface (IPMI) and how it can be used to manage field replaceable units (FRUs) and system health independently of the operating system.

**Chapter 7** provides an alternative method of managing your server—through the command-line interface (CLI).

**Chapter 8** helps you understand the basics of the Simple Network Management Protocol (SNMP) and how it is important to your server management.

[Appendix A](#) gives you a quick reference to the commands you can use with Embedded Lights Out Manager.

---

## Using UNIX Commands

This document might not contain information about basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to the following for this information:

- Software documentation that you received with your system
- Solaris™ Operating System documentation, available at <http://docs.sun.com>

---

## Typographic Conventions

Typeface*	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; onscreen computer output.	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. % You have mail.
<b>AaBbCc123</b>	What you type, when contrasted with onscreen computer output.	% <b>su</b> Password:
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be a superuser to do this. To delete a file, enter <code>rm filename</code> .

\* The settings on your web browser might differ from these settings.

---

## Related Documentation

For the most up-to-date information about the Sun Fire X4150 and X4450 servers, navigate to the Sun Fire server x64 document collection using the High-End Servers, Hardware product category link at <http://docs.sun.com/>.

Translated versions of some of these documents might also be available. Select a language from the drop-down list and browse or navigate to the Sun Fire server x64 document collection. Available translations for the Sun Fire servers include Simplified Chinese, Traditional Chinese, French, Japanese, and Korean.

English documentation is revised more frequently and might be more up-to-date than the translated documentation.

For all Sun hardware documentation, go to <http://docs.sun.com/>.

---

## Sun Documentation, Support, and Training

Sun Function	URL
Documentation	<a href="http://www.sun.com/documentation/">http://www.sun.com/documentation/</a>
Support	<a href="http://www.sun.com/support/">http://www.sun.com/support/</a>
Training	<a href="http://www.sun.com/training/">http://www.sun.com/training/</a>

---

## Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

---

# Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions, which you can submit at <http://www.sun.com/hwdocs/feedback>.

Please include the title and part number of this document with your feedback:

*Embedded Lights Out Manager Administration Guide for the Sun Fire X4150 and X4450 Servers, 820-1855*



# Embedded Lights Out Manager Overview

---

This chapter serves as an overview of the capabilities of the Sun Fire X4150 and X4450 server Embedded Lights Out Manager (ELOM), and contains the following sections:

- [“ELOM Features” on page 2](#)
- [“ELOM Common Tasks” on page 2](#)
- [“Server Default Settings” on page 3](#)
- [“About the Preconfigured Administrator Account” on page 3](#)
- [“About the Indicator and Fault LEDs” on page 4](#)

---

# ELOM Features

The ELOM provides a dedicated system of hardware and supporting software that enables you to manage your server independent of an operating system, and in low-power situations. ELOM is composed of four components:

- Web GUI (requires JavaR v5 or later)
- Command-line Interface (accessed via serial or ethernet using ssh)
- IPMI v2
- SNMP v3

You can access the ELOM using a web browser, secure shell (SSH), or via the Sun Fire server's serial port. Your server's default network setting is configured as DHCP for easy access via a web browser or SSH, and the ELOM output is directed by default to the serial port.

---

# ELOM Common Tasks

The following table shows common tasks and the management interfaces used to perform each task.

**TABLE 1-1** ELOM Common Tasks

Task	IPMI	Web GUI	CLI	SNMP
Redirect the system graphical console to a remote client web browser.	-	Yes	-	-
Connect a remote diskette drive to the system as a virtual diskette drive.	-	Yes	-	-
Connect a remote CD-ROM drive to the system as a virtual CD-ROM drive.	-	Yes	-	-
Monitor system fans, temperatures, and voltages remotely.	Yes	Yes	Yes	Yes
Monitor system BIOS messages remotely.	Yes	Yes	Yes	-
Monitor system operating system messages remotely.	Yes	Yes	Yes	-
Interrogate system components for their IDs and serial numbers.	Yes	-	Yes	Yes
Redirect the system serial console to a remote client.	Yes	-	Yes	-
Monitor system status (health check) remotely.	Yes	Yes	Yes	Yes

**TABLE 1-1** ELOM Common Tasks (*Continued*)

Task	IPMI	Web GUI	CLI	SNMP
Interrogate system network interface cards remotely for MAC addresses.	Yes	Yes	Yes	-
Manage user accounts remotely.	Yes	Yes	Yes	-
Manage system power status remotely (power on, power off, power reset).	Yes	Yes	Yes	-
Monitor and manage environmental settings for key system components (CPUs, motherboards, fans).	Yes	Yes	Yes	Monitor only

---

## Server Default Settings

Sun has configured the SP controller and SP firmware on your server to use the most common default settings. It is unlikely that you will need to change any of these defaults.

**TABLE 1-2** SP Controller and Firmware Default Settings

System Component	Default Status	Action Required
Service processor card	Preinstalled	None
Service processor firmware	Preinstalled	None
IPMI interface	Enabled	None
Web GUI	Enabled	None
Command-line interface (CLI)	Enabled	None
SNMP interface	Enabled	None

---

## About the Preconfigured Administrator Account

The ELOM is shipped with one preconfigured administrator account:

User name: **root**  
 Password: **changeme**

The preconfigured administrator account, root, is the default account. It cannot be deleted or modified. You can only change the password for the root account. This default account contains administrator privileges (read and write access) to all service processor features and commands. For security reasons you should change the root password and create an alternate user account that also has administrator privileges. To change a user password or to create a new user, see [Chapter 4](#).

If you've changed the root password, but have not created an alternate account, and the new root password is lost or forgotten, you will have to reset the SP to return the ELOM to its default settings. For information about how to do this, see "[Resetting the Service Processor](#)" on page 54.

---

## About the Indicator and Fault LEDs

The LEDs on the front and rear panel of your server allow you to manage the server at a rudimentary level. The LEDs are helpful for indicating when a problem has occurred, and you can use these LEDs in combination with the internal fault indicator LEDs and buttons to troubleshoot and repair component failure issues. However, using the ELOM it is possible not only to troubleshoot component failure issues, but also to configure, manage, and maintain the server remotely and to implement an effective preventative maintenance program. Using the ELOM as part of a regular maintenance regimen allows you to take a proactive approach to server repair. This can improve system performance and minimize downtime.

For information about the Indicator and Fault LEDs, see the server service manual.

For information about managing, maintaining, and configuring your server, see [Chapter 4](#) of this guide.

## Connecting to the ELOM

---

This chapter details the ways to connect to and communicate with your Sun Fire server. It contains the following sections:

- [“About Connection Tasks” on page 6](#)
- [“Connecting Using a Serial Connection” on page 6](#)
- [“Connecting Using Ethernet” on page 7](#)

---

**Note** – You must install your server and configure the ELOM before communicating with the server. Information about installing the server and configuring the ELOM is available in the server installation guide.

---

---

# About Connection Tasks

You have two methods to connect to the ELOM in your server:

- Serial/Local
- Ethernet/Remote

Both methods require making physical cable connections to the server and logging in to the ELOM; refer to [TABLE 2-1](#).

**TABLE 2-1** Methods of Connecting to the ELOM

Connection Method	Supported Interface	Required Cable	Comments/Description
Serial, direct	CLI only	RJ-45 serial (supplied)	Connect directly to the serial management port the on server with a terminal or laptop running terminal emulation software.
Ethernet	CLI and Web browser	Ethernet LAN	You must know the ELOM's Ethernet address. <b>Note: This is the only method that supports web browser access.</b>

---

**Note** – The ELOM supports a maximum of 10 active sessions, including serial, SSH, and web browser sessions.

---

---

## Connecting Using a Serial Connection

You access the ELOM CLI by connecting a terminal or a PC running terminal emulation software to the RJ-45 serial port on the server using the supplied cable.

### ▼ To Connect Using a Serial Connection

1. Verify that your terminal, laptop, or terminal server is operational.
2. Configure the terminal device or terminal emulation software to use the following settings:
  - 8,N,1: eight data bits, no parity, one stop bit.

- 9600 baud (default, can be set to any standard rate up to 57600).
  - Disable software flow control (XON/XOFF).
3. **Connect a serial cable to the RJ-45 connection on the back of the server.**
  4. **Connect the other end to the terminal or laptop.**
  5. **Press Enter on the terminal device.**

This action establishes the connection between the terminal device and the ELOM. When the server has booted, the ELOM displays its login prompt:

```
SUNSP##### login:
```

The first string in the prompt is the default host name. It consists of the prefix SUNSP and the ELOM's MAC address. The MAC address for each ELOM is unique.

6. **Log in to the CLI.**

Accounts created using the web browser are available for the CLI. If this is the first login, you will need to use the preconfigured default account:

User name: **root**.

Password: **changeme**.

Once you have successfully logged in, the default command prompt appears:

```
->
```

You can now run CLI commands ([Chapter 7](#) describes how to use the CLI).

To log out of the CLI

- **Enter the following command:**

```
-> exit
```

---

## Connecting Using Ethernet

Ethernet connectivity provides full access to both the ELOM command-line interface (CLI) and the web GUI. Both connection options allow you to manage, maintain, and configure the server remotely. This section contains the following two connection procedures:

- Connecting to the CLI. See [Connecting to the CLI](#).
- Connecting to the web GUI. See [Connecting to the Web GUI](#).

---

**Note** – You will need the IP address of your ELOM, which you obtained during the setup and installation of your server (see the server installation guide).

---

## Connecting to the CLI

Be sure that you have connected a LAN to the NET MGT 0 port on the server, and that you have an SSH client installed on your remote system.

### ▼ To Connect to the CLI

1. If necessary start your SSH client.

2. To log in to the ELOM, enter the following command:

```
$ ssh username@ipaddress
```

*username* The user ID and *ipaddress* is the IP address of the ELOM. Accounts created using the web browser are available for the CLI. If this is the first login, you will need to use the preconfigured default account. For example,

```
$ ssh root@ipaddress
```

3. When prompted, enter the password for the username used in Step 2.

The password for root is **changeme**.

The CLI command prompt appears:

```
->
```

For information about managing the server using the CLI, see [Chapter 7](#). For information about the default account, see [“About the Preconfigured Administrator Account”](#) on page 3.

To Log Out of the CLI:

● Enter the following command:

```
-> exit
```



## Connecting to the Web GUI

Be sure that you have connected a LAN to the NET MGT 0 port on the server.

### ▼ To Connect to the Web GUI

1. **Type the IP address of the ELOM into your web browser.**

The login screen appears.

2. **Type a user name and password.**

Accounts created using the CLI are available for the web GUI. If this is the first login, you will need to use the preconfigured default account:

- Default user name: **root**
- Default password: **changeme**

For more information about the default account, see [“About the Preconfigured Administrator Account”](#) on page 3.

3. **Click Log In.**

The web GUI appears. [Chapter 3](#) shows how to use the interface.

To Log Out of the web GUI:

- **Click the Log Out button.**

The Log Out button is located in the upper right corner of the screen.



## Monitoring the Server System Using the Web GUI

---

This chapter provides information about how to use the web GUI and the Sun Fire X4150 server software to monitor your server.

It includes the following sections:

- [“Using the Web GUI” on page 11](#)
- [“Accessing the ELOM Using a Web Browser” on page 13](#)
- [“Viewing System and Component Information” on page 16](#)
- [“Monitoring the System Sensors” on page 19](#)
- [“Viewing and Managing the Event Log” on page 23](#)

---

**Note** – You can monitor the rudimentary state of the server using the LED fault light. A solidly lit amber LED indicates critical error. Further details about the fault light can be found in your *Service Manual*. For information about controlling the state of the fault LEDs see [“To Manage the State of the System Locator Indicator LED” on page 52](#).

---

---

## Using the Web GUI

The web-based graphical user interface (GUI) allows you to use a standard web browser to monitor and manage local and remote systems.

You can redirect the server’s console to a remote workstation or laptop system. This requires configuring the remote system’s keyboard and mouse to act as the server’s keyboard and mouse. You can configure the diskette drive or CD-ROM drive on the

remote system as if it were connected to the Sun server. You can also redirect diskette images (.img files) and CD-ROM images (.iso files) for remote access. Remote configuration issues are covered in [Chapter 5](#).

## Browser and Software Requirements

The web GUI has been tested successfully with recently released Mozilla™ Firefox and Internet Explorer web browsers, and might be compatible with other web browsers.

The ELOM product is preinstalled on the Sun server. However, you need Java™ software on the client to perform redirection as described in [Chapter 5](#).

## Users and Privileges

After you log in to the web GUI, you can perform basic software tasks, Intelligent Platform Management Interface (IPMI) tasks, and system monitoring.

ELOM user accounts define what you can do by roles:

- **Administrator** – Enables read/write access to all ELOM features, functions, and commands.
- **Operator, User, and Callback** – Enable limited access to ELOM features, functions, and commands. For example, users with these permissions cannot change their assigned roles or privileges.

For more information about users, including how to manage user accounts using the web GUI, see [Chapter 4](#).

## Web GUI Tasks

Some of the common tasks you can perform using the web GUI include:

Configuring connection methods:

- Redirect the system's console to a remote client browser.
- Connect a remote diskette drive or diskette image to the system as a virtual diskette drive.
- Connect a remote CD-ROM drive or CD-ROM image to the system as a local or virtual CD-ROM drive.

Monitoring and managing system status:

- Monitor the status of system fans, temperatures, and voltages remotely.
- Monitor BIOS power-on self-test (POST) progress log entries remotely.
- View, save, and clear system event logs.
- Examine component information, including CPUs, DIMMs, voltages, and fans.
- Power on, power off, power cycle, reset the system remotely, reboot and enter the system BIOS, reboot and enter diagnostics (Pc-Check), and send NMI.

Managing and modifying system variables:

- Manage user accounts locally and remotely.
- Configure settings.
- Update BIOS firmware.

---

## Accessing the ELOM Using a Web Browser

The ELOM boots automatically when a Sun server is cabled appropriately and plugged in to an AC power supply. This usually occurs within one minute. However, if the management Ethernet is not connected, or if the ELOM's Dynamic Host Configuration Protocol (DHCP) process fails due to the absence of a DHCP server on the management network, the ELOM might take a few minutes longer to boot.

---

**Note** – Disabling the use of the browser proxy server (if one is used) for access to the management network might speed the browser response time.

---

### ▼ To Access the ELOM Using a Web Browser

1. **To log in to the web GUI, type the IP address of the ELOM in your web browser.**

The login screen appears.

2. **In the login screen that appears, type the default user name and password.**

Username: **root**

Password: **changeme**

### 3. Click Log In.

The web GUI appears.

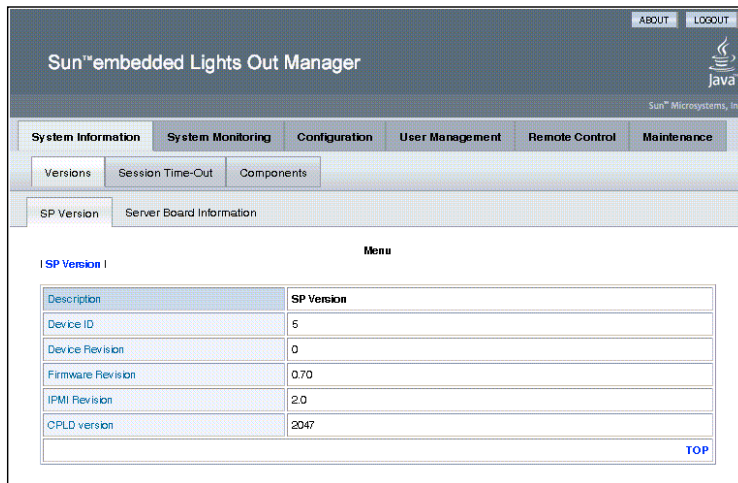
To log out of the web GUI:

- Click the **Logout** button in the upper right corner of the screen.

## Viewing the System From the Web Browser

The system is equipped with a number of sensors that measure voltages, temperatures, fan speed, and so on. The System Information tab shows the current system status and provides access to the Version, Session Time-Out, and the Components submenu tabs (see [FIGURE 3-1](#)).

**FIGURE 3-1** ELOM System Information Screen



[TABLE 3-1](#) lists the ELOM main menu and submenu tabs and points to relevant sections in this manual.

**TABLE 3-1** ELOM Tab Detail Choices

Main Tab	Submenu Tab	Where to Find Details
<b>System Information</b>		<a href="#">“Viewing System and Component Information” on page 16.</a>
	Server Board Information	<a href="#">“Viewing SP Version Information” on page 16.</a>
	SP Version	<a href="#">“Viewing SP Version Information” on page 16.</a>
	Session Time-Out	<a href="#">“Managing Session Timeout” on page 57</a>

**TABLE 3-1** ELOM Tab Detail Choices (*Continued*)

<b>Main Tab</b>	<b>Submenu Tab</b>	<b>Where to Find Details</b>
<b>System Monitoring</b>	Components	<a href="#">“Viewing Component Information” on page 17</a>
	Sensor Reading	<a href="#">“Monitoring the System Sensors” on page 19</a>
	Event Logs	<a href="#">“Viewing and Managing the Event Log” on page 23</a>
	Locator Indicator Fault LED	<a href="#">“Managing the State of the System Locator Indicator LED” on page 52</a>
<b>Configuration</b>	Network	<a href="#">“Configuring Network Settings” on page 30</a>
	E-mail Notification	<a href="#">“To Configure E-mail Notification” on page 30</a>
	Platform Event Filter	<a href="#">“Configuring Platform Event Filters” on page 30</a>
	Clock Settings	<a href="#">“Setting the Time” on page 58</a>
	System Management Access	<a href="#">“Configuring System Management Access” on page 33</a>
		<a href="#">“Recovering from a Corrupt SP” on page 59</a>
<b>User Management</b>	User Account	<a href="#">“Managing Users and Accounts” on page 46</a>
	ADS Configuration	<a href="#">“Configuring Active Directory Service” on page 37</a>
		<a href="#">“Starting the Remote Console Application” on page 64</a>
<b>Remote Control</b>	Redirection	<a href="#">“Redirecting Keyboard, Video, Mouse, or Storage Devices” on page 66</a>
	Remote Power Control	<a href="#">“Setting Power Control” on page 54</a>
	Hotkey Setup	<a href="#">“To Set Parameters for the Remote Console” on page 65</a>
<b>Maintenance</b>	Firmware Upgrade	<a href="#">“Updating the Firmware” on page 55</a>
	Reset SP	<a href="#">“Resetting the Service Processor” on page 54</a>

The following section describes how to monitor the server using the web browser and the Embedded Lights Out Manager software.

---

# Viewing System and Component Information

The System Information tab provides information about system components, such as the service processor (SP), the server board, the CPU, and the memory. Details are found in the Versions and Components submenu tabs.

## ▼ To View System Information

- **On the main menu, click the System Information tab.**

The System Information submenu appears, allowing you to view the Versions, Session Time-Out, and Components tabs.

## Viewing SP Version Information

### ▼ To View SP Version Information

- **From the Versions submenu, select the SP Version tab.**

The SP Version screen appears, displaying information about the server board installed in the system. It presents the information in a tabular format. For example, [TABLE 3-2](#) shows a sample of the SP information as it is displayed in the SP Version screen:

**TABLE 3-2** Sample SP Information

Description	SP Version
Device ID	5
Device Revision	0
Firmware Revision	1.0
IPMI Revision	2.0
CPLD version	3041



# Viewing Server Board Information

## ▼ To View Server Board Information

- From the Versions submenu, select the Server Board Information tab.

The Server Board Information screen appears, displaying information such as the BIOS version and the serial number. It presents the information in a tabular format. TABLE 3-3 show a sample of the server board information as it is displayed:

**TABLE 3-3** Sample Server Board Information

Description	Server Board Information
BIOS version:	1ADQWOO9
Manufacture Date:	Wed Dec 31 23:59:59 1969
Product:	Sun Fire X4150
Serial Number:	12345678901234

# Viewing Component Information

## ▼ To View CPU Information

The CPU menu selection provides information about the processor.

- From the System Information menu, click the Components submenu tab, then select CPU.

The CPU information screen appears. The CPU information is presented in a tabular format. A separate table of information is available for each of the server's CPUs, whether a CPU is installed or not. TABLE 3-4 shows a sample of the CPU information for CPU0:

**TABLE 3-4** Sample CPU Information

CPU:	0
Status:	Enable
Socket:	CPU0

**TABLE 3-4** Sample CPU Information (Continued)

Manufacturer:	Intel
Model:	
Frequency:	

## Viewing Memory Information

### ▼ To View Memory Information

- From the System menu, select Components, and then select Memory. The Memory screen appears. It displays information about total memory installed in your server; see [TABLE 3-5](#).

**TABLE 3-5** Sample Memory Information

Description	Memory Size Information
Total Memory Size:	12288 MB

The Memory screen also displays information about each DIMM installed in your system, presenting it in a tabular format that includes such information as the memory module number, the status, and module size; see [TABLE 3-6](#) for a sample of the memory information for DIMM\_A0.

**TABLE 3-6** Sample Memory for DIMM\_A0

Description	Memory Information
Memory Module:	1
Status:	Ok
Socket:	DIMM_A0
Module Size:	1024MB
Type:	FBDIMM
Frequency:	667MHz

---

# Monitoring the System Sensors

Sensors placed throughout the system provide information about the state of critical server components. The sensors read temperature and voltage and report on operational status. Using the System Monitoring submenu screens you can view the these sensors and monitor the health of your server's critical components. For example, you can check the temperature of each CPU or DIMM and read the actual DC voltage of each of the system's power supply lines. The System Monitoring submenu screens also allows you to view and manage the system log, the Locator Indicator LED, and the Fault LED. For information about the Locator Indicator LED and the Fault LED, see [“Managing the State of the System Locator Indicator LED” on page 52](#).

## ▼ To Monitor the System Sensors

- **On the main menu, click System Monitoring.**

The System Monitoring submenu appears, allowing you to view the Sensor Reading, Event Logs, Locator Indicator, and Fault LED tabs.

## Reading Sensors

### ▼ To Read Sensors

- **From the System Monitoring tab, click the Sensor Reading Tab.**

The Sensor Reading tab allows you to select the Summary, Temperature, Voltage, and Chassis Status tabs.

# Viewing a Sensor Summary

## ▼ To View a Sensor Summary

- From the **Sensor Reading tab**, select the **Summary tab**.

The Summary screen appears. It provides an overview of the status of the system sensors. The screen provides the status of the Fault LED, the power, the temperature of all critical components, and each of the monitored voltage lines. For example, [TABLE 3-7](#) shows the top portion of the summary table summarizing the status of the Fault LED and the system power.

**TABLE 3-7** Top Portion of the Summary Table Showing the Fault LED and Power Status.

<b>Fault LED Status</b>	On
<b>Power Status</b>	Off

[TABLE 3-8](#) shows a detail of the Summary table that summarizes the status of each of the system fans.

**TABLE 3-8** Detail of the Summary Table Showing the Status of the System Fans.

	Fanbd1/FM1	:ok
	Fanbd1/FM0	:ok
	Fanbd1/FM3	:ok
	Fanbd1/FM2	:ok
	Fanbd1/FM5	:ok
	Fanbd1/FM4	:ok
<b>Fan Status</b>	Fanbd0/FM1	:ok
	Fanbd0/FM0	:ok
	Fanbd0/FM3	:ok
	Fanbd0/FM2	:ok
	Fanbd0/FM5	:ok
	Fanbd0/FM4	:ok
	Fanbd0/FM7	:ok
	Fanbd0/FM8	:ok

TABLE 3-9 shows a detail of the Summary table that summarizes the status of the temperature sensors.

**TABLE 3-9** Detail of the Summary Table Showing the Status of the Temperature Sensors.

	CPU 0 Temp	:too high
<b>Temperature Status</b>	CPU 1 Temp	:ok
	Ambient Temp0	:ok

TABLE 3-10 shows a detail of the Summary table that summarizes the status of the DC power supply lines.

**TABLE 3-10** Detail of the Summary Table Showing the Status of the Power Supply Lines.

	Vcc 12V	:ok
	Vtt 1.2V	:ok
	MCH 1.5V	:ok
	Vcc 3.3V	:ok
<b>Voltage Status</b>	Vcc 5V	:ok
	NIC Vtt 1.2V	:ok
	Vcc 3.3V STB	:ok
	Vcc 2.5V STB	:ok
	Vcc 1.8V	:ok

TABLE 3-11 shows a detail of the Summary table that summarized the status of the systems power supplies.

**TABLE 3-11** Detail of the Summary Table Showing the Status of the Power Supplies.

	PS0 Under Volt	:ok
	PS1 Under Volt	:ok
<b>Power Status</b>	PS0 OC Fault	:ok
	PS1 OC Fault	:ok
	Power Supply 0	:ok
	Power Supply 1	:ok

# Monitoring Fans

## ▼ To Monitor Fans

- **From the Sensor Reading tab, select the Fan tab.**

The Fan screen appears, displaying the critical thresholds, the actual sensor reading, and the status for each of the systems fans. The readings are in RPM. The information is presented in tabular format. [TABLE 3-12](#) shows sample information on the Fan screen. The sample is for the fan labeled Fanbd1/FM1.

**TABLE 3-12** Sample of Fan Information for Fanbd1/FM1

Description	Fanbd1/FM1
Lower critical threshold is readable:	1463
Upper critical threshold is readable:	14936
Sensor Reading:	13629
Status:	ok

# Monitoring Temperatures

## ▼ To Monitor Temperatures

- **From the Sensor Reading tab, select the Temperature tab.**

The Temperature screen appears, displaying the ambient chassis and CPU temperatures. The temperatures are displayed in degrees celsius. The Sensor Reading screen shows the current temperature reading. [TABLE 3-13](#) shows sample Temperature information for CPU 0. A separate table is presented for each CPU and each ambient sensor.

**TABLE 3-13** Sample Temperature Monitor Readings

Description	CPU 0 Temp
Upper noncritical threshold is readable:	93.0
Upper critical threshold is readable:	95.0
Sensor Reading:	54.0
Status:	ok

A similar panel is repeated for each monitored entity.

## Monitoring Voltages

### ▼ To Monitor Voltage

- **From the Sensor Reading tab, click the Voltage tab.**

The Voltage screen appears. The Voltage screen displays the critical and noncritical thresholds, the actual sensor reading, and the status for the nine monitored DC system voltage lines. The Sensor Reading value represents the actual voltage reading for that sensor. [TABLE 3-14](#) shows a sample from the Voltage screen. The sample is for the Vcc 12V line:

**TABLE 3-14** Sample of the Voltage Monitor Screen

Description	Vcc 12V
Lower noncritical threshold is readable:	11.999
Lower critical threshold is readable:	10.821
Upper noncritical threshold is readable:	12.837
Upper critical threshold is readable:	13.215
Sensor Reading:	12.081
Status:	ok

## Viewing and Managing the Event Log

The Event Logs screen allows you to view and manage the system event log (SEL). The SEL is a record of event occurrences. To record events in the SEL, you must have previously determined which events require logging. See [“Configuring Platform Event Filters”](#) on page 30.

## ▼ To Display the Event Log

- From the **System Monitoring** tab on the main menu, click the **Event Logs** submenu tab.

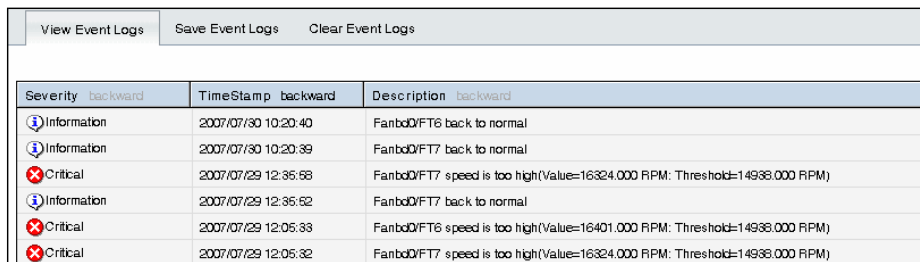
The Event Logs screen appears. The View Event Logs, Save Event Logs, and Clear Event Logs submenus become available.

## ▼ To View the Event Logs

- From the **Event Logs** tab, select **View Event Logs**.

The system event log appears. Each entry in the log represents an action that occurred on the system. The information is presented in a tabular format. The system lists each action, rates the action's severity, provides a time stamp, and describes the event. The severity field includes icons for both Information and Critical ratings. [FIGURE 3-2](#) shows an excerpt from the View Event Logs screen.

**FIGURE 3-2** An Excerpt of the View Event Logs Screen



The screenshot shows a web interface with three tabs: "View Event Logs", "Save Event Logs", and "Clear Event Logs". Below the tabs is a table with three columns: "Severity", "TimeStamp", and "Description". Each cell in the table has a small "backward" link. The table contains six rows of event data.

Severity	TimeStamp	Description
Information	2007/07/30 10:20:40	Fanbd0FT6 back to normal
Information	2007/07/30 10:20:39	Fanbd0FT7 back to normal
Critical	2007/07/29 12:35:58	Fanbd0FT7 speed is too high(Value=16324.000 RPM: Threshold=14938.000 RPM)
Information	2007/07/29 12:35:52	Fanbd0FT7 back to normal
Critical	2007/07/29 12:05:33	Fanbd0FT6 speed is too high(Value=16401.000 RPM: Threshold=14938.000 RPM)
Critical	2007/07/29 12:05:32	Fanbd0FT7 speed is too high(Value=16324.000 RPM: Threshold=14938.000 RPM)

## ▼ To Save the Event Log

You might want to save the event log for administrative or diagnostic purposes.

1. From the **Event Logs** tab, click the **Save Event Logs** tab.  
The Save Event Log screen appears.
2. Click the **Save Event Log** button to prompt the browser to ask you where to save a copy of the event log.
3. Select the location, name the file (if necessary), and click save.



## ▼ To Clear the Event Log

The Event Log might need to be cleared to signify a fresh procedure, or identify system performance under load.

1. **From the Event Logs tab, click Clear Event Log.**
2. **Click the Clear Event Log button to start a fresh event log.**



# Configuring, Managing and Maintaining the Server Using the Web GUI

---

This chapter provides information about how to use a web browser and the Sun Fire X4150 server software to manage your server. The sections include:

- [“Configuring the System” on page 28](#)
- [“Managing and Maintaining the System” on page 46](#)

This chapter addresses your local system. For information about how to redirect your commands to a remote system, see [Chapter 5](#).

# Configuring the System

The Configuration submenu tabs enable you to configure the network operation and other important functions of the server. These functions are described in the following sections:

- “Configuring Network Settings” on page 30
- “Configuring E-mail Notification” on page 30
- “Configuring Platform Event Filters” on page 30
- “Configuring System Management Access” on page 33
- “Configuring SNMP” on page 34
- “Configuring Active Directory Service” on page 37

## ▼ To Configure the System

- From the main menu, click the Configuration tab.

The Configuration tabs appear (see [FIGURE 4-1](#)). You are now able to access the Network, E-mail Notification, Platform Event Filter, Clock Settings, and System Management Access screens.

**FIGURE 4-1** The Configuration Screen

Screenshot of the Sun embedded Lights Out Manager Configuration screen. The interface shows a navigation menu with tabs for System Information, System Monitoring, Configuration, User Management, Remote Control, and Maintenance. Under the Configuration tab, there are sub-tabs for Network, E-mail Notification, Platform Event Filter, Clock Settings, and System Management Access. The Network configuration section is active, showing fields for IP (129.129.53.161), Net Mask (255.255.255.0), Gateway (129.129.53.248), and Mac Address (00:18:24:4D:F3:0C). The DNS server field is set to 0.0.0.0. There are Submit and Reset buttons for both sections.



# Configuring Network Settings

## ▼ To Configure the Network Settings

- **From the Configure submenu, click the Network tab.**

The Network configuration screen appears (see [FIGURE 4-1](#)). Use this screen to enable or disable DHCP and set DNS. If you disable DHCP, you must manually supply the IP address, the netmask, and the gateway.

# Configuring E-mail Notification

The E-mail Notification screen enables you to configure the e-mail recipients for any ELOM generated events. The system allows you to designate up to 10 recipients. e-mail notification is used in conjunction with Platform Event Filters (PEF). PEFs are event traps that allow you to associate an action, or a set of actions, with the occurrence of a specific event. One such action is mail notification. The Send Mail action is enabled in the Platform Event Filter screen and configured in the E-mail Notification screen.

## ▼ To Configure E-mail Notification

- **From the Configuration submenu, click the E-mail Notification tab.**

The Enable E-mail Notification screen appears. You must supply the name of the SMTP server and the sender and designate the receiver e-mail addresses.

# Configuring Platform Event Filters

The Platform Event Filter option allows you to configure actions for system generated events. A system generated event is an alert that occurs when a threshold for a system sensor is reached. For example, the system uses the sensors to monitor various critical components. The components are most effective when operating within a specific range. The limits of that range are defined as thresholds. All components, such as fans, have an upper and lower critical threshold (see [“To Monitor Fans” on page 22](#)). When either critical threshold is crossed the system generates an alert. For example a fan failure would cause an alert for the lower critical threshold. You can configure an event filter to trigger off the alert and perform one or several actions. These actions include:

- Performing one of three power actions
- Performing an NMI diagnostic interrupt
- Sending alert to the SEL
- Sending mail

An event is configured in two parts: the event (or alert) and the response or action to be taken when that event occurs. You can configure up to six filters. You begin by determining what sort of event you want to trap.

## ▼ To Configure a Platform Event Filter

### 1. From the Configuration submenu click Platform Event Filter tab.

The Platform Event Filter screen appears (see [FIGURE 4-2](#)). The PEF screen is divided into five sections:

- Platform Event Filter
- Trap Receiver Destination Address
- PEF Action Global Control
- Event Filter Configuration
- Event Action Configuration

**FIGURE 4-2** The Platform Event Filter Screen

Platform Event Filter	
PEF Global Control :	<input checked="" type="radio"/> Enable PEF <input type="radio"/> Disable PEF
Community :	public
Trap Receiver Destination Address	
IP Address (Ex: 192.168.1.33)	
192.168.1.33	
PEF Action Global Control :	<input checked="" type="checkbox"/> Enable Power Off Action <input checked="" type="checkbox"/> Enable Power Cycle Action <input checked="" type="checkbox"/> Enable Power Reset Action <input checked="" type="checkbox"/> Enable Diagnostic Interrupt Action <input checked="" type="checkbox"/> Enable Send Alert Action <input checked="" type="checkbox"/> Enable Send Mail Action
Event Filter Configuration :	Event Action Configuration :
04 h - Fan	<input checked="" type="checkbox"/> Power Control <span>Power Cycle</span>
	<input type="checkbox"/> Diagnostic Interrupt(NMI)
	<input checked="" type="checkbox"/> Send Alert
	<input checked="" type="checkbox"/> Send Mail

- In the The Platform Event Filter section click the Enable PEF radio button.**  
To configure/create a filter, you must first enable PEF.
- Type the address of the trap receiver in the Trap Receiver Destination Address section.**
- Enable all actions that you would like to be available for your filters by selecting the appropriate check box in the PEF Action Global Control section.**  
The actions are:
  - Enable Power Off Action
  - Enable Power Cycle Action
  - Enable Power Reset Action
  - Enable Diagnostic Interrupt Action
  - Enable Send Alert Action
  - Enable Send Mail Action
- Select the sensor group for which you would like to filter alerts from the drop-down list in the Event Filter Configuration.**  
The options are:
  - ffh - All sensors



- 01h - Temperature
  - 02h - Voltage
  - 04h - Fan
  - 07h - Processor
  - 0Ch - Memory
6. **Select the action for the alerts by selecting the check boxes in the Event Action Configuration section.**
- If you are selecting a power control action, select the action from the drop-down list after selecting the Power Control check box.
- In the example shown in [FIGURE 4-2](#), the system is configured to enable all actions. A filter has been created to filter fan alerts. When an alert occurs, the system will cycle power, send an alert to the SEL, and send mail to the addresses listed in the E-mail Notification screen (see [“Configuring E-mail Notification” on page 30](#)).
7. **Click Submit to create the filter.**
- You can configure up to six filters.

## Configuring System Management Access

The System Management Access submenus allow you to set up the SSL certificate and SNMP. The SSL configuration is used for creating certificates required in the Certificate Signing Request (CSR). The certificate is required to enable encryption for when you use HTTPS for secure web browser access. HTTPS requires a digitally signed certificate to be installed at the applicant’s site. The SNMP screen allows the configuration of SNMP settings, communities, and users.

### ▼ To access the System Management Access Submenus

- **From the Configuration submenu click the System Management Access tab.**  
The System Management Access submenu tabs appear.

# Configuring the SSL Certificate

## ▼ To Configure the SSL Certificate

1. From the **System Management Access** submenu, click the **SSL Certificate** tab.  
The SSL Certificate screen appears.
2. Select either **Certificate** or **CSR** from the drop-down list.
3. Fill in the required fields in the **SSL Configuration** section.
4. Click **Generate** to create the certificate.
5. Click **Upload** to bring the certificate into view.

---

**Note** – If no certificate has yet been assigned, follow the directions below to generate a new CSR.

---

6. Follow the onscreen directions, and fill in the fields using the example as a guide.

The example in [TABLE 4-1](#) represents the kind of information required.

**TABLE 4-1** Example of Required SSL Information

---

Common Name (CN):	<i>localhost.localdomain</i>
Organization Unit (OU):	<i>Your Name</i>
Organization (O):	<i>Your Company Name</i>
Country Code (C):	<i>U.S.A. (drop-down list of countries)</i>
Locality (L):	<i>Your Location</i>
State (S):	<i>Your State</i>
E-mail Address (E):	<i>youradmin@localhost.localdomain</i>

---

7. Click **Generate** to create a new CSR.

## Configuring SNMP

A series of screens allow you to set port, requests, and SNMP permission parameters for the system you are logged in to.

---

**Note** – The SNMP MIB file is located on the Tools and Drivers CD in the directory /SNMP/mib/.  

---

## ▼ To Configure SNMP

1. **From the System Management submenu, click the SNMP tab.**  
The SNMP screen appears.
2. **Select SNMP settings from the drop-down list, and then click Select.**  
The SNMP Settings screen appears.
3. **Select the Set Request check box to set one or more SNMP variables.**  
This check box acts as a global override for the user and community read/write permissions. For example, if you disable Set Requests, a member of the private community accessing your Sun server or stand-alone system via the SNMP interface cannot set sysContact despite having write permission.
4. **Select the check box beside the preferred version of SNMP protocols to override the delivered system default.**
5. **Click Submit to save the configuration, or click Reset to clear your entries.**

## ▼ To Add an SNMP Community

1. **In the SNMP screen, select SNMP Communities from the drop-down list and click Select.**  
The SNMP Communities screen appears.
2. **Select the radio button at the head of an unoccupied row.**
3. **Click Add to create a new community.**  
The Community Setting screen appears.
4. **Type the name of the new community in the Community field.**
5. **Select a permission from the Permission drop-down list.**
6. **Click Submit to add the community.**

## ▼ To Delete an SNMP Community

1. **In the SNMP screen, select SNMP Communities from the drop-down list, and then click Select.**

The SNMP Communities screen appears.

1. **Select the radio button at the head of the row for the community that you want to delete.**
2. **Click the Delete button to delete the community.**

The system does not prompt for a confirmation.

## ▼ To Modify an SNMP Community

1. **In the SNMP screen, select SNMP Communities from the drop-down list, and then click Select.**

The SNMP Communities screen appears.

2. **To change permissions for an existing community, select the radio button at the head of the row for the community you would like to modify.**
3. **Click Modify.**

The displayed screen allows you to change file permissions for that community.

4. **Select the permission from the Permission drop-down list.**

The permission is either read-only (ro) or read/write (rw).

5. **Click Submit to modify the community, or click Reset to clear your changes.**

## ▼ To Add an SNMP User

1. **In the SNMP screen, select SNMP User Settings from the drop-down list, and then click Select.**

The SNMP User Settings screen appears.

2. **Select the radio button at the head of an unoccupied row.**
3. **Click Add to create a new user.**

The User Setting screen appears.

4. **Fill in the open fields for the new user in the User Setting screen.**

The Authentication Protocol options are MD5 and SHA.

The Permission options are rw (read/write) and ro (read-only).

5. Click **Submit** to create the new user.

## ▼ To Delete an SNMP User

1. In the **SNMP** screen, select **SNMP User Settings** from the drop-down list, and then click **Select**.

The **SNMP User Settings** screen appears.

2. Select the radio button at the head of the row for the user that you want to delete.

3. Click the **Delete** button to delete the user.

The system does not prompt for a confirmation

## ▼ To Edit an SNMP User

1. In the **SNMP** screen, select **SNMP User Settings** from the drop-down list, and then click **Select**.

The **SNMP User Settings** screen appears. This screen allows you to add, delete, and edit users.

2. Select the radio button at the head of the row for the user setting that you would like to edit.

3. Click the **Edit** button in the same row.

The **User Settings** screen appears.

4. Edit the necessary user settings.

You cannot edit the user name. To change a user name, delete and re-create the user with a different name.

5. Click **Submit** to save your changes.

## Configuring Active Directory Service

The **ADS Configuration** screen enables you to browse and upload a certificate from **Active Directory Service (ADS)** for a **Microsoft Windows** environment. Administrators can simplify their tasks by monitoring multiple machines in one node using **ADS**.

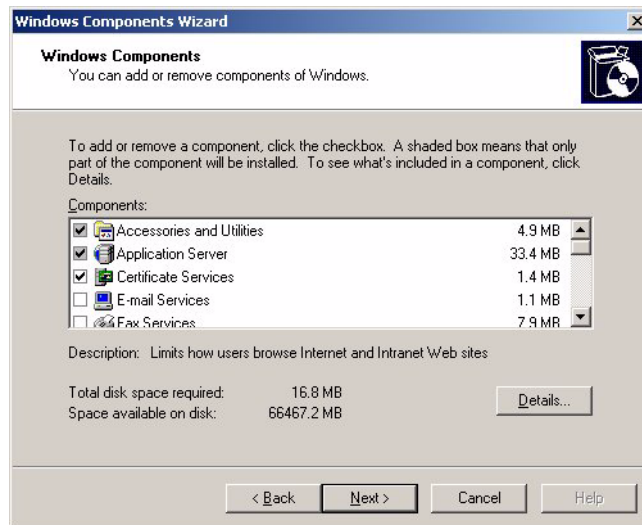
## ▼ To Configure Active Directory Service

1. Install Windows 2003 and make it the Domain Controller in an Active Directory environment.
2. Create and configure the DNS server.
3. Add a new user and set privilege level (administrator or user) in AD server.
4. Use Control Panel to access Add or Remove Programs, and click Add/Remove Windows Components.

The Windows Components Wizard appears.

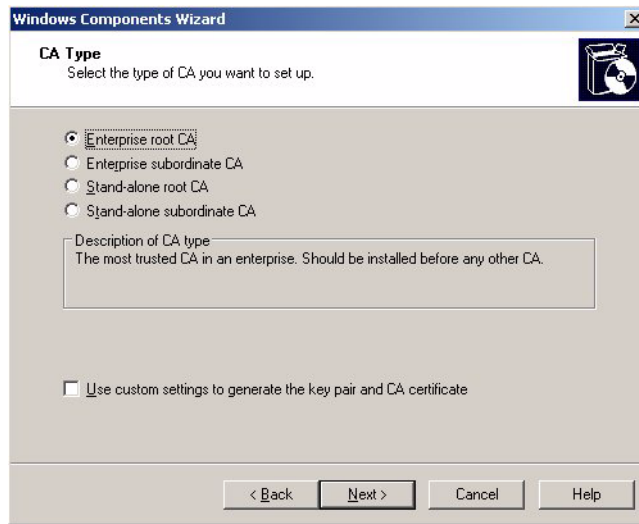
5. In the list of components, in the Windows Components screen, click the check box to enable Certificate Services (see [FIGURE 4-3](#)).

**FIGURE 4-3** Windows Components Screen



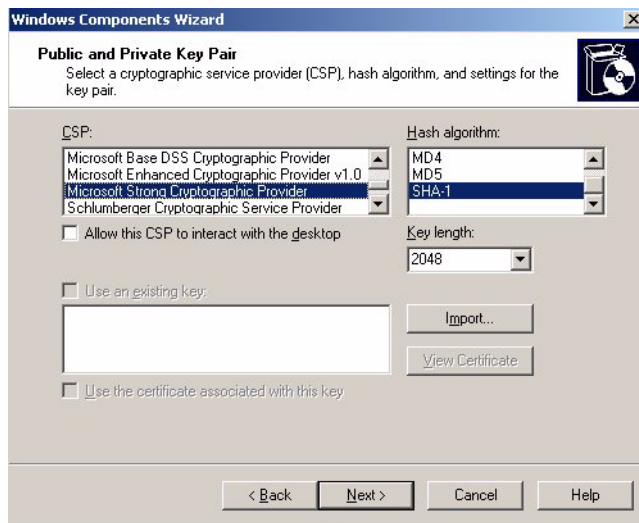
6. Click Next to begin the Create CA Root Domain Certificate process.  
This will require IIS to be installed also.
7. In the CA Type screen of the Windows Components Wizard, select the type of CA you want to set up (see [FIGURE 4-4](#)).

**FIGURE 4-4** CA Type Windows Components Wizard Screen



8. In the Public and Private Key Pair screen, select a cryptographic service provider (CSP), a hash algorithm, and settings for the key pair (see [FIGURE 4-5](#)).

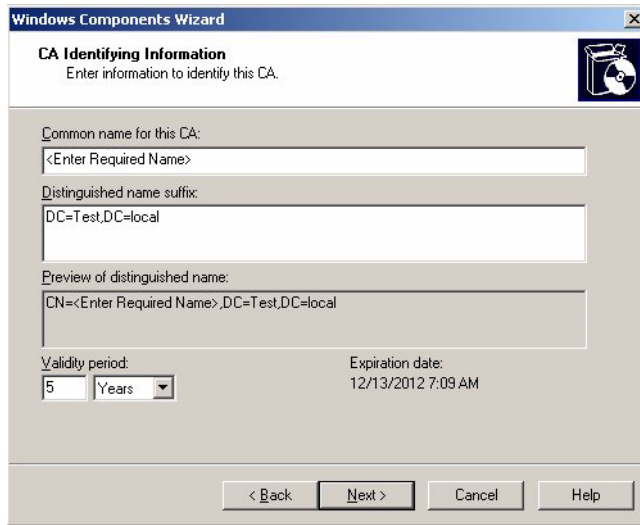
**FIGURE 4-5** Public and Private Key Pair Windows Components Wizard Screen



9. Click Next.

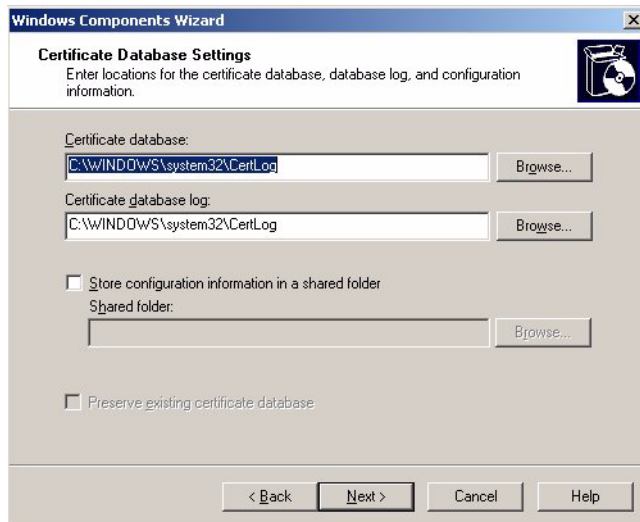
10. In the CA Identifying Information screen, enter the necessary information to identify this CA (FIGURE 4-6), and click Next.

FIGURE 4-6 CA Identifying Information Windows Components Wizard Screen



11. In the Certificate Database Settings screen, enter the locations for the certificate database, database log, and configuration information (see FIGURE 4-7).

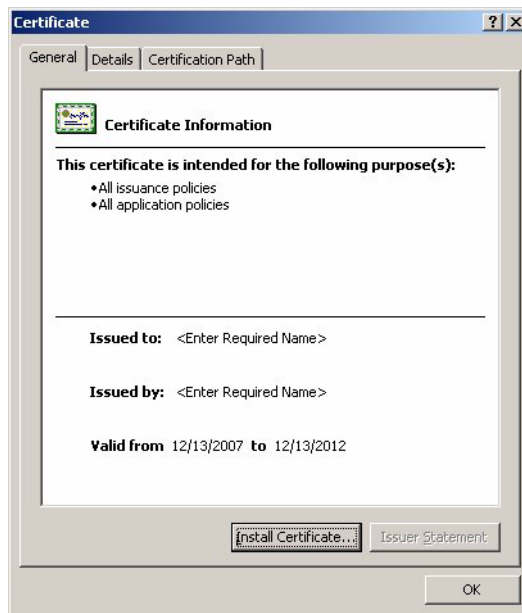
FIGURE 4-7 Certificate Database Settings Windows Components Wizard Screen





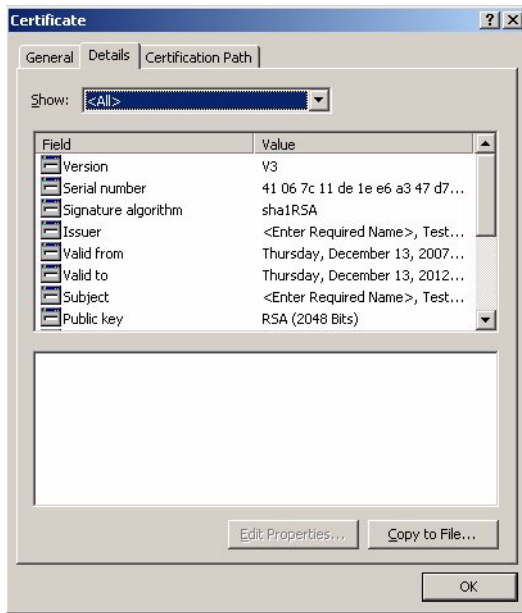
12. To finish the Create CA Root Domain Certificate process, click Next.
13. To export the AD certificate, locate the net certificate for your Domain.  
You will see a certificate called, C:/xxx.crt.
14. Double-click the Certificate.  
The certificate screen appears.

**FIGURE 4-8** The Certificate Information Screen



15. Click the Details tab.  
The Certificate Details screen appears (see [FIGURE 4-9](#)).

**FIGURE 4-9** The Certificate Details Screen



**16. Click the Copy to File... button.**

The Certificate Export Wizard screen appears (see [FIGURE 4-10](#)).

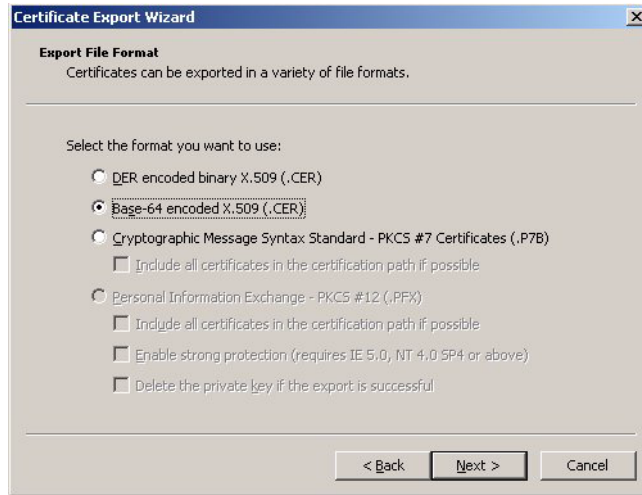
**FIGURE 4-10** The Certificate Export Wizard Screen



**17. Click Next.**

The Export File Format screen appears.

**FIGURE 4-11** The Export File Format



**18. Under the heading Select the format that you want to use, click the radio button for the second option, Base-64 Encoded X.509 (.CER).**

**19. Click Next.**

The File to Export screen appears (see [FIGURE 4-12](#))

**FIGURE 4-12** The File to Export Screen



20. **Name the file, `ad.cer`.**

---

**Note – DNS resolution issues might occur if the filename is incorrect.**

---

Store this exported certificate in a shared folder of your choice.

21. **Click Next.**  
The `ad.cer` file is exported to the shared folder.
22. **To set the Certificate server to respond to the CA request automatically, open Default Domain Controller Security Settings.**
23. **Expand Public Key Policies, and in the Automatic Certificate Request Settings, create a new Computer entry from the supplied entry list.**
24. **Use a web browser to connect to an SP ELOM web GUI.**  
Enter the URL of the SP in the address bar.
25. **Log in as root, or as a user with administrator privileges.**
26. **Click the User Management tab, and click the ADS Configuration submenu tab.**  
The ADS Configuration screen appears.
27. **Upload the `ad.cer` file from the share network folder.**
28. **Enter the Primary, Secondary DNS and the Root Domain addresses.**

29. Click **Submit** to save the configuration.
  
  30. **Log out of the web GUI.**  
Click the Logout button.
  
  31. **To test your configuration, log in as the new user created in the Active Directory structure.**
- 

## Managing and Maintaining the System

The User Management, System Monitoring, Remote Control, Maintenance, and System Information submenus enable you to manage and maintain server-related functions. These functions are described in the following sections:

- [“Managing Users and Accounts” on page 46](#)
- [“Managing the State of the System Locator Indicator LED” on page 52](#)
- [“Managing the Front Panel and On-Board Fault LEDs” on page 52](#)
- [“Setting Power Control” on page 54](#)
- [“Resetting the Service Processor” on page 54](#)
- [“Updating the Firmware” on page 55](#)
- [“Managing Session Timeout” on page 57](#)
- [“Setting the Time” on page 58](#)
- [“Changing the Administrator Password Using the BIOS Setup Utility” on page 58](#)
- [“Recovering from a Corrupt SP” on page 59](#)

## Managing Users and Accounts

The User Management tab provides access to the User Account screen, which lists current users by privilege and status, and enables the administrator to add, delete, modify and enable/disable user accounts.

The ELOM supports up-to 10 user accounts. One of the user accounts is root, which is set by default and cannot be removed. Therefore, you can configure 9 additional accounts. Each user account consists of a user name, a password, and a permission.

---

**Note** – User permissions extend to both the web GUI and the serial connection methods.

---

The permissions that a user can be assigned include:

- **Administrator** – Enables read and write access to all ELOM software features, functions, and commands.
- **Operator** – Enables read-only access to a limited number of ELOM software features, functions, and commands, plus management access to Indicator and Fault LEDs.
- **User** – Enables read-only access to a limited number of ELOM software features, functions, and commands.
- **Callback** – Enables read-only access to a limited number of ELOM software features, functions, and commands.

TABLE 4-2 shows the user permission levels and the access each level has to the ELOM menus and screens.

---

**Note** – If the SP password has been changed and then lost, a BIOS option exists to reset the password back to the default changeme. See [“Resetting the Service Processor” on page 54](#).

---

**TABLE 4-2** User Permission Levels and Menu Access

Main Level Tabs	Sub-level 1	Sub-level 2	Administrator	Operator	User	Callback
System Information			Yes	Yes	Yes	Yes
	Versions		Yes	Yes	Yes	Yes
		SP Version	Yes	Yes	Yes	Yes
		Server Board Information	Yes	Yes	Yes	Yes
	Session Time-Out		Yes	–	–	–
	Components		Yes	Yes	Yes	Yes
		CPU	Yes	Yes	Yes	Yes
		Memory	Yes	Yes	Yes	Yes
		NIC	Yes	Yes	Yes	Yes
System Monitoring			Yes	Yes	Yes	Yes

**TABLE 4-2** User Permission Levels and Menu Access (Continued)

Main Level Tabs	Sub-level 1	Sub-level 2	Administrator	Operator	User	Callback
	Sensor Reading		Yes	Yes	Yes	Yes
		Summary	Yes	Yes	Yes	Yes
		Fan	Yes	Yes	Yes	Yes
		Temperature	Yes	Yes	Yes	Yes
		Voltage	Yes	Yes	Yes	Yes
		Power Supply	Yes	Yes	Yes	Yes
	Event Logs		Yes	Yes	Yes	Yes
		View Event Logs	Yes	Yes	Yes	Yes
		Save Event Logs	Yes	-	-	-
		Clear Event Logs	Yes	-	-	-
	Locator Indicator		Yes	Yes	-	-
	Fault LED		Yes	Yes	-	-
Configuration			Yes	-	-	-
	Network		Yes	-	-	-
	E-mail Notification		Yes	-	-	-
	Platform Event Filter		Yes	-	-	-
	Clock Setting		Yes	-	-	-
	System Management Access		Yes	-	-	-
		SSL Certificate	Yes	-	-	-
		SNMP	Yes	-	-	-
User Management			Yes	-	-	-
	User Account		Yes	-	-	-
	ADS Configuration		Yes	-	-	-
Remote Control			Yes	-	-	-
	Redirection		Yes	-	-	-
	Remote Power Control		Yes	-	-	-
	Hotkey Setup		Yes	-	-	-

**TABLE 4-2** User Permission Levels and Menu Access (Continued)

Main Level Tabs	Sub-level 1	Sub-level 2	Administrator	Operator	User	Callback
Maintenance			Yes	–	–	–
	Firmware Upgrade		Yes	–	–	–
	Reset SP		Yes	–	–	–

## ▼ To Add a User

1. **From the User Management submenu, click the User Account tab.**

The User List screen appears.

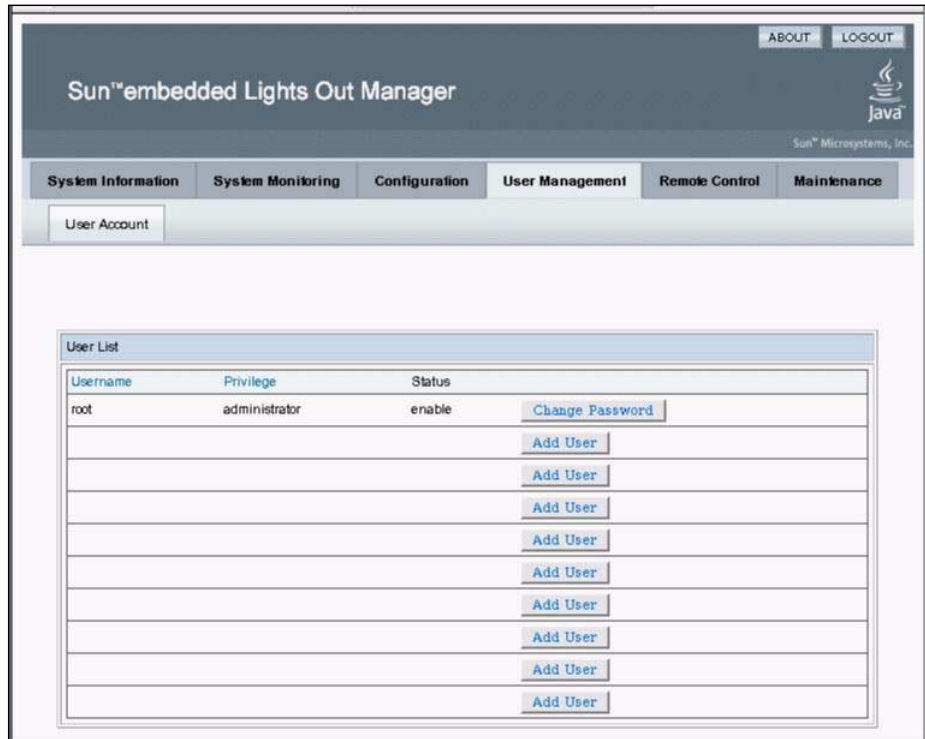
2. **Click any button labeled Add User.**

The Manage User Account screen appears (see [FIGURE 4-13](#)).

If all 10 user account slots are configured, you must delete an existing user account before you can add a new user account. See [“To Delete a User Account” on page 51](#).



FIGURE 4-13 The User Management Screen



3. Complete the following information.

a. Type a user name in the User Name field.

The user name must be at least 4 characters and no more than 20 characters. User names are case-sensitive and must start with an alphabetical character. You can use alphabetical characters, numerals, hyphens, and underscores. Do not include spaces in user names.

b. Type a password in the Password field.

The password must be at least 8 characters and no more than 16 characters. The password is case-sensitive. Use alphabetical, numeric, and special characters for better security. You can use any character except a colon. Do not include spaces in passwords.

c. Retype the password in the Confirm Password field to ensure that the password is correct.

d. Select either Administrator, Operator, User, or Callback for the user permission (see TABLE 4-2 for a listing of permission levels and access).

- e. **When you finish entering the new user's information, click Add.**

The User Accounts screen appears. The new user account and associated information is displayed on the User Accounts screen.

## ▼ To Change a User Password or Privilege

1. **From the User Management submenu, click the User Account tab.**  
The User List screen appears.
2. **Click either the Change Password or Change Permission button for the user.**
3. **Change the password or privilege as needed.**
4. **After you have modified the user information, click Submit for your changes to take effect, or click Reset to return to the previous settings.**

A confirmation screen verifies that the user account was modified successfully. To change the administrator password using the BIOS Setup Utility, see [“Changing the Administrator Password Using the BIOS Setup Utility”](#) on page 58.

## ▼ To Delete a User Account

1. **From the User Management submenu, click the User Account tab.**  
The User List screen appears.
2. **Click the Delete button for the user that you would like to delete.**  
You do *not* receive a confirmation prompt.

## ▼ To Disable or Enable a User

Disabling a user makes the user account inactive. This might be preferable to deleting the account.

1. **From the User Management submenu, click the User Account tab.**  
The User List screen appears.
2. **Click the Disable or Enable button for the appropriate user.**  
You do *not* receive a confirmation prompt.

# Managing the State of the System Locator Indicator LED

The System Locator Indicator LED is located on the front and rear panel of the server. You can activate the Locator Indicator LED in the ELOM. By activating the Locator Indicator LED for a particular server, you can identify that server from the many other servers installed in a rack. You can manage the state of the System Locator Indicator LED from the ELOM Maintenance screens.

## ▼ To Manage the State of the System Locator Indicator LED

1. **From the main menu, click the System Monitoring tab.**

The System Monitoring submenu tabs appear.

2. **Click the Locator Indicator tab.**

The System Indicator LED screen appears.

3. **Select the appropriate radio button to either turn the LED on or turn it off.**

4. **Click Submit to change the state of the LED, or click Reset to cancel.**

## Managing the Front Panel and On-Board Fault LEDs

Your server is equipped with six fault LEDs. Four of the LEDs are on the front panel, and two are located inside the server on the motherboard. Three of the front panel LEDs are located on the right front side of the server front panel, the Top Open (Check Fan Status) LED, the Power Supply (PS) LED, and the Overtemperature Warning LED. These LEDs alert you to problems specific to a particular subsystem. Use these LEDs in conjunction with the ELOM to troubleshoot down to the component level.

The Fault LED (Service Required LED) is located on the left side of the server front panel. This LED alerts you to an internal problem on the motherboard. Use the Fault LED in conjunction with the two internal on-board fault LEDs, the CPU LED and the DIMM LED to troubleshoot issues related to a specific CPU or DIMM.

You can monitor and manage the state of the Fault LEDs from the ELOM Maintenance screens. For more information about using the fault LEDs to troubleshoot server problems, see the server service manual.

## ▼ To View the State of the Fault LEDs

1. In the main menu, click the **System Monitoring** tab.

The System Monitoring submenu tabs appear.

2. Click the **Fault LED** submenu tab.

The Fault LED Control screen appears (see [FIGURE 4-14](#)).

**FIGURE 4-14** The Fault LED Screen

Fault LED Control	
Current Status : On	<input type="radio"/> Turn Fault LED Off
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	
Front Panel Fault LED Control	
Fan Current Status : Off	
PS Current Status : Off	
Temperature Current Status : On	<input type="radio"/> Turn Front Panel Temperature LED Off
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	
On-Board Fault LED Control	
<input type="radio"/> Turn On-Board CPU LED Off	
<input type="radio"/> Turn On-Board DIMM LED Off	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

The Fault LED screen is divided into three sections, the Fault LED Control section, the Front Panel Fault LED Control, and the On-Board Fault LED Control. These sections allow you to monitor and change the status of each LED. If the current status of an LED is On, then you will have the option to turn it Off. Otherwise, the LED status is shown as Off. For example in [FIGURE 4-14](#), the front panel Fault LED, the Overtemperature Warning LED and the internal on-board CPU LED and DIMM LED are On.

## ▼ To Turn the Fault LEDs Off

1. Select the appropriate radio button for the fault LED that you would like to turn off.
2. Click the appropriate **Submit** button for the particular section to turn the LED off.

## Setting Power Control

You can control power to the server you are logged in to by using the Remote Power Control submenu screen to set the power control action.

### ▼ To Set Power Control

1. **From the Remote Control tab, click Remote Power Control.**

The Power Control screen appears showing a drop-down list of various power-off and restart options: Force Power Off, Reset, Graceful Shutdown, Boot Option: BIOS Setup, Boot Option: PC Check, and NMI.

2. **Select power option you want and click Save.**

For example, select Boot Option: BIOS Setup to reboot the system and enter the BIOS.

3. **When you have made your changes, click Submit to save the changes, or click Reset to clear the changes.**

## Resetting the Service Processor

The baseboard management controller holds the original default settings of the service processor. In the event of system lock-up or panic you can reset the SP to its original state.

### ▼ To Reset the Service Processor

1. **From the main menu click the Maintenance tab.**

The Maintenance submenus appear.

2. **Click the Reset SP submenu tab.**

The Reset SP screen appears.

---

**Note** – Resetting the SP is a hard reset. Because you are logged in to the web GUI when the SP is reset, the interface will become inactive and your session will end. To continue working within the ELOM web GUI, you need to log in again.

---

3. **Click Reset SP button.**

The following message appears:

Please wait for SP reset then reconnect.

## Updating the Firmware

There are several ways to update the SP firmware. Use one of the following procedures:

1. [“Updating the firmware using the Tools and Drivers CD” on page 55.](#)
2. [“Updating the Firmware Using a Web Browser” on page 56.](#)
3. Updating the firmware using `TftpUpdate` through the CLI. See [“To Update the Firmware” on page 100.](#)
4. Use `CPLDUpdate` through the CLI. See to [“To Update the Firmware” on page 100.](#)
5. [“Updating the Firmware Using a Web Browser” on page 56.](#)

## Updating the firmware using the Tools and Drivers CD

### ▼ To Update the firmware Using the Tools and Drivers CD

1. **Insert the latest version of the Tools and Drivers CD into the CD/DVD drive.**
2. **Power on the system.**

The system boots using the Tools and Drivers CD, and a menu with five options appears.
3. **To update the firmware, select one of the following two options:**
  - a. **Flash System BIOS/Service Processor Firmware—Clear BIOS CMOS and load default settings (recommended).**

-or-

**b. Flash the System BIOS/Service Processor Firmware—Preserve BIOS CMOS settings (advanced use only).**

---

**Note** – Use the second option only if you have customized BIOS settings and would like to retain these settings. This option might require user intervention during the reboot.

---

## Updating the Firmware Using a Web Browser

This section explains how to update firmware to a remote server. There are two options for updating firmware.

1. Clear CMOS (default)
2. Preserve CMOS

If the system BIOS has not been customized, select option #1: Clear CMOS. If the system BIOS has been customized, select option #2: Preserve CMOS.

---

**Note** – Selecting option #2 might require user interaction during the reboot.

---

## ▼ To Update the Firmware Using a Web Browser

---

**Note** – The system *must* be powered off for you to perform an update. If the server is powered on, the SP warns the user to power off before continuing. The option to update firmware will not be available if the server is powered on. For information about how to power-off the server, see [“Setting Power Control” on page 54](#).

---

**1. From the main menu, select the Maintenance tab.**

The Maintenance submenu tabs appear.

**2. Click the Firmware Update tab.**

The Firmware Update screen appears.

**3. Select the firmware file or CPLD file to update.**

These files are located on the Tools and Drivers CD in the Remote\_Firmware directory.

4. **Choose whether to preserve the system BIOS CMOS and load optimized defaults.**

---

**Note** – A hardware procedure for clearing the NVRAM is available in the server service manual.

---

5. **Firmware will perform a check and ask the user to confirm the update by displaying current and proposed firmware revisions.**
6. **When the update is finished, after approximately five minutes, the SP resets and you are logged out.**

## Managing Session Timeout

The session timeout is an inactivity timer. If an open session enters a state of inactivity that exceeds the preset timer, the system closes (logs out) the session. This function prevents unauthorized access to the system by providing an automated logout function. The session timeout is *enabled* by default. It might be helpful to disable the session timeout when performing updates or remote sessions.

### ▼ To Set the Session Timeout

1. **From the main menu, click the System Information tab.**  
The Versions, Session Time-Out, and Components submenu tabs appear.
2. **Select the Session Time-Out tab.**  
The Session Time-Out screen appears.
3. **Click the Enable Timeout radio button.**
4. **Select a session time from the Session Time drop-down list.**  
The options are 15 minutes (default), 30 minutes, 1-hour, and 2 hours.
5. **Click the Submit button to set the session timeout.**

### ▼ To Disable the Session Timeout

1. **From the main menu, click the System Information tab.**  
The Versions, Session Time-Out, and Components submenu tabs appear.



2. **Select the Session Time-Out tab.**  
The Session Time-Out screen appears.
3. **Click the Disable Time-Out radio button.**
4. **Click the Submit button to disable the session timeout.**

## Setting the Time

The Configuration submenu tab allows you to set the correct time for the ELOM. Accurate time is important for tracking and troubleshooting occurrences reported in the system event log (SEL).

### ▼ To Set the Time

- **From the Configuration submenu, click the Set Time tab.**

The Set Time screen appears. Use the radio buttons to either manually input the date and time, or to use an NTP server. For the latter, you will have to input the IP address of the server.

## Changing the Administrator Password Using the BIOS Setup Utility

You can change the administrator password using the BIOS Setup Utility. If you've changed the root password, but have not created an alternate account, and the new root password is lost or forgotten, you will have to reset the SP to return the ELOM to its default settings. For information about how to reset the SP, see [“Resetting the Service Processor” on page 54](#). Additionally, hardware options for resetting the BIOS password and the NVRAM are available in the product *Service Manual*.

### ▼ To Change the Administrator Password using the BIOS Setup Utility

1. **Connect a KVM to the server.**

**2. Reboot the server, and watch the output.**

A prompt appears at the bottom of the screen instructing you to press F2 to enter the BIOS settings.

**3. Press F2 when prompted.**

The BIOS Setup Utility screen appears (for information about the BIOS Setup Utility, see the server service manual).

**4. Use the right arrow key to navigate to the Security menu tab.**

Highlight the Security menu tab so that the Security screen appears.

**5. Use the down arrow key to highlight the Supervisor (administrator) password.**

**6. To change the administrator password, press enter.**

Follow the BIOS prompts to change the password.

**7. To save your change and exit the BIOS Setup Utility, press F10.**

The server reboots.

## Recovering from a Corrupt SP

Should the SP (service processor) software become corrupted, you can reinstall the default image from the CD. You need a bootable USB flash device and a jumper cap. For procedures on recovering from a corrupt SP, see the product *Service Manual*.





# Using the Remote Console Application

---

This chapter describes how to use the remote console application. It includes the following sections:

- “Accessing the Remote Console” on page 61
- “Starting the Remote Console Application” on page 64
- “Redirecting Keyboard, Video, Mouse, or Storage Devices” on page 66
- “Installing an Operating System on a Remote Server” on page 72
- “Other Remote Options” on page 73

---

## Accessing the Remote Console

The remote console application, which you access via a web browser, enables you to control your server’s operating system remotely using the screen, mouse, and keyboard, and to redirect local CD and diskette drives as if they were connected directly to the server.

## Requirements

A compatible web browser and a minimum of JRE™ 1.6.0 are required to operate the remote console application. See [TABLE 5-1](#).

---

**Note** – You do not need to install any OS-specific drivers or helper applications on client systems to run the remote console application.

---

**TABLE 5-1** Client Installation Requirements

Client OS	Java Runtime Environment Including Java Web Start	Web Browsers
Microsoft Windows XP Pro	JRE 1.6 (Java 6.0 or later)	Internet Explorer 6.0 and later Mozilla 1.7.5 or later Mozilla Firefox 1.0
Red Hat Linux 4.0 or later Desktop and Workstation Editions	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5 or later Mozilla Firefox 1.0
Solaris 9	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5
Solaris 10	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5
SUSE Linux 9.2	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5

---

**Note** – You can download the JRE 1.6 at <http://java.sun.com>.

---

---

**Note** – To start the remote console successfully, pop-ups must be allowed on the browser. With some browsers you can do this by pressing and holding the Control key when launching the remote console session.

---

## CD and Diskette Redirection Operational Model

When you redirect the local client CD drive or diskette drive to a remote host server, the following rules apply:

- In all cases, the CD drive and diskette drive appear to be plugged in to the host.
- If you do not redirect them, the host acts as if there is no medium unless there is a CD in the host CD drive. If there is a CD in the host CD drive, the host accesses it normally.

The information in [TABLE 5-2](#) describes different case scenarios in which the remote console application and CD drive and diskette drive redirection operate.

**TABLE 5-2** Remote Console Operation With DVD Drive and Diskette Drive

Case	Status	DVD Seen by Host	Diskette Seen by Host
1	Remote console application not started or remote console started but DVD/diskette redirection not started.	DVD device present. No medium indication is sent to the host from the ELOM when the hosts asks.	Diskette device present. No medium indication is sent to the host from the ELOM when the host asks.
2	Remote console application started with no medium present in the drive.	DVD device present. Whenever the host asks, which may be automatic or when you access the device on the host, the remote client sends a status message. In this case since there is no medium, the status is no medium.	Diskette device present. Whenever the host asks (for example, you double-click a drive), the remote client sends a status message. In this case since there is no medium, the status is no medium.
3	Remote console application started with no medium, then medium is inserted.	DVD device present. Whenever the hosts asks (automatic or manual), the remote client sends a status message as medium present and also indicates the medium change.	Diskette device present. Whenever the host asks (manual), the remote client sends a status message as medium present and also indicates the medium change.
4	Remote console application started with medium inserted.	Same as 3.	Same as 3.
5	Remote console application started with medium present, then medium is removed.	Next command from the host gets a status message indicating medium not present.	Next command from the host gets a status message indicating medium not present.
6	Remote console application started with image redirection.	Same as 3.	Same as 3.
7	Remote console application started with image, but redirection is stopped (which is the only way to stop ISO redirection).	Driver knows DVD redirection stopped so it sends a medium absent status on the next host query.	Driver knows DVD redirection stopped so it sends a medium absent status on the next diskette query.
8	Network failure.	The software has a keep alive mechanism. The software detects keep alive failure since there is no communication and closes the socket, assuming the client is unresponsive. Driver sends a no medium status to the host.	The software has a keep alive mechanism. The software detects and unresponsive client, closes the socket, and indicates to the driver that the remote connection went away. Driver sends a no medium status to the host.
9	Client crashes.	Same as 8.	Same as 8.

---

# Starting the Remote Console Application

Use this procedure to start the remote console application from a web browser. You might be presented with a series of questions. In each case, select Run.

---

**Note** – Each new ELOM system is delivered with DHCP set as the default. If an IP address is not found within 5 seconds, the system retries three times to find a DHCP server. If it is still unsuccessful, the SP will allow instant web access by defaulting to the IP address 192.168.xxx.xxx. Where xxx.xxx is based upon the last two fields of the SP MAC address.

---

## ▼ To Start the Remote Console Application

1. **Open your web browser.**
2. **In the address bar, enter the IP address of the SP.**

The login screen appears.

3. **Type an administrator user name and password.**

Or use the default preconfigured account:

Username: **root**

Password: **changeme**

4. **Click Login.**

The main menu screen appears.

5. **Click the Remote Control tab, and select Redirection.**

The screen displays a Launch Redirection button.

6. **Click Launch Redirection.**

A screen identifies your current host name, IP address, and user name. The Launch button opens the remote console.

7. **Click Launch.**

---

**Note** – For systems using Firefox and Mozilla web browsers, the required version of JRE must be at least version 1.6 or later.

---



The web browser downloads the embedded remote control application automatically, and the Remote Console screen appears.

If the remote console does not appear, it might be blocked by web browser security controls. Reduce security configuration to allow the remote console to appear.

---

**Note** – To start the remote console successfully, pop-ups must be allowed on the browser. With some browsers you can do this by pressing and holding the Control key when launching the remote console session.

---

Changing the format of the screen is described in the following section, [“To Set Parameters for the Remote Console” on page 65](#).

## Setting Parameters for the Remote Console

This section explains how to define the quality of video, the size of the screen, and set hot keys for the remote console application.

### ▼ To Set Parameters for the Remote Console

#### 1. From the Remote Control submenu, select Hotkey Setup.

The User Profile screen appears. The User Profile screen allows you to set up separate video, KVM, and hot key settings for each user. The subsequent window displays a version of the screen output. This requires a Java Webstart application to be launched.

**a. The first time this application is launched you must respond to accept various security questions before the application is installed and operates correctly.**

#### **b. Right-click to display the remote console as a full screen.**

By default, the remote console will synchronize both mouse cursors, and display only one mouse cursor within the remote console screen.

When the mouse cursor leaves the screen, the local cursor takes over and the other mouse cursor remains in the remote console screen.

You can enable user modes in the setup of the web GUI or in the remote console screen.

## 2. When the login is successful, the remote console screen appears.

The remote console application starts with the video and keyboard enabled by default. In most cases, you need only enable the mouse redirection. You can now use the remote console application to start your server's operating system.

---

**Note** – For detailed instructions on how to enable and disable I/O and storage devices (CD-ROM and diskette drives), see [“Redirecting Keyboard, Video, Mouse, or Storage Devices” on page 66.](#)

---

---

# Redirecting Keyboard, Video, Mouse, or Storage Devices

The remote console application supports the redirection of the following types of devices:

- Video quality display – the server's video output is automatically displayed on the local console screen.
- Hot key – enable a single key to mimic a series of keystrokes.
- Keyboard and mouse devices – Standard keyboards, mouse, and other pointing devices.
  - Keyboard redirection is enabled by default.
  - Mouse redirection must be enabled manually.
- Storage devices – CD/DVD drives, USB flash, DVD-ROM or diskette disk drives, hard drives, or NFS.

---

**Note** – When attempting to mount a virtual USB device with the Solaris OS, the USB device might need to be physically removed and inserted.

---

Some redirection and mounting issues might occur with some versions of RHEL. To resolve RHEL redirection and mounting issues, see the workaround procedures in [“Redirection and Mount Workarounds for RHEL” on page 68.](#)

## ▼ To Redirect Keyboard and Mouse Devices

Use the following procedure to redirect your local workstation or laptop keyboard and mouse to a remote server.

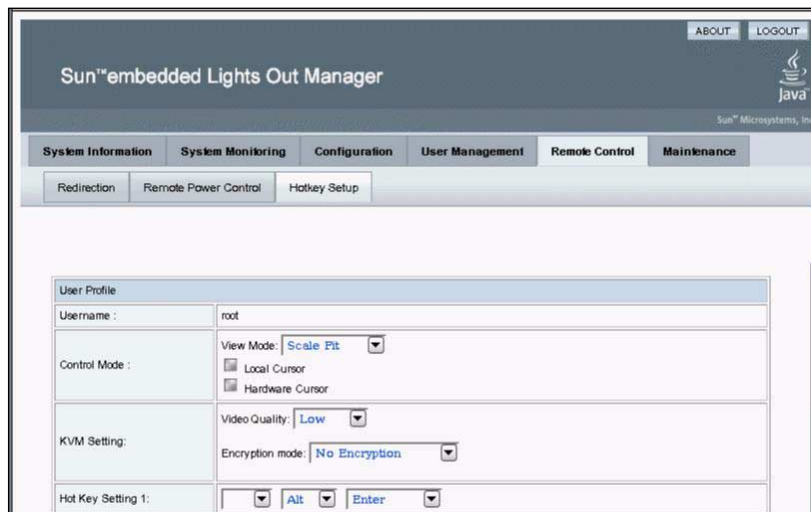
1. Start the remote console application as described in “Starting the Remote Console Application” on page 64.
2. From the Remote Control submenu, select the Hotkey Setup tab.  
The Control Mode section of the Hotkey Setup screen enables mouse redirection.
3. Select Hardware Cursor to enable a variety of cursor movements.

---

**Note** – For the mouse to work correctly, you might have to change the mouse mode. Click the double mouse cursor on the navigation bar to toggle between local and remote mouse cursor movement. Keyboard redirection is selected by default.

---

**FIGURE 5-1** Keyboard, Video, and Mouse Selections



4. You can click Submit to enable your options after each choice to observe the consequences, or continue directly to Step 5.
5. When you have completed your selections, click Submit to enable your options.

## ▼ To Redirect Storage Devices

Use the following procedure to enable a storage device attached to your local workstation or laptop to serve as a storage device for a server. You can use this option to install software from a local CD/DVD drive to multiple remote servers.

You can also redirect a CD image file or a diskette image file stored on your hard drive.

1. **Start the remote console application as described in “Starting the Remote Console Application” on page 64.**

The Remote Console screen appears.

2. **Select Storage from the drop-down list, and click Mount Device.**

This enables the corresponding local storage device to connect to the remote server as though it were a storage device attached directly to that remote server.

---

**Note** – With the RHEL 5 OS, virtual USB devices are not shown in the drop-down list. For a workaround, see “Mounting a Virtual USB Drive with RHEL 5” on page 70.

---

3. **Select a source device from the drop-down list.**

- To store a selection to a real CD-ROM device, select from the Drive Name drop-down list.
- To store a CD image file or a diskette image file to your hard drive, select ISO file from the Source Device drop-down list.

---

**Note** – You cannot select two CD-ROM devices or two diskette devices. For example, you cannot select CD-ROM and CD-ROM image. Use the web browser to navigate to the corresponding file, then click Submit.

---

## Redirection and Mount Workarounds for RHEL

The procedures in this section describe redirection and mount workarounds for some versions of RHEL. The procedures included here are:

- “Redirecting a CD/DVD Drive Using RHEL 3” on page 68
- “Mounting More Than One Virtual Device with RHEL 4” on page 70
- “Manually Mounting a Virtual Device Connected to a RHEL 5 System” on page 70
- “To Mount a Virtual USB Drive with RHEL 5” on page 71

### Redirecting a CD/DVD Drive Using RHEL 3

When using RHEL 3, the system might not see any virtual CD/DVD drive. To resolve this issue, use the following procedure.

## ▼ To Redirect a CD/DVD Drive Using RHEL 3

1. Open a terminal window.

2. Obtain the device ID of the CD/DVD drive using the following command:

```
# ls -al /dev/cdrom
```

The result of the command might look similar to:

```
/dev/hda
```

hda is the CD/DVD-ROM device ID.

3. Edit the `lilo.conf` file by adding the following line:

```
xxx=ide-scsi
```

xxx The CD/DVD drive device ID obtained in Step 2

Example:

```
image=/boot/bmlinuz-2.4.21-40.EL
```

```
label=linux
```

```
initrd=/boot/initrd--2.4.21.40.EL.img
```

```
read-only
```

```
root=/dev/hda1
```

```
append=xxx=ide-scsi
```

4. Save and exit the file.

5. Edit `grub.conf` file by adding the following line:

```
xxx=ide-scsi
```

xxx The CD/DVD drive device ID obtained in Step 2

Example:

```
timeout=1-
```

```
splashimage=(hd0,0)/grub/splash.xpm.gz
```

```
title Red Hat Enterprise Linux AS (2.4.21-40.EL)
```

```
root (hd0,0)
```

```
kernel /vmlinuz-2.4.21-40.EL ro root=LABEL=/ xxx=ide-scsi
```

```
initrd-2.4.21-40.EL.img
```

6. Save and exit the file.

7. Reboot the system.

## Mounting More Than One Virtual Device with RHEL 4

### ▼ To Mount More Than One Virtual Device with RHEL 4

1. **Edit the `/etc/modprobe.conf` file by adding the following line:**

```
options scsi_mod max_luns=xxx.
```

*xxx* The number of LUNs to support

2. **Build the initial ramdisk to implement the change.**

```
mkinitrd -f /boot/newimage-2.6.xx 2.6.xx
```

*xx* The kernel version

3. **Change the `boot/grub/menu.1st` parameter to:**

```
newimage-2.6.xx
```

*xx* The kernel version

4. **Save and exit the file.**

5. **Reboot the system.**

After the reboot, the LUNs should appear.

## Manually Mounting a Virtual Device Connected to a RHEL 5 System

When mounting a virtual device, sometimes the device might not automount on the remote system with RHEL 5. Use this procedure to manually mount the device.

### ▼ To Manually Mount a Virtual Device Remotely Connected to a RHEL 5 System

1. **Double-click on the computer icon on desktop.**
2. **Right-click on the new device and select Mount.**

## Mounting a Virtual USB Drive with RHEL 5

With the RHEL 5, virtual USB devices are *not* shown in the drop-down list. Use this procedure to mount a virtual USB drive on a RHEL 5 system.

## ▼ To Mount a Virtual USB Drive with RHEL 5

1. **Edit the file** `/usr/share/hal/fdi/policy/10osvendor/20-storage-methods.fdi`.

2. **Search for the following string:** `<match key="volume.fsusage" string="filesystem">`

The search returns the following information:

```
<append key="volume.mount.valid_options" type="strlist">codepage=
</append>
<append key="volume.mount.valid_options" type="strlist">iocharset=
</append>
<append key="volume.mount.valid_options" type="strlist">umask=
</append>
<append key="volume.mount.valid_options" type="strlist">uid=</append>
</match>
</match>
```

3. **Add the following text to the file:**

Place this text immediately after the text that was returned in Step 2.

```
<match key="@block.storage_device:storage.vendor" string=
"Virtual">
    <match key="@block.storage_device:storage.model"
string="DVD/CD-ROM">
        <match key="info.category" string="volume">
            <match key="block.is_volume" bool="true">
                <match key="volume.fsusage" string="">
                    <merge key="volume.fsusage" type=
"string">filesystem</merge>
                    <merge key="volume.fstype" type=
"string">iso9660</merge>
                </match>
            </match>
        </match>
    </match>
</match>
```

4. **Save and exit the file.**
5. **Reboot the system.**

---

# Installing an Operating System on a Remote Server

This method includes using a CD or DVD drive or image of the operating system on a remote networked system to install the operating system onto the server.

Requirements for Remote KMVS Over IP installation include:

- Remote system connected to the network
- CD/DVD drive connected to the remote system
- Media for installing the operating system of your choice
- SP of the server set up as instructed in the server installation guide.

## ▼ To Install an OS on a Remote Server Using a Virtual CD-ROM

---

**Note** – Disable the timeout function when installing remotely from the virtual CD-ROM.

---

1. **On your laptop or local terminal, open a web browser, and enter the IP address of the Sun Fire X4150 server service processor for the target system.**  
This is the server on which you want to install the operating system.
2. **Type the user name and password in the login screen.**
3. **From the Remote Control submenu, click the Redirection tab.**
4. **Click the Launch Redirection button to open a remote console screen.**
5. **Insert the operating system CD/DVD to be installed on the server into your laptop or local CD/DVD drive.**
6. **In the remote console screen, choose Storage →Mount devices.**  
The Device Configuration screens appears.
7. **Under Storage 1, in the drop-down list, select the local CD/DVD that you will be using for the installation.**
8. **Click Submit.**



**9. Reboot the server.**

The system will add the virtual CD-ROM to the boot order, and boot from it.

---

## Other Remote Options

Command-line options that are available to address many of these tasks include IPMI tools ([Chapter 6](#)), CLI ([Chapter 7](#)), and SSH (Secure Shell).



## Using IPMI

---

This chapter describes the Intelligent Platform Management Interface (IPMI) functionality and lists the supported IPMI commands. It includes the following sections:

- [“About IPMI” on page 75.](#)
- [“Supported IPMI 2.0 Commands” on page 77.](#)

---

## About IPMI

The Intelligent Platform Management Interface (IPMI) is an open-standard hardware management interface specification that defines a specific way for embedded management subsystems to communicate. IPMI information is exchanged through the service processor (SP), an IPMI-compliant hardware component. Using low-level hardware intelligence instead of the operating system has two main benefits: First, this configuration allows for out-of-band server management, and second, the operating system is not burdened with transporting system status data.

You can manage your server with the IPMI v.1.5/2.0 on your server or stand-alone server, which runs a daemon to do the following:

- Support low pin count (LPC) host interface in two modes:
  - KCS Mode (3 channels)
  - BT Mode (1 channel with 32 bytes of FIFO)
- Support dedicated NIC or shared lights out management (LOM)
- Support Serial-On-LAN (SOL)
- Customize FRU/Sensor Data Record data (firmware independent)
- Provide KVM over IP (remote access to the server)
- Enable the user interface (UI) for hot key definitions (for example Ctrl-Alt-Del)

- Provide full screen display switch
- Set dynamic video scaling (4x4 Video Scalar)

Your Sun Fire X4150 server is IPMI v2.0 compliant. You can access IPMI functionality through the command line with the IPMItool utility either in-band or out-of-band. Additionally, you can generate an IPMI-specific trap from the web interface or manage the server's IPMI functions from any external management solution that is IPMI v1.81 or v2.0 compliant. For more information about the IPMI v2.0 specification, go to:

<http://www.intel.com/design/servers/ipmi/spec.htm#spec2>

## IPMItool

IPMItool is a simple command-line interface that is useful for managing IPMI-enabled devices. You can use this utility to perform IPMI functions with a kernel device driver or over a LAN interface. IPMItool enables you to manage system field-replaceable units (FRUs), monitor system health, and monitor and manage system environmentals, independent of the operating system.

Download this tool from <http://ipmitool.sourceforge.net/>, or locate IPMItool and its related documentation on your server Tools and Drivers CD.

When IPMItool is installed, it includes a man page. To view it, enter:

```
man ipmitool
```

If your client machine has a default installation of Solaris 10, you can find a preinstalled version of IPMItool in the following directory: `/usr/sfw/bin`. The binary file is called `ipmitool`.

## Sensors

Your server includes a number of IPMI-compliant sensors. Some sensors measure voltages, and temperature ranges, and others are capable of monitoring switches, such as the chassis interlocks, which detect whether the chassis cover is open or shut. For a complete list of sensors, see your platform supplement. To obtain sensor information on specific sensors, enter the following command:

```
ipmitool -H ipaddressof the SP -U username -P password [sensor | sdr]
```

The sensors can activate system fault lights, and register events in the system event log (SEL). To see the system event log from the IPMItool, at the prompt, enter the following command:

```
ipmitool -H ipaddress of the SP -U root -P password sel list
```

Depending on where IPMItool is installed from, the `-P` option might be missing. In such a case, do not type the `-P` in the previous command, and enter the password when prompted.

---

## Supported IPMI 2.0 Commands

TABLE 6-2 lists the supported IPMI 2.0 commands.

For details on individual commands, see the IPMI Intelligent Platform Management Interface Design Specification, v2.0. A copy is available at:

<http://www.intel.com/design/servers/ipmi/spec.htm>

**TABLE 6-1** Supported IPMI 2.0 Commands

Commands	Description
raw	Send a RAW IPMI request and print response
i2c	Send an I2C Master Write-Read command and print response
lan	Configure LAN channels
chassis	Get chassis status and set power state
power	Shortcut to chassis power commands
event	Send predefined events to MC
mc	Management Controller status and global enables
sdr	Print Sensor Data Repository entries and readings
sensor	Print detailed sensor information
fru	Print built-in FRU and scan SDR for FRU locators
sel	Print system event log (SEL)
pef	Configure platform event filtering (PEF)
sol	Configure and connect IPMIv2.0 Serial-over-LAN
tsol	Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
isol	Configure IPMIv1.5 Serial-over-LAN
user	Configure Management Controller users
channel	Configure Management Controller channels
session	Print session information

**TABLE 6-1** Supported IPMI 2.0 Commands *(Continued)*

<b>Commands</b>	<b>Description</b>
sunoem	OEM commands for Sun servers
kontronoem	OEM commands for Kontron devices
picmg	Run a PICMG/ACTA extended cmd
fwum	Update IPMC using Kontron OEM Firmware Update Manager
exec	Run list of commands from file
set	Set runtime variable for shell and exec

**TABLE 6-2** Supported IPMI 2.0 Commands

<b>Supported IPMI 2.0 Commands</b>
<b>General Commands</b>
Get Device ID
Cold Reset
Get Self Test Results
Set/Get ACPI Power State
Reset/Set/Get Watchdog Timer
Set/Get BMC Global Enables
Clear/Get Message Flags
Enable Message Channel Receive
Get/Send Message
Read Event Message Buffer
Get Channel Authentication Capabilities
Get Session Challenge
Activate/Close Session
Set Session Privilege Level
Get Session Info
Set/Get Channel Access
Get Channel Info
Set/Get User Access
Set/Get User Name

**TABLE 6-2** Supported IPMI 2.0 Commands (*Continued*)

---

**Supported IPMI 2.0 Commands** (*Continued*)

---

Set User Password

Master Write-Read

Set/Get System Boot Options

Set/Get Event Receiver IPMI

System Interface Support

KCS

BT

Serial Over LAN

RCMP

- Multiple Payloads
- Enhanced Authentication
- Encryption

**PEF and Alerting Commands**

Get PEF Capabilities

Arm PEF Postpone Timer

Set/Get PEF Configuration Parameters

Set/Get Last Processed Event ID

Alert Immediate

PET Acknowledge

**Sensor Device Commands**

Get Sensor Reading Factors

Set/Get Sensor Hysteresis

Set/Get Sensor Threshold

Set/Get Sensor Event Enable

Get Sensor Reading

**FRU Device Commands**

Get FRU Inventory Area Info

---

**TABLE 6-2** Supported IPMI 2.0 Commands (*Continued*)

---

**Supported IPMI 2.0 Commands (*Continued*)**

---

Read/Write FRU Data SDR Device

Get SDR Repository Info

Get SDR Repository Allocation

Reserve SDR Repository

Get/Add SDR

Clear SDR Repository

Get SDR Repository Time

Run Initialization Agent

**SEL Device Commands**

Get SEL Info

Get SEL Allocation Info

Reserve SEL

Get/Add SEL Entry

Clear SEL

Set/Get SEL Time

**LAN Device Commands**

Get LAN Configuration Parameters

**Serial/Modem Device Commands**

Set/Get Serial Modem Configuration

Set Serial Modem MUX

Get TAP Response Codes

Serial/Modem Connection Active

Callback

Set/Get User Callback Options

**Event Commands**

Get Event Count

---



**TABLE 6-2** Supported IPMI 2.0 Commands (*Continued*)

---

**Supported IPMI 2.0 Commands** (*Continued*)

---

Set/Get Event Destination

Set/Get Event Reception State

Send ICMB Event Message

---



## Using the Command-Line Interface

---

This chapter describes how to use the Embedded Lights Out Manager command-line interface (CLI). The sections include:

- [“Logging In to the CLI” on page 83.](#)
- [“Command Syntax” on page 84.](#)
- [“Managing the Host” on page 86.](#)
- [“Managing ELOM Network Settings” on page 88.](#)
- [“Managing Local User Accounts With the CLI” on page 89.](#)
- [“Managing Alerts” on page 92.](#)
- [“Displaying Version Information” on page 99.](#)
- [“Updating the Firmware” on page 100.](#)

---

### Logging In to the CLI

You can access the command-line interface through the serial port or over the Ethernet.

- **Serial port** – The serial port provides access to the CLI and to the system console. IPMI terminal mode and PPP mode are not available on the serial port. For information about logging in to the CLI using the serial port, see [“Connecting Using a Serial Connection” on page 6.](#)
- **SSH** –You can connect to the CLI using an Ethernet connection. Secure Shell connections (SSC) are enabled by default. For information about logging in to the CLI using an Ethernet connection, see [“Connecting Using Ethernet” on page 7.](#)

The server ELOM supports a maximum of 10 active sessions, including serial, SSH, and web interface sessions. Telnet connections to the ELOM are not supported.

---

**Note** – If you have changed the serial redirection output in the system BIOS from SP to SYSTEM, the system output is displayed on the serial connection. To view the SP output on the serial connection, change the system BIOS back to the default BMC.

---

## Command Syntax

The CLI architecture is based on a hierarchical namespace, which is a predefined tree that contains every managed object in the system. This namespace defines the targets for each command verb.

The Embedded Lights Out Manager (ELOM) software includes the `/SP` and `/SYS` namespaces.

The `/SP` namespace manages the ELOM, which allow you to manage users, clock settings, and other issues.. The children of this namespace are `/user`, `/network`, `/clock`, `/AgentInfo`, `/TftpUpdate`, and `/CPLDUpdate`.

The `/SYS` namespace monitors the ELOM, which allows you to display and view critical and system-specific information. The children of this namespace include `/BoardInfo`, `/ProductInfo`, `/ChassisInfo`, `/CtrlInfo`, `/CPU`, `/MemModule`, `/Fan`, `/Temperature`, and `/Voltage`

The CLI provides four privilege levels: administrator, operator, user, and callback. The administrator privilege allows full read and write access to ELOM functionality. The operator privilege has limited write access. The user, and callback privileges have read-only access to the ELOM.

---

**Note** – The default user, root, has administrator privileges. For information about how to create a user account with user privileges, see [“Adding a User Account Using the CLI” on page 90](#).

---

CLI commands are case-sensitive.

### *Syntax*

The syntax of a command is *verb options target properties*.

## Command Verbs

TABLE 7-1 describes the CLI command verbs.

**TABLE 7-1** CLI Command Verbs

Command	Description
cd	Navigates the object namespace.
create	Sets up an object in the namespace.
delete	Removes an object from the namespace.
exit	Terminates a session to the CLI.
help	Displays Help information about commands and targets.
load	
reset	Resets the target's state.
set	Sets target properties to the specified value.
show	Displays information about targets and properties.
start	Starts the target.
stop	Stops the target.
version	Displays the version of ELOM firmware that is running.

## Options

The CLI supports the following options. Not all options are supported for all commands. See a specific command section for the options that are valid with that command. The `-help` and `-examine` options can be used with any command.

**TABLE 7-2** CLI Options

Option	Long Form	Short Form	Description
-default			Causes the verb to perform only its default functions.
-destination			Specifies the destination for data.
-display		-d	Shows the data you want to display.
-examine		-x	Examines the command but does not execute it.
-force		-f	Causes an immediate action instead of an orderly shutdown.
-help		-h	Displays Help information.

**TABLE 7-2** CLI Options (*Continued*)

Option Long Form	Short Form	Description
-keep	-k	Establishes a holding time for command job ID and status.
-level	-l	Executes the command for the current target and all targets contained through the level specified.
-output	-o	Specifies the content and form of command output.
-resetstate		Indicates to what target-specific state to reset the target.
-script		Skips warnings or prompts normally associated with the command.
-source		Indicates the location of a source image.

## *Targets*

Every object in your namespace is a target. Not all targets are supported for all commands. Each command section lists the valid targets for that command.

## *Properties*

Properties are the configurable attributes specific to each object. An object can have one or more property. Each command section lists the valid properties for each target.

---

# Managing the Host

You can use the ELOM to change the host's state and to access the host console.

## Managing the Host State

- To power on the host, enter one of the following commands:

```
set /SYS/CtrlInfo PowerCtrl=on
```

```
-or-
```

```
start SYS
```

- To power off the host gracefully, enter the following command:  
**set /SYS/CtrlInfo PowerCtrl=graceful\_off**
- To power off the host, enter one of the following commands:  
**set /SYS/CtrlInfo PowerCtrl=off**  
 -or-  
**stop SYS**
- To reset the host, enter one of the following commands:  
**set /SYS/CtrlInfo PowerCtrl=reset**  
 -or-  
**reset SYS**
- To reboot and enter the BIOS automatically, enter the following command:  
**set /SYS/CtrlInfo PowerCtrl=BIOSSetup**
- To reboot and enter Pc-Check diagnostic automatically, enter the following command:  
**set /SYS/CtrlInfo BootCtrl=PCCheck\_enable**

## Managing the Host Console

To start a session to the server console, enter this command:

```
start /SP/AgentInfo/Console
```

To revert to CLI once the console has been started, press Esc-Shift-9 keys.

To terminate a server console session started by another user, enter this command:

```
stop /SP/AgentInfo/Console
```

## Viewing Host Sensors

Host systems are equipped with sensors that monitor the state of critical components. For example, they record things like temperatures, voltages, and fan speeds. The `show` command can be used to show the state of the critical components. Use the command:

```
show /SYS/CPU/component
```

*component* The name of the critical component.

For example, the following command shows the state of CPU 0:

**show /SYS/CPU/CPU0**

For more information about sensors, including how to view them using a web browser, see [“Monitoring the System Sensors” on page 19](#).

---

## Managing ELOM Network Settings

You can display or configure the ELOM network settings from the CLI.

### ▼ To Display Network Settings

Use the show command in the /SP/network namespace:

**show /SP/network** *(This will display all network settings.)*

### ▼ To Configure Network Settings

Use the set command to change properties and values for network settings.

---

**Note** – Ensure that the same IP address is always assigned to an ELOM by either assigning a static IP address to your ELOM after initial setup, or configuring your DHCP server to always assign the same IP address to an ELOM. This enables the ELOM to be easily located on the network.

---



## Targets, Properties, and Values

These targets, properties, and values are valid for ELOM network settings.

**TABLE 7-3**

Target	Property	Value	Default
/SP/network	IPAddress	<i>ipaddress   none</i>	192.168. <i>last 2 digits of MAC address</i> enabled (only if DHCP not found)
	IPSource	<i>static/dhcp</i>	dhcp
	Gateway	<i>ipaddress   none</i>	None
	Netmask	<i>ipdotteddecimal</i>	255.255.255.0

### Examples

To change the IP address for the ELOM, Enter:

---

**Note** – Changing the IP address will disconnect your active session if you are connected to the ELOM via a network.

---

### Syntax

```
set /SP/network IPAddress=n.n.n.n
set /SP/network Gateway=n.n.n.n
set /SP/network DNS=n.n.n.n
set /SP/network IPSource=[static | dhcp]
```

---

## Managing Local User Accounts With the CLI

This section describes how to add, modify, and delete user accounts using the CLI.

The ELOM supports up to 10 user accounts. One of those, root, is set by default and cannot be removed. Therefore, you can configure 9 additional accounts.

Each user account consists of a user name, a password, and a permission.

The permissions include:

- **Administrator** – Enables read and write access to all ELOM software features, functions, and commands.
- **Operator** – Enables limited access to SP software features, functions, and commands. Operators cannot change their assigned roles.
- **User** – Enables a user to access the system without being able to add, modify, or delete accounts.
- **Callback** – Enables access to commands that set up the callback feature.

The syntax is:

```
set username Permission=[administrator|operator|user]
```

## Adding a User Account Using the CLI

### ▼ To Add a User Account Using the CLI

- Enter the following command:

```
create /SP/users/username
```

You are prompted for a password.

The username must be 4-20 characters long, and passwords must be a minimum of eight characters long.

## To Delete a User Account Using the CLI

- Enter the following command:

```
delete /SP/users/username
```

### ▼ To Display User Accounts Using the CLI

- Enter the following command:

```
show /SP/users
```

# Configuring User Accounts

Use the `set` command to change passwords and permissions for configured user accounts.

---

**Note** – You must have administrator privileges to change user properties.

---

## *Syntax*

**set target** [*propertyname=value*]

## *Targets, Properties, and Values*

These targets, properties, and values are valid for local user accounts.

**TABLE 7-4**

Target	Property	Value	Default
/SP/users/ <i>username</i>	permissions	administrator   operator	operator
	password	<i>string</i>	

## *Examples*

When changing the permissions for `user1` from administrator to operator Enter:

```
set /SP/users/user1 Permission=operator
```

To change `user1`'s password Enter:

```
set /SP/users/user1 password=password
```

---

# Managing Alerts

The system is equipped with sensors that read several system critical parameters, such as voltages and temperatures. The system monitors these sensors and creates an alert when a sensor reading crosses an upper or lower critical threshold level (for more information, see [“Configuring Platform Event Filters” on page 30](#)).

You can manage these alerts, by using the CLI to create filters that trap alerts based on the sensor type. You can then have the filters perform various preconfigured actions in response to the alert. Configuring alerts with the CLI is a two step process. First, configure a destination IP address in the PET. Second, configure a platform event filter (PEF) to enable and perform various alert-triggered actions.

You manage alerts from the `/SP/AgentInfo` namespace, using the `show` and `set` commands. The `show` command allows you to display current alert property and value settings. The `set` command allows you to configure alert property and value settings.

## Displaying Alerts

Use the `show` command to display PET and PEF targets, properties, and values.

### ▼ To Display Alerts

- To display targets, properties, and target commands for PET, enter the following command:

```
show /SP/AgentInfo/PET.
```

- To display targets, properties, and target commands for PEF, enter the following command:

```
show /SP/AgentInfo/PEF
```

Before configuring alerts, you might want to display a target’s current settings. This allows you to examine the current status of alerts. Use the `cd` command and the `show` command, respectively, to navigate to targets and display property values. For example:

```
-> cd /SP/AgentInfo/PET  
/SP/AgentInfo/PET -> show
```

The output of the show command appears:

```
/SP/AgentInfo/PET
Targets:
    Destination1
    Destination2
    Destination3
    Destination4

Properties:
    CommunityString = public

Target Commands:
    show
    cd
    set
```

## Displaying PET Target Properties

### ▼ To Display PET Target Properties

- To display properties, enter the following commands:

```
/SP/AgentInfo/PET -> cd Destination1
```

```
/SP/AgentInfo/PET -> show
```

The result of executing the show command for the target, Destination1 appears:

```
/SP/AgentInfo/PET/Destination1
Targets:

Properties:
    IPAddress = 10.5.157.112

Target Commands:
    show
    set
```

# Configuring Alerts

The first step to configuring alerts is to configure the PET IP address. After you configure the IP address, you need to configure the individual PEF filter tables. Filter tables are where you designate the specific alert-triggered actions

Use the set command to configure alerts in PET and PEF:

## *Syntax*

**set** *target* *propertyname=value*

## *Targets, Properties, and Values*

This target, property, and value is valid when using the set command to set the IPMI PET IP address:

Target	Property	Value	Default
/SP/AgentInfo/PET/[Destination1...Destination4]	IPAddress	<i>ipaddress</i>	(None)

# Configuring the PET IP Address

## ▼ To Configure the PET IP Address

- To set the IP address for Destination1, enter the following commands:

```
-> cd /SP/AgentInfo/PET/Destination1
```

```
/SP/AgentInfo/PET/Destination1 -> set IPAddress=xxx.xxx.xxx.xxx
```

Repeat the above set command to configure the IP address for additional destination targets.

# Configuring the PEF Global Controls

PEF Global Controls allow you to enable PEF actions globally. These settings override settings in the PEF filter table. These targets and properties are valid for configuring the global PEF controls:

Target	Property*
/SP/AgentInfo/PEF/PEFGlobalCtrl	= enable   disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlPowerOff	= enable   disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlPowerCycle	= enable   disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlPowerReset	= enable   disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlAlert	= enable   disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlMail	= enable   disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlInterrupt	= enable   disable (default)

## ▼ To Configure the PEF Global Controls

1. To configure the PEF global controls, you must first enable global control by entering the following commands:

```
-> cd /SP/AgentInfo/PEF
```

```
/SP/AgentInfo/PEF -> set PEFGlobalCtrl=enable
```

After enabling global control, you can enable global control for specific actions.

2. To enable global PEF control for a specific action, enter the following commands for each PEFActionGlobalCtrl that you want to enable:

---

**Note** – This example shows how to enable the power reset PEF global action:

---

```
-> cd /SP/AgentInfo/PEF
```

```
/SP/AgentInfo/PEF -> set PEFActionGlobalCtrlPowerReset=enable
```

## Configuring the Event Filter Tables

The event filter table is where you designate the specific alert-triggered actions. You can configure up to six event filter tables. These targets, properties, and values are valid for setting the PEF:

Target	Property
/SP/AgentInfo/PEF/EventFilterTable[1-6]/status	enable   disable
/SP/AgentInfo/PEF/EventFilterTable[1-6]/sensortype	All, Memory, Processor, Temperature, Voltage, Fan
/SP/AgentInfo/PEF/EventFilterTable[1-6]/powerctrl	enable   disable
/SP/AgentInfo/PEF/EventFilterTable[1-6]/diagnosticinterrupt	enable   disable
/SP/AgentInfo/PEF/EventFilterTable[1-6]/sendalert	enable   disable
/SP/AgentInfo/PEF/EventFilterTable[1-6]/sendmail	enable   disable



## ▼ To Configure the Event Filter Tables

1. To configure a PEF EventFilterTable target, enter the following commands:

```
-> cd /SP/AgentInfo/PEF
```

```
/SP/AgentInfo/PEF -> show
```

The result of executing the show command appears:

```
/SP/AgentInfo/PEF
```

```
Targets:
```

```
EventFilterTable1
```

```
EventFilterTable2
```

```
EventFilterTable3
```

```
EventFilterTable4
```

```
EventFilterTable5
```

```
EventFilterTable6
```

```
Properties:
```

```
PEFGlobalCtrl = enable
```

```
PEFActionGlobalCtrlPowerOff = enable
```

```
PEFActionGlobalCtrlPowerCycle = enable
```

```
PEFActionGlobalCtrlPowerReset = enable
```

```
PEFActionGlobalCtrlAlert = enable
```

```
PEFActionGlobalCtrlMail = enable
```

```
PEFActionGlobalCtrlInterrupt = enable
```

```
Target Commands:
```

```
show
```

```
cd
```

```
set
```

By examining the output of the show command, you can view the current global control configuration. If necessary use the cd and show commands to navigate to and examine the individual event filter table targets. You will need to decide which table you are going to configure.

2. When you have decided which EventFilterTable to configure, enable the table by entering the following commands:

---

**Note** – This example uses EventFilterTable1.

---

```
/SP/AgentInfo/PEF -> cd EventFilterTable1
```

```
/SP/AgentInfo/PEF/EventFilterTable1-> set status=enable
```

3. **Display EventFilterTable1 by entering the following command:**

```
/SP/AgentInfo/PEF/EventFilterTable1-> show
```

The result of executing the show command appears:

```
/SP/AgentInfo/PEF/EventFilterTable1
```

```
Targets:
```

```
Properties:
```

```
Status = enable  
SensorType = All  
PowerCtrl = disable  
DiagnosticInterrupt = disable  
SendAlert = disable  
SendMail = disable
```

```
Target Commands:
```

```
show  
set
```

Next, set the sensor type. There are six values for the sensor type: All, Memory, Processor, Temperature, Voltage, and Fan.

4. **Use the set command to configure the sensor type.**

```
set sensortype=value
```

For example, to set the temperature sensor, enter:

```
/SP/AgentInfo/PEF/EventFilterTable1-> set sensortype=Temperature
```

5. **Enable the properties or triggered actions for the sensor.**

6. **Use the set command to enable (or disable) actions. For example, to set the sendalert and sendmail actions, enter:**

```
/SP/AgentInfo/PEF/EventFilterTable1-> set sendalert=enable
```

```
/SP/AgentInfo/PEF/EventFilterTable1-> set sendmail=enable
```

7. When you are finished, use the `show` command to verify the PEF configuration:

```
/SP/AgentInfo/PEF/EventFilterTable1-> show
```

The output from the command appears:

```
/SP/AgentInfo/PEF/EventFilterTable1
Targets:

Properties:
  Status = enable
  SensorType = temperature
  PowerCtrl = disable
  DiagnosticInterrupt = disable
  SendAlert = enable
  SendMail = enable

Target Commands:
  show
  set
```

In the example above, `EventFilterTable1` is enabled to activate the `SendAlert` and `SendMail` actions, based on temperature related alerts.

---

## Displaying Version Information

You can display active session, current versions, and other information about the SP using the CLI.

### To Display the Current SP Version Information

- To display the current SP version, enter the following command:  
**version**

---

# Updating the Firmware

You can use CLI to update the SP firmware. Updating the ELOM from the command line enables you to update both the SP firmware and the BIOS at the same time. If you are using the CLI to update the firmware, a TFTP server is required.

## ▼ To Update the Firmware



---

**Caution** – Power interruptions during the update process could leave the SP in a unbootable or nonrecoverable state. Before upgrading your firmware, ensure that you have reliable power and protect against accidental power interruptions.

---

---

**Note** – The upgrade takes about 5 minutes to complete, depending on network traffic. During this time, no other tasks can be performed in the Embedded Lights Out Manager software.

---

1. **Copy the combined image from the Tools and Driver CD to your TFTP server.**  
The image is located in the `/remoteflash` directory.
2. **If the server OS is running, perform a clean shutdown.**
3. **Log in to the CLI and change to the `TftpUpdate` directory:**

```
/SP ->cd TftpUpdate
```

---

**Note** – A network failure during the file upload will result in a timeout. This causes the SP to reboot with the prior version of the firmware.

---

4. **Enter the following command to set the IP address of the TFTP server:**

```
/SP/TftpUpdate -> set ServerIP=n.n.n.n
```

*n.n.n.n* The server IP address.

5. **Enter the following command to set the file name of the combined `bmc.bios` image:**

```
/SP/TftpUpdate ->set Filename=filename
```

*filename* The name of the file in the `/remoteflash` directory (for example: **x4150-10\_3A01**)

a. **To update the firmware, enter one of the following commands:**

- To erase BIOS settings and load optimized defaults (recommended):

```
/SP/TftpUpdate -> set BIOSCMOS=notsave
```

---

**Note** – A hardware procedure for clearing the NVRAM is available in the server service manual.

---

- To preserve the BIOS CMOS settings for all subsequent updates:

```
/SP/TftpUpdate -> set BIOSCMOS=save
```

**6. Start the TFTP download:**

```
/SP/TftpUpdate -> set Update=action
```

After you enter this command, the system displays the current firmware version and the upgrade version and prompts for confirmation.

**7. Select Yes to continue, or No to exit.**



# Using Simple Network Management Protocol

---

This chapter describes how to use Simple Network Management Protocol (SNMP). It includes the following sections:

- [“About SNMP” on page 103.](#)
- [“SNMP MIB Files” on page 104.](#)
- [“MIBs Integration” on page 104.](#)
- [“SNMP Messages” on page 105.](#)
- [“Configuring SNMP on the ELOM” on page 106.](#)
- [“Managing SNMP User Accounts” on page 106.](#)

---

## About SNMP

The Sun server supports the Simple Network Management Protocol (SNMP) interface, versions 1, 2c, and 3. SNMP is an open technology that enables the management of networks and devices, or nodes, connected to the network. SNMP messages are sent over IP using the User Datagram Protocol (UDP). Any management application that supports SNMP can manage your server.

## How SNMP Works

Utilizing SNMP requires two components, a network management station and a managed node (in this case, the ELOM). Network management stations host management applications, which monitor and control managed nodes.

Managed nodes are any number of devices, including servers, routers, and hubs, that host SNMP management agents responsible for carrying out the requests from management stations. The management station monitors nodes by polling management agents for the appropriate information using queries. Managed nodes can also provide unsolicited status information to a management station in the form of a trap. SNMP is the protocol used to communicate management information between the management stations and agents.

The SNMP agent is preinstalled and runs on the ELOM, so all SNMP management of the server should occur through the ELOM. To utilize this feature, your operating system must have an SNMP client application. See your operating system vendor for more information. The SNMP agent on your ELOM provides inventory management and sensor and system state monitoring capabilities.

---

## SNMP MIB Files

The base component of an SNMP solution is the management information base (MIB). MIB is a text file that describes a managed node's available information and where it is stored. When a management station requests information from a managed node, the agent receives the request and retrieves the appropriate information from the MIBs. The Sun server supports the following MIB files. Download and install the MIB files from the Tools and Drivers CD. The files are located in the `/SNMP/mib` directory.

- The system group and SNMP group from RFC1213 MIB
- SNMP-FRAMEWORK-MIB
- SNMP-USER-BASED-MIB
- SNMP-MPD-MIB
- SUN-PLATFORM-MIB
- ENTITY-MIB

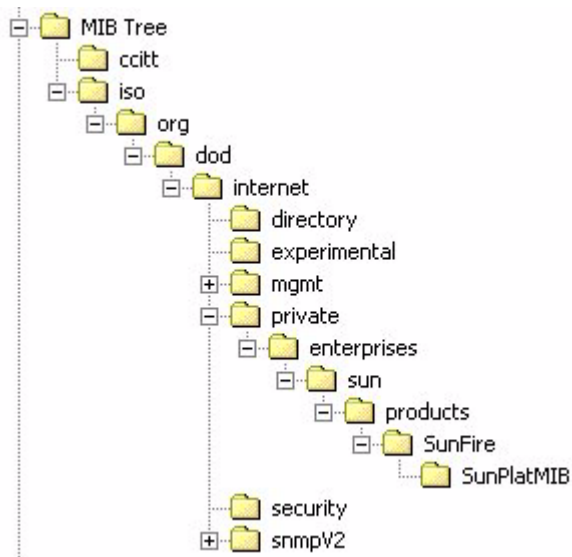
---

## MIBs Integration

Use the MIBs to integrate the management and monitoring of the server into SNMP management consoles. The MIB branch is a private enterprise MIB, located at MIB object iso(1).org (3). dod (6).internet (1).private (4).enterprises (1).sun (42).products (2). See [FIGURE 8-1](#). The standard SNMP port, 161, is used by the SNMP agent on the ELOM.



**FIGURE 8-1** Sun Server MIB Tree



---

## SNMP Messages

SNMP is a protocol, not an operating system, so you need some type of application to use SNMP messages. Your SNMP management software might provide this functionality, or you can use an open-source tool like net-SNMP, which is available at <http://net-snmp.sourceforge.net/>.

Both management stations and agents use SNMP messages to communicate. Management stations can send and receive information. Agents can respond to requests and send unsolicited messages in the form of a trap. There are five functions that management stations and agent, use:

- Get
- GetNext
- GetResponse
- Set
- Trap

By default, port 161 is used for SNMP messages, and port 162 is used to listen for SNMP traps.

---

# Configuring SNMP on the ELOM

The ELOM has a preinstalled SNMP agent that supports trap delivery to an SNMP management application.

To use this feature, you must integrate the platform-specific MIBs into your SNMP environment, tell your management station about your server, then configure the specific traps.

## Adding Your Server to Your SNMP Environment

Add your Sun server as a managed node using your SNMP management application. See your SNMP management application documentation for further details.

## Configuring Receipt of SNMP Traps

Configure a trap in your ELOM. See [“Managing Alerts” on page 92](#), or [“Configuring E-mail Notification” on page 30](#).

---

# Managing SNMP User Accounts

You can add, delete, or configure SNMP user accounts from the CLI. By default, SNMP v3 is enabled, and SNMP v1 and v2c are disabled.

## Adding a User Account

To add an SNMP v3 read-only user account, enter the following command:

```
create /SP/AgentInfo/SNMP/user/username authenticationpassword=  
password
```

To add an SNMP v1/v2c user account, enter the following command:

```
create /SP/AgentInfo/SNMP/communities/communityname
```

# Deleting a User Account

To delete an SNMP v3 user account, enter the following command:

```
delete /SP/AgentInfo/SNMP/user/username
```

To delete an SNMP v1/v2c user account, enter the following command :

```
delete /SP/AgentInfo/SNMP/communities/communityname
```

# Configuring User Accounts

To configure SNMP user accounts, use the `set` command

## *Syntax*

```
set target [propertyname=value]
```

## *Targets, Properties, and Values*

These targets, properties, and values are valid for SNMP user accounts.

**TABLE 8-1** SNMP Targets, Properties, and Values

Target	Property	Value	Default
<code>/SP/AgentInfo/SNMP/communities/ communityname</code>	Permission	ro rw	ro
<code>/SP/AgentInfo/SNMP/users/username</code>	AuthProtocol	MD5 SHA	MD5
	AuthPassword	string	(Null string)
	Permission	ro rw	ro
	PrivacyProtocol	None DES	None*
	PrivacyPassword	string	(Null string)

\* If the PrivacyProtocol property has a value other than none, then PrivacyPassword must be set.

## *Examples*

```
-> set /SP/AgentInfo/SNMP/users/al privacyprotocol=DES
```

---

**Tip** – To reduce the length of commands, navigate to the target first using the `cd` command.

---

```
-> cd /SP/AgentInfo/SNMP/users/albert
-> set PrivacyProtocol=DES
-> set PrivacyPassword=password AuthProtocol=SHA AuthPassword=
password
```

---

**Note** – You can change SNMP user permissions without resetting the privacy and authentication properties.

---

To show an SNMP user's properties, Enter this command:

```
-> show
```

The result appears as follows:

```
/SP/AgentInfo/SNMP/users/sicilian
Targets:
Properties:
    Permission = ro
    AuthProtocol = MD5
    AuthPassword = (Cannot show property)
    PrivacyProtocol = none
    PrivacyPassword = (Cannot show property)

Target Commands:
    show
    set

/SP/AgentInfo/SNMP/users/sicilian ->
```

# Command-Line Interface Reference

---

This chapter contains the most common Embedded Lights Out Manager (ELOM) commands used to administer your Sun server from the command-line interface (CLI). This chapter contains the following sections:

- [“CLI Command Quick Reference” on page 109.](#)
- [“CLI Command Reference” on page 113.](#)
- [“Properties and Values for Targets” on page 122](#)

---

## CLI Command Quick Reference

The following tables provide a quick reference to the most common ELOM CLI commands.

**TABLE A-1** Command Syntax and Usage

Content	Typeface	Description
Your input	<b>Fixed-width bold</b>	Text that you type into the computer. Type it in exactly as shown.
Onscreen output	Fixed-width regular	Text that the computer displays.
Variable	<i>Italic</i>	Replace these with a name or value you choose.
Square brackets, [ ]		Text in square brackets is optional.
Vertical bars,		Text separated by a vertical bar represents the only available values. Select one.

**TABLE A-2** General Commands

Description	Command
Log out of the CLI.	<code>exit</code>
Display the version of the ELOM firmware running on the SP.	<code>version</code>
Display information about commands and targets.	<code>help</code>
Display information about a specific command.	<code>help show</code>

**TABLE A-3** User Commands

Description	Command
Add a local user.	<code>create /SP/users/user1</code>
Set or change password.	<code>set /SP/users/username Password=password</code>
Set or change permission.	<code>set /SP/users/username Permission=operator administrator user callback</code>
Delete a local user named user1.	<code>delete /SP/users/user1</code>
Change the permission level of a local user named user1.	<code>set /SP/users/user1 Permission=operator</code>

**TABLE A-4** Network and Serial Port Setting Commands

Description	Command
Display network configuration information.	<code>show /SP/network</code>
Change network properties for the ELOM. Changing certain network properties, like the IP address, will disconnect your active session.	<code>set /SP/network IPAddress=xxx.xxx.xxx.xxx NetMask=xxx.xxx.xxx.xxx Gateway=xxx.xxx.xxx.xxx</code>
Set DHCP or change to static settings.	<code>set /SP/network IPSource=dhcp static</code>

**TABLE A-5** Alert Commands

Description	Command
Display information about PET alerts Destination1.	<b>show /SP/AgentInfo/PET/Destination1</b>
Change alert configuration.	<b>set /SP/AgentInfo/PET/Destination[n] IPAddress=ipaddress</b>

**TABLE A-6** SNMP Commands

Description	Command
Display information about SNMP settings. By default, the SNMP port is 161, and v3 is enabled.	<b>show /SP/AgentInfo/SNMP port=snmpportnumber set=enabled disabled version1=enabled disabled version2c=enabled disabled version3=enabled disabled</b>
Display SNMP users.	<b>show /SP/AgentInfo/SNMP/user</b>
Add an SNMP user.	<b>create /SP/AgentInfo/SNMP/user/snmpusername AuthPassword=password AuthProtocol=MD5 SHA Permission=rw ro PrivacyPassword=password PrivacyProtocol=none DES</b>
Delete an SNMP user.	<b>delete /SP/AgentInfo/SNMP/user/snmpusername</b>
Display information about SNMP public (read-only) communities.	<b>show /SP/AgentInfo/SNMP/communities/public</b>

**TABLE A-7** System Start, Stop, and Reset Commands

Description	Command
Start the host system.	<b>set /SYS/CtrlInfo PowerCtrl=on</b>
Stop the host system.	<b>set /SYS/CtrlInfo PowerCtrl=off</b>
Stop the host system gracefully.	<b>set /SYS/CtrlInfo PowerCtrl=gracefuloff</b>

**TABLE A-7** System Start, Stop, and Reset Commands *(Continued)*

Description	Command
Reset the host system.	<b>set /SYS/CtrlInfo PowerCtrl=reset</b>
Start a session to connect to the host console.	<b>start /SP/AgentInfo/Console</b>
Stop the session connected to the host console.	<b>stop /SP/AgentInfo/Console</b>



---

# CLI Command Reference

This section provides reference information about the CLI commands.

## cd

Use the `cd` command to navigate the namespace. When you use `cd` to change to a target location, that location then becomes the default target for all other commands.

Using the `- default` option with no target returns you to the top of the namespace. Typing just `cd` displays your current location in the namespace. Typing `help targets` displays a list of all targets in the entire namespace.

### *Syntax*

**cd** *target*

### *Options*

**[-h|help]**

### *Targets and Properties*

Any location in the namespace.

### *Examples*

To create a user named **sally**, use `cd` to change to `/SP/User`, then execute the `create` command with `/SP/User` as the default target.

```
SP-> cd /SP/User
```

```
SP-> create sally
```

## create

Use the `create` command to set up an object in the namespace. Unless you specify properties with the `create` command, they are empty.

### *Syntax*

```
create [options] target [propertyname=value]
```

### *Options*

```
[-h|help]
```

### *Targets, Properties, and Values*

**TABLE A-8** Create command Targets, Properties, Values, and Defaults

Valid Targets	Properties	Values	Default
<i>/SP/User/username</i>	password	<i>string</i>	(None)
	permission	administrator   operator   user   callback	operator
<i>/SP/SNMP/communities/ communityname</i>	Permissions	ro   rw	ro
<i>/SP/SNMP/communities/user/ username</i>	AuthProtocol	MD5	MD5
	AuthPassword	<i>string</i>	(Null string)
	Permissions	ro   rw	ro
	PrivacyProtocol	none   DES	DES
	PrivacyPassword	<i>string</i>	(Null string)

### *Example*

```
-> create /SP/User/susan role=administrator
```

# delete

Use the `delete` command to remove an object from the namespace. You are not prompted to confirm a `delete` command.

Eliminate this prompt by using the `-script` option.

## *Syntax*

**delete** [*options*] *target*

## *Options*

**[-h|help]**

## *Targets*

**TABLE A-9** delete Command Targets

---

**Valid Targets**

---

*/SP/User/username*

*/SP/SNMP/communities/communityname*

*/SP/SNMP/communities/user/username*

---

## *Examples*

-> **delete /SP/User/susan**

-> **delete /SP/SNMP/communities/johnny**

# exit

Use the `exit` command to terminate a session to the CLI.

## *Syntax*

**exit** [*options*]

## Options

**[-h|help]**

## help

Use the `help` command to display Help information about commands and targets. Using the `-output terse` option displays usage information only. The `-output verbose` option displays usage, description, and additional information including examples of command usage. If you do not use the `-output` option, usage information and a brief description of the command are displayed.

Specifying command *targets* displays a complete list of valid targets for that command from the fixed targets in */SP*. Fixed targets are targets that cannot be created by a user.

Specifying command *targets legal* displays copyright information and product use rights.

## Syntax

**help** [*options*] **command** [*targets*]

## Options

**[-h|help]**

## Commands

**cd, create, delete, exit, help, load, reset, set, show, start, stop, version**

## Examples

-> **help load**

Use the `load` command to transfer a file from a server and update a target.

Usage: **load -source URL** [*target*]

`-source`: specific the location to get a file

-> **help reset**

Use the reset command to reset a target.

Usage: reset **[-script] [target]**

Available options for this command:

**-script** : do not prompt for yes/no confirmation, and act as if yes was specified.

## set

Use the set command to change the value of a property associated with a target.

### *Syntax*

**set [target] property=value [propertyname=value]**

### *Options*

**[-h help]**

### *Targets, Properties, and Values*

**TABLE A-10** set Command Targets, Properties, and Values

Valid Targets	Properties	Values	Default
<b>/SP/User/username</b>	password	<i>string</i>	(None)
	permission	administrator   operator	operator
<b>/SP/clock</b>	Date	MM/DD/YYYY	/SP/clock
	Time	hh:mm:ss	
	NTPstatus	enabled   disabled	
	NTPserver	<i>ipaddress</i>	
<b>/SP/AgentInfo/SNMP</b>	port	<i>decimal</i>	161
	snmpset	enabled   disabled	disabled
	version1	enabled   disabled	disabled
	version2	enabled   disabled	disabled
	version3	enabled   disabled	enabled

**TABLE A-10** set Command Targets, Properties, and Values (Continued)

Valid Targets	Properties	Values	Default
<b>/SP/AgentInfo/SNMP community</b> /communityname	Permission	ro   rw	ro
<b>/SP/AgentInfo/SNMP/user</b> /username	AuthProtocol	MD5   SHA	MD5
	AuthPassword	string	(Null string)
	Permission	ro   rw	ro
	PrivacyProtocol	none   DES	DES
	PrivacyPassword	string	(null string)
<b>/SP/network</b>	IIPAddress	IP address   none	(None)
	DNS	IP address   none	(None)
	IPSource	dhcp   static	dhcp
	Gateway	IP address   none	(None)
	Netmask	IP dotted decimal	xxx.xxx.xxx.xxx

### Examples

```
-> set /SP/users/susan permission=administrator
```

### show

Use the show command to display information about targets and properties.

The show command is used to display information about managed elements. It can be used to view information about single managed elements, a tree of managed elements, or managed elements matching a property value filter.

The `-level` option controls the depth of the show command, and it applies to all modes of the `-display` option. Specifying `-level 1` displays the level of the namespace where the object exists. Values greater than 1 return information for the target's current level in the namespace and the *specified value* levels below. If the argument is `-level all`, it applies to the current level in the namespace and everything below.

### Syntax

```
show [options] target [propertyname]
```

## Options

**[-h|help]**

## Targets and Properties

## Examples

->**show /SP/network** (This is the only valid command as it displays all parameters)

```
/SP/network
```

Targets:

```
Target Commands:  
  show  
  set
```

## start

Use the `start` command to turn on the target or to initiate a connection to the host console.

## Syntax

**start [options] target**

## Options

**[-h|help]**

## Targets

**TABLE A-11** start Command Target

Valid Target	Description
/SP/AgentInfo/Console	Starts an interactive session to the console.

## Examples

```
-> start /SP/AgentInfo/Console
```

## stop

Use the `stop` command to shut down the target or to terminate another user's connection to the host console. You will be prompted to confirm a `stop` command. Eliminate this prompt by using the `-script` option.

## Syntax

```
stop [options] target
```

## Options

```
[-h|help] [-s|script]
```

## Targets

**TABLE A-12** stop Command Target

Valid Target	Description
/SP/AgentInfo/Console	Terminate another user's connection to the host console.

## Examples

```
-> stop /SP/AgentInfo/Console
```

## reset

Use the `reset` command to reset the target's state. This command can be used with and without options.



## *Syntax*

**reset** [*target*]

## *Options*

**[-h|help]**

## *Example*

-> **reset /system3**

# version

Use the `version` command to display ELOM version information.

## *Syntax*

**version**

## *Options*

**[-x|examine] [-h|help]**

## *Example*

-> **version**

```
version SP firmware version: 1.0.0
SP firmware build number: 4415
SP firmware date: Mon Mar 28 10:39:46 EST 2005
SP filesystem version: 0.1.9
```

---

# Properties and Values for Targets

This section contains all the properties and values for each target.

## Targets and Verbs

Targets and verbs for / and /SP/ are shown below:

Relative Targets	Supported Verbs											
	cd	exit	help	load	create	delete	Set	show	start	stop	reset	version
/	x	x	x				x	x				x
/SP/	x	x	x	x			x	x			x	x

### /SP/

Properties, values, and access for /SP/ are shown below:

Property Name	Valid Value	Access	Description
Firmwareversion	N/A	R	firmware version
Timeout	N/A	R/W	timeout value of CLI session
CPLDVersion	N/A	R	display CPLD version

## User

The user target is used to change and display information on the access rights of individual users. A user is selected via her or his user name. When the configurations have been modified by CLI. Targets and verbs for user are shown below:

Relative Targets	Supported Verbs											
	cd	exit	help	load	create	delete	Set	show	start	stop	reset	version
/SP/user	x	x	x				x	x				x
/SP/user/username	x	x	x	x			x	x			x	x

## /SP/user/username

Properties, values, and access for /SP/user/username are shown below:

Property Name	Valid Value	Access	Description
status	enable, disable	R/W	status of this user
permission	administrator, operator, user, callback	R/W	permission of this user
password	STRING	W	password of this user

## Network

### Targets and Verbs

Targets and verbs for /SP/network are shown below:

Relative Targets	Supported Verbs											
	cd	exit	help	load	create	delete	Set	show	start	stop	reset	version
/SP/network	x	x	x									

## /SP/network

Properties, values, and access for /SP/network are shown below:

Property Name	Valid Value	Access	Description
MACaddress	N/A	R	Agent ethernet MAC address
IPAddress	IP ADDRESS	R/W	Configuration of the agent IP address
Netmask	IP ADDRESS	R/W	Configuration of the agent IP subnet mask
Gateway	IP ADDRESS	R/W	Configuration of the agent IP gateway address

Property Name	Valid Value	Access	Description
DNS	IP ADDRESS	R/W	Configuration of the agent DNS server address
IPsource	static, dhcp	R/W	Configuration of the agent IP address source
Hostname	STRING	R/W	Configuration of the agent hostname

## Targets and Verbs

Targets and verbs for /SP/clock are shown below:

Relative Targets	Supported Verbs											
	cd	exit	help	load	create	delete	Set	show	start	stop	reset	version
/SP/clock	x	x	x				x	x				x

## Clock

### /SP/clock

Properties, values, and access for /SP/clock are shown below:

Property Name	Valid Value	Access	Description
Date	MM/DD/YYYY	R/W	Date of agent
Time	hh:mm:ss	R/W	Time of agent
NTPstatus	enable, disable	R/W	Synchronize time using NTP.
NTPserver	IP ADDRESS	R/W	IP address of NTP server
TimeZoneID	Time zone id	R/W	Time zone id show in TimeZoneList
TimeZone	Time zone name	R	Time zone places of TimeZoneID show in TimeZoneList

/SP/clock/TimeZoneList

N/A

## TftpUpdate

/SP/TftpUpdate

Properties, values, and access for /SP/TftpUpdate are shown below:

Property Name	Valid Value	Access	Description
ServerIP	IP ADDRESS	R/W	Set the IP address for the TFTP server.
FileName	STRING	R/W	Set the file name for the image.
BIOSCMOS	save, notsave (w) SaveCMOS, NotSaveCMOS (r)	R/W	Flag of TftpUpdate
Update	action	W	Start the firmware and BIOS update.

## CPLDUpdate

/SP/CPLDUpdate

Properties, values, and access for /SP/CPLDUpdate are shown below:

Property Name	Valid Value	Access	Description
ServerIP	IP ADDRESS	R/W	Set the IP address for the TFTP server.
FileName	STRING	R/W	Set the file name for the image.
CPLDUpdate	action	W	Start to update the firmware and BIOS.

# Management Agent Information

## Targets and Verbs

The targets and verbs for /SP/AgentInfo are shown below:

Relative Targets	Supported Verbs											
	cd	exit	help	load	create	delete	Set	show	start	stop	reset	version
/SP/AgentInfo	x	x	x				x	x	x	x		x
/SP/AgentInfo/ PEF	x	x	x				x	x				x
/SP/AgentInfo/ PEF/EventFilter Table[1:6]	x	x	x				x	x				x
/SP/AgentInfo/ PET	x	x	x				x	x				x
/SP/AgentInfo/ PET/Destination [1:4]	x	x	x				x	x				x
/SP/AgentInfo/ SEL	x	x	x				x	x				x
/SP/AgentInfo/ Console	x	x	x						x	x		x
/SP/AgentInfo/ Mail	x	x	x				x	x				x
/SP/AgentInfo/ Mail/receiver[1: 10]	x	x	x				x	x				x
/SP/AgentInfo/ SNMP	x	x	x				x	x				x
/SP/AgentInfo/ SNMP/communi- ties	x	x	x		x	x	x	x				x
/SP/AgentInfo/ SNMP/users	x	x	x		x	x	x	x				x

## /SP/AgentInfo/PEF

Properties, values, and access for /SP/Agent/PEF are shown below:

Property Name	Valid Value	Access	Description
PEFGlobalCtrl	enable, disable	R/W	PEF global control switch
PEFActionGlobalCtrlPowerOff	enable, disable	R/W	PEF action global control – power
PEFActionGlobalCtrlPowerCycle	enable, disable	R/W	PEF action global control – power
PEFActionGlobalCtrlPowerReset	enable, disable	R/W	PEF action global control – power
PEFActionGlobalCtrlAlert	enable, disable	R/W	PEF action global control – alert
PEFActionGlobalCtrlMail	enable, disable	R/W	PEF action global control – mail
PEFActionGlobalCtrlInterrupt	enable, disable	R/W	PEF action global control – interrupt

## /SP/Agent/PEF/EventFilterTable[1:6]

Properties, values, and access for /SP/AgentInfo/PEF/EventFilterTable[1:6] are shown below:

Property Name	Valid Value	Access	Description
Status	enable, disable	R/W	Enable/Disable this table
Sensortype	all, voltage, temperature, memory	R/W	Event filter sensor type
powerctrl	PowerOff, PowerReset, PowerCycle, disable	R/W	Event action – power
diagnosticInterrupt	enable, disable	R/W	Event action – interrupt
sendalert	enable, disable	R/W	Event action – alert
sendmail	enable, disable	R/W	Event action – mail

## /SP/AgentInfo/PET/Destination[1:4]

Properties, values, and access for /SP/AgentInfo/PET/Destination[1:4] are shown below:

Property Name	Valid Value	Access	Description
IP	IP ADDRESS	R/W	PET IP Address

## /SP/AgentInfo/SEL/

Properties, values, and access for /SP/AgentInfo/SEL are shown below:

Property Name	Valid Value	Access	Description
CearEventlog	action	R/W	Clear event logs

## /SP/AgentInfo/Mail

Properties, values, and access for /SP/AgentInfo/Mail are shown below:

Property Name	Valid Value	Access	Description
SMTPServer	IP ADDRESS	R/W	SMTP server IP address
Sender	STRING	R/W	Mail notification sender
ClearSMTPServer	action	W	Clear SMTP server IP address
ClearSender	action	W	Clear Mail notification sender

## /SP/AgentInfo/Mail/receiver[1:10]

Properties, values, and access for /SP/AgentInfo/Mail/receiver[1:10] are shown below:

Property Name	Valid Value	Access	Description
EmailAddress	MAIL ADDRESS	R/W	Receiver mail address
ClearReceiver	action	W	Clear the mail address



## /SP/AgentInfo/SNMP

Properties, values, and access for /SP/AgentInfo/SNMP are shown below:

Property Name	Valid Value	Access	Description
port	INTEGER(0-65535)	R/W	SNMP daemon port
snmpset	enable, disable	R/W	SNMP management information settable
version1	enable, disable	R/W	SNMP protocol version 1 support
version2c	enable, disable	R/W	SNMP protocol version 2c support
version3	enable, disable	R/W	SNMP protocol version 3 support

## /SP/AgentInfo/SNMP/communities/community

Properties, values, and access for /SP/AgentInfo/SNMP/communities/community are shown below:

Property Name	Valid Value	Access	Description
Permission	ro, rw	R/W	SNMP community permission

## /SP/AgentInfo/SNMP/users/user

Properties, values, and access for /SP/AgentInfo/SNMP/users/user are shown below:

Property Name	Valid Value	Access	Description
Permission	ro, rw	R/W	SNMP user permission
AuthProtocol	MD5, SHA	R/W	SNMP v3 user authentication protocol
AuthPassword	STRING	W	SNMP v3 user authentication protocol
PrivacyProtocol	none, DES	R/W	SNMP v3 user privacy protocol
PrivacyPassword	STRING	W	SNMP v3 user privacy password

# System Information

The System Information contains board, product, chassis, CPU, memory module, and health information. It also allows you to control the power state.

## Targets and Verbs

The targets and verbs for /SYS/ are shown below:

Relative Targets	Supported Verbs											
	cd	exit	help	load	create	delete	Set	show	start	stop	reset	version
/SYS	x	x	x					x				x
/SYS/BoardInfo	x	x	x					x				x
/SYS/CtrlInfo	x	x	x					x				x
/SYS/CPU	x	x	x					x				x
/SYS/CPU/CPU[1:N]	x	x	x					x				x
/SYS/MemModule	x	x	x					x				x
/SYS/MemModule/MemModule[1:N]	x	x	x					x				x
/SYS/NICInfo0	x	x	x					x				x
/SYS/NICInfo1	x	x	x					x				x
/SYS/Fan	x	x	x					x				x
/SYS/Fan/Fan[1:N]	x	x	x					x				x
/SYS/Temperature	x	x	x					x				x
/SYS/Temperature/Temperature[1:N]	x	x	x					x				x
/SYS/Voltage	x	x	x					x				x
/SYS/Voltage/Voltage[1:N]	x	x	x					x				x

## /Sys/BoardInfo

Properties, values, and access for /SYS/BoardInfo are shown below:

Property Name	Valid Value	Access	Description
BIOSVersion	-	R	Display the BIOS version.
BoardMfgDateTime	-	R	Displays the date of manufacture for the management board.
BoardProductName	-	R	Displays the product name of the management board.
BoardSerialNumber	-	R	Displays the serial number of the management board.

## /SYS/CtrlInfo

Properties, values, and access for /SYS/CtrlInfo are shown below:

Property Name	Valid Value	Access	Description
PowerStatus	on, off	R	Displays the power status.
PowerCtrl	on, off, gracefuloff, reset	W	Control power.
BootCtrl	regular, PXE, BIOSSetup, PCCheck_enable, PCCheck_disable	RW	Control boot and display boot status.
IdLedCtrl	on, off	RW	Control IdLed and display IdLed status.

## /SYS/CPU/CPU[0:N]

Properties, values, and access for /SYS/CPU/CPU[1:N] are shown below:

Property Name	Valid Value	Access	Description
SocketDesignation	-	R	Displays the CPU socket designation.
Manufacturer	-	R	Displays the CPU manufacturer.

Property Name	Valid Value	Access	Description
Name	-	R	Displays the CPU name.
Speed	-	R	Displays the CPU speed
Status	-	R	Displays the CPU status

## /SYS/NICInfo0

Properties, values, and access for /SYS/NICInfo0 are shown below:

Property Name	Valid Value	Access	Description
Name	-	R	Displays the NIC name.
PartNumber	-	R	Displays the NIC part number.
MACAddress1	-	R	Displays the NIC MAC address 1.
MACAddress2	-	R	Displays the NIC MAD address 2.

## /SYS/NICInfo1

Properties, values, and access for /SYS/NICInfo1 are shown below:

Property Name	Valid Value	Access	Description
Name	-	R	Displays the NIC name.
PartNumber	-	R	Displays the NIC part number.
MACAddress1	-	R	Displays the NIC MAC address 1.
MACAddress2	-	R	Displays the NIC MAD address 2.

## /SYS/MemModule/MemModule[1:N]

Properties, values, and access for /SYS/MemModule/MemModule[1:N] are shown below:

Property Name	Valid Value	Access	Description
Designation	-	R	Displays the Memory Module designation.
Type	-	R	Displays the Memory Module type.
Speed	-	R	Displays the Memory Module speed.
Size	-	R	Displays the Memory Module size.

## /SYS/Fan/Fan[1:N]

Properties, values, and access for /SYS/Fan/Fan[1:N] are shown below:

Property Name	Valid Value	Access	Description
Designation	-	R	Displays the temperature designation.
Status	-	R	Displays the temperature status.
SensorReading	-	R	Displays the temperature current value.
LNCT	-	R	Displays the temperature lower warning threshold.
LCT	-	R	Displays the temperature lower critical threshold.
UNCT	-	R	Displays the temperature upper warning threshold.
UCT	-	R	Displays the temperature upper critical threshold.

## /SYS/Voltage[1:N]

Properties, values, and access for /SYS/Voltage[1:N] are shown below:

Property Name	Valid Value	Access	Description
Designation	-	R	Displays the voltage designation.
Status	-	R	Displays the voltage status.
Sensor Reading	-	R	Displays the voltage current value.
LNCT	-	R	Displays the voltage lower warning threshold.
LCT	-	R	Displays the voltage lower critical threshold.
UNCT	-	R	Displays the voltage upper warning threshold.
UCT	-	R	Displays the voltage upper critical threshold.

# Index

---

## A

- Active Directory Service (ADS), 37
- adding a user, 49
- administrator password, changing, 3
- alerts, 30
  - configuring with a web browser, 31
  - configuring with the CLI, 94

## B

- baseboard management controller (BMC), 54

## C

- CD/DVD, 68
- Certificate Signing Request (CSR), 33
- check fan status LED, 52
- CLI
  - alerts
    - configuring, 94
  - command syntax, 109
  - commands
    - alert, 111
    - cd, 113
    - character case, 84
    - command verbs overview, 85
    - create, 114
    - delete, 115
    - exit, 115
    - help, 116
    - miscellaneous, 110
    - network and serial port, 110
    - options, 85
    - set, 117

- show, 118
- start, 119
- stop, 120
- user, 110
- version, 121
- managing
  - host console, 87
  - host state, 86
  - network settings, 88
  - power state, 86
  - user accounts, 89
- namespaces, 84
- properties and values for targets, 122 to 134
- clock, setting with CLI, 117
- configuring
  - active directory service, 37
  - alerts with the CLI, 94
  - connection methods, 12
  - email notification, 30
  - network settings, 30
  - network settings with the CLI, 88
  - platform event filters, 30
  - SNMP, 34 to 37
  - SSL, 33
  - SSL certificate, 34
  - system management access, 33
  - terminal device, 6
  - user accounts with the CLI, 91
- configuring the system, 28 to 46
- connecting to the ELOM, 5
- corrupt SP, recovering from, 59
- CPU LED, 52
- cursor settings, 65

- D**
  - default SP settings, 3
  - DIMM LED, 52
- E**
  - ELOM serial connection, 6
  - e-mail, creating event triggers, 30
  - Embedded Lights Out Manager
    - definition, 2
    - namespaces, 84
    - redirecting keyboard and mouse, 66
  - event log, 23
  - events, 30
- F**
  - fault LED, 52
  - firmware, updating, 55, 100
- H**
  - hardware cursor, 65
  - hardware, redirecting
    - keyboard and mouse, 66
    - storage devices, 68
  - host, managing, 86
- I**
  - ID LED Control, 52
  - IPMI, 12
    - IPMItool, 76
    - overview, 75
    - sensors, 76
- J**
  - Java RTE, for remote console, 62
- L**
  - LED
    - check fan status LED, 52
    - CPU, 52
    - DIMM, 52
    - fault LED, 52
    - over temperature, 52
    - power supply, 52
    - top open, 52
  - LED control, 52
  - local cursor, 65
  - logging events, 23
  - logging using a web browser, 13
- M**
  - MAC address, server module level, 7
  - management information base (MIB)
    - description of, 104
  - managing alerts, CLI, 92
  - managing network settings, 88
  - mouse settings, 65
- N**
  - namespace, SP, 85
  - network, default, 118
- O**
  - over temperature LED, 52
- P**
  - password
    - default, 3
    - parameters, 50
    - set using CLI, 117
  - platform event filter (PEF), 30
  - power supply LED, 52
  - preconfigured ELOM Administrator account, 3
- R**
  - redirecting local storage, 61
  - remote client, redirecting hardware to, 62
  - remote console
    - benefits of using, 61
    - difficulty, 65
    - redirecting
      - keyboard and mouse, 66
      - storage devices, 68
    - requirements for, 61
  - remote console, Java RTE, 62
  - remote cursor, 65
  - remote storage devices, 62, 67
  - remotely updating firmware, 56
  - resetting BMC, 54
- S**
  - security certificate, 33



- sensors, IPMI, 76
- server module ELOM, connecting with serial connector, 6
- service required LED, see fault LED, 52
- setting password, CLI, 117
- SNMP, 103 to 108
  - communities, 36
  - host state, managing, 86
  - MIB and, 104
  - overview, 103
  - settings, 35
  - user accounts, 106, 107
- SP**
  - default settings, 3
  - firmware update, 55
  - logging in with a web browser, 13
  - managing network settings, 88
  - namespace, 85
  - recovering from a corrupt, 59
  - resetting, 54
  - tasks and management interfaces, 2
- SP namespace, 84
- SSL configuration, 33
- starting the remote console application, 64
- storage media
  - redirection, 62
  - remote, 67
- system panic, 54
- T**
- thresholds, 22, 23
- top open LED, 52
- U**
- updating firmware using the CLI, 100
- user accounts
  - CLI, 89
  - overview, 12
- users, SNMP, 33
- V**
- voltage thresholds, 23
- W**
- web browser login, 13
- web GUI
  - configuring
    - active directory service, 37
    - alert, 31
    - email notification, 30
    - network settings, 30
    - platform event filters, 30 to 33
    - SNMP, 34 to 37
    - SSL certificate, 34
    - system management access, 33
  - managing
    - event log, 23
    - front panel and onboard fault LEDs, 52
    - session timeout, 57
    - system locator indicator LED, 52
    - users and accounts, 46 to 51
  - monitoring
    - fans, 22
    - system sensors, 19
    - temperatures, 22
    - voltages, 23
  - power control, setting, 54
  - remote console, benefits of using, 61
  - service processor, resetting, 54
  - setting ADS, 37
  - setting time, 58
  - storage device redirection, 68
  - updating firmware, 56
  - viewing
    - component information, 17
    - event logs, 24
    - memory information, 18
    - sensor summary, 20
    - server board information, 17
    - SP version information, 16
    - the system from web browser, 14

