

# Oracle<sup>®</sup> Integrated Lights Out Manager (ILOM) CMM

Administration Guide for Sun Blade 6000 and  
Sun Blade 6048 Modular Systems



Copyright © 2007, 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompression of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

---

Copyright © 2007, 2010, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.



# Contents

---

## **Using This Documentation ix**

### **1. CMM ILOM Overview 1**

CMM ILOM Function Overview 2

ILOM Versions 2

CMM ILOM Documentation 3

This Document 3

### **2. CMM ILOM Initial Setup 5**

Connecting to the CMM ILOM 5

▼ Connect to the CMM ILOM Using a Serial Connection 7

▼ View and Set IPv4 Network Address 8

▼ View and Set Dual-Stack IPv4 and IPv6 Network Address 10

▼ Test IPv4 or IPv6 Network Configuration 15

Log In to CMM ILOM Using a Network Connection 16

▼ Log In to ILOM 3.0 Using the Web Interface 17

▼ Log In to ILOM 3.0 Using the CLI 17

Activating CMM Ethernet Ports 18

▼ Enable Ethernet Ports Using the Web Interface 18

▼ Enable Ethernet Ports Using the CLI 19

- Changing the Blade SP CLI Prompt 21
  - ▼ Set the Blade SP CLI Prompt 21
  - ▼ Reset the Blade SP CLI Prompt to the Default 22

### 3. Firmware Update Procedures 23

Updating the CMM ILOM Firmware 23

Obtaining the CMM IP Address 24

Determining Your Current Firmware Version 24

- ▼ Determine the Firmware Version Using the Web Interface 24
- ▼ Determine the Firmware Version Using the Management Ethernet Port CLI 26
- ▼ Determine the Firmware Version Using the Serial Management Port CLI 26

Downloading Firmware Files 27

- ▼ Download Firmware Files 27

Updating ILOM Firmware 28

- ▼ Update ILOM Firmware Using the Web Interface 28
- ▼ Update ILOM Firmware Using the CLI 30

Updating the NEM Firmware 30

- ▼ Update NEM Firmware Using the CLI 31
- ▼ Update NEM Firmware Using the Web Interface 33

Updating Chassis Component Firmware Using the CMM 36

- ▼ Update Firmware Using the Web Interface 37
- ▼ Update Firmware Using the CLI 39

Resetting the CMM 40

- ▼ Reset the CMM Using the Web Interface 40
- ▼ Reset the CMM Using the CLI 41

### 4. CMM Power Management 43

Light Load Efficiency Mode (LLEM) 44

About LLEM	44
Setting LLEM Using the Web Interface	44
▼ Enable or Disable LLEM Using the Web Interface	44
▼ Enable or Disable Redundant Mode Using the Web Interface	46
Setting LLEM Using the CLI	46
▼ Enable or Disable LLEM Using the CLI	46
▼ Enable Redundant Mode Using the CLI	47
▼ Enable Non-Redundant Mode Using the CLI	47
Force Power Supply Fan Speed	48
▼ Set the Power Supply Fan Speed Using the Web Interface	48
▼ Set the Power Supply Fan Speed Using the CLI	49
Disabling the Power Management Policy	49
▼ Disable Power Management Policy Using the Web Interface	50
▼ Disable Power Management Policy Using the CLI	50
ILOM 3.0 for Specific Sun Blade 6048 Cases	51
ILOM Behavior With Two Power Cord Configuration	51
▼ Configure the CMM for Two Power Cords	51
ILOM Readings for Specific Power Supply States	52
AC Cables Are Disconnected	52
AC Cables Are Disconnected, Then Are Reconnected	53
stop /CH Command	54
start /CH Command	54
One PSU Is Removed	55
PSU Is Reinserted	56
<b>5. Sun Blade Zone Manager</b>	<b>57</b>
Introduction to the Sun Blade Zone Manager	58
Sun Blade Zone Manager Overview	58
Supported ILOM Interfaces	58

Accessing Zone Manager Using the Web Interface	59
Accessing Zone Manager Using the CLI	61
Zoning Configuration Overview	62
Zoning Commands	62
Assigning Storage to a Server Blade	63
Assigning a Server Blade to Storage	64
Supported Hardware and Firmware Configurations	65
SAS-2 Capable Hardware	65
Additional System Requirements	65
Accessing the Sun Blade Zone Manager	66
▼ Access and Enable the Sun Blade Zone Manager Using the Web Interface	66
▼ Access and Enable the Sun Blade Zone Manager Using the CLI	70
Creating the Chassis Storage Access Configuration	72
Creating the Chassis Storage Access Configuration Using Quick Setup	72
Quick Setup Options	73
▼ Use Quick Setup to Create an Initial Chassis Storage Configuration Using the Web Interface	76
Creating the Chassis Storage Access Configuration Using Detailed Setup	78
▼ Use Detailed Setup to Create the Chassis Storage Configuration Using the Web Interface	78
Creating a Chassis Storage Configuration Using the CLI	81
▼ Create a Chassis Storage Configuration Using the CLI	82
Viewing or Modifying the Chassis Storage Access Configuration	83
▼ View and Modify the Chassis Storage Configuration Using the Web Interface	84
▼ View and Modify the Chassis Storage Configuration Using the CLI	90
▼ Assign Multiple Server Blades to a Storage Device Using the Web Interface	92
▼ View the Storage Access Configuration Table Using the Web Interface	95

Saving the Chassis Storage Access Configuration	97
Important Considerations About Saving the Zoning Configuration	98
Saving a New or Modified Storage Access Configuration	98
Backing Up the Storage Access Configuration	100
▼ Save the Zoning Configuration to a Backup File Using the Web Interface	100
▼ Save the Zoning Configuration to a Backup File Using the CLI	101
Recovering Zoning Configurations	102
▼ Recover Zoning Configurations Using the Web Interface	102
▼ Recover Zoning Configurations Using the CLI	104
Resetting the Zoning Configuration	106
▼ Reset the Zoning Configuration Using the Web Interface	106
▼ Reset the Zoning Configuration Using the CLI	107
Resetting the Zoning Password	107
▼ Reset the Zoning Password Using the Web Interface	107
▼ Reset the Zoning Password Using the CLI	108
<b>Index</b>	<b>109</b>





# Using This Documentation

---

The *Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and 6048 Modular Systems* provides instructions for managing the Sun Blade Modular System Chassis using a modified version of the Oracle Integrated Lights Out Manager (ILOM) called the chassis monitoring module (CMM). Throughout this document, it is referred to as the CMM ILOM.

---

## Related Documentation

The document sets for the Sun Blade Modular Systems are described in the documentation sheet that is packed with your system.

- *Where to Find Sun Blade 6000 Modular System Documentation* (820-1701)
- *Where to Find Sun Blade 6048 Modular System Documentation* (820-2311)

You can find the modular system documentation at:

- Sun Blade 6000: <http://docs.sun.com/app/docs/prod/blade.6000mod>
- Sun Blade 6048: <http://docs.sun.com/app/docs/prod/blade.6048mod>

You can find the Oracle Integrated Lights Out Manager (ILOM) 3.0 Documentation Collection at:

<http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic>

Translated versions of some of these documents are available at:

<http://docs.sun.com>

Available translations for the documents include Simplified Chinese, Traditional Chinese, French, Japanese, and Korean.

---

# Documentation, Support, and Training

These web sites provide additional resources:

- Documentation: <http://docs.sun.com/>
- Support: <http://www.sun.com/support/>
- Training: <http://www.sun.com/training/>

---

## Documentation Comments

Submit comments about this document by clicking the Feedback[+] link at:

<http://docs.sun.com>.

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

*Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and 6048 Modular Systems*, part number 820-0052-15.

## CMM ILOM Overview

---

The Sun Blade 6000 Modular System chassis holds up to 10 blades and the Sun Blade 6048 Modular System holds up to 48 blades. Supported blades include Sun Blade server modules and storage modules.

Each server module has its own ILOM service processor (SP) which is separate from the chassis monitoring module (CMM) ILOM. The CMM ILOM manages the Sun Blade 6000 and 6048 Modular System chassis. It provides management of chassis components, and a method of accessing the service processors in individual server modules.

Users interact with the CMM ILOM through a command-line interface (CLI) or web interface.

This section covers the following topics:

- [“CMM ILOM Function Overview” on page 2](#)
- [“ILOM Versions” on page 2](#)
- [“CMM ILOM Documentation” on page 3](#)
- [“This Document” on page 3](#)

---

# CMM ILOM Function Overview

ILOM on the CMM offers a tiered management architecture that enables system management of individual components or aggregated management of components at the chassis level.

A summary of the management functions include:

- Implementation of an IPMI satellite controller, making the chassis environmental sensors visible to the server module's BMC functions
- Direct environmental and inventory management using CLI, web, SNMP, and IPMI interfaces
- Firmware management of CMM, network express module (NEM), and server module SPs
- Pass-through management of server modules and HTTP links along with command-line interface (CLI) SSH contexts
- Chassis power control
- Access to the following components:
  - Chassis
  - Power supplies
  - Fans
  - Network express modules (NEMs)
  - Server module SPs
- Assignment of storage devices from SAS-2 capable storage modules to SAS-2 capable server blades in the chassis, using the Sun Blade Zone Manager. This is only available for the Sun Blade 6000 chassis.

---

## ILOM Versions

The ILOM information in this document refers to 3.x.x versions of ILOM (ILOM 3.0.3 and later).

For information on ILOM 2.x, refer to the following documentation:

ILOM 2.0 Documentation Set: <http://docs.sun.com/app/docs/coll/ilom2.0>

---

# CMM ILOM Documentation

The following documentation provides information on the functionality and use of the CMM ILOM:

- Oracle Integrated Lights Out Manager (ILOM) 3.0 Documentation Collection: Comprehensive documentation on features and use of ILOM 3.0
- Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and 6048 Modular Systems (this document): Provides information on ILOM functionality that is specific to the CMM ILOM.
- *Oracle Integrated Lights Out Manager (ILOM) 3.0 Supplement for Sun Blade 6000 and Sun Blade 6048 Modular Systems*: Supplementary information specific to the ILOM 3.x version of the CMM ILOM.

Oracle Integrated Lights Out Manager (ILOM) 3.0 Documentation Collection is available at:

<http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic>

Sun Blade 6000 and 6048 modular system documentation is available at:

Sun Blade 6000: <http://docs.sun.com/app/docs/prod/blade.6000mod>

Sun Blade 6048: <http://docs.sun.com/app/docs/prod/blade.6048mod>

---

## This Document

This document covers administration tasks specific to the Sun Blade 6000 and 6048 Modular Systems. The topics covered are shown in the following table.

Description	Chapter
Perform initial set up of the CMM ILOM	• “CMM ILOM Initial Setup” on page 5
Update chassis and component firmware	• “Firmware Update Procedures” on page 23
Use ILOM power management features	• “CMM Power Management” on page 43
View or modify the storage zoning configuration	• “Sun Blade Zone Manager” on page 57



## CMM ILOM Initial Setup

---

This chapter describes how to access the CMM ILOM and do the initial setup.

Initial access to the CMM ILOM is through the serial connector or the NET MGT 0 Ethernet connector on the chassis rear panel.

This chapter contains information on CMM ILOM setup as described in the following table.

Description	Links
Connect to the CMM ILOM and configure CMM IP address	• <a href="#">“Connecting to the CMM ILOM” on page 5</a>
Log in to the CMM ILOM for the first time	• <a href="#">“Log In to CMM ILOM Using a Network Connection” on page 16</a>
Activate CMM Ethernet ports	• <a href="#">“Activating CMM Ethernet Ports” on page 18</a>
Change the CLI blade prompt	• <a href="#">“Changing the Blade SP CLI Prompt” on page 21</a>

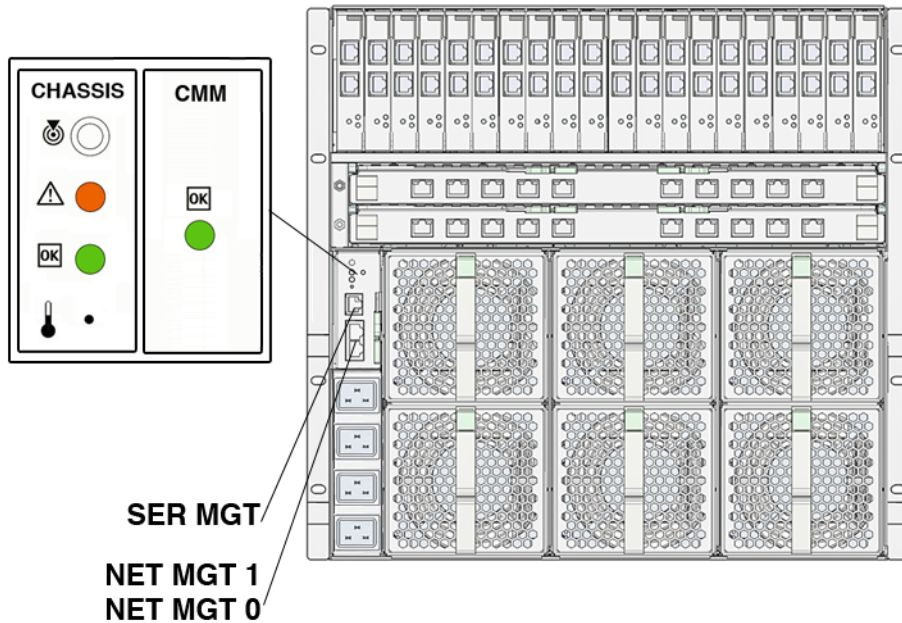
---

---

## Connecting to the CMM ILOM

To set up the CMM with initial network configuration information, you must establish a connection through ILOM to the CMM. You can establish a local connection to ILOM through the serial management port (SER MGT) on the CMM or a remote connection to ILOM through the network management (NET MGT) port on the CMM (see [FIGURE 2-1](#).)

**FIGURE 2-1** Network and serial ports on CMM



When you establish a connection to ILOM through the network management port, ILOM will, by default, automatically learn the IP address of the CMM using DHCP for IPv4 and stateless for IPv6. If a network management connection has not been established to the NET MGT port on the CMM, ILOM is unable to learn the IP address of the CMM therefore, you will need to connect to ILOM through a serial connection. After you have established a connection to ILOM, you can view and, if necessary, modify the IP address assigned to the CMM.

**Next Steps:**

- If you do not know the IP address assigned to the CMM, see [“Connect to the CMM ILOM Using a Serial Connection”](#) on page 2-7.
- or -
- If you do know the IP address assigned to the CMM and you have an established network management connection to the CMM, see one of the following sections to view or modify the CMM IP address.
  - [“View and Set IPv4 Network Address”](#) on page 8
  - [“View and Set Dual-Stack IPv4 and IPv6 Network Address”](#) on page 10



## ▼ Connect to the CMM ILOM Using a Serial Connection

You can access the CMM ILOM at any time by connecting a terminal or a PC running terminal emulation software to the serial connector on the chassis.

1. **Verify that your terminal, laptop, or terminal server is operational.**
2. **Configure that terminal device or the terminal emulation software to use the following settings:**
  - 8N1: eight data bits, no parity, one stop bit
  - 9600 baud
  - Disable software flow control (XON/XOFF)
3. **Connect a serial cable from the serial port (SER MGT) on the chassis panel to a terminal device.**

---

**Note** – The serial port requires that the serial cable connected to it use the pin assignments shown in the following table.

---

Pin	Signal Description
1	Request To Send (RTS)
2	Data Terminal Ready (DTR)
3	Transmit Data (TXD)
4	Ground
5	Ground
6	Receive Data (RXD)
7	Data Carrier Detect (DCD)
8	Clear To Send (CTS)

4. **Press Enter on the terminal device.**

This establishes the connection between the terminal device and the CMM ILOM.

---

**Note** – If you connect a terminal or emulator to the serial port before the CMM ILOM has been powered on or during its power on sequence, you will see boot messages.

---

When the system has booted, the CMM ILOM displays its login prompt:

```
<hostname> login:
```

## 5. Log in to the CLI:

a. Type the default user name, **root**.

b. Type the default password, **changeme**.

When you have successfully logged in, the CMM ILOM displays the default command prompt:

```
->
```

The CMM ILOM is running the CLI. You can now run CLI commands.

**Next Steps:** View or set a CMM ILOM IP address using one of the following procedures:

- [“View and Set IPv4 Network Address” on page 8](#)
- [“View and Set Dual-Stack IPv4 and IPv6 Network Address” on page 10](#)

## ▼ View and Set IPv4 Network Address

1. Log in to the CMM ILOM using either a remote SSH connection or a local serial connection.

For more information, see one of the following sections:

- [“Connect to the CMM ILOM Using a Serial Connection” on page 7.](#)
- [“Log In to ILOM 3.0 Using the CLI” on page 17](#)

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

- For a chassis CMM: `cd /CMM/network`
- For a chassis server blade server module: `cd /SP/network`

3. Type the `show` command to view the IP address network properties.

4. To set IPv4 network settings for DHCP or static, perform one of the following:

- **To configure DHCP IPv4 network settings**, set values for the following properties:

Property	Set Property Value	Description
state	set state=enabled	The network state is enabled by default for IPv4. <b>Note</b> - To enable the DHCP network option for IPv4 the state must be set to enabled.
pendingipdiscovery	set pendingipdiscovery=dhcp	The property value for ipdiscovery is set to dhcp by default for IPv4. <b>Note</b> - If the dhcp default property value was changed to static, you will need to set the property value to dhcp.
commitpending=	set commitpending=true	Type set commitpending=true to commit the changes made to the state and ipdiscovery property values.

- **To configure static IPv4 network settings**, set values for the following properties:

Property	Set Property Value	Description
state	set state=enabled	The network state is enabled by default for IPv4. <b>Note</b> - To enable the static IPv4 network option the state must be set to enabled.
pendingipdiscovery	set pendingipdiscovery=static	To enable a static IPv4 network configuration, you need to set the pendingipdiscovery property value to static. <b>Note</b> - The property value for ipdiscovery is set to dhcp by default for IPv4.
pendingipaddress pendingipnetmask pendingipgateway	set pendingipaddress= <ip_address> pendingipnetmask= <netmask> pendingipgateway= <gateway>	To assign multiple static network settings, type the set command followed by the pending command for the each property value (IP address, netmask, and gateway), then type the static value that you want to assign.
commitpending=	set commitpending=true	Type set commitpending=true to commit the changes made to the IPv4 network properties.

---

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

---

5. **Test the IPv4 network configuration from ILOM use the Network Test Tools (Ping).** For details, see [“Test IPv4 or IPv6 Network Configuration”](#) on page 2-15

## ▼ View and Set Dual-Stack IPv4 and IPv6 Network Address

---

**Note** – This procedure provides instructions for configuring ILOM to operate in a dual-stack IPv4 and IPv6 network environment. Dual-stack IPv4 and IPv6 network settings are only in ILOM for the A90-D model chassis. For more information about dual-stack IPv4 and IPv6 support in ILOM, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

---

1. **Log in to the CMM ILOM using either a remote SSH connection or a local serial connection.**

For more information, see one of the following sections:

- [“Connect to the CMM ILOM Using a Serial Connection”](#) on page 7.
- [“Log In to ILOM 3.0 Using the CLI”](#) on page 17

2. **Perform the network configuration instructions that apply to your network environment:**

- To configure IPv4 network settings, perform [Step 3](#) to [Step 5](#) in this procedure.
- To configure IPv6 network settings, perform [Step 6](#) to [Step 10](#) in this procedure.

3. **For IPv4 network configurations, use the `cd` command to navigate to the `/x/network` working directory for the device.**

For example:

- For a chassis CMM type: `cd /CMM/network`
- For a chassis blade server SP type: `cd /CH/BLn/network`
- For a chassis blade server with multiple SP nodes type:  
`cd /CH/BLn/Noden/network`

4. **Type the `show` command to view the configured IPv4 network settings configured on the device.**

5. **To set IPv4 network settings for DHCP or static, perform one of the following:**

- **To configure DHCP IPv4 network settings**, set values for the following properties:

Property	Set Property Value	Description
state	set state=enabled	The network state is enabled by default for IPv4. <b>Note</b> - To enable the DHCP network option for IPv4 the state must be set to enabled.
pendingipdiscovery	set pendingipdiscovery=dhcp	The property value for ipdiscovery is set to dhcp by default for IPv4. <b>Note</b> - If the dhcp default property value was changed to static, you will need to set the property value to dhcp.
commitpending=	set commitpending=true	Type set commitpending=true to commit the changes made to the state and ipdiscovery property values.

- **To configure static IPv4 network settings**, set values for the following properties:

Property	Set Property Value	Description
state	set state=enabled	The network state is enabled by default for IPv4. <b>Note</b> - To enable the static IPv4 network option the state must be set to enabled.
pendingipdiscovery	set pendingipdiscovery=static	To enable a static IPv4 network configuration, you need to set the pendingipdiscovery property value to static. <b>Note</b> - The property value for ipdiscovery is set to dhcp by default for IPv4.
pendingipaddress pendingipnetmask pendingipgateway	set pendingipaddress= <ip_address> pendingipnetmask= <netmask> pendingipgateway= <gateway>	To assign multiple static network settings, type the set command followed by the pending command for the each property value (IP address, netmask, and gateway), then type the static value that you want to assign.
commitpending=	set commitpending=true	Type set commitpending=true to commit the changes made to the IPv4 network properties.

**6. For IPv6 network configurations, use the `cd` command to navigate to the `/x/network/ipv6` working directory for the device.**

For example:

- For a chassis CMM type: `cd /CMM/network/ipv6`
- For a chassis blade server SP type: `cd /CH/BLn/network/ipv6`
- For a chassis blade server with multiple SP nodes type:  
`cd /CH/BLn/NodeN/network/ipv6`

**7. Type the `show` command to view the configured IPv6 network settings configured on the device.**

For example, see the following sample output values for the IPv6 properties on a server SP device.

```
-> show

/SP/network/ipv6
  Targets:

  Properties:
    state = enabled
    autoconfig = stateless
    dhcpv6_server_duid = (none)
    link_local_ipaddress = fe80::214:4fff:feca:5f7e/64
    static_ipaddress = ::/128
    ipgateway = fe80::211:5dff:febe:5000/128
    pending_static_ipaddress = ::/128
    dynamic_ipaddress_1 = fec0:a:8:b7:214:4fff:feca:5f7e/64

  Commands:
    cd
    show
```

---

**Note** – When the `autoconfig=` property is set to `dhcpv6_stateful` or `dhcpv6_stateless`, the read-only property for `dhcpv6_server_duid` will identify the DHCP Unique ID of the DHCPv6 server that was last used by ILOM to retrieve the DHCP information.

---

---

**Note** – The default IPv6 `autoconfig` property value provided in ILOM 3.0.14 (and later) is `autoconfig=stateless`. However, if you have ILOM 3.0.12 installed on your CMM or server module, the default property value for `autoconfig` appears as `autoconfig=stateless_only`.

---

**8. To configure an IPv6 auto-configuration option, use the `set` command to specify the following auto-configuration property values.**

Property	Set Property Value	Description
state	<code>set state=enabled</code>	The IPv6 network state is enabled by default. To enable an IPv6 auto-configuration option this state must be set to enabled.
autoconfig	<code>set autoconfig=&lt;value&gt;</code>	Specify this command followed by the <code>autoconf</code> value you want to set. Options include: <ul style="list-style-type: none"> <li>• <code>stateless</code> (default setting provided in ILOM 3.0.14 or later) <i>or</i> <code>stateless_only</code> (default setting provided in ILOM 3.0.12) Automatically assigns IP address learned from the IPv6 network router.</li> <li>• <code>dhcpv6_stateless</code> Automatically assigns DNS information learned from the DHCP server. The <code>dhcpv6_stateless</code> property value is available in ILOM as of 3.0.14.</li> <li>• <code>dhcpv6_stateful</code> Automatically assigns the IPv6 address learned from the DHCPv6 server. The <code>dhcpv6_stateful</code> property value is available in ILOM as of 3.0.14.</li> <li>• <code>disable</code> Disables all auto-configuration property values and sets the read-only property value for link local address.</li> </ul>

---

**Note** – The IPv6 configuration options take affect after they are set. You do not need to commit these changes under the `/network` target.

---



---

**Note** – IPv6 auto-configuration addresses learned for the device will not affect any of the active ILOM sessions to the device. You can verify the newly learned auto-configured addresses under the `/network/ipv6` target.

---

---

**Note** – As of ILOM 3.0.14 or later, you can enable the `stateless` auto-configuration option to run at the same time as when the option for `dhcpv6_stateless` is enabled or as when the option for `dhcpv6_stateful` is enabled. However, the auto-configuration options for `dhcpv6_stateless` and `dhcpv6_stateful` should not be enabled to run at the same time.

---

**9. Perform the following steps to set a static IPv6 address:**

**a. To set a pending static IPv6 address, specify the following property values:**

Property	Set Property Value	Description
<code>state</code>	<code>set state=enabled</code>	The IPv6 network state is enabled by default. To enable a static IP address this state must be set to enabled.
<code>pendingipaddress</code>	<code>set pending_static_ipaddress=&lt;ip6_address&gt;/&lt;subnet mask length in bits&gt;</code>	Type this command followed by the property value for the static IPv6 address and net mask that you want to assign to the device. IPv6 address example: <code>fec0:a:8:b7:214:4fff:feca:5f7e/64</code>

**b. To commit (save) the pending IPv6 static network parameters, perform the steps in the following table:**

Step	Description
1	Use the <code>cd</code> command to change the directory to the device network target. For example: <ul style="list-style-type: none"> <li>• For chassis CMM type: <code>cd /CMM/network</code></li> <li>• For chassis blade server SP type: <code>cd /CH/BLn/network</code></li> <li>• For chassis blade server SP with multiple nodes type: <code>cd /CH/BLn/NodeN/network</code></li> </ul>
2	Type the following command to commit the changed property values for IPv6: <code>set commitpending=true</code>

---

**Note** – Assigning a new static IP address to the device (SP or CMM) will end all active ILOM sessions to the device. To log back in to ILOM, you will need to create a new browser session using the newly assigned IP address.

---

**10. To test the IPv4 or IPv6 network configuration from ILOM use the Network Test Tools (Ping and Ping6). For details, see [“Test IPv4 or IPv6 Network Configuration”](#) on page 2-15.**



## ▼ Test IPv4 or IPv6 Network Configuration

### 1. Log in to the ILOM SP CLI or the CMM CLI.

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

### 2. Use the `cd` command to navigate to the `/x/network/test` working directory for the device, for example:

- For a chassis CMM type: `cd /CMM/network/test`
- For a chassis blade server SP type: `cd /CH/BLn/network/test`
- For a chassis blade server with multiple SP nodes type:  
`cd /CH/BLn/Node $n$ /network/test`

### 3. Type the `show` command to view the network test targets and properties.

For example, see the following output the shows the test target properties on a CMM device.

```
-> show

/CMM/network/test
Targets:

Properties:
  ping = (Cannot show property)
  ping6 = (Cannot show property)

Commands:
  cd
  set
  show
```

4. Use the `set ping` or `set ping6` command to send a network test from the device to a specified network destination.

Property	Set Property Value	Description
ping	<code>set ping=&lt;IPv4_address&gt;</code>	Type the <code>set ping=</code> command at the command prompt followed by the IPv4 test destination address. For example: -> <code>set ping=10.8.183.106</code> Ping of 10.8.183.106 succeeded
ping6	<code>set ping6=&lt;IPv6_address&gt;</code>	Type the <code>set ping6=</code> command followed by the IPv6 test destination address. For example: -> <code>set ping6=fe80::211:5dff:febe:5000</code> Ping of fe80::211:5dff:febe:5000 succeeded

**Next Steps:**

- If you have not already used the network management connection to log in to ILOM, see [“Log In to CMM ILOM Using a Network Connection” on page 16](#).
- Perform CMM administration tasks as described in this document or the Oracle Integrated Lights Out Manager (ILOM) 3.0 Documentation Collection

---

## Log In to CMM ILOM Using a Network Connection

This section describes initial steps for logging in to the CMM ILOM using a network connection. For further information on setting up ILOM, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide*.

This section covers the following procedures:

- [“Log In to ILOM 3.0 Using the Web Interface” on page 17](#)
- [“Log In to ILOM 3.0 Using the CLI” on page 17](#)

## ▼ Log In to ILOM 3.0 Using the Web Interface

Follow these steps to log in to the ILOM web interface for the first time using the `root` user account:

1. **Connect an Ethernet cable to the NET0 Ethernet port.**
2. **Type `http://system_ipaddress` into a web browser.**  
The web interface Login page appears.



3. **Type the user name and password for the `root` user account:**  
User Name: **root**  
Password: **changeme**
4. **Click Log In.**  
The Version page in the web interface appears.

## ▼ Log In to ILOM 3.0 Using the CLI

To log in to the ILOM CLI for the first time, use SSH and the `root` user account.

1. **Connect an Ethernet cable to the NET0 Ethernet port.**

2. To log in to the ILOM CLI using the `root` user account, type:

```
$ ssh root@system_ipaddress
```

Password: **changeme**

The ILOM CLI prompt appears (->).

---

## Activating CMM Ethernet Ports

By default, Ethernet port 0 is enabled on the CMM. You can enable port 1 or enable both ports through the CLI or the web interface.



---

**Caution** – You can cause Ethernet networking problems and bring down the external network if you activate both Ethernet ports on the CMM. Before you activate both ports, ensure that the external switch supports trunk mode. The upstream Ethernet switch needs to be configured correctly, so that no Ethernet traffic loop is created. This is done usually by the spanning tree algorithm.

---

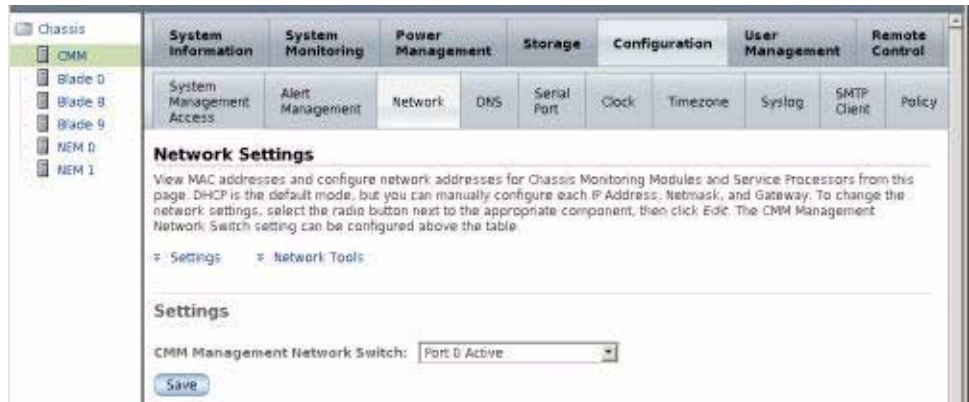
This section contains the following procedures:

- [“Enable Ethernet Ports Using the Web Interface” on page 18](#)
- [“Enable Ethernet Ports Using the CLI” on page 19](#)

### ▼ Enable Ethernet Ports Using the Web Interface

To enable an Ethernet port using the web interface:

1. **Log in to the ILOM web interface.**
2. **Click on CMM in the left panel.**
3. **Navigate to Configuration --> Network.**



4. In the CMM Management Network Switch drop-down list, select one of the following:
  - Port 0 Active: To activate port 0 only
  - Port 1 Active: To activate port 1 only
  - Trunking (Link Aggregation) to activate both ports
5. Click Save.
6. Remove the CMM and reinstall it into the chassis.
 

See the chassis Service Manual for instructions on removing and replacing the CMM in the chassis.

The active port is now updated.

## ▼ Enable Ethernet Ports Using the CLI

To enable port 1 using the CLI:

1. Log in to the ILOM CLI.
2. Type:
 

```
-> cd /CMM/network
```

### 3. Type **show** to view the switchconf variable setting.

For example:

```
-> show
/CMM/network
  Targets:

  Properties:
    commitpending = (Cannot show property)
    ipaddress = 10.6.153.71
    ipdiscovery = dhcp
    ipgateway = 10.6.152.1
    ipnetmask = 255.255.252.0
    macaddress = 00:14:4F:6B:6F:C1
    pendingipaddress = 10.6.153.71
    pendingipdiscovery = dhcp
    pendingipgateway = 10.6.152.1
    pendingipnetmask = 255.255.252.0
    switchconf = port0

  Commands:
    cd
    set
    show
```

In this example, the switchconf variable is set to port 0.

- To activate port 1 and disable port 0, type: **set switchconf=port1**
- To activate port 1 and keep port 0 active, type: **set switchconf=trunk**

### 4. Remove the CMM and reinstall it into the chassis.

See the chassis Service Manual for instructions on removing and replacing the CMM in the chassis.

The active port is now NET MGT port 1 or both NET MGT ports.

---

# Changing the Blade SP CLI Prompt

Starting with CMM software 3.2 (ILOM 3.0.10), you can change the default CLI prompt for a server blade SP through the CMM. This prompt is used when you execute the following command to navigate to a server blade SP from the CMM:

```
-> start /CH/BLn/SP/cli
```

Instead of seeing the -> prompt, you will see one of the following default prompts:

- [BLn/SP] -> for single node blades
- [BLn/NODEn/SP] -> for blades with multiple nodes

---

**Note** – A node is an independent computer that resides on the server blade. The Sun Blade X6275 server module is an example of a blade with two nodes per blade.

---

This feature requires that the server blade SP is running ILOM 3.0.9 or later.

This section contains the following procedures:

- [“Set the Blade SP CLI Prompt” on page 21](#)
- [“Reset the Blade SP CLI Prompt to the Default” on page 22](#)

## ▼ Set the Blade SP CLI Prompt

1. Log in to the ILOM CLI.
2. Use one of the following commands to change the server blade default CLI prompt:

- For single-node blades: **set /CH/BLn/SP/cli prompt="newprompt"**
- For two-node blades: **set /CH/BLn/NODEn/SP/cli prompt="newprompt"**

Where *newprompt* is the value that you want to set for the new prompt.

For example, if you want to set the blade SP prompt to “blade SP”, on BL0, you would use the following command:

```
-> set /CH/BL0/SP/cli prompt="blade SP"
```

## ▼ Reset the Blade SP CLI Prompt to the Default

- If you have changed the blade SP CLI prompt from the default, and want to return to the default, use the following command:

```
-> set /CH/BLn/SP/cli prompt=""
```



## Firmware Update Procedures

---

This chapter contains information on updating system firmware as described in the following table.

Description	Links
Update CMM ILOM firmware	<ul style="list-style-type: none"><li>• <a href="#">“Updating the CMM ILOM Firmware” on page 23</a></li></ul>
Update NEM firmware	<ul style="list-style-type: none"><li>• <a href="#">“Updating the NEM Firmware” on page 30</a></li></ul>
Update chassis component firmware	<ul style="list-style-type: none"><li>• <a href="#">“Updating Chassis Component Firmware Using the CMM” on page 36</a></li></ul>
Reset the CMM	<ul style="list-style-type: none"><li>• <a href="#">“Updating Chassis Component Firmware Using the CMM” on page 36</a></li></ul>

---

---

## Updating the CMM ILOM Firmware

This information is covered in more detail in the ILOM 3.0 Documentation Collection at:

<http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic>

Use the following sections, in order:

1. Obtain the IP address of the CMM. See [“Obtaining the CMM IP Address” on page 24](#).
2. Log on to the CMM to check the versions of firmware you have. See [“Determining Your Current Firmware Version” on page 24](#).
3. Use ILOM to download the new versions of firmware. See [“Downloading Firmware Files” on page 27](#).

4. Use ILOM to install the new firmware. See [“Updating ILOM Firmware” on page 28](#).
5. Reset the CMM. See [“Updating Chassis Component Firmware Using the CMM” on page 36](#).

---

**Note** – For information on backing up and restoring the ILOM configuration, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* or the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

---

## Obtaining the CMM IP Address

You must use the CMM IP address to access the CMM ILOM. If you do not already know the CMM IP address, you must determine it.

Refer to [“Connecting to the CMM ILOM” on page 5](#) for instructions on how to determine the IP address of the CMM.

## Determining Your Current Firmware Version

Three procedures are provided in this section for determining your current firmware version:

- [“Determine the Firmware Version Using the Web Interface” on page 24](#)
- [“Determine the Firmware Version Using the Management Ethernet Port CLI” on page 26](#)
- [“Determine the Firmware Version Using the Serial Management Port CLI” on page 26](#)

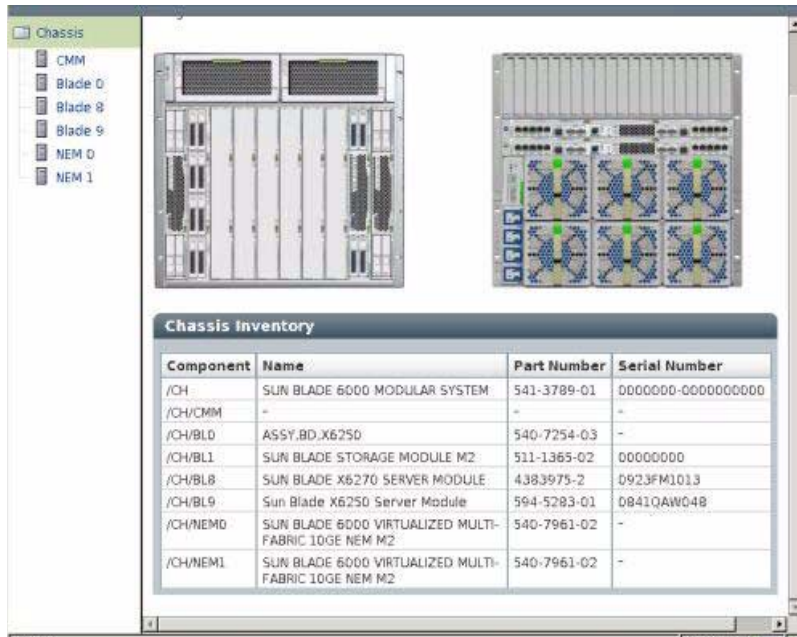
### ▼ Determine the Firmware Version Using the Web Interface

1. **Connect to the ILOM web interface by entering the IP address of the server’s CMM in your browser’s address field.**

For example:

**https://129.146.53.150**

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



3. Click on the CMM in the left corner of the chassis navigation pane.

4. Navigate to System Information --> Versions.

The Versions page is displayed, which includes the firmware version and build number.



## ▼ Determine the Firmware Version Using the Management Ethernet Port CLI

See the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide* for more detailed information on this procedure.

1. Log in to the ILOM CLI.
2. Type the `version` command, which returns output similar to the following:

```
-> version
CMM firmware 3.0.10.15
CMM firmware build number: 55335
CMM firmware date: Thu Apr 22 19:41:07 EDT 2010
CMM filesystem version: 0.1.22
```

The ILOM (CMM) firmware version and build number are listed in the output.

## ▼ Determine the Firmware Version Using the Serial Management Port CLI

1. Configure your terminal device or the terminal emulation software running on a laptop or PC to the following settings:
  - 8N1: eight data bits, no parity, one stop bit
  - 9600 baud
  - Disable hardware flow control (CTS/RTS)
  - Disable software flow control (XON/XOFF)

2. Connect a serial cable from the RJ-45 SER MGT port on the CMM to your terminal device or PC.

3. Press Enter on the terminal device to establish a connection between that terminal device and the CMM.

The CMM displays a login prompt.

```
<hostname>login:
```

Where *hostname* could be `SUNCM` followed by the product serial number, or if you have enabled hostnames in DHCP, it will be the assigned host name.

4. Log in to the ILOM CMM and type the default user name (`root`) with the default password (`changeme`).

After you have successfully logged in, the CMM displays its default command prompt:

```
->
```

5. **Type the version command, which returns output similar to the following:**

```
-> version
```

```
CMM firmware version: 3.0.3.32
```

```
CMM firmware build number: 42331
```

```
CMM firmware date: Wed Feb 18 11:46:55 PST 2009
```

```
CMM filesystem version: 0.1.22
```

The ILOM firmware version and build number are listed in the output.

## Downloading Firmware Files

The following procedure explains how to download the ILOM firmware from the web.

### ▼ Download Firmware Files

Download the flash image .ima file using these steps:

1. **Browse to <http://www.oracle.com/us/products/servers-storage/servers/blades/index.html>**
2. **Navigate to the Sun Blade 6000 Modular System or Sun Blade 6048 Modular System.**
3. **Click the Download link for the firmware version that you want to download.**
4. **Enter your Username and Password.**  
If you do not have a Username and Password, you can register free of charge by clicking **Register Now**.
5. **Click Accept License Agreement.**
6. **Click the appropriate firmware image file name:**

```
ILOM-version-Sun_Blade_6000.ima
```

or

```
ILOM-version-Sun_Blade_6048.ima
```

For example:

```
ILOM-3_0_10_15-Sun_Blade_6048.ima
```

or

```
ILOM-3_0_10_15-Sun_Blade_6000.ima
```

# Updating ILOM Firmware



---

**Caution** – ILOM enters a special mode to load new firmware. No other tasks can be performed in ILOM until the firmware upgrade is complete and the ILOM is reset.

---

This is the procedure that actually updates the firmware, replacing the existing images with the new images from the .ima file you downloaded previously.

This section describes two methods of updating the ILOM/BIOS firmware:

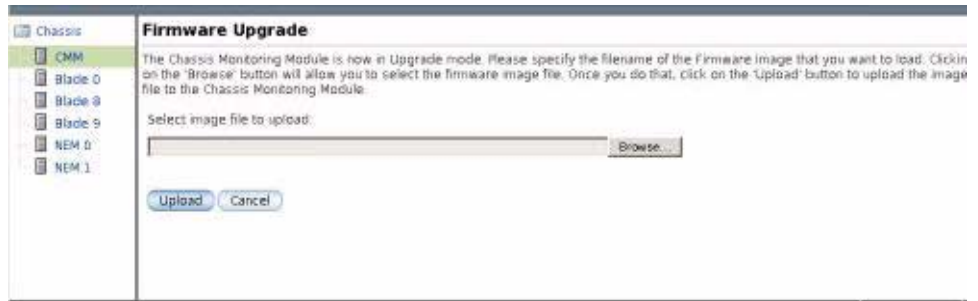
- “Update ILOM Firmware Using the Web Interface” on page 28
- “Update ILOM Firmware Using the CLI” on page 30

## ▼ Update ILOM Firmware Using the Web Interface

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



3. Click the Enter Upgrade Mode button.  
An Upgrade Verification dialog appears, indicating that other users who are logged in will lose their session when the update process completes.
4. In the Upgrade verification dialog, click OK to continue.  
The Firmware Upgrade page appears.



5. **Browse for the flash image file.**

6. **Click the Upload button.**

Wait for the file to upload and validate.

The Firmware Verification page appears.

7. **(Optional) In the Firmware Verification page, enable the Preserve Configuration.**

Enable this option if you want to save your existing configuration in ILOM and restore that existing configuration after the update process completes.

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

When you click Start Upgrade the upload process will start and a prompt to continue the process appears.

9. **At the prompt, click OK to continue.**

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

When the update completes, the system automatically reboots.

---

**Note** – The ILOM web interface might not refresh properly after the update completes. If the ILOM web is missing information or displays an error message, you might be viewing a cached version of the page from the version previous to the update. Clear your browser cache and refresh your browser before continuing.

---

10. **Reconnect to the CMM ILOM web interface.**

11. **Navigate to System Information --> Version to verify that the firmware version on the CMM corresponds to the firmware image you installed.**

---

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

---

## ▼ Update ILOM Firmware Using the CLI

1. **Log in to the ILOM CLI through the Management Ethernet port or the Serial Management port.**

**For the Management Ethernet port:** See [“Determine the Firmware Version Using the Management Ethernet Port CLI”](#) on page 26.

**For the Serial Management Port:** See [“Determine the Firmware Version Using the Serial Management Port CLI”](#) on page 26.

2. **From the ILOM CLI, use the following command:**

```
-> load -source tftp://tftpserver/ILOM-version-Sun_Blade_60x0.ima
```

Where *tftpserver* is the trivial file-transfer protocol (TFTP) server that contains the update and *ILOM-version-Sun\_Blade\_60x0.ima* is the firmware image file, for example:

**For Sun Blade 6000:** ILOM-3\_0\_10\_15-Sun\_Blade\_6000.ima

or

**For Sun Blade 6048:** ILOM-3\_0\_10\_15-Sun\_Blade\_6048.ima

---

## Updating the NEM Firmware

As of ILOM 3.0.9, the update firmware capability in ILOM was enhanced on some Oracle modular chassis systems to support firmware updates for Network Express Modules (NEMs). Prior to ILOM 3.0.9, NEM firmware updates were not supported from ILOM.

You can perform a NEM firmware update directly from the ILOM CLI or web interface. Supported file transfer methods for uploading the firmware package to the NEM include: TFTP, HTTPS, FTP, SFTP, SCP, HTTP, and browser-based.

---

**Note** – The browser-based local file transfer option is only available from the ILOM web interface.

---

For more information about how to perform the NEM firmware update from the ILOM web interface or CLI, see the following topics:



- “Before You Begin” on page 31
- “Update NEM Firmware Using the CLI” on page 31
- “Update NEM Firmware Using the Web Interface” on page 33

### **Before You Begin**

- From the NEM’s vendor product download web site, download the NEM firmware update package to a system on your network where you can later gain access to it from ILOM.
- To update the NEM firmware in ILOM, you need the Admin (a) role enabled.

## ▼ Update NEM Firmware Using the CLI

1. **Log in to the ILOM CMM CLI.**

2. **Use the `cd` command to navigate to the NEM requiring the firmware update.**

For example:

```
cd /CH/NEM#
```

Where # is the slot location where the NEM is installed in the chassis.

If your chassis system does not support multiple NEMs and one NEM is supported, the NEM location would equal 0. For this example, you would type:

```
cd /CH/NEM0
```

3. **Type the `show` command to view the NEM properties and the firmware version presently installed on the NEM.**

For example, see the NEM `show` property output below for the Sun Blade 6000 Virtualized Multi-Fabric 10GE NEM M2.

---

**Note** – The `fru_extra_1=` property field identifies the firmware version presently installed on the NEM.

---

```

-> show /CH/NEM0

/CH/NEM0
  Targets:
    MB
    SAS
    SP
    PRSNT
    STATE
    ERR
    OK
    SERVICE
    OK2RM
    LOCATE

  Properties:
    type = Network Express Module
    ipmi_name = NEM0
    system_identifier = SUNSP-0000000000
    fru_name = SUN BLADE 6000 VIRTUALIZED MULTI-FABRIC 10GE NEM
M2
    fru_version = FW 3.0.10.16, SAS 5.3.4.0
    fru_part_number = 540-7961-02
    fru_extra_1 = FW 3.0.10.16, SAS 5.3.4.0
    fault_state = OK
    load_uri = (none)
    clear_fault_action = (none)
    prepare_to_remove_status = NotReady
    prepare_to_remove_action = (none)
    return_to_service_action = (none)

  Commands:
    cd
    load
    reset
    set
    show

```

**4. Use the `load` command to upload and install the firmware update package on the NEM.**

For example, you would type:

**`load_uri=uri`**

Where *uri* equals the URI transfer method and location of the firmware package.

See the following CLI load examples for each supported file transfer method

Transfer Method	CLI load Command Examples
TFTP	<b>load_uri=tftp://ip_address/rom_nem.pkg</b>
FTP	<b>load_uri=ftp://username:password@ip_address/rom_nem.pkg</b>
SCP	<b>load_uri=scp://username:password@ip_address/rom_nem.pkg</b>
HTTP	<b>load_uri=http://username:password@ip_address/rom_nem.pkg</b>
HTTPS	<b>load_uri=https://username:password@ip_address/rom_nem.pkg</b>
SFTP	<b>load_uri=sftp://username:password@ip_address/rom_nem.pkg</b>

Where:

- *ip\_address* is the IP address of the system where the file is stored.
- *username* is the login user name to the system where the file is stored.
- *password* is the login password to the system where the file is stored.
- *rom\_nem.pkg* is the name of the firmware update package.

The user name and password for HTTP and HTTPS are optional.

---

**Note** – Alternatively, you can use the `set` and `load` commands in the ILOM CLI to specify the path of the NEM location, as well as the location of the firmware update package to upload. For example: `set /CH/NEM#/load_uri=uri`

---

**5. Wait a few moments for ILOM to confirm the completion of the firmware update process.**

A success or failure status appears.

**6. Use the `show` command to view and confirm the firmware version that is installed on the NEM.**

## ▼ Update NEM Firmware Using the Web Interface

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

**2. In the ILOM web interface, click CMM from the left pane.**

**3. Click the System Information --> Components tab.**

The Components page appears.

ABOUT 2 Warnings REFRESH

User: root Role: auro CMM Hostname: mpk12-2404-143-186

## Oracle® Integrated Lights Out Manager

Chassis

- CMM
  - Blade 0
  - Blade 5
  - NEM 0
  - NEM 1

System Information System Monitoring Power Management Storage Configuration User Management Remote Control Maintenance

Overview Components Fault Management Identification Information Banner Messages Session Timeout Versions

### Component Management

View component information, prepare to install or remove a component, update firmware, or clear fault status from this page. To modify a component, select the radio button next to that component, then choose an option from the Action drop down list. Components without radio buttons cannot be modified. Choosing the *Prepare to Remove* action shuts down the selected component and lights its blue *Ready to Remove* LED. To view further details, click on a Component Name.

Component Status

Actions: Update Firmware, Clear Faults

Component Name	Type	Fault Status	Ready to Remove Status
/CH/NEM0	Network Express Module	OK	Not Ready
/CH/NEM0/MB	Motherboard	-	-
/CH/NEM1	Network Express Module	OK	-

**4. In the Component Status table, do the following:**

- Select the radio button for the NEM that you want to update.
- Click the NEM name appearing in the Component Name column to view the firmware version presently installed on the NEM, then click Close to dismiss the dialog.
- In the Actions drop-down list box, select Update Firmware to initiate the firmware update process for the NEM.

The Upload Firmware dialog appears.

To update this component select the desired Transfer Protocol and fill in the appropriate fields.

Component: /SYS/NEMO

Current Version: (unknown)

Upload

Transfer Method:

Select File:

**5. In the Upload Firmware dialog, do the following:**

- a. Select the Upload Transfer Method from the drop-down list box.
- b. Specify the required fields for the selected transfer method as follows:

Transfer Method Option	Required Field	Instructions
Browser	Select File	Use the Browse button to specify the location of the NEM firmware update package.
FTP, SCP, HTTP, HTTPS, TFTP, SFTP	Host	Specify the IP address of the host system where the NEM firmware update package is stored.

Transfer Method Option	Required Field	Instructions
FTP, SCP, HTTP, HTTPS, TFTP, SFTP	Filepath	Specify the complete path to where the NEM firmware update package is stored.
FTP, SCP, HTTP, HTTPS, SFTP	Username	Specify the login user name to the system where the NEM firmware update package is stored.
FTP, SCP, HTTP, HTTPS, SFTP	Password	Specify the login password to the system where the NEM firmware update package is stored.

**6. Wait a few moments for ILOM to confirm the completion of the firmware update process.**

A success or failure status appears in the Upload Firmware dialog.

## Updating Chassis Component Firmware Using the CMM

As of ILOM 3.0.10, the CMM ILOM offers a centralized user interface for viewing the firmware version installed and initiating firmware updates on the following chassis components:

- Storage blades
- CPU blades
- Network Express Modules (NEMs): Not all NEMs have firmware. Check your NEM documentation to determine NEM firmware availability. For a detailed procedure for updating NEM firmware, see [“Updating the NEM Firmware” on page 30](#).

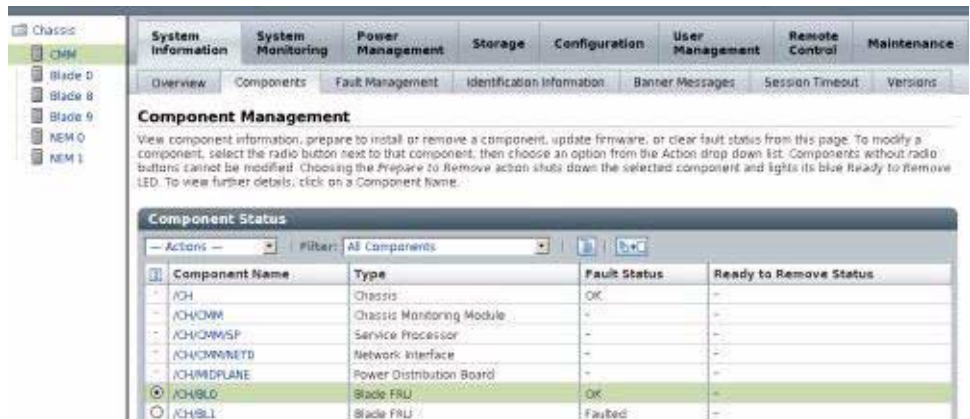
You must have CMM ILOM version 3.0.10 (available on the Oracle download site with Sun Blade 6000 Modular System Software release 3.2) installed on the CMM before using this firmware update tool. Server modules (blades) must be running ILOM 2.x or later.

You can update the ILOM firmware in two ways:

- [“Update Firmware Using the Web Interface” on page 37](#)
- [“Update Firmware Using the CLI” on page 39](#)

## ▼ Update Firmware Using the Web Interface

1. Download the firmware that you need from the Oracle software download site:  
<http://www.oracle.com/us/products/servers-storage/servers/blades/index.html>
  - a. Search the page for the blade or NEM that you want to update.
  - b. Download the latest firmware package and extract it to an accessible folder on the network.
2. Log in to the CMM ILOM as any user with Administrator privileges.
3. In the Chassis navigation pane, click on CMM.
4. Select System Information --> Components.
5. Select the component for which you want to upgrade the firmware.  
For example: /CH/BL0.



6. Select Update Firmware from the Actions drop-down menu.  
A dialog box appears.



7. Select the transfer method that you want to use from the Transfer Method field.

8. Fill in the required fields for the selected transfer method.

Transfer Method Option	Required Field	Instructions
Browser	Select File	Use the Browse button to specify the location of the NEM firmware update package.
FTP, SCP, HTTP, HTTPS, TFTP, SFTP	Host	Specify the IP address of the host system where the NEM firmware update package is stored.
FTP, SCP, HTTP, HTTPS, TFTP, SFTP	Filepath	Specify the complete path where the NEM firmware update package is stored.
FTP, SCP, HTTP, HTTPS, SFTP	Username	Specify the login user name to the system where the NEM firmware update package is stored.
FTP, SCP, HTTP, HTTPS, SFTP	Password	Specify the login password to the system where the NEM firmware update package is stored.

9. Click Update.

The firmware update process can take several minutes. A success or failure status appears in the Upload Firmware dialog.



## ▼ Update Firmware Using the CLI

1. Download the firmware that you need from the Oracle software download site:  
<http://www.oracle.com/us/products/servers-storage/servers/blades/index.html>

2. Search the page for the blade or NEM that you want to update.

3. Download the latest firmware package and extract it to an accessible folder on the network.

4. From a network connected terminal, log in to the CMM ILOM CLI using the root user account by entering the following command:

```
$ ssh root@cmm_ipaddress
```

Where *cmm\_ipaddress* is the IP address of the CMM ILOM.

5. Enter the password (the default is changeme).

The ILOM CLI prompt appears:

```
->
```

6. Change directories to the blade slot containing the blade or NEM to be upgraded:

```
-> cd /CH/BLn
```

or

```
-> cd /CH/NEMn
```

Where *BLn* is the chassis blade slot number of the blade to be upgraded and *NEMn* is the NEM to be upgraded.

7. Enter the following command:

```
-> load -source transfer_method://transfer_server_ipaddress/firmware-version.pkg
```

Where

- *transfer\_method* is one of the following: FTP, SCP, HTTP, HTTPS, TFTP, SFTP
- *transfer\_server\_ipaddress* is the domain name or IP address of your transfer server where you copied the image file
- *firmware-version* is the name of the .pkg file.

8. When the process completes, ensure that the proper firmware version was installed. Enter the following command:

```
-> version /CH/BL $n$ 
```

or

```
-> version /CH/NEM $n$ 
```

Where BL $n$  is the chassis slot number of the blade that was upgraded and NEM $n$  is the NEM that was upgraded.

---

## Resetting the CMM

If neither of the procedures in this section is available, you can remove the CMM from the chassis and reinstall it to reset the CMM.

Refer to the *Sun Blade 6000 Modular System Service Manual* or the *Sun Blade 6048 Modular System Service Manual* for information on how to remove and install the CMM.

The following procedures are covered in this section:

- [“Reset the CMM Using the Web Interface” on page 40](#)
- [“Reset the CMM Using the CLI” on page 41](#)

### ▼ Reset the CMM Using the Web Interface

1. Log in to the ILOM web interface.
2. Navigate to Maintenance --> Reset Components.
3. Select /CH/CMM, then click Reset.



## ▼ Reset the CMM Using the CLI

1. Log in to the ILOM CLI.
2. From the ILOM CLI, type the following command:

```
-> reset /CMM
```



## CMM Power Management

---

This chapter contains ILOM power management information that is specific to the Sun Blade 6000 and Sun Blade 6048 CMM and ILOM 3.x.

For more information on power management, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

This chapter contains the information described in the following table.

Description	Links
Enable or disable Light Load Efficiency Mode (LLEM)	<ul style="list-style-type: none"><li>• <a href="#">“Light Load Efficiency Mode (LLEM)” on page 44</a></li></ul>
Force power supply fans to low speed	<ul style="list-style-type: none"><li>• <a href="#">“Force Power Supply Fan Speed” on page 48</a></li></ul>
Disable power management	<ul style="list-style-type: none"><li>• <a href="#">“Disabling the Power Management Policy” on page 49</a></li></ul>
Learn about ILOM readings for specific Sun Blade 6048 Modular System cases	<ul style="list-style-type: none"><li>• <a href="#">“ILOM 3.0 for Specific Sun Blade 6048 Cases” on page 51</a></li></ul>

---

# Light Load Efficiency Mode (LLEM)

The Light Load Efficiency Mode (LLEM) is a new feature of CMM ILOM 3.0.6.11.

This section covers the following sections:

- [“About LLEM” on page 44](#)
- [“Setting LLEM Using the Web Interface” on page 44](#)
- [“Setting LLEM Using the CLI” on page 46](#)

## About LLEM

Under the LLEM, the CMM monitors the power being used and automatically shuts down the power supply unit (PSU) sides to achieve higher efficiency. While enabled, LLEM runs in both redundant and non-redundant mode.

The CMM always disables PSU sides in descending order. When the power load level increases, the CMM renews those disabled sides to cover the demand. If a new blade is inserted into the chassis, it can be powered on even if its power budget exceeds the power available from the sides currently turned on.

When an unexpected AC fault occurs, LLEM is suspended and all sides will become enabled, verified by the sensor value of `I_V12` and `V_OUT_OK`. If the fault is cleared, configured LLEM policy automatically goes back into effect.

When the LLEM is disabled, all PSU sides, including those previously disabled, become enabled. This can be verified by the sensor value of `I_V12` and `V_OUT_OK`.

For further information on ILOM power management features, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

## Setting LLEM Using the Web Interface

This section covers the following procedures:

- [“Enable or Disable LLEM Using the Web Interface” on page 44](#)
- [“Enable or Disable Redundant Mode Using the Web Interface” on page 46](#)

### ▼ Enable or Disable LLEM Using the Web Interface

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

2. Click on CMM in the Chassis navigation pane.
3. Navigate to the Configuration --> Policy page.



4. Select Light Load Efficiency Mode.
5. Select Enable or Disable from the Actions drop-down list.
6. To turn power supplies on or off in the Policy page:
  - a. Select Monitor Power Supply  $x$  Side  $y$  for power.

In the following example, Monitor Power Supply 0 Side 0 is selected.



- b. Select Enable or Disable from the Actions menu.

## ▼ Enable or Disable Redundant Mode Using the Web Interface

1. Log in to the ILOM web interface.
2. Click on CMM in the Chassis navigation pane.
3. Navigate to the Power Management --> Redundancy page.



4. Select one of the following from the drop-down menu:
  - None: To set non-redundant mode.
  - N+N: To set redundant mode.
5. Click Save.

## Setting LLEM Using the CLI

This section covers the following procedures:

- [“Enable or Disable LLEM Using the CLI” on page 46](#)
- [“Enable Redundant Mode Using the CLI” on page 47](#)
- [“Enable Non-Redundant Mode Using the CLI” on page 47](#)

## ▼ Enable or Disable LLEM Using the CLI

1. Log in to the CMM ILOM CLI.
2. To enable or disable LLEM, use the command:

```
-> set /CMM/policy LIGHT_LOAD_EFFICIENCY_MODE=  
[enabled|disabled]
```



3. When LLEM is disabled, you can turn the PSU sides on or off with this command:

```
-> set /CMM/policy MONITOR_PSn_SIDEn=[enabled|disabled]
```

---

**Note** – It is advisable to disable any PSU side first before unplugging the power cord.

---

You can check the sensor value of `/CH/PSn/Sn/I_12V` or `/CH/PSn/Sn/V_OUT_OK`, where the value of `I_12V` being 0 or `V_OUT_OK` deasserted indicates the corresponding side is disabled.

You can disable any PSU sides monitoring. In both redundant and non-redundant modes, LLEM works on those sides that are under monitoring.

## ▼ Enable Redundant Mode Using the CLI

1. Log in to the CMM ILOM CLI.
2. Set redundant mode using this command:

```
-> set /CMM/powermgmt redundancy=n+n
```

All `MONITOR_PSn_SIDEn` are set to enabled, and any attempt to disable any PSU side's monitoring is not allowed.

## ▼ Enable Non-Redundant Mode Using the CLI

1. Log in to the CMM ILOM CLI.
2. Set non-redundant mode using this command:

```
-> set /CMM/powermgmt redundancy=none
```

# Force Power Supply Fan Speed

A new feature introduced in ILOM 3.0.6.11 allows the adjustment of power supply fan speed.

The high and low speed settings are defined as follows:

- High speed refers to the fans running at 100% capacity.
- Low speed refers to the fans running at 80% capacity.

---

**Note** – Only force power supply unit (PSU) fans to low speed if half the PEM slots or fewer are in use.

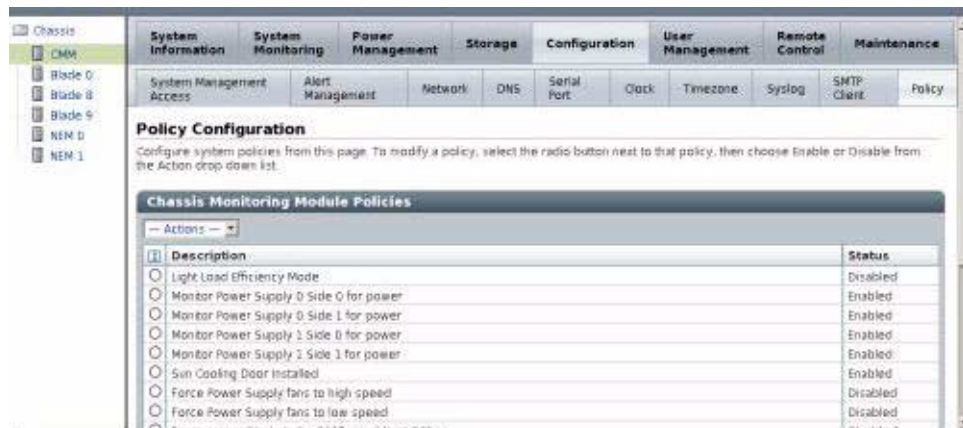
---

This section covers the following topics:

- [“Set the Power Supply Fan Speed Using the Web Interface”](#) on page 48
- [“Set the Power Supply Fan Speed Using the CLI”](#) on page 49

## ▼ Set the Power Supply Fan Speed Using the Web Interface

1. Log in to the ILOM web interface.
2. Click on CMM in the Chassis navigation pane.
3. Navigate to the Configuration --> Policy.



4. Choose one of the following options:

- Force Power Supply fans to low speed
- Force Power Supply fans to high speed

5. Select **Enable** or **Disable** from the **Actions** drop-down menu.

As the power supply fans cool the power supplies, the power supply fans also cool the PEM slots.

---

**Note** – If you enable both fan speed policies, high speed policy dominates.

---

## ▼ Set the Power Supply Fan Speed Using the CLI

1. Log in to the ILOM CLI interface.

2. Execute the following command:

```
-> set /CMM/policy PS_FANS_HIGH=[enabled|disabled]
-> set /CMM/policy PS_FANS_LOW=[enabled|disabled]
```

As the power supply fans cool the power supplies, the power supply fans also cool the PEM slots.

---

**Note** – If you enable both fan speed policies, high speed policy dominates.

---

---

## Disabling the Power Management Policy

A new power management option has been added to CMM ILOM 3.0.6.11c (Software Version 3.1.13), which enables the user to disable power management so that blades in the chassis attempt to power on even if power allocation has been exceeded.



---

**Caution** – Chassis shutdown can occur. Do not disable power management unless you are advised to by Oracle Services personnel.

---

To disable power management, when instructed by Oracle Services, use one of the following procedures:

- [“Disable Power Management Policy Using the Web Interface” on page 4-50](#)
- [“Disable Power Management Policy Using the CLI” on page 4-50](#)

## ▼ Disable Power Management Policy Using the Web Interface

1. Log in to the ILOM web interface.
2. Select CMM from the Chassis navigation pane.
3. Navigate to the Configuration --> Policy.
4. Select Manage Chassis Power.
5. Select Disable from the Actions drop-down list.

The following ILOM screen graphic shows the Manage Chassis Power option at the bottom of the Policy Configuration page.



## ▼ Disable Power Management Policy Using the CLI

1. Log in to the CMM ILOM CLI.
2. Type the following command:  

```
-> set /CMM/policy POWER_MANAGEMENT=disabled
```

---

# ILOM 3.0 for Specific Sun Blade 6048 Cases

The power supply configurations covered in this section apply only to the Sun Blade 6048 Modular System.

This section covers the following topics:

- [“ILOM Behavior With Two Power Cord Configuration” on page 51](#)
- [“ILOM Readings for Specific Power Supply States” on page 52](#)

## ILOM Behavior With Two Power Cord Configuration

This section specifies how CMM and server module firmware behave when only two of the three power plugs are connected to an A231 power supply unit (PSU).

There are three plugs on the back of each A231 PSU. These plugs are named AC0, AC1, and AC2. Each plug allows connection of a 220V power cord. When only two of the available three plugs are connected to the A231 PSUs, this provides 5600 watts to the entire chassis.

If you connect only two of the total three plugs, connect them to AC0 and AC1. AC2 should not be connected.

For further information on Sun Blade 6048 Modular System sensors, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Supplement for Sun Blade 6000 and Sun Blade 6048 Modular Systems (820-7603)*.

### ▼ Configure the CMM for Two Power Cords

1. To set up a two power cord configuration, disable the power supply side in the CMM ILOM with the following commands:

```
-> set /CMM/policy MONITOR_PS0_SIDE2=disabled
```

```
-> set /CMM/policy MONITOR_PS1_SIDE2=disabled
```

2. To view the disabled power cord side 2 configuration, type:

```
-> show /CMM/policy/

/CMM/policy
  Targets:

  Properties:
    COOLING_DOOR_INSTALLED = disabled
    MONITOR_PS0_SIDE0 = enabled
    MONITOR_PS0_SIDE1 = enabled
    MONITOR_PS0_SIDE2 = disabled
    MONITOR_PS1_SIDE0 = enabled
    MONITOR_PS1_SIDE1 = enabled
    MONITOR_PS1_SIDE2 = disabled
    PS_FANS_HIGH = disabled

  Commands:
    cd
    set
    show
```

## ILOM Readings for Specific Power Supply States

This section provides some of the sensor readings for the system event log (SEL) in cases that are specific to the Sun Blade 6048 Modular System.

To view the SEL using IPMItool, use the following command:

```
ipmitool -H SPIPaddress -U root -P changeme sel list
```

## AC Cables Are Disconnected

When an AC cable gets disconnected, the SEL displays the readings as shown in the example for power supply module 0, side 0 in [TABLE 4-1](#).

---

**Note** – The order of the events might not match the real time event exactly, because that is based on how the sensors are being scanned.

---

**TABLE 4-1** AC Cable Disconnect SEL Readings

Event ID	Device	State	Description
8	Voltage PS0/S0/V_OUT_OK	State Deasserted	PSU 0 side 0 DC output is out (because AC is unplugged).
9	Voltage PS0/S0/V_IN_ERR	Predictive Failure Asserted	PSU 0 side 1 AC is disconnected.

## AC Cables Are Disconnected, Then Are Reconnected

When an AC cable gets disconnected, then plugged back in, the SEL displays the readings as shown for power supply module 0, side 0 in [TABLE 4-2](#).

**TABLE 4-2** AC Cables Reconnected SEL Readings

Event ID	Device	State	Description
8	Voltage PS0/S0/V_OUT_OK	State Deasserted	PSU 0 side 0 DC output is out (because AC is unplugged).
9	Voltage PS0/S0/V_IN_ERR	Predictive Failure Asserted	PSU 0 side 0 AC is disconnected.
a	Voltage PS0/S0/V_OUT_OK	State Asserted	PSU 0 side 0 DC output is OK (because AC is plugged in).
b	Voltage PS0/S0/V_IN_ERR	Predictive Failure Deasserted	PSU 0 side 0 is connected.

## stop /CH Command

When the `stop /CH` command is applied, the SEL displays the readings as shown in the example in [TABLE 4-3](#). This example describes a two power cord configuration.

**TABLE 4-3** stop /CH SEL Readings

Event ID	Device	State	Description
29	Module/Board NEM1/STATE	Transition to Power Off	Not enough power for the NEM 1, since the PSU shuts off.
2a	Voltage PS0/S0/V_OUT_OK	State Deasserted	PSU 0 side 0 is out.
2b	Voltage PS0/S1/V_OUT_OK	State Deasserted	PSU 0 side 1 is out.
2c	Module/Board NEM0/STATE	Transition to Power Off	Not enough power for the NEM 0, since the PSU shuts off.
2d	Voltage PS1/S0/V_OUT_OK	State Deasserted	PSU 1 side 0 is out.
2e	Voltage PS1/S1/V_OUT_OK	State Deasserted	PSU 1 side 0 is out.

## start /CH Command

When the `start /CH` command is applied, the SEL displays the readings as shown in the example in [TABLE 4-4](#). This example describes a two power cord configuration.

**TABLE 4-4** start /CH SEL Readings

Event ID	Device	State	Description
2f	Module/Board NEM1/STATE	Transition to Running	NEM 1 is powering on.
30	OEM BL7/ERR	Predictive Failure Deasserted	Blade module does not have an error.
31	Module/Board NEM0/STATE	Transition to Running	NEM 0 is powering on.
32	Voltage PS1/S0/V_OUT_OK	State Asserted	PSU 1 side 0 is on.
33	Voltage PS1/S1/V_OUT_OK	State Asserted	PSU 1 side 1 is on.



**TABLE 4-4** start /CH SEL Readings (Continued)

Event ID	Device	State	Description
34	OEM BL1/ERR	Predictive Failure Deasserted	Blade module does not have an error.
35	Voltage PS0/S0/V_OUT_OK	State Asserted	PSU 0 side 0 is on.
36	Voltage PS0/S1/V_OUT_OK	State Asserted	PSU 0 side 1 is on.

## One PSU Is Removed

When one PSU is removed, and there is too much power consumption in the chassis to support PSU redundancy, the SEL displays the readings shown in [TABLE 4-5](#).

**TABLE 4-5** PSU Removed SEL Readings

Event ID	Device	State	Description
1	Entity Presence PS0/PRSNT	Device Absent	PS0 is absent from the system.
2	Voltage PS0/S0/V_OUT_OK	State Deasserted	PSU 0 side 0 DC power is out.
3	Voltage PS0/S1/V_OUT_OK	State Deasserted	PSU 0 side 1 DC power is out.
4	Voltage PS0/S2/V_OUT_OK	State Deasserted	PSU 0 side 2 DC power is out.

## PSU Is Reinserted

TABLE 4-6 shows the SEL readings as a PSU is reinserted into the system and the system recognizes that power has been reapplied.

**TABLE 4-6** PSU Reinserted SEL Readings

Event ID	Device	State	Description
5	Entity Presence PS0/PRSNT	Device Present	PS0 is present in the system.
6	Voltage PS0/S0/V_OUT_OK	State Asserted	PSU 0 side 0 DC power is on.
7	Voltage PS0/S1/V_OUT_OK	State Asserted	PSU 0 side 1 DC power is on.
8	Voltage PS0/S2/V_OUT_OK	State Asserted	PSU 0 side 2 DC power is on.

# Sun Blade Zone Manager

---

This chapter contains information on the Sun Blade Zone Manager feature as described in the following table.

Description	Links
Learn about features of the Sun Blade Zone Manager and prerequisites for use of the application	<ul style="list-style-type: none"><li>• <a href="#">“Introduction to the Sun Blade Zone Manager” on page 58</a></li></ul>
Access and enable the Sun Blade Zone Manager	<ul style="list-style-type: none"><li>• <a href="#">“Accessing the Sun Blade Zone Manager” on page 66</a></li></ul>
Create a storage zoning configuration	<ul style="list-style-type: none"><li>• <a href="#">“Creating the Chassis Storage Access Configuration” on page 72</a></li></ul>
View or modify the storage zoning configuration	<ul style="list-style-type: none"><li>• <a href="#">“Viewing or Modifying the Chassis Storage Access Configuration” on page 83</a></li></ul>
Save the storage zoning configuration	<ul style="list-style-type: none"><li>• <a href="#">“Saving the Chassis Storage Access Configuration” on page 97</a></li></ul>
Back up the storage zoning configuration	<ul style="list-style-type: none"><li>• <a href="#">“Backing Up the Storage Access Configuration” on page 100</a></li></ul>
Recover the storage zoning configuration	<ul style="list-style-type: none"><li>• <a href="#">“Recovering Zoning Configurations” on page 102</a></li></ul>
Reset the zoning configuration	<ul style="list-style-type: none"><li>• <a href="#">“Resetting the Zoning Configuration” on page 106</a></li></ul>
Reset the zoning password	<ul style="list-style-type: none"><li>• <a href="#">“Resetting the Zoning Password” on page 107</a></li></ul>

---

# Introduction to the Sun Blade Zone Manager

This section covers the following topics:

- [“Sun Blade Zone Manager Overview” on page 58](#)
- [“Supported ILOM Interfaces” on page 58](#)
- [“Zoning Configuration Overview” on page 62](#)
- [“Supported Hardware and Firmware Configurations” on page 65](#)

## Sun Blade Zone Manager Overview

The Sun Blade Zone Manager handles the SAS-2 storage assignments for the Sun Blade Modular System CPU blades, storage devices, and NEMs. The Zone Manager runs on the chassis monitoring module (CMM) and communicates to the storage resources over Ethernet links between it and the SAS-2 expanders on the storage blades and the NEMs.

Zone Manager allows storage devices from a storage module installed in the chassis to be assigned to a server blade. Storage devices can be assigned to more than one server module (blade) in the case of a cluster.

Currently, Zone Manager is only available for the Sun Blade 6000 Modular System.

## Supported ILOM Interfaces

The Sun Blade Zone Manager is available in the Sun Blade 6000 Modular System CMM SW 3.0.10 or later, which includes ILOM 3.0.10 and later.

You can access the Zone Manager through either the ILOM web interface or command-line interface (CLI). The web interface and the CLI are functionally equivalent, but the web interface has some additional ease-of-use features.

This section covers the following topics:

- [“Accessing Zone Manager Using the Web Interface” on page 59](#)
- [“Accessing Zone Manager Using the CLI” on page 61](#)



**Note** – NEM0 and NEM1 targets appear in the Zone Manager when these NEMs are installed; however, external SAS connections in the Sun Blade Zone Manager are not supported at this time.

See [“Creating the Chassis Storage Access Configuration Using Quick Setup”](#) on page 72 for more information on Quick Setup.

Detailed Setup enables you to make changes to the zoning configuration that you set up in Quick Setup or to make individual assignments of storage devices to server blades. The following example shows drives being selected for removal from the server blade assignment.

**Modify Group**

Indicated below is your selected group of components that currently have assigned access. Click on those within the group that you would like to remove access to. Click on any components outside the group that you want added. When you are ready to apply the changes, click 'Save'.

SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-0000000-000000000

Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9
Server Blade	Server Blade	Storage Blade	Server Blade	Server Blade	Storage Blade	Server Blade	Storage Blade	Server Blade	Storage Blade
SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2
		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1			HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty			empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty

NEM Slot 0	NEM Slot 1	NAC name:	-
SAS NEM NEM-2	SAS NEM NEM-2	Disk type:	-
EXT 0 EXT 1 EXT 2 EXT 3	EXT 0 EXT 1 EXT 2 EXT 3	WWN:	-

Drives HDD4-HDD7 are selected and highlighted in blue. When the configuration is saved, these storage devices will no longer be associated with the server blade in Slot 1.

For more information on changing a zoning configuration using Detailed Setup, see [“View and Modify the Chassis Storage Configuration Using the Web Interface”](#) on page 84.

## Accessing Zone Manager Using the CLI

The command-line interface (CLI) provides access to the zoning for blades and storage devices through the `/STORAGE/sas_zoning` namespace.

When zoning is enabled, blades and NEMs that are SAS-2 capable will be displayed as targets under `/STORAGE/sas_zoning`. For example:

```
-> show /STORAGE/sas_zoning

Targets:
  BL0
  BL6
  BL7
  BL8
  BL9
  NEM0
  NEM1

Properties
  zone_management_state = enabled
  reset_password_action = (Cannot show property)
  reset_access_action = (Cannot show property)

Commands:
  cd
  set
  show
```

---

**Note** – NEM0 and NEM1 targets appear in the Zone Manager when these NEMs are installed; however, external SAS connections in the Sun Blade Zone Manager are not supported at this time.

---

Storage devices installed on a storage blade are shown as targets of the storage blade. For example, if BL9 is a storage blade installed in Slot 9, the storage devices installed on this blade are shown as follows:

```
-> show /STORAGE/sas_zoning/BL9

Targets:
  HDD0
  HDD2
  HDD3
  HDD5
```

You can access and modify the zoning configurations either through the server blade or the storage blade. Either method has the same result.

# Zoning Configuration Overview

The following topics provide an overview of the zoning configurations through the CLI:

- [“Zoning Commands” on page 62](#)
- [“Assigning Storage to a Server Blade” on page 63](#)
- [“Assigning a Server Blade to Storage” on page 64](#)

## Zoning Commands

You can assign storage to a server blade or a server blade to a storage device. Either method produces the same result.

When you are assigning storage devices to a server blade, use the following command:

```
-> set add_storage_access=/CH/BL $n$ /HDD $n$ 
```

Where BL $n$  is the storage blade, HDD $n$  is a hard disk drive installed on the storage blade.

Optionally, you can assign multiple storage devices to a blade in the same command line by separating storage devices with a comma. For example:

```
-> set add_storage_access=/CH/BL $n$ /HDD0,/CH/BL $n$ /HDD1
```

When you are assigning a server blade to a storage device, use the following command:

```
-> set add_host_access=/CH/BL $n$ 
```

Where BL $n$  is the server blade that you are assigning the storage device to.



## Assigning Storage to a Server Blade

Before a server blade has a storage device assigned to it, no targets are displayed under the blade. In the following example, BL0 is a server blade in Slot 0.

```
-> cd /STORAGE/sas_zoning/BL0
-> show

/STORAGE/sas_zoning/BL0
  Targets:

  Properties:
    add_storage_access = (Cannot show property)
    remove_storage_access = (Cannot show property)
```

The following command assigns the HDD0 installed on the storage blade in chassis Slot 9 to the server blade installed in Slot 0.

```
-> set add_storage_access=/CH/BL9/HDD0
```

After a storage device is assigned to a server blade, the storage device appears as a target under the server blade. For example:

```
-> show

/STORAGE/sas_zoning/BL0
  Targets:
    0 (/CH/BL9/HDD0)

  Properties:
    add_storage_access = (Cannot show property)
    remove_storage_access = (Cannot show property)
```

## Assigning a Server Blade to Storage

Before a storage device has a blade assigned to it, no targets are displayed under the storage device. In the following example, HDD0 is a storage device installed on a storage blade installed in Slot 9 of the chassis.

```
-> cd /STORAGE/sas_zoning/BL9/HDD0
-> show

/STORAGE/sas_zoning/BL9/HDD0

Targets:

Properties:
  type = Hard Disk
  disk_type = SAS
  wwn = 0x5000c50003d3a765, 0x5000c50003d3a766
  sas_speed = 6.0 Gbps
  add_host_access = (Cannot show property)
  remove_host_access = (Cannot show property)
```

The following command assigns server blade in Slot 0 to HDD0 on storage blade 9:

```
-> set add_host_access=/CH/BL0
```

After a server blade is assigned to the storage device, the server blade appears as a target under the storage device. For example:

```
-> show

/STORAGE/sas_zoning/BL9/HDD0

Targets:
  0 (/CH/BL0)

Properties:
  type = Hard Disk
  disk_type = SAS
  wwn = 0x5000c50003d3a765, 0x5000c50003d3a766
  sas_speed = 6.0 Gbps
  add_host_access = (Cannot show property)
  remove_host_access = (Cannot show property)
```

For detailed instructions on creating and modifying zoning, see the following procedures:

- [“Creating the Chassis Storage Access Configuration” on page 72](#)
- [“Viewing or Modifying the Chassis Storage Access Configuration” on page 83](#)

# Supported Hardware and Firmware Configurations

The following sections describe the hardware and firmware configurations to support the Sun Blade Zone Manager:

- [“SAS-2 Capable Hardware”](#) on page 65
- [“Additional System Requirements”](#) on page 65

## SAS-2 Capable Hardware

All of the following hardware in the chassis must be SAS-2 capable in order to be recognized by the Sun Blade Zone Manager:

- Server blades with SAS-2 REMs
- Network express modules (NEMs)
- Storage blades

If a storage module or server blade is not SAS-2 capable, it is not included in the Zone Manager configuration. The web interface acknowledges the presence of the blade, but it is labeled as a “non SAS-2” device. The blade is not displayed at all in the CLI if it is not SAS-2 enabled.

SAS-2 devices, except for CPU blades, must be powered on to be recognized by the Zone Manager. In addition, SAS-2 devices in a failed state might not be recognized by Zone Manager. Refer to your platform ILOM Supplement documentation or platform Administration Guide for information on detecting component faults.

## Additional System Requirements

- Your Sun Blade 6000 Modular System must have a PCIe 2.0 compliant midplane. For more information on determining this, refer to the *Sun Blade 6000 Modular System Product Notes*.
- Your Sun Blade 6000 Modular System must have software release 3.2.1 installed. This release includes the minimum CMM ILOM firmware version (3.0.10.15a), which supports SAS-2 and includes the Sun Blade Zone Manager.
- You must have already installed your SAS-2 supported components (server module with SAS-2 REM, SAS-2 NEMs, and SAS-2 storage modules).
- Your SAS-2 NEM must be at a firmware version level that supports zoning. Check your NEM Product Notes for version information and available updates.
- You must have already performed initial setup and configuration of your CMM ILOM and planned your connection method (web browser or CLI) as described in [Chapter 2](#) of this document.

---

# Accessing the Sun Blade Zone Manager

This section contains information on how to access and enable the Zone Manager. This section covers the following topics:

- [“Access and Enable the Sun Blade Zone Manager Using the Web Interface” on page 66](#)
- [“Access and Enable the Sun Blade Zone Manager Using the CLI” on page 70](#)

## ▼ Access and Enable the Sun Blade Zone Manager Using the Web Interface

**Before You Begin:** Ensure that your chassis configurations meets the requirements in [“Supported Hardware and Firmware Configurations” on page 65](#).

Follow these steps to access and enable the Zone Manager using the web interface:

1. **Open a web browser and log in to the CMM by entering the following URL:**

**http://chassis\_sp\_ipaddress/**

Where *chassis\_sp\_ipaddress* is the IP address of your chassis service processor.

The ILOM login page appears.

2. **Log in as the root user account.**

The CMM ILOM main page is displayed.

ABOUT 2 Warnings User: root Role: auro CMM Hostname: SUNCMM-0000000-0000000000 REFRESH LOG OUT


Oracle® Integrated Lights Out Manager

Chassis

- CMM
- Blade 0
- Blade 1
- Blade 3
- Blade 4
- Blade 7
- NEM 0
- NEM 1

### Chassis View

To manage a Blade or Chassis Monitoring Module, click on it in the left navigation pane or in the image below.



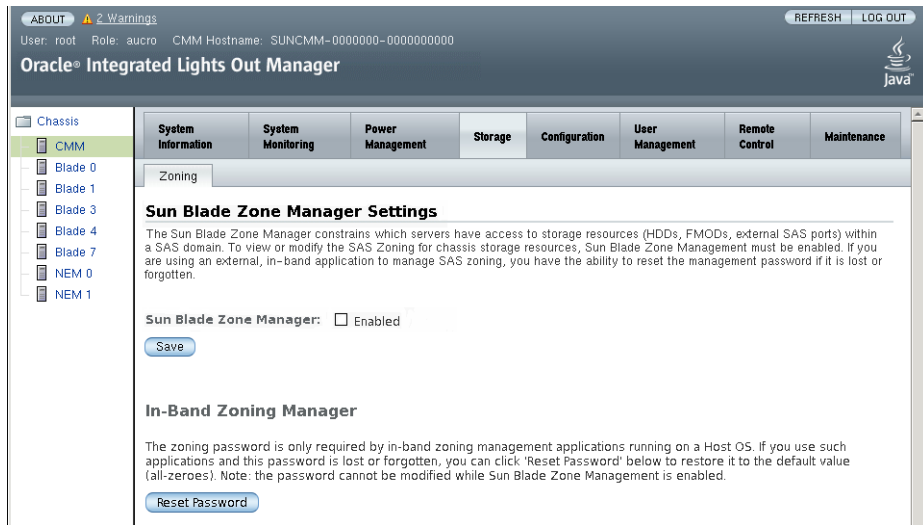
#### Chassis Inventory

Component	Name	Part Number	Serial Number
/CH	SUN BLADE 6000 MODULAR SYSTEM	541-3789-01	0000000-0000000000
/CH/CMM	CMM	371-1447-09	0111APO-0828YC07AD
/CH/BL0	SUN BLADE X6270 M2 SERVER MODULE	541-2861-00	1005LCB-07385M0035
/CH/BL1	SUN BLADE X6270 M2 SERVER MODULE	541-2861-00	1005LCB-07385M8265
/CH/BL2	SUN BLADE STORAGE MODULE M2	511-1365-02	00000000
/CH/BL3	SUN BLADE X6270 M2 SERVER MODULE	541-2861-00	1005LCB-07385M0828
/CH/BL4	SUN BLADE X6270 M2 SERVER MODULE	541-2861-00	1005LCB-07385M011A
/CH/BL5	SUN BLADE STORAGE MODULE M2	511-1365-02	00000000
/CH/BL6	SUN BLADE STORAGE MODULE M2	511-1365-02	00000000
/CH/BL7	SUN BLADE X6270 M2 SERVER MODULE	541-2861-00	1005LCB-11A85M0035
/CH/BL8	SUN BLADE STORAGE MODULE M2	511-1365-02	00000000
/CH/BL9	SUN BLADE STORAGE MODULE M2	511-1365-02	0000000000
/CH/NEM0	SUN BLADE 6000 VIRTUALIZED MULTI-FABRIC 10GE NEM M2	540-7961-02	0000000-7001

**Note** – In the left pane, installed server blades are listed, but not installed storage modules. This is because the CMM ILOM controls storage module Integrated Lights Out Management functions.

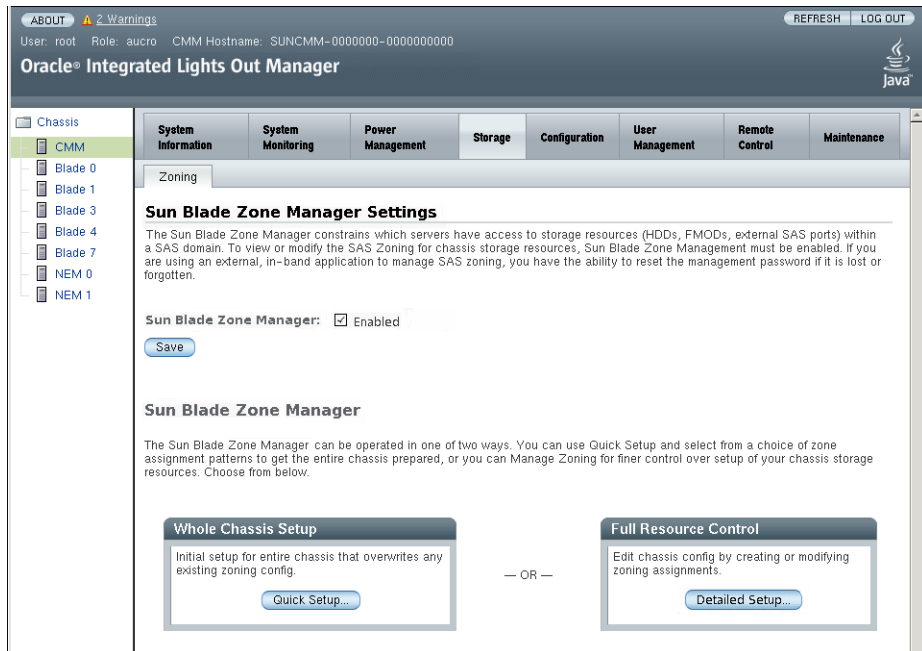
3. Click on CMM in the left Chassis navigation pane and then click the Storage tab.

The Zone Manager Settings sub-page is displayed.

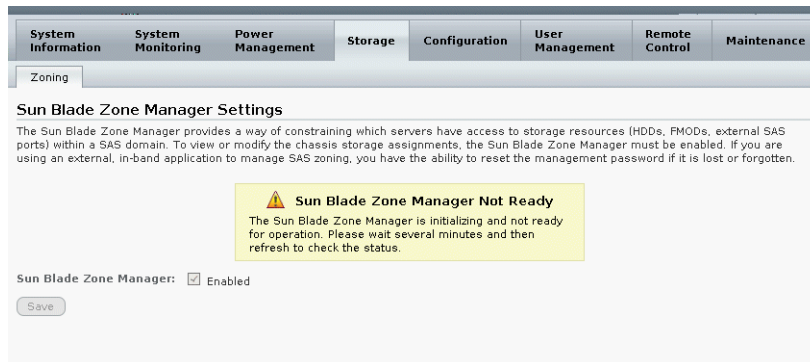


4. Enable CMM zoning by clicking the Enable check box, and then clicking the Save button.

This enables you to create, view, and manage zoning settings through the CMM.



You might get the following message if the CMM ILOM services are still initializing:



If you get this message, wait an additional five minutes and then try again. You need to close and reopen, or refresh the page.

5. Use the procedures in “Creating the Chassis Storage Access Configuration” on page 72 to set up the storage zoning.

## ▼ Access and Enable the Sun Blade Zone Manager Using the CLI

**Before You Begin:** Ensure that your chassis configurations meets the requirements in “Supported Hardware and Firmware Configurations” on page 65.

Follow these steps to access and enable Zone Manager using the CLI:

1. **Open a terminal window and establish an SSH connection to the CMM by entering the following command:**

```
# ssh -l root cmm_ipaddress
```

Where *cmm\_ipaddress* is the IP address of the CMM.

The login prompt is displayed.

2. **Log in as root and enter the root password:**

```
/hostname/login: root
```

```
password: xxxxxxxx
```

After you have successfully logged in, the CLI prompt is displayed:

```
->
```

3. **Confirm that you have the minimum CMM firmware version required for zoning by entering the command:**

```
-> version
```

You need ILOM firmware 3.0.10 at a minimum. If you have an earlier version, you need to download CMM ILOM software version 3.2.1 (or later). See [Chapter 3](#) for firmware download and upgrade procedures. Then you need to upgrade your CMM ILOM firmware.

4. **Change directories to `sas_zoning` by entering the command:**

```
-> cd /STORAGE/sas_zoning/
```



5. Check whether `sas_zoning` is enabled by entering the `show` command. For example:

```
-> show
/STORAGE/sas_zoning

Targets:

Properties:
  zone_management_state = disabled
  reset_password_action = (Cannot show property)
  reset_access_action = (Cannot show property)

Commands:
  cd
  set
  show
```

If the `zone_management_state = disabled`, then there are no saved SAS-2 zone configurations.

6. If necessary, enable zoning by entering:

```
-> set zone_management_state=enabled
```

- If the zone manager is ready to be enabled, you get the following message:  
Enabling the Sun Blade Zone Manager will result in the clearing of all zoning configuration in the installed chassis SAS hardware, and any SAS disk I/O in progress will be interrupted.

```
Are you sure you want to enable the Sun Blade Zone Manager (y/n)? y
```

```
Set 'zone_management_state' to 'enabled'
```

- If the CMM ILOM has not initialized, you will get the following message:  
set: The Sun Blade Zone Manager is initializing and not ready for operation. Please wait several minutes and try again.

If you get this message, wait five minutes and retry the command.

7. Use the procedures in [“Creating the Chassis Storage Access Configuration” on page 72](#) to set up the storage zoning.

---

# Creating the Chassis Storage Access Configuration

There are three options for creating chassis storage access: the web interface using Quick Setup, the web interface using Detailed Setup, and the CLI. You can also use a backup zoned configuration by recovering the configuration as shown in [“Recovering Zoning Configurations” on page 102](#).

Quick Setup is a wizard for automating the process of creating an initial chassis storage access configuration for SAS-2 compliant CPU blades. Quick Setup is only available through the ILOM web interface. There is no Quick Setup equivalent for the CLI.

This section covers the following topics:

- [“Creating the Chassis Storage Access Configuration Using Quick Setup” on page 72](#)
- [“Creating the Chassis Storage Access Configuration Using Detailed Setup” on page 78](#)
- [“Creating a Chassis Storage Configuration Using the CLI” on page 81](#)

## Creating the Chassis Storage Access Configuration Using Quick Setup

The Quick Setup option through the ILOM web interface enables you to choose from four different configuration options to zone the blades and storage devices in the chassis.

---

**Note** – NEM0 and NEM1 targets appear in the Zone Manager when these NEMs are installed; however, external SAS connections in the Sun Blade Zone Manager are not supported at this time.

---

This section covers the following topics:

- [“Quick Setup Options” on page 73](#)
- [“Use Quick Setup to Create an Initial Chassis Storage Configuration Using the Web Interface” on page 76](#)



## Option 2: Assign per Adjacent Individual Disks

This option equally divides the number of storage devices among the server blades. All servers are assigned as close to the same number of disks as possible.

Instead of assigning the storage in a round-robin fashion among all available storage blades, the storage is assigned from storage blades that are adjacent to the server blades. If there are no storage blades adjacent to the server blade, then the nearest possible storage blade is used.

This is a good option to use if you have more server blades than storage blades, and want to have an equal number of storage devices assigned to each storage blade.

**Quick Setup**

Select how you would like all chassis storage resources allocated and click 'Save'.

1. Assign per individual disks.  
  2. Assign per adjacent individual disks.

3. Assign per storage blade.  
  4. Assign per adjacent storage blade.

---

**SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-0000000-0000000000**

Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9
Server Blade	Server Blade	Storage Blade	Server Blade	Server Blade	Storage Blade	Server Blade	Storage Blade	Server Blade	Storage Blade
SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	Vvgr+	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2
		HDD 6   HDD 7 HDD 4   HDD 5 HDD 2   HDD 3 HDD 0   HDD 1			HDD 6   HDD 7 HDD 4   HDD 5 HDD 2   HDD 3 HDD 0   HDD 1		HDD 6   HDD 7 HDD 4   HDD 5 HDD 2   HDD 3 HDD 0   HDD 1		HDD 6   HDD 7 HDD 4   HDD 5 HDD 2   HDD 3 HDD 0   HDD 1
		empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty			empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty		empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty		empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty

**NEM Slot 0**

SAS NEM NEM-2

EXT 0	EXT 1	EXT 2	EXT 3
-------	-------	-------	-------

**NEM Slot 1**

SAS NEM NEM-2

EXT 0	EXT 1	EXT 2	EXT 3
-------	-------	-------	-------

**NAC name:** -

**Disk type:** -

**WWN:** -







**4. Choose one of the Quick Setup options.**

See [“Quick Setup Options” on page 73](#) for explanation of each option.

After you make the selection, the screen shows the color-coded zoning assignments between the CPU blades and storage devices (HDDs). Although the Sun Blade Zone Manager assigns the NEM0 and NEM1 External SAS connections, these connections are not officially supported.

---

**Note** – Until you click the Save button, the configuration is not saved.

---

**5. Click the Save button to save the configuration.**

See [“Saving the Chassis Storage Access Configuration” on page 97](#) for more information on what happens when you save the configuration.

**6. Back up the configuration.**

See [“Backing Up the Storage Access Configuration” on page 100](#).

## Creating the Chassis Storage Access Configuration Using Detailed Setup

You can use the New Assignments option in Detailed Setup to manually create the chassis storage access configuration.

---

**Note** – NEM0 and NEM1 targets appear in the Zone Manager when these NEMs are installed; however, external SAS connections in the Sun Blade Zone Manager are not supported at this time.

---

### ▼ Use Detailed Setup to Create the Chassis Storage Configuration Using the Web Interface

**Before You Begin:** Ensure that your chassis configuration meets the requirements in [“Supported Hardware and Firmware Configurations” on page 65](#).

**1. Access the Sun Blade Zone Manager.**

See [“Accessing the Sun Blade Zone Manager” on page 66](#).

**2. In the Sun Blade Zone Manager section, click the Detailed Setup button.**

The following message appears if you do not have a chassis storage configuration set up.





There are no zoning assignments currently configured in the chassis. Would you prefer to use Quick Setup to more easily configure the whole chassis?

OK

Cancel

### 3. Do one of the following:

- If you want to continue with the Detailed Setup setup, click Cancel.

Clicking Cancel will open the Detailed Setup page.

- If you want to set up the original configuration in Quick Setup, click OK.

Clicking OK will open the Quick Setup page. See [“Creating the Chassis Storage Access Configuration Using Quick Setup”](#) on page 72 for more information on Quick Setup.

**Zoning Config**

The current access permission assignments are displayed below. Click 'New Assignments' to make new access groupings. Or, click on any component to select all those to which it has access assigned, then click 'Modify Group' to make changes to that selected group.

SUN BLADE 6000 MODULAR SYSTEM - bnr\_02\_core\_0item

Slot 0 Server Blade	Slot 1 Storage Blade SUN BLADE STORAGE MODULE M2	Slot 2 Server Blade	Slot 3 Storage Blade SUN BLADE STORAGE MODULE M2	Slot 4 Server Blade	Slot 5 Storage Blade SUN BLADE STORAGE MODULE M2	Slot 6 Server Blade	Slot 7 Storage Blade SUN BLADE STORAGE MODULE M2	Slot 8 Server Blade	Slot 9 Storage Blade SUN BLADE STORAGE MODULE M2
	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
	empty empty		empty empty		empty empty		empty empty		empty empty

NEM Slot 0				NEM Slot 1				NAC name:	
SAS NEM NEM-2				SAS NEM NEM-2				-	
EXT 0	EXT 1	EXT 2	EXT 3	EXT 0	EXT 1	EXT 2	EXT 3	Disk type:	
								-	
								WWN:	
								-	

### 4. Click the New Assignments button.





## ▼ Create a Chassis Storage Configuration Using the CLI

**Before You Begin:** Ensure that your chassis configuration meets the requirements in “Supported Hardware and Firmware Configurations” on page 65.

### 1. Access the Sun Blade Zone Manager.

See “Accessing the Sun Blade Zone Manager” on page 66.

### 2. Use one of the following methods to create a chassis storage configuration:

- **Method 1:** To assign a storage module device to a server blade, use the following commands:

```
-> cd /STORAGE/sas_zoning/BLn
-> set add_storage_access=path_to_storage_device
```

Where *BLn* is a server blade and *path\_to\_storage\_device* is the path to the storage device that you want to assign to the blade. For example, /CH/BL1/HDD0.

- **Method 2:** To assign a server blade to a storage device:

Use the following command:

```
-> cd /STORAGE/sas_zoning/BLn/HDDn
```

Followed by:

```
-> set add_host_access=path_to_blade_server
```

Where *BLn* is a storage blade, *HDDn* is a storage device installed on the storage blade, and *path\_to\_blade\_server* is the path to the server that you want to assign to the storage device. For example, /CH/BL0.

The following examples show how to use these commands to set up zoning between storage devices on a storage blade in Slot 1 and a server blade in Slot 0.

- **Method 1** - Command examples for assigning storage module devices to a server blade:

Command	Description
-> cd /STORAGE/sas_zoning/BL0	Use the cd command to access the host server blade that will be assigned storage.

Command	Description
-> <b>set add_storage_access=/CH/BL1/HDD0</b>	Assign HDD0 of the storage module in blade Slot 1 to the current host.
-> <b>set add_storage_access=/CH/BL1/HDD0, /CH/BL1/HDD1</b>	Assign multiple devices in a single command line. Use the full path to the device and separate each device with a comma (no space).
-> <b>show</b> /STORAGE/sas_zoning/BL0 Targets: 0 (/CH/BL1/HDD0) 1 (/CH/BL1/HDD1)	Use the show command to confirm assigned devices to the current host.

- **Method 2** - Command examples for assigning a server blade (BL0) to storage module devices (BL1/HDD0).

Command	Description
-> <b>cd /STORAGE/sas_zoning/BL1/HDD0</b>	Use the cd command to access the storage module device (in this case BL1/HDD0).
-> <b>set add_host_access=/CH/BL0</b>	Assign the current device (HDD0) of the storage module to the host in blade Slot 0.
-> <b>show</b> /STORAGE/sas_zoning/BL1/HDD0 Targets: 0 (/CH/BL0)	Use the show command to confirm assignment of the current device.

### 3. Back up the configuration.

See [“Backing Up the Storage Access Configuration”](#) on page 100.

## Viewing or Modifying the Chassis Storage Access Configuration

You can use the Detailed Setup through the web interface or the CLI to view or modify the current chassis storage access configuration.

Use one of the procedures in the following table to view or modify the current storage configuration.

Task	Link
View and modify the current storage configuration using the web interface.	<a href="#">“View and Modify the Chassis Storage Configuration Using the Web Interface” on page 84</a>
View and modify the current storage configuration using the CLI.	<a href="#">“View and Modify the Chassis Storage Configuration Using the CLI” on page 90</a>
Assign multiple server blades to a storage device.	<a href="#">“Assign Multiple Server Blades to a Storage Device Using the Web Interface” on page 92</a>
View the storage configuration in table format.	<a href="#">“View the Storage Access Configuration Table Using the Web Interface” on page 95</a>

## ▼ View and Modify the Chassis Storage Configuration Using the Web Interface

**Before You Begin:** Ensure that your chassis configuration meets the requirements in [“Supported Hardware and Firmware Configurations” on page 65](#).

**1. Access the Sun Blade Zone Manager.**

See [“Accessing the Sun Blade Zone Manager” on page 66](#).

**2. In the Sun Blade Zone Manager section, click the Detailed Setup button.**

The current chassis zoning configuration is displayed, as shown in the following example.

**Zoning Config**

The current access permission assignments are displayed below. Click 'New Assignments' to make new access groupings. Or, click on any component to select all those to which it has access assigned, then click 'Modify Group' to make changes to that selected group.

[New Assignments](#) [Modify Group](#)

SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-0000000-000000000

Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9
Server Blade	Server Blade	Storage Blade	Server Blade	Server Blade	Storage Blade	Server Blade	Storage Blade	Server Blade	Storage Blade
SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2
		HDD 6   HDD 7 HDD 4   HDD 5 HDD 2   HDD 3 HDD 0   HDD 1			HDD 6   HDD 7 HDD 4   HDD 5 HDD 2   HDD 3 HDD 0   HDD 1		HDD 6   HDD 7 HDD 4   HDD 5 HDD 2   HDD 3 HDD 0   HDD 1		HDD 6   HDD 7 HDD 4   HDD 5 HDD 2   HDD 3 HDD 0   HDD 1
		empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty			empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty		empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty		empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty empty   empty

NEM Slot 0			
SAS NEM NEM-2	EXT 0	EXT 1	EXT 2

NEM Slot 1			
SAS NEM NEM-2	EXT 0	EXT 1	EXT 2

NAC name:	-
Disk type:	-
WWN:	-

**Note** – Any HDD slots that do not have a storage device installed are labeled “empty.” These slots cannot be assigned to a server blade.

- To modify a blade/storage group, select a blade that is part of the group. The storage that is assigned to the group will be highlighted.





**Modify Group**

Indicated below is your selected group of components that currently have assigned access. Click on those within the group that you would like to remove access to. Click on any components outside the group that you want added. When you are ready to apply the changes, click 'Save'.

Save Cancel

SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-000000-00000000

Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9
Server Blade	Server Blade	Storage Blade	Server Blade	Server Blade	Storage Blade	Server Blade	Storage Blade	Server Blade	Storage Blade
SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X8270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2
		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1			HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty			empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty

<b>NEM Slot 0</b>	<b>NEM Slot 1</b>	NAC name: -
SAS NEM NEM-2	SAS NEM NEM-2	Disk type: -
EXT 0 EXT 1 EXT 2 EXT 3	EXT 0 EXT 1 EXT 2 EXT 3	WWN: -

- Click Save to remove the modules from the group.  
See [“Saving the Chassis Storage Access Configuration”](#) on page 97 for more information on what happens when you save the configuration.
- If you do not plan to make additional storage assignments, back up the configuration.  
See [“Backing Up the Storage Access Configuration”](#) on page 100.
- To make a new storage group assignment, click the New Assignments button.





**Zoning Config**

The current access permission assignments are displayed below. Click 'New Assignments' to make new access groupings. Or, click on any component to select all those to which it has access assigned, then click 'Modify Group' to make changes to that selected group.

[New Assignments](#) [Modify Group](#)

**SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-0000000-0000000000**

Slot 0 Server Blade	Slot 1 Server Blade	Slot 2 Storage Blade SUN BLADE STORAGE MODULE M2	Slot 3 Server Blade	Slot 4 Server Blade	Slot 5 Storage Blade SUN BLADE STORAGE MODULE M2	Slot 6 Server Blade	Slot 7 Storage Blade SUN BLADE STORAGE MODULE M2	Slot 8 Server Blade	Slot 9 Storage Blade SUN BLADE STORAGE MODULE M2
SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	SUN BLADE X6270 M2 SERVER MODULE	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	SUN BLADE X6270 M2 SERVER MODULE	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty			empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	

NEM Slot 0 SAS NEM NEM-2 EXT 0 EXT 1 EXT 2 EXT 3				NEM Slot 1 SAS NEM NEM-2 EXT 0 EXT 1 EXT 2 EXT 3				NAC name: -
								Disk type: -
								WWN: -

## 11. Back up the configuration.

See [“Backing Up the Storage Access Configuration”](#) on page 100.

## ▼ View and Modify the Chassis Storage Configuration Using the CLI

**Before You Begin:** Set up the initial chassis zoning configuration using Quick Setup or Detailed Setup. See [“Creating the Chassis Storage Access Configuration”](#) on page 72.

### 1. Access Zone Manager using the CLI.

See [“Accessing the Sun Blade Zone Manager”](#) on page 66.

## 2. To view storage device assignments to a server blade, you can either view the assignments per server blade or per storage module.

In the following examples, HDD0 and HDD1 from a storage blade in Slot 2 are assigned to server blade in Slot 0.

- To view storage assignments per server blade, use the show command with the host blade SAS zoning directory. For example:

```
-> show /STORAGE/sas_zoning/BL0

Targets:
0      (/CH/BL2/HDD0)
1      (/CH/BL2/HDD1)
```

In this example, HDD0 and HDD1 from a storage blade in Slot 2 are assigned to server blade in Slot 0.

- To view storage assignments per storage device, use the show command with the storage blade SAS zoning directory for the storage device. For example:

```
-> show /STORAGE/BL2/HDD0

Targets:
0      (/CH/BL0)

-> show /STORAGE/BL2/HDD1

Targets:
0      (/CH/BL0)
```

## 3. Modify storage assignments.

You can modify storage device assignments to server blades or modify server blade assignments to storage devices. Either method provides the same result.

**Method 1:** Add or remove storage access to the server blade.

- To assign a storage module to a server blade:
  - > **cd** /STORAGE/sas\_zoning/BLn
  - > **set add\_storage\_access=***path\_to\_storage\_device*
- To remove a storage module from a server blade:
  - > **cd** /STORAGE/sas\_zoning/BLn
  - > **set remove\_storage\_access=***path\_to\_storage\_device*

Where BLn is a server blade and *path\_to\_storage\_device* is the path to the storage device that you want to assign to the blade. For example, /CH/BL1/HDD0.

**Method 2:** Add or remove server blade access to storage blades.

- To assign a server blade to a storage device:

Use one of the following commands:

```
-> cd /STORAGE/sas_zoning/BLn/HDDn
```

Followed by:

```
-> set add_host_access=path_to_blade_server
```

- To remove a server blade from a storage device:

Use one of the following commands:

```
-> cd /STORAGE/sas_zoning/BLn/HDDn
```

Followed by:

```
-> set remove_host_access=path_to_blade_server
```

Where BLn is a storage blade, and HDDn is storage device in the storage blade, and *path\_to\_blade\_server* is the path to the server that you want to assign to the storage device. For example, /CH/BL0.

---

**Note** – You can also add or remove multiple devices in a single command line. Use the full path to the device and separate each device with a comma (no space). For example: `-> set add_storage_access=/CH/BL1/HDD0,/CH/BL1/HDD1.`

---

#### 4. Back up the configuration.

See [“Backing Up the Storage Access Configuration”](#) on page 100.

## ▼ Assign Multiple Server Blades to a Storage Device Using the Web Interface

The Sun Blade Zone Manager enables you to assign more than one server blade to a single storage device. This option should only be used with an Oracle-supported clustering solution. See the *Sun Blade Storage Module Administration Guide* for more information.

---

**Note** – Check your server blade documentation for information on whether the server module is enabled for sharing storage with another server.

---

#### 1. Access the Sun Blade Zone Manager.

See [“Accessing the Sun Blade Zone Manager”](#) on page 5-66.

#### 2. In the Sun Blade Zone Manager section, click the Detailed Setup button.

In the following example, HDD6 in storage module Slot 2 is assigned only to the server blade in Slot 0.

**Zoning Config**

The current access permission assignments are displayed below. Click 'New Assignments' to make new access groupings. Or, click on any component to select all those to which it has access assigned, then click 'Modify Group' to make changes to that selected group.

[New Assignments](#) [Modify Group](#)

**SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-000000-000000000**

Slot 0 Server Blade	Slot 1 Server Blade	Slot 2 Storage Blade	Slot 3 Server Blade	Slot 4 Server Blade	Slot 5 Storage Blade	Slot 6 Server Blade	Slot 7 Storage Blade	Slot 8 Server Blade	Slot 9 Storage Blade
SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2
		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1			HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
		empty empty			empty empty		empty empty		empty empty

NEM Slot 0 SAS NEM NEM-2 EXT 0 EXT 1 EXT 2 EXT 3				NEM Slot 1 SAS NEM NEM-2 EXT 0 EXT 1 EXT 2 EXT 3				NAC name: -	
								Disk type: -	
								WWN: -	

3. Click New Assignments.

4. To assign HDD6 to both the server blade in Slot 0 and the server blade in Slot 1, click Slot 1 and click HDD6 in Slot 2.





**Zoning Config**

The current access permission assignments are displayed below. Click 'New Assignments' to make new access groupings. Or, click on any component to select all those to which it has access assigned, then click 'Modify Group' to make changes to that selected group.

[New Assignments](#) [Modify Group](#)

This color indicates that the component is accessible by more than one server blade.  
Click the component to view which blades share access.

**SUN BLADE 6000 MODULAR SYSTEM - SUNCMM-000000-000000000**

Slot 0 Server Blade	Slot 1 Server Blade	Slot 2 Storage Blade	Slot 3 Server Blade	Slot 4 Server Blade	Slot 5 Storage Blade	Slot 6 Server Blade	Slot 7 Storage Blade	Slot 8 Server Blade	Slot 9 Storage Blade
SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2	SUN BLADE X6270 M2 SERVER MODULE	SUN BLADE STORAGE MODULE M2
		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1			HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
		empty empty			empty empty		empty empty		empty empty

NEM Slot 0 SAS NEM NEM-2 EXT 0 EXT 1 EXT 2 EXT 3				NEM Slot 1 SAS NEM NEM-2 EXT 0 EXT 1 EXT 2 EXT 3				NAC name: -	
								Disk type: -	
								WWN: -	

7. Back up the configuration.  
See “Backing Up the Storage Access Configuration” on page 5-100

▼ View the Storage Access Configuration Table Using the Web Interface

1. Access the Sun Blade Zone Manager.  
See “Accessing the Sun Blade Zone Manager” on page 5-66.
2. In the Sun Blade Zone Manager section, click the Detailed Setup button.  
The following is an example storage access configuration.



5. To detach the table from the rest of the screen, click **Detach Table**.

[Close]

Current Assignments for /CH/BLO		
Component	Type	WWN
/CH/BLO	Server Blade (Virgo+)	-
/CH/NEM0/EXT0	SAS Port	-
/CH/NEM1/EXT0	SAS Port	-
/CH/BL2/HDD6	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD4	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD5	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/HDD7	SAS HDD	80205010:12124556 80205010:12124557
/CH/BL2/FMOD23	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD21	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD19	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD18	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD20	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD22	SAS FMOD	80205010:33333336 80205010:33333337

---

## Saving the Chassis Storage Access Configuration

This section lists important considerations when saving a new or modified storage access zoning configuration and describes the actions that occur when a storage access zoning configuration is saved.

This section covers the following sections:

- [“Important Considerations About Saving the Zoning Configuration” on page 98](#)
- [“Saving a New or Modified Storage Access Configuration” on page 98](#)

## Important Considerations About Saving the Zoning Configuration

When you save a storage access configuration, keep the following in mind:

- The configuration information is saved with the SAS-2 NEMs and storage blades. Changes in zoning hardware configurations can result in loss of the zoning configuration. Back up the configuration immediately after saving it. See [“Backing Up the Storage Access Configuration” on page 100](#).

Refer to the storage blade or NEM documentation for further information on the effect of hot-plugging these components.

- The Zone Manager windows must remain open during the entire Save operation. If the Zone Manager window is closed while the Save operation is in progress, only the portion of the configuration that was processed before the window was closed will be preserved.
- Do not remove or power cycle any of the components included in a zoning assignment while a Save operation is in progress. The zoning configuration will not save properly.

## Saving a New or Modified Storage Access Configuration

You can save a new or modified storage access configuration using either the ILOM web interface or the CLI.

- **From the web interface:** Press the Save button after making the storage access assignments in the Quick Setup or Detailed Setup screens.
- **From the CLI:** As soon as you execute the `set` command for the storage assignment, the configuration is saved.

While the new configuration is being saved, the following takes place:

- In Quick Setup, the existing configuration is overridden.
- All storage controls are disabled while the configuration is being saved.
- For the web interface, check marks indicate where the new configuration is applied.



# Backing Up the Storage Access Configuration

After saving the zoning configuration, you should back up the configuration in case you lose it and need to recover it.

This section covers the following procedures:

- [“Save the Zoning Configuration to a Backup File Using the Web Interface” on page 100](#)
- [“Save the Zoning Configuration to a Backup File Using the CLI” on page 101](#)

## ▼ Save the Zoning Configuration to a Backup File Using the Web Interface

1. After saving a configuration in the Quick Setup or Detailed Setup screen, Click the Maintenance tab for the CMM.

The CMM maintenance sub-tabs are displayed.

2. Click the Backup/Restore tab.

The Configuration Backup/Restore page is displayed.



The screenshot shows the Oracle ILOM CMM Administration Guide interface. The left sidebar displays a tree view with 'Chassis' expanded to show 'CMM', 'Blade 0', 'Blade 1', 'Blade 9', 'REM 0', and 'REM 1'. The main content area has a top navigation bar with tabs: System Information, System Monitoring, Power Management, Storage, Configuration, User Management, Remote Control, and Maintenance. Below this is a sub-navigation bar with tabs: Firmware Upgrade, Backup/Restore, Configuration Management, Reset Components, and Snapshot. The 'Backup/Restore' tab is active, displaying the 'Configuration Backup/Restore' page. The page contains a form with the following fields: 'Operation' (a drop-down menu set to 'Backup'), 'Transfer Method' (a drop-down menu set to 'Browser'), and a note: 'The downloaded file will be saved according to your browser settings.' Below these are two text input fields for 'Passphrase' and 'Confirm Passphrase', and a 'Run' button at the bottom.

3. Select Backup from the Operation drop-down list.

#### 4. Fill out the information on the page to create your backup file.

For complete instructions on using ILOM Backup/Restore, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

## ▼ Save the Zoning Configuration to a Backup File Using the CLI

### 1. After setting the storage access configuration, change to the `/SP/config` directory.

```
-> cd /SP/config
```

### 2. If you want sensitive data, such as user passwords, SSH keys, certificates, and so forth, to be backed up, you must provide a passphrase.

```
-> set passphrase=passphrase
```

### 3. To initiate the Backup operation, enter the command:

```
-> set dump_uri=
```

```
transfer_method://username:password@ipaddress_or_hostname/directorypath/filename.config
```

Where:

- *transfer\_method* can be tftp, ftp, sftp, scp, http, or https.
- *username* is the name of the user account on the remote system. (*username* is required for scp, sftp, and ftp. *username* is not used for tftp, and it is optional for http and https.)
- *password* is the password for the user account on the remote system. (*password* is required for scp, sftp, and ftp. *password* is not used for tftp, and it is optional for http and https.)
- *ipaddress\_or\_hostname* is the IP address or the host name of the remote system.
- *directorypath* is the storage location on the remote system.
- *filename* is the name assigned to the backup file.

For complete instructions on using ILOM Backup/Restore, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

---

# Recovering Zoning Configurations

This section describes how to recover host-to-storage zoning configurations that might have been lost by accident or due to hardware replacement.

This section covers the following procedures:

- [“Recover Zoning Configurations Using the Web Interface”](#) on page 102
- [“Recover Zoning Configurations Using the CLI”](#) on page 104

## ▼ Recover Zoning Configurations Using the Web Interface

You must have previously created a backup CMM ILOM configuration file that contains the zoning configurations you want to restore.

---

**Note** – For advanced users or Oracle technicians: The CMM ILOM configuration backup file is an XML file. If you have multiple CMM ILOM configuration backup files and the latest version does not have the zoning configurations you need, you have the option of copying the storage assignments section of one file and pasting it into another. For this to work, your storage modules and server blades must be in the same physical slots for the zoning configurations you want to restore. For more information on performing this procedure, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

---

1. **Open a web browser and log in to the CMM by entering the following URL:**

**http://chassis\_sp\_ipaddress/**

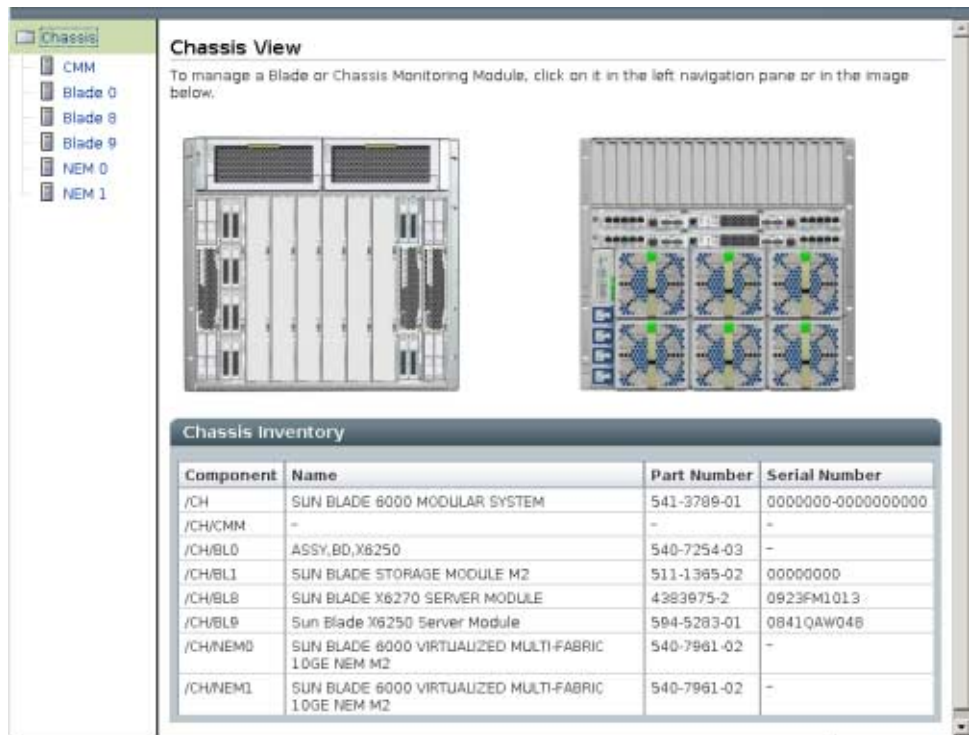
Where *chassis\_sp\_ipaddress* is the IP address of your chassis service processor.

The ILOM login page appears.

2. **Log in as root.**

The CMM ILOM main page is displayed.





3. With CMM selected in the Chassis navigation pane, click the Maintenance tab for the CMM.

The CMM maintenance sub-tabs are displayed.

4. Click the Backup/Restore tab.

The Configuration Backup/Restore page is displayed.



## 5. Select Restore from the Operation drop-down list.

Fill out the information on the page to restore your backup file.

For complete instructions on using ILOM Backup/Restore, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide*.

## 6. To initiate the Restore operation, click Run.

The Restore operation executes.

---

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

---

# ▼ Recover Zoning Configurations Using the CLI

You must have previously created a backup CMM ILOM configuration file that contains the zoning configurations you want to restore.

---

**Note** – For advanced users or Oracle technicians: The CMM ILOM configuration backup file is an XML file. If you have multiple CMM ILOM configuration backup files and the latest version does not have the zoning configurations you need, you have the option of copying the storage assignments section of one file and pasting it into another. For this to work, your storage modules and server blades must be in the same physical slots for the zoning configurations you want to restore. For more information on performing this procedure, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide*.

---

## 1. Open a terminal window and establish an SSH connection to the CMM by entering the following command:

```
# ssh -l root cmm_ipaddress
```

Where *cmm\_ipaddress* is the IP address of the CMM.

The login prompt is displayed.

## 2. Log in as root and enter the root password:

```
/hostname/login: root
```

```
password:xxxxxxx
```

After you have successfully logged in, the CLI prompt is displayed:

```
->
```

### 3. Change to the `/SP/config` directory:

```
-> cd /SP/config
```

### 4. To initiate the Restore operation, enter the command:

```
-> set load_uri=
```

```
transfer_method://username:password@ipaddress_or_hostname/directorypath/filename.config
```

Where:

- *transfer\_method* can be tftp, ftp, sftp, scp, http, or https.
- *username* is the name of the user account on the remote system. (*username* is required for scp, sftp, and ftp. *username* is not used for tftp, and it is optional for http and https.)
- *password* is the password for the user account on the remote system. (*password* is required for scp, sftp, and ftp. *password* is not used for tftp, and it is optional for http and https.)
- *ipaddress\_or\_hostname* is the IP address or the host name of the remote system.
- *directorypath* is the storage location on the remote system.
- *filename* is the name assigned to the backup file.

The Restore operation executes.

---

## Resetting the Zoning Configuration

This section describes how to reset the current zoning configuration.

The following procedures are included in this configuration:

- [“Reset the Zoning Configuration Using the Web Interface” on page 106](#)
- [“Reset the Zoning Configuration Using the CLI” on page 107](#)

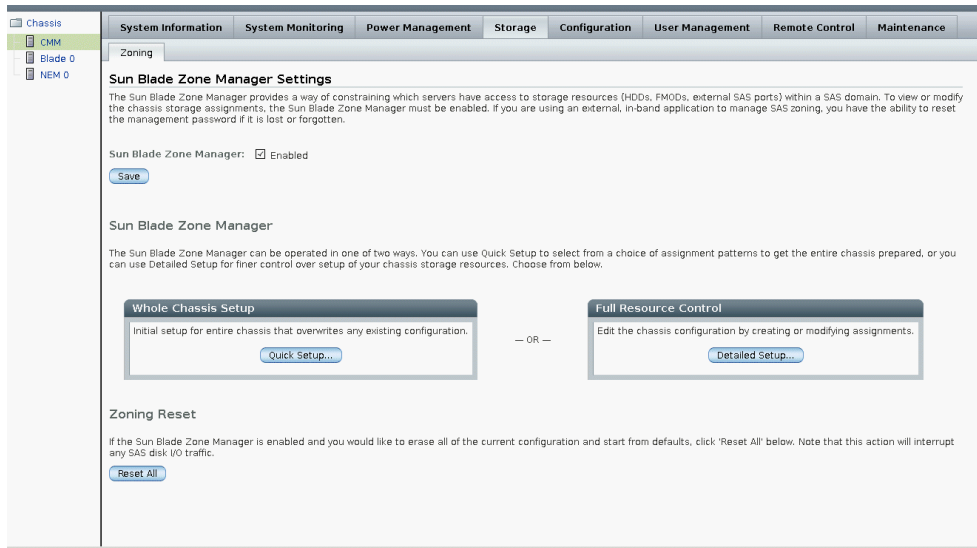
### ▼ Reset the Zoning Configuration Using the Web Interface

#### 1. Access the Sun Blade Zone Manager.

See [“Accessing the Sun Blade Zone Manager” on page 66](#).

#### 2. Navigate to Storage --> Zoning.

If Zoning is enabled, a Reset All button is available on the Zone Manager Settings page.



3. Click the Reset All button to reset the current zoning assignments.

## ▼ Reset the Zoning Configuration Using the CLI

1. Access the Sun Blade Zone Manager using the CMM CLI.  
See [“Accessing the Sun Blade Zone Manager”](#) on page 66.
2. Navigate to `/STORAGE/sas_zoning` using the following command:  
-> `cd /STORAGE/sas_zoning`
3. Reset the current zoning assignments using the following command:  
-> `set reset_access_action=true`

If the Zone Manager is disabled, you will get the following warning:

```
set: The CMM is not the SAS Zone Manager
```

If you receive this message, enable Zone Manager and re-issue the reset command.

---

## Resetting the Zoning Password

The zoning password is only required by in-band zoning management applications running on a Host OS.

If you use such applications and this password is lost or forgotten, restore the password to the default value (all-zeroes).

---

**Note** – The Sun Blade Zone Manager must be disabled to reset this password.

---

The following procedures are included in this configuration:

- “Reset the Zoning Password Using the Web Interface” on page 107
- “Reset the Zoning Password Using the CLI” on page 108

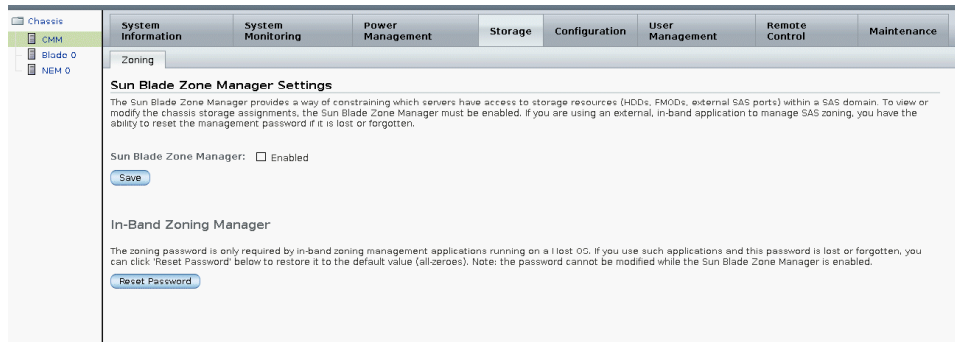
## ▼ Reset the Zoning Password Using the Web Interface

### 1. Access the Sun Blade Zone Manager.

See “Accessing the Sun Blade Zone Manager” on page 66.

### 2. Navigate to Storage --> Zoning.

If Zoning is disabled, a Reset Password button is available on the Zoning page.



### 3. Click the Reset Password button to reset the password to the default (all zeros).

## ▼ Reset the Zoning Password Using the CLI

### 1. Access the Sun Blade Zone Manager using the CMM CLI.

See “Accessing the Sun Blade Zone Manager” on page 66.

### 2. Navigate to `/STORAGE/sas_zoning` using the following command:

```
-> cd /STORAGE/sas_zoning
```

3. Reset the current zoning assignments using the following command:

-> **set reset\_password\_action=true**

The password is set to the default (all zeros).

# Index

---

## B

blade SP CLI prompt  
changing, 21

## C

### CLI

- accessing and enabling Sun Blade Zone Manager, 70
- backing up a storage zoning configuration, 101
- changing the blade SP prompt, 21
- enabling Ethernet ports, 19
- Ethernet management port CLI
  - using to determine firmware version, 26
- logging in, 17
- recovering a storage zoning configuration, 104
- resetting a storage zoning configuration, 107
- resetting CMM, 41
- resetting the zoning password, 108
- serial management port CLI
  - using to determine firmware version, 26
- Sun Blade Zone Manager, 61
- updating component firmware, 39
- using to create Sun Blade Zone Manager chassis storage configuration, 82
- using to update CMM ILOM firmware, 30
- using to view and modify storage configuration, 90

CMM Ethernet ports, enabling, 18

connecting to CMM ILOM

- configuring static IP address, 8, 10
- DHCP, 10
- serial connection, 7

## D

Detailed Setup for Sun Blade Zone Manager, 78

DHCP

- accessing CMM IP address, 10

## E

Ethernet ports

- enabling through CLI, 19
- enabling through web interface, 18

## F

firmware

- determining current CMM version
  - using Ethernet management port CLI, 26
  - using serial management port CLI, 26
  - using web interface, 24
- downloading, 27
- Sun Blade Zone Manager requirements, 65
- updating CMM ILOM, 23
  - using CLI, 30
  - using web interface, 28
- updating component firmware, 36
  - using the CLI, 39
  - using the web interface, 37

## I

ILOM CLI interface

- logging in, 17

initial login to CMM ILOM, 16

IP address assignment

- editing using the CLI, ?? to 10

- L**  
 logging in to CMM ILOM  
   using CLI, 17  
   using web interface, 17
- M**  
 multiple blades assigned to storage device, 92
- O**  
 overview of CMM ILOM, 2  
 overview of Sun Blade Zone Manager, 58
- Q**  
 Quick Setup for Sun Blade Zone Manager, 72, 76
- R**  
 resetting CMM  
   using CLI, 41  
   using web interface, 40
- S**  
 saving a storage access configuration, 97  
 static IP address  
   configuring, 8, 10  
 storage access configuration table in Sun Blade Zone Manager, 95  
 Sun Blade Zone Manager  
   accessing using CLI, 70  
   accessing using web interface, 66  
   assigning multiple server blades to a storage device, 92  
   backing up a zoning configuration  
     using CLI, 101  
     using web interface, 100  
   CLI, 61  
   creating the chassis storage access configuration  
     using CLI, 82  
     using detailed setup, 78  
     using quick setup, 72, 76  
   enabling using CLI, 70  
   enabling using web interface, 66  
   overview, 58  
   recovering a zoning configuration  
     using CLI, 104  
     using web interface, 102  
   resetting a zoning configuration  
     using CLI, 107  
     using web interface, 106  
   resetting the zoning password  
     using CLI, 108  
     using web interface, 107  
   saving a storage access configuration, 97  
   storage access configuration table, 95  
   supported hardware and firmware configurations, 65  
   supported ILOM interfaces, 58  
   view and modify storage configuration  
     using the CLI, 90  
     using the web interface, 84
- V**  
 version of CMM ILOM, 2
- W**  
 web interface  
   accessing and enabling Sun Blade Zone Manager, 66  
   backing up a storage zoning configuration, 100  
   enabling Ethernet ports, 18  
   logging in, 17  
   recovering a storage zoning configuration, 102, 106  
   resetting CMM, 40  
   resetting the zoning password, 107  
   updating component firmware, 37  
   using to determine firmware version, 24  
   using to update CMM ILOM firmware, 28  
   using to view and modify storage configuration, 84