



# SGI® Origin® 400 System User's Guide

007-5661-001

---

## COPYRIGHT

© 2010 SGI. All rights reserved; provided portions may be copyright in third parties, as indicated elsewhere herein. No permission is granted to copy, distribute, or create derivative works from the contents of this electronic documentation in any manner, in whole or in part, without the prior written permission of SGI.

---

## LIMITED RIGHTS LEGEND

The software described in this document is “commercial computer software” provided with restricted rights (except as to included open/free source) as specified in the FAR 52.227-19 and/or the DFAR 227.7202, or successive sections. Use beyond license provisions is a violation of worldwide intellectual property laws, treaties and conventions. This document is provided with limited rights as defined in 52.227-14.

The electronic (software) version of this document was developed at private expense; if acquired under an agreement with the USA government or any contractor thereto, it is acquired as “commercial computer software” subject to the provisions of its applicable license agreement, as specified in (a) 48 CFR 12.212 of the FAR; or, if acquired for Department of Defense units, (b) 48 CFR 227-7202 of the DoD FAR Supplement; or sections succeeding thereto. Contractor/manufacturer is SGI, 46600 Landing Parkway, Fremont, CA 94538.

---

## TRADEMARKS AND ATTRIBUTIONS

Origin, SGI, the SGI logo, and Supportfolio are trademarks or registered trademarks of Silicon Graphics International Corp. or its subsidiaries in the United States and other countries.

Adobe is a trademark or registered trademark of Adobe Systems Incorporated in the United States and/or other countries. Firefox, the Firefox logo, and Mozilla are trademarks or registered trademarks of the Mozilla Foundation. Internet Explorer, Microsoft, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Java and Sun are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries. Linux is a registered trademark of Linus Torvalds, used with permission by SGI.

All other trademarks mentioned herein are the property of their respective owners.

# Preface

---

## About this Manual

Thank you for purchasing and using the SGI Origin 400 system.

This manual is written for system technicians who are responsible for troubleshooting, upgrading, and repairing Origin 400 systems. This document provides reference information, feature information, and step-by-step instructions for adding and replacing components in the Origin 400 system.

## Manual Organization

Chapter 1 provides a brief overview of the Origin 400 system. This includes a list of the Origin 400 system features, illustrations of the product, and product diagrams to help you identify components and their locations.

Chapter 2 provides instructions for adding and replacing components. It provides step-by-step instructions and diagrams for installing or replacing components such as the fans, power supplies, hard drives, and compute modules.

Chapter 3 provides information on using the Origin 400 system. This includes information for powering on and powering off the server and installing an operating system.

Chapter 4 provides information on how to use the Origin 400 Management Center user interface to configure the Origin 400 system. This includes step-by-step instructions and screenshots for configuring the system components, updating the Origin 400 system firmware, and monitoring system health.

Chapter 5 provides information to assist you in troubleshooting the Origin 400 system. This includes information on hardware diagnostics as well as a list of possible solutions for problems like no video display, no available storage, network problems, and several other possible issues.

The back of this manual provides technical specifications, regulatory information, "getting help" information, and the warranty.





# Safety Information

---

## Important Safety Instructions

Read all caution and safety statements in this document before performing any of the instructions.

## Warnings

These warnings and cautions apply whenever you remove the compute module enclosure cover to access components inside the system. Only a technically qualified person should maintain or configure the system.

**Heed safety instructions:** Before working with your server product, whether you are using this guide or any other resource as a reference, pay close attention to the safety instructions. You must adhere to the assembly instructions in this guide to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this guide. Use of other products / components will void the UL listing and other regulatory approvals of the product and will most likely result in noncompliance with product regulations in the regions in which the product is sold.

**System power on/off:** The power button DOES NOT turn off the system AC power. To remove power from the system, you must unplug the AC power cord from the wall outlet or the chassis. Make sure the AC power cord is unplugged before you open the chassis, add, or remove any components.

**Hazardous conditions, devices and cables:** Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the system and disconnect the power cord, telecommunications systems, networks, and modems attached to the system before opening it. Otherwise, personal injury or equipment damage can result.

**Electrostatic discharge (ESD) and ESD protection:** ESD can damage disk drives, boards, and other parts. We recommend that you perform all procedures in this document only at an ESD workstation. If one is not available, provide some ESD protection by wearing an anti-static wrist strap attached to chassis ground (any unpainted metal surface) on your system when handling parts.

**ESD and handling electronic devices:** Always handle electronic devices carefully. They can be extremely sensitive to ESD. Do not touch the connector contacts.

**Installing or removing jumpers:** A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that you can grip with your fingertips or with a pair of fine needle-nosed pliers. If your jumpers do not have such a tab, take care when using needle-nosed pliers to remove or install a jumper; grip the

narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can damage the contacts inside the jumper, causing intermittent problems with the function controlled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool you use to remove a jumper, or you may bend or break the pins on the board.

**Reinstalling enclosure cover:** To protect internal components and for proper cooling and airflow, the compute module should not be inserted into the chassis with the cover removed; operating it without the enclosure cover in place can damage system parts.

# Contents

---

<b>Preface</b> .....	<b>iii</b>
About this Manual .....	iii
Manual Organization .....	iii
<b>Safety Information</b> .....	<b>v</b>
Important Safety Instructions .....	v
Warnings .....	v
<b>Origin 400 System Features</b> .....	<b>1</b>
Origin 400 Feature Overview .....	2
Origin 400 Contents .....	3
Major Components .....	4
Front View .....	4
Rear View .....	8
Front Chassis Connectors and Indicators.....	10
Compute Module Connectors and Indicators .....	11
Back Chassis Connectors and Indicators .....	12
Rack Mount Options .....	13
<b>Hardware Installations and Upgrades</b> .....	<b>15</b>
Before You Begin .....	15
Tools and Supplies Needed .....	15
Chassis References .....	15
Installing the Origin 400 System in a Rack .....	15
Installation Guidelines .....	15
Installing Temporary Handles on System .....	16
Mounting System in Rack .....	17
Hot-Swap Module Installation and Removal Guidelines .....	17
Replacing the Management Module .....	18
Removing the Management Module .....	18
Installing the Management Module .....	19
Installing and Removing an Ethernet Switch Module .....	21
Installing an Ethernet Switch Module .....	21
Removing an Ethernet Switch Module .....	22
Installing and Removing a Storage Control Module .....	24
Installing a Storage Control Module .....	24
Removing a Storage Control Module .....	25
Installing and Removing the Backup Battery .....	27
Installing a Backup Battery .....	27
Removing a Backup Battery .....	28
Installing and Removing a Power Supply Module .....	30

Installing a Power Supply Module .....	31
Removing a Power Supply Module .....	32
Replacing a Main Cooling Module .....	33
Removing a Main Cooling Module .....	34
Installing a Main Cooling Module .....	35
Replacing the I/O Cooling Module .....	35
Removing the I/O Cooling Module .....	36
Installing the I/O Cooling Module .....	37
Installing and Removing Hard Drives .....	37
Installing a 2.5-inch Hard Drive into the Storage Bay .....	38
Removing a 2.5-inch Hard Drive from the Storage Bay .....	40
Installing a 3.5-inch Hard Drive into the Storage Bay .....	42
Removing a 3.5-inch Hard Drive from the Storage Bay .....	45
Installing and Removing an SGI Compute Module .....	48
Installing an SGI Compute Module .....	48
Removing an SGI Compute Module .....	49
<b>Using the Origin 400 System .....</b>	<b>51</b>
Minimum Hardware Requirements .....	51
Starting Up the Origin 400 System .....	51
Installing an Operating System .....	51
Monitoring the System .....	52
Shutting Down the System .....	52
<b>Using the Origin 400 Management Center .....</b>	<b>53</b>
Introduction .....	53
System Configuration Requirements .....	54
Setting Up a Remote Connection .....	55
Remote Client System Requirements .....	56
Log in to the Origin 400 Management Center .....	56
Layout and Key Navigation Features .....	58
Chassis Front .....	62
System .....	63
Compute Module View .....	63
Storage Configuration .....	68
SGI Gigabit Ethernet Switch Module 1 and 2 .....	88
Chassis Back .....	94
Storage Control Module 1 and 2 .....	95
SGI Management Module .....	99
Origin 400 Fans and Power Supplies .....	102
Reports .....	103
Storage Layout .....	104
Events .....	106
Dashboard .....	108
Diagnostics .....	109
Settings .....	113

Storage Drive Caching Options .....	113
IP Configuration .....	115
Date and Time .....	117
Simple Network Management Protocol (SNMP) .....	119
User Accounts .....	123
Event Policies .....	123
Notification .....	125
Language Option Setting .....	126
Feature Activation .....	127
Firmware Updates .....	128
Restore System Settings .....	130
Access Online Help .....	132
Log Out from the Origin 400 Management Center .....	132
<b>Troubleshooting .....</b>	<b>133</b>
First Steps Checklist .....	133
Specific Issues and Corrective Actions .....	133
Chassis Fan Module Not Functioning .....	133
Cannot Connect to the Management Module .....	134
Cannot Connect to a Compute Module .....	134
Cannot Connect a Compute Module to a Storage Control Module .....	135
Diagnostic LED Information .....	135
<b>A Product Regulatory Requirements .....</b>	<b>139</b>
Regulatory and Certification Information .....	139
Product Regulatory Compliance .....	139
Regulated Specified Components .....	142
Electromagnetic Compatibility Notice FCC Verification Statement.....	143
<b>B Installation/Assembly Safety Instructions .....</b>	<b>145</b>
.....	145
<b>C Safety Information .....</b>	<b>147</b>
Server Safety Information .....	147
Safety Warnings and Cautions .....	147
Intended Application Uses .....	148
Site Selection .....	148
Equipment Handling Practices .....	148
Power and Electrical Warnings .....	149
Access Warnings .....	149
Electrostatic Discharge (ESD) .....	150
Other Hazards .....	150



# List of Figures

---

Figure 1. 2.5-in Drive Enclosure.....	1
Figure 2. 3.5-in Drive Enclosure.....	2
Figure 3. Front View of 2.5-in Drive Enclosure.....	5
Figure 4. Front View of 3.5-in Drive Enclosure.....	6
Figure 5. Rear View of the System.....	8
Figure 6. 2.5-in Drive Enclosure Front Chassis Connectors and Indicators.....	10
Figure 7. 3.5-in Drive Enclosure Front Chassis Connectors and Indicators.....	11
Figure 8. Rear Chassis Connectors and Indicators.....	12
Figure 9. Installing Temporary Handles .....	16
Figure 10. Removing the Management Module .....	19
Figure 11. Installing the Management Module .....	20
Figure 12. Installing an Ethernet Switch Module .....	22
Figure 13. Removing an Ethernet Switch Module .....	23
Figure 14. Installing a Storage Control Module .....	25
Figure 15. Removing a Storage Control Module .....	26
Figure 16. Removing Top Cover from Storage Control Module .....	27
Figure 17. Installing Backup Battery.....	28
Figure 18. Removing Top Cover from Storage Control Module .....	29
Figure 19. Removing Backup Battery.....	30
Figure 20. Removing Filler Module .....	31
Figure 21. Installing Power Supply Module .....	32
Figure 22. Removing a Power Supply Module .....	33
Figure 23. Removing a Main Cooling Module .....	34
Figure 24. Installing a Main Cooling Module .....	35
Figure 25. Removing an I/O Cooling Module .....	36
Figure 26. Installing an I/O Cooling Module .....	37
Figure 27. Removing a 2.5-inch Drive Carrier from a Drive Bay Module .....	38
Figure 28. Installing Hard Drive into Drive Carrier.....	39
Figure 29. Installing 2.5-inch Drive Carrier in Drive Bay Module.....	40
Figure 30. Removing a 2.5-inch Drive Carrier from the Drive Bay Module .....	41
Figure 31. Removing Hard Drive from a Drive Carrier .....	42
Figure 32. Removing a 3.5-inch Drive Carrier from the Drive Bay Module .....	43
Figure 33. Installing Hard Drive into Drive Carrier.....	44
Figure 34. Installing 3.5-inch Drive Carrier in Drive Bay Module.....	45
Figure 35. Removing a 3.5-inch Drive Carrier from the Drive Bay Module .....	46
Figure 36. Removing Hard Drive from a Drive Carrier .....	47
Figure 37. Installing an SGI Compute Module .....	48
Figure 38. Removing an SGI Compute Module .....	49
Figure 39. Origin 400 Management Center Login .....	57
Figure 40. Origin 400 Management Center General Layout .....	58
Figure 41. Origin 400 Management Center Configuration Screen Layout .....	59
Figure 42. Chassis Front View .....	62

Figure 43. SGI Compute Module View .....	63
Figure 44. Server Action - Remote KVM & CD .....	67
Figure 45. Initial Storage Configuration Screen .....	69
Figure 46. Create Storage Pool Dialog Box.....	69
Figure 47. Create Storage Pool Dialog Box Example.....	71
Figure 48. Storage Pool Screen.....	72
Figure 49. Create Virtual Drive Dialog Box .....	76
Figure 50. Virtual Drive Screen.....	77
Figure 51. Assign Virtual Drive .....	81
Figure 52. Deleted Virtual Drive.....	82
Figure 53. Physical Drives .....	83
Figure 54. External Ports .....	88
Figure 55. Gigabit Ethernet Switch Module View.....	89
Figure 56. Configure Ports Dialog Box .....	93
Figure 57. Advanced Configuration Screen .....	94
Figure 58. Chassis Back View .....	95
Figure 59. Storage Control Module View .....	96
Figure 60. SGI Management Module View .....	100
Figure 61. Storage Layout Graphical View .....	105
Figure 62. Storage Layout Tabular View .....	106
Figure 63. System Event Log Screen .....	107
Figure 64. Event Policy Record Window.....	108
Figure 65. Dashboard View .....	109
Figure 66. Diagnostics .....	110
Figure 67. Diagnostic Tests .....	111
Figure 68. System Information Report Download .....	111
Figure 69. System Information Report .....	112
Figure 70. Diagnostics - Service Data .....	113
Figure 71. Settings - Storage Caching Options Configuration .....	114
Figure 72. Settings - IP Configuration.....	116
Figure 73. Settings - System Date and Time Configuration.....	117
Figure 74. Calendar .....	118
Figure 75. SNMP Options.....	120
Figure 76. SNMP V3.....	121
Figure 77. Reset SNMP v3.....	122
Figure 78. Settings - User Account Configuration Screen .....	123
Figure 79. Settings - Event Policies Configuration Screen .....	124
Figure 80. Settings - Notification Screen .....	126
Figure 81. Settings - Help Language Selection .....	127
Figure 82. Settings - Feature Activation.....	128
Figure 83. Settings - Firmware Update Screen.....	129
Figure 84. Settings - Restore System Settings .....	130
Figure 85. Online Help.....	132



# List of Tables

---

Table 1. Origin 400 Features.....	3
Table 2. 2.5-in Drive Enclosure Contents.....	3
Table 3. 3.5-in Drive Enclosure Contents.....	4
Table 4. Hardware Requirements .....	51
Table 5. Minimum System Requirements for Remote Web Console .....	56
Table 6. Origin 400 Management Center Configuration Screen Layout .....	60
Table 7. Health Icons .....	64
Table 8. Server Action Menu.....	64
Table 9. Server Tabs.....	66
Table 10. Health Icons .....	72
Table 11. Storage Pool Actions Menu.....	73
Table 12. Storage Pool Tabs.....	75
Table 13. Health Icons .....	78
Table 14. Virtual Drive Action Menu.....	79
Table 15. Virtual Drive Tabs.....	80
Table 16. Health Icons .....	84
Table 17. Physical Drive Action Menu.....	85
Table 18. Physical Drive Tabs.....	86
Table 19. Health Icons .....	90
Table 20. Switch Module Action Menu .....	90
Table 21. Switch Module Tabs .....	91
Table 22. Health Icons .....	97
Table 23. Status Messages.....	97
Table 24. Storage Control Module Action Menu .....	98
Table 25. Storage Control Module Tabs .....	99
Table 26. Health Icons .....	101
Table 27. Management Module Action Menu.....	101
Table 28. Management Module Tabs.....	102
Table 29. Health Icons .....	103
Table 30. Fans and Power Supplies Tabs .....	103
Table 31. Diagnostic LEDs.....	136
Table 32. NIC LEDs .....	137



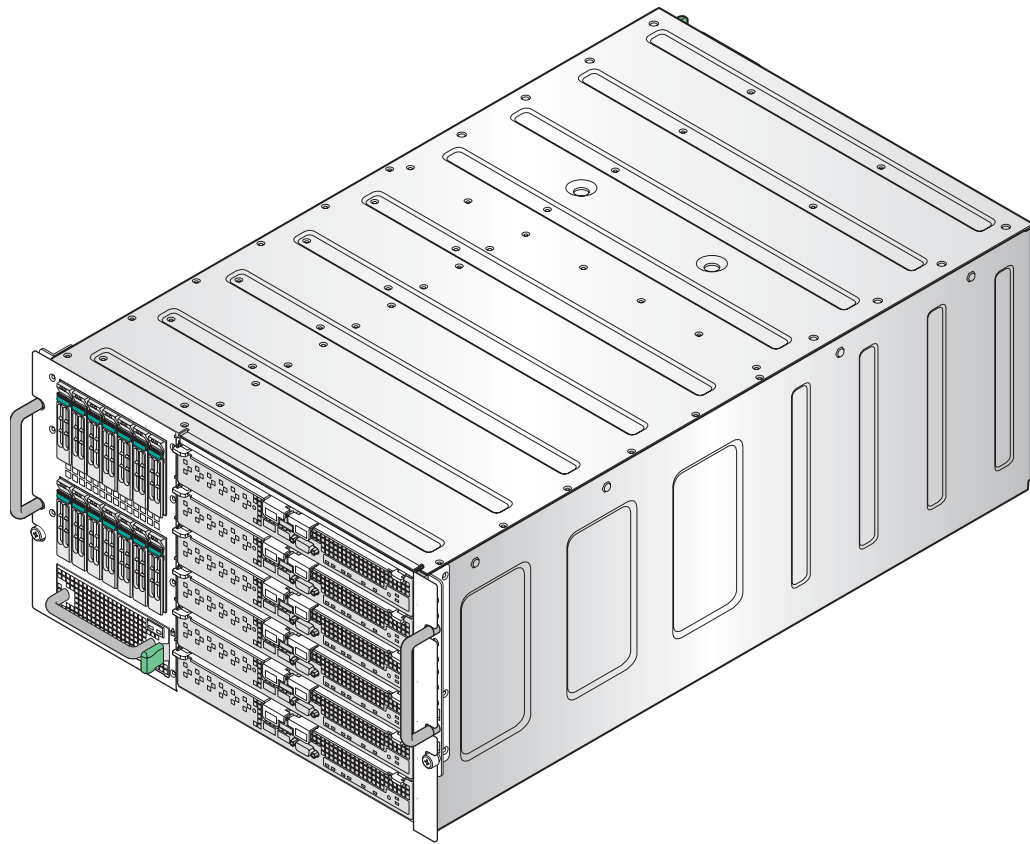
# 1 Origin 400 System Features

---

The following two versions of the Origin 400 are available:

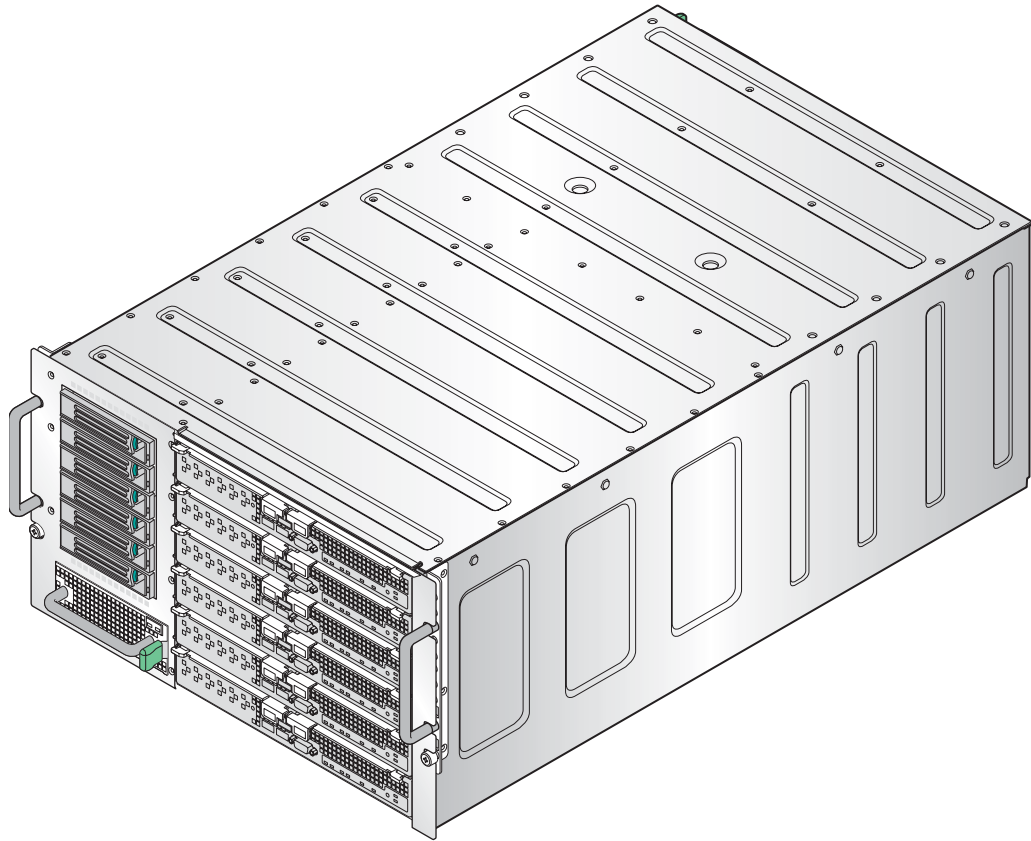
- 2.5-in drive enclosure
- 3.5-in drive enclosure

Unless noted otherwise, all information provided refers to both versions. This chapter briefly describes the main features of the Origin 400 system. This chapter provides photographs and illustrations of the product, a features list, and diagrams showing the location of important components and connections on the server chassis.



AF002423

**Figure 1. 2.5-in Drive Enclosure**



AF002661

**Figure 2. 3.5-in Drive Enclosure**

## **Origin 400 Feature Overview**

Table 1 provides an overview of the Origin 400 system configuration.

**Table 1. Origin 400 Features**

<b>Feature</b>	<b>Description</b>
Chassis Dimensions	<ul style="list-style-type: none"> <li>• 10.3 inches (261.4 mm) high – 6U</li> <li>• 17.5 inches (444.4 mm) wide</li> <li>• 28.4 inches (720.2) mm long</li> <li>• 187 lbs (85 kg) - maximum full configuration weight</li> </ul>
Module Bays (rear)	<ul style="list-style-type: none"> <li>• Four hot-plug 110/220V power module bays</li> <li>• Two hot-swap Ethernet switch module bays</li> <li>• Two hot-swap storage control module bays</li> <li>• Two hot-swap main cooling module bays</li> <li>• One hot-swap management module bay</li> </ul>
Module Bays (front)	<ul style="list-style-type: none"> <li>• Six hot-plug compute module bays</li> <li>• One hot-swap I/O cooling module bay</li> <li>• One hard disk drive bay</li> </ul>
Hard Disk Drive Bay	<ul style="list-style-type: none"> <li>• 2.5-in drive enclosure: 14 hot-swap 2.5-inch SAS hard disk drive carriers with filler blanks installed (hard disk drives are NOT included)</li> <li>• 3.5-in drive enclosure: 6 hot-swap 3.5-inch SAS or SATA hard disk drive carriers with filler blanks installed (hard disk drives are NOT included)</li> </ul>
Origin 400 Management Center	<ul style="list-style-type: none"> <li>• Powerful integrated graphical user interface for configuration and chassis management</li> <li>• Provides a single interface for system updates</li> </ul>

## Origin 400 Contents

### 2.5-in Drive Enclosure Contents

The Origin 400 2.5-in drive enclosure ships with the following items:

**Table 2. 2.5-in Drive Enclosure Contents**

<b>Quantity</b>	<b>Description</b>
One	Chassis enclosure
One	SGI management module
One	SGI gigabit Ethernet switch module
One	SGI storage control module
14	2.5" hard disk drive carriers
Two	1000W power supply modules
Two	Main cooling fan modules
One	I/O cooling fan module
Two	Blank power supply fan blanks

**Table 2. 2.5-in Drive Enclosure Contents**

Quantity	Description
Five	Server blanks (compute module filler panels)
Two	Blank filler panels for rear module bays SCM2 and SWM2

**Note:** *The 2.5-in drive enclosure base configuration does not include hard drives, compute modules or power cords.*

### 3.5-in Drive Enclosure Contents

The 3.5-in drive enclosure ships with the following items:

**Table 3. 3.5-in Drive Enclosure Contents**

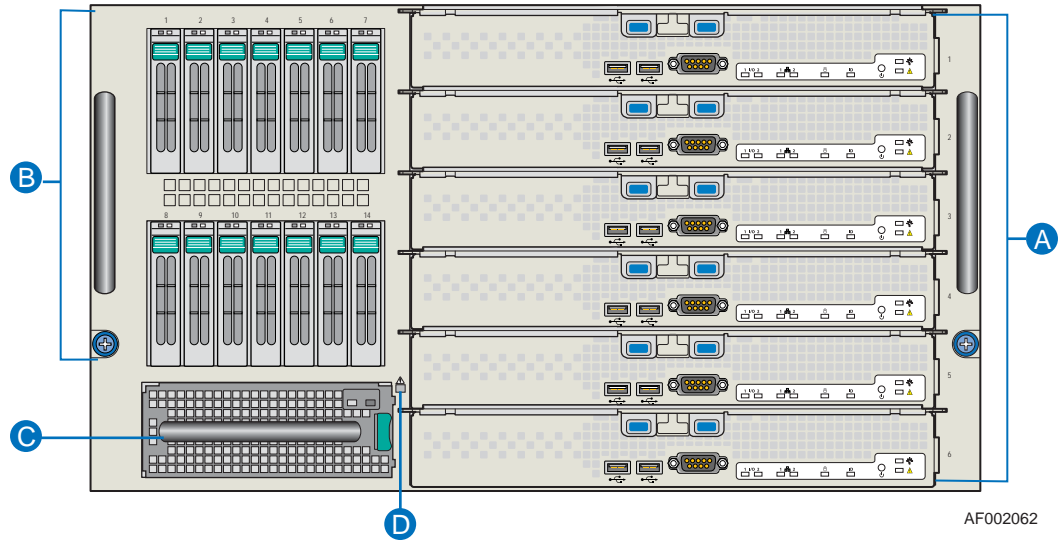
Quantity	Description
One	Chassis enclosure
One	SGL management module
One	SGL gigabit Ethernet switch module
One	SGL storage control module
Six	3.5" hard disk drive carriers
Two	1000W power supply modules
Two	Main cooling fan modules
One	I/O cooling fan module
Two	Blank power supply fan blanks
Five	Server blanks (compute module filler panels)
Two	Blank filler panels for rear module bays SCM2 and SWM2

**Note:** *The 3.5-in drive enclosure base configuration does not include hard drives, compute modules or power cords.*

## Major Components

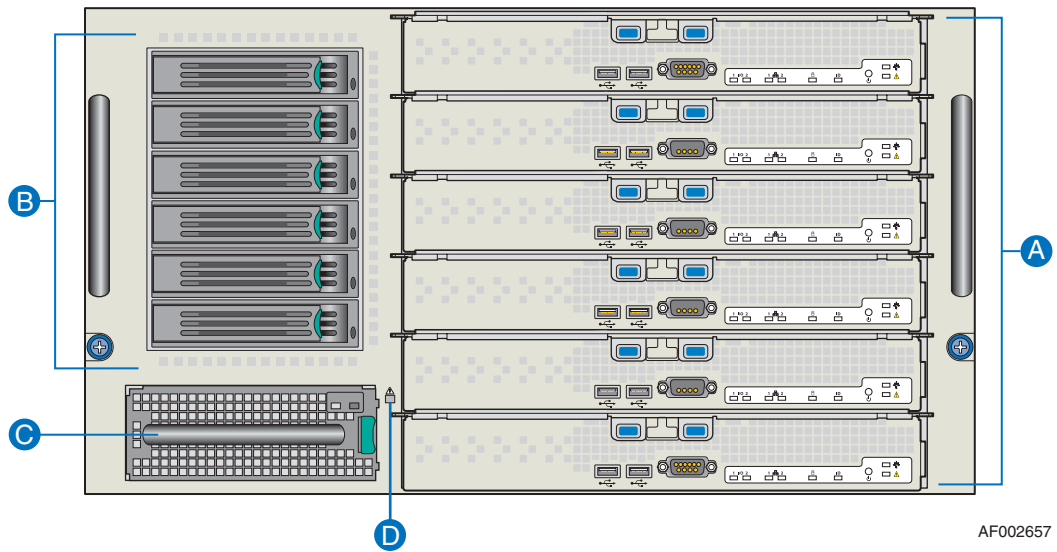
### Front View

Figure 3 shows the front view of the platform. The front provides access to the following components.



Item	Description
A	Compute modules or filler panels (six) [compute module 1 on top and compute module 6 on bottom]
B	Hard disk drive (HDD) bay module with hot-swap 2.5-inch SAS hard disk drives (14) [HDD 1 on the upper left and HDD 14 on the lower right]
C	I/O cooling module
D	System status LED

**Figure 3. Front View of 2.5-in Drive Enclosure**



Item	Description
A	Compute modules or filler panels (six) [compute module 1 on top and compute module 6 on bottom]
B	Hard disk drive bay module with hot-swap 3.5-inch SAS or SATA hard disk drives (6) [HDD 1 on top and HDD 6 on bottom]
C	I/O cooling module
D	System status LED

**Figure 4. Front View of 3.5-in Drive Enclosure**

## Compute Module

The Origin 400 system supports up to six compute modules. Each compute module is a general-purpose server built around the following minimum features:

- Processor(s)
- Memory
- Integrated baseboard management controller
- Network interface
- Storage control module

For more information, refer to your SGI Technical Support representative.

## Hard Disk Drive Bay Module

The Origin 400 system has an integrated hard disk drive bay module with the following features:



- The 2.5-in drive enclosure has an integrated hot-swap 2.5-inch SAS hard disk drive bay module that can support up to a maximum of 14 hard disk drives.
- The 3.5-in drive enclosure has an integrated hot-swap 3.5-inch SAS/SATA hard disk drive bay module that can support up to a maximum of 6 hard disk drives.
- Storage configuration and management are supported via the Origin 400 Management Center.

To access the installed physical drives, you must install at least one SGI storage control module in the rear bay labeled SCM1.

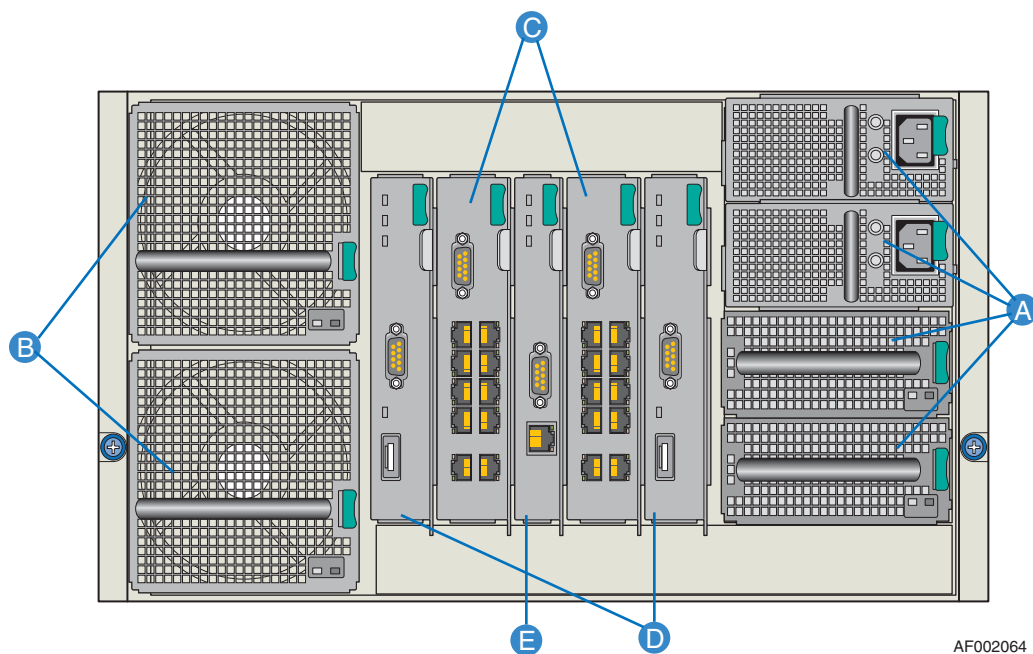
Because hard disk drives have different cooling, power, and vibration characteristics, SGI validates specific hard disk drive types in the platforms. For a list of qualified drives, consult your SGI Technical Support representative.

## **I/O Cooling Module**

The I/O cooling module consists of six fans in a hot-swap module with power and status indicators. These fans provide cooling for all I/O modules. The I/O cooling module is accessible from the front of the system even though it cools the I/O modules in the rear of the system.

## Rear View

Figure 5 shows a rear view of the platform. The rear provides access to the following components:



AF002064

Item	Description
A	Power supply module bays (four) (as illustrated: two top bays occupied by power supply modules; two bottom bays occupied by power supply blanks)
B	Main cooling module bays (two)
	<b>I/O Module Slots</b>
C	Ethernet switch module slots (two)
D	Storage control module slots (two)
E	Management module slot (one)

**Figure 5. Rear View of the System**

## Power Supply Module

Up to four hot-swap power supply modules can be installed in the right rear of the chassis. Each supply has its own AC input power connector and is rated at 1000 watts over an input range of 100-240 VAC. Each power supply includes two fans that provide cooling for hot-swap disk drives. All four power supply bays must be populated with either a power supply module or a power supply blank. The power supply blank has two fans that ensure proper system cooling.

One power supply supports one compute module plus all other modules in the system.

Two power supplies support two to three compute modules (in any slot) plus all other modules in the system.

Three power supplies support four to six compute modules (in any slot) plus all other modules in the system.

Any additional power supplies above the minimum required (based on configuration) provide redundancy.

## **I/O Module Slots**

The middle-rear of the chassis can accommodate up to four expansion modules.

### **Ethernet Switch Module**

One or two hot-swap SGI gigabit Ethernet switch modules can be installed. Each switch has ten uplink ports and twelve internal server bay ports, two ports routed to each compute module. One switch module is the minimum configuration; a second switch module allows for network redundancy.

### **Storage Control Module**

One or two hot-swap SGI storage control modules can be used for up to 14 hot-swap SAS hard drives in the 2.5-in drive enclosure and up to 6 hot-swap SAS/SATA hard drives in the 3.5-in drive enclosure. One storage control module is the minimum configuration; a second storage control module allows for storage control module redundancy. When two storage control modules are installed and one fails, drive access is maintained through the operational storage control module.

### **Management Module**

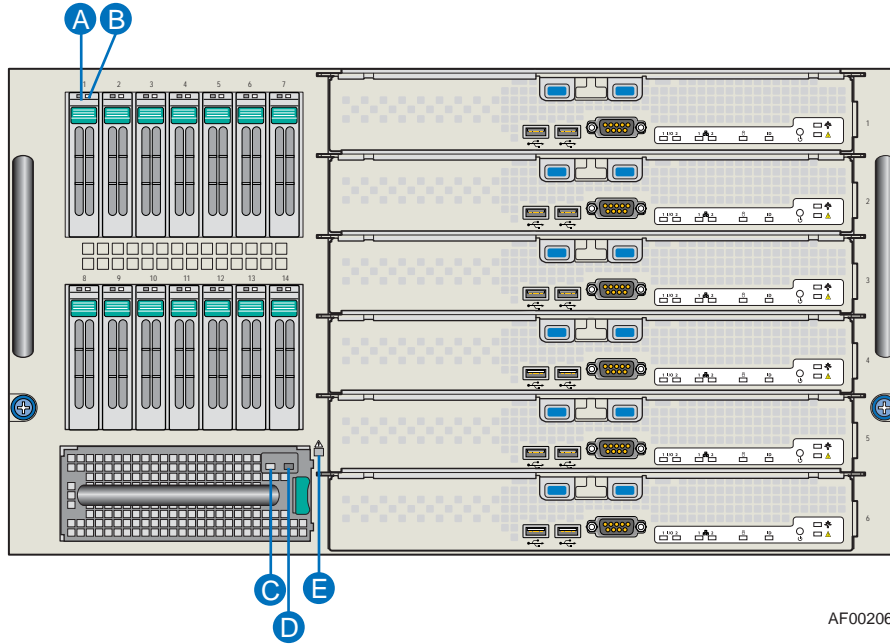
The SGI management module is installed in the middle-rear of the chassis, between the four I/O slots. This module provides an Internet browser interface that enables the configuration and management of the entire Origin 400 system. This module is not redundant but the system will continue to operate normally if this module fails. However, any changes to the system configuration will not be recognized until the failed management module is replaced.

### **Main Cooling Modules**

Two hot-swap main cooling modules are installed on the left rear of the chassis. Each module contains a redundant fan. Main cooling modules maintain separate zones in the chassis. Both modules are required to properly cool all compute modules.

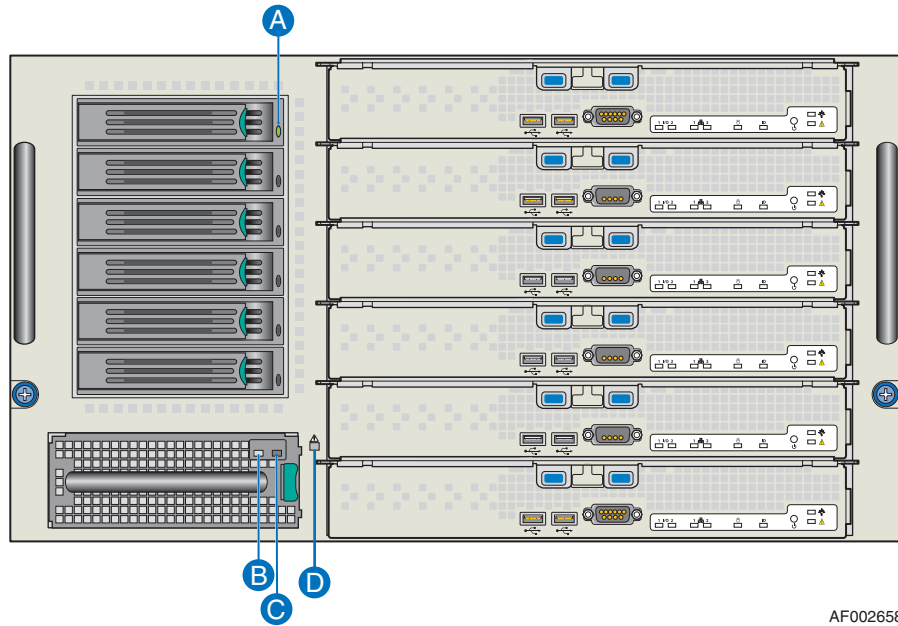
## Front Chassis Connectors and Indicators

The indicator modes for the hard drive carrier, I/O cooling module, and chassis indicators illustrated in the following figures are described in “Diagnostic LED Information” on page 135.



Hard Drive Carrier	
A	Hard drive power/activity LED – Green
B	Hard drive fault LED – Amber
I/O Cooling Module	
C	I/O cooling module power LED – Green
D	I/O cooling module fault LED – Amber
Chassis	
E	System fault LED - Amber

**Figure 6. 2.5-in Drive Enclosure Front Chassis Connectors and Indicators**



AF002658

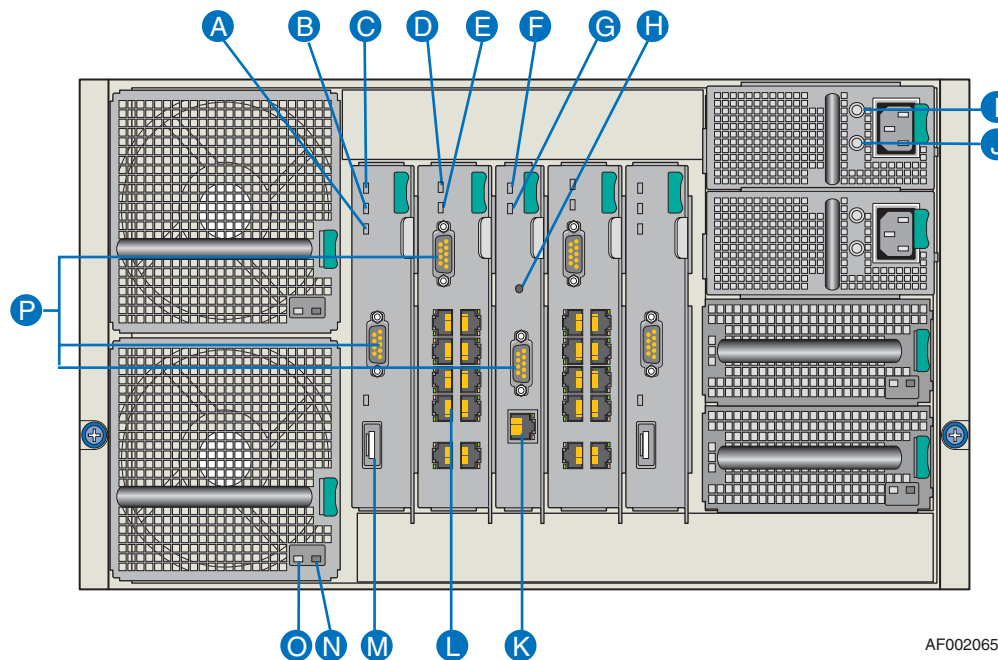
Hard Drive Carrier	
A	Hard drive power/activity LED – Green
I/O Cooling Module	
B	I/O cooling module power LED – Green
C	I/O cooling module fault LED – Amber
Chassis	
D	System fault LED - Amber

**Figure 7. 3.5-in Drive Enclosure Front Chassis Connectors and Indicators**

### Compute Module Connectors and Indicators

For detailed information on compute module connectors and indicators, refer to your Technical Support representative.

## Back Chassis Connectors and Indicators



<b>Storage Control Module</b>	
A	Storage control module dirty cache LED – Green
B	Storage control module fault LED – Amber
C	Storage control module power LED – Green
M	Storage control module Ethernet SAS connector
<b>Ethernet Switch Module</b>	
D	Ethernet switch module power LED – Green
E	Ethernet switch module fault LED – Amber
L	Ethernet switch module 1-Gb Ethernet connectors (10) with LEDs
P	Serial cable connectors (manufacturing only)
<b>Management Module</b>	
F	Management module power LED – Green
G	Management module fault LED – Amber
H	Management module reset switch
K	Management module NIC connectors with LEDs
<b>Power Supply Module</b>	
I	Power supply module power LED – Green
J	Power supply fault indicator LED – Amber
<b>Main Cooling Module</b>	
N	Main cooling module fault LED – Amber
O	Main cooling module power LED – Green

**Figure 8. Rear Chassis Connectors and Indicators**

All indicator modes are described in [“Diagnostic LED Information”](#) on page 135.

## **Rack Mount Options**

The Origin 400 system can be mounted into a 4-post fixed mount rack.

For instructions on installing your Origin 400 system into a rack, refer to your SGI Technical Support representative.





# 2 Hardware Installations and Upgrades

---

## Before You Begin

Before working on your server system, review the safety and ESD information at the beginning of this manual and in the appendices.

## Tools and Supplies Needed

- Phillips (cross head) screwdriver (#1 bit and #2 bit)
- Needle-nosed pliers
- A ruler
- Pen or pencil
- Anti-static wrist strap and conductive foam pad (recommended)

## Chassis References

All references to left, right, front, top, and bottom are based on the reader facing the front of the chassis as it would be positioned for normal operation.

## Installing the Origin 400 System in a Rack

The Origin 400 system is designed for fixed mount rack installation only; all service events will be performed from either the front or back of the system.

**Caution:** *When removing the system from its packaging, DO NOT lift the system by the power supply or fan module handles.*

## Installation Guidelines

- Review the safety and ESD information at the beginning of this manual and in the appendices.
- Use a mechanical lift to install the Origin 400 system in a rack cabinet.
- When lifting the system, DO NOT lift by the power supply or fan module handles.
- All compute modules, hard drives, power supply modules, I/O modules, and cooling modules should be removed before placing the Origin 400 system in a rack.
- The Origin 400 system can only be installed in a rack cabinet with perforated front and rear doors.
- Plan device installation starting with the bottom of the rack cabinet.

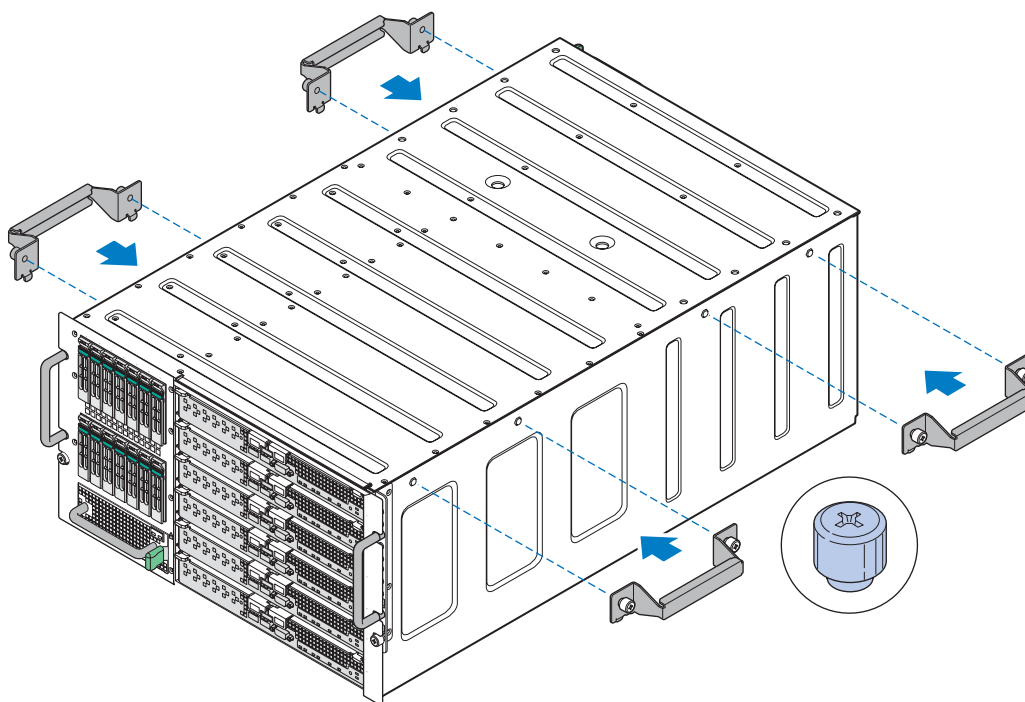
- Do not leave unused space within the rack cabinet opening; blank filler panels must be used to fill gaps and prevent recirculation of warm air.
- Ensure the power outlets in the rack are sufficient in quantity and load capacity to support all devices intended to be installed in the rack.

## Installing Temporary Handles on System

Temporary handles are provided with your Origin 400 system. These handles are intended to aid in the movement of the system during removal from packaging and during initial configuration and installation. However, the profile of the handles is such that it prevents their use when the system is installed in a standard 19-inch rack.

To install the temporary handles on the system, follow these steps:

1. Mount the handles to the top edges of both the front and rear of the system.
2. Insert the handle tabs of each front and rear handle into the chassis slots and tighten captive screws.



AF002418

**Figure 9. Installing Temporary Handles**

The system can now be moved as required to aid in removal from packaging, installation of the remaining modules in the system, or installation of the system in a rack.

**Warning:** *If using the handles during rack installation, the rear handles must be removed prior to setting the system on the rack rails to avoid interference of the handles with the rack. The*

*front handles must also be removed before sliding the system completely into the rack and securing the front chassis tabs to the rack.*

## Mounting System in Rack

Please read the safety information at the beginning of this book before installing the chassis in a rack.

**Warning:** *If you have installed temporary handles to aid in moving and / or configuring the system, you must remove the rear handles prior to setting the system on the rack rails to avoid interference of the handles with the rack. The front handles must also be removed before sliding the system completely into the rack and securing the front chassis tabs to the rack.*

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Identify the location within the rack where the server system is to be installed.
3. Install the rack mount rails as described in the rail installation instructions.
4. Remove the compute modules, hard drives, power supply modules, I/O modules, and cooling modules.
5. Working with at least two people, slide the server system into the rack so that it rests on the rack mounting rails.
6. Secure the server system in the rack as described in the rail installation instructions.
7. Install all compute modules, hard drives, power supply modules, I/O modules, and cooling modules.

## Hot-Swap Module Installation and Removal Guidelines

- The green color on components and labels in your chassis identifies hot-swap components. You can install or remove hot-swap modules and hot-plug compute modules, with some restrictions, while the server system is powered on.
- You do not need to disconnect the server system from power to install or replace any of the hot-swap modules; however, to avoid data corruption, you must shut down the operating system and power off the compute module before removing it from the server system.
- Hot-swap cooling modules must be replaced within one minute. All other hot-swap and hot-plug components must be replaced within two minutes. Compute modules, management modules, switch modules, storage control modules, power modules, and cooling modules should be replaced with a like component or a filler panel within two minutes.

## Replacing the Management Module

The Origin 400 system ships with a management module pre-installed in the middle bay of the rear of the chassis. The middle bay is dedicated to the management module and is labeled CMM. For the exact location of the management module bay, see [Figure 5](#).

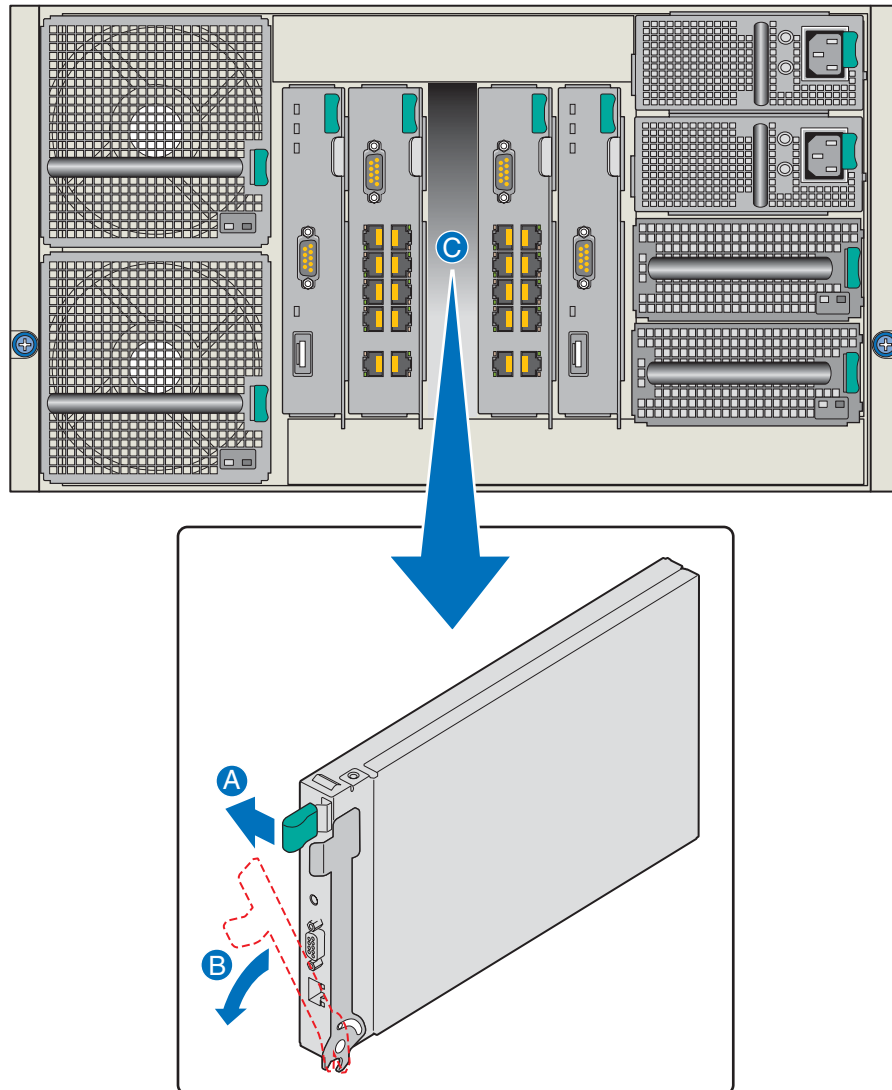
The management module can only be installed in a module bay that is designed to support that device type. If necessary, the management module may be removed and replaced using the steps detailed in the following sections:

- [“Removing the Management Module” on page 18](#)
- [“Installing the Management Module” on page 19](#)

## Removing the Management Module

To remove the management module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Remove the Ethernet cable from the management module.
3. Press the retention latch (see letter “A” in [Figure 10](#)) to release the retention lever.
4. Rotate the lever out and away from the module bay (see letter “B” in [Figure 10](#)) and pull the module straight out the back of the chassis (see letter “C” in [Figure 10](#)).



AF002436

**Figure 10. Removing the Management Module**

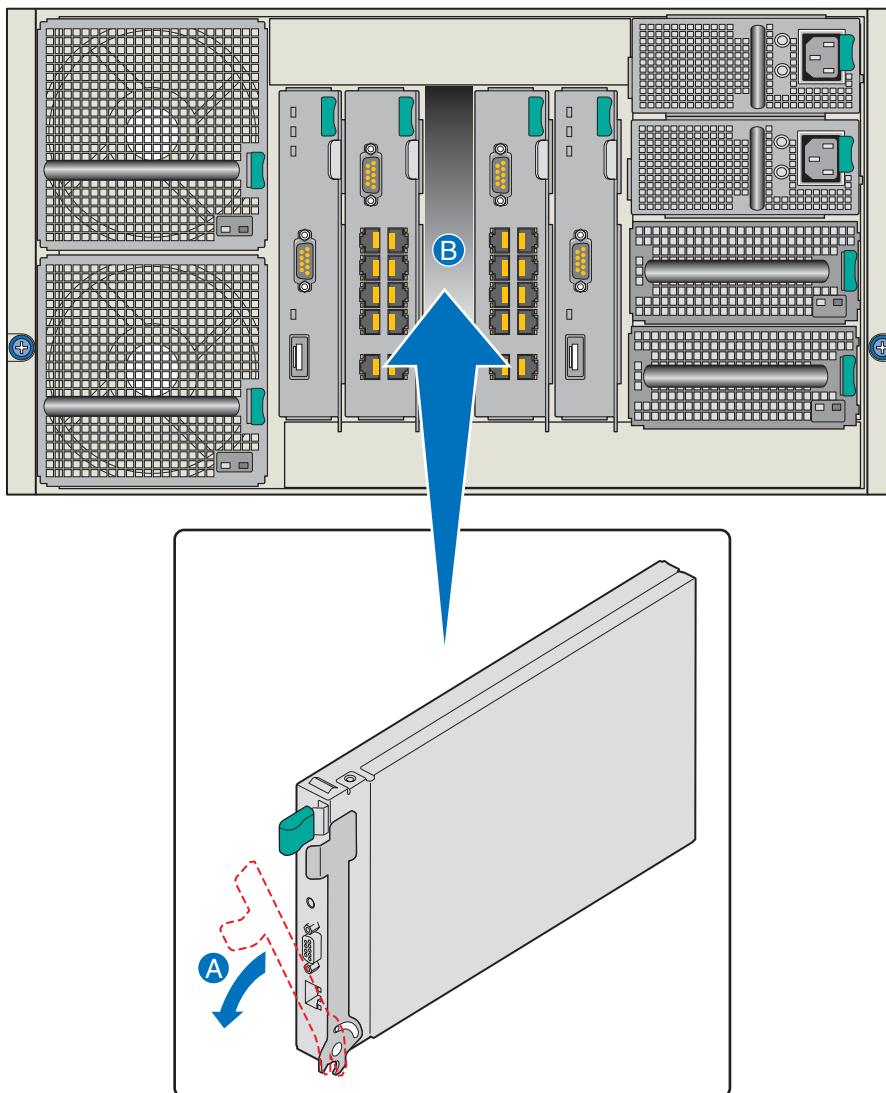
5. Install another management module in the management module bay within two minutes.

## Installing the Management Module

To install the management module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Locate the management module bay and remove the module to be replaced.

3. Release and rotate the module retention lever out and away from the replacement management module (see letter “A” in [Figure 11](#)).
4. Slide the replacement management module into the management module bay (see letter “B” in [Figure 10](#)) until the bottom of the retention lever engages with the module bay.



AF002414

**Figure 11. Installing the Management Module**

5. Rotate the lever handle in toward the module bay until it is latched.
6. Reconnect the Ethernet management port to the management network.

## Installing and Removing an Ethernet Switch Module

The Origin 400 system ships with one Ethernet switch module pre-installed. Optionally, a second switch module may be installed in the second switch module bay. An Ethernet switch module can only be installed in a module bay that is designed to support that device type. The two bays located immediately to the left and right of the management module are dedicated to the Ethernet switch modules and are labeled “ESM”. For the exact location of the switch module bay, see [Figure 5](#).

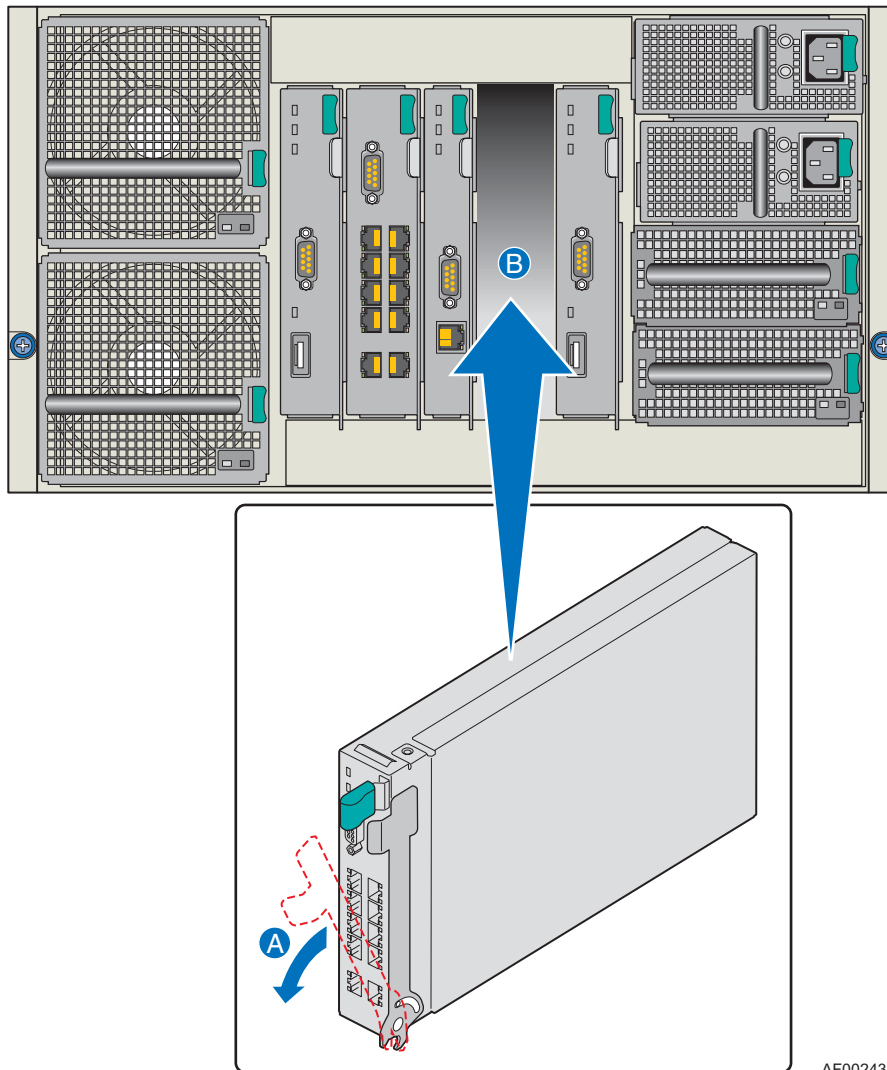
The Ethernet switch module may be removed and installed using the steps detailed in the following sections:

- [“Installing an Ethernet Switch Module” on page 21](#)
- [“Removing an Ethernet Switch Module” on page 22](#)

### Installing an Ethernet Switch Module

To install an Ethernet switch module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Locate an available switch bay and remove any installed module or filler panel.
3. Release and rotate the module retention lever out and away from the switch module (see letter “A” in [Figure 12](#)).
4. Slide the switch module into the selected module bay (see letter “B” in [Figure 12](#)) until the bottom of the retention lever engages the bay.



AF002437

**Figure 12. Installing an Ethernet Switch Module**

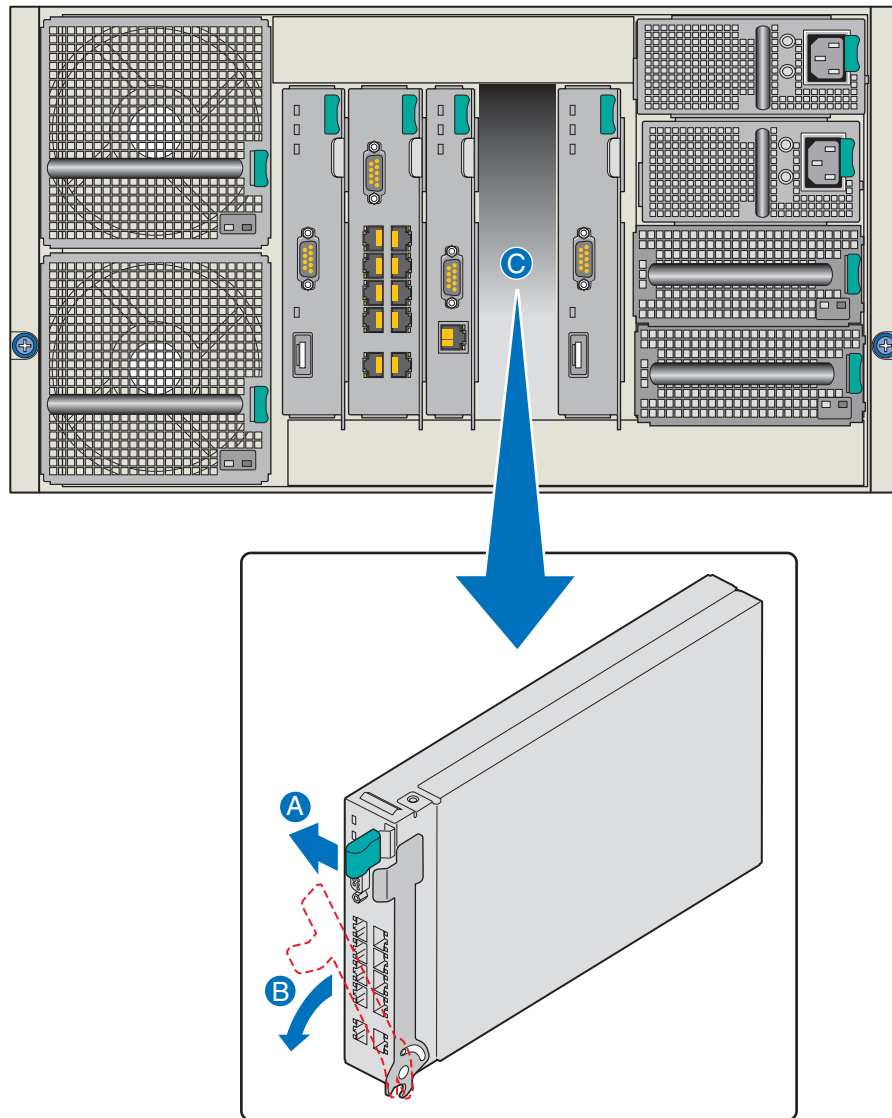
5. Rotate the lever handle in toward the module bay until it is latched.
6. Connect one or more Ethernet switch ports to your network as is appropriate.

## Removing an Ethernet Switch Module

To remove an Ethernet switch module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Remove and label the connected Ethernet cables, as necessary.
3. Press the retention latch (see letter “A” in [Figure 13](#)) to release the retention lever.
4. Rotate the lever out and away from the module bay (see letter “B” in [Figure 13](#)) and pull the module straight out the back of the chassis (see letter “C” in [Figure 13](#)).





AF002413

**Figure 13. Removing an Ethernet Switch Module**

5. Install a filler panel or another Ethernet switch module in the switch module bay within two minutes.

## Installing and Removing a Storage Control Module

The Origin 400 system ships with one storage control module pre-installed. Optionally, a second storage control module may be installed in the open storage control module bay. A storage control module can only be installed in a module bay that is designed to support that device type. The farthest bay on the left and the farthest bay on the right are dedicated to the storage control modules and are labeled “SCM”. For the exact location of the storage control module bay, see [Figure 5](#).

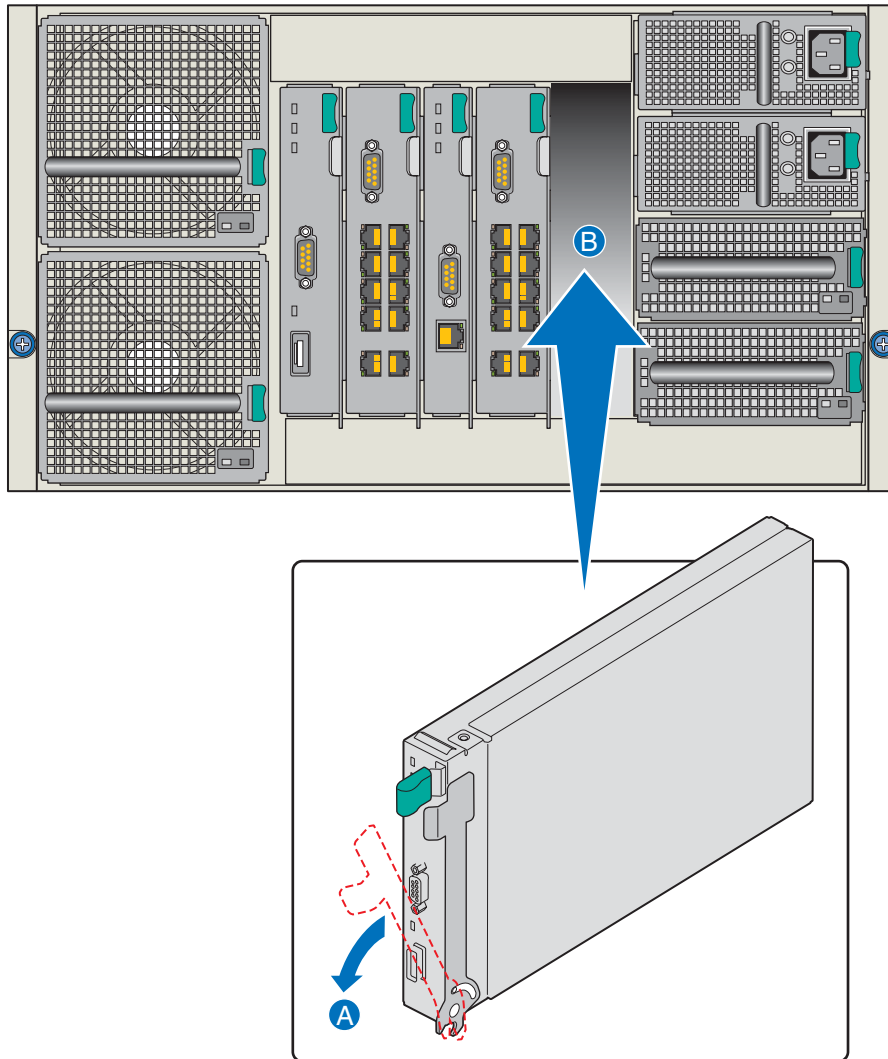
The storage control module may be removed and installed using the steps detailed in the following sections:

- [“Installing a Storage Control Module” on page 24](#)
- [“Removing a Storage Control Module” on page 25](#)

### Installing a Storage Control Module

To install a storage control module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Locate an available storage control module bay and remove any installed module or filler panel.
3. Release and rotate the module retention lever out and away from the storage control module (see letter “A” in [Figure 14](#)).
4. Slide the storage control module into the selected module bay (see letter “B” in [Figure 14](#)) until the bottom of the retention lever engages with the module bay.



AF002412

**Figure 14. Installing a Storage Control Module**

5. Rotate the lever handle in toward the module bay until it latches.

## Removing a Storage Control Module

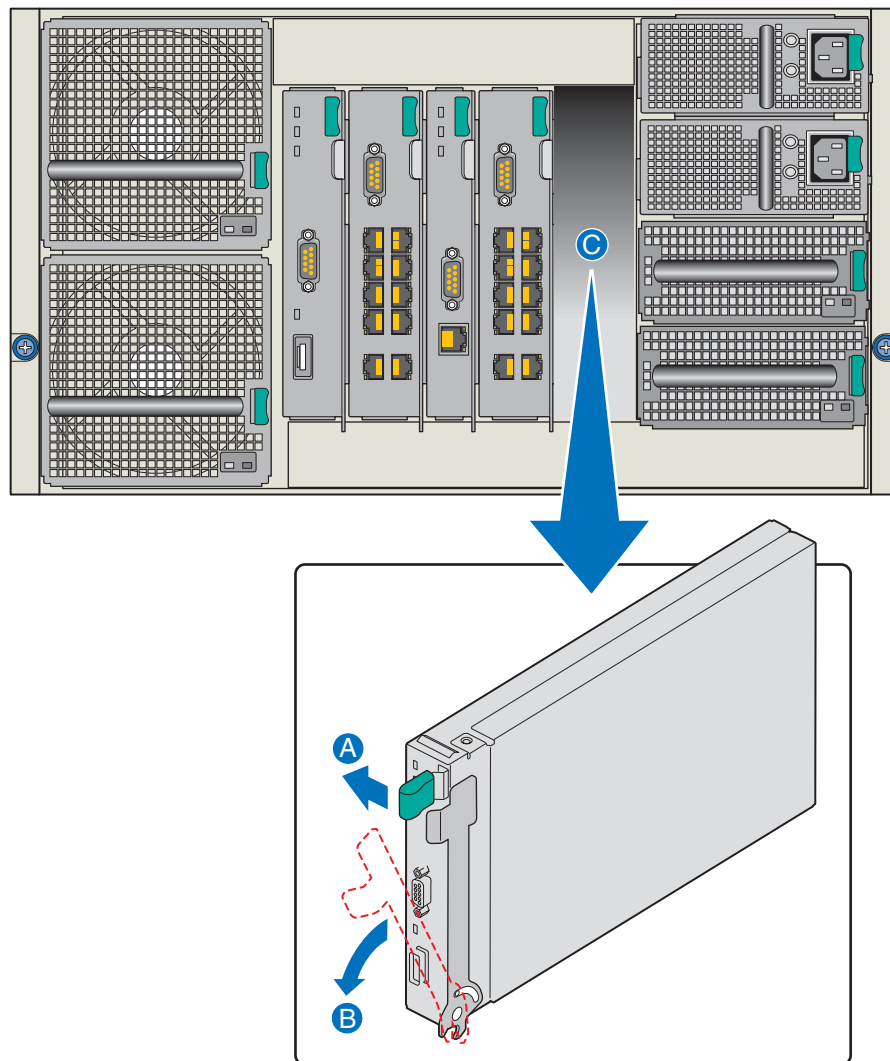
If only one SGI storage control module is installed in the Origin 400, power off all compute modules prior to removing the storage control module.

To remove a storage control module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Press the retention lever latch button to release the retention lever (see letter “A” in Figure 15).

3. Rotate the lever out and away from the module bay (see letter “B” in Figure 15) and pull the storage control module straight out the back of the chassis (see letter “C” in Figure 15).

**Warning:** You must replace the storage control module with a filler panel or another storage control module within two minutes.



AF002430

**Figure 15. Removing a Storage Control Module**

4. Install a filler panel or another storage control module in the storage control module bay within two minutes.

## Installing and Removing the Backup Battery

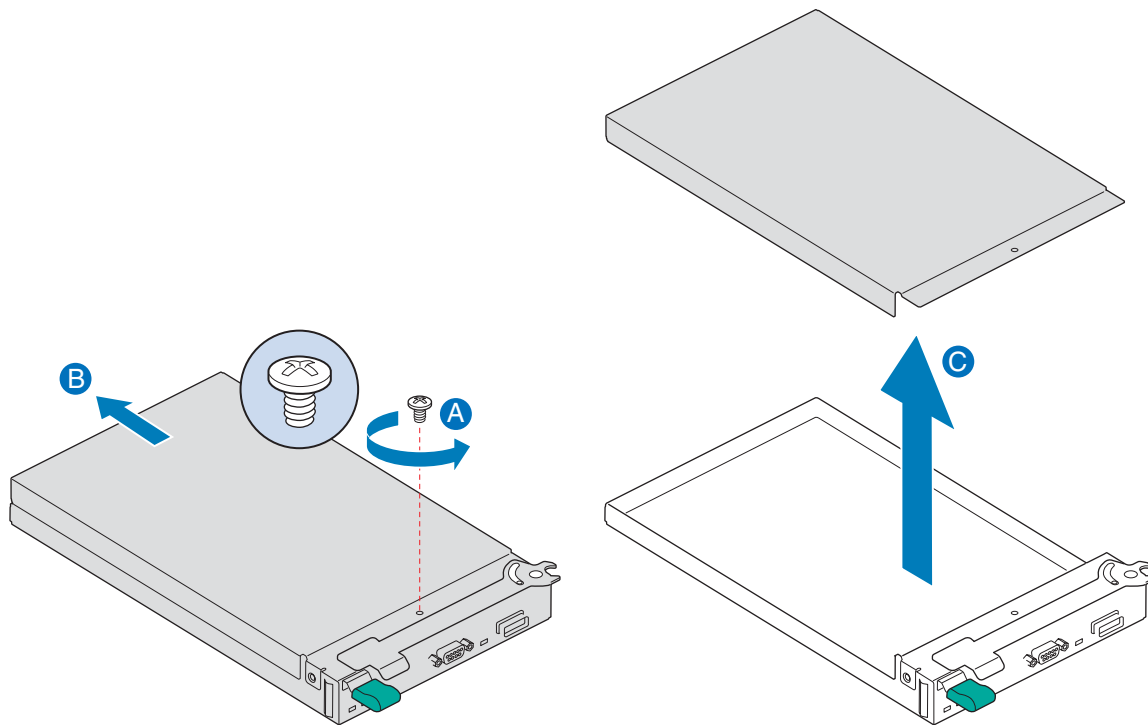
### Installing a Backup Battery

To install a backup battery, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Remove the storage control module from the system. For instructions, see “[Removing a Storage Control Module](#)” on page 25.

**Warning:** *You must replace the storage control module with a filler panel or another storage control module within two minutes.*

3. Place the storage control module sideways on a work surface so that its largest surface area is touching the work surface and the retention lever is on the top.
4. With a Phillips screwdriver, remove the screw securing the top cover to the storage control module (see letter “A” in [Figure 16](#)).

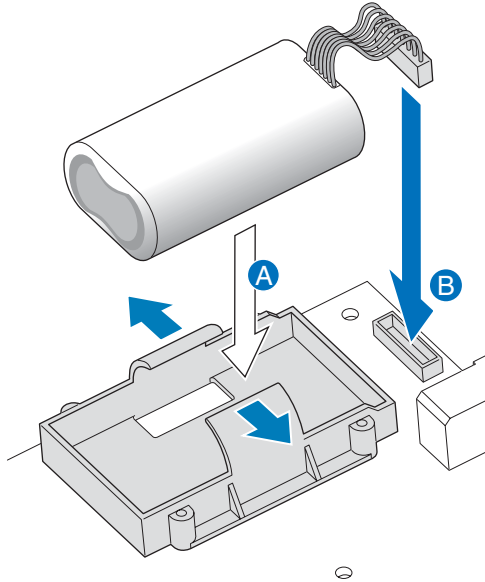


AF002563

**Figure 16. Removing Top Cover from Storage Control Module**

5. Slide the cover towards the rear of the storage control module (see letter “B” in [Figure 16](#)) and lift upward (see letter “C” in [Figure 16](#)).

6. Install the backup battery in the black plastic battery holder (see letter “A” in [Figure 17](#)). Connect the battery cable to the battery connector on the printed circuit board (see letter “B” in [Figure 17](#)).



AF002440

**Figure 17. Installing Backup Battery**

7. Align notches in the top cover with corresponding tabs in the storage control module. Slide the top cover forward to close.
8. Secure the top cover to the storage control module with the two screws previously removed.
9. Re-install the storage control module in the server system. For instructions, see [“Installing a Storage Control Module” on page 24](#).

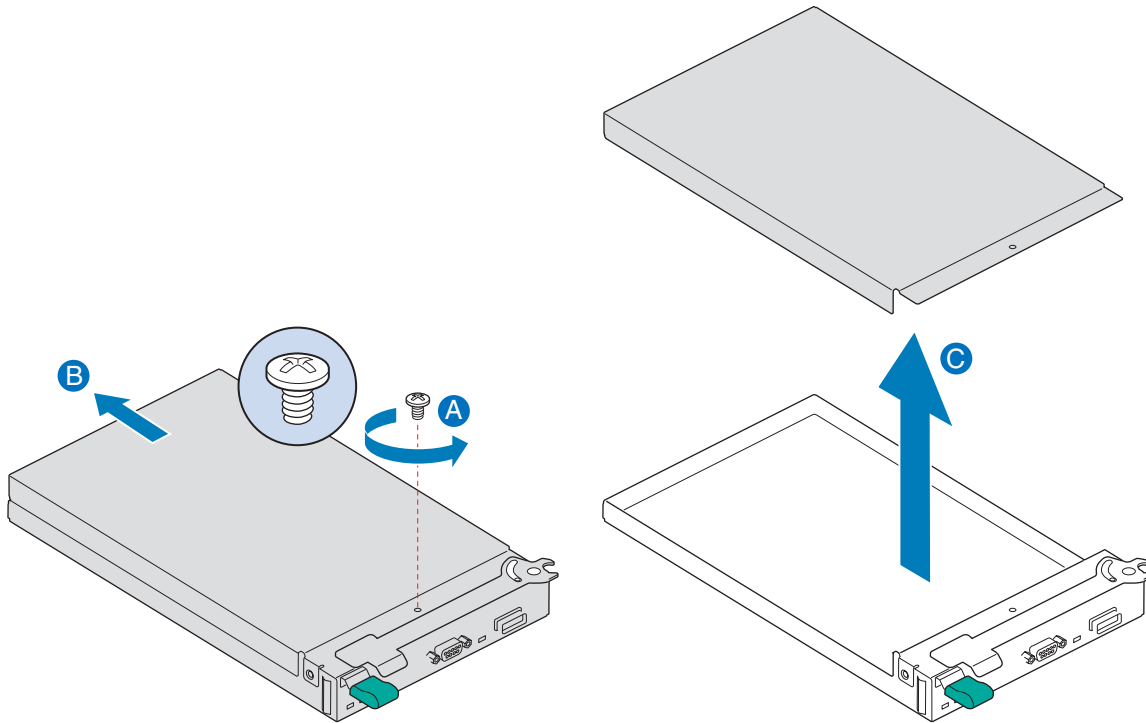
## Removing a Backup Battery

To remove a backup battery, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Remove the storage control module from the system. For instructions, see [“Removing a Storage Control Module” on page 25](#).

**Warning:** *You must replace the storage control module with a filler panel or another storage control module within two minutes.*

3. Place the storage control module sideways on a work surface so that its largest surface area is touching the work surface and the retention lever is on the top.
4. With a Phillips screwdriver, remove the screw securing the top cover to the storage control module (see letter “A” in [Figure 18](#)).

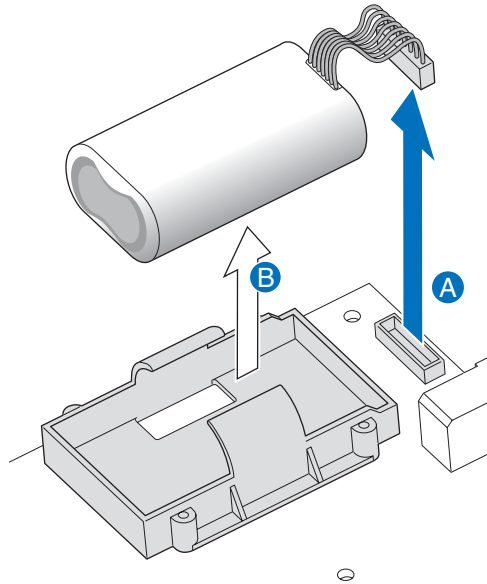


AF002563

**Figure 18. Removing Top Cover from Storage Control Module**

5. Slide the cover towards rear of the storage control module (see letter “B” in [Figure 18](#)) and lift upward (see letter “C” in [Figure 18](#)).

6. Disconnect the battery cable from the battery connector on the printed circuit board (see letter “A” in [Figure 19](#)). Remove the battery from the black plastic battery holder (see letter “B” in [Figure 19](#)).



AF002461

**Figure 19. Removing Backup Battery**

7. Align notches in the top cover with corresponding tabs in the storage control module. Slide the top cover forward to close.
8. Secure the top cover to the storage control module with the two screws previously removed.
9. Re-install the storage control module in the server system. For instructions, see [“Installing a Storage Control Module”](#) on page 24.

## Installing and Removing a Power Supply Module

The Origin 400 system ships with two power supply modules pre-installed. A single power supply is suitable to support the power requirement for the chassis, including fan modules, storage control module, switch module, storage bay, and a single compute module. Additional power modules are required as the number of installed compute modules increases.

**Note:** *One power supply module supports one compute module plus all other modules in the system.*

*Two power supply modules support two to three compute modules (in any slot) plus all other modules in the system.*



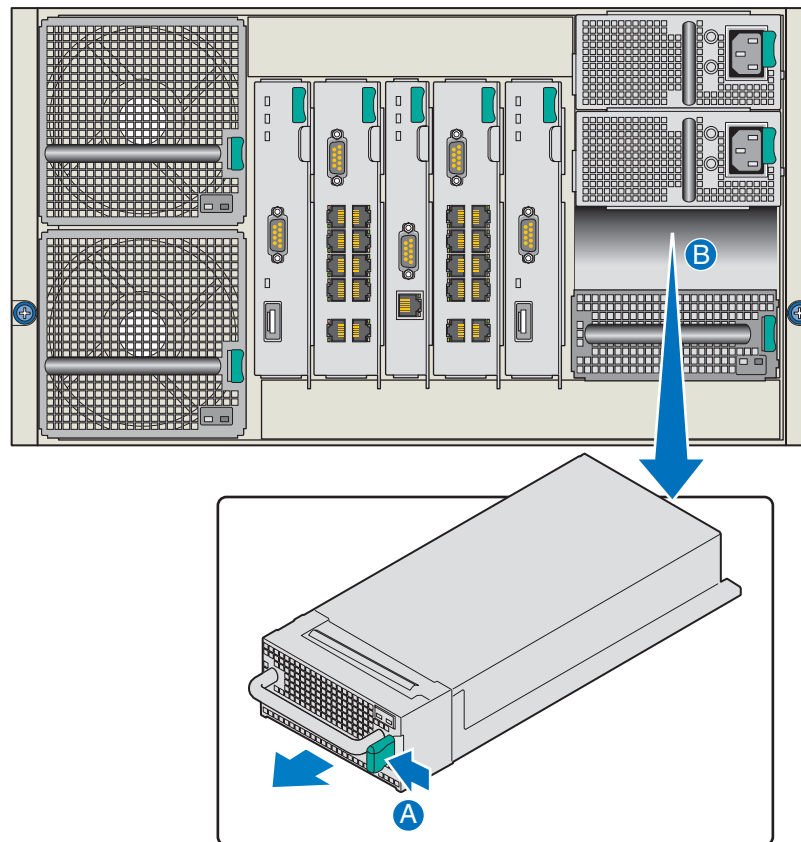
Three power supply modules support four to six compute modules (in any slot) plus all other modules in the system.

Any additional power supply modules above the minimum required (based on configuration) provide redundancy.

## Installing a Power Supply Module

To install a power supply module, follow these steps:

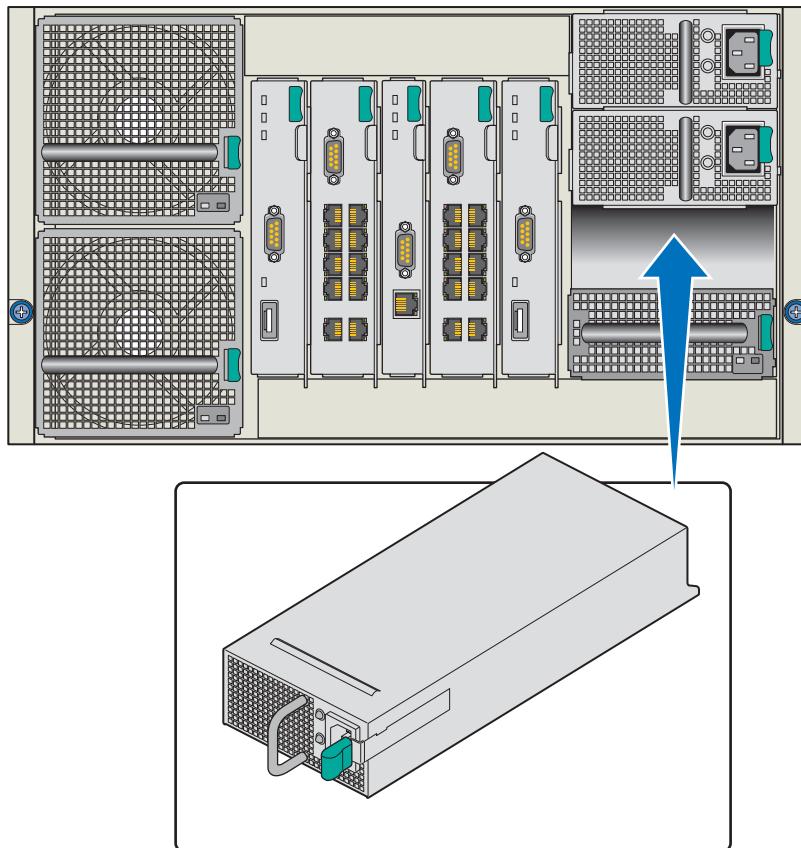
1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Locate the power supply module bay and remove any installed module or filler module.
  - For instructions on removing a power supply module, see “[Removing a Power Supply Module](#)” on page 32.
  - To remove a filler module, press the retention lever latch (see letter “A” in [Figure 20](#)) to release the filler module from the module bay. Slide the filler module out of the bay (see letter “B” in [Figure 20](#)).



AF002420

**Figure 20. Removing Filler Module**

3. Slide the power supply module into the power supply module bay until the retention latch engages.



AF002434

**Figure 21. Installing Power Supply Module**

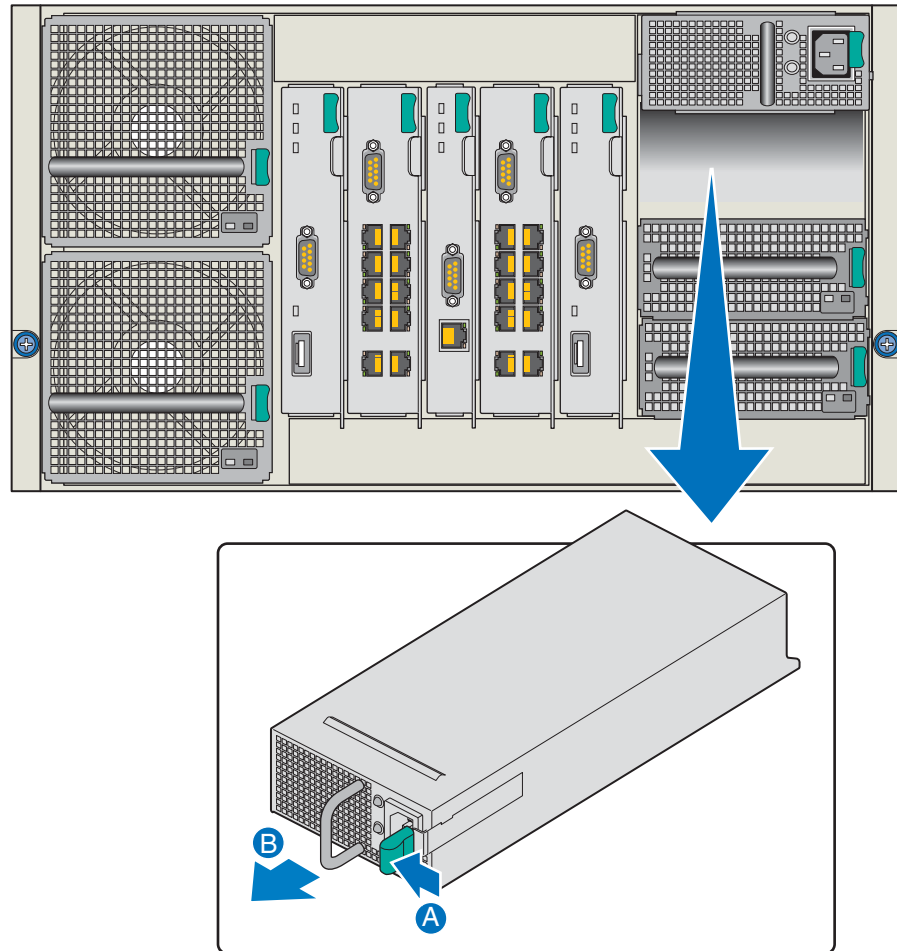
4. Connect a power cable from the power supply module to an appropriate power source.

## Removing a Power Supply Module

To remove a power supply module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Locate the power supply module to be removed.
3. Remove the power cord from both the power supply module and the power source.

4. Press the power supply module retention latch to release the power supply module from the bay (see letter “A” in [Figure 22](#)). Slide the power supply module out of the module bay (see letter “B” in [Figure 22](#)).



AF002433

**Figure 22. Removing a Power Supply Module**

5. Replace the power supply module with a filler panel or another power supply module within two minutes.

## Replacing a Main Cooling Module

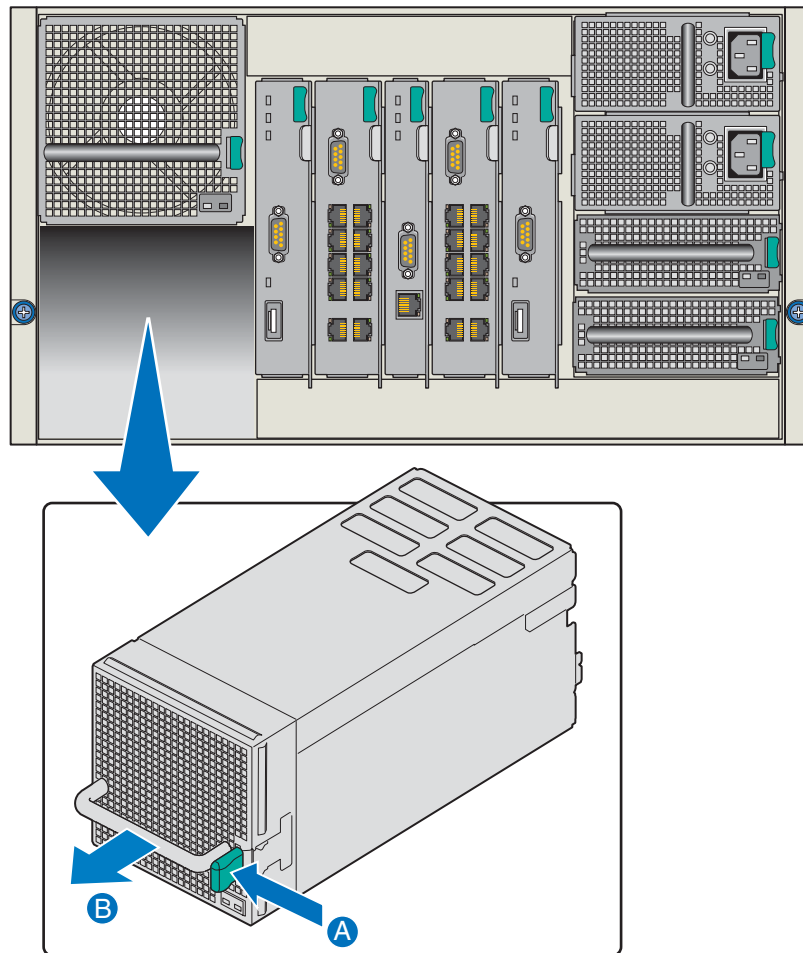
The Origin 400 system ships with two main cooling modules pre-installed at the back of the chassis. For the exact location of the Main Cooling Modules, see [Figure 5](#).

## Removing a Main Cooling Module

To remove a main cooling module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Locate the main cooling module to be replaced.
3. Press the main cooling module retention clip to release the main cooling module from the module bay (see letter “A” in [Figure 23](#)).
4. Slide the main cooling module out of the module bay (see letter “B” in [Figure 23](#)).

**Warning:** Replace the cooling module with another cooling module within two minutes.



AF002438

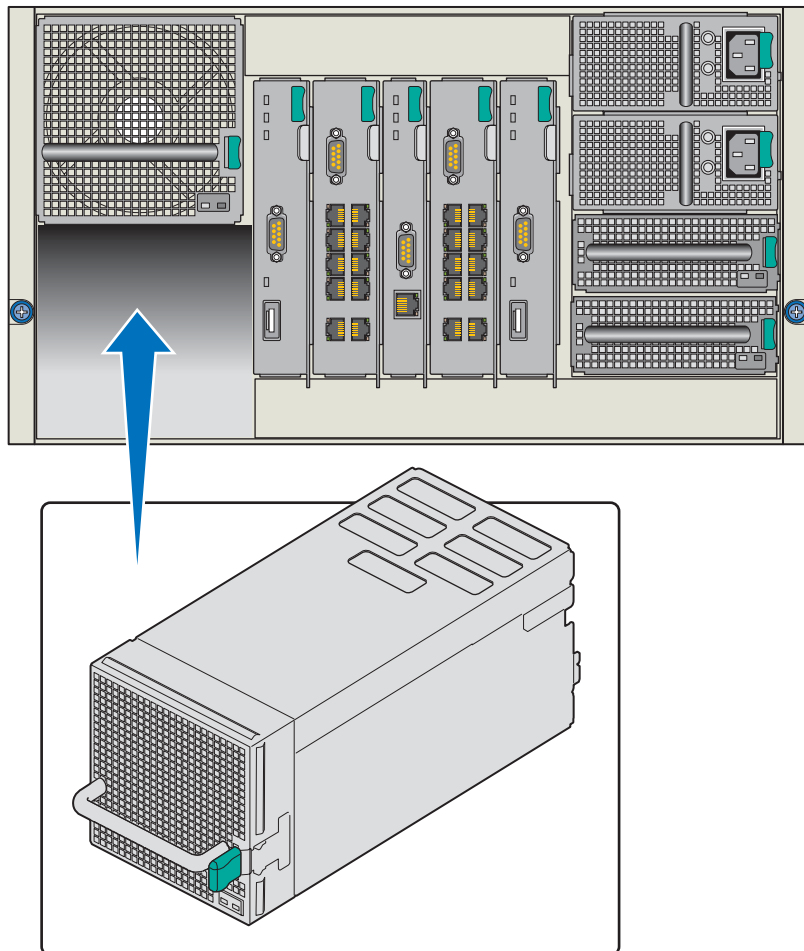
**Figure 23. Removing a Main Cooling Module**

5. Install another cooling module into the cooling module bay within two minutes.

## Installing a Main Cooling Module

To install a main cooling module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Locate the cooling module bay and remove the cooling module to be replaced.
3. Slide the replacement cooling module into the unoccupied cooling module bay until the retention latch engages (see [Figure 24](#)).



AF002439

**Figure 24. Installing a Main Cooling Module**

## Replacing the I/O Cooling Module

The Origin 400 system ships with one I/O cooling module pre-installed at the front of the chassis. For the exact location of the I/O Cooling Module in

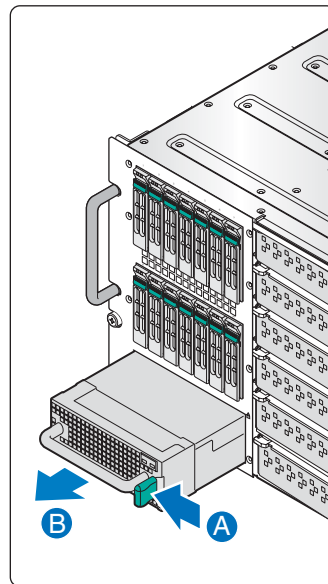
- 2.5-in drive enclosure, see [Figure 3](#)

- 3.5-in drive enclosure, see [Figure 4](#)

## Removing the I/O Cooling Module

To remove the I/O cooling module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Locate the I/O cooling module to be replaced.
3. Press the I/O cooling module retention latch to release the I/O cooling module from the module bay (see letter “A” in [Figure 26](#)).
4. Slide the I/O cooling module out of the module bay (see letter “B” in [Figure 26](#)).



AF003160

**Figure 25. Removing an I/O Cooling Module**

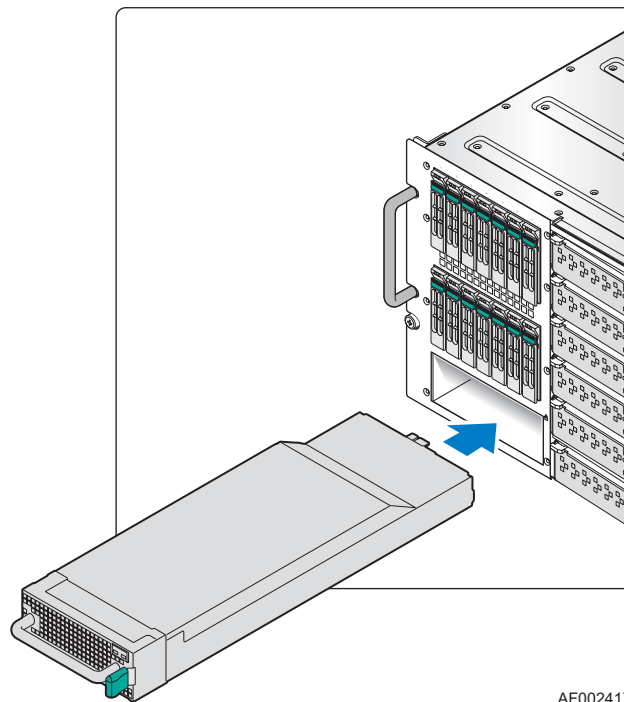
5. Install another cooling module into the cooling module bay within two minutes.

## Installing the I/O Cooling Module

To install the I/O cooling module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Locate the cooling module bay and remove the cooling module to be replaced.
3. Slide the replacement I/O cooling module into the vacant module bay (see [Figure 26](#)) until the retention latch engages.

**Warning:** Replace the cooling module with another cooling module within two minutes.



**Figure 26. Installing an I/O Cooling Module**

## Installing and Removing Hard Drives

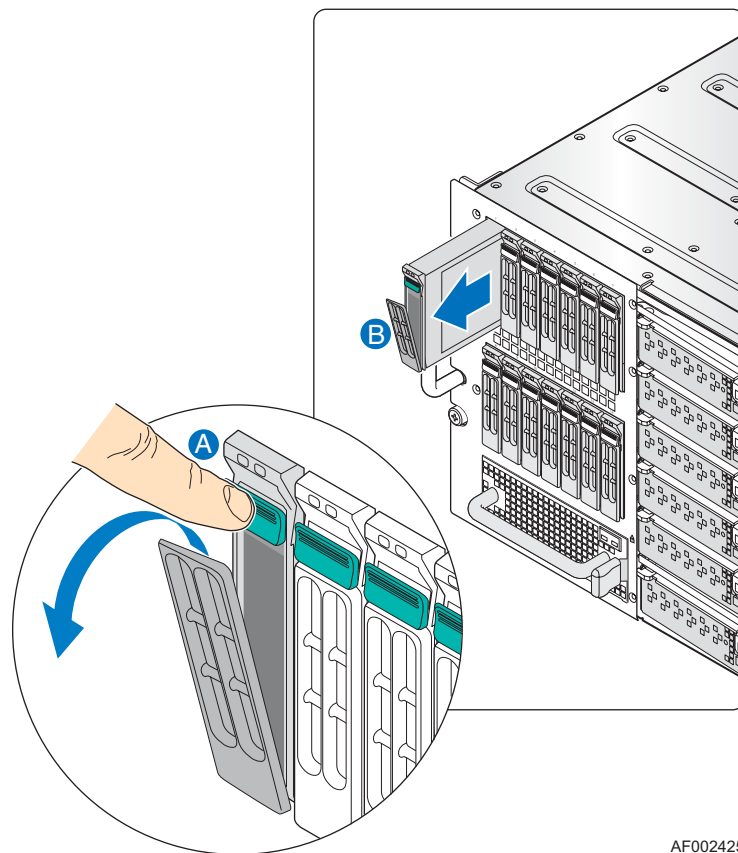
The Origin 400 system provides storage for installed compute modules by way of an on-board storage bay combined with a storage management module. The on-board storage bay supports the installation of up to 14 hot-swap 2.5-inch SAS hard drives in the 2.5-in drive enclosure or 6 hot-swap 3.5-inch SAS/SATA hard drives in the 3.5-in drive enclosure that are configured through the integrated Origin 400 Management Center user interface. For more information, see [“Using the Origin 400 Management Center” on page 53](#).

**Caution:** You must only install hard drives that are sold as Origin 400 drives. For more information, refer to your SGI Sales representative.

## Installing a 2.5-inch Hard Drive into the Storage Bay

To install a 2.5-inch hard drive into the storage bay, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Press the retaining lever on an available drive carrier to release the drive carrier from the drive bay module (see letter “A” in Figure 27). Remove the drive carrier from the drive bay module (see letter “B” in Figure 27).



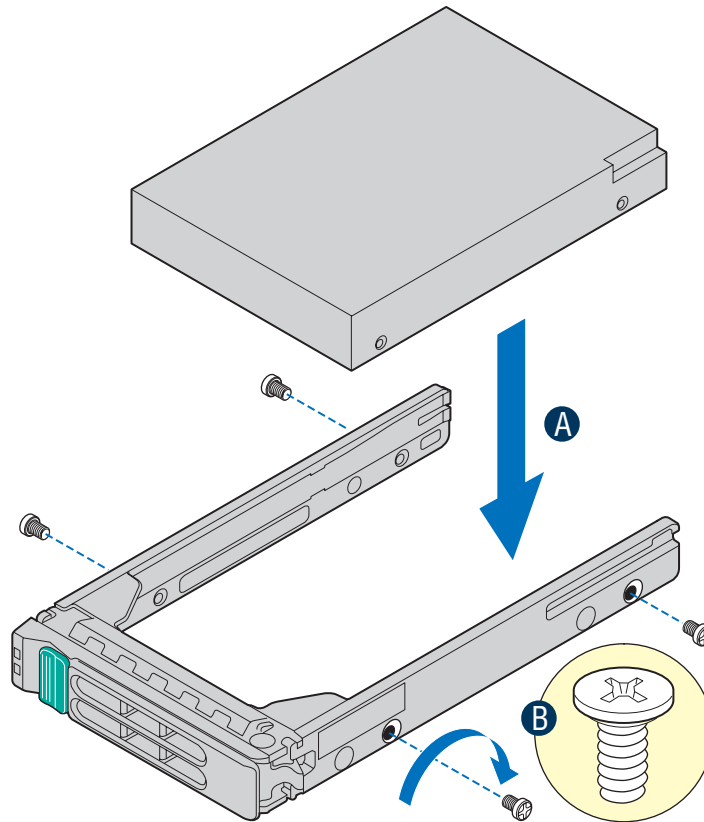
AF002425

**Figure 27. Removing a 2.5-inch Drive Carrier from a Drive Bay Module**

3. With a Phillips screwdriver, remove the four screws securing the filler panel to the drive carrier.



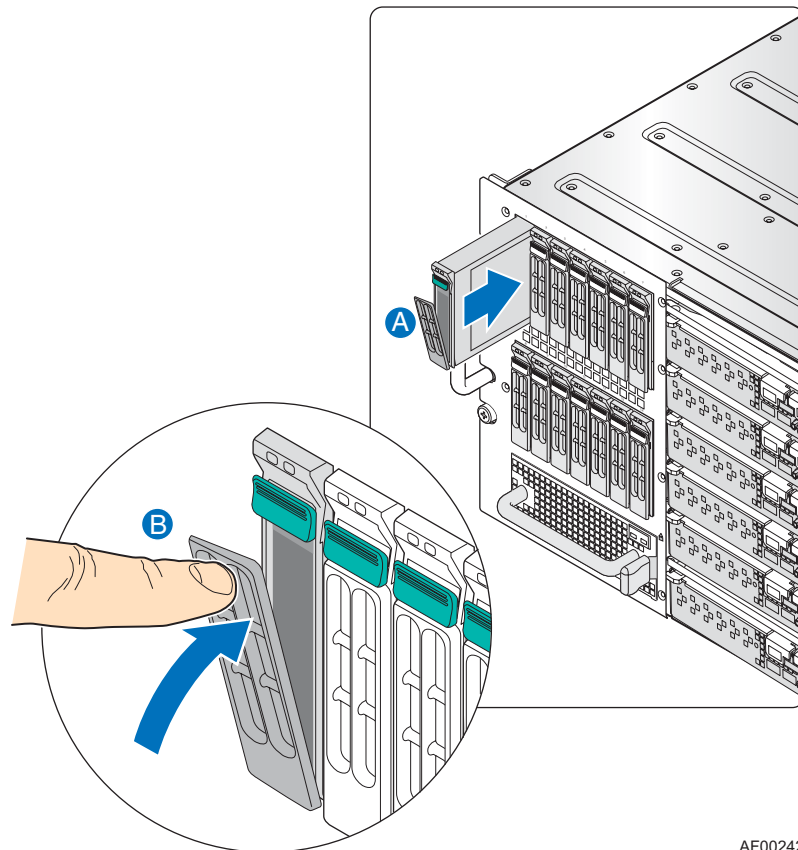
4. Align the holes in the hard drive to the holes in the drive carrier (see letter “A” in [Figure 28](#)) and attach it to the drive carrier using the four screws removed in the previous step (see letter “B” in [Figure 28](#)).



AF002428

**Figure 28. Installing Hard Drive into Drive Carrier**

5. With the drive carrier retaining lever in the open position (see letter “A” in [Figure 29](#)), carefully slide the drive carrier into the drive bay module until it is fully seated and the retaining lever starts to engage. Press firmly to latch the retaining lever (see letter “B” in [Figure 29](#)).



AF002426

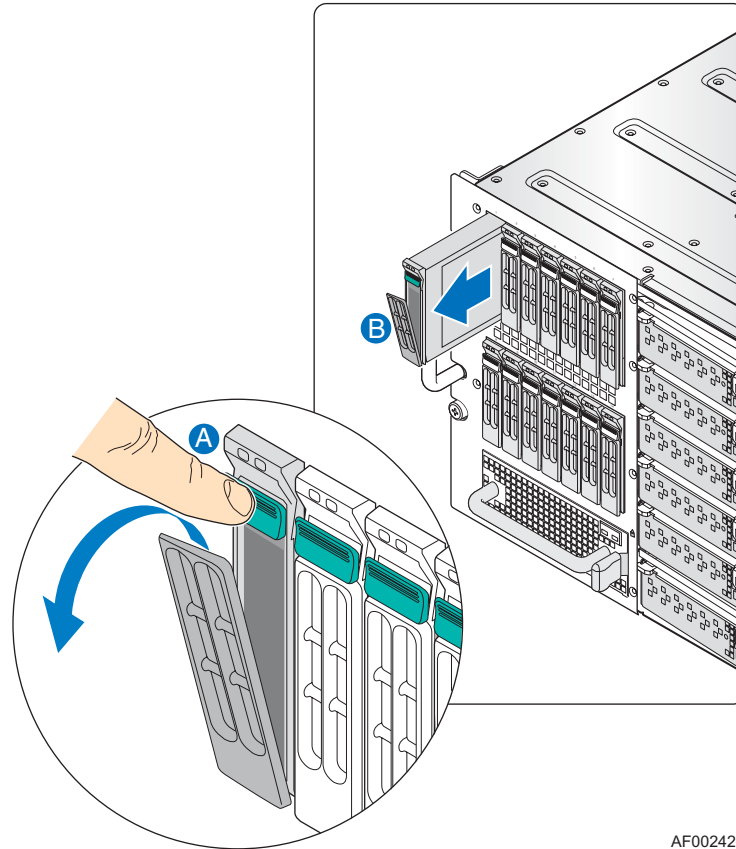
**Figure 29. Installing 2.5-inch Drive Carrier in Drive Bay Module**

## Removing a 2.5-inch Hard Drive from the Storage Bay

To remove a 2.5-inch hard drive from the storage bay, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. To avoid data corruption, ensure that the drive you intend to remove is not online and actively providing data storage to any of the installed compute modules.

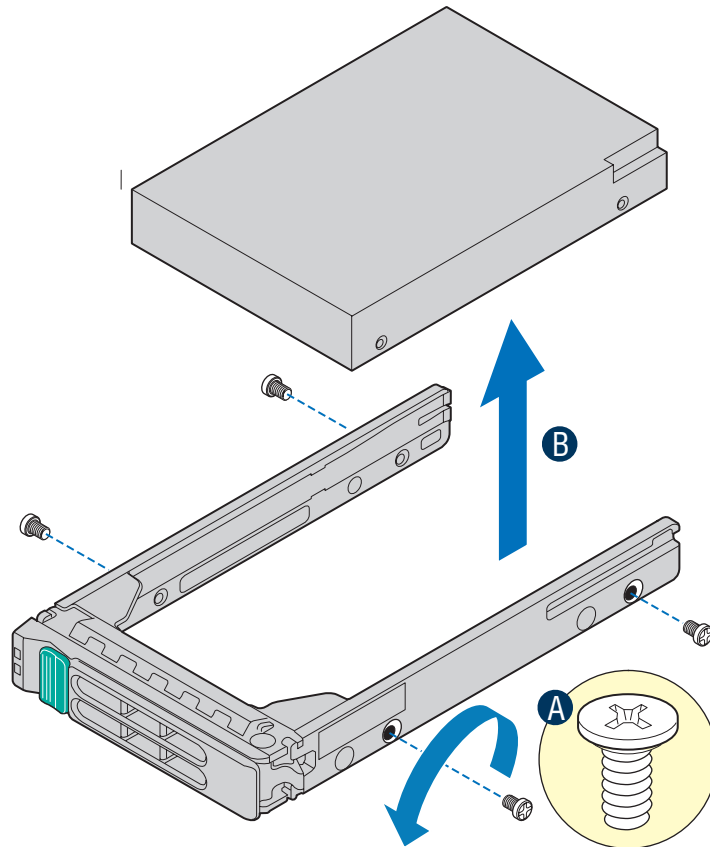
3. Press the retaining lever on the selected drive carrier to release the drive carrier from the drive bay module (see letter “A” in [Figure 30](#)). Remove the drive carrier from the drive bay module (see letter “B” in [Figure 30](#)).



AF002425

**Figure 30. Removing a 2.5-inch Drive Carrier from the Drive Bay Module**

4. With a Phillips screwdriver, remove the four screws securing the hard drive to the drive carrier (see letter “A” in [Figure 31](#)). Lift the hard drive from the carrier (see letter “B” in [Figure 31](#)) and store the hard drive in an anti-static container or bag.



AF002429

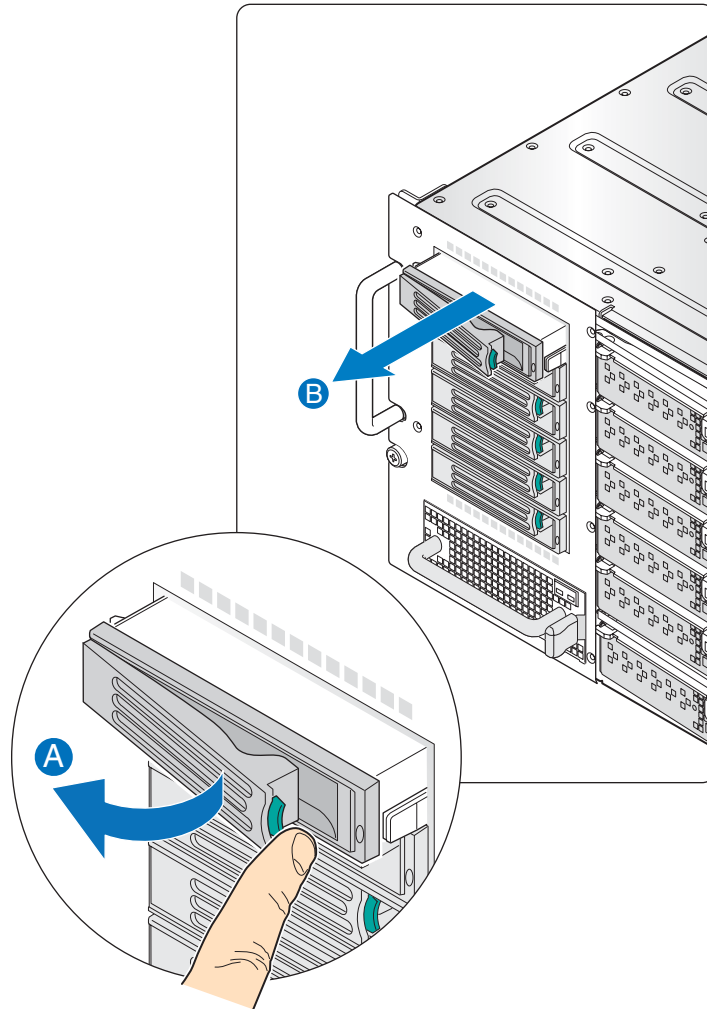
**Figure 31. Removing Hard Drive from a Drive Carrier**

5. Install either another hot-swap hard drive or a filler blank in the drive carrier.
6. Install the drive carrier into the empty drive bay module within two minutes; this step is required to maintain proper airflow throughout the chassis and to ensure proper system cooling.

## Installing a 3.5-inch Hard Drive into the Storage Bay

To install a 3.5-inch hard drive into the storage bay, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. Press the retaining lever on an available drive carrier to release the drive carrier from the drive bay module (see letter “A” in [Figure 32](#)). Remove the drive carrier from the drive bay module (see letter “B” in [Figure 32](#)).

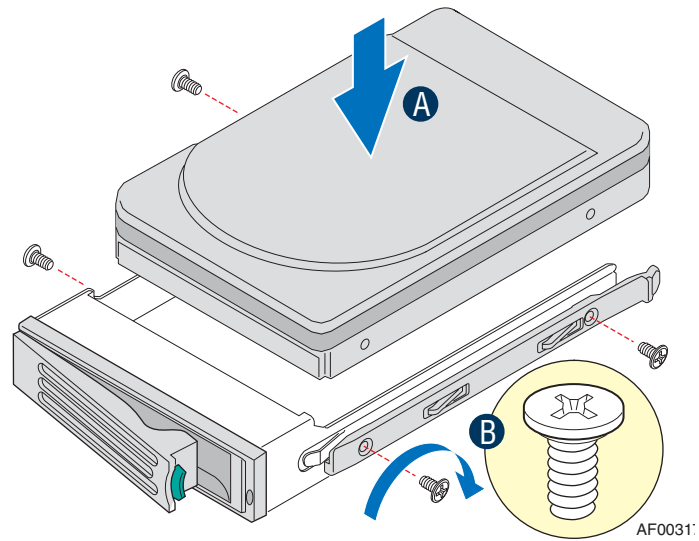


AF002662

### Figure 32. Removing a 3.5-inch Drive Carrier from the Drive Bay Module

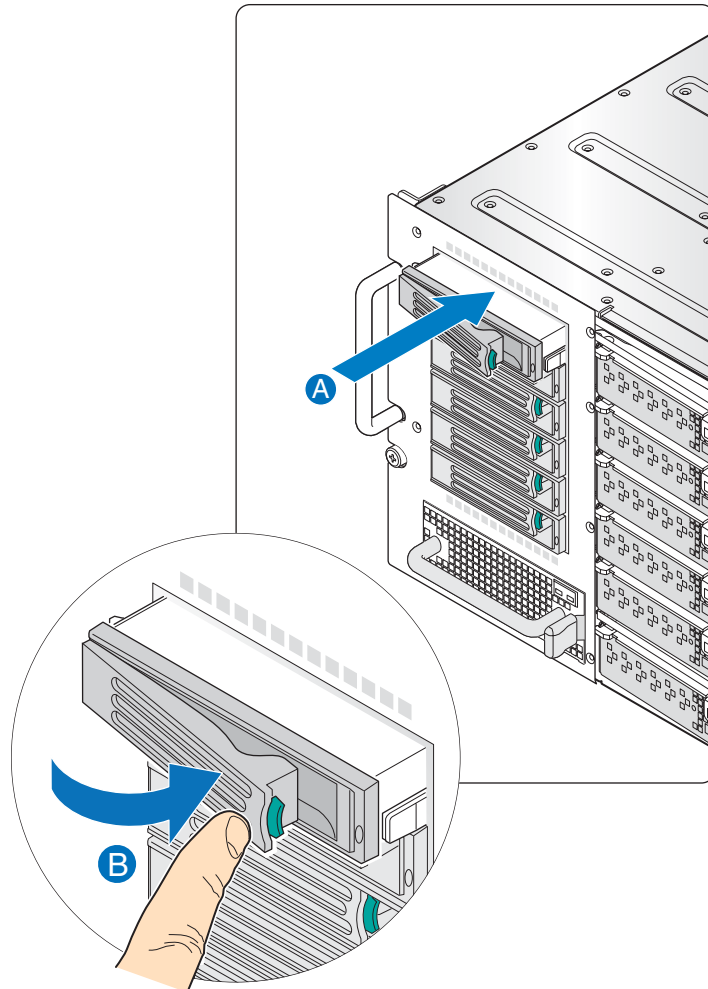
3. With a Phillips screwdriver, remove the four screws securing the filler panel to the drive carrier.

4. Align the holes in the hard drive to the holes in the drive carrier (see letter “A” in [Figure 33](#)) and attach it to the drive carrier using the four screws removed in the previous step (see letter “B” in [Figure 33](#)).



**Figure 33. Installing Hard Drive into Drive Carrier**

5. With the drive carrier retaining lever in the open position (see letter “A” in [Figure 34](#)), carefully slide the drive carrier into the drive bay module until it is fully seated and the retaining lever starts to engage. Press firmly to latch the retaining lever (see letter “B” in [Figure 34](#)).



AF002663

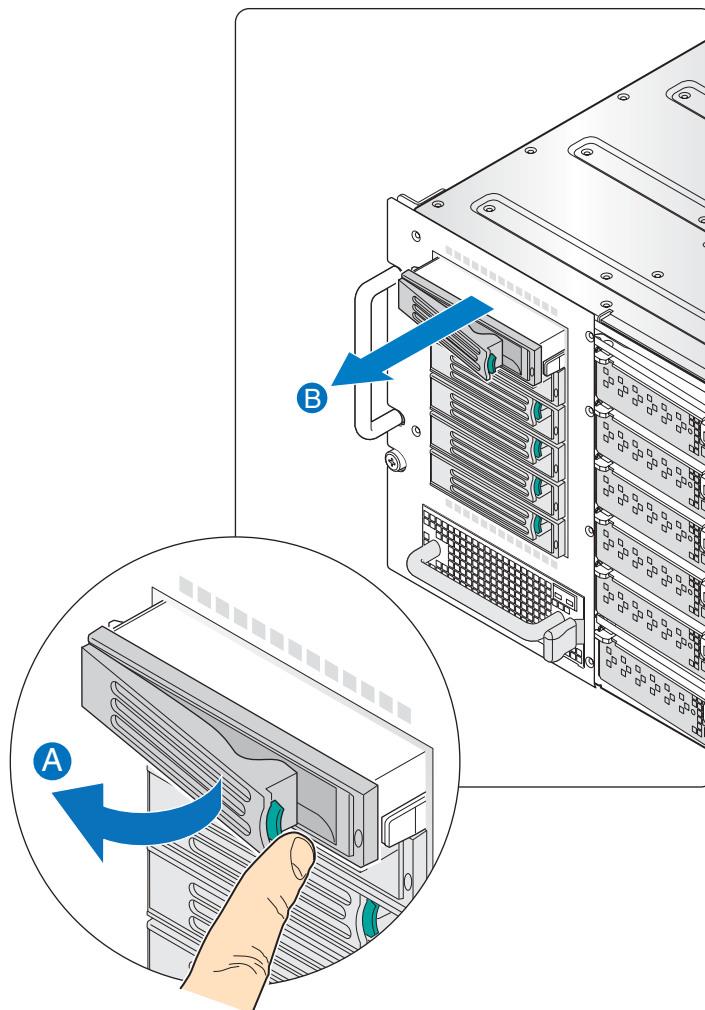
**Figure 34. Installing 3.5-inch Drive Carrier in Drive Bay Module**

## **Removing a 3.5-inch Hard Drive from the Storage Bay**

To remove a 3.5-inch hard drive from the storage bay, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. To avoid data corruption, ensure that the drive you intend to remove is not online and actively providing data storage to any of the installed compute modules.

3. Press the retaining lever on the selected drive carrier to release the drive carrier from the drive bay module (see letter “A” in [Figure 35](#)). Remove the drive carrier from the drive bay module (see letter “B” in [Figure 35](#)).

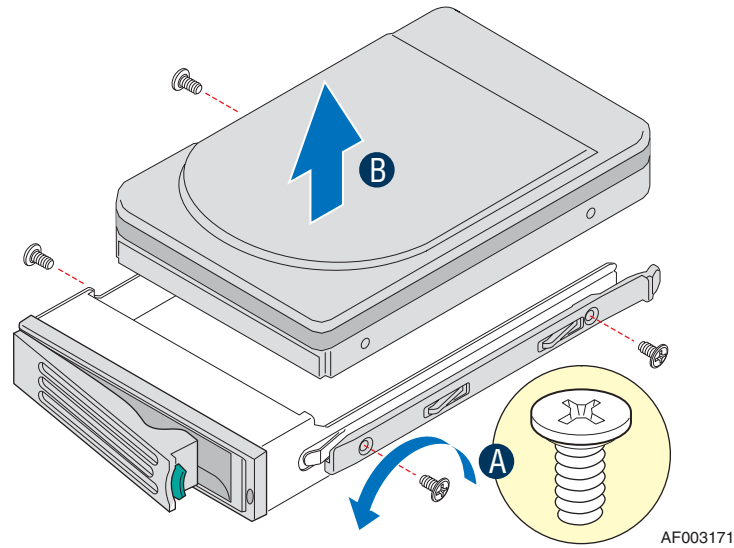


AF002662

**Figure 35. Removing a 3.5-inch Drive Carrier from the Drive Bay Module**



4. With a Phillips screwdriver, remove the four screws securing the hard drive to the drive carrier (see letter “A” in Figure 36). Lift the hard drive from the carrier (see letter “B” in Figure 36) and store the hard drive in an anti-static container or bag.



**Figure 36. Removing Hard Drive from a Drive Carrier**

5. Install either another hot-swap hard drive or a filler blank in the drive carrier.
6. Install the drive carrier into the empty drive bay module within two minutes; this step is required to maintain proper airflow throughout the chassis and to ensure proper system cooling.

# Installing and Removing an SGI Compute Module

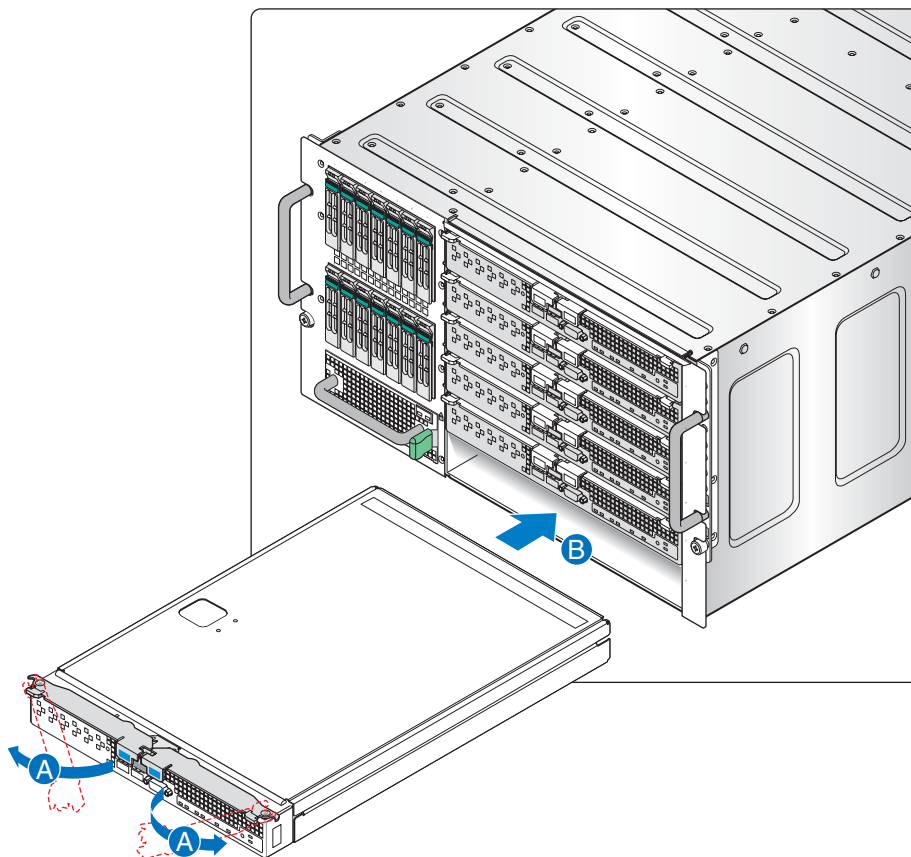
## Installing an SGI Compute Module

To install an SGI compute module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. If you have not done so already, install any necessary options, such as processor and memory, in the compute module.

**Note:** *The top cover is a required component of the compute module assembly. Do not attempt to insert a compute module into the chassis without ensuring an installed top cover is in place.*

3. Make sure the release handles on the compute module are in the open position (see letter “A” in [Figure 37](#)). Insert the compute module into an open slot in the chassis and slide it in until it stops (see letter “B” in [Figure 37](#)).



AF002431

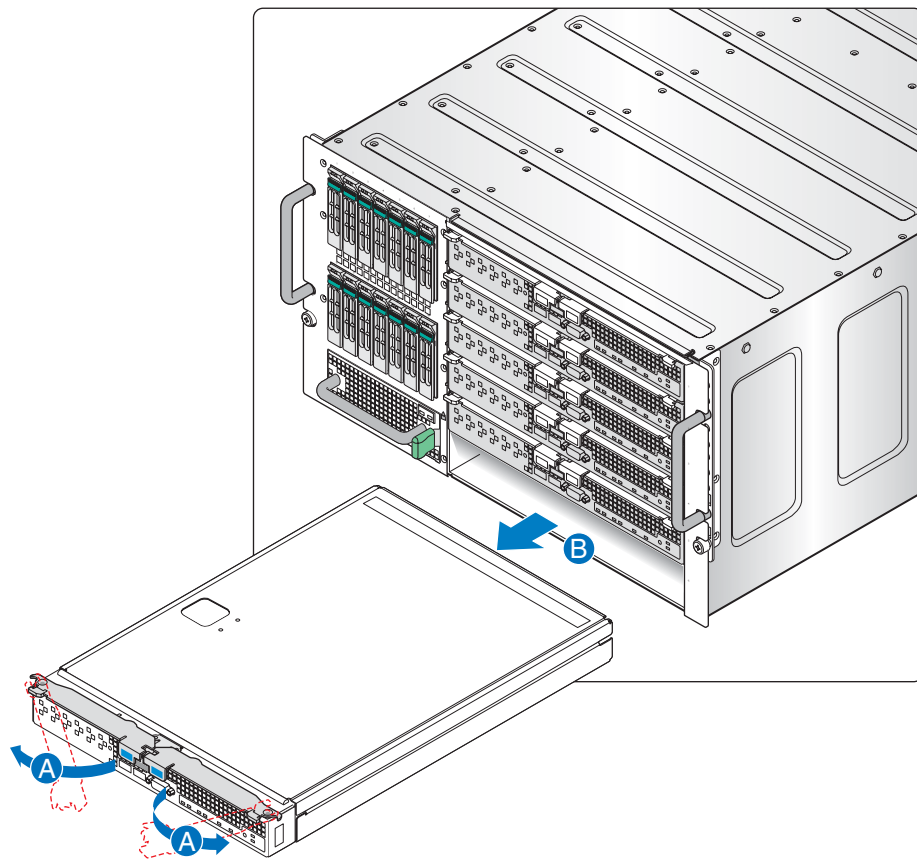
**Figure 37. Installing an SGI Compute Module**

4. Close the release handles on the front of the compute module.

## Removing an SGI Compute Module

To remove an SGI compute module, follow these steps:

1. Review the safety and ESD information at the beginning of this manual and in the appendices.
2. If the compute module is operating, shut down the operating system and power it down.
3. Open the two release handles at the front of the compute module (see letter “A” in [Figure 38](#)) and pull the compute module out of the server system (see letter “B” in [Figure 38](#)).



AF002432

**Figure 38. Removing an SGI Compute Module**

4. Place either a filler or another compute module in the bay within two minutes. This step is required to maintain proper airflow throughout the server system and to ensure proper system cooling.



# 3 Using the Origin 400 System

---

## Minimum Hardware Requirements

To successfully power up the Origin 400 system and to avoid integration difficulties and possible system damage, your Origin 400 system must meet the minimum hardware requirements listed in the following table.

**Table 4. Hardware Requirements**

Component	Quantity	Location
Ethernet switch module	1	Slot labeled SWM1
Storage control module	1	Slot labeled SCM1
Management module	1	Slot labeled CMM
Power supply module	1*	Power supply module bay 1
Power supply blank	3	Power supply module bays 2, 3 and 4
I/O cooling module	1	I/O cooling module bay
Main cooling module	2	Main cooling module bays 1 and 2
SGI compute module	1	Compute module slot 1
Compute module blanks	5	Compute module slots 2, 3, 4, 5, and 6

*Note:* \* Base 2.5-in drive enclosure and 3.5-in drive enclosure configurations include two power supply modules and two blank power supply fan modules

## Starting Up the Origin 400 System

The Origin 400 system does not have a power switch. When the chassis has at least one power supply with power cord plugged into an appropriate electrical outlet, standby power is available. With standby current, a user can remotely connect to the management module and/or power on a compute module. Each compute module has a front panel power switch.

## Installing an Operating System

Before installing an operating system, you must first configure storage and networking via the Origin 400 Management Center user interface.

One possible way to install an operating system is as follows:

1. Connect a remote client machine to the management module in the Origin 400 system via a cross-over cable.
2. Connect a USB hub to one of the USB ports to allow more than two USB devices to be used.
3. Connect a video monitor and USB mouse and keyboard to the front of the compute module using the USB hub.
4. Connect a USB CD-ROM/DVD-ROM drive to the compute module.
5. From the remote client machine, log into the management module and configure storage and (optionally) networking for the compute module.
6. Power on the CD-ROM/DVDROM drive and insert the operating system install media.
7. Power on the compute module and install the operating system.

For configuration details, see [“Using the Origin 400 Management Center” on page 53](#).

## Monitoring the System

The management module reports complete system health. From a remote client, an IT administrator can easily monitor the state of the server system. For more details, see [“Using the Origin 400 Management Center” on page 53](#).

## Shutting Down the System

To remove power from the Origin 400 system, you must first properly power down all compute modules. Next, disconnect all power cables from the power source.

# 4 Using the Origin 400 Management Center

---

This section provides an overview of the Origin 400 Management Center user interface, which provides complete system hardware management by enabling users to securely configure and monitor the system. The system is intended to be managed over a secure, private management network. It is recommended that the SGI management module not be connected to a publicly accessible network.

Full system management is only supported via the Origin 400 Management Center. In addition, administrators can access system-level information remotely via SNMP. For information regarding SNMP v2 and v3 support, refer to your SGI Technical Support representative.

This section covers the Origin 400 Management Center features and provides detailed instructions for configuring the Origin 400 system.

## Introduction

The SGI management module provides a simple and intuitive browser-based graphical user interface, referred to as the *Origin 400 Management Center*, that IT administrators can use to monitor and configure the Origin 400 system. No CDs or additional installation steps are required. To initially launch the user interface and configure the system hardware, a default static IP address and user account are provided. After logging into the Origin 400 Management Center, IT administrators can:

- Quickly access system and component information.
- Configure and manage storage subsystems, including but not limited to:
  - Create, delete and/or rename a storage pool
  - Create, delete, rename and/or reassign a virtual drive to a compute module
  - Create or delete hot spares
- Configure and manage switch modules, including but not limited to:
  - Assign internal and external ports to a virtual LAN (VLAN)
  - Configure external port settings
  - Launch an Advanced Configuration for additional switch configuration features
- Quickly view hardware inventory, system event logs, storage allocation and system configuration reports.
- Easily view current status for all hardware components (servers, hard drives, switch modules, storage control modules, management module, cooling modules, and power modules).

- Configure common settings, such as:
  - View and modify the IP address assigned to the management module.
  - Configure alert notification destinations and policies
  - Manage Origin 400 Management Center user accounts
  - Update system firmware

## System Configuration Requirements

This section provides an overview of the Origin 400 system configuration requirements. Specifically, you must complete each of the following requirements:

- Update system firmware (recommended):
 

Prior to configuring the Origin 400 system, it is recommended that you update the system firmware to the latest release. For more information regarding the firmware update process, see [“Steps to Update the System Firmware” on page 129](#).
- Install physical hard drives (required):
 

Physical hard drives must be present in the Origin 400 system before you can configure the Origin 400 system storage.
- Configure storage (required):
 

Configuring storage includes grouping installed physical hard drives into storage pools, creating virtual drives, and assigning the virtual drives to one or more compute modules. Storage configuration also includes creating and assigning hot spares to storage pools. For more information, see [“Storage Configuration” on page 68](#).
- Install at least one SGI compute module(required):
 

When configuring storage, a compute module does not need to be present in the system. Virtual drives can be assigned to a compute module slot/bay in the chassis regardless of whether or not a compute module is present. However, in order to install an operating system, you must first insert a compute module into the Origin 400 system.
- Modify the Origin 400 Management Center administrator account password (recommended):
 

For security reasons, it is recommended that you change the default administrator password once the system is configured. For more information, see [“User Accounts” on page 123](#).
- Modify the external IP address for the SGI management module (required):
 

This is the IP Address used to access the Origin 400 Management Center. Before installing the Origin 400 system on a network, change the external IP address and hostname as needed. You will need to change the management module default static IP address if more than one Origin 400 system is present on the network, or if the default management module IP address cannot be accessed in the installed network environment. For more information, see [“IP Configuration” on page 115](#).
- View Origin 400 system health and additional required actions (recommended):



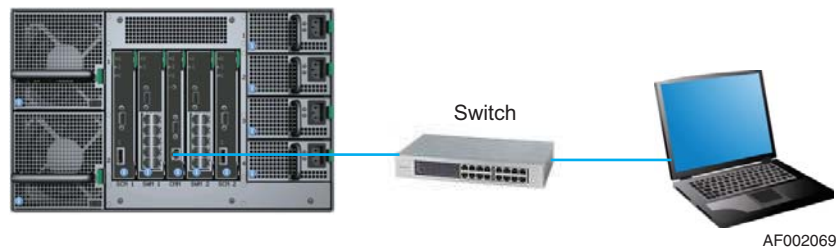
To ensure the Origin 400 system is functioning properly, it is recommended that you review the current health status for installed components and verify that all required actions are completed. The Dashboard provides an easy-to-use interface to quickly view all required actions, health status for all installed components, and information on all recent critical events. From the Dashboard, you can select any required action, component, or event to get detailed information. For more information, see [“Dashboard” on page 108](#).

## Setting Up a Remote Connection

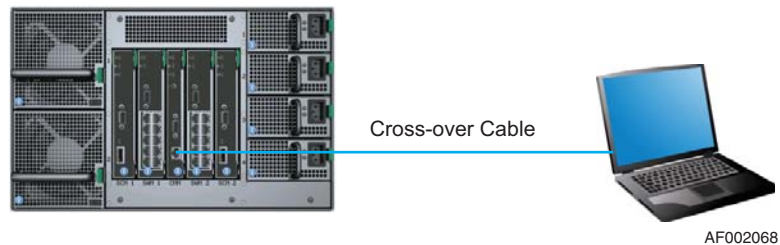
The Origin 400 system is intended to be managed over a secure, private management network. It is recommended that the SGI management module not be connected to a publicly accessible network.

The two recommended options for connecting a client system to the SGI management module in order to launch the Origin 400 Management Center are illustrated below. Before connecting the remote system, ensure all hardware components (servers, hard drives, switch modules, storage control modules, the management system module, cooling modules, and power modules) are installed in the Origin 400 system.

**Option 1:** Connect the client system and the SGI management module to an external switch using two Ethernet cables, as illustrated in the following image.



**Option 2:** Connect the client system directly to the SGI management module using a cross-over cable, as illustrated in the following image.



## Remote Client System Requirements

This section describes the minimum system requirements for a client computer that is accessing the Origin 400 Management Center user interface through a web browser.

**Table 5. Minimum System Requirements for Remote Web Console**

Requirement	Remote Web Consoles/Clients
Operating System	Any operating system that supports either the Microsoft Internet Explorer or Mozilla Firefox web browser.
Web Browser	Microsoft Internet Explorer 6 or 7 Mozilla Firefox version 2.0 or later
Browser Plug-ins	Adobe Flash Player Version 9 plug-in or later Java SE Runtime Environment 6 Update 1 or later
TCP/IP Network Stack	Yes

### Download Browser Plug-ins

Download the latest required Microsoft Internet Explorer and Mozilla Firefox plug-ins at:

- Adobe Flash Player: <http://www.adobe.com/products/flashplayer/>
- Java SE Runtime Environment 6, Update 1: <http://www.java.sun.com/javase/downloads/index.jsp>

## Log in to the Origin 400 Management Center

To launch the Origin 400 Management Center, open a browser session on the remote client system.

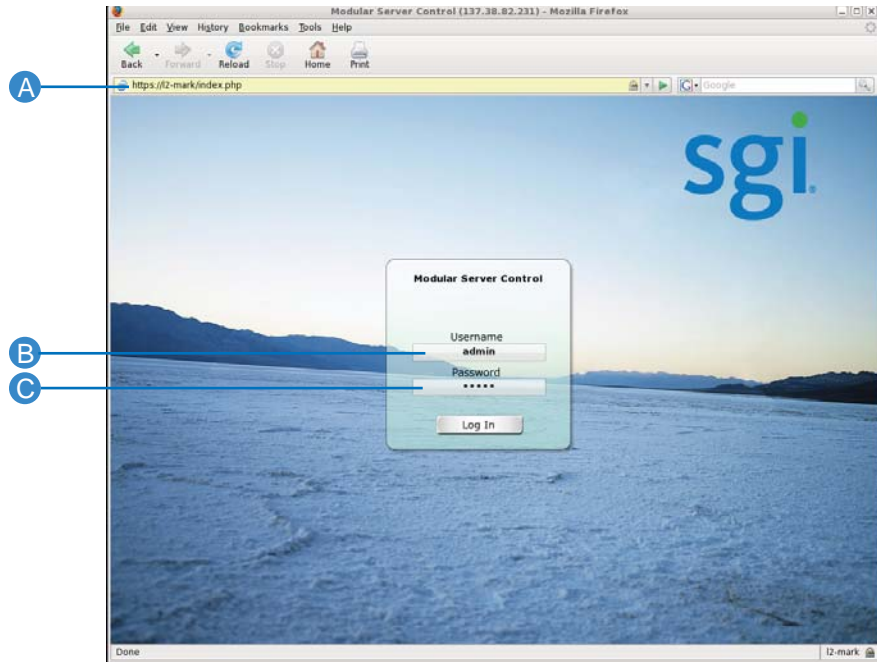
Enter the SGI management module default static IP address of 192.168.150.150 in the address bar of the web browser. The login screen (see [Figure 39](#)) is displayed.

An administrator user account is enabled for the system. This default administrator account provides access to all available management configuration settings and actions.

User Account information:

- Username: admin
- Password: admin

**Note:** Username and password are case sensitive.



AF002066

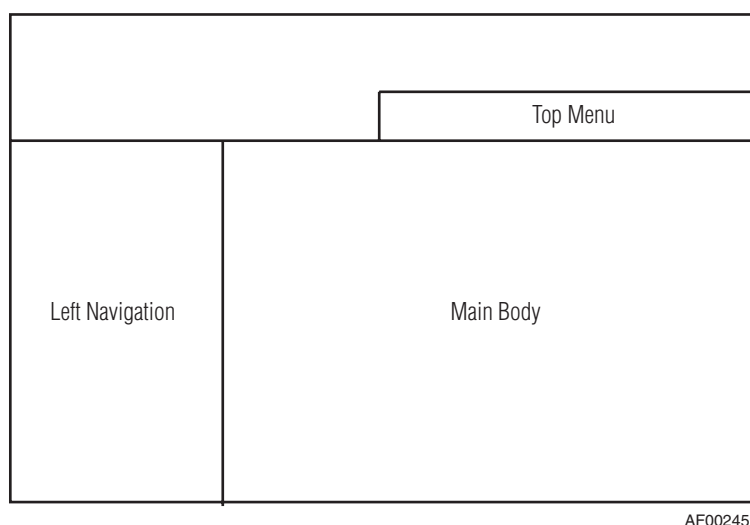
A	Enter Management Module IP Address, 192.168.150.150
B	Enter Default Username ( <i>admin</i> )
C	Enter Default Password ( <i>admin</i> )

**Figure 39. Origin 400 Management Center Login**

## Layout and Key Navigation Features

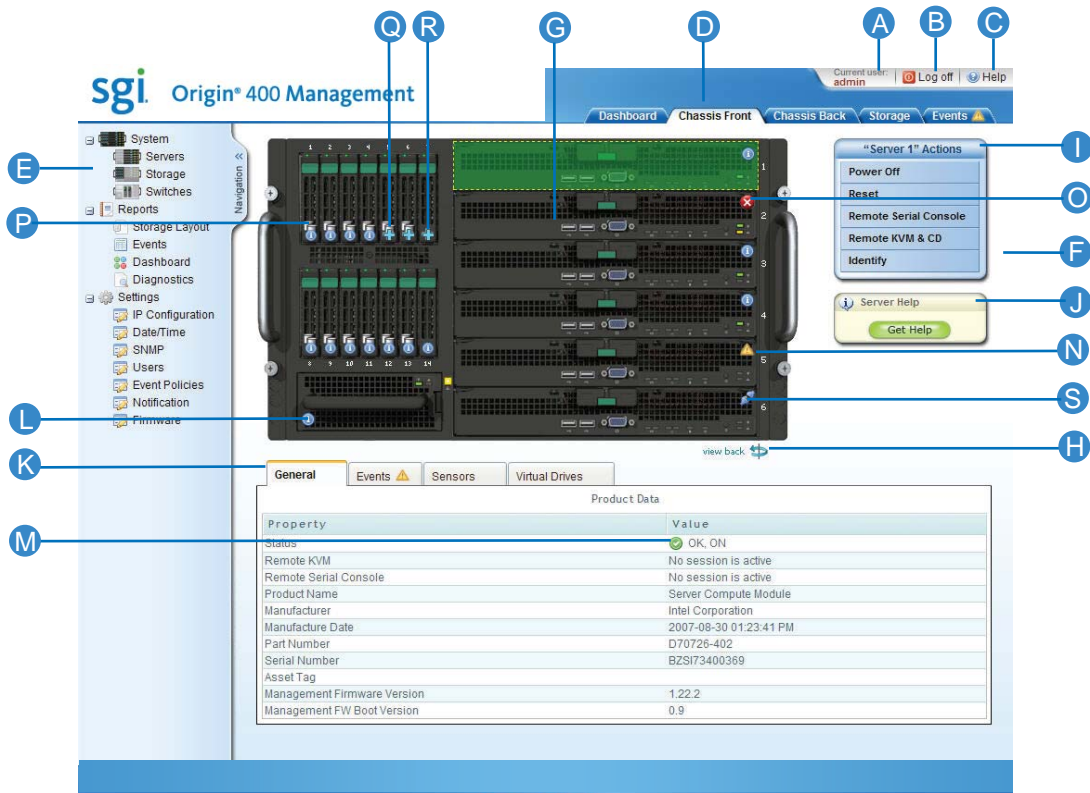
The Origin 400 Management Center interface simplifies system configuration and management through use of navigation and common layouts. The general screen layout consists of the following:

- **Top Menu:** This menu provides tabs for quick access to multiple system views. For more information regarding the top menu tabs, see [Table 6](#).
- **Left navigation panel:** This panel provides access to system configuration screens, reports, and general setting configuration screens. For more information regarding the menus in the left navigation panel, see [Table 6](#).
- **Main body:** This section provides the content for the selected view or screen. The system configuration screens are designed to present all available information and actions for a selected system component in the main body of the interface.



**Figure 40. Origin 400 Management Center General Layout**

Figure 6 illustrates the layout and types of information presented on the system configuration screens.















AF002067

Figure 41. Origin 400 Management Center Configuration Screen Layout

**Table 6. Origin 400 Management Center Configuration Screen Layout**

	Item	Description
<b>General Navigation</b>		
A	Current User	Displays username for the currently logged in user.
B	Logoff	Ends current session and returns to Login screen.
C	Help	Origin 400 Management Center help
D	Top Menu Tabs	<p>Quickly switches between key sections of the Origin 400 Management Center. In particular, the following tabs are provided:</p> <ul style="list-style-type: none"> <li>• <b>Dashboard:</b> This tab is displayed by default after logging into the Origin 400 Management Center. It provides a snapshot view of the overall system and component health, and also lists all the required actions and critical events. This screen can also be accessed from the left navigation panel by clicking Reports &gt; Dashboard. For more information, see <a href="#">“Dashboard” on page 108</a>.</li> <li>• <b>Chassis Front:</b> This tab provides an accurate visual view of the front of the chassis, which can be used to view the current health and determine the availability of each component. For more information, see <a href="#">“Chassis Front” on page 62</a>.</li> <li>• <b>Chassis Back:</b> This tab provides an accurate visual view of the back of the chassis, which can be used to view the current health and determine the availability of each rear component. For more information, see <a href="#">“SGI Gigabit Ethernet Switch Module 1 and 2” on page 88</a>.</li> <li>• <b>Storage:</b> This tab provides access to the Storage Configuration screen, which can be used to quickly group drives, create and assign virtual drives to servers, assign hot-spare drives, and also view system health, status, and product details. This screen can also be accessed from the left navigation panel by clicking System &gt; Storage. For more information, see <a href="#">“Storage Configuration” on page 68</a>.</li> <li>• <b>Events:</b> This tab provides access to the Events screen, which can be used to quickly view and acknowledge new events for all system components in a single location. This screen can also be accessed from the left navigation panel by clicking Reports &gt; Events. For more information, see <a href="#">“Events” on page 106</a>.</li> </ul>
E	Left Navigation Panel	<p>The left navigation panel contains links to the following main menus:</p> <ul style="list-style-type: none"> <li>• <b>System:</b> This menu provides direct links to configure and manage individual hardware components. For detailed information on the System menu and the submenus available under the System menu, see <a href="#">“System” on page 63</a>.</li> <li>• <b>Reports:</b> This menu provides access to various reports. For detailed information on the Reports menu and the submenus available under the Reports menu, see <a href="#">“Reports” on page 103</a></li> <li>• <b>Settings:</b> This menu provides access to general configuration settings. For detailed information on the Settings menu and the submenus available under the Settings menu, see <a href="#">“Settings” on page 113</a>.</li> </ul>
F	Main Body	Displays content for the selected menu item or view. For the system items, the main body is divided into four panes: the system graphic, action menu, context-sensitive help, and informational tabs.
<b>System Screen Layout</b>		
G	System Graphic	Interactive visual representation of the current state of the system hardware. By selecting a system component from the chassis graphic, the content changes in the main body to display all available actions and information for the selected component.

	<b>Item</b>	<b>Description</b>
H	Change Chassis View	Switches between the front and back views of the system chassis.
	 	Switches the chassis view from back to front.  Switches the chassis view from front to back.
I	Action Menu	Displays all available actions for the selected chassis component.
J	Context-Sensitive Help	Quick tips and links to context-sensitive help for the selected component.
K	Informational Tabs	Displays detailed information, including, but not limited to, current status, configuration and events for the selected component.
<b>Component Health and State Icons</b>		
L		Information Icon – hover over icon to view component summary information.
M		Health Icon - health OK
N		Health Icon – warning; hover over icon to view component summary information.
O		Health Icon – critical; hover over icon to view component summary information.
P		Storage Pool - indicates drive is included in an existing storage pool.
Q		Dedicated Hot Spare Icon - indicates hard drives that have been designated as designated hot spares to specific storage pools. Hover over icon to view component summary information.
R		Global Hot Spare Icon – indicates hard drives that have been designated as global hot spares. Hover over icon to view component summary information.
S		Server is powered off.
		Ready for Transport

	Item	Description
		Transitioning – Indicates either a firmware update or other background activity is in progress

## Chassis Front

The Chassis Front view provides an accurate visual view of the front of the chassis, which includes all compute modules, hard drives and the I/O fan. This real-time view enables an IT administrator to select the component of interest, quickly view the current health, and also determine which components are present or not present. The icons present on each component indicate the current health and provide additional information regarding power state and role. By hovering over the component icon, a brief summary of the current health, state and component description is displayed in a pop-up box.

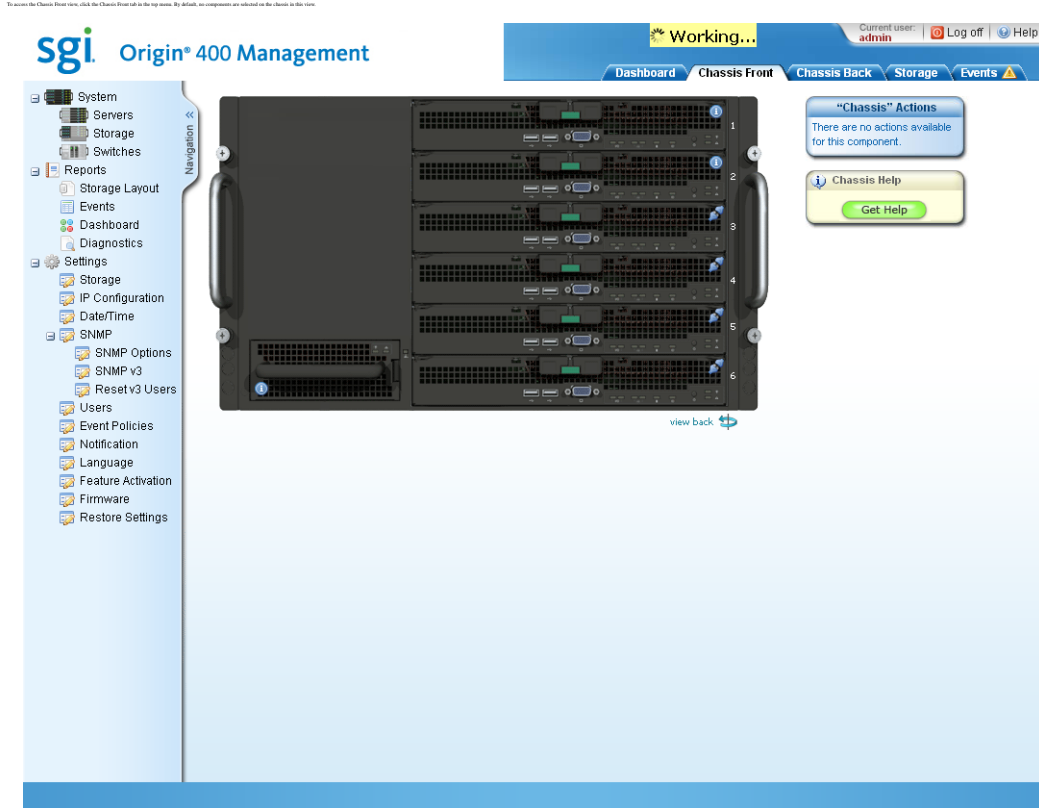


Figure 42. Chassis Front View



# System

The System menu in the left navigation panel enables IT administrators to quickly configure and view the most commonly accessed components (compute modules, storage control modules, and switch modules). When a system component is selected, the content in the action box, help box and informational tabs change to reflect the current actions and information for the selected component.

## Compute Module View

The Origin 400 system supports up to six SGI compute modules. To maintain the proper cooling within the Origin 400 system, all empty bays must be populated with the appropriate filler panels.

The Origin 400 Management Center enables an IT administrator to remotely power-cycle compute modules, launch a remote KVM (keyboard, video and mouse) session, and view health information and product details. To view the current status, available actions, and product details for an installed compute module, either click System > Servers in the left navigation panel or click the Chassis Front tab in the top menu to display the front of the system and select the specific compute module from the system graphic. The content displayed on the informational tabs, action box, and help box will be updated with product-specific information and actions available for the selected compute module highlighted in green. The current health and product summary information is quickly available by moving the mouse over the Health/Information icon located on the selected compute module.

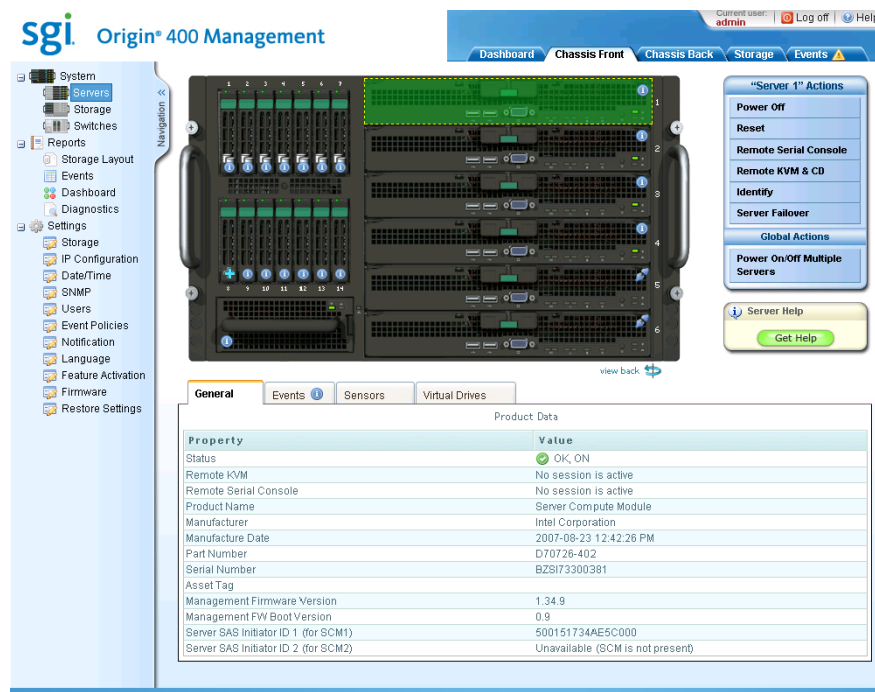








Figure 43. SGI Compute Module View

The following information and actions are available for a selected server.

## Health Icons

The health icons are displayed on the graphical representation of the component when the component is selected.

**Table 7. Health Icons**

Health Icon	Meaning
	Critical (For details, see the Event Log. For information about accessing the Event Log, see <a href="#">“Events” on page 106.</a> )
	Warning (For details, see the Event Log. For information about accessing the Event Log, see <a href="#">“Events” on page 106.</a> )
	Information
	OK
	Powered Off
	Firmware update or other background activity

## SGI Compute Module Actions

The actions available for a selected server are displayed to the right of the system graphic. For a description of these actions, refer to the following table.

**Table 8. Server Action Menu**

Action Menu Item	Description
Power On (if Off)	Allows the user to remotely power on the selected server.

**Table 8. Server Action Menu**

Action Menu Item	Description
Power Off (if On)	<p>Allows the user to remotely power off the selected server. The following two options are presented in a pop-up menu when Power Off is selected:</p> <ul style="list-style-type: none"> <li>• <b>Graceful:</b> Ends the current operating system session on the selected server before powering off the server.</li> <li>• <b>Forced:</b> Bypasses the shutdown of the operating system and immediately powers down the server.</li> </ul> <p><b>CAUTION:</b> A “Forced” Power Off could result in a loss of data and/or damage to the server. It is highly recommended to use the “Graceful” option under normal circumstances.</p>
Reset	<p>Allows the user to remotely reset the selected server. This action has the same effect as pressing the front panel reset button.</p> <p><b>CAUTION:</b> This may cause data loss on the server. Use the Graceful Shutdown to shut down applications and the operating system.</p>
Remote Serial Console	<p>Opens a new window that includes instructions on how to connect to the server’s remote serial port using a secure shell (SSH) client application. The serial port, if enabled in BIOS enables you to view server startup messages, enter the BIOS Setup (use &lt;Escape&gt;+2 key sequence), view OS initialization messages and interact with an application or OS that makes use of the serial port.</p>
Remote KVM & CD	<p>Opens a new window, allowing an IT administrator to use remote keyboard, video, and mouse (KVM) and media to monitor and manage the selected server remotely. The KVM functionality allows you to view server startup messages, enter the BIOS setup, and interact with the server operating system. The remote CD capability allows you to share a CD drive or CD image on your client machine with the remote server.</p>
Terminate KVM Session	<p>Sends a message to the KVM session user and terminates the KVM session.</p>
Identify	<p>Illuminates the server ID LED, which enables easy onsite identification of a selected server.</p>
Server Failover	<p>Rapidly reassigns all virtual drives from the currently assigned server slot to another server slot. As an example, this may be required when a server encounters hardware problems.</p> <p><b>Note:</b> All drive positions are preserved during this operation.</p>
Global Action Menu Item	Description
Power On/Off Multiple Servers	<p>Enables an IT administrator to power on or off multiple servers at once. Select the type of action first (power on, power off, reset). Then select the servers to apply the action.</p> <p><b>CAUTION:</b> To avoid potential data loss when selecting power off, the Graceful Shutdown option is recommended to shut down applications and the operating system.</p>

## SGI Compute Module Details

The tabs displayed below the system graphic provide detailed information on the selected server. For a description of these tabs, refer to the following table.

**Table 9. Server Tabs**

Tab Heading	Description
General	Displays: <ul style="list-style-type: none"><li>• Current status of the selected server (i.e., health, power state, etc.)</li><li>• Product data information (i.e., manufacturer, model number, serial number, firmware versions, etc.)</li></ul>
Events	Displays all system events for the selected server.
Sensors	Displays current sensor information.
Virtual Drives	Displays a detailed table of all virtual drives assigned to the selected server. The table provides the following details: Name, Size, RAID Level, Status, Drive Number and Assigned Server.

## SGI Compute Module Help

To quickly access additional help regarding the SGI compute module screen, actions, and tabs, click the Get Help button in the Server help box located under Actions.

## Remote KVM & CD

The remote KVM & CD feature can be used to connect a remote text-based or graphical console to any of the compute modules. This feature supports remote keyboard, video, mouse, and CD drive. This may be used, for example, to load an operating system.

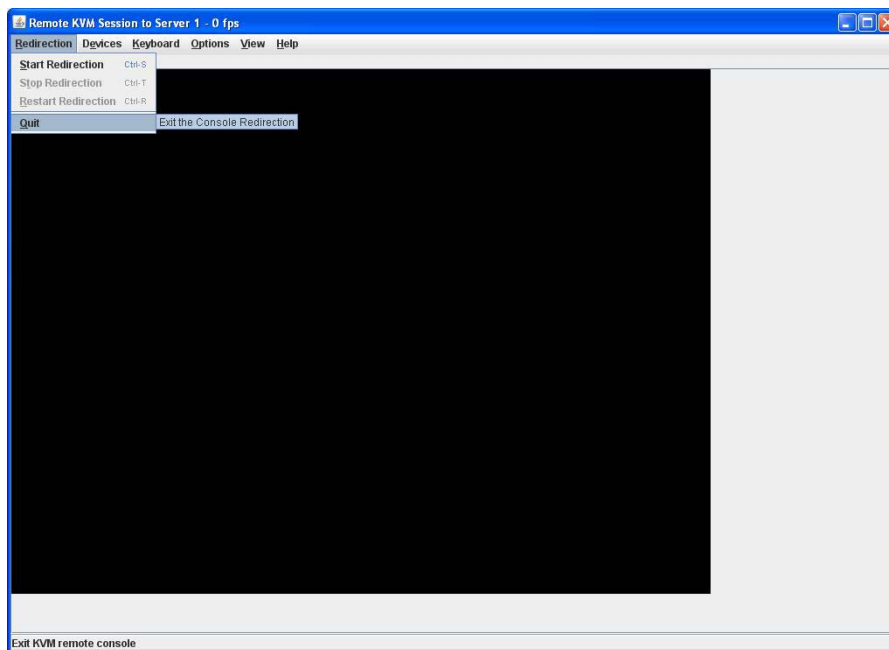
### Steps to Launch the Remote KVM Console

1. Click System > Servers in the left navigation panel.
2. Select the target compute module server.

A compute module must be present in the system to start a remote KVM & CD session.
3. If the server is off, click Power On on the Actions menu and click Apply to confirm the action.
4. Click Remote KVM & CD to start a KVM Remote Console.
5. In the dialog box that appears, complete the following:
  - a. Select Video display color resolution: High resolution for 65,536 colors, or Low resolution for 125 colors. Choose the lower color depth if you are experiencing network or performance problems on the client computer.
  - b. Select Mouse Mode. Choose Absolute if the remote server is running the Microsoft Windows operating system. Choose Relative if the remote server is running the Linux operating system.

- c. If you selected the Relative Mouse Mode, enter the Mouse Acceleration and Threshold values. These values must match the settings on your remote server.
  - d. Click Apply to start a Remote Keyboard, Video, Mouse (KVM) with CD redirection on the target server.
6. Accept all the dialog boxes that appear to open the KVM session in a new window.

The following KVM window is displayed.



**Figure 44. Server Action - Remote KVM & CD**

7. Select Start Redirection from the Redirection menu.  
If the option is grayed out, then the session has been automatically started.
8. To install an application from a CD, insert the CD into the remote console's CD-ROM drive and select CD from the Devices menu.

## Storage Configuration

The Origin 400 2.5-in drive enclosure supports up to 14 2.5-inch SAS drives and the 3.5-in drive enclosure supports up to six 3.5-inch SAS/SATA drives. These drives are shared between all compute modules. The physical disk drives are not directly connected to the compute modules. To assign storage to a compute module, a storage pool must be created first. Once a storage pool is created, a virtual drive can be created and assigned to one or more compute modules. This process is referred to as *storage configuration*. The Origin 400 Management Center is used to configure storage for the Origin 400 system. Storage configuration involves the creation and management of storage pools, virtual drives, and hot spares. This includes assigning virtual drives to one or more compute modules.

This section provides information on creating an initial storage pool, creating an initial virtual drive and mapping the virtual drive to a compute module using the Origin 400 Management Center. Once a virtual drive is mapped to a compute module, an operating system can be installed.

To access the storage configuration screen, either click the top menu Storage tab or click System > Storage in the left navigation panel.

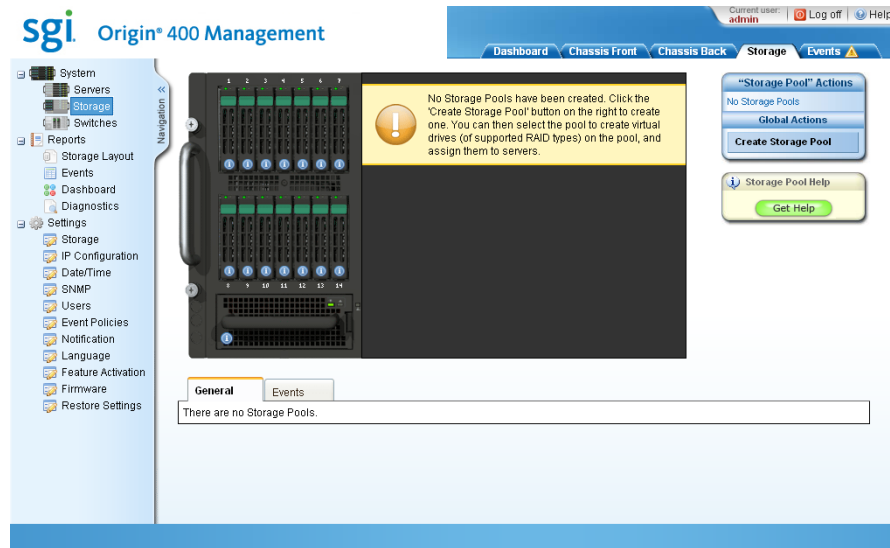
### Creating a Storage Pool

The initial storage configuration step is to create a storage pool or grouping of physical disk drives. Once a storage pool is created, virtual drives can be created within the storage pool and assigned to a compute module.

#### Steps to create a storage pool

1. To configure storage, click the top menu Storage tab or click System > Storage in the left navigation panel.

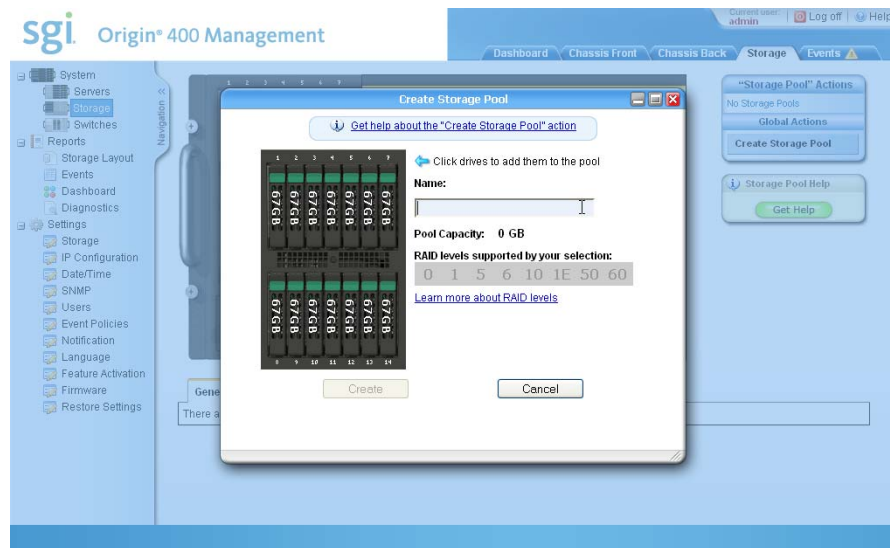
When the storage configuration screen is displayed for the first time, no storage pools or virtual drives are present. The storage screen looks similar to the following image.



**Figure 45. Initial Storage Configuration Screen**

2. To assign one or more drives to a storage pool, click **Create Storage Pool** on the Storage Pool Actions menu.

The following dialog box appears.



**Figure 46. Create Storage Pool Dialog Box**

3. Enter a name or label for the storage pool.
4. Select the physical hard drives that are to be grouped together to create a single storage pool.

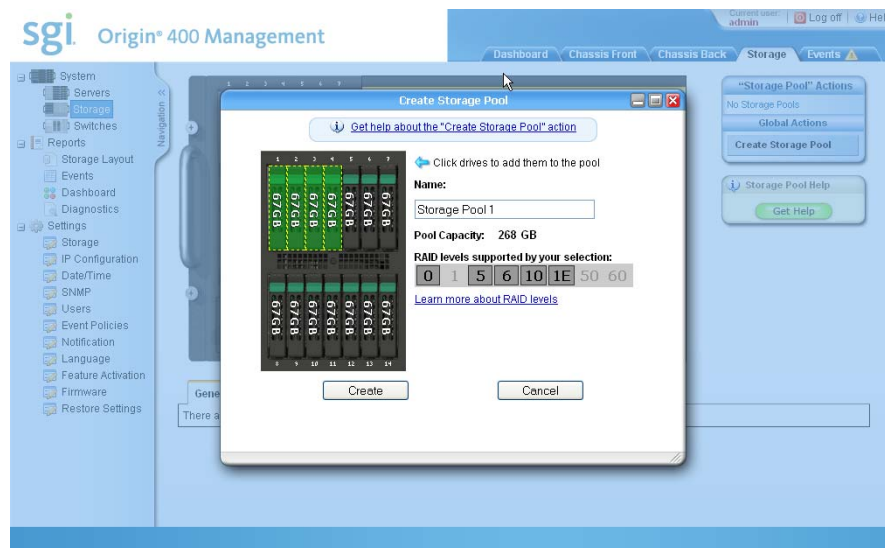
If a hard drive is available, the drive size is displayed. Selected drives are highlighted in green with the drive size displayed on each of the drives. Hard drives that are either included in an existing storage pool or configured as a hot-spare drive cannot be selected on this screen and are considered unavailable. Unavailable drives are displayed as darker than the available hard drives and do not have the drive size displayed on the image. The highlighted drive carriers identify the physical hard drives that have been selected for the storage pool. In this example (see [Figure 47](#)), drives 1, 2, 3, and 4 are selected.

5. Verify that the overall storage pool capacity and available RAID level options supported by the number of physical drives selected meets your storage requirements.

The Pool Capacity displays the total available storage space for the new storage pool. In [Figure 47](#), four 67-GB hard drives are selected to be grouped together to create a single storage pool with a Pool Capacity of 268 GB.

The RAID level options are determined based on the number of hard drives selected for the storage pool. In [Figure 47](#), four hard drives are selected. The RAID levels supported by grouping hard drives 1, 2, 3, and 4 together as a single storage pool are: 0, 5, 6, 10, and 1E. RAID levels that are not available are displayed in light gray text. In this example, RAID levels 1, 50, and 60 are grayed out. It is important to note that the RAID level is not assigned to a storage pool. Instead, it is assigned to the virtual drives within a storage pool. This enables a single storage pool to support many virtual drives with different RAID levels.



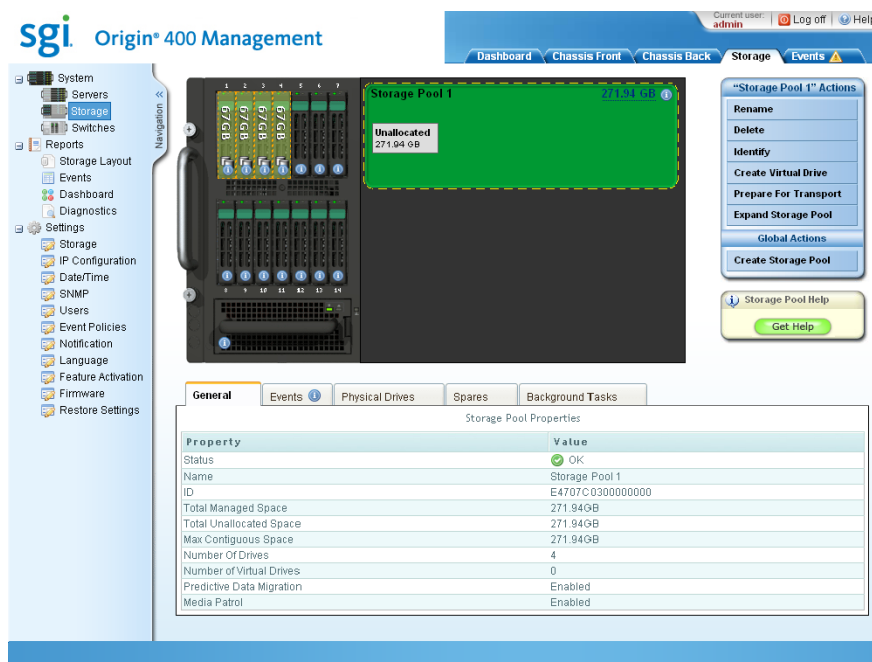


**Figure 47. Create Storage Pool Dialog Box Example**

6. Click Create to create the new storage pool.

Once a storage pool has been created, the Storage screen changes to highlight the newly created storage pool. The action box, help box, and informational tabs update to provide all available actions and information for the selected storage pool. Current health and product summary is quickly available by moving the mouse over the Health/Information icon located on the selected storage pool.

The following image displays information for the storage pool.







**Figure 48. Storage Pool Screen**

## Health Icons

The health icons are displayed on the graphical representation of the component when the component is selected.

**Table 10. Health Icons**

Health Icon	Meaning
	Critical (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Warning (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Information
	OK

You may see one of the following health status descriptions as you move the mouse cursor over the storage pool icon or the status health icon on the General tab:

- **Incomplete:** The Storage Pool is missing one or more physical disk drives. This can occur if the drives in a Storage Pool are transported to another system, but not all the drives are inserted. You can insert the missing drives, or choose to accept the incomplete status when prompted.
- **Media Patrol Running:** The storage pool is operational and the media patrol background task is running (this is a background task that looks for defects).
- **Rebuilding:** The storage pool is rebuilding as a background task.
- **Migrating:** The storage pool has a background task that is expanding the storage pool or one of the virtual drives.
- **Transitioning:** The storage pool is running a background task that is rebuilding the storage pool to another drive using a hot spare.
- **Predictive Data Migration Running:** An error detection background task is running.
- **Degraded:** One or more physical disk drives in the storage pool are offline and the storage pool is operating in a degraded mode.
- **Offline:** All the physical disk drives are offline.
- **Transport Ready:** All the physical disk drives are prepared for transport and can now be removed from the system.

## Storage Pool Actions

The Storage Pool Actions displayed to the right of the system graphic enable an IT administrator to modify existing storage pools, remotely identify drives contained in a storage pool and create virtual drives. For a complete list of actions, refer to the following table.

**Table 11. Storage Pool Actions Menu**

<b>Global Action Menu Item</b>	<b>Description</b>
Create Storage Pool	Designates one or more drives as a storage pool. Global storage actions are available at all times on the storage screen.
<b>Selected Storage Pool Action Menu Items</b>	<b>Description</b>
Rename	Renames an existing storage pool. A dialog box will be displayed prompting the user for the new storage pool name.
Delete	Deletes an existing storage pool. This action will delete all virtual drives contained in the selected storage pool and release the drives for future storage pool configuration.  ALL DATA WILL BE LOST.
Identify	Illuminates the hard drive ID LED, which enables easy onsite identification of the drives included in the selected storage pool.
Create Virtual Drive	A virtual drive is assigned a name, RAID level, size and server. Once a virtual drive is created, an operating system can be installed.

**Table 11. Storage Pool Actions Menu**

<b>Global Action Menu Item</b>	<b>Description</b>
Expand Storage Pool	Allows the user to add one or more physical drives to an existing storage pool to increase available space.
Prepare for Transport	Prepares drives for removal from system.
Accept Incomplete State	Enables an IT administrator to accept a condition where the storage pool has fewer physical drives than it requires. The incomplete state occurs when some but not all physical drives belonging to a storage pool have been transported to a new system.  <b>NOTE:</b> Virtual drives in an incomplete storage pool can be recovered by rebuilding the storage pool after you accept the incomplete state only if the RAID level of the virtual drive allows it to handle the loss of the number of drives that are missing from the storage pool.
Start Rebuild	This action is available if a physical drive in a storage pool has failed and needs to be recovered by rebuilding with the hot-spare drive.

### Storage Pool Details

The tabs displayed below the system graphic provide detailed information on the selected storage pool. For a description of these tabs, refer to the following table.

**Table 12. Storage Pool Tabs**

<b>Tab Heading</b>	<b>Description</b>
General	Displays: <ul style="list-style-type: none"><li>• Current status of the storage pool (i.e., status, health, operation state)</li><li>• Storage pool configuration data (i.e., storage pool ID, name, total managed space, total unallocated space, number of physical and virtual drives included in the selected storage pool)</li></ul>
Events	Displays all system events for the selected storage pool.
Physical Drives	Displays a table with detailed information on the physical drives included in the selected storage pool (i.e., Drive number, Manufacturer, Product ID, Serial Number, Firmware Revision, Size, Status).
Virtual Drives	Displays a table with detailed information on all virtual drives contained within the selected storage pool. The table provides the following details: Name, Size, RAID Level, Status, Drive Number, and Assigned Server.
Spares	Displays a table with detailed information on all hot-spare drives. The table includes the following information: Drive Number, Role (Global versus Dedicated), Manufacturer, Product ID, Serial Number, Firmware Revision, Size and Status.
Background Tasks	Displays status and state of current tasks, such as Predictive Data Migrations and Media Patrol.

## Storage Pool Help

To quickly access additional help regarding the storage pool screen, actions, and tabs, click on the Get Help button in the Storage Pool help box located under the actions.

## Creating a Virtual Drive

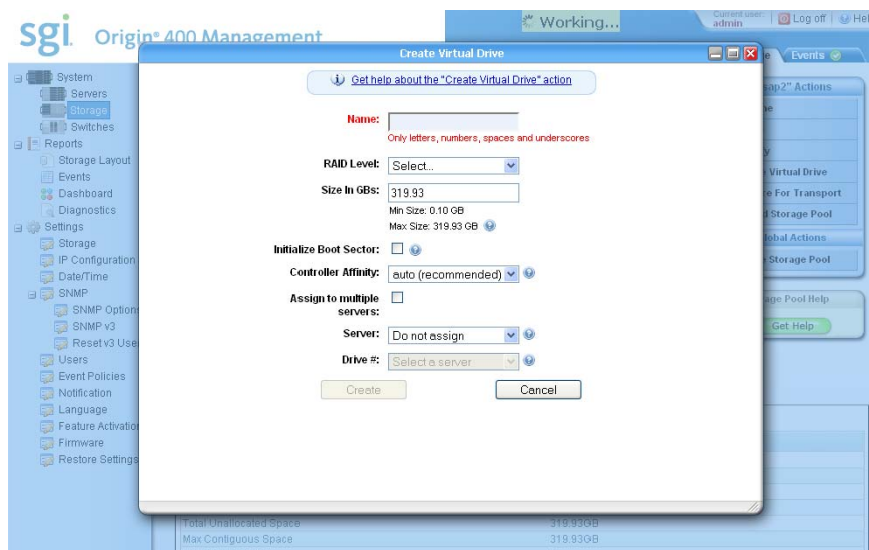
Once a storage pool has been created, the next step is to create a virtual drive. Virtual drives are created in the storage pools and assigned to individual Server Compute Modules. The following are the key benefits of virtual drives:

- Virtual drives can be quickly reassigned to different servers with a couple of mouse clicks in the Origin 400 Management Center without powering down the server or storage pool.
- Virtual drives in a single storage pool can be set to any RAID level that is supported by the selected storage pool.
- You can quickly and easily expand the size of a virtual drive to increase storage capacity.
- The assigned server's operating system will detect the virtual drive (and its associated drive position) during the boot process. Drive position 0 is the boot device. To the operating system, the virtual drive will be indistinguishable from the local physical drive on the server (if installed).
- If the SGI Shared LUN feature is activated and the operating system supports sharing LUNs, a virtual drive can be assigned to two or more servers.

The steps to create a virtual drive are as follows:

1. Select the existing storage pool, which will contain the virtual drive.
2. Select **Create Virtual Drive** from the storage pool action menu.

The following dialog box is displayed.



**Figure 49. Create Virtual Drive Dialog Box**

3. Enter a name for the virtual drive.
4. Select the RAID level for the virtual drive from the drop-down box.

The options available in the drop-down box are determined by the number of drives in the selected storage pool.

5. Enter the size for the virtual drive.

Depending on the RAID level selected, the maximum size displayed may change (i.e., if mirroring is selected).

6. Select the Initialize Boot Sector check box if an operating system will be installed on this virtual drive.

This will ensure a fresh volume for partitioning.

7. In the Controller Affinity list, select the preferred storage control module to handle requests for the virtual drive.

By default, this option is set to “auto (recommended)” but can be changed to either SGI storage control module 1 (SCM1) or storage control module 2 (SCM2). By selecting “auto (recommended)”, the system assigns a storage control module for the virtual drive.

8. Assign or map the virtual drive to a server.

A virtual drive can be assigned to any of the six server slots. A server does not have to be present in the Origin 400 system for selection. This enables an IT administrator to assign virtual drives to servers that will be added to the system.

If the SGI Shared LUN feature is activated, the “Assign to multiple servers” check box is displayed. When the check box is selected, the Shared LUN feature allows a virtual drive to be assigned to two or more servers. This feature requires operating system support for sharing LUNs.

9. Select the “Drive Position” for the virtual drive.

The drive position sets the drive number for this server. The drop-down box will show all available drive numbers (0 through 127).

10. Click Apply to create the virtual drive and return to the main Storage screen.

The virtual drive created will be displayed as a volume in the selected storage pool on the main storage screen. Depending on the RAID level selected, the virtual drive may continue to synchronize after it is created and displayed on the storage screen.

11. To view current status of the virtual drive, select the General, Virtual Drive or Background Tasks tab to view more information about the virtual drive created.

Once a virtual drive is created and selected, the action menu and tabs change to display all available actions and details for the selected virtual drive. The following image shows the storage screen with a virtual drive selected.








**Figure 50. Virtual Drive Screen**

## Health Icons

The health icons are displayed on the graphical representation of the component when the component is selected.

**Table 13. Health Icons**

Health Icon	Meaning
	Critical (For details, see the Event Log. For information about accessing the Event Log, see <a href="#">“Events” on page 106.</a> )
	Warning (For details, see the Event Log. For information about accessing the Event Log, see <a href="#">“Events” on page 106.</a> )
	Information
	OK
	Activity (such as rebuild or data migration)

You may see the following health status description as you move the mouse cursor over the health icon:

- **Degraded:** The virtual drive RAID array is available but has lost one or more disks. The virtual drive will be rebuilt automatically if a global or dedicated spare is available.



## Virtual Drive Actions

The actions available for a selected virtual drive are displayed to the right of the system graphic. For a description of these actions, refer to the following table.

**Table 14. Virtual Drive Action Menu**

<b>Global Action Menu Item</b>	<b>Description</b>
Create Storage Pool	Designates one or more drives as a storage pool. Global storage actions are available at all times on the storage screen.
<b>Selected Virtual Drive Action Menu Item</b>	<b>Description</b>
Assign	Allows an IT administrator to: <ul style="list-style-type: none"> <li>• Assign an existing virtual drive to a different server</li> <li>• Change the current drive assignment for a server</li> <li>• Assign the virtual drive to no server</li> </ul>
Delete	Deletes an existing virtual drive. This action will delete the selected virtual drive.  ALL DATA WILL BE LOST.
Rename	Renames an existing virtual name. A dialog box will display prompting the IT administrator for the new virtual drive name.
Expand	Expands the size of an existing virtual drive using any unallocated space within the storage pool in which the virtual drive resides.
Initialize Boot Sector	Clears the first 64 MB of data that is used on boot disks for the Master Boot Record, which ensures that a fresh volume for partitioning is available for operating system installation.
Change Affinity	Changes the storage control module affinity for the selected virtual drive. The dialog box indicates which storage control module is currently assigned and provides the capability to change control modules.  <b>NOTE:</b> Changing affinity will cause the selected virtual drive (LUN) to failover to the selected controller. If the virtual drive is in active use, there will be a slight pause in system I/O while the failover operation is handled by the multipath driver on the host operating system.

## Virtual Drive Details

The tabs displayed below the system graphic provide detailed information on the selected virtual drive. For a description of these tabs, refer to the following table.

**Table 15. Virtual Drive Tabs**

<b>Tab Heading</b>	<b>Description</b>
General	Displays a table with the following information: <ul style="list-style-type: none"><li>• Current status of the virtual drive (i.e., status, health, operation state)</li><li>• Virtual drive configuration data (i.e., name, total space, RAID level, server assignment and drive number)</li></ul>
Events	Displays all system events for the selected virtual drive.
Background Tasks	Displays all active tasks.

## Virtual Drive Help

To quickly access additional help regarding the virtual drive actions and tabs, click on the Get Help button in the Virtual Drive help box located under the actions box.

## Editing Virtual Drive Server Configuration

Once a virtual drive is created, an IT administrator can change the name, size, server assignment, and storage control module affinity at any time. This section describes the Assign action.

Use the assign action to change the current virtual drive server assignment. A virtual drive can be assigned to one or more servers and can be assigned any drive number that is available on the selected server. Each drive found by the operating system is given a number (drive position) based on the order found. The server does not need to be present to assign a drive because the system maintains the assignment based on server slot position.

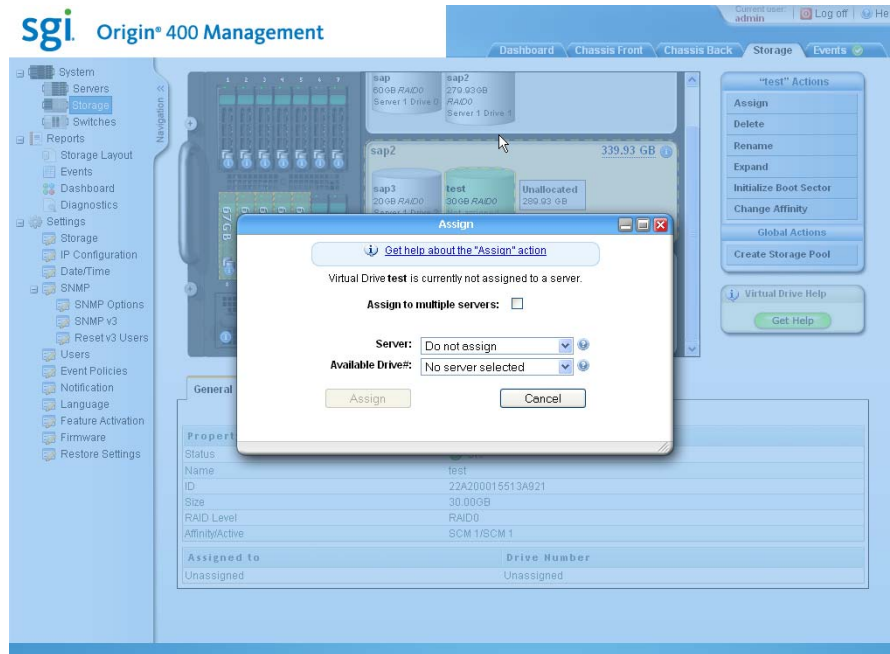
When a compute module is replaced, the virtual drives assigned to the compute module bay are automatically assigned to the replacement compute module. This allows an IT administrator to quickly replace a compute module without changing the storage configuration or assigned resources, thereby resulting in no impact to stored data.

The virtual drive in drive position 0 is the only drive available for the boot device. For example, if you assign five virtual drives to a server and then enter the BIOS boot order setup menu for that server, you will only see one virtual drive listed there and that would be the virtual drive at drive position 0. However, after the operating system boots, all five virtual drives will be available for use.

To assign a virtual drive to a server, follow these steps:

1. From the Storage view, select a virtual drive.
2. Choose Assign from the action menu.

The following dialog box appears.



**Figure 51. Assign Virtual Drive**

3. From the Server list, either select a server or select **Do not assign**.
4. Select the desired drive number if you selected a server in step 3. (Drive #0 is the boot device.)
5. Click Assign to apply the changes.

To assign a virtual drive to multiple servers (available only when the SGI Shared LUN feature has been activated - for instructions to activate the Shared LUN feature, see [“Feature Activation” on page 127](#)), follow these steps:

1. From the Storage view, select a virtual drive.
2. Choose Assign from the action menu.
3. Select Assign to multiple servers check box.
4. Select the desired drive number or the **Do not assign** option for each server.
5. Click Assign to apply the changes.

**Warning:** *It is not safe to unassign virtual drives from a compute module that is powered on because the compute module may be actively using the virtual drive. It is recommended to power off the compute module before reassigning virtual drives to another compute module. However, it is safe to make new assignments to compute modules regardless of whether the compute module is powered on or off.*

## Deleting a Virtual Drive

Deleting a virtual drive deletes all data stored on the selected virtual drive. Once a virtual drive is deleted, the space used for the virtual drive will be displayed on the system graphic as unallocated space in the same location as the original virtual drive. A new virtual drive or multiple drives can be created in the unused space as long as the new virtual drive total space requirement does not exceed the space available. The following figure displays the Storage screen after a virtual drive has been deleted from a storage pool that contained more than three virtual drives.

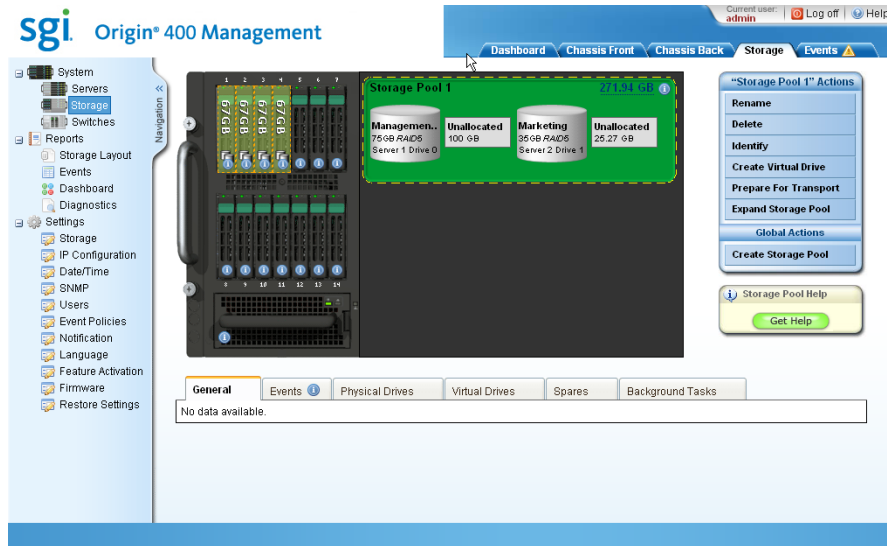


Figure 52. Deleted Virtual Drive

## Physical Drives

The Origin 400 has an integrated hard disk drive bay. Storage is shared among all installed servers by grouping physical drives together into storage pools, and then creating virtual drives that are then assigned to individual servers.

To view current status, available actions and product details for all installed hard drives, select a specific hard drive from the system graphic. The selected hard drive will be highlighted on the system graphic. The action box, help box and informational tabs will update to provide all available actions and information for the selected hard drive. Current health and product summary is quickly available by moving the mouse over the Health/Information icon located on the selected hard drive.

**Note:** For drives that are included in a storage pool, limited drive details are also displayed on the physical drive tab for the assigned storage pool.



The screenshot shows the SGI Origin 400 Management interface. The main area displays a storage pool with 271.94 GB of capacity. The pool is divided into four categories: Management (75 GB RAID5, Server 1 Drive 0), Finance (75 GB RAID5, Server 3 Drive 0), Marketing (35 GB RAID5, Server 2 Drive 0), and Unallocated (25.27 GB). Below this, the Physical Drive Properties for Drive 4 are shown in a table.









Property	Value
Status	OK
Drive	4
Manufacturer	Seagate
Firmware Version	0002
Product ID	ST973402SS (SAS)
Serial Number	3NP1MYW4
Drive Size	68.36GB
Usable Space	67.88GB
Role	Member of Storage Pool
HDD Write Back Cache	Disabled

Figure 53. Physical Drives

## Health Icons

The health icons are displayed on the graphical representation of the component when the component is selected.

**Table 16. Health Icons**

Health Icon	Meaning
	Critical (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Warning (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	OK
	Hot Spare
	Informational
	Ready for Transport
	Assigned to Storage Pool
	Data Migration or Other Background Operation In Progress

You may see one of the following health status descriptions as you move the mouse cursor over the health icon:

- **Dead:** The disk was configured to be part of a storage pool or as a spare, but was taken offline due to an extraction or insertion of the drive, a user action (for example, Force Offline), or a drive hardware error. Choose the appropriate action from the Action Menu to bring it back online (for example, the appropriate action may include one of the following actions: Start Rebuild, Force Online, or Cancel Hot spare Action).
- **Stale:** The drive was at one time part of a storage pool, but was taken offline by an error or was transported without being installed, and is no longer required by the storage pool. You may keep the drive in the stale state to preserve the data (for

example, if required for forensic purposes), or clear the stale condition and reuse the disk.

- **Not Accessible:** This physical drive is not usable.
- **Predictive Failure (PFA):** A drive media error has been found by the media patrol background task, or by a SMART error reported for the drive.
- **Rebuilding:** A storage pool is currently being rebuilt on this drive to replace an offline physical drive.
- **Migrating:** A storage pool is currently being expanded that includes this physical drive.
- **Media Patrol Running:** The Media Patrol background task is currently checking this physical drive for errors.
- **Transitioning:** A storage pool has been rebuilt to a spare from this physical drive, and now the error on this drive has been cleared, or the drive has been replaced, and the storage pool is being rebuilt back to this drive.
- **Predictive Data Migration Running:** The Predictive Data Migration (PDM) background task is running on this physical drive.

## Physical Drive Actions

The actions available for a selected hard drive are displayed to the right of the system graphic. For a description of these actions, refer to the following table.

**Table 17. Physical Drive Action Menu**

<b>Global Action Menu Item</b>	<b>Description</b>
Create Storage Pool	Designates one or more drives as a storage pool. Global storage actions are available at all times on the storage screen.
<b>Selected Physical Drive Action Menu Items</b>	<b>Description</b>
Identify Drive	Illuminates the drive ID LED, which enables easy onsite local identification.
Force Offline (present if drive is a hot spare or included in an existing storage pool)	Removes the selected drive from a storage pool (if assigned) or from hot-spare status. The status will be indicated as Dead, forced offline. The physical drive must first be forced offline before it can safely be removed.
Force Online (available if the drive is offline)	Changes a Dead (Offline) drive back online. This may be needed, in some cases, to restore a drive that was forced offline or if you need to recover data from a drive that went offline from some other cause.
Make Hot Spare (present if drive is available (i.e., not included in a storage pool or already a hot spare)	Designates whether the drive is a global or dedicated hot spare. A global hot spare is applied to any storage pool as needed. A dedicated hot spare is assigned to a specific storage pool. See <a href="#">“Create a Hot-spare Drive ” on page 87</a> for instructions on creating a hot spare. Make Hot Spare is present only if the drive is available (i.e., not included in a storage pool or already a hot spare).
Cancel Hot Spare (present if drive role is assigned as either a global or dedicated hot-spare drive)	Removes hot-spare status and sets the drive to available. Available drives can be assigned to existing storage pools, new storage pools or used as hot-spare drives. Cancel Hot Spare is present if a drive role is assigned as either a global or dedicated hot spare.

**Table 17. Physical Drive Action Menu**

<b>Global Action Menu Item</b>	<b>Description</b>
Create Storage Pool	Designates one or more drives as a storage pool. Global storage actions are available at all times on the storage screen.
<b>Selected Physical Drive Action Menu Items</b>	<b>Description</b>
Clear PFA State	Sets the drive state to OK. The Predictive Failure (PFA) State indicates that the background PFA scan found bad data blocks or sectors on the drive.
Clear Stale State	Sets the drive state to OK. Clear Stale State is present if a drive is in a stale state (the drive has obsolete array information). This can occur when the drive is taken offline by the user, by physically removing the drive or by a disk error. When the storage pool is rebuilt to correct for the missing drive, the drive is marked as "stale".
Start Data Migration	Enables an IT administrator to move data from a defective physical disk drive to a good physical disk drive.

## Physical Drive Details

The tabs displayed in the system graphic provide detailed information on the selected physical drive. For a description of these tabs, refer to the following table.

**Table 18. Physical Drive Tabs**

<b>Tab Heading</b>	<b>Description</b>
General	Displays a table with the following information: <ul style="list-style-type: none"> <li>• Current status of the physical drive (i.e., status, health, operation state)</li> <li>• Drive product data (i.e., Drive Number, Manufacturer, Serial Number, Size, Firmware, Role)</li> </ul>
Events	Displays all system events for the selected physical drive.
Storage Pool (displayed if drive is included in an existing storage pool)	Displays the Storage Pool property table, which includes information such as Storage Pool ID, Storage Pool Name, Status, Total Managed Space, Total Unallocated Space, Number of Physical Drives, Number of Virtual (Logical) Drives.
Virtual Drives (displayed if drive is included in a storage pool with virtual drives)	Displays the Virtual Drive to Server Mapping table, which includes virtual drive name, size, RAID level, status, assigned server, and drive number/position.
Background Tasks (displayed if drive is included in a storage pool)	Lists any Active Tasks currently involving the physical drive, such as creating, expanding, rebuilding, or migrating storage pools or virtual drives.

## Physical Drive Help

To quickly access additional help regarding physical drive actions and tabs, click on the Get Help button in the Shared Drive help box located under the action box.




## Create a Hot-spare Drive

Unused physical hard drives may be designated as hot-spare drives. A hot-spare drive automatically replaces a physical hard drive in a storage pool when it fails, or a when the Predictive Failure Analysis (PFA) indicates a physical drive will fail.


The Origin 400 system supports both dedicated and global hot-spare drives. A dedicated hot-spare drive is assigned to a specific storage pool. If a physical drive fails in the assigned storage pool, the dedicated hot-spare drive will replace the failed drive as long as the hot-spare drive is equal to or greater than the size of the failed drive. A global hot spare can replace any failed drive in any storage pool as long as the global hot-spare drive size is equal to or greater than the failed drive size. Both dedicated and global hot-spare drives will revert to being a hot-spare drive once the failed physical drive is replaced.

Once a hot spare is created, the following information is updated:

- The information icon for the physical drive changes to the hot spare icon,  .
- The Role description on the General tab for the selected physical drive indicates whether the physical drive is a dedicated or global spare.
- If the drive is a dedicated hot-spare drive, it will be listed on the Spares tab for the assigned Storage Pool.
- If the drive is a global hot-spare drive, it will be listed on the Spares tab under all Storage Pools.

To create a hot-spare drive, follow these steps:

1. Click Storage in the top menu or click System > Storage in the left navigation panel to open the Storage screen.
2. Select an available or unused physical hard drive from the system graphic.  
This is a drive that is currently not used in a storage pool.
3. From the “Drive <#>” Action menu, select Make Hot Spare.
4. Configure the hot spare as either a global hot spare (available to all storage pools) or a dedicated hot-spare drive (assigned to a specific storage pool) and click Apply.

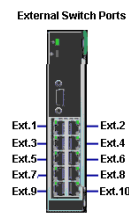
Once the hot spare has been created, a successful action dialog will be displayed and the information icon will change to the hot spare icon,  .

## SGI Gigabit Ethernet Switch Module 1 and 2

The Origin 400 comes with one SGI gigabit Ethernet switch module installed in the rear module bay labeled “ESM1”. The Origin 400 system can support up to two gigabit Ethernet switch modules. Each switch module has 12 internal ports and ten external ports. By default, the gigabit Ethernet switch module assigns all internal and external ports to a default virtual LAN (VLAN).

The internal ports connect the compute modules to the switch modules. There are two internal ports assigned to each compute module bay. The internal ports are labeled “Server 1: Port 1”, “Server 1: Port 2”, “Server 2: Port 1”, ... “Server 6, Port2”. All internal ports are enabled by default. Using the Configure Ports action dialog, an IT administrator can assign any internal port to a VLAN whether or not the compute module is installed.

The external ports are visible from the rear of the system and must be physically patched by an IT administrator to an external network device. Using the Configure Ports action dialog, an IT administrator can enable or disable any external port, assign an external port to a VLAN, change the external port speed, and enable or disable Spanning Tree. The external ports are numbered as shown in [Figure 54](#).



**Figure 54. External Ports**

The Origin 400 Management Center enables an IT administrator to modify internal and external port settings, view health information and product details, and launch an advanced configuration interface. To view current status, available actions, and product details for an installed gigabit Ethernet switch module, either click System > Switches in the left navigation panel or click the Chassis Back tab to display the back of the system and select the specific switch module from the back of the system graphic. The content displayed on the informational tabs, action box, and help box will be updated with product-specific information and actions available for the selected switch module highlighted in green. The current health and product summary information is quickly available by moving the mouse over the Health/Information icon located on the selected switch module.








**Figure 55. Gigabit Ethernet Switch Module View**

## Health Icons

The health icons are displayed on the graphical representation of the component when the component is selected.

**Table 19. Health Icons**

Health Icon	Meaning
	Critical (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Warning (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Information
	OK
	Firmware update or other background activity

## Gigabit Ethernet Switch Module Actions

The actions available for a selected switch module are displayed to the right of the system graphic. For a description of these actions, refer to the following table.

**Table 20. Switch Module Action Menu**

Action Menu Item	Description
Configure Ports	Configures port and Virtual LAN (VLAN) settings within the Origin 400 Management Center. This action provides quick access to frequently configured port and VLAN options.
Reset	Enables remote reset of the selected switch module.
Advanced Configuration	Launches a third-party Advanced Switch Configuration interface in a new window to view all switch configuration options. Refer to your SGI Technical Support representative for more information on how to use the Advanced Configuration Switch interface.

## Gigabit Ethernet Switch Details

The tabs displayed below the system graphic provide detailed information for the selected switch module. For a description of these tabs, refer to the following table.

**Table 21. Switch Module Tabs**

Tab Heading	Description
General	Displays current status and general gigabit Ethernet switch information, such as product ID, uptime, hardware and software versions, and MAC address.
Events	Displays all system events for the selected gigabit Ethernet switch.
Ports	Displays table of key port settings, including Port ID, VLAN ID, Enabled/Disabled Status, Link Status, Set Speed, Current Speed, VLAN Mode, and Spanning Tree (STP).
VLANs (Virtual LANs)	Displays a table of configured VLANs for the selected switch, including VLAN number, VLAN name, and members.
Statistics	Displays a table of statistics for the selected switch, including Port ID, Input, Output, and Error Information.

## Gigabit Ethernet Switch Module Help

To quickly access additional help regarding the gigabit Ethernet switch module screen, actions, and tabs, click on the Get Help button in the Switch help box located under the Actions box.

## Configuring a Gigabit Ethernet Switch

Gigabit Ethernet switches come pre-configured with all available ports enabled in a single default VLAN. No additional configuration is required to connect the Origin 400 system to a network.

Two options are available to modify the default switch configuration:

- The Configure Ports action menu item enables an IT administrator to quickly and easily modify port and Virtual LAN (VLAN) settings. [Figure 56](#) displays the Configure Ports dialog box within the Origin 400 Management Center.
- To make additional changes to the switch configuration, click Advanced Configuration in the Actions menu. The Advanced Configuration action launches a separate switch configuration interface in a new window. Refer to your SGI Technical Support representative for more information on how to use the Advanced Configuration.

## Configure Ports Dialog

The Configure Ports dialog enables an IT administrator to modify the following parameters for each SGI Ethernet switch module:

- Enable or disable external ports
- Assign any port (internal or external) to a VLAN
- Set the external port speed
- Enable or disable spanning tree on external ports

### *Steps to assign an internal or external port to a VLAN:*

1. Click System > Switches in the left navigation panel.
2. Select the switch module to be configured.
3. Click Configure Ports in the selected switch Action menu.
4. To add ports to a new or existing VLAN, type the VLAN number in the box under the VLAN column for the specific port.

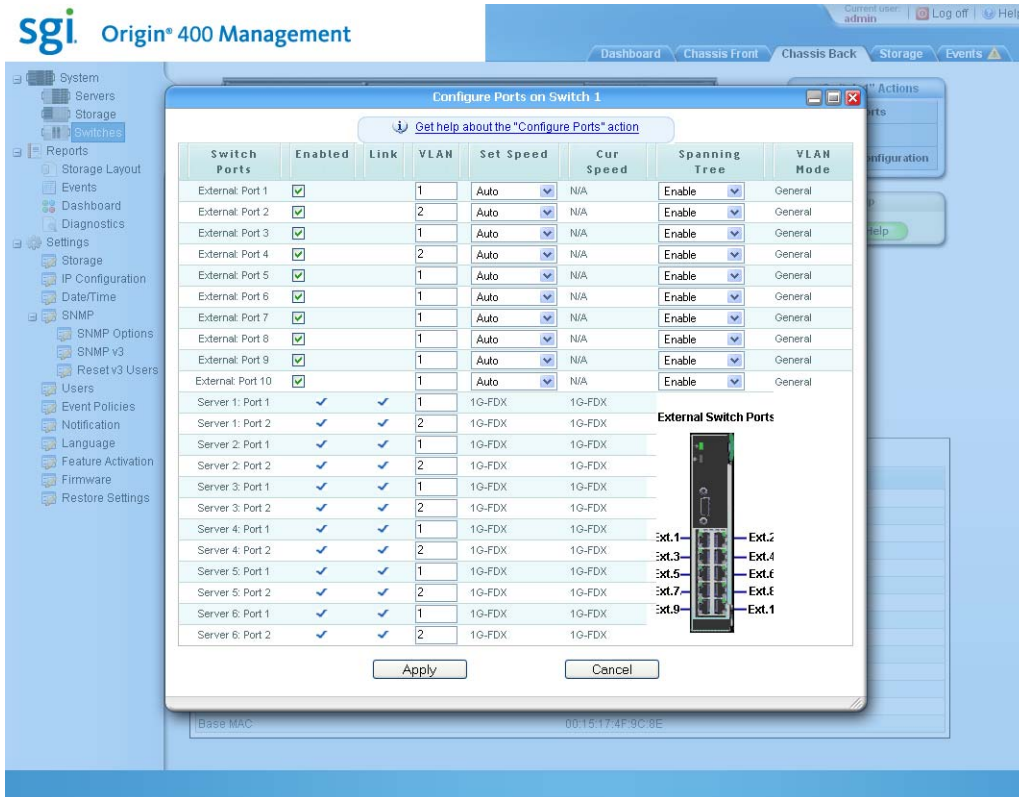
Each individual port can be assigned to only one VLAN at a time.

The compute module does not have to be present in the system in order to assign the internal ports to a VLAN.

5. Click Apply.

The Configure Ports dialog simplifies the VLAN configuration process by removing the step to create a VLAN before assigning ports. The VLAN number entered in the Configure Ports dialog in step 4 can either be a new VLAN number or an existing VLAN number, since the Apply process creates the VLAN and also assigns the ports.

The following image illustrates the Configure Ports dialog.

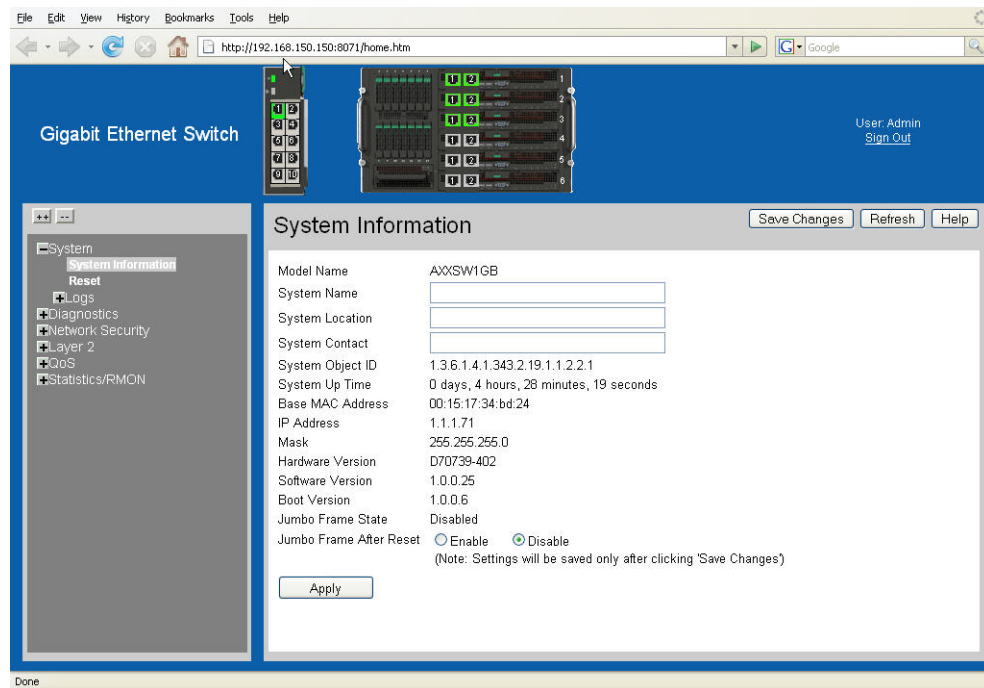


**Figure 56. Configure Ports Dialog Box**

### Advanced Configuration

The Advanced Configuration action launches the embedded switch user interface for the SGI gigabit Ethernet switch module in a new window. This interface exposes all configuration settings for the switch. Configuration settings modified in either the Advanced Configuration or the Origin 400 Management Center are displayed in both interfaces.

The following image illustrates the Advanced Configuration screen.



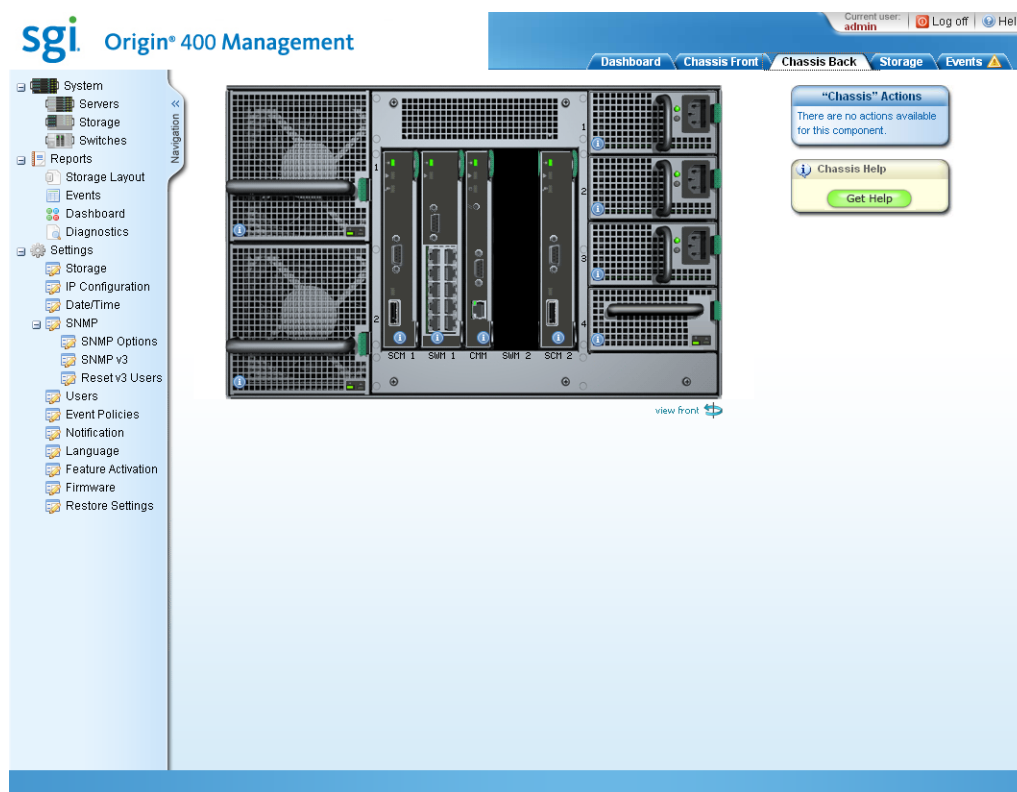
**Figure 57. Advanced Configuration Screen**

## Chassis Back

The Chassis Back view provides an accurate visual view of the back of the chassis, which includes the management module, switch modules, storage control modules, power supplies and fans. This real-time view enables an IT administrator to select the component of interest, quickly view the current health, and also determine which components are present or not present. The icons present on each of the components indicate the current health. By hovering over the component icon, a brief summary of the current health, state and component description is displayed in a pop-up box.



To access the Chassis Back view, click the Chassis Back tab in the top menu. By default, no components are selected on the chassis in this view.



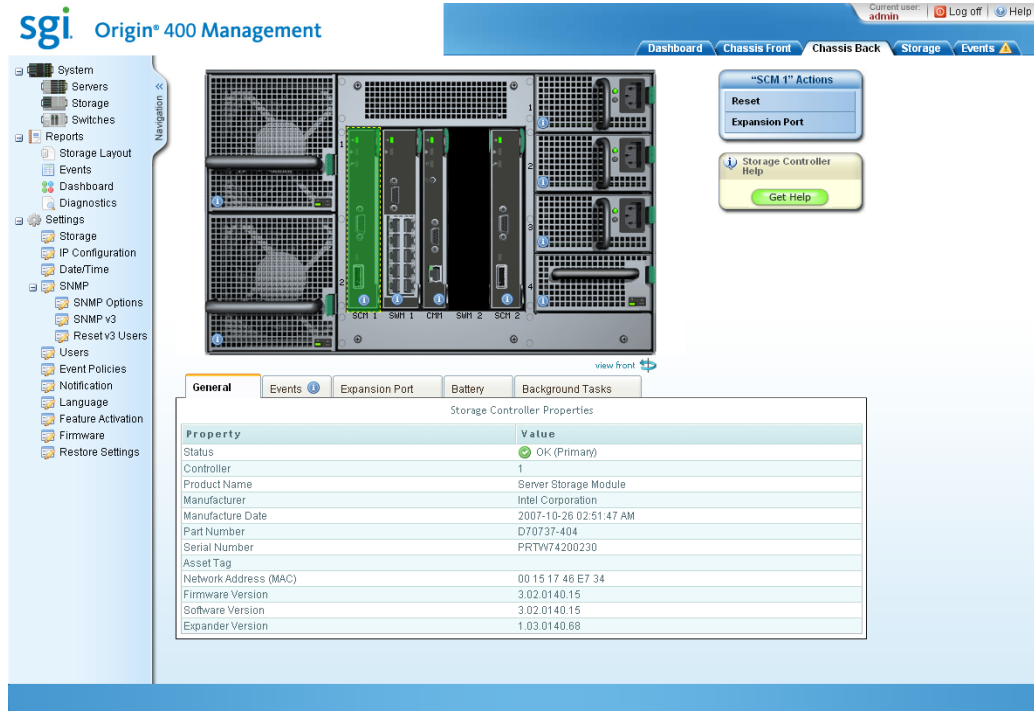
**Figure 58. Chassis Back View**

## Storage Control Module 1 and 2

The Origin 400 system contains at least one storage module in slot SCM1. A second storage module may be added to improve performance and provide redundancy in the event one SCM fails. If there are two SCMs installed in the system, the SCMs are redundant and in the event of an SCM failure, the remaining SCM will become the primary control module for all virtual drives.

The Origin 400 Management Center enables an IT administrator to grant compute modules with access to external storage via the expansion port, view health information, and view product details. To view the current status, available actions, and product details for an installed SGI storage control module, click the Chassis Back tab in the top menu to display the back of the system and select the specific storage control module from the system graphic. The content displayed on the informational tabs, action box, and help box will be updated with product-specific information and available actions for the selected

storage control module highlighted in green. The current health and product summary information is quickly available by moving the mouse over the Health/Information icon located on the selected storage control module.








**Figure 59. Storage Control Module View**

## Health Icons







The health icons are displayed on the graphical representation of the component when the component is selected.





**Table 22. Health Icons**

Health Icon	Meaning
	Critical (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Warning (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Information
	OK
	Firmware update or other background activity

**Status Messages**

**Table 23. Status Messages**

Health Icon	Status Message	Meaning
	Firmware update in progress.	The SCM firmware update is in progress.
	Initializing (Offline)	The SCM is initializing after a reboot.
	Rebooting (Offline)	The SCM is rebooting.
	Unmanageable (Offline)	The SCM is not responding to the CMM.
	OK (Primary)	The SCM is operational. In a dual SCM configuration, this SCM is the primary controller. In a single SCM configuration, this SCM is the primary controller by default.
	OK (Secondary)	The SCM is operational and this SCM is the secondary controller in a dual SCM configuration. The SCMs have redundancy.

Health Icon	Status Message	Meaning
	OK (Primary)(Critical)	This SCM is operational, but the status is critical because redundancy has been lost in a dual SCM configuration. This SCM is now the primary controller for all virtual drives.
	Status (Component Error)	The SCM is not operational due to an internal failure or a failed firmware update.
	Safe Mode (Offline)	The SCM is in Safe Mode. The SCM will not process any I/O requests.
	Status (Firmware Update Pending)	A firmware update is pending for this SCM. For details, see <a href="#">“Firmware Updates”</a> on page 128.

## Storage Control Module Actions

The actions available for a selected storage control module are displayed to the right of the system graphic. For a description of these actions, refer to the following table.

**Table 24. Storage Control Module Action Menu**

Action Menu Item	Description
Reset	Enables remote reset of the selected storage control module.
Expansion Port	Enable/Disable server access to the external expansion port on the selected storage control module. Additional external storage options are available to the server via the expansion port.

## Storage Control Module Details

The tabs displayed below the system graphic provide detailed information for the selected storage control module. For a description of these tabs, refer to the following table.

**Table 25. Storage Control Module Tabs**

Tab Heading	Description
General	Displays: <ul style="list-style-type: none"><li>• Current status of the selected storage control module (i.e., status, health, boot state, master state, battery state)</li><li>• Product data information, including manufacturer, firmware revision, serial number, product ID, etc.</li></ul>
Events	Displays all events for the selected storage control module.
Expansion Port	Displays the expansion port access table.
Battery	Displays the battery property table, which includes battery status, temperature, remaining capacity percentage, cycle count, voltage, current, cell type, estimated hold time, etc.
Background Tasks (displayed if an action is occurring on a virtual drive)	Lists any Active Tasks currently involving the virtual drive, such as creating, expanding, rebuilding, or migration.

## Storage Control Module Help

To quickly access additional help regarding the storage control module screen, actions, and tabs, click on the Get Help button in the storage control module help box located under the actions box.

## SGI Management Module

The SGI management module, installed in the middle bay (labeled “CMM1”) of the rear of the system, provides the Origin 400 Management Center that is used to configure and manage the Origin 400 system hardware. This module is not redundant, but the system will continue to operate normally should this module fail. However, configuration changes cannot be made until a failed SGI management module is replaced.

The Origin 400 Management Center enables an IT Administrator to reset the SGI management module, view health information, and view product details. To view current status, available actions, and product details for the installed SGI management module, click the Chassis Back tab in the top menu to display the back of the system and select the management module from the system graphic. The content displayed on the informational tabs, action box, and help box will be updated with product-specific information and available actions for the management module highlighted in green. The current health and product summary information is quickly available by moving the mouse over the Health/Information icon located on the management module graphic.







**Figure 60. SGI Management Module View**

## Health Icons

The health icons are displayed on the graphical representation of the component when the component is selected.

**Table 26. Health Icons**

Health Icon	Meaning
	Critical (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Warning (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Information
	OK

### SGI Management Module Actions

The actions available for a selected management module are displayed to the right of the system graphic. For a description of these actions, refer to the following table.

**Table 27. Management Module Action Menu**

Action Menu Item	Description
Reset	Enables remote reset of the selected management module.

### SGI Management Module Details

The tabs displayed below the system graphic provide detailed information for the management module. For a description of these tabs, refer to the following table.

**Table 28. Management Module Tabs**

Tab Heading	Description
General	Displays: <ul style="list-style-type: none"><li>• Current status of the selected management module</li><li>• Product data information, including manufacturer, firmware revision, serial number, product ID, etc.</li></ul>
Events	Displays all events for the selected SGI management module.
Midplane	Displays product data information for the midplane, including manufacturer, firmware revision, serial number, part number, etc.

## SGI Management Module Help

To quickly access additional help regarding the SGI management module screen, actions, and tabs, click on the Get Help button in the management module help box located under the actions box.

## Origin 400 Fans and Power Supplies

Fans and power supplies are available for selection and viewing from the system graphic.

The system has three fan modules:

- One I/O cooling module (front panel)
- Two server cooling modules (rear panel)
- Each power supply also has integrated cooling fans.

The system can have up to four power supplies that are accessed from the rear panel. Each power supply also has integrated cooling fans. If a power supply is not installed, a fan blank panel must be installed in the power supply slot to ensure proper cooling.

To view current status, available actions, and product details for all installed fans and power supplies, select the specific component from the system graphic. Once selected, the main screen graphic will change to display the selected fan or power supply highlighted in green. The help box and informational tabs will update to provide all available information for the selected fan or power supply. Current health and product summary is quickly available by moving the mouse over the Health/Information icon located on the selected component.





*Note: No actions are available for fans or power supplies.*

## Health Icons

The health icons are displayed on the graphical representation of the component when the component is selected.



**Table 29. Health Icons**

Health Icon	Meaning
	Critical (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Warning (For details, see the Event Log. For information about accessing the Event Log, see “Events” on page 106.)
	Information
	OK

## Origin 400 Fans and Power Supplies Details

The tabs displayed below the system graphic provide detailed information for the selected fan or power supply. For a description of these tabs, refer to the following table.

**Table 30. Fans and Power Supplies Tabs**

Tab Heading	Description
General	Displays: <ul style="list-style-type: none"><li>• Current status of the selected fan or power supply (i.e., status, health)</li><li>• Product data table will display information, including manufacturer, model number, serial number, etc.</li></ul>
Events	Displays all events for the selected fan or power supply.
Sensors	Displays current sensor information, including fan speed, input/output power, temperature, etc.

## Reports

The Origin 400 Management Center generates several standard reports. These reports are used by IT administrators to view overall system health, system configuration information, event logs, diagnostic information, storage resource allocation map, switch performance, and hardware and firmware inventory. The following reports are supported: Storage Layout, Events, Dashboard, and Diagnostics.

## Storage Layout

The Storage Layout report shows a graphical or tabular representation of all the components in the storage subsystem. This report shows you:

- Physical drives and drive groups (physical drives assigned to a storage pool)
- Storage pools with the assigned hot-spare drives
- Virtual drives showing the drive name, storage capacity, and RAID level
- The drive mappings to the servers showing the drive numbers for each drive on the server
- The storage control module affinity for each virtual drive.

To access the Storage Layout report, click Reports > Storage Layout in the left navigation panel.

You can switch between the graphical and table views by clicking on the link at the top of the report.

**Note:** *The Physical drives and Server columns represent the physical slots for hard drives and servers. If a drive is not present, it will be marked as not present.*

The Storage Layout graphics in [Figure 61](#) and [Figure 62](#) illustrate both the graphical and tabular views for the following storage configuration:

- Fourteen physical drives present in the system.
- Drives 1, 2, and 3 are grouped together in a single storage pool named “Storage Pool 1”.
- Drive 14 is a global hot spare.
- Drives 4 - 13 are available/unused.
- One storage pool is present. The storage pool is named “Storage Pool 1” and is 100.58 GB in size.
- Two virtual drives are present. One virtual drive is named “Finance” and is configured as a 25-GB RAID 0 drive. The second virtual drive is named “Marketing” and is configured as a 30-GB RAID 0 drive.
- The virtual drive “Finance” is assigned to Server 1 as Drive 0. The virtual drive “Marketing” is assigned to Server 2 as Drive 0.

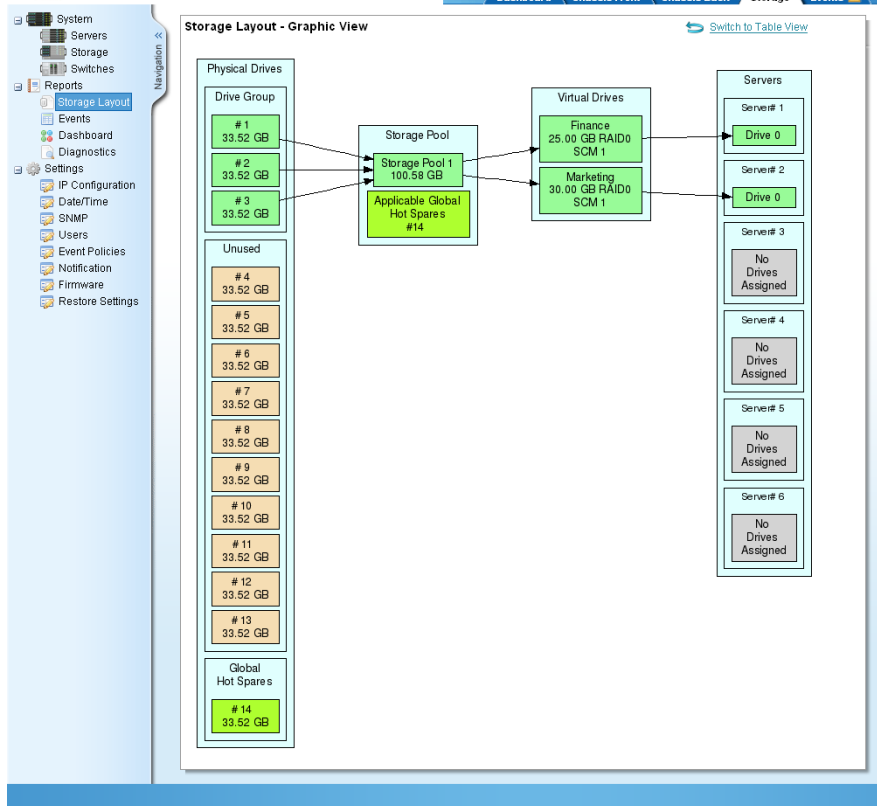
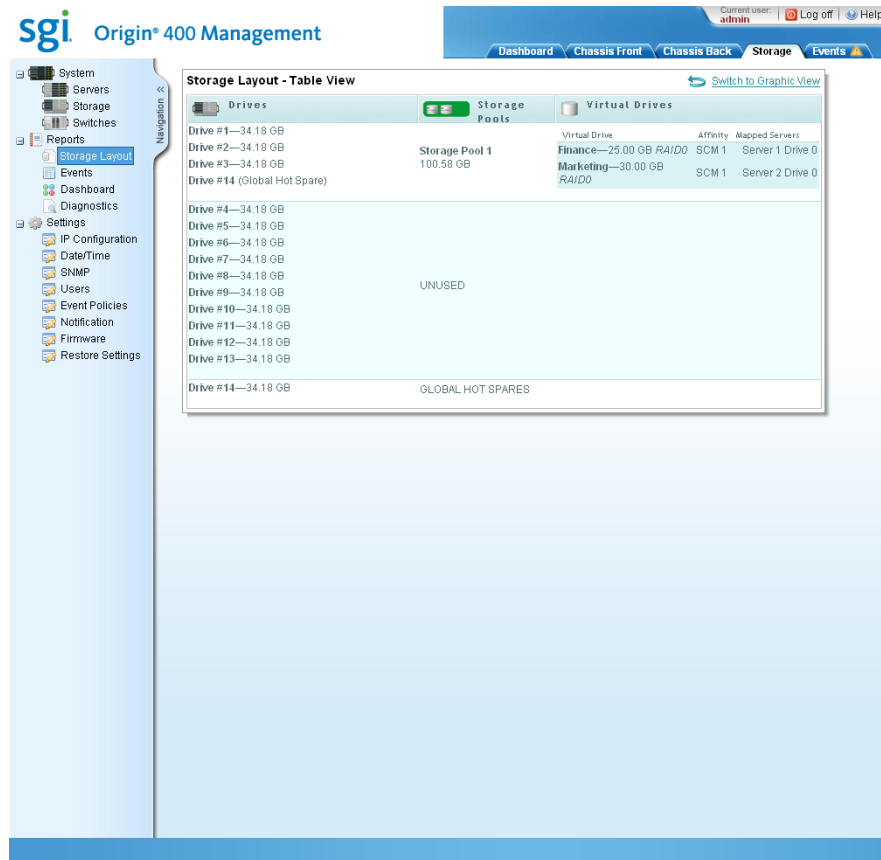


Figure 61. Storage Layout Graphical View



**Figure 62. Storage Layout Tabular View**

## Events

The Events screen contains a table of all open and unacknowledged system events. This screen enables an IT administrator to quickly view and acknowledge new events for all system components in a single location.

To access the Events screen, click the Events tab in the top menu or click Reports > Events in the left navigation panel.

The following features enable the IT administrator to quickly access specific information from the System Event Log screen:

- Sort events: Sort the events in the table by ID, Date/Time, Component Type, Description, Severity, and User by clicking on the appropriate column header.
- View filter: Filter events by Active, Closed, or All events.
- Severity filter: Filter events by Info +, Warning +, or Critical Severities.
- Close events: Close individual events by selecting the checkbox next to the event and clicking the Close Selected button. Once an event is closed, it is no longer displayed on this screen.

- **Delete All events:** Delete all events in the log by selecting the Delete All button.
- **View event details:** Click on the + sign to the left of the specific event row to display further details about the event, as shown in Figure 63. Clicking on the Policy ID number opens the Event Policy Definition dialog as shown in Figure 64. The Event Policy actions can be modified in this window.
- **XML:** Download the system event information in XML format. This will download all unacknowledged events, not just the default 20 events displayed on the events screen.
- **CSV:** Download the system event information in CSV format. This will download all unacknowledged events, not just the default 20 events displayed on the events screen.
- **View Component screen:** Click on the component link in the specific event row to be redirected to the component screen to view available actions and additional information to resolve or troubleshoot the issue.
- **Rows per screen:** IT administrators can customize the event view by indicating how many rows (between 10 and 50, in increments of 5) that they would like displayed on each screen.
- **Navigate events:** If more than 20 events are present, links to additional pages is displayed at the top of the screen next to the Rows drop-down list. Click on the page number to view additional events.

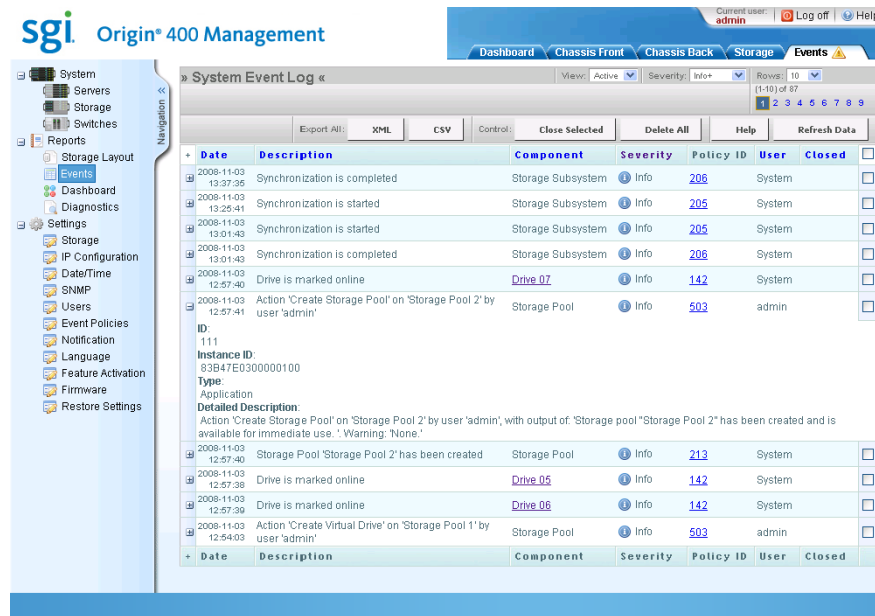
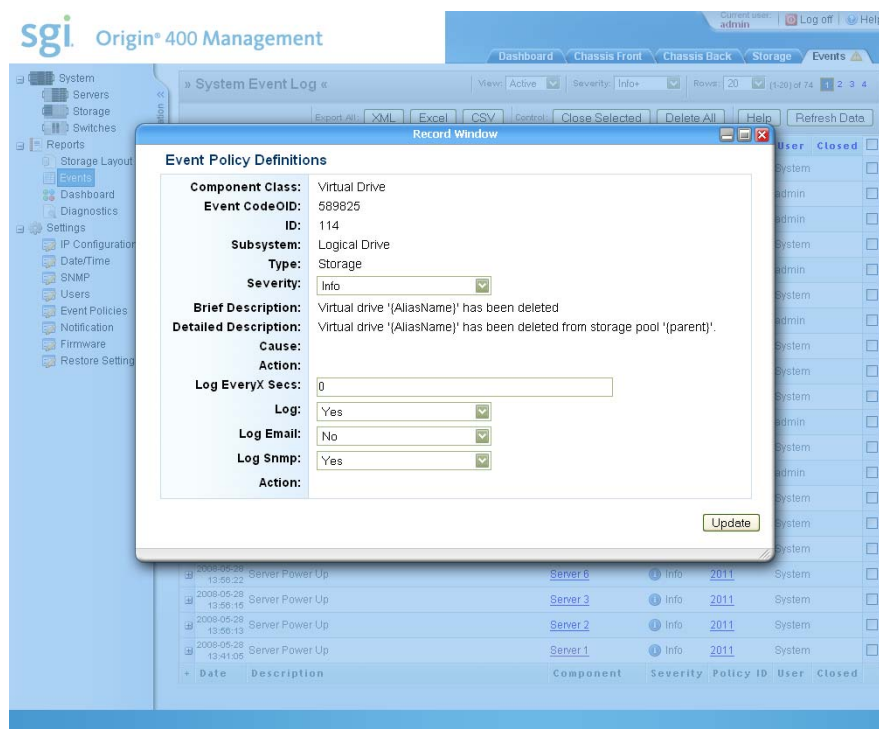


Figure 63. System Event Log Screen

*Note:* To view a history of events, select the Events tab on each component screen.



**Figure 64. Event Policy Record Window**

## Dashboard

The Dashboard view provides an interactive snapshot of the overall system and component health, as well as a list of all required actions and critical events. To get detailed information about any component presented on the dashboard, move the mouse over the component or icon to view summary information, or click the component to be redirected to the component screen.

To access the Dashboard view, click the Dashboard tab in the top menu or click Reports > Dashboard in the left navigation panel. This view is displayed by default after successfully logging into the Origin 400 Management Center.

The Dashboard consists of the following five main areas:

- **Required Actions:** The required actions box includes, but is not limited to, initial system configuration steps, steps to replace a failed component, or steps to resolve a system error. The actions are listed as links that direct the IT administrator to the appropriate screen to complete the required action.
- **System Health:** The system health box lists all possible system components with a visual health icon indicator. Moving the mouse over either the component name or health icon will display summary information, including whether the component is present or not present in the system, its current health and a component description.

To view detailed information and available actions for any component, click the component name to be redirected to the specific component configuration screen.

- **Power Load:** Quickly enables the IT administrator to view the current power consumption of the system. If the arrows are in the green area of the indicator bar, power redundancy is enabled. The yellow area of the indicator bar shows non-redundant power. The red area indicates a critical state.
- **Temperature:** Displays the current system temperature.
- **Recent Critical Events:** Displays all recent (unacknowledged) critical events and a link to View All Events. The View All Events link redirects the IT administrator to the Events view.

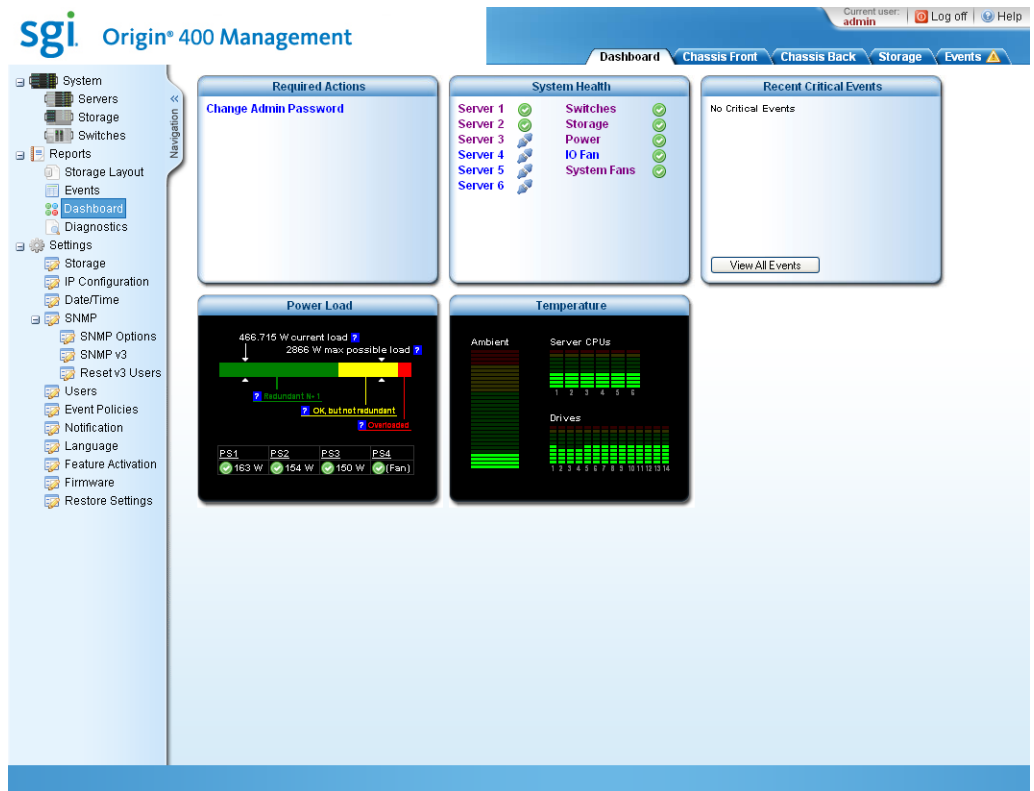
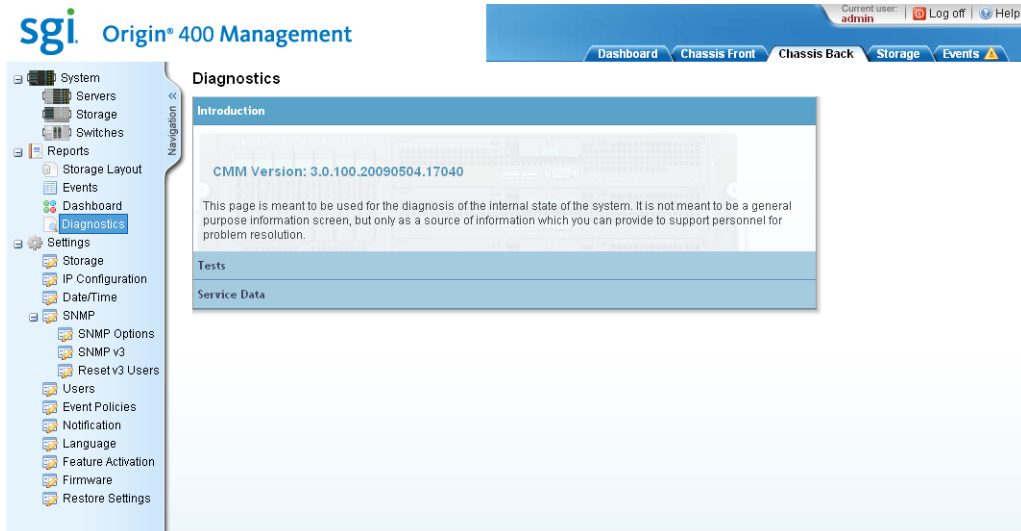


Figure 65. Dashboard View

## Diagnostics

The Diagnostics screen enables an IT administrator to obtain information about recent events generated by the servers, chassis, and storage components, and to run tests to diagnose the internal state of the system. This screen is not meant to be used as a general purpose information screen, but only as a source of information that can be provided to support personnel for problem resolution.

To access the Diagnostics screen, click Reports > Diagnostics in the left navigation panel.



**Figure 66. Diagnostics**

## Tests

The Internal Communications Test and System Information Report can be found in the test portion of the Diagnostics screen.

The Internal Communications Test verifies that each component can communicate with the management module. Clicking on the Internal Communications Test will open the results within the Record Window. The Record Window will display all present devices as well as pass/fail information from the test. The Internal Communications Test will test communications for every installed Ethernet switch module, storage control module, fan, chassis, and server.

The System Information Report generates a complete report about your system and the system settings (this does not include user account information). Clicking the System Information Report will download the service information, which can be saved or opened as shown in [Figure 68](#) and [Figure 69](#).



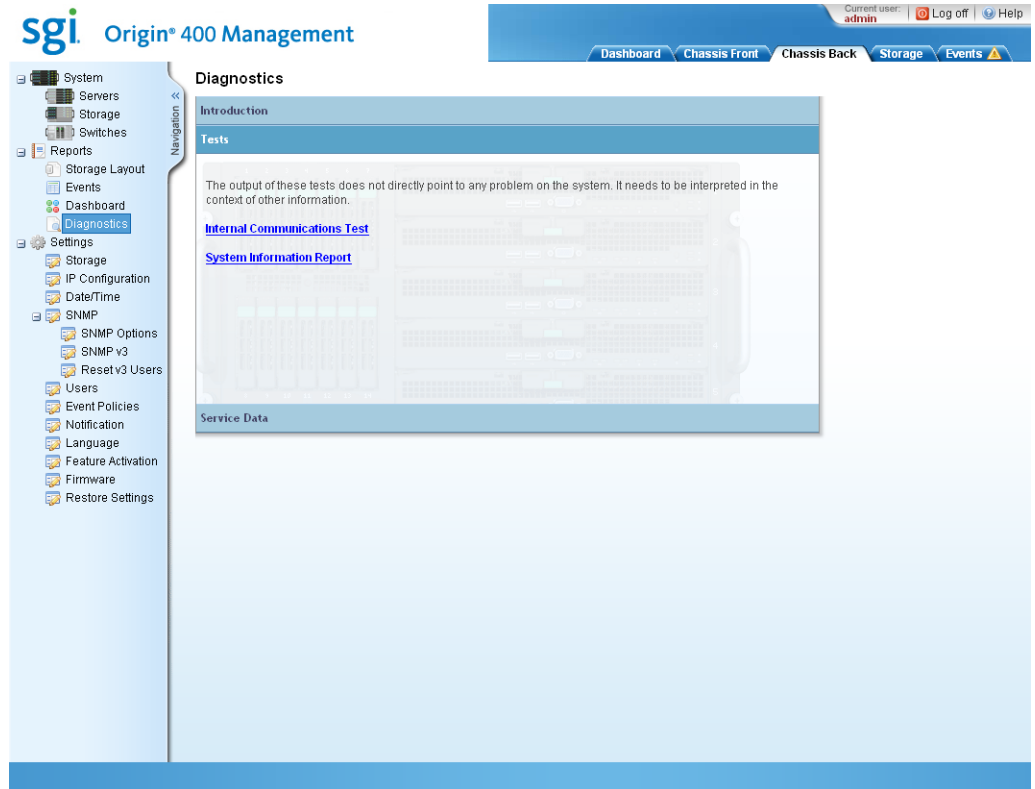


Figure 67. Diagnostic Tests

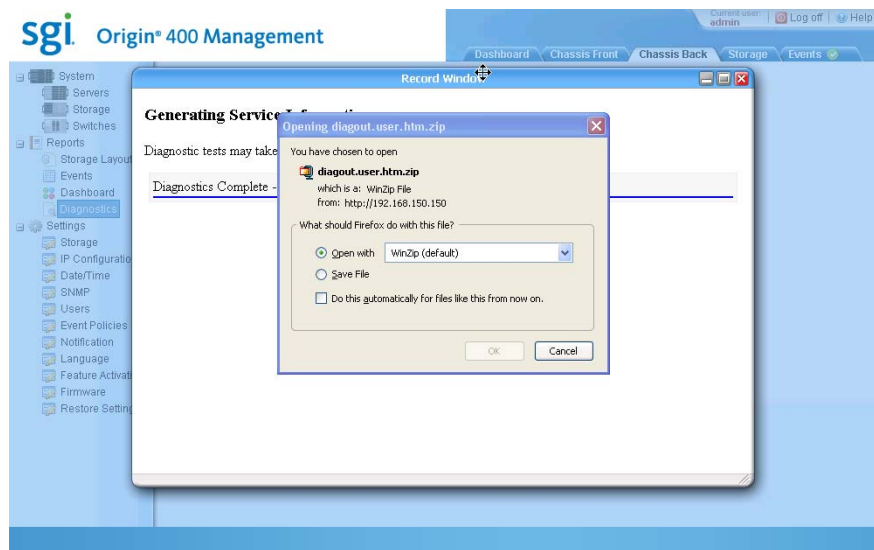


Figure 68. System Information Report Download

**DIAGNOSTIC INFORMATION**

Test run: 11/18/2008 16:30:03

- [Event Log Table](#)
- [ID ROM Data](#)
- [SD Card Utilization](#)
- [Dashboard](#)
- [Firmware](#)
- [All Component Status](#)
- [Component Data - Servers](#)
- [Component Data - Switches](#)
- [Component Data - Storage Controllers](#)
- [Component Data - Management Module \(CMM\)](#)
- [Component Data - Fans](#)
- [Component Data - Power Supplies](#)
- [Storage - Layout](#)
- [Storage - Physical Drives](#)
- [Storage - Virtual Drives](#)
- [Storage - Pools](#)
- [Configuration - IP Configuration](#)
- [Configuration - Notification](#)
- [Configuration - SNMP](#)
- [Configuration - Date/Time](#)

Event Log

EventLogId	Date	EventPolicyId	ComponentId	InstanceId	EventSeverityId	EventTypeId	DetailedDescription	EventCause	EventAction	BriefDesc
3	2008-11-07 10:38:41	Attention State - Identify LED off	Server 1		Info	IPMI	Sensor: Attention State - Identify LED off.	Server Sensor: Attention State	No action is required	Attention State - LED off
4	2008-11-07 10:38:43	Attention State - Identify LED off	Server 2		Info	IPMI	Sensor: Attention State - Identify LED off.	Server Sensor: Attention State	No action is required	Attention State - LED off
5	2008-11-07 10:38:44	Attention State - Identify LED off	Server 3		Info	IPMI	Sensor: Attention State - Identify LED off.	Server Sensor: Attention	No action is required	Attention State - LED off

**Figure 69. System Information Report**

## Service Data

The Service Data window provides the IT administrator with the ability to collect information about the storage subsystem, gigabit switches, or the entire system. This information should be provided to a service technician to troubleshoot any issues with the system. The test report is encrypted and can only be unlocked by a service technician. The test report does not contain user account information.

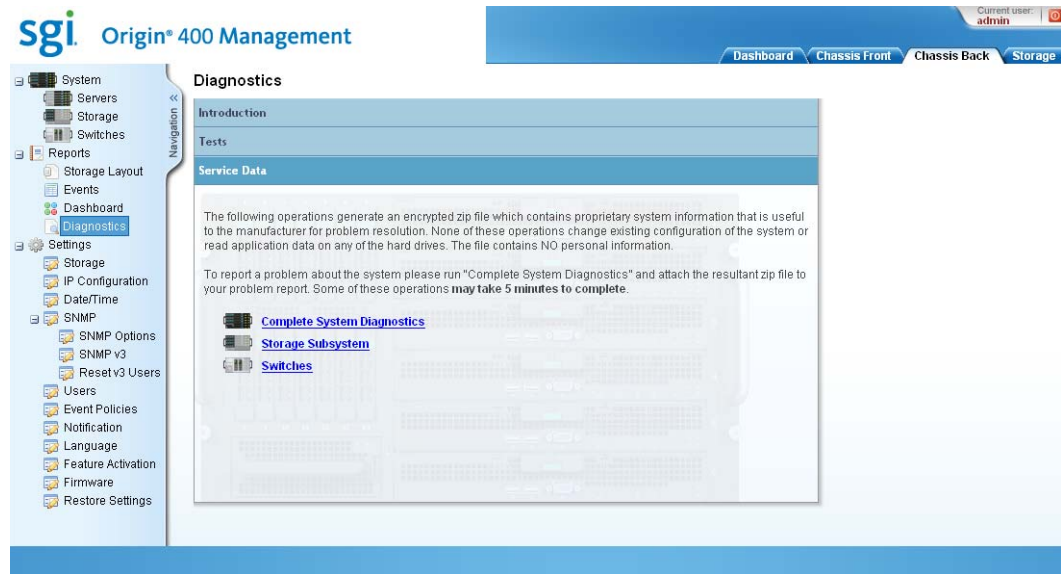


Figure 70. Diagnostics - Service Data

## Settings

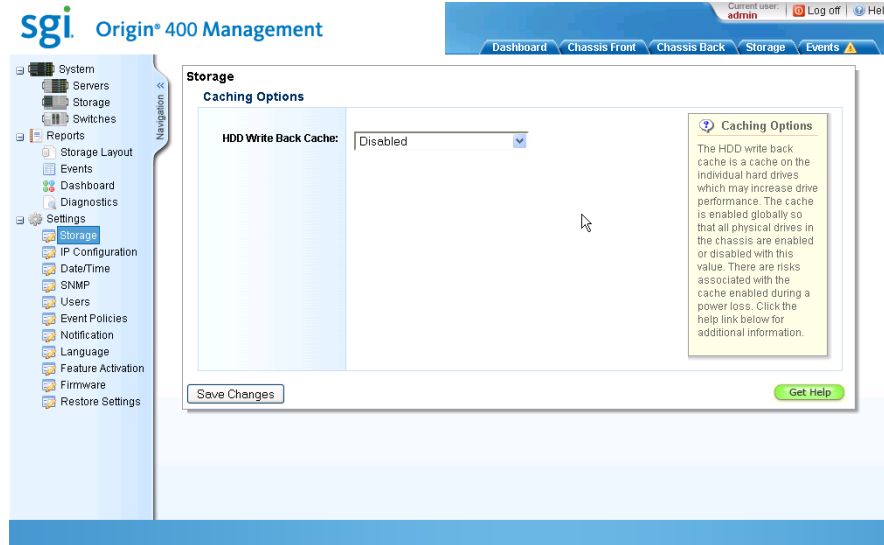
To access the general configuration settings, click Settings in the left navigation panel. These screens enable an IT administrator to modify and view general system settings for maintenance and hardware management.

## Storage Drive Caching Options

Every physical hard drive in the chassis has an on-board cache. The cache generally improves the I/O performance of a drive by acting as a fast data buffer during large read and write operations.

This is a chassis-wide setting, that is, all drive write-back caches are either enabled or all are disabled.

Drive write-back cache is disabled by default because there are some risks involved. In the case of a sudden power loss to the chassis, all hard drives would immediately power off. If there were data in a cache waiting to be written to the drive, it would be lost and unrecoverable. To avoid this situation, provide a power backup (such as an UPS) for the chassis. The backup power supply should be capable of and configured to trigger an orderly shutdown of each server in the chassis.



**Figure 71. Settings - Storage Caching Options Configuration**

## IP Configuration

The SGI management module has two gigabit Ethernet connections to each gigabit Ethernet switch. These internal connections allow the management module to communicate to the switch module and the external network. The external IP address allows remote browsers to connect to the Origin 400 Management Center and sets the source IP address for email alerts and SNMP traps.

The factory default IP address is 192.168.150.150. The default netmask is 255.255.255.0.

The IP Configuration screen enables an IT Administrator to change the SGI management module host name and external network access, as well as view the internal configuration. The following is a description of the settings and information found in the IP Configuration tab:

- Host Name: Change the management module host name.
- MAC Address: Displays the MAC address for the management module.
- Method: Choose between static-Address or Automatic-DHCP. The initial management module IP address is set to the static IP address of 192.168.150.150. This IP address may be set to DHCP or a different IP address to enable access within an existing network environment.
- External IP configuration settings: IP address, netmask, gateway IP, DNS 1 (Enter Domain Name Server IP Address, if applicable), DNS 2 (Alternate Domain Name Server)
- Internal IP configuration information for the management module is displayed as read only.

To access the IP Configuration screen, click Settings > IP Configuration in the left navigation panel. The Origin 400 Management Center IP Configuration screen similar to the following image is displayed.

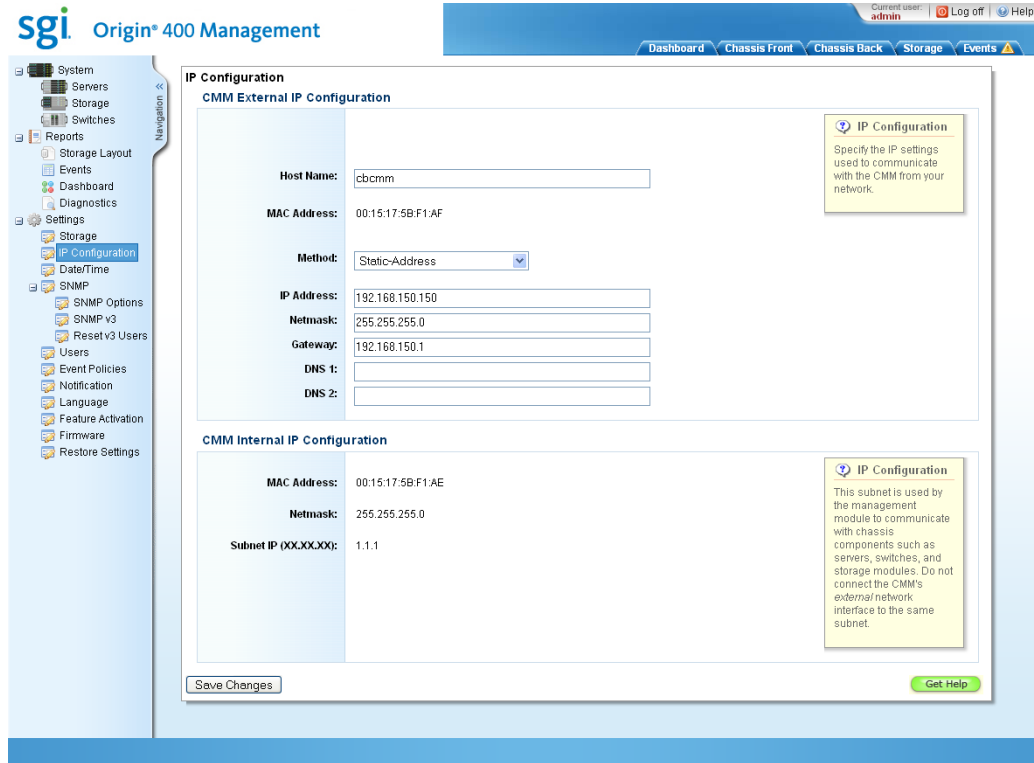


Figure 72. Settings - IP Configuration

## Date and Time

The Date and Time setting enables an IT administrator to directly set the date and time or specify a network time server to set the date and time on the management module. The new date and time will be displayed once the management module is reset.

The screenshot displays the 'sgl Origin® 400 Management' web interface. The top navigation bar includes 'Dashboard', 'Chassis Front', 'Chassis Back', 'Storage', and 'Events'. The left sidebar shows a navigation tree with categories like System, Reports, Settings, and SNMP. The main content area is titled 'Time' and contains three sections: 'CMM Date/Time', 'Time Server', and 'Time Zone'. Each section has a configuration area and a help box. The 'CMM Date/Time' section shows the current date and time as '05/20/09 06:19:26' and a 'Set Current Date/Time' button with a calendar icon. The 'Time Server' section has a 'Network Time Server' text input field. The 'Time Zone' section has a 'Time Zone' dropdown menu set to 'Greenwich Mean Time (GMT)'. A 'Save Changes' button is located at the bottom of the configuration area.

Figure 73. Settings - System Date and Time Configuration

## Steps to Manually Update the Origin 400 System Date and Time

**Note:** Use the manual setting only if the network time server is not configured.

1. Click Settings > Date/Time in the left navigation panel.
2. Click the Calendar icon and follow the instructions in the bottom pane of the calendar.



**Figure 74. Calendar**

3. To change the date, click the buttons beneath the printed month to change the Year and Month.
  - Click the single right angle bracket (>) to increment to the next Month; click the single left angle bracket (<) to decrement to the previous Month.
  - Click the double right angle bracket (>>) to increment to the next Year; click the double left angle bracket (<<) to decrement to the previous Year.
4. To change the time, click the values in the Hour, Minute and AM/PM box next to Time as follows:
  - To increment the Hour value, click the Hour value or drag the mouse to the right.
  - To decrement the Hour value, hold the <Shift> key and click the Hour value or drag the mouse to the left.
  - To increment the Minute value, click the Minute value or drag the mouse to the right.
  - To decrement the Minute value, either hold the <Shift> key and click the Minute value or drag the mouse to the left.
  - Click am/pm to set the time in am or pm, as required. The button toggles between the two options.
5. Click Save Changes.

In the Update dialogue box **Update** and **Reboot**. This action will reset the management module to enable the changes to take effect.



## Steps to Add a Network Time Server

1. Click Settings > Date/Time in the left navigation panel.
2. Enter the IP address or DNS hostname for the network time server.
3. Click Save Changes.

In the Update dialogue box **Update** and **Reboot**. This action will reset the management module to enable the changes to take effect.

## Steps to Change the Time Zone

1. Click Settings > Date/Time in the left navigation panel.
2. Select the Time Zone to be used for displaying the date and time.
3. Click Save Changes.

In the Update dialogue box **Update** and **Reboot**. This action will reset the management module to enable the changes to take effect.

## Simple Network Management Protocol (SNMP)

The Origin 400 system supports Simple Network Management Protocol (SNMP). An IT administrator can view system configuration settings and health information using either SNMP v2 or SNMP v3. However, an IT administrator cannot configure the Origin 400 system via SNMP. Full hardware management and configuration is supported via the Origin 400 Management Center interface. For more information regarding SNMP v2 and SNMP v3 support for the installed Unified Firmware Update (UFU) release, refer to your SGI Technical Support representative.

## SNMP Options

The Simple Network Management Protocol (SNMP) settings allow external SNMP management applications to communicate with the SNMP agent on the management module. The SNMP Options must be configured in order to use SNMP v2, SNMP v3, or both SNMP v2 and SNMP v3.

The screenshot displays the 'SNMP' configuration page in the SGI Origin 400 Management interface. The 'Agent' section includes a dropdown for 'SNMPv2 Support' (set to 'enabled'), and text input fields for 'Public Community' (public), 'Sys Location' (Office), 'Admin Contact' (Admin), and 'Sys Description' (Intel Modular Server System). The 'SNMP Trap Destination' section features four sets of input fields for 'SNMP 1-4 IP' and 'Community'. A 'Send a Test Trap' button is located below these fields. A 'Save Changes' button is at the bottom left, and a 'Get Help' button is at the bottom right. A yellow callout box titled 'SNMP Settings' provides instructions on forwarding traps to external agents, with an example: 'E.g. IP: 10.0.0.1:111, Community: public' and a note that 'Community string may not contain spaces.' The left sidebar shows a navigation tree with 'SNMP Options' selected. The top right shows the user is 'admin' and there are links for 'Log off' and 'Help'.

Figure 75. SNMP Options

## Agent

The first option on the screen in the Agent section is to enable or disable SNMP v2. By default, this setting is set to enabled. The Origin 400 system supports read-only access to system information via SNMP v2. To use SNMP v3, SNMP v2 does not need to be enabled; however, before changing this setting, you must verify that your management software does not require SNMP v2 access.

The Public Community string entered in the Agent section must match the community string on the remote management console.

## SNMP Trap Destination

The SNMP Trap Destination section enables an IT administrator to send traps/events to four separate remote management applications. If Event Policies are configured to send SNMP Traps, you must set the SNMP Trap Destination settings for at least one destination.

To configure the SNMP Trap destination, enter the IP address and Community string for each destination. By default, SNMP uses port 162. To specify a different port in the destination IP setting, enter the IP address followed by a colon (:), followed by the port number (for example, 10.7.155.62:162).

To verify the SNMP trap destination settings, click the Send a Test Trap button and verify that the trap was received by the target system.

## SNMP V3

SNMP v3 adds additional authentication and privacy features to SNMP v2. The Authentication feature provides a means to verify users or agents and the privacy feature provides a way to encrypt the data to prevent unauthorized disclosure.

The SNMP v3 Access screen enables the IT administrator to configure an SNMP v3 user account with these additional authentication and privacy features. However, to use SNMP v3, you must also configure the SNMP v2 settings on the SNMP Options screen.

**Note:** You do not need to enable the SNMP v2 Support option in order to use the SNMP v3 features.

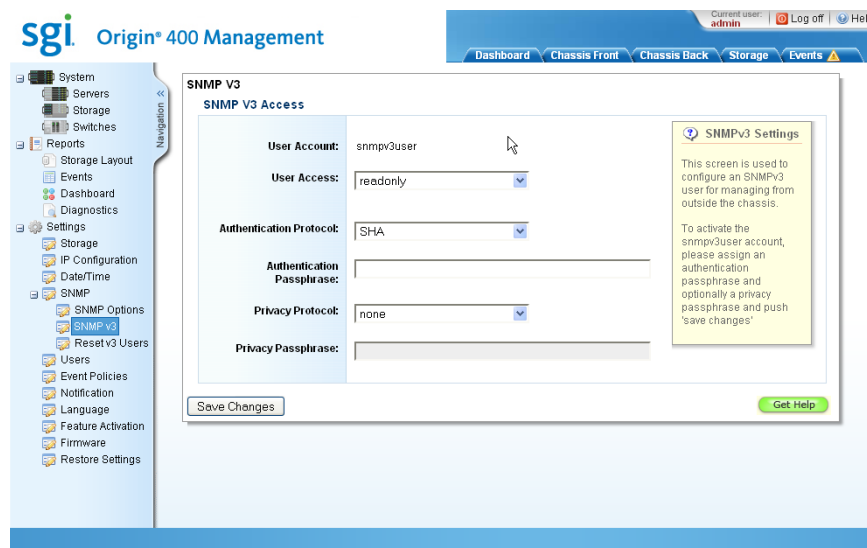


Figure 76. SNMP V3

To configure an SNMP v3 user account on the SNMP v3 Access screen, you must first set User Access to either read-only or read-write. With read-only access, an SNMP v3 user account can view system settings remotely. With read-write access, an SNMP v3 user account can view system settings remotely and change the SGI compute module's power state (on/off) and identify LED (on/off). Read/write access does not enable an SNMP v3 user account to remotely configure the Origin 400 system. Full hardware management and configuration is only supported via the Origin 400 Management Center.

**Note:** For more information regarding SNMP v3 support for the installed Unified Firmware Update (UFU), refer to your SGI Technical Support representative.

To activate the SNMP v3 user account, configure the authentication and privacy settings on this screen. First, select the authentication protocol and set the Authentication passphrase. The authentication protocol is used by the management console to authenticate the user account. Select either Secure Hash Algorithm (SHA) or Message-Digest Algorithm 5 (MD5). By default, SHA is selected. Next, select the Privacy protocol and assign the privacy passphrase. The privacy protocol is used to encrypt the SNMP data. Select either DES, AES, or none. By default, none is selected.

## Reset SNMP V3

The Reset SNMP v3 screen enables an IT administrator to delete all SNMP v3 users and recreate all internal-chassis management users. Use this procedure if an outside SNMP tool has modified or deleted the internal-chassis management users. This procedure may take up to a minute to complete. To reactivate the SNMP v3, go to the SNMP v3 settings screen.

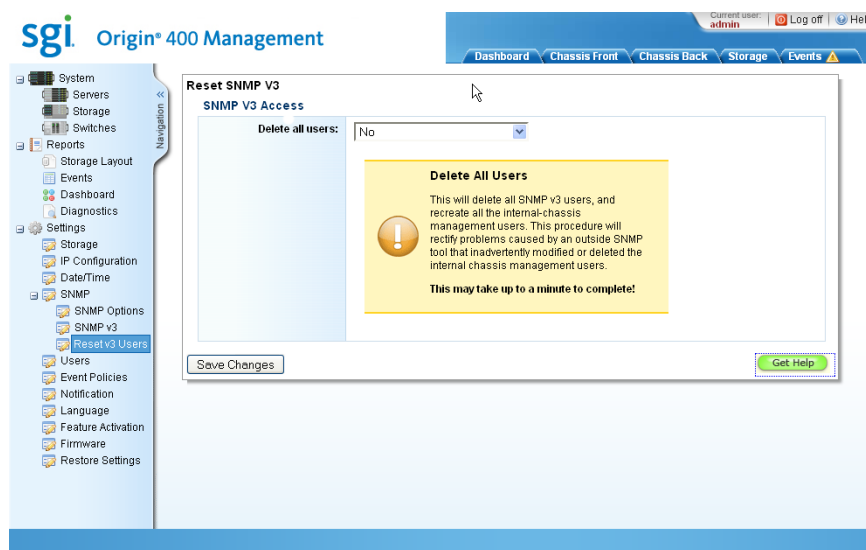


Figure 77. Reset SNMP v3

## User Accounts

The Origin 400 Management Center I supports both administrator and user accounts. To create a new account or modify an existing account click Settings then User Accounts in the left navigation menu. An administrator account is enabled by default to allow the IT administrator to access the Origin 400 Management Center for initial configuration. It is recommended that the default administrator password is changed before adding the Origin 400 to the production network. The administrator password supports a maximum of 10 characters. Supported characters are limited to letters, numbers and the following special characters ! @ # \$ ^ & \* + - = \_ . ?. User Account passwords do not have these restrictions. For more information regarding default login accounts, see [Section , “Log in to the Origin 400 Management Center”](#) on page -56



**Figure 78. Settings - User Account Configuration Screen**

## Event Policies

The Event Policy screen enables the IT administrator to configure event severity and notification process. To configure an event policy, click Edit for a specific event. The Edit dialog box appears. Use the dialog box to change the severity of a specific event, as well as to select who to notify when the event occurs.

Dashboard Chassis Front Chassis Back Storage Events

Event Policy Definitions Severity: Info+ Rows: 10 (1-10) of 752

Toggle notification for selected: Log Email SNMP Export All: XML CSV Help

Component Class	Event Code/ID	ID	Subsys	Type	Severity	Brief Description	Log Every	Log	Email	SNMP	act
39	2293760	3493	Virtual Drive Copy	Storage	Info	Source and target association created for virtual drive copy operation	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit
39	2293763	3495	Virtual Drive Copy	Storage	Warning	Virtual drive copy operation failed	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit
39	2293764	3496	Virtual Drive Copy	Storage	Info	Virtual drive copy operation stopped by user	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit
39	2293765	3497	Virtual Drive Copy	Storage	Info	Virtual drive copy operation paused by user	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit
39	2293766	3498	Virtual Drive Copy	Storage	Info	Virtual drive copy operation resumed by user	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit
39	2293767	3498	Virtual Drive Copy	Storage	Info	Source and target virtual drive association has been removed	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit
39	2293768	3500	Virtual Drive Copy	Storage	Warning	Virtual drive copy operation in Disjoint state	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit
39	2293769	3501	Virtual Drive Copy	Storage	Warning	Virtual drive copy operation in Inconsistent state	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit
39	2293770	3502	Virtual Drive Copy	Storage	Info	Virtual drive copy operation completed	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit
CMM	2293761	3494	Virtual Drive Copy	Storage	Info	Virtual drive copy operation started	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	edit

Figure 79. Settings - Event Policies Configuration Screen

## Notification

The Notification screen enables an IT administrator to configure the SGI management module to send alert messages to users by going through a Simple Mail Transport Protocol (SMTP) email server and to send system events to an external syslog server.

### Steps to configure the SGI management module to send email alert messages to users

1. Click Settings > Notifications in the left navigation panel.
2. Enter the SMTP Mail Server Address.
3. Enter the Mail Sender Address (the “from” address).
4. Click Send a Test Email to ensure the SGI management module is able to send emails.
5. Click Save Changes to save the changes.

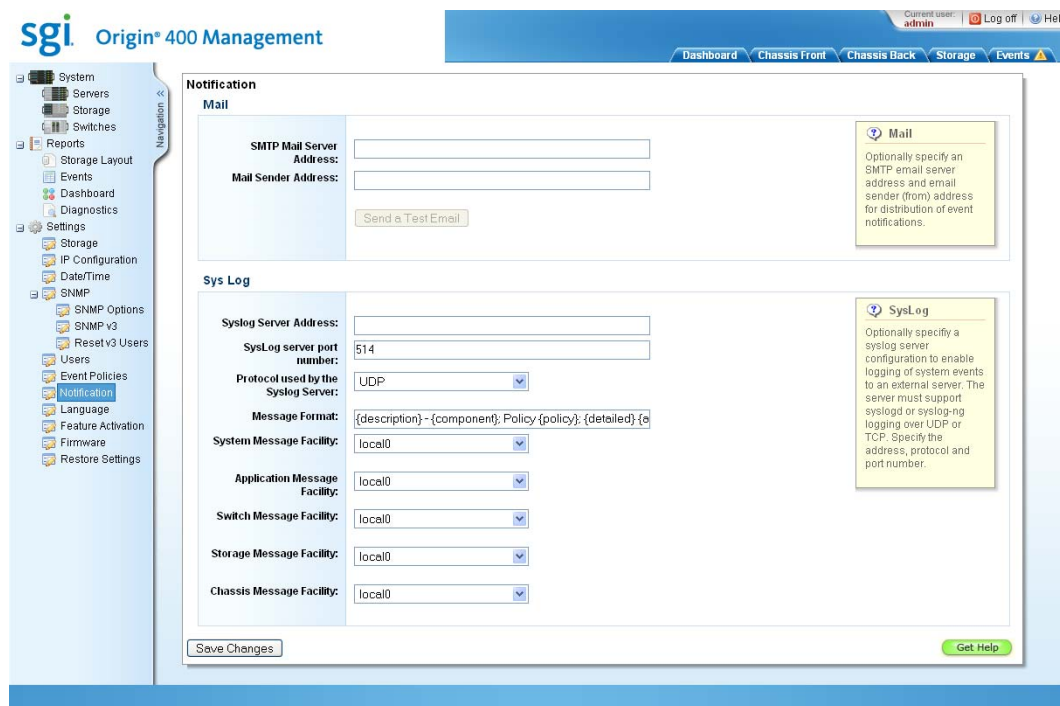
To configure the email destination address and control the email notification settings for each user account, see [“User Accounts” on page 123](#)

To configure the events that generate email notifications, see [“Event Policies” on page 123](#).

### Steps to configure the SGI management module to forward system events to an external syslog server

1. Click Settings > Notifications in the left navigation panel.
2. Enter the Syslog Server Address.
3. Enter the SysLog server port number.
4. Select the protocol used by the syslog server (UDP or TCP). The syslog server must support either syslogd or syslog-ng logging using either UDP (User Datagram Protocol) or TCP (Transmission Control Protocol).
5. Enter message format. The default format is as follows:
  - Event Description
  - Component
  - Event Policy information including detailed description and action information
6. Select the System Message Facility.
7. Select the Application Message Facility.
8. Select the Switch Message Facility.
9. Select the Storage Message Facility.
10. Select the Chassis Message Facility.

11. Click Save Changes to save the changes in the settings.



**Figure 80. Settings - Notification Screen**

## Language Option Setting

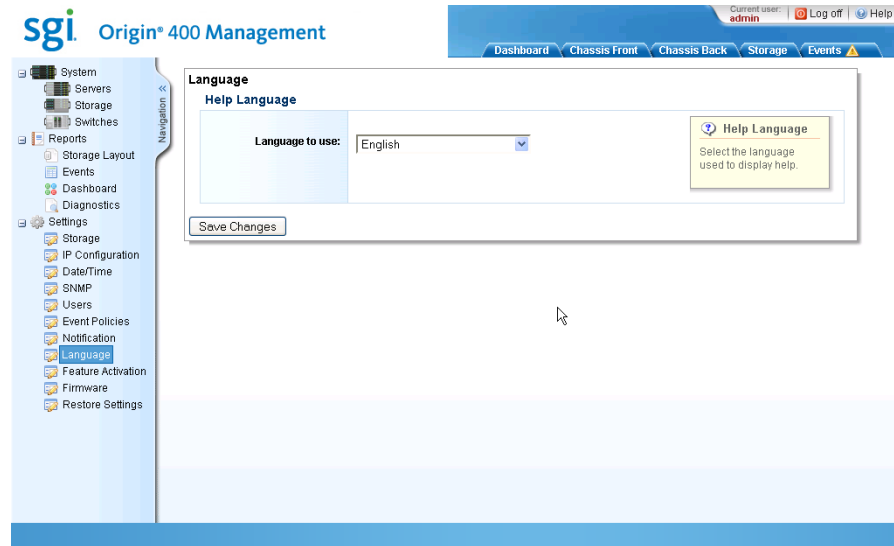
The Origin 400 Management Center provides the capability to change the language for the on-line help content. Available languages are:

- English
- Russian
- Simplified Chinese

### Steps to change the language of the on-line help

1. Click Settings > Language in the left navigation panel.
2. Select a language for the online help.
3. Click Save Changes to save the changes.





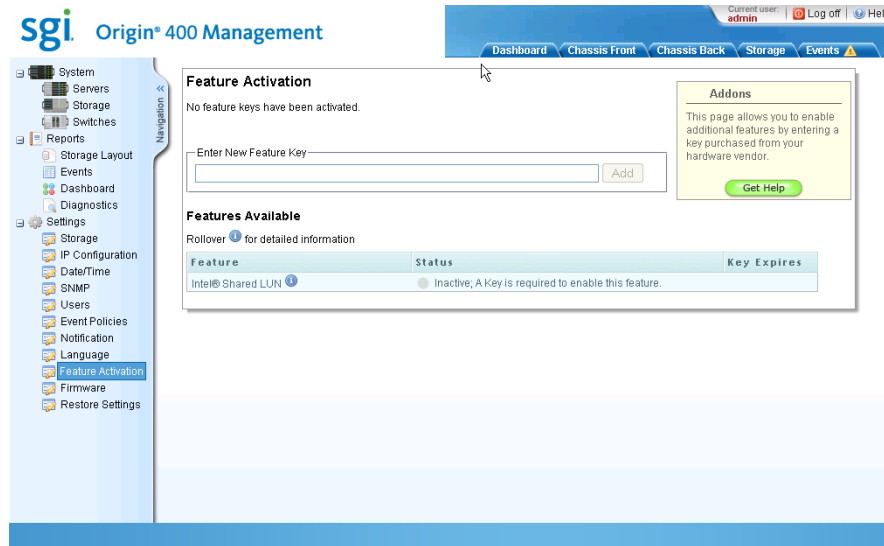
**Figure 81. Settings - Help Language Selection**

## Feature Activation

The Origin 400 Management Center provides the capability to activate features using a feature activation code or key. The SGI shared LUN feature allows two or more servers to share a virtual drive. This feature requires operating system support for sharing LUNs and requires activation before you can use it.

### Steps to activate a feature

1. Obtain a feature activation code or key. Contact your SGI Sales representative for information on how to obtain a key.
2. Click Settings > Feature Activation in the left navigation panel.
3. Enter your activation code.
4. Click Add.



**Figure 82. Settings - Feature Activation**

## Firmware Updates

The Origin 400 Management Center provides a simple interface to update the system firmware from a single compressed update package released by SGI called a UFU (Unified Firmware Update). In addition to providing an easy-to-use interface to update the firmware for the entire system, this screen will display all currently installed component firmware versions, as well as current status. This will enable the IT administrator to quickly view the installed versions and determine if an update is required.

The Unified Firmware Update supports firmware updates for the management module, storage control modules, switch modules, fans, server BIOS, and firmware.

**Firmware**  
 Current Build Version: 3.0.100.20090504.17040  
 Prior Version: 2.6.100.20081104.14276

**Upload New Firmware**

**Firmware Inventory**  
 Rollover ⓘ for detailed information

Component	Subsystem	Status	Current Version
Server 1	BMC Firmware	ok	1.15.1
	BMC Boot	ok	0.25
	BIOS	ok	S5500.86B.01.10.0034.050420091255
Server 2	BMC Firmware	ok	1.35.30
	BMC Boot	ok	0.9
	BIOS	ok	SB5000.86B.10.10.0048.112120081113
Server 3	BMC Firmware	ok	1.35.30
	BMC Boot	ok	0.9
	BIOS	ok	SB5000.86B.10.10.0048.112120081113
Server 4	BMC Firmware	ok	1.35.30
	BMC Boot	ok	0.9
	BIOS	ok	SB5000.86B.10.10.0048.112120081113
Server 5	BMC Firmware	ok	1.35.30
	BMC Boot	ok	0.9
	BIOS	ok	SB5000.86B.10.10.0048.112120081113
Server 6	BMC Firmware	ok	1.35.30
	BMC Boot	ok	0.9
	BIOS	ok	SB5000.86B.10.10.0048.112120081113
Switch 1	Firmware	ok	1.0.0.27
	Boot	ok	1.0.0.6
Switch 2	Firmware	not present	--
	Boot	not present	--
Storage Control Module 1	Firmware	ok	3.2.140.15
Storage Control Module 2	Firmware	ok	3.2.140.15
System Fan 1	Firmware	ok	1.2
System Fan 1	Boot	ok	1.2
	Firmware	ok	1.2
System Fan 2	Boot	ok	1.2
	Firmware	ok	1.2
I/O Fan	Boot	ok	1.2
	Firmware	ok	1.2
Power Supply 1	Boot	not applicable ⓘ	--
	Firmware	not applicable ⓘ	--
Power Supply 2	Boot	not applicable ⓘ	--
	Firmware	not applicable ⓘ	--
Power Supply 3	Boot	not applicable ⓘ	--
	Firmware	not applicable ⓘ	--
Power Supply Blank 4	Boot	ok	1.2
	Firmware	ok	1.2

**Figure 83. Settings - Firmware Update Screen**

### Steps to Update the System Firmware

1. Click Settings > Firmware in the left navigation panel.
2. In the Upload New Firmware section, click Browse.
3. Select the file from the console system. File must be accessible from the console system.

Refer to your SGI Technical Support representative for detailed instructions on how to update the system firmware.

## Restore System Settings

It may be necessary to restore your system configuration to an earlier time or to factory defaults. The following settings are affected:

- Users and passwords used to access the user interface.
- Network configuration (management module IP address)
- Event policies
- Notification settings (email addresses)
- SNMP configuration

To restore system settings, click Settings > Restore Settings in the left navigation panel.

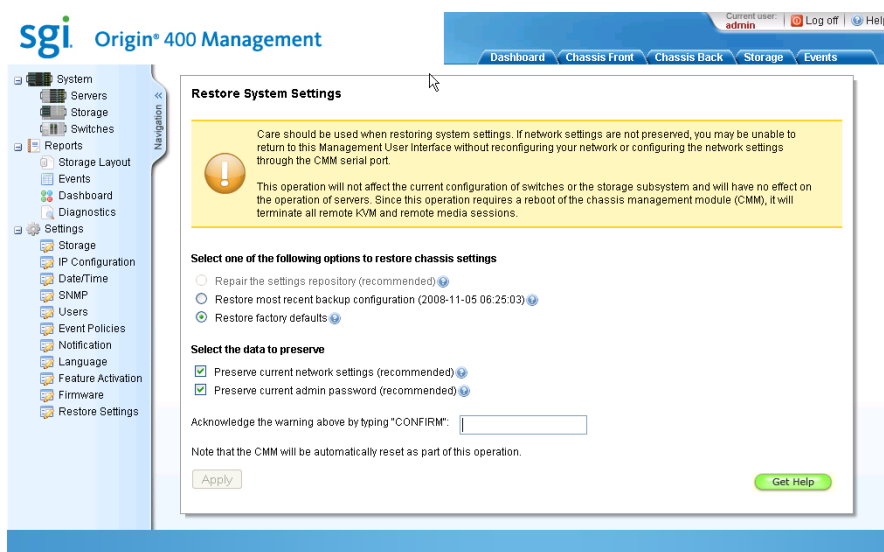


Figure 84. Settings - Restore System Settings

## Restore Options

One of the following three methods may be used to restore system settings:

### 1. Repair the settings repository

It is possible, but rare, for system settings to become corrupt after an unexpected chassis power loss. This option is only available to the administrative user and only when system settings are actually corrupt.

After selecting this option and clicking **Apply**, the management module will reset. As the management module boots, the settings will be repaired. If this operation is unsuccessful, the management module will automatically attempt to restore the most recent backup settings (see explanation below).

### 2. Restore the most recent backup

System settings are automatically backed up each time the management module is reset or inserted into the chassis, and backups are made daily thereafter. Choose this

option to revert to the most recent backup configuration. The dialog indicates the date of the last known backup.

After selecting this option and clicking **Apply**, the management module will reset. As the management module boots, the backup settings will be applied. If this process fails, the management module settings will be automatically restored to factory defaults corresponding to the installed firmware version (see explanation below).

### 3. Restore factory defaults

Removes all setting changes made by the customer and clears the event log. All user accounts other than the administrative user will be removed. Restores factory defaults corresponding to the installed firmware version (which may differ from the original defaults set in the factory if the chassis firmware has been updated).

After selecting this option and clicking **Apply**, the management module will reset. As the management module boots, factory defaults are restored.

## Preserving Critical Data

The following two additional options may be selected to preserve certain settings that may be difficult to reconfigure:

### 1. Preserve current network settings

If network settings are not preserved, you may be unable to return to the user interface without reconfiguring your network or configuring the network settings through the management module serial port.

### 2. Preserve current administrative password

If the password for the administrative account is not preserved, you will need to either log in to the user interface using the administrative account password saved at the time of the backup if “Restore most recent backup configuration (date and time stamp)” is selected, or use the factory default password if “Restore factory defaults” is selected. If restoring from factory defaults, check the user manual for the factory default password (this password is not affected by any prior firmware updates).

## Access Online Help

The Help link located at the top right of the banner opens the Origin 400 Management Center Help in a new window. Use the table of contents to quickly access help and tips for specific screens and functions.

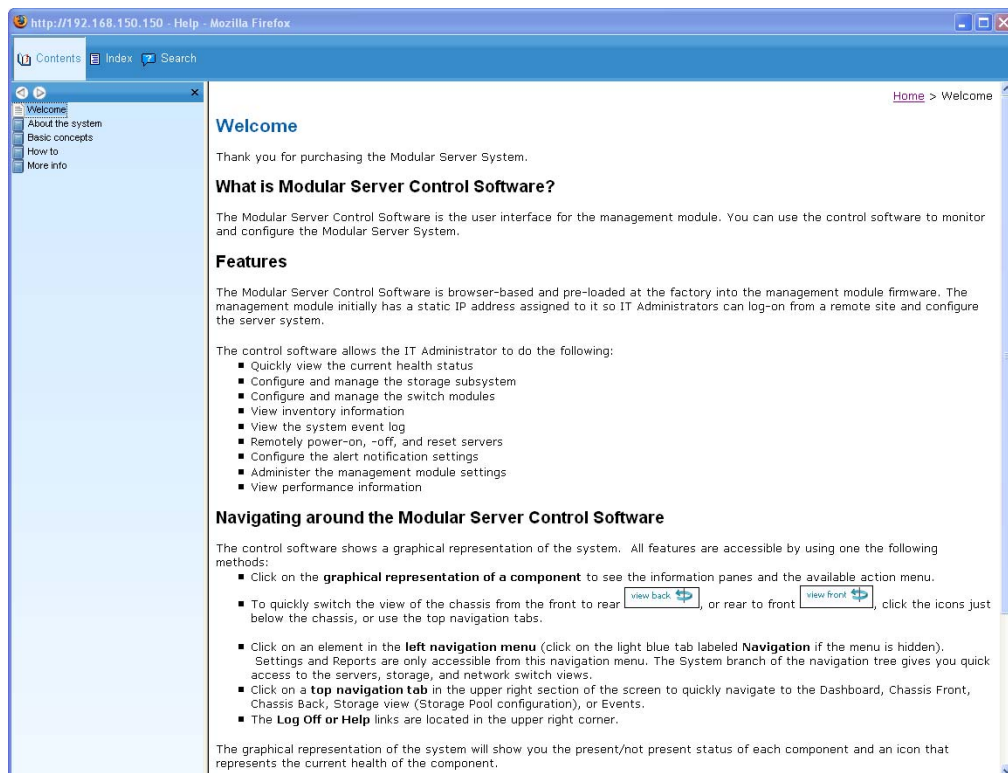


Figure 85. Online Help

## Log Out from the Origin 400 Management Center

The Log Off link is located at the top right of the banner. Clicking it ends the current Origin 400 Management Center session and returns the user to the login screen.

# 5 Troubleshooting

---

This chapter provides information to assist in troubleshooting the Origin 400 system.

A common cause of system function issues is outdated firmware. Before performing extensive troubleshooting steps, ensure that all installed system components are configured with current firmware, including the management module, storage control modules and Ethernet switch modules. Also, ensure that the installed compute modules have all been configured with the latest BIOS and BMC firmware code and device drivers. Current firmware and driver packages are available for download from Supportfolio.

## First Steps Checklist

- Is the power LED lit on all modules installed in the Origin 400 system?
- Is the chassis properly connected to an AC power source?
- Are the various chassis modules fully seated?
  - Power supply modules
  - Management module
  - Storage control modules
  - Ethernet switch modules
  - Fan modules
- Are the installed compute modules fully seated?

## Specific Issues and Corrective Actions

This section provides possible solutions for these specific problems:

- Chassis fan module not functioning
- Cannot connect to management module
- Cannot connect to a compute module
- Cannot connect a compute module to a storage control module

Try the following solutions in the order given. If you still cannot correct the problem, contact your service representative or authorized dealer for help.

### Chassis Fan Module Not Functioning

Check the following:

- Is only a single fan in error? If so, check the power and fault LEDs.

- Is the power LED on? If not, re-seat the fan module. If so, check the fault LED.
- Is the fault LED on? Check the status of the system using the Origin 400 Management Center.
- Are both fan modules in error? If so, verify that the power supply modules are properly installed and connected to grounded AC outlets.

## Cannot Connect to the Management Module

Check the following:

- Is the power LED lit?
  - If not, is it the only module in the system with an unlit power LED?
    - If so, reseat the module, or try replacing it with a different module.
    - If not, verify that the chassis power supply modules are properly installed and connected to grounded AC outlets.
  - Is the fault LED lit?
    - If so, re-seat the module, or try replacing it with a different module.
    - If not, verify that the chassis power supply modules are properly installed and connected to grounded AC outlets.
- Is the Ethernet management port connected to the network?
  - If yes, is the cable good? Try replacing the cable.
  - If yes, is the management module configured properly for the network to which it is connected? Try resetting the management module by pushing the management module reset button.

## Cannot Connect to a Compute Module

Check the following:

- Verify that all jumpers are located in the proper default positions (CMOS Clear J1F2: default pins 1-2; BMC Force Update J7A1: default pins 2-3).
- Is the compute module powered on and operating normally?
  - If so, is an operating system installed on the compute module?
  - If so, is the operating system installed on the compute module operating properly and configured properly for the network?
  - Verify that both the compute module and the client are connected to the correct physical LAN and VLAN?
- Is the power LED lit on the Ethernet switch module?
  - If not, try to re-seat the switch module.
  - If so, check the fault LED on the switch module.
- Is the power fault LED lit on the Ethernet switch module?



- If so, check the status of the system using the Origin 400 Management Center.
- If not, check the switch port link.
- Is the switch connected to the network by way of an Ethernet cable?
  - If not, connect the switch to the network.
  - If so, verify that the link light is lit for the connected port.
- Is the link light lit for the connected port?
  - If not, move the Ethernet cable to a different port. If the link light on the other port does not light, replace the cable.

If the switches and connections are correct and AC power is available at the wall outlet, contact your service representative or authorized dealer for additional help.

## **Cannot Connect a Compute Module to a Storage Control Module**

Check the following:

- Verify that storage space in the storage control module has been allocated for and assigned to the compute module.
- Make sure the drive(s) assigned to the compute module are installed and operating properly.
- Make sure the installed drives were bought from SGI as Origin 400 drives. For more information, refer to your SGI Sales representative.
- Check the status of the system using the Origin 400 Management Center.

## **Diagnostic LED Information**

The various modules and compute modules designed for use with the Origin 400 system provide a number of diagnostic LEDs that may aid in troubleshooting your system. A list of these LEDs, with usage descriptions for each LED, is provided in the following two tables.

**Table 31. Diagnostic LEDs**

<b>LED Name</b>	<b>Function</b>	<b>Location</b>	<b>Color</b>	<b>Indicator</b>
Chassis ID LED	Aids in server identification from the back panel	Chassis front	Blue	Press ID LED button or use the Origin 400 Management Center to turn off the LED.
System Fault LED	Visible fault warning	Chassis front	Amber	Green = No Fault Green Blink = Degraded Amber = Critical error or non-recoverable Amber blink = Non-critical
Hard Drive Power/Activity LED	Identifies the power state of the hard drive, indicate drive activity	Hard drive carrier front panel	Green	On = Hard drive power on Green Blink = Hard drive activity
Hard Drive Fault LED	Visible fault warning	Hard drive carrier front panel	Amber	On = Hard drive fault
I/O Cooling Module Power LED	Identifies the power state of the I/O cooling module	I/O cooling module front panel	Green	On = Cooling module power on
I/O Cooling Module Fault LED	Visible fault warning	I/O cooling module front panel	Amber	On = I/O cooling module fault
Fan Module Power LED	Identifies the power state of the fan module	Fan module front panel	Green	On = Fan module power on
Fan Module Fault LED	Visible fault warning	Fan module front panel	Amber	On = Fan module fault
Storage Control Module Power LED	Identifies the power state of the storage control module	Storage control module front panel	Green	On = Storage control module power on
Storage Control Module Fault LED	Visible fault warning	Storage control module front panel	Amber	On = Storage control module fault
Storage Control Module Dirty Cache LED	Identifies the state of storage control module cache	Storage control module front panel	Green	Slow blink = Dirty cache
Ethernet Switch Module Power LED	Identifies the power state of the Ethernet switch module	Ethernet switch module front panel	Green	On = Ethernet switch module power on
Ethernet Switch Module Fault LED	Visible fault warning	Ethernet switch module front panel	Amber	On = Ethernet switch module fault

Ethernet Switch Module Port Link/Activity LED	Active Ethernet Port Link	Ethernet switch port	Green	On green = Link Blinking Green = Port activity
Management Module Power LED	Identifies the power state of the management module	Management module front panel	Green	On = Management module power on
Management Fault LED	Visible fault warning	Management module front panel	Amber	On = Management module fault
Power Supply Module Power LED	Identifies the power state of the Power Supply module	Power supply module front panel	Green	On = Power supply module power on
Power Supply Fault LED	Visible fault warning	Power supply module front panel	Amber	On = Power supply module fault

**Table 32. NIC LEDs**

LED Color	LED State	Description
Left LED	Off	No network connection
	Solid Amber	Network connection in place
	Blinking Amber	Transmit/receive activity
Right LED	Off	10 Mbps connection (if Left LED is on or blinking)
	Solid Amber	100 Mbps connection
	Solid Green	1000 Mbps connection



# A Product Regulatory Requirements

---

## Regulatory and Certification Information

---

### WARNING

---

To ensure regulatory compliance, you must adhere to the assembly instructions in this guide to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this guide. Use of other products / components will void the UL listing and other regulatory approvals of the product and will most likely result in noncompliance with product regulations in the regions) in which the product is sold.

To help ensure EMC compliance with your local regional rules and regulations, before computer integration, make sure that the chassis, power supply, and other modules have passed EMC testing using a server board with a microprocessor from the same family (or higher) and operating at the same (or higher) speed as the microprocessor used on this server board. The final configuration of your end system product may require additional EMC compliance testing. For more information please contact your local SGI Representative.

This is an FCC Class A device. Integration of it into a Class B chassis does not result in a Class B device.

---

## Product Regulatory Compliance

The Server Chassis product, when correctly integrated per this guide, complies with the following safety, electromagnetic compatibility (EMC), and Product Ecology regulations and requirements.

**Intended Application** - This product was evaluated as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product categories and environments (such as: medical, industrial, telecommunications, NEBS, residential, alarm systems, test equipment, etc.), other than an ITE application, may require further evaluation.

## Product Safety Compliance

UL60950 - CSA 60950(USA / Canada)  
EN60950 (Europe)  
IEC60950 (International)  
CB Certificate & Report, IEC60950 (report to include all country national deviations)  
GS Certification (Germany)  
GOST R 50377-92 - Certification (Russia)  
Belarus Certification (Belarus)  
Ukraine Certification (Ukraine)  
CE - Low Voltage Directive 73/23/EEE (Europe)  
IRAM Certification (Argentina)  
GB4943- CNCA Certification (China)

## Product EMC Compliance - Class A Compliance

FCC /ICES-003 - Emissions (USA/Canada) Verification  
CISPR 22 - Emissions (International)  
EN55022 - Emissions (Europe)  
EN55024 - Immunity (Europe)  
EN61000-3-2 - Harmonics (Europe)  
EN61000-3-3 - Voltage Flicker (Europe)  
CE - EMC Directive 89/336/EEC (Europe)  
VCCI Emissions (Japan)  
AS/NZS 3548 Emissions (Australia / New Zealand)  
BSMI CNS13438 Emissions (Taiwan)  
GOST R 29216-91 Emissions (Russia)  
GOST R 50628-95 Immunity (Russia)  
Belarus Certification (Belarus)  
Ukraine Certification (Ukraine)  
KCC Notice No. 1997-41 (EMC) & 1997-42 (EMI) (Korea)  
GB 9254 - CNCA Certification (China)  
GB 17625 - (Harmonics) CNCA Certification (China)

## Product Ecology Compliance

SGI has a system in place to restrict the use of banned substances in accordance with world wide regulatory requirements. A Material Declaration Data Sheet is available for SGI products. For more reference on material restrictions and compliance you can view SGI's Environmental Product Content Specification by contacting SGI Sales.

### Europe - European Directive 2002/95/EC

Restriction of Hazardous Substances (RoHS)  
Threshold limits and banned substances are noted below.  
Quantity limit of 0.1% by mass (1000 PPM) for:  
Lead, Mercury, Hexavalent Chromium, Polybrominated Biphenyls Diphenyl Ethers (PBB/PBDE)  
Quantity limit of 0.01% by mass (100 PPM) for:  
Cadmium

**California Code of Regulations, Title 22, Division 4.5, Chapter 33:**

Best Management Practices for Perchlorate Materials

**China - Restriction of Hazardous Substances (China RoHS)**

**WEEE Directive (Europe)**

**Packaging Directive (Europe)**

**Certifications / Registrations / Declarations**

UL Certification (US/Canada)

CE Declaration of Conformity (CENELEC Europe)

FCC/ICES-003 Class A Attestation (USA/Canada)

VCCI Certification (Japan)

C-Tick Declaration of Conformity (Australia)

MED Declaration of Conformity (New Zealand)

BSMI Certification (Taiwan)

GOST R Certification / License (Russia)

Belarus Certification / License (Belarus)

KCC Certification (Korea)

IRAM Certification (Argentina)

CNCA Certification (China)

Ecology Declaration (International)

China RoHS Environmental Friendly Use Period

Packaging & Product Recycling Marks

## Regulated Specified Components

To maintain the UL listing and compliance to other regulatory certifications and/or declarations, the following regulated components must be used and conditions adhered to. Interchanging or use of other component will void the UL listing and other product certifications and approvals.

You can find updated product information for configurations by contacting SGI Sales.

1. **Server Chassis:** Base chassis is provided with power supply and fans—UL listed.
2. **Server board:** You must use an SGI server board—UL recognized.
3. **Add-in Boards:** Must have a printed wiring board flammability rating of minimum UL94V-1. Add-in boards containing external power connectors and/or lithium batteries must be UL recognized or UL listed. Any add-in board containing modem telecommunication circuitry must be UL listed. In addition, the modem must have the appropriate telecommunications, safety, and EMC approvals for the region in which it is sold.
4. **Peripheral Storage Devices:** Must be UL recognized or UL listed accessory and TUV or VDE licensed. Maximum power rating of any one device is 19 watts. Total server configuration is not to exceed the maximum loading conditions of the power supply.



## Electromagnetic Compatibility Notice FCC Verification Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

SGI  
46600 Landing Parkway  
Fremont, CA 94538  
Tel: 510-933-830

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

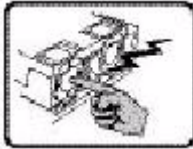

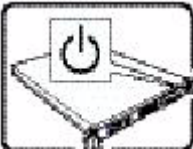

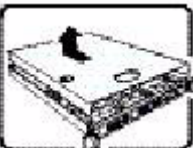
Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

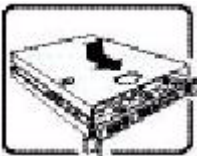
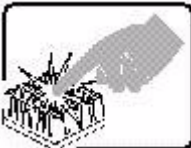

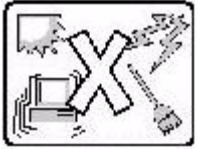
Only peripherals (computer input/output devices, terminals, printers, etc.) that comply with FCC Class A or B limits may be attached to this computer product. Operation with noncompliant peripherals is likely to result in interference to radio and TV reception.

All cables used to connect to peripherals must be shielded and grounded. Operation with cables, connected to peripherals that are not shielded and grounded may result in interference to radio and TV reception.



# B Installation/Assembly Safety Instructions

	<p>The power supply in this product contains no user-serviceable parts. Refer servicing only to qualified personnel.</p>
	<p>Do not attempt to modify or use the supplied AC power cord if it is not the exact type required. A product with more than one power supply will have a separate AC power cord for each supply.</p>
	<p>The power button on the compute module does not turn off system AC power. To remove AC power from the system, you must unplug each AC power cord from the wall outlet or power supply.</p> <p>The power cord(s) is considered the disconnect device to the main (AC) power. The socket outlet that the system plugs into shall be installed near the equipment and shall be easily accessible.</p>
	<p><b>SAFETY STEPS:</b> Whenever you remove the chassis covers to access the inside of the system, follow these steps:</p> <ol style="list-style-type: none"> <li>1. Turn off all peripheral devices connected to the system.</li> <li>2. Turn off each compute module by pressing the power button.</li> <li>3. Unplug all AC power cords from the system or from wall outlets.</li> <li>4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system.</li> <li>5. Provide some electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system-any unpainted metal surface-when handling components.</li> <li>6. Do not operate the system with the chassis covers removed.</li> </ol>
	<p>After you have completed the six SAFETY steps above, you can remove the system covers. To do this:</p> <ol style="list-style-type: none"> <li>1. Unlock and remove the padlock from the back of the system if a padlock has been installed.</li> <li>2. Remove and save all screws from the covers.</li> <li>3. Remove the cover(s).</li> </ol>

	<p>For proper cooling and airflow, always reinstall the chassis covers before turning on the system. Operating the system without the covers in place can damage system parts. To install the covers:</p> <ol style="list-style-type: none"> <li>1. Check first to make sure you have not left loose tools or parts inside the system.</li> <li>2. Check that cables, add-in boards, and other components are properly installed.</li> <li>3. Attach the covers to the chassis with the screws removed earlier, and tighten them firmly.</li> <li>4. Insert and lock the padlock to the system to prevent unauthorized access inside the system.</li> <li>5. Connect all external cables and the AC power cord(s) to the system.</li> </ol>
	<p>A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts. Contact should be made with care. Consider wearing protective gloves.</p>
	<p>Danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the equipment manufacturer. Dispose of used batteries according to manufacturer's instructions.</p>
	<p>The system is designed to operate in a typical office environment. Choose a site that is:</p> <ul style="list-style-type: none"> <li>• Clean and free of airborne particles (other than normal room dust).</li> <li>• Well ventilated and away from sources of heat including direct sunlight.</li> <li>• Away from sources of vibration or physical shock.</li> <li>• Isolated from strong electromagnetic fields produced by electrical devices.</li> <li>• In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.</li> <li>• Provided with a properly grounded wall outlet.</li> <li>• Provided with sufficient space to access the power supply cord(s), because they serve as the product's main power disconnect.</li> </ul>

# C Safety Information

---

## Server Safety Information

This document applies to SGI server boards, SGI server chassis and installed peripherals. To reduce the risk of bodily injury, electrical shock, fire, and equipment damage, read this document and observe all warnings and precautions in this guide before installing or maintaining your SGI server product.




In the event of a conflict between the information in this document and information provided with the product or on the website for a particular product, the product documentation takes precedence.




Your server should be integrated and serviced only by technically qualified persons.

You must adhere to the guidelines in this guide and the assembly instructions in your server manuals to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this guide. Use of other products / components will void the UL Listing and other regulatory approvals of the product, and may result in noncompliance with product regulations in the region(s) in which the product is sold.

## Safety Warnings and Cautions

To avoid personal injury or property damage, before you begin installing the product, read, observe, and adhere to all of the following safety instructions and information. The following safety symbols may be used throughout the documentation and may be marked on the product and / or the product packaging.

<b>CAUTION</b>	Indicates the presence of a hazard that may cause minor personal injury or property damage if the CAUTION is ignored.
<b>WARNING</b>	Indicates the presence of a hazard that may result in serious personal injury if the WARNING is ignored.
	Indicates potential hazard if indicated information is ignored.
	Indicates shock hazards that result in serious injury or death if safety instructions are not followed.
	Indicates hot components or surfaces.

	Indicates do not touch fan blades, may result in injury.
	Indicates to unplug all AC power cord(s) to disconnect AC power
	Please recycle battery

## Intended Application Uses

This product was evaluated as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations. The suitability of this product for other product categories and environments (such as medical, industrial, residential, alarm systems, and test equipment), other than an ITE application, may require further evaluation.

## Site Selection

The compute module is designed to operate in a typical office environment. Choose a site that is:

- Clean, dry, and free of airborne particles (other than normal room dust).
- Well-ventilated and away from sources of heat including direct sunlight and radiators.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your compute module into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.
- Provided with a properly grounded wall outlet.
- Provided with sufficient space to access the power supply cord(s), because they serve as the product's main power disconnect.

## Equipment Handling Practices

Reduce the risk of personal injury or equipment damage:

- Conform to local occupational health and safety requirements when moving and lifting equipment.
- Use mechanical assistance or other suitable assistance when moving and lifting equipment.
- To reduce the weight for easier handling, remove any easily detachable components.

## Power and Electrical Warnings

**Caution:** *The power button, indicated by the stand-by power marking, DOES NOT completely turn off the compute module AC power, 5V standby power is active whenever the compute module is plugged in. To remove power from compute module, you must unplug the AC power cord from the wall outlet. Your compute module may use more than one AC power cord. Make sure all AC power cords are unplugged. Make sure the AC power cord(s) is/ are unplugged before you open the chassis, or add or remove any non hot-plug components.*

*Do not attempt to modify or use an AC power cord if it is not the exact type required. A separate AC cord is required for each compute module power supply.*

*Some power supplies in SGI servers use Neutral Pole Fusing. To avoid risk of shock use caution when working with power supplies that use Neutral Pole Fusing.*

*The power supply in this product contains no user-serviceable parts. Do not open the power supply. Hazardous voltage, current and energy levels are present inside the power supply. Return to manufacturer for servicing.*

*When replacing a hot-plug power supply, unplug the power cord to the power supply being replaced before removing it from the server.*

*To avoid risk of electric shock, turn off the server and disconnect the power cord, telecommunications systems, networks, and modems attached to the server before opening it.*

## Access Warnings

**Caution:** *To avoid personal injury or property damage, the following safety instructions apply whenever accessing the inside of the product:*

- *Turn off all peripheral devices connected to this product.*
- *Turn off the compute module by pressing the power button off.*
- *Disconnect the AC power by unplugging all AC power cords from the chassis or wall outlet.*
- *Disconnect all cables and telecommunication lines that are connected to the compute module.*
- *Retain all screws or other fasteners when removing access cover(s). Upon completion of accessing inside the product, refasten access cover with original screws or fasteners.*
- *Do not access the inside of the power supply. There are no serviceable parts in the power supply. Return to manufacturer for servicing.*
- *Power down the chassis and disconnect all power cords before adding or replacing any non hot-plug component.*
- *When replacing a hot-plug power supply, unplug the power cord to the power supply being replaced before removing the power supply from the chassis.*

**Caution:** *If the compute module has been running, any installed processor(s) and heat sink(s) may be hot. Unless you are adding or removing a hot-plug component, allow the compute module to cool before opening the covers. To avoid the possibility of coming into contact with hot component(s) during a hot-plug installation, be careful when removing or installing the hot-plug component(s).*

**Caution:** *To avoid injury do not contact moving fan blades. If your chassis is supplied with a guard over the fan, do not operate the chassis without the fan guard in place.*

## Electrostatic Discharge (ESD)

**Caution:** *ESD can damage disk drives, boards, and other parts. We recommend that you perform all procedures at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground -- any unpainted metal surface -- on your server when handling parts.*

*Always handle boards carefully. They can be extremely sensitive to ESD. Hold boards only by their edges. After removing a board from its protective wrapper or from the server, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.*

## Other Hazards

### Battery Replacement

**Caution:** *There is the danger of explosion if the battery is incorrectly replaced. When replacing the battery, use only the battery recommended by the equipment manufacturer.*

*Dispose of batteries according to local ordinances and regulations.*

*Do not attempt to recharge a battery.*

*Do not attempt to disassemble, puncture, or otherwise damage a battery.*

### Cooling and Airflow

**Caution:** *Carefully route cables as directed to minimize airflow blockage and cooling problems.*

*For proper cooling and airflow, operate the chassis only with the chassis covers installed. Operating the chassis without the covers in place can damage chassis parts. To install the covers:*

- *Check first to make sure you have not left loose tools or parts inside the chassis.*
- *Check that cables, add-in boards, and other components are properly installed.*
- *Attach the covers to the chassis according to the product instructions.*



## **Laser Peripherals or Devices**

**Caution:** *To avoid risk of radiation exposure and/or personal injury:*

- *Do not open the enclosure of any laser peripheral or device*
- *Laser peripherals or devices are not user serviceable*
- *Return to manufacturer for servicing*

