FUJITSU

Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide

C120-E574-01EN

FUJITSU

Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide

Manual Code C120-E574-01EN
Part No. 875-4534-10
April 2009, Revision A

Entrée et revue tecnical fournies par FUJITSU LIMITED sur des parties de ce matériel.

Contents

Preface

The *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* describes how to perform the required ILOM setup procedures, as well as the typical procedures you might perform while accessing ILOM features and functions.

This ILOM Web Procedures Guide is written for system administrators who are familiar with networking concepts and basic system management protocols.

Note – The description in this document is limited to the servers which support ILOM. In the description, "all server platforms" refers to all Fujitsu servers which support ILOM. Depending on the server in use, some of the ILOM functions are not supported. Please confirm the ILOM Supplement manual and the Product Notes of each server in advance.

FOR SAFE OPERATION

This manual contains important information regarding the use and handling of this product. Read this manual thoroughly. Use the product according to the instructions and information available in this manual. Keep this manual handy for further reference.

Fujitsu makes every effort to prevent users and bystanders from being injured or from suffering damage to their property. Use the product according to this manual.

Related Documentation

To fully understand the information that is presented in this guide, use this document in conjunction with the documents listed in the following table. The latest versions of all the SPARC Enterprise Series manuals are available at the following Web sites:

Global Site

http://www.fujitsu.com/sparcenterprise/manual/

Japanese Site

http://primeserver.fujitsu.com/sparcenterprise/manual/

First read the ILOM 3.0 Concepts Guide to learn about ILOM's features and functionality. To set up a new system supported by ILOM, refer to the ILOM 3.0 Getting Started Guide, where you will find the procedures for connecting to the network, logging in to ILOM for the first time, and configuring a user account or directory service. Then, decide which ILOM interface you want to use to perform other ILOM tasks. You can now refer to the appropriate ILOM 3.0 Procedures Guide for your selected interface.

The following table lists the ILOM 3.0 Documentation Collection.

TABLE P-1 ILOM 3.0 Documentation Collection

Title	Content	Manual Code
Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide	Information that describes ILOM features and functionality	C120-E573
Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide	Information and procedures for network connection, logging in to ILOM for the first time, and configuring a user account or a directory service	C120-E576
Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM web interface	C120-E574
Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM CLI	C120-E575
Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide	Information and procedures for accessing ILOM functions using SNMP or IPMI management hosts	C120-E579

In addition to the ILOM 3.0 Documentation Collection, associated ILOM Supplement documents present ILOM features and tasks that are specific to the server platform you are using. Use the ILOM 3.0 Documentation Collection in conjunction with the ILOM Supplement that comes with your server platform.

ILOM 3.0 Version Numbers

ILOM 3.0 has implemented a new version numbering scheme to help you identify which version of ILOM you are running on your system. The numbering scheme includes a five-field string, for example, `a.b.c.d.e`, where:

- `a` – Represents the major version of ILOM.
- `b` – Represents a minor version of ILOM.
- `c` – Represents the update version of ILOM.
- `d` – Represents a micro version of ILOM. Micro versions are managed per platform or group of platforms. See your platform Product Notes for details.
- `e` – Represents a nano version of ILOM. Nano versions are incremental iterations of a micro version.

For example, ILOM 3.1.2.1.a would designate:

- ILOM 3 as the major version of ILOM
- ILOM 3.1 as a minor version of ILOM 3
- ILOM 3.1.2 as the second update version of ILOM 3.1
- ILOM 3.1.2.1 as a micro version of ILOM 3.1.2
- ILOM 3.1.2.1.a as a nano version of ILOM 3.1.2.1

Product Identity Information

Product identity information enables a system to register itself and use certain automated services based on the service contract associated with its identity. You can use product identity information to uniquely identify a system. You also need to supply the product identity information to service engineers when you request service for the system. Product identity consists of the following information:

- `product_name`: Name under which a product is sold.
- `product_part_number`: Namespace assigned by manufacturing within which the product serial number is unique. A product part number never maps to more than one product. For example, "602-3098-01."

- `product_serial_number`: Unique identity assigned to each instance of a product by manufacturing. For example, “0615AM0654A.”
- `product_manufacturer`: Manufacturer of the product. For example, ‘FUJITSU.”

TABLE P-2 describes the common product identity information used by ILOM.

TABLE P-2 Common Product Identity Information

Required Information	Target	Minimal Properties

Basic product information on server (rackmounted and blade)	`/SYS`	`product_name`
		`product_part_number`
		`product_serial_number`
		`product_manufacturer`

Basic product information on chassis monitoring module (CMM)	`/CH`	`product_name`
		`product_part_number`
		`product_serial_number`
		`product_manufacturer`

Basic chassis information on blade	`/SYS/MIDPLANE`	`product_name`
		`product_part_number`
		`product_serial_number`
		`product_manufacturer`

Location of blade within the chassis	`/SYS/SLOTID`	`type`
		`class`
		`value`

Location of chassis within a rack	`/CH`	`rack_location`

Text Conventions

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

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

Fujitsu Welcomes Your Comments

If you have any comments or requests regarding this document, or if you find any unclear statements in the document, please state your points specifically on the form at the following URL.

For Users in U.S.A., Canada, and Mexico

https://download.computers.us.fujitsu.com/

For Users in Other Countries

http://www.fujitsu.com/global/contact/computing/sparce_index.html

CHAPTER 1

Web Interface Overview

Topics

Description	Links
Learn about ILOM web interface features and functionality	• "About the Web Interface" on page 2 • "Browser and Software Requirements" on page 2 • "Web Interface Components" on page 3 • "Navigation Tabs" on page 4

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• ILOM Overview	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• CLI	• CLI Overview	*Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*
• SNMP and IPMI hosts	• SNMP Overview • IPMI Overview	*Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/

This chapter introduces the basic information you need to know before you perform procedures using the ILOM web interface.

About the Web Interface

The ILOM web interface is accessible through a browser. 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 keyboard and mouse. You can also configure the diskette drive or CD-ROM drive on the remote system as a device virtually connected to your system. You can access these features using the ILOM Remote Console application.

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.

ILOM supports the browsers listed in the following table.

TABLE 1-1 Supported Web Browsers

Operating System	Web Browser
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 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`. See Chapter 12 for a list of web browsers and operating systems supported by the Remote Console application.

Web Interface Components

The following figure shows the ILOM web interface main page that is displayed after you log in to ILOM.

FIGURE 1-1 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 Navigation Pane appears to the left of the ILOM web page.

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 – Use the Refresh and Log Out buttons that are part of the ILOM web interface. Do not use the Refresh or Log Out 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. The content area is where you find information about the specific topic or operation.

Navigation Tabs

The following table describes the various tabs and sub-tabs that you can use to access the most common ILOM functions using the web interface. For more detail about how to use the features and functions on the web pages that appear when you select a tab, see the related chapters in this guide.

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

TABLE 1-2 ILOM 3.0 Web Interface Tabs

Main Tab	Second and Third-level Tabs	What You Can Do
System Information		
	Versions	View the version of ILOM that is running
	Session Time-Out	Set the amount of idle time for which the ILOM session will remain active
	Components	View the names, types, and status of the components that ILOM is monitoring
	Fault Management	View information about components that are in a faulted state
	Identification Information	Enter or change the service processor identification information by assigning a host name or system identifier
System Monitoring		
	Sensor Readings	View the name, type, and reading of the sensors
	Indicators	View the name and status of the indicators and LEDs
	Event Logs	View various details about each particular event, including the event ID, class, type, severity, date and time, and description of the event
	Power Management	Use available power management interfaces to monitor power consumption and to manage power usage
Configuration		
	System Management Access --> Web Server	Edit or update the web server settings, such as the HTTP web server or the HTTP port
	System Management Access --> SSL Certificate	View information about the default SSL certificate, or optionally find and enter a new SSL certificate
	System Management Access --> SNMP	Edit or update SNMP settings
	System Management Access --> SSH Server	Configure Secure Shell (SSH) server access and key generation
	System Management Access --> IPMI	Use a command-line interface to monitor and control your server platform, as well as to retrieve information about your server platform
	Alert Management	View details about each alert and change the list of configured alerts
	Network	View and edit the network settings for ILOM

TABLE 1-2 ILOM 3.0 Web Interface Tabs *(Continued)*

Main Tab	Second and Third-level Tabs	What You Can Do
	DNS	Specify host names, and have those host names resolved into IP addresses using the Domain Name Service (DNS)
	Serial Port	View and edit the baud rate of the internal and external serial ports
	Clock	View and edit the ILOM clock time manually, or synchronize the ILOM clock with an NTP server
	Timezone	Specify a particular timezone so that timestamps displayed by the service processor can be correlated to logs created elsewhere (for example, in the Solaris operating system)
	Syslog	Configure the server addresses to which the syslog messages will be sent
	SMTP Client	Configure the state of the SMTP client, which is used for sending email notifications of alerts
	Policy	Enable or disable settings that control the behavior of the system, such as power-on policies
User Management		
	User Accounts	Add, delete, or modify local ILOM user accounts
	Active Sessions	View the users currently logged in to ILOM, as well as the type of session users have initiated
	LDAP	Configure ILOM access for LDAP users
	LDAP/SSL	Configure ILOM access for LDAP users with enhanced security settings enabled by Secure Socket Layer (SSL) technology
	RADIUS	Configure ILOM access for RADIUS users
	Active Directory	Configure ILOM access for Active Directory users
Remote Control		
	Redirection	Manage the host remotely by redirecting the system console to your local machine
	KVMS	Enable or disable the remote management state of the keyboard, video, mouse, or storage device
	Remote Power Control	Select a power state: Immediate Power Off, Graceful Shutdown and Power Off, Power On, Power Cycle, or Reset
	Diagnostics	Enable or disable diagnostics for x64 processor-based systems or SPARC processor-based systems

TABLE 1-2 ILOM 3.0 Web Interface Tabs *(Continued)*

Main Tab	Second and Third-level Tabs	What You Can Do
Maintenance		
	Firmware Upgrade	Start the process to obtain an upgrade of the ILOM firmware
	Backup/Restore	Backup and restore the service processor configuration to a remote host or removable storage device in a secure manner
	Reset SP	Reset the service processor
	Configuration Management	Manage the service processor configuration data
	Snapshot	Collect environmental, log, error, and FRUID data and send it to a USB thumbdrive, an external host using CLI, or as a downloaded file

CHAPTER 2

Prerequisites for Using the Web Interface

Prior to performing the procedures presented in this guide, the following prerequisites must be met.

Prerequisites

Steps	Description	Chapter or Section	Related Guide
1	You must establish initial communication with the ILOM SP (CMM or server)	• Connecting to ILOM	• *Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*
2	You should have already created a user account in ILOM	• Add User Account and Assign Privileges (web interface) • Add User Account and Assign Privileges (CLI)	• *Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*

You can download the ILOM 3.0 Documentation Collection at:
http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/

CHAPTER 3

Logging In to and Out of ILOM

Topics

Description	Links
Review the prerequisites	• "Before Your Initial Login" on page 12
Log in to ILOM for the first time	• "Log In to ILOM Using the `root` User Account" on page 13
Set up a user account	• "Set Up a User Account" on page 14
Log in to ILOM as a regular user	• "Log In to ILOM as a User" on page 14
Log out of ILOM	• "Log Out of ILOM" on page 15

Related Topics

For ILOM	Chapter or Section	Guide
• Getting Started	• ILOM Getting Started Process • Initial ILOM Setup Procedures Using the Web Interface	*Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*
• CLI	• Logging In to and Out of ILOM	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
`http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/`

Use this chapter as a quick reference for the ILOM login and logout procedures. For additional information, refer to the initial login process and procedures as described in the *Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*.

Before Your Initial Login

Prior to performing the procedures in this chapter, you should ensure that the following requirements are met.

- Plan how you want to set up ILOM on your server to work in your data center environment. Refer top "Initial Setup Worksheet to Establish Communication With ILOM" in the *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- Connect to ILOM over a serial port without a network connection, or log in to ILOM over a network. To log in using a direct serial connection, attach a serial cable to the workstation, terminal, or terminal emulator and to the SER MGT port on the server, or if you are using a modular chassis system, to the chassis monitoring module (CMM) port. To log in using a network connection, attach an Ethernet cable to the NET MGT port on the server or CMM. Refer to your platform documentation for more information.
- Configure the network settings. You can use either DHCP or a static network connection. By default, ILOM will attempt to obtain network settings using DHCP. See or "Connecting to ILOM" in the *Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*.

Logging In to ILOM

Topics

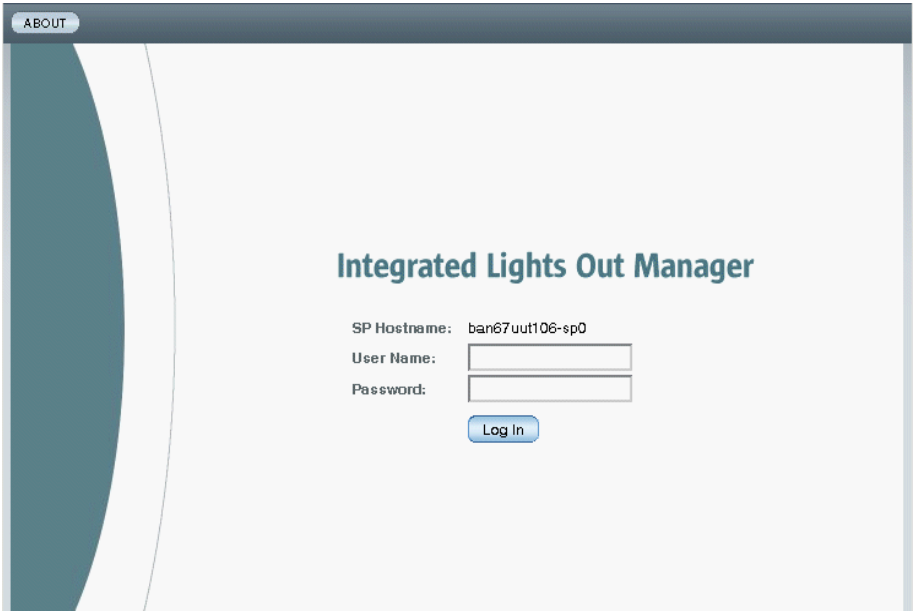
Description	Links
Log in to ILOM and set up a user account	• "Log In to ILOM Using the `root` User Account" on page 13 • "Set Up a User Account" on page 14 • "Log In to ILOM as a User" on page 14

▼ Log In to ILOM Using the `root` User Account

To log in to the ILOM web interface for the first time using the `root` user account, open a web browser and do the following:

1. **Type `http://`*system_ipaddress* into the web browser.**

   The web interface Login page appears.



2. **Type the user name and password for the `root` user account:**

   User Name: **`root`**

   Password: **`changeme`**

3. **Click Log In.**

   The Version page in the web interface appears.

▼ Set Up a User Account

Once you are logged in to ILOM, you need to create a regular (non-`root`) user account. You will use this regular user account to configure ILOM settings for your system and environment.

Follow this step to set up a user account:

- **Set up a user account in one of these five classes of users:**
  - Local users
  - Active Directory users
  - LDAP users
  - LDAP/SSL users
  - RADIUS users

  You can create and configure with advanced roles up to 10 local user accounts or configure a directory service.

  For information about setting up a user account, see "Add User Accounts and Assign Roles" on page 31.

▼ Log In to ILOM as a User

Use this procedure to log in to ILOM to verify that the user account or directory service is functioning properly.

Follow these steps to log in to ILOM using a non-`root` user account:

1. **In the web browser, type `http://`*system_ipaddress***

   The web interface Login page appears.

2. **Type the user name and password of a user account that you previously configured.**

3. **Click Log In.**

   The ILOM web interface appears, displaying the Version page.

Logging Out of ILOM

Topics

Description	Links
Log out of ILOM	• "Log Out of ILOM" on page 15

▼ Log Out of ILOM

- **Click the Log Out button in the ILOM web interface.**

  The Log Out button is located in the top right corner of the web interface. Do not use the Log Out button on your web browser to exit ILOM.

What Next

After you have set up a user account or configured a directory service, you are now ready to configure ILOM. The remaining chapters in this guide provide complete descriptions of the tasks you can perform to access ILOM's functions.

CHAPTER 4

Configuring ILOM Communication Settings

Topics

Description	Links
Configure network settings	• "Assign Host Name and System Identifier" on page 19 • "View and Configure Network Settings" on page 20 • "View and Configure DNS Settings" on page 21 • "View and Configure Serial Port Settings" on page 22 • "Enable HTTP or HTTPS Web Access" on page 24 • "Upload the SSL Certificate" on page 26
Configure Secure Shell settings	• "Enable or Disable SSH" on page 27 • "Generate a New SSH Key" on page 27 • "Restart the SSH Server" on page 28

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• ILOM Network Configurations	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• Getting started	• Getting Started With ILOM	*Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*
• CLI	• Configuring ILOM Communication Settings	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
• IPMI and SNMP hosts	• Configuring ILOM Communication Settings	*Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/

Configuring Network Settings

This section describes how to configure the network parameters for ILOM using the ILOM web interface. Dynamic Host Configuration Protocol (DHCP) is the default setting. If your network does not support this protocol, you need to set the parameters manually.

Topics

Description	Links
Review the prerequisites	• "Before You Begin" on page 19
Configure network settings	• "Assign Host Name and System Identifier" on page 19 • "View and Configure Network Settings" on page 20 • "View and Configure DNS Settings" on page 21 • "View and Configure Serial Port Settings" on page 22 • "Enable HTTP or HTTPS Web Access" on page 24 • "Upload the SSL Certificate" on page 26

Before You Begin

Prior to configuring ILOM communication settings, ensure that the same IP address is always assigned to ILOM by either assigning a static IP address to ILOM after initial setup, or by configuring your DHCP server to always assign the same IP address to ILOM. This enables ILOM to be easily located on the network.

By default, ILOM will attempt to obtain network settings using DHCP.

▼ Assign Host Name and System Identifier

Before You Begin

- To assign a host name and system identifier, you need the Admin (a) role enabled.

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

1. **Log in to the ILOM web interface.**
2. **Select System Information --> Identification Information.**

   The Identification Information page appears.
3. **In the SP host name field, type the SP host name.**

   The host name can contain up to 60 characters.
4. **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.
5. **In the SP System Contact field, type the name of a person you will contact.**

   The system contact can consist of a text string using any standard keyboard keys except quotation marks.
6. **In the SP System Location field, type the text that describes the physical location of the system.**

   The system location can consist of a text string using any standard keyboard keys except quotation marks.
7. **Click Save for your settings to take effect.**

▼ View and Configure Network Settings

Before You Begin

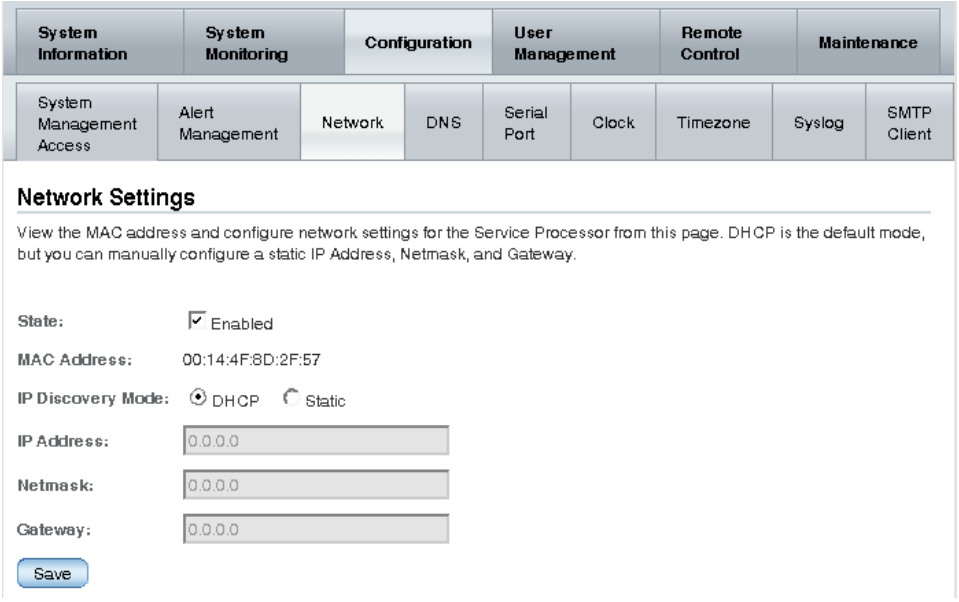
- To view network settings, you need the Read Only (o) role enabled. To configure network settings, you need the Admin (a) role enabled.

Follow these steps to view and configure network settings:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> Network.**

   The Network Settings page appears. From the Network Settings page, you can view MAC addresses and configure network addresses for the server's chassis monitoring module (CMM) and service processors (SP).

3. **You can have DHCP assign IP addresses automatically, or you can choose to assign the addresses manually.**
   - To automatically obtain an IP address, click the radio button next to DHCP. See the following figure.



- To manually set a static IP address, complete the information in the Network Settings page; use the descriptions in the following table.

Item	Description
State	Click the check box to enable the network state.
MAC Address	The SP'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. The MAC address is provided on a label on the SP or CMM, on the Customer Information Sheet included in the ship kit, and in the BIOS Setup screen.
IP Discovery Mode	Click the radio button next to Static to manually assign an IP address, netmask, and gateway.
IP Address	Type the server's IP address. The IP address is a unique name that identifies the system on a TCP/IP network.
Netmask	Type the subnet mask of the network on which the SP resides.
Gateway	Type SP'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 might need to log back in with a new browser session.

▼ View and Configure DNS Settings

Before You Begin

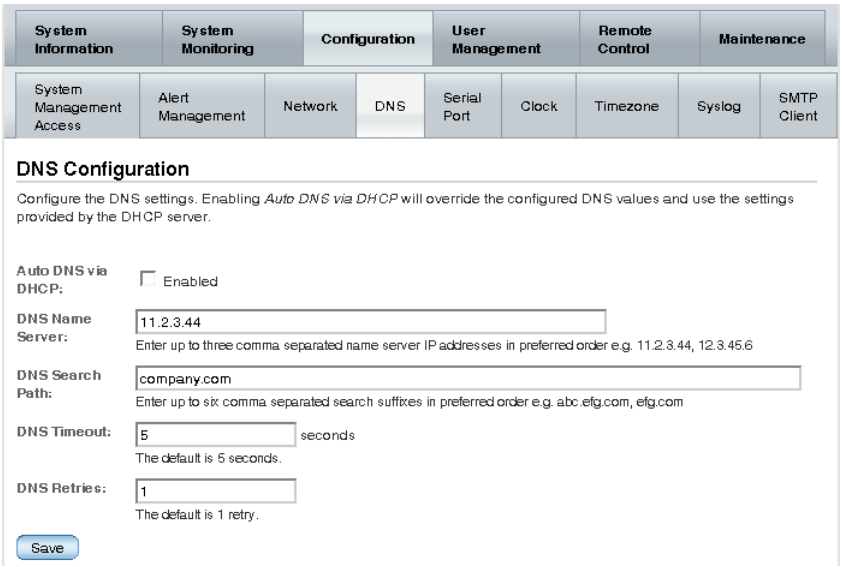
- To view Domain Name Service (DNS) settings, you need the Read Only (o) role enabled. To configure DNS settings, you need the Admin (a) role enabled.

Follow these steps to view and configure DNS settings:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> DNS.**

   The DNS Configuration page appears.

3. **You can have DHCP assign DNS Name Server and Search Path automatically, or you can choose to assign the addresses manually.**
   - To automatically assign the addresses, click the radio button next to Auto DNS via DHCP.
   - To manually assign the addresses, complete the DNS Name Server and DNS Search Path text boxes. See the following figure.



▼ View and Configure Serial Port Settings

Before You Begin

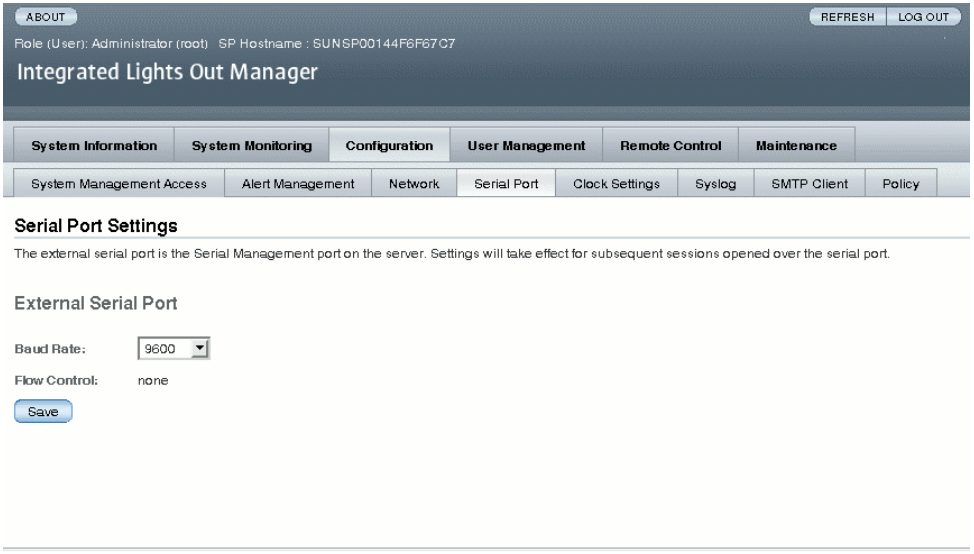
- To display serial port settings, you need the Read Only (o) role enabled. To configure serial port settings, you need the Admin (a) role enabled.

Follow these steps to view and configure serial port settings:

1. **Log in to the ILOM web interface.**

2. **Select Configuration --> Serial Port.**

   The Serial Port Settings page appears. See the following figure.



3. **View the baud rate for the internal host serial port and the external serial port.**

Note – The internal serial port is not supported on SPARC servers.

---

4. **Select the baud rate for the internal serial port from the Host Serial Port Baud Rate drop-down list.**

   For x64 systems, 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).

5. **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 server.

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

▼ Enable HTTP or HTTPS Web Access

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.

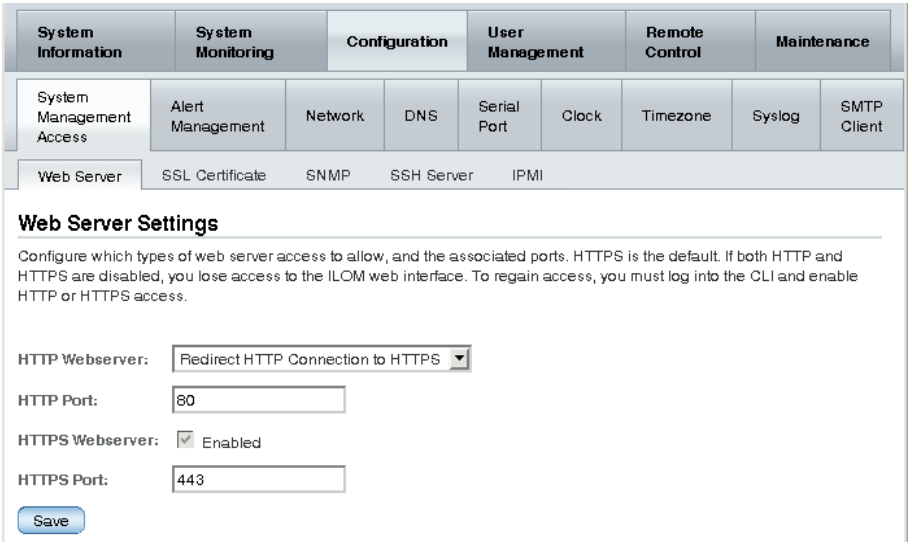
Before You Begin

- To modify HTTP or HTTPS settings, you need the Admin (a) role enabled.

Follow these steps to enable HTTP or HTTPS web access:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> System Management Access --> Web Server.**

   The Web Server Settings page appears.



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" in the *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

---

4. **Assign an HTTP or HTTPS port number.**
5. **Click Save for your settings to take effect.**
6. **To edit IP addresses assigned to the SP interfaces, do the following:**

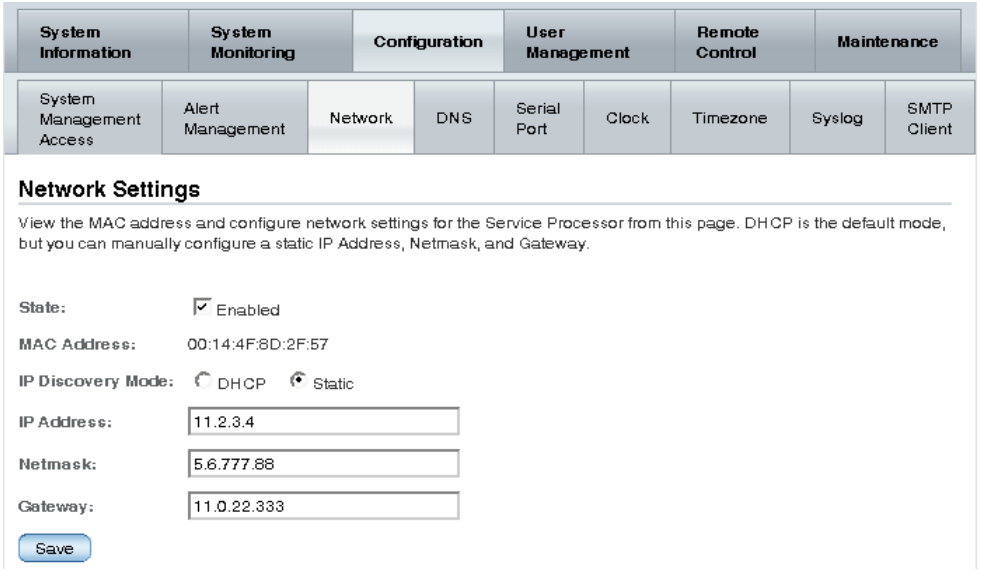
   a. **Select Configuration --> Network to access the Network Settings page.**

   b. **Select the radio button for Static IP Discovery Mode.**

   c. **Enter values for IP Address, Netmask, and Gateway in the text boxes.**

   d. **Click Save for your new settings to take effect.**

   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.



▼ 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.

Before You Begin

- To upload the SSL certificate, you need the Admin (a) role enabled.

Follow these steps to upload the SSL certificate:

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

   The SSL Certificate Upload page appears.
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.

Configuring Secure Shell Settings

Topics

Description	Links
Configure Secure Shell settings	• "Enable or Disable SSH" on page 27 • "Generate a New SSH Key" on page 27 • "Restart the SSH Server" on page 28

▼ Enable or Disable SSH

Before You Begin

- To restart the Secure Shell (SSH) server, you need the Admin (a) role enabled.

Follow these steps to enable or disable SSH:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> System Management Access --> SSH Server.**
   The SSH Server Settings page appears.
3. **To enable the SSH server, click the Enabled check box next to State.**
4. **Click Save for your settings to take effect.**

▼ Generate a New SSH Key

Before You Begin

- To generate a new SSH key, you need the Admin (a) role enabled.

Follow these steps to generate a new SSH key:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> System Management Access --> SSH Server.**
   The SSH Server Settings page appears.

3. **Select RSA by clicking the Generate RSA Key button, or select DSA by clicking the Generate DSA Key button.**

   Click OK or Cancel when you are prompted.

   A new key will not take effect until the SSH server is restarted.

▼ Restart the SSH Server

Before You Begin

- To restart the SSH server, you need the Admin (a) role enabled.

Note – Restarting the SSH server will end any existing SSH connections.

Follow these steps to restart the SSH server:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> System Management Access --> SSH Server.**

   The SSH Server Settings page appears.
3. **Click the Restart button to restart the SSH Server.**

CHAPTER 5

Managing User Accounts

Topics

Description	Links
Configure user accounts	• "Configure Single Sign On" on page 30 • "Set the Session Time-Out" on page 31 • "Add User Accounts and Assign Roles" on page 31 • "Configure a User Account" on page 33 • "Delete a User Account" on page 36 • "View User Sessions" on page 36
Configure SSH host key	• "Add an SSH Key" on page 37 • "Delete an SSH Key" on page 41
Configure Active Directory settings	• "View and Configure Active Directory Settings" on page 41 • "Configure Active Directory Tables" on page 45 • "Troubleshoot Active Directory Authentication and Authorization" on page 49
Configure LDAP settings	• "Configure the LDAP Server" on page 51 • "Configure ILOM for LDAP" on page 52
Configure LDAP/SSL settings	• "View and Configure LDAP/SSL Settings" on page 53 • "Configure LDAP/SSL Tables" on page 57 • "Troubleshoot LDAP/SSL Authentication and Authorization" on page 60
Configure RADIUS settings	• "Configure RADIUS Settings" on page 61

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• User Account Management • Guidelines for Managing User Accounts	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• CLI	• Managing User Accounts	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
• SNMP	• Managing User Accounts	*Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/

Configuring User Accounts

Topics

Description	Links
Configure user accounts	• "Configure Single Sign On" on page 30 • "Set the Session Time-Out" on page 31 • "Add User Accounts and Assign Roles" on page 31 • "Configure a User Account" on page 33 • "Delete a User Account" on page 36 • "View User Sessions" on page 36

▼ Configure Single Sign On

Before You Begin

- To disable or enable Single Sign On, you need the Admin (a) role enabled.

Follow these steps to enable or disable Single Sign On:

1. Log in to the ILOM web interface.

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.**

▼ 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.

Before You Begin

- To set the session time-out, you need the Read Only (o) role enabled.

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

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

   The Session Time-Out page appears.

3. **Select your preferred time increment from the drop-down list.**
4. **Click the Apply button to save your change.**

▼ Add User Accounts and Assign Roles

Before You Begin

- To add, modify, or delete user accounts, you need the Admin (a) role enabled.

Note – Only accounts with the User Management (u) role are allowed to add, modify, or delete user accounts. However, you need only the Read Only (o) role to modify your own password. If a new user is assigned the User Management (u) role, those privileges are also automatically granted for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to ILOM.

Follow these steps to add user accounts and assign roles:

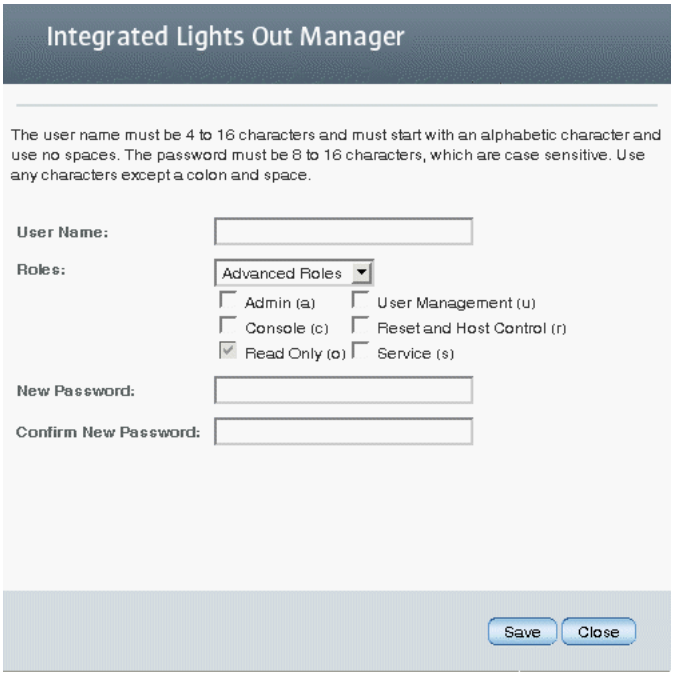
1. **Log in to the ILOM web interface.**

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

   The User Account Settings page appears.

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

   The Add User dialog appears.



4. **Complete the following information:**

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

   b. **Choose a profile. Options include:**

   - `Advanced Role` for all new ILOM 3.0 installations. Choosing `Advanced Role` gives you the option of selecting Admin (`a`), Console (`c`), Read Only (`o`), User Management (`u`), Reset and Host Control (`r`), and Service (`s`). For a description of the roles and privileges assigned to user accounts, see "Roles for ILOM User Accounts" in the *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
   - `Administrator` or `Operator` for customers who are upgrading from ILOM 2.0 to ILOM 3.0.
   - `None`

   c. **Select the appropriate roles.**

d. 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.

e. Retype the password in the Confirm Password field to confirm the password.

f. 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.

▼ Configure a User Account

You can modify a user account by changing the user's password, and the user's network and serial privileges.

Before You Begin

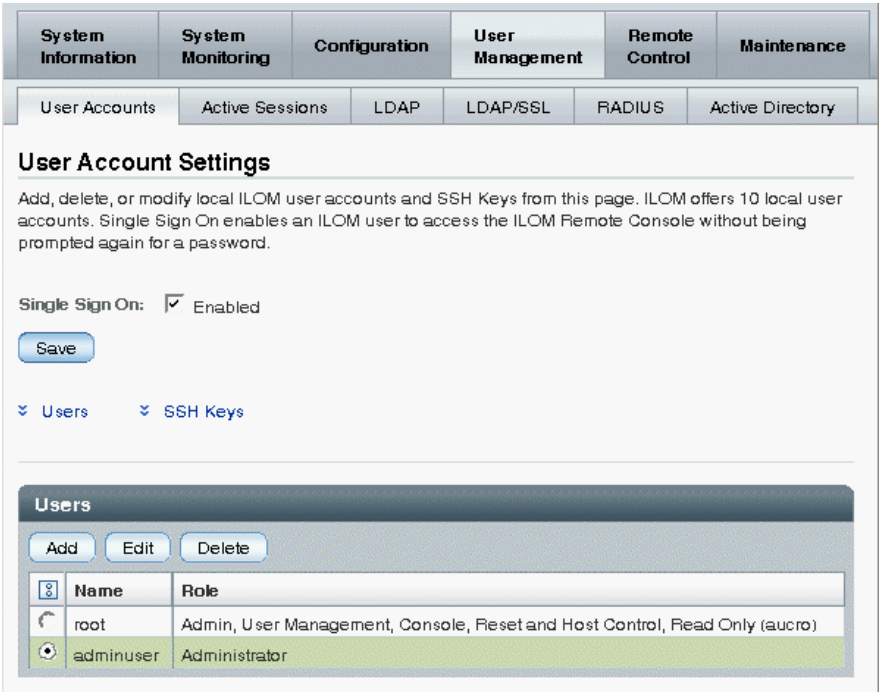
- To add, modify, or delete user accounts you need the User Management (u) role enabled.

Follow these steps to configure a user account:

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

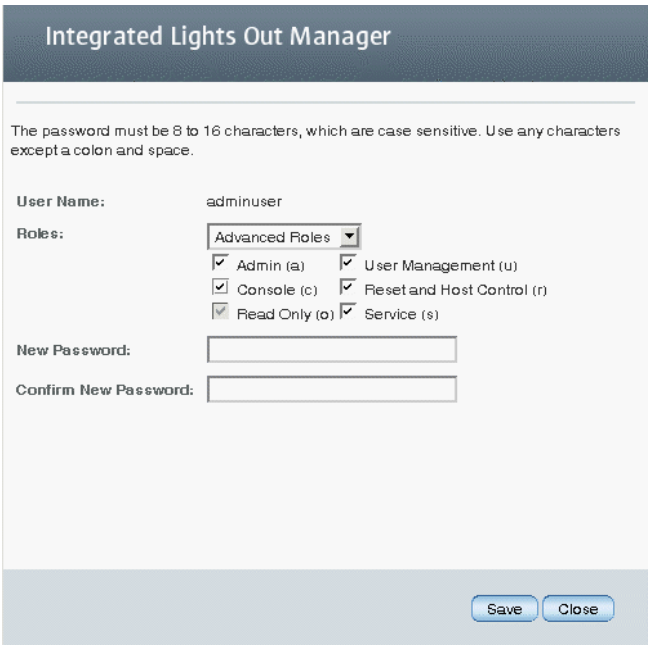
   The User Account Settings page appears.
3. **In the Users table, select a radio button next to the user account you want to modify.**

   The following figure shows user1 is selected.



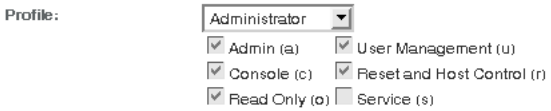
4. **Click Edit.**

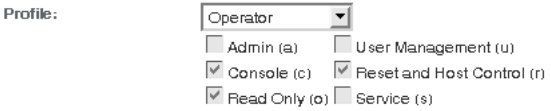
   The Edit User dialog appears. See the following figure.



5. **Modify the profile.**

   When `Advanced Role` is selected as the profile, a user with the `u` role can select any of the six available roles. However, if you have chosen `Administrator` or `Operator` as your profile, individual roles will be selected automatically. The two following figures illustrate the roles that are made available to users who chose `Administrator` and `Operator`.





6. **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.

7. **Retype the password in the Confirm New Password field to confirm the password.**
8. **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 with your changes.

▼ Delete a User Account

Before You Begin

- To add, modify, or delete user accounts you need the User Management (u) role enabled.

Follow these steps to delete a user account:

1. **Log in to the ILOM 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.**
4. **In the Users table, click Delete.**

   A confirmation dialog opens.
5. **Click OK to delete the account or click Cancel to stop the process.**

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

▼ View User Sessions

Before You Begin

- To view a list of user sessions, you need the Read Only (o) role enabled.

Follow these steps to view user sessions:

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.

Configuring SSH Keys

Topics

Description	Links
Configure SSH host key	• "Add an SSH Key" on page 37 • "Delete an SSH Key" on page 41

You can use SSH keys to automate password authentication. The following procedures describe how to add and delete SSH keys.

▼ Add an SSH Key

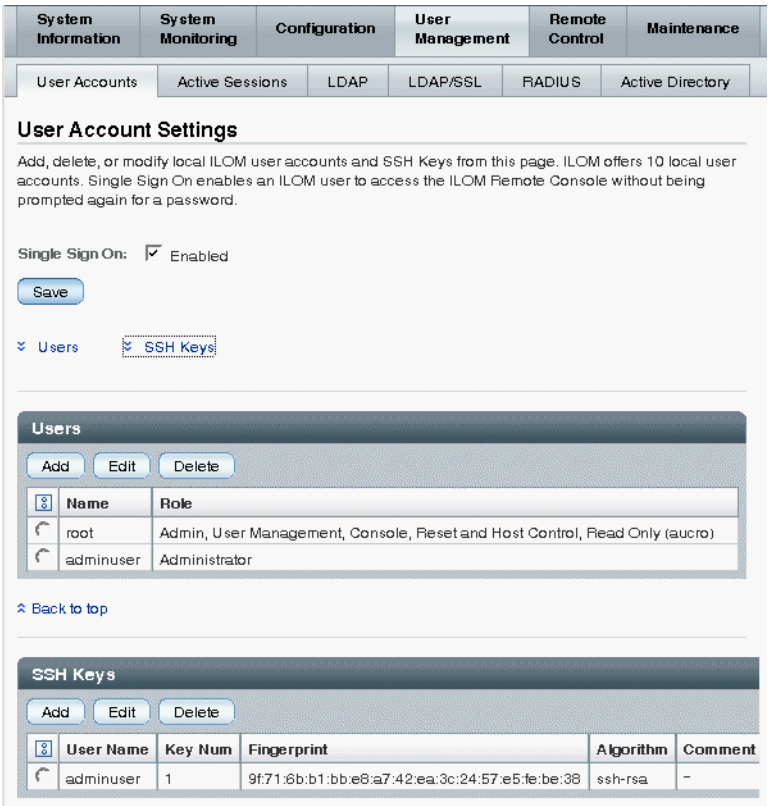
Before You Begin

- To add an SSH key, you need the Admin (a) role enabled.

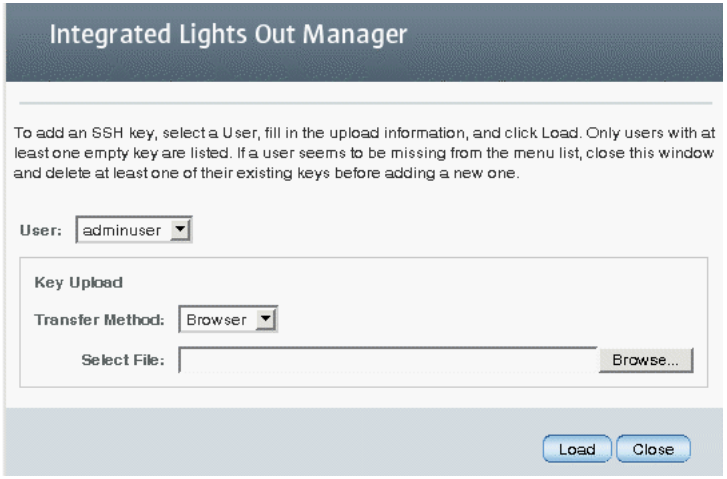
Follow these steps to add an SSH key:

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

   The User Accounts Setting page appears.



3. **Scroll down to the SSH Keys listing at the bottom of the page and click Add.**
   The SSH key add screen appears.



4. **Select a user account from the User drop-down list.**
5. **Select a transfer method from the Transfer Method drop-down list.**

   The following transfer methods are available:

   - Browser
   - TFTP
   - FTP
   - SFTP
   - SCP
   - HTTP
   - HTTPS
6. **If you select the Browser transfer method, click Browse and browse to the location of the SSH key. Proceed to Step 9.**
7. **If you select the TFTP transfer method, the prompts shown in the following figure appear and you must provide the following information, then proceed to Step 9:**
   - **Host** – Enter the remote host IP address or, if you have DNS configured, the name of the remote host.
   - **Filepath** – Enter the path to which to save the configuration file in the format: `directoryPath/filename`.

8. **If you select the SCP, FTP, SFTP, HTTP, or HTTPS transfer method, the prompts shown in the next figure appear and you must provide the following information, then proceed to Step 9:**
   - **Host** – Enter the remote host IP address or, if you have DNS configured, the name of the remote host.
   - **Filepath** – Enter the path to which to save the configuration file in the format: `directoryPath/filename`.
   - **Username** – Enter the user name of your account on the remote system.
   - **Password** – Enter the password for your account on the remote system.

9. **To add the SSH key to the selected user account, click Load.**

   The SSH key is added to the user account.

▼ Delete an SSH Key

Before You Begin

- To delete an SSH key, you need the Admin (a) role enabled.

Follow these steps to delete an SSH key:

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

   The User Account Settings page appears.
3. **Scroll down to the SSH Keys section at the bottom of the page, select a user, and click Delete.**

   A confirmation dialog box appears.
4. **Click OK.**

   The SSH key is deleted.

Configuring Active Directory

Topics

Description	Links
Configure Active Directory settings	• "View and Configure Active Directory Settings" on page 41 • "Configure Active Directory Tables" on page 45 • "Troubleshoot Active Directory Authentication and Authorization" on page 49

▼ View and Configure Active Directory Settings

Before You Begin

- To configure Active Directory settings, you need the User Management (u) role enabled.

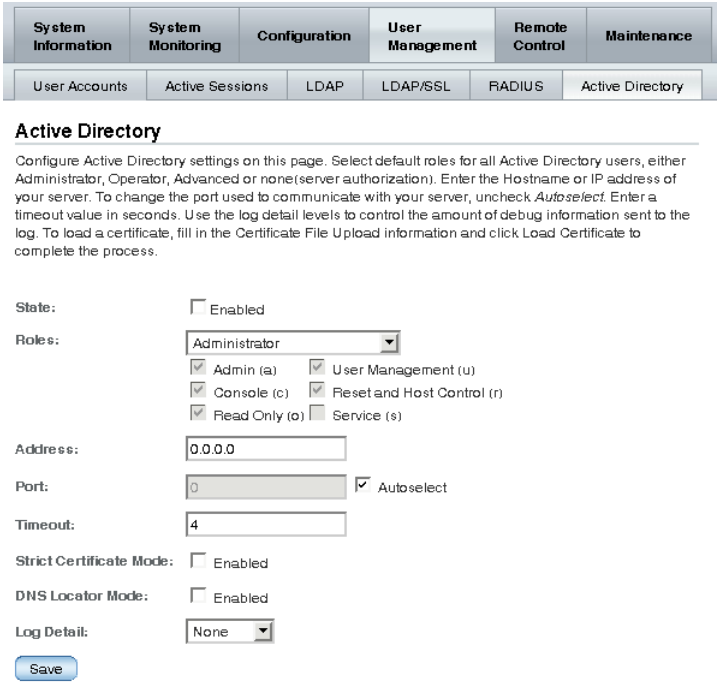
Follow these steps to view and configure Active Directory settings:

1. **Log in to the ILOM web interface.**

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

   The Active Directory page appears. There are three sections to the Active Directory page, as shown in the following figures.

   - The top section, which includes targets and properties.



   - The middle section, which includes the primary certificate information.

- The bottom section, which includes the Active Directory tables.

3. **Configure the Active Directory settings displayed in the top section of the Active Directory Settings page.**

   See the following table for a description of the Active Directory settings.

Property	Default	Description
State	Disabled	Enabled | Disabled
Roles	(none)	Administrator | Operator | Advanced | none Access role granted to all authenticated Active Directory users. This property supports the legacy roles of Administrator or Operator, or any of the individual role ID combinations of 'a', 'u', 'c', 'r', 'o' and 's'. For example, `aucros`, where `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, `o`=Read-Only, and `s`=Service. If you do not configure a role, the Active Directory server is used to determine the role.
Address	0.0.0.0	IP address or DNS name of the Active Directory server. If DNS name is used, then DNS must be configured and operational.
Port	0	Port used to communicate with the server. If `autoselect` is selected, the port is set to 0. Available in the unlikely event of a non-standard TCP port being used.
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.

Property	Default	Description
Strict Certificate Mode	Disabled	Enabled | Disabled If enabled, the server certificate contents are verified by digital signatures at the time of authentication. Certificate must be loaded before Strict Certificate Mode can be set to enabled.
DNS Locator Mode	Disabled	Enabled | Disabled If enabled, an attempt to locate the Active Directory server is performed, based on the DNS locator queries that are configured.
Log Detail	None	None | High | Medium | Low Specifies the amount of diagnostics that go into the event log.

4. **Click Save in the top section of the Active Directory settings page for your settings to take effect.**

5. **View the Active Directory certificate information in the middle section of the Active Directory settings page.**

   See the following table for a description of Active Directory certificate settings.

Property	Displays	Description
Certificate File Status	`certificate not present`	Read-only indicator of whether a certificate exists.
Certificate File Status	`certificate present (details)`	Click on "details" for information about issuer, subject, serial number, valid_from, valid_to, and version.

6. **Complete the "Certificate File Upload" section by selecting a transfer method for uploading the certificate file and the requested parameters.**

Note – This section is only required if Strict Certificate Mode is going to be enabled. If Strict Certificate Mode is disabled, data will still be protected but a certificate will not be needed.

The following table describes the required parameters for each transfer method:

Transfer Method	Required Parameters
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

7. **Click the Load Certificate button or Remove Certificate button.**
8. **If a certificate is loaded, click on the "details" link to show the following information.**

`Issuer`	Certificate Authority who issued the certificate.
`Subject`	Server or domain for which the certificate is intended.
`Valid From`	Date when the certificate becomes valid.
`Valid Until`	Date when the certificate becomes invalid.
`Serial Number`	Serial number of the certificate.
`Version`	Version number of the certificate.

▼ Configure Active Directory Tables

Before You Begin

- To configure Active Directory table settings, you need the User Management `(u)` role enabled.

Follow these steps to configure Active Directory table settings:

1. **Log in to the ILOM web interface.**
2. **Select User Management --> Active Directory.**

   The Active Directory page appears.

3. **At the bottom of the Active Directory page, click the link to access the category of table you want to configure:**
   - Admin Groups
   - Operator Groups
   - Custom Groups
   - User Domains
   - Alternate Servers
   - DNS Locator Queries
4. **Select the radio button of the individual table, then click Edit.**
5. **Enter the required data into the tables.**

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

   - **Admin Groups Table:**

     The Admin Groups table contains the names of the Microsoft Active Directory groups in the Distinguished Name (DN) format, Simple Name format, or NT-Style Name.

ID	Name
1	`CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=sun,DC=com`
2	

   - **Operator Groups Table:**

     The Operator Groups table contains the names of the Microsoft Active Directory groups in the Distinguished Name (DN) format, Simple Name format, or NT-Style Name.

ID	Name
1	`CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=sun,DC=com`
2	

- **Custom Groups Table**:

  The Custom Groups table contains the names of the Microsoft Active Directory groups in the Distinguished Name (DN) format, Simple Name format, or NT-Style Name. The associated roles for the entry are also configured.

ID	Name	Roles
1	custom_group_1	Admin, User Management, Console, Reset and Host Control, Read Only (aucro)

- **User Domains Table:**

  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. User authentication is attempted based on the user name that is entered and the configured user domains.

  In the example below, 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 with the first entry failed.

Note – In the example below, <USERNAME> will be replaced with the user's login name. During authentication, the user's login name replaces <USERNAME>.

ID	Domain
1	<USERNAME>@sales.east.sun.com
2	CN=<USERNAME>,CN=Users,DC=sales,DC=east,DC=sun, DC=com

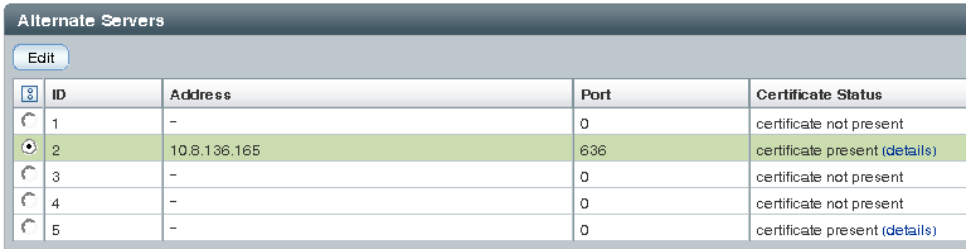
- **Alternate Servers Table:**

  The Alternate Servers table provides redundancy as well as a choice of different servers if required due to isolated domains. If a certificate is not supplied, but is required, the top-level primary certificate is used. 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.

ID	Address	Port	Certificate Status
1	-	0	`certificate not present`
2	`10.8.136.165`	0	`certificate present (details)`

The following image shows an Alternate Servers table with a certificate present in ID 2:



The following certificate information is displayed when you click on the "details" link:

`Issuer`	Certificate Authority who issued the certificate.
`Subject`	Server or domain for which the certificate is intended.
`Valid From`	Date when the certificate becomes valid.
`Valid Until`	Date when the certificate becomes invalid.
`Serial Number`	Serial number of the certificate.
`Version`	Version number of the certificate.

- **DNS Locator Queries Table:**

  The DNS Locator Queries table queries DNS servers to learn about the hosts to use for authentication.

The DNS Locator service query identifies the named DNS service. The port ID is generally part of the record, but it can be overridden by using the format <PORT:636>. Also, named services specific for the domain being authenticated can be specified by using the <DOMAIN> substitution marker.

Name	Domain
1	_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
2	_ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>

Note – DNS and DNS Locator Mode must be enabled for DNS Locator Queries to work.

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

▼ Troubleshoot Active Directory Authentication and Authorization

Before You Begin

- To view authentication and authorization events, you need the Read Only (o) role enabled.

Follow these steps to troubleshoot Active Directory authentication and authorization:

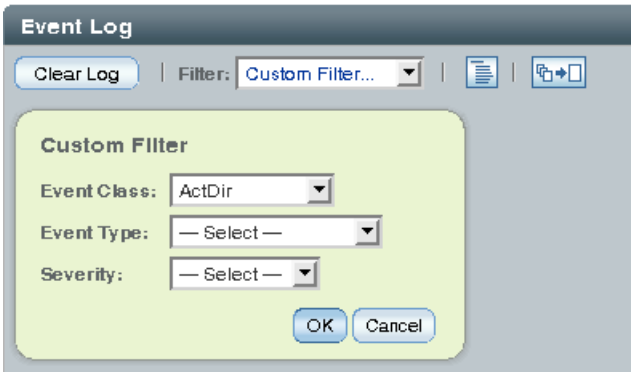
1. **Log in to the ILOM web interface.**
2. **Select User Management --> Active Directory.**

   The Active Directory page appears.
3. **In the Log Detail drop-down list, select the level of detail that you would like the event log to capture.**

   Choices are None, High, Medium, Low, and Trace.
4. **Click Save to save your changes.**
5. **Attempt an authentication to generate events. Follow these steps:**

   a. **From the System Monitoring tab select Event Logs.**

   b. **In the Filter drop-down list, select Custom Filter.**



c. In the Event Class drop-down list, select ActDir.

d. Click OK.

All Active Directory events will appear in the event log.

Event Log

Displays every event in the SP, including IPMI, Audit, and FMA events. Click the *Clear Log* button to delete all current log entries.

Event Log

Clear Log | Filter: Custom Filter Applied

Event ID	Class	Type	Severity	Date/Time	Description
92	ActDir	Log	critical	Mon Jul 7 11:27:15 2008	(ActDir) authentication status: auth-ERROR
91	ActDir	Log	major	Mon Jul 7 11:27:15 2008	(ActDir) server-authenticate: auth-error idx 2 cfg-server 0.0.0.0
90	ActDir	Log	major	Mon Jul 7 11:27:15 2008	(ActDir) ServerUserAuth - Error 0, config not valid
89	ActDir	Log	major	Mon Jul 7 11:27:15 2008	(ActDir) server-authenticate: auth-error idx 0 cfg-server 0.0.0.0
88	ActDir	Log	major	Mon Jul 7 11:27:15 2008	(ActDir) ServerUserAuth - Error 0, config not valid
87	ActDir	Log	minor	Mon Jul 7 11:27:15 2008	(ActDir) _DNS_MaxServers: num-svrs - 0

Configuring Lightweight Directory Access Protocol

Topics

Description	Links
Configure LDAP settings	• "Configure the LDAP Server" on page 51 • "Configure ILOM for LDAP" on page 52

▼ Configure the LDAP Server

Before You Begin

- To configure LDAP settings, you need the User Management (u) role enabled.

Follow these steps to 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."**

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

   For example:

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

   or

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

2. **Add object classes `posixAccount` and `shadowAccount`, and populate the required property values for this schema (RFC 2307). See the following table for a description of the required property values.**

Required Property	Description
uid	User name for logging in to ILOM
uidNumber	Any unique number
gidNumber	Any unique number

Required Property	Description
userPassword	Password
homeDirectory	Any value (this property is ignored by ILOM)
loginShell	Any value (this property is ignored by ILOM)

3. **Configure the LDAP server to enable LDAP server access to ILOM user accounts.**

   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

Before You Begin

- To configure LDAP settings, you need the User Management (u) role enabled.

Follow these steps to configure ILOM for LDAP:

1. **Log in to the ILOM web interface.**
2. **Select User Management --> LDAP.**

   The LDAP Settings page appears.
3. **Enter the following values:**
   - **State** – Select the Enabled check box to authenticate LDAP users.
   - **Role** – The default role of LDAP users.
   - **Address** – Either the IP address or DNS name of the LDAP server.
   - **Port** – The port number on the LDAP server. The default port is 389.
   - **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 for your changes to take effect.**
5. **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.

Configuring LDAP/SSL Settings

Topics

Description	Links
Configure LDAP/SSL settings	• "View and Configure LDAP/SSL Settings" on page 53 • "Configure LDAP/SSL Tables" on page 57 • "Troubleshoot LDAP/SSL Authentication and Authorization" on page 60

▼ View and Configure LDAP/SSL Settings

Before You Begin

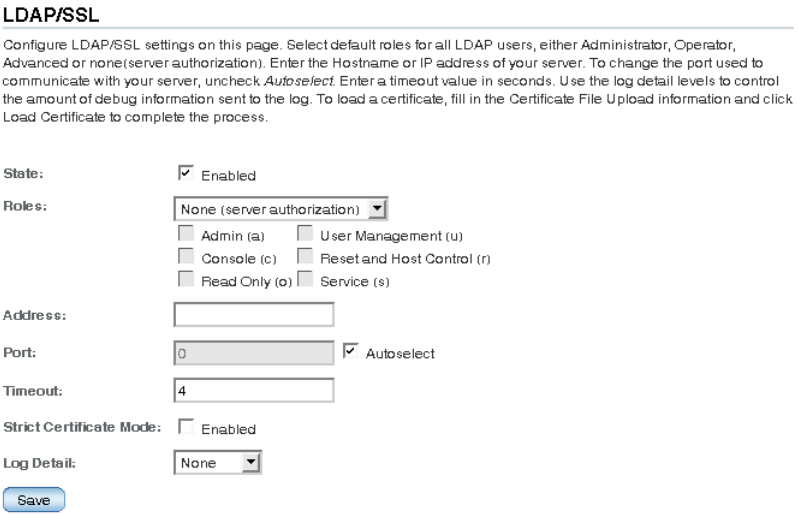
- To configure LDAP/SSL settings, you need the User Management (u) role enabled.

Follow these steps to view and configure LDAP/SSL settings:

1. **Log in to the ILOM web interface.**
2. **Select User Management --> LDAP/SSL.**

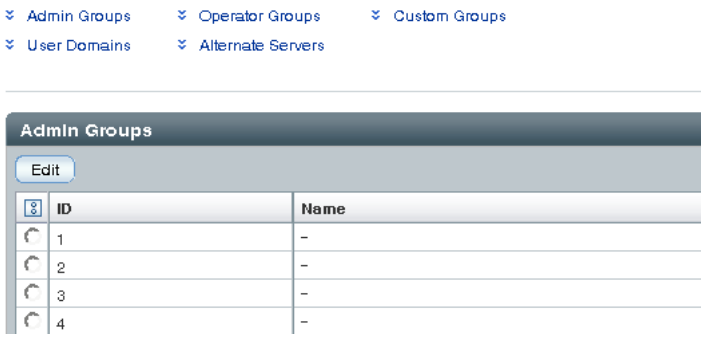
   The LDAP/SSL page appears. There are three sections to the LDAP/SSL page.

- The top section, which includes targets and properties.



- The middle section, which includes certificate information.

- The bottom section, which includes the LDAP/SSL tables.



3. **Configure the LDAP/SSL settings displayed in the top section of the LDAP/SSL Settings page.**

   See the following table for a description of the LDAP/SSL settings.

Property (Web)	Default	Description
State	Disabled	Enabled | Disabled
Roles	(none)	Administrator | Operator | Advanced | (none) Access role granted to all authenticated LDAP/SSL users. This property supports the legacy roles of Administrator or Operator, or any of the individual role ID combinations of 'a', 'u', 'c', 'r', 'o' and 's'. For example, `aucros`, where `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, `o`=Read-Only, and `s`=Service. If you do not configure a role, the LDAP/SSL server is used to determine the role.
Address	0.0.0.0	IP address or DNS name of the LDAP/SSL server.
Port	0	Port used to communicate with the server. If `autoselect` is enabled, then the port is set to 0. Available in the unlikely event of a non-standard TCP port being used.
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	Disabled	Enabled | Disabled If enabled, the server certificate contents are verified by digital signatures at the time of authentication. Certificate must be loaded before Strict Certificate Mode can be set to enabled.
Log Detail	None	None | High | Medium | Low Specifies the amount of diagnostics that go into the event log.

4. **Click Save in the top section of the LDAP/SSL settings page to save any changes made to this section.**

5. **View the LDAP/SSL certificate information in the middle section of the LDAP/SSL settings page.**

   See the following table for a description of LDAP/SSL certificate settings.

Property	Displays	Description
Certificate File Status	`certificate not present`	Read-only indicator of whether a certificate exists.
Certificate File Status	`certificate present (details)`	Click on "details" for information about issuer, subject, serial number, valid_from, valid_to, and version.

6. **Complete the "Certificate File Upload" section by selecting a transfer method for uploading the certificate file.**

Note – This section is only required if Strict Certificate Mode is used. If Strict Certificate Mode is disabled, data will still be protected but a certificate will not be needed.

The following table describes the required parameters for each transfer method:

Transfer Method	Required Parameters
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

7. **Click the Load Certificate button or Remove Certificate button.**

8. **If a certificate was loaded, click on the "details" link in the web interface to show the following information.**

`Issuer`	Certificate Authority who issued the certificate.
`Subject`	Server or domain for which the certificate is intended.
`Valid From`	Date when the certificate becomes valid.
`Valid Until`	Date when the certificate becomes invalid.
`Serial Number`	Serial number of the certificate.
`Version`	Version number of the certificate.

▼ Configure LDAP/SSL Tables

Before You Begin

- To configure LDAP/SSL settings, you need the User Management (`u`) role enabled.

Follow these steps to configure LDAP/SSL tables:

1. **Log in to the ILOM web interface.**
2. **Select User Management --> LDAP/SSL.**

   The LDAP/SSL page appears.
3. **At the bottom of the LDAP/SSL page, click the link to access the category of table you want to configure:**
   - Admin Groups
   - Operator Groups
   - Custom Groups
   - User Domains
   - Alternate Servers
4. **Select the radio button of the individual table, then click Edit.**
5. **Enter the required data in the tables.**

   In the following tables, default data shows the expected format of the LDAP/SSL data.

- **Admin Groups Table:**

  The Admin Groups table contains the names of the LDAP/SSL groups in the Distinguished Name (DN) format.

ID	Name
1	CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=sun,DC=com
2	

- **Operator Groups Table:**

  The Operator Groups table contains the names of the LDAP/SSL groups in the Distinguished Name (DN) format.

ID	Name
1	CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=sun,DC=com
2	

- **Custom Groups Table**:

  The Custom Groups table contains the names of the LDAP/SSL groups in the Distinguished Name (DN) format, Simple Name format, or NT-Style Name. The associated roles for the entry are also configured. The name listed in entry 1 uses the Simple Name format.

ID	Name	Roles
1	custom_group_1	Admin, User Management, Console, Reset and Host Control, Read Only (aucro)

- **User Domains Table:**

  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. User authentication is attempted based on the user name that is entered and the configured user domains.

  Entry 1 shows the complete Distinguished Name, which LDAP/SSL would use if the attempt to authenticate the first entry failed.

Note – <USERNAME> will be replaced with the user's login name during authentication. Either the principle or Distinguished Name format is supported.

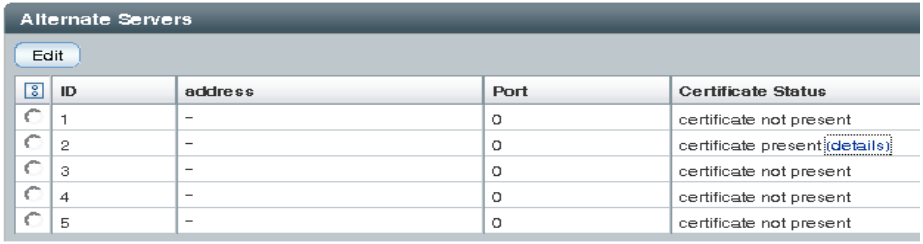
ID	Domain
1	UID=<USERNAME>,OU=people,DC=sun,DC=com
2	

- **Alternate Servers Table:**

  The Alternate Servers table provides redundancy for authentication. If a certificate is not supplied, but is required, the top-level primary certificate is used. 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.

ID	Address	Port	Certificate Status
1	-	0	certificate not present
2	-	0	certificate not present
3	10.7.143.246	0	certificate present (details)

The following image shows an Alternate Servers table with a certificate present in ID 2:



The following information is displayed when you click on the "details" link:

Issuer	Certificate Authority who issued the certificate.
Subject	Server or domain for which the certificate is intended.
Valid From	Date when the certificate becomes valid.

`Valid Until`	Date when the certificate becomes invalid.
`Serial Number`	Serial number of the certificate.
`Version`	Version number of the certificate.

▼ Troubleshoot LDAP/SSL Authentication and Authorization

Before You Begin

- To view authentication and authorization events, you need the Read Only (o) role enabled.

Follow these steps to troubleshoot LDAP/SSL authentication and authorization:

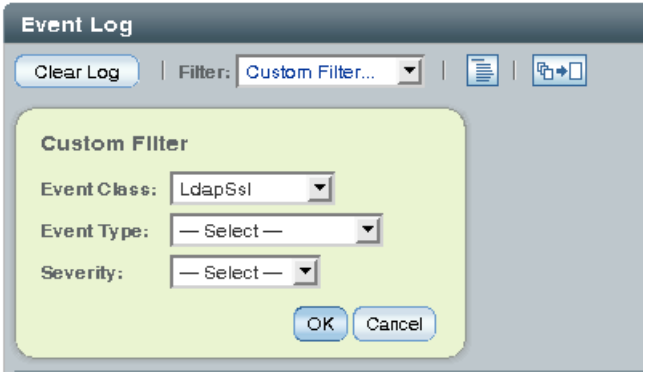
1. **Log in to the ILOM web interface.**
2. **Select User Management --> LDAP/SSL.**

   The LDAP/SSL page appears.
3. **In the Log Detail drop-down list, select the level of detail that you would like the event log to capture.**

   Choices are None, High, Medium, Low, and Trace.
4. **Click Save to save your changes.**
5. **Attempt an authentication to generate events:**

   a. **Select System Monitoring --> Event Logs.**

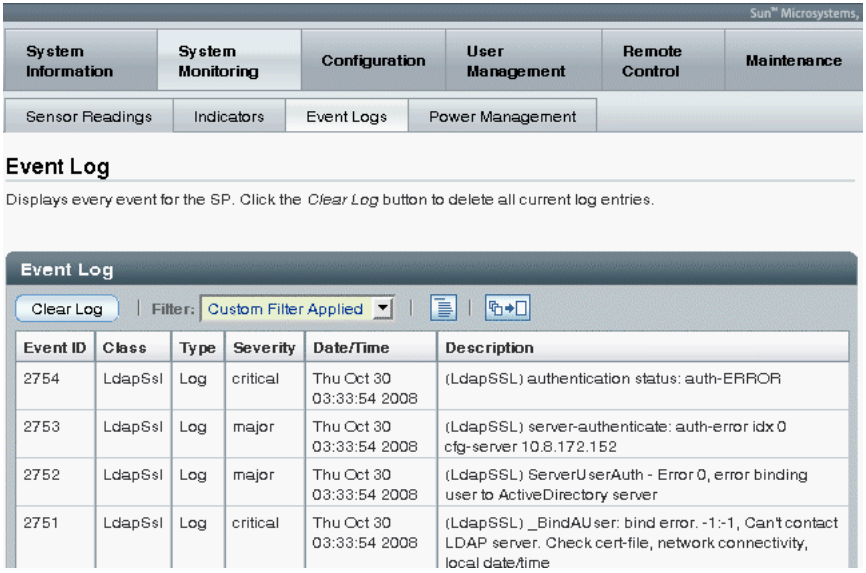
   b. **In the Filter drop-down list, select Custom Filter.**



   c. **In the Event Class drop-down list, select LdapSsl.**

d. Click OK for your changes to take effect.

All LDAP/SSL events will appear in the event log.



Configuring RADIUS

Topics

Description	Links
Configure RADIUS settings	• "Configure RADIUS Settings" on page 61

▼ Configure RADIUS Settings

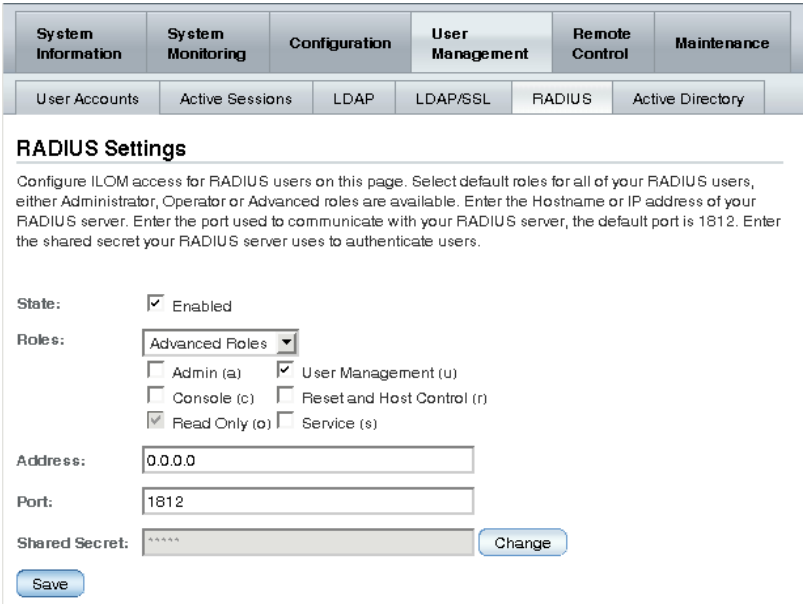
Before You Begin

- To configure RADIUS settings, you need the User Management (u) role enabled.

Follow these steps to configure RADIUS settings:

1. **Log in to the ILOM web interface.**
2. **Select User Management --> RADIUS.**

   The RADIUS Settings page appears.



3. **Complete the settings.**

Property (Web)	Default	Description
State	Disabled	Enabled | Disabled Specifies whether the RADIUS client is enabled or disabled.
Role	Operator	Administrator | Operator | Advanced Roles Access role granted to all authenticated RADIUS users. This property supports the legacy roles of Administrator or Operator, or any of the individual role ID combinations of 'a', 'u', 'c', 'r', 'o', and 's'. For example, `aucrs`, where `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, `o`=Read Only, and `s`=Service.

Property (Web)	Default	Description
Address	0.0.0.0	IP address or DNS name of the RADIUS server. If the DNS name is used, DNS must be configured and functional.
Port	1812	Specifies the port number used to communicate with the RADIUS server. The default port is 1812.
Shared Secret	(none)	Specifies the shared secret that is used to protect sensitive data and to ensure that the client and server recognize each other.

4. **Click Save for your changes to take effect.**

CHAPTER 6

Managing System Components

Topics

Description	Links
Manage system components	• "Viewing and Changing Component Information" on page 66 • "Prepare to Remove a Component" on page 68 • "Return a Component to Service" on page 68 • "Enable and Disable Components" on page 68

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• About Fault Management	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• CLI	• Managing System Components	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/

Viewing Component Information and Managing System Components

Topics

Description	Links
Review the prerequisites	• "Before You Begin" on page 66
View and manage system components	• "Viewing and Changing Component Information" on page 66 • "Prepare to Remove a Component" on page 68 • "Return a Component to Service" on page 68 • "Enable and Disable Components" on page 68

Before You Begin

Prior to performing the procedures in this section, you should ensure that the following requirement is met.

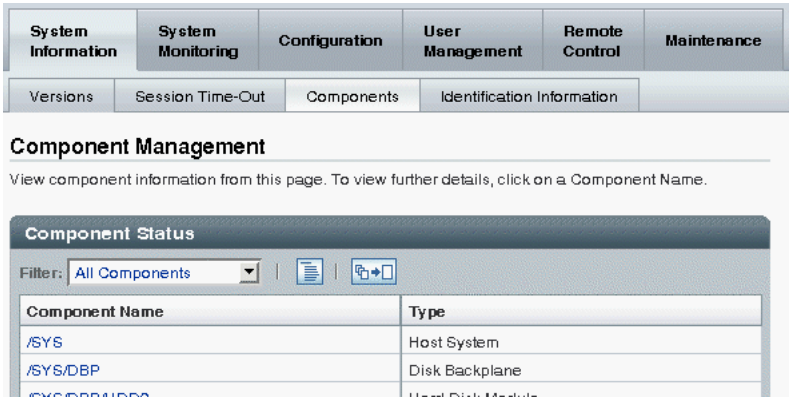
- To manage system components, you need the Reset and Host Control (`r`) role enabled.

▼ Viewing and Changing Component Information

Follow these steps to view and change component information:

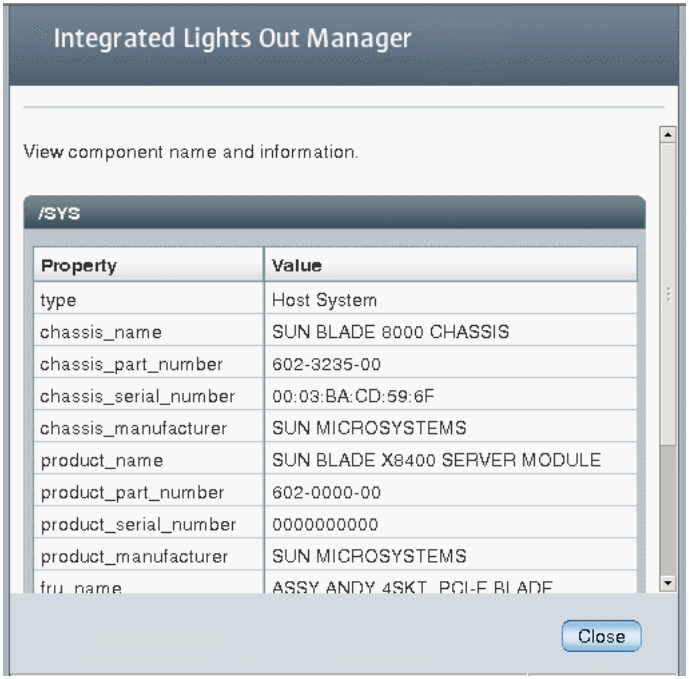
1. **Log in to the ILOM web interface.**
2. **Select System Information --> Components.**

   The Component Management page appears.



3. **When a component is faulted, a radio button will appear to the left of the component name. Click on the radio button to check the fault status. If radio buttons do not appear, click on the name of a component to verify the status.**

   A dialog box appears with information about the selected component. See the following figure.



▼ Prepare to Remove a Component

Follow these steps to prepare to remove a component:

1. **Log in to the ILOM web interface.**
2. **Select System Information --> Components.**
   The Component Management page appears.
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

Follow these steps to return a component to service:

1. **Log in to the ILOM web interface.**
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

Follow these steps to enable and disable components:

1. **Log in to the ILOM web interface.**
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.

CHAPTER 7

Monitoring System Components

Topics

Description	Links
View sensor readings	• "View Sensor Readings" on page 71
Configure system indicators, clock, and timezone settings	• "Configure System Indicators" on page 72 • "Configure Clock Settings" on page 73 • "Configure Timezone Settings" on page 74
Filter, view, clear, and configure event logs	• "Filter Event Log Output" on page 74 • "View and Clear the ILOM Event Log" on page 76 • "Configure Remote Syslog Receiver IP Addresses" on page 77
View fault status	• "View Fault Status" on page 78
Collect data for use by service engineers to diagnose system problems	• "Collect SP Data to Diagnose System Problems" on page 78

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• System Monitoring and Alert Management • Collect SP Data to Diagnose System Problems	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• CLI	• Monitoring System Sensors, Indicators, and ILOM Event Logs • Collect SP Data to Diagnose System Problems	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
• SNMP	• Monitoring the System	*Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/

Monitoring System Sensors, Indicators, and ILOM Event Logs

Topics

Description	Links
View sensor readings	• "View Sensor Readings" on page 71
Change the state of a system indicator	• "Configure System Indicators" on page 72
View and set clock settings	• "Configure Clock Settings" on page 73
Configure timezone settings	• "Configure Timezone Settings" on page 74
Set filters for event log data	• "Filter Event Log Output" on page 74
View and clear the event log	• "View and Clear the ILOM Event Log" on page 76
Set the remote syslog receiver IP addresses	• "Configure Remote Syslog Receiver IP Addresses" on page 77
View the fault state of a component	• "View Fault Status" on page 78
Collect SP data to diagnose system problems	• "Collect SP Data to Diagnose System Problems" on page 78

▼ View Sensor Readings

Before You Begin

- To view the indicator state, you need the Read Only (o) role enabled.

Follow these steps to view sensor readings:

1. **Log in to the ILOM web interface.**
2. **Select System Monitoring --> Sensors Readings.**

   The Sensor Readings page appears.

Note – If the server is powered off, many components will appear as "no reading."

---

3. **In the Sensor Readings page, do the following:**

   a. **Locate the name of the sensor you want to configure.**

   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 server platform.

▼ Configure System Indicators

Before You Begin

- To configure the indicator state, you need the User Management (u) role enabled.

Follow these steps to configure system indicators:

1. **Log in to the ILOM web interface.**
2. **Select System Monitoring --> Indicators.**

   The Indicators page appears.

Note – If the server is powered off, many indicators will appear as "no reading."

---

3. **In the Indicators page, do the following:**

   a. **Locate the name of the indicator you want to configure.**

   b. **To change the state of an indicator, click the radio button associated with the indicator that you want to change. 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.**

▼ Configure Clock Settings

Before You Begin

- To view and set clock settings, you need the Admin (a) role enabled.
- You need the IP address of your NTP server to complete this procedure.

Follow these steps to configure clock settings:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> Clock Settings.**

   The Clock Settings page appears.
3. **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. See Step 4.
   - Synchronize the date and time of the host server SP with an NTP server. See Step 5.
4. **To manually set the date and time of the host server SP, follow these steps:**
   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.**
   c. **Go to Step 6.**
5. **To configure an IP address of an NTP server and enable synchronization, follow these steps:**
   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.**
6. **Click Save for your changes to take effect.**

   Consult your 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.

▼ Configure Timezone Settings

Before You Begin

- To view and set clock timezone settings, you need the Admin (a) role enabled.

Follow these steps to configure timezone settings:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> Timezone.**
   The Timezone Settings page appears.
3. **Select the timezone using the Timezone drop-down list.**

Consult your 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.

▼ Filter Event Log Output

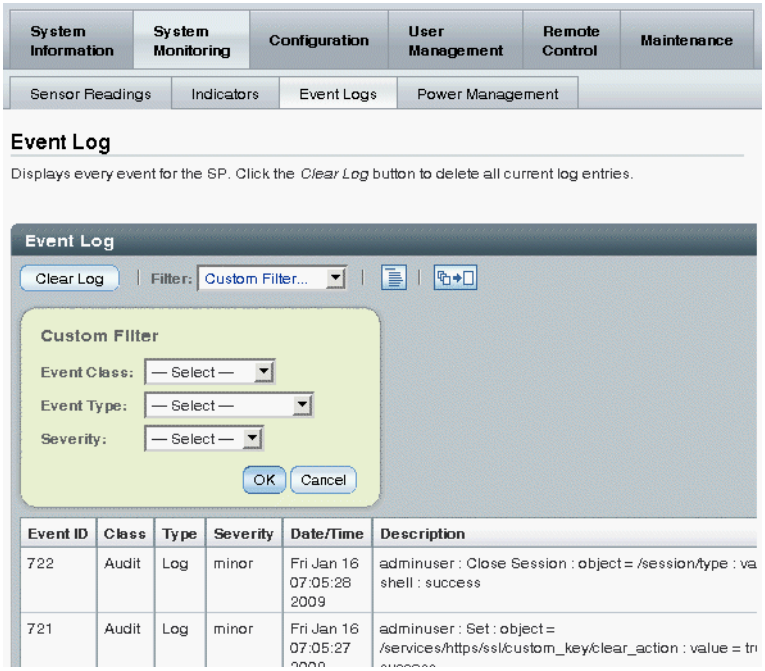
Before You Begin

- To filter event log output, you need the Read Only (o) role enabled.

Follow these steps to filter event log output:

1. **Log in to the ILOM web interface.**
2. **Select System Monitoring --> Event Logs.**
   The Event Log page appears.
3. **In the Event Log page, choose from among the following standard filters:**
   - All Events
   - Class: Fault
   - Type: Action
   - Severity: Down
   - Severity: Critical

4. **Alternatively, you can choose from among the custom output filters shown in the following figure.**



The table below lists the options available in each filter.

Event Class	Event Type	Severity
Developer	`Log`	`Debug`
Email	`Connection`	`Down`
Captive Shell	`Send`	`Critical`
Backup	`Command Entered`	`Major`
Restore	`State`	`Minor`
Reset	`Action`	
Chassis	`Fault`	
Audit	`Repair`	
IPMI	`Warning`	
Fault		
System		
ActDir		

▼ View and Clear the ILOM Event Log

Before You Begin

- To view or clear the event log, you need the Admin (a) role enabled.

Follow these steps to view and clear the ILOM event log:

1. **Log in to the ILOM web interface.**
2. **Select System Monitoring --> Event Logs.**

   The Event Log page appears.
3. **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 greater number of entries might cause the web interface to respond slower than selecting a fewer 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	• Audit/ Log – Commands that result in a configuration change. Description includes user, command, command parameters, and success/fail. • IPMI/Log – Any event that is placed in the IPMI SEL is also put in the management log. • Chassis/State – For changes to the inventory and general system state changes. • Chassis/Action – Category for shutdown events for server module/chassis, hot insert/removal of a FRU, and Reset Parameters button pushed. • Fault/Fault – For Fault Management faults. Description gives the time the fault was detected and suspect component. • Fault/Repair – For Fault repairs. Description gives component.
Severity	Debug, Down, 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.

▼ Configure Remote Syslog Receiver IP Addresses

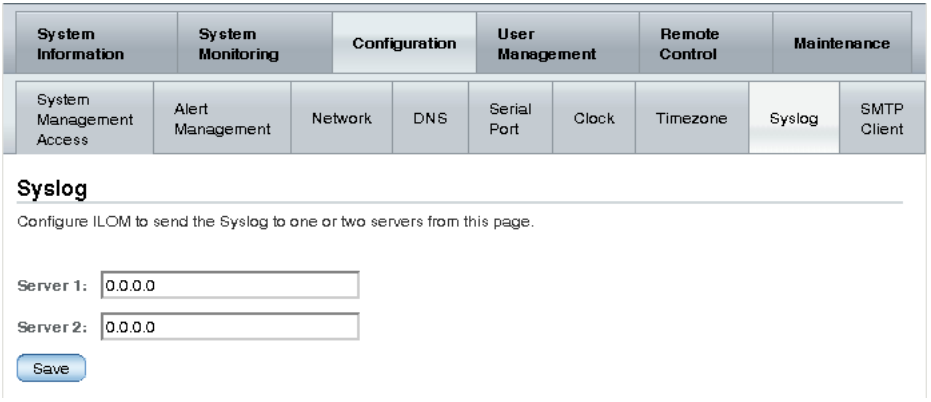
Before You Begin

- To configure remote syslog receiver IP addresses, you need the Admin (a) role enabled.

Follow these steps to configure remote syslog receiver IP addresses:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> Syslog.**

   The Syslog page appears.



3. **In the Server 1 and 2 fields, type the IP addresses for the two locations to which you want to send syslog data.**
4. **Click Save for your settings to take effect.**

▼ View Fault Status

Before You Begin

- To view fault status, you need the Read Only (o) role enabled.

Follow these steps to view fault status:

1. **Log in to the ILOM web interface.**
2. **Select the Fault Management tab.**

   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.
3. **Alternatively, in the ILOM web interface, you can identify the fault status of a component on the Component Management page.**

   a. **Select the Components tab.**

   b. **Click on a component name to view the fault state.**

      The status of the component will appear in a separate window as illustrated in the following figure.

View component name and information.

/SYS

Property	Value
type	Host System
ipmi_name	/SYS
fault_state	OK
power_state	Off

For more information about the ILOM fault management features offered on your system, consult the user documentation provided with the server platform.

▼ Collect SP Data to Diagnose System Problems

Before You Begin

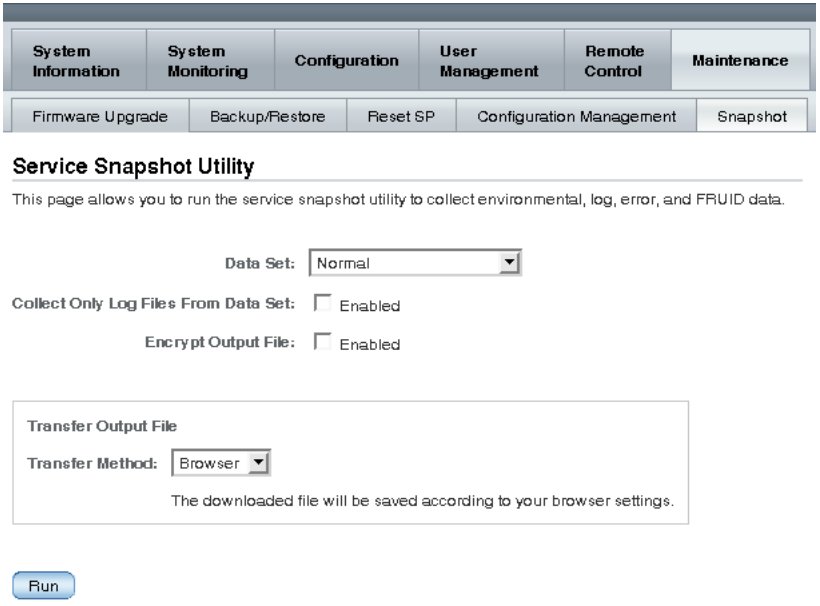
- To collect SP data using the Service Snapshot utility, you need the Admin (a) role enabled.

Caution – The purpose of the ILOM Service Snapshot utility is to collect data for use by service engineers to diagnose system problems. Customers should not run this utility unless requested to do so by service engineers.

Follow these steps to run the Service Snapshot utility:

1. **Log in to the ILOM web interface.**
2. **Select Maintenance --> Snapshot.**

   The Service Snapshot Utility page appears.



3. **Select the desired Data Set: Normal, Full, or Custom.**
   - **Normal** – Specifies that ILOM, operating system, and hardware information is collected.
   - **Full** – Specifies that all data is to be collected. Selecting Full might reset the system.
   - **Custom** – Allows you to choose one or more of the following data sets:
     - ILOM Data
     - Hardware Data
     - Basic OS Data
     - Diagnostic Data

4. **Click the Enabled check box if you want to collect only log files from the data set.**
5. **Click the Enabled check box if you want to encrypt the output file.**
6. **Select one of the following methods to transfer the output file:**
   - Browser
   - SFTP
   - FTP
7. **Click Run.**

   A Save As dialog box appears.
8. **In the dialog box, specify the directory to which to save the file and the file name.**
9. **Click OK.**

   The file is saved to the specified directory.

CHAPTER 8

Managing System Alerts

Topics

Description	Links
Review the prerequisites	• "Before You Begin" on page 82
Manage alert rule configurations	• "Create or Edit Alert Rules" on page 82 • "Disable an Alert Rule" on page 83
Generate test alert to confirm alert configuration is working	• "Generate Test Alerts" on page 84
Notify recipient of system alerts using email	• "Enable SMTP Client" on page 85

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• System Monitoring and Alert Management	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• CLI	• Managing System Alerts	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
• SNMP	• Managing Alerts	*Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/

Managing Alert Rule Configurations

Topics

Description	Links
Review the prerequisites	• "Before You Begin" on page 82
Manage alert rule configurations	• "Create or Edit Alert Rules" on page 82 • "Disable an Alert Rule" on page 83 • "Generate Test Alerts" on page 84

Before You Begin

- 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 user will be unable to decode the SNMP alert message.
- If you are using a modular chassis system, 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.

▼ Create or Edit Alert Rules

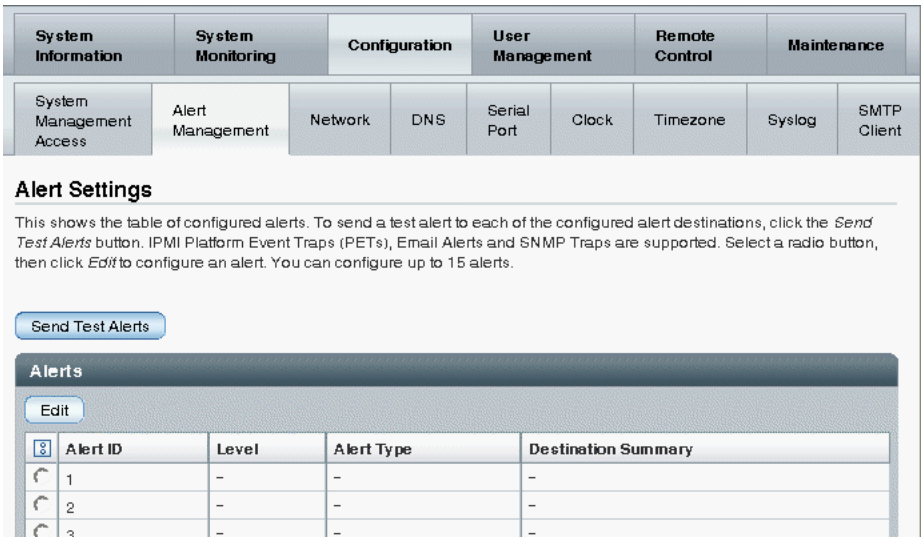
Before You Begin

- To create or edit alert rules, you need the Admin (a) role enabled.

Follow these steps to configure alert rules:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> Alert Management.**

   The Alert Settings page appears.



3. **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 property values 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 "Alert Management" in the *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

   d. **Click Save to apply the values specified and to close the properties dialog.**

▼ Disable an Alert Rule

Before You Begin

- To disable an alert rule, you need the Admin (a) role enabled.

Follow these steps to disable an alert rule:

1. **Log in to the ILOM web interface.**

2. **Select Configuration --> Alert Management.**

   The Alert Settings page appears.

3. **In the Alert Settings page, select the radio button for the alert rule you want to disable then select Edit in the Actions drop-down list box.**

   A dialog appears presenting properties you can define about the alert rule.

4. **In the properties dialog box, select Disabled in the Alert Levels drop-down list box.**

5. **Click Save to apply the value specified and to close the properties dialog.**

▼ Generate Test Alerts

Before You Begin

- To generate test alerts, you need the Admin (a) role enabled.
- You can test each *enabled* alert rule configuration in ILOM by sending a test alert.

Follow these steps to generate test alerts:

1. **Log in to the ILOM web interface.**

2. **Select Configuration --> Alert Management.**

   The Alert Settings page appears.

3. **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.

Configuring SMTP Client for Email Notification Alerts

Topics

Description	Links
Notify recipient of system alerts using email	• "Enable SMTP Client" on page 85

▼ Enable SMTP Client

Before You Begin

- To enable SMTP Clients, you need the Admin (a) role enabled.
- To generate configured Email Notification alerts, you must enable the ILOM client to act as an SMTP client to send the email alert messages.
- Prior to enabling the ILOM client as an SMTP client, determine the IP address and port number of the outgoing SMTP email server that will process the email notification.

Follow these steps to enable an SMTP client:

1. **Log in to the ILOM web interface.**
2. **Select Configuration --> SMTP Client.**

   The SMTP Client page appears.
3. **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.

4. **Click Save to apply the SMTP settings.**

CHAPTER 9

Monitoring Power Consumption

Topics

Description	Links
Monitor power consumption interfaces	• "Monitor System Power Consumption" on page 88 • "Monitor Individual Power Supply Consumption" on page 89

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Power Consumption Management Interfaces	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• CLI	• Managing Power Consumption	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*
• SNMP	• Managing Power Consumption	*Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/

Monitoring the Power Consumption Interfaces

Topics

Description	Links
Monitor power supply consumption	• "Monitor System Power Consumption" on page 88 • "Monitor Individual Power Supply Consumption" on page 89

This chapter describes how to use available power consumption interfaces to monitor power consumption. Terms that pertain to power consumption monitoring are defined in the section "Power Monitoring Terminology" in the *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*

Note – The power consumption interfaces described in this chapter might or might not be implemented on the platform that you are using. See the platform-specific ILOM Supplement or Product Notes for implementation details. You can find the ILOM Supplement and Product Notes within the documentation set for your system.

▼ Monitor System Power Consumption

Before You Begin

- To view system power consumption, you need the Read Only (o) role enabled.

Follow these steps to view system power consumption:

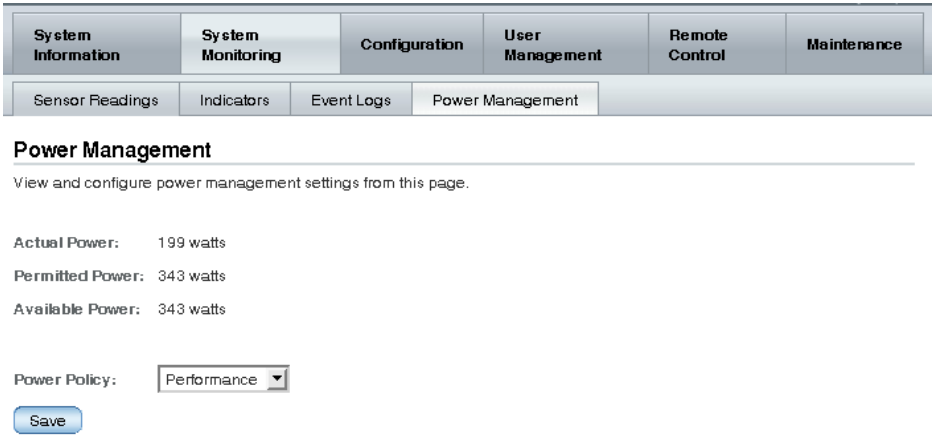
1. **Log in to the ILOM web interface.**
2. **Select System Monitoring --> Power Management.**

   The Power Management page appears.

Note – The ability to monitor power varies depending on server platform implementation of this feature. Refer to the platform-specific ILOM Supplement for details and procedures.

3. **In the Power Management page, you can view actual power, permitted power, and available power.**

   Refer to "Power Monitoring Terminology" in the *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* for a description of these power monitoring terms.



▼ Monitor Individual Power Supply Consumption

Before You Begin

To monitor individual power supply consumption, you need the Read Only (o) role enabled.

Follow this step to view individual power supply consumption:

- **For instructions on viewing sensors, refer to** "View Sensor Readings" on page 71**.**

CHAPTER 10

Backing Up and Restoring ILOM Configuration

Topics

Description	Links
Back up the ILOM configuration	• "Back Up the ILOM Configuration" on page 92
Restore the ILOM configuration	• "Restore the ILOM Configuration" on page 95
Reset ILOM configuration to default settings	• "Reset the ILOM Configuration to Defaults" on page 101

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Configuration Management and Firmware Updates	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• CLI	• Backing Up and Restoring ILOM Configuration	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
`http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/`

Backing Up the ILOM Configuration

Topics

Description	Links
Back up the ILOM configuration	• "Back Up the ILOM Configuration" on page 92

▼ Back Up the ILOM Configuration

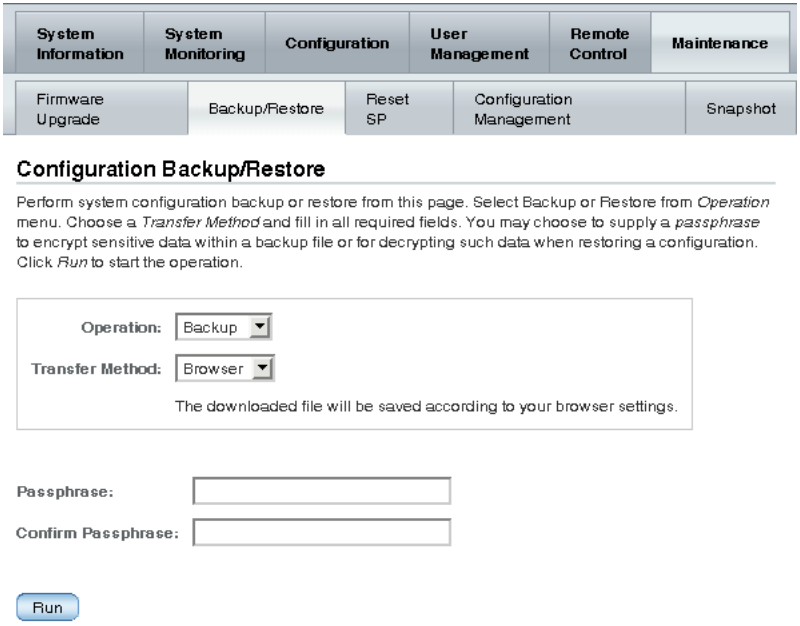
Before You Begin

- To back up the ILOM configuration you need the Admin (a), User Management (u), Console (c), Reset and Host Control (r), and Read Only (o) roles enabled.
- If you use a user account that does *not* have the roles listed above, the configuration backup file created might not include all of the ILOM SP configuration data.

Follow these steps to back up the ILOM configuration:

1. **Log in to the ILOM web interface.**
2. **Select Maintenance --> Backup/Restore.**

   The Configuration Backup/Restore page appears.



3. **Select Backup from the Operation drop-down list.**
4. **Select a transfer method from the Transfer Method drop-down list.**

   The following transfer methods are available:

   - Browser
   - TFTP
   - FTP
   - SFTP
   - SCP
   - HTTP
   - HTTPS

5. **If you select the Browser transfer method, the backup file is saved according to your browser settings.**
6. **If you select the TFTP transfer method, the prompts shown in the following figure appear and you must provide the following information:**

   - **Host** – Enter the remote host IP address or, if you have DNS configured, the name of the remote host.
   - **Filepath** – Enter the path to which to save the configuration file in the format: `directoryPath/filename`.

7. **If you select the SCP, FTP, SFTP, HTTP, or HTTPS transfer method, the prompts shown in the following figure appear and you must provide the following information:**
   - **Host** – Enter the remote host IP address or, if you have DNS configured, the name of the remote host.
   - **Filepath** – Enter the path to which to save the configuration file in the format: `directoryPath/filename`.
   - **Username** – Enter the user name of your account on the remote system.
   - **Password** – Enter the password for your account on the remote system.

8. **If you want sensitive data, such as passwords, SSH keys, certificates, and so forth, to be backed up, you must provide a passphrase. Type a passphrase in the Passphrase field and confirm the passphrase in the Confirm Passphrase field.**

   If you do not type a passphrase, sensitive data will not be backed up.

9. **To initiate the backup operation, click Run.**

   The Backup operation is executed.

Note – While the Backup operation is executing, sessions on the ILOM SP will be momentarily suspended. The sessions will resume normal operation once the Backup operation is complete. A Backup operation typically takes two to three minutes to complete.

Restoring the ILOM Configuration

Topics

Description	Links
Restore the ILOM configuration	• "Restore the ILOM Configuration" on page 95 • "Edit the Backup XML File" on page 98

▼ Restore the ILOM Configuration

Before You Begin

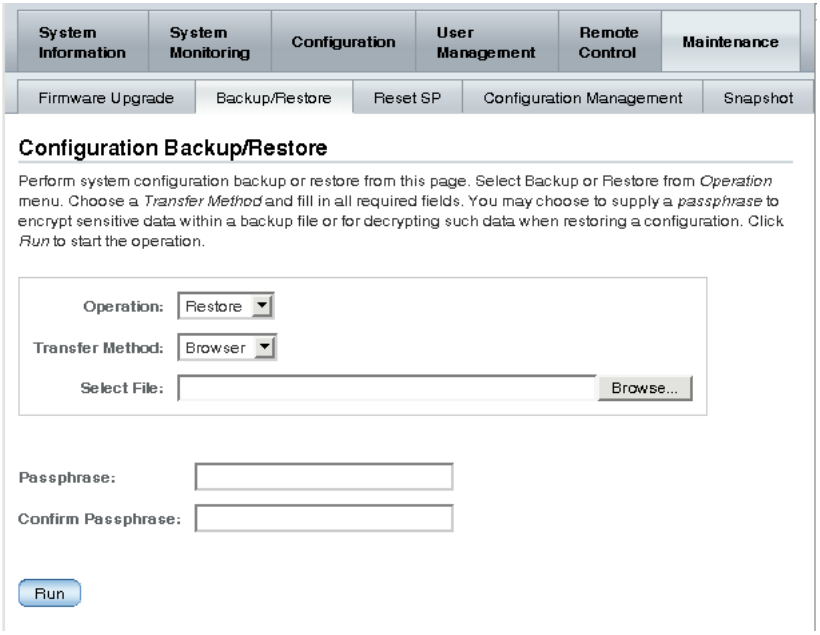
- To restore the ILOM configuration you need the Admin (a), User Management (u), Console (c), Reset and Host Control (r), and Read Only (o) roles enabled.
- If you use a user account that does not have the roles listed above, some of the information in the configuration file might not be restored. When executing a Restore operation, use a user account that has the same or more privileges than the user account that was used to create the backup file; otherwise, some of the backed up configuration data might not be restored. All configuration properties that are not restored appear in the event log. Therefore, you can verify whether all the configuration properties were restored by checking the event log.

Follow these steps to restore the ILOM configuration:

1. **Log in to the ILOM web interface.**
2. **Select Maintenance --> Backup/Restore.**

   The Configuration Backup/Restore page appears.
3. **Select Restore from the Operation drop-down list.**

   The Configuration Backup/Restore page used for Restore operations appears.



4. **Select the transfer method from the Transfer Method drop-down list.**

   The following transfer methods are available:

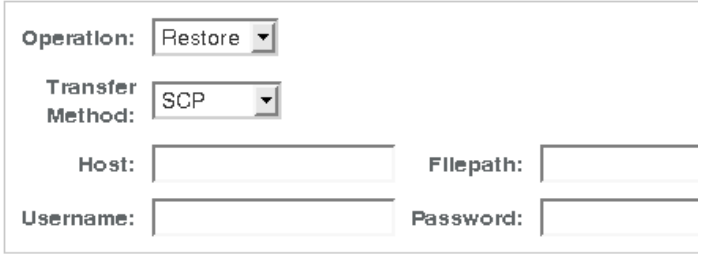
   - Browser
   - TFTP
   - FTP
   - SFTP
   - SCP
   - HTTP
   - HTTPS

5. **If you select the Browser transfer method, type the directory path and file name for the backup file or click the Browse button to determine the backup file location.**

6. **If you select the TFTP transfer method, the prompts shown in the following figure appear and you must provide the following information:**

   - **Host** – Enter the remote host IP address or, if you have DNS configured, the name of the remote host.
   - **Filepath** – Enter the path to which to save the configuration file in the format: `directoryPath/filename`.

7. **If you select the SCP, FTP, SFTP, HTTP, or HTTPS transfer method, the prompts shown in the following figure appear and you must provide the following information:**
   - **Host** – Enter the remote host IP address or, if you have DNS configured, the name of the remote host.
   - **Filepath** – Enter the path to for the configuration file in the format: `directoryPath/filename`.
   - **Username** – Enter the user name of your account on the remote system.
   - **Password** – Enter the password for your account on the remote system.



8. **If a passphrase was provided when the backup file was created, type the passphrase in the Passphrase field and confirm it in the Confirm Passphrase field.**

   The passphrase must be the same passphrase that was used when the backup file was created.

9. **To initiate the Restore operation, click Run.**

   The Restore operation executes.

Note – While the Restore operation is executing, sessions on the ILOM SP will be momentarily suspended. The sessions will resume normal operation once the Restore operation is complete. A Restore operation typically takes two to three minutes to complete.

▼ Edit the Backup XML File

Before You Begin

- Before you use a backed up XML file on another system, you should edit the file to remove any information that is unique to a particular system, for example, the IP address.

The following is an example of a backed up XML file. The content of the file is abbreviated for this procedure.

```
<SP_config version="3.0">
<entry>
<property>/SP/check_physical_presence</property>
<value>false</value>
</entry>
<entry>
<property>/SP/hostname</property>
<value>labysystem12</value>
</entry>
<entry>
<property>/SP/system_identifier</property>
<value>SUN BLADE X8400 SERVER MODULE, ILOM v3.0.0.0, r32722
</value>
</entry>
.
.
.
<entry>
<property>/SP/clock/datetime</property>
<value>Mon May 12 15:31:09 2008</value>
</entry>
.
.
.
<entry>
<property>/SP/config/passphrase</property>
<value encrypted="true">89541176be7c</value>
</entry>
.
.
.
<entry>
<property>/SP/network/pendingipaddress</property>
<value>1.2.3.4</value>
</entry>
.
.
.
```

```
<entry>
<property>/SP/network/commitpending</property>
<value>true</value>
</entry>
.
.
.
<entry>
<property>/SP/services/snmp/sets</property>
<value>enabled</value>
</entry>
.
.
.
<entry>
<property>/SP/users/john/role</property>
<value>aucro</value>
</entry>
<entry>
<entry>
<property>/SP/users/john/password</property>
<value encrypted="true">c21f5a3df51db69fdf</value>
</entry>
</SP_config>
```

1. **Consider the following in the example XML file:**
   - The configuration settings, with exception of the password and the passphrase, are in clear text.
   - The `check_physical_presence` property, which is the first configuration entry in the file, is set to `false`. The default setting is `true` so this setting represents a change to the default ILOM configuration.
   - The configuration settings for `pendingipaddress` and `commitpending` are examples of settings that should be deleted before you use the backup XML file for a Restore operation because these settings are unique to each server.
   - The user account `john` is configured with the `a,u,c,r,o` roles. The default ILOM configuration does *not* have any configured user accounts so this account represents a change to the default ILOM configuration.
   - The SNMP `sets` property is set to enabled. The default setting is disabled.
2. **To modify the configuration settings that are in clear text, change the values or add new configuration settings.**

   For example:

- To change the roles assigned to the user `john`, change the text as follows:

```
<entry>
<property>/SP/users/john/role</property>
<value>auo</value>
</entry>
<entry>
```

- To add a new user account and assign that account the `a`,`u`,`c`,`r`,`o` roles, add the following text directly below the entry for user `john`:

```
<entry>
<property>/SP/users/bill/role</property>
<value>aucro</value>
</entry>
<entry>
```

- To change a password, delete the `encrypted="true"` setting and the encrypted password string and enter the password in plain text. For example, to change the password for the user `john`, change the text as follows:

```
<entry>
<property>/SP/users/john/password</property>
<value>newpassword</value>
</entry>
```

3. **After you have made the changes to the backup XML file, save the file so that you can use it for a Restore operation on the same system or a different system.**

Resetting the ILOM Configuration

Topics

Description	Links
Reset the ILOM configuration to default settings	• "Reset the ILOM Configuration to Defaults" on page 101

▼ Reset the ILOM Configuration to Defaults

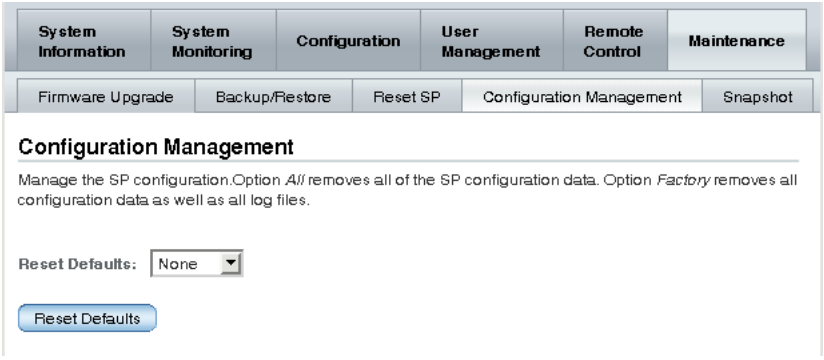
Before You Begin

- To reset the ILOM configuration to defaults, you need the Admin (a) role enabled.

Follow these steps to reset the ILOM configuration to defaults:

1. **Log in to the ILOM web interface.**
2. **Select Maintenance --> Configuration Management.**

   The Configuration Management page appears.



3. **Select one of the following options in the Reset Defaults drop-down list, then click Reset Defaults.**

   - **All** – If you want to reset all of the ILOM configuration data to the default settings with the exception of the log files, select All in the Reset Defaults drop-down list and click Reset Defaults. The next time the ILOM SP reboots, the configuration will be restored to the default settings.

- **Factory** – If you want to reset all of the ILOM configuration data to default settings and also erase the log files, select Factory in the Reset Defaults drop-down list and click Reset Defaults. The next time the ILOM SP reboots, the configuration will be restored to the default settings and the log files are erased.
- **None** – If you want to cancel the reset to defaults operation just previously issued, select None in the Reset Defaults drop-down list and click Reset Defaults. The previously issued reset to defaults operation is canceled provided the None option is executed before the ILOM SP reboots.

CHAPTER 11

Updating ILOM Firmware

Topics

Description	Links
Review the prerequisites	• "Before You Begin" on page 104
Update ILOM firmware	• "Identify ILOM Firmware Version" on page 105 • "Download New Firmware on SPARC-Based Systems" on page 105 • "Update the Firmware Image" on page 105 • "Recover From a Network Failure During Firmware Update" on page 107
Reset the ILOM SP	• "Reset ILOM SP" on page 108

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Configuration Management and Firmware Updates	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• CLI	• Updating ILOM Firmware	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
`http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/`

Updating the Firmware

Topics

Description	Links
Review the prerequisites	• "Before You Begin" on page 104
Update ILOM firmware	• "Identify ILOM Firmware Version" on page 105 • "Download New Firmware on SPARC-Based Systems" on page 105 • "Update the Firmware Image" on page 105 • "Recover From a Network Failure During Firmware Update" on page 107

Before You Begin

Prior to performing the procedures in this section, the following requirements must be met:

- Identify the version of ILOM that is currently running on your system.
- Download the firmware image for your server or CMM from the platform's product web site.
- Copy the firmware image to a server using a supported protocol (TFTP, FTP, HTTP, HTTPS). For a CLI update, copy the image to a local server. For a web interface update, copy the image to the system on which the web browser is running.
- If required by your platform, shut down your host operating system before changing the firmware on your server SP.
- Obtain an ILOM user name and password that has Admin (a) role account privileges. You must have Admin (a) privileges to update the firmware on the system.
- The firmware update process takes about six minutes to complete. During this time, do not perform other ILOM tasks. When the firmware update is complete, the system will reboot.

▼ Identify ILOM Firmware Version

Before You Begin

- To identify the firmware version, you need the Read Only (o) role enabled.

Follow these steps to identify the firmware version:

1. **Log in to the ILOM web interface.**
2. **Select User Management -->Version.**

   The current firmware version information appears.

▼ Download New Firmware on SPARC-Based Systems

1. **Navigate to** `http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/firmware/`
2. **Select the latest firmware update for your server.**
3. **Confirm the terms and conditions for use of the firmware, and click Accept.**
4. **Click Download to download the zip file package.**
5. **Put the zip package on a TFTP server that is accessible from your network.**
6. **Unzip the package.**
7. **Go to** "Update the Firmware Image" on page 105**.**

▼ Update the Firmware Image

Before You Begin

- To update the ILOM firmware, you need the Admin (a) role enabled.
- If required by your platform, shut down your host operating system before updating the firmware on your server SP.
- To gracefully shut down your host operating system, use the `Remote Power Controls -> Graceful Shutdown and Power Off` option in the ILOM web interface, or issue the `stop /SYS` command from the ILOM CLI.

Follow these steps to update the firmware image:

1. **Log in to the ILOM web interface.**
2. **Select Maintenance --> Firmware Upgrade.**

   The Firmware Upgrade page appears.
3. **In the Firmware Upgrade page, click Enter Upgrade Mode.**

   An Upgrade Verification dialog appears, indicating that other users who are logged in will lose their session when the update process completes.
4. **In the Upgrade verification dialog, click OK to continue.**

   The Firmware Upgrade page appears.
5. **In the Firmware Upgrade page, perform the following actions:**

   a. **Specify the image location by performing one of the following:**
      - Click Browse to select the location of the firmware image you want to install.
      - If supported on your system, click Specify URL. Then type the URL that will locate the firmware image into the text box.

   b. **Click the Upload button to upload and validate the file.**

      Wait for the file to upload and validate.

      The Firmware Verification page appears.
6. **In the Firmware Verification page, enable any of the following options:**
   - **Preserve Configuration.** Enable this option if you want to save your existing configuration in ILOM and restore that existing configuration after the update process completes.
   - **Delay BIOS upgrade until next server poweroff.** Enable this option if you want to postpone the BIOS upgrade until the next time the system reboots.

Note – The "Delay BIOS upgrade" option appears only for firmware updates to ILOM 3.0 or later on x64 systems.

---

7. **Click Start Upgrade to start the upgrade process or click Exit to cancel the process.**

   When you click Start Upgrade the upload process will start and a prompt to continue the process appears.
8. **At the prompt, click OK to continue.**

   The Update Status page appears providing details about the update progress. When the update indicates 100%, the firmware upload is complete.

   When the upload completes, the system *automatically* reboots.

Note – The ILOM web interface might not refresh properly after the update completes. If the ILOM web is missing information or displays an error message, you might 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.

9. **Reconnect to the SP (or CMM) ILOM web interface. Select System Information --> Version to verify that the firmware version on the SP or CMM corresponds to the firmware image you installed.**

Note – If you did not preserve the ILOM configuration before the firmware update, you will need to perform the initial ILOM setup procedures to reconnect to ILOM.

▼ Recover From a Network Failure During Firmware Update

If you were performing the firmware update process via the ILOM web interface using a *local file* and a network failure occurs, ILOM will automatically time-out and reboot the system.

Follow these steps to recover from a network failure during firmware update:

1. **Address and fix the network problem.**
2. **Reconnect to the ILOM SP.**
3. **Restart the firmware update process.**

Resetting ILOM SP

Topics

Description	Links
Reset the ILOM SP	• "Reset ILOM SP" on page 108 • "Recover From a Network Failure During Firmware Update" on page 107

▼ Reset ILOM SP

If you need to reset your ILOM service processor (SP), you can do so without affecting the host OS. However, resetting an SP disconnects your current ILOM session and renders the SP unmanageable during reset.

Before You Begin

- To reset the SP, you need the Reset and Host Control (`r`) role enabled.
- After updating the ILOM/BIOS firmware, you must reset the ILOM SP.

Follow these steps to reset the ILOM SP after updating the ILOM/BIOS firmware:

1. **Log in to the ILOM SP web interface.**
2. **Select Maintenance --> Reset SP.**

   The Reset Service Processor page appears
3. **Click the Reset SP button.**

   ILOM reboots. The web interface is unavailable while ILOM reboots.

CHAPTER 12

Managing Remote Hosts

Topics

Description	Links
Review the prerequisites	• "Preparing to Manage Remote Hosts" on page 110
Perform initial setup for ILOM remote console	• "Configure ILOM Remote Control Video Redirection Settings" on page 112
Redirect host devices using ILOM remote console	• "Launch the ILOM Remote Console" on page 114 • "Start, Stop, or Restart Device Redirection" on page 116 • "Redirect Keyboard Input" on page 116 • "Control Keyboard Modes and Key Send Options" on page 117 • "Redirect Mouse Input" on page 118 • "Redirect Storage Media" on page 118 • "Add a New Server Session" on page 120 • "Exit the ILOM Remote Console" on page 120
Control the power state of a remote server module	• "Control Power State of Remote Host Server" on page 121
Diagnose SPARC system hardware issues	• "Configure Diagnostics Settings for SPARC Systems" on page 122

Related Topics

For ILOM	Chapter or Section	In this guide
• Concepts	• Remote Host Management Options	*Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*
• CLI	• Managing Remote Hosts	*Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*

The ILOM 3.0 Documentation Collection is available at:
http://www.fujitsu.com/global/services/computing/server/sparcenterprise/downloads/manual/

Preparing to Manage Remote Hosts

ILOM provides different options for remotely managing hosts, including:

- Power control
- Diagnostics configuration
- Storage redirection command-line interface (CLI)
- ILOM Remote Console

Review the prerequisites described below.

Before You Begin

Prior to performing the procedures in this chapter, ensure that the following requirements are met.

- You must use an Admin (a) or Console (c) role account to use the ILOM Remote Console.
- The ILOM Remote Console supports two methods of redirection: video and serial console. Video redirection is supported on some SPARC processor-based servers. Serial console redirection is supported on all SPARC servers.
- To run the ILOM Remote Console, you must have the JRE 1.5 or higher (Java 5.0 or higher) software installed on your local client. To download the Java 1.5 runtime environment, go to: http://java.com.
- The ILOM Remote Console is supported on your local client with the operating systems and browser listed in the following table:

Operating System	Web Browser
Solaris (9 and 10)	• Mozilla 1.7.5 and above • Firefox 1.0 and above
Linux (Red Hat, SuSE, Ubuntu)	• Mozilla 1.7.5 and above • Firefox 1.0 and above • Opera 6.x and above
Microsoft Windows (98, 2000, XP, Vista)	• Internet Explorer 6.0 and above • Mozilla 1.7.5 and above • Firefox 1.0 and above • Opera 6.x and above

Performing the Initial Setup Tasks to Enable ILOM Remote Console Video Redirection

Topics

Description	Links
Perform initial setup for ILOM Remote Console	• "Configure ILOM Remote Control Video Redirection Settings" on page 112

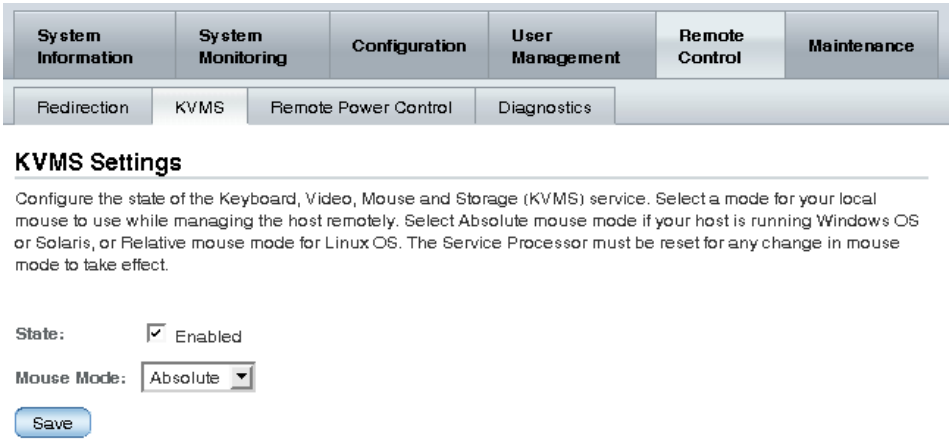
Note – The initial setup procedures described in this section only apply to video redirection. If you are using only a serial console redirection, the initial setup tasks described in this section are not necessary. You can skip this initial setup section and proceed to "Launching Redirection Using the ILOM Remote Console" on page 113.

▼ Configure ILOM Remote Control Video Redirection Settings

Follow these steps to configure ILOM settings for remote management of host servers:

1. **Log in to the ILOM web interface for the server SP.**
2. **Click Remote Control --> KVMS.**

   The KVMS Settings page appears.



Note – The Remote Control second level tab options that are shown in the figure above differ depending on your server. Likewise, the KVMS settings options on the KVMS Settings page differ depending on your server. For more information, see the descriptions provided for the remote control settings in Step 3 of this procedure.

---

3. **Use the options on the KVMS Settings page to specify the following remote control settings for managing a remote server.**

Remote Control Setting	Applies To	Action
KVMS State	Video redirection	Check Enabled to enable the redirection of keyboard, video, mouse, and storage devices of the managed host. If left unchecked, the KVMS device redirection will be disabled.
Mouse Mode Settings	Video redirection	Select one of the following mouse mode settings: • **Absolute.** Select Absolute Mouse Mode for best performance when you are using Solaris or Windows operating systems. Absolute is the default. • **Relative.** Select Relative Mouse Mode when you are using a Linux operating system. Note that not all Linux operating systems support Absolute mode.

Launching Redirection Using the ILOM Remote Console

Topics

Description	Links
Review the prerequisites	• "Before You Begin" on page 114
Launch redirection using ILOM Remote Console	• "Launch the ILOM Remote Console" on page 114 • "Add a New Server Session" on page 120 • "Start, Stop, or Restart Device Redirection" on page 116 • "Redirect Keyboard Input" on page 116 • "Control Keyboard Modes and Key Send Options" on page 117 • "Redirect Mouse Input" on page 118 • "Redirect Storage Media" on page 118 • "Exit the ILOM Remote Console" on page 120

Before You Begin

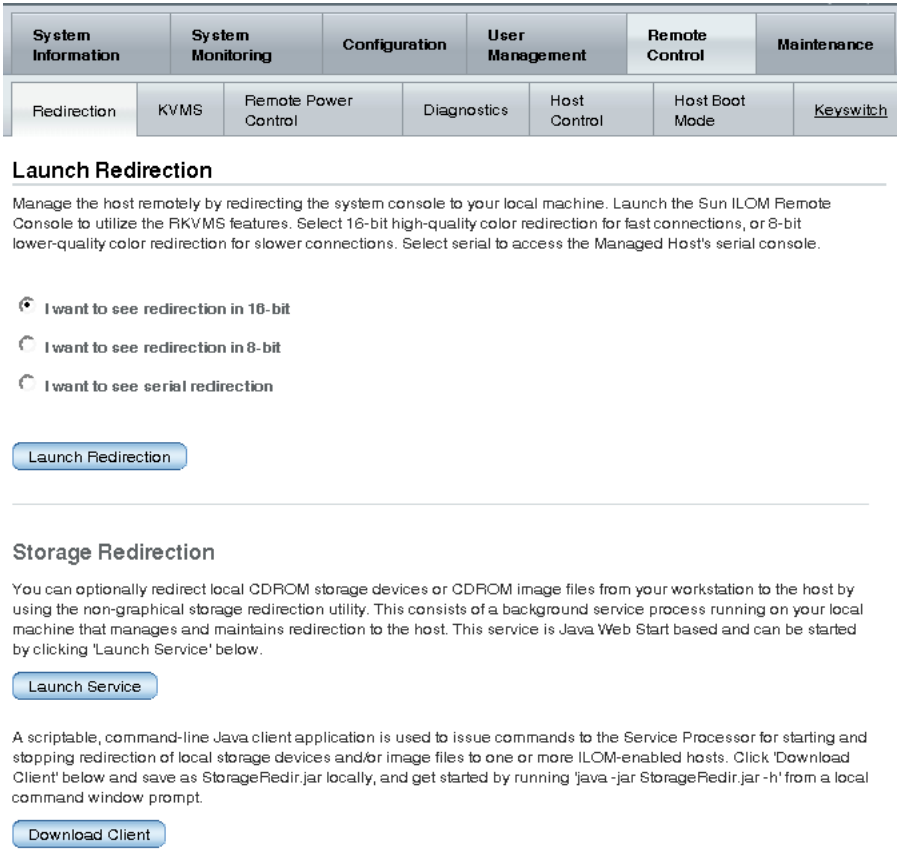
The following requirements must be met prior to performing the remote management procedures in this section.

- You must have the Java Runtime Environment (1.5 or later) installed on your local system. To download the latest Java runtime environment, go to: `http://java.com.`
- You must log in to the ILOM SP web interface using an Admin (`a`) or Console (`c`) role account. Either an Admin or Console role account is required to launch the ILOM Remote Console.
- You must have configured the Remote Control Settings in the ILOM web interface. For instructions, see "Configure ILOM Remote Control Video Redirection Settings" on page 112.

▼ Launch the ILOM Remote Console

1. **Log in to the ILOM web interface for the server SP.**
2. **Click Remote Control --> Redirection.**

   The Launch Redirection page appears.



Note – Depending on your platform, the Launch Redirection page will offer different combinations of redirection options. If multiple options are presented, select the type of redirection that you want to use to remotely manage this host.

---

3. **To specify how you want to see the redirected system console, click one of the radio buttons.**
4. **Click Launch Redirection.**
5. **If a certificate warning message appears stating that the name of the site does not match the name on the certificate, click Run to continue.**

   The ILOM Remote Console window appears.

▼ Start, Stop, or Restart Device Redirection

1. **In the ILOM Remote Console menu bar, click Redirection.**
2. **In the Redirection menu, specify, one of the following redirection options.**

Option	Description
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 Input

Before You Begin

- This procedure only applies to serial console redirection.
- Although multiple users can connect to the system console, only one user at a time has write access to the console (that is, only one user can type commands into the system console). Any characters that other users type are ignored. This is referred to as a write lock, and the other user sessions are in read-only mode. If no other users are currently logged in to the system console, then you obtain the write lock automatically when you start keyboard redirection. If another user currently has write access to the console, you will be prompted to forcibly transfer write access away from their session.
- A server redirection session must be active for the remote host server SP. For details, see "Add a New Server Session" on page 120.
- Device redirection must be started. For details, "Start, Stop, or Restart Device Redirection" on page 116.

Follow these steps to redirect a remote host server keyboard to your local client:

1. **Select Remote Control --> KVMS.**

   The KVMS Settings page appears.

2. **Select the KVMS Settings check box to enable the remote management state of the keyboard.**

   The KVMS State is enabled by default.

▼ Control Keyboard Modes and Key Send Options

Before You Begin

- A server redirection session must be active for the remote host server SP. For details, see "Add a New Server Session" on page 120.
- Device redirection must be started. For details, "Start, Stop, or Restart Device Redirection" on page 116
- Keyboard redirection must be enabled. For details, see "Redirect Keyboard Input" on page 116.

Follow these steps to control keyboard modes and individual key send options:

1. **In the ILOM Remote Console window, click the Keyboard menu.**
2. **In the Keyboard menu, specify any of the following keyboard settings.**

Option	Description
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. Stateful Key Locking applies to these three lock keys: Caps Lock, Num Lock, and Scroll Lock.
Left Alt Key* *Not available on Windows Client	Select the Left Alt Key to toggle the left Alt Key on or off.
Right Alt Key* *Not available on Windows Client	Select Right Alt Key to toggle the right Alt Key on or off for non-US keyboards. When enabled, this option enables 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.

Note – Not all of these keyboard settings apply during serial redirection.

▼ Redirect Mouse Input

Before You Begin

- Mouse redirection is only supported for video redirection settings.
- Configure your mouse settings to Absolute or Relative Mouse Mode. See "Configure ILOM Remote Control Video Redirection Settings" on page 112.
- A server redirection session must be active for the remote host server SP. For details, see "Add a New Server Session" on page 120.
- Device redirection must be started. For details, "Start, Stop, or Restart Device Redirection" on page 116.

Follow these steps to redirect a remote host server mouse to your local client:

1. **Select Remote Control --> KVMS.**

   The KVMS Settings page is displayed.

2. **Select the KVMS State check box to enable the remote host management state of the mouse.**

   The KVMS State is set to Enabled by default.

▼ Redirect Storage Media

Before You Begin

- A server redirection session must be active for the remote host server SP. For details, see "Add a New Server Session" on page 120.
- Device redirection must be started. For details, "Start, Stop, or Restart Device Redirection" on page 116

- For Solaris client systems, you must perform the following actions 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 ILOM Remote Console by entering these commands:

    ```
    su to root
    ppriv -s +file_dac_read pid_javarconsole
    ```

Follow these steps to redirect storage media (CD/DVD or ISO image) from your desktop to a host server:

1. **In the ILOM Remote Console menu bar, select Devices.**
2. **In the Devices menu, perform the following actions:**

   a. **Enable the appropriate storage device or image setting.**

Option	Description
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.

Note – Floppy storage media redirection is not supported on SPARC systems.

Note – If you are installing software from distribution media (CD/DVD), ensure that the media is inserted in the redirected drive. If you are installing software from an ISO image, ensure that the ISO image is stored on your local client or network shared file system.

   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, perform one of the following actions:**
      - In the Drive Selection dialog, select or type a drive location, then click OK.

- In the File Open dialog, browse 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.**

▼ Add a New Server Session

1. **In the 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 server SP, then click OK.**

   The Login dialog appears.

3. **In the Login dialog, type a user name and password.**

   A session tab for the newly added remote host server appears in the tab set of the ILOM Remote Console.

Note – The Login dialog will also ask you whether the new session is to be video redirection (which is supported on some SPARC systems) or serial redirection (which is currently supported on all SPARC systems). Consult your platform documentation for more information about which type of redirection is supported.

▼ Exit the ILOM Remote Console

Follow this step to exit the ILOM Remote Console and close all remote server sessions:

- **In the ILOM Remote Console menu bar, select Redirection --> Quit.**

Controlling Remote Host Power States

Topics

Description	Links
Control the power state of the remote host server	• "Control Power State of Remote Host Server" on page 121

▼ Control Power State of Remote Host Server

Before You Begin

- To control the power state of the remote host server, you need the Admin (a) role enabled.

Follow these steps to control the power state of the remote host server.

1. **Log in to the ILOM web interface for the server SP.**
2. **Click the Remote Power Control tab.**

   The Server Power Control page appears.
3. **From the Server Power Control page, you can remotely control the power state of a host server by selecting one of the following options from the Action menu:**
   - **Reset** – This option immediately reboots the remote host server.
   - **Immediate Power Off** – This option immediately turns off the power on the remote host server.
   - **Graceful Shutdown and Power Off** – This option shuts down the OS gracefully prior to powering off the remote host server.
   - **Power On** (default) – This option turns on full power to the remote host server.
   - **Power Cycle** – This option immediately turns off the power on the remote host server, then applies full power to the remote host server.

Diagnosing SPARC Systems Hardware Issues

Topics

Description	Links
Diagnose SPARC system hardware issues	• "Configure Diagnostics Settings for SPARC Systems" on page 122

▼ Configure Diagnostics Settings for SPARC Systems

Before You Begin

- To configure and run diagnostic tests on a SPARC processor-based system, you need the Reset and Host control (`r`) role enabled.

Follow these steps to configure diagnostic settings for SPARC systems:

1. **Log in to the ILOM web interface.**
2. **Select Remote Control --> Diagnostics.**

   The Diagnostics page appears.
3. **Select a value for Trigger:**
   - **Power On** – Diagnostics will be run when power is applied.
   - **User Reset** – Diagnostics will be run upon a user-invoked reset.
   - **Error Reset** – Diagnostics will be run upon any error-invoked reset.
4. **Select a value for Verbosity for each trigger type:**
   - **None** – Diagnostics do not print any output on the system console when running, unless a fault is detected.
   - **Min** – Diagnostics print a limited amount of output on the system console (the default value).
   - **Normal** – Diagnostics print a moderate amount of output on the system console, including the name and results of each test being run.
   - **Debug** – Diagnostics print extensive debugging output on the system console, including devices being tested and debug output of each test.

5. **Select a value for Level for each trigger type:**
   - **Min** – Run the minimum level of diagnostics to verify the system.
   - **Max** – Run the maximum set of diagnostics to fully verify system health (the default value).
6. **Select a value for Mode:**
   - **Off** – Do not run any diagnostics.
   - **Normal** – Run diagnostics (the default value).
7. **Click Save for your settings to take effect.**

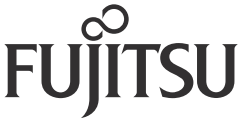
Index

U

V

W

X


FUJITSU