

# Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 5.1.x



F48377-03  
October 2022



Oracle ILOM Protocol Management Reference SNMP and IPMI Firmware Release 5.1.x,  
F48377-03

Copyright © 2022, 2022, Oracle and/or its affiliates.

Primary Author: Cheryl Smith

Copyright © 2022, 2022, Oracle et/ou ses affiliés.

# Contents

## 1 Using This Documentation

---

Product Documentation Library	1-1
Feedback	1-1

## 2 SNMP Overview

---

Related Information	2-1
About Simple Network Management Protocol	2-1
SNMP Components	2-2
Oracle ILOM SNMP MIBs	2-3
SNMP Command-Line Syntax Examples	2-6
Configure the SNMP Network Environment	2-7

## 3 Configuring SNMP Settings in Oracle ILOM

---

Related Information	3-1
Managing SNMP User Accounts and SNMP Trap Alerts (CLI)	3-1
Set SNMP Access and Authorization	3-1
Managing SNMP User Accounts and Communities	3-2
Before You Begin SNMP User Accounts	3-2
SNMP User Account Targets, Properties, and Values	3-3
SNMPv3 User Name and Password Requirements	3-4
Add an SNMP v3 User Account	3-4
Edit an SNMP v3 User Account	3-4
Delete an SNMP v3 User Account	3-5
Set SNMP v3 User Account Privacy Protocol Value	3-5
Managing SNMP Trap Alerts Using the Oracle ILOM	3-6
Configure SNMP Trap Rule Destinations and Properties	3-6
CLI Commands for Managing Alert Rule Configurations	3-8
Managing SNMP User Accounts and SNMP Trap Alerts (Web)	3-8
Set SNMP Management Access and Authorization	3-9
Managing SNMP User Accounts and Communities	3-9
Before You Begin SNMP User Accounts	3-9

Add or Edit an SNMP v3 User Account	3-10
Delete an SNMP v3 User Account	3-11
Manage SNMP Trap Alerts	3-11
Downloading SNMP MIBs Using Oracle ILOM	3-13
Before You Begin Download SNMP MIBs	3-13
Download SNMP MIBs (CLI)	3-13
Download SNMP MIBs (Web)	3-13

## 4 View Component Information and the Oracle ILOM Event Log (SNMP)

---

Related Information	4-1
Viewing Component Information	4-1
Viewing the Oracle ILOM Event Log	4-2

## 5 Server Management Using IPMI

---

Related Information	5-1
Intelligent Platform Management Interface (IPMI)	5-1
About IPMI	5-1
IPMI Service State and Supported IPMI Sessions	5-1
IPMI TLS Service and Interface	5-2
TLS Session Feature Summary	5-2
TLS IPMItool Interface Download Requirement	5-3
IPMItool	5-4
IPMI Alerts	5-4
IPMI Administrator and Operator Roles	5-5
Managing IPMI Properties in Oracle ILOM	5-5
Set the IPMI State and Session Properties (CLI)	5-5
Set the IPMI State and Session Properties (Web)	5-6
Using IPMItool to Run Oracle ILOM CLI Commands	5-7
IPMItool and Oracle ILOM Requirements	5-7
Access the Oracle ILOM CLI From IPMItool	5-9
Disable Default TLS Behavior for SSL Certificate Check	5-9
Scripting Oracle ILOM CLI Commands With IPMItool	5-9
Performing System Management Tasks (IPMItool)	5-10
Display Sensor List	5-11
View Single Sensor Details	5-12
View and Interpret Presence Sensor Type Values	5-13
Manage Host Power-On, Power-Off and Shutdown Functions	5-14
Manage Oracle ILOM Power Budget Interfaces	5-15

Manage the System Power Policy	5-19
Display FRU Manufacturing Details	5-21
Display Oracle ILOM Event, Audit, or Session Log	5-22
IPMItool Options and Command Summary	5-24

## 6 SNMP Command Examples

---

Related Information	6-1
snmpwalk Command	6-1
snmpbulkwalk Command	6-2
snmptable Command	6-2
snmptrapd Command	6-5

## Index

---

# 1

## Using This Documentation

- **Overview** – Provides instructions for managing remote Oracle hardware devices using the following supported management protocols: Simple Network Management Protocol (SNMP) and Intelligent Platform Management Interface (IPMI).
- **Audience** – This guide is intended for technicians, system administrators, and authorized Oracle service providers.
- **Required knowledge** – Users should have experience managing system hardware.

Copyright © 1994, 2022, Oracle et/ou ses affiliés.

## Product Documentation Library

Documentation and resources for this product and related products are available at [Systems Management and Diagnostics Documentation](#).

## Feedback

Provide feedback about this documentation at [Oracle Feedback](#).

# 2

## SNMP Overview

Description	Links
Learn about Oracle ILOM support for SNMP.	<ul style="list-style-type: none"><li>• <a href="#">About Simple Network Management Protocol</a></li></ul>
Learn about management using SNMP.	<ul style="list-style-type: none"><li>• <a href="#">SNMP Components</a></li></ul>
Learn about the Oracle ILOM SNMP Management Information Base (MIB) files.	<ul style="list-style-type: none"><li>• <a href="#">Oracle ILOM SNMP MIBs</a></li></ul>
Learn about the command-line syntax used in this guide.	<ul style="list-style-type: none"><li>• <a href="#">SNMP Command-Line Syntax Examples</a></li></ul>

### Related Information

- [Modifying Default Management Access Configuration Properties](#)
- [Oracle ILOM Overview](#)

### About Simple Network Management Protocol

Oracle ILOM supports 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. When 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 a host, router, web server, or other server on the network. SNMP messages are sent over IP using the User Datagram Protocol (UDP). Any management application that supports SNMP can monitor your server.

Because SNMP is a protocol, not an application, you need an application to issue SNMP commands. Your SNMP management software might provide this functionality, or you can use an open-source tool like Net-SNMP, which is available at [NET - SNMP](#).

For a more complete description of SNMP, see the five-part, introductory SNMP tutorial available at [SNMP Tutorial](#).

Oracle ILOM supports management access properties for SNMP v3 protocol, as well as configuration properties for setting SNMP v2 or v3 trap alert notifications. Using SNMP v3 is strongly advised since SNMP v3 provides additional security, authentication, and privacy beyond SNMP v2c.



 **Note:**

As of Oracle ILOM firmware version 4.0, support for all SNMP set operations and writeable SNMP MIBs have been removed. All permission properties for SNMP communities and users have also been removed. As of Oracle ILOM firmware version 5.0, management access properties were removed for the SNMP v2c protocol and communities. SNMP should be used for system monitoring and not for management. Configuration of SNMP traps are still supported.

 **Note:**

Oracle 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 [NET - SNMP](#). This tutorial is more advanced than the introductory tutorial.

## 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 Oracle 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 Oracle server and runs on Oracle ILOM, so all SNMP management occurs through Oracle ILOM. To use 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
- Trap

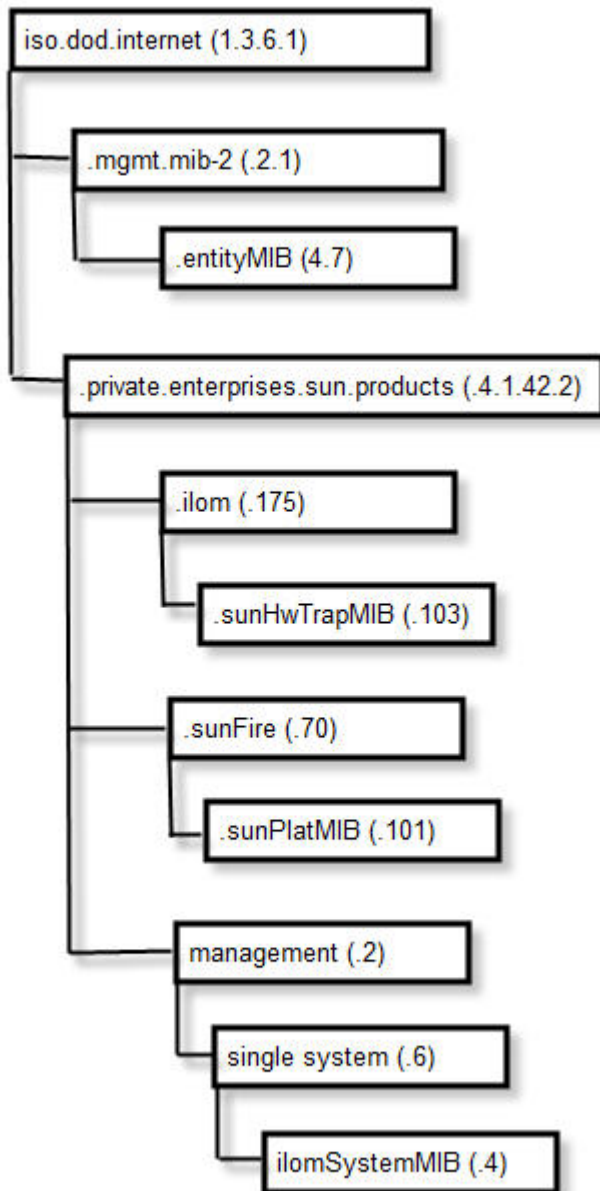
## Oracle ILOM SNMP MIBs

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 Oracle ILOM, the MIB makes it possible to access the server's network configuration, status, and statistics.

SNMP MIBs are a part of the Oracle ILOM firmware. You can download MIBs directly from Oracle ILOM. For more information about MIBs, and instructions for downloading MIBs from Oracle ILOM, see [Before You Begin Download SNMP MIBs](#).


The following figure shows the standard MIB hierarchy and the location of the Oracle ILOM MIB modules in that hierarchy. The Oracle ILOM MIB modules are described in the table that follows.

Location of Oracle ILOM MIB Modules



The following table lists the Oracle ILOM MIB modules and the object ID for each MIB name.

**Table 2-1 Description of Oracle ILOM MIB Modules, Object ID, and MIB Name**


MIB Name	Description	MIB Object ID
ENTITY-MIB	<p>The MIB module for representing multiple physical entities supported by a single SNMP agent.</p> <div style="border: 1px solid #0070C0; background-color: #E6F2FF; padding: 10px; margin: 10px 0;"> <p> <b>Note:</b></p> <p>The entPhysicalTable is the only part of this MIB that is implemented.</p> </div>	1.3.6.1.2.1.47
SUN-Hw-TRAP-MIB	<p>This MIB describes the hardware-related notifications and traps that can be generated by Oracle Sun server platforms.</p> <p>For more information about managing SNMP traps in Oracle ILOM, see <a href="#">Configuring SNMP Settings in Oracle ILOM</a>.</p>	1.3.6.1.4.1.42.2.175.103
SUN-PLATFORM-MIB	<p>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.</p>	1.3.6.1.4.1.42.2.70.101
ilomSystemMIB	<p>This MIB provides Oracle single system management logs and open problems data.</p>	.1.3.6.1.4.1.42.2.2.6.4

Portions of the standard MIBs listed in the following table are implemented by Oracle ILOM.

**Table 2-2 Standard MIBs Implemented by Oracle ILOM**

MIB Name	Description	MIB Object ID
IF-MIB	<p>This MIB module describes 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.</p>	1.3.6.1.2.1.31
IP-MIB	<p>This MIB module is for managing IP and ICMP implementations, but excluding their management of IP routes.</p>	1.3.6.1.2.1.4.
SNMP-FRAMEWORK-MIB	<p>This is the SNMP Management Architecture MIB.</p>	1.3.6.1.6.3.10

**Table 2-2 (Cont.) Standard MIBs Implemented by Oracle ILOM**

MIB Name	Description	MIB Object ID
SNMPv2-MIB	This is the MIB module for SNMP entities.  <div style="border: 1px solid #0070c0; background-color: #e6f2ff; padding: 10px; margin: 10px 0;">  <b>Note:</b> Only the system and SNMP groups from this MIB module apply to Oracle ILOM. </div>	1.3.6.1.6.3.1
TCP-MIB	This is the MIB module for managing TCP implementations.	1.3.6.1.2.1.49
UDP-MIB	This is the MIB module for managing UDP implementations.	1.3.6.1.2.1.50

The following table lists MIBs that are used in support of the Oracle ILOM SNMP implementation.

**Table 2-3 MIBs Used in Support of the Oracle ILOM SNMP Implementation**

MIB Name	Description	MIB Object ID
HOST-RESOURC ES-MIB	This MIB is for use in managing host systems. The 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

## SNMP Command-Line Syntax Examples

In some network environments, you are required to specify the SNMP version, community name, hostname, and default port when issuing SNMP commands. For

example, to request the value of the object identifier (OID) `sysDescr.0` in an IPv4 environment, you might type the following:

```
%snmpget -v3 -c public 192.0.2.1:161 sysDescr.0
```

However, it is possible to configure your network environment such that most command-line arguments are not necessary. For example, for SNMP v3, if you set default values for the default SNMP version, community name, and default port, the following syntax is considered valid:

```
%snmpget SNMP_agent sysDescr.0
```

Throughout this guide, *SNMP\_agent* refers to the hostname or IP address of the system you are querying.

#### Note:

If you query a device using IPv6 addressing, you must use the following syntax: `udp6:[IPv6 address]` If the following message appears in response to the query: `getaddrinfo: node name or service name not known, try adding -YdefaultPort=<port_number>` to the SNMP command line arguments.

In addition, the examples in this guide omit most command-line arguments. To configure your network so that most command-line arguments are not necessary, see the following procedure:

- [Configure the SNMP Network Environment](#)

## Configure the SNMP Network Environment

Follow these steps to configure SNMP network properties for a managed device.

1. Log in the Oracle ILOM command-line interface (CLI).  
For instructions on logging in to Oracle ILOM, refer to the [Log In to the Oracle ILOM CLI](#).
2. In Oracle ILOM, issue the create command to create an SNMP Community Name.  

```
-> create /SP/services/snmp/communities/community name
```
3. Issue the set command to enable SNMP access and specify the SNMP agent port address, for example:  

```
-> set /SP/services/snmp servicestate=enabled v3=enabled port=161
```
4. Download the Oracle ILOM MIBs to the `$HOME/mibs` directory.  
For instructions on downloading the Oracle ILOM MIBs, see [Downloading SNMP MIBs Using Oracle ILOM](#).
5. In the `$HOME/.snmp/snmp.conf` file in the `$HOME/mibs` directory, specify the following:

```
defversion          3
defcommunity        community_name
defaultPort         161
```

```
mibs          ALL
mibdirs       +$HOME/mibs
```

6. Test the new configuration by issuing the following command:

```
%snmp SNMP_agent sysName.0
```

The command should produce similar output on your system:

```
RFC1213-MIB::sysName.0 = STRING: "systemname"
```

# 3

## Configuring SNMP Settings in Oracle ILOM

Description	Links
Learn about Oracle ILOM CLI procedures for managing SNMP access, user accounts, and SNMP trap alerts.	<ul style="list-style-type: none"><li>• <a href="#">Managing SNMP User Accounts and SNMP Trap Alerts (CLI)</a></li><li>• <a href="#">Managing SNMP User Accounts and SNMP Trap Alerts (Web)</a></li></ul>
Learn how to download SNMP MIBs directly from Oracle ILOM.	<ul style="list-style-type: none"><li>• <a href="#">Downloading SNMP MIBs Using Oracle ILOM</a></li></ul>

### Related Information

- [Modifying Default Management Access Configuration Properties](#)
- [Configuring Alert Notifications](#)

### Managing SNMP User Accounts and SNMP Trap Alerts (CLI)

- [Set SNMP Access and Authorization](#)
- [Managing SNMP User Accounts and Communities](#)
- [Managing SNMP Trap Alerts Using the Oracle ILOM](#)

### Set SNMP Access and Authorization

#### Before You Begin

- To modify SNMP properties in Oracle ILOM, you must have the Admin role (a) enabled.
- The SNMP `servicestate` property is, by default, shipped from the factory *enabled*.
- Oracle ILOM provides authentication properties for SNMP v3.
  - For SNMP v3, Oracle ILOM provides a `users` target for managing user authentication. The SNMPv3 `users` target is not shipped from the factory with pre-packaged values for users.

To set the SNMP service state, properties, follow these steps:

1. Log in to the Oracle ILOM CLI.
2. To view the Oracle ILOM SNMP properties, type:

```
-> show /SP/services/snmp
```

The following SNMP output appears.

```
-> show /SP/services/snmp
    /SP/services/snmp
    Targets:
      communities
```



```

mibs
users
Properties:
  engineid = none
  port = 161
  servicestate = (enabled)
  v3 = enabled
Commands:
  cd
  set
  show

```

3. Use the set command to change any of the SNMP properties, for example:

- To enable SNMP with read-only access, type:  
-> set /SP/services/snmp servicestate=enabled
- To enable the SNMP protocol version property, type:  
-> set /SP/services/snmp v3=enabled

where # is the SNMP protocol version you want to enable.

For more information about SNMP user accounts and read and write access, see [Managing SNMP User Accounts and Communities](#).

4. Use the create command to create an SNMP v3 user account, for example:

- To create a user account for authorization and provide read and write access, type:

```

-> create /SP/services/snmp/users/<useraccountname>
authenticationpassword=password

```

For more information about SNMP user accounts and read and write access, see [Managing SNMP User Accounts and Communities](#).

## Managing SNMP User Accounts and Communities

- [Before You Begin SNMP User Accounts](#)
- [SNMP User Account Targets, Properties, and Values](#)
- [SNMPv3 User Name and Password Requirements](#)
- [Add an SNMP v3 User Account](#)
- [Edit an SNMP v3 User Account](#)
- [Delete an SNMP v3 User Account](#)
- [Set SNMP v3 User Account Privacy Protocol Value](#)

### Before You Begin SNMP User Accounts

Before performing the procedures in this section, ensure that the following requirements are met:

- To set SNMP user account properties in Oracle ILOM, you need the User Management (u) role enabled.
- Verify that the proper SNMP settings are enabled in Oracle ILOM. See [Set SNMP Access and Authorization](#).

 **Note:**

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

## SNMP User Account Targets, Properties, and Values

You can access the SNMP user account targets, properties, and values under the `/SP/services/snmp` target. The following table identifies the targets, properties, and values that are valid for SNMP user accounts.

**Table 3-1 SNMP User Account Targets, Properties, and Values**

Target	Property	Value	Default
<code>/SP/services/snmp/users/ <i>username</i></code>	<code>authenticationprotocol</code>	MD5 SHA <string>	MD5 (null string)
	<code>authenticationpassword<sup>1</sup></code>	none DES AES <sup>3</sup> <string>	none (null string)
	<code>privacyprotocol</code>		
	<code>privacypassword<sup>2</sup></code>		
<code>/SP/services/snmp</code>	<code>engineid = none</code>	<string>	(null string)
	<code>port = 161</code>	<integer>	161
	<code>servicestate = enabled</code>	enable disabled enabled disabled	enabled disabled
	<code>v3 = disabled</code>	enable disabled	enabled

<sup>1</sup> You must provide an authentication password when you create or modify users (SNMP v3 only).

<sup>2</sup> If the `privacyprotocol` property has a value other than `none`, then you must set a privacy password.

<sup>3</sup> AES (Advanced Encryption Standard) privacy protocol option is available for SNMPv 3 as of Oracle ILOM 3.0.16.

For example, to change `privacyprotocol` for user `al` to `DES`, use the following syntax:

```
-> set /SP/services/snmp/users/al privacyprotocol=DES
privacypassword=password authenticationprotocol=SHA
authenticationpassword=password
```

Note that the changes would be invalid if the following syntax was specified:

```
-> set /SP/services/snmp/users/al privacyprotocol=DES
```

 **Note:**

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

## SNMPv3 User Name and Password Requirements

Property	Description
User Name	The SNMP user name can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers). Spaces not allowed.
Authentication Password	The Authentication Password is required when authentication protocol property is set to either MD5 or SHA.  Enter a case-sensitive Authentication password. The Authentication password can contain 8 to 12 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
Privacy Password	The Privacy Password is required when the privacy protocol property is set to DES or AES. The Privacy password must contain exactly 8 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers)

## Add an SNMP v3 User Account

1. Log in to the Oracle ILOM CLI.
2. To add an SNMP v3 read-only user account, type:

```
-> create /SP/services/snmp/users/ username
authenticationpassword= Password privacypassword= Password
```

Where:

- *username* can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
- authenticationpassword= *Password* is required when creating or modifying an SNMP v3 user account. The Authentication password can contain 8 to 12 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
- privacypassword= *Password* is only required when the Privacy Protocol property is set to DES or AES (default = None). The Privacy password must contain exactly 8 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers). To set the Privacy Protocol property, see [Set SNMP v3 User Account Privacy Protocol Value](#)

## Edit an SNMP v3 User Account

1. Log in to the Oracle ILOM CLI.

2. To edit an SNMP v3 user account, type:

```
-> set /SP/services/snmp/users/ username authenticationpassword=  
password privacypassword= Password
```

 **Note:**

When changing the parameters of SNMP users, you must provide a value for authenticationpassword, even if you are not changing the password.

*Where:*

- *username* can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
- authenticationpassword= *Password* is required when creating or modifying an SNMP v3 user account. The Authentication password can contain 8 to 12 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
- privacypassword= *Password* is only required when the Privacy Protocol property is set to DES or AES (default = None). The Privacy password must contain exactly 8 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers). To set the Privacy Protocol property, see [Set SNMP v3 User Account Privacy Protocol Value](#)

## Delete an SNMP v3 User Account

1. Log in to the Oracle ILOM CLI.
2. To delete an SNMP v3 user account, type:

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

## Set SNMP v3 User Account Privacy Protocol Value

### Before You Begin

- By default, the Privacy Protocol property is set to None.
- If the Privacy Protocol property is set to DES or AES, a privacy password must be provided when creating or modifying an SNMP v3 User Account. For further details about creating or editing an SNMP v3 User Account, see [Add an SNMP v3 User Account](#) or [Edit an SNMP v3 User Account](#).

1. Log in to the Oracle ILOM CLI.
2. To modify the privacyprotocol property value assigned to an SNMP v3 user account, type:

```
-> set /SP/services/snmp/users/ username authenticationpassword=  
password privacyprotocol=<DES|AES|None>
```

 **Note:**

When changing the parameters of SNMP users, you must provide a value for `authenticationpassword`, even if you are not changing the password.

 **Note:**

The SNMPv3 AES (Advanced Encryption Standard) option is available in Oracle ILOM as of 3.0.16.

Where:

- `username` can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
- `authenticationpassword= password` is required when creating or modifying an SNMP v3 user account. The Authentication password can contain 8 to 12 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
- DES is the acronym for Digital Encryption Standard and AES is the acronym for Advanced Encryption Standard.

## Managing SNMP Trap Alerts Using the Oracle ILOM

- [Configure SNMP Trap Rule Destinations and Properties](#)
- [CLI Commands for Managing Alert Rule Configurations](#)

## Configure SNMP Trap Rule Destinations and Properties

### Before You Begin

- To create or edit alert rules in Oracle ILOM, you need the Admin (a) role enabled.
- For you to define an SNMP v3 trap alert, the SNMPv3 user name must be defined in Oracle ILOM. If the SNMP v3 user name is not defined in Oracle ILOM, the SNMP v3 user receiving the SNMP alert will not be able to decode the SNMPv3 alert message. For more information about defining SNMPv3 authorization and SNMP v3 users in Oracle ILOM, see [Managing SNMP User Accounts and SNMP Trap Alerts \(CLI\)](#).
- Review [CLI Commands for Managing Alert Rule Configurations](#).
- For additional information about configuring alert management settings in Oracle ILOM, refer to *Configuring Alert Notifications in Oracle ILOM 5.1 Administrator's Guide*.

To configure the destinations to which the SNMP traps are sent, follow these steps:

1. Log in to the Oracle ILOM CLI.
2. To display the current settings of the alert rule, type the show command.

For example:

```
-> show /SP/alertmgmt/rules/1
/SP/alertmgmt/rules/1
  Targets:

  Properties:
    type = snmptrap
    level = disable
    destination = 0.0.0.0
    destination_port = 0
    community_or_username = public
    testrule = (Cannot show property)

  Commands:
    cd
    set
    show
```

 **Note:**

When you test an alert notification rule, Oracle ILOM will send a test from all configured SNMP traps. Oracle ILOM does not have the ability to filter SNMP traps by destination.

3. To show the /SP/alertmgmt/rules directory, type:

```
-> cd /SP/alertmgmt/rules
-> show
```

For example:

```
->
    cd /SP/alertmgmt/rules

-> show
/SP/alertmgmt/rules
  Targets:
    1
    2
    .
    .
    15
  Properties:

  Commands:
    cd
    show
```

Choose a rule (from targets 1 through 15) for which you would like to configure a destination for SNMP traps, and go to that directory.

For example:

```
-> cd 4
```

4. To change the rule properties, within that rule directory, type the set command.

For example, to set a rule to send critical traps to a management client using SNMP v2c using a community name of “public”, enter:

```
-> set type=snmptrap level=critical destination=  
IPAddress_of_snmp_management_station destination_port=port  
snmp_version=2c community_or_username=public
```

## CLI Commands for Managing Alert Rule Configurations

The following table describes the CLI commands that you use to manage alert rule configurations in the Oracle ILOM CLI.

**Table 3-2 CLI Commands for Managing Alert Rule Configurations**

CLI Command	Description
show	The <code>show</code> command enables you to display any level of the alert management command tree by specifying either the full or relative path.
cd	The <code>cd</code> command enables you to set the working directory. To set alert management as a working directory on a server SP, type the following command at the command prompt:  -> cd /SP/alertmgmt
set	The <code>set</code> command enables you to set values to properties from any place in the tree. You can specify either a full or relative path for the property depending on the location of the tree. For example: <ul style="list-style-type: none"> <li>For full paths, type the following at the command prompt: -&gt; set /SP/alertmgmt/rules/1 type=snmptrap</li> <li>For relative path (tree location is /SP/alertmgmt), type the following command path at the command prompt: -&gt; set rules/1 type=snmptrap</li> <li>For relative path (tree location is /SP/alertmgmt/rules/1), type the following command path at the command prompt: -&gt; set type=snmptrap</li> </ul>

## Managing SNMP User Accounts and SNMP Trap Alerts (Web)

- [Set SNMP Management Access and Authorization](#)
- [Managing SNMP User Accounts and Communities](#)

- [Manage SNMP Trap Alerts](#)

## Set SNMP Management Access and Authorization

### Before You Begin

- To modify SNMP properties in Oracle ILOM, you must have the Admin role (a) enabled.
- The SNMP `service` state is, by default, shipped from the factory *enabled*.
- Oracle ILOM provides authentication properties for SNMP v3.
  - For SNMP v3, Oracle ILOM provides a `users` property to manage user authentication. The `users` property is, by default, shipped from the factory *enabled*. The SNMP v3 `users` property is not shipped from the factory with pre-packaged values for users.

To set the SNMP service state, properties:

1. Log in to the Oracle ILOM web interface.
2. On the left navigation panel, click ILOM Administration.
3. Click Management Access > SNMP.  
The SNMP Management page appears.
4. To enable the SNMP port, click the State check box.  
When State is disabled, the SNMP port is blocked, prohibiting all SNMP communication between Oracle ILOM and the network.
5. In the Port text field, type the port number.
6. Leave the Engine ID field blank. This allows the default setting to be used.  
The engine ID is automatically set by the SNMP agent. While you can use this field to set the engine ID, you should leave this field blank. The engine ID uniquely identifies the SNMP engine and enables users to query the SNMP agent. Use this field to set the engine ID only if you are familiar with SNMP v3 security and how this setting is used.
7. To enable SNMP v3, click a Protocols check box.  
SNMP v3 is enabled by default.
8. Click Save.  
At the bottom of the SNMP Management page, you can also add, edit, or delete SNMP communities or users.

## Managing SNMP User Accounts and Communities

- [Before You Begin SNMP User Accounts](#)
- [Add or Edit an SNMP v3 User Account](#)
- [Delete an SNMP v3 User Account](#)

### Before You Begin SNMP User Accounts

Before performing the procedures in this section, ensure that the following requirements are met:



- To set user account properties in Oracle ILOM, you need the User Management (u) role enabled.
- Verify that the proper SNMP settings are enabled in Oracle ILOM. For more details, see [Set SNMP Management Access and Authorization](#).
- To execute the `snmpset` command, you need to use an SNMP v3 user account with read-write (rw) privileges.

## Add or Edit an SNMP v3 User Account

To add or edit an SNMP v3 user account, follow these steps:

1. Log in to the Oracle ILOM web interface.
2. On the left navigation panel, click ILOM Administration.
3. Then click Management Access > SNMP.  
The SNMP Management page appears.
4. Click the Users link to expand the SNMP Settings page and display SNMP Users.
5. To add an SNMP user, click Add.  
The Add User dialog box appears.
6. To edit an SNMP user, do the following:
  - a. Click the appropriate user radio button
  - b. Click Edit.  
The Edit SNMP User Information dialog box appears.
7. If you are adding a user, type a user name in the User Name text field; otherwise proceed to the next step.  
The user name can include up to 35 characters. It must start with an alphabetic character and cannot contain spaces.
8. In the Authentication Protocol drop-down list, select either Message Digest 5 (MD5) or Secure Hash Algorithm (SHA).
9. In the Authentication Password text field, type a password.  
The authentication password is case-sensitive and must contain 8 to 16 characters, with no colons or space characters.
10. In the Confirm Password text field, retype the authentication password.
11. (Optional) To specify a privacy protocol, perform the following steps:
  - a. In the Privacy Protocol list box, select DES (Digital Encryption Standard) or AES (Advanced Encryption Standard).

 **Note:**

The AES privacy protocol option is available only for SNMPv3 as of ILOM 3.0.16.

- b. In the Privacy Password text box, type a password for the privacy algorithm specified in Step 12a.

The Privacy password must contain exactly 8 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers) .

 **Note:**

The privacy password is only required if you selected DES or AES in Step 12a.

- c. In the Confirm Password field, retype the privacy password to ensure that it matches the privacy password specified in Step 12b.
12. Click Save to apply the SNMP user account properties.

## Delete an SNMP v3 User Account

To delete an SNMP v3 user account, follow these steps:

1. Log in to the Oracle ILOM web interface.
2. On the left navigation panel, click ILOM Administration.
3. Then click Management Access > SNMP.  
The SNMP Management page appears.
4. Click the Users link or scroll down to the SNMP Users list.
5. Click the radio button of the SNMP user account to delete.
6. Click Delete under the SNMP User's List.  
A confirmation dialog box opens.
7. Click OK to delete the user account.

## Manage SNMP Trap Alerts

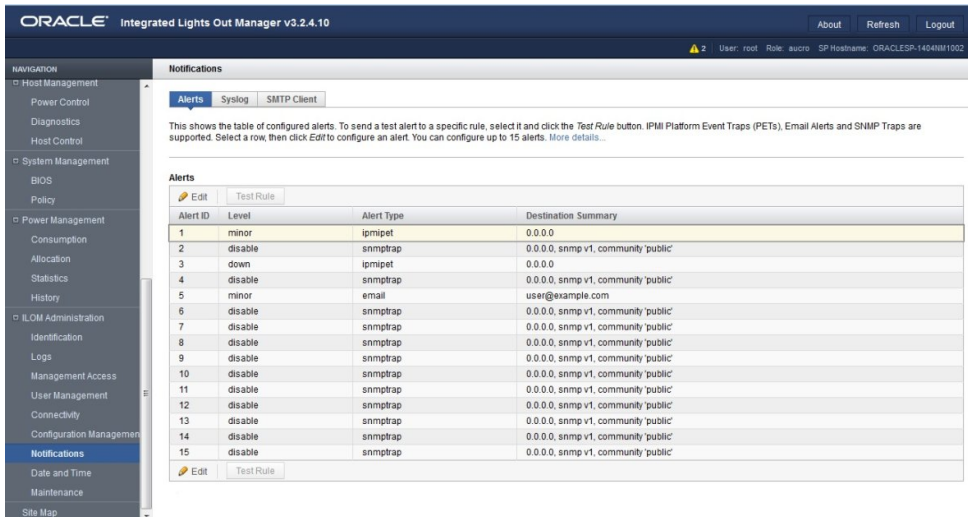
### Before You Begin

- To create or edit SNMP trap alert rules in Oracle ILOM, you need the Admin (a) role enabled.
- To define an SNMP v3 trap alert, you must define the SNMP v3 user name must be defined in Oracle ILOM. If the SNMP v3 user name is not defined in Oracle ILOM, the SNMP v3 user receiving the SNMP alert cannot decode the SNMP v3 alert message. For more information about defining SNMP v3 authorization and SNMP v3 users in Oracle ILOM, see [Managing SNMP User Accounts and SNMP Trap Alerts \(Web\)](#).
- For additional information about configuring alert management settings in Oracle ILOM, refer to [Configuring Alert Notifications](#).

To configure SNMP Trap Alert properties, follow these steps:

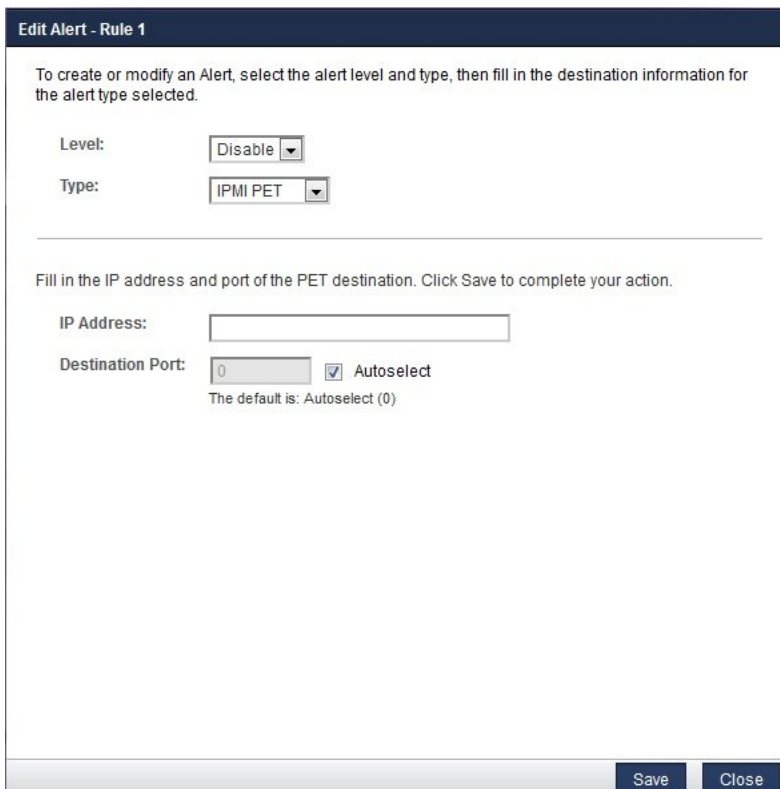
1. Log in to the Oracle ILOM web interface.
2. On the left navigation panel, click ILOM Administration.
3. Click Notifications > Alerts.

The Alert Settings page appears. This page shows a table of the alerts that you can configure. You can configure up to 15 alerts.



4. To create or modify an alert, click the alert radio button.
5. Then click Edit.

The Create or Modify Alert dialog appears.



6. In the Level drop-down list, select the level of the alert.

7. In the Type drop-down list, select the alert type.
8. In the IP Address field, specify the alert destination IP address.
9. Click Save for your changes to take effect.

## Downloading SNMP MIBs Using Oracle ILOM

- [Before You Begin Download SNMP MIBs](#)
- [Download SNMP MIBs \(CLI\)](#)
- [Download SNMP MIBs \(Web\)](#)

### Before You Begin Download SNMP MIBs

- The Reset and Host Control (r) role is required for you to download SNMP MIBs to Oracle ILOM.
- You must be using Oracle ILOM firmware version 3.0.4 or later.

### Download SNMP MIBs (CLI)

1. Log in to the Oracle ILOM CLI.
2. Use the show command to display the SNMP MIBs.

For example:

```
-> show /SP/services/snmp/mibs

/SP/services/snmp/mibs
  Targets:

  Properties:
    dump_uri = (Cannot show property)

  Commands:
    cd
    dump
    set
    show
```

3. To download the files, type either of the following commands:

```
-> dump -destination URI /SP/services/snmp/mibs
```

or

```
-> set /SP/services/snmp/mibs dump_uri=URI
```

where *URI* specifies the target to which the files are downloaded.

A zip file containing the MIBs are transferred to the destination server.

### Download SNMP MIBs (Web)

1. Log in to the Oracle ILOM web interface.
2. On the left navigation panel, click ILOM Administration.

3. Click Management Access > SNMP.  
The SNMP Management page appears.
4. Click the MIBs link at top of page or scroll down to the MIBs section.
5. Click Download, and then click Save and enter the destination to save the zip file.  
A zip file containing the MIBs is transferred to the destination server.

# 4

## View Component Information and the Oracle ILOM Event Log (SNMP)

Description	Links
Learn how to view component information.	<ul style="list-style-type: none"><li><a href="#">Viewing Component Information</a></li></ul>
Learn how to view the log entries in the Oracle ILOM Event Log.	<ul style="list-style-type: none"><li><a href="#">Viewing the Oracle ILOM Event Log</a></li></ul>

### Related Information

- Configuring Alert Notifications, Service Requests, or Remote Logging

### Viewing Component Information



#### Note:

You can use `get` commands to view component information. For a description of valid MIB objects for this procedure, see the table following this procedure.

Follow these steps to view component MIB information.

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

```
ssh username @ snmp_manager_ip_address
```

```
Password : password
```

2. To view the firmware revision, type:

```
% snmpget  
  
SNMP_agent  
entPhysicalFirmwareRev.1
```

The following table describes the Component Information SNMP MIB objects.

MIB Object	Description	Values	Type	Default
entPhysicalName	The textual name of the physical entity.	Size: 0 to 255	String	Zero-length string
entPhysicalDescr	A textual description of the physical entity.	Size: 0 to 255	String	None

MIB Object	Description	Values	Type	Default
entPhysical ContainedIn	The value of entPhysicalIndex for the physical entity that <i>contains</i> this physical entity. A value of 0 indicates this physical entity is not contained in any other physical entity.	Range: 0 to 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 to 255	String	Zero- length string

## Viewing the Oracle ILOM Event Log



### Note:

You can use the `get` command to view the Oracle ILOM event log and the `set` command to configure the event log. For a description of valid MIB objects for this procedure, see the table following this procedure.

Follow these steps to view the MIB objects associated with the Oracle Event Log.

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

```
ssh username @ snmp_manager_ip_address
```

```
Password: password
```

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

```
% snmpget
```

```
SNMP_agent  
ilomSystemLogTable
```

The following table describes the Oracle ILOM Event Logs SNMP MIB objects.

<b>MIB Object</b>	<b>Description</b>	<b>Type</b>
ilomSystemLogRecordID	Unsigned32	The record number uniquely identifying the ilomSystem log entry.
ilomSystemLogTimestamp	DateAndTime	The date and time that the ilomSystem log entry was recorded.
ilomSystemLogSubsystem	SnmpAdminString	The subsystem the event pertains to.
ilomSystemLogComponent	SnmpAdminString	The component the event pertains to.
ilomSystemLogDescription	OCTET STRING	A textual description of the event.



# 5

## Server Management Using IPMI

Description	Links
Learn about using IPMItool to manage Oracle servers.	<ul style="list-style-type: none"><li>• <a href="#">Intelligent Platform Management Interface (IPMI)</a></li></ul>
Learn how to configure the IPMI state and perform various management functions using the IPMItool.	<ul style="list-style-type: none"><li>• <a href="#">Managing IPMI Properties in Oracle ILOM</a></li><li>• <a href="#">Using IPMItool to Run Oracle ILOM CLI Commands</a></li><li>• <a href="#">Performing System Management Tasks (IPMItool)</a></li></ul>
Learn about the IPMI commands.	<ul style="list-style-type: none"><li>• <a href="#">IPMItool Options and Command Summary</a></li></ul>

### Related Information

- [Modifying Default Management Access Configuration Properties in Oracle ILOM 5.1 Administrator's Guide](#)

## Intelligent Platform Management Interface (IPMI)

- [About IPMI](#)
- [IPMI TLS Service and Interface](#)
- [IPMItool](#)
- [IPMI Alerts](#)
- [IPMI Administrator and Operator Roles](#)

### About IPMI

Oracle ILOM supports the Intelligent Platform Management Interface (IPMI), which enables you to monitor and control your server, as well as to retrieve information about your server.

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 management functionality that is built into the platform hardware.

### IPMI Service State and Supported IPMI Sessions

By default, the IPMI service state in Oracle ILOM is enabled. The following IPMI sessions are supported as of Oracle ILOM firmware version 5.0.0:

- TLS Sessions — Enabled by default.
- IPMI v2.0 Sessions — Disabled by default

The service processors (SPs) on your Oracle managed devices (servers, blade server modules, and so on) are IPMI compliant. You can access IPMI functionality through the command line using the `IPMITool` interface 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 Oracle ILOM web interface, or manage the SP IPMI functions from any external management solution that is IPMI compliant. For more information about the IPMITool utility, see [IPMITool](#).



#### Note:

For IPMI technical resources, including specifications, refer to the Intel and Sourceforge sites: <http://openipmi.sourceforge.net>

## IPMI TLS Service and Interface

IPMI TLS is an Oracle improvement to IPMI security which requires a special version of the `ipmitool` client that supports TLS sessions. The `IPMITool` command option to access the TLS interface is:


```
ipmitool -I orcltls
```

Note that in cases where the `-I` option is not specified, the `IPMITool` utility will negotiate to the most secure interface available (in the following order):

- TLS 1.2 (`orcltls` interface)
- IPMI 2.0 (`lanplus` interface)

## TLS Session Feature Summary

Feature	Description
Secure Communication Protocol Data Transmission	A secure TLS/TCP socket connection is used (over Ethernet and LAN over USB) to transmit and receive data between the IPMI client the server SP.
Negotiation of Highest Cipher Suite	IPMI/TLS client sessions negotiate to highest cipher suite supported on the server SP.

Feature	Description
Authentication	<p>Uses local SP authorization to validate user credentials and to set client session privileges.</p> <div data-bbox="1084 365 1378 716" style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <p>LDAP, Active Directory, and RADIUS user authorization is currently not supported as of firmware Oracle ILOM 3.2.8.</p> </div>
Audit Log of IPMI Login Events	<p>The Audit Log captures all IPMI login events (successful and failed attempts).</p>
SSL Certificate Validation	<p>Automatically validates the SSL client certificate against a list of trusted certificates stored in the user specified directory (<code>ipmitool --cert-dir</code> option).</p> <p>Note that when the IPMI TLS interface (<code>orcltls</code>) is unable to validate the client certificate, the user is prompted to cross-check the certificate's authentic fingerprint with the SSL certificate authentic fingerprints stored in the local SP directory (<code>/SP/services/https/ssl</code>). If a match is not found, the user should respond <code>No</code>. Otherwise, if a match is found, the user should respond <code>Yes</code> to proceed.</p> <p>For information about how to disable the check option for certificate validation when the <code>orcltls</code> interface is specified see, <a href="#">Disable Default TLS Behavior for SSL Certificate Check</a>.</p> <p>For information about uploading and managing SSL certificates on the server SP, see <i>SSL Certificate and Private Key Configuration Properties for HTTPS Web Server</i> in <i>Oracle ILOM 5.1 Administrator's Guide</i>.</p>

## TLS IPMItool Interface Download Requirement

Prior to executing Oracle ILOM commands from the TLS ipmitool interface, you must download the Oracle TLS components (OS compliant driver and the `orcltls` IPMItool interface) from Oracle Hardware Management Pack. For instance, to download the Oracle TLS components from Oracle Hardware Management Pack, follow this process:

1. On the managed device, download Oracle Hardware Management Pack (v2.4 or later for Linux or v4.0 or later for Oracle Solaris) from My Oracle Support.

 **Note:**

The Oracle TLS components (OS compliant driver and the `orcltls` IPMItool interface) are not available for download from the Oracle Hardware Management Pack for Windows.

2. Launch the installer for the Hardware Management Component GUI by following the instructions in the *Oracle Hardware Management Pack Installation Guide*.

The Oracle Hardware Management Pack documentation is available for download at: <http://docs.oracle.com/en/servers/management.html>

3. After launching the installer for the Hardware Management Component GUI, choose the Custom Install.
4. In the Custom Install Set menu, choose IPMItool.
5. Continue to follow the instructions in the *Oracle Hardware Management Pack Installation Guide* to complete the installation.

## IPMItool

IPMItool is an open-source simple command-line interface (CLI) utility for managing and configuring IPMI-enabled devices. The utility can be used to manage the IPMI functions of a local or remote system with a kernel device driver or over a LAN interface. Versions of the IPMItool utility for all Oracle ILOM supported IPMI interfaces are available for download from the Oracle Hardware Management Pack.

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.

IPMItool features command-line help, which can be accessed by typing `ipmitool help` at the command-line prompt.

IPMItool supports a feature that enables you to enter Oracle ILOMCLI 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. For additional information, see [Using IPMItool to Run Oracle ILOM CLI Commands](#).

## IPMI Alerts

Oracle ILOM supports alerts in the form of IPMI Platform Event Trap (PET) alerts. Alerts provide advance warning of possible system failures. Alert configuration is available from the SP on your server. IPMI PET alerts are supported on Oracle server SPs; however, IPMI PET alerts are not supported on chassis monitoring modules (CMMs). For more information about IPMI alerts, refer to *Configuring Alert Notifications* in *Oracle ILOM 5.1 Administrator's Guide*.

## IPMI Administrator and Operator Roles

The *IPMI Administrator* role maps to these user roles in Oracle ILOM: `aucro`. The *IPMI Operator* role maps to these user roles in Oracle ILOM: `cro`. A brief explanation of these Oracle ILOM roles appears in the following table.

**Table 5-1 IPMI Administrator and Operator Roles in Oracle ILOM**

IPMI Role	Enabled ILOM Role Privileges	Description
Administrator	<ul style="list-style-type: none"> <li>Admin (a)</li> <li>User Management (u)</li> <li>Console (c)</li> <li>Reset and Host Console (r)</li> <li>Read-Only (o)</li> </ul>	These user roles enable read and write privileges to these management features in Oracle ILOM: system management configuration properties, user account properties, remote console management properties, remote power management properties, and reset and host control management properties.
Operator	<ul style="list-style-type: none"> <li>Console (c)</li> <li>Reset and Host Console (r)</li> <li>Read-Only (o)</li> </ul>	These user roles enable read and write privileges to these management features in Oracle ILOM: remote console management properties, remote power management properties, and reset and host control management properties.



### Note:

The Read-Only role provides read access to system management configuration properties and user management properties.

For more information about Oracle ILOM roles and privileges, refer to *Managing User Credentials* in *Oracle ILOM 5.1 Administrator's Guide*.

## Managing IPMI Properties in Oracle ILOM

- [Set the IPMI State and Session Properties \(CLI\)](#)
- [Set the IPMI State and Session Properties \(Web\)](#)

### Set the IPMI State and Session Properties (CLI)

#### Before You Begin

- The IPMI state property in Oracle ILOM is enabled by default.
- As of Oracle ILOM firmware v5.0.x, the following IPMI properties are shipped enabled: **Service State**, and **TLS Sessions**. The session property for v2.0 is shipped disabled.

- Admin (a) role privileges are required to change the IPMI Service State or Session properties in Oracle ILOM.

 **Note:**

The TLS Session property is always enabled and cannot be modified.

Follow these steps to set the IPMI state and sessions properties using the Oracle ILOM CLI:

1. Log in to the Oracle ILOM CLI using an account with admin (a) role privileges.
2. To set the IPMI state property, issue the following command:

```
-> set /SP/services/ipmi state=[enabled|disabled]
```

Where: `[enabled|disabled]`, type `enabled` to enable the `ipmi state` property, or type `disabled` to disable the `ipmi state` property.

 **Note:**

If the IPMI Service State is disabled, system management information using the IPMItool utility is not accessible.

3. To set the IPMI session properties, issue the following command:

```
-> set /SP/services/ipmi [v2_0_sessions=enabled|disabled]
```

 **Note:**

TLS sessions (`tls_sessions`) are enabled by default. To disable TLS sessions, you must disable the IPMI State property.

Where:

- `[v2_0_sessions=enabled|disabled]` applies only to the IPMI v2.0 session property. Type: `v_2_0_sessions=enabled` to enable the IPMI v2.0 sessions; **or** Type: `v_2_0_sessions=disabled` to disable the IPMI v2.0 sessions.

## Set the IPMI State and Session Properties (Web)

### Before You Begin

- The IPMI state property in Oracle ILOM is enabled by default.
- As of Oracle ILOM firmware v5.0.x, the following IPMI properties are shipped enabled: **Service State**, and **TLS Sessions**. The session property for v2.0 is shipped disabled.

- Admin (a) role privileges are required to change the IPMI state or session properties in Oracle ILOM.

Follow these steps to set the IPMI state and sessions properties using the Oracle ILOM web interface:

1. Log in to the Oracle ILOM web interface using an account with admin (a) role privileges.
2. Click ILOM Administration → Management Access > IPMI.

The IPMI page appears.

3. In the IPMI page, enable or disable the property check boxes for IPMI State and v2.0 Sessions.

 **Note:**

If the IPMI Service State property is disabled, system management information using the IPMItool utility is not accessible.

## Using IPMItool to Run Oracle ILOM CLI Commands

The IPMItool CLI is a convenient alternative method to executing Oracle ILOM CLI commands. It enables you to enter commands just as if you were using the Oracle ILOM CLI directly. Most Oracle ILOM CLI commands are supported.

- [IPMItool and Oracle ILOM Requirements](#)
- [Access the Oracle ILOM CLI From IPMItool](#)
- [Disable Default TLS Behavior for SSL Certificate Check](#)
- [Scripting Oracle ILOM CLI Commands With IPMItool](#)

## IPMItool and Oracle ILOM Requirements

Prior to using the IPMItool to execute Oracle ILOM commands, review these requirements:

- Use the latest IPMItool that is available from the Oracle Hardware Management Pack.

 **Note:**

IPMItool users can check the version number of the IPMItool by specifying the `-v` option (`ipmitool -v`).

- To use the IPMI TLS interface, IPMItool users must use IPMItool v1.8.15.0 or later that is available for download from Oracle Hardware Management Pack for Linux (as of v2.4 and later) and Oracle Hardware Management Pack for Solaris (as of v4.0 and later).

 **Note:**

To access the IPMI TLS interface, IPMItool users can either specify the `-I orcltls` option or not specify an option and the IPMItool will automatically detect the most secure interface available.

- Ensure that you have the proper user roles assigned in Oracle ILOM when using the IPMItool utility to execute Oracle ILOM commands. For more information, see [IPMI Administrator and Operator Roles](#).
- Unless otherwise noted, commands described in this section accept options and other arguments according to the following syntax:

```
ipmitool [option(s) -I [orcltls|lanplus] -H
[hostserveraddress] [hostserveroptions]

[command issued]

[system output]
```

**Where:**

- `[option(s)]` can include: `-c [cipher suite level]` | `-h` (to display help) | `-v` (to display verbose output) | `-V` (to display version number)
- `-I` identifies the selected IPMI interface such as `-I orcltls` (IPMI TLS interface) | `-I lanplus` (IPMI v2.0 interface).

 **Note:**

If an IPMI interface is not specified, the IPMItool defaults to the most secure IPMI interface supported on the host server.

- `-H [hostserveraddress]` identifies the remote server SP hostname or IP address. The `[hostserveroption(s)]` must always specify: `-U [username]` `-P [password]`. The `[hostserveroption(s)]` can also include optional options such as `-p [portnumber]` | `-R [retries count]`

 **Note:**

Required host options for all IPMI interfaces include: `-H [hostserveraddress]` `-U [username]` and `-P [password]`.

- `[ command issued ]` can either identify a dedicated ILOM IPMItool command or a Sunoem ILOM command.
- `[system output]` displays the command results.

For more details, see the [IPMItool Options and Command Summary](#) .



 **Note:**

If you encounter command-syntax problems with your particular operating system, you can use the IPMItool `-h` option to determine which parameters can be passed with the IPMItool command on your operating system. Also refer to the IPMItool man page by typing: `man ipmitool`.

## Access the Oracle ILOM CLI From IPMItool

Follow these steps to access Oracle ILOM from an IPMItool client.

1. To enable the Oracle ILOM CLI using IPMItool, type:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U  
username  
-P  
password  
sunoem cli
```

The Oracle ILOM CLI prompt appears as follows:

```
Connected. Use ^D to exit.  
->
```

2. To use the Oracle ILOM CLI, type CLI commands.

For information on how to script Oracle ILOM CLI commands, see [Scripting Oracle ILOM CLI Commands With IPMItool](#).

## Disable Default TLS Behavior for SSL Certificate Check

Follow this step to disable the default TLS option for SSL Certificate checks.

- To disable the validation of the SSL certificate when accessing the IPMI TLS interface (orcltls), issue the `--no-check-certificate` command. For example:

```
$ ipmitool -I orcltls -H SP_hostname_or_IPaddress -U username -P  
password --no-cert-check
```

 **Note:**

For security reasons, the SSL certificate is automatically verified upon accessing the IPMI TLS interface (orcltls). For additional information about the SSL certificate check, see [IPMI TLS Service and Interface](#).

## Scripting Oracle ILOM CLI Commands With IPMItool

A key benefit of using Oracle 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 Oracle ILOM CLI command. Command separation is achieved by including quotation marks at the beginning and end of each Oracle ILOM CLI command.

The following example shows how to include two CLI commands on the IPMItool command line. In the example, notice that each command begins and ends with quotation marks.

```
#
ipmitool -H
SP_hostname_or_IPaddress
-U
username
-P
password
sunoem cli
"show /SP/services" "show /SP/logs"
Connected. Use ^D to exit.
-> show /SP/services
/SP/services
Targets:
  http
  https
  ipmi
  kvms
  servicetag
  snmp
  ssh
  sso

Properties:

Commands:
  cd
  show

-> show /SP/logs
/SP/logs
Targets:
  audit
  event

Properties:

Commands:
  cd
  show
-> Session closed
Disconnected
```

## Performing System Management Tasks (IPMItool)

To perform system management tasks using the IPMItool, see these topics:

- [Display Sensor List](#)
- [View Single Sensor Details](#)

- [View and Interpret Presence Sensor Type Values](#)
- [Manage Host Power-On, Power-Off and Shutdown Functions](#)
- [Manage Oracle ILOM Power Budget Interfaces](#)
- [Manage the System Power Policy](#)
- [Display FRU Manufacturing Details](#)
- [Display Oracle ILOM Event or Audit Log](#)

## Display Sensor List

Follow this step to display the sensor list for a managed device.

- To view a list of sensors on a managed device, type:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U  
username  
-P  
password  
  
sdr list
```

### Note:

The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IPMITool utility. For more information about using the IPMI TLS interface from Oracle, see these topics: [IPMI TLS Service and Interface](#) and [Configure IPMI Management Access for Increased Security in Oracle ILOM Security Guide For Firmware Release 5.1.x](#).

The output might look like the following:

```
/SYS/T_AMB          | 24 degrees C          | ok  
/RFM0/FAN1_SPEED   | 7110 RPM              | ok  
/RFM0/FAN2_SPEED   | 5880 RPM              | ok  
/RFM1/FAN1_SPEED   | 5880 RPM              | ok  
/RFM1/FAN2_SPEED   | 6360 RPM              | ok  
/RFM2/FAN1_SPEED   | 5610 RPM              | ok  
/RFM2/FAN2_SPEED   | 6510 RPM              | ok  
/RFM3/FAN1_SPEED   | 6000 RPM              | ok  
/RFM3/FAN2_SPEED   | 7110 RPM              | ok  
/RFM4/FAN1_SPEED   | 6360 RPM              | ok  
/RFM4/FAN2_SPEED   | 5610 RPM              | ok  
/RFM5/FAN1_SPEED   | 5640 RPM              | ok  
/RFM5/FAN2_SPEED   | 6510 RPM              | ok  
/RFM6/FAN1_SPEED   | 6180 RPM              | ok  
/RFM6/FAN2_SPEED   | 6000 RPM              | ok  
/RFM7/FAN1_SPEED   | 6330 RPM              | ok  
/RFM7/FAN2_SPEED   | 6330 RPM              | ok  
/RFM8/FAN1_SPEED   | 6510 RPM              | ok  
/RFM8/FAN2_SPEED   | 5610 RPM              | ok
```

 **Note:**

The sensor output shown in the preceding example was shortened. The actual output will depend on the hardware platform.

## View Single Sensor Details

Follow this step to view details of a single sensor on a managed device.

- To view details about a single sensor on a managed device, type:

```
sensor get /target/sensor_name
```

For example, to view sensor details about the system temperature (/SYS/T\_AMB), you would type:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -
U
username
-P
password
```

```
sensor get /SYS/T_AMB
```

 **Note:**

The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IPMItool utility. For more information about using the IPMI TLS interface from Oracle, see these topics: [IPMI TLS Service and Interface](#) and *Configure IPMI Management Access for Increased Security in Oracle ILOM Security Guide For Firmware Release 5.1.x*

The output might look like the following:

```
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+
```

## View and Interpret Presence Sensor Type Values

### Before You Begin

- The IPMItool supports the output of a `States Asserted` field for each presence sensor type record. This `States Asserted` field can appear in the IPMItool output as either:
  - `States Asserted = Entity Presence`  
When the `States Asserted = Entity Presence` field appears, the sensor output for a hardware component can show one of three valid values: `Present (=1)`, `Absent (=2)`, `Disabled (=4)`.
  - `States Asserted = Availability State`  
When the `States Asserted = Availability State` field appears, the sensor output for a hardware component can show one of two valid values: `Device Absent (=1)` and `Device Present (=2)`.

#### Note:

Oracle ILOM supports the output of both `States Asserted` fields. However, some Oracle hardware platforms might support both or one of the possible `States Asserted` fields (`Entity Presence` or `Availability State`).

For additional information about how to interpret values presented for IPMI presence sensor types, refer to Section 42 - Sensor and Event Code Tables in the IPMI 2.0 Specifications. Understanding all of Section 42 is critical in understanding how to interpret a sensor value.

To view and interpret IPMItool present sensor type values, follow these steps:

1. To view the actual sensor reading for hardware components, use the IPMItool `sdr list` command.

For example, after issuing the `sdr list` command the following presence sensor type readings appear for PCIe hardware components.

```
PCIE_CC/PRSNT | 0x02 | ok
PCIE0/F20/PRSNT | 0x01 | ok
```

2. To determine the `States Asserted` field value for a presence sensor type, use the IPMItool `sensor get` command.

One of the following `States Asserted` fields appear after issuing the `sensor get` command from the IPMItool:

- `States Asserted = Entity Presence`

In the following example, the value shown for the `States Asserted = Entity Presence` field is *Absent*.

```
$ ipmitool sensor get PCIE_CC/PRSNT
Locating sensor record...
Sensor ID           : PCIE_CC/PRSNT (0xad)
```

```
Entity ID           : 49.0
Sensor Type (Discrete): Entity Presence
States Asserted    : Entity Presence
[Absent]
```

- States Asserted = Availability State

In the following example, the value shown for the States Asserted = Availability State field is *Device Absent*.

```
$ ipmitool sensor get PCIE1/PRSNT
Locating sensor record...
Sensor ID           : PCIE1/PRSNT (0xe6)
Entity ID           : 11.0
Sensor Type (Discrete): Entity Presence
States Asserted    : Availability State
[Device Absent]
```

## Manage Host Power-On, Power-Off and Shutdown Functions

### Note:

The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IPMITool utility. For more information about using the IPMI TLS interface from Oracle, see these topics: [IPMI TLS Service and Interface](#) and *Configure IPMI Management Access for Increased Security in Oracle ILOM Security Guide For Firmware Release 5.1.x*

Follow these steps to specify the host power functions for a managed device.

1. To power on the host on a managed device, type: chassis power on

Example:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -
U
username
-P
password

chassis power on
```

2. To power off the host on a managed device, type: chassis power off

Example:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -
U username

-P
password
```

```
chassis power off
```

3. To power cycle the host on a managed device, type: chassis power cycle

Example:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U
username -P password
```

```
chassis power cycle
```

4. To gracefully shut down the host power on a managed device, type: chassis power soft

Example:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U
username -P password
```

```
chassis power soft
```

## Manage Oracle ILOM Power Budget Interfaces

### Note:

The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IPMItool utility. For more information about using the IPMI TLS interface from Oracle, see these topics: [IPMI TLS Service and Interface](#) and *Configure IPMI Management Access for Increased Security in Oracle ILOM Security Guide For Firmware Release 5.1.x*

Follow these steps to set the power budget properties on a managed device.

1. To set the Power Limit Activation State on a managed device, use one of the following commands:

- To activate, type:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U
username -P password
```

```
raw 0x2e 0x49 0x00 0x01 0xFF 0xFF
```

Upon command completion:

```
dc
```

- To deactivate, type:

```
$ ipmitool -I [orclt1s|lanplus] -H
SP_hostname_or_IPaddress -U username -P password
```

```
raw 0x2e 0x49 0x00 0x00 0xFF 0xFF
```

Upon command completion:

```
dc
```

The following table describes the Power Limit Activation State (IPMITool) input and output fields.

Fields	Byte	Description
Input Data	1	Sunoem command group number: 0x2e.
	2	Command code 0x49 sets the power limit activation state.
	3	Group extension identification: 0x00. The value for this field is ignored.
	4	Sub-commands for power limit activation: 0x00 - Deactivate power limit 0x01 - Activate power limit
	5-6	Reserved fields 0xFF. The values for these fields are ignored.
Output Data	1	Completion code consumed by IPMITool.  The system does not display a status for successful completion code. However, if the result of the completion code is anything other than 'successful', a failure message appears.
	2	Group extension identification dc' appears upon command completion.

- To get Power Limit Budget properties, type:

 **Note:**

You should use a Get Power Limit Budget Wattage command prior to setting the Power Limit Budget Wattage property.



```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U
username -P password
```

```
raw 0x2e 0x4A 0x00 0x00 0x00
```

Upon command completion:

```
dc 00 01 b3 00 02 fa 00 00 00 00 01 e9 00 00
```

The following table describes the Get Power Limit (IPMItool) input and output fields:

Field	Byte	Description
Input Data	1	Sunoem command group number: 0x2e.
	2	Command code 0x4A gets Power Budget settings.
	3	Group extension identification: 0x00. The value for this field is ignored.
	4-5	Reserved fields 0x00. Values for these fields are ignored.
Output Data	1	Completion code, consumed by IPMItool. Not displayed upon command completion. However if completion code is anything other than success, then a failure message is displayed upon command completion.
	2	Group extension identification. Displayed as 'dc' in the preceding example.
	3	Activation state: 00 - Deactivated 01 - Activated
	4	Reserved field. Note that the value b3 in the preceding example can be ignored.
	5	Exception action, taken if power limit is exceeded and cannot be controlled within the correction time limit. Return values: 00 - None 01 - Hard power-off
	6-7	Power limit in watts. 02 fa in the preceding example.
	8-11	Correction time limit in milliseconds. 00 00 00 00 in the preceding example.

Field	Byte	Description
	12	Flag indicating whether the correction time limit is the system default time limit. 00 - Not default 01 - Default
	13	Reserved field. Note that the value shown (e9) in the preceding example can be ignored.
	14-15	Reserved fields. Note that the value shown (00 00) in the preceding example can be ignored.

3. To set the Power Limit, type:

 **Note:**

The set power limit commands sets the power budget limit for the system. Use this command to set the maximum system power usage. The power limit should always be persistent across AC and DC cycles.

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -
U username -P password
```

```
raw 0x2e 0x4B 0x00 0xff 0xff 0xff 0x01 0x02 0xaa 0x00 0x00
0x1b 0x58 0x00 0xff 0x00 0x00
```

Upon command completion:

```
dc 00
```

The following table describes Set Power Limit (IPMItool) input and output fields:

Fields	Byte	Description
Input Data	1	Sunoem command group number: 0x2e.
	2	Command code 0x4B sets power budget settings.
	3	Group extension identification: 0x00. The value for this field is ignored.
	4-6	Reserved fields: 0xff 0xff 0xff. The values for this field are ignored.

Fields	Byte	Description
	7	Exception action taken: 00 - none 01 - hard power-off
	8-9	Power limit in watts. For example: 0x2a 0xaa
	10-13	Correction time limit in milliseconds. For example: 0x00 0x00 0x1b 0x58. This value is ignored if the time limit is set to default; see next byte.
	14	A flag indicating whether to use the system default time limit. Correction time limit in bytes 10-13 will be ignored. 0x00 - not default 0x01 - default
	15	Reserved field 0xff. The value for this field is ignored.
	16-17	Reserved field 0x00 0x00. The values for these fields are ignored.
Output Data	1	Completion code that is consumed by IPMItool. The system does not display a status for successful completion code. However, if the result of the completion code is anything other than successful, a failure message appears.
	2	Group extension identification 'dc' appears upon command completion.

## Manage the System Power Policy



### Note:

The settings defined in this procedure are not applicable to all server platforms.

 **Note:**

The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IPMItool utility. For more information about the IPMI TLS interface that is provided by Oracle, see [IPMI TLS Service and Interface](#).

Follow these steps to manage the system power policy settings on a managed device.

1. To get the current system power policy, type:

```
$ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password
```

```
raw 0x2e 0x43 4
```

2. To set the power manage policy to performance, type

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password
```

```
raw 0x2e 0x42 2 00 00 00 00
```

3. To set the power manage policy to elastic, type:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password
```

```
raw 0x2e 0x42 2 00 00 00 01
```

4. To set the power manage policy to disabled, type:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password
```

```
raw 0x2e 0x42 2 00 00 00 02
```

The following table describes the Power Management Policy State (IPMItool) input fields:

Fields	Byte	Description
Input Data	1	Sunoem command group number: 0x2e.
	2	Command code 0x42 sets the Power Policy Activation State.

Fields	Byte	Description
	3	Group extension identification: 2.
	4-6	Reserved fields.
	7	Sub-commands for power policy activation: 00 - Performance policy 01 - Elastic policy 02 - Disable the policy

## Display FRU Manufacturing Details

### Note:

The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IPMItool utility. For more information about the IPMI TLS interface that is provided by Oracle, see [IPMI TLS Service and Interface](#).

Follow this step to view the manufacturing details for a field replacement unit.

- To display Field Replacement Unit (FRU) manufacturing details on a managed device, use the `fru print` command.

Example:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U
username
-P
password
```

```
fru print
```

The output might look like the following:

```
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   : ORACLE
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 : ORACLE
Product Name        : SUN BLADE X8400 SERVER MODULE
Product Part Number : 602-0000-00
Product Serial      : 0000000000
Product Extra       : 080020ffffffffffffffff0003baf15c5a

FRU Device Description : /P0 (ID 5)
Product Manufacturer  : ADVANCED MICRO DEVICES
Product Part Number   : 0F21
Product Version       : 2

FRU Device Description : /P0/D0 (ID 6)
Product Manufacturer  : MICRON TECHNOLOGY
Product Name          : 1024MB DDR 400 (PC3200) ECC
Product Part Number   : 18VDDF12872Y-40BD3
Product Version       : 0300
Product Serial        : D50209DA
Product Extra         : 0190
Product Extra         : 0400

FRU Device Description : /P0/D1 (ID 7)
Product Manufacturer  : MICRON TECHNOLOGY
Product Name          : 1024MB DDR 400 (PC3200) ECC
Product Part Number   : 18VDDF12872Y-40BD3
Product Version       : 0300
Product Serial        : D50209DE
Product Extra         : 0190
Product Extra         : 0400

```

## Display Oracle ILOM Event, Audit, or Session Log



### Note:

The IPMI TLS interface (`orcltls`) interface is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the `IPMItool` utility. For more information about using the IPMI TLS interface from Oracle, see these topics: [IPMI TLS Service and Interface](#) and [Configure IPMI Management Access for Increased Security in Oracle ILOM Security Guide For Firmware Release 5.1.x](#).

Follow these steps to display the Oracle ILOM Event, Audit, or Session Log.

1. To display the Oracle ILOM Audit log, type: `sunoem cli "show /SP/logs/audit/list"`

Example:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -
U username-P password
```

```
sunoem cli "show /SP/logs/audit/list"
```

The Audit Log output might look like the following:

 **Note:**

As of Oracle ILOM firmware version 5.1, all user login and logout events are captured in the Session log (`show /SP/logs/session/list`). All login and logout events captured prior to firmware release 5.1 will continue to remain in the Audit log.

```
Audit
ID      Date/Time          Class   Type      Severity
-----
12050   Sat Dec 31 20:33:17 2016   Audit    UI        minor
        root : Open Session : object = "/SP/sessions/38701/type" : value =
        "shell" : success
12049   Sat Dec 31 20:31:19 2016   Audit    UI        minor
        root : Close Session : object = "/SP/sessions/38699/type" : value =
        "shell" : success
12048   Sat Dec 31 20:30:57 2016   Audit    UI        minor
        root : Open Session : object = "/SP/sessions/38699/type" : value =
        "shell" : success
12047   Sat Dec 31 20:29:16 2016   Audit    IPMI     minor
        root : Close Session : session ID = 3279888664 : success
12046   Sat Dec 31 20:29:16 2016   Audit    IPMI     minor
        root : Set Session Privilege Level: privilege level = admin : success
12045   Sat Dec 31 20:29:16 2016   Audit    IPMI     minor
        IPMI 2.0 Login Success : User = root, Client IP = #.#.#.#
12044   Sat Dec 31 19:02:28 2016   Audit    IPMI     minor
        root : Close Session : session ID = 3075033282 : success
12043   Sat Dec 31 19:02:28 2016   Audit    IPMI     minor
        root : Set Session Privilege Level: privilege level = admin : success
Paused: press any key to continue, or 'q' to quitSession closed
```

**2. To display the Oracle ILOM Event log, type: sel list**

Example:

```
$ ipmitool -I [orclt1s|lanplus] -H SP_hostname_or_IPaddress -U
username -P password
```

```
sel list
```

The Event Log output might look like the following:

```
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

```

## IPMItool Options and Command Summary

The following tables summarize the supported IPMItool options and commands:

- [Supported IPMItool Options](#)
- [Supported IPMItool Commands](#)

### Note:

The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IPMItool utility. For more information about using the IPMI TLS interface from Oracle, see these topics: [IPMI TLS Service and Interface](#) and *Configure IPMI Management Access for Increased Security in Oracle ILOM Security Guide For Firmware Release 5.1.x*.

**Table 5-2 Supported IPMItool Options**

IPMI Option	Function
<code>-a</code>	Prompt for the remote server password.
<code>-A[authype]</code>	Specify the authentication type to use during an IPMI lan session activation. Supported authentication types are NONE, PASSWORD, MD2, MD5, or OEM.
<code>-c</code>	Present output in CSV (comma separated variable) format. This is not available with all commands.
<code>-e [sol_escape_char]</code>	Use supplied character for SOL session escape character. The default is to use but this can conflict with SSH sessions.
<code>-K</code>	Read Kg key from IPMI_KGKEY environment variable.



Table 5-2 (Cont.) Supported IPMItool Options

IPMI Option	Function
-k [ <i>key</i> ]	Use supplied Kg key for IPMI v2 authentication. The default is not to use any Kg key.
-y [ <i>hex key</i> ]	Use supplied Kg key for IPMI v2 authentication. The key is expected in hexadecimal format and can be used to specify keys with non-printable characters. For example: '-k PASSWORD' and 'y 50415353574F5244' are equivalent. The default is not to use any Kg key.
-Y	Prompt for the Kg key for IPMI v2 authentication.
-C [ <i>ciphersuite</i> ]	The remote server authentication, integrity, and encryption algorithms to use for IPMI v2 <code>lanplus</code> connections. See table 22-19 in the IPMIv2 specification. The default is 3 which specifies RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity, and AES-CBC-128 encryption algorithms.
-E	The remote server password is specified by the environment variable <code>IPMI_PASSWORD</code> .
-f [ <i>password_file</i> ]	Specifies a file containing the remote server password. If this option is absent, or if <code>password_file</code> is empty, the password will default to NULL.
-h	Get basic usage help from the command line.
-H [ <i>address</i> ]	Remote server address, can be IP address or hostname. This option is required for <code>lan</code> and <code>lanplus</code> interfaces.
-i [ <i>interface</i> ]	Selects the IPMI interface to use. Supported interfaces that are compiled in are visible in the usage help output. No auto-detect is attempted. See the <code>-I</code> description for more information.

Table 5-2 (Cont.) Supported IPMItool Options



IPMI Option	Function
<code>-I [interface]</code>	<p>Attempt the most secure interface first (<code>orcltls</code>). If the BMC does not support the interface, attempt the next most secured interface until the specified interface. Supported interfaces that are compiled in are visible in the usage help output. If <code>lanplus</code> interface or <code>lan</code> interface is specified, certificate checking is disabled when attempting the <code>orcltls</code> interface.</p> <div data-bbox="1084 642 1380 1056" style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Note:</b></p> <p>If the <code>-I</code> option is not specified, auto-detect is enabled and certificate checking is enabled when attempting the <code>orcltls</code> interface.</p> </div>
<code>-m [local_address]</code>	Set the local IPMB address. The default is 0x20 and there should be no need to change it for normal operation.
<code>-N [sec]</code>	Specify number of seconds between retransmissions of <code>lan</code> or <code>lanplus</code> messages. Default are 2 seconds for <code>lan</code> and 1 second for <code>lanplus</code> interfaces.
<code>-o [oemtype]</code>	Select OEM type to support. This usually involves minor hacks in place in the code to work around quirks in various BMCs from various manufacturers. Use <code>-o list</code> to see a list of current supported OEM types.
<code>-O [sel oem]</code>	Open selected file and read OEM SEL event descriptions to be used during SEL listings.
<code>-p [port]</code>	<p>The remote server TLS TCP connection port is 443 (default).</p> <p>For IPMI v2.0 and 1.5, the remote server UDP TCP connection is port 623 (default).</p>

Table 5-2 (Cont.) Supported IPMItool Options

IPMI Option	Function
-P <i>[password]</i>	Remote server password is specified on the command-line. If supported it will be obscured in the process list.
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Note:</b></p> <p>Specifying the password as a command-line option is not recommended.</p> </div>
-R <i>[count]</i>	Set the number of retries for <code>lan</code> interface or <code>lanplus</code> interface (default=4).
-S <i>[sdr_cache_file]</i>	Use local file for remote SDR cache. Using a local SDR cache can drastically increase performance for commands that require knowledge of the entire SDR to perform their function. Local SDR cache from a remote system can be created with the <code>sdr dump</code> command.
-t <i>[target_address]</i>	Selects IPMI interface to use. Supported interfaces that are compiled in are visible in the usage help output.
-U <i>[username]</i>	Remote server username, default is NULL user.
-d N	Use device number N to specify the <code>/dev/ipmiN</code> (or <code>/dev/ipmi/N</code> or <code>/dev/ipmidev/N</code> ) device to use for in-band BMC communication. Used to target a specific BMC on a multi-node, multi-BMC system through the IPMI device driver interface. Default is 0.
-v	Increase verbose output level. This option may be specified multiple times to increase the level of debug output. If given three times you will get hexdumps of all incoming and outgoing packets.
-V	Display version information.
--no-cert-check	Disables the check for validating the SSL certificate when the <code>orcltis</code> IPMI interface is specified.
--cert-dir <i>[path]</i>	Location of trusted SSL certificates on host server SP.

**Table 5-3 Supported IPMItool Commands**

IPMI Command	Function
<code>sunoem sshkey set</code>	Configure an SSH key for a remote shell user.
<code>ipmitool sunoem sshkey del</code>	Remove an SSH key from a remote shell user.
<code>ipmitool sunoem led get</code>	Read LED status.
<code>ipmitool sunoem led set</code>	Set LED status.
<code>ipmitool sunoem cli</code>	Enter Oracle ILOM CLI commands as if you were using the ILOM CLI directly. The <code>lan</code> interface or <code>lanplus</code> interface should be used.
<code>ipmitool sunoem CLI force</code>	Available as of Oracle ILOM 3.0.10, a <code>force</code> option can be invoked as an argument to the <code>sunoem CLI</code> command.
<code>ipmitool raw</code>	Execute raw IPMI commands.
<code>ipmitool lan print</code>	Print the current configuration for the given channel.
<code>ipmitool lan set (1) (2)</code>	Set the given parameter on the given channel.
<code>ipmitool chassis status</code>	Display information regarding the high-level status of the system chassis and main power subsystem.
<code>ipmitool chassis power</code>	Perform a chassis control command to view and change the power state.
<code>ipmitool chassis identify</code>	Control the front panel identify light. Default is 15. Use 0 to turn off.
<code>ipmitool chassis restart_cause</code>	Query the chassis for the cause of the last system restart.
<code>ipmitool chassis bootdev (1)</code>	Request the system to boot from an alternative boot device on next reboot.
<code>ipmitool chassis bootparam (1)</code>	Set the host boot parameters.
<code>ipmitool chassis selftest</code>	Display the BMC self-test results.
<code>ipmitool power</code>	Return the BMC self-test results.
<code>ipmitool event</code>	Send a predefined event to the system event log.
<code>ipmitool sdr</code>	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.
<code>ipmitool sensor</code>	List sensors and thresholds in a wide table format.
<code>ipmitool fru print</code>	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.
<code>ipmitool sel</code>	View the Oracle ILOM SP system event log (SEL).

**Table 5-3 (Cont.) Supported IPMItool Commands**

<b>IPMI Command</b>	<b>Function</b>
<code>ipmitool pef info</code>	Query the BMC and print information about the PEF- supported features.
<code>ipmitool pef status</code>	Print the current PEF status (the last SEL entry processed by the BMC, and so on).
<code>ipmitool pef list</code>	Print the current PEF list (the last SEL entry processed by the BMC, and so on).
<code>ipmitool user</code>	Display a summary of user ID information, including maximum number of user IDs, the number of enabled users, and the number of fixed names defined.
<code>ipmitool session</code>	Get information about the specified sessions. 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.
<code>ipmitool firewall (1)</code>	Enable or disable individual command and command sub-functions; determine which commands and command sub-functions can be configured on a given implementation.
<code>ipmitool set (1)</code>	Set the runtime options including session host name, user name, password, and privilege level.
<code>ipmitool exec</code>	Execute IPMItool commands from file name. Each line is a complete command.

# 6

## SNMP Command Examples

Description	Links
Example SNMP Commands	<ul style="list-style-type: none"><li>• <a href="#">snmpwalk Command</a></li><li>• <a href="#">snmpbulkwalk Command</a></li><li>• <a href="#">snmptable Command</a></li><li>• <a href="#">snmptrapd Command</a></li></ul>

### Related Information

- [SNMP Overview](#)
- [Configuring SNMP Settings in Oracle ILOM](#)

### `snmpwalk` Command

The `snmpwalk` command performs a sequence of chained `GETNEXT` requests automatically. It is a work-saving command. Rather than having to issue a series of `snmpgetnext` requests, one for each object ID, or node, in a subtree, you can issue one `snmpwalk` request on the root node of the subtree and the command gets the value of every node in the subtree.

For example:

```
% snmpwalk
                               SNMP_agent
                               system
SNMPv2-MIB::sysDescr.0 = STRING: ILOM machine custom description
SNMPv2-MIB::sysObjectID.0 = OID: SUN-HW-TRAP-MIB::products.200.2.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (16439826) 1 day, 21:39:58.26
SNMPv2-MIB::sysContact.0 = STRING: set via snmp test
SNMPv2-MIB::sysName.0 = STRING: SUNSPHOSTNAME
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.3 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.4 = OID: RFC1213-MIB::ip
SNMPv2-MIB::sysORID.5 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.6 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.7 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.8 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.9 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module to describe generic objects
for network interface sub-layers
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.3 = STRING: The MIB module for managing TCP
implementations
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for managing IP and ICMP
implementations
```

```

SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing UDP
implementations
SNMPv2-MIB::sysORDescr.6 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.7 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB for Message Processing and
Dispatching.
SNMPv2-MIB::sysORDescr.9 = STRING: The management information definitions for
the SNMP User-based Security Model.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (14) 0:00:00.14

```

## snmpbulkwalk Command

The `snmpbulkwalk` command uses the `GETBULK` SNMP protocol feature to query for an entire tree of information about a network entity. This command can pack more objects into the packets by specifying “repeaters.” As a result, the `snmpbulkwalk` command is faster than the `snmpwalk` command.

Here is an example of the `snmpwalk` command with approximate start and end time stamps.

```

% date ; snmpwalk
                               SNMP_agent
                               entPhysicalTable >
                               /dev/null ; date
Sun Jun 30 18:15:38 EDT 2013
Sun Jun 30 18:16:46 EDT 2013

```

Here is an example of the `snmpbulkwalk` command performing the same operation. Notice that the `snmpbulkwalk` command is faster than the `snmpwalk` command.

```

% date ; snmpbulkwalk
                               SNMP_agent
                               entPhysicalTable >
                               /dev/null ; date
Sun Jun 30 18:19:19 EDT 2013
Sun Jun 30 18:19:38 EDT 2013

```

## snmptable Command

The `snmptable` command retrieves the contents of an SNMP table and displays the contents in a tabular format, that is, one table row at a time, such that the resulting output resembles the table being retrieved. This is contrasted with the `snmpwalk` command, which displays the contents of the table one column at a time.

Here is an example of the `snmptable` command:

```

% snmptable
                SNMP_agent
                sysORTable
SNMP table: SNMPv2-MIB::sysORTable
sysORID          sysORDescr          sysORUpTime
IF-MIB::ifMIB    The MIB module to                  0:0:00:00.01
describe generic objects
SNMPv2-MIB::snmpMIB    The MIB module for SNMPv2      0:0:00:00.02
for network interface
entities.
TCP-MIB::tcpMIB      The MIB module for              0:0:00:00.02
sub-layers.
managing TCP
UDP implementations.
UDP-MIB::udpMIB      The MIB module for managing      0:0:00:00.02
RFC1213-MIB::ip      The MIB module for managing      0:0:00:00.02
implementations.
SNMP-VIEW-BASED-ACM-  View-based Access Control        0:0:00:00.02
SNMP-FRAMEWORK-MIB::  The SNMP Management             0:0:00:00.14
IP and ICMP implementations.
MIB::vacmBasicGroup  Model for SNMP.
snmpFrameworkMIB    Architecture MIB.
Compliance
SNMP-MPD-MIB::snmp    The MIB for Message              0:0:00:00.14
MPDCompliance        Processing and Dispatching.
SNMP-USER-BASED-SM-  The management information       0:0:00:00.14
MIB::usmMIBCompliance definitions for the SNMP
User-based Security Model.

```

 **Note:**

While the `snmpget`, `snmpgetnext`, and `snmpwalk` command can be used on any type of MIB object, the `snmptable` command can be used only on MIB table objects. If this command is given any other type of object ID, it will be rejected. This restriction applies to a table entry object, a table column object, and any object that represents information within a table. Only a MIB table object ID can be used with the `snmptable` command.

In the examples of the `snmptable` command, the `-Ci` and `-Cb` options are used. For example, here is an `snmptable` command with the `-Ci` option:

```

% snmptable -Ci
                SNMP_agent
                sunPlatFanTable
SNMP table: SUN-PLATFORM-MIB::sunPlatFanTable
index sunPlatFanClass
10                fan
11                fan
17                fan
23                fan
29                fan
30                fan

```



```
36                fan
42                fan
```

Here is an example of an `snmptable` command without the `-Ci` option. Notice that the index column is not displayed:

```
% snmptable
           SNMP_agent
           sunPlatFanTable
SNMP table: SUN-PLATFORM-MIB::sunPlatFanTable
sunPlatFanClass
fan
fan
fan
fan
fan
```

Here is an example of an `snmptable` command with the `-Ci` and `-Cb` options. The output is abbreviated.

```
% snmptable -Ci -Cb SNMP_agent entPhysicalTable
index      Descr              VendorType  ContainedIn
SNMP table: ENTITY      ?SNMPv2-    0           chassis
-MIB::entPhysical      SMI:zeroDotZero
1
Table
```

Here is an example of the same `snmptable` command with the `-Ci` option but without the `-Cb` option. Again the output is abbreviated. Notice that the name of the MIB object is repeated on each heading.

```
% snmptable -Ci SNMP_agent entPhysicalTable
index      entPhysicalDescr  entPhysical  entPhysical
VendorType  ContainedIn
SNMP table: ENTITY      ?SNMPv2-    0           chassis
1
-MIB::entPhysical      SMI:zeroDotZero
```

Here is an example of an `snmptable` command using version 3 of the SNMP protocol:

```
% snmptable -Cb -Ci -mALL -v3 -aMD5 -utestuser -Apassword -lauthNoPriv
           SNMP_agent:port
           sunPlatPowerSupplyTable
SNMP table: SUN-PLATFORM-MIB::sunPlatPowerSupplyTable
index sunPlatPowerSupplyClass
90          powerSupply
92          powerSupply
96          powerSupply
```

The following `snmptable` command returns an empty table.

```
% snmptable -Cb -Ci
           SNMP_agent
```

```
sunPlatBatteryTable  
SUN-PLATFORM-MIB::sunPlatBatteryTable: No entries
```

## snmptrapd Command

snmptrapd is an SNMP application that receives and logs SNMP trap and inform messages.

The following alert management rule example shows how to configure Oracle ILOM to send traps to a particular trap-receiver, such as, snmptrapd running on a server with the specified destination ip address.

```
-> set /SP/alertmgmt/rules/1 type=snmptrap snmp_version= v2C|v3  
destination=dest_ipaddress destination_port=port_number  
community_or_username=name level=minor
```



### Note:

It is important to test the alert management rule configuration to ensure the it is configured properly.

To verify traps are sent and received, type:

```
-> set /SP/alertmgmt/rules/n testrule=true
```

The following screen shows a sample output when a `testalert` trap is received at the management station:

```
SUN-HW-TRAP-MIB::sunHwTrapTestMessage.0 = STRING:
```

# Index

## A

---

- alert rules
  - CLI commands, [3-8](#)
- alerts
  - CLI commands for managing alerts, [3-8](#)

## C

---

- component information
  - view, [4-1](#)

## E

---

- event log
  - configuring, [4-2](#)

## I

---

- IPMI
  - about IPMItool, [5-4](#)
  - detailed specifications
    - location of, [5-1](#)
  - generating IPMI-specific traps, [5-2](#)
  - IPMI Platform Event Trap (PET) alerts, [5-4](#)
  - overview, [5-1](#)
  - PET alerts, [5-4](#)
  - user roles, [5-5](#)
  - using for server management, [5-1](#)
  - versions supported by ILOM, [5-1](#)
- IPMItool
  - about, [5-4](#)
  - accessing the ILOM CLI, [5-9](#)
  - capabilities, [5-4](#)
  - commands, [5-24](#)
  - disable SSL certificate check, [5-9](#)
  - display FRU information, [5-21](#)
  - display ILOM event, audit, or session log, [5-22](#)
  - display sensor list, [5-11](#)
  - display single sensor, [5-12](#)
  - functions of, [5-4](#)
  - help, [5-4](#)
  - manage system power budget, [5-15](#)

## IPMItool (*continued*)

- manage system power policy, [5-20](#)
- management tasks, [5-10](#)
- power on/off and shutdown system, [5-14](#)
- requirements for using, [5-7](#)
- running CLI commands with, [5-7](#)
- scripting commands, [5-9](#)

## M

---

- Management Information Base (MIB)
  - definition, [2-3](#)
  - MIB tree, [2-3](#)
  - standard MIBs supported by ILOM, [2-5](#)

## N

---

- Net-SNMP
  - web site, [2-1](#)

## P

---

- PET alerts, [5-4](#)
- Platform Event Traps (PET), [5-4](#)

## S

---

- SNMP
  - functions supported, [2-2](#)
  - managed node, [2-2](#)
  - management station monitoring, [2-2](#)
  - MIBs used to support ILOM, [2-6](#)
  - Net-SNMP
    - web site, [2-1](#)
  - network management station, [2-2](#)
  - syntax, [2-6](#), [2-7](#)
  - tutorial web sites, [2-1](#)
  - versions supported, [2-1](#)
- SNMP traps
  - configuring destinations using the web interface, [3-11](#)
- SNMP user accounts
  - managing with the CLI, [3-6](#)
  - targets, properties, and values of, [3-3](#)

syntax examples  
SNMP, [2-6](#)

system alerts  
commands for managing, [3-8](#)