



Embedded Lights Out Manager Administration Guide

For the Sun Fire™ X2200 M2 and Sun Fire X2100 M2
Servers

Sun Microsystems, Inc.
www.sun.com

Part No. 819-6588-13
October 2007, Revision A

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

Copyright 2006-2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, AnswerBook2, docs.sun.com, Solaris, and Sun N1 System Manager are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

AMD Opteron is a trademark or registered trademark of Advanced Microdevices, Inc.

IBM Tivoli is a trademark or registered trademark of IBM Corp.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2006-2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054, États-Unis. Tous droits réservés.

Sun Microsystems, Inc. possède les droits de propriété intellectuels relatifs à la technologie décrite dans ce document. En particulier, et sans limitation, ces droits de propriété intellectuels peuvent inclure un ou plusieurs brevets américains listés sur le site <http://www.sun.com/patents>, un ou les plusieurs brevets supplémentaires ainsi que les demandes de brevet en attente aux les États-Unis et dans d'autres pays.

Ce document et le produit auquel il se rapporte sont protégés par un copyright et distribués sous licences, celles-ci en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Tout logiciel tiers, sa technologie relative aux polices de caractères, comprise, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit peuvent dériver des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays, licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, AnswerBook2, docs.sun.com, Solaris et Sun N1 System Manager sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface utilisateur graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox dans la recherche et le développement du concept des interfaces utilisateur visuelles ou graphiques pour l'industrie informatique. Sun détient une licence non exclusive de Xerox sur l'interface utilisateur graphique Xerox, cette licence couvrant également les licenciés de Sun implémentant les interfaces utilisateur graphiques OPEN LOOK et se conforment en outre aux licences écrites de Sun.

AMD Opteron est une marque de fabrique ou une marque déposée de Advanced Microdevices, Inc.

IBM Tivoli est une marque de fabrique ou une marque déposée de IBM Corp.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DÉCLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES DANS LA LIMITE DE LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.

Contents

Preface xv

1. Embedded Lights Out Manager Overview 1

Embedded Lights Out Manager Features 1

 ELOM Common Tasks 3

 Embedded Lights Out Manager Default Settings 4

About Sun N1 System Manager 4

2. Using the Embedded Lights Out Manager System 7

Embedded Lights Out Manager System Components 7

Accessing the Service Processor 8

Setting Up Communications 9

 Determining a DHCP Address 9

Connecting Through the Serial Port 10

 To View System Output Within CLI 11

 Setting Up Serial Over LAN 12

 Instructions for Solaris 12

 Instructions for Linux 13

Connecting Over Ethernet 14

 To View the System IP Address in the BIOS 15

To Configure Your DHCP Server	16
Finding Task Information	17
3. Setting Up the Service Processor	19
Service Processor Components	19
Powering On the Server	20
Apply Standby Power for Initial Service Processor Configuration	20
Communicating with the System SP	21
To Set Up the Service Processor with the Web-Based Interface	21
Configuring the IP Address Manually	23
4. Accessing and Monitoring the Server Using the Web-Based Interface	25
Accessing the System Using the Web-Based Interface	25
▼ To Access the System Using the Web-Based Interface	26
Using the System Information Screens	28
Getting System Version Information	28
▼ To access the Version screen	28
▼ To access the SP Version screen	29
▼ To access the Server Board Version screen	29
Setting the Session Time-out	30
▼ To Set the Session Time-out	30
Getting System Components Information	31
▼ To access the Components submenu screens	31
▼ To access the CPU screen	31
▼ To access the Memory screen	33
▼ To access the Get NIC Information screen	33
Using the System Monitoring Screens	36
Using the Sensor Reading Screens	36
▼ Monitoring the System Using the Summary Screen	36

- ▼ Diagnosing Fan Performance 38
- ▼ Diagnosing Temperature Issues 40
- ▼ Diagnosing Voltage Issues 42
- Examining, Saving, and Clearing the Event Log 44
 - ▼ To Examine the Event Logs Screen 44
- Saving the Event Log 45
 - ▼ To Save the Event Log 45
- Clearing the Event Log 45
 - ▼ To Clear the Event Log 45
- Activating the System Indicator LED 45
 - ▼ To Activate the Locator Indicator Screen 45
- Resetting the Fault LED 46
 - ▼ To Reset the Fault LED Screen 46
- 5. Configuring and Managing the Server System Using the Web-Based Interface 47**
 - Configuring the Server 47
 - Configuring the Network Settings 48
 - ▼ To access the Network Settings screen: 48
 - ▼ To configure the Network Settings manually 49
 - ▼ To configure the Network Settings using DHCP 49
 - Setting Up E-Mail Notification 50
 - ▼ To set up E-Mail Notification: 50
 - Defining Traps with the Platform Event Filter 52
 - ▼ To define traps with the Platform Event Filter screen 52
 - Setting the System Time 56
 - ▼ To set the Time screen 56
 - Enabling or Disabling Syslog 57
 - ▼ To access the Syslog screen 57

Configuring System Management Access 57

- ▼ To access the System Management Access screens 58

The SSL Certificate screen 58

- ▼ To Create a CSR 58

The SNMP Screen 59

- ▼ To access the SNMP screen 59

The SNMP Settings Screen 60

- ▼ To Configure SNMP Port and Permit 61

The SNMP Communities Screen 61

- ▼ To Add a Community 62

- ▼ To Modify a Community 63

- ▼ To Delete a Community 63

The SNMP User Settings Screen 63

- ▼ To Add an SNMP User 64

- ▼ To Edit an SNMP User 66

- ▼ To Delete an SNMP User 66

Managing Users 66

User Account 66

- ▼ To Access the User Account Screen 67

- ▼ To Add Users 68

- ▼ To Change a User Password 70

- ▼ To Change User Privilege 70

- ▼ To Disable and Enable a User 71

- ▼ To Delete a User 71

ADS Configuration 72

- ▼ To Configure ADS 72

Service Processor Maintenance 73

- ▼ To Access the Maintenance Screens 73

- ▼ To Upgrade Firmware 74
- ▼ To Reset the Service Processor 76

- 6. Using the Remote Control Screens 79**
 - About the Remote Console Application 79
 - Remote Console Operating Requirements 80
 - Launching the Remote Console Application 80
 - ▼ To Launch the Remote Console Application 81
 - Configuring KVM Functionality for a Remote Console Session 85
 - ▼ To Configure KVM Functionality for a Remote Console Session 85
 - Controlling Power to a Remote Server 89
 - Installing an Operating System on a Remote Server 90
 - ▼ To Install an OS on a Remote Server Using Virtual CDROM 91
 - Other Remote Options 92

- 7. Using IPMI 93**
 - About IPMI 93
 - IPMItool 94
 - Sensors 94
 - Supported IPMI 2.0 Commands 95

- 8. Using the Command-Line Interface 99**
 - Logging In to the CLI 99
 - ▼ To Log In Using SSH 100
 - ▼ To Log In From the Serial Port 100
 - Command Syntax 101
 - Managing the Host 103
 - Managing the Host State 103
 - Managing the Host Console 104
 - Viewing Host Sensors 104

Managing the ELOM Network Settings	105
Displaying Network Settings	105
Configuring Network Settings	105
Managing User Accounts	106
Adding a User Account	107
Deleting a User Account	107
Displaying User Accounts	107
Configuring User Accounts	107
Resetting the SP Password	108
Managing Alerts	109
Displaying Alerts	109
Configuring Alerts	110
Updating the Firmware	113
▼ How to Update the Firmware	113
Displaying Version Information	114
9. Using Simple Network Management Protocol	115
About SNMP	115
How SNMP Works	115
SNMP MIB Files	116
MIBs Integration	116
SNMP Messages	117
Configuring SNMP on the ELOM	118
Integrating the MIBs	118
▼ To use SNMP on the SP	118
Adding Your Server to Your SNMP Environment	119
Configuring Receipt of SNMP Traps	119
Managing SNMP User Accounts	119
Adding a User Account	119

Deleting a User Account 120

Configuring User Accounts 120

A. Command-Line Interface Reference 123

CLI Command Quick Reference 123

CLI Command Reference 125

cd 125

create 126

delete 127

exit 128

help 128

set 129

show 130

start 131

stop 132

version 133

Glossary 135

Index 157

Figures

FIGURE 2-1	ELOM Communications	8
FIGURE 3-1	The ELOM Login Screen	22
FIGURE 3-2	Configuration Network Submenu	24
FIGURE 4-1	The SP version Screen	26
FIGURE 4-2	The Server Board Version Screen	29
FIGURE 4-3	The Session Time-out Screen	31
FIGURE 4-4	The CPU Screen	32
FIGURE 4-5	DIMM Information Displayed in the Memory Submenu	33
FIGURE 4-6	The Get NIC Information Screen	34
FIGURE 4-7	The Summary Screen	37
FIGURE 4-8	Fan Submenu of the Hardware Monitor Screen	39
FIGURE 4-9	The Temperature Submenu	41
FIGURE 4-10	The Voltage Submenu Screen	43
FIGURE 4-11	The Event Logs Screen	44
FIGURE 4-12	The Locator Indicator Screen	46
FIGURE 5-1	The Network Settings screen	49
FIGURE 5-2	The E-mail Notification Screen	51
FIGURE 5-3	The Platform Event Filter screen	52
FIGURE 5-4	The Platform Event Filter Section	53
FIGURE 5-5	The Platform Event Filter and Trap Receiver Destination Address sections of the Platform Event Filter screen.	54

FIGURE 5-6	The Event Filter and Event Action Configuration Sections	55
FIGURE 5-7	The Time screen	56
FIGURE 5-8	The Syslogd screen	57
FIGURE 5-9	The SSL Certificate screen	58
FIGURE 5-10	The SNMP screen	60
FIGURE 5-11	The SNMP drop-down List	60
FIGURE 5-12	The SNMP Settings Screen	61
FIGURE 5-13	The SNMP Communities Screen	62
FIGURE 5-14	Community Setting Screen	62
FIGURE 5-15	The SNMP User Setting Screen	64
FIGURE 5-16	The SNMP User Setting Screen	65
FIGURE 5-17	The User Account Screen	67
FIGURE 5-18	The User and Callback Screen Limitation	69
FIGURE 5-19	The Operator System Screen Limitation	69
FIGURE 5-20	The Add User Screen	69
FIGURE 5-21	The Change User Password Screen	70
FIGURE 5-22	The Change User Privilege Screen	70
FIGURE 5-23	The ADS Configuration Screen	72
FIGURE 5-24	The Firmware Upgrade Screen	73
FIGURE 5-25	The Firmware Upgrade Screen	74
FIGURE 5-26	The Firmware Upgrade Mode Screen: Method A Selected	75
FIGURE 5-27	The Reset SP Screen	77
FIGURE 5-28	The SP Reset Screen During Reset	77
FIGURE 6-1	The ELOM System Status Screen	81
FIGURE 6-2	The Remote Console Redirection Screen	82
FIGURE 6-3	The Remote Console Screen	83
FIGURE 6-4	The Remote Console Main Menu	84
FIGURE 6-5	The Control Menu	85
FIGURE 6-6	The HotKeys Setup Window	87
FIGURE 6-7	HotKey drop-down list	88

- FIGURE 6-8 The Remote Power Control Screen 89
- FIGURE 9-1 Sun server MIB Tree 117
- FIGURE 9-2 Sun server MIB Tree 118

Preface

This *Embedded Lights Out Manager Administration Guide* provides instructions for managing Sun Fire X2100 M2 and Sun Fire X2200 M2 servers using the Embedded Lights Out Manager (ELOM) with the service processor.

The service processor (SP) is included on Sun Fire X2100 M2 and Sun Fire X2200 M2 servers. If you have one of these servers, you might also receive a supplement dealing with platform-specific differences.

How This Document Is Organized

[Chapter 1](#) describes the embedded lights out manager from an architectural standpoint, and indicates tasks that can be accomplished with the management software.

[Chapter 2](#) details the hardware connections, and the ways of communicating with your Sun Fire X2100 M2 or Sun Fire X2200 M2 server.

[Chapter 3](#) helps you in initially setting up the service processor on your Sun Fire X2100 M2 and Sun Fire X2200 M2 systems. You will only have to do this once—when you first set up your server.

[Chapter 4](#) describes how to use the web-based interface to monitor your server from the web browser with the embedded System Management software.

[Chapter 5](#) provides information about managing and controlling the Sun Fire X2100 M2 and Sun Fire X2200 M2 server system with a web browser interface to access local and remote systems.

[Chapter 6](#) describes how to use the remote console through the web-based interface.

[Chapter 7](#) describes the Intelligent Platform Interface (IPMI), and how it can be used to manage FRUs and system health independently of the operating system.

[Chapter 8](#) provides an alternative method of managing your server—through the command-line interface (CLI).

[Chapter 9](#) 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 the embedded lights out manager.

[Glossary](#) is a list of words and phrases and their definitions.

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. See the following for this information:

- Software documentation that you received with your system
- Solaris™ Operating System documentation, which is at:

<http://docs.sun.com>

Typographic Conventions

Typeface*	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. % You have mail.
AaBbCc123	What you type, when contrasted with onscreen computer output	% su 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 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 X2100 M2 and Sun Fire X2200 M2 servers, go to:

<http://docs.sun.com/app/docs/coll/x2200m2>

Translated versions of some of these documents are available at <http://docs.sun.com>. Select a language from the drop-down list, and navigate to the Sun Fire X2200 M2 server document collection using the High-End Servers and the x64 category links. Available translations for the Sun Fire X2200 M2 server 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.

Sun Documentation, Support, and Training

Sun Function	URL
Documentation	http://www.sun.com/documentation/
Support	http://www.sun.com/support/
Training	http://www.sun.com/training/

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. You can submit your comments by going to:

<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 X2100 M2 and Sun Fire X2200 M2 Servers, 819-6588-13

Embedded Lights Out Manager Overview

This chapter serves as an overview to the Embedded Lights Out Manager (ELOM). It contains the following sections:

- [“Embedded Lights Out Manager Features” on page 1](#)
- [“ELOM Common Tasks” on page 3.](#)
- [“Embedded Lights Out Manager Default Settings” on page 4](#)
- [“About Sun N1 System Manager” on page 4.](#)

Embedded Lights Out Manager Features

Embedded Lights Out Manager provides a dedicated system of hardware and supporting software that allows you to manage your Sun server independently of the operating system.

This management system is comprised of a system on a chip that includes the following:

- Service processor (SP) –This is the hardware that consists of a dedicated processor that communicates through the system serial port. The SP can also communicate through an Ethernet port that is shared with the OS.
- Embedded server management software – This is embedded software running on the SP.
- Command line interface (CLI) – The command-line interface is a dedicated software application that enables you to operate the SP and associated software using keyboard commands. You can use the command-line interface to send commands to the SP. You can connect a terminal or emulator directly to the system serial port or connect over the Ethernet using a Secure Shell (SSH).

To log in to and use the CLI, see [Chapter 8](#).

- Web-based interface - The web-based interface provides a powerful, yet easy-to-use web browser interface that allows you to log in to the SP, and perform system management, monitoring, and certain IPMI tasks. For instructions on how to use the web-based interface, see [Chapter 3](#) and [Chapter 4](#).
- Remote Console/Java™ Client – The Java Client supports the remote console functionality, which allows you to access your server’s graphical display remotely across the network, as if you were physically located there. It redirects the keyboard, mouse, and video screen, and can redirect input and output from the local machine’s CD and diskette drives. It can also redirect ISO images of the media for these devices; that is, it can create virtual devices based on media images.

For instructions on how to use the remote console, see [Chapter 6](#).

You do not need to install additional hardware or software to begin managing your Sun Fire X2100 M2 or Sun Fire X2200 M2 server with the Embedded Lights Out Manager.

Embedded LOM also supports industry-standard IPMI and SNMP management interfaces.

- Intelligent Platform Management Interface (IPMI) v2.0 – Using remote toolsets, such as the command line `ipmitool` (supplied with Solaris 10 and most Linux distributions, and also supplied on the tools and drivers CD), remote users can securely interrogate the server and carry out simple configuration changes over the network (power on, off, reset and so on). They can also access the Serial stream from the server.
- Secure Shell (SSH) v2.0 – Using conventional ssh connectivity, you can remotely access the CLI of the service processor, and interact with the industry standard DMTF SMASH Command Line Protocol provided by the SP. This CLI allows you to examine the configuration and status of the server and carry out reconfiguration operations, monitor system logs, receive reports from replaceable components, and redirect the server serial console.

For more information about IPMI, see [Chapter 7](#).

- Simple Network Management Protocol (SNMP) interface – The Embedded LOM system also provides an SNMP v3.0 interface (with limited support for SNMP v1 and SNMP v2c) for external data center management applications such as Sun N1™ System Manager, IBM® Tivoli, and Hewlett-Packard OpenView.

For more information about SNMP, see [Chapter 9](#).

Which interface you use depends on your overall system management plan and the specific tasks that you want to perform.

ELOM Common Tasks

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

TABLE 1-1 Common Tasks

Task	IPMI	Web Interface	CLI	SNMP
Redirect the system graphical console to a remote client web browser.	–	Yes	–	–
Connect a remote diskette disk drive to the system as a virtual diskette disk 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/or serial numbers.	Yes	–	Yes	Yes
Redirect the system serial console to a remote client.	Yes	No	Yes	–
Monitor system status (health check) remotely.	Yes	Yes	Yes	Yes
Interrogate system network interface cards remotely for MAC addresses.	Yes	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

Embedded Lights Out Manager Default Settings

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

TABLE 1-2 Default Settings

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

About Sun N1 System Manager

If you plan to manage your server as one resource in a comprehensive data center management solution, Sun N1 System Manager provides an alternative resource. This software suite provides advanced features that enable you to monitor, maintain, and provision multiple Solaris™, Linux, and Microsoft Windows servers in your data center.

Note – Version 1.3.1 of Sun N1 System Manager does not support Sun Fire X2100 M2 or Sun Fire X2200 M2 servers. Although these systems are recognized by the software, customers should upgrade to v1.3.2 (or later versions) of Sun N1 System Manager for Sun Fire X2100 M2 or Sun Fire X2200 M2 server support.

The Sun N1 System Manager is available to download from:

www.sun.com/software/solaris/get.jsp

You can also install it from the Sun N1 System Manager DVD shipped in your system box. This software suite is installed on a dedicated server in your data center and enables one or more remote management clients to perform the following tasks on multiple managed servers:

- Manage multiple servers—Configure, provision, deploy, manage, monitor, patch, and update from one to hundreds of Sun servers

- Monitor system information—System manufacturer, make, model, serial number, management MAC addresses, disk information, and platform CPU and memory information
- Manage power remotely—Power off, power on, power reset, and power status
- Manage lights-out management and BIOS—Information about system LOM firmware, and version. You can also perform remote upgrades to firmware on LOM
- Control system boot commands and options—Remote boot control via IPMI and the serial console tool provided with N1 SM to remotely map boot devices and boot options
- Manage remote system health checks—Information about the status of a server
- Manage operating systems—Deploy, monitor, and patch both Solaris and Linux operating systems
- Perform bare-metal discovery.

To learn more about this suite of powerful data center management tools, go to:

http://www.sun.com/software/products/system_manager/

Using the Embedded Lights Out Manager System

This chapter assumes that you have your server cabled, powered on, and the operating system installed. Setting up and cabling your system is covered in your server operating system installation guide. If you have not completed these steps, please return to the server operating system installation guide appropriate for your platform.

This chapter includes the following sections:

- [“Embedded Lights Out Manager System Components” on page 7](#)
- [“Accessing the Service Processor” on page 8](#)
- [“Setting Up Communications” on page 9](#)
- [“Connecting Through the Serial Port” on page 10](#)
- [“Connecting Over Ethernet” on page 14](#)
- [“Finding Task Information” on page 17](#)

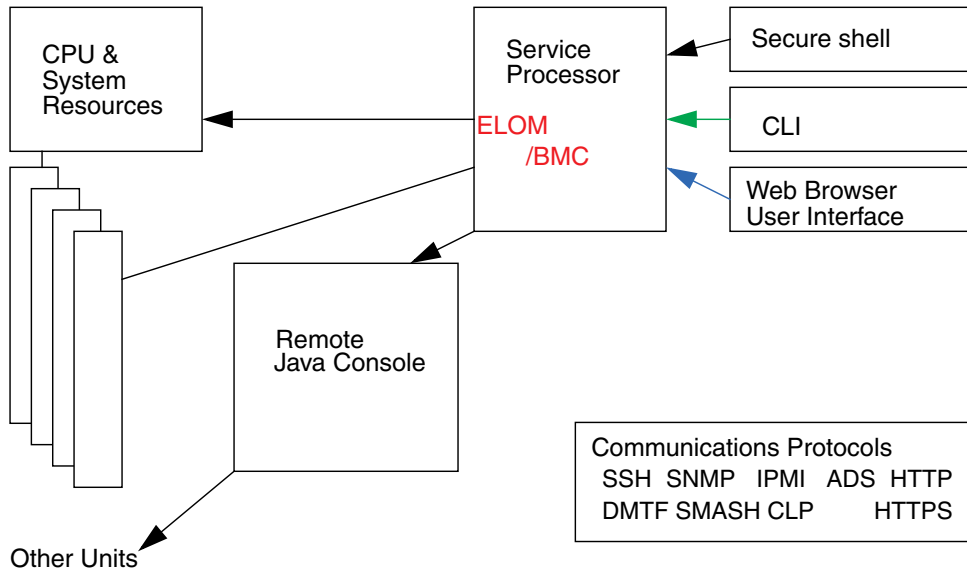
Embedded Lights Out Manager System Components

The embedded lights out manager (ELOM) system provides an embedded service processor (SP), flash memory, RAM, separate Ethernet interfaces, and server management software. This server management software provides superior management tools to help you administer local or remote servers efficiently.

You can use the web-based interface, the command-line interface (CLI), SNMP integration with third-party frameworks, or IPMI to configure and manage the platform through the SP.

The dedicated SP provides complete operating system independence and maximum availability of server management. Through the integrated service processor you can configure and manage the server hardware, firmware, and associated applications from a single point of entry.

FIGURE 2-1 ELOM Communications



Accessing the Service Processor

Make sure your server system is properly set up and cabled. See your platform documentation for instructions on installing the hardware and cabling and for instructions on powering on the server. Your point of entry to the system is the service processor (SP).

You can access the SP on your server from your laptop or from a workstation or PC.

- You can gain access using a serial port. To use the serial port, connect a serial null modem cable to the “SERIAL MGT” connector. See [“Connecting Through the Serial Port”](#) on page 10.
- You can gain access using a server Ethernet port. To do this, make sure your Ethernet cables are connected to the “NET” connectors as required for your Gigabit Ethernet or a management network. The connectors labeled “LAN-0”

through “LAN-*n*” are Gigabit Ethernet ports. The port labeled “LAN1 NET MGT” is a 10/100/1000 Ethernet port that can connect your system to a management network. For more information about connecting over the Ethernet, see [“Connecting Over Ethernet” on page 14](#).

To begin, apply only standby power to your server to access the service processor. Setting up the SP is covered in [Chapter 3](#).

Setting Up Communications

From the system serial port or the dedicated Ethernet port you will be able to communicate with the service processor’s ELOM in several ways.

- You can run the command-line interface (CLI) connected directly to the serial port.
- You can run both the web-based interface and the CLI through the Ethernet port. This enables you to use SSH and IPMI commands. Connecting with the Ethernet port requires some configuration.

Determining a DHCP Address

Dynamic Host Configuration Protocol (DHCP) is a powerful tool in connecting to the Ethernet because it automatically assigns IP addresses, subnet masks, default routers, and other IP parameters. Your embedded lights out manager is shipped with DHCP enabled by default.

Note – If the IP address assigned to the 10/100 ELOM Ethernet port by DHCP is known, the 10/100 ELOM Ethernet port can be accessed without using the Serial A port.

TABLE 2-1

If a DHCP Server is Present	If a DHCP Server is Not Present
Obtain an IP address using serial port: See “Connecting Through the Serial Port” on page 10	Change IP address using serial port: See “Connecting Through the Serial Port” on page 10
To view the IP address in System BIOS: See “To View the System IP Address in the BIOS” on page 15.	
To view IP address from DHCP server: See “To Configure Your DHCP Server” on page 16	Configure system using SSH or web-based interface: See “Managing the ELOM Network Settings” on page 105 and “Accessing the System Using the Web-Based Interface” on page 25

Connecting Through the Serial Port

See your platform documentation for instructions on installing the hardware and cabling and for applying standby power to your server.

1. **Open a terminal window to connect to the ELOM service processor through the serial port.**
 - a. **On Solaris, issue the command `tip -9600 /dev/term/a` to connect through serial port A.**
 - b. **On Windows, use `hypertrm`. The settings should be 9600, 8, N, 1.**
2. **Press Enter on the terminal device.**

This will make the service processor issue a login prompt.

3. To log in to the CLI:

- a. Enter the default user name, **root**.
- b. Enter the default password, **changeme**.

Once you have successfully logged in, the service processor displays the SP default command prompt:

```
SP->
```

You can now run CLI commands (see [Appendix A](#) for a list of commands).

By default each new system comes with the IP address and DHCP enabled. [Step 4](#) explains what to do if the DHCP is not enabled. Change the IP address if you need a different static IP address.

Note – If you connect a terminal or emulator to the serial port before it has been powered up or during its power up sequence, you will see bootup messages.

4. Do one of the following, depending on whether the DHCP server is present:

- If no DHCP server is present, enter the following commands to assign an IP address to the ELOM SP. You must run the `set /SP/AgentInfo DhcpConfigured=disable` command first. Then fill in the appropriate values for `netmask`, `gateway`, and `ipaddress`.

```
set /SP/AgentInfo DhcpConfigured=disable
set /SP/AgentInfo NetMask=netmask
set /SP/AgentInfo Gateway=gateway
set /SP/AgentInfo IpAddress=ipaddress
```

- If a DHCP server is present, the IP information can be obtained by running the following command:

```
show /SP/AgentInfo
```

Note – Be sure to record the IP address assigned to the ELOM SP.

To View System Output Within CLI

When you are connected to the host, you can see that system's output within the CLI. To access the host serial console (host COM0), enter the following command:

```
SP-> start /SP/AgentInfo/console
```

Note – Use the Esc-Shift-9 key sequence to toggle back to the local console flow. Enter **Ctrl-b** to terminate the connection to the serial console.

[Chapter 8](#) describes how to use the CLI.

For instructions on how to use the serial console, see your platform-specific documentation.

Setting Up Serial Over LAN

See the section that corresponds to the operating system that you are using to use serial over LAN to interact with the ELOM SP.

- [“Instructions for Solaris” on page 12](#)
- [“Instructions for Linux” on page 13](#)

Instructions for Solaris

1. Log in to the Solaris system as root (superuser).
2. Edit the `/boot/solaris/bootenv.rc` file to point to `ttyb` speed to 115200 as follows:

```
setprop ttyb-mode 115200,8,n,1,-
setprop console `ttyb`
```
3. In the `/boot/grub/menu.lst` file, edit the `splashimage` and `kernel` lines to read as follows:

```
# splashimage /boot/grub/splash.xpm.gz
kernel /platform/i86pc/multiboot -B console=ttyb
```
4. Change the login service to listen at 115200 by making the following edits to `/var/svc/manifest/system/console-login.xml`:
 - a. Change `console` to 115200 in the `propval` line to read as follows:

```
<propval name='label' type='astring' value='115200'>
```

b. Add the following text to the file `/kernel/drv/asy.conf`:

```
bash-3.00# more /kernel/drv/asy.conf
#
# Copyright (c) 1999 by Sun Microsystems, Inc.
# All rights reserved.
#
# pragma ident "@(#)asy.conf 1.12 99/03/18 SMI" interrupt-
priorities=12;name="asy" parent="isa" reg=1,0x2f8,8 interrupts=3;
```

5. Enter the following to reboot the operating system:

```
# reboot -- -r
```

Instructions for Linux

These instructions apply for all supported Red Hat and SUSE operating systems, except as noted.

1. Log in to the system as root (superuser).
2. Open the `/etc/inittab` file in a text editor.
3. Change the following in the `/etc/inittab` file:
 - a. Find the `getty` section of the `inittab`, and edit the `gettys` for init level 3 so that the line reads as follows:

```
3:2345:respawn:/sbin/agetty -L 115200 ttyS1 vt100t
```
 - b. Locate the following line in the file:

```
id:5:initdefault
```
 - c. Change the default init level from 5 to 3 as shown in the following example:

```
id:3:initdefault
```
4. If you plan to log in to the OS as root using the Remote Console, add the following line to edit the `/etc/securetty` file:

```
ttys1
```

Alternatively, you can create a non-root account, to which you can log in without this change.
5. To see all of the startup messages in Red Hat, edit the `/etc/grub.conf` file as follows:

- a. Open the `/etc/grub.conf` file in a text editor.
- b. Add the following to the kernel line:

```
'console=tty1 console=ttyS1,115200'
```

Connecting Over Ethernet

The embedded lights out manager (ELOM) software on the SP offers several interfaces to support system management on your server. Before you take advantage of those interfaces over your Ethernet local area network (LAN), you need to do the following:

- Establish an Ethernet connection between your server and your Ethernet LAN.
- Determine the IP address assigned to your SP by your DHCP server, or by following the instructions in [“Connecting Through the Serial Port” on page 10](#).
- View host system output using the command shown in [“To View System Output Within CLI” on page 11](#) or view IP address in the BIOS by following instructions in [“To View the System IP Address in the BIOS” on page 15](#).

Note – This procedure assumes that you have already completed the hardware setup, and have applied standby power for your server, as described in your platform documentation.

Once you have determined the IP address of the SP, you can access its firmware applications through a secure command shell (SSH) or a web browser.

1. **Insert an Ethernet cable into the Net Mgmt RJ-45 port.**

See your platform documentation setup guide for an illustration and instructions on installing the hardware and cabling, and for powering on.

2. **Open an Internet Explorer web browser.**

See [TABLE 2-2](#) for other browsers able to run the web-based interface.

TABLE 2-2 Minimum Level of Supported Browsers

Operating System	Mozilla	Firefox
Solaris x86	1.7	1.5.0.4
RHEL 32 bit	1.7.12	1.0.7

TABLE 2-2 Minimum Level of Supported Browsers (Continued)

Operating System	Mozilla	Firefox
RHEL 64 bit	1.7.13	1.5.0.4
SLES 32 bit	1.7.8	1.5.0.4
SLES 64 bit	1.7.13	1.5.0.4

3. In the address bar enter the address assigned to the SP.

By default, each new Sun Fire X2100 M2 and Sun Fire X2200 M2 server system comes with DHCP enabled. If no DHCP server is found within five seconds, the system defaults to the static IP address **192.168.1.2**. Change the IP address if you need a different static IP address. If you change to a different static IP address it must be on the same network segment.

4. You are now connected to the Service Processor.

The account name is “root” and the password is “changeme”

See [Chapter 3](#) for access from a terminal using a web browser.

To View the System IP Address in the BIOS

1. **Attach a local video display screen to the server’s video port.**
2. **Attach a USB keyboard to one of the USB ports on the server.**
3. **Attach an Ethernet cable from the network to the NET MGT Ethernet port on the server.**

4. Apply power to the server.

The system will begin displaying the large full screen Sun Logo. During this process perform [Step 5](#).

5. Press the F2 key on the USB keyboard to enter the BIOS setup mode.

The system will carry out some additional configuration operations before entering the blue BIOS setup mode.

a. If you have a system without a display you can:

- i. **Start the CLI, and log in.**
- ii. **Launch a system console by entering the command:**
`start /SP/AgentInfo/console`
- iii. **Reboot the server, and press the hot keys to enter the BIOS.**

6. Under Advanced choose: Ipmi 2.0 configuration.
7. Choose: Set Lan Configuration,
8. Select IP Address and the Current IP address is displayed.

To Configure Your DHCP Server

You will need to verify that your DHCP server will accept new MAC addresses.

1. **Confirm that an Ethernet cable is connected to the RJ-45 NET MGT Ethernet port on your server.**

If the SP is not using static IP addresses, it broadcasts a DHCPDISCOVER packet with the ID of its MAC address. A DHCP server on your LAN returns a DHCPOFFER packet containing an IP address and other information. The SP then manages its “lease” of that IP address assigned by the DHCP server.

2. **Obtain the SP MAC address from one of the following locations. Record that address for future reference.**

MAC addresses are 12-digit hexadecimal strings in the format `xx:xx:xx:xx:xx:xx`.

`x` represents a single hexadecimal letter (0–9, A–F, a–f).

- CLI commands. From a terminal attached to the SP serial port, log in to the SP, and enter the CLI command `show /SP/network`. The SP displays the MAC address.
 - The Customer Information Sheet shipped with your server.
 - The system BIOS setup screen. Choose Advanced -> IPMI 2.0 -> Configuration-> Set LAN Configuration MAC address.
3. **Obtain the SP IP address from one of the following locations. Record the IP address for future reference.**
 - CLI commands: From a terminal attached to the SP serial port, log in to the SP, and enter the CLI command `show /SP/AgentInfo`. The SP displays the current IP address.
 - The system BIOS setup screen. Choose Advanced -> IPMI 2.0 Configuration>Set LAN Configuration> IP address.
 - DHCP server log files. If you use this method, use [Step a](#) through [Step b](#) below. Otherwise, skip to [Step 4](#).
- a. **Log in to your DHCP server, and view its DHCP log file.**

Note – Different DHCP server applications running on different operating systems store these log files in different locations. Consult your DHCP system administrator to locate the correct path to the log file.

b. In the log file, identify the IP address that corresponds to the MAC address of your SP.

Typically, DHCP log file entries are individual lines with the following comma-separated fields:

ID, Date, Time, Description, IP Address, Host Name, MAC Address

Locate the MAC address of your SP in the MAC Address (seventh) field of the correct DHCP file entry, and record the corresponding value of the IP Address (fifth) field. This is the IP address that you must use to access the system management firmware applications on your SP.

4. Open a session to the SP using the IP address that you obtained in Step 3.

Each SP firmware application requires a different web browser or shell.

To establish a Secure Shell (SSH) connection to the SP command-line interface (CLI), enter the appropriate connection command in the SSH application. For example, to connect to the SP with the DHCP-assigned IP address of 192.168.0.0, enter the following command:

```
# ssh -l root 198.168.0.0
```

Once you have entered the default password for the SP, changeme, you can enter commands to manage user accounts or to monitor the status of devices on your server.

Finding Task Information

The following table describes where to find the information you need for the task you want to perform.

TABLE 2-3 Task Information

Task	Where to Find the Information
Communicate with the system.	“Setting Up Communications” on page 9
Use the SSH to log in to the SP.	“To Log In Using SSH” on page 100
Set up the Service Processor (SP) from the web browser.	“To Set Up the Service Processor with the Web-Based Interface” on page 21

TABLE 2-3 Task Information

Task	Where to Find the Information
Find out the health of the system using the web-based interface.	“Accessing the System Using the Web-Based Interface” on page 25
Discover what hardware is installed using the web-based interface.	“Using the System Information Screens” on page 28
Monitor temperatures, voltages, fans, and chassis from the web-based interface.	“Using the System Monitoring Screens” on page 36
View the Event Log.	“Examining, Saving, and Clearing the Event Log” on page 44
Determine which events to monitor from the web-based interface.	“Defining Traps with the Platform Event Filter” on page 52
Add and delete users, and set user access	“Managing Users” on page 66
Update the SP firmware	“Service Processor Maintenance” on page 73
Start a remote console session from the web-based interface.	“Launching the Remote Console Application” on page 80
Get system information using intelligent Platform Management Interface (IPMI) commands.	“Supported IPMI 2.0 Commands” on page 95
Manage the system from the command line.	“Logging In to the CLI” on page 99

Setting Up the Service Processor

This chapter describes how to set up the service processor for the first time on your Sun Fire X2100 M2 or Sun Fire X2200 M2 system. It includes the following sections:

- [“Service Processor Components” on page 19](#)
 - [“Powering On the Server” on page 20](#)
 - [“Communicating with the System SP” on page 21](#)
 - [“Configuring the IP Address Manually” on page 23](#)
-

Service Processor Components

The Sun Fire X2100 M2 and Sun Fire X2200 M2 server service processors consists of four components, three of which are on your host server and one of which is on the client system that accesses your host server. The four components are as follows:

- SP hardware. Your server is equipped with a service processor (SP) that performs the following functions:
 - Monitors the status and configuration of field-replaceable components of your server, such as fans, disk drives, and power supplies.
 - Provides serial and Ethernet connections to external terminals or local area networks (LANs).
- SP firmware. Preinstalled on the SP is a library of system management firmware applications. This firmware is operating system independent, and applications provide the following system management interfaces into your server:
 - A web-based graphical interface
 - A Secure Shell (SSH) command-line interface
 - An IPMI v2.0 command interface
 - A Simple Network Management Protocol (SNMP) v1, v2c, or v3 interface

These interfaces call the same underlying system management functions on your SP, so you can choose to work with one or more of these SP interfaces to integrate with the other management interfaces running in your data center.

- Remote Console application. The Remote Console application is a piece of layered software that enables remote clients to view the graphical console of your host server as though they were directly attached to its video connector. The Remote Console is a mirror of the video output (up to resolutions of 1600 x 1200) from the server's VGA video connector. The remote keyboard, mouse, CD drive, or diskette drive will appear as standard USB devices.

Note – The Remote Console application is automatically installed on your client as a Java™ Webstart application when the remote console is viewed for the first time, and requires only a web browser correctly configured with a Sun Java plug-in version 1.5.0 or greater. You can download Java for free from <http://java.sun.com>.

- Client-side secure shell application. To access the SP through a remote secure shell (SSH), you must install a secure shell communications application on the remote client system (server, workstation, or laptop). Many secure shell communications applications are available from commercial or open-source distribution. Go to <http://www.openssh.org> for information about open-source client-side SSH applications.

Your Sun Fire X2100 M2 and Sun Fire X2200 M2 server SP hardware and firmware is configured to reflect the most common default settings used in the field. It is unlikely that you will need to change these defaults.

Powering On the Server

Apply standby power only to the server at this point so that you can perform initial configuration of the service processor. See the procedures for powering on to main power mode and for shutting down from main power mode, which are included in your server installation manual. See your platform-specific *Server Installation Guide* for instructions.

Apply Standby Power for Initial Service Processor Configuration

Apply standby power to the service processor (SP) before initial configuration.



Caution – Do not operate the server without all fans, component heatsinks, air baffles, and the cover installed. Severe damage to server components can occur if operated without adequate cooling mechanisms.

See your server hardware installation guide for information and cautions regarding power, cabling, and system hardware.

At this point, standby power is supplied only to the service processor (SP) board and power supply fans. You can proceed with [“Communicating with the System SP” on page 21](#) to begin initial configuration.



Caution – Do not apply main power to the rest of the server until you are ready to install or change a platform operating system.

Communicating with the System SP

The on-board service processor communicates through the system serial port as well as through a dedicated Ethernet port. In [Chapter 2](#) you saw that:

- You can run the command-line interface (CLI) connected directly to the serial port. See [“Connecting Through the Serial Port” on page 10](#)
- You can run the CLI and the web-based interface through the Ethernet port. See [“Connecting Over Ethernet” on page 14](#)

Both or either of these methods are initiated through a terminal console on your laptop or PC.

Next you must set up the environment in which the SP will function. The simplest way is through the web-based interface.

To Set Up the Service Processor with the Web-Based Interface

Each new Sun Fire X2100 M2 and Sun Fire X2200 M2 server system is delivered with DHCP set at the default. If an IP address is not found within 5 seconds, the system will use the default IP address to allow instant Web access: 192.168.xx.xx (xx.xx is the last two digits of the MAC address).

1. Open your web browser.

See TABLE 2-2 in “Connecting Over Ethernet” on page 14 for minimum browser versions supported by the web-based interface.

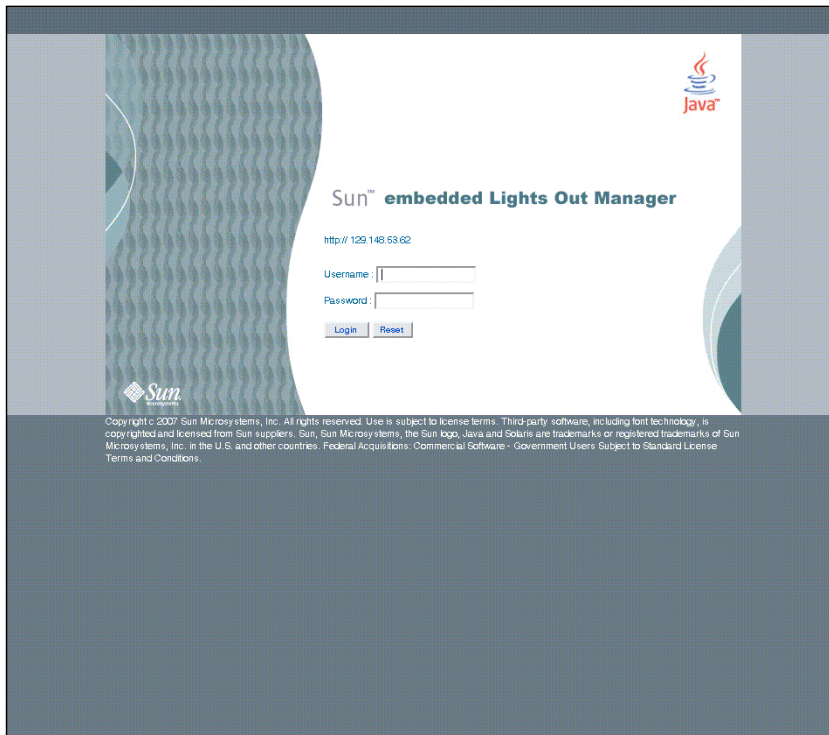
2. Enter the address you determined earlier in the address bar.

See “Setting Up Communications” on page 9 for initial communications procedures. The IP address enables you to connect directly to the service processor and the server system software.

The ELOM Login screen appears (see FIGURE 3-1).

Note – Web browser connections to the web-based interface over the insecure HTTP protocol will be automatically redirected to the secure SSL encrypted HTTPS protocol by default.

FIGURE 3-1 The ELOM Login Screen



3. Enter the user name and password, and click Login.

Username: **root**

Password: **changeme**

Configuring the IP Address Manually

If you have difficulty connecting to the web-based interface, check that you are using the correct IP address as noted in the previous sections of this guide.

Note – You will only need to do this if you cannot initially log in to the SP. Once you have established a connection through the web browser, you can configure the IP address from the web-based interface by choosing Control → Network.

1. Click the **Configuration** tab to display the configuration menus for the ELOM interface.
2. Click **Network**, and deselect the **Enable DHCP** check box.
3. Enter the **IP address, Mask, Gateway, and DNS settings**.

If you leave **Enable DHCP** selected, the choice provides dynamic IP addresses according to their availability, see the Note at [Step 5](#).

FIGURE 3-2 Configuration Network Submenu

The screenshot displays the Sun Embedded Lights Out Manager web interface. At the top, there is a header with 'ABOUT' and 'LOGOUT' links, and the title 'Sun Embedded Lights Out Manager'. Below the header is a navigation menu with tabs for 'System Information', 'System Monitoring', 'Configuration', 'User Management', 'Remote Control', and 'Maintenance'. The 'Configuration' tab is selected, and a submenu is visible with options: 'Network', 'E-mail Notification', 'Platform Event Filter', 'Time', 'Syslog', and 'System Management Access'. The 'Network' submenu is active, showing a configuration form. The form includes a checkbox for 'Enable DHCP' (unchecked). Below this are input fields for 'IP' (129.148.53.52), 'Net Mask' (255.255.255.0), 'Gateway' (129.148.53.248), 'Set DNS' (129.148.13.40), and 'Mac Address' (00:16:36:58:97:E4). At the bottom of the form are 'Submit' and 'Reset' buttons.

Note – If you change the IP address manually so that it differs from the default address of the SP, make sure to deselect the Enable DHCP box. When you reconnect through your web browser you will use the new IP address.

4. Click Submit.

The connection might appear to freeze; this is because the IP address is changed.

5. Enter the new IP address into the web browser address bar, and log in again.

Note – If you choose DHCP, there are three ways to determine an IP address: Find out the IP address through the CLI. See [“Connecting Through the Serial Port” on page 10](#); Configure a DHCP server. See [“To Configure Your DHCP Server” on page 16](#); View the IP address through the system BIOS. See [TABLE A-4](#).

Continue with initial software setup tasks.

Accessing and Monitoring the Server Using the Web-Based Interface

This chapter describes how to access the server using the embedded lights out manager (ELOM), and how to use the System Information and System Monitoring screens for diagnosing and troubleshooting system components. Using your web browser you can view system information, set system functions, and monitor system sensors.

This chapter includes the following sections:

- [“Accessing the System Using the Web-Based Interface” on page 25](#)
- [“Using the System Information Screens” on page 28](#)
- [“Using the System Monitoring Screens” on page 36](#)

Accessing the System Using the Web-Based Interface

The simplest way of accessing your server is through a web browser.

▼ To Access the System Using the Web-Based Interface

Note – To use the web-based interface, you must have previously logged on to the service processor (SP) as described in “[To Set Up the Service Processor with the Web-Based Interface](#)” on page 21.

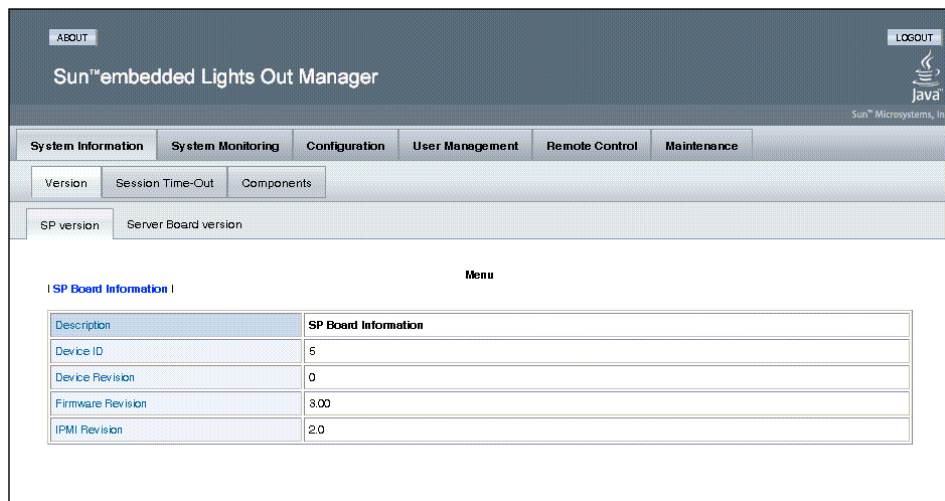
1. Open your web browser.
2. Enter the IP address of the service processor (SP) in the browser’s address bar.
See “[Setting Up Communications](#)” on page 9 for initial communications procedures. The IP address enables you to connect directly to the Service Processor (SP) and the server system software.
3. Enter the root user name and password when the login screen appears.

Username: **root**
Password: **changeme**

4. Click Login.

The SP Version screen appears (see [FIGURE 4-1](#)).

FIGURE 4-1 The SP version Screen



This is the first screen to appear when you log in. The main menu tabs appear across the top row. The choices are:

- System Information
- System Monitoring
- Configuration
- User Management
- Remote Control
- Maintenance

Using the System Information Screens

Once you are logged on to the system, you can view component-level metadata, and set system functions by selecting the System Information tab. For example, you can use the System Information submenu screens to find the service processor (SP) version number. You can also find the manufacturer of the system's CPUs, and the size and type of DIMM installed in the system. You can also use the System Information screen to set the Session Time-Out function.

This section contains the following procedures:

- [“Getting System Version Information” on page 28](#)
- [“Setting the Session Time-out” on page 30](#)
- [“Getting System Components Information” on page 31](#)

Getting System Version Information

The Version screens display version information about the SP and server board. The SP and server board version information can be useful for troubleshooting and for planning updates.

▼ To access the Version screen

1. **Click the System Information tab.**
2. **Click the Version submenu tab.**

The Version screen appears (see [FIGURE 4-1](#)). The available screen tabs are:

- SP Version
- Server Board Version

▼ To access the SP Version screen

- **Select the SP Version submenu tab.**

The SP Version screen appears. The screen displays information about the SP, such as the device ID and revision numbers. The system presents this information in a tabular format. See [TABLE 4-1](#) for a sample of the SP Version information screen.

TABLE 4-1 Sample SP Version Information

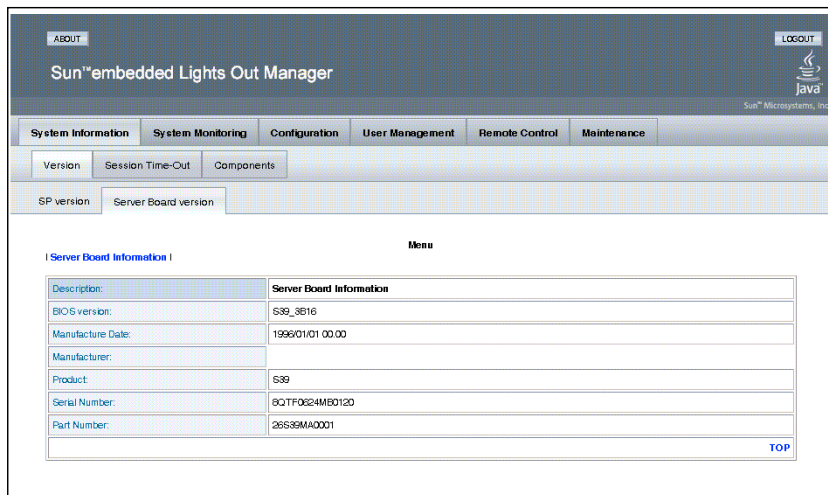
Description	BMC Board Information
Device ID	5
Device Revision	0
Firmware Revision	3.00
IPMI Revision	2.0

▼ To access the Server Board Version screen

- **Select the Server Board Version submenu tab.**

The Server Board Version screen appears. The screen displays information specific to the server board, such as, BIOS version, serial number, and manufacturer (see [FIGURE 4-2](#)).

FIGURE 4-2 The Server Board Version Screen



The system presents this information in a tabular format. See [TABLE 4-2](#) for a sample of the Server Board information.

TABLE 4-2 Sample Server Board Information

Description:	Server Board Information
BIOS version:	S40_1A03
Manufacture Date:	MM/DD/YYYY
Manufacturer:	Sun Microsystems
Product:	S40
Serial Number:	12345678901234
Part Number:	xxx-xxxx-xx

Setting the Session Time-out

The Session Time-out screen allows you to enable (set) or disable the inactive session time-out function. This function automatically performs a session logout from the web-based interface, when a preset period of inactive session time expires. When you enable this function, you must select an expiration time-period from the Session Time drop-down list. Setting the Session Time-out is a simple but effective security measure that prevents unauthorized access to an unattended session.

▼ To Set the Session Time-out

- 1. Click the Session Time-out submenu tab.**

The Time-out screen appears displaying the Timeout window (see [FIGURE 4-3](#)). The status of the inactivity time-out function is displayed next to the label:

Current Status:

- 2. Select the Enable Time-out radio button.**

Note – If you are disabling the time-out function, click the Disable Time-out radio button, and click Submit.

FIGURE 4-3 The Session Time-out Screen

Timeout

Current Status : **Enable** Timeout value:15
 Enable Timeout Disable Timeout

Select an inactivity timeout for this session.
If your session is inactive for the selected you will be logged out.

session time: 15 minutes ▾

3. **Select a period of time from the Session Time drop-down list.**
The options are: 15-minutes, 30-minutes, 1-hour, or 2-hours.
4. **Click Submit to set the session time-out.**

Getting System Components Information

The System Components submenu screens provide information about the CPUs, the memory, and the network interface cards (NIC) installed in a system. Accessing this information is useful for creating system inventories and obtaining configuration data for diagnostic or maintenance/upgrade purposes.

▼ To access the Components submenu screens

1. **Click the System Information tab.**
2. **Select the Components submenu tab.**

The Components screen appears. The available submenu screen tabs are:

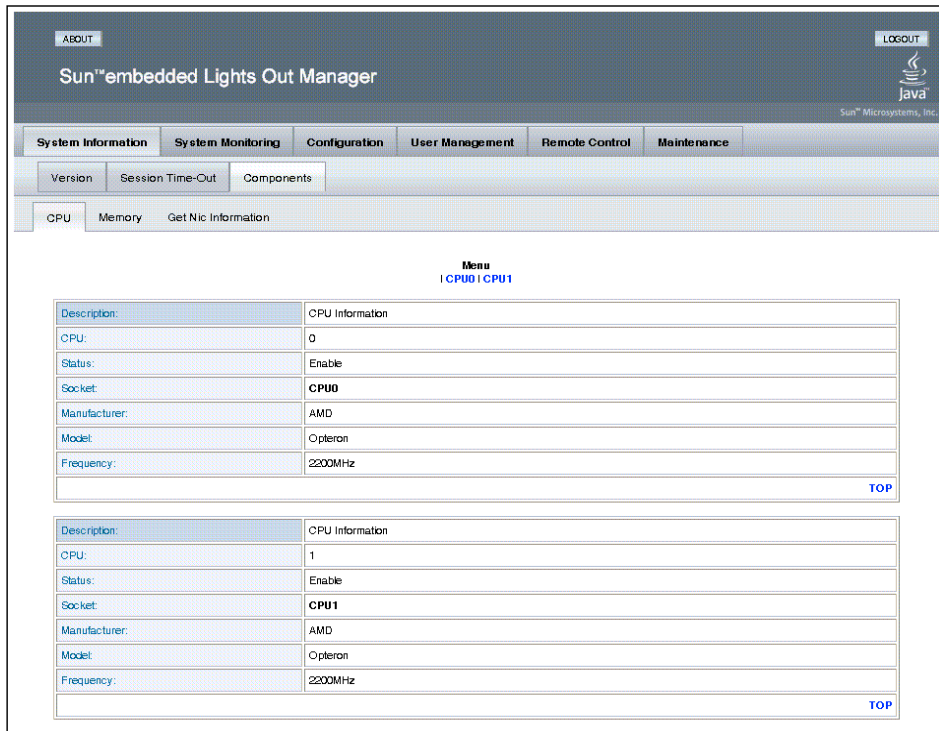
- CPU
- Memory
- Get NIC Information

▼ To access the CPU screen

- **Select the CPU submenu tab.**

The CPU screen appears, displaying information about the CPUs in your system. The information includes CPU number, Status, Socket, Manufacturer, Model, and Frequency (see [FIGURE 4-4](#)).

FIGURE 4-4 The CPU Screen



The system displays the CPU information in a tabular format for every CPU in the system. The CPU screen in [FIGURE 4-4](#) shows a server system containing two CPUs. [TABLE 4-3](#) shows a sample of CPU information for one, CPU0:

TABLE 4-3 Sample CPU Information

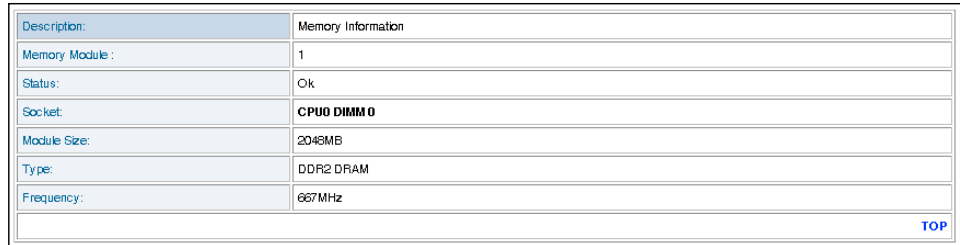
CPU:	0
Status:	Enable
Socket:	CPU0
Manufacturer:	AMD
Model:	Opteron
Frequency:	2200 MHz

▼ To access the Memory screen

- **Select the Memory submenu tab.**

The Memory screen appears, displaying information about the system DIMMs. The information includes, module number, status, size, type, and frequency (see [FIGURE 4-5](#)).

FIGURE 4-5 DIMM Information Displayed in the Memory Submenu



Description:	Memory Information
Memory Module :	1
Status:	Ok
Socket:	CPU0 DIMM 0
Module Size:	2048MB
Type:	DDR2 DRAM
Frequency:	667MHz

[TOP](#)

The system displays memory information in a tabular format for every DIMM in the system. The following table shows a sample of memory information for one DIMM, the DIMM installed in socket DIMM0 for CPU0:

TABLE 4-4 Sample of Memory Information

Description	Memory Information
Memory Module	1
Status:	Ok
Socket:	CPU0 DIMM0
Module Size:	2048MB
Type:	DDR2 DRAM
Frequency:	667MHz

▼ To access the Get NIC Information screen

- **Select Get NIC Information submenu tab.**

The Get NIC Information screen appears, displaying information about the network interface cards installed in the system. The information includes, Manufacturer, Product Name, Product Part Number, Product Serial Number, Port Number, MAC Address 1, and MAC Address 2 (see [FIGURE 4-6](#)).

FIGURE 4-6 The Get NIC Information Screen

The system shown in [FIGURE 4-6](#) has two NICs. [TABLE 4-5](#) shows a sample of the information for one, NIC 0:

TABLE 4-5 Sample Information for Get NIC Information

Description:	Network Interface Card 0 Information
Manufacturer:	Broadcom
Product Name:	Dual Port Gigabit NIC
Product Part Number:	5715C
Product Serial Number	00:16:36:6D:BB:DF
Port Number:	02
MAC Address 1:	00:16:36:6D:BB:DF
MAC Address 2:	00:16:36:6D:BB:E0

Using the System Monitoring Screens

The System Monitoring screens provide the troubleshooting and diagnostic capabilities you will need to maintain your servers. The server hardware is equipped with sensors that the system uses to monitor and measure critical hardware parameters, such as the status of the power, the fan speed, the voltages from the power supply, and the CPU and chassis ambient temperatures. The system polls these sensors, and displays the readings in the Sensor Reading submenu screens.

The Summary, Fan, Temperature, and Voltage submenu screens are useful diagnostic tools that you can use to monitor and diagnose your server. The Event Logs, Locator Indicator, and Fault LED submenu screens allow you to maintain the system log, activate the System Indicator, and reset the Fault LED.

This section contains the following sub-sections:

- [“Monitoring the System Using the Summary Screen” on page 36](#)
- [“Diagnosing Fan Performance” on page 38](#)
- [“Diagnosing Temperature Issues” on page 40](#)
- [“Diagnosing Voltage Issues” on page 42](#)
- [“Examining, Saving, and Clearing the Event Log” on page 44](#)
- [“Activating the System Indicator LED” on page 45](#)

Using the Sensor Reading Screens

▼ Monitoring the System Using the Summary Screen

The Summary screen provides a single-screen overview of every system critical parameter and component. With the Summary screen you can monitor the status of the Fault LED, the system power, the fans, the temperature sensors, and the DC voltage lines. If a problem occurs with a system critical component or parameter, the Summary screen will help you to identify and diagnose the problem.

To Access the Summary screen:

1. **Click the System Monitoring tab from the main menu (top row).**
2. **Select the Sensor Reading tab.**
3. **Select the Summary submenu tab.**

The Summary submenu appears, displaying the status of all the system critical parameters (see [FIGURE 4-7](#)).

FIGURE 4-7 The Summary Screen

The system displays the status of each component and parameter as OK when the component is operational and functioning within thresholds, or Fail when it is not. The information is displayed in a tabular format. [TABLE 4-6](#) shows a sample of the Summary screen information.

TABLE 4-6 Sample of the Summary Screen Information

Fault LED Status:	On
Power Status:	power on
Fan Status:	Blower Fan 0(ok) Blower Fan 1(ok) Axial Fan 0(ok) Axial Fan 1(ok)
Temperature Status:	CPU 0 Temp(ok) CPU1 Temp(ok) Ambient Temp0(ok) Ambient Temp1(ok)
Voltage Status:	Vcc 12V(ok) DDRP0 1.8(ok) DDRP1 1.8(ok) Vcc 3.3V(ok) Vcc 5V(ok) Vcc 3.3V STB(ok)

You can diagnose individual sensors in greater detail by clicking the Fan, Temperature, or Voltage submenu tabs.

▼ Diagnosing Fan Performance

With the Fan submenu tab you can view the threshold parameters and the actual tachometer readings of each fan. You can use the Fan screen to diagnose temperature-related problems by identifying under performing or non-functioning fans.

To access the Fan screen:

1. **Click the System Monitoring tab.**

2. Click the Sensor Reading tab.
3. Select the Fan tab.

The Fan submenu appears (see [FIGURE 4-8](#)).

FIGURE 4-8 Fan Submenu of the Hardware Monitor Screen

The screenshot shows the Sun Embedded Lights Out Manager interface. The top navigation bar includes 'ABOUT' and 'LOGOUT'. Below the navigation bar are tabs for 'System Information', 'System Monitoring', 'Configuration', 'User Management', 'Remote Control', and 'Maintenance'. Under 'System Monitoring', there are sub-tabs for 'Sensor Reading', 'Event Logs', 'Locator Indicator', and 'Fault LED'. The 'Fan' sub-tab is selected, showing a submenu with 'Summary', 'Fan', 'Temperature', and 'Voltage'. The main content area displays a 'Menu' for fans: 'Blower Fan 0 | Blower Fan 1 | Axial Fan 0 | Axial Fan 1'. Three fan detail panels are shown, each with a table of sensor data.

Blower Fan 0	
Description:	Blower Fan 0
Lower critical threshold is readable:	784
Upper critical threshold is readable:	8977
SensorReading:	3920
Status:	ok
TOP	

Blower Fan 1	
Description:	Blower Fan 1
Lower critical threshold is readable:	784
Upper critical threshold is readable:	8977
SensorReading:	3993
Status:	ok
TOP	

Axial Fan 0	
Description:	Axial Fan 0
Lower critical threshold is readable:	2272
Upper critical threshold is readable:	15975
SensorReading:	9656
Status:	ok
TOP	

The system displays both the upper and lower critical speed thresholds for each fan. If the system is unable to read the thresholds, it shows the status as Unreadable, otherwise it shows the status as Readable. The system also displays a direct RPM reading from the fan sensor, and shows status indicators for the Blower and Axial fans.

The system displays the information in a tabular format for each fan in the system. The following table shows a sample of fan information for Blower Fan 0.

TABLE 4-7 Sample Fan Information

Description:	Blower FAN 0
Lower critical threshold is readable:	784
Upper critical threshold is readable:	8977
Sensor Reading:	3988
Status:	ok

▼ Diagnosing Temperature Issues

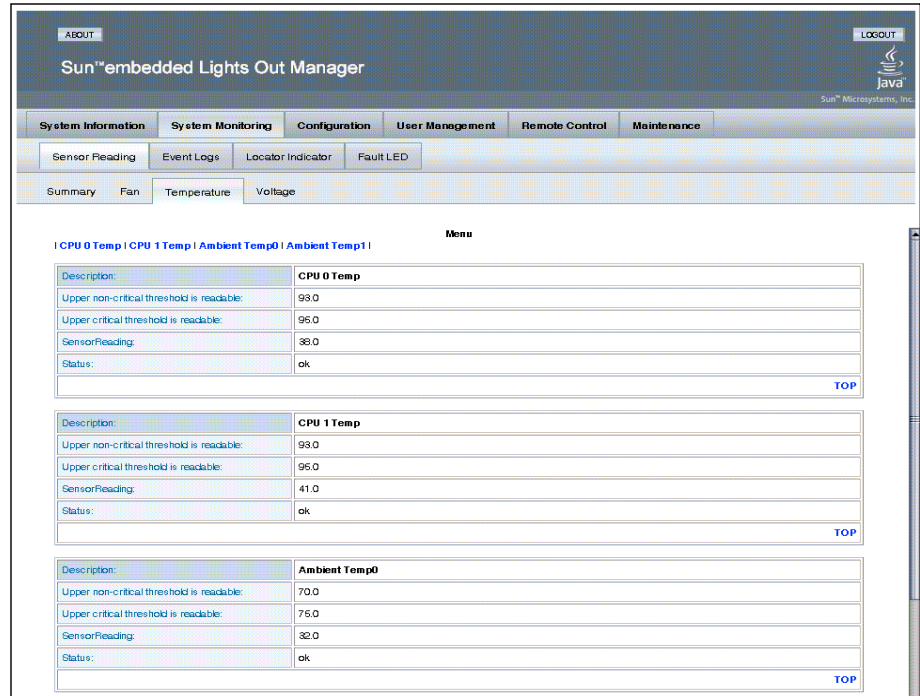
Temperature is one of the most important system critical parameters. The system monitors both the CPU and the chassis ambient temperature sensors, and displays the results in the Temperature submenu screen. An increase in temperature could be indicative of an under-performing or non functioning fan, a failing component, or a clogged air filter.

To access the Temperature screen:

1. **Click the System Monitoring tab.**
2. **Click the Sensor Reading tab.**
3. **Select the Temperature tab.**

The Temperature submenu screen appears, displaying direct readings of ambient and CPU temperature sensors (see [FIGURE 4-9](#)).

FIGURE 4-9 The Temperature Submenu



The system reads both the Lower and Upper Non-critical and the Lower and Upper Critical temperature thresholds, reporting back if the thresholds are readable. The system also provides a direct Celsius reading from each sensor, and reports on its status, showing it as either OK or Critical.

The system displays the information in a tabular format for each temperature sensor in the system. The following table shows a sample of temperature information for a CPU Fan (see TABLE 4-8).

TABLE 4-8 Sample Temperature Sensor Readings

Description:	CPU Temp (°C)
Upper non-critical threshold is readable:	93.0
Upper critical threshold is readable:	95.0
Sensor Reading:	54.0
Status:	ok

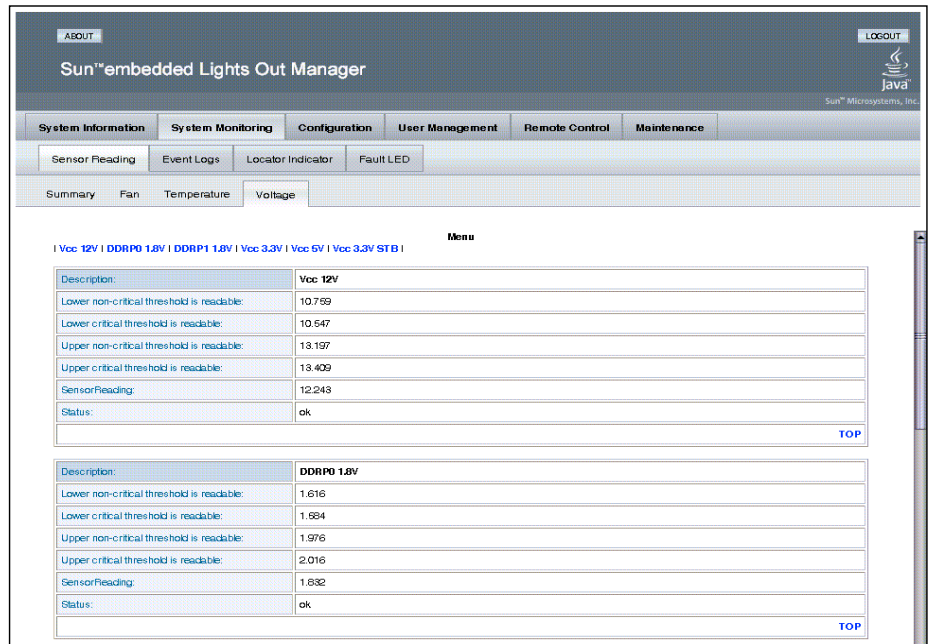
▼ Diagnosing Voltage Issues

The system monitors the DC power supplies, and displays the results in the Voltage submenu. You can use the Voltage screen to monitor each voltage line watching for low or fluctuating voltages. Low or fluctuating voltages can cause component failure, system errors, and intermittent performance issues. It can also be indicative of a failing power supply.

1. **Click the System Monitoring tab.**
2. **Click the Sensor Reading tab.**
3. **Select the Voltage tab.**

The Voltage submenu appears, displaying DC voltage power supply readings for Vcc 12V, DDRP0 1.8V, DDRP1 1.8V, Vcc 3.3V, Vcc 5V, Vcc 3.3V STB (see [FIGURE 4-10](#)).

FIGURE 4-10 The Voltage Submenu Screen



The system reads both the Lower and Upper Non-critical and the Lower and Upper Critical thresholds, and reports if the voltages are readable. The system also provides a direct reading of each voltage line, and reports on the status of the line.

The system displays the information in a tabular format for each of the power supplies voltage lines. The following table shows a sample of voltage information for the Vcc 12V line (see TABLE 4-9).

TABLE 4-9 Sample Voltage Information

Description:	Vcc 12V
Lower non-critical threshold is readable:	10.504
Lower critical threshold is readable:	10.297
Upper non-critical threshold is readable:	12.884
Upper critical threshold is readable:	13.091
Sensor Reading:	11.797
Status:	ok

Examining, Saving, and Clearing the Event Log

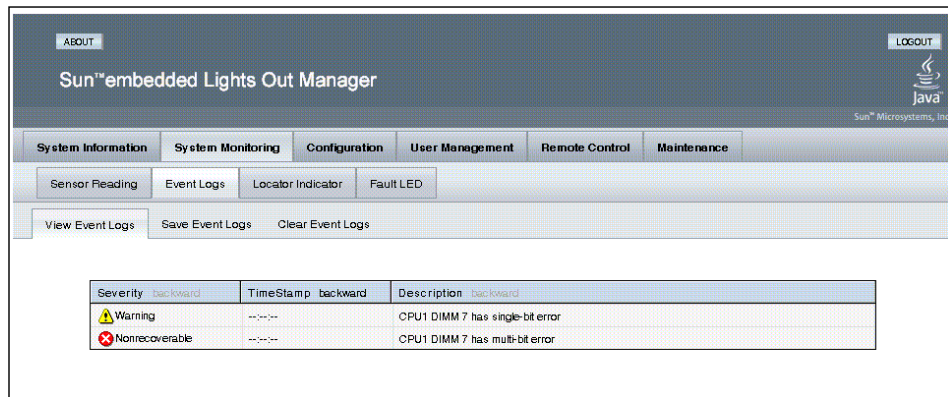
With the Event Logs submenus you can examine and manage a record of system events using the View Event Logs, Save Event Logs, and Clear Event Logs screens.

▼ To Examine the Event Logs Screen

1. Click **System Monitoring** tab.
2. Click the **Event Logs** submenu tab.

The Event Logs submenu appears (see [FIGURE 4-11](#)).

FIGURE 4-11 The Event Logs Screen



The Event Log provides a record of system events related to system critical parameters and components, such as when fans under-perform or fail, or when voltages breach threshold limits. The system logs the events, rating the level of severity, and provides a timestamp and a description of the occurrence.

Note – Before Event logging can occur, you must define in the Platform Event Filter screen which events you would like to trap. See [“Defining Traps with the Platform Event Filter”](#) on page 52.

Saving the Event Log

If you want to save the event log for record keeping or diagnostic purposes, the system provides the option to save the log to a file named: `eventlog.txt`. To maintain a contiguous record be sure to save before you clear the Event Log.

▼ To Save the Event Log

1. Click the **Save Event Logs** tab in the Event Logs screen.
2. Click the **Save Event Log** button.

The browser prompts you for a save location.

Clearing the Event Log

Clearing the event log can be useful, especially when the log becomes too big. It can also be beneficial to clear the event log after a save, a software or firmware upgrade, or a component replacement. If necessary save before you clear the Event Log (see [“Saving the Event Log” on page 45](#)).

▼ To Clear the Event Log

1. Click the **Clear Event Logs** tab from the System Monitoring menu.
2. Click the **Clear Event Log** button.

Activating the System Indicator LED

The System Indicator LED is an identification LED located on the front of the server. The purpose of the System Indicator LED is to help you find a server that might be mounted in a rack with several other servers or located in a room with many other racks of systems. By activating the System Indicator LED from the Locator Indicator screen, you can identify a server that you have designated for diagnostics or maintenance.

▼ To Activate the Locator Indicator Screen

1. Click **Locator Indicator** submenu tab from the System Monitoring menu.

The System Indicator LED screen appears (see [FIGURE 4-12](#)).

FIGURE 4-12 The Locator Indicator Screen

SYSTEM INDICATOR LED
Current Status : off
<input type="radio"/> Turn system indicator LED blink.
<input type="radio"/> Turn system indicator LED off
<input type="radio"/> system indicator LED blink , blink time interval : <input type="text" value="15"/> seconds (1-255)
<input type="button" value="Submit"/> <input type="button" value="Reset"/>

The System Indicator LED screen shows the status of the LED, and provides the option to:

Blink the System Indicator LED continuously

Turn the System Indicator LED off

Blink the System Indicator LED for a specific number of seconds (1-255)

2. **Select one of the three LED options**
3. **Click Submit.**

Resetting the Fault LED

The Fault LED is mounted on the front of the server cabinet. The LED lights, providing an alert that a system error has occurred, and that the server requires attention. After the required maintenance or repair has been performed you will need to reset the Fault LED. You can do this using the Fault LED screen.

▼ To Reset the Fault LED Screen

1. **Click the Fault LED submenu tab from the System Monitoring menu.**
2. **Select the Turn Fault ID LED off radio button.**
3. **Click Submit.**

Configuring and Managing the Server System Using the Web-Based Interface

This chapter provides information about configuring and managing local server systems using a web browser and the embedded lights out manager (ELOM). For initial ELOM configuration information, see [Chapter 3](#).

The chapter includes the following sections:

- “Configuring the Server” on page 47
- “Managing Users” on page 66
- “Service Processor Maintenance” on page 73

This chapter addresses your local system. To redirect your commands to a remote system, see [Chapter 6](#).

Configuring the Server

The embedded lights out manager Configuration screens provide access to the system administrative functions associated with configuring and customizing the system. The Configuration tab consists of six screens:

- Network
- E-mail Notification
- Platform Event Filter
- Time
- Syslog
- System Management Access

Note – This section contains advanced information about configuring and customizing ELOM services for your server. For information about the initial server configuration using the web-based interface, see [Chapter 3](#). For information about configuring your server using the command-line interface (CLI), see [Chapter 8](#).

This section contains the following:

- [“Configuring the Network Settings” on page 48](#)
- [“Setting Up E-Mail Notification” on page 50](#)
- [“Defining Traps with the Platform Event Filter” on page 52](#)
- [“Setting the System Time” on page 56](#)
- [“Enabling or Disabling Syslog” on page 57](#)
- [“Configuring System Management Access” on page 57](#)

Configuring the Network Settings

This section describes how to access the Network Settings Configuration screen, and how to use it to configure and change the network parameters. You can configure the network settings manually, or by using Dynamic Host Configuration Protocol (DHCP).

- [“To access the Network Settings screen:” on page 48](#)
- [“To configure the Network Settings manually” on page 49](#)
- [“To configure the Network Settings using DHCP” on page 49](#)

▼ To access the Network Settings screen:

1. **Start your web browser, and enter the IP address of the server.**

The login screen appears.

2. **Enter a user name and password that has Administrator privileges.**

The default login account has Administrator privileges. To use the default login, enter the following information:

Username: **root**

Password: **changeme**

3. **Click Login.**

The Sun embedded Lights Out Manager web-based interface appears.

4. **Click the Configuration tab to access the Configuration submenu screens.**

5. Click the Network Settings tab.

The Network Settings screen appears (see [FIGURE 5-1](#)).

FIGURE 5-1 The Network Settings screen

The screenshot displays the Sun™ embedded Lights Out Manager interface. At the top, there are 'ABOUT' and 'LOGOUT' links. The main title is 'Sun™ embedded Lights Out Manager'. Below the title is a navigation bar with tabs: 'System Information', 'System Monitoring', 'Configuration', 'User Management', 'Remote Control', and 'Maintenance'. Under the 'Configuration' tab, there are sub-tabs: 'Network', 'E-mail Notification', 'Platform Event Filter', 'Time', 'Syslog', and 'System Management Access'. The 'Network' sub-tab is selected, showing a form with the following fields:

- Enable DHCP
- IP: 129 . 148 . 53 . 62
- Net Mask: 255 . 255 . 255 . 0
- Gateway: 129 . 148 . 53 . 248
- Set DNS
- DNS server: 129 . 148 . 13 . 40
- Mac Address: 00 . 16 . 36 . 58 . 97 . E4

At the bottom of the form are 'Submit' and 'Reset' buttons.

▼ To configure the Network Settings manually

The Network Settings screen has input fields for the server IP address, the net mask, the gateway address, and the address for the DNS server. The fields are open for input allowing you to manually configure the server.

1. Enter the IP address, the net mask, the gateway address, and the address for the DNS server in the appropriate fields.
2. Click Submit to save your changes.

▼ To configure the Network Settings using DHCP

The Network Settings screen also has an Enable DHCP (Dynamic Host Configuration Protocol) check box. If you enable DHCP, the IP address, the gateway, the subnet mask, and the DNS Server address will be supplied by the server.

1. **Select the Enable DHCP check box.**

Notice that the IP Address, Gateway, Subnet Mask, and DNS Server fields are now closed for manual input. The server will supply this information.

2. **Click Submit to enable DHCP.**

Setting Up E-Mail Notification

The E-Mail Notification screen is a useful configuration and server management tool that allows you to designate email recipients for notification of trapped system event messages and alerts. You can designate up to ten email address recipients. When trapped events and alerts occur, the system will send an email containing the details of the traps to the designated addresses. The email will contain the server name, the IP address of the server, the date and time of the occurrence, the severity of the event, and a description of the event. By configuring email notification, you can set up a level of accountability and redundancy for the management and maintenance of a server.

Note – System event traps are defined in the Platform Event Filter screen, see [“Defining Traps with the Platform Event Filter” on page 52](#)

▼ **To set up E-Mail Notification:**

1. **Click Configuration, from the main menu.**

2. **Select the E-mail Notification submenu tab.**

The E-mail Notification screen appears (see [FIGURE 5-2](#))

FIGURE 5-2 The E-mail Notification Screen

The screenshot shows the 'Enable E-mail Notification' configuration page. It features a navigation bar 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', 'Time', 'Syslog', and 'System Management Access'. The main content area is titled 'Enable E-mail Notification' and contains three main sections: 'SMTP Server' with a text field containing '192.168.1.100', 'Sender' with an empty text field, and 'Receiver E-mail Address' with a table of ten empty text fields. At the bottom right of the form are 'Submit' and 'Reset' buttons.

The E-Mail Notification Screen has twelve input fields, one field for the SMTP Server name, one field for the Sender name, and ten fields for the Receiver E-mail Addresses.

- 3. Fill in the name of the SMTP server in the SMTP Server field.**
This is the name of the server used to send the email.
- 4. Fill in the name of the user or script that is sending the email in the Sender field.**
- 5. Fill in the receiver e-mail addresses in the Receiver E-mail Address fields.**
The system provides for up to ten receiver e-mail addresses.

Tip – Press the Tab key to advance to the next field to enter each address.

- 6. Click Submit to save your changes, and initiate email notification.**

Defining Traps with the Platform Event Filter

To capture the event messages for the system logs and email notification, you must define the system generated events that you want to trap and the actions you want to allow. The Platform Event Filter (PEF) screen allows you to activate this feature, configure PEF parameters, and define traps by creating event filters.

▼ To define traps with the Platform Event Filter screen

1. Click the **Configuration** tab.
2. Click the **Platform Event Filter** tab.

The Platform Event Filter screen appears (see [FIGURE 5-3](#)).

FIGURE 5-3 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	
	129.148.53.206
	129.148.97.209
	129.148.181.212
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 :	
All sensors	
Event Action Configuration :	
	<input type="checkbox"/> Power Control
	<input type="checkbox"/> Diagnostic Interrupt(NMI)
	<input checked="" type="checkbox"/> Send Alert
	<input type="checkbox"/> Send Mail

The PEF screen is divided into Four sections:

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

3. Click the **Enable PEF** radio button in the **Platform Event Filter** section (see [FIGURE 5-4](#)).

FIGURE 5-4 The Platform Event Filter Section

Platform Event Filter	
PEF Global Control :	<input checked="" type="radio"/> Enable PEF <input type="radio"/> Disable PEF
Community :	<input type="text" value="public"/>

- 4. Enter the IP of the servers receiving the trapped system event messages in the Trap Receiver Destination Address section (see [FIGURE 5-5](#)).**

You can designate up to four servers.

FIGURE 5-5 The Platform Event Filter and Trap Receiver Destination Address sections of the Platform Event Filter screen.

The screenshot shows the 'Platform Event Filter' configuration interface. At the top, there is a 'PEF Global Control' section with two radio buttons: 'Enable PEF' (selected) and 'Disable PEF'. Below this is a 'Community' field with the value 'public'. The main section is titled 'Trap Receiver Destination Address' and contains a table with three rows, each representing an IP address: 129.148.53.206, 129.148.97.209, and 129.148.181.212. There is an empty row at the bottom of the table.

5. Select the PEF Global Actions by clicking the check box for each of the actions you want to enable (see [FIGURE 5-5](#)).

There are six possible PEF Actions. [TABLE 5-1](#) lists and describes the actions.

TABLE 5-1 PEF Actions and Descriptions

Action	Description
Enable Power Off Action	The system is powered off by this action.
Enable Power Cycle Action	The system power is cycled (turned off and turned on) by this action.
Enable Power Reset Action	Power reset enabled.
Enable Diagnostic Interrupt Action	Enables diagnostic information dump.
Enable Send Alert Action	Alerts are sent to the trap receiving server by this action.
Enable Send Mail Action	Email notification is enabled by this action.

When you select an action you are enabling that function globally. For example, if you select all three power-related actions, you are enabling the functionality of those actions, and you will be able to select them in the Configure Event Filter section.

6. Select the sensor you want to filter from the Configure Event Filter drop-down list (see [FIGURE 5-6](#)).

FIGURE 5-6 The Event Filter and Event Action Configuration Sections

<input checked="" type="checkbox"/> Enable Send Mail Action	
Event Filter Configuration :	Event Action Configuration :
<input type="text" value="fff - All sensors"/>	<input type="checkbox"/> Power Control <input type="text" value=""/>
<ul style="list-style-type: none">fff - All sensors01h - Temperature02h - Voltage04h - Fan07h - Processor0Ch - Memory	<input type="checkbox"/> Diagnostic Interrupt(NMI)
	<input checked="" type="checkbox"/> Send Alert
	<input type="checkbox"/> Send Mail

The drop-down list has the following six sensor options:

drop-down list Options

- fff - All sensors
 - 01h - Temperature
 - 02h - Voltage
 - 04h - Fan
 - 07h - Processor
 - 0Ch - Memory
-

Each option corresponds to the sensors associated with that component/subsystem. The Event Filter Configuration and Event Action Configuration sections allow you to configure each of these six options separately.

7. **Select all the actions that apply for the sensor by clicking the corresponding check boxes in the Event Action Configuration section (see [FIGURE 5-6](#)). The four check box options are:**

Check box Options

- Power Control
 - Diagnostic Interrupt(NMI)
 - Send Alert
 - Send Mail
-

The Power Control option has a drop-down list with three power-related actions: Power Cycle, Power Off, and Power Reset. If you select the Power Control action, you must also select one of the three actions.

8. **Repeat step 6 and step 7 for each sensor you want to configure.**

9. Click the **Submit** button to save your settings.

Setting the System Time

The System Time screen allows you to see the date and time for the system. The system date and time is referenced in the Event Logs and in the E-Mail Notification function, and it is an important part of diagnostics and troubleshooting procedures. For proper server management always make sure the correct date and time are set for the system.

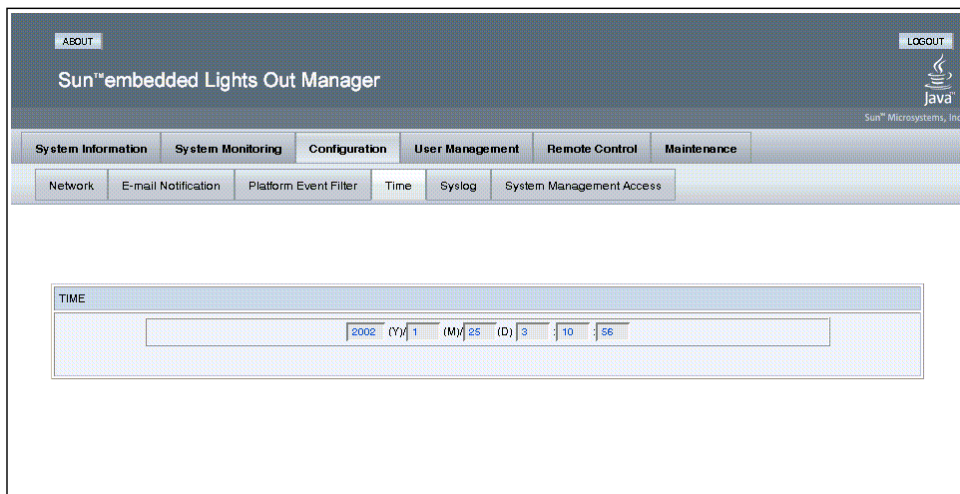
Note – Set the system time using the system BIOS setup.

▼ To set the Time screen

1. Click the **Configuration** tab.
2. Select the **Time** tab.

The Time screen appears (see [FIGURE 5-7](#)).

FIGURE 5-7 The Time screen



Note – The time is displayed using the 24-hour format.

Enabling or Disabling Syslog

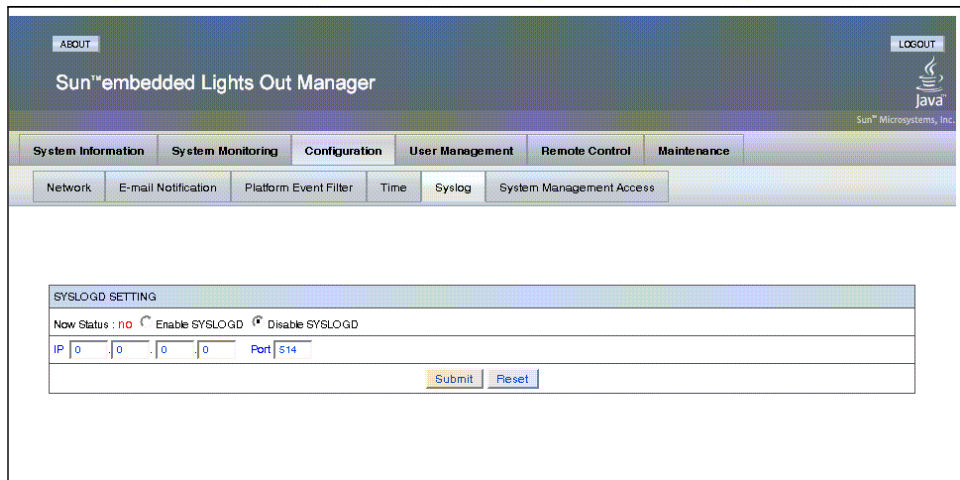
The Syslog screen allows you to enable the Syslog protocol for the server.

▼ To access the Syslog screen

1. Click the **Configuration** tab.
2. Select the **Syslog** tab.

The Syslogd screen appears (see [FIGURE 5-8](#)).

FIGURE 5-8 The Syslogd screen



The screenshot shows the Sun™ embedded Lights Out Manager web interface. At the top, there is a navigation bar with tabs for System Information, System Monitoring, Configuration, User Management, Remote Control, and Maintenance. Below this, there is a sub-navigation bar with tabs for Network, E-mail Notification, Platform Event Filter, Time, Syslog, and System Management Access. The main content area displays the 'SYSLOGD SETTING' form. The form includes a 'Now Status' field showing 'no' (disabled), with radio buttons for 'Enable SYSLOGD' and 'Disable SYSLOGD'. Below this, there are input fields for IP address (0.0.0.0) and Port (514). At the bottom of the form, there are 'Submit' and 'Reset' buttons.

The current status is shown as either Yes (enabled) or No (disabled).

3. Click either the **Enable Syslogd** or **Disable Syslogd** radio button.
If you are enabling syslog, enter the server IP address and the port.
4. Click **Submit** to save your changes.

Configuring System Management Access

System Management Access is composed of two screens:

- SSL Certificate (see [“The SSL Certificate screen”](#) on page 58)
- SNMP (see [“The SNMP Screen”](#) on page 59).

▼ To access the System Management Access screens

1. Click the **Configuration** tab.
2. Select the **System Management Access** tab.

The SSL Certificate screen appears, and the SNMP tab is available (see [FIGURE 5-9](#)).

FIGURE 5-9 The SSL Certificate screen

The screenshot shows the Sun embedded Lights Out Manager interface. At the top, there is a navigation bar 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, Time, Syslog, and System Management Access. The System Management Access sub-tab is selected, showing the SSL Certificate screen. The screen has two tabs: SSL Certificate and SNMP. The SSL Certificate tab is selected, displaying the SSL Configuration form. The form includes a Certificate Upload section with a 'Browse...' button and an 'Upload' button. Below this is a section for generating a new CSR, with a prompt: 'Fill in the details below and click Generate to create a new CSR.' The form fields include: Common Name(CN), Organization Unit(OU), Organization(O), Country Code(C) (set to United States), Locality(L), State(S), and E-mail Address(E). At the bottom of the form are 'Generate' and 'Reset' buttons.

The SSL Certificate screen

The SSL Certificate screen allows you to create the certificate required for the Certificate Signing Request (CSR). This is necessary when using a browser to access a secure (HTTPS) site. HTTPS requires that a digitally signed certificate is installed at the applicant's site.

▼ To Create a CSR

1. Browse for the SSL Certificate on your local system.
2. Click **Upload**.

3. Enter the information for the following fields:

Common Name(CN)

Organization Unit(OU)

Organization(O)

Locality(L)

State(S)

E-mail Address(E)

Country Code(C)

4. Click Generate to create an SSL Certificate.

The SNMP Screen

▼ To access the SNMP screen

1. Select the System Management Access tab.

2. Select the SNMP tab.

The SNMP screen appears (see [FIGURE 5-10](#)).

FIGURE 5-10 The SNMP screen

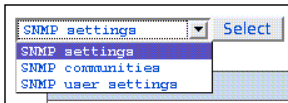


The SNMP screen is composed of three screens:

- SNMP Settings
- SNMP Communities
- SNMP User Settings

Use the drop-down list to access the three screens (see [FIGURE 5-11](#)).

FIGURE 5-11 The SNMP drop-down List



The SNMP Settings Screen

The SNMP Settings screen allows you to configure the SNMP Port and the SNMP Permit (see [FIGURE 5-12](#)).

FIGURE 5-12 The SNMP Settings Screen

SNMP settings ▼ Select	
SNMP SETTING	
Port	161
Permit	<input type="checkbox"/> Set Requests <input type="checkbox"/> v1 Protocol <input type="checkbox"/> v2c Protocol <input checked="" type="checkbox"/> v3 Protocol
Submit Reset	

▼ To Configure SNMP Port and Permit

1. Select SNMP Settings from the SNMP drop-down list, and click Select.
2. Enter the Port number.
3. Select the Permit check boxes that apply.

The Permit check box options are:

Set Requests

v1 Protocol

v2cProtocol

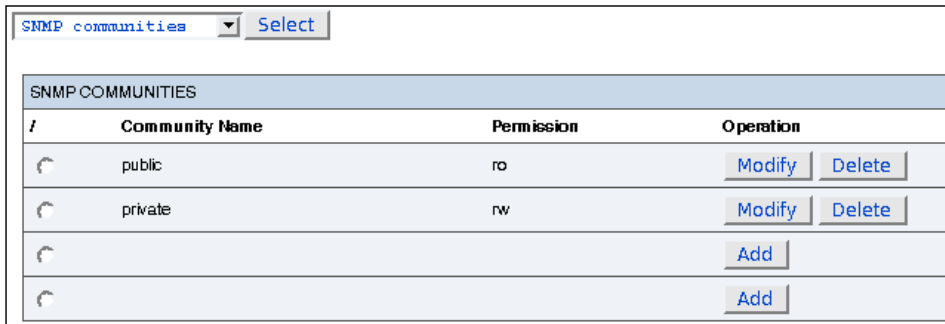
v3 Protocol

4. Click Submit to save your changes.

The SNMP Communities Screen

The SNMP Communities screen allows you to Add, Modify, or Delete communities (see [FIGURE 5-13](#)).

FIGURE 5-13 The SNMP Communities Screen



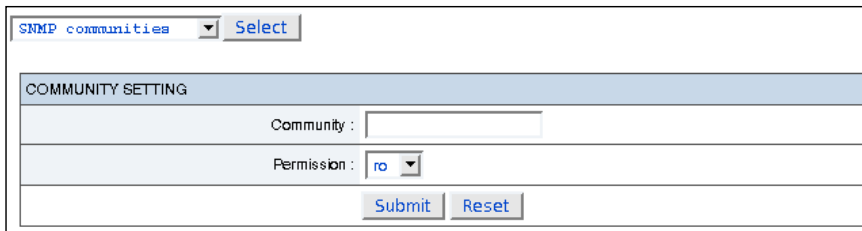
SNMP COMMUNITIES			
/	Community Name	Permission	Operation
<input type="radio"/>	public	ro	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
<input type="radio"/>	private	rw	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
<input type="radio"/>			<input type="button" value="Add"/>
<input type="radio"/>			<input type="button" value="Add"/>

▼ To Add a Community

1. Select Communities Settings from the SNMP drop-down list, and click Select.
2. Click the radio button next to a vacant field in the Community Name column.
3. Click the Add button in the Operation column.

The Community Setting Screen appears (see [FIGURE 5-14](#)).

FIGURE 5-14 Community Setting Screen



COMMUNITY SETTING	
Community :	<input type="text"/>
Permission :	<input type="text" value="ro"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

4. Enter a the new name in the Community field.

5. **Select the permission level from the Permissions drop-down list.**

The two options are:

Permission	Definition
ro	Read-only
rw	Read and write

6. **Click Submit to save your changes and add a new Community.**

▼ To Modify a Community

1. **Click the radio button next to the name of the Community you want to modify (see [FIGURE 5-13](#)).**
2. **Click the Modify button in the same row in the Operation column.**
The Community Setting screen appears (see [FIGURE 5-14](#)). You can change the Community Name and the Permission.
3. **Click Submit to save your changes, or click Reset and Submit to exit the User Setting screen without modifying the settings.**

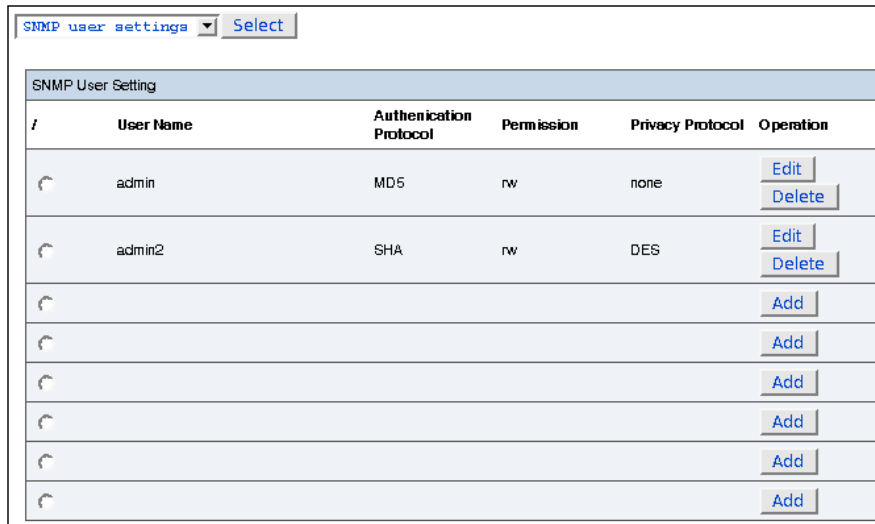
▼ To Delete a Community

1. **Click the radio button next to the name of the Community you want to delete (see [FIGURE 5-13](#)).**
2. **Click the Delete button in the same row in the Operation column.**
The Community is deleted.

The SNMP User Settings Screen

The SNMP User Settings screen summarizes the current SNMP users, and allows you to Add, Modify or Delete Users (see [FIGURE 5-15](#)).

FIGURE 5-15 The SNMP User Setting Screen



SNMP user settings

SNMP User Setting					
#	User Name	Authentication Protocol	Permission	Privacy Protocol	Operation
<input type="radio"/>	admin	MD5	rw	none	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="radio"/>	admin2	SHA	rw	DES	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="radio"/>					<input type="button" value="Add"/>
<input type="radio"/>					<input type="button" value="Add"/>
<input type="radio"/>					<input type="button" value="Add"/>
<input type="radio"/>					<input type="button" value="Add"/>
<input type="radio"/>					<input type="button" value="Add"/>
<input type="radio"/>					<input type="button" value="Add"/>

▼ **To Add an SNMP User**

1. **Select SNMP User Settings from the SNMP drop-down list, and click Select.**
2. **Click the radio button next to a vacant field in the User Name column.**
3. **Click the Add button in the same row in the Operation column.**

The User Setting screen appears (see [FIGURE 5-16](#)).

FIGURE 5-16 The SNMP User Setting Screen

4. Enter the required information to create a new User. The User Setting fields and applicable options are defined in TABLE 5-2.

TABLE 5-2 User Setting Fields.

User Setting Fields	Options
Username	1-32 characters
Auth Protocol	MD5, SHA
Auth Password	1-2 characters
Confirm Password	
Permission	rw (read/write) ro (read-only)
Privacy Protocol	none, DES
Privacy Password	1-32 characters
Confirm Password	

5. Click Submit to create a new user, or click Reset and Submit to exit the User Setting screen without creating a new User.

▼ To Edit an SNMP User

1. Click the radio button next to a User name in the User Name column (see [FIGURE 5-15](#)).
2. Click the Edit button in the same row in the Operations column.
3. The User Setting screen appears (see [FIGURE 5-16](#)).
Edit the User Setting fields (see [TABLE 5-2](#)).
4. Click Submit to save your edit, or click Reset and Submit to exit the User Setting screen without changing the settings.

▼ To Delete an SNMP User

1. Click the radio button next to a User name in the User Name column (see [FIGURE 5-15](#)).
2. Click the Delete button in the same row in the Operation column.
The User is deleted.

Managing Users

The ELOM User Management screens provide access to the system administrative functions associated with the management of users. The User Management tab consists of two screens:

- [“User Account” on page 66](#)
- [“ADS Configuration” on page 72](#)

User Account

The User Account screen allows users with Administrator privileges to manage user access to the ELOM. Administrators can add users, change user passwords and privileges, and enable, disable and delete users.

This section contains the following:

- [“To Access the User Account Screen” on page 67](#)
- [“To Add Users” on page 68](#)
- [“To Change a User Password” on page 70](#)

- “To Change User Privilege” on page 70
- “To Disable and Enable a User” on page 71
- “To Delete a User” on page 71

▼ To Access the User Account Screen

1. **Log in to the ELOM using root or another account with Administrator privileges.**

The ELOM main screen appears.

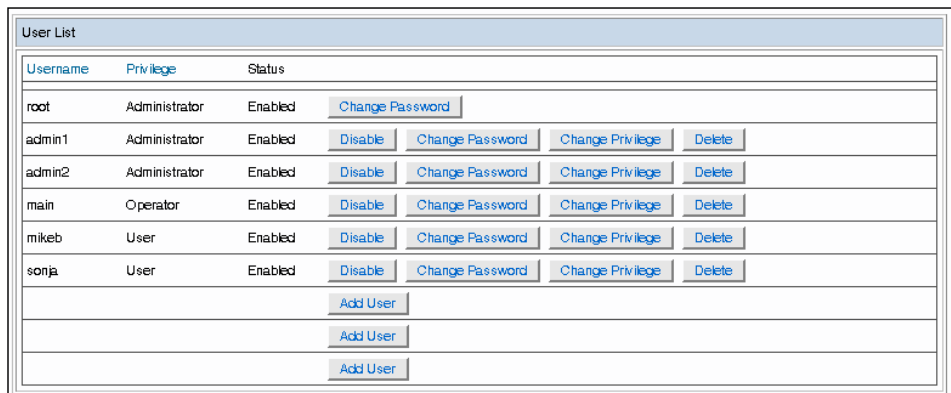
2. **Click the User Management tab on the main menu.**

The User Management submenu screen appears.

3. **Click the User Account submenu tab.**

The User Account screen appears (see [FIGURE 5-17](#)).

FIGURE 5-17 The User Account Screen



User List			
Username	Privilege	Status	
root	Administrator	Enabled	Change Password
admin1	Administrator	Enabled	Disable Change Password Change Privilege Delete
admin2	Administrator	Enabled	Disable Change Password Change Privilege Delete
main	Operator	Enabled	Disable Change Password Change Privilege Delete
mikeb	User	Enabled	Disable Change Password Change Privilege Delete
sonja	User	Enabled	Disable Change Password Change Privilege Delete
Add User			
Add User			
Add User			

The User Account screen summarizes the current user accounts for the ELOM. The ELOM allows up to nine users, eight user accounts and the root account. The root account is the default account. Root has permanent Administrator privileges. The root account cannot be deleted, nor can it be disabled. However, additional user accounts with Administrator privileges can be added.

The User Account screen allows an Administrator to perform the following functions:

- Add users (up to eight)
- Change a user password
- Disable user access

- Change user privileges
- Delete users

▼ To Add Users

The ELOM allows for a total of nine user accounts, including the root account. When adding users, Administrators must enter values for the following settings: the Username, the Password, and the Privilege. [TABLE 5-3](#) lists the three User variables and the value limitations or options for each.

TABLE 5-3 User Variables and Limitations

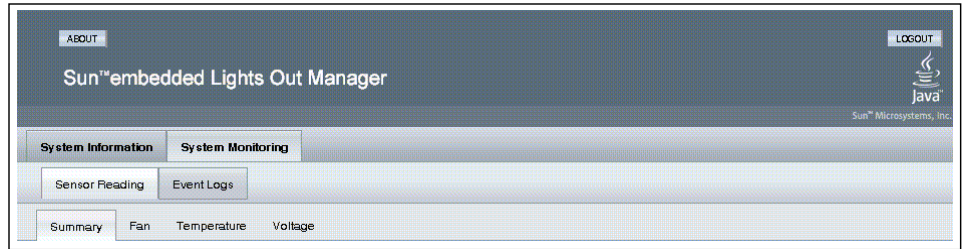
Setting	Limitations or Options
Username	1-16 characters A-Z or 0-9
Password	8-20 characters Any character
Privilege	Administrator Operator User Callback

The Privilege Setting

The privilege setting determines user access to the ELOM.

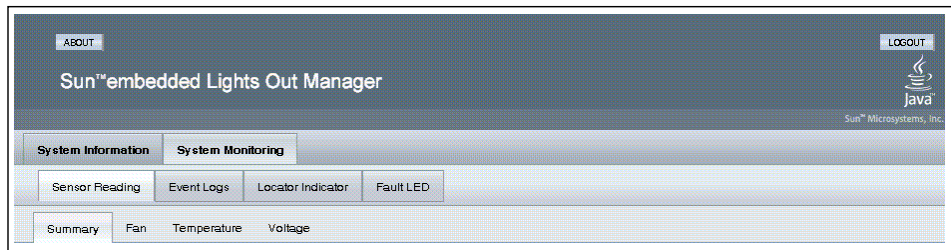
- The Administrator privilege has full access to all menus, and can configure the software and add users.
- The User and Callback privileges have the least amount of system access. Both privileges are limited to the System Management and System Monitoring screens (see [FIGURE 5-18](#)).

FIGURE 5-18 The User and Callback Screen Limitation



- The Operator privilege has limited access. Operators are limited to the System Management and System Monitoring screens. However, unlike the User and Callback privileges, Operators have access to the Locator Indicator and the Fault LED submenu screens (see [FIGURE 5-19](#)).

FIGURE 5-19 The Operator System Screen Limitation



1. Click on the Add button (see [FIGURE 5-17](#)).

The Add User screen appears (see [FIGURE 5-20](#)).

FIGURE 5-20 The Add User Screen

The screenshot shows the 'Manage User Account' form. It has a title bar 'Manage User Account' and a light blue header. The form contains four input fields: 'Username', 'Password', 'Confirm', and 'Privilege'. The 'Privilege' field is a drop-down menu currently set to 'Administrator'. At the bottom of the form, there are two buttons: 'Submit' and 'Reset'.

2. Enter the values for each field, based on the limitations listed in [TABLE 5-3](#).

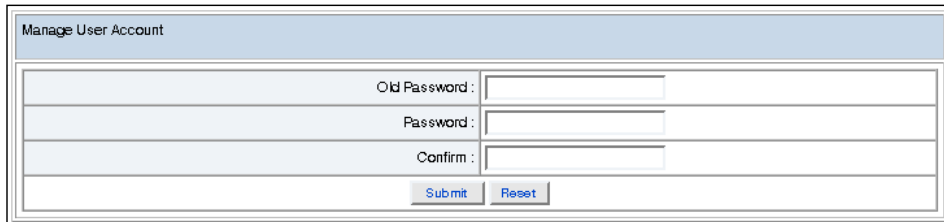
Use the Privilege drop-down list to set privilege level.

3. Click **Submit** to save your changes and add the user.

▼ To Change a User Password

1. Click the **Change Password** button for the User (see [FIGURE 5-17](#)).
The Change User Password screen appears (see [FIGURE 5-21](#)).

FIGURE 5-21 The Change User Password Screen



Manage User Account	
Old Password :	<input type="text"/>
Password :	<input type="text"/>
Confirm :	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

2. Enter the original password in the **Old Password** field.
3. Enter the new password in both the **Password** and the **Confirm** field.

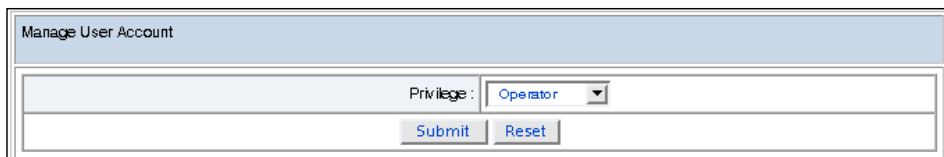
Note – Passwords can be any character, but must be between 8 - 16 characters in length (see [TABLE 5-3](#)).

4. Click the **Submit** button to change the password.

▼ To Change User Privilege

1. Click the **Change User Privilege** button in the User Account screen (see [FIGURE 5-17](#)).
The Change User Privilege screen appears (see [FIGURE 5-22](#)).

FIGURE 5-22 The Change User Privilege Screen



Manage User Account	
Privilege :	Operator ▼
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

2. **Select the new privilege from the Privilege drop-down list. For information about the Privilege setting, see “The Privilege Setting” on page 68.**
3. **Click Submit to save your changes.**

▼ To Disable and Enable a User

Disabling a user allows you to remove a User’s access to the ELOM, without deleting the user entirely.

Disabling a User

- **Click the Disable button for the User in the User Account screen.**
The system disables the user without requesting confirmation.

Enabling a User

- **Click the Enable button for the User in the User Account screen.**
The system enables the user.

▼ To Delete a User

1. **Click the Delete button for the User in the User Account screen.**
The system prompts you for confirmation in a pop-up window.
2. **Click OK in the Confirmation pop-up window to delete the user.**

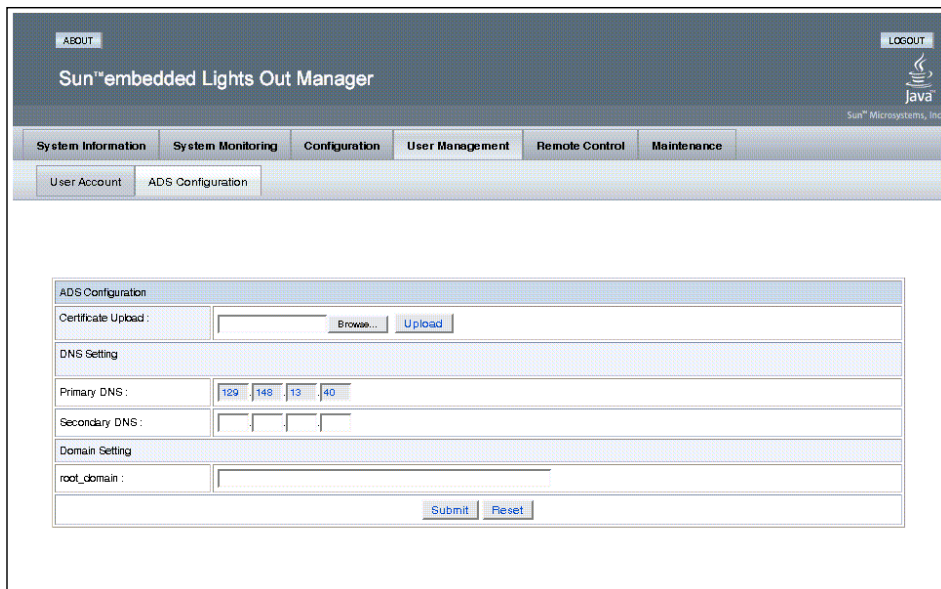
ADS Configuration

The ADS Configuration screen allows you to set up Active Directory Service (ADS).

▼ To Configure ADS

1. **Click the ADS Configuration tab from the User Management submenu.**
The ADS Configuration screen appears (see [FIGURE 5-23](#)).

FIGURE 5-23 The ADS Configuration Screen



The screenshot shows the Sun Embedded Lights Out Manager interface. At the top, there is a navigation bar with tabs for 'System Information', 'System Monitoring', 'Configuration', 'User Management', 'Remote Control', and 'Maintenance'. Below this, there is a sub-menu with 'User Account' and 'ADS Configuration'. The main content area is titled 'ADS Configuration' and contains the following fields:

- Certificate Upload:** A text input field with 'Browse...' and 'Upload' buttons.
- DNS Setting:**
 - Primary DNS:** A text input field with the value '129.148.13.40'.
 - Secondary DNS:** A text input field.
- Domain Setting:**
 - root_domain:** A text input field.

At the bottom of the form, there are 'Submit' and 'Reset' buttons.

2. **Browse for the Certificate on your local machine, and click Upload.**
3. **Provide the Primary and Secondary DNS addresses.**
4. **Enter the root_domain name.**
5. **Click Submit to save your settings.**

Service Processor Maintenance

This section contains information about the ELOM Maintenance menu. The ELOM Maintenance menu allows you to perform basic service processor-related tasks. The Maintenance submenu consists of two screens:

- Firmware Upgrade
- Reset SP

This section contains the following sub-sections:

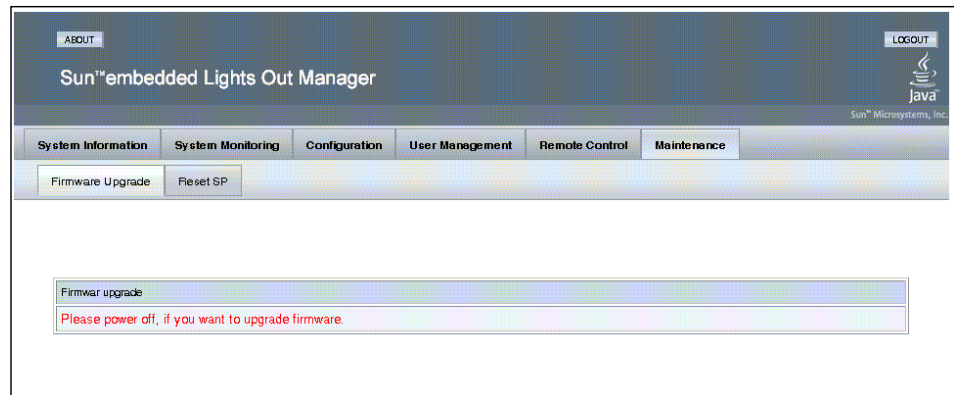
- [“To Access the Maintenance Screens” on page 73](#)
- [“To Upgrade Firmware” on page 74](#)
- [“To Reset the Service Processor” on page 76](#)

▼ To Access the Maintenance Screens

1. **Login in to the ELOM using root, or another account that has Administrator privileges.**
2. **Click the Maintenance tab.**

The Maintenance submenu appears (see [FIGURE 5-24](#)).

FIGURE 5-24 The Firmware Upgrade Screen

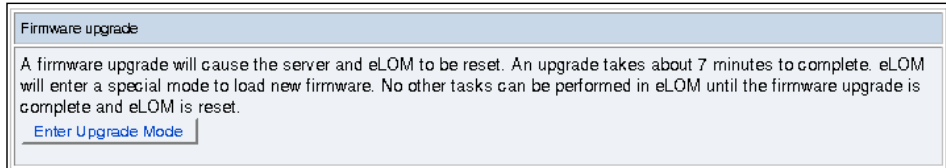


▼ To Upgrade Firmware

1. Click the Firmware Upgrade tab.

The Firmware Upgrade screen appears (see [FIGURE 5-25](#)).

FIGURE 5-25 The Firmware Upgrade Screen



The screen contains an Enter Upgrade Mode Button, and displays the following informational message regarding the upgrade process:

A Firmware upgrade will cause the server and eLOM to be reset. An upgrade takes about 7 minutes to complete. eLOM will enter a special mode to load new firmware. No other tasks can be performed in eLOM until the firmware upgrade is complete and eLOM reset.

2. Click the Enter Upgrade Mode button.

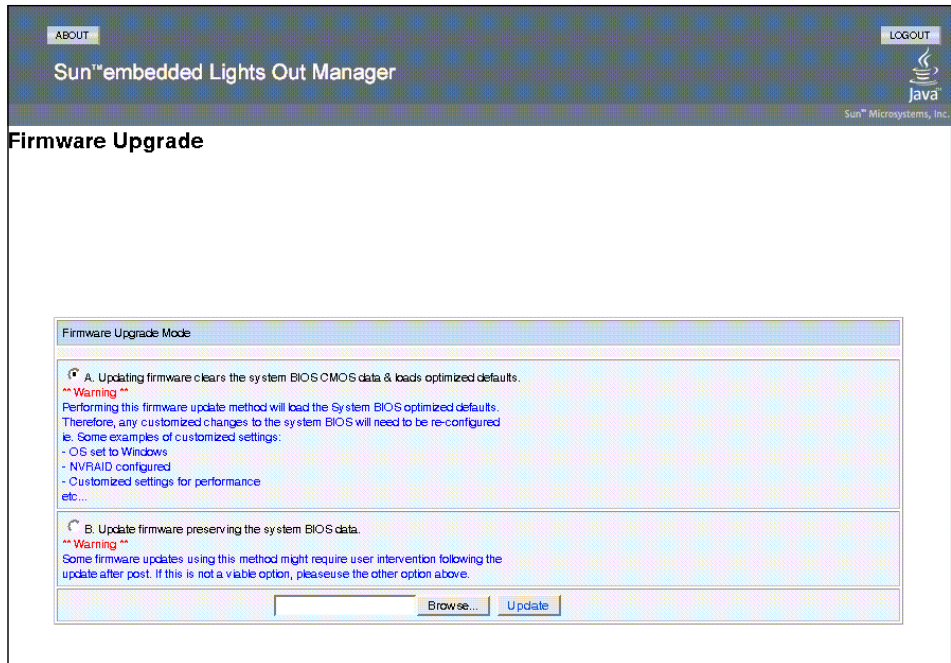
An Upgrade Mode confirmation screen appears.

Caution – You will not be able to perform any tasks until the upgrade is complete and the Service Processor is rebooted.

3. Click OK at the Confirmation screen.

The Firmware Upgrade screen appears (see [FIGURE 5-26](#)).

FIGURE 5-26 The Firmware Upgrade Mode Screen: Method A Selected



The Firmware Upgrade Mode Screen presents you with two upgrade options:

- Option A updates the firmware, clearing the system BIOS CMOS data and loading optimized defaults. Use this option if you want to clear previous BIOS settings. This option is accompanied by the following onscreen warning:

****Warning****

Performing this firmware update method will load the System BIOS optimized defaults.
Therefore, any customized changes to the system BIOS will need to be re-configured
ie. Some examples of customized settings:
- OS set to Windows
- NVRAID configured
- Customized settings for performance
etc...

- Option B updates the firmware preserving the system BIOS data. Use this option if you want to preserve your system's customized BIOS data. For example, you might use this option if you have your OS set to Windows, and do not want to reconfigure it. This option is accompanied by the following onscreen warning:

**** Warning ****

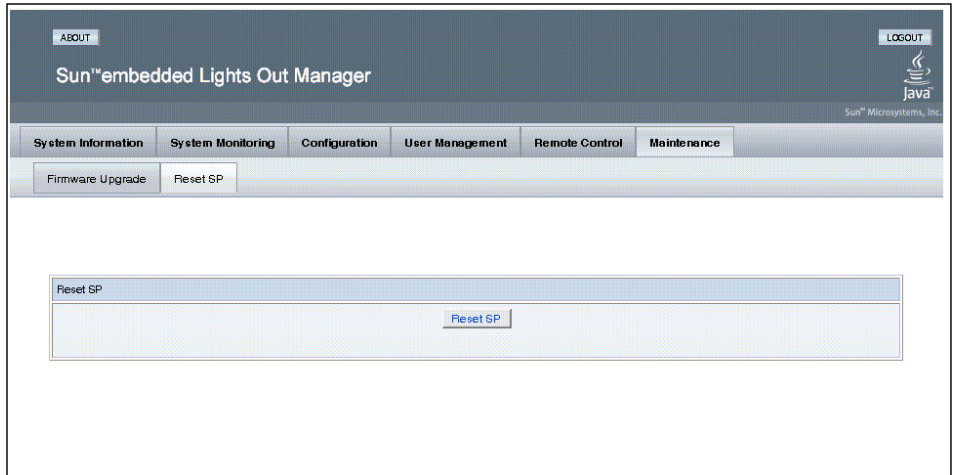
Some firmware updates using this method might require user intervention following the update after post. If this is not a viable option, please use the other option above.

4. **Click the radio button for the update option that you prefer.**
5. **Click Browse, and point to the file located on the Tools and Drivers CD/DVD in: */remoteflash/fwrev/filename***
fwrev The directory of the firmware revision.
filename The name of the firmware update file.
6. **Click Update.**
The update process begins. After the upgrade process is complete, you will have to log out and log back in to the ELOM web-based interface.

▼ To Reset the Service Processor

1. **Click the Reset SP tab.**
The Reset SP screen appears (see [FIGURE 5-27](#)).

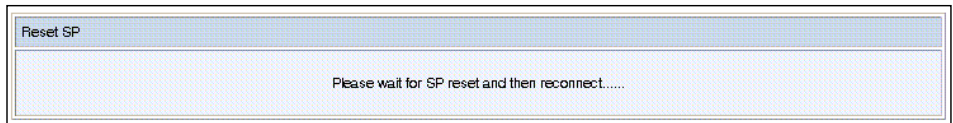
FIGURE 5-27 The Reset SP Screen



2. Click the Reset SP button.

The SP begins the reset process (see [FIGURE 5-28](#)).

FIGURE 5-28 The SP Reset Screen During Reset



3. Wait for the SP to reset, and then reconnect to the ELOM.

Using the Remote Control Screens

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

- [“About the Remote Console Application” on page 79](#)
 - [“Launching the Remote Console Application” on page 80](#)
 - [“Configuring KVM Functionality for a Remote Console Session” on page 85](#)
 - [“Controlling Power to a Remote Server” on page 89](#)
 - [“Installing an Operating System on a Remote Server” on page 90](#)
 - [“Other Remote Options” on page 92](#)
-

About the Remote Console Application

The Remote Console application, which you launch using the web-based interface Remote Control Redirection sub-menu screen, enables you to:

- Control your server’s operating system remotely using the local keyboard, video and mouse (KVM).

The redirection of the KVM enables you to use the operating system and other GUI-based programs instead of restricting you to the command-line based utilities provided by terminals and emulators.

- Redirect CD/DVD drives, Flash drives, diskette drives, hard drives, or NFS as if they were connected directly to the server.

This enables you to download and upload software using the CD and diskette drives as if they were local to the server.

Remote Console Operating Requirements

A compatible web browser and a minimum of JRE 1.5 Update 7 are required to operate the remote console application. See [TABLE 6-1](#) for Client installation requirements.

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

TABLE 6-1 Client Installation Requirements

Client OS	Java Runtime Environment Including Java Web Start	Web Browsers
Microsoft Windows XP Pro	JRE 1.5 (Java 5.0 Update 7 or later)	Internet Explorer 6.0 and later Mozilla 1.7.5 or later Mozilla Firefox 1.0
Red Hat Linux 3.0 and 4.0 Desktop and Workstation Editions	JRE 1.5 (Java 5.0 Update 7 or later)	Mozilla 1.7.5 or later Mozilla Firefox 1.0
Solaris 10	JRE 1.5 (Java 5.0 Update 7 or later)	Mozilla 1.7.5
SUSE Linux 9.2	JRE 1.5 (Java 5.0 Update 7 or later)	Mozilla 1.7.5

Note – You can download the Java 1.5 runtime environment at <http://java.com>.

Launching the Remote Console Application

Use this procedure to launch the Remote Console application from the web-based interface.

Note – Each new Sun Fire X2100 M2 and Sun Fire X2200 M2 system is delivered with DHCP set as the default. If an IP address is not found within 5 seconds, the system will default to an IP address based on the MAC address and starting with 192.

▼ To Launch the Remote Console Application

1. **Open your web browser.**

2.

The Sun embedded Lights Out Manager (ELOM) login screen appears.

3. **Enter a login that has administrator privileges, or use the default user name and password:**

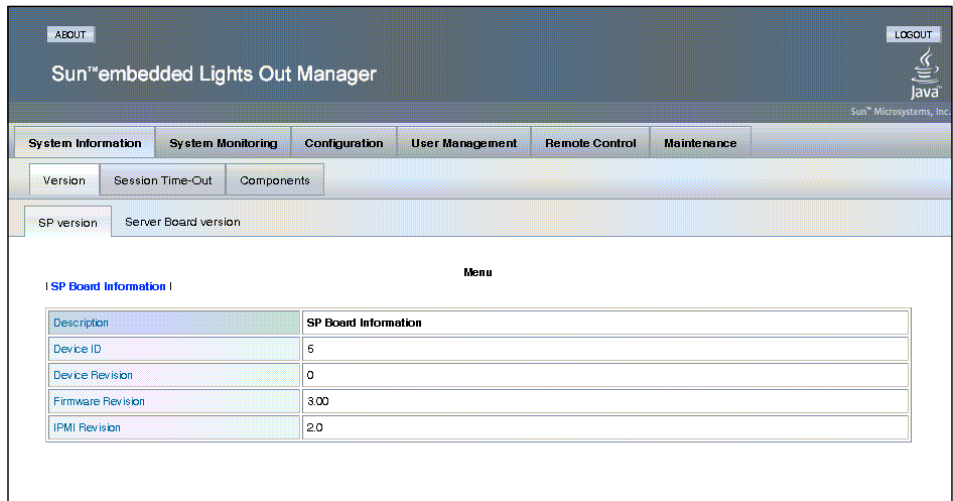
Username: **root**

Password: **changeme**

4. **Click Login.**

The Embedded LOM Manager screen appears (see [FIGURE 6-1](#)).

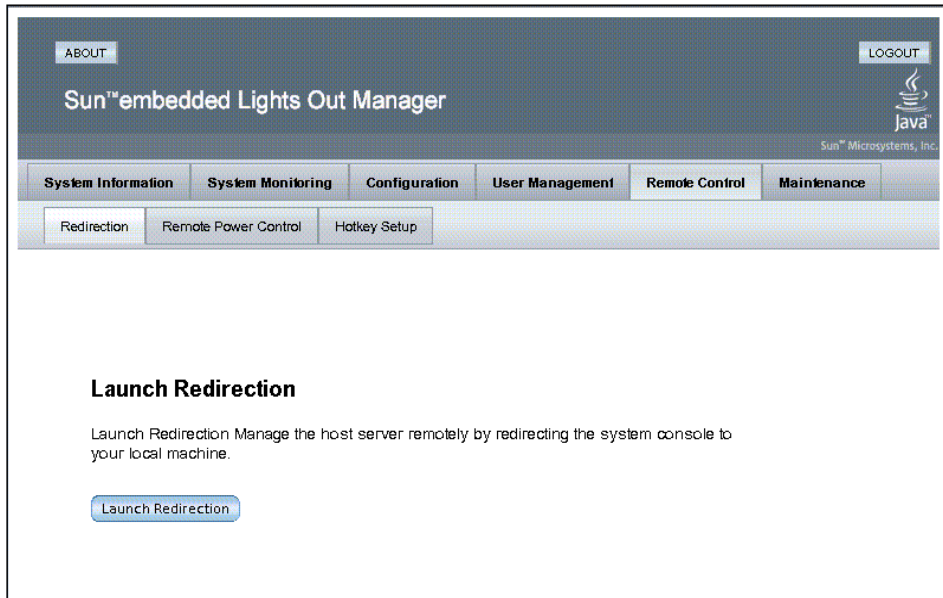
FIGURE 6-1 The ELOM System Status Screen



5. **Click the Remote Console tab on the main menu.**

The Remote Console screen appears (see [FIGURE 6-2](#)).

FIGURE 6-2 The Remote Console Redirection Screen



6. Click the Redirection tab.

The Redirection screen appears (see [FIGURE 6-2](#)). The Redirection screen consists of a Launch Redirection button and the following message:

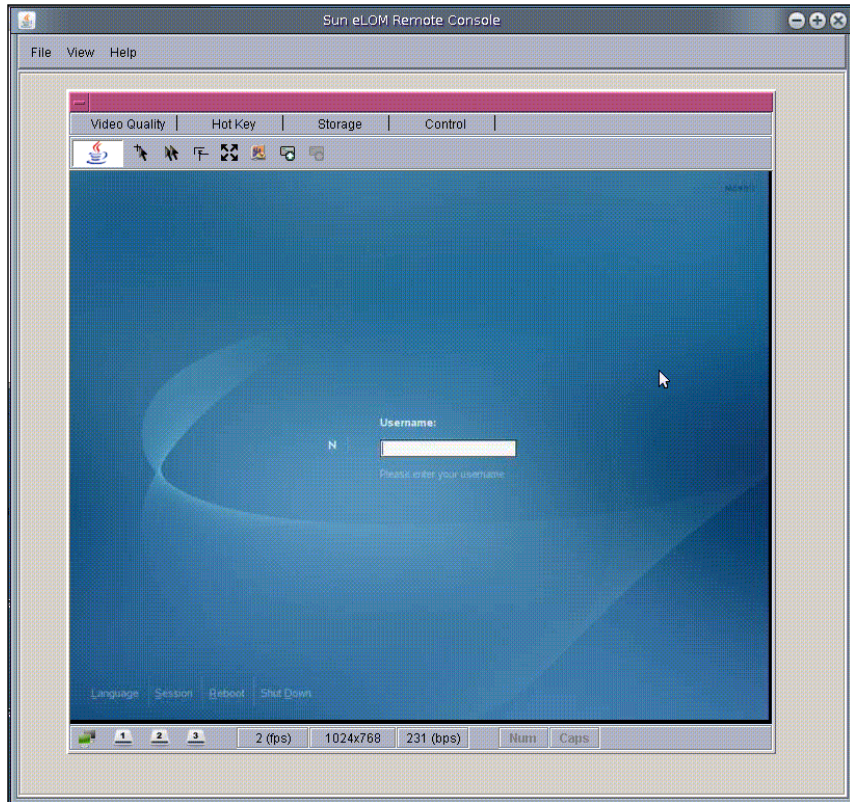
Launch Redirection Manage the host server remotely by redirecting the system console to your local machine.

7. Click the Launch Redirection button.

Note – For systems using Firefox and Mozilla web browsers, the required version of Java RTE must be at least version 5 update 7 or later.

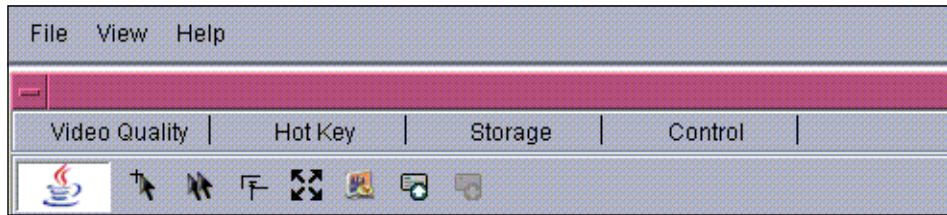
The web browser downloads and automatically starts the remote control application. The remote server console screen appears inside the Sun ELOM Remote Console screen (see [FIGURE 6-3](#)).

FIGURE 6-3 The Remote Console Screen



Nested within the Sun ELOM Remote Console screen is the remote sever screen. Both screens have a menu bar (see [FIGURE 6-4](#)).

FIGURE 6-4 The Remote Console Main Menu



The Sun ELOM Remote Console screen menu bar has the following selections:

File: allows you to log in to and exit from the Remote Console application.

View: show or hides the server window tool bar display.

Help: provides copyright, version, and release information.

The remote server console window consists of a main menu and a tool bar (see [FIGURE 6-4](#)) with the following selections:

Video Quality: offers choice of low, medium, high video display resolutions.

HotKey: enables access to the current hot keys.

Storage: allows you to Mount and Unmount devices and change the ISO image.

Control: provides access to configurable KVM functions, allows you to save a KVM configuration, and exit remote console.

Toolbar: change the video gamma and access to storage and KVM functions.

Configuring KVM Functionality for a Remote Console Session

This section details the server window menus, and explains how to configure, customize, and save the keyboard, video, and mouse (KVM) functionality for a Remote Console session.

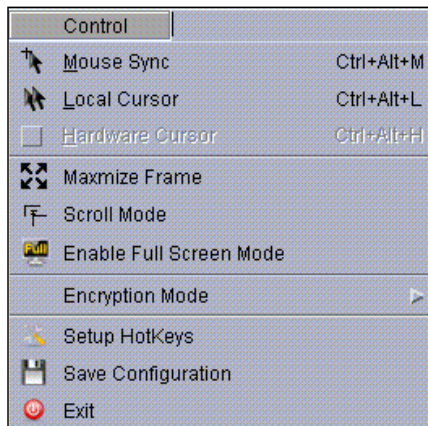
▼ To Configure KVM Functionality for a Remote Console Session

1. **Launch the Remote Console application** (see [“Launching the Remote Console Application”](#) on page 80).

2. **Click the Control tab from the server console main menu.**

The Control menu appears (see [FIGURE 6-5](#)).

FIGURE 6-5 The Control Menu



The Control menu consists of ten configurable KVM functions/modes. [TABLE 6-2](#) lists and describes the functions.

TABLE 6-2 Control Menu Functions

Function	Description
Mouse Sync	Displays a single mouse cursor in the Remote Console screen. When the mouse leaves the remote server console screen the local cursor takes over and the server console mouse remains in the remote server console screen.
Local Cursor	Produces two separate mouse cursors (local and remote) that are displayed at all times, even when the local mouse is moved within the server console screen.
Hardware Cursor	Displays a single mouse cursor, similar to Mouse Sync mode. However, the mouse data is separated from the video data, producing smoother mouse action.
Maximize Frame	Resizes the server console screen to actual size.
Scroll Mode/Fit Mode	Determines whether the console display will scale-to-fit a manually resized screen (Fit Mode), or whether resizing the screen will have no scaling effect on the display (Scroll Mode). In Scroll Mode, decreasing the screen size will produce scroll bars.
Enable Full Screen Mode	Resizes the server screen to full size of the local monitor.
Encryption Mode	Allows the securing of KVM data over the network. The choices are: Encrypt All, None, Keyboard and Mouse Only, or Video Only.
Setup Hotkeys	Setup and define up to 16 hot keys (see “To setup up hot keys:” on page 86).
Save Configuration	Retain the current KVM settings for the current session and future sessions (login-specific).
Exit	Exit the Remote Console application.

3. Configure the KVM by selecting the functions/modes you would like enabled.

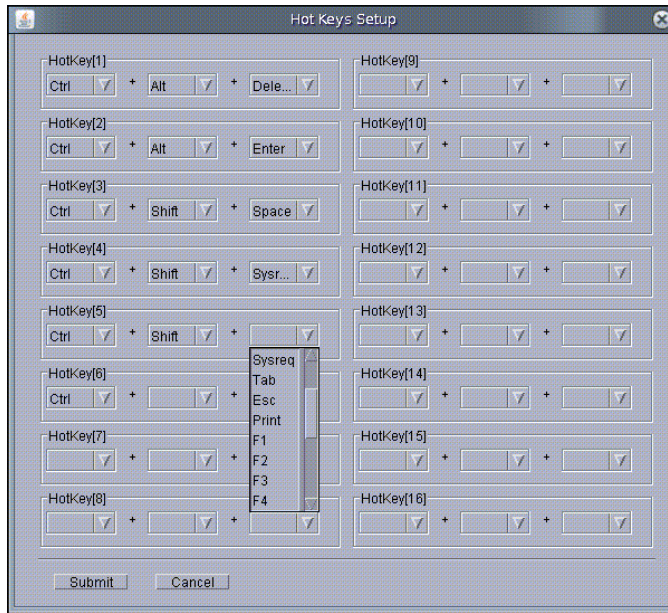
4. Click Save Configuration to save the KVM configuration.

To setup up hot keys:

1. Click Setup Hotkeys from the Control menu.

The Setup Hotkeys window appears (see [FIGURE 6-6](#)).

FIGURE 6-6 The HotKeys Setup Window



The Hotkeys Setup window allows you to configure up to 16 hot keys, using three key combinations. TABLE 6-3 lists the choices for each key. Key 1 has a single key associated with it and two possible choices (no key or the Ctrl key). Key2 has two key choices (three possibilities), and Key 3 has 20 key choices (21 possibilities).

TABLE 6-3 Hot Key Combinations

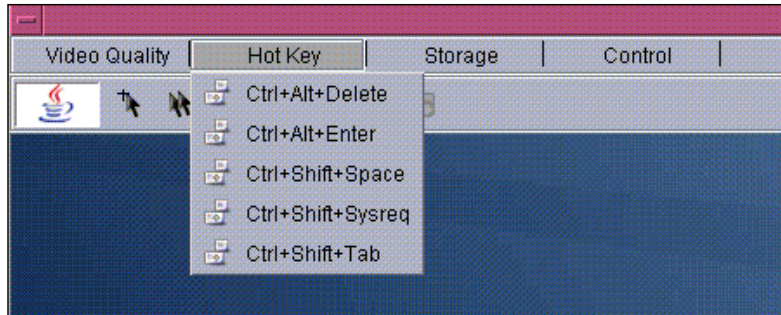
Key 1	+ Key 2	+ Key 3
None	+ None	+ None
Ctrl	Alt	Delete
	Shift	Enter
		Space
		SysReq
		Tab
		Esc
		Print
		F1 - F12
		Backspace

2. Configure the hot key combinations by clicking on the drop-down list and selecting the keystroke for each of the three keys (see FIGURE 6-6).

3. Click Submit.

To use a hot key, click the HotKey tab and select the key from the drop-down list (see [FIGURE 6-7](#)).

FIGURE 6-7 HotKey drop-down list



Controlling Power to a Remote Server

This section explains how to access the web-based interface's Remote Power Control submenu screen, and how to initiate power-related actions to control the remote server's power status.

To access the Remote Power Control submenu screen:

1. **Log in to the web-based interface using a login with Administrator privileges, or use the default user name and password:**

Username: **root**

Password: **changeme**

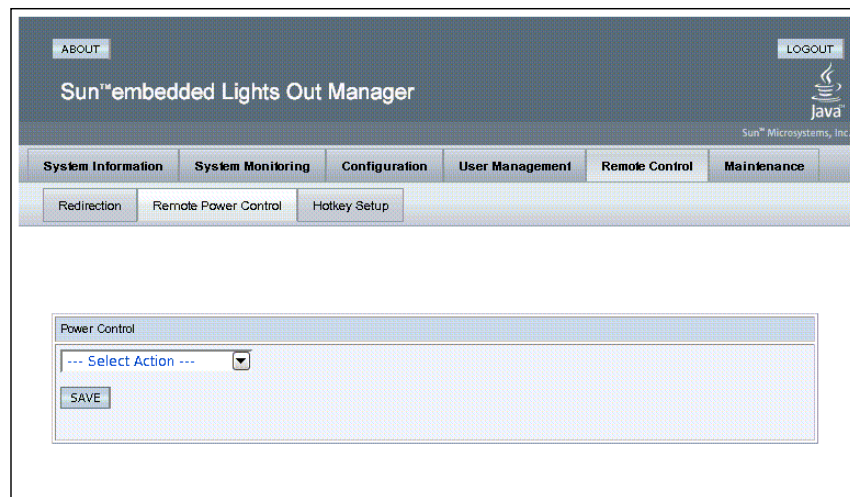
2. **Click the Remote Control tab on the main menu.**

The Remote Control submenu appears.

3. **Click the Remote Power Control submenu tab.**

The Remote Power Control screen appears (see [FIGURE 6-8](#)).

FIGURE 6-8 The Remote Power Control Screen



This screen contains the Power Control window. Using the Power Control's drop-down list, you can perform the following five power-related actions on the remote server:

Power Action	Description
Reset	Reboots the server
Force Power Off	Instant power-off
Graceful Shutdown	Normal power-off
Boot Option: BIOS Setup	Restarts the server and automatically enters the BIOS setup menu.
NMI	Non-Maskable Interrupt

Tip – Use the Remote Power Control submenu screen during a Remote console session to access the remote server’s BIOS setup menu and to view start-up messages.

To initiate power-related actions on the remote server:

1. **Select an action from the drop-down list in the Power Control window.**
2. **Click Save.**

The power action is initiated immediately.

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 a remote 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 remote server has been set up as instructed in the platform-specific *Server Installation Guide*.

▼ To Install an OS on a Remote Server Using Virtual CDROM

Note – Disable the time-out function when installing remotely from the virtual CD-ROM.

1. Open a web browser, and enter the IP address for the service processor (SP) of the remote server on which you want to install the operating system.
2. Enter your user name and password at the login screen, and click Login.

Note – The user must have Administrator privileges.

3. Select the Remote Control tab from the main menu.
4. Click the Redirection submenu tab.
5. Click the Launch Redirection button in the Redirection screen.
6. Insert the Operating System CD/DVD into the local CD/DVD drive.
7. In the remote server console screen, click Storage, and select Mount Device.
The Device Configuration screens appears.
8. Under Storage 1, click the drop-down arrow, and highlight the local CD/DVD to be used for installing.
9. Click Submit.
10. Click the Remote Power Control tab in the Remote Control submenu screen (in the web-based interface).
The Remote Power Control submenu screen appears.
11. Select Reset from the Power Control drop-down list.
12. Click Save to reboot the server.
The remote server boots off the local CD/DVD drive, and the OS installation begins.

Note – After the OS is installed, unmount the local CD-ROM if you want to use a CD or DVD device installed or connected to your system.

Other Remote Options

Command line options that are available on your local server include IPMI tools ([Chapter 7](#)), CLI ([Chapter 8](#)), 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 93.](#)
- [“Supported IPMI 2.0 Commands” on page 95.](#)

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 baseboard management controllers (BMCs), which are located on IPMI-compliant hardware components such as the service processor (SP). Using low-level hardware intelligence instead of the operating system has two main benefits: first, this configuration enables 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 Sun Fire X2100 M2 or Sun Fire X2200 M2 server which runs a daemon to:

- 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 (ELOM)
- Support Serial-On-LAN (SOL)
- Customize FRU/Sensor Data Record data (firmware independent)
- Provide KVM over IP (remote access to the server)

- Enable 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 Embedded Lights Out Manager 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 v1.5 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 Resource 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 pre-installed version of IPMItool in the following directory: `/usr/sfw/bin`. The binary is called `ipmitool`.

Sensors

Your server includes a number of IPMI-compliant sensors that measure things such as voltages, temperature ranges, and security latches that detect when the enclosure is opened. For a complete list of sensors, see your platform supplement.

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, remove the `-P` from the command line above, and enter the password when prompted.

Supported IPMI 2.0 Commands

TABLE 7-1 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 7-1 Supported IPMI 2.0 Commands

Supported IPMI 2.0 Commands

General Commands

Get Device ID
Cold Reset
Warm 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 Command

TABLE 7-1 Supported IPMI 2.0 Commands (*Continued*)

Supported IPMI 2.0 Commands (Continued)

Set/Get User Access Command

Set/Get User Name

Set User Password Command

Master Write-Read

Set/Get Chassis Capabilities

Get Chassis Status

Chassis Control

Chassis Identify

Set Power Restore Policy

Get System Restart Cause

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

TABLE 7-1 Supported IPMI 2.0 Commands (*Continued*)

Supported IPMI 2.0 Commands (Continued)

Sensor Device Commands

Get Sensor Reading Factors
Set/Get Sensor Hysteresis
Set/Get Sensor Threshold
Set/Get Sensor Event Enable
Get Sensor Reading
Set Sensor Type

FRU Device Commands

Get FRU Inventory Area Info
Read/Write FRU Data SDR Device
Commands
Get SDR Repository Info
Get SDR Repository Allocation
Reserve SDR Repository
Get/Add SDR
Partial Add SDR
Clear SDR Repository
Get SDR Repository Time
Enter/Exit SDR Repository Update
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

TABLE 7-1 Supported IPMI 2.0 Commands (*Continued*)

Supported IPMI 2.0 Commands (Continued)

LAN Device Commands

Get LAN Configuration Parameters

Suspend BMC ARPs

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

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 99.](#)
- [“Command Syntax” on page 101.](#)
- [“Managing the Host” on page 103.](#)
- [“Managing the Host” on page 103.](#)
- [“Managing the ELOM Network Settings” on page 105.](#)
- [“Managing User Accounts” on page 106.](#)
- [“Resetting the SP Password” on page 108](#)
- [“Managing Alerts” on page 109.](#)
- [“Updating the Firmware” on page 113.](#)
- [“Displaying Version Information” on page 114](#)

Logging In to the CLI

You can access the command line 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.
- **SSH** –You can connect to the CLI using an Ethernet connection. Secure shell connections (SSH) are enabled by default.

The embedded lights out manager (Embedded LOM) supports a maximum of 10 active sessions, including serial, SSH, and web interface sessions.

Note – Telnet connections to the ELOM are not supported.

▼ To Log In Using SSH

This section describes how to log in to the service processor using secure shell.

1. **Start your SSH client.**
2. **To log into the ELOM, enter:**

```
$ ssh root@SPipaddress
```

3. **Enter your password when prompted.**

Note – The default user name is **root**, and the default password is **changeme**.

For example:

```
$ ssh root@192.168.25.25
```

```
root@192.168.25.25's password:
```

```
Sun (TM) Embedded Lights Out Manager
```

```
Version 1.0
```

```
Copyright 2006 Sun Microsystems, Inc. All rights reserved.
```

```
Warning: password is set to factory default.
```

```
/SP ->
```

▼ To Log In From the Serial Port

This section describes how to log in to the service processor from the serial port using a terminal device.

1. **Configure your terminal device or the terminal emulation software running on a laptop or PC to the following settings:**
 - 8N1: eight data bits, no parity, one stop bit
 - 9600 baud
 - Disabled software flow control (CTS/RTS)
2. **Connect a serial cable from the server RJ-45 Serial Mgt port to a terminal device.**

3. **Press ENTER on the terminal device to establish a connection between that terminal device and the SP.**

You should see the following prompt:

```
SP -> SUNSP0016364A9934 login:
```

4. **Log in to the SP, and enter the user name and password.**

The default user name is **root**, and the default password is **changeme**.

Note – Once you have logged in to the SP as root, change the default password for increased security.

Note – If you have changed the serial redirection output in the system BIOS from BMC (that is, from the SP) to system, the system output will be 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 software includes the `/SP` namespace.

The `/SP` namespace manages the embedded lights out manager. Children of this namespace are `/AgentInfo` and `/SystemInfo` which allow you to use this space to manage users, clock settings, and other issues.

The CLI provides two privilege levels: Administrator and User. Administrators have full access to ELOM functionality and users have read-only access to information.

Note – The default user, root, has administrator privileges. To create a user account with user privileges, see [“Adding a User Account” on page 107](#).

CLI commands are case-sensitive.

Syntax

The syntax of a command is: <verb><options><target><properties>

Command Verbs

TABLE 8-1 describes the CLI command verbs.

TABLE 8-1 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.
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 the ELOM firmware that is running.

Options

The CLI supports the following options. All options are not 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 8-2 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 the user wants to display.
-examine	-x	Examines the command but does not execute it.

TABLE 8-2 CLI Options

Option	Long Form	Short Form	Description
-force		-f	Causes an immediate action instead of an orderly shutdown.
-help		-h	Displays Help information.
-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. All targets are not 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 properties. 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 the following command:

```
set /SP/SystemInfo/CtrlInfo PowerCtrl=on
```

To power off the host gracefully, enter the following command:

```
set /SP/SystemInfo/CtrlInfo PowerCtrl=gracefuloff
```

To power off the host forcefully, enter the following command:

```
set /SP/SystemInfo/CtrlInfo PowerCtrl=forceoff
```

To reset the host, enter the following command:

```
set /SP/SystemInfo/CtrlInfo PowerCtrl=reset
```

To reboot and enter the BIOS automatically, enter the following command:

```
set /SP/SystemInfo/CtrlInfo BootCtrl=BIOSSetup
```

Managing the Host Console

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

```
start /SP/AgentInfo/console
```

Note – After running the start command, no output will be displayed until the server is rebooted.

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 show 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 sensors. Use the command:

```
show /SP/SystemInfo/CPU/sensor
```

sensor A particular sensor. For example, the following command shows the state of sensor /CPU/CPU0:

```
show /SP/SystemInfo/CPU/CPU0
```

For more information about sensors, including how to view them using the web-based interface, see [“Using the System Monitoring Screens” on page 36](#).

For details on individual sensors, see your platform supplement.

Managing the ELOM Network Settings

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

Displaying Network Settings

Enter the following command to display network settings:

```
show /SP/AgentInfo
```

TABLE 8-3

Where:	3=enable
	2=disable

Configuring 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 the ELOM. This enables the ELOM to be easily located on the network.

Syntax

```
set /SP/AgentInfo IpAddress=xxx.xxx.xxx.xxx
```

Targets, Properties, and Values

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

TABLE 8-4

Target	Property	Value	Default
/SP/AgentInfo	IpAddress	iIP address none	192.168. <i>Last 2 digits of MAC address</i>
	DhcpConfigured	enabled disabled	enabled
	Gateway	iIP address none	none
	Netmask	IP address format	255.255.255.0

Examples

To change the IP address for the ELOM, enter:

```
set /SP/AgentInfo IpAddress=xxx.xxx.xxx.xxx
```

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

To set the Gateway address for the ELOM, enter:

```
set /SP/AgentInfo Gateway=xxx.xxx.xxx.xxx
```

To change the network settings from static to DHCP settings, enter:

```
set /SP/AgentInfo DhcpConfigured=enable
```

To disable DHCP network settings, enter:

```
set /SP/AgentInfo DhcpConfigured=disable
```

Managing User Accounts

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

The ELOM supports up to 10 user accounts. Two of those, root and anonymous, are set by default, and cannot be removed. Therefore, you can configure eight additional accounts.

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

The roles include:

- **Administrator** – Enables access to all features, functions, and commands.
- **Operator** – Enables limited access to features, functions, and commands. In general, Operators cannot change configuration settings.
- **User** – Enables access to benign commands such as sensor reading.

The syntax is:

```
set Permission=[Administrator|Operator|User]
```

Adding a User Account

Enter the following command to add a local user account:

```
create /SP/User username[1:10]
```

You will be prompted for a password. Then change to the User directory:

```
cd User /SP/User/username
```

```
set /SP/user/user[1:10] Password=password
```

Deleting a User Account

Enter the following command to delete a local user account:

```
delete /SP/User/username
```

Displaying User Accounts

Enter the following command to display information about all local user accounts:

```
show /SP/User
```

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 8-5

Target	Property	Value	Default
/SP/User/ <i>username</i>	Permission	[Administrator Operator User]	Operator
	Password	<i>string</i>	

Examples

To change the permissions for user1 from Administrator to Operator enter:

```
set /SP/User/user1 Permission=Operator
```

To change user1's password enter:

```
set /SP/users/user1 Password=string
```

Resetting the SP Password

You might need to reset the Service Processor password to the original factory default for any number of reasons including a user forgetting the password.

1. Press F2 to enter the BIOS.
2. Under the Advanced tab point to Ipmi 2.0 Configuration.
3. Choose Reset BMC Root Password.
4. To save and exit changes, click OK.

The BMC (SP) password is reset to the default changeme.

Managing Alerts

The system is equipped with a number of strategically placed sensors. The service processor (SP) uses these sensors to monitor critical system parameters for certain key components, such as, power supplies (voltages), CPUs (temperature), and fans (RPM). For the SP to operate efficiently, the components being monitored must perform within a specific range. The SP continually monitors each sensor to see if it is within its range. When a component exceeds its range, the SP generates an alert and posts an event in the system event log (SEL).

Note – All alerts are IPMI PEF traps, as defined in the Intelligent Platform Management Interface (IPMI) v2.0.

You can define which alerts the SP will report. This entails using the Platform Event Traps (PET) and the Platform Event Filters (PEF) to configure alerts to respond to certain rules. You can also configure a destination IP address for the alert. For example, you can configure the SP to send an IPMI trap to a specified destination when any sensor crosses the upper or lower critical temperature (CT) threshold.

Note – The Informational alert level, is reserved for system events that are not related to sensors.

Displaying Alerts

Use the `show` command to display current configurations or to verify changes.

Syntax

set target *propertyname=value*

Enter the following command to display alerts:

show /SP/AgentInfo/PET/Destination[1...4]

show /SP/AgentInfo/PEF

show /SP/AgentInfo/PEF/EventFilterTable[1...6]

Configuring Alerts

Use the set command to change values for properties and configure alerts.

Syntax

```
set target propertyname=value
```

Targets, Properties, and Values

These targets, properties, and values are valid for PET alerts.

TABLE 8-6 PET Targets, Properties, Values, and Defaults

Target	Property	Value	Default
<i>/SP/AgentInfo/PET/[Destination1... Destination4]</i>	IPAddress	IP address	(none)
	MACAddress	MAC Address	(none)
	Status	enable disable	disable

Examples

To configure an alert for Destination1, enter:

```
set /SP/AgentInfo/PET/Destination1=128.145.77.21 Status=enable
```

To turn off Destination1 alert, enter:

```
set /SP/AgentInfo/PEF/Destination1 Status=disable
```


Targets, Properties, and Values

These targets, properties, and values are valid for PEF alerts.

TABLE 8-7 Platform Event Filter Table Properties

Targets	Property	Value	Default
EventFilterTable[1...6]	PEFGlobalCtrl	enable disable	disable
	PEFActionGlobalCtrlPowerOff	enable disable	disable
	PEFActionGlobalCtrlPowerCycle	enable disable	disable
	PEFActionGlobalCtrlPowerReset	enable disable	disable
	PEFActionGlobalCtrlAlert	enable disable	disable
	PEFActionGlobalCtrlMail	enable disable	disable
	PEFActionGlobalCtrlInterrupt	enable disable	disable

Examples

To enable global control of PEF actions, enter the following commands:

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

```
set PEFGlobalCtrl=enable
```

To enable global control for individual actions, such as power cycle, enter:

```
set PEFActionGlobalCtrlPowerCycle=enable
```

To enable global control for individual actions, such as mail, enter:

```
set PEFActionGlobalCtrlMail=enable
```

To disable global control for mail, enter:

```
set PEFActionGlobalCtrlMail=disable
```

Targets, Properties, and Values

These targets, properties, and values are valid for PET event filter tables.

TABLE 8-8 PEF Table Target Properties

Property	Value
Status	enable disable
SensorType	all, temperature, voltage, fan, processor, memory
PowerCtrl	enable disable
DiagnosticInterrupt	enable disable
SendAlert	enable disable
SendMail	enable disable

Examples

To configure EventFilterTable1 to filter all sensors and enable all actions, enter the following commands:

```
cd /SP/AgentInfor/PEF/EventFilterTable1  
set Status=enable  
set SensorType=all  
set PowerCtrl=enable  
set DiagnosticInterrupt=enable  
set SendAlert=enable  
set SendMail=enable
```

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 firmware and the BIOS at the same time.

▼ How to Update the Firmware



Caution – Ensure that you have reliable power before upgrading your firmware. If power to the system fails (for example, if the wall socket power fails or the system is unplugged) during the firmware update procedure, the SP could be left in an unbootable state.



Caution – Shut down your host operating system before proceeding. Otherwise the SP will shut the host down ungracefully, which could cause file system corruption.

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 `bios/bmc` image to your Tftp server.
2. If the server OS is running, perform a clean shutdown.
3. Log in to the CLI, and change to the TftpUpdate directory:
`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:
`set ServerIPAddress=129.148.53.204`
5. Enter the following command to set the file name of the combined `bmc.bios` image:
`set FileName=X2100_96_2a10`

- a. To set the update method to overwrite existing customizations, enter:

```
set UpdateMethod=ClearCMOS
```

This is the default method; it clears the CMOS and overwrites all customized BIOS settings.

- b. To set the update method to preserve existing customizations, enter:

```
set UpdateMethod=PreserveCMOS
```

This method preserves the CMOS settings.

6. Start the tftp download:

```
set Update=action
```

Example:

```
/SP ->cd TftpUpdate  
/SP/TftpUpdate ->set ServerIPAddress=129.148.53.204  
/SP/TftpUpdate ->set FileName=X2100_96_2a10  
/SP/TftpUpdate -> set Update=action  
getting image...  
getting image successfully.  
prepare to update...  
Prepare OK!  
Update Successful  
starting update...
```

Displaying Version Information

Enter the following command to display the current SP version:

```
version
```

Example

```
SM CLP Version v1.0.0  
SM ME Addressing Version v1.0.0
```

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 115.](#)
- [“SNMP MIB Files” on page 116.](#)
- [“MIBs Integration” on page 116.](#)
- [“SNMP Messages” on page 117.](#)
- [“Configuring SNMP on the ELOM” on page 118.](#)
- [“Managing SNMP User Accounts” on page 119.](#)

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, which 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 the following capabilities: inventory management, and sensor and system state monitoring.

SNMP MIB Files

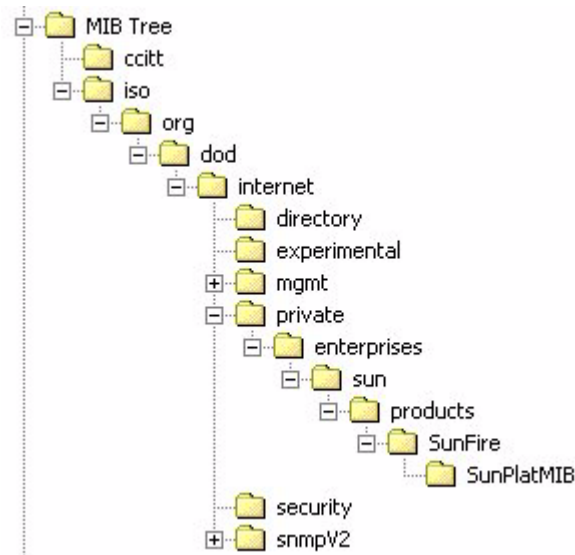
The base component of an SNMP solution is the Management Information Base (MIB). A MIB is a text file that describes a managed node's available information and where it is stored. When a management station requests information from a managed node, the agent receives the request and retrieves the appropriate information from the MIBs. The Sun server supports the following SNMP classes of Management Information Base (MIB) files. Download and install the product-specific MIB files from your Resource CD or Tools and Drivers CD for your platform.

- 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). It appears in [FIGURE 9-1](#). The standard SNMP port, 161, is used by the SNMP agent on the ELOM.

FIGURE 9-1 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

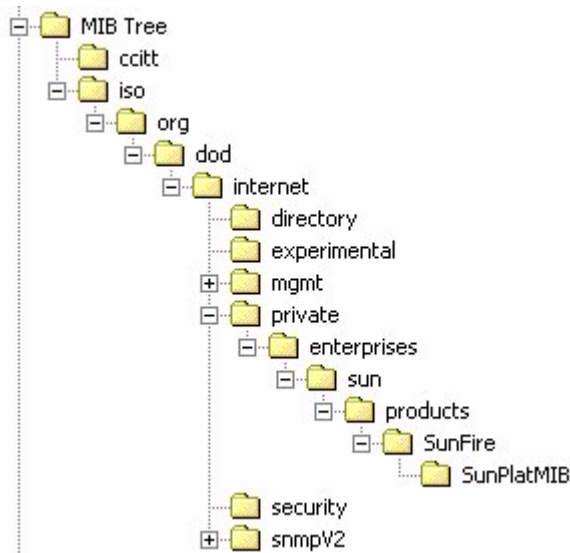
The ELOM has a preinstalled SNMP agent that supports trap delivery to an SNMP management application.

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.

Integrating the MIBs

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). It appears in [FIGURE 9-2](#).

FIGURE 9-2 Sun server MIB Tree



▼ To use SNMP on the SP

This example shows how to use SNMP with a third-party MIB web browser.

1. **From the Manager Preferences menu, choose Load/Unload MIBS: SNMP.**
2. **Locate and select the SUN-PLATFORM-MIB.mib.**
The SUN-PLATFORM-MIB is available on your Resource CD.
3. **Click Load.**
4. **Specify the directory where server MIBs are placed, and click Open.**
5. **Repeat Steps 2 through 4 to load other MIBs.**
6. **Exit the Manager Preferences menu.**
7. **Open an SNMP MIB web browser.**
The SNMP standard tree appears in the MIB web browser.
8. **Locate the Sun branch located under private.enterprises.**
Verify that the SUN-PLATFORM_MIB is integrated.

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 109](#), or [“Setting Up E-Mail Notification” on page 50](#).

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

Enter the following command to add an SNMP v3 read-only user account:

```
create /SP/AgentInfo/SNMP/users/username AuthPassword=password
```

Enter the following command to add an SNMP v1/v2c user account:

```
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/users/username
```

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

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

Configuring User Accounts

Use the `set` command to configure SNMP user accounts.

Syntax

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

Targets, Properties, and Values

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

TABLE 9-1 Configuring User Accounts

Target	Property	Value	Default
/SP/AgentInfo/SNMP/communities/ communityname	Permission	ro rw	ro
/SP/AgentInfo/SNMP/users/username	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

When changing the parameters of SNMP users, you must set values for all of the properties, even if you are not changing all of the values. For example, to change user Al's PrivacyProtocol to DES you must enter:

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

Your changes would be invalid if you only entered:

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

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

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

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

The result appear 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 appendix contains the following sections:

- [“CLI Command Quick Reference” on page A -123.](#)
- [“CLI Command Reference” on page A -125.](#)

CLI Command Quick Reference

This appendix contains the most common embedded lights out manager commands used to administer your Sun server from the command-line interface (CLI).

TABLE A-1 Command Syntax and Usage

Content	Typeface	Description
Your input	Fixed-width bold	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/User/user1</code>
Set or change password.	<code>set /SP/User/user Password=xxxx</code>
Set or change permission.	<code>pset /SP/User/user Permission=Operator Administrator</code>
Delete a local user.	<code>delete /SP/User/user1</code>
Change a local user's properties.	<code>set /SP/User/user1 Permission=operator</code>
Display information about all local users.	<code>show -display [targets properties all] -level [value all] /SP/User</code>

TABLE A-4 Network and Serial Port Setting Commands

Description	Command
Display network configuration information.	<code>show /SP/AgentInfo</code>
Change network properties for the ELOM. Changing certain network properties, like the IP address, will disconnect your active session.	<code>set /SP/AgentInfo 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/AgentInfo DhcpConfigured=[enable disable]</code>

TABLE A-5 Alert Commands

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

TABLE A-8 Host System Commands

Description	Command
Start the host system.	set /SP/SystemInfo/CtrlInfo PowerCtrl=on
Stop the host system gracefully.	set /SP/SystemInfo/CtrlInfo PowerCtrl=gracefuloff
Stop the host system forcefully.	set /SP/SystemInfo/CtrlInfo PowerCtrl=forceoff
Reset the host system.	set /SP/SystemInfo/CtrlInfo PowerCtrl=reset
Start a session to connect to the host console.	start /SP/AgentInfo/console
Stop the session connected to the host console.	stop /SP/AgentInfo/console

CLI Command Reference

This section provides reference information about the CLI commands.

cd

Use the **cd** command to navigate the namespace. When you **cd** 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. Entering just **cd** displays your current location in the namespace. Entering **help targets** displays a list of all targets in the entire namespace.

Syntax

cd *target*

Options

[-d|default] [-e|examine] [-h|help]

Targets and Properties

Any location in the namespace.

Examples

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

```
cd /SP/User
```

```
create sally
```

To find your location, enter **cd**.

```
cd /SP/User
```

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

[-d|default] [-e|examine] [-h|help]

Targets, Properties, and Values

TABLE A-9 Properties and Values for the Create Command

Valid Targets	Properties	Values	Default
/SP/User/username	Password	<i>string</i>	(none)
	Permission	administrator operator user	operator
	Status		
/SP/AgentInfo/SNMP/communities/ communityname	Permission	ro rw	ro
/SP/AgentInfo/SNMP/users/ username	AuthProtocol	MD5	MD5
	AuthPassword	<i>string</i>	(null string)
	Permission	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 will be prompted to confirm a **delete** command.

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

Syntax

```
delete [options] [-script] target
```

Options

[-x|examine] [-f|force] [-h|help] [-script]

Targets

TABLE A-10

Valid Targets

/SP/User/username

Examples

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

-> **delete /SP/AgentInfo/SNMP/users/john**

exit

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

Syntax

exit [*options*]

Options

[-x|examine] [-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

[-x|examine] [-h|help] [-output terse|verbose]

Commands

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

Examples

-> **help load**

The **load** command is used to transfer a file from a server to a target.

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

-source : specific the location to get a file

help -output verbose reset

The **reset** command is used 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 specify the properties of the target.

Syntax

set [*options*] **[-default]** **target** [*propertyname=value*]

Options

[-x examine] [-h help]

Targets, Properties, and Values

TABLE A-11 Set Command Targets, Properties, and Values

Valid Targets	Properties	Values	Default
/SP/User/username	Password	<i>string</i>	(none)
	Permission	administrator operator user	operator
	Status	enable disable	disable

Examples

```
-> set /SP/User/susan Permission=administrator
```

show

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

Using the **-display** option determines the type of information shown. If you specify **-display targets**, then all targets in the namespace below the current target are shown. If you specify **-display properties**, all property names and values for the target are shown. With this option you can specify certain property names, and only those values are shown. If you specify **-display all**, all targets in the namespace below the current target are shown, and the properties of the specified target are shown. If you do not specify a **-display** option, the show command acts as if **-display all** were specified.

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] [-display targets|properties|all] [-level  
value|all] target propertyname
```

Options

[-d|-display] [-e|examine] [-l|level]

Targets and Properties

TABLE A-12 Show Command Targets

Valid Targets	Properties	Values
/SP/User	(none)	(none)
/SP/User/ <i>username</i>	Status Permission Password	enable disable Administrator Operator <i>string</i>

Examples

```
show -display properties /SP/User/susan
```

```
/SP/User/susan
Targets:

Properties:
  Status=enable
  Permission= Administrator
  Password=(Cannot show property)
```

start

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

Syntax

```
start [options] target
```

Options

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

Targets

TABLE 0-1

Valid Targets	Description
/SP/console	Starts an interactive session to the console stream.

Examples

-> **start /SP/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] [-script] target

Options

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

Targets

TABLE 0-2

Valid Targets	Description
/SP/console	Terminate another user's connection to the host console.

Examples

stop /SP/console

version

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

Syntax

version

Options

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

Example

version

```
SM CLP Version v1.0.0  
SM ME Addressing Version v1.0.0
```


Glossary

The following terms are used within the Sun server documentation.

A

**access control list
(ACL)**

A software authorization mechanism that enables you to control which users have access to a server. You can define ACL rules that are specific to a particular file or directory, granting or denying access to one or more users or groups.

address In networking, a unique code that identifies a node in the network. Names such as "host1.sun.com" are translated to dotted-quad addresses like "168.124.3.4" by the Domain Name Service (DNS).

address resolution A means for mapping Internet addresses into physical media access control (MAC) addresses or domain addresses.

**Address Resolution
Protocol (ARP)**

A protocol used to associate an Internet Protocol (IP) address with a network hardware address (MAC address).

Administrator The person with full access (root) privileges to the managed host system.

**Advanced
Configuration and
Power Interface
(ACPI)**

An open-industry specification that provides power management capabilities to a system that enables the operating system to determine when peripheral devices are idle and to utilize ACPI-defined mechanisms for putting the devices into low power modes. The ACPI specification also describes a large number of power states for CPUs, devices, and systems as a whole. One feature of the ACPI enables the OS to modify the voltage and frequency of a

CPU in response to system load, thus enabling the system's main power-consuming element (the CPU) to vary its power consumption based on system load.

**Advanced
Programmable
Interrupt Controller
(APIC)**

A device that manages interrupt requests for multiple central processing units (CPUs). The APIC decides which request has the highest priority and sends an interrupt to the processor for that request.

**Advanced Technology
Attachment (ATA)**

A specification that describes the physical, transport, electrical, and command protocols used to attach storage devices to host systems.

**Advanced Technology
Attachment Packet
Interface (ATAPI)**

An extension to the Advanced Technology Attachment (ATA) standard for connecting removable media storage devices in host systems, including CD/DVD drives, tape drives, and high-capacity diskette drives. Also called "ATA-2" or "ATA/ATAPI."

agent A software process, usually corresponding to a particular local managed host, that carries out manager requests and makes local system and application information available to remote users.

alert A message or log generated by the collection and analysis of error events. An alert indicates that there is a need to perform some hardware or software corrective action.

**Alert Standard Format
(ASF)**

A preboot or out-of-band platform management specification that enables a device, such as an intelligent Ethernet controller, to autonomously scan ASF-compliant sensors on the motherboard for voltage, temperature, or other excursions and to send Remote Management and Control Protocol (RMCP) alerts according to the Platform Event Trap (PET) specification. ASF was intended primarily for out-of-band management functions for client desktops. ASF is defined by the Distributed Management Task Force (DMTF).

authentication The process that verifies the identity of a user in a communication session, or a device or other entity in a computer system, before that user, device, or other entity can access system resources. Session authentication can work in two directions. A server authenticates a client to make access control decisions. The client can authenticate the server as well. With Secure Sockets Layer (SSL), the client always authenticates the server.

authorization The process of granting specific access privileges to a user. Authorization is based on authentication and access control.

AutoYaST An installation program for SUSE Linux that automates the process of configuring one or more servers.

B

- bandwidth** A measure of the volume of information that can be transmitted over a communication link. Often used to describe the number of bits per second a network can deliver.
- baseboard management controller (BMC)** A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The BMC provides another interface to the system event log (SEL). Typical functions of the BMC are to measure processor temperature, power supply values, and cooling fan status. The BMC can take autonomous action to preserve system integrity. The BMC is also known as the service processor (SP).
- baud rate** The rate at which information is transmitted between devices, for example, between a terminal and a server.
- bind** In the Lightweight Directory Access Protocol (LDAP), refers to the authentication process that LDAP requires when users access the LDAP directory. Authentication occurs when the LDAP client binds to the LDAP server.
- BIOS (Basic Input/Output System)** System software that controls the loading of the operating system and testing of hardware at system power-on. BIOS is stored in read-only memory (ROM).
- bits per second (bps)** The unit of measurement for data transmission speed.
- boot loader** A program contained in read-only memory (ROM) that automatically runs at system power-on to control the first stage of system initialization and hardware tests. The boot loader then transfers control to a more complex program that loads the operating system.

C

- cache** A copy of original data that is stored locally, often with instructions or the most frequently accessed information. Cached data does not have to be retrieved from a remote server again when requested. A cache increases effective memory transfer rates and processor speed.

certificate Public key data assigned by a trusted Certificate Authority (CA) to provide verification of an entity's identity. This is a digitally signed document. Both clients and servers can have certificates. Also called a "public key certificate."

Certificate Authority (CA)

A trusted organization that issues public key certificates and provides identification to the owner of the certificate. A public key Certificate Authority issues certificates that state a relationship between an entity named in the certificate, and a public key that belongs to that entity, which is also present in the certificate.

client In the client/server model, a system or software on a network that remotely accesses resources of a server on a network.

command-line interface (CLI)

A text-based interface that enables you to enter executable instructions at a command prompt.

Common Information Model (CIM)

An open systems information model published by the Distributed Management Task Force (DMTF) that enables a common application to manage disparate resources, such as printers, disk drives, or CPUs.

console A terminal or dedicated window on a screen where system messages are displayed. The console window enables you to configure, monitor, maintain, and troubleshoot many server software components.

Coordinated Universal Time (UTC)

The international standard for time. UTC was formerly called Greenwich Meridian Time (GMT). UTC is used by Network Time Protocol (NTP) servers to synchronize systems and devices on a network.

core file A file created by the Solaris or Linux operating system when a program malfunctions and terminates. The core file holds a snapshot of memory, taken at the time the fault occurred. Also called a "crash dump file."

critical event A system event that seriously impairs service and requires immediate attention.

custom JumpStart A type of installation in which the Solaris software is automatically installed on a system that is based on a user-defined profile.

customer-replaceable unit (CRU)

A system component that the user can replace without special training or tools.

D

Data Encryption Standard (DES)	A common algorithm for encrypting and decrypting data.
Desktop Management Interface (DMI)	A specification that sets standards for accessing technical support information about computer hardware and software. DMI is hardware and operating system (OS) independent, and can manage workstations, servers, or other computing systems. DMI is defined by the Distributed Management Task Force (DMTF).
digital signature	A certification of the source of digital data. A digital signature is a number derived from a public key cryptographic process. If the data is modified after the signature was created, the signature becomes invalid. For this reason, a digital signature can ensure data integrity and detection of data modification.
Digital Signature Algorithm (DSA)	A cryptographic algorithm specified by the Digital Signature Standard (DSS). DSA is a standard algorithm used to create digital signatures.
direct memory access (DMA)	The transfer of data directly into memory without supervision of the processor.
directory server	In the Lightweight Directory Access Protocol (LDAP), a server which stores and provides information about people and resources within an organization from a logically centralized location.
disk array	A storage subsystem containing an arrangement of multiple disk drives, designed to provide performance, high availability, serviceability, and other benefits.
disk partition	A logical section of a physical hard disk drive reserved for a specific file system and function.
Distinguished Name (DN)	In the Lightweight Directory Access Protocol (LDAP), a unique text string that identifies an entry's name and location within the directory. A DN can be a fully qualified domain name (FQDN) that includes the complete path from the root of the tree.
Distributed Management Task Force (DMTF)	A consortium of over 200 companies that authors and promotes standards for the purpose of furthering the ability to remotely manage computer systems. Specifications from the DTMF include the Desktop Management Interface (DMI), the Common Information Model (CIM), and the Alert Standard Format (ASF).

domain	A grouping of hosts that is identified by a name. The hosts usually belong to the same Internet Protocol (IP) network address. The domain also refers to the last part of a fully qualified domain name (FQDN) that identifies the company or organization that owns the domain. For example, "sun.com" identifies Sun Microsystems as the owner of the domain in the FQDN "docs.sun.com."
domain name	The unique name assigned to a system or group of systems on the Internet. The host names of all the systems in the group have the same domain name suffix, such as "sun.com." Domain names are interpreted from right to left. For example, "sun.com" is both the domain name of Sun Microsystems, and a subdomain of the top-level ".com" domain.
Domain Name Server (DNS)	The server that typically manages host names in a domain. DNS servers translate host names, such as "www.example.com," into Internet Protocol (IP) addresses, such as "030.120.000.168."
Domain Name Service (DNS)	The data query service that searches domains until a specified host name is found.
Domain Name System (DNS)	A distributed, name resolution system that enables computers to locate other computers on a network or the Internet by domain name. The system associates standard Internet Protocol (IP) addresses, such as "00.120.000.168," with host names, such as "www.sun.com." Machines typically get this information from a DNS server.
dual inline memory module (DIMM)	A circuit board that holds double the amount of surface-mount memory chips that a single inline memory module (SIMM) holds. A DIMM has signal and power pins on both sides of the board, whereas a SIMM has pins on only one side of the board. A DIMM has a 168-pin connector and supports 64-bit data transfer.
Dynamic Host Configuration Protocol (DHCP)	A protocol that enables a DHCP server to assign Internet Protocol (IP) addresses dynamically to systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) network.
dynamic random-access memory (DRAM)	A type of random-access memory (RAM) that stores information in integrated circuits that contain capacitors. Because capacitors lose their charge over time, DRAM must be periodically recharged.

E

- electrically erasable programmable read-only memory (EEPROM)** A type of nonvolatile programmable read-only memory (PROM) that can be erased by exposing it to an electrical charge.
- electrostatic discharge (ESD)** The sudden dissipation of static electrical charge. ESD can easily destroy semiconductor components.
- enhanced parallel port (EPP)** A hardware and software standard that enables systems to transmit data at twice the speed of standard parallel ports.
- erasable programmable read-only memory (EPROM)** A nonvolatile programmable read-only memory (PROM) that can be written to as well as read from.
- Ethernet** An industry-standard type of local area network (LAN) that enables real-time communication between systems connected directly through cables. Ethernet uses a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) algorithm as its access method, wherein all nodes listen for, and any node can begin transmitting data. If multiple nodes attempt to transmit at the same time (a collision), the transmitting nodes wait for a random time before attempting to transmit again.
- event** A change in the state of a managed object. The event-handling subsystem can provide a notification to which a software system must respond when it occurs, but which the software did not solicit or control.
- externally initiated reset (XIR)** A signal that sends a “soft” reset to the processor in a domain. XIR does not reboot the domain. An XIR is generally used to escape from a hung system in order to reach the console prompt. A user then can generate a core dump file, which can be useful in diagnosing the cause of the hung system.

F

- failover** The automatic transfer of a computer service from one system, or more often a subsystem, to another to provide redundant capability.

Fast Ethernet	Ethernet technology that transfers data up to 100M bits per second. Fast Ethernet is backward compatible with 10M-bit per second Ethernet installations.
fdisk partition	A logical partition of a physical disk drive that is dedicated to a particular operating system on an x86-based system.
Fibre Channel (FC)	A connector that provides high bandwidth, increased distance, and additional connectivity from hosts to peripherals.
Fibre Channel-Arbitrated Loop (FC-AL)	A 100-Mbyte per second loop topology used with Fibre Channel that enables connection of multiple devices such as disk drives and controllers. An arbitrated loop connects two or more ports, but enables only two ports to communicate at a given time.
field-replaceable unit (FRU)	A system component that is replaceable at the customer site.
file system	A consistent method by which information is organized and stored on physical media. Different operating systems typically have different file systems. File systems are often a tree-structured network of files and directories, with a root directory at the top and parent and child directories below root.
File Transfer Protocol (FTP)	A basic Internet protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP) that enables the retrieving and storing of files between systems on the Internet without regard for the operating systems or architectures of the systems involved in the file transfer.
firewall	A network configuration, usually both hardware and software, that protects networked computers within an organization from outside access. A firewall can monitor or prohibit connections to and from specified services or hosts.
firmware	Software that is typically used to help with the initial booting stage of a system and with system management. Firmware is embedded in read-only memory (ROM) or programmable ROM (PROM).
flash PROM	A programmable read-only memory (PROM) that can be reprogrammed while installed within the system, from software on a disk, by a voltage pulse, or flash of light.
fully qualified domain name (FQDN)	The complete and unique Internet name of a system, such as “www.sun.com.” The FQDN includes a host server name (www) and its top-level (.com) and second-level (.sun) domain names. A FQDN can be mapped to a system’s Internet Protocol (IP) address.

G

- gateway** A computer or program that interconnects two networks and then passes data packets between the networks. A gateway has more than one network interface.
- Gigabit Ethernet** Ethernet technology that transfers data up to 1000M-bits per second.
- Grand Unified Bootloader (GRUB)** A boot loader that can install two or more operating systems (OS) onto a single system and that can manage which OS to boot at power-on.
- graphical user interface (GUI)** An interface that uses graphics, along with keyboard and mouse, to provide easy-to-use access to an application.

H

- heatsink** A structure, attached to or part of a semiconductor device, that can dissipate heat to the surrounding environment.
- host** A system, such as a backend server, with an assigned Internet Protocol (IP) address and host name. The host is accessed by other remote systems on the network.
- host ID** Part of the 32-bit Internet Protocol (IP) address used to identify a host on a network.
- host name** The name of a particular machine within a domain. Host names always map to a specific Internet Protocol (IP) address.
- hot plug** Describes a component that is safe to remove or add while the system is running. Typically, the system must be rebooted before the hot-plug component is configured into the system.
- hot swap** Describes a component that can be installed or removed by simply pulling the component out and putting a new component into a running system. The system either automatically recognizes the component change and configures it, or requires user interaction to configure the system. However, in neither case is a reboot required. All hot-swappable components are hot pluggable, but not all hot-pluggable components are hot swappable.

Hypertext Transfer Protocol (HTTP)

The Internet protocol that retrieves hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client. HTTP is based on Transmission Control Protocol/Internet Protocol (TCP/IP).

Hypertext Transfer Protocol Secure (HTTPS)

An extension of HTTP that uses Secure Sockets Layer (SSL) to enable secure transmissions over a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

I

in-band system management

Server management capability that is enabled only when the operating system is initialized and the server is functioning properly.

install server

A server that provides the Solaris software DVD or CD images from which other systems on a network can install the Solaris software.

Integrated Lights-Out Manager (ILOM)

An integrated hardware, firmware, and software solution for in-chassis or in-blade system management.

Intelligent Platform Management Interface (IPMI)

A hardware-level interface specification that was designed primarily for out-of-band management of server systems over a number of different physical interconnects. The IPMI specification describes extensive abstractions regarding sensors, enabling a management application running on the operating system (OS) or in a remote system to comprehend the environmental makeup of the system and to register with the system's IPMI subsystem to receive events. IPMI is compatible with management software from heterogeneous vendors. IPMI functionality includes FRU inventory reporting, system monitoring, logging, system recovery (including local and remote system resets and power on and off capabilities), and alerting.

Internet Control Message Protocol (ICMP)

An extension to the Internet Protocol (IP) that provides for routing, reliability, flow control, and sequencing of data. ICMP specifies error and control messages used with the IP.

Internet Protocol (IP) The basic network layer protocol of the Internet. IP enables the unreliable delivery of individual packets from one host to another. IP does not guarantee that the packet will be delivered, how long it will take, or if multiple packets will be delivered in the order they were sent. Protocols layered on top of IP add connection reliability.

Internet Protocol (IP) address In Transmission Control Protocol/Internet Protocol (TCP/IP), a unique 32-bit number that identifies each host or other hardware system on a network. The IP address is a set of numbers separated by dots, such as “192.168.255.256,” that specifies the actual location of a machine on an intranet or the Internet.

interrupt request (IRQ) A signal that a device requires attention from the processor.

IPMItool A utility used to manage IPMI-enabled devices. IPMItool can manage IPMI functions of either the local system or a remote system. Functions include managing field-replaceable unit (FRU) information, local area network (LAN) configurations, sensor readings, and remote system power control.

J

Java Web Start application A web application starter. With Java Web Start, applications are started by clicking on the web link. If the application is not present on your system, Java Web Start downloads it and caches it onto your system. Once an application is downloaded to its cache, it can be started from a desktop icon or web browser link. The most current version of the application is always presented.

JumpStart installation A type of installation in which the Solaris software is automatically installed on a system by using the factory-installed JumpStart software.

K

kernel The core of the operating system (OS) that manages the hardware and provides fundamental services, such as filing and resource allocation, that the hardware does not provide.

Keyboard Controller Style (KCS) interface A type of interface implemented in legacy personal computer (PC) keyboard controllers. Data is transferred across the KCS interface using a per-byte handshake.

**keyboard, video,
mouse, storage
(KVMS)**

A series of interfaces that enables a system to respond to keyboard, video, mouse, and storage events.

L

**lights out management
(LOM)**

Technology that provides the capability for out-of-band communication with the server even if the operating system is not running. This enables the system administrator to switch the server on and off; view system temperatures, fan speeds, and so forth; and restart the system from a remote location.

**Lightweight Directory
Access Protocol
(LDAP)**

A directory service protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data. LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP) and across multiple platforms.

**Lightweight Directory
Access Protocol (LDAP)
server**

A software server that maintains an LDAP directory and service queries to the directory. The Sun Directory Services and the Netscape Directory Services are implementations of an LDAP server.

Linux Loader (LILO)

A boot loader for Linux.

**local area network
(LAN)**

A group of systems in close proximity that can communicate via connecting hardware and software. Ethernet is the most widely used LAN technology.

local host

The processor or system on which a software application is running.

M

Major event

A system event that occurred that impairs service, but not seriously.

**Management
Information Base
(MIB)**

A tree-like, hierarchical system for classifying information about resources in a network. The MIB defines the variables that the master Simple Network Management Protocol (SNMP) agent can access. The MIB provides access to

the server's network configuration, status, and statistics. Using SNMP, you can view this information from a network management station (NMS). By industry agreement, individual developers are assigned portions of the tree structure to which they may attach descriptions that are specific to their own devices.

man pages Online UNIX documentation.

media access control (MAC) address Worldwide unique, 48-bit, hardware address number that is programmed in to each local area network interface card (NIC) at the time of manufacture.

Message Digest 5 (MD5) A secure hashing function that converts an arbitrarily long data string into a short digest of data that is unique and of fixed size.

minor event A system event that occurred that does not currently impair service, but which needs correction before it becomes more severe.

N

namespace In the tree structure of a Lightweight Directory Access Protocol (LDAP) directory, a set of unique names from which an object name is derived and understood. For example, files are named within the file namespace and printers are named within the printer namespace.

Network File System (NFS) A protocol that enables disparate hardware configurations to function together transparently.

Network Information Service (NIS) A system of programs and data files that UNIX systems use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computer systems.

network interface card (NIC) An internal circuit board or card that connects a workstation or server to a networked device.

network management station (NMS) A powerful workstation with one or more network management applications installed. The NMS is used to remotely manage a network.

network mask A number used by software to separate the local subnet address from the rest of a given Internet Protocol (IP) address.

Network Time Protocol (NTP)	An Internet standard for Transmission Control Protocol/Internet Protocol (TCP/IP) networks. NTP synchronizes the clock times of networked devices with NTP servers to the millisecond using Coordinated Universal Time (UTC).
node	An addressable point or device on a network. A node can connect a computing system, a terminal, or various peripheral devices to the network.
nonmaskable interrupt (NMI)	A system interrupt that is not invalidated by another interrupt.
nonvolatile memory	A type of memory that ensures that data is not lost when system power is off.
nonvolatile random-access memory (NVRAM)	A type of random-access memory (RAM) that retains information when system power is off.

O

object identifier (OID)	A number that identifies an object's position in a global object registration tree. Each node of the tree is assigned a number, so that an OID is a sequence of numbers. In Internet usage the OID numbers are delimited by dots, for example, "0.128.45.12." In the Lightweight Directory Access Protocol (LDAP), OIDs are used to uniquely identify schema elements, including object classes and attribute types.
OpenBoot PROM	A layer of software that takes control of an initialized system after the power-on self-test (POST) successfully tests components. OpenBoot PROM builds data structures in memory and boots the operating system.
OpenIPMI	An operating system-independent, event-driven library for simplifying access to the Intelligent Platform Management Interface (IPMI).
Operator	A user with limited privileges to the managed host system.
out-of-band (OOB) system management	Server management capability that is enabled when the operating system network drivers or the server are not functioning properly.

P

- parity** A method used by a computer for checking that data received matches data sent. Also refers to information stored with data on a disk that enables the controller to rebuild data after a drive failure.
- partition** A physical section on a hard disk drive.
- Peripheral Component Interconnect (PCI)** A local bus standard used to connect peripherals to 32-bit or 64-bit systems.
- Peripheral Interface Controller (PIC)** An integrated circuit that controls peripherals in an interrupt request (IRQ)-driven system, taking away that load from the central processing unit (CPU).
- permissions** A set of privileges granted or denied to a user or group that specify read, write, or execution access to a file or directory. For access control, permissions state whether access to the directory information is granted or denied, and the level of access that is granted or denied.
- physical address** An actual hardware address that matches a memory location. Programs that refer to virtual addresses are subsequently mapped to physical addresses.
- Platform Event Filtering (PEF)** A mechanism that configures the service processor to take selected actions when it receives event messages, for example, powering off or resetting the system or triggering an alert.
- Platform Event Trap (PET)** A configured alert triggered by a hardware or firmware (BIOS) event. A PET is an Intelligent Platform Management Interface (IPMI)-specific, Simple Network Management Protocol (SNMP) trap, which operates independently of the operating system.
- port** The location (socket) to which Transmission Control Protocol/Internet Protocol (TCP/IP) connections are made. Web servers traditionally use port 80, the File Transfer Protocol (FTP) uses port 21, and Telnet uses port 23. A port enables a client program to specify a particular server program in a computer on a network. When a server program is started initially, it binds to its designated port number. Any client that wants to use that server must send a request to bind to the designated port number.
- port number** A number that specifies an individual Transmission Control Protocol/Internet Protocol (TCP/IP) application on a host machine, providing a destination for transmitted data.
- power cycling** The process of turning the power to a system off then on again.

power-on self-test (POST) A program that takes uninitialized system hardware and probes and tests its components at system startup. POST configures useful components into a coherent, initialized system and hands it over to the OpenBoot PROM. POST passes to OpenBoot PROM a list of only those components that have been successfully tested.

PowerPC An embedded processor.

Preboot Execution Environment (PXE) An industry-standard client/server interface that enables a server to boot an operating system (OS) over a Transmission Control Protocol/Internet Protocol (TCP/IP) network using Dynamic Host Configuration Protocol (DHCP). The PXE specification describes how the network adapter card and BIOS work together to provide basic networking capabilities for the primary bootstrap program, enabling it to perform a secondary bootstrap over the network, such as a TFTP load of an OS image. Thus, the primary bootstrap program, if coded to PXE standards, does not need knowledge of the system's networking hardware.

Privacy Enhanced Mail (PEM) A standard for Internet electronic mail that encrypts data to ensure privacy and data integrity.

programmable read-only memory (PROM) A memory chip on which data can be programmed only once and which retains the program forever. PROMs retain data even when power is off.

protocol A set of rules that describes how systems or devices on a network exchange information.

proxy A mechanism whereby one system acts on behalf of another system in responding to protocol requests.

public key encryption A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt messages, the recipients use their unpublished private keys, which are known only to them. Knowing the public key does not enable users to deduce the corresponding private key.

R

rack unit (U) A measure of vertical rack space equal to 1.75 inches (4.45 cm).

random-access memory (RAM)	Volatile, semiconductor-based memory in which any byte of memory can be accessed without touching the preceding bytes.
read-only file	A file that a user cannot modify or delete.
read-only memory (ROM)	A nonvolatile memory chip on which data has been prerecorded. Once written onto a ROM chip, data cannot be removed and can only be read.
real-time clock (RTC)	A battery-backed component that maintains the time and date for a system, even when the system is powered off.
reboot	An operating system-level operation that performs a system shutdown followed by a system boot. Power is a prerequisite.
Red Hat Package Manager (RPM)	A collection of tools developed by Red Hat, Inc. for Red Hat Linux that can automate the install, uninstall, update, verify, and query software processes on a computer. RPM is now commonly used by multiple Linux vendors.
redirection	The channeling of input or output to a file or device rather than to the standard input or output of a system. The result of redirection sends input or output that a system would normally display to the display of another system.
redundant array of independent disks (RAID)	A way of storing the same data at different places, thus redundantly, on multiple hard disks. RAID enables a set of disk drives to appear as a single logical disk drive to an application such as a database or file system. Different RAID levels provide different capacity, performance, high availability, and cost characteristics.
Remote Management and Control Protocol (RMCP)	A networking protocol that enables an administrator to respond to an alert remotely by powering the system on or off, or forcing a reboot.
remote procedure call (RPC)	A method of network programming that enables a client system to call functions on a remote server. The client starts a procedure at the server and the result is transmitted back to the client.
remote system	A system other than the one on which the user is working.
reset	A hardware-level operation that performs a system power off, followed by a system power on.
root	In UNIX operating systems, the name of the superuser (root). The root user has permissions to access any file and carry out other operations not permitted to ordinary users. Roughly equivalent to the Administrator user name on Windows Server operating systems.

- root directory** The base directory from which all other directories stem, either directly or indirectly.
- router** A system that assigns a path over which to send network packets or other Internet traffic. Although both hosts and gateways do routing, the term “router” commonly refers to a device that connects two networks.
- RSA algorithm** A cryptographic algorithm developed by RSA Data Security, Inc. It can be used for both encryption and digital signatures.

S

- schema** Definitions that describe what type of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.
- Secure Shell (SSH)** A UNIX shell program and network protocol that enables secure and encrypted log in and execution of commands on a remote system over an insecure network.
- Secure Sockets Layer (SSL)** A protocol that enables client-to-server communication on a network to be encrypted for privacy. SSL uses a key exchange method to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. SSL creates a secure connection between a web server and a web client. Hypertext Transfer Protocol Secure (HTTPS) uses SSL.
- sensor data record (SDR)** To facilitate dynamic discovery of features, the Intelligent Platform Management Interface (IPMI) includes this set of records that include software information such as how many sensors are present, what type they are, their events, threshold information, and so forth. The sensor data records enable software to interpret and present sensor data without any prior knowledge about the platform.
- Serial Attached SCSI (SAS)** A point-to-point serial peripheral interface that links controllers directly to disk drives. SAS devices include two data ports that enable failover redundancy, which guarantees data communication through a separate path.
- serial console** A terminal or a tip line connected to the serial port on the service processor. A serial console is used to configure the system to perform other administrative tasks.

server certificate	A certificate used with Hypertext Transfer Protocol Secure (HTTPS) to authenticate web applications. The certificate can be self-signed or issued by a Certificate Authority (CA).
Server Message Block (SMB) protocol	A network protocol that enables files and printers to be shared across a network. The SMB protocol provides a method for client applications to read and write to files on, and to request services from, server programs in the network. The SMB protocol enables you to mount file systems between Windows and UNIX systems. The SMB protocol was designed by IBM and subsequently modified by Microsoft Corp. Microsoft renamed the protocol the “Common Internet File System (CIFS).”
service processor (SP)	A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The SP provides another interface to the system event log (SEL). Typical functions of the SP are to measure processor temperature, power supply values, and cooling fan status. The SP can take autonomous action to preserve system integrity. See also Baseboard Management Controller (BMC).
session timeout	A specified duration after which a server can invalidate a user session.
Simple Mail Transfer Protocol (SMTP)	A Transmission Control Protocol/Internet Protocol (TCP/IP) used for sending and receiving email.
Simple Network Management Protocol (SNMP)	A simple protocol used to exchange data about network activity. With SNMP, data travels between a managed device and a network management station (NMS). A managed device can be any device that runs SNMP, such as hosts, routers, web servers, or other servers on the network.
Small Computer System Interface (SCSI)	An ANSI standard for controlling peripheral devices by one or more host computers. SCSI defines a standard I/O bus-level interface and a set of high-level I/O commands.
Spanning Tree Protocol (STP)	A networking protocol based on an intelligent algorithm that enables bridges to map a redundant topology and eliminates packet looping in local area networks (LANs).
subnet	A working scheme that divides a single logical network into smaller physical networks to simplify routing. The subnet is the portion of an Internet Protocol (IP) address that identifies a block of host IDs.

subnet mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Also called an “address mask.”

superuser A special user who has privileges to perform all administrative functions on a UNIX system. Also called “root.”

system event log (SEL) A log that provides nonvolatile storage for system events that are logged autonomously by the service processor, or directly with event messages sent from the host.

T

Telnet The virtual terminal program that enables the user of one host to log in to a remote host. A Telnet user of one host who is logged in to a remote host can interact as a normal terminal user of the remote host.

threshold Minimum and maximum values within a range that sensors use when monitoring temperature, voltage, current, and fan speed.

timeout A specified time after which the server should stop trying to finish a service routine that appears to be hung.

transmission control block (TCB) Part of the Transmission Control Protocol/Internet Protocol (TCP/IP) that records and maintains information about the state of a connection.

Transmission Control Protocol/Internet Protocol (TCP/IP) An Internet protocol that provides for the reliable delivery of data streams from one host to another. TCP/IP transfers data between different types of networked systems, such as systems running Solaris, Microsoft Windows, or Linux software. TCP guarantees delivery of data and that packets will be delivered in the same sequence in which they were sent.

trap Event notification made by Simple Network Management Protocol (SNMP) agents by their own initiative when certain conditions are detected. SNMP formally defines seven types of traps and permits subtypes to be defined.

Trivial File Transport Protocol (TFTP) A simple transport protocol that transfers files to diskless systems. TFTP uses User Datagram Protocol (UDP).

U

uninterruptible power supply (UPS)

An auxiliary or backup power supply that provides electrical service over extended system power outages. A UPS for a LAN or computer system provides continuous power in the event of a power failure.

Universal Serial Bus (USB)

An external bus standard that supports data transfer rates of 450M-bits per second (USB 2.0). A USB port connects devices, such as mouse pointers, keyboards, modems, and printers to the computer system.

unshielded twisted pair/shielded twisted pair (UTP/STP)

A type of Ethernet cable.

user account

A record of essential user information that is stored on the system. Each user who accesses a system has a user account.

User Datagram Protocol (UDP)

A connectionless, transport layer protocol that adds some reliability and multiplexing to the Internet Protocol (IP). UDP enables one application program to deliver, via IP, datagrams to another application program on another machine. The Simple Network Management Protocol (SNMP) is usually implemented over UDP.

user identification (userid)

A unique string identifying a user to a system.

user identification number (UID number)

The number assigned to each user accessing a UNIX system. The system uses UID numbers to identify, by number, the owners of files and directories.

user name

A combination of letters, and possibly numbers, that identifies a user to the system.

V

voltage regulator module (VRM)

An electronic device that regulates a system's microprocessor voltage requirements in order to maintain the correct voltage.

volume

One or more disk drives that can be grouped into a unit for data storage.

volume manager Software that organizes data blocks on physical disk drives into logical volumes, which makes the disk data independent of the physical path name of the disk drives. Volume manager software provides data reliability through disk striping, concatenation, mirroring, and dynamic growth of metadevices or volumes.

W

W3C Refers to the World Wide Web Consortium. W3C is an international organization that governs Internet standards.

web server Software that provides services to access the Internet or an intranet. A web server hosts web sites, provides support for HTTP/HTTPS and other protocols, and executes server-side programs.

wide area network (WAN) A network consisting of many systems that provides file transfer services. A WAN can cover a large physical area, sometimes worldwide.

X

X.509 certificate The most common certificate standard. X.509 certificates are documents containing a public key and associated identity information, digitally signed by a Certificate Authority (CA).

X Window System A common UNIX window system that enables a workstation or terminal to control multiple sessions simultaneously.

Index

A

- accessing the service processor, 19
- accessing the system with the web-based interface, 25

B

- BIOS
 - finding the version number, 30

C

- changing alert, CLI, 125
- CLI
 - command syntax, 123
 - commands
 - access settings, 125
 - alert, 125
 - cd, 125
 - character case, 101
 - command verbs overview, 102
 - create, 126
 - delete, 127
 - exit, 128
 - help, 128
 - host, 125
 - miscellaneous, 124
 - network and serial port, 124
 - options, 102
 - set, 129
 - show, 130
 - SNMP, 125
 - start, 131
 - stop, 132
 - user, 124

- version, 133
- managing
 - network settings, 105
 - user accounts, 106
- namespaces, 101
- overview
- serial port log in, 100
- SSH log in, 100

command line interface *See* CLI

D

- data center management, 4
- default settings, SP, 4
- DHCP alternatives, 24
- DIMM information, 33

E

- embedded lights out manager
 - definition, 1
 - namespaces, 101
- event log, 44

F

- fan performance, diagnosing with the web-based interface, 38
- firmware
 - overview, 19
 - updating using CLI, 113

H

- host, managing, 103

- I**
- IPMI
 - IPMItool, 94
 - overview, 2, 93
 - sensors, 94
- J**
- Java Client, overview, 2
- Java RTE, for remote console, 80
- L**
- launching, remote console, 80
- log in
 - CLI and SSH, 100
 - CLI serial port, 100
 - web-based interface, 26
- logging events, 44
- M**
- MAC address, 5
- Management Information Base (MIB)
 - description of, 116
 - integrating, 118
- N**
- N1 System Manager, 4
- network settings, managing, 105
- P**
- PET from CLI, 125
- power, controlling using CLI, 125
- R**
- redirecting local storage, 79
- remote console
 - benefits, 79
 - launching, 80
 - overview, 2, 20
 - requirements for, 80
 - starting, 80
- remote console, Java RTE, 80
- S**
- serial port
 - CLI log in, 100
- service processor
 - See* SP
 - setting session timeout with the web-based interface, 30
 - setting up the SP, 19
- SNMP, 115 to 121
 - and MIB, 116
 - host state, how to manage, 103
 - integrating MIBs, 118
 - overview, 2, 115
 - user accounts
 - adding, 119
 - configuring, 120
 - deleting, 120
 - properties, 120
- SP
 - default settings, 4
 - firmware overview, 19
 - initial setup, 20
 - interfaces, 19
 - logging in to, 26
 - managing network settings, 105
 - namespace, 102
 - overview, 1
 - set up with web-based interface, 22
 - setting up, 19
 - software, *See* Embedded Lights Out Manager
 - tasks and management interfaces, 3
- SP namespace, 101
- SSH
 - CLI log in, 100
 - overview, 20
- start console, CLI, 125
- syslog, enabling and disabling with the web-based interface, 57
- system component information, getting using the web-based interface, 31
- system indicator LED, activating, 45
- system management using N1, 4
- T**
- temperature issues, diagnosing with the web-based interface, 40
- thresholds
 - temperature, 41
 - voltage, 43

U

updating firmware using CLI, 113

user accounts

CLI, 106

V

version information, getting with the web-based interface, 28

voltage issues, diagnosing with the web-based interface, 42

voltage thresholds, 43

W

web-based interface

accessing

CPU screen, 31

memory screen, 33

NIC information screen, 33

the system, 25

activating the system indicator LED, 45

adding users, 68

changing

user password, 70

user privileges, 70

configuring

network settings, 48

system management access, 57 to 66

the server, 47 to 66

defining traps with the PEF, 52 to 56

deleting users, 71

diagnosing

fan performance, 38

temperature issues, 40

voltage issues, 42

disabling and enabling

syslog, 57

users, 71

getting system component information, 31

getting version information, 28

launching remote console, 80

log in, 26

managing, users, 66 to 71

monitoring the system, 36

overview, 2

remote console benefits, 79

resetting the fault LED, 46

setting

session timeout, 30

system time, 56

setting up

email notification, 50

the SP, 22

users

changing passwords, 70

changing privileges, 70

deleting, 71

disabling and enabling, 71

managing, 66 to 71

using the event log, 44 to 45

using the system monitoring screens, 36 to 46

