FUJITSU

# Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide

C120-E579-01EN

FUJITSU

# Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide

Manual Code C120-E579-01EN
Part No. 875-4536-10
April 2009, Revision A

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

# Contents

**Preface xi**

**1. SNMP Overview 1**

About Simple Network Management Protocol 2

Preparing Your System to Use SNMP 3

SNMP Components 3

ILOM SNMP MIBs 4

**2. Configuring ILOM Communication Settings 9**

Before You Begin 10

Configuring Network Settings 11

- Assign Host Name and System Identifier 11
- View and Configure Network Settings 13
- View and Configure Serial Port Settings 17
- View and Configure HTTP and HTTPS Settings 20
- Configure IP Addresses 21

Configuring Secure Shell Settings 25

- View the Current Key and Key Length 25
- Enable and Disable SSH 26
- Generate a New SSH Key 27

- Restart the SSH Server 28

**3. Managing User Accounts 31**

Before You Begin 33

Configuring User Accounts 34

- Configure User Accounts 34
- Configure Single Sign On 36

Configuring Active Directory Settings 37

- View and Configure Active Directory Settings 38
- View and Configure Active Directory Administrator Groups Settings 43
- View and Configure Active Directory Operator Groups Settings 44
- View and Configure Active Directory Custom Groups Settings 46
- View and Configure Active Directory User Domain Settings 49
- View and Configure Active Directory Alternate Server Settings 50
- View and Configure Redundancy Settings 54
- View and Configure Active Directory DNS Locator Settings 55

Configuring DNS Name Server 57

- View and Configure DNS Name Server Settings 57

Configuring ILOM for LDAP 58

- Configure LDAP Settings 58

Configuring ILOM for LDAP/SSL 62

- Configure LDAP/SSL Settings 62
- View and Configure LDAP/SSL Certificate Settings 66
- View and Configure LDAP/SSL Administrator Groups Settings 67
- View and Configure LDAP/SSL Operator Groups Settings 68
- View and Configure LDAP/SSL Custom Groups Settings 70
- View and Configure LDAP/SSL User Domain Settings 73
- View and Configure LDAP/SSL Alternate Server Settings 74

Configuring RADIUS Settings 77

▼ Configure RADIUS Settings 77

**4. Inventory and Component Management 81**

Before You Begin 82

Viewing Component Information 82

▼ View Component Information 83

Monitoring System Sensors, Indicators, and ILOM Event Log 84

▼ View and Set Clock Settings 85

▼ View and Clear the ILOM Event Log 86

▼ Configure Remote Syslog Receiver IP Addresses 88

▼ Configure an Alert Rule 89

Configuring SMTP Client for Email Notification Alerts 91

▼ Configure SMTP Client for Email Notification Alerts 91

Configuring Email Alert Settings 93

▼ View and Configure Email Alert Settings 93

▼ View and Configure Telemetry Harness Daemon Settings 94

**5. Monitoring Power Consumption 97**

Before You Begin 98

Monitoring the Power Consumption Interfaces 99

▼ Monitor System Total Power Consumption 99

▼ Monitor Actual Power Consumption 100

▼ Monitor Individual Power Supply Consumption 100

▼ Monitor Available Power 102

▼ Monitor Hardware Configuration Maximum Power Consumption 102

▼ Monitor Permitted Power Consumption 102

▼ Monitor Power Management Settings 102

Using the Power Consumption Control Interfaces 103

▼ View and Set the Power Policy 103

**6. Configuring ILOM Firmware Settings 105**

Before You Begin 105

Configuring ILOM Firmware Interfaces 106

- View and Configure ILOM Firmware Settings 106

**7. Managing the ILOM Configuration 109**

Before You Begin 109

Configuring ILOM Configuration Management Interfaces 110

- View and Configure Policy Settings 110
- Configure Power Setting 111
- View and Configure Backup and Restore Settings 112
- Configure the Reset Setting 113

**8. Managing a SPARC System Configuration 115**

Before You Begin 116

Configuring SPARC Management Interfaces 116

- View and Configure SPARC Diagnostic Settings 117
- View and Configure SPARC Host Settings 120
- View and Configure SPARC Boot Mode Settings 123
- View and Configure SPARC Keyswitch Setting 124

**9. IPMI Overview 129**

About Intelligent Platform Management Interface 130

`IPMItool` 130

IPMI Alerts 131

Configuring the IPMI State 131

- Enable IPMI State Using the CLI 132
- Enable IPMI State Using the Web Interface 132

Using IPMItool to Run ILOM CLI Commands 133

Before You Begin 133

- Access the ILOM CLI From IPMItool 133
- Script ILOM CLI Commands With IPMItool 133

IPMItool Examples 135

- View a List of Sensors and Their Values 135
- View Details About a Single Sensor 136
- Power On the Host 136
- Power Off the Host 136
- Power Cycle the Host 137
- Shut Down the Host Gracefully 137
- View Manufacturing Information for FRUs 137
- View the System Event Log 138

IPMI Commands 139

**Index 141**

# Preface

The *Integrated Lights Out Manager (ILOM) 3.0 SNMP and IPMI Procedures Guide* describes how to perform the required procedures to access ILOM functions using the Simple Network Management Protocol (SNMP). This document also provides descriptions of the procedures you can perform to access ILOM functions using the Intelligent Platform Management Interface (IPMI).

This SNMP and IPMI 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`<br>`product_part_number`<br>`product_serial_number`<br>`product_manufacturer` |
| Basic product information on chassis monitoring module (CMM) | `/CH` | `product_name`<br>`product_part_number`<br>`product_serial_number`<br>`product_manufacturer` |
| Basic chassis information on blade | `/SYS/MIDPLANE` | `product_name`<br>`product_part_number`<br>`product_serial_number`<br>`product_manufacturer` |
| Location of blade within the chassis | `/SYS/SLOTID` | `type`<br>`class`<br>`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.<br>Use `ls -a` to list all files.<br>`% You have mail.` |
| **`AaBbCc123`** | What you type, when contrasted with on-screen computer output | `% su`<br>`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*.<br>These are called *class* options.<br>You *must* be superuser to do this.<br>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

# PART I SNMP

Part 1 of this document provides an overview of the Simple Network Management Protocol (SNMP), and descriptions of the procedures you can perform to access ILOM functions.

CHAPTER 1

# SNMP Overview

**Topics**

| Description | Links |
|---|---|
| Learn about SNMP, SNMP components, and SNMP MIBs | • "About Simple Network Management Protocol" on page 2 |
| Learn about preparing your system to use SNMP, SNMP components, and SNMP MIBs | • "Preparing Your System to Use SNMP" on page 3<br>• "SNMP Components" on page 3<br>• "ILOM SNMP MIBs" on page 4 |

**Related Topics**

| For ILOM | Section | Guide |
|---|---|---|
| • Concepts | • ILOM Overview | *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* |
| • CLI | • CLI Overview | *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* |
| • Web interface | • Web Interface Overview | *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* |
| • IPMI | • 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/`

# About Simple Network Management Protocol

ILOM supports the Simple Network Management Protocol (SNMP), which is used to exchange data about network activity. SNMP is an open, industry-standard protocol technology that enables the management of networks and devices, or nodes, that are connected to the network. Using SNMP, data travels between a managed device (node) and a management station with network access. A managed device can be any device that runs SNMP, such as hosts, routers, web servers, or other servers on the network. SNMP messages are sent over IP using the User Datagram Protocol (UDP). Any management application that supports SNMP can manage your server.

For a more complete description of SNMP, see the SNMP five-part, introductory tutorial available at:

http://www.dpstele.com/layers/l2/snmp_l2_tut_part1.php

ILOM supports SNMP versions 1, 2c, and 3. Using SNMP v3 is strongly advised since SNMP v3 provides additional security, authentication, and privacy beyond SNMP v1 and v2c.

SNMP is a protocol, not an application, so you need an application to utilize SNMP messages. Your SNMP management software might provide this functionality, or you can use an open source tool like Net-SNMP, which is available at:

http://net-snmp.sourceforge.net/

---

**Note –** ILOM users reading this document are assumed to have a working knowledge of SNMP. SNMP client-side commands are used in this text as examples of using SNMP. Users who do not have a working knowledge of SNMP should complete the tutorial at http://net-snmp.sourceforge.net/wiki/index.php/Tutorials. This tutorial is more advanced than the introductory tutorial referred to above.

---

# Preparing Your System to Use SNMP

To prepare your system to use SNMP, you must download and install the latest version (version 5.2.1 or higher) of Net-SNMP that works with the operating system of your management station or the SNMP tool of your choice.

For more information about preparing your system to use SNMP, see one of the following guides:

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

# SNMP Components

SNMP functionality requires the following two components:

- **Network management station** – A network management station hosts management applications, which monitor and control managed nodes.
- **Managed node** – A managed node is a device such as a server, router, or hub that hosts SNMP management agents that are responsible for carrying out requests from management stations, such as a service processor (SP) running ILOM. Managed nodes can also provide unsolicited status information to a management station in the form of a trap.

SNMP is the protocol used to communicate management information between management stations and SNMP agents.

The SNMP agent is preinstalled on your server platform and runs on ILOM, so all SNMP management occurs through ILOM. To utilize this feature, your operating system must have an SNMP client application.

Both management stations and agents use SNMP messages to communicate. Management stations can send and receive information. Agents can respond to requests and send unsolicited messages in the form of traps. Management stations and agents use the following functions:

- Get
- GetNext
- GetResponse
- Set
- Trap

# ILOM SNMP MIBs

The base component of an SNMP implementation is the Management Information Base (MIB). A MIB is a text file that describes a managed node's available information. This tree-like, hierarchical system classifies information about resources in a network as a list of data objects, each with a unique identifier, or object ID. Thus, the MIB defines the data objects, or variables, that the SNMP agent can access. When a management station requests information from a managed node, the agent receives the request and retrieves the appropriate information from the MIBs. In ILOM, the MIB makes it possible to access the server's network configuration, status, and statistics.

For more information about SNMP MIBs, see "ILOM Interfaces" in the *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*

FIGURE 1-1 shows the standard MIB tree and the location of the ILOM MIB modules in that tree. The ILOM MIB modules are highlighted in boldface text.

**FIGURE 1-1** Location of ILOM MIB Modules

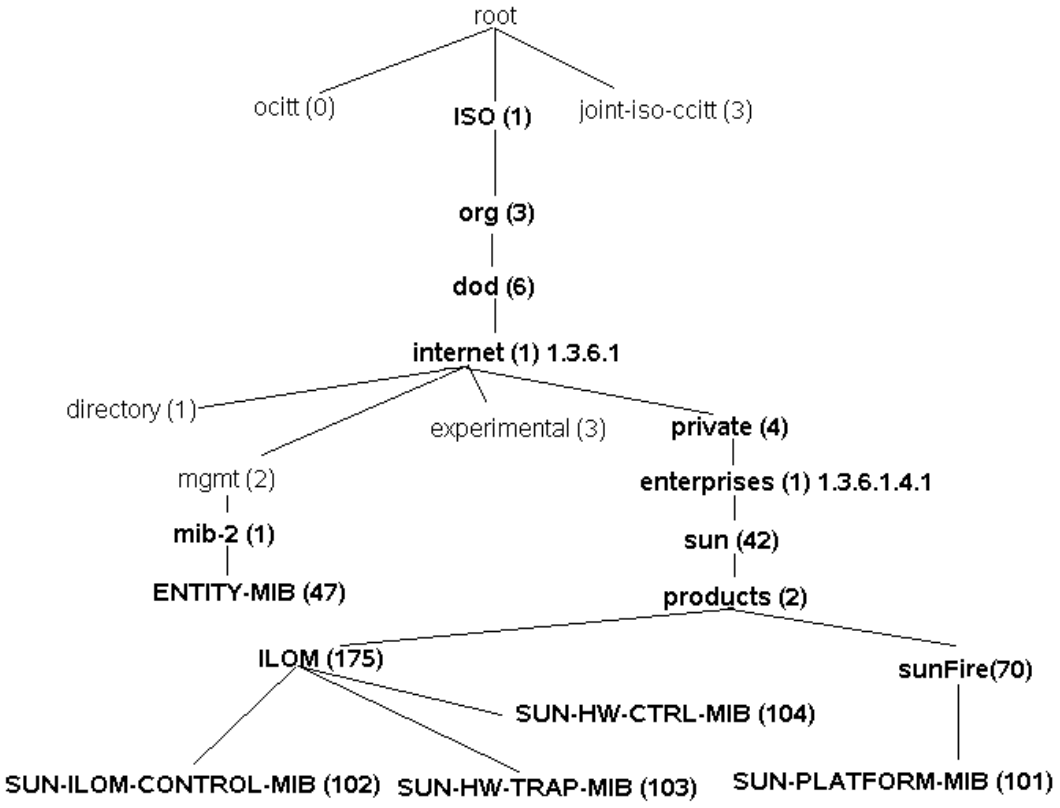



TABLE 1-1 provides a description of the ILOM MIB modules and lists the object ID for each MIB name.

**TABLE 1-1** SNMP MIBs Used With ILOM

| MIB Name | Description | MIB Object ID |
|---|---|---|
| ENTITY-MIB | The MIB module for representing multiple physical entities supported by a single SNMP agent.<br>**Note -** The entPhysicalTable is the only part of this MIB that is implemented. | 1.3.6.1.2.1.47 |
| SUN-HW-CTRL-MIB | This MIB allows controls for all platform devices using ILOM.<br>**Note -** Only the Power Management portions of this MIB are implemented. | 1.3.6.1.4.1.42.2.175.104 |

**TABLE 1-1** SNMP MIBs Used With ILOM *(Continued)*

| MIB Name | Description | MIB Object ID |
|---|---|---|
| SUN-HW-TRAP-MIB | This MIB describes the hardware related notifications/traps that may be generated by systems. | 1.3.6.1.4.1.42.2.175.103 |
| SUN-ILOM-CONTROL-MIB | This MIB provides objects for configuring and managing all ILOM functions. Configuration covered by this MIB includes functions such as authorization, authentication, logging, services, networking, and firmware management. | 1.3.6.1.4.1.42.2.175.102 |
| SUN-PLATFORM-MIB | This MIB provides extensions to the ENTITY-MIB (RFC 2737) where each entity modeled in the system is represented by means of extensions to the entPhysicalTable. | 1.3.6.1.4.1.42.2.70.101 |

Portions of the standard MIBs listed in TABLE 1-2 are implemented by ILOM.

**TABLE 1-2** Standard MIBs Implemented by ILOM

| MIB Name | Description | MIB Object ID |
|---|---|---|
| IF-MIB | The MIB module for describing generic objects for network interface sub-layers. This MIB is an updated version of MIB-II's ifTable, and incorporates the extensions defined in RFC 1229. | 1.3.6.1.2.1.31 |
| IP-MIB | The MIB module for managing IP and ICMP implementations, but excluding their management of IP routes. | 1.3.6.1.2.1.4. |
| SNMP-FRAMEWORK-MIB | The SNMP Management Architecture MIB. | 1.3.6.1.6.3.10 |
| SNMPv2-MIB | The MIB module for SNMP entities.<br>**Note -** Only the system and SNMP groups from this MIB module apply to ILOM. | 1.3.6.1.6.3.1 |
| TCP-MIB | The MIB module for managing TCP implementations. | 1.3.6.1.2.1.49 |
| UDP-MIB | The MIB module for managing UDP implementations. | 1.3.6.1.2.1.50 |

TABLE 1-3 describes MIBs that are used in support of the ILOM SNMP implementation.

**TABLE 1-3** MIBs Used in Support of the ILOM SNMP Implementation

| MIB Name | Description | MIB Object ID |
|---|---|---|
| HOST-RESOURCES-MIB | This MIB is for use in managing host systems. This MIB supports attributes common to all internet hosts including, for example, both personal computers and systems that run variants of UNIX. | 1.3.6.1.2.1.25.1 |
| IANAifType-MIB | This MIB module defines the IANAifType Textual Convention, and thus the enumerated values of the ifType object defined in MIB-II's ifTable. | 1.3.6.1.2.1.30 |
| NOTIFICATION-LOG-MIB | This MIB module is used for logging SNMP notifications (traps). | 1.3.6.2.1.92.1.1.3 |
| SNMP-MPD-MIB | This MIB module is used for Message Processing and Dispatching. | 1.3.6.1.6.3.11 |
| SNMPv2-TM | This MIB module is used for SNMP transport mappings. | 1.3.6.1.6.3.19 |
| SNMPv2-SMI | This MIB module contains definitions for the structure of management information, version 2. | 1.3.6.1.6 |

CHAPTER 2

# Configuring ILOM Communication Settings

**Topics**

| Description | Links |
|---|---|
| Review the prerequisites | • "Before You Begin" on page 10 |
| Configure network settings | • "Assign Host Name and System Identifier" on page 11<br>• "View and Configure Network Settings" on page 13<br>• "View and Configure Serial Port Settings" on page 17<br>• "View and Configure HTTP and HTTPS Settings" on page 20<br>• "Configure IP Addresses" on page 21 |
| Configure Secure Shell settings | • "View the Current Key and Key Length" on page 25<br>• "Enable and Disable SSH" on page 26<br>• "Generate a New SSH Key" on page 27<br>• "Restart the SSH Server" on page 28 |

**Related Topics**

| For ILOM | Section | Guide |
|---|---|---|
| • Concepts | • ILOM Network Configurations and Log In Requirements | *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* |
| • CLI | • Configuring ILOM Communication Settings | *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* |
| • Web Interface | • Configuring ILOM Communication Settings | *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* |

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

# Before You Begin

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

- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or SNMP v3 user with read/write (rw) privileges.
- Before you can use SNMP to view and configure ILOM settings, you must configure SNMP. For more information, see "Configuring Network Settings" on page 11.

**Note –** The example SNMP commands presented in this chapter are based on the Net-SNMP sample applications and, therefore, will only work as presented if you have Net-SNMP and the Net-SNMP sample applications installed.

# Configuring Network Settings

**Topics**

| Description | Links |
|---|---|
| Configure network settings | • "Assign Host Name and System Identifier" on page 11<br>• "View and Configure Network Settings" on page 13<br>• "View and Configure Serial Port Settings" on page 17<br>• "View and Configure HTTP and HTTPS Settings" on page 20<br>• "Configure IP Addresses" on page 21 |

This section describes how to configure the network parameters for ILOM using the SNMP interface.

If you are using the Net-SNMP sample applications, you can use the `snmpget` and `snmpset` commands to view and configure network settings.

## ▼ Assign Host Name and System Identifier

### Before You Begin

- You can use the `get` and `set` commands to view and configure host name and system identifier MIB object settings. For a description of the MIB objects used in this procedure, see "Host Name and System Identifier MIB Objects" on page 12.

Follow these steps to assign a host name and system identifier:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **To get the host name, type:**

```
% snmpget -v2c -cprivate SNMP_agent_ipaddress ilomCtrlHostName.0
SUN-ILOM-CONTROL-MIB::ilomCtrlHostName.0 = STRING: wgs97-218
```

3. **To set the host name, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlHostName.0 s wgs97-200
SUN-ILOM-CONTROL-MIB::ilomCtrlHostName.0 = STRING: wgs97-200
```

4. **To get the system identifier, type:**

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSystemIdentifier.0
SUN-ILOM-CONTROL-MIB::ilomCtrlSystemIdentifier.0 = STRING: none
```

5. **To set the system identifier, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSystemIdentifier.0 s wgs97-200
SUN-ILOM-CONTROL-MIB::ilomCtrlSystemIdentifier.0 = STRING: wgs97-
200
```

## Host Name and System Identifier MIB Objects

The following MIB objects, values, and types are valid for host name and system identifier.

**TABLE 2-1** Valid MIB Objects, Values, and Types for Host Name and System Identifier Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| ilomCtrlHostName | The host name for ILOM. | hostname (Size: 0 to 255) | String | None |
| ilomCtrlSystemIdentifier | The identifier that is sent out on the varbind for all traps that ILOM generated. This string is often the host name of the server that is associated with ILOM. | systemidentifier (Size: 0 to 255) | String | None |

# ▼ View and Configure Network Settings

### Before You Begin

- For a description of the MIB objects used in this procedure, see "Network Settings MIB Objects" on page 16 and the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure network settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username@snmp_manager_ipaddress*

   `Password:` *password*

2. **To determine the name of the network target and the current network settings, type:**

```
% snmpwalk -v2c -cprivate -mALL SNMP_agent_ipaddress ilomCtrlNetwork
```

   This command displays the following information:

```
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkMacAddress."SP/network" = STRING:
00:14:4F:0E:23:B8
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpDiscovery."SP/network" = INTEGER:
static(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpAddress."SP/network" = IpAddress:
ipaddress
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpGateway."SP/network" = IpAddress:
ipaddress
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkIpNetmask."SP/network" = IpAddress:
ipaddress
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpDiscovery."SP/network" = INTEGER:
static(1)
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpAddress."SP/network" = IpAddress:
ipaddress
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpGateway."SP/network" = IpAddress:
ipaddress
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkPendingIpNetmask."SP/network" = IpAddress:
ipaddress
SUN-ILOM-CONTROL-MIB::ilomCtrlNetworkCommitPending."SP/network" = INTEGER:
false(2)
```

The network target name as shown above is "`SP/network`."

3. **To view the current network IP address for network target named "/SP/network", type:**

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlNetworkIpAddress."/SP/network"
```

4. **To specify a new network IP address, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlNetworkPendingIpAddress."/SP/network" s 10.300.10.15
```

5. **To put the new network IP address into effect, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlNetworkCommitPending."/SP/network" i 1
```

6. **Refer to the following SNMP commands for other examples:**
   - To view the MAC address of the out-of-band management interface (where applicable), type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlNetworkOutOfBandMacAddress.0
```

   - To view the MAC address of the sideband management interface (where applicable), type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlNetworkSidebandMacAddress.0
```

   - To view the pending management port for the given target, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlNetworkPendingManagementPort.TARGET_INTERFACE
```

   - To set the pending management port for the given target, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlNetworkPendingManagementPort.TARGET_INTERFACE s
'pendingmanagementport'
```

---

**Note –** This property setting does not take effect until the `ilomCtrlNetworkCommitPending` property is set to `true` for the given row.

---

- To view the current management port for the given target, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlNetworkgManagementPort.0
```

- To set the current management port for the given target, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlNetworkManagementPort.0 s 'managementport'
```

- To view the address of the DHCP server for this row, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlNetworkDHCPServerAddr.0
```

- To view whether the network state row is enabled, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlNetworkState.0
```

- To set the network state row to enabled, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlNetworkState.0 i 1
```

## Network Settings MIB Objects

The following MIB objects, values, and types are valid for network settings.

**TABLE 2-2** Valid MIB Objects, Values, and Types for Network Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlNetwork Target` | This is the nomenclature name for a target that has a configurable network. On some systems, there are multiple targets that have networks. On a rackmount stand-alone server, this table will contain only one row for the network configuration of the service processor, which has a nomenclature name of '/SP'. On blade systems, this table will contain multiple rows. There will be a row for each blade's service processor. For example, a blade's service processor nomenclature takes the form of '/CH/BL0/SP', '/CH/BL1/SP' and so on.<br>**Note -** This object is not accessible. | *network_target_name* | String | None |
| `ilomCtrlNetwork MacAddress` | Indicates the MAC address of the service processor.<br>**Note -** This object is read-only. | *MAC_address* | String | None |
| `ilomCtrlNetwork IPDiscovery` | Indicates whether the current target is configured to have static IP settings or whether these settings are retrieved dynamically from DHCP.<br>**Note -** This object is read-only. | `Static(1), Dynamic(2)` | Integer | None |
| `ilomCtrlNetwork IpAddress` | Indicates the current IP address for the given target.<br>**Note -** This object is read-only. | *ipaddress* | String | None |
| `ilomCtrlNetwork IpGateway` | Indicates the current IP gateway for the given target.<br>**Note -** This object is read-only. | *ip_gateway* | String | None |
| `ilomCtrlNetwork IpNetmask` | Indicates the current IP netmask for the given target.<br>**Note -** This object is read-only. | *ip_netmask* | String | None |

**TABLE 2-2** Valid MIB Objects, Values, and Types for Network Settings *(Continued)*

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlNetwork PendingIp Discovery` | This object is used to set the pending value for the mode of IP discovery for the given target. The possible values are `static(1)` or `dynamic(2)`. Static values can be specified by setting the other pending properties in this table: `ilomCtrlNetworkPendingIp-Address`, `ilomCtrlNetworkPendingIp-Gateway`, and `ilomCtrlNetworkPendingIpNetmask`. If dynamic is specified, the other pending properties should not be set. This setting does not take effect until the `ilomCtrlNetworkCommitPending` property is set to `true` for the given row. | `static(1)`, `dynamic(2)` | Integer | None |
| `ilomCtrlNetwork PendingIp Address` | This object is used to set the pending IP address for the given target. This setting does not take effect until the `ilomCtrlNetworkCommitPending` property is set to `true` for the given row. | *pending_ip_address* | String | None |
| `ilomCtrlNetwork PendingIp Gateway` | This object is used to set the pending IP gateway for the given target. This setting does not take effect until the `ilomCtrlNetworkCommitPending` object is set to `true` for the given row. | *pending_ip_gateway* | String | None |
| `ilomCtrlNetwork PendingIp Netmask` | This object is used to set the pending IP netmask for the given target. This setting does not take effect until the `ilomCtrlNetworkCommitPending` object is set to `true` for the given row. | *pending_ip_netmask* | String | None |
| `ilomCtrlNetwork CommitPending` | This object is used to commit pending settings for the given row. Settings this object to `true(1)` will cause the network to be reconfigured according to the values specified in the other pending settings. | `true(1)`, `false(2)` | Integer | None |

# ▼ View and Configure Serial Port Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure serial port settings. For a description of the MIB objects used in this procedure, see "Serial Port Settings MIB Objects" on page 18.

Follow these steps to view and configure serial port settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   Password**:** *password*

2. **To determine whether the service processor has an internal serial port that is configurable, type:**

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSerialInternalPortPresent.0
```

3. **To set the baud rate of the internal port to 9600, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSerialInternalPortBaudRate.0 i 1
```

## Serial Port Settings MIB Objects

The following MIB objects, values, and types are valid for serial port settings.

**TABLE 2-3** Valid MIB Objects, Values, and Types for Serial Port Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| ilomCtrlSerial Internal PortPresent | Indicates whether the given device has an internal serial port that is configurable.<br>**Note -** This object is read-only. | true(1), false(2) | Integer | None |
| ilomCtrlSerial InternalPort BaudRate | Specifies the current baud rate setting for the internal serial port. This object is only readable or settable if ilomCtrlSerialInternal-PortPresent is true. | baud9600(1), baud19200(2), baud38400(3), baud57600(4), baud115200(5) | Integer | None |

**TABLE 2-3** Valid MIB Objects, Values, and Types for Serial Port Settings *(Continued)*

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlSerial ExternalPort Present` | Indicates whether the given device has an external serial port that is configurable.<br>**Note -** This object is read-only. | `true(1), false(2)` | Integer | None |
| `ilomCtrlSerial ExternalPort BaudRate` | Specifies the current baud rate setting for the external serial port. This object is only readable or settable if `ilomCtrlSerialExternalPort-Present` is `true`. | `baud9600(1), baud19200(2), baud38400(3), baud57600(4), baud115200(5)` | Integer | None |
| `ilomCtrlSerial ExternalPort FlowControl` | Specifies the current flow control setting for the external serial port. This object is only readable or settable if `ilomCtrlSerialExternalPort-Present` is `true`. | `unknown(1), hardware(2), software(3), none(4)` | Integer | None |

# ▼ View and Configure HTTP and HTTPS Settings

ILOM supports both HTTP or HTTPS connections. ILOM enables you to automatically redirect HTTP access to HTTPS. ILOM also enables you to set the HTTP and HTTPS ports.

### Before You Begin

- You can use the `get` and `set` commands to view and configure HTTP or HTTPS web access. For a description of the MIB objects used in this procedure, see "HTTP and HTTPS Settings MIB Objects" on page 21.

Follow these steps to view and configure HTTP and HTTPS settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP commands for examples:**
   - To get the HTTP state, type:

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlHttpEnabled.0
```

   - To enable HTTP, type:

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlHttpEnabled.0 i 1
```

   - To set the HTTP port number, type:

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlHttpPortNumber.0 i 80
```

   - To configure HTTP to redirect HTTP connections to HTTPS, type:

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlHttpSecureRedirect.0 i 1
```

## HTTP and HTTPS Settings MIB Objects

The following MIB objects, values, and types are valid for HTTP and HTTPS settings.

**TABLE 2-4** Valid MIB Objects, Values, and Types for HTTP and HTTPS Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| **HTTP** | | | | |
| `ilomCtrlHttp Enabled` | Specifies whether the embedded web server should be running and listening on the HTTP port. | `true(1), false(2)` | Integer | None |
| `ilomCtrlHttp PortNumber` | Specifies the port number that the embedded web server should listen on for HTTP requests. | Range: 0..65535 | Integer | None |
| `ilomCtrlHttp SecureRedirect` | Specifies whether the embedded web server should redirect HTTP connections to HTTPS. | `true(1), false(2)` | Integer | Enabled |
| **HTTPS** | | | | |
| `ilomCtrlHttps Enabled` | Specifies whether the embedded web server should be running and listening on the HTTPS port. | `true(1), false(2)` | Integer | True |
| `ilomCtrlHttps PortNumber` | Specifies the port number that the embedded web server should listen on for HTTPS requests. | Range: 0..65535 | Integer | None |

# ▼ Configure IP Addresses

### Before You Begin

- You can use `get` and `set` commands to edit existing IP addresses in ILOM. For a description of the MIB objects used in this procedure, see "Valid MIB Objects for IP Addresses" on page 23.

Follow these steps to configure IP addresses:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **To get a network IP address, type:**

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlNetworkIpAddress.0
```

3. **To set a network IP address, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlNetworkPendingIpAddress.0 s ipaddress
ilomCtrlNetworkCommitPending.0 i 1
```

## Valid MIB Objects for IP Addresses

The following MIB objects, properties, values, and types are valid for IP addresses.

**TABLE 2-5** Valid MIB Objects, Properties, Values, and Types for IP Addresses

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlNetworkTarget` | This is the nomenclature name for a target that has a configurable network. On some systems, there are multiple targets that have networks. On a rackmount stand-alone server, this table will contain only one row for the network configuration of the service processor, which has a nomenclature name of '/SP'. On blade systems, this table contains multiple rows. There will be a row for '/SC' which allows for configuration of the network settings. In addition, there are rows for each blade's service processor. For example, a blade's service processor nomenclature takes the form of '/CH/BL0/SP', '/CH/BL1/SP' and so on. This allows for the configuration of the service processors from the CMM.<br>**Note -** This MIB object is not accessible. | *target* | String | none |
| `ilomCtrlNetworkMacAddress` | The MAC address of the service processor or system controller.<br>**Note -** This object is read-only. | *MAC_address* | String | none |
| `ilomCtrlNetworkIpDiscovery` | Indicates whether the current target is configured to have static IP settings or whether these settings are retrieved dynamically from DHCP.<br>**Note -** This object is read-only. | `static(1), dynamic(2)` | Integer | none |
| `ilomCtrlNetworkIpAddress` | Indicates the current IP address for the given target.<br>**Note -** This object is read-only. | *ip_address* | String | none |
| `ilomCtrlNetworkIpGateway` | Indicates the current IP gateway for the given target.<br>**Note -** This object is read-only. | *ip_gateway* | String | none |
| `ilomCtrlNetworkIpNetmask` | Indicates the current IP netmask for the given target.<br>**Note -** This object is read-only. | *ip_netmask* | String | none |

**TABLE 2-5** Valid MIB Objects, Properties, Values, and Types for IP Addresses *(Continued)*

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlNetworkPending IpAddress` | This object is used to set the pending IP address for the given target. This property does not take effect until the `ilomCtrlNetworkCommitPending` property is set to `true` for the given row. | *pending_ipaddress* | String | None |
| `ilomCtrlNetworkPending IpGateway` | This object is used to set the pending IP gateway for the given target. This setting does not take effect until the `ilomCtrlNetworkCommitPending` property is set to `true` for the given row. | *pending_ip_gateway* | String | None |
| `ilomCtrlNetworkPending IpDiscovery` | This object is used to set the pending value for the mode of IP discovery for the given target. The possible values are `static(1)` or `dynamic(2)`. Static values can be specified by setting the other pending properties in this table: `ilomCtrlNetworkPendingIp Address`, `ilomCtrlNetworkPendingIp Gateway`, and `ilomCtrlNetworkPendingIp Netmask`. If dynamic is specified, the other pending properties should not be set. This property does not take effect until the `ilomCtrlNetworkCommitPending` MIB object is set to `true` for the given row. | `static(1)`, `dynamic(2)` | Integer | None |
| `ilomCtrlNetworkPendingIpNetmask` | This object is used to set the pending IP netmask for the given target. This property does not take effect until the `ilomCtrlNetworkCommitPending` property is set to `true` for the given row. | *pending_ip_netmask* | String | none |
| `ilomCtrlNetworkCommitPending` | This object is used to commit pending properties for the given row. Setting this property to `true(1)` will cause the network to be reconfigured according to the values specified in the other pending properties. | `true(1)`, `false(2)` | Integer | None |

# Configuring Secure Shell Settings

**Topics**

| Description | Links |
|---|---|
| Configure Secure Shell settings | • "View the Current Key and Key Length" on page 25<br>• "Enable and Disable SSH" on page 26<br>• "Generate a New SSH Key" on page 27<br>• "Restart the SSH Server" on page 28 |

## ▼ View the Current Key and Key Length

### Before You Begin

- You can use `get` commands to view current key and key length information. For a description of the MIB objects used in this procedure, see "RSA and DSA Current Key and Key Length MIB Objects" on page 26.

Follow these steps to view the current key and key length:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - For RSA keys, to view the current key and key length, type the following:

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSshRsaKeyFingerprint.0
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSshRsaKeyLength.0
```

   - For DSA keys, to view the current key and key length, type the following:

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSshDsaKeyFingerprint.0
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSshDsaKeyLength.0
```

## RSA and DSA Current Key and Key Length MIB Objects

You use the following MIB objects to view key information.

**TABLE 2-6** Valid MIB Objects, Values, and Types for the Key Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlSshRsaKey Fingerprint` | The fingerprint of the RSA key used for the SSH protocol. | Size: 0..255 | String | None |
| `ilomCtrlSshRsaKey Length` | The length of the RSA key used for the SSH protocol. | Range: 0..65535 | Integer | None |
| `ilomCtrlSshDsaKey Fingerprint` | The fingerprint of the DSA key used for the SSH protocol. | Size: 0..255 | String | None |
| `ilomCtrlSshDsaKey Length` | The length of the DSA key used for the SSH protocol. | Range: 0..65535 | Integer | None |

# ▼ Enable and Disable SSH

### Before You Begin

- You can use the `set` command enable and disable SSH. For a description of the MIB objects used in this procedure, see "SSH Enabled MIB Object" on page 27.

Follow these steps to enable and disable SSH:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username***`@`***snmp_manager_ipaddress*

   `Password:` *password*

2. **To enable or disable SSH, type the following command to set the** `ilomCtrlSshEnabled` **MIB object to** `1` **(enabled) or** `2` **(disabled):**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSshEnabled.0 i 1|2
```

## SSH Enabled MIB Object

Use the following MIB object to enable or disable SSH.

**TABLE 2-7** Valid MIB Object, Value, and Type for SSH Enabled Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlSsh Enabled` | Specifies whether or not the SSH is enabled. | `true(1), false(2)` | Integer | Enabled |

# ▼ Generate a New SSH Key

### Before You Begin

- You can use the `set` command to generate a new SSH key. For a description of the MIB objects used in this procedure, see "SSH Key MIB Objects" on page 28.

Follow these steps to generate a new SSH key:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username***`@`***snmp_manager_ipaddress*

   `Password:` *password*

2. **To set the SSH key type to RSA, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSshGenerateNewKeyType.0 i 2
```

3. **To generate a new RSA key, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSshGenerateNewKeyAction.0 i 1
```

**Note –** The fingerprint and key will look different.

## SSH Key MIB Objects

The following MIB objects, values, and types are valid for generating SSH keys.

**TABLE 2-8** Valid MIB Objects, Values, and Types for Generating SSH Keys

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlSsh GenerateNewKey Action` | This MIB object is used to initiate a new public key generation. | `true(1), false(2)` | Integer | None |
| `ilomCtrlSsh GenerateNewKey Type` | This MIB object is used to specify the type of SSH key to generate. | `none(1), rsa(2), dsa(3)` | Integer | None |

# ▼ Restart the SSH Server

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

### Before You Begin

- You can use the `set` command to restart SSH. For a description of the MIB object used in this procedure, see "Restart SSH MIB Object" on page 29.

---

**Note –** Restarting SSH will end any existing SSH connections.

---

Follow these steps to restart the SSH server:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username***`@`***snmp_manager_ipaddress*

   **`Password:`** *password*

2. **To restart the SSH server, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSshRestartSshAction.0 i 1
```

## Restart SSH MIB Object

The following MIB object, value, and type are valid for restarting SSH.

**TABLE 2-9** Valid MIB Object, Value, and Type for Restarting SSH

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlSshRestart SshdAction` | This object is used to initiate an SSHD restart. | `true(1), false(2)` | Integer | None |

CHAPTER 3

# Managing User Accounts

**Topics**

| Description | Links |
|---|---|
| Review the prerequisites | • "Before You Begin" on page 33 |
| Configure user accounts | • "Configure User Accounts" on page 34<br>• "Configure Single Sign On" on page 36 |

**Topics**

| Description | Links |
|---|---|
| Configure Active Directory settings | • "View and Configure Active Directory Settings" on page 38<br>• "View and Configure Active Directory Administrator Groups Settings" on page 43<br>• "View and Configure Active Directory Operator Groups Settings" on page 44<br>• "View and Configure Active Directory Custom Groups Settings" on page 46<br>• "View and Configure Active Directory User Domain Settings" on page 49<br>• "View and Configure Active Directory Alternate Server Settings" on page 50<br>• "View and Configure Redundancy Settings" on page 54<br>• "View and Configure Active Directory DNS Locator Settings" on page 55<br>• "View and Configure DNS Name Server Settings" on page 57 |
| Configure LDAP settings | • "Configure LDAP Settings" on page 58 |
| Configure LDAP/SSL settings | • "View and Configure LDAP/SSL Administrator Groups Settings" on page 67<br>• "View and Configure LDAP/SSL Operator Groups Settings" on page 68<br>• "View and Configure LDAP/SSL Custom Groups Settings" on page 70<br>• "View and Configure LDAP/SSL User Domain Settings" on page 73<br>• "View and Configure LDAP/SSL Alternate Server Settings" on page 74 |

**Related Topics**

| For ILOM | Section | Guide |
|---|---|---|
| • Concepts | • User Account Management | *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* |
| • Web | • Managing User Accounts | *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* |
| • CLI | • Managing User Accounts | *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/

# Before You Begin

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

- To view user account information, you need the Read Only (`o`) role enabled.
- To configure user account information, you need the User Management (`u`) role enabled.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user account with read/write (rw) privileges.

**Note –** The example SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will only work as presented if you have Net-SNMP and the Net-SNMP sample applications installed.

# Configuring User Accounts

**Topics**

| Description | Links |
|---|---|
| Configure user accounts | • "Configure User Accounts" on page 34<br>• "Configure Single Sign On" on page 36 |

## ▼ Configure User Accounts

### Before You Begin

- You can use `get` and `set` commands to configure user account MIB object settings. For a description of the MIB objects used in this procedure, see "User Account MIB Objects" on page 35.

Follow these steps to configure user accounts:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **To create a new user account with a user role of Operator, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLocalUserRowStatus.'user1' i 4
ilomCtrlLocalUserRoles.'user1' s "operator"
ilomCtrlLocalUserPassword.'user1' s "password"
```

3. **To delete a user account, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLocalUserRowStatus.'user1' i 6
```

# User Account MIB Objects

The following MIB objects, properties, values, and types are valid for local user accounts.

**TABLE 3-1** Valid MIB Objects, Properties, Values, and Types for Local User Accounts

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLocal UserUsername` | A local user user name. It must start with an alphabetical letter and may contain alphabetical letters, digits, hyphens and underscores, but cannot contain spaces. It cannot be the same as the password. | *username* | String | None |
| `ilomCtrlLocal UserPassword` | A local user password. | *password* | String | None |
| `ilomCtrlLocal UserRoles` | Specifies the role that is associated with a user. The roles can be assigned for the legacy roles of 'Administrator' or 'Operator', or any of the individual role IDs of 'a', 'u', 'c', 'r', 'o' and 's'. The role IDs can be joined together. For example, 'aucros', where a=admin, u=user, c=console, r=reset, o=read-only, s= service. | `administrator, operator, admin(a), user(u), console(c), reset(r), read-only(o), service(s)` | String | None |
| `ilomCtrlLocal UserRowStatus` | This object is used to create a new row or to delete an existing row in the table. This property can be set to either `createAndWait(5)` or `destroy(6)`, to create and remove a user respectively. | `active(1), notInService(2), notReady(3), createAndGo(4), createAndWait(5), destroy(6)` | Integer | None |
| `ilomCtrlLocal UserCLIMode` | An enumerated value that describes the possible CLI modes. The `default` mode corresponds to the ILOM DMTF CLP. The `alom` mode corresponds to the ALOM CMT. | `default(1), alom(2)` | Integer | None |

# ▼ Configure Single Sign On

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

### Before You Begin

- You can use the `set` command to configure single sign on MIB object settings. For a description of the MIB object used in this procedure, see "Single Sign On MIB Object" on page 37.

Follow these steps to configure single sign on:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username*@*snmp_manager_ipaddress*

   `Password:` *password*

2. **To enable Single Sign On, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlSingleSignonEnabled.0 i 1
```

## Single Sign On MIB Object

The following MIB object, value, and type are valid for Single Sign On.

**TABLE 3-2** Valid MIB Object, Value, and Type for Single Sign On

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlSingleSignonEnabled` | Specifies whether Single Sign On (SSO) authentication should be enabled on the device. SSO allows tokens to be passed so that it is not necessary to re-enter passwords between different applications. This allows SSO between the system controller (SC) web interface and the service processor (SP) web interface, between the SC command-line interface and the SP command-line interface, and between the SC and SP interfaces and the Java Remote Console application. | `true(1), false(2)` | Integer | None |

# Configuring Active Directory Settings

**Topics**

| Description | Links |
|---|---|
| Configure Active Directory Settings | • "View and Configure Active Directory Settings" on page 38<br>• "View and Configure Active Directory Administrator Groups Settings" on page 43<br>• "View and Configure Active Directory Operator Groups Settings" on page 44<br>• "View and Configure Active Directory Custom Groups Settings" on page 46<br>• "View and Configure Active Directory User Domain Settings" on page 49<br>• "View and Configure Active Directory Alternate Server Settings" on page 50<br>• "View and Configure Active Directory DNS Locator Settings" on page 55 |

# ▼ View and Configure Active Directory Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure Active Directory settings. For a description of the MIB objects used in this procedure, see "Active Directory MIB Objects" on page 41.
- For descriptions of the other MIB objects, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure Active Directory settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username*@*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - To view the Active Directory state, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryEnabled.0
```

   - To enable the Active Directory, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryEnabled.0 i 1
```

   - To view the Active Directory port number, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryPortNumber.0
```

   - To set the Active Directory port number, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryPortNumber.0 i portnumber
```

   - To view the Active Directory default user roles, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryDefaultRoles.0
```

   - To set the Active Directory default user roles, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryDefaultRoles.0 s acro
```

- To view the Active Directory certificate file URI, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertFileURI.0
```

- To set the Active Directory certificate file URI, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertFileURI.0 s URI
```

- To view the Active Directory time out, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryTimeout.0
```

- To set the Active Directory time out, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryTimeout.0 i 6
```

- To view the Active Directory certificate validation mode, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryStrictCertEnabled.0
```

- To set the Active Directory certificate validation mode, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryStrictCertEnabled.0 i 1
```

- To view the Active Directory certificate file status, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertFileStatus.0
```

- To view the event log setting for the amount of messages sent to the event log, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryLogDetail.0
```

- To configure the event log setting so that only the highest priority messages are sent to the event log, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryLogDetail.0 i 2
```

- To view the role that user1 is to have when authenticated via Active Directory, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryDefaultRoles.'user1'
```

- To specify the Admin (a) role for user1 when authenticated via Active Directory, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryDefaultRoles.'user1' s a
```

- To view and clear the certificate information associated with the server when it is set to true, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertClear.0
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertClear.0 i 0
```

- To view the version of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertVersion.0
```

- To view the serial number of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertserialNo.0
```

- To view the issuer of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertIssuer.0
```

- To view the subject of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertSubject.0
```

- To view the valid start date of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertValidBegin.0
```

- To view the valid end date of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirectoryCertValidEnd.0
```

## Active Directory MIB Objects

The following MIB objects, values, and types are valid for the Active Directory.

**TABLE 3-3** Valid MIB Objects, Values, and Types for Active Directory

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlActive Directory Enabled` | Specifies whether the Active Directory client is enabled. | `true(1), false(2)` | Integer | true |
| `ilomCtrlActive DirectoryIP` | The IP address of the Active Directory server used as a name service for user accounts. | *ipaddress* | String | None |
| `ilomCtrlActive Directory PortNumber` | Specifies the port number for the Active Directory client. Specifying zero as the port means auto-select while specifying 1 to 65535 configures the actual port. | portnumber Range: 0 to 65535 | Integer | None |

**TABLE 3-3** Valid MIB Objects, Values, and Types for Active Directory *(Continued)*

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrl Active Directory DefaultRoles` | Specifies the role that a user authenticated via Active Directory should have. Setting this property to legacy roles of 'Administrator' or 'Operator', or any of the individual role IDs of 'a', 'u', 'c', 'r', 'o' and 's' will cause the Active Directory client to ignore the schema stored on the Active Directory server. Setting this to 'none' clears the value and indicates that the native Active Directory schema should be used. The role IDs can be joined together. For example, 'aucros,' where a=admin, u= user, c=console, r=reset, o=read-only, and s=service. | `administrator, operator, admin(a), user(u), console(c), reset(r), read-only(o), service(s), none` | String | None |
| `ilomCtrlActive Directory CertFileURI` | This is the URI of a certificate file needed when Strict Certificate Mode is enabled. Setting the URI causes the transfer of the file, making the certificate available immediately for certificate authentication. | *URI* | String | None |
| `ilomCtrlActive Directory Timeout` | Specifies the number of seconds to wait before timing out if the Active Directory server is not responding. | Range: 1 to 20 seconds | Integer | 4 |
| `ilomCtrlActive Directory StrictCert Enabled` | Specifies whether the Strict Certificate Mode is enabled for the Active Directory client. If enabled, the Active Directory certificate must be uploaded to the SP so that certificate validation can be performed when communicating with the Active Directory server. | `true(1), false(2)` | Integer | true |
| `ilomCtrlActive DirectoryCert FileStatus` | A string indicating the status of the certificate file. This is useful in determining whether a certificate file is present or not. | *status* | String | None |

# ▼ View and Configure Active Directory Administrator Groups Settings

### Before You Begin

- If you were using the Net-SNMP sample applications, you could use the `snmpget` and `snmpset` commands to configure the Active Directory Administrator Groups settings. For a description of the MIB objects used in this procedure, see "Active Directory Administrator Groups MIB Objects" on page 44.

Follow these steps to view and configure Active Directory Administrator Groups settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **To view the name of Active Directory administrator group ID number 2, type:**

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAdminGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAdminGroupName.2 = STRING:
CN=spAdmins,DC=spc,DC=north,DC=sun,DC=com
```

3. **To set the name of Active Directory administrator group ID number 2 to CN=spAdmins,DC=spc,DC=south,DC=sun,DC=com, type:**

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAdminGroupName.2 s CN=spAdmins,DC=spc,DC=
south,DC=sun,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAdminGroupName.2 = STRING:
CN=spAdmins,DC=spc,DC=south,DC=sun,DC=com
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAdminGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAdminGroupName.2 = STRING:
CN=spAdmins,DC=spc,DC=south,DC=sun,DC=com
```

## Active Directory Administrator Groups MIB Objects

The following MIB objects, values, and types are valid for Active Directory Administrator Groups settings.

**TABLE 3-4** Valid MIB Objects, Values, and Types for Active Directory Administrator Groups Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlActive DirAdminGroupId` | An integer identifier of the Active Directory Administrator Groups entry. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlActive DirAdminGroup Name` | This string should contain a Distinguished Name that exactly matches one of the group names on the Active Directory server. Any user belonging to one of these groups in this table will be assigned the ILOM role of Administrator. | *name* (maximum of 255 characters) | String | None |

# ▼ View and Configure Active Directory Operator Groups Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the Active Directory Operator Groups settings. For a description of the MIB objects used in this procedure, see "Active Directory Operator Groups MIB Objects" on page 45.

Follow these steps to view and configure Active Directory Operator Groups settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **To view the name of Active Directory operator group ID number 2, type:**

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirOperatorGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirOperatorGroupName.2 =
STRING: ad-oper-group-ent-2
```

3. **To set the name of Active Directory operator group ID number 2 to new-name-2, type:**

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirOperatorGroupName.2 s new-name-2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirOperatorGroupName.2 =
STRING: new-name-2
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirOperatorGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirOperatorGroupName.2 =
STRING: new-name-2
```

## Active Directory Operator Groups MIB Objects

The following MIB objects, values, and types are valid Active Directory Operator Groups settings.

**TABLE 3-5** Valid MIB Objects, Values, and Types for Active Directory Operator Groups Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlActiveDirOperatorGroupId` | An integer identifier of the Active Directory Operator Groups entry. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlActiveDirOperatorGroupName` | This string should contain a Distinguished Name that exactly matches one of the group names on the Active Directory server. Any user belonging to one of these groups in this table will be assigned the ILOM role of Operator. | *name* (maximum of 255 characters) | String | None |

# ▼ View and Configure Active Directory Custom Groups Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the Active Directory Custom Groups settings. For a description of the MIB objects used in this procedure, see "Active Directory Custom Groups MIB Objects" on page 48.

Follow these steps to view and configure Active Directory Custom Groups settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **To view the name of Active Directory custom group ID number 2, type:**

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirCustomGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupName.2 =
STRING: CN=SpSuperCust,OU=Groups,DC=johns,DC=sun,DC=com
```

3. **To set the name of Active Directory custom group ID number 2 to CN= SpSuperCust,OU=Groups,DC=bills,DC=sun,DC=com, type:**

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirCustomGroupName.2 s CN=SpSuperCust,OU=Groups,DC=
bills,DC=sun,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupName.2 =
STRING: CN=SpSuperCust,OU=Groups,DC=bills,DC=sun,DC=com
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirCustomGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupName.2 =
STRING: CN=SpSuperCust,OU=Groups,DC=bills,DC=sun,DC=com
```

4. **To view the roles of Active Directory custom group ID number 2, type:**

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirCustomGroupRoles.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupRoles.2 =
STRING: "aucro"
```

5. **To set the roles of Active Directory custom group ID number 2 to User Management and Read Only (u,o), type:**

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirCustomGroupRoles.2 s "uo"
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupRoles.2 =
STRING: "uo"
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirCustomGroupRole.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupRoles.2 =
STRING: "uo"
```

# Active Directory Custom Groups MIB Objects

The following MIB objects, values, and types are valid for Active Directory Custom Groups settings.

**TABLE 3-6** Valid MIB Objects, Values, and Types for Active Directory Custom Groups Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlActiveDirCustomGroupId` | An integer identifier of the Active Directory Custom Groups entry. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlActiveDirCustomGroupName` | This string should contain a Distinguished Name that exactly matches one of the group names on the Active Directory server. Any user belonging to one of these groups in this table will be assigned the ILOM role based on the entry's configuration for roles. | *name* (maximum of 255 characters) | String | None |
| `ilomCtrlActiveDirCustomGroupRoles` | Specifies the role that a user authenticated via Active Directory should have. Setting this property to legacy roles of 'Administrator' or 'Operator', or any of the individual role IDs of 'a', 'u', 'c', 'r', 'o' and 's' will cause the Active Directory client to ignore the schema stored on the Active Directory server. Setting this object to 'none' clears the value and indicates that the native Active Directory schema should be used. The role IDs can be joined together. For example, 'aucros,' where a= admin, u=user, c=console, r= reset, o=read-only, and s= service. | `administrator, operator, admin(a), user(u), console(c), reset(r), read-only(o), service(s), none` | String | None |

# ▼ View and Configure Active Directory User Domain Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the Active Directory User Domain settings. For a description of the MIB objects used in this procedure, see "Active Directory User Domain MIB Objects" on page 50.

Follow these steps to view and configure Active Directory User Domain settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **To view the name of Active Directory user domain ID number 2, type:**

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirUserDomain.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirUserDomain.2 = STRING:
<USERNAME>@davidc.example.sun.com
```

3. **To set the name of Active Directory user domain ID number 2 to <USERNAME>@johns.example.sun.com, type:**

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirUserDomain.2 s "<USERNAME>@johns.example.sun.com"
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirUserDomain.2 = STRING:
<USERNAME>@johns.example.sun.com
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirUserDomain.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirUserDomain.2 = STRING:
<USERNAME>@johns.example.sun.com
```

## Active Directory User Domain MIB Objects

The following MIB objects, values, and types are valid for Active Directory User Domain settings.

**TABLE 3-7** Valid MIB Objects, Values, and Types for Active Directory User Domain Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlActiveDirUserDomainId` | An integer identifier of the Active Directory domain. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlActiveDirUserDomain` | This string should match exactly with an authentication domain on the Active Directory server. This string should contain a substitution string (<USERNAME>), which will be replaced with the user's login name during authentication. Either the principle or Distinguished Name format is allowed. | *name* (maximum of 255 characters) | String | None |

# ▼ View and Configure Active Directory Alternate Server Settings

### Before You Begin

- You can use the `get` and `set` commands to set the values of MIB object properties to configure the Active Directory Alternate Server settings. For a description of the MIB objects used in this procedure, see "Active Directory Alternate Server MIB Objects" on page 53.

Follow these steps to view and configure Active Directory Alternate Server settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

- To view the IP address of Active Directory alternate server ID number 2, type:

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerIp.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerIp.2 =
IpAddress: 10.7.143.236
```

- To set the IP address of Active Directory alternate server ID number 2 to 10.7.143.246, type:

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerIp.2 a 10.7.143.246
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerIp.2 =
IpAddress: 10.7.143.246
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerIp.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerIp.2 =
IpAddress: 10.7.143.246
```

- To view the port number of Active Directory alternate server ID number 2, type:

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerPort.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerPort.2 =
INTEGER: 636
```

- To set the port number of Active Directory alternate server ID number 2 to 639, type:

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerPort.2 i 639
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerPort.2 =
INTEGER: 639
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerIp.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerPort.2 =
INTEGER: 639
```

- To view the certificate status of Active Directory alternate server ID number 2, type:

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerCertStatus.2
SUN-ILOM-CONTROL-
MIB::ilomCtrlActiveDirAlternateServerCertStatus.2 = STRING:
certificate not present
```

- To view the certificate URI of Active Directory alternate server ID number 2, type:

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerCertURI.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerCertURI.2 =
STRING: none
```

- To clear the certificate information associated with the server when it is set to true, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerCertClear.0 i 1
```

- To view the certificate version of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerCertVersion.0
```

- To view the serial number of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerCertSerialNo.0
```

- To view the issuer of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerCertIssuer.0
```

- To view the subject of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerCertSubject.0
```

- To view the valid start date of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerCertValidBegin.0
```

- To view the valid end date of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlActiveDirAlternateServerCertValidEnd.0
```

# Active Directory Alternate Server MIB Objects

The following MIB objects, values, and types are valid for Active Directory Alternate Server settings.

**TABLE 3-8** Valid MIB Objects, Values, and Types for Active Directory Alternate Server Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlActive DirAlternate ServerId` | An integer identifier of the Active Directory alternate server table. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlActive DirAlternate ServerIP` | The IP address of the Active Directory alternate server used as a name service for user accounts. | *ipaddress* | String | None |
| `ilomCtrlActive DirAlternate ServerPort` | Specifies the port number for the Active Directory alternate server. Specifying 0 as the port indicates that auto-select will use the well known port number. Specifying 1-65535 is used to explicitly set the port number. | *portnumber* (range: 0 to 65535) | Integer | None |
| `ilomCtrlActive DirAlternate ServerCert Status` | A string indicating the status of the certificate file. This is useful in determining whether a certificate file is present or not. | *status* (maximum size: 255 characters) | String | None |
| `ilomCtrlActive DirAlternate ServerCertURI` | This is the URI of a certificate file needed when Strict Certificate Mode is enabled. Setting the URI causes the transfer of the file, making the certificate available immediately for certificate authentication. Additionally, either `remove` or `restore` are supported for direct certificate manipulation. | *URI* | String | None |

# ▼ View and Configure Redundancy Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure redundancy settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure redundancy settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - To view the status of the server in a redundant configuration, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRedundancyStatus.0
```

   - To view the property that controls whether the server is to be promoted or demoted from active or standby status, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRedundancyAction.0
```

   - To promote a redundant server from standby to active status, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRedundancyAction.0 i 2
```

   - To view the FRU name of the chassis monitoring module (CMM) on which this agent is running, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRedundancyFRUName.0
```

# ▼ View and Configure Active Directory DNS Locator Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the Active Directory DNS Locator settings. For a description of the MIB objects used in this procedure, see "Active Directory DNS Locator MIB Objects" on page 56.

Follow these steps to view and Active Directory DNS Locator settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **To view the state of Active Directory DNS Locator, type:**

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirDnsLocatorEnabled.0
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorEnabled.0 =
INTEGER: false(2)
```

3. **To set the state of Active Directory DNS Locator ID number 2 to enabled, type:**

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirDnsLocatorEnabled.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorEnabled.0 =
INTEGER: true(1)
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirDnsLocatorEnabled.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorEnabled.2 =
INTEGER: true(1)
```

4. **To view the service name of Active Directory DNS Locator ID number 2, type:**

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirDnsLocatorQueryService.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorQueryService.2 =
STRING: _ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>
```

5. **To set the service name and port number of Active Directory DNS Locator ID number 2, type:**

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirDnsLocatorQueryService.2 s
"_ldap._tcp.pdc._msdcs.<DOMAIN>.<PORT:936>"
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorQueryService.2 =
STRING: _ldap._tcp.pdc._msdcs.<DOMAIN>.<PORT:936>
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlActiveDirDnsLocatorQueryService.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorQueryService.2 =
STRING: _ldap._tcp.pdc._msdcs.<DOMAIN>.<PORT:936>
```

## Active Directory DNS Locator MIB Objects

The following MIB objects, values, and types are valid for Active Directory DNS Locator settings.

**TABLE 3-9** Valid MIB Objects, Values, and Types for Active Directory DNS Locator Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlActiveDirDnsLocatorEnabled` | Specifies whether or not the Active Directory DNS Locator functionality is enabled. | `true(1)`, `false(2)` | Integer | false |
| `ilomCtrlActiveDirDnsLocatorQueryId` | An integer identifier of the Active Directory DNS Locator Query entry. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlActiveDirDnsLocatorQueryService` | The service name that is used to perform the DNS query. The name may contain '<DOMAIN>' as a substitution marker, being replaced by the domain information associated for the user at the time of authentication. The service name may also contain '<PORT:> ', which can be used to override any learned port information, if necessary. For example, <PORT:636> may be specified for the standard LDAP/SSL port 636. | *name* (maximum of 255 characters) | String | None |

# Configuring DNS Name Server

## ▼ View and Configure DNS Name Server Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure DNS name server settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure DNS Name Server settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - To view and specify the name server for DNS, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSNameServers.0
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSNameServers.0 s 'nameservername'
```

   - To view and specify the search path for DNS, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSSearchPath.0
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSSearchPath.0 s 'searchpath'
```

   - To view state of DHCP autodns for DNS, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSdhcpAutoDns.0
```

   - To set the state of DHCP autodns for DNS to enabled, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSdhcpAutoDns.0 i 1
```

- To view the number of seconds to wait before timing out if the server does not respond, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSTimeout.0
```

- To set the number of seconds to wait before timing out if the server does not respond to 5, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSTimeout.0 i 5
```

- To view the number of times a request is attempted again after a timeout, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSRetries.0
```

- To set the number of times a request is attempted again after a timeout to 5, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlDNSRetries.0 i 5
```

# Configuring ILOM for LDAP

**Topics**

| Description | Links |
|---|---|
| Configure ILOM for LDAP | • "Configure LDAP Settings" on page 58 |

## ▼ Configure LDAP Settings

### Before You Begin

- You can use the `get` and `set` commands to configure ILOM for LDAP. For a description of the MIB objects used in this procedure, see "ILOM for LDAP MIB Objects" on page 61.

Follow these steps to configure ILOM for LDAP:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   Password**:** *password*

2. **Refer to the following SNMP command examples:**

   - To view whether the LDAP server is enabled to authenticate LDAP users, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapEnabled.0
```

   - To set the LDAP server state to enabled to authenticate LDAP users, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapEnabled.0 i 1
```

   - To view the LDAP server IP address, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapServerIP.0
```

   - To set the LDAP server IP address, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapServerIP.0 a ipaddress
```

   - To view the LDAP server port number, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapPortNumber.0
```

   - To set the LDAP server port number, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapPortNumber.0 i 389
```

   - To view the LDAP server Distinguished Name, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapBindDn.0
```

   - To set the LDAP server Distinguished Name, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapBindDn.0 s ou=people,ou=sales,dc=sun,dc=com
```

- To view the LDAP server password, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapBindPassword.0
```

- To set the LDAP server password, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapBindPassword.0 s password
```

- To view the branch of your LDAP server on which user searches are made, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSearchBase.0
```

- To set the branch of your LDAP server on which to search for users, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSearchBase.0 s ldap_server_branch
```

- To view the LDAP server default role, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapDefaultRoles.0
```

- To set the LDAP server default role to Administrator, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapDefaultRoles.0 s administrator
```

# ILOM for LDAP MIB Objects

The following MIB objects, values, and types are valid for ILOM for LDAP settings.

**TABLE 3-10** Valid MIB Objects, Values, and Types for LDAP Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLdap Enabled` | Specifies whether the LDAP client is enabled. | `true(1), false(2)` | Integer | false |
| `ilomCtrlLdap ServerIP` | The IP address of the LDAP server used as a name service for user accounts. | *ipaddress* | String | None |
| `ilomCtrlLdap PortNumber` | Specifies the port number for the LDAP client. | Range: 0..65535 | Integer | 389 |
| `ilomCtrlLdap BindDn` | The Distinguished Name (DN) for the read-only proxy user used to bind to the LDAP server. For example: cn=proxyuser,ou= people,dc=sun,dc=com" | *distinguished_name* | String | None |
| `ilomCtrlLdap BindPassword` | The password of a read-only proxy user which is used to bind to the LDAP server. This property is essentially write-only. The write-only access level is no longer supported as of SNMPv2. This property must return a null value when read. | *password* | String | None |
| `ilomCtrlLdap SearchBase` | A search base in the LDAP database below which to find users. For example: “ou= people,dc=sun,dc=com" | The branch of your LDAP server on which to search for users | String | None |
| `ilomCtrlLdap DefaultRoles` | Specifies the role that a user authenticated via LDAP should have. 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, c=console, r=reset, o=read-only, and s=service. | `administrator, operator, admin(a), user(u), console(c), reset(r), read-only(o), service(s)` | String | None |

# Configuring ILOM for LDAP/SSL

**Topics**

| Description | Links |
|---|---|
| Configure LDAP/SSL settings | • "Configure LDAP/SSL Settings" on page 62<br>• "View and Configure LDAP/SSL Certificate Settings" on page 66<br>• "View and Configure LDAP/SSL Administrator Groups Settings" on page 67<br>• "View and Configure LDAP/SSL Operator Groups Settings" on page 68<br>• "View and Configure LDAP/SSL Custom Groups Settings" on page 70<br>• "View and Configure LDAP/SSL User Domain Settings" on page 73<br>• "View and Configure LDAP/SSL Alternate Server Settings" on page 74 |

## ▼ Configure LDAP/SSL Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the LDAP/SSL settings. For a description of the MIB objects used in this procedure, see "LDAP/SSL MIB Objects" on page 64.

Follow these steps to configure ILOM for LDAP/SSL.

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - To set the LDAP/SSL state to Enabled to authenticate LDAP/SSL users, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslEnabled.0 i 1
```

- To set the LDAP/SSL IP address, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslIP.0 a ipaddress
```

- To set the LDAP/SSL port number, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslPortNumber.0 i portnumber
```

- To set the LDAP/SSL default user role, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslDefaultRoles.0 s operator
```

- To set the LDAP/SSL certificate file URI, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslCertFileURI.0 s URI
```

- To set the LDAP/SSL timeout, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslTimeout.0 i 6
```

- To set the LDAP/SSL strict certificate enabled value, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslStrictCertEnabled.0 s true
```

- To set the LDAP/SSL certificate file status, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslCertFileStatus.0 s status
```

- To set the LDAP/SSL log detail value to medium, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslLogDetail.0 i 3
```

# LDAP/SSL MIB Objects

The following MIB objects, values, and types are valid for LDAP/SSL settings.

**TABLE 3-11** Valid MIB Objects, Values, and Types (Global Variables) for LDAP/SSL Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLdapSslEnabled` | Specifies whether or not the LDAP/SSL client is enabled. | `true(1), false(2)` | Integer | true |
| `ilomCtrlLdapSslIP` | The IP address of the LDAP/SSL server used as a directory service for user accounts. | *ipaddress* | String | None |
| `ilomCtrlLdapSslPortNumber` | Specifies the port number for the LDAP/SSL client. Specifying 0 as the port means auto-select while specifying 1-65535 configures the actual port value. | *portnumber* (range: 0 to 65535) | Integer | 389 |
| `ilomCtrlLdapSslDefaultRoles` | Specifies the role that a user authenticated via LDAP/SSL should have. Setting this property to legacy roles of 'Administrator' or 'Operator', or any of the individual role IDs of 'a', 'u', 'c', 'r', 'o' and 's' will cause the LDAP/SSL client to ignore the schema stored on the LDAP server. Setting this object to 'none' clears the value and indicates that the native LDAP/SSL schema should be used. The individual role IDs can be joined together in any combination of two or more roles. For example, this object can be set to 'aucros', where a=admin, u=user, c=console, r=reset, o=read-only, and s=service. | `administrator, operator, admin(a), user(u), console(c), reset(r), read-only(o), service(s), none` | String | None |

**TABLE 3-11** Valid MIB Objects, Values, and Types (Global Variables) for LDAP/SSL Settings *(Continued)*

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLdapSslCertFileURI` | The TFTP URI of the LDAP/SSL server's certificate file that should be uploaded in order to perform certificate validation. Setting the URI causes the transfer of the specified file, making the certificate available immediately for certificate authentication. The server certificate file is needed when Strict Certificate Mode is enabled. Additionally, either `remove` or `restore` are supported for direct certificate manipulation. | *URI* | String | None |
| `ilomCtrlLdapSslTimeout` | Specifies the number of seconds to wait before timing out if the LDAP/SSL server is not responding. | Range: 1 to 20 | Integer | 4 |
| `ilomCtrlLdapSslStrictCertEnabled` | Specifies whether or not the Strict Certificate Mode is enabled for the LDAP/SSL Client. If enabled, the LDAP/SSL server's certificate must be uploaded to the SP so that certificate validation can be performed when communicating with the LDAP/SSL server. | `true(1)`, `false(2)` | Integer | true |
| `ilomCtrlLdapSslCertFileStatus` | A string indicating the status of the certificate file. This is useful in determining whether a certificate file is present or not. | *status* (maximum size: 255 characters) | String | None |
| `ilomCtrlLdapSslLogDetail` | Controls the amount of messages sent to the event log. The high priority has the least number of messages going to the log, while the lowest priority 'trace' has the most messages logged. When this object is set to `none`, no messages are logged. | `none(1)`, `high(2)`, `medium(3)`, `low(4)`, `trace(5)` | Integer | None |

# ▼ View and Configure LDAP/SSL Certificate Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure LDAP/SSL certificate settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

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

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - To clear the certificate information associated with the server when it is set to true, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslCertFileClear.0 i 0
```

   - To view the certificate version of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslCertFileVersion.0
```

   - To view the serial number of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslCertFileSerialNo.0
```

   - To view the issuer of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslCertFileIssuer.0
```

   - To view the subject of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslCertFileSubject.0
```

- To view the valid start date of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslCertFileValidBegin.0
```

- To view the valid end date of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslCertFileValidEnd.0
```

# ▼ View and Configure LDAP/SSL Administrator Groups Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the LDAP/SSL Administrator Groups settings. For a description of the MIB objects used in this procedure, see "LDAP/SSL Administrator Groups MIB Objects" on page 68.

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

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - To view the name of LDAP/SSL administrator group ID number 3, type:

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslAdminGroupName.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAdminGroupName.3 = STRING:
CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
```

   - To set the name of LDAP/SSL administrator group ID number 3 to CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=sun,DC=com, type:

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslAdminGroupName.3 s CN=SpSuperAdmin,OU=
Groups,DC=tomp,DC=example,DC=sun,DC=com
```

```
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAdminGroupName.3 = STRING:
CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=sun,DC=com
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslAdminGroupName.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAdminGroupName.3 = STRING:
CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=sun,DC=com
```

## LDAP/SSL Administrator Groups MIB Objects

The following MIB objects, values, and types are valid for LDAP/SSL Administrator Groups settings.

**TABLE 3-12** Valid MIB Objects, Values, and Types for LDAP/SSL Administrator Groups Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLdapSslAdminGroupId` | An integer identifier of the LDAP/SSL AdminGroup entry. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlLdapSslAdminGroupName` | This string should contain a Distinguished Name that exactly matches one of the group names on the LDAP/SSL server. Any user belonging to one of these groups in this table will be assigned the ILOM role of Administrator. | *name* (maximum of 255 characters) | String | None |

# ▼ View and Configure LDAP/SSL Operator Groups Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the LDAP/SSL Operator Groups settings. For a description of the MIB objects used in this procedure, see "LDAP/SSL Operator Groups MIB Objects" on page 70.

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

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   Password**:** *password*

2. **Refer to the following SNMP command examples:**

   - To view the name of LDAP/SSL operator group ID number 3, type:

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslOperatorGroupName.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslOperatorGroupName.3 =
STRING: CN=SpSuperOper,OU=Groups,DC=davidc,DC=example,DC=
sun,DC=com
```

   - To set the name of Active Directory operator group ID number 3 to CN= SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=sun,DC=com, type:

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslOperatorGroupName.3 s CN=SpSuperOper,OU=
Groups,DC=tomp,DC=example,DC=sun,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslOperatorGroupName.3 =
STRING: CN=SpSuperOper,OU=Groups,DC=tomp,DC=example,DC=sun,DC=
com
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslOperatorGroupName.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslOperatorGroupName.3 =
STRING: CN=SpSuperOper,OU=Groups,DC=tomp,DC=example,DC=sun,DC=
com
```

## LDAP/SSL Operator Groups MIB Objects

The following MIB objects, values, and types are valid for LDAP/SSL Operator Groups settings.

**TABLE 3-13** Valid MIB Objects, Values, and Types for LDAP/SSL Operator Groups Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLdapSslOperatorGroupId` | An integer identifier of the LDAP/SSL Operator Group entry. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlLdapSslOperatorGroupName` | This string should contain a Distinguished Name that exactly matches one of the group names on the LDAP/SSL server. Any user belonging to one of these groups in this table will be assigned the ILOM role of Operator. | *name* (maximum of 255 characters) | String | None |

# ▼ View and Configure LDAP/SSL Custom Groups Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the LDAP/SSL Custom Groups settings. For a description of the MIB objects used in this procedure, see "LDAP/SSL Custom Groups MIB Objects" on page 72.

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

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

- To view the name of LDAP/SSL custom group ID number 2, type:

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslCustomGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupName.2 = STRING:
CN=SpSuperCust,OU=Groups,DC=johns,DC=sun,DC=com
```

- To set the name of LDAP/SSL custom group ID number 2 to CN= SpSuperCust,OU=Groups,DC=bills,DC=sun,DC=com, type :

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslCustomGroupName.2 s CN=SpSuperCust,OU=Groups,DC=
bills,DC=sun,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupName.2 = STRING:
CN=SpSuperCust,OU=Groups,DC=bills,DC=sun,DC=com
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslCustomGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupName.2 = STRING:
CN=SpSuperCust,OU=Groups,DC=bills,DC=sun,DC=com
```

- To view the roles of LDAP/SSL custom group ID number 2, type:

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslCustomGroupRoles.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupRoles.2 = STRING:
"aucro"
```

- To set the roles of LDAP/SSL custom group ID number 2 to User Management and Read Only (u,o), type:

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslCustomGroupRoles.2 s "uo"
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupRoles.2 = STRING:
"uo"
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslCustomGroupRoles.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupRoles.2 = STRING:
"uo"
```

# LDAP/SSL Custom Groups MIB Objects

The following MIB objects, values, and types are valid LDAP/SSL Custom Groups settings.

**TABLE 3-14** Valid MIB Objects, Values, and Types for LDAP/SSL Custom Groups Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLdapSslCustomGroupId` | An integer identifier of the LDAP/SSL custom group entry. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlLdapSslCustomGroupName` | This string should contain a Distinguished Name that exactly matches one of the group names on the LDAP/SSL server. Any user belonging to one of these groups in this table will be assigned the ILOM role based on the entry's configuration for roles. | *name* (maximum of 255 characters) | String | None |
| `ilomCtrlLdapSslCustomGroupRoles` | Specifies the role that a user authenticated via LDAP/SSL should have. Setting this property to legacy roles of 'Administrator' or 'Operator', or any of the individual role IDs of 'a', 'u', 'c', 'r', 'o' and 's' will cause the LDAP/SSL client to ignore the schema stored on the LDAP/SSL server. Setting this object to 'none' clears the value and indicates that the native LDAP/SSL schema should be used. The role IDs can be joined together. For example, 'aucros,' where a=admin, u=user, c= console, r=reset, o=read-only, and s=service. | `administrator`, `operator`, `admin(a)`, `user(u)`, `console(c)`, `reset(r)`, `read-only(o)`, `service(s)`, `none` | String | None |

# ▼ View and Configure LDAP/SSL User Domain Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the LDAP/SSL User Domain settings. For a description of the MIB objects used in this procedure, see "LDAP/SSL User Domain MIB Objects" on page 74.

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

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username***`@`***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - To view the name of LDAP/SSL user domain ID number 3, type:

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslUserDomain.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslUserDomain.3 = STRING: CN=
<USERNAME>,CN=Users,DC=davidc,DC=example,DC=sun,DC=com
```

   - To set the name of LDAP/SSL user domain ID number 3 to CN=<USERNAME>, CN=Users,DC=tomp,DC=example,DC=sun,DC=com, type:

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslUserDomain.3 s CN=<USERNAME>,CN=Users,DC=
tomp,DC=example,DC=sun,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslUserDomain.3 = STRING: CN=
<USERNAME>,CN=Users,DC=tomp,DC=example,DC=sun,DC=com
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslUserDomain.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslUserDomain.3 = STRING: CN=
<USERNAME>,CN=Users,DC=tomp,DC=example,DC=sun,DC=com
```

## LDAP/SSL User Domain MIB Objects

The following MIB objects, values, and types are valid for LDAP/SSL User Domain settings.

**TABLE 3-15** Valid MIB Objects, Values, and Types for LDAP/SSL User Domain Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLdapSslUserDomainId` | An integer identifier of the LDAP/SSL domain. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlLdapSslUserDomain` | This string should match exactly with an authentication domain on the LDAP/SSL server. This string should contain a substitution string (<USERNAME>), which will be replaced with the user's login name during authentication. Either the principle or Distinguished Name format is allowed. | *name* (maximum of 255 characters) | String | None |

# ▼ View and Configure LDAP/SSL Alternate Server Settings

### Before You Begin

- You can use the `get` and `set` commands to configure the LDAP/SSL Alternate Server settings. For a description of the MIB objects used in this procedure, see "LDAP/SSL Alternate Server MIB Objects" on page 76 and the SUN-ILOM-CONTROL MIB.

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

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

- To view the IP address of LDAP/SSL alternate server ID number 3, type:

```
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerIp.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAlternateServerIp.3 =
IpAddress: 10.7.143.236
```

- To set the IP address of LDAP/SSL alternate server ID number 3 to 10.7.143.246, type:

```
% snmpset -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerIp.3 a 10.7.143.246
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAlternateServerIp.3 =
IpAddress: 10.7.143.246
% snmpget -v1 -cprivate -mALL SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerIp.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAlternateServerIp.3 =
IpAddress: 10.7.143.246
```

- To view and clear the certificate information associated with the alternate server when it is set to true, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerCertClear.0
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerCertClear.0 i 0
```

- To view the alternate server certificate version of the certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerCertVersion.0
```

- To view the serial number of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerCertSerialNo.0
```

- To view the issuer of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerCertIssuer.0
```

- To view the subject of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerCertSubject.0
```

- To view the valid start date of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerCertValidBegin.0
```

- To view the valid end date of the alternate server certificate file, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlLdapSslAlternateServerCertValidEnd.0
```

## LDAP/SSL Alternate Server MIB Objects

The following MIB objects, values, and types are valid for LDAP/SSL Alternate Server settings.

**TABLE 3-16** Valid MIB Objects, Values, and Types for LDAP/SSL Alternate Server Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLdapSslAlternateServerId` | An integer identifier of the LDAP/SSL alternate server table. | 1 to 5<br>**Note -** This object is not accessible for reading or writing. | Integer | None |
| `ilomCtrlLdapSslAlternateServerIP` | The IP address of the LDAP/SSL alternate server used as directory server for user accounts. | *ipaddress* | String | None |

**TABLE 3-16** Valid MIB Objects, Values, and Types for LDAP/SSL Alternate Server Settings *(Continued)*

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlLdapSslAlternateServerPort` | Specifies the port number for the LDAP/SSL alternate server. Specifying zero as the port indicates that auto-select will use the well known port number. Specifying 1-65535 is used to explicitly set the port number. | *portnumber* (range: 0 to 65535) | Integer | None |
| `ilomCtrlLdapSslAlternateServerCertStatus` | A string indicating the status of the certificate file. This is useful in determining whether a certificate file is present or not. | *status* (maximum size: 255 characters) | Sting | None |
| `ilomCtrlLdapSslAlternateServerCertURI` | This is the URI of a certificate file needed when Strict Certificate Mode is enabled. Setting the URI causes the transfer of the file, making the certificate available immediately for certificate authentication. Additionally, either `remove` or `restore` are supported for direct certificate manipulation. | *URI* | String | None |

# Configuring RADIUS Settings

## ▼ Configure RADIUS Settings

### Before You Begin

- Before completing this procedure, collect the appropriate information about your RADIUS environment.
- You can use the `get` and `set` commands to configure RADIUS. For a description of the MIB objects used in this procedure, see "RADIUS MIB Objects" on page 79.

Follow these steps to configure RADIUS settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - To view whether the RADIUS server is enabled to authenticate RADIUS users, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusEnabled.0
```

   - To set the RADIUS server state to Enabled to authenticate RADIUS users, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusEnabled.0 i 1
```

   - To view the RADIUS server IP address, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusServerIP.0
```

   - To set the RADIUS server IP address, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusServerIP.0 a ipaddress
```

   - To view the RADIUS server port number, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusPortNumber.0
```

   - To set the RADIUS server port number, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusPortNumber.0 i portnumber
```

   - To view the RADIUS server shared secret, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusSecret.0
```

- To set the RADIUS server shared secret, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusSecret.0 s secret
```

- To view the RADIUS server default user roles, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusDefaultRoles.0
```

- To set the RADIUS server default user roles to console, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlRadiusDefaultRoles.0 s c
```

## RADIUS MIB Objects

The following MIB objects, values, and types are valid for RADIUS settings.

**TABLE 3-17** Valid MIB Objects, Values, and Types for RADIUS Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlRadiusEnabled` | Specifies whether or not the RADIUS client is enabled. | `true(1)`, `false(2)` | Integer | false |
| `ilomCtrlRadiusServerIP` | The IP address of the RADIUS server used as a name service for user accounts. | *ipaddress* | String | None |
| `ilomCtrlRadiusPortNumber` | Specifies the port number for the RADIUS client. | *portnumber* (range: 0 to 65535) | Integer | 1812 |
| `ilomCtrlRadiusSecret` | The shared secret encryption key that is used to encrypt traffic between the RADIUS client and server. | *secret* (maximum length: 255 characters) | Sting | None |
| `ilomCtrlRadiusDefaultRoles` | Specifies the role that a user authenticated via RADIUS should have. 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, 'aucro', where a=admin, u=user, c= console, r=reset, o=read-only, and s=service. | `administrator`, `operator`, `admin(a)`, `user(u)`, `console(c)`, `reset(r)`, `read-only(o)`, `service(s)` | String | None |

CHAPTER 4

# Inventory and Component Management

**Topics**

| Description | Links |
|---|---|
| Review the prerequisites | • "Before You Begin" on page 82 |
| View component information and manage inventory | • "View Component Information" on page 83<br>• "View and Set Clock Settings" on page 85<br>• "View and Clear the ILOM Event Log" on page 86<br>• "Configure Remote Syslog Receiver IP Addresses" on page 88 |
| Manage alert rules | • "Configure an Alert Rule" on page 89 |
| Configure SMTP client for email notification alerts | • "Configure SMTP Client for Email Notification Alerts" on page 91 |
| Configure alerts | • "View and Configure Email Alert Settings" on page 93 |
| Configure Telemetry Harness Daemon | • "View and Configure Telemetry Harness Daemon Settings" on page 94 |

**Related Topics**

| For ILOM | Section | Guide |
|---|---|---|
| • Concepts | • System Monitoring and Alert Management | *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* |
| • CLI | • Managing Alerts | *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* |
| • Web | • Managing Alerts | *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* |

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

# Before You Begin

- Before you can use SNMP to view and configure ILOM settings, you must configure SNMP. For more information, see "Preparing Your System to Use SNMP" on page 3.
- When executing the `snmpset` command, you need to use a v1/v2c community or a v3 user with read/write (rw) privileges.

**Note –** The example SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will only work as presented if you have Net-SNMP and the Net-SNMP sample applications installed.

# Viewing Component Information

**Topics**

| Description | Links |
|---|---|
| View the component information | • "View Component Information" on page 83<br>• "Component MIB Objects" on page 83 |

# ▼ View Component Information

### Before You Begin

- You can use `get` commands to view component information. For a description of the MIB objects used in this procedure, see "Component MIB Objects" on page 83.

Follow these steps to view component information:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username***`@`***snmp_manager_ip_address*

   `Password:` *password*

2. **To view the firmware revision, type:**

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ip_address
entPhysicalFirmwareRev.1
```

## Component MIB Objects

TABLE 4-1 lists several of the MIB objects provided by the ENTITY-MIB that you can use to view components.

**TABLE 4-1** MIB Objects, Values, and Types for Component Settings

| MIB Object | Description | Values | Type | Default |
|---|---|---|---|---|
| `entPhysical Name` | The textual name of the physical entity. | Size: 0..255 | String | Zero-length string |
| `entPhysical Descr` | A textual description of physical entity. | Size: 0..255 | String | None |

**TABLE 4-1** MIB Objects, Values, and Types for Component Settings *(Continued)*

| MIB Object | Description | Values | Type | Default |
|---|---|---|---|---|
| `entPhysical ContainedIn` | The value of entPhysicalIndex for the physical entity that *contains* this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity. | Range: 0..2147483647 | Integer | None |
| `entPhysical Class` | An indication of the general hardware type of the physical entity. | `other(1), unknown(2), chassis(3), backplane(4), container(5), powerSupply(6), fan(7), sensor(8), module(9), port(10), stack(11)` | Integer | None |
| `entPhysical FirmwareRev` | The vendor-specific firmware revision string for the physical entity. | Size: 0..255 | String | Zero-length string |

# Monitoring System Sensors, Indicators, and ILOM Event Log

**Topics**

| Description | Links |
|---|---|
| View and set clock settings | • "View and Set Clock Settings" on page 85 |
| View and clear the ILOM event log | • "View and Clear the ILOM Event Log" on page 86 |
| Configure remote syslog receiver IP addresses | • "Configure Remote Syslog Receiver IP Addresses" on page 88 |
| Configure alert rules | • "Configure an Alert Rule" on page 89 |

# ▼ View and Set Clock Settings

### Before You Begin

- You can use the `get` and `set` commands to view and set clock settings with respect to Network Time protocol (NTP) synchronization. For a description of the MIB objects used in this procedure, see "ILOM Clock Setting MIB Objects" on page 86.

Follow these steps to view and configure clock settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username***`@`***snmp_manager_ip_address*

   `Password:` *password*

2. **Refer to the following SNMP commands for examples:**

   - To view the NTP server state, type:

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlNTPEnabled.0
```

   - To set the NTP server state to enabled, type:

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlNTPEnabled.0 i 1
```

   - To view the date and time of the device, type:

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlDateAndTime.0
```

   - To set the date and time of the device, type:

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlDateAndTime.0 s 2008-3-24,4:59:47.0
```

## ILOM Clock Setting MIB Objects

The following MIB objects, values, and types are valid for ILOM clock settings.

**TABLE 4-2** Valid MIB Objects, Values, and Types for ILOM Clock Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlDateAndTime` | The date and time of the device. | *date/time* | String | None |
| `ilomCtrlNTPEnabled` | Specifies whether the Network Time Protocol is enabled. | `true(1)`, `false(2)` | Integer | false |
| `ilomCtrlTimezone` | The configured timezone string. | Size: 0..255 | String | None |

# ▼ View and Clear the ILOM Event Log

### Before You Begin

- You can use the `get` command to view the ILOM event log and the `set` command to configure the ILOM event log. For a description of the MIB objects used in this procedure, see "ILOM Event Log MIB Objects" on page 87.

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

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ip_address*

   `Password:` *password*

2. **To view the ILOM event log type for an event log with a record ID of 2, type:**

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlEventLogType.2
```

3. **To clear the ILOM event log, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlEventLogClear.0 i 1
```

# ILOM Event Log MIB Objects

The following MIB objects, values, and types are valid for ILOM event log settings.

**TABLE 4-3** MIB Objects, Values, and Types for Event Log Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlEventLog RecordID` | The record number for a given event log entry.<br>**Note -** This object is not accessible. | Range: 1..10000 | Integer | None |
| `ilomCtrlEventLog Type` | An integer representing the type of event.<br>**Note -** This object is read-only. | `log(1), action2), fault(3), state(4), repair(5)` | Integer | None |
| `ilomCtrlEventLog Timestamp` | The date and time that the event log entry was recorded.<br>**Note -** This object is read-only. | *date/time* | String | None |
| `ilomCtrlEventLog Class` | An integer representing the class of event.<br>**Note -** This object is read-only. | `audit(1), ipmi(2), chassis(3), fma(4), system(5) pcm(6)` | Integer | None |
| `ilomCtrlEventLog Severity` | The event severity corresponding to the given log entry.<br>**Note -** This object is read-only. | `disable(1), critical(2), major(3), minor(4), down(5` | Integer | None |
| `ilomCtrlEventLog Description` | A textual description of the event.<br>**Note -** This object is read-only. | *description* | String | None |
| `ilomCtrlEventLog Clear` | Setting this object to true clears the event log. | `true(1), false(2)` | Integer | None |

# ▼ Configure Remote Syslog Receiver IP Addresses

### Before You Begin

- You can use the `get` and `set` commands to view and set IP addresses for a remote Syslog receiver. For a description of the MIB objects used in this procedure, see "Remote Syslog Receiver IP Addresses MIB Objects" on page 88.

Follow these steps to view and configure remote syslog receiver IP addresses:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username@snmp_manager_ip_address*

   `Password:` *password*

2. **To view a remote syslog destination IP address, type:**

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlRemoteSyslogDest1.0
```

3. **To set a remote syslog destination IP address, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlRemoteSyslogDest1.0 s ip_address
```

## Remote Syslog Receiver IP Addresses MIB Objects

The following MIB objects, values, and types are valid for remote syslog receiver IP addresses.

**TABLE 4-4** MIB Objects, Values, and Types for Remote Syslog Receiver IP Addresses

| MIB Object | Description | Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlRemote SyslogDest1` | The IP address of the first remote syslog destination (log host). | *ip_address* | String | None |
| `ilomCtrlRemote SyslogDest2` | The IP address of the second remote syslog destination (log host). | *ip_address* | String | None |

# ▼ Configure an Alert Rule

### Before You Begin

- You can use the `get` and `set` commands to view and configure alert rule configurations. For a description of the MIB objects used in this procedure, see "Alert Rule Configuration MIB Objects" on page 90.

Follow these steps to configure an alert rule:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ip_address*

   `Password:` *password*

2. **To view the severity level for the alert rule with an AlertID of 2, type:**

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlAlertSeverity.2
```

3. **To set the severity level to critical for the alert rule with an AlertID of 2, type:**

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlAlertSeverity.2 i 2
```

# Alert Rule Configuration MIB Objects

The following MIB objects, values, and types are valid for alert rule settings.

**TABLE 4-5** MIB Objects, Values, and Types for Alert Rule Settings

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlAlertID` | An integer ID associated with a given alert rule.<br>**Note -** This object is not accessible. | Range: 0..65535 | Integer | None |
| `ilomCtrlAlertSeverity` | Specifies the minimum event severity that should trigger an alert for a given class. | `disable(1)`, `critical(2)`, `major(3)`, `minor(4)`, `down(5)` | Integer | None |
| `ilomCtrlAlertType` | Specifies the type of notification for a given alert. If the type is `snmptrap(2)` or `ipmipet(3)`, the `ilomCtrlAlertDestinationip` must be specified. If the type is `email(1)`, the `ilomCtrlAlertDestinationEmail` must be specified. | `email(1)` `snmptrap(2)` `ipmipet(3)` `remotesyslog(4)` | Integer | None |
| `ilomCtrlAlertDestinationip` | Specifies the IP address to send alert notifications when the alert type is `snmptrap(2)`, `ipmipet(3)`, or `remotesyslog(4)`. | *ip_address* | String | None |
| `ilomCtrlAlertDestinationEmail` | Specifies the email address to send alert notifications when the alert type is `email(1)`. | *email address*, size: 0..255 | String | None |
| `ilomCtrlAlertSNMPVersion` | Specifies the version of SNMP trap that should be used for the given alert rule. | `v1(1)`, `v2c(2)`, `v3(3)` | Integer | None |

**TABLE 4-5** MIB Objects, Values, and Types for Alert Rule Settings *(Continued)*

| MIB Object | Description | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlAlert SNMPCommunity OrUsername` | Specifies the community string to be used when the `ilomCtrlAlertSNMPVersion` property is set to `v1(1)` or `v2c(2)`. Specifies the SNMP user name to use when the `ilomCtrlAlertSNMPVersion` is set to `v3(3)`. | Size: 0..255 | String | None |
| `ilomCtrlAlert EmailEvent ClassFilter` | A class name or `all` to filter emailed alerts on. | Size: 0..255 | String | None |
| `ilomCtrlAlert EmailEventType Filter` | A class name or `all` to filter emailed alerts on. | Size 0..255 | String | None |

# Configuring SMTP Client for Email Notification Alerts

To generate configured Email Notification alerts, you must enable the ILOM client to act as an SMTP client to send the email alert messages. To enable the ILOM client as an SMTP client, you must specify the IP address and port number of an outgoing SMTP email server that will process the email notifications.

## ▼ Configure SMTP Client for Email Notification Alerts

### Before You Begin

- Prior to enabling the ILOM client as an SMTP client, gather the IP address and port number of the outgoing SMTP email server.
- You can use the `get` and `set` commands to configure the SMTP client. For a description of the MIB objects used in this procedure, see "SMTP Client MIB Objects" on page 93 and the SUN-ILOM-CONTROL-MIB.

Follow these steps to configure an SMTP client:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ip_address*

   `Password:` *password*

2. **Refer to the following SNMP commands for examples:**

   - To view a SMTP client state, type:

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlSMTPEnabled.0
```

   - To set a SMTP client state to enabled, type:

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlSMTPEnabled.0 i 1
```

   - To view a SMTP server IP address, type:

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlSMTPServerip.0
```

   - To set a SMTP server IP address, type:

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlSMTPServerip.0 s ip_address
```

   - To view a SMTP client port number, type:

```
% snmpget -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlSMTPPortNumber.0
```

   - To set a SMTP client port number, type:

```
% snmpset -v2c -cprivate -mALL SNMP_agent_ip_address
ilomCtrlSMTPPortNumber.0 i 25
```

   - To view an optional format to identify the sender or the 'from' address, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSMTPCustomSender.0
```

- To configure an optional format to identify the sender or the 'from' address, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSMTPCustomSender.0 s 'ilom-alert@HOSTNAME.abc.com'
```

## SMTP Client MIB Objects

The following MIB objects, values, and types are valid settings for SMTP clients.

**TABLE 4-6** Valid MIB Objects, Values, and Types for SMTP Clients

| MIB Object | Property | Allowed Values | Type | Default |
|---|---|---|---|---|
| `ilomCtrlSMTP Enabled` | Specifies whether or not the SMTP client is enabled. | `true(1), false(2)` | Integer | false |
| `ilomCtrlSMTP Serverip` | The IP address of the SMTP server used as a name service for user accounts. | *ip_address* | String | None |
| `ilomCtrlSMTP PortNumber` | Specifies the port number for the SMTP client. | Range: 0..65535 | Integer | None |

# Configuring Email Alert Settings

## ▼ View and Configure Email Alert Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure email alert settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure email alert settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username***`@`***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

- To view the optional format used to identify the sender or the 'from' address, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlAlertEmailCustomSender.0
```

- To set the optional format used to identify the sender or the 'from' address, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlAlertEmailCustomSender.0 s 'ilom-
alert@HOSTNAME.abc.com'
```

- To view an optional string that can be added to the beginning of the message body, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlAlertEmailMessagePrefix.0
```

- To define an optional string (for example: BeginMessage) that can be added to the beginning of the message body, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlAlertEmailMessagePrefix.0 s 'BeginMessage'
```

# ▼ View and Configure Telemetry Harness Daemon Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure Telemetry Harness Daemon (THD) settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure THD settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username*@*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

- To view the state of the THD daemon, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdState.0
```

- To view the control action for THD daemon, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdAction.0
```

- To set the control action for THD daemon to `suspend`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdAction.0 i 1
```

- To view the description of the THD module named `THDMod1`, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdModuleDesc.'THDMod1'
```

- To view the state of the THD module named `THDMod1`, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdModuleState.'THDMod1'
```

- To view the control action for the THD module named `THDMod1`, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdModuleAction.'THDMod1'
```

- To set the control action for the THD module named `THDMod1` to `suspend`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdModuleAction.0 i 1
```

- To view the state of the THD instance named `myTHDinstance` that is in the THD class named `myTHDclase`, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdInstanceState.'myTHDclass.myTHDinstance'
```

- To view the action of the THD instance named `myTHDinstance` that is in the THD class named `myTHDclase`, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdInstanceAction.'myTHDclass.myTHDinstance'
```

- To set the action of the THD instance named `myTHDinstance` that is in the THD class named `myTHDclase` to `resume`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlThdInstanceAction.'myTHDclass.myTHDinstance' i 2
```

CHAPTER 5

# Monitoring Power Consumption

**Topics**

| Description | Links |
|---|---|
| Review the prerequisites | • "Before You Begin" on page 98 |
| Monitor the power consumption interfaces | • "Monitor System Total Power Consumption" on page 99<br>• "Monitor Actual Power Consumption" on page 100<br>• "Monitor Individual Power Supply Consumption" on page 100<br>• "Monitor Available Power" on page 102<br>• "Monitor Hardware Configuration Maximum Power Consumption" on page 102<br>• "Monitor Permitted Power Consumption" on page 102<br>• "Monitor Power Management Settings" on page 102 |
| View and set power policy | • "View and Set the Power Policy" on page 103 |

**Related Topics**

| For ILOM | Section | Guide |
|---|---|---|
| • Concepts | • Power Monitoring and Management Interfaces | *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* |
| • Web | • Monitoring Power Consumption | *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* |
| • CLI | • Monitoring Power Consumption | *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/`

# Before You Begin

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

- Before you can use SNMP to view and configure ILOM settings, you must configure SNMP. For more information, see "Preparing Your System to Use SNMP" on page 3.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user with read/write (rw) privileges.

**Note –** The example SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will only work as presented if you have Net-SNMP and the Net-SNMP sample applications installed.

# Monitoring the Power Consumption Interfaces

**Topics**

| Description | Links |
|---|---|
| Monitor the power consumption interfaces | • "Monitor System Total Power Consumption" on page 99<br>• "Monitor Actual Power Consumption" on page 100<br>• "Monitor Individual Power Supply Consumption" on page 100<br>• "Monitor Available Power" on page 102<br>• "Monitor Hardware Configuration Maximum Power Consumption" on page 102<br>• "Monitor Permitted Power Consumption" on page 102 |
| View and set power policy | • "View and Set the Power Policy" on page 103 |

**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 Total Power Consumption

- **To view total system power consumption using SNMP, type this command:**

```
% snmpget -v2c -cprivate -mALL snmp_agent_ipaddress
entPhysicalName.308
```

## ▼ Monitor Actual Power Consumption

- **To view actual power consumption using SNMP, type this command:**

```
% snmpget -v2c -cprivate -mALL snmp_agent_ipaddress
sunHwCtrlPowerMgmtActual.0
```

## ▼ Monitor Individual Power Supply Consumption

Before you can use SNMP to monitor individual power supply consumption, you must determine the `entPhysicalName` index numbers that correspond to the output and input power sensors for a particular power supply.

- **To view the individual power supply consumption, type a command similar to the following command.**

  For example, if you know that the `entPhysicalIndex` of `/SYS/VPS` is 303, you can view total output power consumption by typing the following command:

```
% snmpget -v2c -cprivate -mALL snmp_agent_ipaddress \
  entPhysicalName.303 \
  entPhysicalClass.303 \
  entPhysicalDescr.303 \
  sunPlatNumericSensorBaseUnits.303 \
  sunPlatNumericSensorExponent.303 \
  sunPlatNumericSensorCurrent.303 \
  sunPlatNumericSensorLowerThresholdNonCritical.303 \
  sunPlatNumericSensorUpperThresholdNonCritical.303 \
  sunPlatNumericSensorLowerThresholdCritical.303 \
  sunPlatNumericSensorUpperThresholdCritical.303 \
  sunPlatNumericSensorLowerThresholdFatal.303 \
  sunPlatNumericSensorUpperThresholdFatal.303
```

TABLE 5-1 provides a brief description of each of the MIB objects included in the above command example. For more information, see the ENTITY-MIB and the SUN-PLATFORM-MIB.

**TABLE 5-1** Individual Power Supply Consumption MIB Objects

| MIB Object | MIB Name | Description |
|---|---|---|
| `entPhysicalName` | ENTITY-MIB | The textual name of the physical entity. |
| `entPhysicalClass` | ENTITY-MIB | The general hardware type of the physical entity. |
| `entPhysicalDescr` | ENTITY-MIB | A textual description of physical entity. |

**TABLE 5-1** Individual Power Supply Consumption MIB Objects *(Continued)*

| MIB Object | MIB Name | Description |
|---|---|---|
| sunPlatNumeric SensorBaseUnits | SUN-PLATFORM-MIB | The base unit of the values returned by this sensor as per CIM_NumericSensor.BaseUnits. |
| sunPlatNumeric SensorExponent | SUN-PLATFORM-MIB | The exponent to be applied to the units returned by this sensor as for CIM_NumericSensor.UnitModifier. |
| sunPlatNumeric SensorCurrent | SUN-PLATFORM-MIB | The sunPlatDiscreteSensorStatesIndex of a row in the sunPlatDiscreteSensorStatesTable that corresponds to the current reading of the sensor. |
| sunPlatNumeric SensorLower ThresholdNon Critical | SUN-PLATFORM-MIB | The lower threshold at which a NonCritical condition occurs as defined for CIM_NumericSensor.LowerThreshold NonCritical. |
| sunPlatNumeric SensorUpper ThresholdNon Critical | SUN-PLATFORM-MIB | The upper threshold at which a NonCritical condition occurs as defined for CIM_NumericSensor.UpperThreshold NonCritical. |
| sunPlatNumeric SensorLower ThresholdCritical | SUN-PLATFORM-MIB | The lower threshold at which a Critical condition occurs as defined for CIM_NumericSensor.LowerThreshold Critical. |
| sunPlatNumeric SensorUpper ThresholdCritical | SUN-PLATFORM-MIB | The upper threshold at which a Critical condition occurs as defined for CIM_NumericSensor.UpperThreshold Critical. |
| sunPlatNumeric SensorLower ThresholdFatal | SUN-PLATFORM-MIB | The lower threshold at which a Fatal condition occurs as defined for CIM_NumericSensor.LowerThreshold Fatal. |
| sunPlatNumeric SensorUpper ThresholdFatal | SUN-PLATFORM-MIB | The upper threshold at which a Fatal condition occurs as defined for CIM_NumericSensor.UpperThreshold Fatal. |

## ▼ Monitor Available Power

- **To view total available power using SNMP, type this command:**

```
% snmpget -v2c -cprivate -mALL snmp_agent_ipaddress
sunHwCtrlPowerMgmtAvailablePower.0
```

## ▼ Monitor Hardware Configuration Maximum Power Consumption

- **To view the hardware configuration maximum power consumption using SNMP, type this command:**

```
% snmpget -v2c -cprivate -mALL snmp_agent_ipaddress
sunPlatCtrlPowerMgmtHWConfigPower.0
```

## ▼ Monitor Permitted Power Consumption

- **To view permitted power consumption using SNMP, type this command:**

```
% snmpget -v2c -cprivate -mALL snmp_agent_ipaddress
sunHwCtrlPowerMgmtPermittedPower.0
```

## ▼ Monitor Power Management Settings

### Before You Begin

- You can use the `get` command to view power management settings. For a description of the MIB objects used in these commands, see the SUN-HW-CTRL-MIB.

Follow these steps to view power management settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username*@*snmp_manager_ipaddress*

   **Password:** *password*

2. **Refer to the following SNMP command examples:**

- To view the name of the power management policy for `PowerMgmtTable` index number 5, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
sunHwCtrlPowerMgmtName.5
```

- To view the units for the value of the power management policy for `PowerMgmtTable` index number 5, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
sunHwCtrlPowerMgmtUnits.5
```

- To view the value of the power management policy for `PowerMgmtTable` index number 5, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
sunHwCtrlPowerMgmtValue.5
```

# Using the Power Consumption Control Interfaces

**Topics**

| Description | Links |
|---|---|
| View and set power policy | • "View and Set the Power Policy" on page 103 |

## ▼ View and Set the Power Policy

### Before You Begin

- You can use the `get` and `set` commands to view and set power policy.

**1. To view the power policy using SNMP, type this command:**

```
% snmpget -v2c -cprivate -mALL snmp_agent_ipaddress
sunHwCtrlPowerMgmtPolicy.0
```

2. **To set the power policy, use the** `snmpset` **command.**

   For example, to set this MIB object to `performance`, type this command:

```
% snmpset -v2c -cprivate -mALL snmp_agent_ipaddress
sunHwCtrlPowerMgmtPolicy.0 i 3
```

TABLE 5-2 shows the MIB object type and values that are supported by the `sunHwCtrlPowerMgmtPolicy` MIB object.

**TABLE 5-2** Valid Values and Type for the sunHwCtrlPowerMgmtPolicy MIB Object

| MIB Object | Values | Type | Default |
|---|---|---|---|
| `sunHwCtrlPowerMgmtPolicy` | `notsupported(1), unknown(2), performance(3), elastic(4)` | Integer | None |

CHAPTER 6

# Configuring ILOM Firmware Settings

**Topics**

| Description | Links |
|---|---|
| Review the prerequisites | • "Before You Begin" on page 105 |
| Configuring ILOM firmware interfaces | • "View and Configure ILOM Firmware Settings" on page 106 |

**Related Topics**

| For ILOM | Section | Guide |
|---|---|---|
| • Concepts | • Configuration Management and Firmware Updates | *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* |
| • Web | • Updating ILOM Firmware | *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures 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/

## Before You Begin

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

- Before you can use SNMP to view and configure ILOM settings, you must configure SNMP. For more information, see "Preparing Your System to Use SNMP" on page 3.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user with read/write (rw) privileges.

---

**Note –** The example SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will only work as presented if you have Net-SNMP and the Net-SNMP sample applications installed.

---

# Configuring ILOM Firmware Interfaces

## ▼ View and Configure ILOM Firmware Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure ILOM firmware settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure ILOM firmware settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username***`@`***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - To view the version of the current firmware image, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareMgmtVersion.0
```

   - To view the build number of the current firmware image, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareMgmtBuildNumber.0
```

- To view the build date and time of the current firmware image, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareMgmtBuildDate.0
```

- To view the IP address of the TFTP server that will be used to download the firmware image, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareTFTPServerIP.0
```

- To set the IP address of the TFTP server that will be used to download the firmware image, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareTFTPServerIP.0 s ipaddress
```

- To view the relative path of the new firmware image file on the TFTP server, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareTFTPFileName.0
```

- To set the relative path of the new firmware image file on the TFTP server, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareTFTPFileName.0 s 'tftpfilename'
```

- To view the property that determines whether the previous configuration of the server should be preserved after a firmware update, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwarePreserveConfig.0
```

- To set the `PreservConfig` property to true so that the previous configuration of the server is preserved after a firmware update, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwarePreserveConfig.0 i 1
```

- To view the property that indicates the status of a firmware update, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareMgmtStatus.0
```

- To view the property that is used to initiate a firmware update using the values of the other firmware management properties as parameters, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareMgmtAction.0
```

- To set the property so as to initiate a firmware update using the values of the other firmware management properties as parameters, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareMgmtAction.0 i 2
```

- To clear the values of the other firmware management properties used if and when a firmware update is initiated, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareMgmtAction.0 i 1
```

- To view the version of the current firmware management file system, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareMgmtFilesystemVersion.0
```

- To view the property that is used to postpone the BIOS upgrade until the next server power off, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareDelayBIOS.0
```

---

**Note –** The commands to view and set the DelayBIOS property are not supported on SPARC servers.

---

- To set the `DelayBIOS` property to postpone the BIOS upgrade until the next server power off, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlFirmwareDelayBIOS.0 i 1
```

---

**Note –** The commands to view and set the DelayBIOS property are not supported on SPARC servers.

---

CHAPTER 7

# Managing the ILOM Configuration

**Topics**

| Description | Links |
|---|---|
| Review the prerequisites | • "Before You Begin" on page 109 |
| Configuring ILOM configuration management interfaces | • "View and Configure Policy Settings" on page 110<br>• "Configure Power Setting" on page 111<br>• "View and Configure Backup and Restore Settings" on page 112<br>• "Configure the Reset Setting" on page 113 |

**Related Topics**

| For ILOM | Section | Guide |
|---|---|---|
| • Concepts | • Configuration Management and Firmware Updates | *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* |
| • Web | • Backing Up and Restoring the ILOM Configuration | *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* |
| • CLI | • Backing Up and Restoring the 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/

## Before You Begin

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

- Before you can use SNMP to view and configure ILOM settings, you must configure SNMP. For more information, see "Preparing Your System to Use SNMP" on page 3.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user with read/write (rw) privileges.

---

**Note –** The example SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will only work as presented if you have Net-SNMP and the Net-SNMP sample applications installed.

---

# Configuring ILOM Configuration Management Interfaces

**Topics**

| Description | Links |
|---|---|
| Configure ILOM configuration management interfaces | • "View and Configure Policy Settings" on page 110<br>• "Configure Power Setting" on page 111<br>• "View and Configure Backup and Restore Settings" on page 112<br>• "Configure the Reset Setting" on page 113 |

## ▼ View and Configure Policy Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure policy settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure policy settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **`ssh`** *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - To view a short description of the policy for policy ID number 2, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlPolicyShortStr.2
```

   - To view a verbose description of the policy for policy ID number 2, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlPolicyLongStr.2
```

   - To view the status of the policy for policy ID number 2, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlPolicyEnabled.2
```

   - To set the status of the policy for policy ID number 2 enabled, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlPolicyEnabled.2 i 1
```

# ▼ Configure Power Setting

### Before You Begin

- You can use the `set` command to configure the power setting. For a description of the MIB object used in this command, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to configure the power setting:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command example:**
   - To specify the action “powerOn” and apply it to the power control target named ‘/SYS’, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlPowerAction.'/SYS' i 1
```

# ▼ View and Configure Backup and Restore Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure backup and restore settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure backup and restore settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - To restore the configuration on the SP to the original factory default state, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlResetToDefaultsAction.0 i 3
```

   - To view the target destination of configuration XML file during backup and restore operation, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
lomCtrlBackupAndRestoreTargetURI.0
```

   - To set the target destination of configuration XML file during the backup and restore operation to tftp://10.8.136.154/remotedir/config_backup.xml, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
lomCtrlBackupAndRestoreTargetURI.0 s
'tftp://10.8.136.154/remotedir/config_backup.xml'
```

   - To set the passphrase to encrypt or decrypt sensitive data during the backup and restore operation, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlBackupAndRestorePassphrase.0 s 'passphrase'
```

   - To view the property used to issue a action, either backup or restore, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlBackupAndRestoreAction.0
```

- To issue a restore action using the `ilomCtrlBackupAndRestoreAction` MIB object, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlBackupAndRestoreAction.0 i 2
```

- To monitor the current status of backup or restore operation, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlBackupAndRestoreActionStatus.0
```

# ▼ Configure the Reset Setting

### Before You Begin

- You can use the `set` command to configure the reset setting. For a description of the MIB objects used in this command, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to configure the reset setting:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command example:**

   - To specify the action "reset" and apply it to the reset control target named '/SP', type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlResetAction.'/SP' i 1
```

CHAPTER 8

# Managing a SPARC System Configuration

**Topics**

| Description | Links |
|---|---|
| Review the prerequisites | • "Before You Begin" on page 116 |
| SPARC management interfaces | • "View and Configure SPARC Diagnostic Settings" on page 117<br>• "View and Configure SPARC Host Settings" on page 120<br>• "View and Configure SPARC Boot Mode Settings" on page 123<br>• "View and Configure SPARC Keyswitch Setting" on page 124 |

**Related Topics**

| For ILOM | Section | Guide |
|---|---|---|
| • Concepts | • Remote Host Management Options | *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* |
| • Web | • Managing Remote Hosts | *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures 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/

# Before You Begin

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

- Before you can use SNMP to view and configure ILOM settings, you must configure SNMP. For more information, see "Preparing Your System to Use SNMP" on page 3.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user with read/write (rw) privileges.

---

**Note –** The example SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will only work as presented if you have Net-SNMP and the Net-SNMP sample applications installed.

---

# Configuring SPARC Management Interfaces

**Topics**

| Description | Links |
|---|---|
| Review the prerequisites | • "Before You Begin" on page 116 |
| SPARC management interfaces | • "View and Configure SPARC Diagnostic Settings" on page 117<br>• "View and Configure SPARC Host Settings" on page 120<br>• "View and Configure SPARC Boot Mode Settings" on page 123<br>• "View and Configure SPARC Keyswitch Setting" on page 124 |

# ▼ View and Configure SPARC Diagnostic Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure SPARC diagnostic settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure SPARC diagnostic settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - To view the triggers of embedded diagnostics for the host, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsTrigger.0
```

   - To set the triggers of embedded diagnostics for the host to “powerOnReset”, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsTrigger.0 i 4
```

   - To view the modes for POST, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsMode.0
```

   - To set the POST mode to `service`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsMode.0 i 3
```

   - To view the level of embedded diagnostics that should be run on the host during a boot for the power-on-reset trigger, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsPowerOnLevel.0
```

- To set the level of embedded diagnostics that should be run on the host during a boot for the power-on-reset trigger to `normal`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsPowerOnLevel.0 i 3
```

- To view the level of embedded diagnostics that should be run on the host during a boot for the user-reset trigger, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsUserResetLevel.0
```

- To set the level of embedded diagnostics that should be run on the host during a boot for the user-reset trigger to `normal`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsUserResetLevel.0 i 3
```

- To view the level of embedded diagnostics that should be run on the host during a boot for the error-reset trigger, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsErrorResetLevel.0
```

- To set the level of embedded diagnostics that should be run on the host during a boot for the error-reset trigger to `normal`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsErrorResetLevel.0 i 3
```

- To view the verbosity level of embedded diagnostics that should be run on the host during a boot, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsPowerOnVerbosity.0
```

- To set the verbosity level of embedded diagnostics that should be run on the host during a boot to `maximum`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsPowerOnVerbosity.0 i 4
```

- To view the verbosity level of embedded diagnostics that should be run on the host during a boot for user-reset trigger, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsUserResetVerbosity.0
```

- To set the verbosity level of embedded diagnostics that should be run on the host during a boot for user-reset trigger to `maximum`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsUserResetVerbosity.0 i 4
```

- To view the verbosity level of embedded diagnostics that should be run on the host during a boot for error-reset trigger, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsErrorResetVerbosity.0
```

- To set the verbosity level of embedded diagnostics that should be run on the host during a boot for error-reset trigger to `maximum`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsErrorResetVerbosity.0 i 4
```

- To view the progress of POST diagnostics on the host, expressed as a percentage, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsStatus.0
```

- To view the property that shows the action to control the POST diagnostics on the host, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsAction.0
```

- To set the property to take control of the POST diagnostics running on the host to `start`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCDiagsAction.0 i 2
```

# ▼ View and Configure SPARC Host Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure SPARC host settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure SPARC host settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - To view the starting MAC address for the host, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostMACAddress.0
```

   - To view the version string for OpenBoot PROM (OBP), type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostOBPVersion.0
```

   - To view the version string for POST, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostPOSTVersion.0
```

   - To view the option that determines whether the host should continue to boot in the event of a non-fatal POST error, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostAutoRunOnError.0
```

   - To configure the host to continue to boot in the event of a non-fatal POST error, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostAutoRunOnError.0 i 1
```

- To view the string that describes the status of POST, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostPOSTStatus.0
```

- To view the option that determines what action the SP will take when it discovers that the host is hung, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostAutoRestartPolicy.0
```

- To configure the SP to reset when it discovers that the host is hung, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostAutoRestartPolicy.0 i 2
```

- To view the string that describes the boot status of host operating system, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostOSBootStatus.0
```

- To view the boot timer time-out value, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostBootTimeout.0
```

- To set the boot timer time-out value to 30 seconds, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostBootTimeout.0 i 30
```

- To view the property that determines what action the SP will take when the boot timer expires, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostBootRestart.0
```

- To configure the SP to reset when the boot timer expires, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostBootRestart.0 i 2
```

- To view the maximum number of boot failures allowed by the SP, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostMaxBootFail.0
```

- To set the maximum number of boot failures allowed by the SP to 10, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostMaxBootFail.0 i 10
```

- To view the property that determines what action the SP will take when the maximum number of boot failures is reached, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostBootFailRecovery.0
```

- To configure the SP to power cycle the host when the maximum number of boot failures is reached, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostBootFailRecovery.0 i 2
```

- To view the version string for the Hypervisor, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostHypervisorVersion.0
```

- To view the version string for the system firmware (SysFw), type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostSysFwVersion.0
```

- To view the property that determines the break action that SP will send, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostSendBreakAction.0
```

- To configure the SP to send a `dumpcore` break action, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostSendBreakAction.0 i 3
```

- To view the property that determines the host I/O reconfiguration policy to apply on next host power-on, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostIoReconfigurePolicy.0
```

- To configure the SP to execute the host I/O reconfiguration policy on the next power-on, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCHostIoReconfigurePolicy.0 i 3
```

# ▼ View and Configure SPARC Boot Mode Settings

### Before You Begin

- You can use the `get` and `set` commands to view and configure SPARC boot mode settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure SPARC boot mode settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - To view the boot mode state for the host, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCBootModeState.0
```

   - To configure the host to retain current NVRAM variable settings, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCBootModeState.0 i 1
```

   - To view the boot script to use when the boot mode state is set to script, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCBootModeScript.0
```

- To specify the boot script to use when the boot mode state is set to `'setenv diag-switch'`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCBootModeScript.0 s 'setenv diag-switch'
```

- To view date and time when the boot mode configuration will expire, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCBootModeExpires.0
```

- To view the string that refers to the LDOM configuration name, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCBootModeLDOMConfig.0
```

- To set the LDOM configuration name to `default`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCBootModeLDOMConfig.0 s default
```

## ▼ View and Configure SPARC Keyswitch Setting

### Before You Begin

- You can use the `get` and `set` commands to view and configure SPARC key switch settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Follow these steps to view and configure SPARC key switch settings:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   **ssh** *username***@***snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**
   - To view the current state of the virtual key switch, type:

```
% snmpget -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCKeySwitchState.0
```

- To set the state of the virtual key switch to `standby`, type:

```
% snmpset -mALL -v2c -cprivate SNMP_agent_ipaddress
ilomCtrlSPARCKeySwitchState.0 i 2
```

# PART II IPMI

Part II of this document provides an overview of the Intelligent Platform Management Interface (IPMI), and descriptions of the procedures you can perform to access ILOM functions.

CHAPTER 9

# IPMI Overview

**Topics**

| Description | Links |
|---|---|
| Learn about IPMI | • "About Intelligent Platform Management Interface" on page 130 |
| Learn how to configure the IPMI state and how to use IPMItool | • "Configuring the IPMI State" on page 131<br>• "IPMItool Examples" on page 135 |
| Learn about the IPMI commands | • "IPMI Commands" on page 139 |

**Related Topics**

| For ILOM | Section | Guide |
|---|---|---|
| • Concepts | • ILOM Overview | *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* |
| • CLI | • CLI Overview | *Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* |
| • Web interface | • Web Interface Overview | *Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* |
| • SNMP | • SNMP 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/

# About Intelligent Platform Management Interface

ILOM supports the Intelligent Platform Management Interface (IPMI), which enables you to monitor and control your server platform, as well as to retrieve information about your server platform.

IPMI is an open, industry-standard interface that was designed for the management of server systems over a number of different types of networks. IPMI functionality includes field-replaceable unit (FRU) inventory reporting, system monitoring, logging of system events, system recovery (including system resets and power on and power off capabilities), and alerting.

The monitoring, logging, system recovery, and alerting functions available through IPMI provide access to the manageability that is built into the platform hardware.

ILOM is compliant with IPMI v1.5 and v2.0.

A Windows port of IPMItool is available at `http://www.sun.com/system-management/tools.jsp`.

Additional information, including detailed specifications about IPMI, is available at the following sites:

- `http://www.intel.com/design/servers/ipmi/spec.htm`
- `http://openipmi.sourceforge.net`

The service processors (SPs) on your servers and server modules (blades) are IPMI v2.0 compliant. You can access IPMI functionality through the command line using the IPMItool utility either in-band (using the host operating system running on the server) or out-of-band (using a remote system). Additionally, you can generate IPMI-specific traps from the ILOM web interface, or manage the SP's IPMI functions from any external management solution that is IPMI v1.5 or v2.0 compliant.

## IPMItool

IPMItool is an open-source, simple command-line interface (CLI) utility for managing and configuring IPMI-enabled devices. IPMItool can be used to manage the IPMI functions of either the local system or a remote system. You can use the IPMItool utility to perform IPMI functions with a kernel device driver or over a LAN interface. You can download IPMItool from this site:

`http://ipmitool.sourceforge.net/`

You can do the following with IPMItool:

- Read the Sensor Data Record (SDR) repository.
- Print sensor values.
- Display the contents of the system event log (SEL).
- Print field-replaceable unit (FRU) inventory information.
- Read and set LAN configuration parameters.
- Perform remote chassis power control.

Detailed information about IPMItool is provided in a man page that is available from this site:

`http://ipmitool.sourceforge.net/manpage.html`

IPMItool supports a feature that enables you to enter ILOM command-line interface (CLI) commands just as though you were using the ILOM CLI directly. CLI commands can be scripted and then the script can be run on multiple service processor (SP) instances.

## IPMI Alerts

ILOM supports alerts in the form of IPMI Platform Event Trap (PET) alerts. Alerts provide advance warning of possible system failures. Alert configuration is available from the ILOM SP on your server or server module. IPMI PET alerts are supported on all server platforms using ILOM, and not supported on the Chassis Monitoring Module (CMM). For more information about the types of IPMI alerts, see "Alert Management" in the *Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*

# Configuring the IPMI State

You can enable or disable the IPMI state using either the CLI or the web interface.

**Topics**

| Description | Links |
|---|---|
| Enable the IPMI state | • "Enable IPMI State Using the CLI" on page 132<br>• "Enable IPMI State Using the Web Interface" on page 132 |

## ▼ Enable IPMI State Using the CLI

### Before You Begin

- To enable IPMI state using the CLI, you need the Admin (a) role enabled.

Follow these steps to enable the IPMI state:

1. **Log in to the ILOM CLI.**
2. **At the command prompt, type:**

   -> **set /SP/services/ipmi servicestate=enabled**

```
-> set /SP/services/ipmi servicestate=enabled
Set 'servicestate' to 'enabled'
```

## ▼ Enable IPMI State Using the Web Interface

### Before You Begin

- To enable IPMI state using the web interface, you need the Admin (a) role enabled.

Follow these steps to enable the IPMI state:

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

   The IPMI Settings page appears.
3. **Click the check box to enable or disable the IPMI state.**

# Using IPMItool to Run ILOM CLI Commands

IPMItool supports a feature that allows you to enter ILOM CLI commands just as if you were using the ILOM CLI directly. Most ILOM CLI commands are supported.

**Topics**

| Description | Links |
|---|---|
| Use IPMItool to run CLI commands | • "Access the ILOM CLI From IPMItool" on page 133<br>• "Script ILOM CLI Commands With IPMItool" on page 133 |

## Before You Begin

To use the ILOM CLI through `ipmitool`, you must be using `ipmitool` version 1.8.9.4 or later. To check the version number of `ipmitool`, type `ipmitool -V`.

## ▼ Access the ILOM CLI From IPMItool

1. **To enable the ILOM CLI using IPMItool, type:**

   # **`ipmitool -H`** *hostname* **`-U`** *username* **`-P`** *userpassword* **`sunoem cli`**

   The ILOM CLI prompt appears as follows:

```
Connected. Use ^D to exit.
->
```

2. **To use the CLI, type CLI commands.**

## ▼ Script ILOM CLI Commands With IPMItool

A key benefit of using ILOM CLI from IPMItool is that the CLI commands can be scripted and then the script can be run on multiple SP instances. Scripting is possible because the CLI commands can be included on the IPMItool command line where each argument on the command line is treated as a separate ILOM CLI command. Command separation is archived by including quotation marks at the beginning and

end of each ILOM CLI command. The following example shows how to include two CLI commands on the `ipmitool` command line. In the example, notice that each ILOM CLI command begins and ends with quotation marks.

```
# ipmitool -H hostname -U username -P userpassword sunoem cli "show
/SP/services" "show /SP/logs"
Connected. Use ^D to exit.
-> show /SP/services
/SP/services
    Targets:
        http
        https
        servicetag
        snmp
        ssh
        sso

    Properties:

    Commands:
        cd
        show

-> show /SP/logs
 /SP/logs
    Targets:
        event

    Properties:

    Commands:
        cd
        show

->Session closed
Disconnected
```

# IPMItool Examples

**Topics**

| Description | Links |
|---|---|
| Perform various functions using IPMItool | • "View a List of Sensors and Their Values" on page 135<br>• "View Details About a Single Sensor" on page 136<br>• "Power On the Host" on page 136<br>• "Power Off the Host" on page 136<br>• "Power Cycle the Host" on page 137<br>• "Shut Down the Host Gracefully" on page 137<br>• "View Manufacturing Information for FRUs" on page 137<br>• "View the System Event Log" on page 138 |

## ▼ View a List of Sensors and Their Values

```
$ ipmitool -H 1.2.3.4 -I lanplus -U username -P userpassword sdr list
/SYS/T_AMB       | 24 degrees C       | ok
/RFM0/FAN1_SPEED | 7110 RPM           | ok
/RFM0/FAN2_SPEED | 5880 RPM           | ok
/RFM1/FAN1_SPEED | 5880 RPM           | ok
/RFM1/FAN2_SPEED | 6360 RPM           | ok
/RFM2/FAN1_SPEED | 5610 RPM           | ok
/RFM2/FAN2_SPEED | 6510 RPM           | ok
/RFM3/FAN1_SPEED | 6000 RPM           | ok
/RFM3/FAN2_SPEED | 7110 RPM           | ok
/RFM4/FAN1_SPEED | 6360 RPM           | ok
/RFM4/FAN2_SPEED | 5610 RPM           | ok
/RFM5/FAN1_SPEED | 5640 RPM           | ok
/RFM5/FAN2_SPEED | 6510 RPM           | ok
/RFM6/FAN1_SPEED | 6180 RPM           | ok
/RFM6/FAN2_SPEED | 6000 RPM           | ok
/RFM7/FAN1_SPEED | 6330 RPM           | ok
/RFM7/FAN2_SPEED | 6330 RPM           | ok
/RFM8/FAN1_SPEED | 6510 RPM           | ok
/RFM8/FAN2_SPEED | 5610 RPM           | ok
```

**Note –** If `ipmitool` is not configured to support the `-P` option, which enables the password to be entered in the command line, you will be prompted to enter the password.

**Note –** The above output was shortened. The actual output displays 163 sensors.

## ▼ View Details About a Single Sensor

```
$ ipmitool -H 1.2.3.4 -v -I lanplus -U username -P userpassword sensor get /SYS/T_AMB
Locating sensor record...
Sensor ID              : /SYS/T_AMB (0x8)
 Entity ID             : 41.0
 Sensor Type (Analog)  : Temperature
 Sensor Reading        : 24 (+/- 0) degrees C
 Status                : ok
 Lower Non-Recoverable : 0.000
 Lower Critical        : 4.000
 Lower Non-Critical    : 10.000
 Upper Non-Critical    : 35.000
 Upper Critical        : 40.000
 Upper Non-Recoverable : 45.000
 Assertions Enabled    : lnc- lcr- lnr- unc+ ucr+ unr+
 Deassertions Enabled  : lnc- lcr- lnr- unc+ ucr+ unr+
```

## ▼ Power On the Host

```
$ ipmitool -H 1.2.3.4 -v -I lanplus -U username -P userpassword chassis
power on
```

## ▼ Power Off the Host

```
$ ipmitool -H 1.2.3.4 -v -I lanplus -U username -P userpassword chassis
power off
```

## ▼ Power Cycle the Host

$ **ipmitool -H 1.2.3.4 -v -I lanplus -U** *username* **-P** *userpassword* **chassis power cycle**

## ▼ Shut Down the Host Gracefully

$ **ipmitool -H 1.2.3.4 -v -I lanplus -U** *username* **-P** *userpassword* **chassis power soft**

## ▼ View Manufacturing Information for FRUs

```
$ ipmitool -H 1.2.3.4 -v -I lanplus -U username -P userpassword fru print
FRU Device Description : Builtin FRU Device (ID 0)
 Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
 Board Serial          : 0000000-7001
 Board Part Number     : 501-7738-01
 Board Extra           : AXX_RevE_Blade
 Product Manufacturer  : SUN MICROSYSTEMS
 Product Name          : ILOM

FRU Device Description : /SYS (ID 4)
 Chassis Type          : Rack Mount Chassis
 Chassis Part Number   : 541-0251-05
 Chassis Serial        : 00:03:BA:CD:59:6F
 Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
 Board Serial          : 0000000-7001
 Board Part Number     : 501-7738-01
 Board Extra           : AXX_RevE_Blade
 Product Manufacturer  : SUN MICROSYSTEMS
 Product Name          : SUN BLADE X8400 SERVER MODULE
 Product Part Number   : 602-0000-00
 Product Serial        : 0000000000
 Product Extra         : 080020ffffffffffffff0003baf15c5a

FRU Device Description : /P0 (ID 5)
 Product Manufacturer  : ADVANCED MICRO DEVICES
 Product Part Number   : 0F21
 Product Version       : 2

FRU Device Description : /P0/D0 (ID 6)
 Product Manufacturer  : MICRON TECHNOLOGY
 Product Name          : 1024MB DDR 400 (PC3200) ECC
```

```
 Product Part Number   : 18VDDF12872Y-40BD3
 Product Version       : 0300
 Product Serial        : D50209DA
 Product Extra         : 0190
 Product Extra         : 0400

FRU Device Description : /P0/D1 (ID 7)
 Product Manufacturer  : MICRON TECHNOLOGY
 Product Name          : 1024MB DDR 400 (PC3200) ECC
 Product Part Number   : 18VDDF12872Y-40BD3
 Product Version       : 0300
 Product Serial        : D50209DE
 Product Extra         : 0190
 Product Extra         : 0400
```

## ▼ View the System Event Log

```
$ ipmitool -H 1.2.3.4 -I lanplus -U username -P userpassword sel list
 100 | Pre-Init Time-stamp   | Power Unit #0x78 | State Deasserted
 200 | Pre-Init Time-stamp   | Power Supply #0xa2 | Predictive Failure Asserted
 300 | Pre-Init Time-stamp   | Power Supply #0xba | Predictive Failure Asserted
 400 | Pre-Init Time-stamp   | Power Supply #0xc0 | Predictive Failure Asserted
 500 | Pre-Init Time-stamp   | Power Supply #0xb4 | Predictive Failure Asserted
 600 | 04/05/2007 | 12:03:24 | Power Supply #0xa3 | Predictive Failure Deasserted
 700 | 04/05/2007 | 12:03:25 | Power Supply #0xaa | Predictive Failure Deasserted
 800 | 04/05/2007 | 12:03:25 | Power Supply #0xbc | Predictive Failure Deasserted
 900 | 04/05/2007 | 12:03:26 | Power Supply #0xa2 | Predictive Failure Asserted
 a00 | 04/05/2007 | 12:03:26 | Power Supply #0xa8 | Predictive Failure Deasserted
 b00 | 04/05/2007 | 12:03:26 | Power Supply #0xb6 | Predictive Failure Deasserted
 c00 | 04/05/2007 | 12:03:26 | Power Supply #0xbb | Predictive Failure Deasserted
 d00 | 04/05/2007 | 12:03:26 | Power Supply #0xc2 | Predictive Failure Deasserted
 e00 | 04/05/2007 | 12:03:27 | Power Supply #0xb0 | Predictive Failure Deasserted
 f00 | 04/05/2007 | 12:03:27 | Power Supply #0xb5 | Predictive Failure Deasserted
1000 | 04/05/2007 | 12:03:27 | Power Supply #0xba | Predictive Failure Asserted
1100 | 04/05/2007 | 12:03:27 | Power Supply #0xc0 | Predictive Failure Asserted
1200 | 04/05/2007 | 12:03:28 | Power Supply #0xa9 | Predictive Failure Deasserted
1300 | 04/05/2007 | 12:03:28 | Power Supply #0xae | Predictive Failure Deasserted
1400 | 04/05/2007 | 12:03:28 | Power Supply #0xb4 | Predictive Failure Asserted
1500 | 04/05/2007 | 12:03:28 | Power Supply #0xbe | Predictive Failure Deasserted
```

# IPMI Commands

You can download the IPMItool utility at:

http://ipmitool.sourceforge.net/

After you install the IPMItool package, you can access detailed information about command usage and syntax from the man page that is installed. The following table summarizes available IPMItool commands.

**TABLE 9-1** IPMItool commands

| IPMI Command | Function |
|---|---|
| `sunoem sshkey set` | Configure an SSH key for a remote shell user. |
| `ipmitool sunoem sshkey del` | Remove an SSH key from a remote shell user. |
| `ipmitool sunoem led get` | Read LED status. |
| `ipmitool sunoem led set` | Set LED status. |
| `ipmitool sunoem cli` | Enter ILOM CLI commands as if you were using the ILOM CLI directly. The LAN/LANplus interface should be used. |
| `ipmitool raw` | Execute raw IPMI commands. |
| `ipmitool lan print` | Print the current configuration for the given channel. |
| `ipmitool lan set (1) (2)` | Set the given parameter on the given channel. |
| `ipmitool chassis status` | Display information regarding the high-level status of the system chassis and main power subsystem. |
| `ipmitool chassis power` | Perform a chassis control command to view and change the power state. |
| `ipmitool chassis identify` | Control the front panel identify light. Default is 15. Use 0 to turn off. |
| `ipmitool chassis restart_cause` | Query the chassis for the cause of the last system restart. |
| `ipmitool chassis poh` | Display the Power-On Hours counter. |
| `ipmitool chassis bootdev (1)` | Request the system to boot from an alternate boot device on next reboot. |
| `ipmitool chassis bootparam (1)` | Set the host boot parameters. |
| `ipmitool chassis selftest` | Display the BMC Self Test results. |

**TABLE 9-1** IPMItool commands *(Continued)*

| IPMI Command | Function |
|---|---|
| `ipmitool power` | Return the BMC Self Test results. |
| `ipmitool event` | Send a predefined event to the system event log. |
| `ipmitool mc (1) (2)` | Instruct the BMC to perform a warm or cold reset. |
| `ipmitool sdr` | Query the BMC for sensor data records (SDR) and extract sensor information of a given type, then query each sensor and print its name, reading, and status. |
| `ipmitool sensor` | List sensors and thresholds in a wide table format. |
| `ipmitool fru print` | Read all field-replaceable unit (FRU) inventory data and extract such information as serial number, part number, asset tags, and short strings describing the chassis, board, or product. |
| `ipmitool sel` | View the ILOM SP system event log (SEL). |
| `ipmitool pef info` | Query the BMC and print information about the PEF supported features. |
| `ipmitool pef status` | Print the current PEF status (the last SEL entry processed by the BMC, etc). |
| `ipmitool pef list` | Print the current PEF status (the last SEL entry processed by the BMC, etc). |
| `ipmitool user` | Display a summary of userid information, including maximum number of userids, the number of enabled users, and the number of fixed names defined. |
| `ipmitool session` | Get information about the specified session(s). You can identify sessions by their ID, by their handle number, by their active status, or by using the keyword “all” to specify all sessions. |
| `ipmitool firewall (1)` | Enable/disable individual command and command sub-functions; determine which commands and command sub-functions can be configured on a given implementation. |
| `ipmitool set (1)` | Set the runtime options including session host name, user name, password and privilege level. |
| `ipmitool exec` | Execute IPMItool commands from file name. Each line is a complete command. |

# Index


## A

Active Directory, 38
  Administrator Groups
    MIB objects, 44
    viewing and configuring, 43
  Alternate Server
    MIB objects, 53
    viewing and configuring, 50
  Custom Groups
    MIB objects, 48
    viewing and configuring, 46
  DNS Locator settings
    MIB objects, 56
    viewing and configuring, 55
  Operator Groups
    MIB objects, 45
    view and configure, 44
  User Domain
    MIB objects, 50
    viewing and configuring, 49
alert rules
  configuring, 89
  MIB objects, 90
alerts
  generating email notification, 91

## B

backup and restore, 112

## C

clock settings
  configuring network time protocol (NTP), 85
  MIB objects, 86
  setting, 85
component information
  MIB objects, 83
  view, 83
current key and key length
  configuring, 25
  MIB objects, 26

## E

email alert settings
  configuring, 93
event log
  configuring, 86
  MIB objects, 87

## F

firmware
  viewing and configuring, 106

## H

Host Name MIB objects, 12
host name settings, 11
HTTP and HTTPS
  MIB objects, 21
HTTP and HTTPS settings
  viewing and configuring, 20

## I

IP addresses
  configuring, 21
  MIB objects, 23
IPMI

detailed specifications
location of, 130
functionality, 130
generating IPMI-specific traps, 130
IPMI Platform Event Trap (PET) alerts, 131
overview, 130
versions supported by ILOM, 130
IPMItool
capabilities, 131
download site
location of, 130
functions of, 131
man page location, 131
references for, 131
running CLI commands with, 133
scripting CLI commands with, 133
using IPMItool, 130
viewing FRU manufacturing information, 137
viewing the system event log, 138

## L

LDAP, 58
configuring, 58
MIB objects, 61
LDAP/SSL, 62
Administrator Groups
MIB objects, 68
viewing and configuring, 67
Alternate Server
MIB objects, 76
viewing and configuring, 74
certificate settings, 66
Custom Groups
MIB objects, 72
viewing and configuring, 70
Operator Groups
MIB objects, 70
viewing and configuring, 68
User Domain
MIB objects, 74
viewing and configuring, 73

## M

Management Information Base (MIB)
definition, 4
MIB tree, 4
standard MIBs supported by ILOM, 6
MIB objects
user accounts, 35

## N

Net-SNMP
web site, 2
network settings
configuring, 11
MIB objects, 16

## P

policy settings
viewing and configuring, 110
power consumption management
entPhysicalName MIB object, 100
monitoring available power
snmpget command, 102
monitoring individual power supply
consumption using an snmpget
command, 100
monitoring permitted power
snmpget command, 102
monitoring power
snmpget command, 100
power monitoring
snmpget command, 99
sunPlatNumericSensor MIB objects, 100
view and set power policy
SNMP commands, 103
Product Identity Interfaces, xiii

## R

RADIUS
configuring, 77
MIB objects, 79
redundancy settings
view and configure, 54
remote Syslog receiver IP addresses
configuring, 88
MIB objects, 88

## S

Secure Shell (SSH) settings
configuring, 26
MIB object, 27
serial port
MIB settings, 18
settings, 17

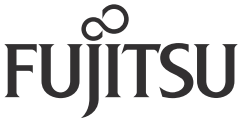
Simple Network Management Protocol
See SNMP
Single Sign On
configuring, 36
enabling, 36
MIB object, 37
single sign on
overview, 36
SMTP clients
configuring, 91
MIB objects, 93
SNMP
agent functions
functions supported, 3
managed node, 3
management station monitoring, 3
MIBs used to support ILOM, 7
Net-SNMP
web site, 2
network management station, 3
prerequisites, 3
software download site, 3
tutorial web sites, 2
versions supported, 2
SPARC boot mode, 123
SPARC diagnostics, 117
SPARC host settings, 120
SPARC key switch, 124
SSH key
generating, 27
MIB objects, 28
SSH server
MIB object, 29
restarting, 28
system identifier MIB objects, 12
system identifier settings, 11

## T

Telemetry Harness Daemon (THD)
configuring, 94

## U

user accounts, 34


FUJITSU