



# Sun™ Integrated Lights Out Manager 2.0 User's Guide

---

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

Part No. 820-1188-12  
September 2008, Revision A

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

Copyright © 2008 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 embodied in the product 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.

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

This distribution may include materials developed by third parties.

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, docs.sun.com and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc., or its subsidiaries, in the U.S. and other countries.

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

The OPEN LOOK and Sun(TM) 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.

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

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

Cette distribution peut comprendre des composants développés par des tierces parties.

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

Sun, Sun Microsystems, le logo Sun, Java, docs.sun.com et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc., ou ses filiales, aux Etats-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 Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

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

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

# Contents

---

<b>Preface</b>	<b>xv</b>
<b>1. Introduction to ILOM</b>	<b>1</b>
What Is ILOM?	1
What Does ILOM Do?	2
ILOM on the SP and CMM	3
ILOM Interfaces	4
ILOM Management Network	5
ILOM Connection Methods	5
Roles for ILOM User Accounts	6
Preconfigured ILOM Administrator Account	7
ILOM Features	7
New Features in ILOM 2.0	9
Other Management Tools	10
<b>2. Establish Initial Communication With ILOM</b>	<b>11</b>
About ILOM's Initial Setup	12
Initial Setup Worksheet	12
DHCP IP Assignment Considerations	14
Sun Server Platform DHCPDISCOVER Packet Broadcast	15
Requirements for DHCP Assignment	15

SP Network Interface MAC Address	15
Post DHCP Requirements	17
Static IP Assignment Considerations	18
Requirements for Static IP Assignment	18
Serial Device - Terminal Emulation Software Settings	19
Post Static IP Assignment	19
Management Network IP Address Configuration	20
ILOM Network Port Assignment	20
Hostname Identity for Server SP and CMM	22
System Identifier Text String for Sun Servers	22
Assign IP Addresses to the Sun Server Platform SP Interfaces	23
▼ Assign DHCP IP Addresses Using an Ethernet Management Connection	23
▼ Assign a Static IP Address to Server SP Using a Serial Connection	25
▼ Assign Static IP Address to CMM Using a Serial Connection	27
Edit IP Address Assignments Using an Ethernet Management Connection	29
▼ Edit Existing IP Addresses in ILOM Using the Web Interface	29
▼ Edit Existing IP Addresses in ILOM Using the CLI	30
Assign Hostname or System Identifier	33
▼ Assign Hostname and System Identifier Using the Web Interface	33
▼ Assign Hostname and System Identifier Using the CLI	35
<b>3. ILOM Command-Line Interface and Log In</b>	<b>37</b>
CLI Overview	38
CLI Hierarchical Architecture	38
CLI Command Syntax	40
CLI Commands	41
Command Options	41
Command Targets	42
Command Properties	42

Command Execution	42
▼ Execute Commands Individually	42
▼ Execute Combined Commands	43
Connect to ILOM Using the CLI	43
▼ Log In to ILOM	44
▼ Log Out of ILOM	44
<b>4. ILOM Web Interface and Log In</b>	<b>45</b>
Web Interface Overview	45
Browser and Software Requirements	46
Web Interface Components	47
Navigation Tab Components	48
Connect to ILOM Using the Web Interface	51
▼ Log In to ILOM	51
▼ Upload the SSL Certificate	54
▼ Set the Session Time-Out	55
▼ Log Out of ILOM	56
<b>5. Manage User Accounts</b>	<b>57</b>
Guidelines for Managing User Accounts	59
User Account Roles and Privileges	59
Preconfigured ILOM Administrator Accounts	60
▼ Change ILOM Root Account Password Using the Web Interface	60
▼ Change ILOM Root Account Password Using the CLI	63
Single Sign On	63
▼ Enable or Disable Single Sign On Using the CLI	63
▼ Enable or Disable Single Sign On Using the Web Interface	64
Manage User Accounts Using the CLI	64
▼ Add a User Account Using the CLI	65

- ▼ Modify a User Account Using the CLI 65
- ▼ Delete a User Account Using the CLI 65
- ▼ View a List of User Accounts Using the CLI 65
- ▼ View Individual User Account Using the CLI 66
- ▼ Configure a User Account Using the CLI 66
  - Targets, Properties, and Values 66
- ▼ View a List of User Sessions Using the CLI 67
- ▼ View an Individual User Session Using the CLI 67
- Manage User Accounts Using the Web Interface 68
  - ▼ Add User Accounts and Set Privileges Using the Web Interface 68
  - ▼ Modify a User Account Using the Web Interface 71
  - ▼ Delete a User Account Using the Web Interface 74
  - ▼ View User Sessions Using the Web Interface 75
- Active Directory 76
  - User Authentication and Authorization 76
  - Determining User Authorization Levels 77
  - Typical Uses of Active Directory 77
  - Active Directory Web Interface 78
  - Active Directory Configuration Properties 79
  - Naming Conventions for Active Directory Group Information 80
  - Active Directory Tables 81
    - Administrator Groups and Operator Groups Tables 83
    - User Domains Table 83
    - Alternate Servers Table 84
  - ▼ Configure Active Directory Settings 84
  - ▼ Edit Active Directory Tables Using the Web Interface 85
  - ▼ Edit Administrator Groups Table Using the CLI 89
  - ▼ Edit Operator Groups Table Using the CLI 90

- ▼ Edit User Domains Table Using the CLI 91
- ▼ Edit Alternate Servers Table Using the CLI 92

About Active Directory Properties 93

- ipaddress Property 94
- defaultrole Property 94
- logdetail Property 94
- port Property 94
- state Property 95
- strictcertmode Property 95
- timeout Property 95
- certfilestatus Property 96
- getcertfile Property 96

Diagnosing Authentication and Authorization Events 97

- ▼ View Authentication and Authorization Events Using the CLI 97
- ▼ View Authentication and Authorization Events Using the Web Interface 98

Set Certificate Validation Using the CLI 98

- ▼ Upload, Remove, or Restore a Certificate Using the CLI 99
- ▼ Enable `strictcertmode` Using the CLI 99
- ▼ Check `certfilestatus` Using the CLI 99

Set Certificate Validation Using the Web Interface 100

- ▼ Upload a Certificate Using the Web Interface 101
- ▼ Check Certificate File Status Using the Web Interface 101
- ▼ Enable Strict Certificate Mode Using the Web Interface 101

Lightweight Directory Access Protocol 102

About LDAP 102

LDAP Clients and Servers 102

LDAP Servers Directory Organization 103

Configure LDAP	104
▼ Configure the LDAP Server	105
▼ Configure ILOM for LDAP Using the CLI	105
▼ Configure ILOM for LDAP Using the Web Interface	106
RADIUS Authentication	108
RADIUS Clients and Servers	108
RADIUS Parameters	109
Configure RADIUS Settings	109
▼ Configure RADIUS Using the CLI	110
▼ Configure RADIUS Using the Web Interface	110
RADIUS Commands	111
show /SP/clients/radius	111
set /SP/clients/radius	112
show /SP/clients	113
<b>6. Inventory and Component Management</b>	<b>115</b>
View Component Information and Manage Inventory	116
▼ View Component Information Using the CLI	116
▼ View Component Information Using the Web Interface	117
Perform an Action on a Component	118
Remove and Replace Components	118
▼ Prepare to Remove a Component Using the CLI	119
▼ Determine Whether a Component Is Ready for Removal Using the CLI	119
▼ Return a Component to Service Using the CLI	120
▼ Prepare to Remove a Component Using the Web Interface	120
▼ Return a Component to Service Using the Web Interface	121
Enable and Disable Components	122
▼ Enable and Disable Components Using the CLI	122
▼ Enable and Disable Components Using the Web Interface	122



Configure Policy Settings	122
▼ Configure Policy Settings Using the CLI	123
▼ Configure Policy Settings Using the Web Interface	123
<b>7. System Monitoring and Alert Management</b>	<b>125</b>
About System Monitoring	126
Sensor Readings	127
Obtain Sensor Readings Using the Web Interface	127
Obtain Sensor Readings Using the CLI	129
Power Monitoring Interfaces	131
Power Monitoring Terminology	132
System Indicators	132
Supported System Indicator States	133
View and Manage Indicators Using the Web Interface	134
View and Manage Indicators Using the CLI	135
ILOM Event Log	136
Event Log Timestamps and ILOM Clock Settings	136
Supported Clock Settings	137
View or Set Clock Settings Using the Web Interface	137
View and Set Clock Settings Using the CLI	137
Syslog Information	138
Fault Management	139
View Fault Status Using the Web Interface	140
View Fault Status Using the CLI	141
ILOM Service Snapshot Utility	142
Monitor System Power, Sensors, Indicators, and ILOM Event Log	142
▼ Monitor System Total Power Consumption Using the CLI	143
▼ Monitor System Actual Power Using the CLI	144
▼ Monitor Individual Power Supply Consumption Using the CLI	145

- ▼ Monitor Available Power Using the CLI 146
- ▼ Monitor Permitted Power Consumption Using the CLI 146
- ▼ Determine the State of Indicators Using the Web Interface 147
- ▼ Obtain Sensor Readings Using the Web Interface 148
- ▼ View or Clear the ILOM Event Log Using the Web Interface 148
- ▼ View or Clear the ILOM Event Log Using the CLI 150
- ▼ View and Configure Clock Settings Using the Web Interface 152
- ▼ Configure Remote Syslog Receiver IP Addresses Using the Web Interface 153
- ▼ Configure Remote Syslog Receiver IP Addresses Using the CLI 154
- ▼ Run the Snapshot Utility Using the CLI 155
- ▼ Run the Snapshot Utility Using the Web Interface 156

About Alert Management 158

- Alert Rule Configuration 158
  - Alert Rule Property Definitions 159

Manage Alert Rule Configurations Using the ILOM Web Interface 161

- Prerequisites 162
  - ▼ Modify an Alert Rule Configuration Using the Web Interface 162
  - ▼ Disable an Alert Rule Configuration Using the Web Interface 163
  - ▼ Generate Alert Tests Using the Web Interface 164

Manage Alert Rule Configurations Using the ILOM CLI 164

- CLI Commands for Managing Alert Rule Configurations 165
- Prerequisites 167
  - ▼ Modify Alert Rule Configurations Using the CLI 167
  - ▼ Disable an Alert Rule Configuration Using the CLI 168
  - ▼ Generate Alert Tests Using the CLI 169

Configure SMTP Client for Email Notification Alerts 170

- ▼ Enable SMTP Client Using the Web Interface 170
- ▼ Enable SMTP Client Using the CLI 171

## 8. Configure ILOM Communication Settings 173

### Manage ILOM Network Settings Using the CLI 174

#### About Network Settings 174

- ▼ View Network Settings Using the CLI 174
- ▼ Configure Network Settings Using the CLI 175
  - Targets, Properties, and Values 175

#### Serial Port Settings 176

- ▼ View Serial Port Settings Using the CLI 176
- ▼ Configure Serial Port Settings Using the CLI 177
  - Targets, Properties, and Values 177
- ▼ Enable HTTP or HTTPS Web Access Using the CLI 178
  - Targets, Properties, and Values 178

### Configure Secure Shell Settings 179

- ▼ Establish a Secure Remote Connection to Run CLI Commands 179
- ▼ View the Current Key Using the CLI 180
- ▼ Enable or Disable SSH Using the CLI 181
- ▼ Enable or Disable SSH Using the Web Interface 181
- ▼ Generate a New Key Using the CLI 182
- ▼ Generate a New Key Using the Web Interface 182
- ▼ Restart the SSH Server Using the CLI 183
- ▼ Restart the SSH Server Using the Web Interface 183

### Manage ILOM Network Settings Using the Web Interface 183

- ▼ View Network Settings Using the Web Interface 184
- ▼ Configure Network Settings Using the Web Interface 184
- ▼ Display Serial Port Settings Using the Web Interface 186
- ▼ Configure Serial Port Settings Using the Web Interface 187
- ▼ Enable HTTP or HTTPS Web Access Using the Web Interface 187

## **9. Intelligent Platform Management Interface 189**

IPMI Overview 189

ILOM and IPMI 190

Using IPMItool 190

IPMI Alerts 191

IPMItool Examples 192

- ▼ View a List of Sensors and Their Values 192
- ▼ View Details About a Single Sensor 193
- ▼ Power On the Host 193
- ▼ Power Off the Host 193
- ▼ Power Cycle the Host 193
- ▼ Shutdown the Host Gracefully 193
- ▼ View Manufacturing Information for FRUs 194
- ▼ View the IPMI System Event Log 195

## **10. Simple Network Management Protocol 197**

SNMP Overview 198

How SNMP Works 199

SNMP Management Information Base Files 199

Alerts and SNMP Traps 200

Manage SNMP Users With the CLI 201

- ▼ Add an SNMP User Account Using the CLI 201
  - ▼ Edit an SNMP User Account Using the CLI 201
  - ▼ Delete an SNMP User Account Using the CLI 201
  - ▼ Add or Edit an SNMP Community Using the CLI 202
  - ▼ Delete an SNMP Community Using the CLI 202
- Targets, Properties, and Values 202
- ▼ Configure SNMP Trap Destinations Using the CLI 203

Manage SNMP Users Using the Web Interface	204
▼ Configure SNMP Settings Using the Web Interface	204
▼ Add or Edit an SNMP User Account Using the Web Interface	206
▼ Delete an SNMP User Account Using the Web Interface	207
▼ Add or Edit an SNMP Community Using the Web Interface	208
▼ Delete an SNMP Community Using the Web Interface	208
▼ Configure SNMP Trap Destinations Using the Web Interface	209
SNMP Examples	209
▼ View and Configure SNMP Settings	210
▼ Obtain Information Using <code>snmpget</code> or <code>snmpwalk net-snmp</code> Commands	211
▼ Set Information Using <code>snmpset</code>	212
▼ Receive Traps Using <code>snmptrapd</code>	212
<b>11. Update ILOM Firmware</b>	<b>213</b>
Firmware Update Process	214
ILOM Firmware Update Overview	214
▼ View ILOM Version Information Using the CLI	215
Using the CLI Through the Management Ethernet Port	215
Using the CLI Through the Serial Port	215
▼ View ILOM Version Information Using the Web Interface	216
▼ Download New Firmware	217
Downloading New Firmware on x64-Based Systems	217
Downloading New Firmware on SPARC-Based Systems	217
▼ Update ILOM Firmware Using the CLI	218
▼ Update ILOM Firmware Using the Web Interface	219
▼ Update ILOM Firmware Using Sun xVM Ops Center	221
▼ Reset ILOM SP	221
▼ Reset SP to Factory Defaults Using the CLI	222
▼ Reset SP to Factory Defaults Using the Web Interface	222

**12. Remote Management of x64 Servers Using the Sun ILOM Remote Console 223**

Sun ILOM Remote Console Overview 224

    Single or Multiple Remote Host Server Management Views 224

    Installation Requirements 226

    Network Communication Ports and Protocols 227

    Administrator Role User Account – Sign In Authentication Required 227

Launch and Configure ILOM for Remote Management 228

    ▼ Connect to the ILOM Web Interface 228

    ▼ Configure ILOM Remote Control Settings Using the Web Interface 229

Launch and Configure Sun ILOM Remote Console for Remote x64 Server Management 232

    ▼ Launch the Sun ILOM Remote Console Using the ILOM Web Interface 232

    ▼ Add a New Server Session 234

    ▼ Start, Stop, or Restart Device Redirection 234

    ▼ Redirect Keyboard and Mouse Devices 235

    ▼ Control Keyboard Modes and Key Send Options 235

    ▼ Redirect Storage Devices 236

    ▼ Exit the Sun ILOM Remote Console 238

CD and Diskette Redirection Operation Scenarios 238

**A. ILOM Command-Line Interface Reference 241**

    CLI Command Quick Reference 241

    CLI Command Reference 247

**B. Glossary 263**

**Index 281**

# Preface

---

*Sun Integrated Lights Out Manager 2.0 User's Guide* discusses ILOM features and tasks that are common to Sun rackmounted servers or blade servers that support ILOM.

You can access these features or perform these tasks in the same way, regardless of the Sun server platform that ILOM is managing. Other user documents present ILOM features and tasks that are specific to the server platform you are using. You can find the ILOM platform-specific information within the documentation set that accompanies your system.

---

## Before You Read This Document

This User's Guide provides detailed information about the ILOM features and functions that are common to all server platforms managed by ILOM. To fully understand the information and perform the tasks discussed in this User's Guide, you should use this document in conjunction with the ILOM documentation that comes with your specific server platform.

---

## How This Document Is Organized

This document includes the following information:

[Chapter 1](#) provides an overview of ILOM features and functions.

[Chapter 2](#) explains how to establish initial communication with ILOM and what type of tasks you can perform with different connections.

[Chapter 3](#) describes how to use the ILOM command-line interface (CLI) and how to log in to ILOM using the CLI.

[Chapter 4](#) describes how to use the ILOM web interface and how to log in to ILOM using the web interface.

[Chapter 5](#) explains how to manage user accounts using the ILOM CLI or web interface, as well as how to configure Active Directory, LDAP, and RADIUS.

[Chapter 6](#) describes how to view and modify component information, how to prepare to remove components and return components to service, and how to configure policy settings.

[Chapter 7](#) explains how to monitor the system using sensors, indicators, and event logs and also describes how to manage alerts.

[Chapter 8](#) presents an overview of ILOM network settings and the tasks you need to perform to configure the network settings using the ILOM CLI or web interface.

[Chapter 9](#) describes the Intelligent Platform Management Interface and IPMItool.

[Chapter 10](#) explains how SNMP works and how to manage SNMP users using the ILOM CLI or web interface.

[Chapter 11](#) explains how to upgrade and reset ILOM firmware using the ILOM CLI or web interface.

[Chapter 12](#) describes the ILOM Remote Console application and how to launch and configure the Remote Console to remotely manage a server platform.

[Appendix A](#) presents a reference to ILOM CLI commands and explains how to use the commands.

[Appendix B](#) is a glossary that provides the definitions of some words and phrases used in this User's Guide.



---

# 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.
<b>AaBbCc123</b>	What you type, when contrasted with on-screen computer output.	% <b>su</b> password:
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be superuser to do this. To delete a file, type <code>rm filename</code> .

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

---

## Related Documentation

You should use this document in conjunction with the ILOM platform supplement documentation that comes with your specific platform.

---

# Documentation, Support, and Training

---

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

---

---

## Third-Party Web Sites

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

---

## Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

<http://www.sun.com/hwdocs/feedback>

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

*Sun Integrated Lights Out Manager 2.0 User's Guide*, part number 820-1188-12.

# Introduction to ILOM

---

Sun™ Integrated Lights Out Manager (ILOM) 2.0 is the system management firmware you can use to monitor, manage, and configure a variety of Sun server platforms.

This chapter includes the following sections:

- [“What Is ILOM?” on page 1](#)
- [“What Does ILOM Do?” on page 2](#)
- [“ILOM on the SP and CMM” on page 3](#)
- [“ILOM Interfaces” on page 4](#)
- [“ILOM Management Network” on page 5](#)
- [“ILOM Connection Methods” on page 5](#)
- [“Roles for ILOM User Accounts” on page 6](#)
- [“Preconfigured ILOM Administrator Account” on page 7](#)
- [“ILOM Features” on page 7](#)
- [“New Features in ILOM 2.0” on page 9](#)
- [“Other Management Tools” on page 10](#)

---

## What Is ILOM?

Sun’s Integrated Lights Out Manager (ILOM) provides advanced service processor hardware and software that you can use to manage and monitor your Sun servers. ILOM’s dedicated hardware and software is preinstalled on a variety of Sun x64-based Sun Fire servers, Sun Blade Modular Systems, and Sun Blade server modules, as well as on SPARC-based servers. ILOM is a vital management tool in the data center and can be used to integrate with other data center management tools already installed on your systems.

Sun is currently transitioning many systems to support ILOM so that customers will have a single, consistent, and standards-based service processor (SP) across Sun's product lines. For customers, this means you will have:

- Single, consistent system management interfaces for operators
- Rich protocol and standards support
- Broadening third-party management support
- System management functions integrated into Sun servers at no extra cost

---

## What Does ILOM Do?

ILOM enables you to actively manage and monitor the server independently of the operating system state, providing you with a reliable Lights Out Management (LOM) system. With ILOM, you can proactively:

- Learn about hardware errors and faults as they occur
- Remotely control the power state of your server
- View the graphical and non-graphical consoles for the host
- View the current status of sensors and indicators on the system
- Determine the hardware configuration of your system
- Receive generated alerts about system events in advance via IPMI PETs, SNMP Traps, or Email Alerts.

The ILOM SP runs its own embedded operating system and a dedicated Ethernet port, which together provide out-of-band management capability. In addition, you can access ILOM from the server's host operating system that Sun supports (Solaris, Linux, and Windows). Using ILOM, you can remotely manage your server as if you were using a locally attached keyboard, monitor, and mouse.

ILOM automatically initializes as soon as power is applied to your server. It provides a full-featured, browser-based web interface and has an equivalent command-line interface. There is also an industry-standard SNMP interface and IPMI interface.

You can easily integrate these management interfaces with other management tools and processes that you may have working already with your servers, such as Sun xVM Ops Center. This easy-to-use system management platform for Solaris and Linux provides the tools you need to efficiently manage systems on your network. Sun xVM Ops Center can discover new and existing systems on your network, update firmware and BIOS configurations, provision the operating environment with off the shelf distributions or Solaris images, manage updates and configuration changes,

and remotely control key aspects of the service processor such as boot control, power status, and indicator lights. For more information about xVM Ops Center, go to:

<http://www.sun.com/software/products/xvmopscenter/index.jsp>

In addition, you can integrate ILOM with these third-party management tools:

- Altiris Deployment Server 6.8
- BMC Patrol
- CA Unicenter Network and Systems Management (NSM)
- HP OpenView Operations for UNIX
- HP OpenView Operations for Windows
- HP Systems Insight Manager
- IBM Director 1.0
- IBM Tivoli Enterprise Console
- IBM Tivoli Monitoring (ITM)
- IBM Tivoli Netcool/OMNIBus
- Microsoft System Management
- Scalent Virtual Operating Environment (V/OE)
- IPMItool 1.8.8 for Microsoft Windows 2003

A description of these third-party system management tools and their support for Sun systems is available at:

<http://www.sun.com/system-management/tools.jsp>

---

## ILOM on the SP and CMM

ILOM is supported on a variety of Sun server platforms, including rackmounted servers and server modules (blades) enclosed in a modular chassis system. ILOM firmware is preinstalled on the service processor (SP) of your rackmounted server or server module, or on the Chassis Monitoring Module (CMM) that is part of the modular chassis system.

ILOM supports two ways to manage a system: using the SP directly or using the CMM, if you are using a modular chassis system.

- **Using the service processor directly** – Communicating directly with the rackmounted server SP or server module SP enables you to manage individual server operations. This approach may be useful in troubleshooting a server module or rackmounted server, or controlling access to specific servers in your data center.
  - **Using the Chassis Monitoring Module** – If you are using a modular chassis system, managing the system from the CMM enables you to set up and manage components throughout the entire modular chassis system, or to drill down to manage the individual blade server SP.
- 

## ILOM Interfaces

ILOM is available through a variety of interfaces.

- **Web interface** – The web interface provides an easy-to-use browser interface that enables you to log in to the SP and to perform system management, monitoring, and IPMI tasks. For information about the ILOM web interface, see [Chapter 4](#).
- **Command-line interface (CLI)** – The command-line interface enables you to operate ILOM using keyboard commands and adheres to industry-standard DMTF-style CLI and scripting protocols. You can connect a terminal or PC running terminal emulator software directly to the system serial port, or connect to the Ethernet network management port using a Secure Shell (SSH). For information about the CLI, see [Chapter 3](#).
- **Remote Console** – The ILOM Remote Console (JavaRConsole) enables you to access your server’s console remotely. It redirects the keyboard, mouse, and video screen, and can redirect input and output from the local machine’s CD and diskette drives. For information about the Remote Console, see [Chapter 12](#).
- **Intelligent Platform Management Interface (IPMI)** – Using IPMI v1.5 and v2.0 and the IPMITool utility, you can manage and configure devices using a CLI to retrieve information from the system’s Baseboard Management Controller (BMC). With IPMITool, you can monitor the status of hardware components remotely, monitor system logs, receive reports about replaceable components, and redirect the server console. For more information about IPMI, see [Chapter 9](#).
- **Simple Network Management Protocol (SNMP) interface** – ILOM 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 Sun xVM Ops Center, or third-party applications such as Hewlett-Packard OpenView® and IBM Tivoli®. For more information about SNMP, see [Chapter 10](#).

---

# ILOM Management Network

Your Sun server platform comes with a network management port and a data port. These separate, physical Ethernet connections are for ILOM and the operating systems that run on the host hardware. You can choose to manage your server platform with ILOM by connecting to the dedicated network management port. If you choose to connect to ILOM through the network management port, traffic destined for ILOM is separate from any data transfers the operating system host makes. No data traffic passes through the network port. This allows management traffic to be completely isolated on a separate network, if desired.

The location and labeling of the network management port is specific to your system. In addition, the type of server platform determines how internal management communications are provided. For example, on a blade server system, the network port provides a connection to all CMMs and SPs in the chassis. Refer to your platform documentation to determine how your system provides its management communications.

If you choose not to use ILOM and the network management port to manage your server, many of the advanced features, such as environmental monitoring, IPMI management, and the web interface, will be unavailable. You can use the data port of the host operating system to access third-party network management applications, SNMP tools, or operating system utilities, however these solutions only have a limited view of the platform. You also can manage your server locally by connecting through the server's serial port using a PC or terminal running terminal emulator software. Note that without some manner of direct connection to ILOM, you will be unable to remotely manage your Sun server platform.

---

# ILOM Connection Methods

The way you connect to ILOM depends on your server platform.

The following table lists the different methods you can use to connect to ILOM.

**TABLE 1-1** ILOM Connection Methods

Connection Method	Rack Mounted Blade		Supported Interface	Description
	Mounted	Blade		
Ethernet network management connection	Yes	Yes	CLI and web interface	Connect to the Ethernet network management port. You must know ILOM's IP address. This method supports a web interface and a command-line interface.
Serial connection, through server or blade	Yes	Yes	CLI only	Connect directly to the serial management port on the server or blade. If needed, use a serial adapter cable to connect to the serial port. This method supports only a command-line interface.
Serial connection, through CMM	No	Yes	CLI only	Connect to the serial port on the CMM. This method supports only a command-line interface.

---

**Note** – ILOM supports a maximum of 10 active sessions, including serial, Secure Shell (SSH), and web interface sessions.

---

To access the management network using the ILOM web interface or CLI, you need the IP address for the CMM or the SP you want to manage. Each CMM and SP is assigned a unique IP address during the initial system setup. To assign the initial IP addresses for SPs and CMMs, see [Chapter 2](#).

---

## Roles for ILOM User Accounts

ILOM user accounts have defined roles that determine ILOM user access and rights. Administrators can manage user accounts using the ILOM web interface or CLI. The roles assigned to ILOM accounts are:

- **Administrator** – Enables access to all ILOM features, functions, and commands.
- **Operator** – Enables access to fully manage and monitor the host system, and also provides read-only access to ILOM configuration.



---

# Preconfigured ILOM Administrator Account

ILOM is preinstalled with one preconfigured Administrator account:

- User name: root
- Password: changeme

The preconfigured Administrator account, known as root, cannot be deleted or changed, other than resetting its default password (changeme). This account provides built-in administrative privileges (read and write access) to all ILOM features, functions, and commands.

The first time you access ILOM, at the SP or CMM level, you will need to log in as root with the default changeme password. After you have logged in to ILOM and established network connectivity to the system, you should consider resetting the default changeme password that is associated with the ILOM root account. To prevent your system from unauthorized access, reset this password on each SP and CMM installed in your system. For information about resetting the ILOM root account password, see [“Reset ILOM SP” on page 221](#).

---

## ILOM Features

[TABLE 1-2](#) shows the ILOM features and tasks that are common to Sun systems supporting ILOM. For information about whether the feature is supported on your system, consult the user documentation provided with your Sun server platform.

**TABLE 1-2** ILOM Features

Feature	Customer Benefit
INTERFACES	
Web interface	<ul style="list-style-type: none"><li>• Provides a browser-based user interface based on Sun standard.</li></ul>
Command-line interface	<ul style="list-style-type: none"><li>• Supports industry-standard CLIs and scripting protocols: DMTF “SMASH” CLP.</li><li>• Reuses existing scripts with Sun systems, automates tasks using familiar interfaces.</li></ul>

**TABLE 1-2** ILOM Features (Continued)

Feature	Customer Benefit
System management interfaces	<ul style="list-style-type: none"> <li>• Supports industry-standard SNMP v1, v2c, v3 and IPMI v1.5 and v2.0. Platform MIB enables platform management using SNMP in addition to IPMI. Control MIB enables custom or third-party management applications to integrate with ILOM.</li> <li>• Provides access to remote system using the ILOM Remote Console.</li> </ul>

## SECURITY

SSH 2.0 support	<ul style="list-style-type: none"> <li>• Enables secure access to the CLI.</li> </ul>
LDAP, MSFT Active Directory, RADIUS	<ul style="list-style-type: none"> <li>• Supports industry-standard authentication and authorization protocols for easy integration into existing environments.</li> </ul>
User management	<ul style="list-style-type: none"> <li>• Supports Administrator and Operator roles with configurable access levels for greater security and control of systems.</li> </ul>
Reset root password capability	<ul style="list-style-type: none"> <li>• Prevents unauthorized access to the system. Password is reset to default using a push button or jumper.</li> </ul>
SSL certificate	<ul style="list-style-type: none"> <li>• Enables secure communications using default SSL certificate and self-signing key for HTTPS access.</li> </ul>

## LOCAL AND REMOTE ACCESS

Access to SP while host is powered down	<ul style="list-style-type: none"> <li>• Enables continuous ILOM operation regardless of the state of the host operating system.</li> </ul>
Dedicated network management port	<ul style="list-style-type: none"> <li>• Separates network management traffic from data network traffic.</li> </ul>
Remote Console	<ul style="list-style-type: none"> <li>• Provides a simple web interface to access remote systems. No need to log in to the SP to start the Remote Console.</li> </ul>
Editable hostname data field	<ul style="list-style-type: none"> <li>• Allows Administrators to use the hostname data field in addition to the IP address for system identification.</li> </ul>
Web interface turns on or off	<ul style="list-style-type: none"> <li>• Restricts ILOM access and enables only CLI access.</li> </ul>

## MONITORING AND LOGGING

SNMP and IPMI monitoring and control	<ul style="list-style-type: none"> <li>• Monitors components using industry-standard SNMP commands and the IPMI IPMItool utility.</li> </ul>
Event logging	<ul style="list-style-type: none"> <li>• Provides a consistent method for logging all “service” data.</li> </ul>

**TABLE 1-2** ILOM Features (Continued)

Feature	Customer Benefit
Configurable alert thresholds	<ul style="list-style-type: none"> <li>Enables users to configure the SP to send an IPMI PET alert when system thresholds are crossed.</li> </ul>
Email event notification	<ul style="list-style-type: none"> <li>Provides quick and convenient notification of events.</li> </ul>
Hardware and system-related errors, as well as ECC memory errors, reported into SP logs, Syslog, and remote log-host	<ul style="list-style-type: none"> <li>Enables faster fault diagnosis and isolation, reducing downtime.</li> </ul>
<b>POWER CONTROL</b>	
Forced power-off	<ul style="list-style-type: none"> <li>Enables emergency power off of the system.</li> </ul>
Graceful shutdown and power cycling	<ul style="list-style-type: none"> <li>Enables users to shut down the host operating system before system power-off.</li> </ul>
Remote power on and power off	<ul style="list-style-type: none"> <li>Enables users to control system power remotely.</li> </ul>
<b>FIRMWARE</b>	
Firmware versions identified from web interface or CLI	<ul style="list-style-type: none"> <li>Provides a simple way to identify firmware versions.</li> </ul>
Firmware updates using web interface or CLI	<ul style="list-style-type: none"> <li>Provides simple procedures to update firmware.</li> </ul>
<b>CONFIGURATION</b>	
Manual SP configuration, including IP address, through BIOS interface, serial or Ethernet SP ports, or host OS	<ul style="list-style-type: none"> <li>Simplifies initial configuration.</li> </ul>
SP IP address programmable from local keyboard and monitor	<ul style="list-style-type: none"> <li>Facilitates manual IP configuration for systems in a data center.</li> </ul>

## New Features in ILOM 2.0

- Active Directory
- Email alerts
- New updated Sun-specific MIBs
- SNMP Traps
- Internationalization of the Remote Console

---

## Other Management Tools

Sun servers support a variety of system management tools that you can use to administer the system. In addition to ILOM, these system management tools include:

- **Sun xVM Ops Center**– Sun xVM Ops Center is a comprehensive system management tool that you can purchase separately. This tool offers flexible capabilities that simplify infrastructure management of SPARC, x64 Sun Fire servers, and Sun Blade Server Modules. With Sun xVM Ops Center, IT administrators can monitor, maintain, and provision multiple systems remotely from any Sun Sun xVM Ops Center. For more information about Sun xVM Ops Center, see the following site:

<http://www.sun.com/software/products/xvmopscenter/>

- **Third-party system management tools** – Sun systems support both SNMP (v1, v2c, v3) and IPMI (v1.5 and v2.0) to integrate third-party system management tools like HP Systems Insight Manager and IBM Tivoli. A listing of some of the key third-party system management tools and their support for Sun x64 systems is available at:

<http://www.sun.com/x64/system-management/tools.jsp>

# Establish Initial Communication With ILOM

---

You can establish communication with ILOM through a console connection to the serial management port on the server or CMM, or through an Ethernet connection to the network management port on the server or CMM.

The type of connection you establish to ILOM determines which type of tasks you can perform. For example, to remotely access the full range of system management functionality in ILOM, you will require both an Ethernet connection and an IP assignment to the server SP and, if applicable, to the CMM.

This chapter includes the following sections:

- [“About ILOM’s Initial Setup” on page 12](#)
  - [“Initial Setup Worksheet” on page 12](#)
  - [“DHCP IP Assignment Considerations” on page 14](#)
  - [“Static IP Assignment Considerations” on page 18](#)
  - [“Management Network IP Address Configuration” on page 20](#)
  - [“ILOM Network Port Assignment” on page 20](#)
  - [“Hostname Identity for Server SP and CMM” on page 22](#)
  - [“System Identifier Text String for Sun Servers” on page 22](#)
- [“Assign IP Addresses to the Sun Server Platform SP Interfaces” on page 23](#)
  - [“Assign DHCP IP Addresses Using an Ethernet Management Connection” on page 23](#)
  - [“Assign a Static IP Address to Server SP Using a Serial Connection” on page 25](#)
  - [“Assign Static IP Address to CMM Using a Serial Connection” on page 27](#)
- [“Edit IP Address Assignments Using an Ethernet Management Connection” on page 29](#)
  - [“Edit Existing IP Addresses in ILOM Using the Web Interface” on page 29](#)
  - [“Edit Existing IP Addresses in ILOM Using the CLI” on page 30](#)
- [“Assign Hostname or System Identifier” on page 33](#)

---

# About ILOM's Initial Setup

Prior to establishing communication with ILOM, you should consult the following topics:

- ["Initial Setup Worksheet" on page 12](#)
- ["DHCP IP Assignment Considerations" on page 14](#)
- ["Static IP Assignment Considerations" on page 18](#)
- ["Management Network IP Address Configuration" on page 20](#)
- ["ILOM Network Port Assignment" on page 20](#)
- ["Hostname Identity for Server SP and CMM" on page 22](#)
- ["System Identifier Text String for Sun Servers" on page 22](#)

## Initial Setup Worksheet

Use the following worksheet in [TABLE 2-1](#) to gather the information that you will need to initially establish communication with ILOM.

**TABLE 2-1** Initial Setup Worksheet to Establish Communication With ILOM

Information for Setup	Requirement	Description
Local Serial Console Connection	<p>Optional - <i>if using DHCP to assign initial IP address</i></p> <p>Mandatory - <i>if DHCP server is not utilized to assign initial IP address</i></p>	<p>If you are not utilizing a DHCP server to assign IP addresses to the server SP or CMM, you must establish a local serial console connection to ILOM via the serial management port on the server or Chassis Monitoring Module (CMM).</p> <p>For more information about how to attach a serial console to a server or CMM, consult the user documentation provided with the Sun server platform.</p>
Remote Ethernet Management Connection	Optional	<p>Attach a network (Ethernet) cable to the network management port on the server or the CMM. The label appearing on the network management port may be different depending on the server platform. Some server and CMM network management ports are labeled NET MGT or MGT. If you have a question about the network management port label, or how to attach an Ethernet cable to the management port, consult the user documentation provided with the Sun server platform.</p> <p>To access ILOM's full range of management functionality, you must connect your local area network to the network management port of a server or CMM.</p> <p>Note that a network management port is provided on all Sun rackmount standalone servers. However, this port is not provided on Sun Blade Server Modules. Ethernet communication with blade server modules is through the network management port on the CMM.</p>
SP IP Assignment	Mandatory	<p>Decide whether to assign DHCP or static IP address(es) to the server SP(s) or CMM(s). All remote system management communication with ILOM is through the server SP or CMM management network.</p> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">"DHCP IP Assignment Considerations" on page 14</a></li> <li>• <a href="#">"Static IP Assignment Considerations" on page 18</a></li> <li>• <a href="#">"Assign IP Addresses to the Sun Server Platform SP Interfaces" on page 23</a></li> </ul>

**TABLE 2-1** Initial Setup Worksheet to Establish Communication With ILOM (Continued)

Information for Setup	Requirement	Description
ILOM Interface	Mandatory	<p>When establishing (or modifying) an IP address on a server SP or CMM, you will use one of the following ILOM interfaces:</p> <ul style="list-style-type: none"> <li>• <b>Command-line interface (CLI) - use to establish the initial IP address.</b> If an IP address has not been assigned to the server SP or CMM, you can connect to ILOM to assign the IP address via a local serial console. The CLI is typically used for all tasks performed in ILOM over a serial connection (local serial console, terminal emulation application, or remote SSH connection).</li> <li>• <b>Web interface - use to edit an existing IP address.</b> If an IP address has been assigned to the server SP or CMM and a LAN connection is established to the MGT port, you can connect to ILOM to edit the existing IP address(es) assigned using the web interface. The web interface is typically used for all tasks performed in ILOM over an Ethernet management connection.</li> </ul> <p>For more information about ILOM interfaces, see <a href="#">Chapter 3</a> and <a href="#">Chapter 4</a>.</p>
ILOM Firewall Access	Optional	Consult ILOM's network port usage for Ethernet networks requiring firewall access. For more information, see <a href="#">"ILOM Network Port Assignment"</a> on page 20.
SP Hostname Assignment	Optional	You can optionally assign a meaningful hostname to a server SP. For more information, see <a href="#">"Hostname Identity for Server SP and CMM"</a> on page 22 or <a href="#">"Assign Hostname or System Identifier"</a> on page 33.
System Identifier Assignment	Optional	You can optionally assign a system identifier (meaningful name) to a Sun server. For more information, see <a href="#">"Hostname Identity for Server SP and CMM"</a> on page 22 or <a href="#">"Assign Hostname or System Identifier"</a> on page 33

## DHCP IP Assignment Considerations

If you are planning to use a Dynamic Host Configuration Protocol (DHCP) server to assign an IP address to a server SP or CMM, consult the following topics:

- ["Sun Server Platform DHCPDISCOVER Packet Broadcast"](#) on page 15
- ["Requirements for DHCP Assignment"](#) on page 15
- ["SP Network Interface MAC Address"](#) on page 15
- ["Post DHCP Requirements"](#) on page 17



# Sun Server Platform DHCPDISCOVER Packet Broadcast

The Sun server SP or CMM automatically broadcasts a DHCPDISCOVER packet when power is applied to the Sun server platform. If you have an established DHCP server on the network, the DHCP server automatically returns a DHCPOFFER packet containing IP address(es) and other network configuration information to the requesting server SP(s) or CMM(s).

---

**Note** – You can choose to have a DHCP server assign Ethernet IP address(es) for you, or you can configure the DHCP server to assign specific Ethernet IP address(es) by providing the MAC address of the SP(s). For more information, consult the DHCP server user documentation. For more information about how to obtain the MAC address of the server SP or CMM, see [“SP Network Interface MAC Address” on page 15](#).

---

## Requirements for DHCP Assignment

The following conditions must be present to assign IP address(es) to the Sun server SP interfaces using a DHCP server:

- An Ethernet cable must be plugged into the server management port or CMM management port.
- A DHCP server must be connected to the same subnet as the Sun server platform.
- The DHCP server must be configured to accept new media access control (MAC) addresses.
- The DHCP configuration setting in ILOM must be enabled. This setting is enabled by default.

## SP Network Interface MAC Address

If you are planning to use a DHCP server to assign IP address(es) to the SP network interface(s), you might need the MAC address of the server SP or CMM.

You can obtain the service processor MAC address via one of the methods described in [TABLE 2-2](#).

**TABLE 2-2** Methods for Obtaining SP MAC Address

<b>ILOM Category</b>	<b>Method</b>	<b>Description</b>
Rackmount server SP	View internal label	Typically, the MAC address label for the server SP on the management network appears on a sticker attached to the server.
Blade server SP		If the MAC address does not appear on a sticker attached to the server, consult the user documentation provided with the Sun server platform.
CMM	View internal label	Typically, the MAC address label for the CMM on the management network appears on a sticker attached to the CMM.  If the MAC address does not appear on a sticker attached to the CMM, consult the user documentation provided with the Sun server platform.
All	Customer Information Sheet	Refer to the Customer Information Sheet provided with the Sun server platform.

## Post DHCP Requirements

After the DHCP server has assigned IP address(es) to the SP network interface(s), you can identify the IP address(es) that were assigned by the DHCP server using one of the methods specified in [TABLE 2-3](#).

**TABLE 2-3** Methods for Identifying IP Address(es) Assigned by DHCP Server

Method	Description
DHCP log file  (Note that this log file is not part of ILOM, it is the log file on the DHCP server.)	Open the DHCP log file and do the following: <ol style="list-style-type: none"><li>1. Locate the MAC address of the service processor in the MAC address field.</li><li>2. Identify the IP value assigned in the IP address field that corresponds to the MAC address in the MAC address field.</li><li>3. Use the IP address you identified in Step 2 to remotely communicate with ILOM using the web interface.</li></ol> <p><b>Tip.</b> Typically, DHCP log file entries are individual lines with the following comma-separated fields: ID, Date, Time, Description, IP Address, Host Name, MAC Address.</p>
Serial console connection	Establish a serial console connection to the serial port on the server or CMM.  Log in to ILOM as root using the CLI and type one of the following commands: <ul style="list-style-type: none"><li>• For rackmount standalone servers: <code>show /SP/network</code></li><li>• For a chassis blade server module: <code>show /CH/BLn/SP network</code></li><li>• For a chassis CMM in slot 0: <code>show /CMM/network/CMM0</code></li><li>• For chassis CMM in slot 1: <code>show /CMM/network/CMM1</code></li></ul>

# Static IP Assignment Considerations

If you are planning to assign static IP address(es) to a server SP or CMM, consult the following topics:

- [“Requirements for Static IP Assignment”](#) on page 18
- [“Serial Device - Terminal Emulation Software Settings”](#) on page 19
- [“Post Static IP Assignment”](#) on page 19

## Requirements for Static IP Assignment

To initially assign a static IP address to a server SP or CMM, you must satisfy the requirements described in [TABLE 2-4](#).

**TABLE 2-4** Requirements for Static IP Assignment

Requirements	Step	Description
Establish serial console connection	1	Establish a serial console connection to the server SP or CMM by connecting a terminal or PC running terminal emulation software to the serial port of a server or CMM. For more information about how to attach a serial terminal or PC to a serial port on a server or CMM, consult the user documentation provided with the Sun server platform. Note that for Sun server platforms that have CMMs, you can configure the static IP address for the blade SPs installed in the chassis using the CMM ILOM command-line interface.
Configure serial port settings	2	Configure the required serial settings for the terminal device or terminal emulation software. For more information, see <a href="#">“Serial Device - Terminal Emulation Software Settings”</a> on page 19.
Assign static IP address using the ILOM CLI	3	Assign the static IP address using the ILOM CLI. For more information, see the following topics that apply to your system configuration: <ul style="list-style-type: none"><li>• <a href="#">“Assign a Static IP Address to Server SP Using a Serial Connection”</a> on page 25.</li></ul> or <ul style="list-style-type: none"><li>• <a href="#">“Assign Static IP Address to CMM Using a Serial Connection”</a> on page 27.</li></ul>

## Serial Device - Terminal Emulation Software Settings

When connecting to ILOM using a serial console, you will need to configure the terminal device or terminal emulation software to use the following serial settings:

- 8N1: eight data bits, no parity, one stop bit
- 9600 baud
- Disable hardware flow control (CTS/RTS)
- Disable software flow control (XON/XOFF)

The following CLI `show` commands enable you to view properties and values associated with a server or CMM external serial port:

```
show <target>
```

Examples:

- For a CMM: `show /CMM/serial/external`
- For a rackmount server: `show /SP/serial/external`
- For a blade server module: `show /CH/BLn/SP/serial/external`

## Post Static IP Assignment

You can remotely manage IP addresses using the ILOM web interface or CLI after satisfying these requirements:

- IP address assignment to a server SP or CMM
- Established Ethernet connection to the server or CMM network management port

For more information about managing the assignment of IP addresses using an Ethernet network management connection, see [“Edit IP Address Assignments Using an Ethernet Management Connection”](#) on page 29.

# Management Network IP Address Configuration

ILOM's IP connections are typically configured to the SP network interface, which enables you to separate management traffic and data traffic. The DHCP or static IP address(es) that you assign to a server SP or CMM are known as the *management network IP address(es)*, not to be confused with the data network IP address(es).

Note that the data network IP addresses are configured after installing a host operating system on a server. It is important to distinguish the data network IP addresses from the management network IP addresses since they serve different purposes.

All future references, in this guide, to the management network IP addresses will be referred to as the "IP address of the server SP" or "IP address of the CMM." Typically, these references are presented when providing instructions for connecting to the ILOM web interface or the ILOM CLI.

For more information about ILOM's management network, see ["ILOM Management Network" on page 5](#).

For information about assigning data network IP addresses to a server, consult the user documentation provided with the host operating system.

## ILOM Network Port Assignment

[TABLE 2-5](#) and [TABLE 2-6](#) identify the default network ports used by ILOM. Most of these network ports are configurable. When configuring firewall security access to ILOM, you should configure these ports with the appropriate ports that are currently being used by the firewall service.

**TABLE 2-5** Direct Server SP ILOM Port Assignment

Ports	Protocols	Applications
80	HTTP over TCP	SP - ILOM user configurable port
443	HTTPS over TCP	SP - ILOM user configurable port
5120	TCP	SP - ILOM Remote Console: CD
5123	TCP	SP - ILOM Remote Console: Diskette
5121	TCP	SP - ILOM Remote Console: Keyboard and Mouse
7578	TCP	SP - ILOM Remote Console: Video
22	SSH over TCP	SSH - Secure Shell
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol
123	NTP over UDP	NTP - Network Time Protocol

**TABLE 2-5** Direct Server SP ILOM Port Assignment *(Continued)*

161	SNMP over UDP	SNMP - Simple Network Management Protocol
162	IPMI over UDP	IPMI - Platform Event Trap (PET) (outgoing port)
389	LDAP over UDP/TCP	LDAP - Lightweight Directory Access Protocol (user configurable port)
514	Syslog over UDP	Syslog - (outgoing port)
546	DHCP over UDP	DHCP - Dynamic Host Configuration Protocol (client)
623	IPMI over UDP	IPMI - Intelligent Platform Management Interface
1812	RADIUS over UDP	RADIUS - Remote Authentication Dial In User Service

**TABLE 2-6** Direct CMM ILOM Network Port Assignment

<b>Ports</b>	<b>Protocols</b>	<b>Applications</b>
80	HTTP over TCP	CMM - ILOM (user configurable port)
443	HTTPS over TCP	CMM - ILOM (user configurable port)
8000 - 8009	HTTP over TCP	CMM - ILOM drill-down (BL0-BL9)
8400 - 8409	HTTPS over TCP	CMM - ILOM drill-down (BL0-BL9)
22	SSH over TCP	SSH - Secure Shell
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol
123	NTP over UDP	NTP - Network Time Protocol
161	SNMP over UDP	SNMP - Simple Network Management Protocol
389	LDAP over UDP/TCP	LDAP - Lightweight Directory Access Protocol (user configurable port)
514	Syslog over UDP	Syslog - (outgoing port)
546	DHCP over UDP	DHCP - Dynamic Host Configuration Protocol (client)
1812	RADIUS over UDP	RADIUS - Remote Authentication Dial In User Service

## Hostname Identity for Server SP and CMM

As an alternative to an IP address, you can use a hostname to identify a particular server SP or CMM in your network. You can also use the hostname to establish a connection with the server SP ILOM or CMM ILOM. Typically, this type of system identification and connection requires you to associate the hostname with the IP address of the server SP (or CMM) in your naming service (such as DNS, NIS, SMB). If you use hostnames in your network environment to identify server SPs or CMMs, you can optionally apply the same identification in ILOM to a server SP or CMM by entering the hostname of the server SP (or CMM) on the System Identification page. For more information see, [“Assign Hostname and System Identifier Using the Web Interface”](#) on page 33.

## System Identifier Text String for Sun Servers

The system identifier is a text string that you can set to help you identify components of a Sun system. For example, you could create a system identifier that identifies the location of a system, a particular server in a rack, or details about the purpose of a system.

System identifiers are also included in SNMP traps. These system identifiers can help you associate the trap with the particular ILOM instance running on the system.

When you set a system identifier in ILOM, you can use any text characters to describe the system or component with the exception of quotation marks. For more information about how to specify a system identifier in ILOM, see [“Assign Hostname or System Identifier”](#) on page 33.



---

# Assign IP Addresses to the Sun Server Platform SP Interfaces

Use the following procedures to assign IP address(es) to the SP network interface(s) on a Sun server platform:

- [“Assign DHCP IP Addresses Using an Ethernet Management Connection” on page 23](#)
- [“Assign a Static IP Address to Server SP Using a Serial Connection” on page 25](#)
- [“Assign Static IP Address to CMM Using a Serial Connection” on page 27](#)
- [“Assign Hostname and System Identifier Using the Web Interface” on page 33](#)
- [“Assign Hostname and System Identifier Using the CLI” on page 35](#)

## ▼ Assign DHCP IP Addresses Using an Ethernet Management Connection

Follow these steps to assign IP addresses using DHCP:

1. **Verify that your DHCP server is configured to accept new media access control (MAC) addresses.**

Consult the documentation supplied with your DHCP server software.

2. **Verify that an Ethernet cable is connected to one of the following ports:**
  - Ethernet port (NET MGT) port on the CMM, if applicable
  - Ethernet port (MGT) on a rackmount standalone server, if applicable.

---

**Note** – Provided that ILOM was not configured previously with a static IP address, ILOM automatically broadcasts a DHCPDISCOVER packet with the ID of its SP network interface(s) MAC address(es). If ILOM was previously configured with a static IP address, you must disable the static IP address setting on the Network Settings tab. For more information about editing IP address settings, see [“Edit IP Address Assignments Using an Ethernet Management Connection” on page 29](#).

---

3. **The DHCP server on your network returns the DHCP OFFER packet containing the IP address and other information. The service processor then manages its “lease” of IP addresses assigned by the DHCP server.**
4. **Use one of the following methods to obtain the DHCP IP address(es) assigned to the SP network interface(s):**

- **ILOM-CMM using serial connection**

Using a serial console attached to the rear panel of the CMM, log in to ILOM as an Administrator. For example, at the Login prompt, you could type the preconfigured Administrator user name `root` and its default password `changeme`, then press Enter.

- To set the working directory for the active CMM, type:

```
cd /CMM/network/CMM0
```

- To view the active CMM IP address, type: **show**
- To drill-down and view the IP addresses of each blade, type:

```
show /CH/BL0/SP/network
```

---

**Note** – CMM0 represents the CMM installed in slot CMM0. BL0 represents the blade installed in slot BL0. To specify the target CMM or blade, you must specify the number of the slot in which the module is installed. Blade slots range from 0 to 9. CMM slots range from 0 to 1.

---

- **ILOM - Server SP using serial connection**

Using a serial console attached to the front panel of a blade, log in to ILOM as an Administrator. For example, at the Login prompt, you could type the preconfigured Administrator user name `root` and its default password `changeme`, then press Enter.

To view the blade SP IP address, type:

```
show /SP/network
```

- **DHCP server logs**

For more information, see [“Post DHCP Requirements” on page 17](#), or consult the DHCP server documentation for details.

## ▼ Assign a Static IP Address to Server SP Using a Serial Connection

Follow these steps to assign a static IP address to a server SP, using a serial connection:

### 1. Establish a local serial console connection to the server SP.

Attach a serial console to the serial port on the server or CMM. For more information, consult the user documentation provided with the Sun server platform.

### 2. Configure the following settings in the terminal window that appears on the connected serial console:

- 8N1: eight data bits, no parity, one stop bit
- 9600 baud
- Disable hardware flow control (CTS/RTS)
- Disable software flow control (XON/XOFF)

### 3. Press Enter to establish a connection between the serial console and the SP interface.

Eventually the ILOM Login prompt appears.

For example: *host name* Login:

### 4. Log in to ILOM as an Administrator by entering an Administrator user name and password, then press Enter.

---

**Note** – You can log in to ILOM using the preconfigured Administrator account shipped with ILOM: `root/changeme`. For more details, see [“Preconfigured ILOM Administrator Account” on page 7](#).

---

The default prompt appears (->). The system is ready to receive CLI commands to establish network settings.

### 5. Type the following command to set the working directory:

```
cd /SP/network
```

6. Use the following CLI commands to specify the IP, NetMask, and Gateway addresses.

Command	Description and Example
<code>set pendingipaddress=</code>	<p>Type this command followed by the static IP address that you want to assign to the server SP.</p> <p>For example, typing: <code>set pendingipaddress=129.144.82.26</code> instructs ILOM to assign 129.144.82.26 as the IP address to the server SP.</p>
<code>set pendingipnetmask=</code>	<p>Type this command followed by the static NetMask address that you want to assign to the server SP.</p> <p>For example, typing: <code>set pendingipnetmask=255.255.255.0</code> instructs ILOM to assign 255.255.255.0 as the NetMask address to the server SP.</p>
<code>set pendingipgateway=</code>	<p>Type this command followed by the static Gateway address that you want to assign to the server SP.</p> <p>For example, typing: <code>set pendingipgateway=129.144.82.254</code> instructs ILOM to assign 129.144.82.254 as the Gateway address to the server SP.</p>
<code>setpendingipdiscovery=</code>	<p>Type the following command to instruct ILOM to set a static IP address on the server SP.</p> <pre>set pendingipdiscovery=static</pre>
<code>set commitpending=true</code>	<p>Type this command (<code>true</code>) to assign the network settings specified.</p> <p>For example: <code>set pendingipaddress=129.144.82.26</code> <code>set pendingipnetmask=255.255.255.0</code> <code>set pendingipgateway=129.144.82.254</code> <code>set commitpending=true</code></p>

Typically, after assigning (or changing) an IP address the connection made to ILOM using the former IP address will timeout. Use the newly assigned IP address to connect to ILOM.

## ▼ Assign Static IP Address to CMM Using a Serial Connection

Follow these steps to assign a static IP address to a CMM, using a serial connection:

- 1. Verify that the serial connection to an active CMM is operational.**

For information about attaching a serial console to a CMM, consult the user documentation provided with the Sun server platform.

- 2. Log in to ILOM as an Administrator by entering an Administrator user name and password, then press Enter.**

---

**Note** – You can log in to ILOM using the preconfigured Administrator account shipped with ILOM: `root/changeme`. For more details, see [“Preconfigured ILOM Administrator Account” on page 7](#).

---

The default prompt appears (->) and the system is ready for you to run the CLI commands to establish network settings.

- 3. To set a static IP address on the CMM through the ILOM CLI, type the following command to set the working directory:**

```
cd /CMM/network/CMM0
```

---

**Note** – CMM0 refers to the CMM installed in slot CMM0. The target CMM is specified by referencing the slot number of the CMM.

---

#### 4. Use the following commands to specify the IP, NetMask, and Gateway addresses.

Command	Description and Example
<code>set pendingipaddress=</code>	Type this command followed by the static IP address that you want to assign to the CMM.  For example, typing: <code>set pendingipaddress=129.144.82.26</code> instructs ILOM to assign 129.144.82.26 as the CMM IP address.
<code>set pendingipnetmask=</code>	Type this command followed by the static NetMask address that you want to assign to the CMM.  For example, typing: <code>set pendingipnetmask=255.255.255.0</code> instructs ILOM to assign 255.255.255.0 as the CMM NetMask address.
<code>set pendingipgateway=</code>	Type this command followed by the static Gateway address that you want to assign to the CMM.  For example, typing: <code>set pendingipgateway=129.144.82.254</code> instructs ILOM to assign 129.144.82.254 as the CMM Gateway address.
<code>set pendingipdiscovery=</code>	Type the following command to tell ILOM that you want to set a static IP address. <code>set pendingipdiscovery=static</code>
<code>set commitpending=true</code>	Type this command (true) to assign the network settings specified.  Example: <code>set pendingipaddress=129.144.82.26</code> <code>set pendingipnetmask=255.255.255.0</code> <code>set pendingipgateway=129.144.82.254</code> <code>set comitpending=true</code>

If you connected to ILOM through a remote SSH connection, the connection made to ILOM using the former IP address will timeout. Use the newly assigned IP address to connect to ILOM.

---

# Edit IP Address Assignments Using an Ethernet Management Connection

Use the following procedures to manage service processor(s) IP assignment(s) over an Ethernet management connection:

- [“Edit Existing IP Addresses in ILOM Using the Web Interface” on page 29](#)
- [“Edit Existing IP Addresses in ILOM Using the CLI” on page 30](#)

## ▼ Edit Existing IP Addresses in ILOM Using the Web Interface

Follow these steps to edit existing IP address(es), using the ILOM web interface, that previously have been assigned to a server SP or CMM:

1. **Using a browser-based client, type the IP address of the server SP or CMM in the browser address box then press Enter.**

The ILOM Login screen appears.

2. **In the ILOM Login screen, log in as an Administrator by entering an Administrator user name and password.**

---

**Tip** – You can log in to ILOM using the preconfigured Administrator account shipped with ILOM: root/change-me. For more details, see [“Preconfigured ILOM Administrator Account” on page 7](#).

---

The ILOM interface appears.

3. **In the right pane of the ILOM interface, click Configuration --> Network.**

The Network Settings page for the server or CMM appears.

**FIGURE 2-1 ILOM Server SP - Network Settings Page**

**FIGURE 2-2 ILOM CMM - Network Settings Page**

Name	MAC	Mode	IP Address	Gateway	Netmask
JCHMASTERCMM	00:03:BA:84:CB:2A	DHCP	0.0.0.0	0.0.0.0	0.0.0.0
JCHCMM0	00:03:BA:F1:3B:88	Static	10.8.145.160	10.8.145.254	255.255.255.0
JCHBL1	00:03:BA:F1:32:66	Static	10.8.145.162	10.8.145.254	255.255.255.0
JCHBL3	00:03:BA:F1:2C:42	Static	10.8.145.184	10.8.145.254	255.255.255.0

4. To edit IP addresses assigned to the SP interfaces, do the following:
  - a. Select the radio button for Use the Following IP Address.
  - b. Enter values for IP Address, Subnet Mask, and Gateway in the text boxes.
  - c. Click Save for your new settings to take effect.

Typically, after assigning (or changing) an IP address the connection made to ILOM using the former IP address will timeout. Use the newly assigned IP address to connect to ILOM

## ▼ Edit Existing IP Addresses in ILOM Using the CLI

Follow these steps to edit existing IP address(es), using the ILOM CLI, that previously have been assigned to a server SP or CMM:

1. Establish a local serial console connection or SSH connection to the server SP or CMM:



- **Local Serial Console Connection**

Attach a serial console to the serial port on the server or CMM.

For more information, consult the user documentation provided with the Sun server platform.

or

- **Remote - Secure Shell (SSH) Connection**

Establish a Secure Shell connection to the server SP or CMM.

From the remote client, establish a secure connection as root to the server SP or CMM. For example, you can establish a secure connection from a remote SSH client to the server SP by typing the following:

```
ssh -l root server_ip_address
```

Password: **changeme**

The default prompt appears (->) and the system is ready for you to run the CLI commands to establish network settings.

**2. Type one of the following commands to set the SP working directory:**

- For a rackmount standalone server: `cd /SP/network`
- For a chassis server blade server module: `cd /SP/network`
- For a chassis CMM in slot 0: `cd /CMM/network/CMM0`
- For a chassis CMM in slot 1: `cd /CMM/network/CMM1`

**3. Type the `show` command to view the IP address(es) assigned, for example:**

- For a rackmount standalone server: `show /SP/network`
- For a chassis blade server module: `show /CH/BLn/SP network`
- For a chassis CMM in slot 0: `show /CMM/network/CMM0`
- For chassis CMM in slot 1: `show /CMM/network/CMM1`

#### 4. Type the following commands to change the existing IP assigned address.

Command	Description and Example
<code>set pendingipaddress=</code>	<p>Type this command followed by the static IP address that you want to assign to the server SP or CMM.</p> <p>For example, typing:</p> <pre>set pendingipaddress=129.144.82.26</pre> <p>instructs ILOM to assign 129.144.82.26 as the IP address to the server SP.</p>
<code>set pendingipnetmask=</code>	<p>Type this command followed by the static NetMask address that you want to assign to the server SP or CMM.</p> <p>For example, typing:</p> <pre>set pendingipnetmask=255.255.255.0</pre> <p>instructs ILOM to assign 255.255.255.0 as the NetMask address to the server SP (or CMM).</p>
<code>set pendingipgateway=</code>	<p>Type this command followed by the static Gateway address that you want to assign to the server SP or CMM.</p> <p>For example, typing:</p> <pre>set pendingipgateway=129.144.82.254</pre> <p>instructs ILOM to assign 129.144.82.254 as the Gateway address to the server SP (or CMM).</p>
<code>setpendingipdiscovery=</code>	<p>Type the following command to tell ILOM that you want to set a static IP address on the server SP or CMM.</p> <pre>set pendingipdiscovery=static</pre>
<code>set commitpending=true</code>	<p>Type this command (<code>true</code>) to assign the network settings specified.</p> <p>For example:</p> <pre>set pendingipaddress=129.144.82.26 set pendingipnetmask=255.255.255.0 set pendingipgateway=129.144.82.254 set commitpending=true</pre>

If you connected to ILOM through a remote SSH connection, the connection made to ILOM using the former IP address will timeout. Use the newly assigned IP address to connect to ILOM.

---

# Assign Hostname or System Identifier

If you use hostnames to identify Sun server SPs or CMMs in your network, you can configure ILOM to present this same identification (hostname) of the server SP or CMM in its banner. In addition, you can configure ILOM with a meaningful text string that will help you to identify the system in your network. For detailed instructions for assigning a hostname or system identification text string in ILOM, see:

- [“Assign Hostname and System Identifier Using the Web Interface” on page 33](#)
- [“Assign Hostname and System Identifier Using the CLI” on page 35](#)

For additional information about hostname assignments or examples of system identifier text strings, see [“Hostname Identity for Server SP and CMM” on page 22](#) or [“System Identifier Text String for Sun Servers” on page 22](#).

## ▼ Assign Hostname and System Identifier Using the Web Interface

Follow these steps to assign a hostname or system identifier in ILOM using the web interface:

- 1. Using a browser-based client, type the IP address of the server SP in the browser address box then press Enter.**

The ILOM Login dialog appears.

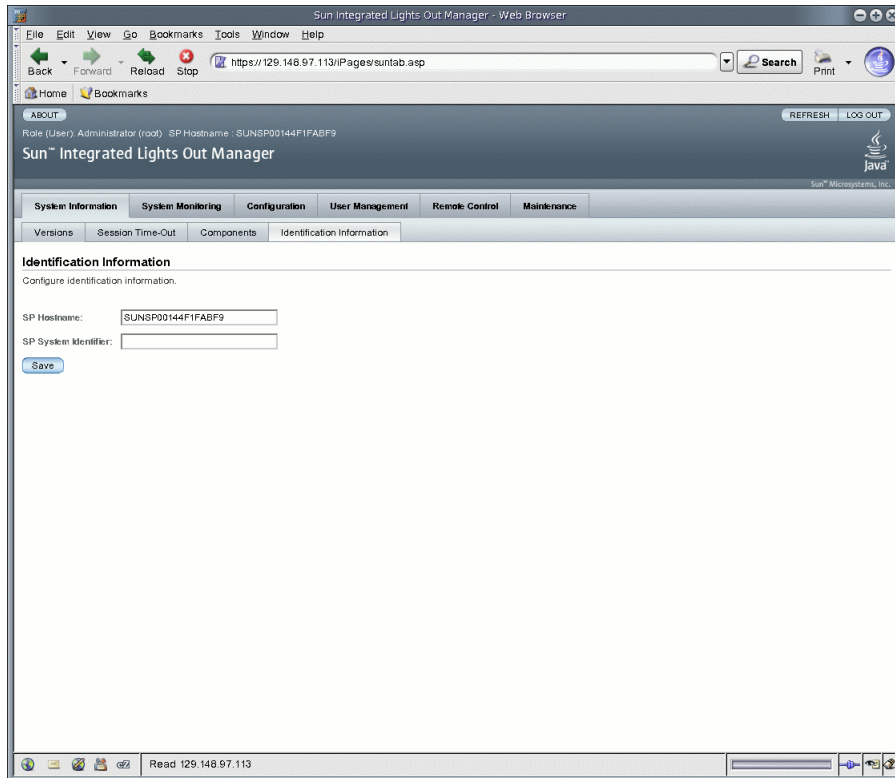
- 2. In the ILOM Login dialog, log in as an Administrator by entering an Administrator user name and password.**

The ILOM interface appears.

- 3. Select System Information --> Identification Information.**

The Identification Information page appears.

**FIGURE 2-3** Identification Information Page



**4. In the SP Hostname field, type the SP hostname.**

The hostname can consist of alphanumeric characters and can include hyphens.

**5. In the SP System Identifier field, type the text that you will use to identify the system.**

The system identifier can consist of a text string using any standard keyboard keys except quotation marks.

**6. Click Save for your settings to take effect.**

## ▼ Assign Hostname and System Identifier Using the CLI

Follow these steps to assign a hostname or system identifier in ILOM using the CLI:

### 1. Establish a local serial console connection or SSH connection to the server SP or CMM:

#### ■ Local Serial Console Connection

Attach a serial console to the serial port on the server or CMM.

For more information, consult the user documentation provided with the Sun server platform.

or

#### ■ Remote - Secure Shell (SSH) Connection

Establish a Secure Shell connection to the server SP or CMM.

From the remote client, establish a secure connection as root to the server SP or CMM. For example, you can establish a secure connection from a remote SSH client to the server SP by typing the following:

```
ssh -l root server_ip_address
```

Password: **changeme**

The default prompt appears (->) and the system is ready for you to run the CLI commands to establish network settings.

### 2. To set the SP hostname and system identifier text, at the command prompt, type:

```
-> set /SP hostname=text_string
```

```
-> set /SP system_identifier=text_string
```

The hostname can consist of alphanumeric characters and can include hyphens. The system identifier can consist of a text string using any standard keyboard keys except quotation marks.



# ILOM Command-Line Interface and Log In

---

The ILOM command-line interface (CLI) enables you to use keyboard commands to configure and manage many ILOM features and functions. Any task that you can perform using the ILOM web interface has an equivalent ILOM CLI command.

This chapter includes the following sections:

- [“CLI Overview” on page 38](#)
- [“CLI Hierarchical Architecture” on page 38](#)
- [“CLI Command Syntax” on page 40](#)
- [“Command Execution” on page 42](#)
  - [“Execute Commands Individually” on page 42](#)
  - [“Execute Combined Commands” on page 43](#)
- [“Connect to ILOM Using the CLI” on page 43](#)
  - [“Log In to ILOM” on page 44](#)
  - [“Log Out of ILOM” on page 44](#)

---

**Note** – Syntax examples in this chapter use the target starting with `/SP/`, which could be interchanged with the target starting with `/CMM/` depending on your Sun server platform. Subtargets are common across all Sun server platforms.

---

---

# CLI Overview

The ILOM command-line interface (CLI) is based on the Distributed Management Task Force specification, *Server Management Command-Line Protocol Specification, version 11.0a.8 Draft* (DMTF CLP). You can view the entire specification at the following site:

<http://www.dmtf.org/>

The DMTF CLP provides a management interface for one or more servers regardless of server state, method of access, or installed operating system.

The DMTF CLP architecture models a hierarchical namespace, a predefined tree that contains every managed object in the system. In this model, a small number of commands operate on a large namespace of targets, which can be modified by options and properties. This namespace defines the targets for each command verb.

---

# CLI Hierarchical Architecture

The following table lists the various hierarchy methods you can use with the ILOM CLI, depending on the particular Sun server platform that you are using.

**TABLE 3-1** ILOM Target Types

Target Type	Description
* /SP	The targets and properties below this target type are used for configuring the ILOM service processor (SP) and for viewing logs and consoles.
* /CMM	On blade platforms, this target type replaces /SP and is used for configuring the ILOM Chassis Monitoring Module (CMM).



**TABLE 3-1** ILOM Target Types (Continued)

Target Type	Description
* /SYS	The targets and properties below this target type provide inventory, environmentals, and hardware management. The targets directly correspond to nomenclature for all hardware components, some of which are printed onto the physical hardware.
* /CH	On blade platforms, this target type replaces /SYS and provides inventory, environmentals, and hardware management at the chassis level. The target types directly correspond to nomenclature names for all hardware components, some of which are printed onto the the physical hardware.
* /HOST	The targets and properties below this target type are used for monitoring and managing the host operating system. This is only available for use with SPARC systems.

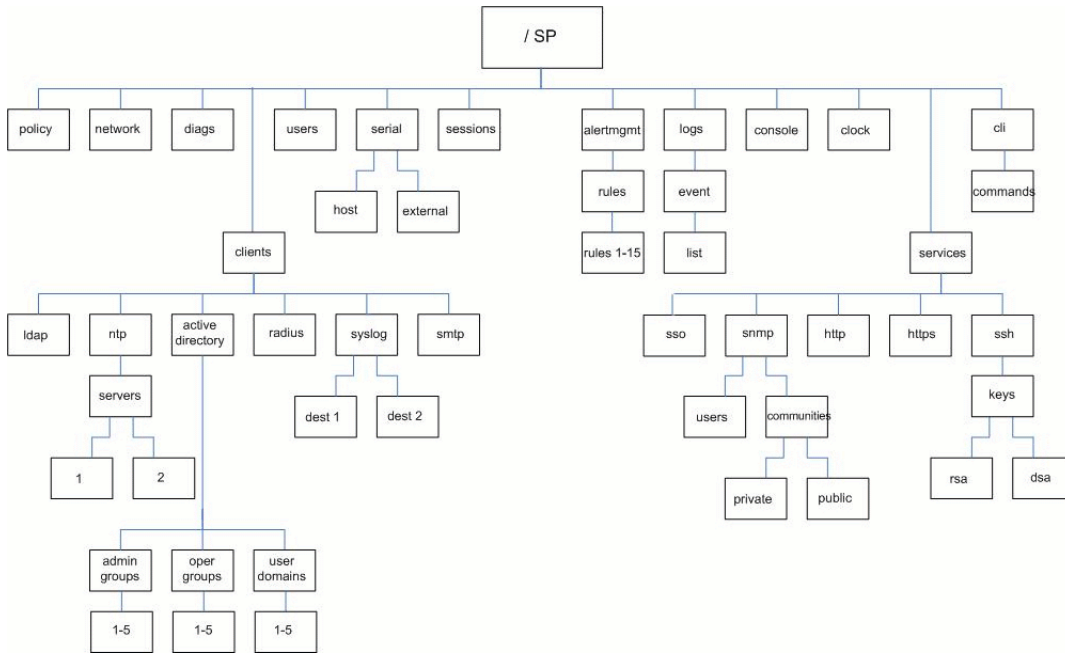
---

**Note** – Your access to some of these subtrees within the hierarchy is dependent on the Sun server platform you are using.

---

Service processors can access two namespaces: the /SP namespace and the overall system namespace /SYS or /HOST for SPARC-based systems. In the /SP namespace, you can manage and configure the service processor. In the /SYS or /HOST namespace you can access other information for managed system hardware.

**FIGURE 3-1** /SP Example of the ILOM CLI Target Tree



For information about user privilege levels, see [“Roles for ILOM User Accounts”](#) on page 6.

---

## CLI Command Syntax

When using the ILOM CLI, information is entered in the following order:

Command syntax: <command> <options> <target> <properties>

The following sections include more information about each part of the syntax.

# CLI Commands

The ILOM CLI supports the DMTF CLP commands listed in the following table. CLI commands are case-sensitive.

**TABLE 3-2** CLI Commands

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 CLI session.
help	Displays Help information for commands and targets.
load	Transfers a file from an indicated source to an indicated target.
reset	Resets the state of the target.
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 service processor running.

# Command Options

The ILOM CLI supports the following options, but note that not every command supports every option. The `help` option can be used with any command.

**TABLE 3-3** CLI Options

Option	Long Form	Short Form	Description
-default			Causes the command to perform its default functions only.
-destination			Specifies the destination for data.
-display		-d	Shows the data the user wants to display.
-force		-f	Specifies that the action will be performed immediately.
-help		-h	Displays Help information.

**TABLE 3-3** CLI Options (*Continued*)

Option	Long Form	Short Form	Description
-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. ILOM only supports <code>-o table</code> , which displays targets and properties in tabular form.
-script			Skips warnings or prompts normally associated with the command.
-source			Indicates the location of a source image.

## Command Targets

Every object in your namespace is a target.

## Command Properties

Properties are the configurable attributes specific to each object.

---

## Command Execution

To execute most commands, specify the location of the target and then enter the command. You can perform these actions individually, or you can combine them on the same command line.

### ▼ Execute Commands Individually

1. **Navigate to the namespace using the `cd` command.**

For example:

```
cd /SP/services/http
```

## 2. Enter the command, target, and value.

For example:

```
set port=80
```

or

```
set prop1=x
```

```
set prop2=y
```

## ▼ Execute Combined Commands

- Using the syntax `<command><target>=value`, enter the command on a single command line.

For example:

```
set /SP/services/http port=80
```

or

```
set /SP/services/http prop1=x prop2=y
```

The following table provides an example and description of the individual and combined command execution methods..

**TABLE 3-4** Executing an Individual Command and a Combined Command

Command Syntax	Command Description
Execute command individually: > <b>cd /SP/services/http</b>	Navigate to the namespace /SP/services/http
> <b>set port=80</b>	Enter the command, target, and value: set "port" to "80"
Execute combined command: > <b>cd /SP/services/http port=80</b>	In the namespace /SP/services/http, set target "port" to "80"

---

## Connect to ILOM Using the CLI

This section describes how to log in to and log out of ILOM. You should first refer to [“Assign IP Addresses to the Sun Server Platform SP Interfaces” on page 23](#) to configure ILOM before logging in to the ILOM CLI.

ILOM supports from 5 to 10 active sessions depending on your platform, including serial, SSH, and web interface sessions. Telnet connections to ILOM are not supported.

## ▼ Log In to ILOM

You can access the ILOM CLI remotely through a Secure Shell (SSH) or serial connection. Secure Shell connections are enabled by default.

The following procedure shows an example using an SSH client on a UNIX system. Use an appropriate SSH client for your operating system. The default user name is `root` and default password is `changeme`.

Follow these steps to log in to ILOM using the default enabled SSH connection:

**1. Type this command to log in to ILOM:**

```
$ ssh root@ipaddress
```

where *ipaddress* is the IP address of the server SP.

**2. Type this password when prompted:**

```
Password: changeme
```

After you log in to ILOM using the default user name and password, you should change the the ILOM root account password (`changeme`). For information about changing the root account password, see [“Change ILOM Root Account Password Using the CLI”](#) on page 63.

## ▼ Log Out of ILOM

Follow this step to log out of ILOM:

● **Type this command to log out of ILOM:**

```
-> exit
```

# ILOM Web Interface and Log In

---

ILOM supports an easy-to-use web interface that runs on many web browsers. You can use this web interface to access all the features and functions provided by ILOM.

This chapter includes the following sections:

- [“Web Interface Overview” on page 45](#)
  - [“Browser and Software Requirements” on page 46](#)
  - [“Web Interface Components” on page 47](#)
  - [“Navigation Tab Components” on page 48](#)
  - [“Connect to ILOM Using the Web Interface” on page 51](#)
    - [“Log In to ILOM” on page 51](#)
    - [“Upload the SSL Certificate” on page 54](#)
    - [“Set the Session Time-Out” on page 55](#)
    - [“Log Out of ILOM” on page 56](#)
- 

## Web Interface Overview

The ILOM web interface is accessible through a browser and uses a Sun standard interface. The ILOM web interface enables you to monitor and manage local and remote systems. One of the most powerful features of ILOM is the ability to redirect the server's graphical console to a local workstation or laptop system. When you redirect the host console, you can configure the local system's keyboard and mouse to act as the server's mouse and keyboard. You can also configure the diskette drive or CD-ROM drive on the remote system as a device virtually connected to your Sun system. You can access these features using the ILOM Remote Console application. For more information about the Remote Console, see [Chapter 12](#). The web interface provides user accounts that have defined roles and privileges. For information about privilege levels, see [“Roles for ILOM User Accounts” on page 6](#).

---

# Browser and Software Requirements

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

You can launch only one instance of the ILOM web interface in a single browser. If you attempt to launch multiple instances of the ILOM web interface in the same browser, only the first instance of the web interface will display.

The following operating systems and web browsers are known to be compatible with ILOM:

- Solaris (9 and 10)
  - Mozilla 1.4 and 1.7
  - Firefox 1.x and above
- Linux (Red Hat, SuSE, Ubuntu)
  - Mozilla 1.x and above
  - Firefox 1.x and above
  - Opera 6.x and above
- Microsoft Windows (98, 2000, XP, Vista)
  - Internet Explorer 5.5, 6.x, 7.x
  - Mozilla 1.x and above
  - Firefox 1.x and above
  - Opera 6.x and above
- Macintosh (OSX v10.1 and above)
  - Internet Explorer 5.2
  - Mozilla 1.x and above
  - Firefox 1.x and above
  - Safari - all

---

**Note** – ILOM comes preinstalled on your Sun system and includes the Remote Console application. To run the ILOM Remote Console, you must have the Java 1.5 runtime environment (JRE 1.5) or later version of the JRE software installed on your local client. To download the JRE software, go to <http://java.com>. For more information about the Remote Console, see [Chapter 12](#).

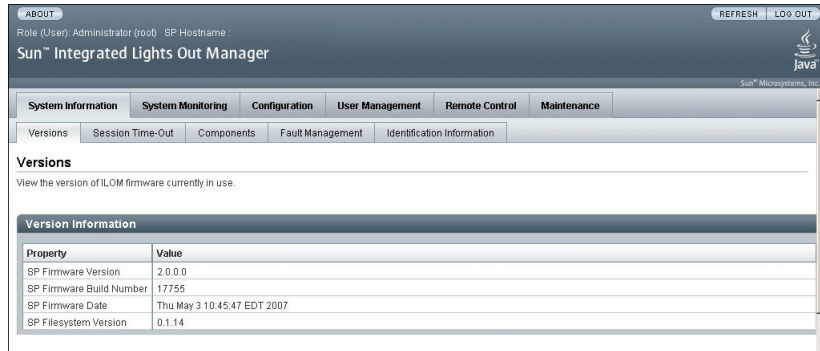
---



# Web Interface Components

The ILOM web interface main page is shown below.

**FIGURE 4-1** ILOM Web Interface Main Page



Each web interface page has three main sections: the masthead, the navigation tabs, and the content area.

---

**Note** – If you are using the ILOM web interface on a Chassis Monitoring Module (CMM), there is another component in the web interface called the Navigation Pane.

---

The masthead provides the following buttons and information on each page of the web interface:

- **About button** – Click to view product and copyright information.
- **User field** – Displays the user name of the current user of the web interface and the user's role.
- **Server field** – Displays the host name of the ILOM SP or CMM.
- **Refresh button** – Click to refresh the information in the content area of the page. The Refresh button does not save new data that you may have entered or selected on the page.
- **Log Out button** – Click to end the current session of the web interface.

---

**Note** – Do not use the Refresh button on your web browser when you are using the web interface.

---

The ILOM web interface navigation structure includes tabs and second-level tabs that you can click to open a specific page. When you click the main tab, second-level tabs are displayed, providing you with further options. For additional information, see [“Navigation Tab Components” on page 48](#).

The content area is where you find information about the specific topic or operation.

## Navigation Tab Components

The following table describes the various tabs and sub-tabs within the most common ILOM components in the web interface. In the cross-referenced sections in this User’s Guide, you can find more detail about how to use the features and functions on the web pages that appear when you select a tab.

---

**Note** – The ILOM web interface navigation tabs differ slightly depending on the features implemented on a specific platform. Therefore, you may have access to different tabs than those described in the following table. Refer to your ILOM Supplement for your specific platform for information about the ILOM interface for your system.

---

**TABLE 4-1** ILOM Web Interface Tabs

Main Tab	Sub-Tabs	What You Can Do	For More Information in This User’s Guide
<b>System Information</b>			
	Versions	View the version of ILOM that is running	<a href="#">“View ILOM Version Information Using the Web Interface” on page 216</a>
	Session Time-Out	Set the amount of idle time that the ILOM session will remain active	<a href="#">“Set the Session Time-Out” on page 55</a>
	Components	View the names, types, and status of the components that ILOM is monitoring	<a href="#">“View Component Information Using the Web Interface” on page 117</a>
	Identification Information	Enter or change the SP identification information	<a href="#">“Assign Hostname and System Identifier Using the Web Interface” on page 33</a>
<b>System Monitoring</b>			
	Sensor Readings	View the name, type, and reading of the sensors	<a href="#">“Sensor Readings” on page 127</a>

**TABLE 4-1** ILOM Web Interface Tabs (Continued)

Main Tab	Sub-Tabs	What You Can Do	For More Information in This User's Guide
	Indicators	View the name and status of the indicators and LEDs	<a href="#">"System Indicators" on page 132</a>
	Event Logs	View various details about each particular event, including the event ID, class, type, severity, date and time, and description of the event	<a href="#">"ILOM Event Log" on page 136</a>
<b>Configuration</b>			
	System Management Access --> Web Server	Edit or update the web server settings, such as the HTTP web server or the HTTP port	<a href="#">"Enable HTTP or HTTPS Web Access Using the Web Interface" on page 187</a>
	System Management Access --> SNMP	Edit or update SNMP settings	<a href="#">"Configure SNMP Settings Using the Web Interface" on page 204</a>
	System Management Access --> SSL Certificate	View information about the default SSL certificate or find and enter a new SSL certificate	<a href="#">"Upload the SSL Certificate" on page 54</a>
	System Management Access --> SSH Server	Configure Secure Shell (SSH) server access and key generation	<a href="#">"Enable or Disable SSH Using the Web Interface" on page 181</a>
	Alert Management	View details about each alert and change the list of configured alerts	<a href="#">"Manage Alert Rule Configurations Using the ILOM Web Interface" on page 161</a>
	Network	View and edit the network settings for ILOM	<a href="#">"View Network Settings Using the Web Interface" on page 184</a>
	Serial Port	View and edit the baud rate of the internal and external serial ports	<a href="#">"Display Serial Port Settings Using the Web Interface" on page 186</a>
	Clock Settings	View and edit the time and NTP settings	<a href="#">"Event Log Timestamps and ILOM Clock Settings" on page 136</a>
	Syslog	Configure the server addresses to which the syslog messages will be sent	<a href="#">"Configure Remote Syslog Receiver IP Addresses Using the Web Interface" on page 153</a>
	SMTP Client	Configure the state of the SMTP client, which is used for sending email notifications of alerts	<a href="#">"Enable SMTP Client Using the Web Interface" on page 170</a>
	Policy	Enable or disable settings that control the behavior of the system, such as power-on policies	<a href="#">"Configure Policy Settings" on page 122</a>

**TABLE 4-1** ILOM Web Interface Tabs (Continued)

<b>Main Tab</b>	<b>Sub-Tabs</b>	<b>What You Can Do</b>	<b>For More Information in This User's Guide</b>
<b>User Management</b>			
	User Accounts	Add, delete, or modify local ILOM user accounts	<a href="#">"Add User Accounts and Set Privileges Using the Web Interface" on page 68</a>
	Active Sessions	View the users currently logged in to ILOM, as well as the type of session users have initiated	<a href="#">"View User Sessions Using the Web Interface" on page 75</a>
	LDAP	Configure ILOM access for LDAP users	<a href="#">"Configure ILOM for LDAP Using the Web Interface" on page 106</a>
	RADIUS	Configure ILOM access for RADIUS users	<a href="#">"Configure RADIUS Using the Web Interface" on page 110</a>
	Active Directory	Configure Active Directory settings	<a href="#">"Configure Active Directory Settings" on page 84</a>
<b>Remote Control</b>			
	Redirection	Manage the host remotely by redirecting the system console to your local machine	<a href="#">"Configure ILOM Remote Control Settings Using the Web Interface" on page 229</a>
	Remote Power Control	Control the system power	<a href="#">"Configure ILOM Remote Control Settings Using the Web Interface" on page 229</a>
	Mouse Mode Settings	Select a mode for your local mouse to use while managing the host remotely	<a href="#">"Configure ILOM Remote Control Settings Using the Web Interface" on page 229</a>
<b>Maintenance</b>			
	Firmware Upgrade	Start the process to obtain an upgrade of the ILOM firmware	<a href="#">"Update ILOM Firmware Using the Web Interface" on page 219</a>
	Reset SP	Start the process to reset the service processor (SP)	<a href="#">"Reset ILOM SP" on page 221</a>
	Configuration Management	Manage the SP configuration	<a href="#">"Reset SP to Factory Defaults Using the Web Interface" on page 222</a>
	Data Collector	Use the Snapshot utility to collect environmental, log, error, and FRUID data and send it to a USB thumbdrive, and external host using the CLI, or as a downloaded file	<a href="#">"Run the Snapshot Utility Using the Web Interface" on page 156</a>

---

# Connect to ILOM Using the Web Interface

This section describes how to log in to and log out of the web interface, as well as how to upload an SSL certificate and set the session time-out.

## ▼ Log In to ILOM

This section describes how to log in to the ILOM web interface.

---

**Note** – ILOM boots automatically when a Sun system is connected to an AC power supply or when a server module is inserted into a powered chassis. If the management Ethernet is not connected, or if ILOM's Dynamic Host Configuration Protocol (DHCP) process fails due to the absence of a DHCP server on the management network, ILOM might take longer to start.

---

Disabling the use of the browser proxy server (if used) for access to the management network can make the web interface response time faster.

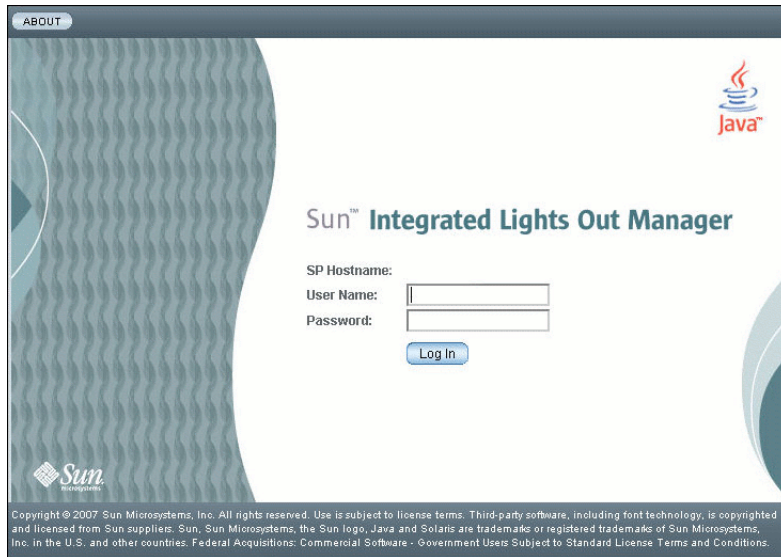
You need the IP address of ILOM. For information on viewing and setting the IP address, see [“Assign IP Addresses to the Sun Server Platform SP Interfaces” on page 23](#).

Follow these steps to log in to the ILOM web interface:

- 1. To log in to the web interface, type the IP address of ILOM into your web browser.**

The web interface Login page appears.

**FIGURE 4-2** Login Page



## 2. Type your user name and password.

You can use the default user name and password.

- Default user name – `root`
- Default password – `changeme`

The default user name and password are lowercase characters.

One local user ID is predefined with the user name `root` assigned with the role Administrator. You cannot delete this user ID or change its role attributes. The initial password `changeme` is also provided. This password is required to log in to the command-line interface (CLI), Secure Shell (SSH), and the web interface.

## 3. Click Log In.

The web interface Versions page appears.

**FIGURE 4-3** Versions Page



After you have logged in to ILOM and established network connectivity to the system, you should reset the default password (changeme) that is associated with the ILOM root account to protect your system from unauthorized access. For information about resetting the ILOM root account password, see [“Change ILOM Root Account Password Using the Web Interface”](#) on page 60.

## ▼ Upload the SSL Certificate

ILOM provides a default SSL certificate and self-signed key for HTTPS access.

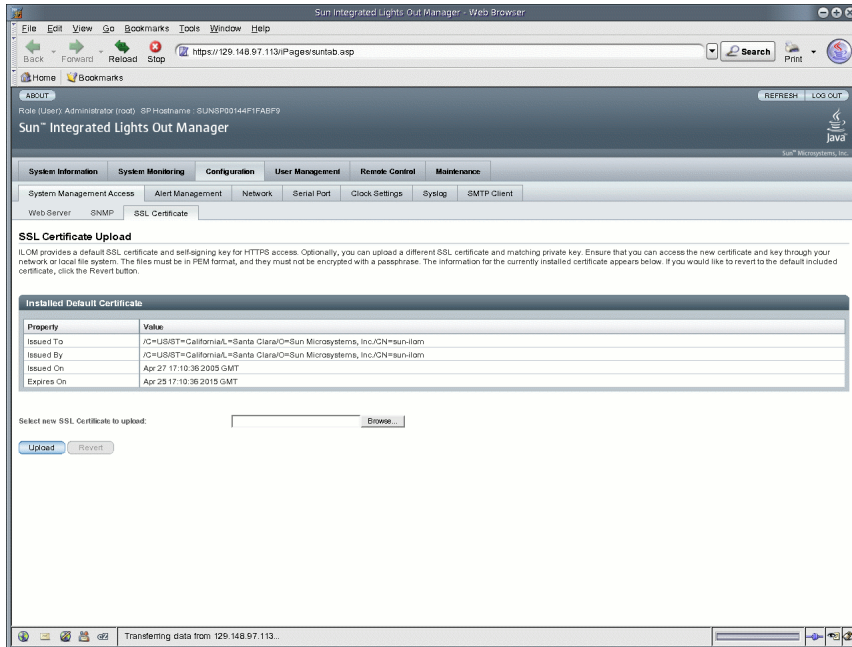
Optionally, you can upload a different SSL certificate and matching private key. Ensure that you can access the new certificate and key through your network or local file system.

Follow these steps to upload the SSL certificate:

1. **Log in to ILOM.**
2. **Select Configuration --> System Management Access --> SSL Certificate.**

The SSL Certificate Upload page appears.

**FIGURE 4-4** SSL Certificate Upload Page



3. **Type the file name of the new SSL certificate or click the Browse button to search for a new SSL certificate.**

The file name has a `.pem` file extension. The service processor does not support pass-phrase encrypted certificates.



4. **Click the Upload button to obtain the selected SSL certificate.**

The SSL Certificate Upload Status dialog box appears.

5. **Once you have uploaded the certificate and private key, click the OK button to reset the ILOM web server and begin using the new SSL certificate.**

The ILOM web server must be reset for the new certificate to take effect.

## ▼ Set the Session Time-Out

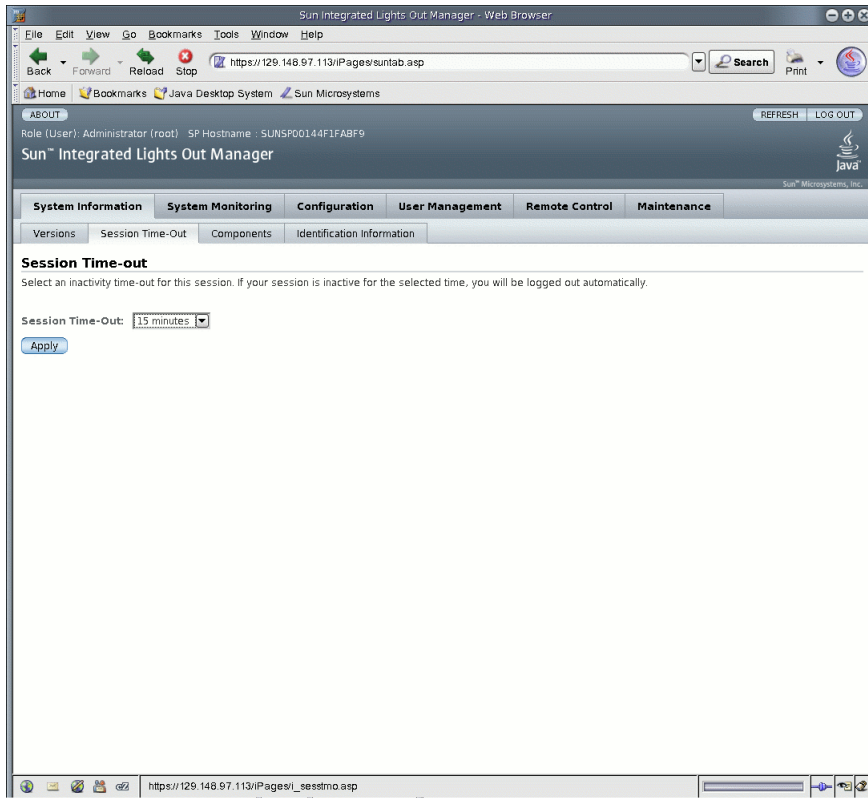
The session time-out setting does not persist after you log out of the current ILOM session. You must reset the session time-out each time you log in to the ILOM web interface.

Follow these steps to set the amount of time an ILOM session will remain idle before logging out:

1. **Log in to ILOM.**
2. **Select System Information --> Session Time-Out.**

The Session Time-Out Page appears.

**FIGURE 4-5** Session Time-Out Page



3. From the Session Time-Out drop-down list, select the amount of time that the ILOM session will remain idle when there is no ILOM activity.  
If your session is inactive for the selected amount of time, you will be logged out of ILOM automatically.

## ▼ Log Out of ILOM

- To log out of the web interface, click the Log Out button.  
The Log Out button is located in the top right corner of the web interface.

## Manage User Accounts

---

ILOM supports up to 10 user accounts. One of these accounts is the preconfigured Administrator account, which provides read and write access to all ILOM features, functions, and commands. Using the ILOM web interface or command-line interface (CLI) you can add, modify, or delete user accounts.

This chapter includes the following sections:

- [“Guidelines for Managing User Accounts” on page 59](#)
- [“User Account Roles and Privileges” on page 59](#)
- [“Preconfigured ILOM Administrator Accounts” on page 60](#)
  - [“Change ILOM Root Account Password Using the Web Interface” on page 60](#)
  - [“Change ILOM Root Account Password Using the CLI” on page 63](#)
- [“Single Sign On” on page 63](#)
  - [“Enable or Disable Single Sign On Using the CLI” on page 63](#)
  - [“Enable or Disable Single Sign On Using the Web Interface” on page 64](#)
- [“Manage User Accounts Using the CLI” on page 64](#)
  - [“Add a User Account Using the CLI” on page 65](#)
  - [“Modify a User Account Using the CLI” on page 65](#)
  - [“Delete a User Account Using the CLI” on page 65](#)
  - [“View a List of User Accounts Using the CLI” on page 65](#)
  - [“View Individual User Account Using the CLI” on page 66](#)
  - [“Configure a User Account Using the CLI” on page 66](#)
  - [“View a List of User Sessions Using the CLI” on page 67](#)
  - [“View an Individual User Session Using the CLI” on page 67](#)
- [“Manage User Accounts Using the Web Interface” on page 68](#)
  - [“Add User Accounts and Set Privileges Using the Web Interface” on page 68](#)
  - [“Modify a User Account Using the Web Interface” on page 71](#)

- “Delete a User Account Using the Web Interface” on page 74
- “View User Sessions Using the Web Interface” on page 75
- “Active Directory” on page 76
  - “User Authentication and Authorization” on page 76
  - “Determining User Authorization Levels” on page 77
  - “Typical Uses of Active Directory” on page 77
  - “Active Directory Web Interface” on page 78
  - “Active Directory Configuration Properties” on page 79
  - “Active Directory Tables” on page 81
  - “Diagnosing Authentication and Authorization Events” on page 97
  - “Set Certificate Validation Using the CLI” on page 98
  - “Set Certificate Validation Using the Web Interface” on page 100
- “Lightweight Directory Access Protocol” on page 102
  - “Configure the LDAP Server” on page 105
  - “Configure ILOM for LDAP Using the CLI” on page 105
  - “Configure ILOM for LDAP Using the Web Interface” on page 106
- “RADIUS Authentication” on page 108
  - “RADIUS Clients and Servers” on page 108
  - “RADIUS Parameters” on page 109
  - “Configure RADIUS Using the CLI” on page 110
  - “Configure RADIUS Using the Web Interface” on page 110
  - “RADIUS Commands” on page 111

---

**Note** – Syntax examples in this chapter use the target starting with `/SP/`, which could be interchanged with the target starting with `/CMM/` depending on your Sun server platform. Subtargets are common across all Sun server platforms.

---

---

# Guidelines for Managing User Accounts

Apply the following general guidelines when you manage user accounts:

- ILOM supports a maximum of 10 user accounts, one of which is the preconfigured Administrator account. The preconfigured Administrator account cannot be deleted. If all 10 user accounts are configured, you must delete an existing user account before you can add a new user account.
- Only accounts with Administrator privileges are allowed to add, modify, or delete user accounts. However, a user with Operator privileges can modify his or her own password.
- The user name of an account must be at least four characters and no more than 16 characters. User names are case sensitive and must start with an alphabetical character. You can use alphabetical characters, numerals, hyphens, and underscores. Do not include spaces in user names.
- You can either configure local accounts or you can have ILOM authenticate accounts against a remote user database, such as Active Directory, LDAP, or RADIUS. With remote authentication, you can use a centralized user database rather than configuring local accounts on each ILOM instance. In addition, remote authentication lets you change a user's password on the server once.

---

## User Account Roles and Privileges

User accounts have two defined roles. Each role grants certain privileges to the ILOM user. User roles and privileges include:

- **Administrator** – Enables access to all ILOM features, functions, and commands.
- **Operator** – Enables limited access to ILOM features, functions, and commands. In general, Operators cannot change configuration settings.

---

# Preconfigured ILOM Administrator Accounts

Preconfigured ILOM Administrator accounts, also known as fixed user accounts, include:

**User name:** `root`

**Password:** `changeme`

The user name, `root`, cannot be deleted or changed, other than resetting its password (`changeme`). This account offers built-in administrative privileges (read and write access) to all ILOM features, functions, and commands.

The first time you access ILOM, at the SP level or CMM level, you will need to log in as `root` with the default password `changeme`. After you have logged in to ILOM and established network connectivity to the system, you should consider resetting the password (`changeme`) associated with the ILOM `root` account to protect your system from unauthorized access. If you are using a blade server system, reset this password on each CMM and blade installed in the system chassis. For more information about resetting the ILOM `root` account password, see [“Change ILOM Root Account Password Using the Web Interface” on page 60](#).

## ▼ Change ILOM Root Account Password Using the Web Interface

Follow these steps to change the password for the `root` account:

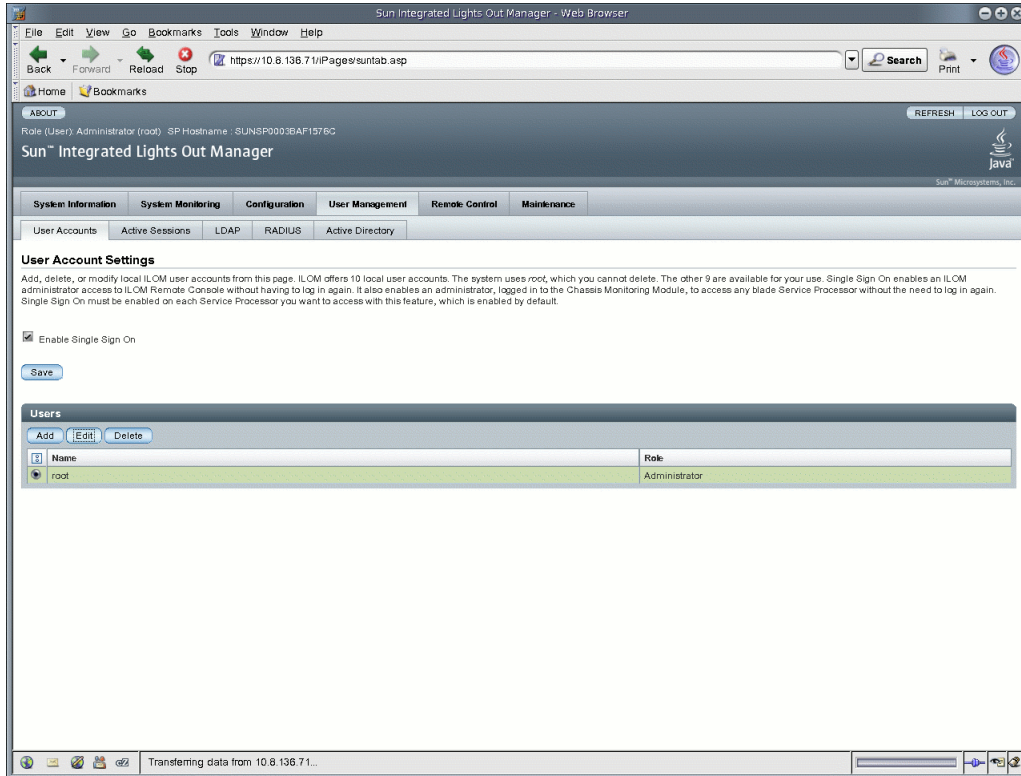
- 1. Open a web browser and type the IP address of a server SP or CMM.**  
The Login page for the ILOM web interface appears.
- 2. In the ILOM Login page, do the following:**
  - a. Type the default user name (`root`) and password (`changeme`).**
  - b. Click Log In.**  
The ILOM web interface appears.
- 3. In the ILOM web interface, do the following:**
  - To change the preconfigured Administrator password click the device in the left navigation pane, then proceed to Step 4.

- To change the preconfigured Administrator password at the blade SP level, click the appropriate blade in the left navigation pane, then proceed to Step 4.

**4. In the ILOM web interface, click User Management --> User Accounts.**

The User Account Settings page appears.

**FIGURE 5-1** User Account Settings Page



- 5. In the User Account Settings page, select the radio button next to root then click Edit.**

A security message appears.

6. Click OK to continue. The User Account Password dialog appears.

**FIGURE 5-2** User Account Password Dialog

https://129.148.97.113 - Web Browser

Sun™ Integrated Lights Out Manager

The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space.

User Name: root  
 Change

New Password:

Confirm New Password:

Role: Administrator ▼

Save Close

Done

7. In the User Account password dialog, do the following:

- a. Select the box next to Change.
- b. In the New Password text box, type the new password.
- c. In the Confirm Password text box, type the new password again.
- d. Click Save.

The new password identified in Step 6b and Step 6c is activated for the root Administrator account.

8. If necessary, repeat Step 2 through Step 6d to change the password for each installed device.



## ▼ Change ILOM Root Account Password Using the CLI

- Type the following command to change the ILOM root account password:

```
-> set /SP/users/root password=password
```

For example:

```
-> set /SP/users/root password=password
Changing password for user /SP/users/root...
Enter new password again: *****
New password was successfully set for user /SP/users/root
```

---

## Single Sign On

---

**Note** – The Single Sign On service is supported on x64-based systems and SPARC-based server modules (blades) running ILOM 2.x. Single Sign On is not supported on SPARC-based rackmount servers running ILOM 2.x.

---

Single Sign On is a convenient authentication service that reduces the number of times you need to enter a password to gain access to ILOM. Single Sign On is enabled by default. As with any authentication service, authentication credentials are passed over the network. If this is not desirable, consider disabling the Single Sign On authentication service.

## ▼ Enable or Disable Single Sign On Using the CLI

Only Administrators can disable or enable Single Sign On.

- Type the following command to enable or disable single sign on:

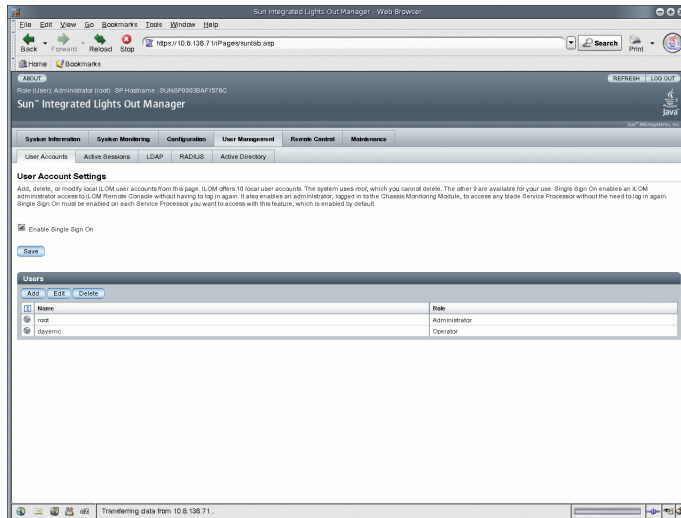
```
-> set /SP/services/sso state=disabled|enabled
```

## ▼ Enable or Disable Single Sign On Using the Web Interface

Follow these steps to enable or disable Single Sign On:

1. **Log in to the ILOM web interface as Administrator.**
2. **Select User Management --> User Accounts.**  
The User Account Settings page is displayed.
3. **Click the check box next to Enable Single Sign On to enable the feature, or deselect the check box to disable the feature.**

**FIGURE 5-3** User Account Settings Page With Single Sign On Enabled



## Manage User Accounts Using the CLI

This section describes how to manage user accounts using the ILOM command-line interface (CLI).

## ▼ Add a User Account Using the CLI

- Type the following command to add a local user account:

```
-> create /SP/users/username password=password role=administrator|operator
```

For example:

```
-> create /SP/users/davemc  
Creating user...  
Enter new password: *****  
Enter new password again: *****  
Created /SP/users/davemc
```

## ▼ Modify a User Account Using the CLI

- Type the following command to modify a local user account:

```
-> set /SP/users/username password=password role=administrator|operator
```

## ▼ Delete a User Account Using the CLI

1. Type the following command to delete a local user account:

```
-> delete /SP/users/username
```

For example:

```
Are you sure you want to delete /SP/users/davemc (y/n)?
```

2. Type **y** to delete, or **n** to cancel.

## ▼ View a List of User Accounts Using the CLI

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

```
-> show -display targets /SP/users
```

For example:

```
-> show -display targets /SP/users  
/SP/users  
Targets:  
    root  
    davemc
```

## ▼ View Individual User Account Using the CLI

- Type the following command to display information about one specific user account:

```
-> show /SP/users/username
```

For example:

```
-> show /SP/users/davemc
/SP/users/davemc
Targets:
Properties:
    role = Operator
    password = *****
Commands:
    cd
    set
    show
```

## ▼ Configure a User Account Using the CLI

Use the `set` command to change targets, properties, passwords, and values for configured user accounts.

- Type the following command to configure a local user account:

```
-> set <target> [<property>=value]
```

### Targets, Properties, and Values

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

**TABLE 5-1** Valid Targets, Properties, and Values for Local User Accounts

Target	Property	Value	Password	Default
/SP/users/username	role	administrator   operator		operator
	password	<string>		

For example, to change the role for `user1` from Administrator to Operator type:

```
-> set /SP/users/user1 role=operator
```

To change the password for user1, type:

```
-> set /SP/users/user1 password
Changing password for user /SP/users/user1/password...
Enter new password:*****
Enter new password again:*****
New password was successfully set for user /SP/users/user1
```

---

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

---

## ▼ View a List of User Sessions Using the CLI

- Type the following command to display information about all local user sessions:

```
-> show /SP/sessions
```

For example:

```
-> show /SP/sessions
/SP/sessions
  Targets:
    108
  Properties:
  Commands:
    cd
    show
```

## ▼ View an Individual User Session Using the CLI

- Type the following command to display information about an individual user session:

```
-> show /SP/sessions/108
```

For example:

```
-> show /SP/sessions/108
/SP/sessions/108
  Targets:
  Properties:
    username = root
    starttime = Tue Jun  5 10:04:05 2007
    type = shell
```

```
Commands :
  cd
  show
```

---

## Manage User Accounts Using the Web Interface

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

### ▼ Add User Accounts and Set Privileges Using the Web Interface

**1. Log in to the ILOM web interface as a user with Administrator privileges.**

Only accounts with Administrator privileges are allowed to add, modify, or delete user accounts. However, Operators can modify their own password.

If a new user is given Administrator privileges, those privileges are also automatically granted for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to ILOM.

**2. Select User Management --> User Accounts.**

The User Account Settings page appears.

**3. In the Users table, click Add.**

The Add User dialog appears.

**FIGURE 5-4** Add User Dialog

https://129.148.97.113 - Web Browser

### Sun™ Integrated Lights Out Manager

The user name must be 4 to 16 characters and must start with an alphabetic character and use no spaces. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space.

User Name:

Password:

Confirm Password:

Role:

Save Close

**4. Complete the following information:**

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

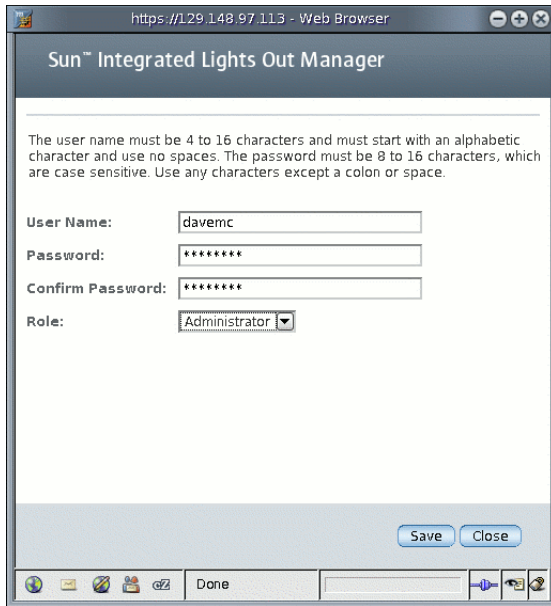
**b. Type a password in the Password field.**

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

**c. Retype the password in the Confirm Password field to confirm the password.**

**d. From the Role drop-down list, select Administrator or Operator.**

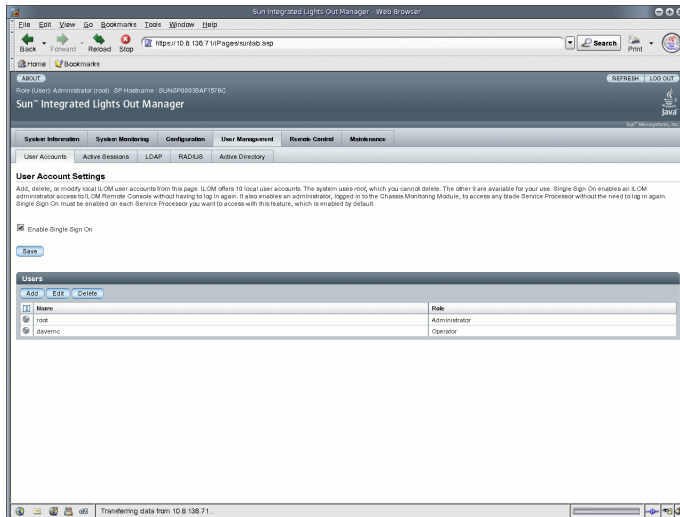
**FIGURE 5-5** Add User Dialog With Populated Fields



e. When you are done entering the new user's information, click Save.

The User Account Settings page is redisplayed. The new user account and associated information is listed on the User Account Settings page.

**FIGURE 5-6** User Account Settings Page Showing New User





## ▼ Modify a User Account Using the Web Interface

This section describes how to modify an ILOM user account. Modifying a user account can change the user's password, and their network and serial privileges.

---

**Note** – Only accounts with Administrator privileges are allowed to add, modify, or delete user accounts. However, Operators can modify their own password.

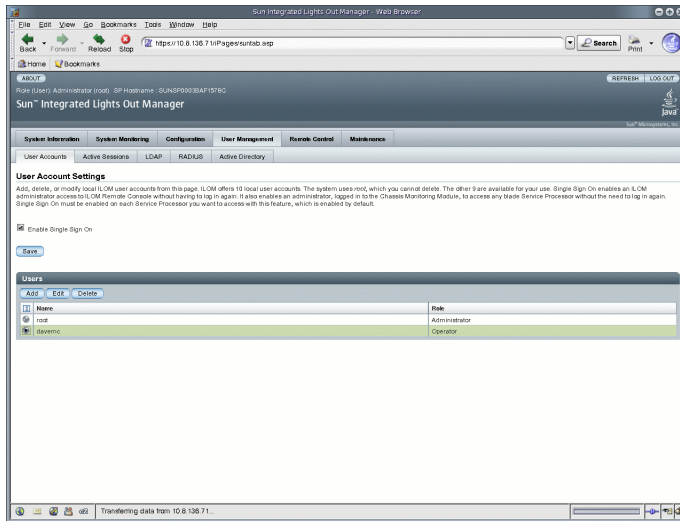
---

If a new user is given Administrator privileges, those privileges are also automatically granted to the user for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to ILOM.

1. **Log in to ILOM as an Administrator to open the web interface.**
2. **Select User Management --> User Accounts.**

The User Account Settings page appears.

**FIGURE 5-7** User Account Settings Page



**3. In the Users table, select a radio button next to the user account you want to modify.**

**4. Click Edit.**

The Edit User dialog appears.

**FIGURE 5-8** Edit User Dialog

https://129.148.97.113 - Web Browser

### Sun™ Integrated Lights Out Manager

The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space.

User Name: davenc

Change

New Password:

Confirm New Password:

Role: Administrator ▼

Save Close

**5. Modify the password if needed.**

**a. Select the Change check box if you want to change the user password. If you do not want to change the password, deselect the check box.**

**b. Type a new password in the New Password field.**

The password must be between 8 and 16 characters. The password is case-sensitive. Use alphabetical, numeric, and special characters for better security. You can use any character except a colon. Do not include spaces in passwords.

**c. Retype the password in the Confirm New Password field to confirm the password.**

**6. From the Role drop-down list, select Administrator or Operator.**

**7. After you have modified the account information, click Save for your changes to take effect, or click Close to return to the previous settings.**

The User Account Settings page is redisplayed.

## ▼ Delete a User Account Using the Web Interface

1. Log in to iLOM as an Administrator to open the web interface.

2. Select User Management --> User Accounts.

The User Account Settings page appears.

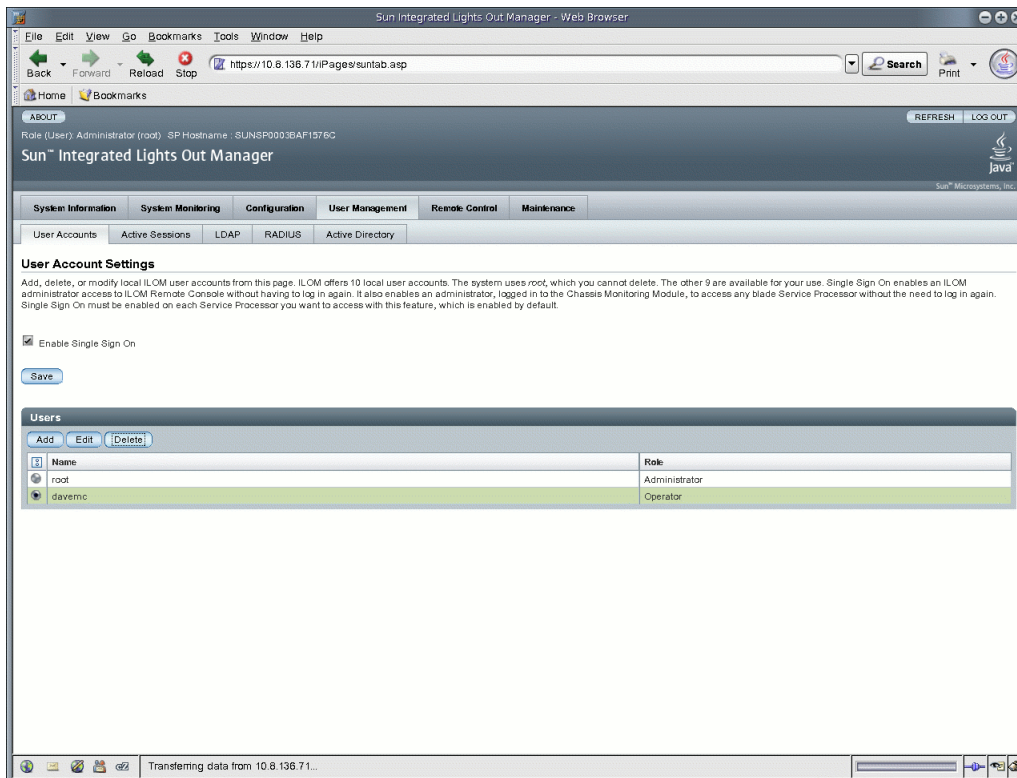
3. Select the radio button next to the user account you want to delete.

---

**Note** – You cannot delete the root account.

---

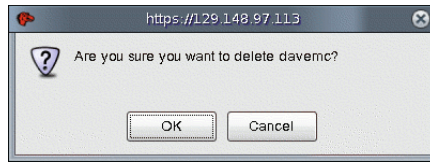
**FIGURE 5-9** User Account Settings Page



4. In the Users table, click Delete.

The confirmation dialog opens.

**FIGURE 5-10** Delete User Configuration Dialog



5. Click **OK** to delete the account or click **Cancel** to stop the process.

The User Account Settings page opens with the user account you deleted no longer listed.

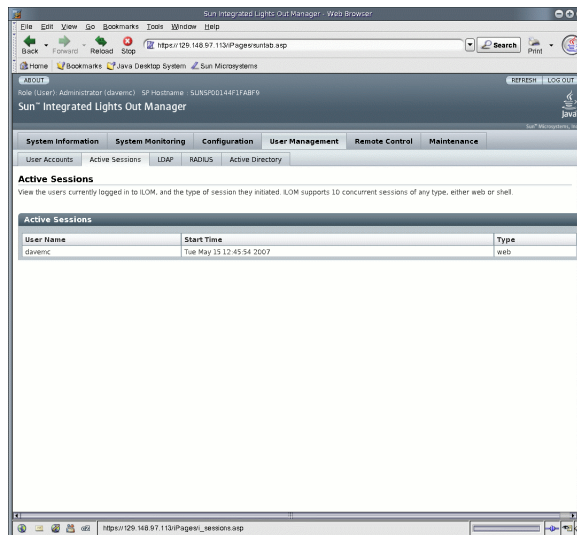
## ▼ View User Sessions Using the Web Interface

1. Log in to the ILOM web interface.

2. Select **User Management --> Active Sessions**.

The Active Sessions page appears. You can find the user name, the date and time that the user initiated the session, and the types of session of the users currently logged in to ILOM.

**FIGURE 5-11** Active Sessions Page



---

# Active Directory

ILOM supports Active Directory, the distributed directory service included with Microsoft Windows Server 2003 and Microsoft Windows 2000 Server operating systems. Like an LDAP directory service implementation, Active Directory is used to authenticate user credentials. Using Active Directory, network administrators also can securely add, modify, and delete policies and software across an organization. In addition, Active Directory uses a centralized directory service database system, called a directory store, which enables administrators to locate information about users, devices, and resources on the network.

## User Authentication and Authorization

Active Directory provides both authentication of user credentials and authorization of user access levels to networked resources. Active Directory uses authentication to verify the identity of a user, a device, or other entity in a computer system, before that entity can access system resources. Active Directory uses authorization to grant specific access privileges to a user in order to control a user's rights to access networked resources. User access levels are configured or learned from the server based on the user's group membership in a network domain, which is a group of hosts identified by a specific Internet name. A user can belong to more than one domain. Active Directory authenticates users in the order in which the user's domains were configured.

# Determining User Authorization Levels

Once authenticated, the user's authorization level can be determined in the following ways.

- In the simplest case, the user authorization of either Operator or Administrator is learned directly through the Active Directory's configuration of the SP. Access and authorization levels are dictated by the `defaultRole` property. Setting up users in the Active Directory database requires only a password with no regard to group membership. On the SP, the `defaultRole` will be set to either `administrator` or `operator`. All users authenticated through Active Directory are assigned the privileges associated with the Administrator or Operator user based solely on this configuration.
- A more integrated approach is also available by querying the server. For configuration, the SP Administrative Group Tables and Operator Group Tables (see ["Active Directory Tables" on page 81](#)) must be configured with the corresponding group names from the Active Directory server that will be used to determine access levels. Up to five Active Directory groups can be entered to designate an Administrator and another five can be used to assign Operator privileges. Group membership of the user is used to identify the proper access level of either Administrator or Operator by looking up each group name in the configured Active Directory tables on the SP. If the user's group list is not in either of the defined SP user groups, then access is denied.

## Typical Uses of Active Directory

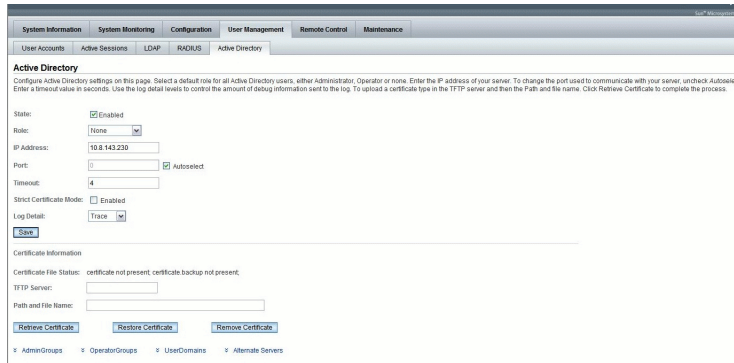
Active Directory is typically used for one of three purposes:

- **Internal directory** – Internal directories are used within the corporate network for publishing information about users and resources within the enterprise.
- **External directory** – External directories typically are located on servers in the perimeter network at the boundary between the corporate local area network (LAN) and the public Internet.
- **Application directory** – Application directories store "private" directory data that is relevant only to the application in a local directory, perhaps on the same server as the application, without requiring any additional configuration to Active Directory.

# Active Directory Web Interface

To configure Active Directory, you need to enter basic data (such as primary server, port number, and certificate mode) and optional data (such as alternate server or event or severity levels). You can enter this data using the Active Directory configuration page of the ILOM web interface or the CLI. [FIGURE 5-12](#) shows a sample display of the Active Directory web interface.

**FIGURE 5-12** Active Directory Web Interface



The screenshot shows the 'Active Directory' configuration page within the ILOM web interface. The page has a navigation bar at the top with tabs for 'System Information', 'System Monitoring', 'Configuration', 'User Management', 'Remote Control', and 'Maintenance'. Under 'Configuration', there are sub-tabs for 'User Accounts', 'Active Sessions', 'LDAP', 'RADIUS', and 'Active Directory'. The 'Active Directory' tab is selected. The main content area is titled 'Active Directory' and contains the following fields and controls:

- State:** A checkbox labeled 'Enabled' is checked.
- Role:** A dropdown menu with 'None' selected.
- IP Address:** A text input field containing '10.8.143.230'.
- Port:** A text input field containing '0', with a checked checkbox labeled 'Autoselect'.
- Timeout:** A text input field containing '4'.
- Strict Certificate Mode:** A checkbox labeled 'Enabled' is unchecked.
- Log Detail:** A dropdown menu with 'Trace' selected.
- Save:** A blue button.

Below the configuration fields is a section titled 'Certificate Information' with the following details:

- Certificate File Status:** 'certificate not present; certificate backup not present.'
- TFTP Server:** An empty text input field.
- Path and File Name:** An empty text input field.
- Buttons:** Three blue buttons labeled 'Retrieve Certificate', 'Restore Certificate', and 'Remove Certificate'.

At the bottom of the page, there are four expandable sections: 'Admin Groups', 'Operator Groups', 'User Objects', and 'Alternate Servers'.

There are four tables at the bottom of the Active Directory page (see [FIGURE 5-13](#)) that represent the following configuration options:

- User Domains
- Administrator Groups
- Operator Groups
- Alternate Servers

See the section, “[Active Directory Tables](#)” on [page 81](#) for more information.



# Active Directory Configuration Properties

TABLE 5-2 describes the settings you must configure to use the Active Directory.

**TABLE 5-2** Active Directory Configuration Settings (Global Variables)

Property (Web)	Property (CLI)	Default	Description
State	state	Enabled	Enabled   Disabled
Role	defaultRole	None	None   Administrator   Operator Access role granted to all authenticated users for the simple configuration case. By default, this access role is not configured so that the more integrated approach is enabled by default. Access level is obtained from the Active Directory server.
IP Address	ipaddress		IP address of the Active Directory server.
Port	port		Port used to communicate with the server or enter autoselect. Indicates use of the standard port (port=0) for transactions. Available in the unlikely event of a non-standard TCP port being used.
Timeout	timeout	4	Timeout value in seconds. Number of seconds to wait for individual transactions to complete. The value does not represent the total time of all transactions because the number of transactions can differ depending on the configuration. This property allows for tuning the time to wait when a server is not responding or is unreachable.
Strict Certificate Mode	strictcertmode	Enabled	Enabled   Disabled If enabled, the server certificate contents are verified by digital signatures.
Log Detail	logdetail	(none)	Specifies the amount of diagnostics that go into the event log. Entries include none, high, medium, low, and trace.

**TABLE 5-2** Active Directory Configuration Settings (Global Variables) (*Continued*)

Property (Web)	Property (CLI)	Default	Description
NA	getcertfile	(none)	Method used to upload a certificate file if needed.
TFTP Server	NA	(none)	The TFTP server used to retrieve the certificate file.
Path and File Name	NA	(none)	The full path name and file name of the certificate file on the server.
Save/Retrieve Certificate	NA	(none)	Retrieves the certificate specified from the TFTP server.
Restore Certificate	NA	(none)	Used when a certificate file has been uploaded over an existing certificate file. The existing file is stored as a backup copy. The restore process takes the backup copy and makes it the current copy.
Remove Certificate	NA	(none)	Used to remove the existing certificate. The remove process cannot remove a certificate if Strict Certificate Mode is enabled.

NA = Not Applicable

**Note** – Certificate File Status is not a configurable parameter.

## Naming Conventions for Active Directory Group Information

Active Directory configured group information supports the standard Distinguished Name (DN) format as well as simple group names.

Group information can be configured in the following ways:

- The original Distinguished Name is supported. The Distinguished Name must match one of the groups configured on the Active Directory Server that will be used to assign access levels to the users associated with the group. For example:
  - 'CN=SpAdmin,OU=Groups,DC=domain,DC=sun,DC=com'
  - 'CN=SpOper,OU=Groups,DC=domain,DC=sun,DC=com'

- A simple group name can be used where the authenticated user's domain is searched for the particular group. For example:
  - 'SpAdmin' – which is the simple group name (a pre-Windows 2000 domain name)
- The domain can be specified along with the group name in an “NT-style” format. You can use either the full Distinguished Name domain or the simple domain name. For example:
  - 'DC=domain,DC=sun,DC=com\SpAdmin' – which is the full DN domain and group name
  - 'domain\SpAdmin' – which is the Windows NT-style domain and group name

## Active Directory Tables

The four tables in the bottom half of the Active Directory web interface ([FIGURE 5-13](#)) are used to configure domains, groups, and alternate servers in order to authenticate and authorize users. These tables store information about:

- Administrator Groups
- Operator Groups
- User Domains
- Alternate Servers

The Administrator Groups and Operator Groups tables contain the names of the Microsoft Active Directory groups in the Distinguished Name (DN) format. If a user is a member of a particular group, then the user is granted access as either an Operator or an Administrator.

User Domains are the authentication domains used to authenticate a user. When the user logs in, the name used is formatted in the specific domain name format template that appears in the cell by default. User authentication is attempted based on the user domain data entered and the login name provided by the user.

In the following figures and tables, default data shows the expected format of the Active Directory data.

**FIGURE 5-13** Active Directory Tables

Admin Groups	
ID	Name
1	CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
2	--
3	--
4	--
5	--

⌕ Back to top

Operator Groups	
ID	Name
1	CN=SpSuperOper,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
2	--
3	--
4	--
5	--

⌕ Back to top

User Domains	
ID	domain
1	<USERNAME>@davidc.example.sun.com
2	CN=<USERNAME>,CN=Users,DC=davidc,DC=example,DC=sun,DC=com
3	--
4	--
5	--

⌕ Back to top

Alternate Servers				
ID	Certificate Status	Certificate Operations	IP Address	Port
1	certificate not present; certificate backup not present;	--	10.8.143.231	0
2	certificate not present; certificate backup not present;	--	--	0
3	certificate not present; certificate backup not present;	--	--	0
4	certificate not present; certificate backup not present;	--	--	0
5	certificate not present; certificate backup not present;	--	--	0

⌕ Back to top

## Administrator Groups and Operator Groups Tables

TABLE 5-3 and TABLE 5-4 show samples of fully qualified Distinguished Names for the Administrator Groups and Operator Groups tables. For more information about the Distinguished Name format, see “LDAP Servers Directory Organization” on page 103..

**TABLE 5-3** Administrator Groups Table

ID	Name
1	CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
2	
3	
4	
5	

**TABLE 5-4** Operator Groups Table

ID	Name
1	CN=SpSuperOper,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
2	
3	
4	
5	

## User Domains Table

TABLE 5-5 provides sample data for the User Domains table. The domain listed in entry 1 shows the principle format that is used in the first attempt to authenticate the user. Entry 2 shows the complete Distinguished Name, which Active Directory would use if the attempt to authenticate the first entry failed.

---

**Note** – In the example below, <USERNAME> represents a user’s login name.

---

**TABLE 5-5** User Domains Table

Name	Domain
1	<USERNAME>@davidc.example.sun.com
2	CN=<USERNAME>, CN=Users, DC=davidc, DC=example, DC=sun, DC=com

## Alternate Servers Table

The Alternate Servers table provides redundancy and authentication. The alternate servers have the same rules and requirements as the top-level certificate mode. Each server has its own certificate status, and its own certificate command to retrieve the certificate if it is needed.

In [FIGURE 5-14](#), the top-level server is listed first, as ID 1.

**FIGURE 5-14** Allalternate Servers Table

Alternate Servers				
Edit				
ID	Certificate Status	Certificate Operations	IP Address	Port
<input type="radio"/> 1	certificate not present; certificate backup not present;	-	10.8.143.231	0
<input type="radio"/> 2	certificate not present; certificate backup not present;	-	-	0
<input type="radio"/> 3	certificate not present; certificate backup not present;	-	-	0
<input type="radio"/> 4	certificate not present; certificate backup not present;	-	-	0
<input type="radio"/> 5	certificate not present; certificate backup not present;	-	-	0

[Back to top](#)

## ▼ Configure Active Directory Settings

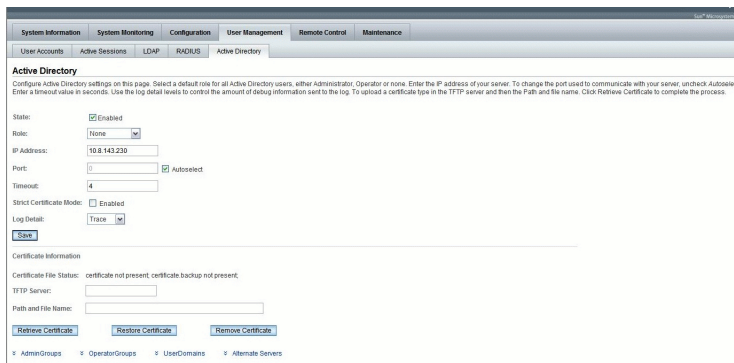
Before you can use Active Directory you need to configure the settings on the Active Directory page.

1. **Log in to ILOM as Administrator to open the web interface.**

## 2. Select User Management --> Active Directory.

The Active Directory page appears. Active Directory configuration settings and the Active Directory tables are displayed. See [FIGURE 5-15](#).

**FIGURE 5-15** Active Directory Configuration Settings



The screenshot shows the 'Active Directory' configuration page. At the top, there are tabs for 'System Information', 'System Monitoring', 'Configuration', 'User Management', 'Remote Control', and 'Maintenance'. Under 'User Management', there are sub-tabs for 'User Accounts', 'Active Sessions', 'LDAP', 'RADIUS', and 'Active Directory'. The 'Active Directory' sub-tab is selected. Below the sub-tabs, there is a heading 'Active Directory' followed by a brief instruction: 'Configure Active Directory settings on this page. Select a default role for all Active Directory users, either Administrator, Operator or none. Enter the IP address of your server. To change the port used to communicate with your server, uncheck Autoselect. Enter a timeout value in seconds. Use the log detail levels to control the amount of debug information sent to the log. To upload a certificate file in the TFTP server and then the Path and file name. Click Retrieve Certificate to complete the process.' The configuration fields include: 'State' (checked 'Enabled'), 'Role' (dropdown menu set to 'None'), 'IP Address' (text box with '10.8.143.230'), 'Port' (text box with '0' and a checked 'Autoselect' checkbox), 'Timeout' (text box with '4'), 'Strict Certificate Mode' (checkbox 'Enabled' and dropdown 'Trace'), and 'Log Detail' (dropdown 'Trace'). A 'Save' button is located below these fields. Below the 'Save' button is a section titled 'Certificate Information' with the status 'Certificate File Status: certificate not present; certificate backup not present.' It includes fields for 'TFTP Server:', 'Path and File Name:', and three buttons: 'Retrieve Certificate', 'Restore Certificate', and 'Remove Certificate'. At the bottom, there are links for 'AdminGroups', 'OperatorGroups', 'UserDomains', and 'Alternate Servers'.

## 3. Configure the Active Directory settings.

Refer to [TABLE 5-2](#) for a description of each setting.

## 4. Click Save for your settings to take effect.

# ▼ Edit Active Directory Tables Using the Web Interface

Follow this procedure to modify information for Administrator Groups, Operator Groups, User Domains, or Alternate Servers.

## 1. Log in to ILOM as Administrator to open the web interface.

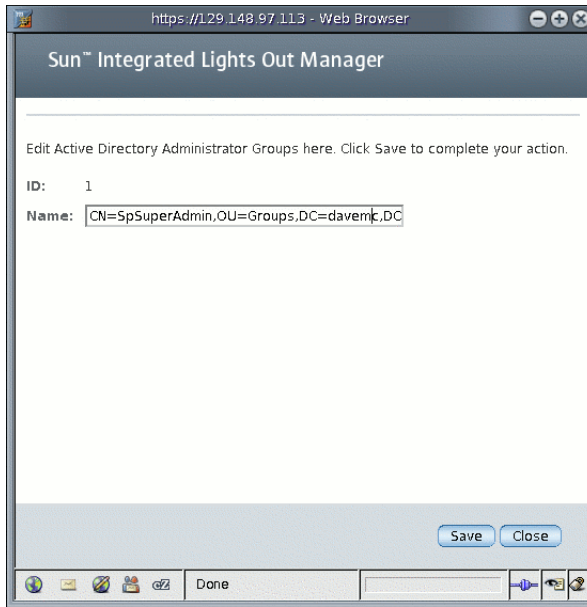
## 2. Select User Management --> Active Directory.

The Active Directory page appears.

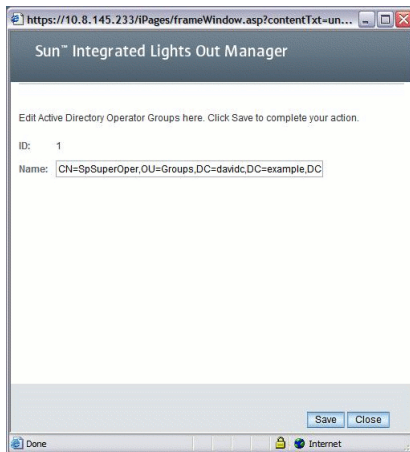
## 3. At the bottom of the Active Directory page, select the radio button next to the type of information you want to edit and click Edit.

The appropriate page appears: Edit Active Directory Administrator Groups page ([FIGURE 5-16](#)), Edit Active Directory Operator Groups page ([FIGURE 5-17](#)), Edit Active Directory User Domains page ([FIGURE 5-18](#)), and Edit Active Directory Alternate Servers page ([FIGURE 5-19](#)). Each “Edit” page provides one or more fields for adding or editing information.

**FIGURE 5-16** Active Directory Administrator Groups Edit Page

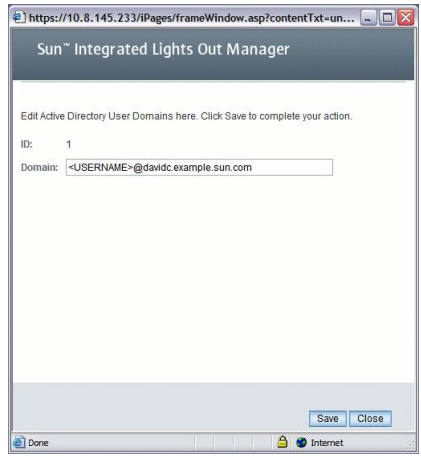


**FIGURE 5-17** Active Directory Operator Groups Edit Page

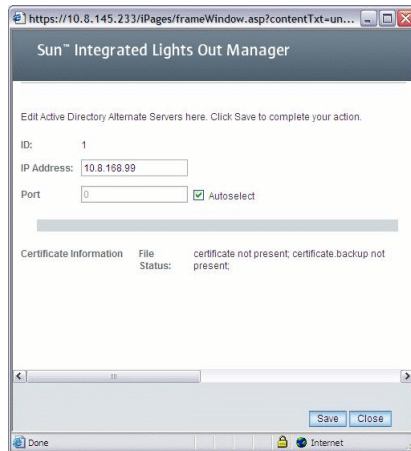




**FIGURE 5-18** Active Directory User Domains Edit Page



**FIGURE 5-19** Active Directory Alternate Servers Edit Page



**4. In the Edit page, add or edit the information you want to modify.**

- 5. In the User Domains table, enter the information in the Name field as text. Use the <USERNAME> substitution marker to hold a place for the user's name.**

For example:

```
domain = <USERNAME>davemcdomain.example.sun.com  
domain = CN=<USERNAME>, CN=Users, DC=davemcdomain, DC=example, DC=  
sun,  
DC=com
```

The user would be allowed access to ILOM with either supplied name as the following examples show.

**CODE EXAMPLE 5-1** Active Directory Login With Principle Format

```
/home/dchase> ssh -l davemcdomain 10.x.xxx.xxx  
Password:*****  
Sun(TM) Integrated Lights Out Manager  
Version 2.0  
Copyright 2007 Sun Microsystems, Inc. All rights reserved.  
->
```

**CODE EXAMPLE 5-2** Active Directory Login With Distinguished Name

```
/home/dchase> ssh -l "David A. Engineer" 10.x.xxx.xxx  
Password:*****  
Sun(TM) Integrated Lights Out Manager  
Version 2.0  
Copyright 2007 Sun Microsystems, Inc. All rights reserved.  
->
```

- 6. Click Save to have your changes take effect.**

The Active Directory page reappears.

## ▼ Edit Administrator Groups Table Using the CLI

1. Log in to the ILOM CLI as Administrator or Operator.
2. Type the following command to display Administrator Groups:

```
-> show /SP/clients/activedirectory/admingroups
```

For example:

```
-> show /SP/clients/activedirectory/admingroups
SP/clients/activedirectory/admingroups
Targets:
    1
    2
    3
    4
    5

Properties:
```

3. Type the following command to display properties for a specific Administrator Group:

```
-> show /SP/clients/activedirectory/admingroups/1
```

For example:

```
-> show /SP/clients/activedirectory/admingroups/1
/SP/clients/activedirectory/admingroups/1
Targets:

Properties: name = CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=
example,DC=sun,DC=com
```

4. Use the set command to modify properties.

For example:

```
-> set name=CN=spSuperAdmin,OU=Groups,DC=davidc,DC=sun,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=davidc,DC=sun,DC=com'
```

## ▼ Edit Operator Groups Table Using the CLI

Follow this procedure to edit information in the Operator Groups table using the ILOM CLI.

1. Log in to the ILOM CLI as Administrator or Operator.
2. Type the following command to display Operator Groups:

```
-> show /SP/clients/activedirectory/opergroups
```

For example:

```
-> show /SP/clients/activedirectory/opergroups
/SP/clients/activedirectory/opergroups
  Targets:
    1
    2
    3
    4
    5

  Properties:
```

3. Type the following command to display properties for a specific Operator Group:

```
-> show /SP/clients/activedirectory/opergroups/1
```

For example:

```
-> show /SP/clients/activedirectory/opergroups/1
/SP/clients/activedirectory/opergroups/1
  Targets:

  Properties: name = CN=SpSuperOper,OU=Groups,DC=davidc,DC=
example,DC=sun,DC=com
```

#### 4. Use the `set` command to modify properties.

For example:

```
-> set name=CN=spSuperOper,OU=Groups,DC=davidc,DC=sun,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=davidc,DC=sun,DC=com'
```

## ▼ Edit User Domains Table Using the CLI

Follow this procedure to edit information in the User Domains table using the ILOM CLI.

#### 1. Log in to the ILOM CLI as Administrator.

#### 2. Type the following command to display User Domains:

```
-> show /SP/clients/activedirectory/userdomains
```

For example:

```
-> show /SP/clients/activedirectory/userdomains
/SP/clients/activedirectory/userdomains
  Targets:
    1
    2
    3
    4
    5

  Properties:
```

#### 3. Type the following command to display properties for a specific User Domain:

```
-> show /SP/clients/activedirectory/userdomains/1
```

For example:

```
-> show /SP/clients/activedirectory/userdomains/1
/SP/clients/activedirectory/userdomains/1
Targets:

Properties:
    domain = <USERNAME>@davidc.example.sun.com
```

#### 4. Use the set command to modify properties.

For example:

```
-> set domain=domaindavidc@davidc.example.sun.com
Set 'domain' to 'domaindavidc@davidc.example.sun.com'
```

## ▼ Edit Alternate Servers Table Using the CLI

Follow this procedure to edit information in the Alternate Servers table using the ILOM CLI.

1. Log in to the ILOM CLI as Administrator.
2. Type the following command to display Alternate Servers:

```
-> show /SP/clients/activedirectory/alternateservers
```

For example:

```
-> show /SP/clients/activedirectory/alternateservers
/SP/clients/activedirectory/alternateservers
Targets:
    1
    2
    3
    4
    5

Properties:

Commands:
    cd
    show
    set
```

3. Type the following command to display properties for a specific Alternate Server:

```
-> show /SP/clients/activedirectory/alternateservers/1
```

For example:

```
-> show /SP/clients/activedirectory/alternateservers/1
/SP/clients/activedirectory/alternateservers/1
  Targets:

  Properties:
certfilestatus = certificate not present; certificate.backup not
present;
getcertfile = (none)
ipaddress = 10.8.143.231
port = 0
```

4. Use the `set` command to modify properties.

For example:

```
-> set /SP/clients/activedirectory/alternateservers/1 port=1
```

## About Active Directory Properties

There are nine Active Directory properties available in the CLI:

- `ipaddress`
- `defaultrole`
- `logdetail`
- `port`
- `state`
- `strictcertmode`
- `timeout`
- `certfilestatus`
- `getcertfile`

## ipaddress Property

Server IP address of the Active Directory server.

```
-> show /SP/clients/activedirectory address

/SP/clients/activedirectory
Properties:
  address = 0.0.0.0
```

## defaultrole Property

Possible values = administrator, operator, or none.

```
-> show /SP/clients/activedirectory defaultrole

/SP/clients/activedirectory
Properties:
  defaultrole = Administrator
```

## logdetail Property

Debug event level for the Active Directory authentication module that controls how much information goes into the event log.

Possible values = none, high, medium, low, trace

```
-> show /SP/clients/activedirectory logdetail

/SP/clients/activedirectory
Properties:
  logdetail = trace
```

## port Property

TCP port of the Active Directory server (0-auto...65535)

Possible values: integer between 0 and 65535, where 0 = autoselect.

```
-> show /SP/clients/activedirectory port

/SP/clients/activedirectory
Properties:
  port = 0
```



## state Property

Administrative mode of Active Directory authentication module.

Possible values = enabled, disabled

```
-> show /SP/clients/activedirectory state

/SP/clients/activedirectory
Properties:
  state = enabled
```

## strictcertmode Property

Strict certificate validation requiring a local copy of the certificate before it can be enabled.

Possible values = enabled, disabled:

```
-> show /SP/clients/activedirectory strictcertmode

/SP/clients/activedirectory
Properties:
  strictcertmode = disabled
```

## timeout Property

Timeout value in seconds. Default is set to 4.

Number of seconds to wait for individual transactions to complete. The value does not represent the total time of all transactions because the number of transactions can differ depending on the configuration.

This property allows for tuning the time to wait when a server is not responding or is unreachable.

```
-> show /SP/clients/activedirectory timeout

/SP/clients/activedirectory
Properties:
  timeout = 4
```

## certfilestatus Property

certfilestatus is a view-only property that should reflect the current certificate state, as well as a backup copy of the certificate. Neither is required to exist if strictcertmode is disabled. However, for the strictcertmode to be enabled, a certificate must be loaded. The backup certificate is always optional and is only stored when an existing certificate is about to be overwritten.

```
-> show /SP/clients/activedirectory certfilestatus
-> show /SP/clients/activedirectory certfilestatus
    Properties:
certfilestatus = certificate not present;certificate.backup not
present;
```

## getcertfile Property

Use the set getcertfile command to upload, remove, or restore a certificate file if needed. For specific instructions see [“Upload, Remove, or Restore a Certificate Using the CLI”](#) on page 99.

# Diagnosing Authentication and Authorization Events

You can view messages from the system event log to determine how user authentication and authorization was obtained. You can set the event log to capture the following detail levels:

- None – No logging of any message types
- High – Critical events only
- Medium – Major and critical events
- Low – Minor, medium, and critical events
- Trace – Debug events

## ▼ View Authentication and Authorization Events Using the CLI

You can configure Active Directory log detail from the top level by setting the `logdetail` variable to one of the desired event levels.

- **Type the following command to configure the event log detail:**

```
-> set /SP/clients/activedirectory logdetail=event_log_detail
```

Where *event\_log\_detail* is either *none*, *high*, *medium*, *low*, or *trace*. For example:  
Set 'logdetail' to 'trace'

Summary information as well as detailed query information is displayed about user authentication and authorization information. The example below shows a detailed 'trace' level debug listing. The most recent events are at the top of the log.

```
-> cd /SP/logs/event
/SP/logs/event

-> show

-> cd event
/SP/logs/event

-> show list
ID      Date/Time                Class      Type      Severity
-----
49      Mon Apr 6 01:41:19 1970  ActDir    Log       minor
      (ActDir) authentication status: auth-OK

48      Mon Apr 6 01:41:19 1970  ActDir    Log       minor
      (ActDir) server-authenticate: auth-success idx 0 server
10.8.143.231

47      Mon Apr 6 01:41:19 1970  ActDir    Log       debug
      (ActDir) accessLvl administrator
```

## ▼ View Authentication and Authorization Events Using the Web Interface

1. **Log in to ILOM as Administrator to open the web interface.**
2. **Select User Management --> Active Directory.**  
The Active Directory page appears.
3. **Use the Log Detail drop-down list box to select the level of log detail you want to view.**

## Set Certificate Validation Using the CLI

Certificate validation enables the secure passing and protecting of data over the network. Certificate validation is optional depending on the security level that your system requires.

## ▼ Upload, Remove, or Restore a Certificate Using the CLI

1. Log in as Administrator to the ILOM CLI.
2. Use these commands to upload, remove, or restore a certificate:
  - To upload a certificate, type the following:

```
-> set getcertfile=tftp://IP address/file-path/filename
```

- To remove or restore a certificate, type the following:

```
-> set getcertfile=remove|restore
```

For example:

```
-> set getcertfile=remove
```

The existing certificate file that had been uploaded will be removed. The restore only works if a certificate file was overwritten. The intent is to save one backup file when a certificate is uploaded. If something goes wrong, the old file can be restored.

## ▼ Enable `strictcertmode` Using the CLI

By default, `strictcertmode` is disabled. When this variable is disabled, the channel is secure, but limited validation of the certificate is performed. If `strictcertmode` is enabled, then the server's certificate must have already been uploaded to the server so that the certificate signatures can be validated when the server certificate is presented.

1. Log in to the ILOM CLI as Administrator.
2. To enable `strictcertmode`, type the following:

```
-> set strictcertmode=enabled
```

## ▼ Check `certfilestatus` Using the CLI

1. Log in to the ILOM CLI as Administrator.

## 2. To check the status of the certificate, type the following:

```
-> show /SP/clients/activedirectory certfilestatus
```

For example:

```
-> show /SP/clients/activedirectory certfilestatus
-> show /SP/clients/activedirectory certfilestatus
    Properties:
certfilestatus = certificate not present;certificate.backup not
present;
```

## Set Certificate Validation Using the Web Interface

The following procedures describe how to secure the Active Directory connection using the web interface.

FIGURE 5-20 shows the security properties of Active Directory and the sequence in which data must be entered.

FIGURE 5-20 Security Properties of Active Directory and the Sequence of Data Entry

The screenshot shows the 'Active Directory' configuration page in the Sun ILOM web interface. The page has a navigation bar at the top with tabs for System Information, System Monitoring, Configuration, User Management, Remote Control, and Maintenance. Below the navigation bar, there are sub-tabs for User Accounts, Active Sessions, LDAP, RADIUS, and Active Directory. The main content area is titled 'Active Directory' and contains the following configuration options:

- State:  Enabled
- Role: None (dropdown)
- IP Address: 10.8.143.230
- Port: 0 (input)  Autoselect
- Timeout: 4 (input)
- Strict Certificate Mode:  Enabled (labeled with '4')
- Log Detail: Trace (dropdown)
- Save button
- Certificate Information section:
  - Certificate File Status: certificate not present; certificate backup not present. (labeled with '3')
  - TFTP Server: (input) (labeled with '1a')
  - Path and File Name: (input) (labeled with '1b')
  - Buttons: Retrieve Certificate (labeled with '2'), Restore Certificate, Remove Certificate

At the bottom of the page, there are links for AdminGroups, OperatorGroups, UserDomains, and Alternate Servers.

## ▼ Upload a Certificate Using the Web Interface

1. Log in to ILOM as Administrator to open the web interface.
2. Select User Management --> Active Directory.  
The Active Directory page appears. [FIGURE 5-20](#) illustrates the order in which to populate the security fields.
3. Enter the TFTP Server and Path and File Name. See [FIGURE 5-20](#), items 1a and 1b.
4. Click the Retrieve Certificate button to initiate the transfer of the certificate. See [FIGURE 5-20](#), item 2.

---

**Note** – The options to restore and remove are available as needed, and can be executed by clicking the Restore Certificate button or the Remove Certificate button.

---

## ▼ Check Certificate File Status Using the Web Interface

1. Log in to ILOM as Administrator to open the web interface.
2. Select User Management --> Active Directory.  
The Active Directory page appears. See [FIGURE 5-20](#), item 3.
3. Verify the Certificate File Status.

## ▼ Enable Strict Certificate Mode Using the Web Interface

1. Log in to ILOM as Administrator to open the web interface.
2. Select User Management --> Active Directory.  
The Active Directory page appears. See [FIGURE 5-20](#), item 4.
3. Click the check box next to Enable to enable Strict Certificate Mode.
4. Click Save for your changes to take effect.

---

# Lightweight Directory Access Protocol

ILOM supports Lightweight Directory Access Protocol (LDAP) authentication for users, based on the OpenLDAP software. LDAP is a general-purpose directory service. A directory service is a centralized database for distributed applications designed to manage the entries in a directory. Thus, multiple applications can share a single user database. For more detailed information about LDAP, see <http://www.openldap.org/>.

## About LDAP

LDAP is based on a client-server model. LDAP provides the directory, and the clients use the directory service to access entries. The data stored in a directory can be distributed among several LDAP servers.

Data in LDAP is organized hierarchically, starting at a root and branching down into individual entries. Entries at the top level of the hierarchy represent larger organizations, and under the larger organizations are entries for smaller organizations. At the bottom of the hierarchy are entries for individual people or resources.

## LDAP Clients and Servers

In the LDAP client-server model, LDAP servers make information about people, organizations, and resources accessible to LDAP clients. Clients make changes to the LDAP database using a client utility, usually bundled with the LDAP server. When a change is made to the LDAP database, all client applications see the change immediately, so there is no need to update each distributed application.

For example, to update an entry in the directory, an LDAP client submits the Distinguished Name of the entry with updated attribute information to the LDAP server. The LDAP server uses the Distinguished Name (dn) to find the entry and performs a modify operation to update the entry in the directory. The updated information is immediately available to all the distributed applications using that LDAP server.

An LDAP client can perform the following operations, among others:

- Search for and retrieve entries from the directory.
- Add new entries to the directory.
- Update entries in the directory.



- Delete entries from the directory.
- Rename entries in the directory.

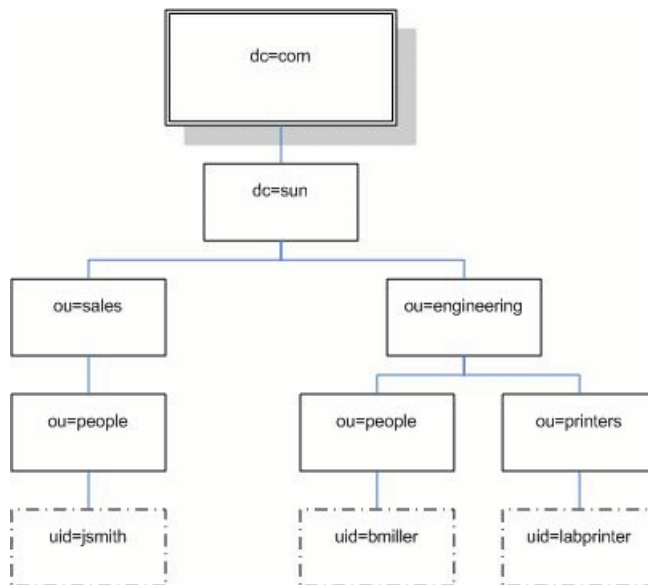
To perform any of these LDAP operations, an LDAP client needs to establish a connection with an LDAP server. LDAP specifies the use of TCP/IP port number 389, although servers may run on other ports.

Your Sun server can be a client of an LDAP server. In order to use LDAP authentication, you need to create a user on your LDAP server that your Sun server can authenticate, or bind to, so the client has permission to search the proper directory on the LDAP server.

## LDAP Servers Directory Organization

Data in LDAP is organized hierarchically, as shown in [FIGURE 5-21](#).

**FIGURE 5-21** LDAP Directory Structure



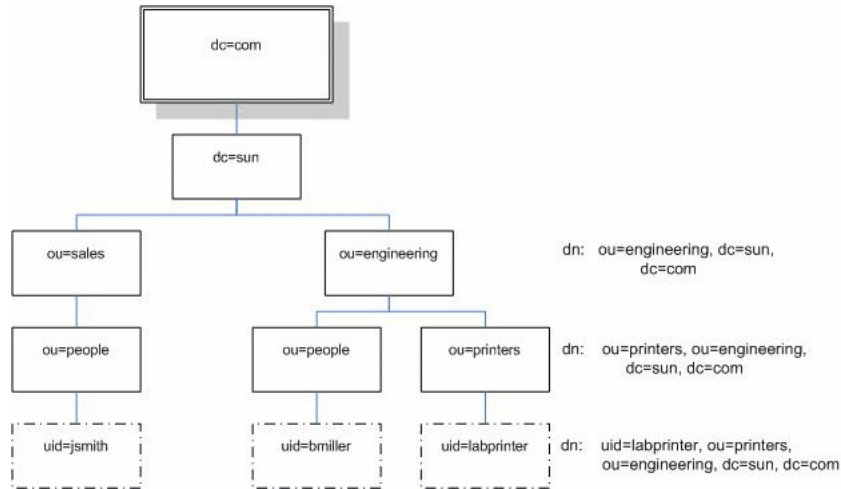
Each entry is uniquely identified by a Distinguished Name (dn). A DN consists of a name that uniquely identifies the entry at that hierarchical level and a path that traces the entry back to the root of the tree.

For example, the DN for jsmith is:

```
dn: uid=jsmith, ou=people, dc=sun.com
```

Here, `uid` represents the user ID of the entry, `ou` represents the organizational unit in which the entry belongs, and `dc` represents the larger organization in which the entry belongs. The following diagram shows how Distinguished Names are used to identify entries uniquely in the directory hierarchy.

**FIGURE 5-22** LDAP Distinguished Names



## Configure LDAP

To use LDAP, you must configure your LDAP server, according to your LDAP server's documentation. You must also configure your ILOM, using either the ILOM CLI or the web interface.

The following procedure requires detailed knowledge of your LDAP server configuration. Before you begin, gather basic network information about your LDAP server, including its IP address.

---

**Note** – This task is similar to configuring LDAP as a name service for Linux or Solaris.

---

## ▼ Configure the LDAP Server

1. Ensure that all users authenticating to ILOM have passwords stored in "crypt" format or the GNU extension to crypt, commonly referred to as "MD5 crypt."

For example:

```
userPassword: {CRYPT}ajCa2He4PJhNo
```

or

```
userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46.
```

ILOM only supports LDAP authentication for passwords stored in these two variations of the crypt format.

2. Add object classes `posixAccount` and `shadowAccount`, and populate the required property values for this schema (RFC 2307).

TABLE 5-6 LDAP Property Values

Required Property	Description
uid	User name for logging in to ILOM
uidNumber	Any unique number
gidNumber	Any unique number
userPassword	Password
homeDirectory	Any value (this property is ignored by ILOM)
loginShell	Any value (this property is ignored by ILOM)

3. Provide ILOM access to user accounts on your LDAP server.

Either enable your LDAP server to accept anonymous binds, or create a proxy user on your LDAP server that has read-only access to all user accounts that will authenticate through ILOM.

See your LDAP server documentation for more details.

## ▼ Configure ILOM for LDAP Using the CLI

1. Enter the proxy user name and password. Type:

```
-> set /SP/clients/ldap binddn="cn=proxyuser, ou=people, ou=sales, dc=sun, dc=com" bindpw=password
```

2. Enter the IP address of the LDAP server. Type:

```
-> set /SP/clients/ldap ipaddress=ldapipaddress
```

3. Assign the port used to communicate with the LDAP server; the default port is 389. Type:

```
-> set /SP/clients/ldap port=ldapport
```

4. Enter the Distinguished Name of the branch of your LDAP tree that contains users and groups. Type:

```
-> set /SP/clients/ldap searchbase="ou=people, ou=sales, dc=sun, dc=com"
```

This is the location in your LDAP tree that you want to search for user authentication.

5. Set the state of the LDAP service to enabled. Type:

```
-> set /SP/clients/ldap state=enabled
```

6. To verify that LDAP authentication works, log in to ILOM using an LDAP user name and password.

---

**Note** – ILOM searches local users before LDAP users. If an LDAP user name exists as a local user, ILOM uses the local account for authentication.

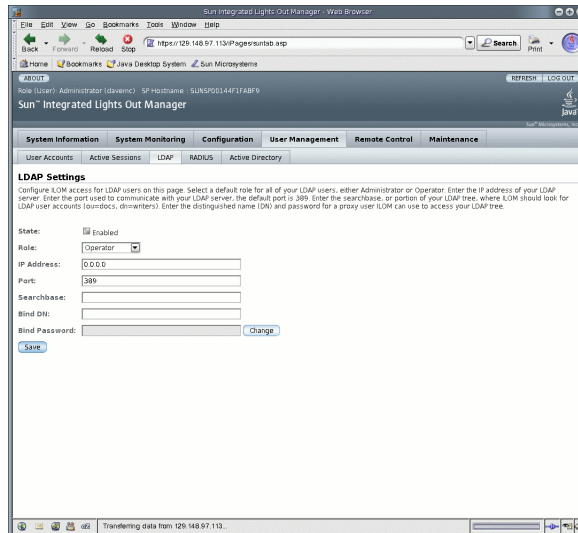
---

## ▼ Configure ILOM for LDAP Using the Web Interface

1. Log in to ILOM as an Administrator to open the web interface.
2. Select User Management --> LDAP.

The LDAP Settings page appears.

**FIGURE 5-23** LDAP Settings Page



**3. Enter the following values:**

- **State** – Select the Enabled check box to authenticate LDAP users.
- **Role** – The default role of LDAP users. Select Operator or Administrator from the drop-down list.
- **IP Address** – The IP address of the LDAP server.
- **Port** – The port number on the LDAP server.
- **Searchbase** – Type the branch of your LDAP server to search for users.
- **Bind DN** – Type the Distinguished Name (DN) of a read-only proxy user on the LDAP server. ILOM must have read-only access to your LDAP server to search for and authenticate users.
- **Bind Password** – Type the password of the read-only user.

**4. Click Save.**

**5. To verify that LDAP authentication works, log in to the ILOM using an LDAP user name and password.**

---

**Note** – The ILOM searches local users before LDAP users. If an LDAP user name exists as a local user, the ILOM uses the local account for authentication.

---

---

# RADIUS Authentication

ILOM supports Remote Authentication Dial-In User Service (RADIUS) authentication. RADIUS is an authentication protocol that facilitates centralized user administration. RADIUS provides many servers shared access to user data in a central database, providing better security and easier administration. A RADIUS server can work in conjunction with multiple RADIUS servers and other types of authentication servers.

## RADIUS Clients and Servers

RADIUS is based on a client-server model. The RADIUS server provides the user authentication data and can grant or deny access, and the clients send user data to the server and receive an accept or deny response. In the RADIUS client-server model, the client sends an Access-Request query to the RADIUS server. When the server receives an Access-Request message from a client, it searches the database for that user's authentication information. If the user's information is not found, the server sends an Access-Reject message and the user is denied access to the requested service. If the user's information is found, the server responds with an Access-Accept message. The Access-Accept message confirms the user's authentication data and grants the user access to the requested service.

All transactions between the RADIUS client and server are authenticated by the use of specific text string password known as a shared secret. The client and server must each know the secret because it is never passed over the network. You must know the shared secret to configure RADIUS authentication for ILOM.

In order to use RADIUS authentication with ILOM, you must configure ILOM as a RADIUS client.

# RADIUS Parameters

[TABLE 5-7](#) describes the RADIUS parameters for the web interface and the CLI.

**TABLE 5-7** RADIUS Web Interface and CLI Settings

Web Interface	CLI	Description
State	<code>state enabled disabled</code>	Enable to authenticate RADIUS users.
Role	<code>defaultrole administrator operator</code>	Sets the default role for all RADIUS users – Administrator or Operator.
IP Address	<code>ipaddress ipaddress</code>	The IP address of the RADIUS server.
Port	<code>port portnum</code>	The port number used to communicate with the RADIUS server. The default port is 1812.
Shared Secret	<code>secret text</code>	The shared secret used to gain access to RADIUS.

## Configure RADIUS Settings

If you need to provide ILOM access beyond the 10 local user accounts, and after the RADIUS server has been properly configured, you can configure ILOM to use RADIUS authentication.

Before completing this procedure, collect the appropriate information about your RADIUS environment, as described in [“Manage User Accounts” on page 57](#).

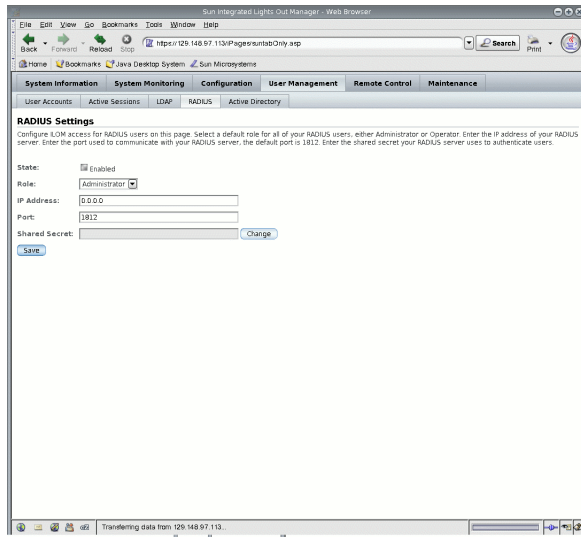
## ▼ Configure RADIUS Using the CLI

1. Log in to the ILOM CLI as a user with Administrator privileges.
2. Navigate to `/SP/clients/radius`. See “RADIUS Commands” on page 111.
3. Set the parameters shown in TABLE 5-7.

## ▼ Configure RADIUS Using the Web Interface

1. Log in to the ILOM as Administrator to open the web interface.
2. Select User Management --> RADIUS.  
The RADIUS Settings page appears.

FIGURE 5-24 RADIUS Settings Page



3. Complete the settings.  
For details, see TABLE 5-7.
4. Click Save for your changes to take effect.



# RADIUS Commands

This section describes the RADIUS commands.

```
show /SP/clients/radius
```

This command is available to Administrators and Operators.

## *Purpose*

Use this command to view the properties associated with RADIUS authentication.

## *Syntax*

```
show /SP/clients/radius
```

## *Properties*

`defaultrole` – This is the role assigned to all RADIUS users: Administrator or Operator.

`ipaddress` – IP address of your RADIUS server.

`port` – Port number used to communicate with your RADIUS server. The default port is 1812.

`secret` – This is the shared secret used to gain access to your RADIUS server.

`state` – This setting is enabled or disabled to allow or deny access to your RADIUS users.

## Example

```
-> show /SP/clients/radius

/SP/clients/radius
Targets:

Properties:
  defaultrole = Operator
  ipaddress = 129.144.36.142
  port = 1812
  secret = (none)
  state = enabled

Commands:
  cd
  set
  show

->
```

`set /SP/clients/radius`

This command is available to Administrators.

## Purpose

Use this command to configure the properties associated with RADIUS authentication on a service processor.

## Syntax

```
set /SP/clients/radius [defaultrole=[Administrator|Operator]
ipaddress=radiusserverIP port=port# secret=radiussecret state=
[enabled|disabled]]
```

## Properties

- `defaultrole` – You must assign a permission level that will apply to all RADIUS users, either Administrator or Operator.
- `ipaddress` – IP address of your RADIUS server.

- `port` – Port number used to communicate with your RADIUS server. The default port is 1812.
- `secret` – Enter the shared secret used to gain access to your RADIUS server. This is also known as an encryption key.
- `state` – Choose enabled or disabled to allow or deny access to your RADIUS users.

### *Example*

```
-> set /SP/clients/radius state=enabled ipaddress=10.8.145.77
Set 'state' to 'enabled'
Set 'ipaddress' to '10.8.145.77'
```

`show /SP/clients`

This command is available to Administrators and Operators.

### *Purpose*

Use this command to view clients that can receive data from a service processor, including LDAP, NTP, RADIUS, and SYSLOG clients.

### *Syntax*

`show /SP/clients`

## Example

```
-> show /SP/clients
```

```
  /SP/clients
```

```
    Targets:
```

```
  ldap
```

```
  ntp
```

```
  radius
```

```
  syslog
```

```
    Properties:
```

```
    Commands:
```

```
      cd
```

```
      show
```

---

**Note** – Users with Operator privileges can only view the `ntp` and `syslog` targets. The `radius` and `ldap` targets remain hidden.

---

# Inventory and Component Management

---

With ILOM, you can view component details such as the component name, type, and fault status. In addition, you can use ILOM to prepare to remove and install components.

This chapter includes the following sections:

- [“View Component Information and Manage Inventory”](#) on page 116
  - [“View Component Information Using the CLI”](#) on page 116
  - [“View Component Information Using the Web Interface”](#) on page 117
- [“Perform an Action on a Component”](#) on page 118
  - [“Prepare to Remove a Component Using the CLI”](#) on page 119
  - [“Determine Whether a Component Is Ready for Removal Using the CLI”](#) on page 119
  - [“Return a Component to Service Using the CLI”](#) on page 120
  - [“Prepare to Remove a Component Using the Web Interface”](#) on page 120
  - [“Return a Component to Service Using the Web Interface”](#) on page 121
- [“Enable and Disable Components”](#) on page 122
  - [“Enable and Disable Components Using the CLI”](#) on page 122
  - [“Enable and Disable Components Using the Web Interface”](#) on page 122
- [“Configure Policy Settings”](#) on page 122
  - [“Configure Policy Settings Using the CLI”](#) on page 123
  - [“Configure Policy Settings Using the Web Interface”](#) on page 123

---

**Note** – Syntax examples in this chapter use the target starting with */SP/*, which could be interchanged with the target starting with */CMM/* depending on your Sun server platform. Subtargets are common across all Sun server platforms.

---

## View Component Information and Manage Inventory

The following procedures explain how to view component information. Both Administrators and Operators can view component information.

### ▼ View Component Information Using the CLI

1. Log in to the ILOM CLI as an Administrator or Operator.
2. At the command prompt, type:

-> **show component\_name type**

For example:

```
-> show /SYS/MB type
Properties:
    type = Motherboard
Commands:
    show
```

The properties that display inventory information are outlined in the following list. The properties that you are able to view depend on the target type you use.

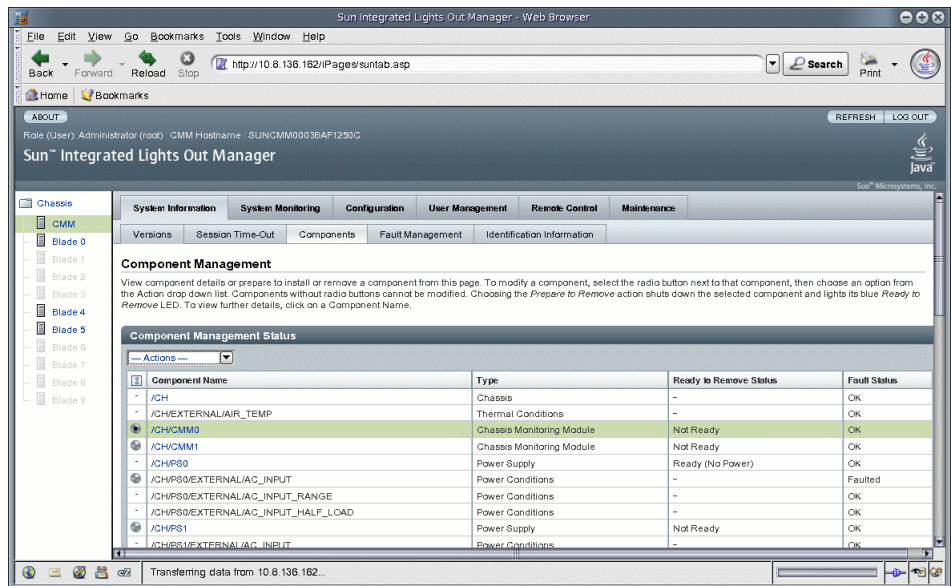
- fru\_part\_number
- fru\_manufacturer
- fru\_serial\_number
- fru\_name
- fru\_description
- fru\_version
- chassis\_serial\_number
- chassis\_part\_number
- product\_name

- product\_serial\_number
- product\_part\_number
- customer\_frudata

## ▼ View Component Information Using the Web Interface

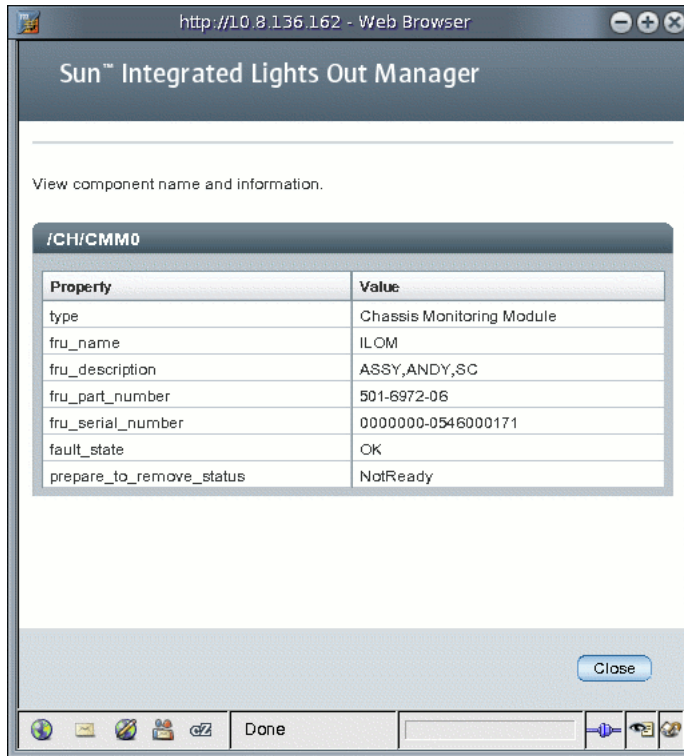
1. Log in to the ILOM web interface as an Administrator or Operator.
2. Select System Information --> Components.  
The Component Management page appears.

**FIGURE 6-1** Component Management Page



3. Click on the name of a component in the Component Management Status table.  
A dialog box appears with information about the selected component.

**FIGURE 6-2** Component Information Dialog



---

## Perform an Action on a Component

In addition to viewing inventory, you can also perform the following actions on components:

- Prepare to Remove/Return to Service – See [“Remove and Replace Components” on page 118](#).
- Enable/Disable – See [“Enable and Disable Components” on page 122](#).
- Clear Fault – See [“Fault Management” on page 139](#).

## Remove and Replace Components

You can replace many components while a system is running by using a remove and replace procedure. The procedure involves removing and inserting modules into a system. Before removing a module from a system, you must prepare the module by using the ILOM CLI or web interface.



## ▼ Prepare to Remove a Component Using the CLI

1. Log in to the ILOM CLI as an Administrator or Operator.

2. At the ILOM command prompt, type:

```
-> set <target> prepare_to_remove_action=true
```

For example:

```
-> set /CH/RFM0 prepare_to_remove_action=true
```

Set 'prepare\_to\_remove\_action' to 'true'

## ▼ Determine Whether a Component Is Ready for Removal Using the CLI

After you prepare the component for removal, you can verify that it is ready to be physically removed.

1. Log in to the ILOM CLI as an Administrator or Operator.

2. At the ILOM command prompt, type:

```
-> show <target> prepare_to_remove_status
```

For example:

```
-> show /CH/RFM0 prepare_to_remove_status
Properties:
  prepare_to_remove_status = Ready|NotReady
Commands:
  cd
  set
  show
  start
  stop
```

The Ready|NotReady statement in the example shows whether the device is ready to be removed.

## ▼ Return a Component to Service Using the CLI

If you have already prepared a component for removal, and you wish to undo the action, you can do so remotely.

1. Log in to the ILOM CLI as an Administrator or Operator.
2. At the ILOM command prompt, type:

```
-> set <target> return_to_service_action=true
```

For example:

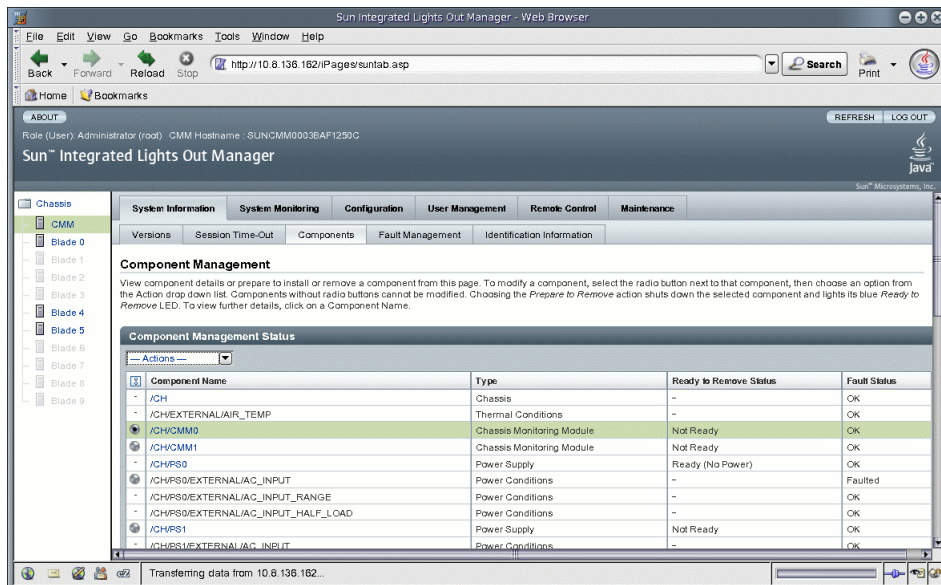
```
-> set /CH/RFM0 return_to_service_action=true
```

Set 'return\_to\_service\_action' to 'true'

## ▼ Prepare to Remove a Component Using the Web Interface

1. Log in to the ILOM web interface as an Administrator or Operator.
2. Select System Information --> Components.  
The Component Management page appears.

FIGURE 6-3 Component Management Page



3. Select the radio button next to the component that you want to remove.  
Components without radio buttons cannot be removed.
4. From the Actions drop-down list, select Prepare to Remove.

## ▼ Return a Component to Service Using the Web Interface

1. Log in to the ILOM web interface as an Administrator or Operator.
2. Select System Information --> Components.  
The Component Management page appears.
3. Select the radio button next to the component you want to return to service.
4. From the Actions drop-down list, select Return to Service.

---

## Enable and Disable Components

Depending on your Sun Server platform, you may be able to enable or disable certain components. See your Sun server platform-specific documentation for more details.

## ▼ Enable and Disable Components Using the CLI

1. Log in to the ILOM CLI as an Administrator.
2. At the ILOM command prompt, type:

```
-> set /SYS/MB/CMP0/P0/C0 component_state=enabled | disabled
```

## ▼ Enable and Disable Components Using the Web Interface

1. Log in to the ILOM web interface as an Administrator.

**2. Select System Information --> Components.**

The Component Management page appears.

**3. Select the radio button next to the component you want to enable or disable.**

**4. From the Actions drop-down list, select either Enable or Disable.**

The component is enabled or disabled, depending on your selection.

---

## Configure Policy Settings

Policies are settings that control the behavior of the system. Policies are shipped with system default settings, which you can easily modify using the ILOM CLI or web interface.

### ▼ Configure Policy Settings Using the CLI

**1. Log in to the ILOM CLI as an Administrator.**

**2. At the ILOM command prompt, type:**

**-> show /CMM/policy**

For example

```
-> show /CMM/policy
/CMM/policy
  Targets:
  Properties:
Policy1Name = enabled
Policy2Name = enabled
Policy2Name = enabled
  Commands:
    cd
    set
    show
```

**3. At the ILOM command prompt, type:**

**-> set /CMM/policy**

For example

**-> set /CMM/Policy1Name=enabled**

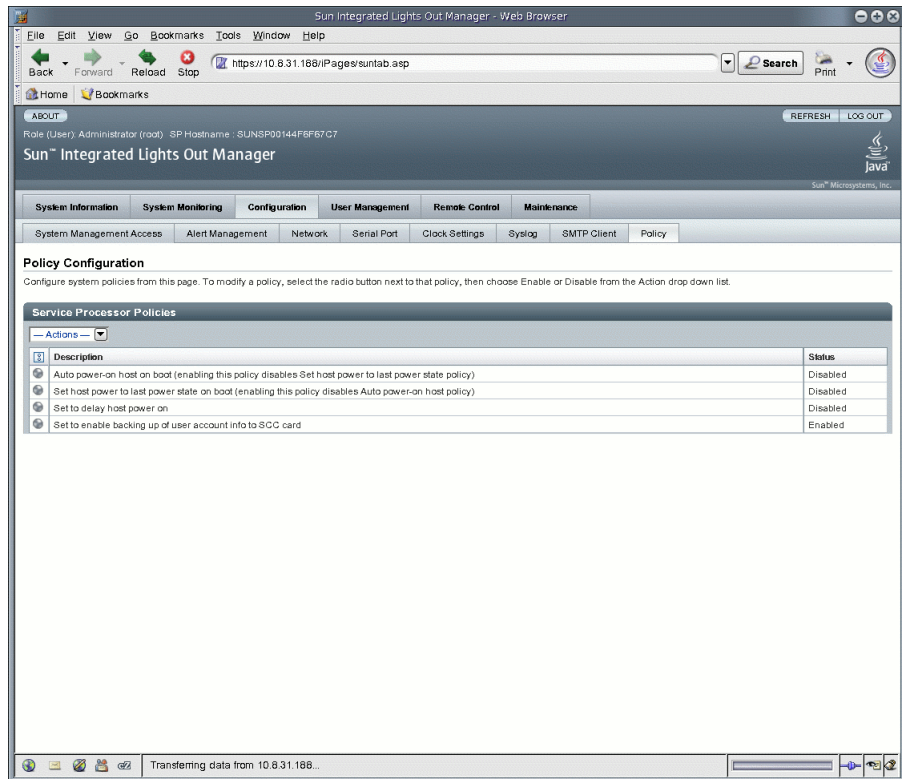
/CMM/Policy1Name=enabled

## ▼ Configure Policy Settings Using the Web Interface

Depending on the Sun server platform you are using, you may have the ability to configure policy settings.

1. Log in to the ILOM web interface as an Administrator.
2. Select Configuration --> Policy.  
The Policy Configuration window appears.
3. Select the radio button next to the policy that you want to modify.
4. Select Enable or Disable from the Actions drop-down list.

FIGURE 6-4 Policy Configuration Page





# System Monitoring and Alert Management

---

The system monitoring features in ILOM enable you to proactively monitor the health of your system. The alert management features in ILOM enable you to receive advance notice of events occurring on your system. You can view and manage the system monitoring and alert management features in ILOM from either the ILOM web interface or command-line interface (CLI).

This chapter includes the following topics:

- [“About System Monitoring” on page 126](#)
  - [“Sensor Readings” on page 127](#)
  - [“Power Monitoring Interfaces” on page 131](#)
  - [“System Indicators” on page 132](#)
  - [“ILOM Event Log” on page 136](#)
  - [“Event Log Timestamps and ILOM Clock Settings” on page 136](#)
  - [“Syslog Information” on page 138](#)
  - [“Fault Management” on page 139](#)
  - [“ILOM Service Snapshot Utility” on page 142](#)
- [“Monitor System Power, Sensors, Indicators, and ILOM Event Log” on page 142](#)
  - [“Monitor System Total Power Consumption Using the CLI” on page 143](#)
  - [“Monitor System Actual Power Using the CLI” on page 144](#)
  - [“Monitor Individual Power Supply Consumption Using the CLI” on page 145](#)
  - [“Monitor Available Power Using the CLI” on page 146](#)
  - [“Monitor Permitted Power Consumption Using the CLI” on page 146](#)
  - [“Determine the State of Indicators Using the Web Interface” on page 147](#)
  - [“Obtain Sensor Readings Using the Web Interface” on page 148](#)
  - [“View or Clear the ILOM Event Log Using the Web Interface” on page 148](#)

- [“View or Clear the ILOM Event Log Using the CLI” on page 150](#)
- [“View and Set Clock Settings Using the CLI” on page 137](#)
- [“View and Configure Clock Settings Using the Web Interface” on page 152](#)
- [“Configure Remote Syslog Receiver IP Addresses Using the Web Interface” on page 153](#)
- [“Configure Remote Syslog Receiver IP Addresses Using the CLI” on page 154](#)
- [“Run the Snapshot Utility Using the CLI” on page 155](#)
- [“Run the Snapshot Utility Using the Web Interface” on page 156](#)
- [“About Alert Management” on page 158](#)
  - [“Alert Rule Configuration” on page 158](#)
  - [“Alert Rule Property Definitions” on page 159](#)
- [“Manage Alert Rule Configurations Using the ILOM Web Interface” on page 161](#)
  - [“Prerequisites” on page 162](#)
  - [“Modify an Alert Rule Configuration Using the Web Interface” on page 162](#)
  - [“Disable an Alert Rule Configuration Using the Web Interface” on page 163](#)
  - [“Generate Alert Tests Using the Web Interface” on page 164](#)
- [“Manage Alert Rule Configurations Using the ILOM CLI” on page 164](#)
  - [“CLI Commands for Managing Alert Rule Configurations” on page 165](#)
  - [“Modify Alert Rule Configurations Using the CLI” on page 167](#)
  - [“Disable an Alert Rule Configuration Using the CLI” on page 168](#)
- [“Configure SMTP Client for Email Notification Alerts” on page 170](#)
  - [“Enable SMTP Client Using the Web Interface” on page 170](#)
  - [“Enable SMTP Client Using the CLI” on page 171](#)

---

## About System Monitoring

The system monitoring features in ILOM enable you to easily determine the health of the system and to detect errors, at a glance, when they occur. For instance, in ILOM you can:

- Obtain instantaneous sensor readings about system component temperatures, current, voltage, speed, and presence. For more information, see [“Sensor Readings” on page 127](#).
- Monitor real-time power consumption. For more information, see [“Power Monitoring Interfaces” on page 131](#).



- Determine the state of indicators throughout the system. For more information, see [“System Indicators” on page 132](#).
- Identify system errors and view event information in the ILOM event log. For more information, see [“ILOM Event Log” on page 136](#).
- View the fault state of a system component. Note that this feature is currently available on the all Sun server platforms with the exception of the Sun Fire X4100 or X4200 series servers. For more information, see [“Fault Management” on page 139](#)
- Receive generated notices about system events in advance via IPMI PET alerts, SNMP Trap alerts, or Email Notification alerts. For more information, see [“About Alert Management” on page 158](#).

## Sensor Readings

All Sun server platforms are equipped with a number of sensors that measure voltage, temperatures, fan speeds, and other attributes about the system. Each sensor in ILOM contains nine properties describing various settings related to a sensor such as sensor type, sensor class, sensor value, as well as the sensor values for upper and lower thresholds.

ILOM regularly polls the sensors in the system and reports any events it encounters about sensor state changes or sensor threshold crossings to the ILOM event log. Additionally, if an alert rule was enabled in the system that matched the crossing threshold level, ILOM would automatically generate an alert message to the alert destination defined.

## Obtain Sensor Readings Using the Web Interface

In the ILOM web interface, you can obtain instantaneous sensor readings about system FRUs (field-replaceable units) or other system inventory on the System Monitoring --> Sensor Readings page.

**FIGURE 7-1** Sensor Readings Page

Role (User): Administrator (root) SP Hostname: DamenRef

Sun™ Integrated Lights Out Manager

REFRESH LOG OUT

Java

Sun Microsystems, Inc.

**Sensor Readings**

View readings for system sensors. Click on a sensor name for more information, including threshold values.

Name	Type	Reading
/SYS/P0_PRSNT	Entity Presence	Present
/SYS/P1_PRSNT	Entity Presence	Present
/SYS/P2_PRSNT	Entity Presence	Present
/SYS/P3_PRSNT	Entity Presence	Present
/SYS/EM_0_PRSNT	Entity Presence	Absent
/SYS/EM_1_PRSNT	Entity Presence	Absent
/SYS/HDD0_PRSNT	Entity Presence	Absent
/SYS/HDD1_PRSNT	Entity Presence	Absent
/SYS/T_AMB	Temperature	29.000 degrees C
/SYS/P0T_AMB	Temperature	50.000 degrees C
/SYS/P1T_AMB	Temperature	54.000 degrees C
/SYS/P2T_AMB	Temperature	51.000 degrees C
/SYS/P3T_AMB	Temperature	61.000 degrees C
/SYS/V_0_+48V	Voltage	48.400 Volts
/SYS/V_1_+48V	Voltage	48.400 Volts
/SYS/V_2_+48V	Voltage	48.000 Volts
/SYS/P0V_VCORE	Voltage	1.344 Volts
/SYS/P0V_VTT	Voltage	0.896 Volts
/SYS/P0V_VDDIO	Voltage	1.784 Volts
/SYS/P1V_VCORE	Voltage	1.344 Volts
/SYS/P1V_VTT	Voltage	0.896 Volts
/SYS/P1V_VDDIO	Voltage	1.784 Volts
/SYS/P2V_VCORE	Voltage	1.358 Volts
/SYS/P2V_VTT	Voltage	0.896 Volts

The Sensor Readings page lists the readings for each sensor by name, type, and reading. For further information about a threshold sensor, click a threshold sensor name on the page to view other threshold properties. For example, if you clicked the threshold sensor name `/SYS/T_AMB`, the following dialog appears displaying additional information about this sensor.

**FIGURE 7-2** Sensor Properties Dialog for /SYS/T\_AMB



For more information about how to obtain sensor readings from the ILOM web interface, see [“Determine the State of Indicators Using the Web Interface” on page 147](#).

## Obtain Sensor Readings Using the CLI

In the ILOM CLI, you can obtain instantaneous sensor readings about system FRUs and other system inventory within the /SYS or /CH namespace. Both of these namespaces support two classes of sensor readings that you can access. These classes are known as *Threshold Sensor Readings* and *Discrete Sensor Readings*. A brief summary describing both of these classes follows.

### *Threshold Sensors*

Threshold sensors provide a sensor property value, as well as upper and lower non-critical and critical predefined thresholds. Threshold sensors typically include temperature readings, voltage readings, or fan readings.

To obtain sensor readings using the ILOM CLI, you must use the `cd` command to navigate to the sensor target then use the `show` command to display the sensor properties.

For example, on some server platforms, you can specify the following path to obtain a temperature reading of a server's intake:

```
cd /SYS/T_AMB  
  
show
```

The properties describing the sensor target appear. For example:

- Type = Sensor
- Class = Threshold Sensor
- Value = 32.000 degree C
- Upper = non-recov\_threshold = 80.00 degree C
- Upper critical\_threshold = 75.00 degree C
- Upper noncritical\_threshold = 70.00 degree C
- Lower non\_recov\_threshold = 0.00 degree C
- Lower critical\_threshold = 0.00 degree C
- Lower noncritical\_threshold = 0.00 degree C

For specific details about the type of threshold sensor targets you can access, as well as the paths to access them, consult the user documentation provided with the Sun server platform.

### *Discrete Sensors*

Discrete sensors offer a set of well-defined values associated with the sensor target. Discrete sensors typically provide information about an entity presence, entity fault, or a power supply state.

To obtain a discrete sensor reading using the ILOM CLI, you must use the `cd` command to navigate to the sensor target then use the `show` command to display the target properties. For example, on some Sun server platforms, you can determine whether a hard disk drive is present in slot 0 by specifying the following path:

```
cd /SYS/HDD0_PRSENT  
  
show
```

The properties describing the discrete sensor target appear. For example:

- Type = Entity Presence
- Class = Discrete Indicator
- Value = Present

For specific details about the type of discrete sensor targets you can access, as well as the paths to access them, consult the user documentation provided with the Sun server platform.

## Power Monitoring Interfaces

Power Monitoring interfaces enable monitoring of real-time power consumption. The service processor (SP) or individual power supply can be polled at any instance to retrieve and report data with accuracy to within one minute of the time the power usage occurred.

---

**Note** – The power management interfaces described in this section may or may not be implemented on the platform that you are using. See your ILOM platform-specific documentation for implementation details. You can find the ILOM platform-specific documentation within the documentation set for your system.

---

You can monitor available power, actual power, and permitted power. *Available power* is the maximum power that a system is capable of consuming. By default, this is a sum of the maximum power that each processor, I/O module, memory module, and other components is capable of consuming or the maximum power that the power supplies in the system can draw. Some systems may be able to guarantee a lower maximum consumption than the available power at any instant in time. This guaranteed maximum is referred to as *permitted power*.

*Actual power* consumption can be monitored for individual power supplies or for all power supplies in a chassis or rack. Actual power consumption can be measured on rackmounted servers, server modules (blade servers), and chassis monitoring modules (CMMs).

Power Monitoring interfaces enable you to perform the following tasks:

- View the total power that is pulled into the system's power supplies from an external source (actual power).
- View any raw sensors that measure voltage or current drawn by an individual power supply.
- View the maximum input power the power supplies are capable of consuming (available power).
- View maximum power consumption permitted by the system (permitted power).

# Power Monitoring Terminology

TABLE 7-1 defines the terminology used in power monitoring.

**TABLE 7-1** Power Management Terms

Term	Definition	Applies to CMM	Applies to Service Processor
Actual Power	The input power measured in watts. This is the actual power consumed by all the power supplies in the system.	Yes	Yes
Permitted Power	The maximum power that the server will permit to be used at any time.	Yes	Yes
Available Power	The input power capacity in watts. The definition of this term differs depending on whether you are using these interfaces with a rackmounted server or a server module. This is because rackmounted servers have their own power supplies; server modules do not. <ul style="list-style-type: none"><li>• On a rackmounted server, available power is defined as the sum of all the power that the power supplies can provide.</li><li>• On a server module, available power is defined as the amount of power the chassis is willing to provide to the server module.</li></ul>	Yes	Yes

## System Indicators

System indicator LEDs are generally illuminated on the system by ILOM based on the Sun server platform policy. Typically the system indicator LEDs are illuminated by ILOM when any of the following conditions occur:

- Fault or error is detected on a component.
- Field-replacement unit (FRU) requires service.
- Hot-plug module is ready for removal.
- Activity is occurring on FRU or system.

You can view the states of system indicators from the ILOM web interface or the ILOM CLI. Additionally, in some instances, you might be able to modify the state of a system indicator.

# Supported System Indicator States

ILOM supports the following system indicator states:

- **Off** – Normal operating status. Service is not required.
- **Steady On** – Component is ready for removal.
- **Slow Blink** – Component is changing state.
- **Fast Blink** – Helps locate system in a data center.
- **Standby Blink** – Component is ready for activation, but is not operational at this time.

## *Types of System Indicator States*

ILOM supports two types of system indicator states: *Customer Changeable* and *System Assigned*.

- **Customer Changeable States** – Some system indicator LEDs in ILOM offer customer changeable states. Typically, these types of system indicators provide operational states of various system components. The type of states presented is determined by the system indicator. For example, depending on the system indicator, the following customer changeable states might be present:

- **Off** – Normal operating status. Service is not required.
- **Fast Blink** – Helps locate system in a data center.

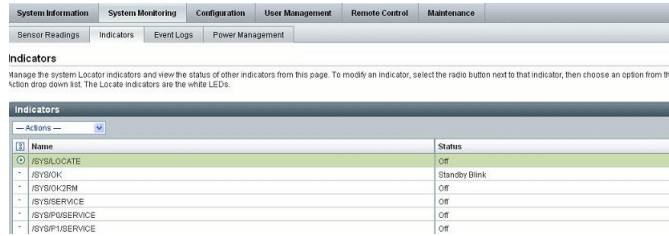
For more information about viewing and managing system indicators from the ILOM web interface or CLI, see [“View and Manage Indicators Using the Web Interface” on page 134](#) or [“View and Manage Indicators Using the CLI” on page 135](#).

- **System Assigned States** – System assigned indicators are *not* customer configurable. These types of system indicators provide ready-only values about the operational state of a component. On most Sun server platforms, system assigned indicators are *Service Action Required LEDs*. These types of LEDs are typically illuminated when any of the following conditions are detected:
  - Fault or error is detected on a system component.
  - Hot-plug module is ready for removal.
  - Field-replacement unit (FRU) requires service.

# View and Manage Indicators Using the Web Interface

In the ILOM web interface, you view and manage system indicators on the Indicators page. This page lists the system indicators by name and status. System indicators offering customer changeable states appear with a radio button. To modify a customer changeable indicator state, select the radio button then select a state from the Actions drop-down list.

**FIGURE 7-3** Indicators Page



For more information about how to obtain instantaneous sensor readings using the ILOM web interface, see [“Obtain Sensor Readings Using the Web Interface”](#) on page 148.



## View and Manage Indicators Using the CLI

In the ILOM CLI, all system indicators are accessible in the `/SYS` or `/CH` namespace. Typically you will use the `cd` command to navigate to the system indicator target then the `show` command to view the target's properties. You can change the state of a system indicator by using the `set` command. The `set` command is only supported for system indicators offering a customer changeable state. To determine whether you can change the state of a system indicator, use the `cd` command to navigate to the indicator target, then use the `show` command to view the system indicator properties. For example:

```
cd /SYS/indicator_target or cd /CH/indicator_target
```

```
show
```

Targets, properties, and commands associated with the system indicator appear, for example:

```
Targets:
Properties:
  Type = indicator
  Value = Off
Commands:
  cd
  set
  show
```

If the `set` command appears in the `Commands` list, you can modify the state of the system indicator. To modify the state of the system indicator, use the following syntax:

```
set value=state_name
```

For more information about which system indicators are supported on your system, and the paths for accessing them, consult the user documentation provided with the Sun server platform.

# ILOM Event Log

The ILOM event log enables you to view information about any event that occurred on the system. Some of these events can include ILOM configuration changes, software events, warnings, alerts, component failure, as well as IPMI events. The type of events recorded in the ILOM event log is determined by the Sun server platform. For specific information about which events are recorded in the ILOM event log, consult the user documentation provided with the Sun server platform.

You can view and manage the ILOM event log from either the ILOM web interface or CLI. For more information about how to view and manage the ILOM event log, see [“View or Clear the ILOM Event Log Using the Web Interface”](#) on page 148 or [“View or Clear the ILOM Event Log Using the CLI”](#) on page 150.

**FIGURE 7-4** ILOM Event Log Example

Event ID	Class	Type	Severity	Date/Time	Description
1570	Audit	Log	minor	Wed May 9 08:49:00 2007	root: Open Session: object= /sessionType : value = www: success
1569	Audit	Log	minor	Wed May 9 08:44:50 2007	root: Close Session: object= /sessionType : value = www: success
1568	Audit	Log	minor	Wed May 9 08:28:46 2007	root: Open Session: object= /sessionType : value = www: success
1567	Audit	Log	minor	Wed May 9 08:22:50 2007	root: Close Session: object= /sessionType : value = www: success
1566	Audit	Log	minor	Wed May 9 07:58:44 2007	root: Open Session: object= /sessionType : value = www: success
1565	Audit	Log	minor	Wed May 9 06:51:02 2007	root: Close Session: object= /sessionType : value = www: success
1564	Audit	Log	minor	Wed May 9 06:30:58 2007	root: Open Session: object= /sessionType : value = www: success
1563	Audit	Log	minor	Wed May 9 05:55:22 2007	root: Close Session: object= /sessionType : value = www: success
1562	Audit	Log	minor	Wed May 9 05:39:19 2007	root: Open Session: object= /sessionType : value = www: success
1561	Audit	Log	minor	Wed May 9 05:23:17 2007	root: Close Session: object= /sessionType : value = www: success
1560	Audit	Log	minor	Wed May 9 05:07:11 2007	root: Open Session: object= /sessionType : value = www: success
1559	Audit	Log	minor	Wed May 9 04:53:52 2007	root: Close Session: object= /sessionType : value = www: success
1558	Audit	Log	minor	Wed May 9 04:42:09 2007	root: Open Session: object= /sessionType : value = www: success
1557	Audit	Log	minor	Tue May 8 14:57:07 2007	root: Open Session: object= /sessionType : value = shell: success
1556	Audit	Log	minor	Tue May 8 14:55:55 2007	root: Close Session: object= /sessionType : value = shell: success
1555	Audit	Log	minor	Tue May 8 14:54:58 2007	root: Open Session: object= /sessionType : value = shell: success
1554	Audit	Log	minor	Tue May 8 14:53:47 2007	root: Close Session: object= /sessionType : value = shell: success
1553	Audit	Log	minor	Tue May 8 14:51:00 2007	root: Open Session: object= /sessionType : value = shell: success
1552	Audit	Log	minor	Tue May 8 14:50:01 2007	root: Close Session: object= /sessionType : value = shell: success
1551	Audit	Log	minor	Tue May 8 14:49:50 2007	root: Open Session: object= /sessionType : value = shell: success
1550	Audit	Log	minor	Tue May 8 14:49:12 2007	root: Close Session: object= /sessionType : value = shell: success
1549	Audit	Log	minor	Tue May 8 14:48:14 2007	root: Open Session: object= /sessionType : value = shell: success
1548	Audit	Log	minor	Tue May 8 14:46:07 2007	root: Close Session: object= /sessionType : value = shell: success

## Event Log Timestamps and ILOM Clock Settings

ILOM captures timestamps in the event log based on the host server UTC/GMT timezone. However, if you view the event log from a client system that is located in a different timezone, the timestamps are automatically adjusted to the timezone of the client system. Therefore, a single event in the ILOM event log might appear with two timestamps.

## Supported Clock Settings

In ILOM, you can choose to manually configure the ILOM clock based on the UTC/GMT timezone of the host server, or you can choose to synchronize the ILOM clock with other systems on your network by configuring the ILOM clock with an NTP server IP address.

## View or Set Clock Settings Using the Web Interface

You can view or set the ILOM clock settings in the ILOM web interface on the Configuration --> Clock Settings page.

**FIGURE 7-5** Clock Settings Page

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

System Management Access | Alert Management | Network | Serial Port | **Clock Settings** | Syslog | SMTP Client | Policy

**Clock Settings**

To set the Service Processor clock manually, type the date in the format mm/dd/yyyy, then select the hour and minute. To synchronize the Service Processor clock with an NTP server, select the Enable check box, then type the IP addresses of the NTP servers to use.

Date:

Time:

Synchronize Time Using NTP:  Enabled

Server 1:

Server 2:

For more information about how to view and set clock settings from the ILOM web interface, see [“View and Configure Clock Settings Using the Web Interface”](#) on page 152.

## View and Set Clock Settings Using the CLI

You can view the ILOM clock settings from the ILOM CLI by using the `show` command. For example, on some server platforms, you can display the clock setting by specifying the following path:

```
show /SP/clock
```

You can manually configure the ILOM clock setting from the CLI using the following `set` command syntax:

```
set target property_name=value
```

You can also, in the ILOM CLI, configure the ILOM clock settings to synchronize with other systems on your network by setting an IP address of an NTP server. For example, on some Sun server platforms, you could type the following path to set the IP address of an NTP server, and then enable NTP synchronization.

- Set NTP server IP address example:

```
set /SP/clients/ntp/server/1 address=ip_address
```

- Enable synchronization example:

```
set /SP/clock usentpserver=enabled
```

For more information about how to configure the ILOM clock settings from the ILOM CLI, consult the user documentation provided with the Sun server platform.

In addition, consult your Sun server platform user documentation for platform specific clock information about whether:

- The current time in ILOM persists across reboots of the SP.
- The current time in ILOM can be synchronized with the host at host boot time.
- There is a real-time clock element that stores the time.

## Syslog Information

Syslog is a standard logging facility used in many environments. Syslog defines a common set of features for logging events and also a protocol for transmitting events to a remote log host. You can use syslog to combine events from multiple instances of ILOM within a single place. The log entry contains all the same information that you would see in the local ILOM event log, including class, type, severity, and description. For information about configuring ILOM to send syslog to one or two IP addresses, see [“Configure Remote Syslog Receiver IP Addresses Using the Web Interface” on page 153](#) or [“Configure Remote Syslog Receiver IP Addresses Using the CLI” on page 154](#).

# Fault Management

Most Sun server platforms include the fault management software feature in ILOM. This feature enables you to proactively monitor the health of your system hardware, as well as diagnose hardware failures as they occur. In addition to monitoring the system hardware, the fault management software monitors environmental conditions and reports when the system's environment is outside acceptable parameters. Various sensors on the system components are continuously monitored. When a problem is detected, the fault management software automatically:

- Illuminates the Server Action Required LED on the faulted component.
- Updates the ILOM management interfaces to reflect the fault condition.
- Records information about the fault in the ILOM event log.

You can view the status of faulted components from the ILOM web interface or ILOM CLI. For more information, see:

- [“View Fault Status Using the Web Interface” on page 140](#)
- [“View Fault Status Using the CLI” on page 141.](#)

The type of system components and environmental conditions monitored by the fault management software are determined by the Sun server platform. For more details about which components are monitored by the fault management software, consult the user documentation provided with the Sun server platform.

---

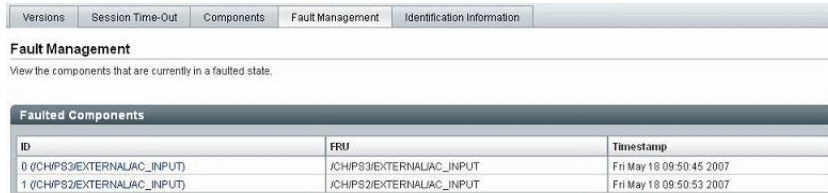
**Note** – The ILOM fault management feature is currently available on some Sun server platforms. Refer to your platform ILOM Supplement or other platform documentation to determine whether your platform supports the ILOM fault management features.

---

## View Fault Status Using the Web Interface

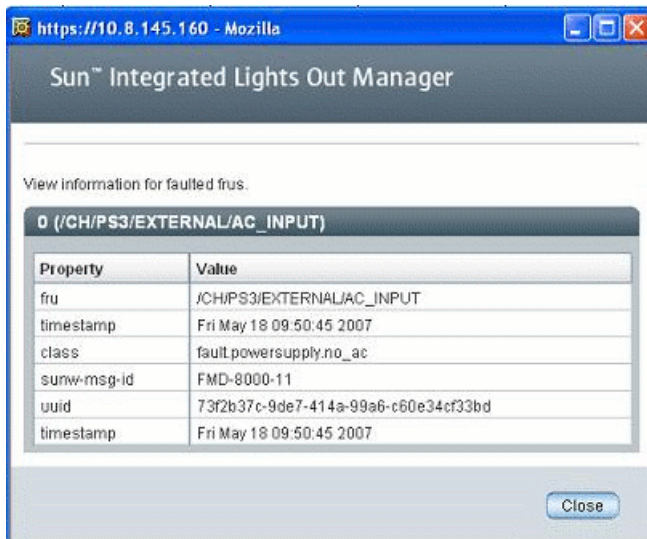
In the ILOM web interface, you can view the system components currently in a fault state using the Fault Management page.

**FIGURE 7-6** Fault Management Page Example



ID	FRU	Timestamp
0 (/CH/PS3/EXTERNAL/AC_INPUT)	/CH/PS3/EXTERNAL/AC_INPUT	Fri May 18 09:50:45 2007
1 (/CH/PS2/EXTERNAL/AC_INPUT)	/CH/PS2/EXTERNAL/AC_INPUT	Fri May 18 09:50:53 2007

The Fault Management page lists faulted components by ID, FRU, and TimeStamp. You can access additional information about the faulted component by clicking the faulted component ID. For example, if you clicked the faulted component ID 0 (CH/PS3/EXTERNAL/AC\_INPUT), the following dialog appears displaying additional details about the faulted component.



Alternatively, in the ILOM web interface, you can identify the fault status of a component on the Component Management page.

**FIGURE 7-7** Component Management Page - Fault Status

Component Management Status			
Component Name	Type	Ready to Remove Status	Fault Status
/	Container	-	OK
/SYS	Host System	-	OK
/SYS/BIOS	BIOS	-	-
/SYS/SP0	Host Processor	-	OK
/SYS/SP0D0	DIMM	-	OK
/SYS/SP0D1	DIMM	-	OK
/SYS/SP1	Host Processor	-	OK
/SYS/SP2	Host Processor	-	OK
/SYS/SP3	Host Processor	-	OK
/SYS/HDD0	Hard Disk	-	OK

For more information about the ILOM fault management features offered on your system, consult the user documentation provided with the Sun server platform.

## View Fault Status Using the CLI

In the ILOM CLI, you can view the fault status of component(s) by using the `show` command. For example, depending on the Sun server platform, you can specify one of the following paths:

```
show /SP/faultmgmt
```

```
show /CH/faultmgmt
```

In addition, the alias, `show faulty`, is a shortcut for the following ILOM command-line interface (CLI) command string:

```
-> show -o table -level all /SP/faultmgmt
```

The alias produces the same output as the above command. Thus, it enables you to view all active faults in the system in a concise, tabular form. For example, it produces output similar to the following:

```
-> show faulty
Target          | Property      | Value
-----+-----+-----
/SP/faultmgmt/0 | fru          | /SYS/MB
/SP/faultmgmt/0 | timestamp    | Jan 16 12:53:00
/SP/faultmgmt/0/ | sunw-msg-id  | NXGE-8000-0U
faults/0        |              |
/SP/faultmgmt/0/ | uuid         | e19f07a5-580e-4ea0-ed6a-f663aa61
faults/0        |              | 54d5
/SP/faultmgmt/0/ | timestamp    | Jan 16 12:53:00
faults/0        |              |
```

For more information about the ILOM fault management features offered on your system, consult the user documentation provided with the Sun server platform.

## ILOM Service Snapshot Utility

---

**Note** – The Service Snapshot utility is supported only on x64-based systems running ILOM 2.x. The Service Snapshot utility is not supported on SPARC-based systems running ILOM 2.x.

---

The ILOM Service Snapshot utility gathers SP state data. The utility collects log files, runs various commands and collects their output, and sends the data collection as a downloaded file to a user-defined location.

This utility enables you to produce a snapshot of the SP at any instant in time and you can run the utility using either the ILOM command-line interface (CLI) or the ILOM web interface. The CLI and web interface procedures follow.

**Note** – The purpose of the ILOM Service Snapshot utility is to collect data for use by Sun Services to diagnose problems. Customers should not run this utility unless requested to do so by Sun Services.

---

You can access the ILOM Service Snapshot utility from either the web interface or the CLI. For more information, see:

- [“Run the Snapshot Utility Using the CLI” on page 155](#)
- [“Run the Snapshot Utility Using the Web Interface” on page 156](#)

---

## Monitor System Power, Sensors, Indicators, and ILOM Event Log

Refer to the following procedures to monitor system sensors, system indicators, as well as events in the ILOM event log.

- [“Monitor System Total Power Consumption Using the CLI” on page 143](#)
- [“Monitor System Actual Power Using the CLI” on page 144](#)
- [“Monitor Individual Power Supply Consumption Using the CLI” on page 145](#)
- [“Monitor Available Power Using the CLI” on page 146](#)
- [“Monitor Permitted Power Consumption Using the CLI” on page 146](#)



- “Determine the State of Indicators Using the Web Interface” on page 147
- “Obtain Sensor Readings Using the Web Interface” on page 148
- “View or Clear the ILOM Event Log Using the Web Interface” on page 148
- “View or Clear the ILOM Event Log Using the CLI” on page 150
- “View and Configure Clock Settings Using the Web Interface” on page 152
- “Configure Remote Syslog Receiver IP Addresses Using the Web Interface” on page 153
- “Configure Remote Syslog Receiver IP Addresses Using the CLI” on page 154

## ▼ Monitor System Total Power Consumption Using the CLI

This interface enables you to view the total power that is pulled into the system’s power supplies from an external source. This is the power that the customer pays for. The power source can be either AC or DC.

- On a rackmounted server, this is the input power consumed by the server.
- On a server module, this is the input power consumed by the server module. It does not include the power consumed by the shared components.
- On a chassis monitoring module (CMM), this is the input power consumed by the entire chassis or shelf—all server modules, network express modules (NEMs), fans, and other components.

The Power Consumption sensor supports the `show` command.

### Syntax

**show** *target property*

To view total power consumption using the CLI, follow these steps:

1. **Log in to the ILOM CLI as Administrator.**
2. **Type the `show` command to display the total power consumption.**

For example:

```
-> show /SYS/VPS
```

```
-> show /SYS/VPS property
```

TABLE 7-2 lists and describes the properties of the Total Power Consumption sensor for the CLI.

**TABLE 7-2** Power Consumption Sensor Properties for CLI

Property	Value
type	Power Unit
class	Threshold Sensor
value	Total consumed power in watts
upper_nonrecov_threshold	100% of /SP/powermgmt available_power
upper_critical_threshold	90% of /SP/powermgmt available_power
upper_noncritical_threshold	80% of /SP/powermgmt available_power
lower_noncritical_threshold	NA
lower_critical_threshold	NA
lower_nonrecov_threshold	NA

**Note** – All platforms support the /SYS/VSP sensor to report power consumption. However, the threshold properties are platform specific. Your system might not support all the thresholds listed in TABLE 7-2 for this sensor. Therefore, some platforms might not receive an event if an unsupported threshold is crossed. Refer to your platform ILOM Supplement for your platform-specific information.

In addition to the properties listed in TABLE 7-2, the total power consumption property `actual_power` can be accessed using the /SP/powermgmt target using the `show` command. The `actual_power` property is the same as /SYS/VPS in that /SYS/VPS is a sensor that has a threshold and `actual_power` is just the value returned by the sensor.

## ▼ Monitor System Actual Power Using the CLI

To use the `actual_power` property to view total power consumption using the CLI, follow these steps:

1. **Log in to the ILOM CLI as Administrator.**
2. **Type the `show` command to display the total power consumption.**

For example:

```
-> show /SP/powermgmt actual_power
```

## ▼ Monitor Individual Power Supply Consumption Using the CLI

This interface enables you to access any raw sensors that measure voltage or current drawn by an individual power supply. In addition, virtual sensors that represent the power supply "input power" (power consumed from an external AC or DC source) and "output power" (power drawn by the system's components) can be accessed.

For the CLI, each power supply contains the following sensors:

- INPUT\_POWER
- OUTPUT\_POWER

All sensors support the `show` command.

### Syntax

**show** *target property*

To monitor total power consumption per power supply using the CLI, follow these steps:

1. **Log in to the ILOM CLI as Administrator.**
2. **Type the `show` command to display the total power consumption. For example:**
  - > **`show /SYS/PS1 INPUT_POWER|OUTPUT_POWER`** (for CLI on rackmounted systems)
  - > **`show /CH/PS1 INPUT_POWER|OUTPUT_POWER`** (for CLI on CMM)

TABLE 7-3 lists and describes the properties of the CLI sensors. Both sensors, INPUT\_POWER and OUTPUT\_POWER, have the same properties.

**TABLE 7-3** Individual Power Supply Consumption Sensor Properties

Property	Value
type	Power Unit
class	Threshold Sensor
value	<total consumed power in watts, for example, "1400">
upper_nonrecov_threshold	N/A
upper_critical_threshold	N/A
upper_noncritical_threshold	N/A

**TABLE 7-3** Individual Power Supply Consumption Sensor Properties (Continued)

Property	Value
lower_noncritical_threshold	N/A
lower_critical_threshold	N/A
lower_nonrecov_threshold	N/A

## ▼ Monitor Available Power Using the CLI

This interface enables you to view available power. On a server module, this is the amount of power guaranteed available to the server module by the chassis.

The system contains one property: `available_power`. The property supports the `show` command and returns the value `<input available power in watts>`.

### Syntax

**show** *target* *property*

To view total available power using the CLI, follow these steps:

1. **Log in to the ILOM CLI as Administrator.**
2. **Type the `show` command to display the available power.**

For example:

```
-> show /SP/powermgmt available_power (for rackmounted systems)
```

```
-> show /CMM/powermgmt available_power (for CMM)
```

## ▼ Monitor Permitted Power Consumption Using the CLI

This interface enables you to view permitted power consumption. The permitted power consumption is the maximum input power the server guarantees it will consume at any instant. This value cannot be changed directly, but can change based on the power policy and budget, and chassis available power.

The system contains one property: `permitted_power`. This property supports the `show` command and returns the value `<maximum permitted power consumption in watts>`.

## Syntax

**show** *target property*

To monitor permitted power consumptions using the CLI, follow these steps:

1. **Log in to the ILOM CLI as Administrator.**
2. **Type the `show` command to display the permitted power consumption.**

For example:

-> **show /SP/powermgmt permitted\_power** (for rackmounted systems)

-> **show /CMM/powermgmt permitted\_power** (for CMM)

## ▼ Determine the State of Indicators Using the Web Interface

Follow these steps to determine the state of system indicators from the ILOM web interface:

1. **Open a web browser and type the IP address of the server SP or CMM.**

The Login page for the ILOM web interface appears.

2. **In the ILOM Login page, enter a user name and password then click OK.**

The ILOM web interface appears.

3. **In the web interface page, select System Monitoring --> Indicators.**

The Indicators page appears.

---

**Note** – If the server is powered off, many indicators will appear as “no reading.”

---

4. **In the Indicators page, do the following:**

- a. **Locate the name of the indicator you want to view.**

- b. **To toggle the state of an indicator, click the radio button associated with the indicator that you want to toggle, then click the Actions drop-down list box and select either Turn LED Off or Set LED to Fast Blink.**

A dialog appears prompting you to confirm the change.

- c. **Click OK to confirm the change.**

## ▼ Obtain Sensor Readings Using the Web Interface

Follow these steps to obtain sensor readings from the ILOM web interface:

- 1. Open a web browser and type the IP address of the server SP or CMM.**  
The Login page for the ILOM web interface appears.
- 2. In the ILOM Login page, enter a user name and password then click OK.**  
The ILOM web interface appears.
- 3. In the web interface page, click System Monitoring --> Sensors Readings.**  
The Sensor Readings page appears.

---

**Note** – If the server is powered off, many components will appear as “no reading.”

---

- 4. In the Sensor Readings page, do the following:**
  - a. Locate the name of the sensor you want to view.**
  - b. Click the name of the sensor to view the property values associated with that sensor.**

For specific details about the type of discrete sensor targets you can access, as well as the paths to access them, consult the user documentation provided with the Sun server platform.

## ▼ View or Clear the ILOM Event Log Using the Web Interface

Follow these steps to view or clear events in the ILOM event log using the ILOM web interface:

- 1. Open a web browser and type the IP address of the server SP or CMM.**  
The Login page for the ILOM web interface appears.
- 2. In the ILOM Login page, enter a user name and password then click OK.**  
The ILOM web interface appears.
- 3. In the web interface page, select System Monitoring --> Event Logs.**  
The Event Log page appears.
- 4. In the Event Log page, perform any of the following:**

- **Page through entries** – Use the page navigation controls at the top and the bottom of the table to navigate forward and back through the available data in the table.

Note that selecting a larger number of entries might cause the web interface to respond slower than selecting a smaller number of entries.

- **View the entries in the display by scrolling through the list** – The following table provides descriptions about each column appearing in the log.

Column Label	Description
Event ID	The number of the event, in sequence from number 1.
Class/Type	<ul style="list-style-type: none"> <li>• Audit/ Log – Commands that result in a configuration change. Description includes user, command, command parameters, and success/fail.</li> <li>• IPMI/Log – Any event that is placed in the IPMI SEL is also put in the management log.</li> <li>• Chassis/State – For changes to the inventory and general system state changes.</li> <li>• Chassis/Action – Category for shutdown events for server module/chassis, hot insert/removal of a FRU, and Reset Parameters button pushed.</li> <li>• FMA/Fault – For Fault Management Architecture (FMA) faults. Description gives time of fault as detected by FMA and suspect component.</li> <li>• FMA/Repair – For FMA repairs. Description gives component.</li> </ul>
Severity	Critical, Major, or Minor.
Date/Time	The day and time the event occurred. If the Network Time Protocol (NTP) server is enabled to set the ILOM time, the ILOM clock will use Universal Coordinated Time (UTC).
Description	A description of the event.

- **Clear the event log** – To clear the event log, click the Clear Event Log button. A confirmation dialog appears. In the confirmation dialog, click OK to clear the entries.

---

**Note** – The ILOM event log accumulates many types of events, including copies of IPMI entries. Clearing the ILOM event log will clear all entries in the log, including the IPMI entries. However, clearing the ILOM event log entries will not clear the actual entries posted directly to an IPMI log.

---

## ▼ View or Clear the ILOM Event Log Using the CLI

Follow these steps to view or clear events in the system event log using the ILOM CLI:

1. Establish a local serial console connection or SSH connection to the server SP or CMM:

- Local Serial Console Connection

Attach a serial console to the serial port on the server or CMM.

For more information, consult the user documentation provided with the Sun server platform.

or

- Remote - Secure Shell (SSH) Connection

Establish a Secure Shell connection to the server SP or CMM.

From the remote client, establish a secure connection as root to the server SP or active CMM.

For example, you can establish a secure connection from a remote SSH client to the server SP by typing the following:

```
ssh -l root server_ip_address
```

Password: **changeme**

The default command prompt appears (->).

2. Type one of the following command paths to set the working directory:

- For a rackmount server SP: **cd /SP/logs/event**

- For a blade server SP in chassis: **cd /CH/BLn/SP/logs/event**

- For a CMM: **cd /CMM/logs/event**

3. Type the following command path to display the event log list.

```
show list
```

The contents of the event log appears. An example follows.

ID	Date/Time	Class	Type	Severity
1522	Sun Jul 30 01:11:36 2006	Audit	Log	minor
	root : Close Session : object = /session/type : value = www : success			
1521	Sun Jul 30 01:05:34 2006	Audit	Log	minor
	root : Close Session : session ID = 1307912184 : success			



#### 4. In the event log, perform any of the following tasks:

- **Scroll down the list to view entries** – Press any key except ‘q’. The following table provides descriptions about each column appearing in the log.

---

Column Label	Description
Event ID	The number of the event, in sequence from number 1.
Class/Type	<ul style="list-style-type: none"><li>• Audit/ Log – Commands that result in a configuration change. Description includes user, command, command parameters, and success/fail.</li><li>• IPMI/Log – Any event that is placed in the IPMI SEL is also put in the management log.</li><li>• Chassis/State – For changes to the inventory and general system state.</li><li>• Chassis/Action – Category for shutdown events for server module/chassis, hot insert/removal of a FRU, and Reset Parameters button pushed.</li><li>• FMA/Fault – For Fault Management Architecture (FMA) faults. Description gives time of fault as detected by FMA and suspect component.</li><li>• FMA/Repair – For FMA repairs. Description gives component.</li></ul>
Severity	Critical, Major, or Minor
Date/Time	The day and time the event occurred. If the Network Time Protocol (NTP) server is enabled to set the ILOM time, the ILOM clock will use Universal Coordinated Time (UTC).
Description	A description of the event.

---

- **Dismiss the event log (stop displaying the log)** – Press the ‘q’ key.
- **Clear entries in the event log** – Perform these steps:

**a. Type: `set clear=true`**

A confirmation message appears.

**b. Type one of the following:**

- To clear the entries. Type: **y**.
- To cancel clearing the log. Type: **n**.

---

**Note** – The ILOM event log accumulates many types of events, including copies of IPMI entries. Clearing the ILOM event log will clear all entries in the log, including the IPMI entries. However, clearing the ILOM event log entries will not clear the actual entries posted directly to an IPMI log.

---

## ▼ View and Configure Clock Settings Using the Web Interface

You need the IP address of your NTP servers to complete this procedure.

- 1. Open a web browser and type the IP address of the server SP or CMM.**  
The Login page for the ILOM web interface appears.
- 2. In the ILOM Login page, enter a user name and password then click OK.**  
The ILOM web interface appears.
- 3. In the web interface page, click Configuration --> Clock Settings.**  
The Clock Settings page appears.
- 4. In the clock settings page, do one of the following:**
  - View the existing settings.
  - Manually configure the date and time of the host server SP:
    - a. In the Date text box, type the date in the format mm/dd/yy.**
    - b. In the Time drop-down list boxes, set the hour and minutes.**
  - Configure an IP address of an NTP server and enable synchronization.
    - a. Select the Enabled check box next to Synchronize Time Using NTP.**
    - b. In the Server 1 text box, type the IP address of the primary NTP server you want to use.**
    - c. (Optional) In the Server 2 text box, type the IP address of the secondary NTP server you want to use.**
- 5. Click Save for your changes to take effect.**

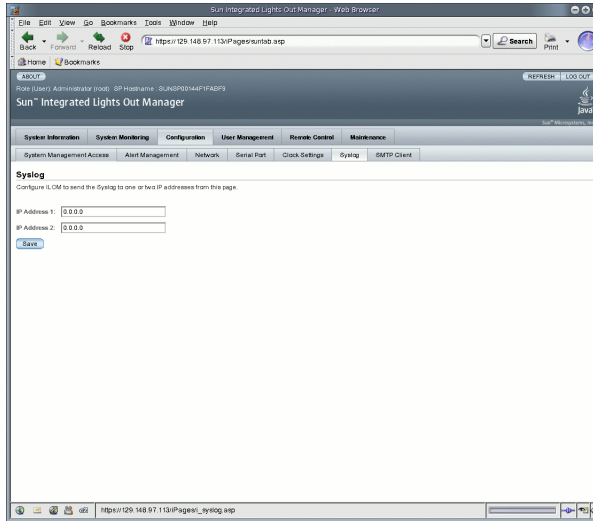
## ▼ Configure Remote Syslog Receiver IP Addresses Using the Web Interface

Follow these steps to configure a remote syslog receiver IP address in ILOM using the web interface.

- 1. Open a web browser and type the IP address of the server SP or CMM.**  
The Login page for the ILOM web interface appears.
- 2. In the ILOM Login page, enter a user name and password then click OK.**  
The ILOM web interface appears.

3. In the ILOM web interface, select Configuration --> Syslog.  
The Syslog page appears.

**FIGURE 7-8** Syslog Page



4. In the IP Address 1 and 2 fields, type the IP addresses for the two locations to which you want to send syslog data.
5. Click Save for your settings to take effect.

## ▼ Configure Remote Syslog Receiver IP Addresses Using the CLI

Follow these steps to configure a remote syslog receiver IP address using the CLI:

### 1. Establish a local serial console connection or SSH connection to the server SP or CMM:

#### ■ Local Serial Console Connection

Attach a serial console to the serial port on the server or CMM.

For more information, consult the user documentation provided with the Sun server platform.

or

#### ■ Remote - Secure Shell (SSH) Connection

Establish a Secure Shell connection to the server SP or CMM.

From the remote client, establish a secure connection as root to the server SP or active CMM.

For example, you can establish a secure connection from a remote SSH client to the server SP by typing the following:

```
ssh -l root server_ip_address
```

Password: **changeme**

The default command prompt appears (->).

### 2. Type one of the following command paths to set the working directory:

■ For a rackmount server SP: **cd /SP/clients/syslog**

■ For a blade server SP in chassis: **cd /CH/BLn/SP/clients/syslog**

■ For a CMM: **cd /CMM/clients/syslog**

### 3. Type the `show` command to display the syslog properties.

The properties appear. For example, accessing the syslog properties for the first time on an SP would appear as follows:

```
/SP/clients/syslog
Targets:
Properties:
  destination_ip1 = 0.0.0.0
  destination_ip2 = 0.0.0.0
Commands:
  cd
  set
  show
```

4. Use the `set` command to identify a destination IP address for IP 1 (and, if applicable, IP 2).

For example to set an IP destination to IP address 11.222.33.4, you would type:

```
set destination_ip1=111.222.33.4
```

5. Press Enter for the setting to take effect.

The results of setting the IP address appear. For example, if you set the destination IP address to 111.222.33.4, the following would appear:

```
Set 'destination_ip1' to '111.222.33.4'
```

## ▼ Run the Snapshot Utility Using the CLI

---

**Note** – The ILOM Service Snapshot utility is supported only on x64-based systems running ILOM 2.x. The Service Snapshot utility is not supported on SPARC-based systems running ILOM 2.x

---

To run the ILOM Service Snapshot utility using the CLI:

1. Log in to CLI as Administrator or Operator. For example:

```
ssh -l root server_ip_address  
Password: password
```

## 2. Type these commands:

```
->set /SP/diag/snapshot/dataset=data  
->set /SP/diag/snapshot/dump_uri=URI
```

Where *data* and *URI* are one of the following:

Variable	Option	Description
<i>data</i>	normal	Specifies that ILOM, operating system, and hardware information is to be collected.
	full	Specifies that all data is to be collected ("full" collection). <b>Note</b> - Using this option may reset the running host.
	normal-logonly or full- logonly	Specifies that only log files are to be collected.
<i>URI</i>	Any valid target directory location	Specifies the URI of the target directory. The URI format is as follows: protocol://username:password@host/directory For example, to store the snapshot information in the directory named <i>data</i> on the host, define the <i>URI</i> as follows: ftp://joe:mypasswd@host_IP_address/data The directory <i>data</i> is relative to the user's login, so the directory would probably be /home/joe/data.

## ▼ Run the Snapshot Utility Using the Web Interface

---

**Note** – The ILOM Service Snapshot utility is supported only on x64-based systems running ILOM 2.x. The Service Snapshot utility is not supported on SPARC-based systems running ILOM 2.x

---

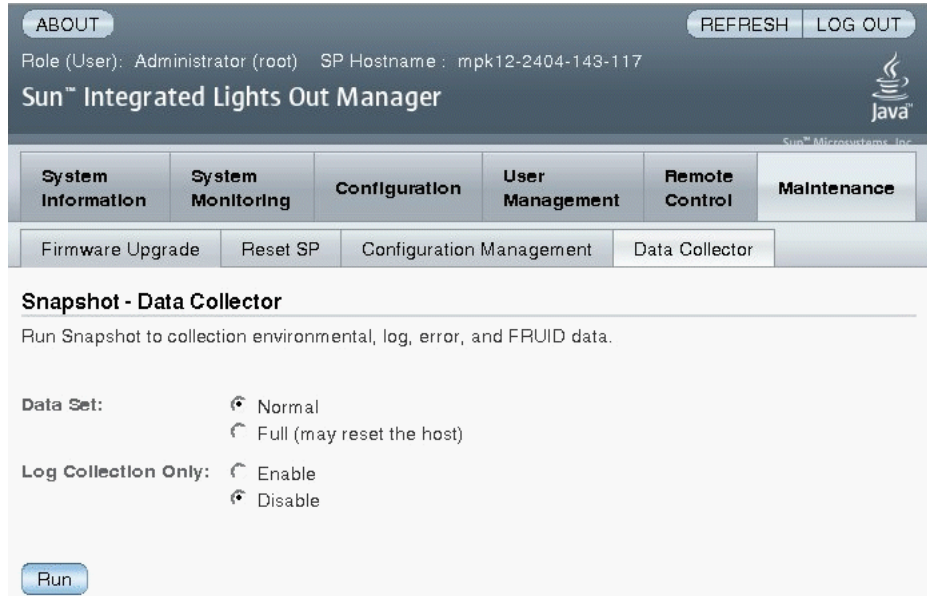
To run the ILOM Service Snapshot utility using the web interface:

1. **Open a browser window and type the IP address of the server SP or CMM.**  
The Login page for the ILOM web interface appears.
2. **In the ILOM Login page, enter a user name and password then click OK.**  
The ILOM web interface appears.

**3. Select the Maintenance --> Data Collector tabs.**

The Data Collector window appears (see [FIGURE 7-9](#).)

**FIGURE 7-9** Snapshot Data Collector Window



**4. Select the desired Data Set radio button: Normal or Full.**

Note that selecting Full may reset the system.

**5. Select the desired Log Collection Only radio button: Enable or Disable.**

**6. Click Run.**

A Save As dialog box appears.

**7. In the dialog box, specify the directory to which to save the file and the file name.**

**8. Click OK.**

The file is saved to the specified directory.

---

# About Alert Management

Alerts provide advance warning of possible system failures. Each Sun server platform is equipped with a number of sensors that measure voltages, temperatures, and other service-related attributes about the system. ILOM automatically polls these sensors and posts any events crossing a threshold to a ILOM event log, as well as generates alert message(s) to one or more customer-specified alert destinations.



---

**Caution** – ILOM tags all events or actions with LocalTime=GMT (or UTC). Browser clients show these events in LocalTime. This can cause apparent discrepancies in the event log. When an event occurs in ILOM, the event log shows it in UTC, but a client would show it in LocalTime. For more information about ILOM timestamps and clock settings, see [“Event Log Timestamps and ILOM Clock Settings” on page 136](#).

---

## Alert Rule Configuration

In ILOM you can configure up to 15 alert rules using the ILOM web interface or CLI. For each alert rule you configure in ILOM, you must define three or more properties about the alert depending on the alert type.

The *alert type* defines the messaging format and the method for sending and receiving an alert message. ILOM supports these three alert types:

- IPMI PET alerts
- SNMP Trap alerts
- Email Notification alerts

All Sun server platforms support all three alert types with the exception of the Sun Chassis Monitoring Module (CMM). The Sun Chassis Monitoring Module supports SNMP Trap alerts and Email Notification alerts but it does not currently support IPMI PET alerts.

A brief discussion about each alert type, as well as the other properties you can use to define an alert rule is discussed further in the following section, [“Alert Rule Property Definitions” on page 159](#).



## Alert Rule Property Definitions

ILOM offers up to five property values for defining an alert rule, they are as follows:

- Alert Type
- Alert Level
- Alert Destination
- SNMP Version (*SNMP Trap alerts only*)
- SNMP Community Name or User Name (*SNMP Trap alerts only*)

For more information about each of these property values, see [TABLE 7-4](#).

**TABLE 7-4** Properties for Defining Alert Rules

Property Name	Requirement	Description
Alert Type	Mandatory	<p>The alert type property specifies the message format and the delivery method that ILOM will use when creating and sending the alert message. You can choose to configure one of the following alert types:</p> <ul style="list-style-type: none"><li>• <b>IPMI PET Alerts.</b> IPMI Platform Event Trap (PET) alerts are supported on all Sun server platforms and modules, with the exception of a Sun Chassis Monitoring Module (CMM). For each IPMI PET alert you configure in ILOM, you must specify an IP address for an alert destination and one of four supported alert levels. Note that the alert destination specified must support the receipt of IPMI PET messages. If the alert destination does not support the receipt of IPMI PET messages, the alert recipient will not be able to decode the alert message.</li><li>• <b>SNMP Trap Alerts.</b> ILOM supports the generation of SNMP Trap alerts to a customer-specified IP destination. All destinations specified must support the receipt of SNMP Trap messages. Note that SNMP Trap alerts are supported on rackmount servers and blade server modules.</li><li>• <b>Email Notification Alerts.</b> ILOM supports the generation of Email Notification alerts to a customer-specified email address. To enable the ILOM client to generate Email Notification alerts, ILOM initially requires you to configure the name of the outgoing SMTP email server that would be sending the email alert messages. For more information, see <a href="#">“Enable SMTP Client Using the Web Interface” on page 170</a>.</li></ul>
Alert Destination	Mandatory	<p>The alert destination property specifies where to send the alert message. The alert type determines which destination you can choose to send an alert message. For example, IPMI PET and SNMP Trap alerts must specify an IP address destination. Email Notification alerts must specify an email address. If the proper format is not entered for an alert destination, ILOM will report an error.</p>

**TABLE 7-4** Properties for Defining Alert Rules (Continued)

Property Name	Requirement	Description
Alert Level	Mandatory	<p>Alert levels act as a filter mechanism to ensure alert recipients only receive the alert messages that they are most interested in receiving. Each time you define an alert rule in ILOM, you must specify an alert level.</p> <p>The alert level determines which events generate an alert. The lowest level alert generates alerts for that level and for all alert levels above it.</p> <p>ILOM offers the following alert levels with Minor being the lowest alert offered:</p> <ul style="list-style-type: none"> <li>• <b>Minor.</b> This alert level generates alerts for informational events, lower and upper non-critical events, upper and lower critical events, and, upper and lower non-recoverable events.</li> <li>• <b>Major.</b> This alert level generates alerts about upper and lower non-critical events, upper and lower critical events, and, upper and lower non-recoverable events.</li> <li>• <b>Critical.</b> This alert level generates alerts for upper and lower critical events and upper and lower non-recoverable events.</li> <li>• <b>Down.</b> This alert level generates alerts for only upper non-recoverable and lower non-recoverable events.</li> <li>• <b>Disabled.</b> Disables the alert. ILOM will not generate an alert message. All the alert levels will enable the sending of a alert with the exception of <i>Disabled</i>.</li> </ul> <p><b>Important.</b> ILOM supports alert level filtering for all IPMI traps and Email Notification traps. ILOM does not support alert level filtering for SNMP traps. To enable the sending of an SNMP trap (but not filter the SNMP trap by alert level) you can choose anyone of the following options: <i>minor</i>, <i>major</i>, <i>critical</i>, or <i>down</i>. To disable the sending of an SNMP trap, you must choose the <i>disabled</i> option.</p>
SNMP Version	Optional	<p>The SNMP version property enables you to specify which version of an SNMP trap that you are sending. You can choose to specify: 1, 2c, or 3.</p> <p>This property value only applies to SNMP trap alerts.</p>
SNMP Community Name or User Name	Optional	<p>The SNMP community name or user name property enables you to specify the community string or SNMP v3 user name used in the SNMP trap alert.</p> <ul style="list-style-type: none"> <li>• For SNMP traps v1 or v2c, you can choose to specify a community name value for a an SNMP alert.</li> <li>• For SNMP v3, you can choose to specify a user name value for an SNMP alert.</li> </ul> <p><b>Important.</b> If you choose to specify an SNMP v3 user name value, you must define this user in ILOM as an SNMP user. If you do not define this user as an SNMP user, the trap receiver will not be able to decode the SNMP trap alert. For more information about defining an SNMP user in ILOM, see <a href="#">Chapter 10</a>.</p>

For more information about how to manage and create alert rule configurations in ILOM, see the following sections:

- [“Manage Alert Rule Configurations Using the ILOM Web Interface”](#) on page 161.
- [“Manage Alert Rule Configurations Using the ILOM CLI”](#) on page 164.
- [“Configure SMTP Client for Email Notification Alerts”](#) on page 170.

---

## Manage Alert Rule Configurations Using the ILOM Web Interface

You can enable, modify, or disable any alert rule configuration in ILOM from the Alert Settings web interface page. All 15 alert rule configurations presented on this page are disabled by default. The Actions drop-down list box on the page enables you to edit the properties associated with an alert rule. To enable an alert rule on this page, you must define an alert type, alert level, and a valid alert destination.

The Alert Settings page also presents a Send Test Alert button. This test alert feature enables you to verify that each alert recipient specified in an enabled alert rule receives an alert message.

**FIGURE 7-10** Alert Settings Page

Alert ID	Level	Alert Type	Destination Summary
1	disable	ipmpet	0.0.0.0
2	disable	ipmpet	0.0.0.0
3	disable	ipmpet	0.0.0.0
4	disable	ipmpet	0.0.0.0
5	disable	ipmpet	0.0.0.0
6	disable	ipmpet	0.0.0.0
7	disable	ipmpet	0.0.0.0
8	disable	ipmpet	0.0.0.0
9	disable	ipmpet	0.0.0.0
10	disable	ipmpet	0.0.0.0
11	disable	ipmpet	0.0.0.0
12	disable	ipmpet	0.0.0.0
13	disable	ipmpet	0.0.0.0
14	disable	ipmpet	0.0.0.0
15	disable	ipmpet	0.0.0.0

For additional information about how to create and manage alert rule configurations in ILOM using the web interface, see the following sections:

- [“Prerequisites”](#) on page 162.
- [“Modify an Alert Rule Configuration Using the Web Interface”](#) on page 162.

- “Disable an Alert Rule Configuration Using the Web Interface” on page 163.
- “Generate Alert Tests Using the Web Interface” on page 164.

## Prerequisites

- If you are defining an Email Notification alert, the outgoing email server that will be used to send the email notification must be configured in ILOM. If an outgoing email server is not configured, ILOM will not be able to successfully generate Email Notification alerts.
- If you are defining an SNMP Trap alert with the version set to SNMP v3, the SNMP user name must be defined in ILOM as an SNMP user. If the user is not defined in ILOM as an SNMP user, the SNMP alert user will not be able to decode the SNMP alert message. For more information about defining SNMP users in ILOM, see [Chapter 10](#).
- To create, modify, or disable an alert rule in ILOM, you must log in to ILOM with an Administrator account.

## ▼ Modify an Alert Rule Configuration Using the Web Interface

Use the following procedure to modify an alert rule configuration in ILOM:

- 1. Open a web browser and type the IP address of the server SP or CMM.**  
The Login page for the ILOM web interface appears.
- 2. In the ILOM Login page, enter an Administrator user name and password then click OK.**  
The ILOM web interface appears.
- 3. In the web interface page, select Configuration --> Alert Management.**

---

**Note** – Alternatively, you can manage alert rule configurations for a server SP from the CMM web interface. To manage alert rule configuration for a server SP from the CMM, select the server SP (blade) in the left frame of the page, then in the right frame of the page, click Configuration -->Alert Management.

---

The Alert Settings page appears.

- 4. In the Alert Settings page, do the following:**
  - a. Select the radio button for alert rule you want to create or edit.**

**b. In the Actions drop-down list box, select Edit.**

A dialog appears displaying the properties value associated with the alert rule.

**c. In the properties dialog box, specify values for an alert type, alert level, and alert destination.**

If the alert type you specify is an SNMP Trap, then you can optionally define a community name or user name value for authenticating the receipt of the alert message.

For more information about the property values you can specify for an alert rule, see [“Properties for Defining Alert Rules” on page 159](#).

**d. Click Save to apply the values specified and to close the properties dialog.**

## ▼ Disable an Alert Rule Configuration Using the Web Interface

Use the following procedure to disable an alert rule configuration in ILOM:

**1. Open a web browser and type the IP address of the server SP or CMM.**

The Login page for the ILOM web interface appears.

**2. In the ILOM Login page, enter an Administrator user name and password then click OK.**

The ILOM web interface appears.

**3. In the web interface page, select Configuration --> Alert Management.**

---

**Note** – Alternatively, you can manage alert rule configurations for a server SP from the CMM web interface. To manage alert rule configuration for a server SP from the CMM, select the server SP (blade) in the left frame of the page, then in the right frame of the page, click Configuration -->Alert Management.

---

The Alert Settings page appears.

**4. In the Alert Settings page, select the radio button for the alert rule you want to modify then click Edit in the Actions drop-down list box.**

A dialog appears presenting properties you can define about the alert rule.

**5. In the properties dialog box, select Disabled in the Alert Levels drop-down list box.**

## ▼ Generate Alert Tests Using the Web Interface

You can test each *enabled* alert rule configuration in ILOM by sending a test alert. To generate test alerts to destinations specified in ILOM's alert rule configurations, follow this procedure:

1. **Open a web browser and type the IP address of the server SP or CMM.**

The Login page for the ILOM web interface appears.

2. **In the ILOM Login page, enter an Administrator user name and password then click OK.**

The ILOM web interface appears.

3. **In the web interface page, select Configuration --> Alert Management.**

---

**Note** – Alternatively, you can manage alert rule configurations for a server SP from the CMM web interface. To manage alert rule configuration for a server SP from the CMM, select the server SP (blade) in the left frame of the page, then in the right frame of the page, click Configuration -->Alert Management.

---

The Alert Settings page appears.

4. **In the Alert Settings page, click the Send Test Alert button.**

ILOM generates test alerts to each of the alert rule configurations enabled on the Alert Settings page.

---

## Manage Alert Rule Configurations Using the ILOM CLI

You can enable, modify, or disable any alert rule configuration in ILOM from the command-line interface (CLI). All 15 alert rule configurations defined in ILOM are disabled by default. To enable alert rule configurations in ILOM, you must set values for the following properties: alert type, alert level, and alert destination.

You can also generate test alerts to any *enabled* alert rule configuration in ILOM from the CLI. This test alert feature enables you to verify that the alert recipient(s) specified in an *enabled* alert rule configuration receives the alert message.

For more information about managing and creating alert rule configurations in ILOM using the CLI, see the following sections:

- “CLI Commands for Managing Alert Rule Configurations” on page 165
- “Prerequisites” on page 167
- “Modify Alert Rule Configurations Using the CLI” on page 167
- “Disable an Alert Rule Configuration Using the CLI” on page 168
- “Generate Alert Tests Using the CLI” on page 169

## CLI Commands for Managing Alert Rule Configurations

TABLE 7-5 identifies CLI commands that you will typically need to use to manage alert rule configuration using the ILOM CLI.

**TABLE 7-5** CLI Commands for Managing Alert Rule Configurations

CLI Command	Description
show	<p>The show command enables you to display any level of the alert management command tree by specifying either the full or relative path.</p> <p><b>Examples:</b></p> <ul style="list-style-type: none"><li>• To display an alert rule along with its properties using a full path, you would type the following at the command prompt:</li></ul> <pre>show /SP/alertmgmt/rules/1 /SP/alertmgmt/rules/1 Properties:     community_or_username = public     destination = 129.148.185.52     level = minor     snmp_version = 1     type = snmptrap Commands:     cd     set     show</pre>

**TABLE 7-5** CLI Commands for Managing Alert Rule Configurations (Continued)

CLI Command	Description
	<ul style="list-style-type: none"> <li>To display a single property using the full path, you would type the following at the command prompt:  <pre>show /SP/alertmgmt/rules/1 type</pre> <pre>Properties:</pre> <pre>  type = snmptrap</pre> <pre>Commands:</pre> <pre>  set</pre> <pre>  show</pre> </li> <li>To specify a relative path if the current tree location is /SP/alertmgmt/rules, you would type the following command at the command prompt:  <pre>show 1/SP/alertmgmt/rules/1</pre> <pre>Targets:</pre> <pre>Properties:</pre> <pre>  community_or_username = public</pre> <pre>  destination = 129.148.185.52</pre> <pre>  level = minor</pre> <pre>  snmp_version = 1</pre> <pre>  type = snmptrap</pre> <pre>Commands:</pre> <pre>  cd</pre> <pre>  set</pre> <pre>  show</pre> </li> </ul>
cd	<p>The cd command enables you to set the working directory. To set alert management as a working directory on a server SP, you would type the following command at the command prompt:</p> <pre>cd /SP/alertmgmt</pre>
set	<p>The set command enables you to set values to properties from any place in the tree. You can specify either a full or relative path for the property depending on the location of the tree. For example:</p> <ul style="list-style-type: none"> <li>For full paths, you would type the following at the command path at the prompt:  <pre>set /SP/alertmgmt/rules/1 type=ipmipet</pre> </li> <li>For relative path (tree location is /SP/alertmgmt), you would type the following command path at the command prompt:  <pre>set rules/1 type=ipmipet</pre> </li> <li>For relative path (tree location is /SP/alertmgmt/rules/1), you would type the following command path at the command prompt:  <pre>set type=ipmipet</pre> </li> </ul>



## Prerequisites

- If you are defining an Email Notification alert, the outgoing email server that will be used to send the email notification must be configured in ILOM. If an outgoing email server is not configured, ILOM will not be able to successfully generate Email Notification alerts.
- If you are defining an SNMP Trap alert with the version set to SNMP v3, the SNMP user name must be defined in ILOM as an SNMP user. If the user is not defined in ILOM as an SNMP user, the SNMP alert user will not be able to decode the SNMP alert message. For more information about defining SNMP users in ILOM, see [Chapter 10](#).
- To create, modify, or disable an alert rule in ILOM, you must log in to ILOM with an Administrator account.

## ▼ Modify Alert Rule Configurations Using the CLI

### 1. Establish a local serial console connection or SSH connection to the server SP or CMM:

#### ■ Local Serial Console Connection

**Attach a serial console to the serial port on the server or CMM.**

For more information, consult the user documentation provided with the Sun server platform.

or

#### ■ Remote - Secure Shell (SSH) Connection

**Establish a Secure Shell connection to the server SP or CMM.**

From the remote client, establish a secure connection as root to the server SP or active CMM.

For example, you can establish a secure connection from a remote SSH client to the server SP by typing the following:

```
ssh -l root server_ip_address
```

Password: **changeme**

The default command prompt appears (->).

### 2. Type one of the following command paths to set the working directory:

- For a rackmount server: **cd /SP/alertmgmt**
- For a blade server module: **cd /SP/alertmgmt**
- For a chassis CMM: **cd /CMM/alertmgmt**

3. **Type the `show` command to view properties associated with an alert rule.**

For example, to view the properties associated with the first alert rule, you would type one of the following:

- For a rackmount server: **`show /SP/alertmgmt/rules/1`**
- For a blade sever module: **`show /CH/BLn/SP/alertmgmt/rules/1`**
- For a chassis CMM: **`show /CMM/alertmgmt/CMM/rules/1`**

4. **Type the `set` command to assign values to properties associated with an alert rule.**

For example, to set IPMI PET as the alert type for rule 1, you would type the following command paths:

```
set type=ipmipet
```

---

**Note** – To enable an alert rule configuration, you must specify a value for the alert type, alert level, and alert destination. If you are defining an SNMP alert type, you can optionally define a value for authenticating the receipt of SNMP trap alerts.

---

For more information about each of the property values you can define for an alert rule, see [TABLE 7-4 “Properties for Defining Alert Rules” on page 159](#).

## ▼ Disable an Alert Rule Configuration Using the CLI

Use the following procedure to disable alert rule configurations in ILOM from the CLI:

1. **Establish a local serial console connection or SSH connection to the server SP or CMM:**

■ **Local Serial Console Connection**

**Attach a serial console to the serial port on the server or CMM.**

For more information, consult the user documentation provided with the Sun server platform.

or

■ **Remote - Secure Shell (SSH) Connection**

**Establish a Secure Shell connection to the server SP or CMM.**

From the remote client, establish a secure connection as root to the server SP or active CMM.

For example, you can establish a secure connection from a remote SSH client to the server SP by typing the following:

```
ssh -l root server_ip_address
```

Password: **changeme**

The default command prompt appears (->).

2. Use the `cd` command to set the working directory to the alert management rule you want to disable.

For example:

- For a rackmount server SP, type: `cd /SP/alertmgmt/rules/n`
- For a blade server SP, type: `cd /CH/BLn/SP/alertmgmt/rules/n`
- For a chassis CMM, type: `cd /CMM/alertmgmt/CMM/rules/n`  
where *n* equals a specific alert rule number, which can be 1 to 15.

3. To disable the alert rule, type the following command:

```
set level=disable
```

## ▼ Generate Alert Tests Using the CLI

You can test each *enabled* alert rule configuration in ILOM by sending a test alert. To generate test alerts to destinations specified in ILOM's alert rule configurations follow this procedure:

1. Establish a local serial console connection or SSH connection to the server SP or CMM:

- **Local Serial Console Connection**

**Attach a serial console to the serial port on the server or CMM.**

For more information, consult the user documentation provided with the Sun server platform.

or

- **Remote - Secure Shell (SSH) Connection**

**Establish a Secure Shell connection to the server SP or CMM.**

From the remote client, establish a secure connection as root to the server SP or active CMM.

For example, you can establish a secure connection from a remote SSH client to the server SP by typing the following:

```
ssh -l root server_ip_address
```

Password: **changeme**

The default command prompt appears (->).

2. Use the `cd` command to set the working directory to the alert management rules.

For example:

- For a rackmount server SP, type: `cd /SP/alertmgmt/rules`
- For a blade server SP, type: `cd /CH/BLn/SP/alertmgmt/rules`
- For a chassis CMM, type: `cd /CMM/alertmgmt/CMM/rules`

3. Type the following command to generate a test alert:

```
set testalert=true
```

---

## Configure SMTP Client for Email Notification Alerts

To generate configured Email Notification alerts, you must enable the ILOM client to act as an SMTP client to send the email alert messages. To enable the ILOM client as an SMTP client, you must specify the IP address and port number of an outgoing SMTP email server that will process the email notifications.

For more information about how to configure an SMTP client for email notification alerts in ILOM, see the following sections:

- [“Enable SMTP Client Using the Web Interface” on page 170](#)
- [“Enable SMTP Client Using the CLI” on page 171](#)

### Prerequisite:

- Prior to enabling the ILOM client as an SMTP client, you should gather the IP address and port number of the outgoing SMTP email server.

## ▼ Enable SMTP Client Using the Web Interface

Follow these steps to configure an SMTP client in ILOM using the web interface:

1. **Open a web browser and type the IP address of the server SP or CMM.**

The Login page for the ILOM web interface appears.

2. **In the ILOM Login page, enter an Administrator user name and password then click OK.**

The ILOM web interface appears.

3. **In the web interface page, select Configuration --> SMTP Client.**

4. In the SMTP Client page, specify the following settings to enable the sending of Email Notification alerts.

SMTP Setting	Description
SMTP State	Select this check box to enable this state.
SMTP Server IP	Type the IP address of the outgoing SMTP email server that will process the email notifications.
SMTP Port	Type the port number of the outgoing SMTP email server.

5. Click Save to apply the SMTP settings.

## ▼ Enable SMTP Client Using the CLI

Follow these steps to configure an SMTP client in ILOM using the CLI:

1. Establish a local serial console connection or SSH connection to the server SP or CMM:

- Local Serial Console Connection

Attach a serial console to the serial port on the server or CMM.

For more information, consult the user documentation provided with the Sun server platform.

or

- Remote - Secure Shell (SSH) Connection

Establish a Secure Shell connection to the server SP or CMM.

From the remote client, establish a secure connection as root to the server SP or active CMM.

For example, you can establish a secure connection from a remote SSH client to the server SP by typing the following:

```
ssh -l root server_ip_address
```

Password: **changeme**

The default command prompt appears (->).

2. Use the `cd` command to set the working directory to `clients/sntp`.

For example:

- For a rackmount server SP, type: `cd /SP/clients/sntp`
- For a blade server SP, type: `cd /CH/BLn/SP/clients/sntp`
- For a chassis CMM, type: `cd /CMM/clients/sntp`

**3. Type the show command to display the SMTP properties.**

For example, accessing the SMTP properties for the first time on an SP would appear as follows:

```
show
/SP/clients/smtp
Targets
  Properties
    address = 0. 0. 0. 0
    port = 25
    state = enabled
Commands:
  cd
  set
  show
```

**4. Use the set command to specify an IP address for the SMTP client or to change the port or state property value.**

For example:

```
set address=222.333.44.5
```

**5. Press Enter for the change to take effect.**

For example, if you typed `set address=222.333.44.5` the following result would appear:

```
Set `address=222.333.44.5`
```

# Configure ILOM Communication Settings

---

Advanced ILOM communication settings include network, serial port, and web configuration.

This chapter includes the following sections:

- “Manage ILOM Network Settings Using the CLI” on page 174
  - “View Network Settings Using the CLI” on page 174
  - “Configure Network Settings Using the CLI” on page 175
  - “View Serial Port Settings Using the CLI” on page 176
  - “Configure Serial Port Settings Using the CLI” on page 177
  - “Enable HTTP or HTTPS Web Access Using the CLI” on page 178
- “Configure Secure Shell Settings” on page 179
  - “Establish a Secure Remote Connection to Run CLI Commands” on page 179
  - “View the Current Key Using the CLI” on page 180
  - “Enable or Disable SSH Using the CLI” on page 181
  - “Enable or Disable SSH Using the Web Interface” on page 181
  - “Generate a New Key Using the CLI” on page 182
  - “Generate a New Key Using the Web Interface” on page 182
  - “Restart the SSH Server Using the CLI” on page 183
  - “Restart the SSH Server Using the Web Interface” on page 183
- “Manage ILOM Network Settings Using the Web Interface” on page 183
  - “View Network Settings Using the Web Interface” on page 184
  - “Configure Network Settings Using the Web Interface” on page 184
  - “Display Serial Port Settings Using the Web Interface” on page 186
  - “Configure Serial Port Settings Using the Web Interface” on page 187
  - “Enable HTTP or HTTPS Web Access Using the Web Interface” on page 187

---

**Note** – Syntax examples in this chapter use the target starting with `/SP/`, which could be interchanged with the target starting with `/CMM/` depending on your Sun server platform. Subtargets are common across all Sun server platforms.

---

## Manage ILOM Network Settings Using the CLI

This section describes how to configure the network settings for ILOM using the ILOM command-line interface (CLI).

### About Network Settings

Network settings have two sets of properties: pending and active. The active settings are currently in use by ILOM. These settings are read-only. If you want to change settings, enter the updated settings as the pending settings (`pendingipaddress` or `pendingipgateway`), then set the `commitpending` property to `true`. This prevents accidental disconnections for both port and network settings.

---

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

---

### ▼ View Network Settings Using the CLI

1. Log in to the ILOM CLI as an Administrator or Operator.
2. At the command prompt, type:  
    -> `show /SP/network`



## ▼ Configure Network Settings Using the CLI

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

1. Log in to the ILOM CLI as an Administrator.

2. At the command prompt, type:

```
-> set /SP/network
```

### Targets, Properties, and Values

The following target, properties, and values are valid for ILOM network settings.

TABLE 8-1 ILOM Network Target, Properties, and Values

Target	Property	Value	Default
/SP/network	ipaddress	These read-only values are updated by the system	
	ipdiscovery		
	ipgateway		
	ipnetmask		
	macaddress	MAC address of ILOM	
	commitpending	true (none)	(none)
	pendingipaddress	<ipaddress none>	none
	pendingipdiscovery	dhcp static	dhcp
	pendingipgateway	<ipaddress none>	none
	pendingipnetmask	<ipdotteddecimal>	255.255.255.255

#### Example

To change the IP address for ILOM, type:

```
-> set /SP/network pendingipaddress=nnn.nn.nn.nn commitpending=true
```

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

To change the network settings from DHCP to static assigned settings, type:

```
-> set /SP/network pendingipdiscovery=static pendingipaddress=  
    nnn.nnn.nnn.nnn pendingipgateway=nnn.nnn.nnn.nnn pendingipnetmask=nnn.nnn.nnn.nnn  
    commitpending=true
```

---

**Note** – Settings take effect as soon you set `commitpending` to `true`.

---

## Serial Port Settings

The serial port provides access to the ILOM web interface, the command-line interface (CLI), and the system console stream using serial port redirection.

- The internal serial port is the connection between the host server and ILOM that allows an ILOM user to access the host serial console. The ILOM internal serial port speed must match the speed of the serial console port on the host server, often referred to as serial port 0, COM1, or `/dev/ttyS0`.

---

**Note** – Normally, the host serial console settings match ILOM's default settings (9600 baud, 8N1 [eight data bits, no parity, one stop bit], no flow control).

---

- The external serial port is the RJ-45 serial port on ILOM. Typically the internal and external serial port connections should run at the same speed to avoid flow control issues when connecting to the host console from the ILOM external serial port.

## ▼ View Serial Port Settings Using the CLI

1. Log in to the ILOM CLI as an Administrator or Operator.
2. At the command prompt:
  - Type the following command to display settings for the external serial port:  
-> **show /SP/serial/external**
  - Type the following command to display settings for the host serial port:  
-> **show /SP/serial/host**

---

**Note** – The `/SP/serial/host` target is supported only on x64-based systems. SPARC-based servers implement a virtual console and not a physical console.

---

## ▼ Configure Serial Port Settings Using the CLI

Use the `set` command to change properties and values for serial port settings. Port settings have two sets of properties: pending and active. The active settings are the settings currently in use by the ILOM. These settings are read-only. If you want to change settings, enter the updated settings as the pending settings, then set the `commitpending` property to `true`. This prevents accidental disconnections for both port and network settings.

1. Log in to the ILOM CLI as an Administrator or Operator.

2. At the command prompt type:

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

### Targets, Properties, and Values

The following targets, properties, and values are valid for ILOM serial ports.

**TABLE 8-2** Valid Targets, Properties, and Values for ILOM Serial Ports

Target	Property	Value	Default
<b>/SP/serial/external</b>	<code>commitpending</code>	<code>true   (none)</code>	<code>(none)</code>
	<code>flowcontrol</code>	<code>none</code>	<code>none</code>
	<code>pendingspeed</code>	<code>&lt;decimal&gt;</code>	<code>9600</code>
	<code>speed</code>	<code>9600</code>	<code>9600</code>
<b>/SP/serial/host</b>	<code>commitpending</code>	<code>true   (none)</code>	<code>(none)</code>
	<code>pendingspeed</code>	<code>&lt;decimal&gt;</code>	<code>(none)</code>
	<code>speed</code>	<code>9600</code>	<code>9600</code>

#### *Example*

To change the speed (baud rate) for the host serial port from 9600 to 57600, type:

- For x64-based systems

```
-> set /SP/serial/host pendingspeed=57600 commitpending=true
```

- For SPARC-based systems

```
-> set /SP/serial/external pendingspeed=57600 commitpending=true
```

---

**Note** – On x64-based systems, the speed of the host serial port must match the speed setting for serial port 0, COM1, or `/dev/ttys0` on the host operating system for ILOM to communicate properly with the host.

---

## ▼ Enable HTTP or HTTPS Web Access Using the CLI

ILOM supports both HTTP or HTTPS connections. ILOM enables you to automatically redirect HTTP access to HTTPS. ILOM also enables you to set the HTTP and HTTPS ports.

1. Log in to the ILOM CLI as a an Administrator.

2. At the command prompt, type:

```
-> set /SP/services/http
```

The properties are located in /SP/services/http and /SP/services/https.

### Targets, Properties, and Values

The following shows the valid targets, properties, and values for HTTP andHTTPS

**TABLE 8-3** Valid Targets, Properties, and Values for HTTP and HTTPS

Target	Property	Value	Default
/SP/services/http	secureredirect	enabled  disabled	enabled
	servicestate	enabled  disabled	disabled
	port	<portnum>	80
/SP/services/https	servicestate	enabled  disabled	enabled
	port	<portnum>	443

The following lists the possible settings HTTP, HTTPS, and automatic redirect.

**TABLE 8-4** Possible Settings for HTTP, HTTPS, and Automatic Redirect

Desired State	Target	Property	Value
Enable HTTP only	/SP/services/http	secureredirect	disabled
	/SP/services/http	servicestate	enabled
	/SP/services/https	servicestate	disabled
Enable HTTP and HTTPS	/SP/services/http	secureredirect	disabled
	/SP/services/http	servicestate	enabled
	/SP/services/https	servicestate	enabled

**TABLE 8-4** Possible Settings for HTTP, HTTPS, and Automatic Redirect (*Continued*)

Desired State	Target	Property	Value
Enable HTTPS only	/SP/services/http	secureredirect	disabled
	/SP/services/http	servicestate	disabled
	/SP/services/https	servicestate	enabled
Automatically redirect HTTP to HTTPS	/SP/services/http	secureredirect	enabled
	/SP/services/http	servicestate	disabled
	/SP/services/https	servicestate	enabled

---

## Configure Secure Shell Settings

Secure Shell (SSH) is the standard protocol used to access a secure remote connection to the ILOM command-line interface (CLI). Using SSH ensures that all management interactions with ILOM are encrypted and secure. Both ends of the server connection are authenticated using digital keys, and passwords are protected by encryption. The ILOM connection is protected by RSA and DSA key encryption.

### ▼ Establish a Secure Remote Connection to Run CLI Commands

- You will need to establish a secure connection from a remote SSH client to the server SP. To establish a secure connection, type the following:

```
ssh -l username server_ip_address
```

```
Password: *****
```

The default prompt appears (->) and the system is ready for you to run the CLI commands to establish network settings.

## ▼ View the Current Key Using the CLI

The need to view keys constitutes advanced configuration; most of the time, you will not need to view keys. You can either view the whole public key, or the abbreviated fingerprint of the key.

---

**Note** – All of the properties below `/SP/services/ssh/keys/rsa|dsa` are read only

---

- To view the RSA key, type:

```
-> show /SP/services/ssh/keys/rsa
  For example:
  /SP/services/ssh/keys/rsa
  Targets:
    Properties:
      fingerprint =
ca:c0:05:ff:b7:75:15:a0:30:df:1b:a1:76:bd:fe:e5
      length = 1024
      publickey
AAAAB3NzaC1yc2EAAAABIwAAAIEAthvlggXbPIxN4OEvkukKupdFPr8GDaOsKGg
BESVlnny4nX8yd8JC/hrw3qDHmXIZ8JAFwoLQgjtZCbEsgpn9nNIMb6nSfu6Y1t
TtUZXSqFBZ48R0mU0Sqqr3i3bgDUR0siphlpqV6Yu0Zd1h3549wQ+RWk3vxqHQ
Ffzhv9c=
    Commands:
      cd
      show
```

- To view the DSA key, type:

```
-> show /SP/services/ssh/keys/dsa
  For example:
  /SP/services/ssh/keys/dsa
  Targets:
    Properties:
      fingerprint =
6a:90:c7:37:89:e6:73:23:45:ff:d6:8e:e7:57:2a:60
      length = 1024
      publickey =
AAAAB3NzaC1kc3MAAACBAInrYecNH86imBbUqE+3FoUfm/fei2ZZtQzqrMx5zBm
bHFIAFdRQKeoQ7gqjc9jQb07ajLxwk2vZzkg3ntnmqHz/hwHvdho2KaolBtAFGc
fLIIdzGVxi4I3phVb6anmT1bqI2AILAa7JvQ8dEGbyATYR9A/pf5VTac/TQ700/J
AAAAFQCIUavkex7wtEhC0CH3s25ON0I3CwAAAIbnfHUop6ZN7i46ZuQOKhD7Mkj
gdHy+8MTBkupVfXqfRE9Zw9yrBZCNsoD8XEeIeyP+pu05k5dJvkzqSqrTVoAXyY
qewyZMFE7stutugw/XEmyj+XqBWaiOAQskdiMvNHa3MSg8PKJyWP8eIMxD3rIu
```

```
PTzkv632uBxzwSwfAQAAAIAtA8/3odDJUprnxLgHTowc8ksGBj/wJDgPfpGGJHB
B1FDBMhSsRbwh6Z+s/gAf1f+S67HJBTUPsVSMz+czmanc1oZeOazT4+zeNG6uCl
u/5/JmJsdkguc1FcoxtBFqf0/fKjyR0ecWaU7L4kjjvWoSsydHJ0pMHasEecEBEr
lg==
```

Commands :

```
cd
show
```

## ▼ Enable or Disable SSH Using the CLI

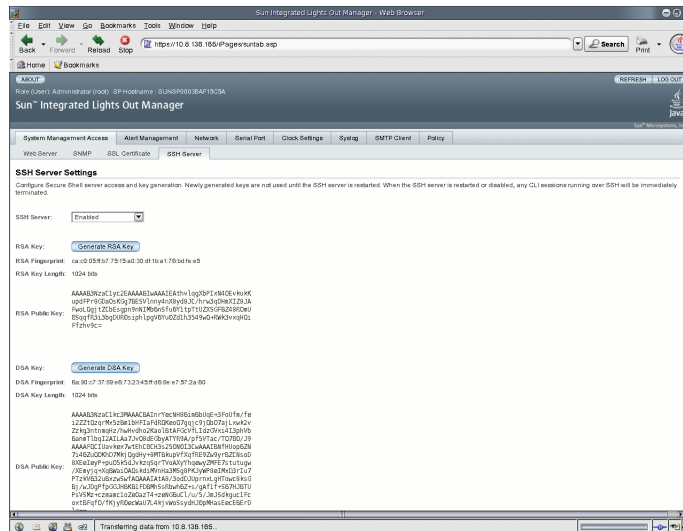
- If you do not want to provide access over the network, or if you do not want to use SSH, type the following:

```
-> set /SP/services/ssh state=enabled | disabled
```

## ▼ Enable or Disable SSH Using the Web Interface

1. Log in to iLOM as an Administrator.
2. Select Configuration --> System Management Access --> SSH Server.
3. From the SSH Server drop-down list, select Enabled or Disabled.

FIGURE 8-1 SSH Server Settings Page



## ▼ Generate a New Key Using the CLI

1. Set the key type by typing the following:

```
-> set /SP/services/ssh generate_new_key_type=dsa | rsa
```

2. Set the action to true.

```
-> set /SP/services/ssh generate_new_key_action=true
```

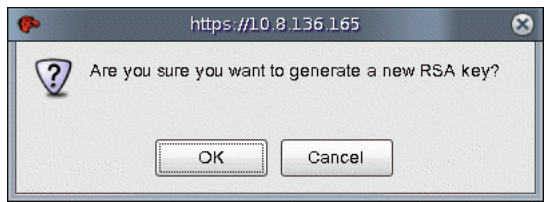
The fingerprint and key will look different.

## ▼ Generate a New Key Using the Web Interface

1. Log in to ILOM as an Administrator.
2. Select Configuration --> System Management Access --> SSH Server.
3. Select RSA by clicking the Generate RSA Key button, or select DSA by clicking the Generate DSA Key button.

Confirm or cancel your selection by clicking OK or Cancel when you are prompted.

FIGURE 8-2 Confirmation Dialog



## ▼ Restart the SSH Server Using the CLI

A new key will not take effect until the SSH server is restarted.

---

**Note** – Restarting will end any existing SSH connections.

---

- To restart the SSH server, type the following:

```
-> set /SP/services/ssh restart_sshd_action=true
```



## ▼ Restart the SSH Server Using the Web Interface

A new key will not take effect until the SSH server is restarted.

---

**Note** – Restarting will end any existing SSH connections.

---

1. **Log in to ILOM as an Administrator.**
2. **Select Configuration --> System Management Access --> SSH Server.**
3. **From the SSH Server drop-down list, select Restart SSH Server.**

---

## Manage ILOM Network Settings Using the Web Interface

This section describes how to configure the network parameters for ILOM using the ILOM web interface.

ILOM automatically configures its IP settings using the Dynamic Host Configuration Protocol (DHCP). If your network does not support this protocol, you need to set the parameters manually.

## ▼ View Network Settings Using the Web Interface

1. **Log in to ILOM as Administrator or Operator to open the ILOM web interface.**
2. **Select Configuration --> Network.**

From the Network Settings page, you can view MAC addresses and configure network addresses for the server's Chassis Monitoring Modules and service processors.

---

**Note** – DHCP is the default mode, but you can manually configure each IP address, Netmask, and Gateway.

---

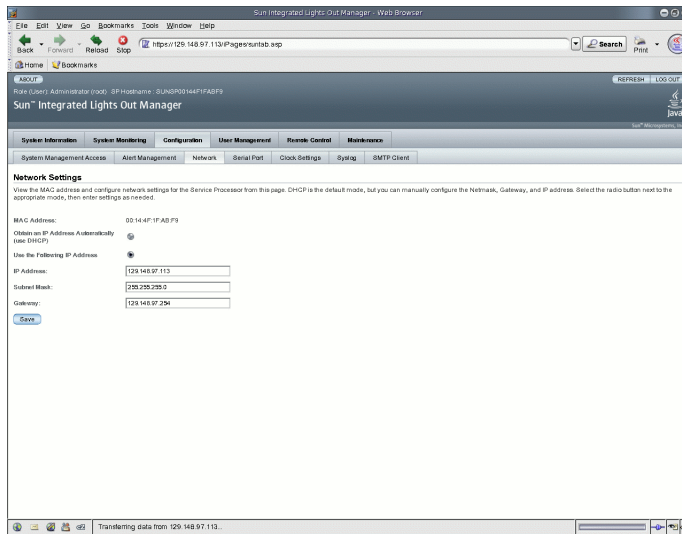
## ▼ Configure Network Settings Using the Web Interface

1. Log in to ILOM as an Administrator to open the ILOM web interface.

2. Select Configuration --> Network.

The Network Settings page appears.

**FIGURE 8-3** Network Settings Page



3. Complete the information in the Network Settings page.

Use the descriptions in the following table when completing the information.

**TABLE 8-5** Network Settings Page Fields

Item	Description
MAC Address	The ILOM's media access control (MAC) address is set at the factory. The MAC address is a hardware address that is unique to each networked device. ILOM's MAC address is provided on a label on the server or CMM, on the Customer Information Sheet included on the ship kit, and in the BIOS Setup screen.
Obtain an IP Address Automatically (use DHCP)	Click the radio button to have the DHCP obtain an IP address.

**TABLE 8-5** Network Settings Page Fields (*Continued*)

<b>Item</b>	<b>Description</b>
IP Address	Type ILOM's IP address. The IP address is a unique name that identifies the system on a TCP/IP network.
Subnet Mask	Type the subnet mask of the network on which ILOM resides.
Gateway	Type ILOM's gateway access address.

**4. Click Save for your settings to take effect.**

Settings are considered pending until you click Save. Changing the IP address will end your ILOM session.

You are prompted to close your web browser.

**5. Log back in to ILOM using the new IP address.**

---

**Note** – If you changed the network settings, you may need to log back in with a new browser session.

---

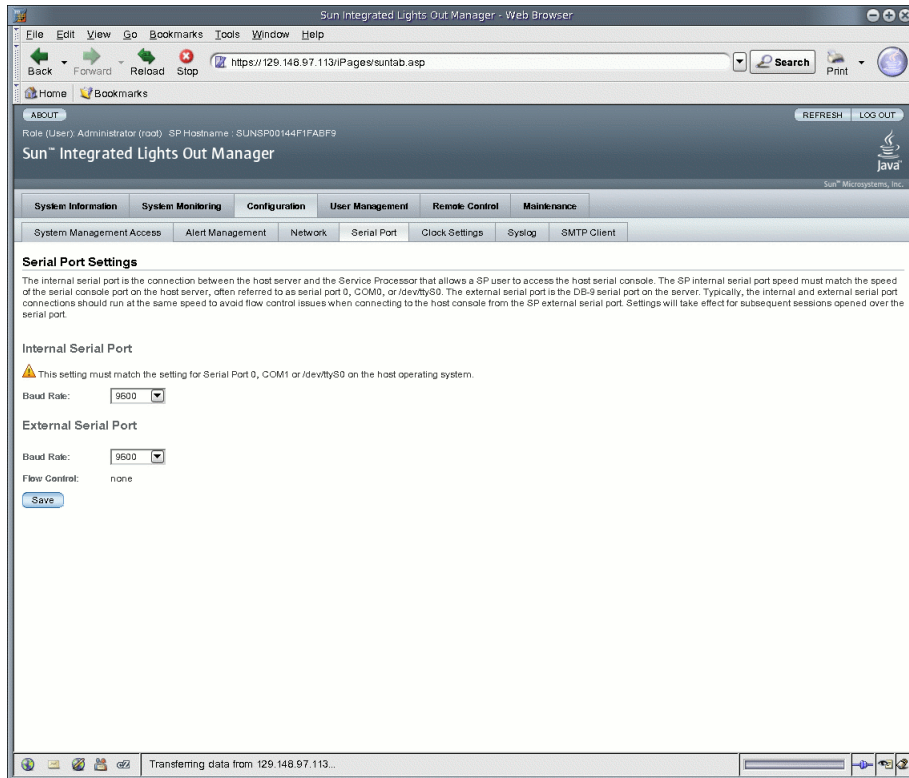
## ▼ Display Serial Port Settings Using the Web Interface

**1. Log in to the ILOM web interface as an Administrator or Operator.**

**2. Select Configuration --> Serial Port.**

The Serial Port Settings page appears.

**FIGURE 8-4** Serial Port Settings Page



3. View the baud rate for the external serial port.

## ▼ Configure Serial Port Settings Using the Web Interface

This section describes how to configure the ILOM serial port. The default settings are 9600 baud and no flow control.

1. Log in to ILOM as an Administrator to open the ILOM web interface.
2. Select Configuration --> Serial Port.

The Serial Port Settings page appears.

**3. Select the baud rate for the internal serial port from the Internal Serial Port Baud Rate drop-down list.**

This setting must match the setting for serial port 0, COM1 or /dev/ttyS0 on the host operating system.

The baud rate value must match the speed that was specified for the BIOS serial redirection feature (default is 9600 baud) and the speed used for the boot loader and operating system configuration.

To connect to the system console using ILOM, ILOM must be set to its default settings (9600 baud, 8N1 [eight data bits, no parity, one stop bit], no flow control).

**4. Select the baud rate for the external serial port from the External Serial Port Baud Rate drop-down list.**

This setting must match the baud rate on the RJ-45 serial port on the Sun server.

**5. Click Save for your changes to take effect, or click Cancel to return to the previous settings.**

## ▼ Enable HTTP or HTTPS Web Access Using the Web Interface

This section describes how to view and modify web server settings.

ILOM provides the option to control access to the web interface. There are four choices:

- HTTP only
- HTTPS only
- HTTP and HTTPS
- HTTPS and HTTP automatically redirected to HTTPS

HTTPS is enabled by default.

**1. Log in to ILOM as an Administrator to open the ILOM web interface.**

**2. Select Configuration --> System Management Access --> Web Server.**

The Web Server Settings page appears.

**FIGURE 8-5** Web Server Settings Page

ABOUT REFRESH LOG OUT  
Role (User): Administrator (root) SP Hostname: SUNSP0003BAF15B3E  
Sun™ Integrated Lights Out Manager  
Sun™ Microsystems, Inc.  
Java™  
System Information System Monitoring Configuration User Management Remote Control Maintenance  
System Management Access Alert Management Network Serial Port Clock Settings Syslog SMTP Client Policy  
Web Server SNMP SSL Certificate SSH Server  
**Web Server Settings**  
Configure which types of web server access to allow, and the associated ports. HTTPS is the default. If both HTTP and HTTPS are disabled, you lose access to the ILOM web interface. To regain access, you must log into the CLI and enable HTTP or HTTPS access.  
HTTP Webserver: Redirect HTTP Connection to HTTPS  
HTTP Port: 80  
HTTPS Webserver:  Enabled  
HTTPS Port: 443  
Save

**3. Select the HTTP or HTTPS web server.**

- **To enable HTTP** – Select Enabled from the drop-down list. You can also select:
  - Redirect HTTP Connection to HTTPS – HTTP connections are automatically redirected to HTTPS.
  - Disabled – Turn HTTP off.
- **To enable HTTPS** – Select the HTTPS Web Server Enabled check box.

The HTTPS web server is enabled by default.

---

**Note** – If you disable HTTP or select Redirect HTTP Connection to HTTPS, and then disable HTTPS, you will be unable to access the ILOM web interface. To restore access, use the CLI `/SP/services/http` or `/SP/services/https` commands, as described in [“Enable HTTP or HTTPS Web Access Using the CLI”](#) on page 178.

---

**4. Assign an HTTP or HTTPS port number.**

**5. Click Save for your settings to take effect.**

# Intelligent Platform Management Interface

---

ILOM supports the Intelligent Platform Management Interface (IPMI), which enables you to use a command-line interface to monitor and control your server platform, as well as to retrieve information about your server platform.

This chapter includes the following sections:

- [“IPMI Overview” on page 189](#)
  - [“ILOM and IPMI” on page 190](#)
  - [“Using IPMItool” on page 190](#)
  - [“IPMI Alerts” on page 191](#)
  - [“IPMItool Examples” on page 192](#)
- 

## IPMI Overview

The Intelligent Platform Management Interface (IPMI) is an open industry-standard interface that was designed primarily for out-of-band management of server systems over a number of different types of networks. IPMI functionality includes field-replaceable unit (FRU) inventory reporting, system monitoring, logging of system events, system recovery (including local and remote system resets and power on and power off capabilities), and alerting. IPMI functions independently of the main processor and operating system.

The independent monitoring, logging, and access functions available through IPMI provide a certain amount of manageability that is built into the platform hardware. IPMI also supports systems when there is no system management software available for a particular operating system or when you elect not to install or load the system management software.

ILOM is compliant with IPMI v1.5 and v2.0.

Additional information, including detailed specifications about IPMI, is available at the following sites:

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

<http://openipmi.sourceforge.net>

---

## ILOM and IPMI

IPMI 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. Using low-level hardware intelligence rather than the operating system has two main benefits: first, this configuration enables out-of-band server management, and second, the operating system is not burdened with transporting system status data.

The service processors (SPs) on your server or blades are IPMI v2.0 compliant. You can access IPMI functionality through the command line using the IPMITool utility either in-band or out-of-band. Additionally, you can generate IPMI-specific traps from the ILOM web interface, or manage the SP's IPMI functions from any external management solution that is IPMI v1.5 or v2.0 compliant.

---

## Using IPMITool

IPMITool is an open-source, simple command-line interface (CLI) utility for managing and configuring IPMI-enabled devices. IPMITool can manage the IPMI functions of either the local system or a remote system. You can use the IPMITool utility to perform IPMI functions with a kernel device driver or over a LAN interface. You can download IPMITool from this site:

<http://ipmitool.sourceforge.net/>

You can do the following with IPMITool:

- Read the Sensor Data Record (SDR) Repository.
- Print sensor values.
- Display the contents of the System Event Log (SEL).
- Print field-replaceable unit (FRU) inventory information.
- Read and set LAN configuration parameters.
- Perform remote chassis power control.



Detailed information about IPMItool is provided in a man page that is available from this site:

<http://ipmitool.sourceforge.net/manpage.html>

---

## IPMI Alerts

ILOM supports alerts in the form of IPMI Platform Event Trap (PET) alerts. Alerts provide advance warning of possible system failures. Alert configuration is available from the SP on your server or blade. IPMI PET alerts are supported on all Sun server platforms and modules, with the exception of the Chassis Monitoring Module (CMM).

Each Sun server platform is equipped with a number of IPMI-compliant sensors that measure voltages, temperatures, and other service-related attributes of the system. ILOM automatically polls these sensors and posts any events crossing a threshold to an ILOM event log. In addition, ILOM generates alert messages to one or more alert destinations that you specify with IP address(es). The alert destination specified must support the receipt of IPMI PET messages. If the alert destination does not support IPMI PET messages, the alert recipient will not be able to decode the alert message.

When configuring IPMI PET alerts, you must also specify an alert level, which filters alert messages so that alert recipients only receive those messages that they are most interested in receiving. ILOM provides five alert levels, with Minor being the lowest alert offered:

- **Minor** – Generates alerts for informational events, upper and lower non-critical events, upper and lower critical events, and, upper and lower non-recoverable events.
- **Major** – Generates alerts about upper and lower non-critical events, upper and lower critical events, and, upper and lower non-recoverable events.
- **Critical** – Generates alerts for upper and lower critical events and upper and lower non-recoverable events.
- **Down** – Generates alerts for only upper non-recoverable and lower non-recoverable events.
- **Disabled** – Disables the alert. ILOM will not generate an alert message.

For information about managing alert rule configurations, including how to modify an alert rule, disable and alert rule, and generate a test alert, see “[Manage Alert Rule Configurations Using the ILOM Web Interface](#)” on page 161 and “[Manage Alert Rule Configurations Using the ILOM CLI](#)” on page 164.

For a description of ILOM CLI commands for managing alert rule configurations, see “[CLI Commands for Managing Alert Rule Configurations](#)” on page 165.

---

# IPMItool Examples

The following are examples of how you can use IPMItool. In the examples, 10.8.136.165 is the IP address of ILOM. The interface can be bmc, lan, or lanplus on Solaris systems; open on Linux systems; and ms on Windows systems. When you use the ipmitool command on a Windows system, you need to add the .exe extension to the ipmitool command (ipmitool.exe). The commands are common to all platforms. However, the output (sensor names, values, thresholds, and so forth) are platform specific.

## ▼ View a List of Sensors and Their Values

```
$ ipmitool -H 10.8.136.165 -I lanplus -U root -P changeme sdr list
```

/SYS/T_AMB	24 degrees C	ok
/RFM0/FAN1_SPEED	7110 RPM	ok
/RFM0/FAN2_SPEED	5880 RPM	ok
/RFM1/FAN1_SPEED	5880 RPM	ok
/RFM1/FAN2_SPEED	6360 RPM	ok
/RFM2/FAN1_SPEED	5610 RPM	ok
/RFM2/FAN2_SPEED	6510 RPM	ok
/RFM3/FAN1_SPEED	6000 RPM	ok
/RFM3/FAN2_SPEED	7110 RPM	ok
/RFM4/FAN1_SPEED	6360 RPM	ok
/RFM4/FAN2_SPEED	5610 RPM	ok
/RFM5/FAN1_SPEED	5640 RPM	ok
/RFM5/FAN2_SPEED	6510 RPM	ok
/RFM6/FAN1_SPEED	6180 RPM	ok
/RFM6/FAN2_SPEED	6000 RPM	ok
/RFM7/FAN1_SPEED	6330 RPM	ok
/RFM7/FAN2_SPEED	6330 RPM	ok
/RFM8/FAN1_SPEED	6510 RPM	ok
/RFM8/FAN2_SPEED	5610 RPM	ok

---

**Note** – The above output was shortened. The actual output displays 163 sensors.

---

## ▼ View Details About a Single Sensor

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme sensor get /SYS/T_AMB
Locating sensor record...
Sensor ID           : /SYS/T_AMB (0x8)
Entity ID          : 41.0
Sensor Type (Analog) : Temperature
Sensor Reading     : 24 (+/- 0) degrees C
Status             : ok
Lower Non-Recoverable : 0.000
Lower Critical      : 4.000
Lower Non-Critical  : 10.000
Upper Non-Critical  : 35.000
Upper Critical      : 40.000
Upper Non-Recoverable : 45.000
Assertions Enabled  : lnc- lcr- lnr- unc+ ucr+ unr+
Deassertions Enabled : lnc- lcr- lnr- unc+ ucr+ unr+
```

## ▼ Power On the Host

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis power on
```

## ▼ Power Off the Host

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis power off
```

## ▼ Power Cycle the Host

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis power cycle
```

## ▼ Shutdown the Host Gracefully

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis power soft
```

## ▼ View Manufacturing Information for FRUs

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme fru print
```

```
FRU Device Description : Builtin FRU Device (ID 0)
Board Product          : ASSY,ANDY,4SKT_PCI-E,BLADE
Board Serial           : 0000000-7001
Board Part Number      : 501-7738-01
Board Extra            : AXX_RevE_Blade
Product Manufacturer   : SUN MICROSYSTEMS
Product Name           : ILOM

FRU Device Description : /SYS (ID 4)
Chassis Type           : Rack Mount Chassis
Chassis Part Number    : 541-0251-05
Chassis Serial         : 00:03:BA:CD:59:6F
Board Product          : ASSY,ANDY,4SKT_PCI-E,BLADE
Board Serial           : 0000000-7001
Board Part Number      : 501-7738-01
Board Extra            : AXX_RevE_Blade
Product Manufacturer   : SUN MICROSYSTEMS
Product Name           : SUN BLADE X8400 SERVER MODULE
Product Part Number    : 602-0000-00
Product Serial         : 0000000000
Product Extra          : 080020ffffffffffffffff0003baf15c5a

FRU Device Description : /P0 (ID 5)
Product Manufacturer   : ADVANCED MICRO DEVICES
Product Part Number    : 0F21
Product Version        : 2

FRU Device Description : /P0/D0 (ID 6)
Product Manufacturer   : MICRON TECHNOLOGY
Product Name           : 1024MB DDR 400 (PC3200) ECC
Product Part Number    : 18VDDF12872Y-40BD3
Product Version        : 0300
Product Serial         : D50209DA
Product Extra          : 0190
Product Extra          : 0400

FRU Device Description : /P0/D1 (ID 7)
Product Manufacturer   : MICRON TECHNOLOGY
Product Name           : 1024MB DDR 400 (PC3200) ECC
Product Part Number    : 18VDDF12872Y-40BD3
Product Version        : 0300
Product Serial         : D50209DE
Product Extra          : 0190
Product Extra          : 0400
```

## ▼ View the IPMI System Event Log

```
$ ipmitool -H 10.8.136.165 -I lanplus -U root -P changeme sel list
```

100		Pre-Init Time-stamp		Power Unit #0x78		State Deasserted		
200		Pre-Init Time-stamp		Power Supply #0xa2		Predictive Failure Asserted		
300		Pre-Init Time-stamp		Power Supply #0xba		Predictive Failure Asserted		
400		Pre-Init Time-stamp		Power Supply #0xc0		Predictive Failure Asserted		
500		Pre-Init Time-stamp		Power Supply #0xb4		Predictive Failure Asserted		
600		04/05/2007		12:03:24		Power Supply #0xa3		Predictive Failure Deasserted
700		04/05/2007		12:03:25		Power Supply #0xaa		Predictive Failure Deasserted
800		04/05/2007		12:03:25		Power Supply #0xbc		Predictive Failure Deasserted
900		04/05/2007		12:03:26		Power Supply #0xa2		Predictive Failure Asserted
a00		04/05/2007		12:03:26		Power Supply #0xa8		Predictive Failure Deasserted
b00		04/05/2007		12:03:26		Power Supply #0xb6		Predictive Failure Deasserted
c00		04/05/2007		12:03:26		Power Supply #0xbb		Predictive Failure Deasserted
d00		04/05/2007		12:03:26		Power Supply #0xc2		Predictive Failure Deasserted
e00		04/05/2007		12:03:27		Power Supply #0xb0		Predictive Failure Deasserted
f00		04/05/2007		12:03:27		Power Supply #0xb5		Predictive Failure Deasserted
1000		04/05/2007		12:03:27		Power Supply #0xba		Predictive Failure Asserted
1100		04/05/2007		12:03:27		Power Supply #0xc0		Predictive Failure Asserted
1200		04/05/2007		12:03:28		Power Supply #0xa9		Predictive Failure Deasserted
1300		04/05/2007		12:03:28		Power Supply #0xae		Predictive Failure Deasserted
1400		04/05/2007		12:03:28		Power Supply #0xb4		Predictive Failure Asserted
1500		04/05/2007		12:03:28		Power Supply #0xbe		Predictive Failure Deasserted



# Simple Network Management Protocol

---

ILOM supports the Simple Network Management Protocol (SNMP), which is used to exchange data about network activity. SNMP is an open, industry-standard protocol.

This chapter includes the following sections:

- [“SNMP Overview” on page 198](#)
- [“How SNMP Works” on page 199](#)
- [“SNMP Management Information Base Files” on page 199](#)
- [“Alerts and SNMP Traps” on page 200](#)
- [“Manage SNMP Users With the CLI” on page 201](#)
  - [“Add an SNMP User Account Using the CLI” on page 201](#)
  - [“Edit an SNMP User Account Using the CLI” on page 201](#)
  - [“Delete an SNMP User Account Using the CLI” on page 201](#)
  - [“Add or Edit an SNMP Community Using the CLI” on page 202](#)
  - [“Delete an SNMP Community Using the CLI” on page 202](#)
  - [“Configure SNMP Trap Destinations Using the CLI” on page 203](#)
- [“Manage SNMP Users Using the Web Interface” on page 204](#)
  - [“Configure SNMP Settings Using the Web Interface” on page 204](#)
  - [“Add or Edit an SNMP User Account Using the Web Interface” on page 206](#)
  - [“Delete an SNMP User Account Using the Web Interface” on page 207](#)
  - [“Add or Edit an SNMP Community Using the Web Interface” on page 208](#)
  - [“Delete an SNMP Community Using the Web Interface” on page 208](#)
  - [“Configure SNMP Trap Destinations Using the Web Interface” on page 209](#)
- [“SNMP Examples” on page 209](#)
  - [“View and Configure SNMP Settings” on page 210](#)

- “Obtain Information Using `snmpget` or `snmpwalk` net-snmp Commands” on page 211
- “Set Information Using `snmpset`” on page 212
- “Receive Traps Using `snmptrapd`” on page 212

---

**Note** – Syntax examples in this chapter use the target starting with `/SP/`, which could be interchanged with the target starting with `/CMM/` depending on your Sun server platform. Subtargets are common across all Sun server platforms.

---

## SNMP Overview

Simple Network Management Protocol (SNMP) is an open technology that enables the management of networks and devices, or nodes, that are connected to the network. Using SNMP, data travels between a managed device (node) and a networked management station. A managed device can be any device that runs SNMP, such as hosts, routers, web servers, or other servers on the network. SNMP messages are sent over IP using the User Datagram Protocol (UDP). Any management application that supports SNMP can manage your server.

ILOM supports SNMP versions 1, 2c, and 3. Using SNMP v3 is strongly advised since SNMP v3 provides additional security, authentication, and privacy beyond SNMP v1 and v2c.

SNMP is a protocol, not an operating system, so you need an application to utilize SNMP messages. Your SNMP management software may 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 traps. Management stations and agents use the following functions:

- Get
- GetNext
- GetResponse
- Set
- Trap



---

# How SNMP Works

SNMP functionality requires the following two components:

- **Network management station** – A network management station hosts management applications, which monitor and control managed nodes.
- **Managed node** – A managed node is a device such as a server, router, or hub that hosts SNMP management agents that are responsible for carrying out requests from management stations, such as an SP running ILOM.

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 management stations and agents.

The SNMP agent is preinstalled on your Sun server platform and runs on ILOM, so all SNMP management occurs through ILOM. To utilize this feature, your operating system must have an SNMP client application.

---

# SNMP Management Information Base Files

The base component of an SNMP implementation 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. The tree-like, hierarchical system classifies information about resources in a network. The MIB defines the variables that the SNMP agent can access. When a management station requests information from a managed node, the agent receives the request and retrieves the appropriate information from the MIBs. The MIB provides access to the server's network configuration, status, and statistics.

The following SNMP MIBs are used with ILOM:

- The system and snmp groups from SNMPv2 MIB (RFC1907)
- SNMP-FRAMEWORK-MIB (RFC2271.txt)
- SNMP-USER-BASED-MIB (RFC 2574)
- SNMP-MPD-MIB (RFC 2572)
- The entPhysicalTable from the ENTITY-MIB (RFC2737)
- SUN-PLATFORM-MIB

This MIB represents an inventory of server and chassis hardware, including all the sensors and indicators along with their status.

- SUN-ILOM-CONTROL-MIB

This MIB represents a Sun SP or CMM configuration such as user or access management, alerts, and more.

- SUN-HW-TRAP-MIB

This MIB describes the hardware-related traps that a Sun SP or CMM may generate.

- SUN-ILOM-PET-MIB

This MIB describes the IPMI Platform Event Traps (PETs) that a Sun SP may generate. See [“About Alert Management” on page 158](#) for more information about PETs.

---

## Alerts and SNMP Traps

Using ILOM, you can configure up to 15 alert rules. For each alert rule that you configure in ILOM, you must define three or more properties about the alert, depending on the type of alert. The alert type defines the message format and the method for sending and receiving an alert message. ILOM supports these three alert types: IPMI PET alerts, email notification alerts, or SNMP traps.

ILOM supports the generation of SNMP trap alerts to a user-specified IP address. All destinations that you specify must support the receipt of SNMP trap messages.

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

To use this feature, you must do the following:

- Integrate and save the platform-specific MIBs into your SNMP directory.
- Inform your management station about your server.
- Configure ILOM to send SNMP traps to your management station.

There are no trap destinations configured by default. By default, agents listen to port 161 for SNMP requests and agents send traps to port 162. However, you can configure the SNMP trap destination port to any valid port.

---

# Manage SNMP Users With the CLI

You can add, delete, or configure SNMP user accounts and communities using the ILOM command-line interface (CLI).

---

**Note** – When working in the ILOM CLI, if Set Requests is disabled, all SNMP objects are read-only.

---

## ▼ Add an SNMP User Account Using the CLI

1. Log in to the ILOM CLI as Administrator.
2. To add an SNMP v3 read-only user account, type the following command:

```
create /SP/services/snmp/users/username authenticationpassword=  
password
```

## ▼ Edit an SNMP User Account Using the CLI

1. Log in to the ILOM CLI as Administrator.
2. To edit an SNMP v3 user account, type the following command:

```
edit /SP/services/snmp/users/username authenticationpassword=password
```

---

**Note** – When changing the parameters of SNMP users, you must provide a value for authenticationpassword, even if you are not changing the password.

---

## ▼ Delete an SNMP User Account Using the CLI

1. Log in to the ILOM CLI as Administrator.
2. To delete an SNMP v3 user account, type the following command:

```
delete /SP/services/snmp/users/username
```

## ▼ Add or Edit an SNMP Community Using the CLI

1. Log in to the ILOM CLI as Administrator.
2. To add an SNMP v1/v2c community, type the following command:  
`create /SP/services/snmp/communities/communityname`

## ▼ Delete an SNMP Community Using the CLI

1. Log in to the ILOM CLI as Administrator.
2. To delete an SNMP v1/v2c community, type the following command:  
`delete /SP/services/snmp/communities/communityname`

## Targets, Properties, and Values

The following table lists the targets, properties, and values that are valid for SNMP user accounts.

**TABLE 10-1** SNMP User Account Targets, Properties, and Values

Target	Property	Value	Default
<i>/SP/services/snmp/communities/communityname</i>	permissions	ro rw	ro
<i>/SP/services/snmp/users/username</i>	authenticationprotocol	MD5 SHA	MD5
	authenticationpassword*	<string>	(null string)
	permissions	ro rw	ro
	privacyprotocol	none DES	none
	privacypassword*	<string>	(null string)
<i>/SP/services/snmp</i>	engineid = none	<string>	(null string)
	port = 161	<integer>	161
	sets = enabled	enabled disabled	disabled
	v1 = disabled	enabled disabled	disabled
	v2c = disabled	enabled disabled	disabled
	v3 = disabled	enabled disabled	enabled

\* If the `privacyprotocol` property has a value other than `none`, then a `privacypassword` must be set. An `authenticationpassword` must be provided when creating or modifying users (SNMP v3 only).

For example, to change the `privacyprotocol` for user `a1` to DES you would type:

```
-> set /SP/services/snmp/users/a1 privacyprotocol=DES
privacypassword=password authenticationprotocol=SHA
authenticationpassword=password
```

Your changes would be invalid if you typed only:

```
-> set /SP/services/snmp/users/a1 privacyprotocol=DES
```

---

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

---

## ▼ Configure SNMP Trap Destinations Using the CLI

Follow these steps to configure the destinations to which the SNMP traps are sent.

1. Log in to the ILOM CLI as Administrator.
2. Type the `show` command to display the current settings of the alert rule.

For example:

```
-> show /SP/alertmgmt/rules/1
/SP/alertmgmt/rules/1
Targets:
Properties:
  community_or_username = public
  destination = 0.0.0.0
  destination_port = 0
  level = disable
  snmp_version = 1
  type = snmptrap
Commands:
  cd
  set
  show
```

3. Go to the `/SP/alertmgmt/rules/snmp` directory. Type:

```
-> cd /SP/alertmgmt/rules/snmp
```

4. Choose a rule (from targets 1 through 15) for which you would like to configure a destination for SNMP traps, and go to that directory.

For example:

```
-> cd 4
```

5. Within that rule directory, type the `set` command to change the rule properties.

For example:

```
-> set type=snmptrap level=critical destination=IPaddress
destination_port=0 snmp_version=2c community_or_username=
public
```

---

## Manage SNMP Users Using the Web Interface

This section describes how to use the ILOM web interface to manage SNMP users and communities.

### ▼ Configure SNMP Settings Using the Web Interface

Follow these steps to configure SNMP settings:

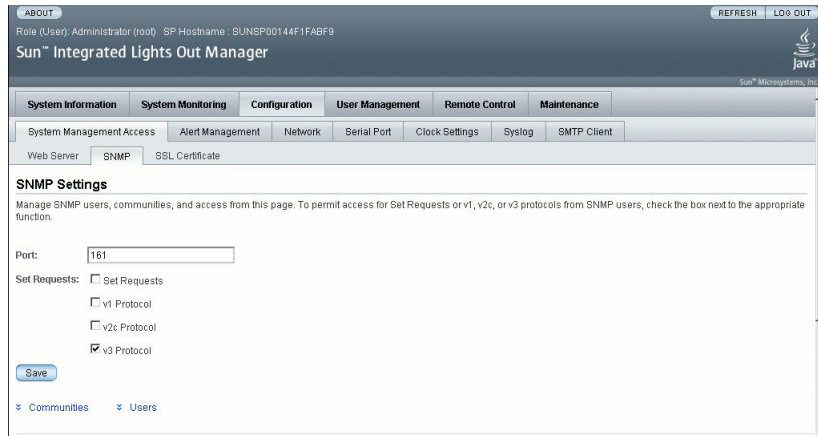
1. **Log in to ILOM as an Administrator to open the web interface.**

You can modify SNMP settings only when logged in to ILOM with Administrator privileges.

2. **Select Configuration --> System Management Access --> SNMP.**

The SNMP Settings page appears.

**FIGURE 10-1** SNMP Settings Page



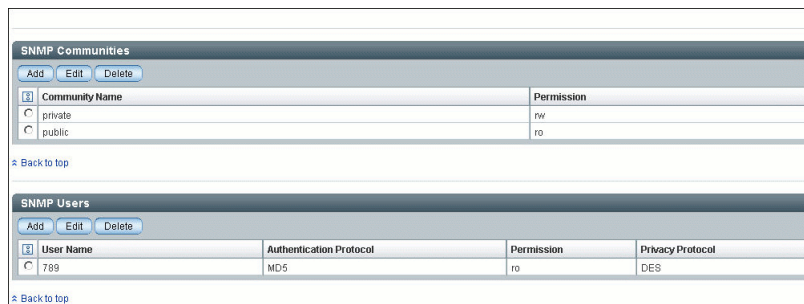
3. Type the port number in the Port text field.
4. Select or clear the Set Requests check box to enable or disable the Set Requests option.  
If Set Requests is disabled, all SNMP objects are read-only.
5. Select a check box to enable SNMP v1, v2c, or v3.  
SNMP v3 is enabled by default. You can enable or disable v1, v2c, and v3 protocol versions.
6. Click Save.

---

**Note** – At the bottom of the page, you can also add, edit, or delete SNMP communities or users, as shown in [FIGURE 10-2](#).

---

**FIGURE 10-2** SNMP Communities and Users



## ▼ Add or Edit an SNMP User Account Using the Web Interface

Follow these steps to add or edit an SNMP v3 user account:

**1. Log in to ILOM as an Administrator to open the web interface.**

You can add an SNMP user or user account only when logged in to ILOM with Administrator privileges.

**2. Select Configuration --> System Management Access --> SNMP.**

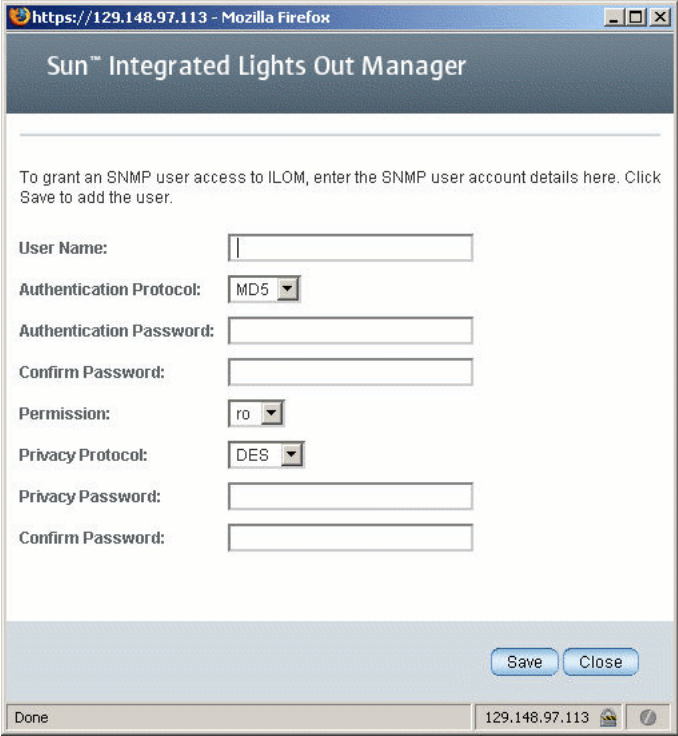
The SNMP Settings page appears.

**3. Click the Users link or scroll down to the SNMP Users list.**

**4. Click Add or Edit under the SNMP Users list.**

The Add dialog box or the Edit dialog box appears as shown in [FIGURE 10-3](#).

**FIGURE 10-3** Add SNMP User Dialog



The screenshot shows a web browser window titled "Sun™ Integrated Lights Out Manager" with the URL "https://129.148.97.113 - Mozilla Firefox". The page content includes the following form fields and controls:

- User Name:** A text input field.
- Authentication Protocol:** A dropdown menu with "MD5" selected.
- Authentication Password:** A text input field.
- Confirm Password:** A text input field.
- Permission:** A dropdown menu with "ro" selected.
- Privacy Protocol:** A dropdown menu with "DES" selected.
- Privacy Password:** A text input field.
- Confirm Password:** A text input field.

At the bottom right of the form area, there are two buttons: "Save" and "Close". The browser's status bar at the bottom shows "Done" and the IP address "129.148.97.113".



5. **Type a user name in the User Name text field.**  
The user name can include up to 35 characters. It must start with an alphabetic character and cannot contain spaces.
6. **Select either Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) in the Authentication Protocol drop-down list.**
7. **Type a password in the Authentication Password text field.**  
The authentication password must contain 8 to 16 characters, with no colons or space characters. It is case-sensitive.
8. **Retype the authentication password in the Confirm Password text field.**
9. **Select read-only (ro) or read-write (rw) in the Permissions drop-down list.**
10. **Select DES or None in the Privacy Protocol drop-down list.**
11. **Type a password in the Privacy Password text field.**  
The privacy password must contain 8 to 16 characters, with no colons or space characters. It is case-sensitive.
12. **Retype the password in the Confirm Password text field.**
13. **Click Save.**

## ▼ Delete an SNMP User Account Using the Web Interface

Follow these steps to delete an SNMP v3 user account:

1. **Log in to ILOM as an Administrator to open the web interface.**  
You can modify SNMP settings only when logged in to accounts with Administrator privileges.
2. **Select Configuration --> System Management Access --> SNMP.**  
The SNMP Settings page appears.
3. **Click the Users link or scroll down to the SNMP Users list.**
4. **Select the radio button of the SNMP user account to delete.**
5. **Click Delete under the SNMP User's List.**  
A confirmation dialog box opens.
6. **Click OK to delete the user account.**

## ▼ Add or Edit an SNMP Community Using the Web Interface

Follow these steps to add or edit an SNMP v1 or v2c community:

- 1. Log in to ILOM as an Administrator to open the web interface.**  
You can add or edit SNMP communities only when logged in to accounts with Administrator privileges.
- 2. Select Configuration --> System Management Access --> SNMP.**  
The SNMP Settings page appears.
- 3. Click the Communities link or scroll down to the Communities list.**
- 4. Click the Add or Edit button for the SNMP Communities list.**  
The Add or Edit dialog box appears.
- 5. Type the name of the community in the Community Name field.**  
The community name can contain up to 35 characters. It must start with an alphabetic character and cannot contain a space.
- 6. Select read-only (ro) or read-write (rw) in the Permissions drop-down list.**
- 7. Click Save.**

## ▼ Delete an SNMP Community Using the Web Interface

Follow these steps to delete an SNMP v1 or v2c community:

- 1. Log in to ILOM as an Administrator to open the web interface.**  
You can delete an SNMP community only when logged in to accounts with Administrator privileges.
- 2. Select Configuration --> System Management Access --> SNMP.**  
The SNMP Settings page appears.
- 3. Click the Communities link or scroll down to the Communities list.**
- 4. Select the radio button of the SNMP community to delete.**
- 5. Click Delete.**  
A confirmation dialog box appears.
- 6. Click OK to delete the SNMP community.**

## ▼ Configure SNMP Trap Destinations Using the Web Interface

Follow these steps to configure the destinations to which the SNMP traps are sent.

**1. Log in to ILOM as an Administrator to open the web interface.**

You can configure SNMP trap destinations only when logged in to accounts with Administrator privileges.

**2. Select Configuration --> Alert Management.**

The Alert Settings page appears. This page shows the table of configured alerts.

**3. To modify an alert, select an alert radio button.**

**4. From the Actions drop-down list, select Edit.**

The Create or Modify Alert dialog appears.

**5. In the dialog, select the level of the alert from the drop-down list.**

**6. In the Type drop-down list, select SNMP Trap.**

**7. Specify the SNMP Trap destination IP address, destination port (selecting Autoselect sets the destination port to the default port 162), SNMP version, or community or user name.**

**8. Click Save for your changes to take effect.**

---

## SNMP Examples

This section includes various examples of using `net-snmp` to query the SNMP agent on an ILOM SP.

To begin, download and install the latest version (version 5.2.1 or higher) of `net-snmp` that works with the operating system of your management station:

<http://net-snmp.sourceforge.net/>

`net-snmp` installs all the standard MIBs (SNMPv2-MIB, SNMP-FRAMEWORK-MIB and ENTITY-MIB) that ILOM supports. You must download the SUN-PLATFORM-MIB.mib, SUN-ILOM-CONTROL-MIB.mib, SUN-HW-TRAP-MIB.mib and SUN-ILOM-PET-MIB.mib files and place those files in the directory where `net-snmp` tools load MIBs. See the following URL for additional information:

[http://net-snmp.sourceforge.net/wiki/index.php/TUT:Using\\_and\\_loading\\_MIBS](http://net-snmp.sourceforge.net/wiki/index.php/TUT:Using_and_loading_MIBS)

For additional information about SNMP, go to the following URLs:

- <http://www.snmpblink.org/>
- <http://www.snmpblink.org/Tools.html>

## ▼ View and Configure SNMP Settings

Configure your SP or CMM as described in the previous sections and then follow these steps to view and configure SNMP settings:

1. **Go to the `/SP/services/snmp` directory by typing:**

```
-> cd /SP/services/snmp
```

2. **Within that directory, type the `show` command to view SNMP settings.**

```
-> show  
/SP/services/snmp  
Targets:  
  communities  
  users  
Properties:  
  engineid = none  
  port = 161  
  sets = disabled  
  v1 = disabled  
  v2c = disabled  
  v3 = enabled  
Commands:  
  cd  
  set  
  show
```

3. **Configure SNMP settings.**

For example:

- Set v2c to enabled by typing:  
-> **set v2c=enabled**
- Set sets to enabled by typing:  
-> **set sets=enabled**

#### 4. View the communities by typing:

```
-> show communities
```

```
-> show communities
/SP/services/snmp/communities
Targets:
  public
Properties:
Commands:
  cd
  create
  delete
  show
```

#### 5. View the public communities by typing:

```
-> show communities/public
```

```
-> show communities/public
/SP/services/snmp/communities/public
Targets:
Properties:
  permission = ro
Commands:
  cd
  set
  show
```

#### 6. Create private communities with read/write access by typing:

```
-> create communities/private permission=rw
```

## ▼ Obtain Information Using snmpget or snmpwalk net-snmp Commands

### 1. Type the the snmpget command to obtain specific information.

For example:

```
$ snmpget -v 2c -c public -m ALL <sp_ip> sysObjectID.0 sysUpTime.0 sysLocation.0
SNMPv2-MIB::sysObjectID.0 =
OID:SUN-FIRE-SMI-MIB::sunBladeX8400ServerModule
SNMPv2-MIB::sysUpTime.0 = Timeticks: (17523) 0:02:55.23
SNMPv2-MIB::sysLocation.0 = STRING:
```

## 2. Type the `snmpwalk` command to obtain information about discrete components.

For example:

```
$ snmpwalk -v 2c -c public -m ALL <sp_ip> entPhysicalName
ENTITY-MIB::entPhysicalName.1 = STRING: /SYS
ENTITY-MIB::entPhysicalName.2 = STRING: /SYS/OK2RM
ENTITY-MIB::entPhysicalName.3 = STRING: /SYS/SERVICE
ENTITY-MIB::entPhysicalName.4 = STRING: /SYS/OK
ENTITY-MIB::entPhysicalName.5 = STRING: /SYS/LOCATE
ENTITY-MIB::entPhysicalName.6 = STRING: /SYS/LOCATE_BTN
ENTITY-MIB::entPhysicalName.7 = STRING: /SYS/POWER_BTN
ENTITY-MIB::entPhysicalName.8 = STRING: /SYS/T_AMB
ENTITY-MIB::entPhysicalName.9 = STRING: /SYS/P0
```

## ▼ Set Information Using `snmpset`

- Type the `snmpset` command to change the location of devices.

For example:

```
$ snmpset -v 2c -c private -m ALL <sp_ip> sysLocation.0 s "<location>"
```

For example:

```
SNMPv2-MIB::sysLocation.0 = STRING: ILOM Dev Lab
```

## ▼ Receive Traps Using `snmptrapd`

- Type the `snmptrapd` command to receive trap information.

For example:

```
$ /usr/sbin/snmptrapd -m ALL -f -Lo
SNMP trap example:
2007-05-21 08:46:41 ban3c9sp4 [10.8.136.94]:
SNMPv2-MIB::sysUpTime.0 = Timeticks: (1418) 0:00:14.18
SNMPv2-MIB::snmpTrapOID.0 = OID:
SUN-HW-TRAP-MIB::sunHwTrapPowerSupplyError
SUN-HW-TRAP-MIB::sunHwTrapSystemIdentifier.0 = STRING:
SUN-HW-TRAP-MIB::sunHwTrapChassisId.0 = STRING:
ban6c4::0000000000 SUN-HW-TRAP-MIB::sunHwTrapProductName.0
= STRING: SUN-HW-TRAP-MIB::sunHwTrapComponentName.0 =
STRING: /PS3/FAN_ERR
SUN-HW-TRAP-MIB::sunHwTrapAdditionalInfo.0 = STRING: Predictive
Failure Asserted SUN-HW-TRAP-MIB::sunHwTrapAssocObjectId.0 =
OID: SNMPv2-SMI::zeroDotZero
```

# Update ILOM Firmware

---

The ILOM firmware update process enables you to install new ILOM firmware and update other modules for your platform, such as BIOS on x64, OpenBoot PROM, and Hypervisor software on SPARC.

This chapter includes the following sections:

- [“Firmware Update Process” on page 214](#)
  - [“ILOM Firmware Update Overview” on page 214](#)
  - [“View ILOM Version Information Using the CLI” on page 215](#)
  - [“View ILOM Version Information Using the Web Interface” on page 216](#)
  - [“Download New Firmware” on page 217](#)
  - [“Update ILOM Firmware Using the CLI” on page 218](#)
  - [“Update ILOM Firmware Using the Web Interface” on page 219](#)
  - [“Update ILOM Firmware Using Sun xVM Ops Center” on page 221](#)
  - [“Reset ILOM SP” on page 221](#)
  - [“Reset SP to Factory Defaults Using the CLI” on page 222](#)
  - [“Reset SP to Factory Defaults Using the Web Interface” on page 222](#)

---

# Firmware Update Process

Review these cautions and these guidelines when updating the firmware.



---

**Caution** – Shut down your host operating system before proceeding. ILOM attempts to shut down the OS gracefully. If a graceful shutdown is not possible, ILOM forces a shutdown, which could cause filesystem corruption.

---



---

**Caution** – ILOM enters a special mode to load new firmware. No other tasks can be performed in ILOM until the firmware upgrade is complete and the ILOM is reset. To ensure a successful update, do *not* attempt to modify the ILOM configuration, or use other ILOM Web, CLI, SNMP, or IPMI interfaces, during the flash update process. Wait until after the update succeeds before making further ILOM configuration changes. The update process requires less than 20 minutes to complete.

---

- The firmware update process takes about five minutes to complete. During this time, no other tasks should be performed in ILOM.
- A network failure during the firmware file upload results in a time-out. This causes ILOM to reboot with the *currently* installed version of ILOM firmware.
- When updating to a later firmware release, the preserve configuration option (when enabled) saves your existing configuration in ILOM and restores the configuration after the update process is completed.

## ILOM Firmware Update Overview

1. View ILOM version information.
2. Download the new firmware image.
3. Copy the image to a TFTP server for a CLI update or to a local file system for a web interface update.
4. Log in as any user with Administrator privileges.
5. Update the firmware on each service processor (SP) and/or Chassis Monitoring Module (CMM) in the system using the CLI or the web interface.
6. When the firmware update is complete, the system *automatically* reboots.



## ▼ View ILOM Version Information Using the CLI

You can view ILOM version information using either of the following methods:

- Using the CLI Through the Management Ethernet Port
- Using the CLI Through the Serial Port

### Using the CLI Through the Management Ethernet Port

1. **Connect an RJ-45 Ethernet cable to the NET MGT Ethernet port.**

Establish an SSH connection using the following command:

```
# ssh -l root sp_ip_address
```

where *sp\_ip\_address* is the IP address of the server's service processor.

Enter the default password when you are prompted:

```
changeme
```

2. **After you have successfully logged in, the SP displays its default command prompt:**

```
->
```

3. **Type the `version` command, which returns output similar to the following:**

```
-> version
```

```
SP firmware version: 2.0
```

```
SP firmware build number: 10644
```

```
SP firmware date: Tue Sep 13 12:50:37 PDT 2007
```

```
SP filesystem version: 0.1.13
```

The ILOM (SP) firmware version and build number are listed above.

### Using the CLI Through the Serial Port

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
```

```
Disable hardware flow control (CTS/RTS)
```

```
Disable software flow control (XON/XOFF)
```

2. **If needed, connect a dongle cable to the server module.**

3. Connect a serial cable from the RJ-45 SER MGT port on the server module dongle or server's back panel to your terminal device or PC.
4. Press **Enter** on the terminal device to establish a connection between that terminal device and the server's SP.

The SP displays a login prompt.

```
SUNSP0003BA84D777 login:
```

Here, 0003BA84D777 is the Ethernet MAC address of the SP. This will be different for each server.

5. Log in to the ILOM SP and type the default user name (`root`) with the default password (`changeme`).

After you have successfully logged in, the SP displays its default command prompt:

```
->
```

6. Type the `version` command, which returns output similar to the following:

```
-> version
```

```
SP firmware version: 2.0
```

```
SP firmware build number: 10644
```

```
SP firmware date: Tue Sep 13 12:50:37 PDT 2007
```

```
SP filesystem version: 0.1.13
```

The ILOM firmware version and build number are listed above.

## ▼ View ILOM Version Information Using the Web Interface

1. Log in to the ILOM web interface.
2. Select System Information -->Version.

The current firmware version information appears.

## ▼ Download New Firmware

The procedure to download the new firmware image differs between x64-based systems and SPARC-based systems. Follow the procedure below that applies to your platform.

### Downloading New Firmware on x64-Based Systems

Download the flash image .ima file using these steps:

1. **Navigate to <http://www.sun.com/download/>**
2. **Locate the Hardware Drivers section.**
3. **Click the X64 Servers and Workstations.**
4. **Click the link for the Integrated Lights Out Manager (ILOM) Server software release version that you want.**
5. **Click Download.**
6. **Select the Platform and Language for your download.**
7. **Enter your Username and Password.**  
If you do not have a Username and Password, you can register free of charge by clicking **Register Now**.
8. **Click Accept License Agreement.**
9. **Click the appropriate firmware image file name:**  
`ilom.firmware.ima`  
For example:  
`ilom.X6220-2.0.3.2-r26980.ima`
10. **Go to “Update ILOM Firmware Using the CLI” on page 218 or “Update ILOM Firmware Using the Web Interface” on page 219.**

### Downloading New Firmware on SPARC-Based Systems

1. **Navigate to <http://sunsolve.sun.com>**
2. **Click Accept to accept the License Agreement.**
3. **Click on Patches and Updates.**

4. Under the heading **Download Product-Specific Patches**, click on **Product Patches**.
5. Under the heading **Hardware**, in the **PROM** row, click on **Sun System Firmware**.
6. Select the latest firmware update for your server. Confirm your choice by clicking on the associated **Readme** link and read the patch update information.
7. Click **HTTP** to download the zip file package.
8. Put the zip package on a TFTP server that is accessible from your network.
9. Unzip the package.
10. Go to [“Update ILOM Firmware Using the CLI” on page 218](#) or [“Update ILOM Firmware Using the Web Interface” on page 219](#).

## ▼ Update ILOM Firmware Using the CLI

1. Log in to the ILOM CLI through the Management Ethernet Port (see [“Using the CLI Through the Management Ethernet Port” on page 215](#)) or the serial port (see [“Using the CLI Through the Serial Port” on page 215](#)).

2. From the ILOM CLI, use the following command:

```
-> load -source tftp://tftpserver/ilom.firmware.xxx
```

where *tftpserver* is the TFTP server that contains the update and *ilom.firmware.xxx* is the firmware image file, for example:

```
ilom.X6220-2.0.3.2-r26980.ima
```

3. At the prompt for confirming that you want to load the specified file, type **y** for yes or **n** for no.
4. At the preserve configuration prompt, type **y** for yes or **n** for n.

The system loads the specified firmware file then automatically reboots to complete the firmware update.

5. Reconnect to the ILOM server SP or CMM using an SSH connection.
6. Verify that the proper firmware version was installed. Type:

```
-> version
```

For example:

```
-> load -source tftp://xxx.xxx.xxx.xxx/ilom.filename.xxx
```

NOTE: A firmware upgrade will cause the server and ILOM to

```

be reset. It is recommended that a clean shutdown of
the server be done prior to the upgrade procedure.
An upgrade takes about 6 minutes to complete. ILOM
will enter a special mode to load new firmware. No
other tasks can be performed in ILOM until the
firmware upgrade is complete and ILOM is reset.

Are you sure you want to load the specified file (y/n)? y
Do you want to preserve the configuration (y/n)? y
. . . . .
Preserving configuration. Please wait.
Done preserving configuration.

Firmware update is complete.
ILOM will now be restarted with the new firmware.

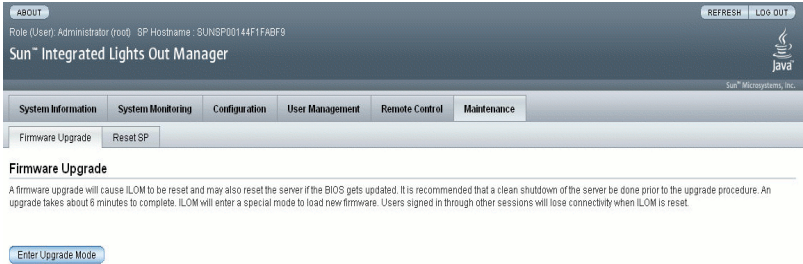
```

## ▼ Update ILOM Firmware Using the Web Interface

**Note** – The web interface screens and options that are available to you during the firmware upgrade process might differ from the information presented in this procedure. Refer to your platform ILOM Supplement for platform-specific information.

1. Log in to the ILOM web interface as Administrator.
2. Select Maintenance --> Firmware Upgrade.  
The Firmware Upgrade page appears.

**FIGURE 11-1** Firmware Upgrade Page



**3. Click Enter Upgrade Mode.**

A dialog box appears asking you to confirm that you want to enter Upgrade mode.

**4. Click OK to enter Upgrade mode or Cancel to exit the process.**

ILOM stops its normal operation and prepares for a flash upgrade.

**5. Enter the path to the new ILOM flash image file in the Select Image File to Upload field or click Browse to locate and select the firmware update file.**

Files with either .pkg or .ima extensions can be used.

**6. Click Upload or Cancel to exit the process.**

The selected file is uploaded and verified as the correct image update for your SP or CMM.

This process takes about one minute with a fast network connection.

The Verify Firmware Image page appears.

**7. In the Verify Firmware Image page, click OK.**

**8. Select Preserve Configuration to keep your existing ILOM configuration settings. If you do not preserve your configuration, the settings will be overwritten by the firmware defaults.**

**9. Click Start Upgrade or click Cancel to exit the process.**

When you click Start Upgrade, a progress screen indicates that the firmware image is being updated. Once the update progress reaches 100%, the firmware update is complete.

When the update is complete, the system *automatically* reboots.

**10. After the SP and/or CMM finishes rebooting, use your browser to reconnect to ILOM.**

---

**Note** – The ILOM web interface might not refresh properly after the update completes. If the ILOM web page looks wrong, is missing information, or displays an error message, you may be viewing a cached version of the page from the version previous to the update. Clear your browser cache and refresh your browser before continuing.

---

## ▼ Update ILOM Firmware Using Sun xVM Ops Center

You can use the Sun xVM Ops Center to update your ILOM firmware.

- Follow the instructions for the Sun xVM Ops Center at:

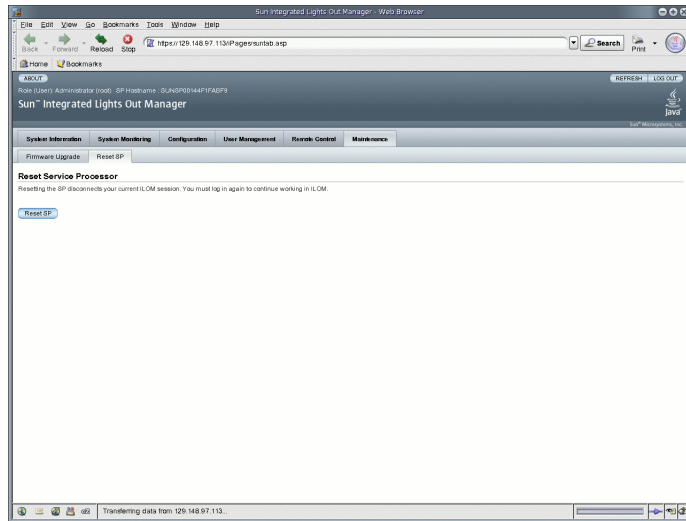
<http://wikis.sun.com/display/xvm0C1dot1/Home>

## ▼ Reset ILOM SP

After updating the ILOM/BIOS firmware, you must reset the ILOM SP.

- To reset the ILOM SP, you can do any of the following:
  - From the ILOM SP web interface, navigate to the Maintenance tab and the Reset SP tab, and then click the Reset SP button.

FIGURE 11-2 Reset Service Processor Page



- From the ILOM CLI, use the following command:

```
reset /SP
```
- Using IPMITool, use the following command:

```
ipmitool -U root -P password -H SP-IP bmc reset cold
```

where *SP-IP* is the IP address of the service processor.
- Reset the ILOM SP by shutting down the host, then removing and restoring AC power cords to the system.

## ▼ Reset SP to Factory Defaults Using the CLI

1. Log in to the ILOM CLI as Administrator.

2. Type the following command:

```
-> set reset_to_defaults=option
```

Where *option* is:

- **All** - (For x64-based systems and SPARC-based systems) Select this option if you want to erase the existing ILOM configuration file. When the ILOM reboots, the configuration file that was included in the SP firmware is used.
- **Factory** - (For x64-based systems only) Select this option if you want to erase the existing configuration file and the internal log files. When the SP reboots, the configuration file that was included in the SP firmware is used instead and the log files are erased.
- **None** - (For x64-based systems and SPARC-based systems) Select this option if you want to cancel the request you initiated previously. To cancel a previously initiated reset operation, you must initiate a reset operation with the None option before the ILOM SP reboots.

## ▼ Reset SP to Factory Defaults Using the Web Interface

1. Log in to the ILOM web interface as Administrator.

2. Select Maintenance --> Configuration Management.

The Configuration Management page appears.

3. In the Reset Defaults drop-down list box, select one of these options:

- **All** - (For x64-based systems and SPARC-based systems) Select this option if you want to erase the existing ILOM configuration file. When the ILOM reboots, the configuration file that was included in the SP firmware is used.
- **Factory** - (For x64-based systems only) Select this option if you want to erase the existing configuration file and the internal log files. When the SP reboots, the configuration file that was included in the SP firmware is used instead and the log files are erased.
- **None** - (For x64-based systems and SPARC-based systems) Select this option if you want to cancel the request you initiated previously. To cancel a previously initiated reset operation, you must initiate a reset operation with the None option before the ILOM SP reboots.

4. Click Reset Defaults.

The SP configuration is restored to the factory settings.





# Remote Management of x64 Servers Using the Sun ILOM Remote Console

---

The Sun ILOM Remote Console is supported on all Sun x64 processor-based servers. The Sun ILOM Remote Console is currently not supported on Sun SPARC servers.

This chapter includes the following sections:

- [“Sun ILOM Remote Console Overview” on page 224](#)
  - [“Single or Multiple Remote Host Server Management Views” on page 224](#)
  - [“Installation Requirements” on page 226](#)
  - [“Network Communication Ports and Protocols” on page 227](#)
  - [“Administrator Role User Account – Sign In Authentication Required” on page 227](#)
- [“Launch and Configure ILOM for Remote Management” on page 228](#)
  - [“Connect to the ILOM Web Interface” on page 228](#)
  - [“Configure ILOM Remote Control Settings Using the Web Interface” on page 229](#)
- [“Launch and Configure Sun ILOM Remote Console for Remote x64 Server Management” on page 232](#)
  - [“Launch the Sun ILOM Remote Console Using the ILOM Web Interface” on page 232](#)
  - [“Add a New Server Session” on page 234](#)
  - [“Start, Stop, or Restart Device Redirection” on page 234](#)
  - [“Redirect Keyboard and Mouse Devices” on page 235](#)
  - [“Control Keyboard Modes and Key Send Options” on page 235](#)
  - [“Redirect Storage Devices” on page 236](#)
  - [“Exit the Sun ILOM Remote Console” on page 238](#)
- [“CD and Diskette Redirection Operation Scenarios” on page 238](#)

---

# Sun ILOM Remote Console Overview

The Sun ILOM Remote Console is a Java application that you can launch from the ILOM web interface. When you use the Sun ILOM Remote Console, you can remotely redirect and control the following devices on a remote x64 host server:

- Keyboard
- Mouse
- Video console display
- Storage devices or images (CD/DVD, floppy device)

The Sun ILOM Remote Console enables the devices on your local client to behave as if they were directly attached to the remote host server. For instance, the redirection functionality, using a network connection to the remote host server, enables you to do the following:

- Install software from your local media drive to a remote host server.
- Run command-line utilities on a remote host server from a local client.
- Access and run GUI-based programs on a remote host server from a local client.
- Remotely configure x64 processor-based server features from a local client.
- Remotely manage x64 processor-based server policies from a local client.
- Remotely monitor x64 processor-based server elements from a local client.
- Perform almost any x64 processor-based software task from a local client that you normally could perform while sitting at a remote host server.

## Single or Multiple Remote Host Server Management Views

The Sun ILOM Remote Console supports both single and multiple remote server management views. Single and multiple server management views are currently supported on all x64 processor-based servers.

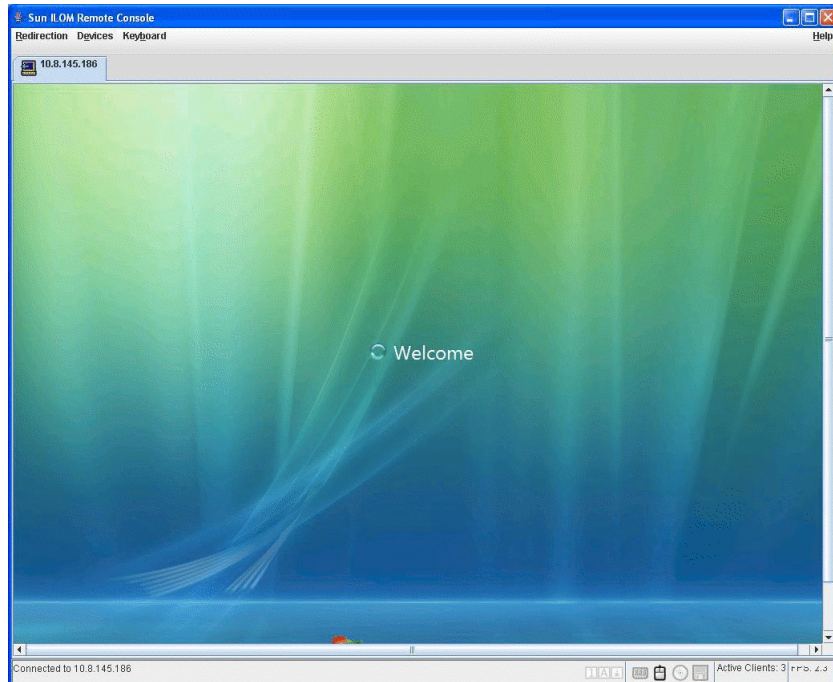
- **Single x64 Remote Server Management View** – You can launch the Sun ILOM Remote Console to manage a single remote host server from one window and utilize the remote Keyboard, Video, Mouse, Storage (KVMS) features.

---

**Note** – Single remote server management views are supported when you connect to the IP address of any x64 server service processor (SP). For more information, see [“Launch and Configure Sun ILOM Remote Console for Remote x64 Server Management”](#) on page 232.

---

**FIGURE 12-1** Single Server Management View



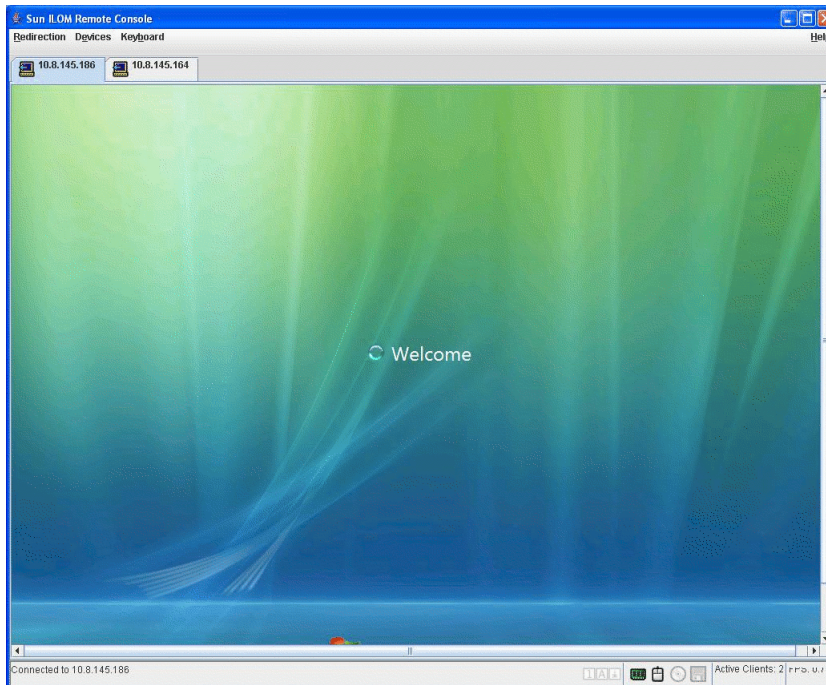
- **Multiple x64 Remote Server Management Views** – You can launch the Sun ILOM Remote Console to manage multiple remote x64 servers from one window and utilize the remote Keyboard, Video, Mouse, Storage (KVMS) features.

---

**Note** – Multiple remote server management views are supported when you either: (1) connect to the IP address of any x64 blade server chassis Chassis Monitoring Module (CMM); or (2) add a new Sun ILOM Remote Control session to manage another remote x64 server. For more information, see [“Launch and Configure Sun ILOM Remote Console for Remote x64 Server Management”](#) on page 232.

---

**FIGURE 12-2** Multiple Server Management Views



## Installation Requirements

The Sun ILOM Remote Console does not require you to install any additional hardware or software. It is built into the ILOM software. However, to run the Sun ILOM Remote Console, you must have the following software installed on your local client:

- **Web browser** – Supported browsers include: Internet Explorer 6.0 or later; Mozilla 1.7.5 or later; Mozilla Fire Fox 1.0 or later.
- **JRE 1.5 or higher (Java 5.0 or higher)** – To download the Java 1.5 runtime environment, see <http://java.com>.

# Network Communication Ports and Protocols

The Sun ILOM Remote Console communicates to a remote host server SP using the following network ports and protocols.

**TABLE 12-1** SP ILOM Remote Console Network Ports and Protocols

Port	Protocol	SP - ILOM Remote Console
5120	TCP	CD
5123	TCP	Diskette
5121	TCP	Keyboard and mouse
7578	TCP	Video

---

**Note** – When remotely managing servers using the CMM ILOM, you must configure access to all of the SP Remote Console ports (5120, 5121, 5123, nd 7578).

---

## Administrator Role User Account - Sign In Authentication Required

To launch the Sun ILOM Remote Console from the ILOM web interface, you must initially log in to ILOM with an Administrator role account (Administrator role-based user name and password).

- If you signed in to ILOM with an *Operator role account* and attempted to launch the Sun ILOM Remote Console, ILOM will prompt you to sign in with a valid Administrator role account using the Login dialog.
- If you initially signed in to ILOM with an *Administrator role account* and launched the Sun ILOM Remote Console, the redirection page for the Sun ILOM Remote Console automatically appears. However, the Sun ILOM Remote Console will prompt you to sign in each time you stop and start the redirection, or restart the redirection.

---

**Note** – If the Single Sign On feature is disabled in ILOM, users with Administrator role privileges will be prompted to sign in to ILOM again using the Login dialog. For additional information about the Single Sign On feature, see [“Single Sign On” on page 63](#).

---

---

# Launch and Configure ILOM for Remote Management

Prior to launching the Sun ILOM Remote Console, you must launch the ILOM web interface and configure ILOM for remote management.

- **Connect to the ILOM web interface** – You must connect to the ILOM web interface of the server (SP or CMM) that you want to remotely manage. For instructions, see [“Connect to the ILOM Web Interface” on page 228](#).
- **Configure ILOM remote control settings** – Prior to remotely managing a Sun x64 server using the Sun ILOM Remote Console, you must initially configure ILOM settings for remote management: *console redirection*, *supported mouse mode*, *remote host power states*, as well as *start-up PC-Check diagnostic tests*. For more information, see [“Configure ILOM Remote Control Settings Using the Web Interface” on page 229](#).

---

**Note** – Typically you will set up the remote management control settings once in ILOM with the exception of the remote host power states.

---

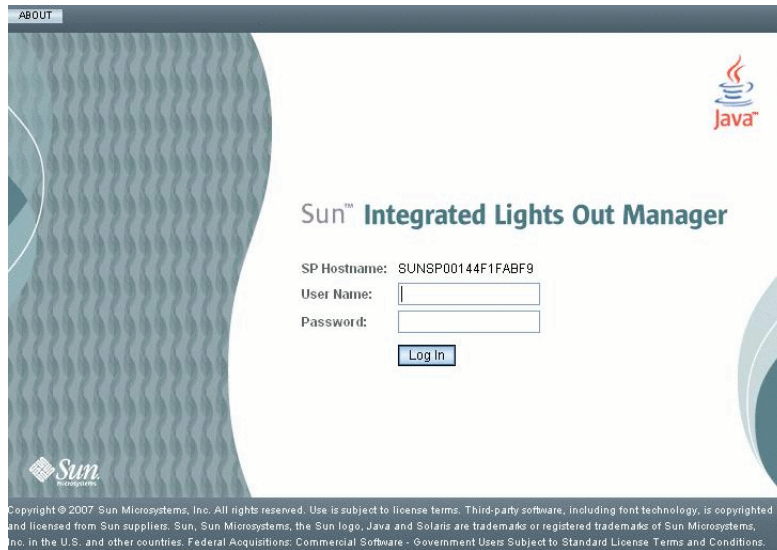
## ▼ Connect to the ILOM Web Interface

Follow these steps to connect to the ILOM web interface:

1. **Open a web browser and specify the IP address of an x64 server SP or x64 CMM that you want to remotely manage, then press Enter.**

The ILOM Login page appears.

**FIGURE 12-3** ILOM Login Page



2. In the ILOM Login page, enter the user name and password of a valid Administrator role account, then press Enter.

---

**Tip** – The preconfigured Administrator role account shipped with ILOM is `root/` `changeme`. For additional information about this preconfigured account, see [“Preconfigured ILOM Administrator Accounts”](#) on page 60.

---

## ▼ Configure ILOM Remote Control Settings Using the Web Interface

### Prerequisite:

- Established connection to the remote host server ILOM web interface (SP or CMM). For instructions, see [“Connect to the ILOM Web Interface”](#) on page 228.

Follow these steps to configure ILOM settings for remote management:

1. In the CMM or SP ILOM web interface, click the Remote Control tab.
  - **For the SP ILOM web interface.** The Remote Control page appears displaying four sub-tabs: *Redirection*, *Remote Power Control*, *Mouse Mode Settings*, and *Diagnostics*.

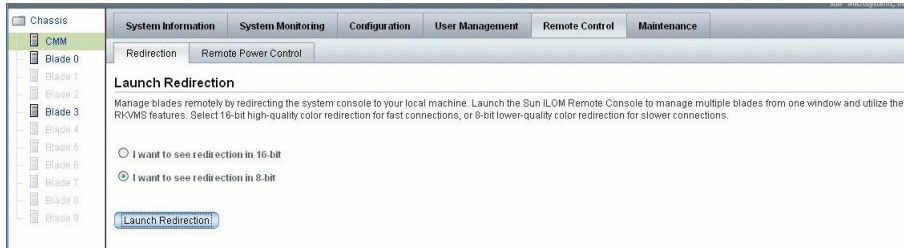


**FIGURE 12-4** SP ILOM – Remote Control Tab



- **For the CMM ILOM web interface.** The Remote Control page appears displaying two sub-tabs: *Redirection* and *Remote Power Control*.

**FIGURE 12-5** CMM ILOM – Remote Control Tab



---

**Note** – Alternatively, you can configure the remote control settings for each server SP associated with the CMM. To access the remote control settings for other server SPs listed in the CMM ILOM web interface, click the server SP in the left frame of the page, then click the Remote Control tab in the right frame of the page.

---

## 2. In the Remote Control page, set the following remote control settings.

**TABLE 12-2** Remote Control Settings

Setting	Action
Console Redirection Settings	<p>Click the Redirection tab and select one of the following console color redirection options:</p> <ul style="list-style-type: none"> <li>• <b>8-bit.</b> Select 8-bit redirection for slower network connections.</li> <li>• <b>16-bit.</b> Select 16-bit redirection for faster network connections.</li> </ul>
Mouse Mode Settings (SP Setting Only)	<p>Click the Mouse Mode Settings tab and select one of the following mouse mode settings:</p> <ul style="list-style-type: none"> <li>• <b>Absolute.</b> Select Absolute Mouse Mode for best performance when you are using Solaris or Windows operating systems. Absolute is the default.</li> <li>• <b>Relative.</b> Select Relative Mouse Mode when you are using a Linux operating system. Note that newer Linux operating systems (RHEL v5 or SUSE v10, or later) support Absolute mode.</li> </ul>
Power State Settings	<p>Click the Remote Power Control tab to select one of the following host server power states:</p> <ul style="list-style-type: none"> <li>• <b>Immediate Power Off.</b> Select Immediate Power Off to immediately turn off the power to the remote host server.</li> <li>• <b>Graceful Shutdown and Power Off.</b> Select Graceful Shutdown and Power Off to attempt to shut down the OS gracefully prior to powering off the remote host server.</li> <li>• <b>Power On.</b> Select Power On to turn on full power to the remote host server. Power On is the default.</li> <li>• <b>Power Cycle.</b> Select Power Cycle to immediately turn off the power on the remote host server, then apply full power to the remote host server.</li> <li>• <b>Reset.</b> Select Reset to immediately reboot the remote host server.</li> </ul>
PC-Check Diagnostic Settings (SP Setting Only)	<p>Click the Diagnostics tab to enable or disable the following PC-Check diagnostic settings:</p> <ul style="list-style-type: none"> <li>• <b>Disabled.</b> Select Disabled if you do not want to run PC-Check diagnostic tests when starting a remote host server.</li> <li>• <b>Enabled.</b> Select Enabled if you want to run basic PC-Check diagnostic tests upon start-up of the remote host server. These basic diagnostic tests typically take 3 minutes to complete.</li> <li>• <b>Extended.</b> Select Extended if you want to run extended PC-Check diagnostic tests upon start-up of the remote host server. These extended diagnostic tests typically take 30 minutes to complete.</li> <li>• <b>Manual.</b> Select Manual if you want to determine which PC-Check diagnostic tests to run upon start-up of the remote host server.</li> </ul>
<p><b>Note:</b> The PC-Check setting is supported on some x64 systems. Refer to your platform ILOM Supplement to determine whether PC-Check is supported on a specific platform.</p>	

---

# Launch and Configure Sun ILOM Remote Console for Remote x64 Server Management

To manage an x64 server remotely, you must launch the Sun ILOM Remote Console and configure the console features, as needed, for remote management. For more information, see these procedures:

- [“Launch the Sun ILOM Remote Console Using the ILOM Web Interface” on page 232](#)
- [“Add a New Server Session” on page 234](#)
- [“Start, Stop, or Restart Device Redirection” on page 234](#)
- [“Redirect Keyboard and Mouse Devices” on page 235](#)
- [“Control Keyboard Modes and Key Send Options” on page 235](#)
- [“Redirect Storage Devices” on page 236](#)
- [“Start, Stop, or Restart Device Redirection” on page 234](#)
- [“Exit the Sun ILOM Remote Console” on page 238](#)

## ▼ Launch the Sun ILOM Remote Console Using the ILOM Web Interface

### Prerequisites:

- Established connection to the ILOM web interface (SP or CMM). For instructions, see [“Connect to the ILOM Web Interface” on page 228](#).
- Configured ILOM Remote Control Settings. For instructions, see [“Configure ILOM Remote Control Settings Using the Web Interface” on page 229](#).

To launch the Sun ILOM Remote Console using the ILOM web interface, follow these steps:

1. **In the ILOM web interface for either a server SP or CMM SP, click the Remote Control tab.**

The Remote Console page appears.

**2. In the Remote Console page, click the Redirection tab.**

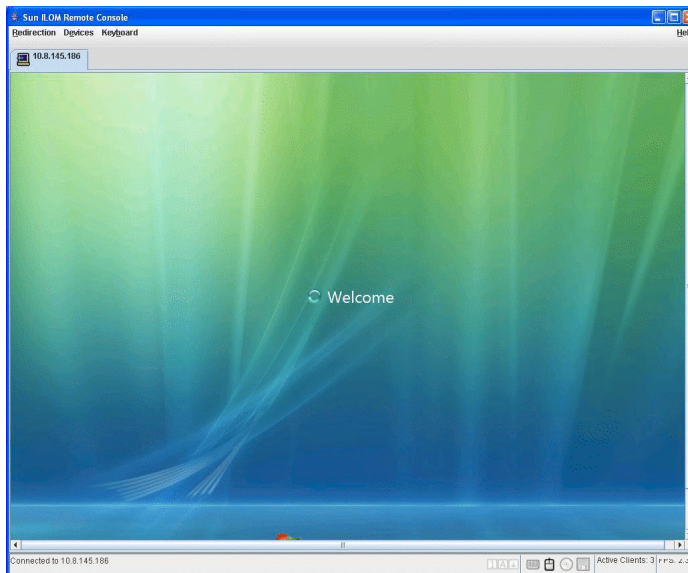
The Redirection page appears.

**3. In the Redirection page, click Launch Redirection.**

A certificate warning message might appear stating that the name of the site does not match the name on the certificate. If this message appears, click Run to continue.

The Sun ILOM Remote Console window appears. If you connected to an x64 server SP then one server session tab appears. If you connected to an x64 CMM then multiple server session tabs could appear (one tab for each server in the chassis).

**FIGURE 12-6** Sun ILOM Remote Console



---

**Note** – If applicable, you can alternatively launch the Sun ILOM Remote Console for each server SP listed in the CMM ILOM web interface. To launch the Sun ILOM Remote Console for a server associated with a CMM, click the server SP in left frame of the page, then click Remote Console --> Redirection --> Launch Redirection.

---

## ▼ Add a New Server Session

### Prerequisite:

- Established connection to the Sun ILOM Remote Console. For instructions, see [“Launch the Sun ILOM Remote Console Using the ILOM Web Interface” on page 232.](#)

Follow these steps to add a new server session to the ILOM Remote Console:

1. **In the Sun ILOM Remote Console window, select Redirection --> New Session.**

The New Session Creation dialog appears.

2. **In the New Session Creation dialog, type the IP address of a remote host x64 server SP, then click OK.**

The Login dialog appears.

3. **In the Login dialog, type an Administrator account user name and password.**

A session tab for the newly added remote host server appears in the tab set of the Sun ILOM Remote Console.

## ▼ Start, Stop, or Restart Device Redirection

### Prerequisite:

- Established connection to the Sun ILOM Remote Console. For instructions, see [“Launch the Sun ILOM Remote Console Using the ILOM Web Interface” on page 232.](#)

Follow these steps to start, stop, or restart the redirection of devices:

1. **In the Sun ILOM Remote Console window, click the Redirection menu.**

2. **In the Redirection menu, specify, if necessary, any of the following redirection options:**

Start Redirection	Select Start Redirection to enable redirection of devices. Start Redirection is enabled by default.
Restart Redirection	Select Restart Redirection to stop and start redirection of devices. Typically, this option is used when a valid redirection is still established.
Stop Redirection	Select Stop Redirection to disable the redirection of devices

A confirmation message appears confirming that you want to change the redirection setting.

3. **In the Confirmation message, click Yes to proceed or No to cancel the operation.**

## ▼ Redirect Keyboard and Mouse Devices

### Prerequisite:

- Established connection to the Sun ILOM Remote Console. For instructions, see [“Launch the Sun ILOM Remote Console Using the ILOM Web Interface” on page 232.](#)

Follow these steps to redirect a remote host server keyboard and mouse to your local client:

1. **In the Sun ILOM Remote Console window, do the following:**
  - a. **Select Devices --> Mouse to enable or disable mouse redirection.**  
Enable (checkmark) is the default.
  - b. **Select Devices --> Keyboard to enable or disable keyboard redirection.**  
Enable (checkmark) is the default.

## ▼ Control Keyboard Modes and Key Send Options

### Prerequisite:

- Established connection to the Sun ILOM Remote Console. For instructions, see [“Launch the Sun ILOM Remote Console Using the ILOM Web Interface” on page 232.](#)

Follow these steps to control keyboard modes and individual key send options:

1. **In the Sun ILOM Remote Console window, click the Keyboard menu.**
2. **In the Keyboard menu, specify, if necessary, any of the following keyboard settings.**

Auto-keybreak Mode	Select Auto-keybreak Mode to automatically send a keybreak after every key press. Use this option to help resolve keyboard problems over slow network connections. The Auto-keybreak Mode is enabled by default.
Stateful Key Locking	Select Stateful Key Locking if your client uses stateful key locking (Solaris with XSun, OSX). Stateful Key Locking applies to these three lock keys: Caps Lock, Num Lock, and Scroll Lock.
Left Alt Key	Select the Left Alt Key to toggle the left Alt Key on or off.

Right Alt Key	Select Right Alt Key to toggle the right Alt Key on or off for non-US keyboards. When enabled, this option allows you to type the third key character on a key. This keyboard option provides the same capabilities of an Alt Graph key.
F10	Select F10 to apply the F10 function key (typically used in BIOS).
Control Alt Delete	Select Control Alt Delete to send the Control-Alt-Delete sequence.
Control Space	Select Control Space to send a Control-Space sequence to enable input on remote host.
Caps Lock	Select Caps Lock to send the Caps Lock key to enable input with Russian and Greek keyboards.

## ▼ Redirect Storage Devices

### Prerequisites:

- Established connection to the Sun ILOM Remote Console. For instructions, see [“Launch the Sun ILOM Remote Console Using the ILOM Web Interface” on page 232](#).
- For Solaris client systems, you must perform the following steps prior to redirecting storage devices:
  - If Volume Manager is enabled, you will need to disable this feature.
  - Assign root privilege to the processor that is running the Sun ILOM Remote Console by entering these commands:
 

```
su to root
ppriv -s +file_dac_read pid_javarconsole
```
- Refer to [“CD and Diskette Redirection Operation Scenarios” on page 238](#) for more information.

Follow these steps to redirect a storage device or ISO image:

1. In the Sun ILOM Remote Console window, select the Devices menu.
2. In the Devices menu, do the following:

**a. Enable the appropriate storage device or image setting.**

CD-ROM	Select CD-ROM to enable the local CD device. This option causes your local CD-ROM drive to behave as though it were a CD device directly attached to the remote host server.
Floppy	Select Floppy to enable the local floppy device. This option causes your local floppy drive to behave as though it were a floppy device directly attached to the remote host server.
CD-ROM Image	Select CD-ROM Image to specify the location of a CD-ROM image on your local client or network share.
Floppy Image	Select Floppy Image to specify the location of a floppy image on your local client or network share.

---

**Tip** – There are only two choices for CD/DVD redirection. You can choose to either redirect a CD-ROM drive or redirect a CD-ROM image.

---

---

**Tip** – If you are installing software from distribution CD/DVD, insert the CD/DVD into the redirected drive and select CD-ROM drive.

---

---

**Tip** – If you are installing software from an ISO image, place the ISO image on your local client or network shared file system then select CD-ROM image.

---

A dialog appears prompting you to specify a storage drive location or image file location.

**b. To specify the storage drive location or image file location, do one of the following:**

- In the Drive Selection dialog, select or type a drive location, then click OK.
- or
- In the File Open dialog, browser to the location of the image, then click OK.

**3. To reuse these storage settings on the host at a later time, click Devices --> Save as Host Default.**



## ▼ Exit the Sun ILOM Remote Console

Follow these steps to exit the Sun ILOM Remote Console and close any remote server sessions that might have remained opened:

1. In the Sun ILOM Remote Console window, select the Redirection menu.
2. In the Redirection menu, select Quit.

---

## CD and Diskette Redirection Operation Scenarios

Use the information in [TABLE 12-3](#) to help identify different case scenarios in which the CD drive or diskette drive redirection functionality might behave during a Remote Console session.

**TABLE 12-3** Remote Console Operation With DVD Drive and Diskette Drive

Case	Status	DVD As Seen by Remote Host	Diskette As Seen by Remote Host
1	Remote Console application not started, or Remote Console started but DVD/diskette redirection not started	DVD device present. No medium indication is sent to the host from ILOM when the hosts asks.	Diskette device present. No medium indication is sent to the host from ILOM when the host asks.
2	Remote Console application started with no medium present in the drive	DVD device present. When the host asks, which may be automatic or when you access the device on the host, the remote client sends a status message. In this case, since there is no medium, the status is no medium.	Diskette device present. When the host asks (for example, you double-click on a drive), the remote client sends a status message. In this case since there is no medium, the status is no medium.
3	Remote Console application started with no medium, then medium is inserted	DVD device present. When the hosts asks (automatic or manual), the remote client sends a status message as medium present and also indicates the medium change.	Diskette device present. When the host asks (manual), the remote client sends a status message as medium present and also indicates the medium change.
4	Remote Console application started with medium inserted	Same as case 3.	Same as case 3.
5	Remote Console application started with medium present, then medium is removed	Next command from the host will get a status message indicating medium not present.	Next command from the host will get a status message indicating medium not present.

**TABLE 12-3** Remote Console Operation With DVD Drive and Diskette Drive *(Continued)*

<b>Case</b>	<b>Status</b>	<b>DVD As Seen by Remote Host</b>	<b>Diskette As Seen by Remote Host</b>
6	Remote Console application started with image redirection	Same as case 3.	Same as case 3.
7	Remote Console application started with image, but redirection is stopped (which is the only way to stop ISO redirection)	Driver knows DVD redirection stopped, so it sends a medium absent status on the next host query.	Driver knows DVD redirection stopped so it sends a medium absent status on the next diskette query.
8	Network failure	The software has a keep alive mechanism. The software will detect keep-alive failure since there is no communication and will close the socket, assuming the client is unresponsive. Driver will send a no medium status to the host.	The software has a keep alive mechanism. The software will detect unresponsive client and close the socket, as well as indicate to the driver that the remote connection went away. Driver will send a no medium status to the host.
9	Client crashes	Same as case 8.	Same as case 8.



# ILOM Command-Line Interface Reference

---

This appendix contains the following sections:

- [“CLI Command Quick Reference” on page 241](#)
- [“CLI Command Reference” on page 247](#)

---

## CLI Command Quick Reference

This section contains the most common ILOM commands used to administer your Sun server from the command-line interface (CLI).

---

**Note** – Syntax examples in this chapter use the target starting with */SP/*, which could be interchanged with the target starting with */CMM/* depending on your Sun server platform. Subtargets are common across all Sun server platforms.

---

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

Content	Typeface	Description
Your input	<b>Fixed-width bold</b>	Text that you type. Type it exactly as shown.
Onscreen output	Fixed-width regular	Text that the computer displays

---

**TABLE A-1** Command Syntax and Usage (Continued)

Content	Typeface	Description
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
Show all valid targets	<b>help targets</b>
Log out of the CLI	<b>exit</b>
Display the version of ILOM firmware running on ILOM	<b>version</b>
Display clock information	<b>show /SP/clock</b>
Display all of the CLI commands	<b>show /SP/cli/commands</b>
Display the active ILOM sessions	<b>show /SP/sessions</b>
Display information about commands and targets	<b>help</b>
Display information about a specific command	<b>help create</b>
Update ILOM and BIOS firmware	<b>load -source tftp://newSPimage</b>
Display a list of ILOM event logs	<b>show /SP/logs/event/list</b>

**TABLE A-3** User Commands

Description	Command
Add a local user	<b>create /SP/users/user1 password=password role=administrator operator</b>
Delete a local user	<b>delete /SP/users/user1</b>
Change a local user's properties	<b>set /SP/users/user1 role=operator</b>

**TABLE A-3** User Commands (Continued)

Description	Command
Display information about all local users	<b>show -display</b> [targets properties all] <b>-level all /SP/users</b>
Display information about LDAP settings	<b>show /SP/clients/ldap</b>
Change LDAP settings	<b>set /SP/clients/ldap binddn=proxyuser</b> <b>bindpw=proxyuserpassword</b> <b>defaultrole=administrator operator</b> <b>ipaddress=ipaddress</b>

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

Description	Command
Display network configuration information	<b>show /SP/network</b>
Change network properties for ILOM. Changing certain network properties, like the IP address, will disconnect your active session	<b>set /SP/network pendingipaddress=ipaddress</b> <b>pendingipdiscovery=dhcp static</b> <b>pendingipgateway=ipgateway</b> <b>pendingipnetmask=ipnetmask commitpending=true</b>
Display information about the external serial port	<b>show /SP/serial/external</b>
Change the external serial port configuration	<b>set /SP/serial/external pendingspeed=integer</b> <b>commitpending=true</b>
Display information about the serial connection to the host	<b>show /SP/serial/host</b>
Change the host serial port configuration.	<b>set /SP/serial/host pendingspeed=integer</b> <b>commitpending=true</b>
Note: This speed setting must match the speed setting for serial port 0, COM1 or /dev/ttyS0 on the host operating system	

**TABLE A-5** Alert Management Commands

Description	Command
Display information about alerts. You can configure up to 15 alerts	<b>show /SP/alertmgmt/rules/1...15</b>
Configure an IPMI PET alert	<b>set /SP/alertmgmt/rules/1...15 type=ipmipet destination=ipaddress level=down critical major minor</b>
Configure a v3 SNMP trap alert	<b>set /SP/alertmgmt/rules/1...15 type=snmptrap snmp_version=3 community_or_username=username destination=ipaddress level=down critical major minor</b>
Configure an email alert	<b>set /SP/alertmgmt/rules/1...15 type=email destination=email_address level=down critical major minor</b>

**TABLE A-6** System Management Access Commands

Description	Command
Display information about HTTP settings	<b>show /SP/services/http</b>
Change HTTP settings, such as enabling automatic redirection to HTTPS	<b>set /SP/services/http port=portnumber secureredirect enabled disabled servicestate=enabled disabled</b>
Display information about HTTPS access	<b>show /SP/services/https</b>
Change HTTPS settings	<b>set /SP/services/https port=portnumber servicestate=enabled disabled</b>
Display SSH DSA key settings	<b>show /SP/services/ssh/keys/dsa</b>
Display SSH RSA key settings	<b>show /SP/services/ssh/keys/rsa</b>

**TABLE A-7** SNMP Commands

Description	Command
Display information about SNMP settings. By default, the SNMP port is 161 and v3 is enabled	<b>show /SP/services/snmp engineid=snmpengineid port=snmpportnumber sets=enabled disabled v1=enabled disabled v2c=enabled disabled v3=enabled disabled</b>
Display SNMP users	<b>show /SP/services/snmp/users</b>
Add an SNMP user	<b>create /SP/services/snmp/users/snmpusername authenticationpassword=password authenticationprotocol=MD5 SHA permissions=rw ro privacypassword=password privacyprotocol=none DES</b>
Delete an SNMP user	<b>delete /SP/services/snmp/users/snmpusername</b>
Display information about SNMP public (read-only) communities	<b>show /SP/services/snmp/communities/public</b>
Add this device to an SNMP public community	<b>create /SP/services/snmp/communities/public/comm1</b>
Delete this device from an SNMP public community	<b>delete /SP/services/snmp/communities/public/comm1</b>
Display information about SNMP private (read-write) communities	<b>show /SP/services/snmp/communities/private</b>
Add this device to an SNMP private community	<b>create /SP/services/snmp/communities/private/comm2</b>
Delete this device from an SNMP private community	<b>delete /SP/services/snmp/communities/private/comm2</b>

**TABLE A-8** Host System Commands

Description	Command
Start the host system or chassis power	<b>start /SYS or start /CH</b>
Stop the host system or chassis power (graceful shutdown)	<b>stop /SYS or stop /CH</b>
Stop the host system or chassis power (forced shutdown)	<b>stop [-f force] /SYS or stop [-f force] /CH</b>



**TABLE A-8** Host System Commands *(Continued)*

<b>Description</b>	<b>Command</b>
Reset the host system or chassis	<b>reset /SYS</b> or <b>reset /CH</b>
Start a session to connect to the host console	<b>start /SP/console</b>
Stop the session connected to the host console (graceful shutdown)	<b>stop /SP/console</b>
Stop the session connected to the host console (forced shutdown)	<b>stop [-f force] /SP/console</b>

**TABLE A-9** Clock Settings Commands

<b>Description</b>	<b>Command</b>
Set ILOM clock to synchronize with a primary NTP server	<b>set /SP/clients/ntp/server/1 address=ntpIPAddress</b>
Set ILOM clock to synchronize with a secondary NTP server	<b>set /SP/clients/ntp/server/2 address=ntpIPAddress2</b>

---

# CLI Command Reference

This section provides reference information about the CLI commands.

## Using the `cd` Command

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. Typing `cd -default` is the equivalent of typing `cd /`. Typing just `cd` displays your current location in the namespace. Typing `help targets` displays a list of all targets in the entire namespace.

### Syntax

`cd target`

### Options

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

### Targets and Properties

Any location in the namespace.

### Examples

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

```
-> cd /SP/users
```

```
-> create emmett
```

To find your location, type `cd`.

```
-> cd /SP/users
```

## Using the create Command

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

### Syntax

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

### Options

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

### Targets, Properties, and Values

**TABLE A-10** Targets, Properties and Values for `create` Command

Valid Targets	Properties	Values	Default
<b>/SP/users/username</b>	password	<string>	(none)
	role	administrator   operator	operator
<b>/SP/services/snmp/communities</b> <i>/communityname</i>	permissions	ro   rw	ro
<b>/SP/services/snmp/user/</b> <i>username</i>	authenticationprotocol	MD5	MD5
	authenticationpassword	<string>	(null string)
	permissions	ro   rw	ro
	privacyprotocol	none   DES	DES
	privacypassword	<string>	(null string)

### Example

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

## Using the delete Command

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

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

### Targets

**TABLE A-11** Targets for `delete` Command

Valid Targets
<i>/SP/users/username</i>
<i>/SP/services/snmp/communities/communityname</i>
<i>/SP/services/snmp/user/username</i>

### Examples

```
-> delete /SP/users/susan  
-> delete /SP/services/snmp/communities/public
```

## Using the exit Command

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

### Syntax

```
exit [options]
```

### Options

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

## Using the help Command

Use the `help` command to display Help information about commands and targets. Using the `-o|output terse` option displays usage information only. The `-o|output verbose` option displays usage, description, and additional information including examples of command usage. If you do not use the `-o|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` and `/SYS`. Fixed targets are targets that cannot be created by a user.

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

### Syntax

```
help [options] command targets
```

### Options

```
[-h|help] [-o|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`: Specify 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 were specified.

## Using the load Command

Use the `load` command to transfer an image file from a source, indicated by a Uniform Resource Indicator (URI), to update ILOM firmware. The URI can specify a protocol and credentials used for the transfer. Only the TFTP protocol is supported, so the URI must begin with `tftp://`. If credentials are required and not specified, the command prompts you for a password. Using the `-script` option eliminates the prompt for a yes or no confirmation and the command acts as if yes were specified.

---

**Note** – Use this command to update your ILOM firmware and BIOS.

---

### Syntax

```
load -source URI
```

### Options

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

### Example

```
-> load -source tftp://ip_address/newmainimage
```

---

**Note** – A firmware upgrade will cause the server and ILOM to be reset. It is recommended that a clean shutdown of the server be done prior to the upgrade procedure. An upgrade takes about five minutes to complete. ILOM will enter a special mode to load new firmware. No other tasks can be performed in ILOM until the firmware upgrade is complete and ILOM is reset.

---

```
-> load -source tftp://archive/newmainimage  
Are you sure you want to load the specified file (y/n)? y  
File upload is complete.  
Firmware image verification is complete.  
Do you want to preserve the configuration (y/n)? n  
Updating firmware in flash RAM:  
.  
Firmware update is complete.  
ILOM will not be restarted with the new firmware.
```

## Using the `reset` Command

Use the `reset` command to reset the state of the target. You will be prompted to confirm a reset operation. Eliminate this prompt by using the `-script` option.

---

**Note** – The `reset` command does not affect the power state of hardware devices.

---

### Syntax

```
reset [options] target
```

### Options

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

### Targets

**TABLE A-12** Targets for `reset` Command

Valid Targets
<code>/SP</code>
<code>/SYS</code>

### Examples

```
-> reset /SP
```

```
-> reset /SYS
```

## Using the set Command

Use the set command to specify the properties of the target.

### Syntax

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

### Options

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

### Targets, Properties, and Values

**TABLE A-13** Targets, Properties, and Values for set Command

Valid Targets	Properties	Values	Default
<b>/SP/users/username</b>	password	<string>	(none)
	role	administrator   operator	operator
<b>/SP/alertmgmt/rules</b>	testalert	true	(none)
<b>/SP/alertmgmt/rules/ rulename</b> (rulename = 1 through 15)	community_or_username	<string>	public
	destination	email_address	(none)
	level	down   critical   major   minor	(none)
	snmp_version	1   2c   3	3
	type	email   ipmipet   snmptrap	(none)
<b>/SP/clock</b>	usentpserver	enabled   disabled	disabled
	datetime	day month date time year	<string>
<b>/SP/services/http</b>	port	<integer>	80
	secureredirect	enabled   disabled	enabled
	servicestate	enabled   disabled	disabled
<b>/SP/services/https</b>	port	<integer>	443
	servicestate	enabled   disabled	disabled
<b>/SP/services/snmp</b>	engineid	<hexadecimal>	<i>IP address</i>
	port	<integer>	161
	sets	enabled   disabled	disabled
	v1	enabled   disabled	disabled
	v2c	enabled   disabled	disabled
	v3	enabled   disabled	enabled
<b>/SP/services/snmp/ communities/private</b>	permission	ro   rw	rw



**TABLE A-13** Targets, Properties, and Values for set Command (Continued)

Valid Targets	Properties	Values	Default
<b>/SP/services/snmp/ communities/public</b>	permission	ro   rw	ro
<b>/SP/services/snmp/user /username</b>	authenticationprotocol	MD5	MD5
	authenticationpassword	<string>	(null string)
	permissions	ro   rw	ro
	privacyprotocol	none   DES	DES
	privacypassword	<string>	(null string)
<b>/SP/services/ssh</b>	generate_new_key_action	true	(none)
	generate_new_key_type	rsa   dsa	(none)
	restart_sshd_action	true	(none)
	state	enabled   disabled	enabled
<b>/SP/services/sso</b>	state	enabled   disabled	enabled
<b>/SP/users/username</b>	role	administrator   operator	(none)
	password	<string>	(none)
<b>/SP/clients/ activedirectory</b>	state	enabled   disabled	disabled
	certfilestatus	<string>	(none)
	defaultrole	<string>	(none)
	getcertfile	<string>	(none)
	ipaddress	<string>	(none)
	port	<string>	(none)
	strictcertmode	enabled   disabled	disabled
	timeout	<integer>	(none)
<b>/SP/clients/ activedirectory/ admingroups/n</b> where <i>n</i> is 1-5	name	<string>	(none)
<b>/SP/clients/ activedirectory/ opergroups/n</b> where <i>n</i> is 1-5	name	<string>	(none)
<b>/SP/clients/ activedirectory/ userdomains/n</b> where <i>n</i> is 1-5	domain	<string>	(none)

**TABLE A-13** Targets, Properties, and Values for set Command (Continued)

Valid Targets	Properties	Values	Default
<b>/SP/clients/ldap</b>	binddn	<username>	(none)
	bindpw	<string>	(none)
	defaultrole	administrator   operator	operator
	ipaddress	<ipaddress>   none	(none)
	port	<integer>	389
	searchbase	<string>	(none)
	state	enable   disabled	disabled
<b>/SP/clients/ntp/server/[1 2]</b>	address	<ipaddress>	(none)
<b>/SP/clients/radius</b>	defaultrole	administrator   operator	operator
	ipaddress	<ipaddress>   none	(none)
	port	<integer>	1812
	secret	<string>   none	(none)
	state	enable   disabled	disabled
<b>/SP/clients/smtp</b>	address	<ipaddress>	<i>IP address</i>
	port	<integer>	25
	state	enabled   disabled	enabled
<b>SP/clients/syslog</b>	destination_ip1	<ipaddress>	<i>IP address</i>
	destination_ip2	<ipaddress>	<i>IP address</i>
<b>/SP/network</b>	commitpending	true	(none)
	pendingipaddress	<ipaddress>   none	(none)
	pendingdiscovery	dhcp   static	dhcp
	pendingipgateway	<ipaddress>   none	(none)
	pendingipnetmask	<IP dotted decimal>	255.255.255.255
<b>/SP/serial/external</b>	commitpending	true	(none)
	flowcontrol	none	none
	pendingspeed	<integer from list>	9600
	speed	<integer from list>	9600
<b>/SP/serial/host</b>	commitpending	true	(none)
	pendingspeed	<integer from list>	9600
	speed		9600
<b>/SP/</b>	system_identifier	<string>	(none)
<b>/SP/</b>	hostname	<string>	default is based on MAC address

## Examples

```
-> set /SP/users/susan role=administrator
-> set /SP/clients/ldap state=enabled binddn=proxyuser bindpw=ez24get
```

## Using the show Command

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.

The `-o|output` option specifies the output and form of command output. ILOM only supports `-o table`. When you use the `-o table` option, the output is formatted in a condensed, three-column table of targets, properties, and values.

The alias, `show components`, is a shortcut for the following CLI command:

```
-> show -o table -level all /SYS component_state
```

The `show components` alias produces the same output as the above command. Thus, it enables you to restrict the table output to a single property below each target.

## Syntax

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

## Options

```
[-d|-display] [-l|level] [-o|output]
```

## Targets and Properties

TABLE A-14 Targets for show Command

Valid Targets	Properties
<b>/SYS</b>	
<b>/SP</b>	
<b>/SP/alertmgmt/rules/ rulename</b> (rulename = 1 through 15)	community   username destination level snmp_version type
<b>/SP/clients/ activedirectory</b>	state certfilestatus defaultrole getcertfile ipaddress port strictcertmode timeout
<b>/SP/clients/ activedirectory/ admingroups/n</b> where <i>n</i> is 1-5	name
<b>/SP/clients/ activedirectory/ opergroups/n</b> where <i>n</i> is 1-5	name
<b>/SP/clients/ activedirectory/ userdomains/n</b> where <i>n</i> is 1-5	domain
<b>/SP/clients/ldap</b>	binddn bindpw defaultrole ipaddress port searchbase state
<b>/SP/clients/ntp/server/[1 2]</b>	ipaddress

**TABLE A-14** Targets for `show` Command (Continued)

<b>Valid Targets</b>	<b>Properties</b>
<b>/SP/clock</b>	datetime usentpserver
<b>/SP/logs/event</b>	clear
<b>/SP/network</b>	ipaddress ipdiscovery ipgateway ipnetmask macaddress pendingipaddress pendingdiscovery pendingipgateway pendingipnetmask
<b>/SP/serial/external</b>	flowcontrol pendingspeed speed
<b>/SP/serial/host</b>	pendingspeed speed
<b>/SP/services/http</b>	port secureredirect servicestate
<b>/SP/services/https</b>	port servicestate
<b>/SP/services/snmp</b>	engineid port sets v1 v2c v3
<b>/SP/services/snmp/communities/private</b>	permissions
<b>/SP/services/snmp/communities/public</b>	permissions
<b>/SP/services/snmp/users/username</b>	password role
<b>/SP/services/ssh</b>	state
<b>/SP/services/ssh/keys/dsa</b>	fingerprint length publickey

**TABLE A-14** Targets for show Command (Continued)

<b>Valid Targets</b>	<b>Properties</b>
<b>/SP/services/ssh/keys/rsa</b>	fingerprint length publickey
<b>/SP/services/sso</b>	state
<b>/SP/sessions</b>	username starttime date
<b>/SP/sessions/sessionid</b>	starttime source type user
<b>/SP/users/username</b>	role password

### Examples

```
-> show -display properties /SP/users/susan
```

```
    /SP/users/susan
```

```
    Properties:
```

```
        role = Administrator
```

```
-> show /SP/clients -level 2
```

```
/SP/clients
```

```
    Targets:
```

```
        ldap
```

```
        ntp
```

```
    Properties:
```

```
    Commands:
```

```
        cd
```

```
        show
```

```
/SP/clients/ldap
```

```
    Targets:
```

```

Properties:
  binddn = cn=Manager,dc=sun,dc=com
  bindpw = secret
  defaultrole = Operator
  ipaddress = 129.144.97.180
  port = 389
  searchbase = ou=people,dc=sun,dc=com
  state = disabled

```

```

Commands:
  cd
  show

```

```
/SP/clients/ntp
```

```

Targets:
  server

```

```
Properties:
```

```

Commands:
  cd
  show

```

```
-> show components
```

Target	Property	Value
/SYS/FRU1	component_state	Enabled
/SYS/FRU2	component_state	Disabled
/SYS/FRU3	component_state	Enabled

```
-> show -o table -level all /SP/sessions
```

Target	Property	Value
/SP/sessions/90	username	root
/SP/sessions/90	starttime	Tue Apr 10 10:57:22 2007
/SP/sessions/90	type	shell

## Using the start Command

Use the `start` command to turn on the target or to initiate a connection to the host console. Using the `-script` option eliminates the prompt for a yes or no confirmation and the command acts as if yes were specified. The `-f|force` option specifies that the action will be performed immediately.

### Syntax

```
start [options] target
```

### Options

```
[-h|help] [-script] [-f|force]
```

### Targets

TABLE A-15 Targets for `start` Command

Valid Targets	Description
<code>/SYS</code> or <code>/CH</code>	Starts (powers on) the system or chassis.
<code>/SP/console</code>	Starts an interactive session to the console stream.

### Examples

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

```
-> start /SYS
```

## Using the stop Command

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. The `-f|force` option specifies that the action will be performed immediately.

### Syntax

```
stop [options] [-script] target
```

### Options

```
[-f|force] [-h|help]
```



## Targets

TABLE A-16 Targets for stop Command

Valid Targets	Description
<code>/SYS</code> or <code>/CH</code>	Perform an orderly shutdown, followed by a power off of the specified system or chassis. Use the <code>-force</code> option to skip the orderly shutdown and force an immediate power off.
<code>/SP/console</code>	Terminate another user's connection to the host console.

## Examples

```
-> stop /SP/console
```

```
-> stop -force /SYS
```

## Using the version Command

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

### Syntax

```
version
```

### Options

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

### Example

```
-> version
```

```
version SP firmware version: 2.0.0
```

```
SP firmware build number: 4415
```

```
SP firmware date: Mon Mar 28 10:39:46 EST 2007
```

```
SP filesystem version: 0.1.9
```

# Glossary

---

---

## A

- access control list (ACL)** A software authorization mechanism that enables you to control which users have access to a server. Users 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, such as “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.
- 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.

---

## 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.

**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), this 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.

**Chassis Monitoring  
Module (CMM)**

A typically redundant, hot-pluggable module that works with the service processor (SP) on each blade to form a complete chassis management system.

**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 users to type executable instructions at a command prompt.

**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.

**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.

**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 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.

**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.

---

## E

**enhanced parallel port  
(EPP)**

A hardware and software standard that enables systems to transmit data at twice the speed of standard parallel ports.

**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 can then 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.

**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).

**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.

**graphical user interface (GUI)** An interface that uses graphics, along with a keyboard and mouse, to provide easy-to-use access to an application.

---

## H

**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. However, before removing the component, the system administrator must prepare the system for the hot-plug operation. After the new component is inserted, the system administrator must instruct the system to reconfigure the device 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.

**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. This enables 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 Field Replacable Unit (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,” which specifies the actual location of a machine on an intranet or the Internet.

**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 launcher. With Java Web Start, applications are launched 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 launched from a desktop icon or browser

---

## 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.

**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 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.

<b>media access control (MAC) address</b>	Worldwide unique, 48-bit, hardware address number that is programmed in to each local area network interface card (NIC) at the time of manufacture.
<b>Message Digest 5 (MD5)</b>	A secure hashing function that converts an arbitrarily long data string into a short digest of data that is unique and of fixed size.
<b>minor event</b>	A system event that does not currently impair service, but which needs correction before it becomes more severe.

---

## N

<b>namespace</b>	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.
<b>Network File System (NFS)</b>	A protocol that enables disparate hardware configurations to function together transparently.
<b>Network Information Service (NIS)</b>	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.
<b>network interface card (NIC)</b>	An internal circuit board or card that connects a workstation or server to a networked device.
<b>network management station (NMS)</b>	A powerful workstation with one or more network management applications installed. The NMS is used to remotely manage a network.
<b>network mask</b>	A number used by software to separate the local subnet address from the rest of a given Internet Protocol (IP) address.
<b>Network Time Protocol (NTP)</b>	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).
<b>node</b>	An addressable point or device on a network. A node can connect a computing system, a terminal, or various peripheral devices to the network.
<b>nonvolatile memory</b>	A type of memory that ensures that data is not lost 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<sup>(TM)</sup> 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.

**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.

**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.

**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

**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.

**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.

**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.

**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.

---

## S

**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. They include software information, such as how many sensors are present, what type they are, their events, threshold information, and so on. The sensor data records enable software to interpret and present sensor data without any prior knowledge about the platform.

**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 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.

**session time-out** 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.

**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.

**time-out** 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 systems. TFTP uses User Datagram Protocol (UDP).

---

## U

**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,

**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.

---

## W

- 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

- Active Directory
  - about domains and groups, 81
  - address Property, 94
  - configuration properties, 79
  - defaultrole Property, 94
  - determining user authorization levels, 77
  - logdetail Property, 94
  - overview, 76
  - port Property, 94
  - purposes used for, 77
  - state Property, 95
  - strictcertmode Property, 95
  - timeout Property, 95, 96
  - typical uses, 77
  - User Authentication and Authorization, 76
- Active Directory Web Interface, 78
- Administrator account
  - default username and password, 60
- Administrator role
  - defined, 6
  - required to launch Remote Console, 227
- alerts
  - CLI commands for managing alerts, 165
  - defining an alert rule, 159, 161
  - delivering SNMP traps, 200
  - disabling an alert rule, 163
  - generating email notification, 170
  - generating test alerts, 164
  - modifying an alert rule, 162
  - specifying destination, 159
  - types of levels, 160
  - types supported, 158, 159, 200

warnings for system failures, 158

Altiris Deployment Server, 3

## B

- baud rate, setting, 187
- BIOS configurations
  - updating, 2
- blade server modules, configuring IP addresses
  - editing through an Ethernet connection, 29 to 30
  - initializing
    - through DHCP, 23 to 24
    - through static assignment, 25 to 26
  - set command (ILOM), table of options, 26

## C

- Chassis Monitoring Module (CMM)
  - managing with ILOM, 4
- Chassis Monitoring Module (CMM), configuring IP addresses
  - editing through an Ethernet connection, 29 to 30
  - initializing
    - through DHCP, 23 to 24
    - through static assignment, 27 to 28
- CLI command syntax
  - cd command, 247
  - create command, 248
  - delete command, 249
  - exit command, 249
  - help command, 250
  - load command, 251
  - reset command, 252
  - set command, 253

- show command, 256
- start command, 261
- stop command, 261
- version command, 262

#### CLI commands

- alert management commands, 244
- clock settings commands, 246
- general commands, 242
- host system commands, 245
- network and serial port commands, 243
- SNMP commands, 245
- syntax, 241
- system access commands, 244
- user commands, 242

#### clock settings

- setting using the CLI, 137
- setting using the web interface, 137, 152

#### command-line interface (CLI)

- command quick reference, 241 to 246
- command reference, 247
- commands syntax, 40
- ILOM target types, 38
- logging in to ILOM, 44
- logging out of ILOM, 44
- overview, 4, 37
- specification based on, 38
- using hierarchical architecture, 38

## D

#### data network

- compared to management network, 5, 20

#### device redirection

- behavior during Remote Console session, 238

#### discrete sensors

- obtaining readings, 130

#### distinguished names

- used with LDAP, 104

#### Dynamic Host Configuration Protocol (DHCP)

- requirements for assigning IP address, 15
- using to assign an IP address, 14

## E

#### Ethernet management port

- connecting to ILOM, 6, 13
- label on server, 13

#### event log

- capturing timestamps, 136

- types of events displayed, 136
- viewing and clearing using the CLI, 150
- viewing and clearing using the web interface, 148

## F

#### fault management

- monitoring and diagnosing hardware, 139
- viewing faulted components, 140 to 142

#### field-replaceable units (FRUs)

- obtaining sensor readings, 127

#### firmware

- updating, 2

#### firmware update process

- overview, 214

## H

#### hardware

- redirecting keyboard and mouse, 235

#### host serial console, 176

#### HP OpenView, 3

#### HP Systems Insight Manager, 3

#### HTTP or HTTPS web access

- enabling using the CLI, 178
- enabling using the web interface, 187 to 188

## I

#### IBM Director, 3

#### IBM Tivoli, 3

#### ILOM

- capabilities, 2

- description, 1

- user interfaces supported, 2

#### ILOM service processor

- what it runs on, 2

#### Integrated Lights Out Manager (ILOM)

- commands

  - set command, blades, table of options, 26

- configuring for Remote Console, 228

- connecting to, 6

- features of, 7

- initial setup, 12

- interfaces, 4

- logging in using the web interface, 51

- new 2.0 features, 9

- preconfigured Administrator account

  - logging in, 60

- redirecting keyboard and mouse, 235
- Remote Console, configuring and launching, 233
- resetting SP using the web interface, 221
- roles assigned to accounts, 6
- root account password, 60
- system monitoring features, 126
- updating firmware using the CLI, 218
- updating firmware using the web interface, 219 to 220
- using Sun N1 System Manager, 10
- using third-party tools, 10
- viewing version using the web interface, 216
- Intelligent Platform Management Interface (IPMI) Baseboard Management Controller, 190
  - functionality, 189
  - overview, 4, 189
  - Platform Event Trap alerts, 191
  - using IPMItool, 190
  - versions compliant with ILOM, 190
- internal serial port, 176
- Internet Protocol (IP) address
  - assigning a static IP address, 18
  - identifying DHCP assigned address, 15
- IP address assignment
  - editing using the CLI, 30 to 32
  - editing using the web interface, 29 to 30
  - for DHCP assigned addresses, 23 to 24
  - for static assigned addresses to CMM, 27 to 28
  - for static assigned addresses to SP, 25 to 26
- IPMItool
  - examples of how to use, 192 to 195
  - functions of, 190
  - references for, 191
- L**
- LDAP
  - client operations, 102
  - client-server model, 102
  - configuring ILOM for LDAP, 105 to 107
  - configuring the LDAP server, 105
  - directory structure, 102 to 104
  - distinguished names, 104
  - overview, 102
- logging in to ILOM
  - using the CLI, 44
  - using the web interface, 51
- logging out of ILOM
  - using the CLI, 44
  - using the web interface, 56
- M**
- Management Information Base (MIB)
  - description of, 199
  - supported MIBs used with ILOM, 199 to 200
- management network
  - assigning IP addresses, 20
  - compared to data network, 5
  - overview, 5
- media access control (MAC) address
  - obtaining for SP or CMM, 15
- N**
- namespaces
  - accessed by SP, 39
- network management port
  - connecting to ILOM, 5
- network port assignment
  - identifying for SP and CMM, 20 to 21
- network settings
  - configuring using the CLI, 175
  - configuring using the web interface, 184 to 185
  - pending and active properties, 174
  - viewing using the CLI, 174
  - viewing using the web interface, 184
- O**
- Operator role, 6
- out-of-band management, 2
- P**
- PC Check Diagnostic setting
  - configuring for Remote Console, 231
- power
  - monitoring available power, 146
  - monitoring individual power supply consumption, 145
  - monitoring permitted power consumption, 146
  - monitoring system actual power, 144
  - monitoring system total power consumption, 143
- power monitoring
  - actual power, 131
  - available power, 131
  - interfaces, 131

terminology, 132

## R

### RADIUS

- client-server model, 108
- commands, 111 to 112
- configuration parameters, 109
- configuring, 110
- default port number, 113
- overview, 108

### Remote Console

- adding new server session, 234
- configuring remote control settings, 229 to 231
- connecting using the web interface, 228 to 229
- controlling device redirection, 234
- exiting the application, 238
- installation requirements, 226
- launching using the web interface, 232 to 233
- network ports and protocols, 227
- overview, 4, 224
- redirecting keyboard and mouse, 235
- redirecting storage device or ISO image, 236 to 237
- remote control settings, 231
- signing in as Administrator, 227
- single and multiple server views, 224 to 225
- using keyboard control modes, 235

### root account password

- changing using the CLI, 63
- changing using the web interface, 60

## S

### Scalent Virtual Operating Environment, 3

#### sensor readings

- classes supported, 129
- monitoring and diagnosing faults, 139
- obtaining using the CLI, 129
- obtaining using the web interface, 127
- types of data reported, 127

#### serial console connection

- configuring serial settings, 19

#### serial management port

- connecting to ILOM, 13

#### serial port settings

- configuring using the CLI, 177
- configuring using the web interface, 187
- default setting, 187
- displaying using the web interface, 186

- internal and external ports, 176
- pending and active properties, 177
- viewing using the CLI, 176

#### serial port, external

- setting baud rate, 187

#### serial port, internal

- setting baud rate, 187

#### service processor (SP)

- managing with ILOM, 4

#### set command (ILOM)

- blade options, table of, 26

### Simple Network Management Protocol (SNMP)

- agents functions, 198
- Management Information Base, 199
- management station monitoring, 199
- overview, 4, 198
- usage examples, 209 to 212
- versions supported, 198

#### single sign on

- enabling or disabling using the CLI, 63
- enabling or disabling using the web interface, 64
- overview, 63
- using to launch the Remote Console, 227

#### SNMP traps

- configuring destinations using the CLI, 203
- configuring destinations using the web interface, 209
- example of, 212

#### SNMP user accounts

- managing using the web interface, 204 to 208
- managing with the CLI, 201 to 204
- targets, properties, and values of, 202

### Solaris 10 Operating System, configuring the factory-installed OS

- using a Secure Shell (SSH) connection, 179
- procedure, 168, 169, 171

#### ssh command (Solaris)

- connecting to a SP, 31, 35, 150, 154, 167, 169, 171, 179

#### SSH settings

- key encryption using the CLI, 180

#### static IP address

- requirements for assigning, 18

#### system indicators

- customer changeable states, 133
- illuminating conditions, 132
- system assigned states, 133

- viewing using the CLI, 135
- viewing using the web interface, 134

system monitoring features

- overview, 126

## T

threshold sensors

- obtaining readings, 129

## U

uploading SSL certificate

- using the web interface, 54

user accounts

- adding and setting privileges using the web interface, 68
- adding using the CLI, 65
- Administrator privileges, 59
- configuring using the CLI, 66
- deleting using the CLI, 65
- deleting using the web interface, 74
- modifying using the CLI, 65
- modifying using the web interface, 71
- number of accounts supported, 59
- roles assigned, 6
- specifying names for, 59
- viewing a list of, 65
- viewing a specific account, 66
- viewing an individual session using the CLI, 67
- viewing using the CLI, 67
- viewing using the web interface, 75

## W

web interface

- buttons, 47
- logging in, 51
- overview, 4, 45
- supported browsers, 46
- types of access, 187
- uploading SSL certificate, 54



