# Intel® Server Continuity Suite

Version 1.1

## User Guide

G51577-001

# Legal Statements

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS FOR THE PURPOSE OF SUPPORTING INTEL DEVELOPED SERVER BOARDS AND SYSTEMS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

This manual may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This manual as well as the software described in it, is furnished under license and may only be used or copied in accordance with the terms of the license. The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Intel and the Intel logo are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

# Revision History

| Revision Number | Date | Modifications |
|---|---|---|
| 001 | January, 2012 | Initial release. |
| 002 | April, 2012 | Version 1.1 |

# Preface

## About This Document

This document provides information required to configure and use Intel® Server Continuity Suite.

## Target Audience

This guide is intended for system administrators who are responsible to deploy, manage, monitor, and troubleshoot Intel® servers.

## Document Conventions

| Convention | Description | Example |
|---|---|---|
| **Bold** | GUI terms and buttons appear in bold. | Click **Continue**. |
| **Note:** | Notes appear with the prefix **Note:** | **Note:** You can download the application from the Intel® download center. |

# Table of Contents

# List of Figures

# 1 Introduction

## 1.1 Intel® Server Continuity Suite for Business Continuity

Business continuity refers to activities performed day to day to maintain servers for data consistency, availability, reliability, and recoverability. These activities include many repetitive tasks such as change control in hardware management, storage management, continuous system backups, and disaster recovery. Business continuity ensures that critical business functions will be available at all times, providing the ability to continue business operations with minimal disruption or downtime in the advent of natural or accidental disasters.

Intel® Server Continuity Suite (referred as Intel® SCS in the remaining part of this document) is a business continuity suite that allows you to effectively manage and control Intel® servers, to improve the overall operational reliability.

Intel® SCS is a server management solution for small and medium enterprises that helps achieve business continuity. Intel® SCS provides distinct features in a simplified manner, and form a part of an IT administrators' daily needs to manage their servers.

Apart from managing and monitoring the server health, the features of Intel® SCS can be tied with one another and appropriate actions can be triggered anytime; especially to avoid potential hardware crash and data loss when the server is not in a healthy state.

Continuous Data Protection feature provides the ability to take data backup continuously and recover when needed. IT administrators can take advantage of various automation options in Intel® SCS, and need not physically inspect the server every time to identify a problem.

### 1.1.1 Intel® SCS Modules

Intel® SCS provides three modules to ensure business continuity:

- Hardware Management
- Storage (RAID) Management
- Continuous Data Protection

### 1.1.2 Hardware Management

The Hardware Management module provides complete control over a supported Intel® server hardware from baseboard management to alerting and reporting.

Hardware Management module allows you to view:

- Information about health of various hardware components such as processors, memory, power supply, and system fans
- Information about health of logical drives
- Events and actions related to hardware components
- Sensor information related to temperature, fan speed, voltage, and current

The Hardware Management module displays a graphical representation of server components in three different views:

- Internal—processors and DIMMs/RAMs on the server board
- Rear—system fans and power supplies
- Front—slots in which hard disk drives are installed

Each view displays the health and technical specifications of components managed and monitored.

### 1.1.3 Storage Management

The Storage Management module provides features with the capability to manage storage dynamically at runtime, using RAID technology. Intel® SCS extends support for all RAID levels by including additional RAID Web Console tool.

The Storage Management module displays a graphical representation of the following components along with their health and specifications:

- Physical disks
- RAID controllers
- RAID arrays

Storage Management allows you to:

- View specifications and health of storage components
- View events and actions related to storage
- Create virtual disks in RAID arrays using RAID controllers
- Perform consistency check on RAID arrays

- Run patrol read using RAID controllers
- Add, locate, initialize, or delete virtual disks in RAID arrays

### 1.1.4 Data Protection

The Data Protection module helps backup data continuously, to increase data security and to enable you to retrieve data with the click of a few buttons, thereby ensuring business continuity. You can create a repository to which you can back up data on the server hard disk drive. Depending on the license, you can also create consistency points to which you can roll back. If the hard disk drive in the server fails and you lose the data stored on the disk, you can roll back to the most recent consistency point and recover data stored in the back up repository at the time the consistency point was created.

The Data Protection module allows you to:

- Create a repository for data backup and consistency points
- View the protection status of storage volumes
- Set up and modify protection plan
- Start or pause protection or unprotect storage volumes
- View events and actions related to continuous data protection
- Manage data backup using recovery point objectives (RPO)

The Continuous Data Protection module displays the health and status of data backup of each volume and the repository.

## 1.2 Intel® SCS Features

Each module provides IT administrators a suite of comprehensive features to provision, control, automate, and monitor servers from a single web console.

### 1.2.1 Reporting

Intel® SCS logs any changes in the server performance and the console as events. The events are obtained from event sensors, physical security management system, power unit, system event log, and hardware sensors.

Events are classified as critical ( ), warning ( ), and informational ( ), along with a description. Administrators can configure Intel® SCS to send event notifications so that the administrator can take necessary actions based on the event.

### 1.2.2 Alerting and Rules

The Alerting and Rules features provide options for sending email based on the modules and events. Alerting feature provides options to send periodic alerts for System Summary, Sensors, and Events. Rules feature provides options to set rules for Hardware, Storage, Data Protection, and Console.

### 1.2.3 Accelerated Protection Mode

When the server is at risk or in an unhealthy state, the system enters Accelerated Protection Mode. When the system is in Accelerated Protection Mode, actions are automatically triggered to protect the system. In this release of Intel® SCS, the time between the creation of Application Consistent Restore Points (ACRP) or consistency points is reduced when the system health status is warning or critical. The automatic reduction in time between ARCPs increases the number of ARCPs from the time the system enters unhealthy state until it is returned to healthy state. This increase in ARCPs provides increased data protection for all protected volumes. In future releases of Intel® SCS, additional protection actions may be added.

## 1.3 Server Management

Intel® SCS provides the following features to monitor the server from a console:

- Dashboard—displays an overview of the system events, system actions, power usage, and system resource usage.
- System Uptime—displays the number of days and hours for which the server has been operational after the last boot.
- License Information—displays the validity of license for hardware management, and data protection.
- User Management—provides tools to add users to access Intel® SCS console and manage users based on roles.
- System Configuration—displays the following details about the server:
  - Server Name
  - BMC Version
  - SDR Version
  - BIOS Version
  - Memory

- Drives
- Processors

If you log in as an administrator, the console also provides features to shut down, restart, and identify the server.

## 1.4 License Information

Intel® Server Continuity Suite (Intel® SCS) is installed with a 60 days trial license. Intel® SCS provides the capability to monitor the hardware and manage the storage of your server. Availability of the other features depends on the license.

The following are the license options for Intel® SCS.

| License Type | Data Backup Period | Data Recovery Window | Accelerated Protection Mode | Benefits |
|---|---|---|---|---|
| Intel® SCS System Manager | Not available | Not available | Not available | 1. Monitor your server health and manage storage.<br>2. Receive updates and fixes free of cost for one year*.<br>* Purchase Intel® SCS Software Maintenance license to receive updates and fixes for the second year and third year. |
| Intel® SCS Data Protection Manager | 30 days | Eight hours | Not available | 1. Monitor your server health and manage storage.<br>2. Backup data and preserve it for up to 30 days.<br>3. Roll back to data created before 8 hours or later. |
| Intel® SCS | 90 days | 1. Two hours if | Available | 1. Monitor your |

| License Type | Data Backup Period | Data Recovery Window | Accelerated Protection Mode | Benefits |
|---|---|---|---|---|
| Advanced Data Protection Manager | | the server health is healthy<br>2. 30 minutes if the server health is warning<br>3. 15 minutes if the server health is critical | | server health and manage storage.<br>2. Backup data and preserve it for up to 90 days.<br>3. Roll back to data created before 15 minutes or later. |
| Intel® SCS Software Maintenance | Not applicable | Not applicable | Not applicable | Receive updates and fixes for the second year and third year. |

# 2 Getting Started

## 2.1 Supported Server Boards

Intel® Server Continuity Suite (Intel® SCS) is supported only on servers built using Intel® server boards. The following table provides information about the Intel® server boards supported by Intel® SCS.

| Intel® Server Board | Key Hardware Components |
|---|---|
| Intel® Server Board S5520HC  | • Up to two Intel® Xeon® Processor 5600 series<br>• DDR3 memory (12 or 9 DIMMs)<br>• Up to six expansion slots, including four PCI Express* 2.0 x8 slots<br>• Integrated six SATA ports plus optional four ports SAS and SAS RAID Intel® I/O Expansion Modules |
| Intel® Server Board S5500BC  | • Up to two Intel® Xeon® processor 5600 series1<br>• DDR3 memory (eight DIMMs)<br>• High-speed PCI Express* 2.0 I/O (up to five slots) |
| Intel® Server Board S1200BTL*  | • Intel® Xeon® processor E3 1200 product family (including lower power processors)<br>• DDR3 memory (up to four DIMMs)<br>• Up to five slots high-speed PCI Express* 2/0 I/O (optional I/O module for six total I/O slots) |

* Intel® Server Board S1200BTS does not support Intel® SCS.

### 2.1.1 Supported Server Systems

Intel® SCS supports the following Intel® server systems:

| Server Systems | Server Type | Server Board Model Number | Server Chassis Model Number |
|---|---|---|---|
| SC5650HCBRPR | Pedestal | S5520HCR | SC5650BRP |
| SC5650HCBRP | Pedestal | S5520HCR | SC5650 |
| SC5650BCDPR | Pedestal | S5500BCR | SC5650DP |
| SR1630BCR (1U Fixed) | Rack | S5500BCR | SR1630 |
| P4304BTLSHCN | Pedestal | 1200BTL | P4304 |
| P4304BTLSFCN | Pedestal | 1200BTL | P4304 |
| R1304BTLSHBN | Rack | 1200BTL | R1304 |
| R1304BTLSFAN | Rack | 1200BTL | R1304 |

Intel® SCS also supports Intel® server systems built on the following server boards:

- S5520HCT
- S5500HCV
- S5500HCVR

However, a generic image of the server built on these server boards is displayed in Front View and Rear View, and a picture of the closest chassis is displayed in the Internal View along with a message to indicate the same.

## 2.2 Supported Software

Intel® SCS works on the following operating systems:

- Microsoft Windows Server 2008* SP2
- Microsoft Windows Server 2008* R2 SP1

The following software is installed automatically when you install Intel® SCS:

- Oracle* Java* Runtime Engine, version 6.31
- Microsoft Visual C++ 2005 Redistributable*, version 8.0.59193
- JRuby for Windows*, version 1.6.5.1
- PostgreSQL*, version 9.1.3

## 2.3 Supported Browsers

Intel® SCS works on the following browsers:

- Mozilla Firefox* 4.0 or higher
- Microsoft Internet Explorer 8* and Microsoft Internet Explorer 9*
- Google Chrome* 15.0.874.106 m

We recommend that you set your screen resolution above 1024 x 768.

**Note**: The visual experience of Intel® SCS in Microsoft Internet Explorer 9* may be better than the visual experience of Intel® SCS in Microsoft Internet Explorer 8*.

**Note**: When starting Intel® SCS using a browser, if you get a message that there is a problem with the website's security certificate, click the appropriate button in the message to continue starting Intel® SCS using the browser.

**Note**: You must enable JavaScript* in your browser for all functionalities in Intel® SCS to work.

## 2.4 Supported RAID Controllers and Hard Disk Drives

You can find supported RAID adapters from the Server Configurator tool in http://support.intel.com/support/motherboards/server/scs/sb/CS-032978.htm.

Intel® SCS supports only Intel® RAID adapters and SATA/SAS/SSD drives mentioned in the Server Configurator tool.

## 2.5 Supported USB Drives

You can use USB drives for backing up the data using Intel® SCS. However, USB drives are not recommended for protecting critical data. The

USB drives that work for a period of two months with medium data change rate (less than 5 MB per hour) are listed in http://support.intel.com/support/motherboards/server/scs/sb/CS-032917.htm.

## 2.6 Installing Intel® Server Continuity Suite

You can install Intel® Server Continuity Suite (Intel® SCS) using the installation disk provided or by downloading the installation package from the Intel® download center.

## 2.7 Starting Intel® Server Continuity Suite

To start Intel® Server Continuity Suite:

1. Click Intel® SCS icon (labeled Intel® Server Continuity Suite) on the Desktop or type **https://localhost:7000/** in the address bar of your browser.

**Note**: When starting Intel® SCS using a browser, if you get a message that there is a problem with the website's security certificate, click the appropriate button in the message to continue starting Intel® SCS using the browser.

The login screen appears.

**Note**: You must enable JavaScript* in your browser for all functionalities in Intel® SCS to work.

2. Enter the user name and password.
3. Click **Sign In**.

The Dashboard appears.

**Note**: If you enter wrong user name or password three times consecutively, your access is temporarily disabled.

## 2.8 Upgrading the License

To upgrade your license:

1. Click **License Information** or **Setting** in the main menu.
2. If you clicked **Settings**, click **License** in the screen that appears.
3. Click **Get License Key** in the screen.

**Note:** You will be redirected to the Intel® website to obtain the license key and support key. Enter the product registration key and the server unique identification number.

The License Key and Maintenance Key are displayed on the screen.

4 Enter the license key in the **License Management** screen.

5 Click the **APPLY** button for the License Key.

The license is updated.

The License and Validity details are updated based on the license purchased.

6 Repeat these steps to obtain license for Data Protection and Maintenance.

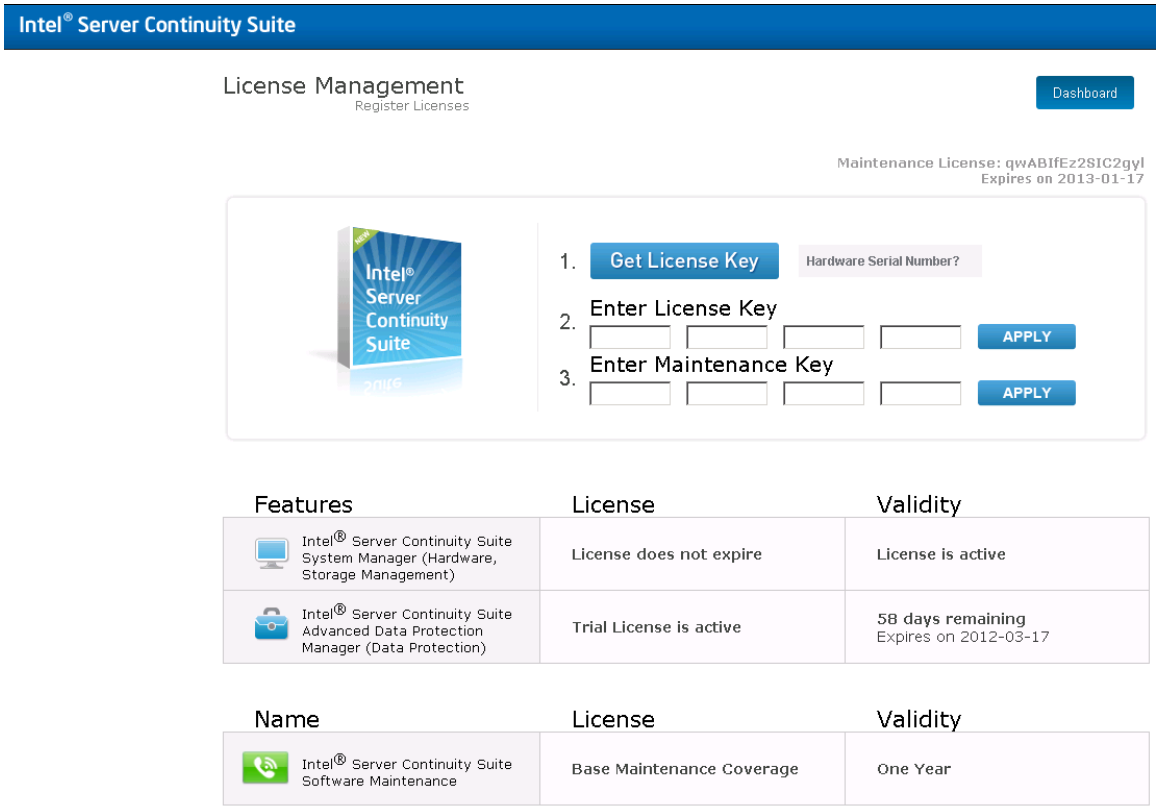


**Figure 2-1: License**

**Note:** If the license expires, an error message is displayed on the screen. The License and Validity details are updated based on the license expiry.

## 2.9 Navigating the User Interface

Intel® SCS is a user friendly business continuity suite, with minimal clicks required to access the main modules and features. The main menu, on the left hand side, provides access to the main modules and features including:

- Dashboard
- Hardware
- Storage
- Data Protection
- Activity
- Settings

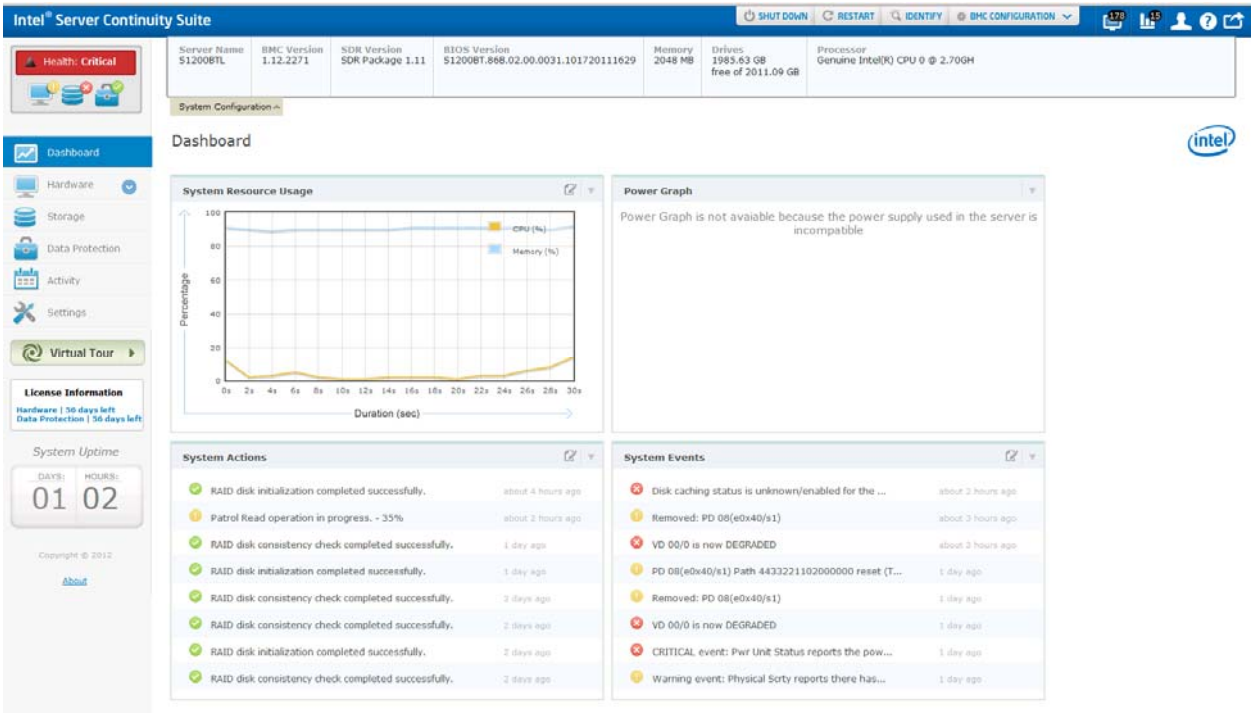


**Figure 2-2: Intel® SCS User Interface**

Information about managing the server using each module is provided in the following chapters.

The health of the server and the health of the hardware, storage, and data protection modules are displayed in the main menu.


The health is indicated using colors. Point the mouse to the icon for a module to know its health.

### 2.9.1 Virtual Tour

You can view a virtual tour of the components and features by clicking the virtual tour button in the main menu.

### 2.9.2 License Information

The validity of the Hardware and Data Protection modules is provided in the license expiry info palette in the main menu.

### 2.9.3 System Uptime

The number of days and hours for which the server has been operational after the last boot is displayed in the system uptime palette in the main menu.

# 3 Dashboard

This section provides information on Dashboard features and functionality.

After you login to Intel® Server Continuity Suite (Intel® SCS), the Dashboard is displayed by default. You can access the Dashboard by clicking Dashboard in the main menu on the left.

In the Dashboard, you can view the following:

- System Events
- System Actions
- System Resource Usage
- Power Graph

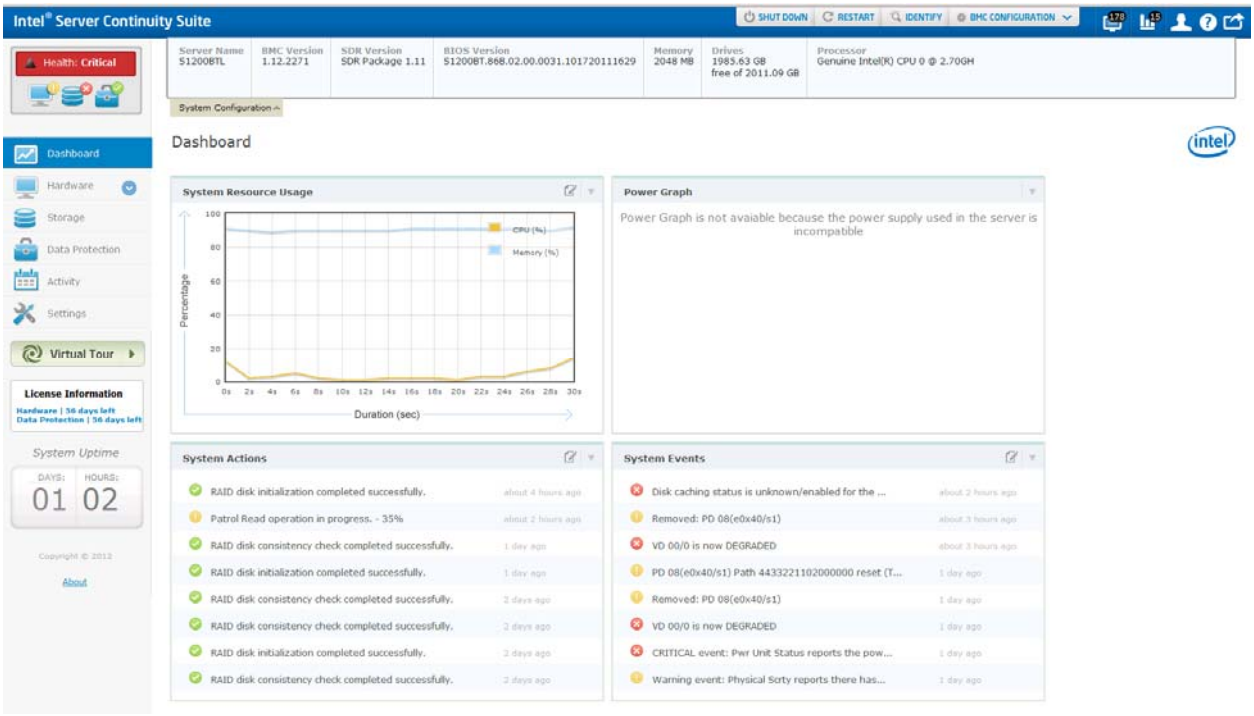


**Figure 3-1: Dashboard**

The details are displayed in separate panels. You can move and arrange the panels in any sequence of your choice.

To change the position of the panels:

1 Place the cursor on a panel's title bar.

A cross arrow appears.

2 Drag the panel to change the position.

**Note:** Click the cross arrow to collapse and expand the panel.

In addition, Dashboard displays the system configuration. The System Configuration palette displays the following details about the server:

- Server Name
- BMC Version
- SDR Version
- BIOS Version
- Memory
- Drives
- Processors

Click **System Configuration** to hide the system configuration palette.

## 3.1 System Events

The Dashboard lists events under System Events, along with the event type, description, and age. System Events displays events generated from the current date up to a month.


**Figure 3-2: System Events**

System Events display events based on the options selected. You can filter events using these options.

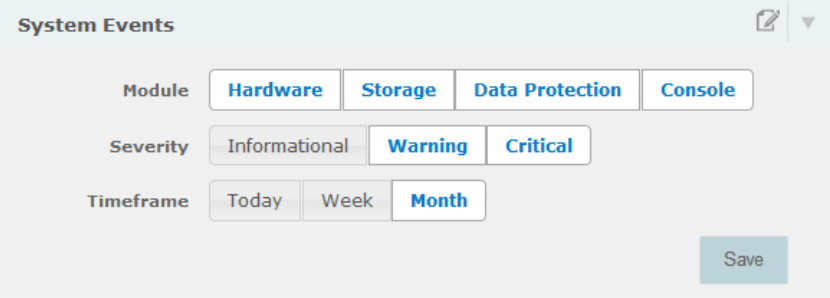


**Figure 3-3: System Events Options**

To configure these options:

1 Click the edit button ( ).

The options appear.

2 Select the Module, Severity, and Timeframe.

**Note:** You can select one or multiple modules and severity.

3 Click **Save**.

Events appear in the list based on the selected options.

## 3.2 System Actions

The Dashboard lists actions under System Actions, along with the action description, age, and status. System Actions menu displays a maximum of eight actions performed from the current date up to a month.

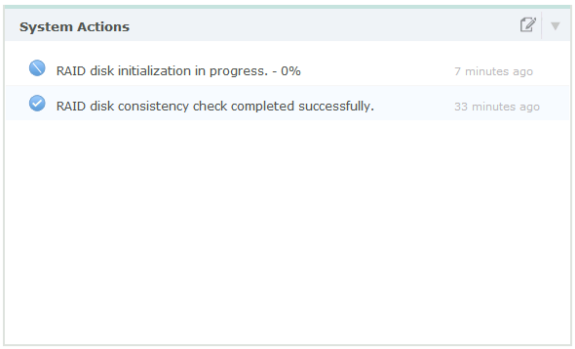


**Figure 3-4: System Actions**

System Actions display actions based on the options selected. You can filter actions using these options.

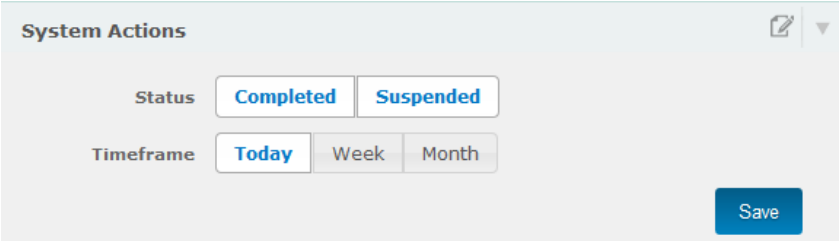


**Figure 3-5: System Actions Options**

To configure these options:

1 Click the edit button ( ).

The options appear.

2 Select the **Status** and **Timeframe**.

**Note:** You can select one or multiple status.

3 Click **Save**.

Actions appear in the list based on the selected options.

## 3.3 System Resource Usage

The Dashboard displays the System Resource Usage, including CPU and Memory usage, in a graph.

In the System Resource Usage Graph, the X axis denotes time in seconds. The time interval between the points on X axis is two seconds. The Y axis denotes resource usage in percentage.

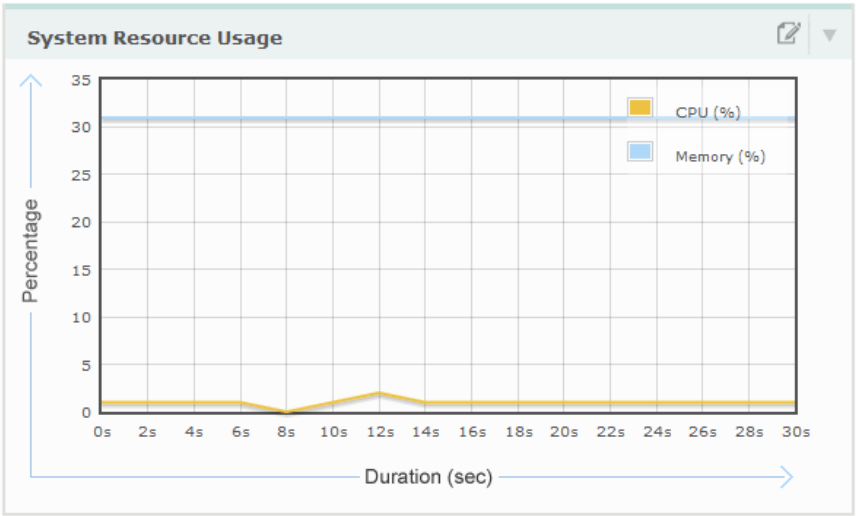


**Figure 3-6: System Resource Usage Graph**

You can display the CPU, Memory, or both in the graph. You can filter the view using the options.

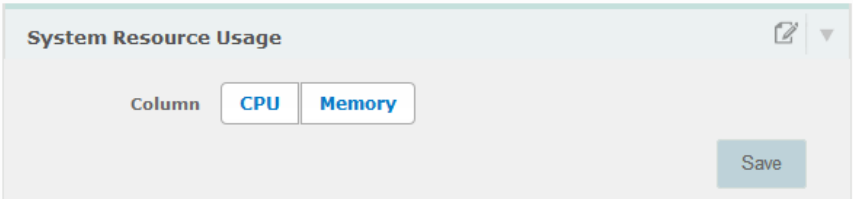


**Figure 3-7: System Resource Usage Options**

To configure these options:

1 Click the edit button ( ).

The options appear.

2 Select **CPU**, **Memory**, or both.

3 Click **Save**.

The graph appears based on the selected options.

## 3.4 Power Graph

The Power Graph displays the current and average reading using the values obtained from the sensors.

In the Power Graph, the X axis denotes time in seconds. The time interval between the points on X axis is ten seconds. The Y axis denotes power in watts.

The power graph is available only if a PMBUS power supply is used.

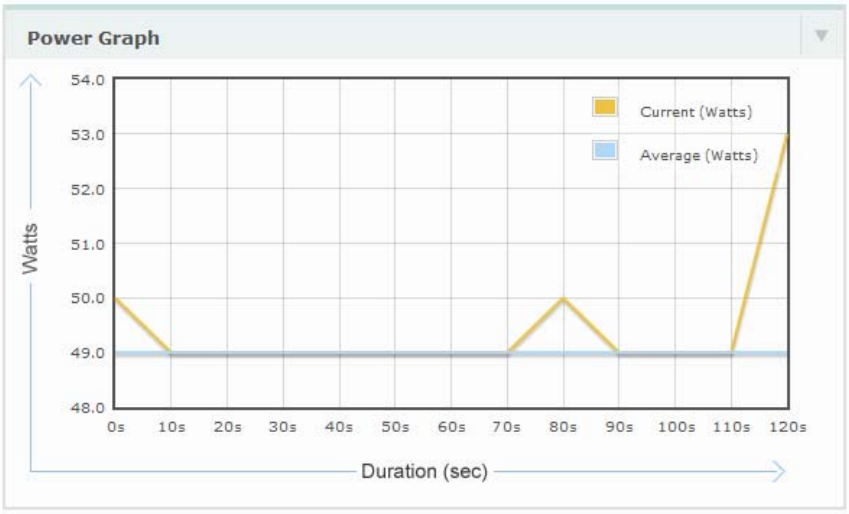


**Figure 3-8: Power Graph**

# 4 Hardware Management

## 4.1 Overview

The Hardware Management module in Intel® Server Continuity Suite (Intel® SCS) provides a real time view of the hardware components in the server and enables you to monitor and manage the hardware components and their health using a dynamic and interactive interface.

The Hardware Management module provides a set of tools designed for:

- Timely identification of faulty or degrading hardware components, which could possibly interrupt business continuity
- Notifying users of system events and actions performed on the server or its components
- Displaying parameter readings such as temperature, fan speeds, voltage, and current

You can access the Hardware Management module by clicking Hardware in the main menu on the left. When you start the module, Intel® SCS automatically detects the server board, the hardware components used, and the type of chassis and displays images of the server and real time information about its components.

Once the chassis and server board are detected, images resembling the server are displayed in three different views.

**Note:** If the server contains a supported Intel® server board, Intel® SCS picks up the relevant server board and chassis pictures from the image bank, installed as part of initial installation. If Intel® SCS is unable to find the relevant picture for the server board and the chassis, an illustrative view (a generic image) of the server is displayed in Front View and Rear Views, whereas an actual picture of the closest chassis is displayed for the Internal View along with a message to indicate the same.

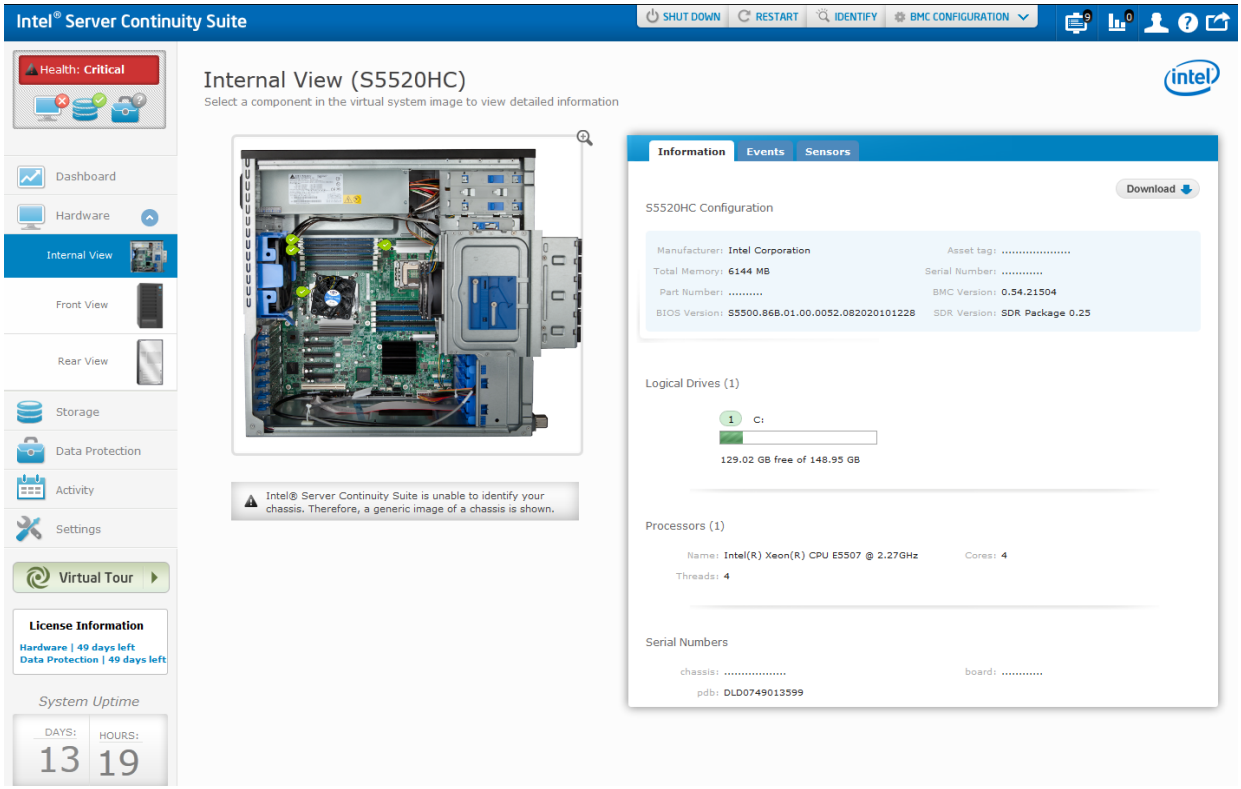


**Figure 4-1: Hardware Management Module**

All information about the hardware components, including the health and sensor readings, is obtained from the BMC. Data collected from sensors are displayed in a separate tab. For more information on sensors, see Sensors.

## 4.2 Intelligent Platform Management Interface

Intel® SCS is implemented based on Intelligent Platform Management Interface (IPMI) specifications. IPMI defines a standardized, abstracted, message-based interface to intelligent platform management hardware. IPMI also defines standardized records for describing platform management devices and their characteristics. Additional information regarding IPMI can be found in the link http://www.intel.com/design/servers/ipmi/ipmi.htm.

## 4.3 Supported Server Boards

Intel® SCS supports only Intel® server boards. This version supports the following Intel® server boards:

- Intel® Server Board S5520HC
- Intel® Server Board S5500BC
- Intel® Server Board S1200BTL*

* Intel® Server Board S1200BTS does not support Intel® SCS.

For more information on these server boards, see http://www.intel.com/support/.

### 4.3.1 Supported Server Systems

Intel® SCS supports the following Intel® server systems:

| Server Systems | Server Type | Server Board Model Number | Server Chassis Model Number |
|---|---|---|---|
| SC5650HCBRPR | Pedestal | S5520HCR | SC5650BRP |
| SC5650HCBRP | Pedestal | S5520HCR | SC5650 |
| SC5650BCDPR | Pedestal | S5500BCR | SC5650DP |
| SR1630BCR (1U Fixed) | Rack | S5500BCR | SR1630 |
| P4304BTLSHCN | Pedestal | 1200BTL | P4304 |
| P4304BTLSFCN | Pedestal | 1200BTL | P4304 |
| R1304BTLSHBN | Rack | 1200BTL | R1304 |
| R1304BTSSFAN | Rack | 1200BTL | R1304 |

Intel® SCS also supports Intel® server systems built on the following server boards:

- S5520HCT
- S5500HCV
- S5500HCVR

However, a generic image of the server built on these server boards is displayed in Front View and Rear View, and a picture of the closest chassis is displayed in the Internal View along with a message to indicate the same

## 4.4 Hardware Components and Views

The module displays three different views along with information about the server, classified under three tabs.

The three views are:

- Internal View—provides a real-time internal view of the server and displays the health of the processors and memory used. If you move the mouse over the components, the module displays their information.
- Rear View—displays an image of the rear panel of the chassis and the health of the system fan and power supply. If you move the mouse over the components, the module displays their information.
- Front View—displays an image of the front panel of the chassis and shows the slots in which hard disk drives are installed. If you move the mouse over the components, the module displays their information.

**Note**: If the server contains a supported Intel® server board, Intel® SCS picks up the relevant server board and chassis pictures from the image bank, installed as part of initial installation. If Intel® SCS is unable to find the relevant picture for the server board and the chassis, a generic image of the server is displayed in Front and Rear views, and a picture of the closest chassis is displayed in the Internal view along with a message to indicate the same. In each view, information about the server is provided under the following three tabs:

  - Information—provides information about the server. Click a component to view information specific to it.
  - Events—provides a list of events generated. Click a component to view events specific to it.
  - Sensors—provides information generated by sensors. Click a component to view sensor information specific to it.

When you click on the icon for one of the three views or when you click on a component in a view, the Information tab for that view or component is displayed. Click the Events or Sensors tab to view events or sensors details for that view or component.

The following image shows the initial screen displaying information of all the components.

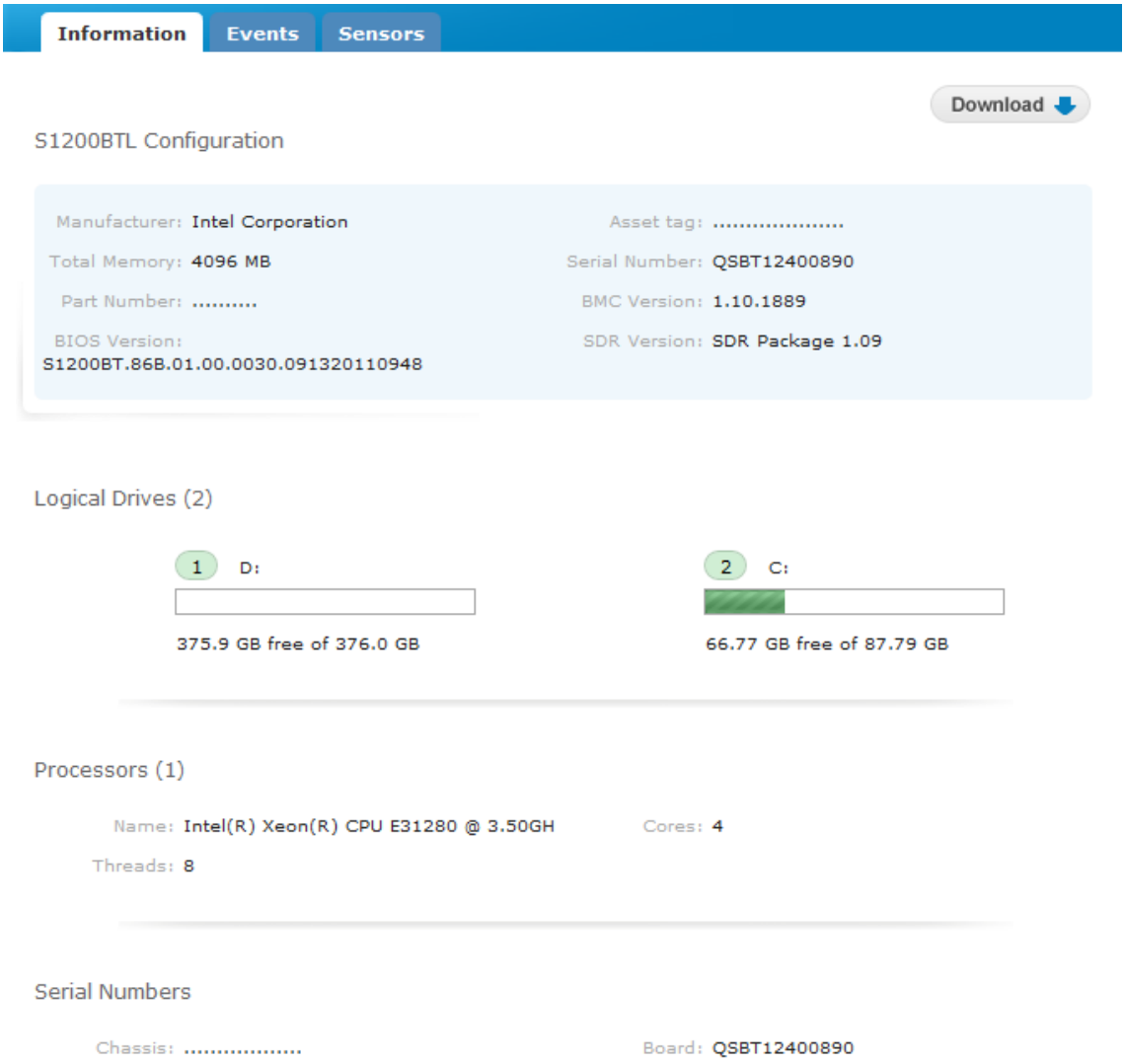


**Figure 4-2: Information Tab**

When you start the Hardware Management module, the internal view is displayed by default. Click the navigation icons representing the different views on the menu in the left hand side to switch between the views. The initial screen in each view displays information of all components in the Information tab.

You can generate a report of the information displayed for all or individual components. The report can be sent as an email or saved as a PDF file. For more information on reporting, see Reporting Events.

You can view the server images in an enlarged view:

- Click the zoom in icon ( ) to enlarge the view
- Click Info/Events to return to the normal view

### 4.4.1 Internal View

The Internal View displays the processors and memory and their health status.

**Figure 4-3: Internal View**

When you click on processors in the Internal View, the Information tab on the right displays the server board and processor details. The details displayed include the processor name and speed.

When you click the DIMMs, the Information tab on the right displays details, including memory type and size.

### 4.4.2 Front View

The Front View displays hard disk drives.

**Figure 4-4: Front View**

When you point to the HDD, a tooltip displays the health. As you click a hard disk, the Information tab displays:

- The slot number
- The status of the slot, whether the physical disk is present or not.

### 4.4.3 Rear View

The Rear View displays the system fan and power supply with health status.

**Figure 4-5: Rear View**

When you click the system fan, the Information tab displays the RPM of the fans. Click the power supply to view its details.

## 4.5 BMC Configuration

Baseboard Management Controller (BMC) provides information about the hardware components displayed in the Hardware Management module.

BMC provides the capability to manage the server remotely, and obtain data of internal variables such as temperature, power supply, voltage, and fan speed from system sensors. BMC monitors the sensors and sends alerts if the variables are not within preset limits. The sensor information is used to calculate the hardware component and server heath. In addition, BMC also enables Simple Network Management Protocol (SNMP) reporting to send alerts to a designated administrator system.

Intel® SCS provides features to configure BMC to connect and send SNMP alerts.

The features include configuration of:

- LAN
- SNMP
- User
- Serial Over LAN
- Node Manager

You can access these features and configure them from the BMC Configuration drop-down menu.

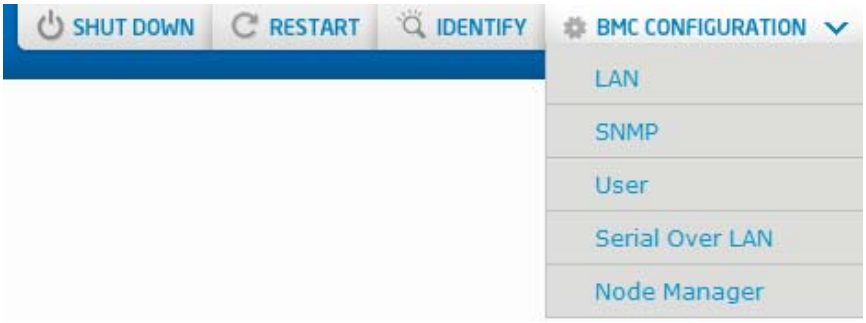


**Figure 4-6: BMC Configuration**

### 4.5.1 Configuring LAN

The settings for LAN in BMC Configuration allow you to configure the IP type, IP address, and gateway IP to establish a LAN connection to BMC.

To configure LAN:

1 Select **LAN** from **BMC Configuration** drop-down menu.

The LAN Configuration | BMC Configuration screen appears.

2 Select the **IP Type**.

**Note:** DHCP option appears by default for IP type. You must choose STATIC in the drop-down menu to enter static IP details.

3 Enter the IP, Subnet Mask, Default Gateway IP, and Backup Gateway IP.

4 Click **Save**.

The settings are saved to connect to the BMC using the LAN connection.

**Note:** Click **Cancel** to exit without saving the settings.

### 4.5.2 Configuring SNMP

The Simple Network Management Protocol (SNMP) settings in BMC Configuration allow you to configure SNMP, to enable the alerting mechanism to send alerts. The administrator can view alerts stored on the configured system.

To configure SNMP:

1 Select SNMP from BMC Configuration.

The SNMP Configuration | BMC Configuration screen appears.

2 Enter the **IP** and **MAC**.

3 Select **Enable** in the **Acknowledge** drop-down list.

**Note:** Enabling acknowledgement helps the system to get response for the SNMP requests.

4 Enter the **Ack Timeout**.

5 Select the **Retry Count**.

6 Click **Save**.

The SNMP settings are saved.

**Note:** Click **Cancel** to exit without saving the settings.

### 4.5.3 Configuring User

The settings for users in BMC Configuration allow you to configure up to five users to connect to the BMC.

To configure BMC user:

1 Select USER from BMC Configuration.

The User Configuration | BMC Configuration screen appears.

2 Enter the **Name**.

3 Select the **Status** and **Privilege**.

4 Enter the **Password**.

5 Select the Authentication.

6 Click **Save**.

The user settings are saved and can be used to connect to the BMC.

**Note:** Click **Cancel** to exit without saving the settings.

### 4.5.4 Configuring Serial Over LAN

The settings for Serial Over LAN (SOL) in BMC Configuration allow you to configure the channel privilege, baud rate, payload authentication and encryption for serial over LAN. You must configure these settings to enable the serial controller interface. The serial controller interface enables the server to communicate through the local serial controller over a LAN connection to transmit serial data.

To configure SOL:

1 Select SOL from BMC Configuration.

The SOL Configuration | BMC Configuration screen appears.

2 Select **Enable** in the **Enable User** drop-down menu.

3 Select the Privilege, Baud Rate, Payload Authentication, and Payload Encryption.

4 Click **Save**.

The settings are saved to connect through SOL using the LAN connection.

**Note:** Click **Cancel** to exit without saving the settings.

### 4.5.5 Configuring Node Manager

The NM (Node Management) settings in BMC Configuration allow you to configure and manage power supply to the server.

**Note**: Power supply should support NM feature to configure NM.

To configure NM:

1 Select NM from BMC Configuration.

The Node Manager | BMC Configuration screen appears.

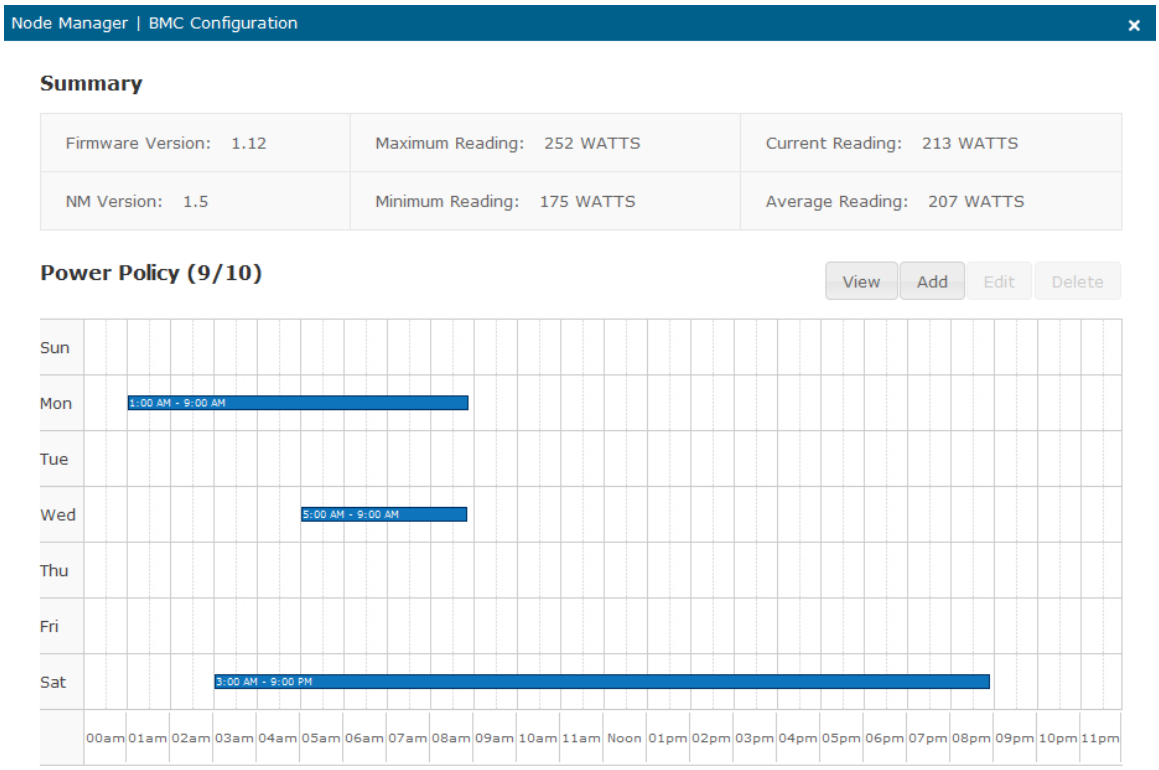


**Figure 4-7: Node Manager**

The Node Manager screen displays the Node Manager Summary and Power Policies. Node Manager Summary provides information about the node manager firmware used and power readings such as:

- Current reading
- Average reading
- Minimum reading
- Maximum reading

The power policies contain information about how much power must be used in a specific duration. The node manager allows you to view, add, edit, and delete power policies.

### 4.5.5.1 Viewing Power Policy

You can view the power policies added in the node manager.

To a view power policy:

1 Click **View** in the Node Manager.

The Node Manager displays the power policy details.

#### 4.5.5.2 Adding a Power Policy

The Node Manager allows you to add up to 10 power policies for different durations in a week.

To add a power policy:

1 Click **Add** in the **Node Manager**.

The Create new policy window appears.

2 Select the day.

3 Enter the **Power Limit**.

4 Select the duration from the **Between** drop-down lists.

5 Click **Create**.

**Note**:

- **Status** shows whether the policy creation was successful or failed.
- Click **Cancel** to exit without saving the settings.

The Node Manager displays the newly added power policy.

#### 4.5.5.3 Editing Power Policy

The Node Manager allows you to edit the existing power policies. The Edit button is enabled after a power policy is selected.

To edit a power policy:

1 Select the power policy in the Node Manager screen.

2 Click Edit in the Node Manager.

The Edit new policy window appears.

3 Select the day.

4 Enter the **Power Limit**.

5 Select the duration from the **Between** drop-down lists.

6 Click **Save**.

**Note**:

- **Status** shows whether the policy creation was successful or failed.
- Click **Cancel** to exit without saving the settings.

The Node Manager displays the changes made to the power policy.

#### 4.5.5.4 Deleting Power Policy

The Node Manager allows you to delete the existing power policies. The Delete button is enabled after a power policy is selected.

To delete a power policy:

1 Select the power policy in the **Node Manager** screen.

2 Click Delete in the Node Manager.

The Delete new policy window appears.

3 Click **Delete**.

**Note:** Click **Cancel** to exit without saving the settings.

The Node Manager displays the changes made to the power policy.

## 4.6 Performing System Actions

If you log in as an administrator, Intel® SCS allows you to shut down, restart, or identify the server.

### 4.6.1 Shut Down

You can shut down the system remotely using Intel® SCS.

To shut down the server:

1 Click **Shut Down** in the top menu.

The Shut Down | System Action window appears.

2 Enter the string displayed in the screen in the box provided.

3 Click **Confirm**.

The server shuts down.

### 4.6.2 Restart

You can restart the server remotely using Intel® SCS.

To restart the server:

1 Click **Restart** in the top menu.

The Restart | System Action window appears.

2 Enter the string displayed in the screen in the box provided.

3 Click **Confirm**.

The server restarts.

### 4.6.3 Identify

In a server setup with multiple server machines, you can identify the server to which Intel® SCS is connected.

To identify the server:

1 Click **Identify** in the top menu.

A message appears and an indicator glows on the server.

2 Click the close button in the message to close the message.

**Note:** If you do not click the close button, the message disappears after a few seconds.

## 4.7 Hardware Management Events

Intel® SCS logs hardware related events and alerts, which can be seen by clicking the Event tab in the Hardware Management module. Events are logged by time and source of generation and marked critical (), warning (), and informational (). Administrators can take actions based on the event's description. Administrators have the option to close an event or delete it from the events list.

The events displayed in Hardware Management module are generated from BMC and Intel® SCS. The events from BMC are obtained from event sensors, physical security management system, power unit, system event log, and hardware sensors. These events are generated when an action is performed on the server. For example, if you open the server chassis, the physical security management system reports a chassis intrusion event, which is logged and displayed in the events list.

Click the Events tab to view all events. The events are displayed based on criticality. For more information on managing events, see Events and Actions.

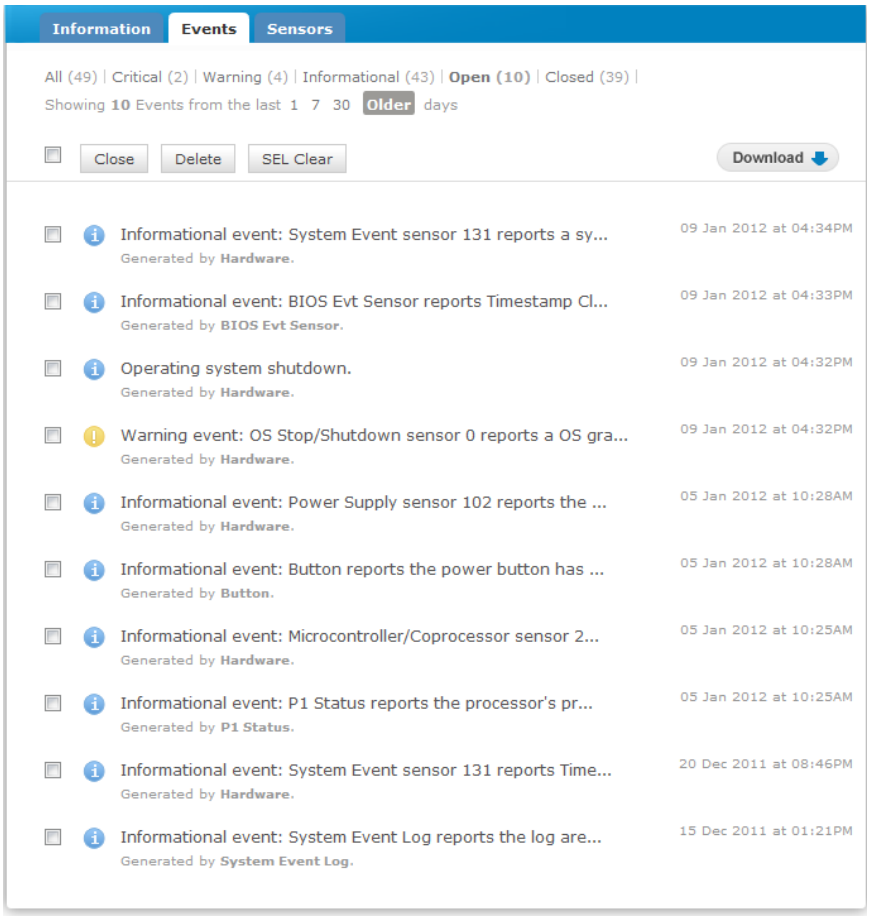


**Figure 4-8: Events tab**

A few examples of hardware events logged are given in the following table.

| Event | Description | Event Severity | Source of Event |
|---|---|---|---|
| Physical Scrty reports there has been a chassis intrusion | The server's chassis was opened | | Physical Security Management |
| Physical Scrty reports the chassis is now closed | The server's chassis was closed | | Physical Security Management |
| Pwr Unit Status reports the power unit is powered off or being powered down | Power supply to the power unit is cut off or the server is shut down | | Power Unit |

| Event | Description | Event Severity | Source of Event |
|---|---|---|---|
| BIOS Evt Sensor reports a system boot event has occurred | The server was restarted or boot sequence in the server was started | | BIOS Event Sensor |
| Operating system bootup | The server was restarted or boot sequence in the server was started | | Hardware |
| OS Boot sensor 0 reports the boot from drive C has been complete | The boot sequence on the boot sectors was complete | | Hardware |
| Pwr Unit Status reports the power unit's AC is lost | The power unit is shutdown | | Power Unit |
| Pwr Unit Status reports the power unit has suffered a failure | The power unit has failed | | Hardware |
| Memory sensor 2 reports uncorrectable error | The memory scrub failed for the memory module | | Hardware |

Intel® SCS provides settings to automatically notify events to the administrator. For more information on event notification settings, see Settings.

## 4.8 Monitoring Hardware Health

Hardware Management module in Intel® SCS provides the capability to monitor server health using sensors and health indicators. This module is included in all types of licenses of the product and is installed by default when you install Intel® SCS.

### 4.8.1 Sensors

Sensors provide information about the temperature, fan speed, voltage, and current of the hardware components. Click the Sensors tab to view information generated by sensors.

Sensor details can be viewed by selecting:

- All
- Critical
- Warning

The sensors display the status information as lower, warning, normal, and higher based on the defined parameter limits. Each state has a lower to higher value, and the dot indicates the actual sensor reading. For example, the temperature sensors for hard disk drives display values ranging from lower, warning, and normal, to higher.

A Green dot indicates normal readings. Critical sensors appear with a red exclamation, and a red dot indicates the actual reading. A yellow dot indicates the reading for warning.

The temperature sensors display the temperature of the processors, hard disk drives, and baseboard.

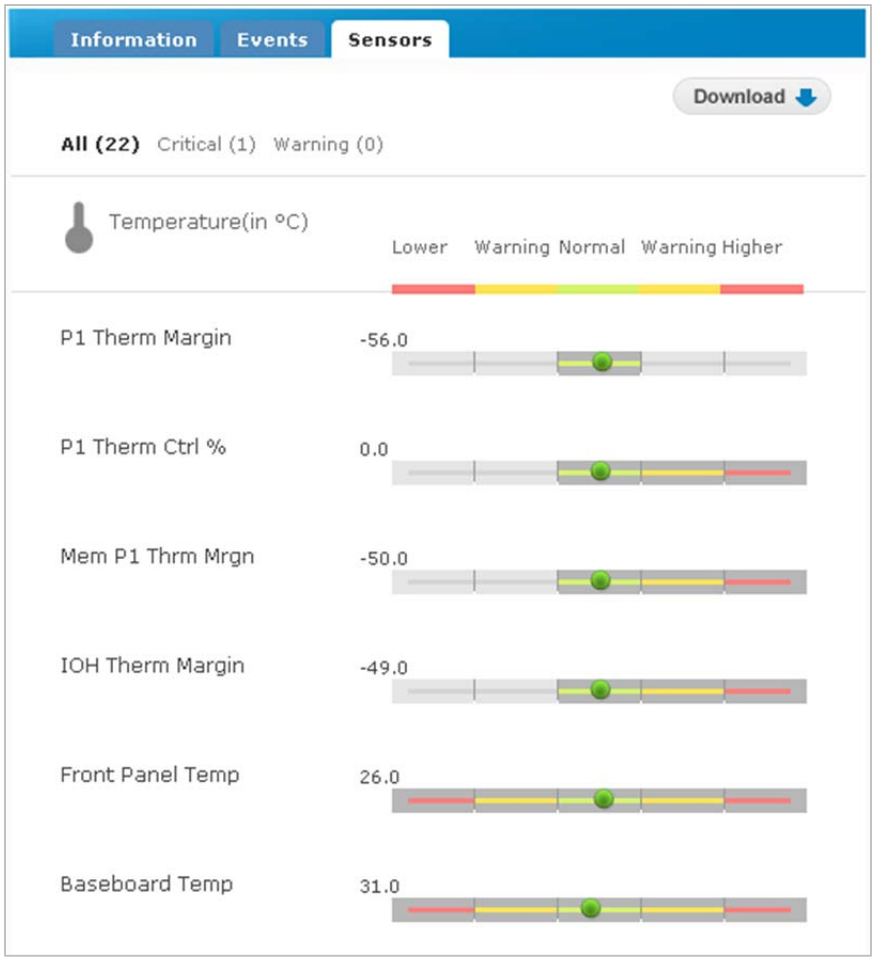


**Figure 4-9: Temperature Sensor Information**

The fan speed sensors display the system and processor fan speeds in RPM with values ranging from lower to normal.


**Figure 4-10: Fan Speed Sensor Information**

The voltage sensors display the voltage supplied to different components.

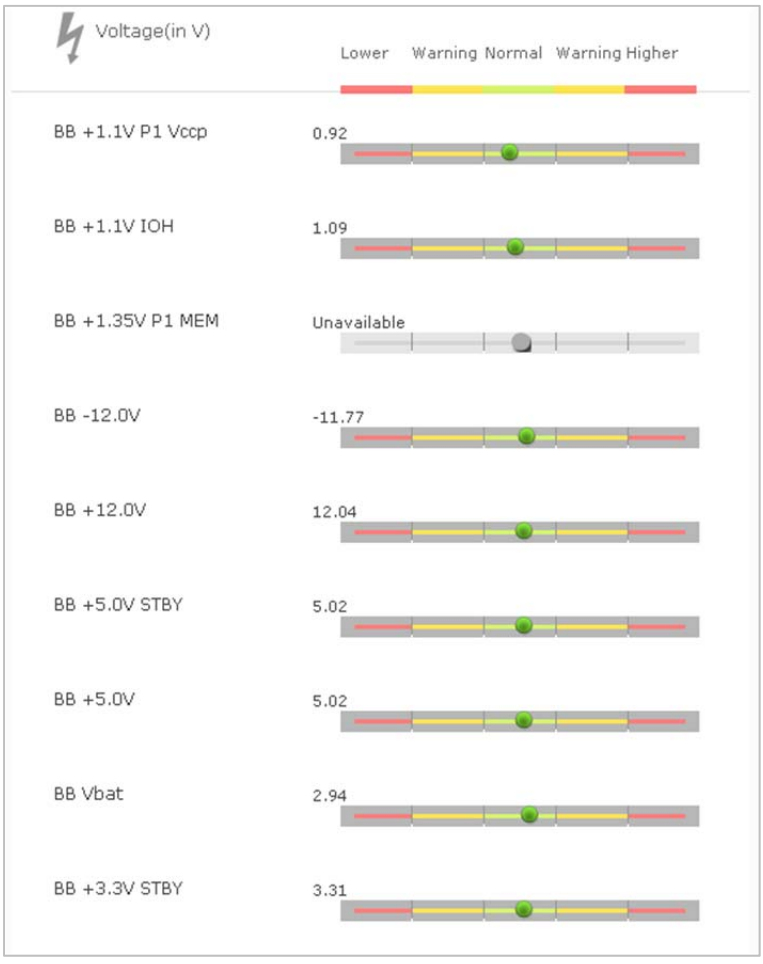


**Figure 4-11: Voltage Sensor Information**

The current sensor displays the PS2 current out percentage in Amps.

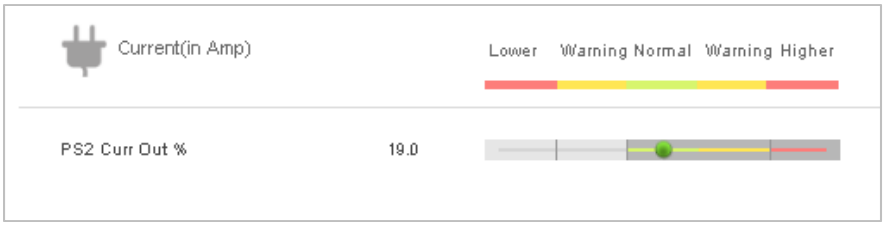


**Figure 4-12: Current Sensor Information**

### 4.8.2 Health Indicators

The Hardware Management module displays the health indicators for the processors, memory, and system fans based on the state of the component. The health indicator displays the health as normal, warning, and critical using icons.

The interface displays the health using one of the following icons:

—Healthy

—Warning

—Critical

Health indicators are displayed for components in the Rear View and Internal View. In the Rear View, the health of the system fan and power supplies is indicated. In the Internal View, the health of the processors and memory is indicated. Information about the health is based on the readings obtained from the sensors.

## 4.9 Monitoring and Reporting

You can monitor the health of hardware components using health indicators, events, and sensors. You can configure Intel® SCS to send emails with details of the events generated using the Email Configuration settings. You can also report events by generating a PDF of the report and sending that to administrators.

For more information on events, see Events and Actions.

The reports sent as an email or generated as PDF contain details displayed on the screen at the time the report was generated. Intel® SCS allows you to create the email and PDF files in a predefined format.

For more information on sending email and generating PDF, see Reporting Events.

## 4.10 Integrating with Storage Management and Continuous Data Protection

When all hardware components function normally, the server health is normal, and all activities run as scheduled. Any sudden or unforeseen changes in hardware components affect the server health. This affects Storage Management and Continuous Data Protection modules.

### 4.10.1 Changes in Physical Disks

The physical disk information displayed in both Hardware Management and Storage Management are synchronized. Any change in the physical disks is displayed in both Hardware Management and Storage Management.

When a physical disk is removed or changed in the server, depending on the RAID type, the state of the physical disks and virtual disks change in Storage Management. The data backup activities in Continuous Data Protection also change.

For example, if a physical disk is removed from the server, the slot corresponding to the physical disk changes to Empty Slot. The change in slot information is seen in both Hardware Management and Storage Management modules.

If a physical disk fails, the health of virtual disks in Storage Management and volumes in Continuous Data Protection change to critical, changing the health status of the server to critical. Data backup is performed as scheduled in Continuous Data Protection and the status of virtual disks and volumes remain in critical state till the physical disk is replaced.

When a new physical disk is inserted or an existing physical disk is configured as hot spare, based on the RAID type, the RAID controller in Storage Management replaces the failed physical disk with hot spare, rebuilding the lost data. As the physical disk is rebuilt, the affected virtual disks and volumes change to normal state and the normal scheduled activities resume.

### 4.10.2 Changes to Other Hardware Components

If all hardware components function normally, all activities in Storage Management and Continuous Data Protection take place normally.

A change in parameters such as temperature or voltage—leading to abnormal functioning of the server—results in changes in all three modules. The sensors in Hardware Management display the information

obtained from BMC. Any abnormal changes in the parameters, changes the health of the affected component and the overall server.

# 5 Storage Management

Storage Management in Intel® Server Continuity Suite (Intel® SCS) refers to RAID configuration, management, and monitoring of data storage devices. This section provides information and step-by-step procedures to manage storage using RAID.

The Storage Management module in Intel® SCS provides the capability to configure RAID volumes in servers built using Intel® server boards, in a simple and easy manner. Using the user friendly interface of Intel® SCS, you can choose the controllers, hard disk drives, and other storage related devices installed on the servers. The interface shows the relations between configured volumes, associated RAID controllers, and hard disk drives.

The module enables you to monitor the health of storage components. It displays information on the status of virtual disks, physical disks, and controllers. System errors and events are also displayed on the screen. In case of failure of any of the storage related components, the administrator can easy identify the components and take necessary action.

The module also supports management functions such as volume initialization, patrol read, and consistency check.

### 5.1.1 RAID Basics

RAID is a technology that allows server users to achieve high levels of storage reliability using arrays that include redundancy for reliability. RAID functionality is implemented at hardware level in the RAID controller, which can be onboard in a server or connected externally. Some RAID configurations are explained below:

- **RAID 0**—this configuration uses disk striping to provide high data throughput, especially for large files in an environment that does not require fault tolerance. In Intel® IT/IR RAID, RAID 0 is also called Integrated Striping (IS) and it supports striped arrays with two to ten disks. If a drive in a RAID 0 array fails, the whole virtual disk (all physical drives associated with the virtual disk) fails.

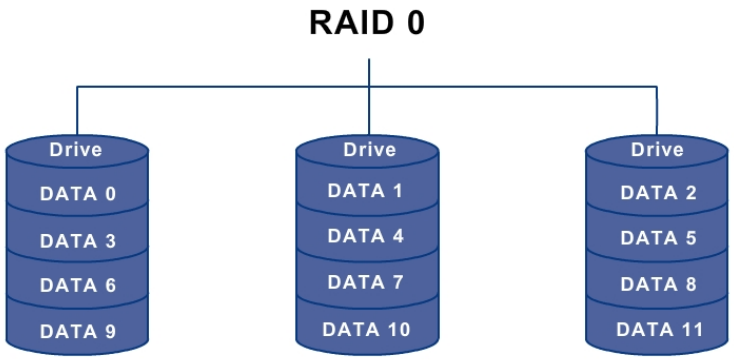


**Figure 5-1: RAID 0**

- **RAID 1**—this configuration uses disk mirroring so that data written on one disk drive is simultaneously written on another disk drive. This is good for small databases or other applications that require small capacity but need complete data redundancy. In Intel® IT/IR RAID, RAID 1 is also called Integrated Mirroring (IM) and it supports two-disk mirrored arrays and hot-spare disks. RAID 1 requires at least two hard disk drives.

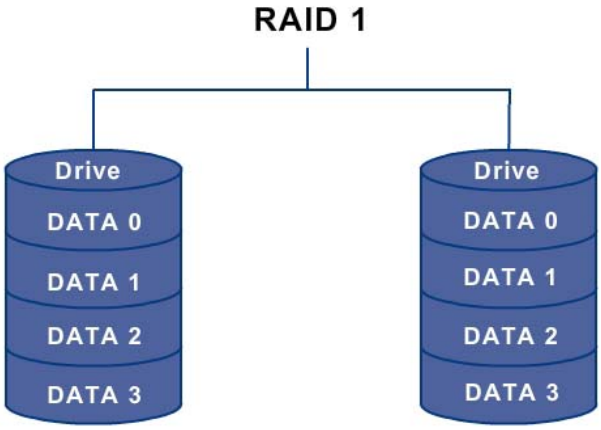


**Figure 5-2: RAID 1**

- **RAID 5**—this configuration uses disk striping with parity data across all drives (distributed parity) to provide high data throughput, especially for small random access. RAID 5 requires at least three hard disk drives. A RAID 5 virtual disk can survive the loss of one disk without losing data.

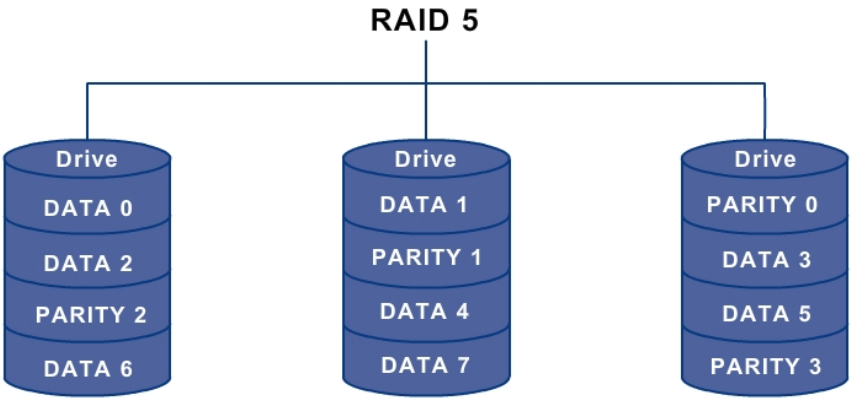


**Figure 5-3: RAID 5**

- **RAID 6**—this configuration uses distributed parity, with two independent parity blocks per stripe, and disk striping. RAID 6 requires at least three hard disk drives. A RAID 6 virtual disk can survive the loss of two disks without losing data.

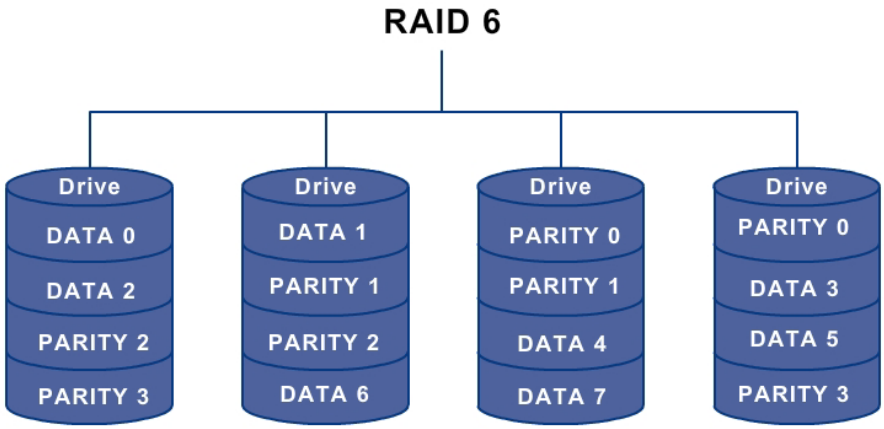


**Figure 5-4: RAID 6**

- **RAID IME**—RAID Integrated Mirroring Enhanced (IME) supports mirrored arrays with three to ten disks and hot-spare disks. This is implemented in Intel® IT/IR RAID. RAID IME requires at least three hard disk drives.
- **RAID 10**—this configuration is a combination of RAID 0 and RAID 1. It consists of striped data across mirrored spans. This configuration provides high data throughput and complete data redundancy, but uses a larger number of spans. RAID 10 requires at least four hard disk drives.

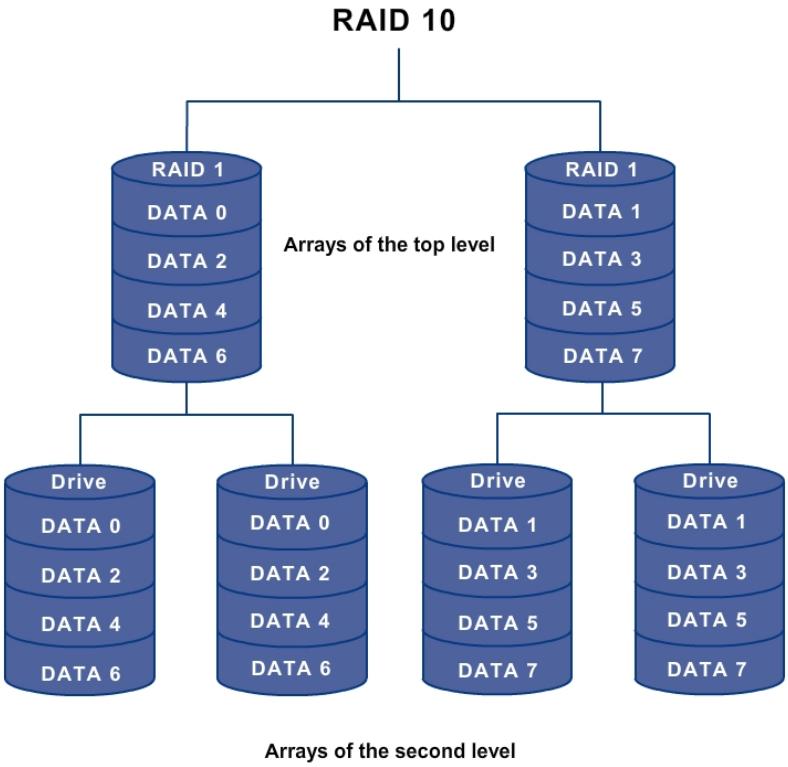


**Figure 5-5: RAID 10**

- **RAID 50**—this configuration is a combination of RAID 0 and RAID 5. This configuration uses distributed parity and disk striping. It works best with data that requires high reliability, high request rates, high data transfers, and medium to large capacity. RAID 50 requires at least six hard disk drives.

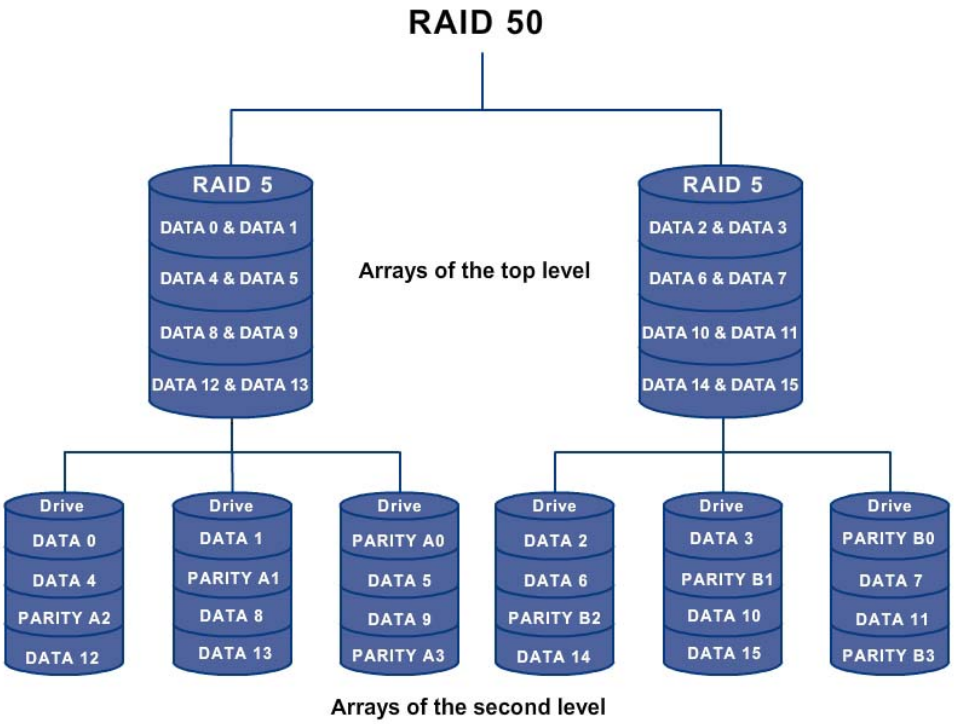


**Figure 5-6: RAID 50**

**Note:** It is not recommended to have a RAID 0, RAID 5, and RAID 6 virtual disk in the same physical array. If a drive in the physical array has to be rebuilt, the RAID 0 virtual disk will cause a failure during the rebuild.

- **RAID 60**—this configuration is a combination of RAID 0 and RAID 6. It uses distributed parity with two independent parity blocks per stripe in each RAID set and disk striping. A RAID 60 virtual disk can survive the loss of two disks in each of the RAID 6 sets without losing data. It works best with data that requires high reliability, high request rates, high data transfers, and medium to large capacity. RAID 60 requires at least six hard disk drives.

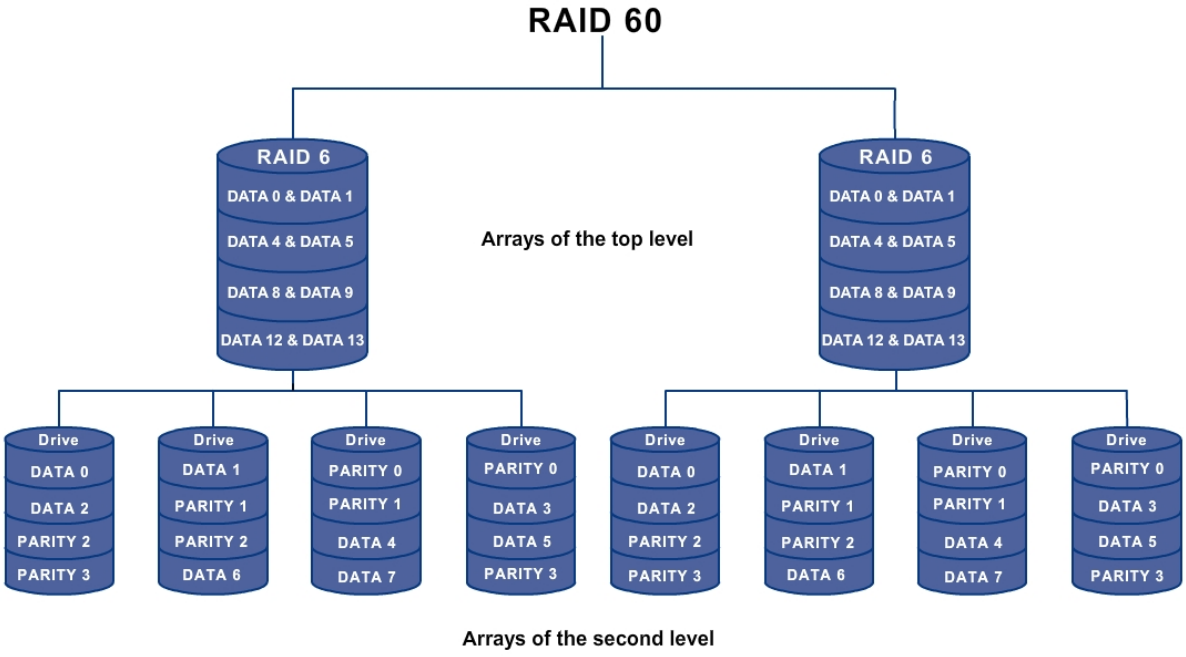


**Figure 5-7: RAID 60**

## 5.2 Supported RAID Levels

Intel® SCS supports RAID levels 0, 1, 5, 6, 10, and 1E. Use RAID Web Console 2 or other RAID management application to manage storage using other RAID levels.

For more information on RAID levels, see RAID Basics.

### 5.2.1 Selecting a RAID Level

The optimal RAID level for a disk array depends on a number of factors such as:

- The number of physical drives in the disk array
- The capacity of the physical drives in the array
- The need for data redundancy
- The disk performance requirements

For details on RAID level and usage scenarios, please refer Intel® RAID Software User's Guide.

### 5.2.2 Intel® RAID Technologies Supported in Intel® SCS

Intel® SCS supports the following RAID technologies.

| Options | RAID Configuration | RAID Monitoring |
|---|---|---|
| Intel® RAID Controllers | Yes | Yes |
| Intel® Integrated Server RAID | Yes | Yes |
| Intel® Software RAID | Not supported | Not supported |
| Intel® Embedded Server RAID Technology | Yes | Yes |

### 5.2.3 Recommendations to RAID and CDP Users

You can find Information on RAID Configuration matrix in http://support.intel.com/support/motherboards/server/scs/.

### 5.2.4 Dependencies on Hardware and Data Protection

Intel® SCS integrates Storage Management with Hardware Management, Continuous Data Protection, and the physical server. The same number of physical disks displayed in Hardware Management is displayed in Storage Management. Virtual disks created in Storage Management are displayed as volumes in Continuous Data Protection. Thus, any change, such as addition or removal of physical disks in the server, results in noticeable changes in all three modules.

The repository, or storage space, for data protection is allocated in Storage Management, using RAID. Failure of physical disk changes the state and health of virtual disks.

An error in storage automatically initiates appropriate actions in data protection, based on the scheduler settings. Continuous Data Protection takes a backup of data on the physical disk, ensuring no loss of data.

## 5.3 Storage Management Capabilities

Intel® SCS enables business continuity by allowing you to manage storage remotely. Actions (both scheduled and unscheduled) performed on storage are run in the background. You can schedule patrol read and event notifications. Scheduling patrol read helps you proactively monitor storage health. Scheduling events enables periodic event notifications based on actions and server health.

Any changes or errors in physical disks, RAID controllers, and virtual disks also affect Storage Management. These changes and errors are logged as events, based on their state, health, or action. Intel® SCS provides options to manage events.

The Storage Management module allows you to:

- View and manage physical disks, RAID controllers, and RAID arrays
- Create and manage virtual disks using RAID controllers
- Monitor storage health using health indicators
- View and manage events generated by the server
- Proactively check storage for errors and consistency

The Storage Management module in Intel® SCS provides options to configure and manage physical disks using RAID controllers.

The Storage Management module has three distinctive parts:

- Display of physical disks with enclosures
- RAID Configuration section consisting of connected RAID controllers and RAID arrays
- Events button, which displays the list of events

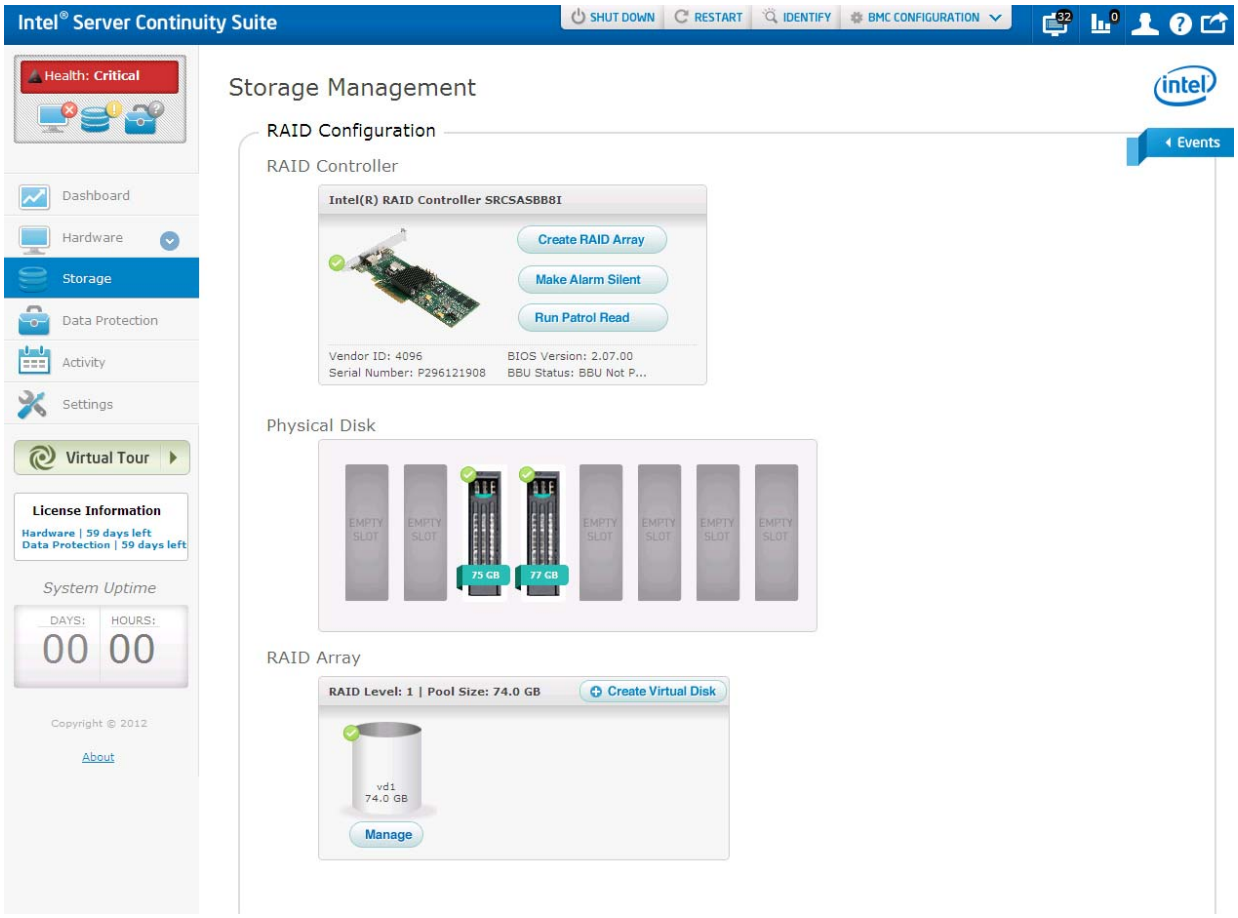


**Figure 5-8: Storage Management**

### 5.3.1 Physical Disks

Physical disks appear in the Storage Management module similar to how they are placed in the drive slots. The graphical view depicts the enclosure and location of the hard disk drives within the enclosure. This display of physical disks makes it easier to identify and locate them on the server, to perform management tasks.

Health is displayed based on the state of the physical disk. The state, slot number, and size of a disk are displayed if you point the mouse over the health indicator. The states can be one of the following:

- Online
- Hot Spare
- Unconfigured Good
- Copyback
- Offline
- Unconfigured Bad

- Failed
- Rebuild
- Unknown

#### 5.3.1.1 Managing the States of Physical Disks

The physical disks can be in one of the following states:

- Online—this state is shown when a physical disk is made part of a logical RAID volume. The state changes to online automatically after the creation of RAID logical volume.
- Hot Spare—a hot spare is used to replace a physical disk during disk failure as a failover mechanism to provide reliability in system configurations. Physical disks, in an Unconfigured Good state, can be made into a hot spare disk. The server automatically replaces a failing or failed disk based on the RAID configuration. The hot spare disk is used by the server to rebuild a damaged physical disk.
- Unconfigured Good—this state means that the disk is ready for RAID volume creation.
- Copyback—this state is shown on the destination disk when copying data due to disk inconsistency. In mirroring, if the physical disks lose consistency, the RAID controller automatically initiates copying of data from source to destination.
- Offline—if the user has explicitly disabled a physical disk for removal, the disk will be in Offline state. This is applicable only in the case of hot swap option support.
- Unconfigured Bad—this state is shown if the metadata of the physical disk is corrupt. You have an option to change the state of Unconfigured Bad to Unconfigured Good. If you do so, the metadata in the disk is updated.
- Failed—this state means the disk is corrupt.
- Rebuild—when a corrupt physical disk from the RAID volume is removed and the hot spare disk takes over, the state of the disk becomes Rebuild.
- Unknown—if the state of the disks does not fall in any of the above categories, then it is marked as Unknown.

#### 5.3.1.2 Unconfigured Good and Unconfigured Bad States

When a RAID controller is unplugged from the physical disk and reconnected, the state changes to Unconfigured Bad. In the Unconfigured Bad state, an option to change the state to Unconfigured Good appears on the physical disk.

To change to an Unconfigured Good state:

1 Click the **Manage** button below the physical disk in the Unconfigured Bad state.


**Figure 5-9: Make Unconfigured Good**

2 Click Make Unconfigured Good.

The state of the physical disk changes to Unconfigured Good.

#### 5.3.1.3 Creating a Hot Spare Disk

Physical disks, in an Unconfigured Good state, can be configured as a hot spare disk. The RAID configuration uses the hot spare disk to rebuild a damaged physical disk automatically.

**Note:** This option is available based on the RAID configuration and server support.

To create a hot spare disk:

1 Click the **Manage** button below the physical disk.

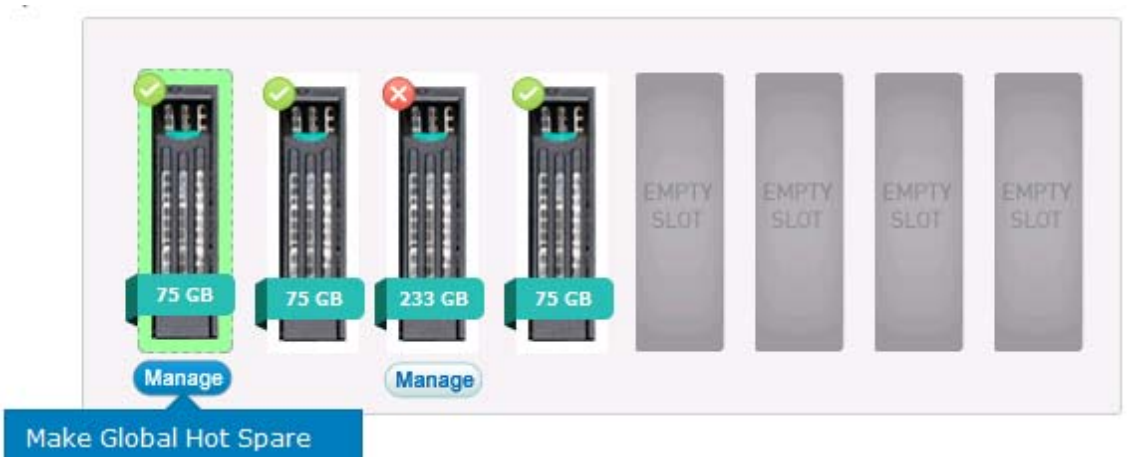


**Figure 5-10: Make Global Hot Spare**

2 Click Make Global Hot Spare.

The state of the physical disk changes to Hot Spare.

After a physical disk is configured as a hot spare, the **Remove Global Hot Spare** option is available.

**Note:** The hot spare disk is not available to create virtual disks using RAID.

#### 5.3.1.4 Removing Hot Spare

After a physical disk is configured as a hot spare, the **Remove Global Hot Spare** option is available.

To remove hot spare:

1 Click the **Manage** button below the physical disk in the Hot Spare state.

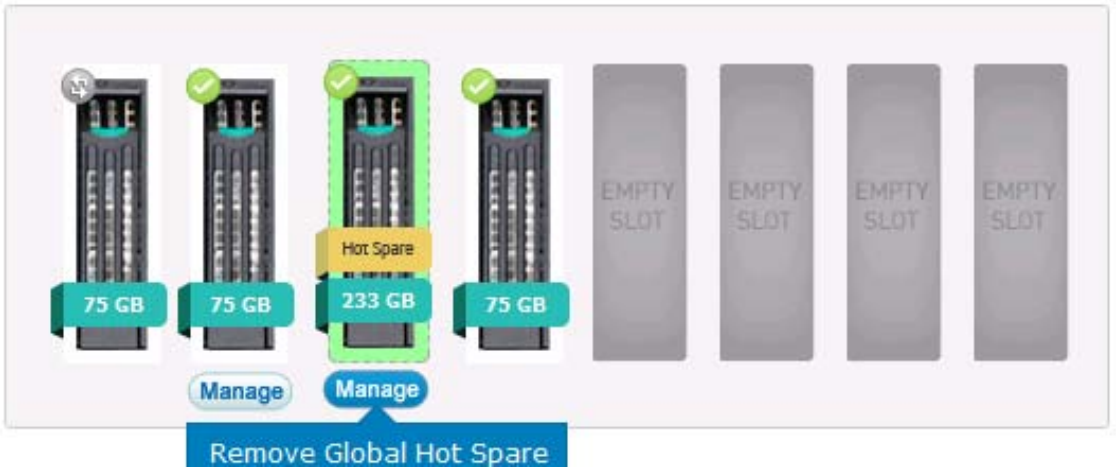


**Figure 5-11: Remove Global Hot Spare**

2 Click Remove Global Hot Spare.

The physical disk is available for creating virtual disks or hot spares.

#### 5.3.1.5 State of Physical Disks

The following table provides the different states of the physical disks.

**Table 5-1: State of Physical Disks**

| State | Description | Indicator |
|---|---|---|
| Unconfigured Good | Disk available for RAID creation |  |
| Online | Disk in use for creating virtual disks | |
| Hot Spare | Unused online disk available to replace a failed active drive, but not used for RAID creation | |
| Rebuild | Disk available for use as hot spare, but not for RAID creation | |
| Unconfigured Bad<br>Failed<br>Offline | Disk Metadata is corrupted | |
| Unknown | The state of the hard disk could not be determined by the RAID controller. | |

## 5.4 RAID Configuration

It is a complex task to create and manage RAID array in a server. System administrators need a good working knowledge of the RAID levels and the scenarios in which they are used to make best use of the RAID arrays.

Intel® SCS has simplified RAID configuration and management by providing an easy to use interface that enables you to use RAID with the click of a few buttons.

For more information on different RAID levels, see RAID Basics.

### 5.4.1 RAID Controllers

The Storage Management module displays all the RAID controllers installed in the server with details such as Vendor ID, BIOS Version, and Serial Number.

The RAID controllers help you:

- Create and manage RAID arrays from physical disks
- Allocate storage dynamically
- Run Patrol Reads to identify disk errors proactively
- Silence alarms remotely
- View and manage health

**Note:** The Patrol Read option is displayed only if it is supported by the RAID controller.


**Figure 5-12: RAID Controller**

The storage space, allocated using RAID controllers, appear under the RAID arrays.

RAID arrays allow you to:

- Add or delete virtual disks
- Locate virtual disks on physical disks
- Initialize virtual disks
- Check consistency on virtual disks
- Change properties of virtual disks

Intel® SCS allows you to manage storage at runtime, to allocate or expand disk space on demand. You can also allocate the repository for data protection.

### 5.4.2 Handling Multiple RAID Controllers

Intel® SCS displays all RAID Controllers associated with physical disks. Intel® SCS allows you to manage storage, using all supported RAID levels.

### 5.4.3 Handling Storage at Runtime

Intel® SCS allows you to manage storage dynamically at run time, without interrupting server performance.

### 5.4.4 Understanding Selection Logic

The selection logic helps to easily identify the RAID controllers and arrays, associated with the hard disk drives. When you click a hard disk drive, RAID controller, or array, Intel® SCS automatically selects the associated hard disk drive, RAID controller, and array.

### 5.4.5 Creating a RAID Array

To create a RAID array:

1 Click the **Create RAID Array** button against the RAID Controller.

The **Create RAID Array** screen appears. This screen shows the hard disk drives connected to the selected controller.

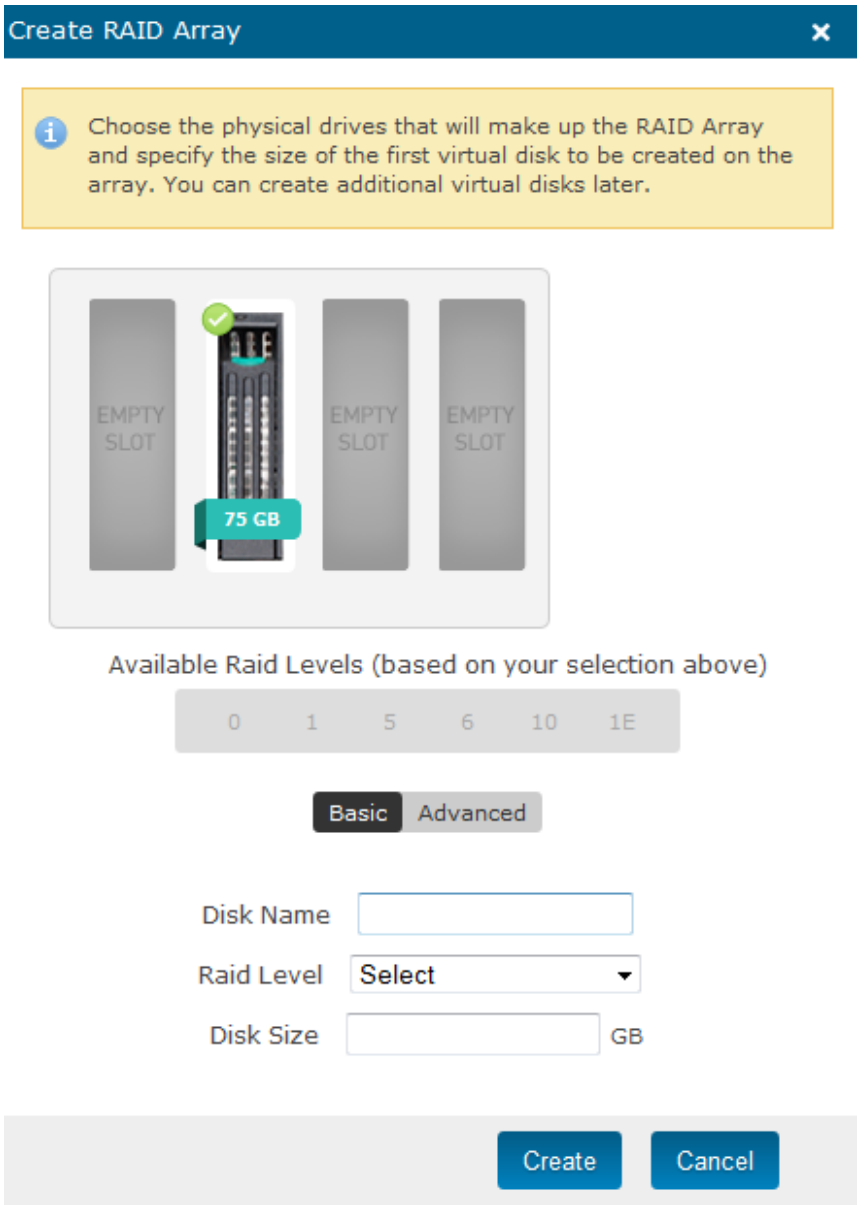


**Figure 5-13: Creating a RAID Array**

2 Select the physical disks to create a RAID volume.

The disks selected are highlighted.

**Note:** You can configure Basic and Advanced settings.

3 Enter the disk name.

4 Select a RAID Level from the **Raid Level** drop-down menu.

Intel® SCS supports RAID levels 0, 1, 5, 6, 10, and 1E.

For more information on RAID levels, see RAID Basics.

5 Enter the disk size.

6 Click **Advanced** to configure the following settings.

- Stripe Size
- Read Policy
- Write Policy

7 Click **Create**.

A RAID volume with the name given is created.

**Note**: Intel® SCS does not support importing of foreign configuration. If a foreign configuration exists in the hard disk drive, the Storage module in Intel® SCS detects the configuration when you click the **Create RAID Array** button. If you continue to create the RAID array, the foreign configuration is removed and the data stored in the hard disk drive is deleted. If you do not want to overwrite the RAID volume configuration and the data in the hard disk drives, you must import the foreign configuration using Intel® RAID Web Console 2 or RAID BIOS Console.

Once a RAID array is created, the RAID array, RAID Controller, and physical disk drives for that RAID array are highlighted in the interface if you select the RAID array.

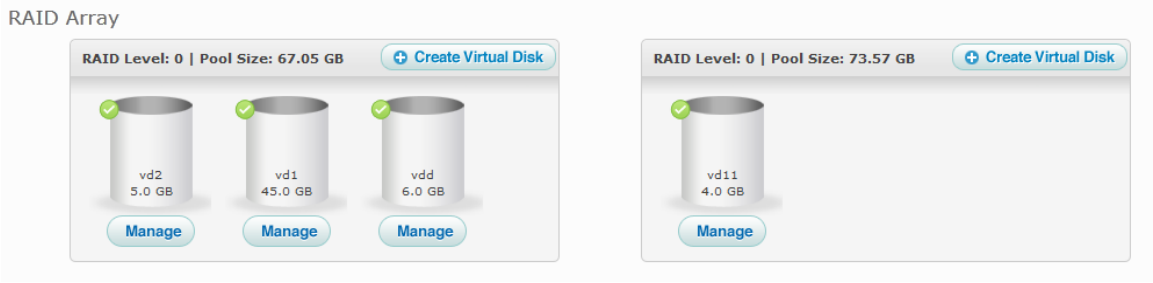


**Figure 5-14: RAID Array**

**Note:** Once a RAID volume is created and RAID firmware is initialized, you must initialize the virtual disk from Microsoft Windows Server Manager* to use the RAID volume.

### 5.4.6 Adding Virtual Disks

The RAID Controller allows you to create a RAID array with only one virtual disk. You can add more virtual disks to the RAID array based on the available disk size.

To add a virtual disk:

1 Click Create Virtual Disk on the RAID array.

**Note:** This option is available only if the RAID array is in an optimal state and healthy.

The Create | Virtual Disk window appears.

**Note:** You can configure only the Basic and Advanced settings. You cannot change the physical disk.

2 Enter the Disk Name and Disk Size.

**Warning:** The disk size cannot be more than the total available disk space.

3 Click **Advanced** to configure the following settings.

- Stripe Size
- Read Policy
- Write Policy

4 Click **Create**.

The new virtual disk appears in the RAID array.

**Note:** Click **Cancel** to exit without creating a virtual disk.

### 5.4.7 Deleting Virtual Disks

You can delete the virtual disks that appear in the RAID arrays only if the operation is supported by the RAID Controller.

**Warning:** Deleting a virtual disk could result in data loss. Before deleting a virtual disk, ensure that you take a backup of important data.

To delete a virtual disk:

1 Click the Manage button below the virtual disk.

2 In the menu, click Delete.

3 Enter the string displayed in the screen in the box provided.

4 Click Confirm.

The virtual disk is removed from the RAID array.

**Note:** Click **Cancel** to exit without deleting the virtual disk.

### 5.4.8 Initializing RAID Virtual Disks

After creating a virtual disk, you must initialize it to make it available for data storage.

To initialize a virtual disk:

1 Click the **Manage** button below the virtual disk image.

2 In the menu, click **Initialize**.

The Initialize | RAID Virtual Disk window appears.

3 Click Confirm.

**Note:** Click **Cancel** to exit without initializing the virtual disk.

Intel® SCS starts initializing the virtual disk. The time taken to initialize virtual disks depends on the disk size.

You can also format the virtual disks using the Disk Management menu in the server's Control Panel.

To initialize RAID virtual disk:

1 Click Start > All Programs > Administrative Tools > Server Manager > Storage.

2 Select Disk Management.

**Note:** You can either select MBR or GPT partition while initializing the virtual disk from Disk Management.

3 Create OS volumes as NTFS or FAT32 file system in the logical volume.

### 5.4.9 Locating Physical Disks

The Storage Management module makes it easier to locate physical disks associated with virtual disks.

To locate a physical disk:

1 Click the **Manage** button below the virtual disk image.

2 In the menu, click **Locate**.

The Locate | Physical Disk window appears.

3 Click **Locate**.

An indicator glows on the physical disk.

**Note:** Click **Cancel** to exit without locating the physical disk.

### 5.4.10 Changing Properties of Virtual Disks

The Storage Management module allows you to change the following properties of virtual disks, depending on the RAID controller.

- Disk Name
- Read Policy
- Write Policy
- Access Policy
- Cache Policy

**Note**: Disk Cache Policy determines whether the hard disk drive write back cache is enabled or disabled. When the Write Policy is set to Write Through mode, the Disk Cache Policy can have a very big impact on the write performance. When the Write Policy is set to Write Back mode, the impact of Disk Cache Policy is much lesser and in many cases, negligible.

Enabling drive write back cache can cause loss of the data in the drive cache if there is a sudden loss of power to the chassis. When using this feature, it is recommended that you connect the chassis to a UPS so that the chassis does not shut down before the data in the cache is saved in the repository. To disable write back cache of repository, refer to the steps in the Prerequisites section of Intel® Recovery Wizard Help pages.

To change properties:

1 Click the **Manage** button below the virtual disk image.

2 In the menu, click **Properties**.

The Properties | RAID Virtual Disk window appears.

3 Change the required properties.

4 Click **Save**.

**Note:** Click **Cancel** to exit without changing properties.

### 5.4.11 State and Health of Virtual Disks

The following table provides an overview of health, based on different states of the virtual disks.

**Table 5-2: State and Health of Virtual Disks**

| State | Description | Indicator |
|---|---|---|
| Optimal | The virtual disk is functioning correctly without errors |  |
| Partially Degraded | The virtual disk is functioning with one of the disk in the RAID array corrupted. The performance of the array is reduced. |  |
| Degraded | The virtual disk is not functional |  |
| Offline | The virtual disk is not functional | |

## 5.5 Monitoring and Reporting

Storage is monitored using health indicators and events. Events are logged for every change in state and action performed. For more information on events and actions, see Events and Actions.

### 5.5.1 Events and Actions

Intel® SCS logs storage related events and alerts. You can see them by clicking on the Event tab in the Storage Management module.

Events are logged by time and source of generation. They are marked as critical (  ), warning (  ), and informational (  ) based on their state and health. Informational events are generated after performing an action, when the components are in a healthy state. Warning events are generated when an action fails to execute or when the components change to a warning state. Critical events are generated when storage is in any of the states that result in critical health.

The events icon on the Intel® SCS title bar displays the total number of events. You can view events by clicking the events icon.

A few examples of RAID events logged are given in the table below.

**Table 5-3: RAID Events**

| Event | Description | Event Severity | Source of event |
|---|---|---|---|
| Firmware initialization started | The user has forced an initialization event on a logical volume. | | RAIDController |
| VD 00/0 is now DEGRADED | Virtual disk 0 | or depending on the RAID controller | RAIDController |
| Removed PD | Physical drive is removed from the enclosure | | Physical Disks |
| Rebuild automatically started on PD | Rebuild happens when the hot spare takes over a removed/damaged physical disk | | Physical Disks |
| Global Hot Spare Created on PD 0b | Hot spare disk is added to a RAID array | | Storage |

The actions performed on the RAID controllers and arrays, such as patrol reads, initialization, and consistency checks can be run in the background and are listed in the Actions list.

Click the Actions icon on the Intel® SCS title bar to see the list of actions. The actions icon displays the total number of actions. For more information on reporting, see Reporting Events.

## 5.6 Managing Storage Health

The Storage Management module displays health indicators and associated events for the physical disks, RAID controllers, and RAID arrays.

In addition to managing the storage health, using health indicators and events, Intel® SCS provides options to run patrol reads and consistency checks.

These operations can be run in the background and are listed in actions. You can monitor the progress by viewing the task in the actions list.

### 5.6.1 Running Patrol Reads

The RAID controller patrol read operation allows you to monitor virtual disks proactively to identify disk errors. Running a patrol read on a virtual disk helps avoid disk failures that could result in data loss.

To run patrol reads:

1 Click the **Run Patrol Read** button against the RAID Controller.

2 Click **Start**.

The RAID controller begins the patrol read operation. The operation continues to run in the background even if you logout from Intel® SCS.

### 5.6.2 Scheduling Patrol Read

Intel® SCS allows you to schedule patrol reads to run:

- Daily
- Weekly
- Monthly

To schedule a patrol read:

1 Click the **Run Patrol Read** button against the RAID Controller.

2 In the **Patrol Read** window, click **Schedule**.

3 Select the **Frequency**.

4 Select **On** to activate the schedule.

5 Click **Save**.

Intel® SCS runs the patrol read operation based on the schedule. The operation will run when the system is idle or during periods of less disk accesses.

#### 5.6.2.1 Checking Consistency of Virtual Disks

The Storage Management module also provides an option to perform a consistency check on the virtual disks.

To check consistency:

1 Click the **Manage** button below the virtual disk.

2 In the menu, click **Consistency**.

The Consistency Check | RAID Virtual Disk window appears.

3 Click **Confirm**.

Intel® SCS starts a consistency check on the virtual disk.

**Note:** Click **Cancel** to exit without starting a consistency check.

# 6 Data Protection

## 6.1 Introduction to Data Protection

The Data Protection module in Intel® Server Continuity Suite (Intel® SCS) helps you protect critical business data round the clock. Data protection is achieved by continuously backing up data on the server hard disk drives to a storage volume that is setup for this purpose, enabling you to retrieve it on demand.

Intel® SCS uses Continuous Data Protection (CDP) to continuously backup data in the server hard disk drives. CDP works to continuously backup data as that is saved in the server hard disk drives, against the paradigm of backing up data discretionally. Thus, you can retrieve the data backed up in the storage volume up to and including the most recent consistency point. Intel® SCS provides a user friendly interface for you to create a protection plan and restore the data with a few clicks.

The Data Protection module is available when you purchase and activate the Intel® SCS Data Protection Manager or Intel® SCS Advanced Data Protection Manager license.

### 6.1.1 Advantages of CDP over Traditional Backup Systems

In today's business scenarios, CDP is essential for instantaneous and timely recovery of the most recent data. Compliance to disaster recovery requirements is also a key factor for business continuity.

The following table outlines the advantages of CDP based backup systems over the traditional backup systems.

**Table 6-1: CDP versus Traditional Backup**

| Traditional Backup Systems | CDP Based Backup Systems |
|---|---|
| Backup is taken once in a while, usually once a day. The difference between the data on the server hard disk drives and its backup is so much that business continuity is not possible. | Backup is taken continuously. The difference between the data on the server hard disk drive and its backup depend on factors such as the rate of data change in the server disk drive and the speed of saving the data on the backup storage volume. |
| Backup is taken when the systems are | Backup is taken even when the server is |

| Traditional Backup Systems | CDP Based Backup Systems |
|---|---|
| least used as the backup activity uses a lot of resources. | operating at its peak, without affecting the performance of the server. |
| Servers and the applications operating on it may have to be stopped while taking a backup to ensure application-level and file-system consistency. | Servers or applications can continue to operate without any downtime because backup is taken continuously; this ensures application-level and file-system consistency. |
| You can roll back data stored at the time a backup was taken. In case of a disk failure, the data saved in the server is lost. | You can roll back data stored at the most recent consistency point created. Depending on your license, Intel® SCS creates consistency points every eight hours, two hours, 30 minutes, or 15 minutes. |

## 6.2 Preparing for Data Protection

### 6.2.1 Prerequisites for the Data Protection Module in Intel® SCS

Intel® SCS uses CDP to continuously backup data in the server hard disk drives. The following are some key factors that must be considered for the Data Protection module in Intel® SCS to work effectively:

1 The total size of the source data—you must determine the size of the data that you want to protect and select the size of the repository accordingly.

**Note:** If you have Intel® SCS Data Protection Manager license, the available space in the repository must be about three and a half times the total size of the virtual disks you want to protect. If you have Intel® SCS Advanced Data Protection Manager license, the available space in the repository must be about four times the total size of the virtual disks you want to protect.

2 The data change rate—you must estimate the data change rate (for example, 1 MB per hour or 24 MB per day). You can do this estimation monitoring the data generated over a period of time.

3 Type of backup disk drive—you must select the appropriate type of disk drive for the server and for the data backup repository. It can be one of the following:

- SATA/SAS/SSD hard disk drive or a combination of these
- USB 2.0
- iSCSI drive
- RAID volume

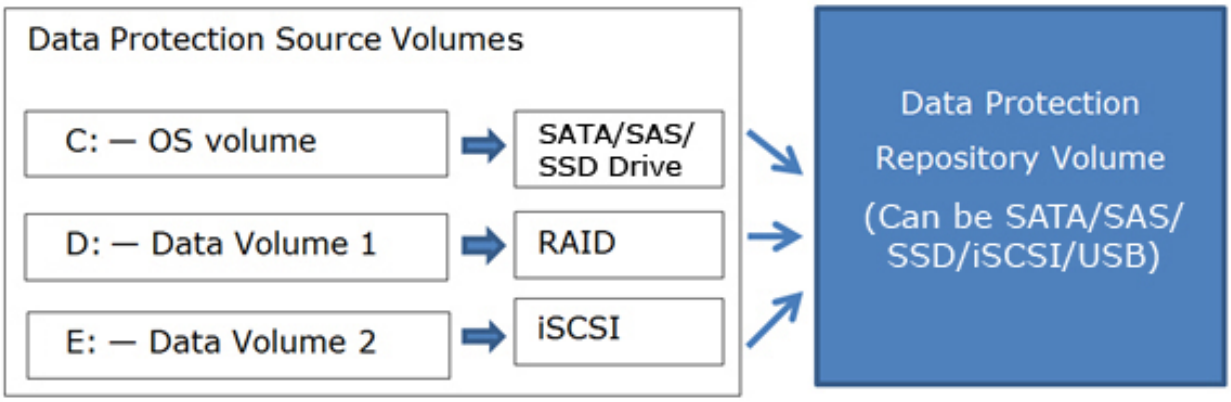


**Figure 6-1: Data Protection on Different Disk Drive Types**

4 Write back cache of repository volume must be disabled. To disable write back cache of repository, refer to the steps in the Prerequisites section of Intel® Recovery Wizard Help pages (**Start** > **All Programs** > **Intel®** > **Intel® Server Continuity Suite – Data Protection** > **Intel® Recovery Wizard**).

### 6.2.2 Configurations Not Supported by the Data Protection Module

For data protection to work, you must:

- Not use a volume in which a virtual machine is installed
- Not use Fat Allocation Table (FAT) file system as the source or repository
- Not use a dynamic disk configuration as a repository or a source volume
- Not use any anti-virus software to scan the repository
- Not use a volume with a physical sector size of 4KB as a source or repository
- Not use a USB drive of more than 2.2 TB size as a repository
- Not use an iSCSI drive as a repository to protect multiple servers (multiple concurrent connections)
- Not use a volume with bad sector as a source or repository

### 6.2.3 Selecting Source and Backup Repository Disk Types

The ability of CDP to keep the data repository up to date with source data depends a lot on factors such as the rate of data change in your business environment and the speed of disk drives used in the source and repository volumes. The speed of the repository disk drive must be high enough to match up to the rate of data change and the speed of the source disk drive for effective data protection. For example, if you use a USB 2.0 drive as a backup repository for an SSD based source drive in an environment with a data change rate greater than 1TB per hour, the data lag time will be very high.

We recommend that you run the trial version of the data protection module in Intel® SCS for a period of about one month to assess the type of disk drives required for the business environment. The Reporting module in Intel® SCS provides a data lag report that you can use to assess whether the data protection lag is within acceptable limits. You can change or continue to use the disk drive accordingly.

**Note:** You can use USB drives for backing up the data using Intel® SCS. However, USB drives are not recommended for protecting critical data. The USB drives that work for a period of two months with medium data change rate (less than 5 MB per hour) are listed in http://support.intel.com/support/motherboards/server/scs/sb/CS-032917.htm.

### 6.2.4 Impact of the Rate of Change of Data on Backup

The rate at which the data on the volumes you protect changes has a direct impact on the performance of the data protection system.

If the data change rate is very high, there may be a difference in the data in the source drive and in the backup drive. The difference in time between the data in the physical hard disks on the server and its backup in the repository is known as Recovery Point Objective (RPO). The greater the RPO value for a volume, the greater is the difference in data between the source disk drive and its backup.

### 6.2.5 Capabilities of the Data Protection Module in Intel® SCS

The data protection feature in Intel® SCS is based on continuous data protection (CDP). Intel® SCS continuously takes a backup of data stored in the server physical hard disks to a volume configured as Repository. You can retrieve this data any time with the click of a few buttons.

**Note:** If the server becomes unbootable or if the boot volume itself is corrupted, you can retrieve the boot volume and boot the server using the rescue disk provided with Intel® SCS.

Using the data protection module in Intel® SCS, you can:

- Configure a repository—configure a suitable storage volume outside the server to back up your business critical data saved in the server hard disk drives.
- Create a data protection plan—by creating consistency points depending on the license and the health of the server and its components.
  If you have Intel® SCS Advanced Data Protection Manager license, consistency points are created every two hours by default. You can change that time to any interval from one hour to four hours. You can modify the protection plan by clicking **Modify** in the main Data Protection page.
  If you have Intel® SCS Data Protection Manager, Intel® SCS creates consistency points every eight hours.
- Start protecting volumes based on the protection plan. You can also pause and resume protection. You can perform these actions on all the volumes in a server or on individual volumes.
- Analyze RPO and optimize data backup—identify lags in data backup using RPO shown in a graph and take steps to optimize data backup.
- Monitor the different states of protection—the status of protection of all the volumes in a server and on individual volumes are displayed in the interface.
- Monitor the health—the health of the module and the volumes is indicated in the interface using colors.
- Manage data backup—monitor the events generated in the Data Protection module and take necessary actions.

### 6.2.6 Dependencies on Hardware and Storage

Data backup is enabled on volumes on the physical hard disks available in Hardware Management and Storage Management modules. A change in the health of the server hardware or storage components automatically triggers an action in data protection.

For example, an abrupt increase in HDD temperature triggers an event with a health issue in Hardware Management and Storage Management.

Depending on the license used, consistency points are created more frequently than when the server is in healthy state. Once the server health

is restored, you can retrieve data of the most recent consistency point stored in the repository, thereby ensuring minimal data loss.

## 6.3 Initiating Data Protection

When you access the Data Protection module for the first time, all the active volumes listed in the **Microsoft Windows Server Manager*** > **Storage** > **Disk Management** except the volume in which the operating system is installed appear on the screen.

To start data protection, you must configure a storage volume as a repository. The Data Protection module takes a backup of the data in the server hard disk drive in the Repository you create. You can configure only one volume as a Repository. The storage volume must have enough space to store the backup data.

**Note:** If you have Intel® SCS Data Protection Manager license, the available space in the repository must be about three and a half times the total size of the virtual disks you want to protect. If you have Intel® SCS Advanced Data Protection Manager license, the available space in the repository must be about four times the total size of the virtual disks you want to protect.

The protection of the volumes is inactive. Once the repository is configured, you must start protecting the volumes.

## 6.4 Configuring a Repository

To start protecting your volumes, you must configure a repository to backup data. The repository must be a volume of a large size that can accommodate the incremental backup of the protected volumes.

**Note:** If you have Intel® SCS Data Protection Manager license, the available space in the repository must be about three and a half times the total size of the virtual disks you want to protect. If you have Intel® SCS Advanced Data Protection Manager license, the available space in the repository must be about four times the total size of the virtual disks you want to protect.

The repository volume can be any of the following:

- A volume on a SATA/SAS/SSD hard disk drive
- A volume on an external USB drive

**Note**: You can find information on supported USB drives in http://support.intel.com/support/motherboards/server/scs/sb/CS-032917.htm.

- An iSCSI volume

**Note**: The repository volume used for data backup must be assigned an NTFS file system.

The CDP module displays the volumes that can be used to configure the Repository. It also displays the total size and free size of the volumes available, to help you choose an appropriate volume.

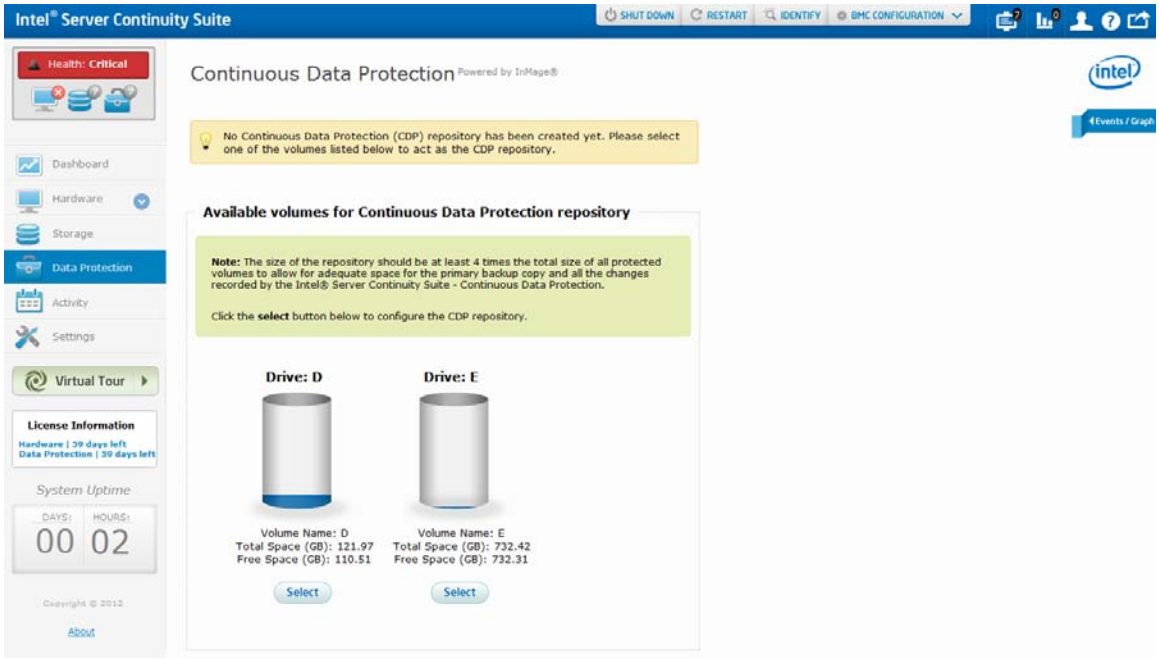


**Figure 6-2: Available Volumes For Repository**

**Note:** If no volume is available, a message to connect a volume and proceed is displayed.

To configure a Repository:

1 Click the **Select** button below the volume you want to configure as the Repository in the **Available Volumes For Repository** screen.

The Configure repository dialog appears.

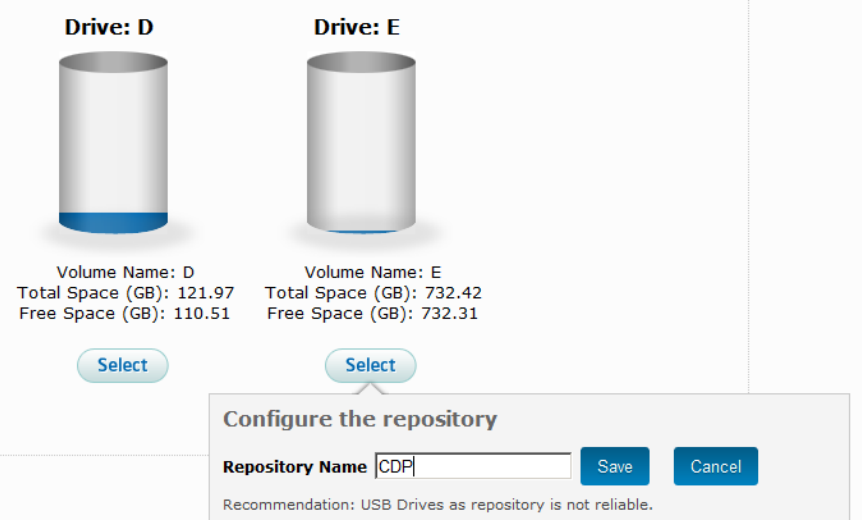


**Figure 6-3: Configure Repository**

2 Enter a Repository Name.

**Note:** The name must not be more than 15 characters long and must not contain special characters.

3 Click **Save**.

During the configuration of the repository, the status of the volume changes to Repository Configuration Pending.

The time taken to configure a repository depends on the selected repository size.

Once the selected volume is configured as the repository, the message changes to Configured Repository; the drive is now ready to backup data.

The volumes are in an unprotected state. You must setup the data protection plan to initialize CDP on the volumes.

## 6.5 Setting Up Data Protection Plan

After a volume is configured as the Repository, you must set up a protection plan to start continuous data backup.

To set up a protection plan:

1 In the Data Protection screen, click **Set up Protection**.

The Set up Protection Plan window appears.

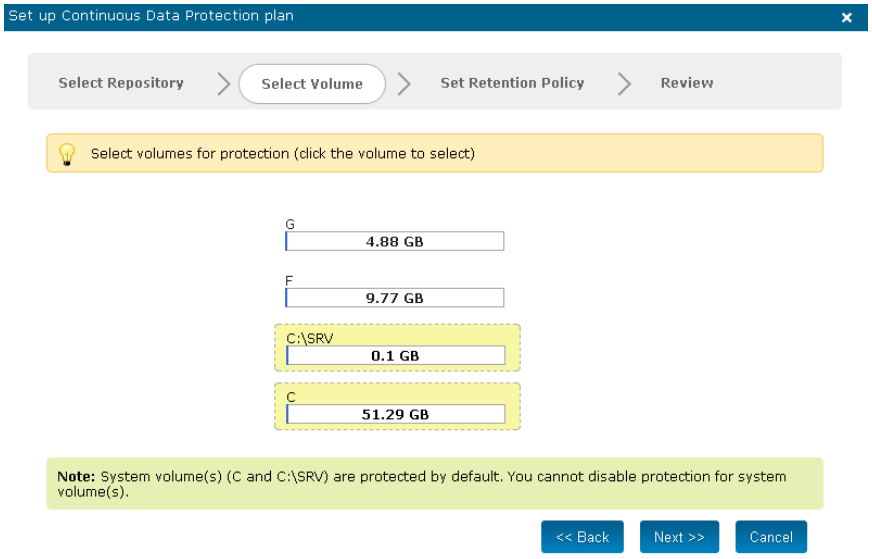


**Figure 6-4: Set up Protection Plan—Select Repository**

2 In the **Select Volume** tab, select the volume you want to protect.

3 Click **Next**.

**Note**: If you have Intel® SCS Advanced Data Protection Manager license, the Scheduler tab provides options to configure the consistency points and retention settings. By default, consistency points are created every two hours. You can change that time to any interval from one hour to four hours. You must select the consistency points for the protected volumes based on the health status.
If you have Intel® SCS Data Protection Manager, Intel® SCS provides the default configuration: consistency points are created every eight hours.

4 Configure the consistency points and retention settings and click **Next**.

The Review tab displays a summary of the protection plan.

5 Click **Confirm** to accept the protection plan settings.

Intel® SCS starts data backup on the volumes selected. The Data Protection screen displays the volumes on the server and their protection status. Intel® SCS synchronizes two volumes at a time with the repository.

The protection status changes to Provisioning Pending while Intel® SCS applies the protection plan to the selected volumes.

If you have Intel® SCS Advanced Data Protection Manager license, you can modify the protection plan by clicking **Modify** in the main Data Protection page.


**Figure 6-5: Data Protection—Active**

Each volume displays:

- The time taken to synchronize data with the repository
- Status of synchronization
- Protection state
- Health

## 6.6 Monitoring Data Protection

Intel® SCS allows you to monitor data protection using the following features:

- Protection Status
- Health
- Data Backup

**Note**: If the message "The configured repository device is missing. Please connect the device back to continue protection." is displayed, you must connect the repository back. If you cannot connect the configured repository back, delete the repository using the **Delete Repository** option in **Data Protection Settings** tab in **Settings** menu and start data protection again.

### 6.6.1 Protection Status

The health of data protection on the volumes and repository is displayed in the interface using different colors:

- Green—data protection is working correctly
- Yellow—warning
- Red—Critical
- Grey—indicates health information is unavailable

### 6.6.2 Health

The health of the protection module is shown in the top bar using the following icons:

—Healthy

—Warning

—Critical

—Health information is unavailable

### 6.6.3 Data Backup

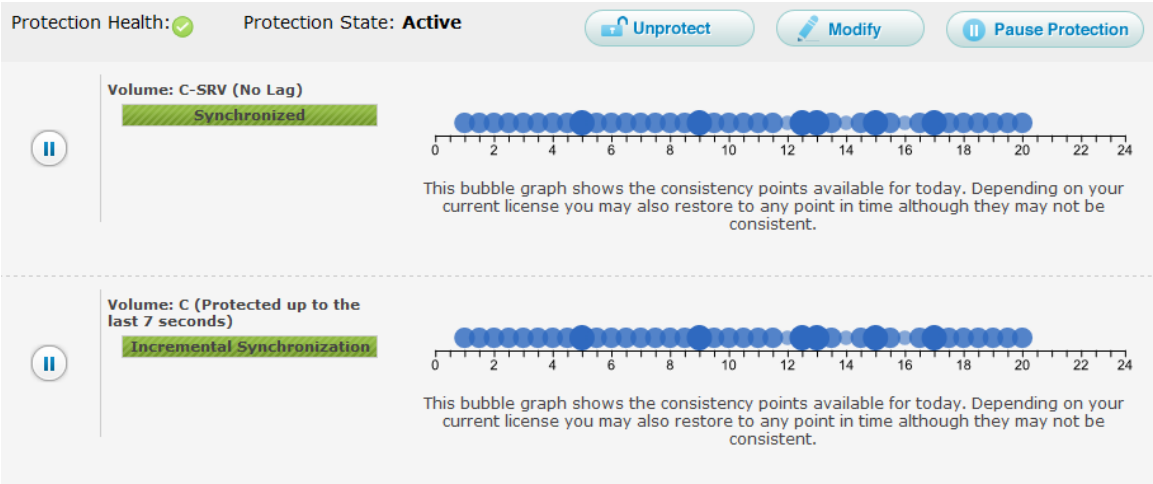


**Figure 6-6: Consistency Points Timeline Graph**

The volumes on the system are displayed, with each row representing one volume.

The status of data synchronization and protection is displayed on the volumes:

- Initial Synchronization—indicates that the volume is being synchronized for data backup for the first time
- Synchronized—indicates that the data backup is complete
- Incremental Synchronization—indicates that the data backup is in progress
- Pause Pending—indicates that the protection is being paused

- Paused—indicates that the protection is paused
- Queued—indicates that the volume is queued for protection
- Re-synchronizing—indicates that the volume is being synchronized again
- Pause for Recovery—indicates that the volume is paused and recovery is going on

## 6.7 Understanding the Data Protection Interface

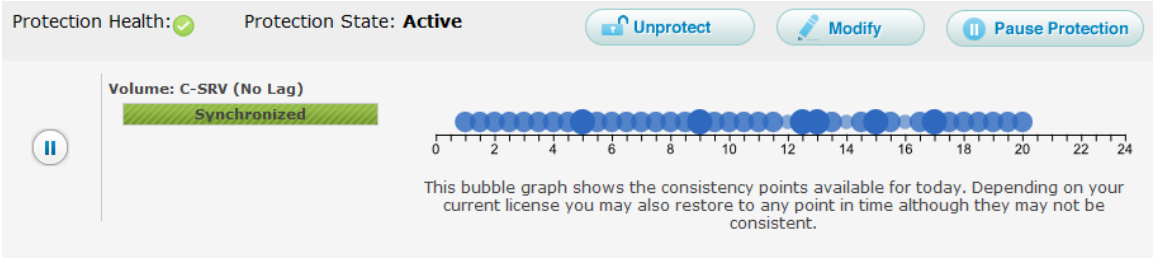


**Figure 6-7: Understanding the Data Protection Interface**

The volumes on the system are displayed, with each row representing one volume.

For each volume, you can see:

- Action buttons—to perform actions that you can perform on the volume based on its state. If no action can be performed on the volume because of the state it is in (for example, Pause pending), the button is not displayed.
- Volume name and RPO value—the name of the volume and the time lag between the source volume and its backup in the Repository. The RPO value indicates the time for which you might lose data.
- Status bar—shows the progress of an action. The percentage of completion is displayed if you point the mouse to the bar.
- Status color—the color of the volume indicates its protection health. If the RPO value for the volume is very high, the health is critical.
- Protection state—the state of the volume is displayed by the text inside the bar.
- Consistency points—denoted by bubbles on timeline graph. The size of the bubble indicates the number of consistency points available. The number of consistency points is displayed if you point the mouse to a bubble. The exact time the consistency points were created is displayed if you click a bubble.

## 6.8 Data Protection Operations

You can modify the protection plan settings for all the volumes in a server or for individual volumes using the options in the interface.

### 6.8.1 Operations Available for Individual Volumes

Depending on the state of a volume, you can perform the following operations:

- Add to protection plan
- Pause protection
- Resume protection

### 6.8.2 Operations Available for the Server

You can perform the following operations to modify the protection of all the volumes in a server:

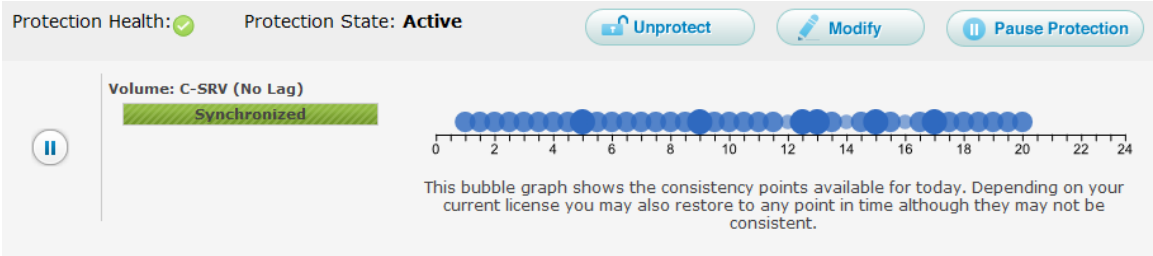


**Figure 6-8: System level Options**

- Pause protection
- Resume protection
- Modify protection plan
- Unprotect

### 6.8.3 Protecting Individual Disk Drives

You can start protecting unprotected or newly added disk drives. If a disk drive is unprotected, a plus button (⊕) is provided for that volume.

To protect a disk drive:

1 Click ⊕ next to the volume.

The Confirmation dialog appears.

**Note:** This option is available only for volumes that are unprotected.

2 Click **Yes**.

The Status Message dialog appears.

3 Click **Ok**.

The protection status changes to active and CDP resumes on volumes.

**Note:** Click **Cancel** to exit without protecting a volume.

### 6.8.4 Pausing and Resuming Protection

You can pause data protection temporarily while performing certain tasks on the disk drives. If you pause protection, data backup for that disk drive is halted until the protection is resumed.

To pause data protection:

1 Click next to the volume.

The Confirmation dialog appears.

**Note:** This option is available only for volumes that are protected.

2 Click **Yes**.

The Status Message dialog appears.

3 Click **Ok**.

**Note:** Click **Cancel** to exit without pausing data protection.

To resume protection:

4 Click next to the volume.

The Confirmation dialog appears.

**Note:** This option is available only for volumes on which data protection is paused.

5 Click **Yes**.

The Status Message dialog appears.

6 Click **Ok**.

**Note:** Click **Cancel** to exit without resuming protection.

If you resize the source volume, follow the steps below to resume protection:

1 Stop the Backup Agent Service. To stop the Backup Agent, click **Start** > **Run** > **services.msc**.

2 In the Backup Agent Service wizard, find Intel® Backup Agent Service and stop that Service.

3 Click **Start** > **My Computer** and right click on **Source Volume Properties**. Note the volume capacity in bytes.

4 Get the respective target volpack. To get the target volpack, execute the command

<*INSTALL_PATH*>\cdp\cdpcli.exe --virtualvolume --op=list

The list of virtual volumes mounted in the system displays.

For example, if the install path is C:\Program Files (x86)\Intel\SCS\, you need to execute the command

c:\Program Files (x86)\Intel\SCS\cdp\cdpcli.exe --virtualvolume --op=list

The list of virtual volumes mounted in the system displays as given below:

- r:\381859e2-4bba-af48-a1cb3d911db4d3b1\f_virtualvolume
- r:\381859e2-4bba-af48-a1cb3d911db4d3b1\e_virtualvolume
- r:\381859e2-4bba-af48-a1cb3d911db4d3b1\c__srv_virtualvolume
- r:\381859e2-4bba-af48-a1cb3d911db4d3b1\c_virtualvolume

5 Resize the target Volpak such that it is either equal to or larger than the source volume by executing the command

cdpcli.exe --virtualvolume --op=resize --devicename=<*device name from the above command*> --size=<*size of modified volume in bytes*> --sizeinbytes

6 Navigate to the Intel® Server Continuity Suite – Data Protection install path and clear the agent cache by issuing the command

drvutil --stopfiltering <*drive letter or mount point*> -deletebitmap

7 Start the Intel® Backup Agent Service.

8 Resume the protected pair for which protection was paused due to volume resize.

9 Restart Resync for that volume using the **Data Protection** tab in the **Settings** page.

**Note**: The steps are valid only for extended volume resize. Shrinking volume resize is not supported.

## 6.9 Events

Intel® SCS logs data protection related events. You can see them by clicking the Events tab in the Data Protection module.

Events are logged by time and source of generation. They are classified as critical (), warning (), and informational () based on their state and health. Informational events are generated after performing an action, when the components are in a healthy state. Warning events are generated when an action fails to execute or when the components change to a warning state. Critical events are generated when data protection is in any of the states that result in critical health.

The events icon on the Intel® SCS title bar displays the total number of events. You can view events by clicking the events icon.

For more information on events, see Events and Actions.

## 6.10 RPO Graph

The difference in time between the data in the physical hard disks on the server and its backup in the repository is known as Recovery Point Objective (RPO). The RPO graph displays the RPO values at each hour for 24 hours. The X axis shows the time and the Y axis shows the RPO value in seconds.

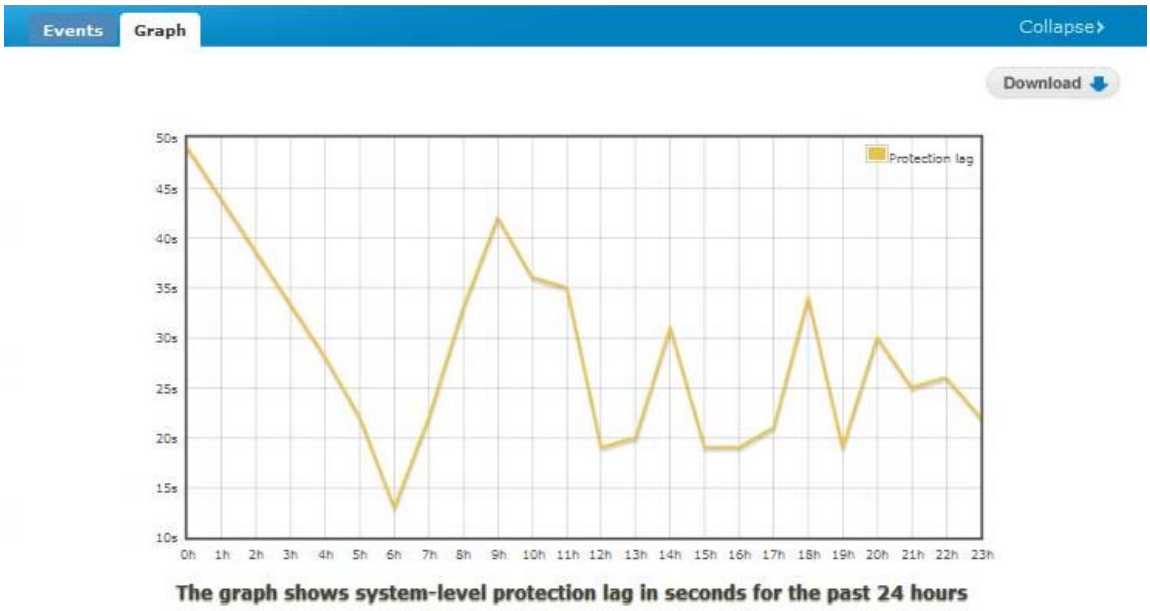


**Figure 6-9: RPO graph**

## 6.11 Data Recovery

Intel® SCS offers several ways to recover the protected data.

Using Intel® SCS Recovery Wizard, you can do the following:

- Recover Volumes
- Clone Volumes
- Recover Files

### 6.11.1 Volume and File Recovery and Volume Clone

You can recover or clone volumes or recover files from a repository to the server hard disk drive.

- Recover Volumes—this option allows you to recover a volume from a consistency point or time.
- Clone Volumes—this option allows you to copy the data on a volume to another. The available memory in the target volume must be equal to or higher than the size of the data in the source volume.
- Recover Files—this option allows you to recover a file or a folder from a consistency point or time.

The initial screen of the Recovery Wizard displays information about the recovery options.

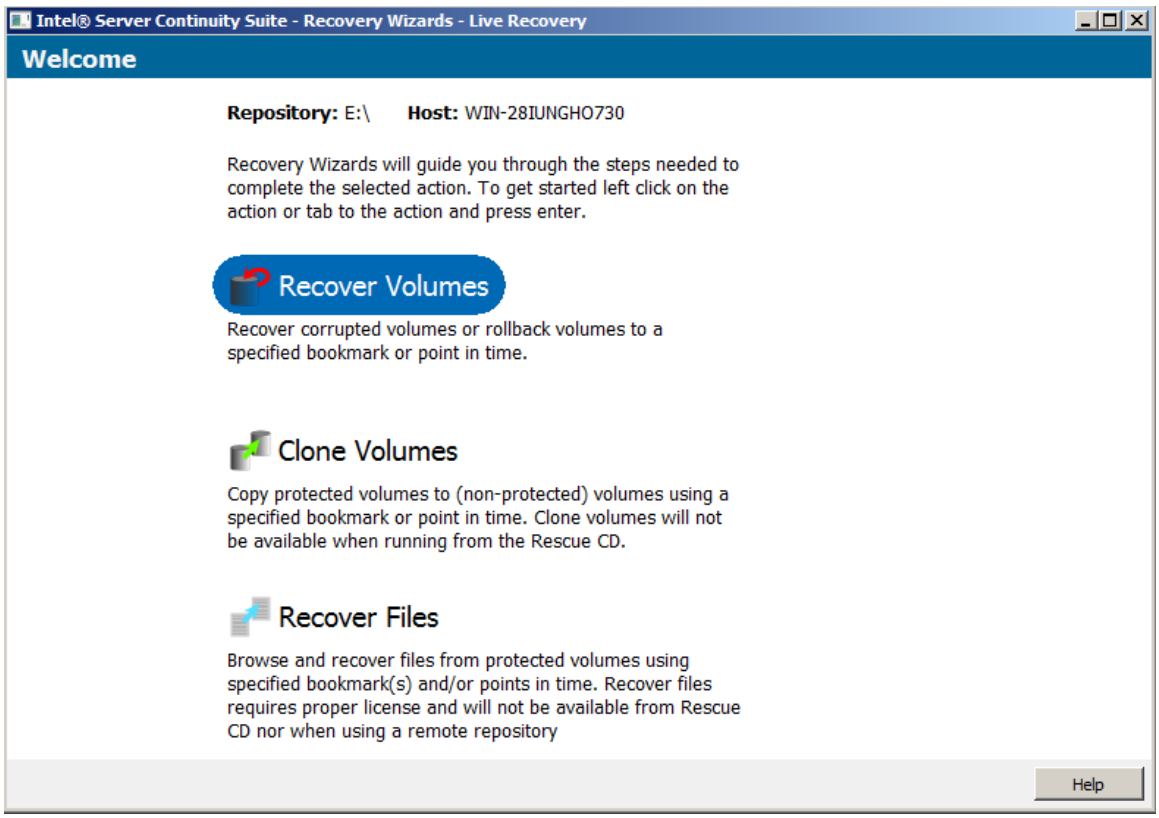


**Figure 6-10: Recovery Wizard**

#### 6.11.1.1 Recovering or Cloning Volume

To start recovering or cloning a volume or volumes:

1 Click the **Recover Volumes** or **Clone Volumes** button.

The Select Recovery screen appears.

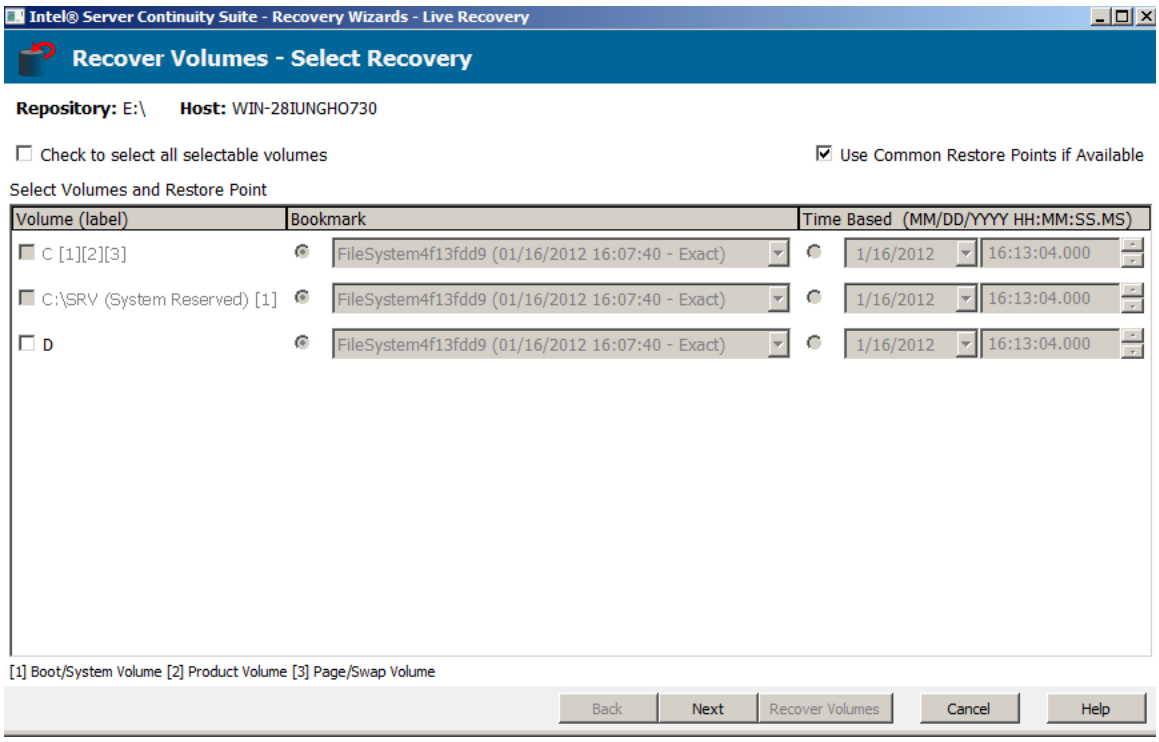


**Figure 6-11: Recover Volumes - Select Recovery screen**

2 Select the volume or volumes you want to recover or clone.

**Note**: Volumes that cannot be recovered or cloned using the Recovery Wizard are disabled in this screen.

3 For each volume, select the consistency point (marked **Bookmark** in the interface) or the time from which you want to recover or clone and click **Next**. The consistency points available for each volume are listed in the **Bookmark** drop down menus.

**Note**: We recommend that you recover or clone from a consistency point. To ensure consistency across recovered or cloned volumes, we also recommend that you select the **Use Common Consistency Points if Available** option.

4 If you are cloning a volume, the Manual Disk Mapping screen appears. Select the target volume using the drop down menu and click **Accept**.

The confirmation screen appears.

5 Verify the details and click **Recover Volumes** or **Clone Volumes**.

6 Click **Done**.

**Note**: If the source and target volumes do not match, a warning message is displayed. Click the **Use the Change Disk Mapping** button to map the correct volumes for recovery.

If the source and target volumes match, the recovery or cloning begins.

#### 6.11.1.2 Recovering Files

To start recovering a file or files:

1 Click the **Recover Files** button.

The Recover Files - Select Recovery screen appears.

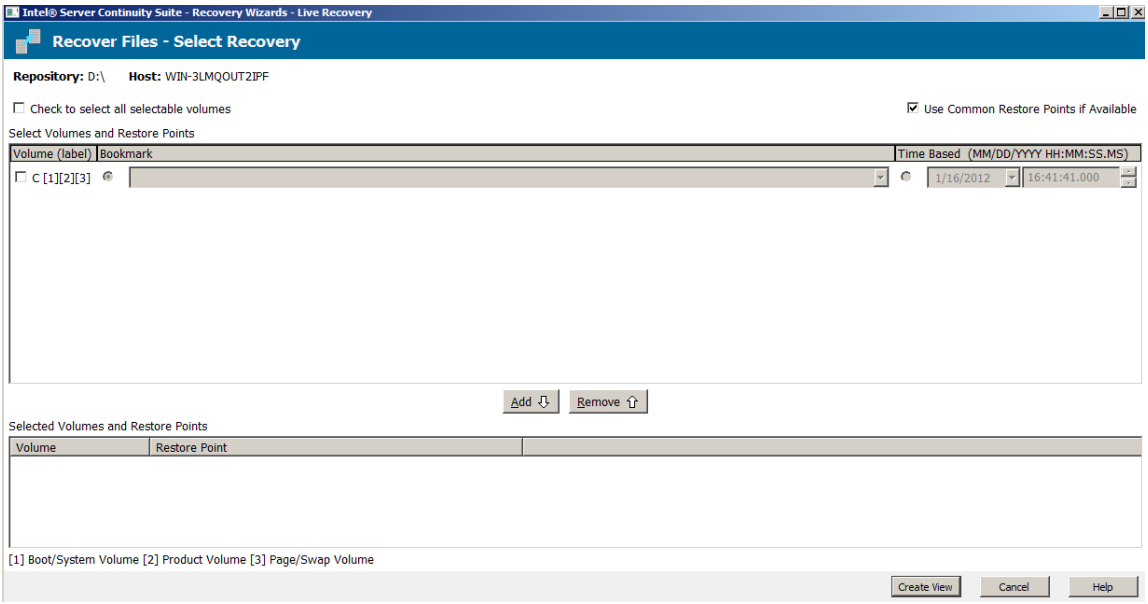


**Figure 6-12: Recover Files - Select Recovery screen**

2 Select the volume or volumes from which you want to recover files and click **Next**.

3 For each volume, select the consistency point (marked **Bookmark** in the interface) or the time from which you want to recover files and click **Add**. The consistency points available for each volume are listed in the **Bookmark** drop down menus. The selections are added to a list displayed in the interface.

**Note**: You can select multiple consistency points for the same volume. You can delete selected files or consistency points from the list by selecting the entry in the list and clicking the **Remove** button.

4 Click **Create View**.

5 In the screen that appears, click **OK**.

The Recover Files screen appears. It provides a snapshot of the files you selected.

6 Right click the consistency points from which you want to recover the files and copy the files to a desired location.

7 After you recover all the files, click **Done**.

### 6.11.2 Live Volume Rescue

Live volume rescue refers to recovering the boot volume of the machine containing the backup data. If the machine is unbootable, you can recover the boot volume using the rescue disk provided with Intel® SCS. This is similar to volume recovery as explained in the previous section, but is done by booting into the rescue disk.

**Note**: If the source or target volume is an iSCSI volume, a DHCP server must be configured. There is no option to enter a static IP address.

To boot into the rescue disk:

1 Insert the rescue disk, and boot the machine.

**Note:** Reboot the machine if it is already powered on. If boot from disk is not the first option in the boot menu, then go to the boot menu and select the option to boot from the rescue disk.

2 On booting into the disk, the rescue application appears on the screen.

This application is similar to the Intel® Recovery Wizard. Using this application, the boot volume can be recovered to a previous state. The previous state can be selected from a list of bookmarks or time stamps.

3 After selecting a bookmark or a time stamp, proceed to rescue the volume(s).

**Note:** When the rescue operation is complete, a message appears asking to reboot the machine. Remove all the disks, including the rescue disk, before you reboot the machine.

On restarting the machine, the state of the bootable volume will be the same as the bookmark or the time stamp selected.

# 7 Activity

The Activity module in Intel® Server Continuity Suite (Intel® SCS) provides an overview of events and actions for a selected period of time. You can access the Activity module by clicking Activity in the main menu on the left hand side. The Activity module displays data in the following tabs:

- Events
- Actions

## 7.1 Events

The Events tab displays events logged in the three modules and console.

When you click Activity in the main menu, the Events tab is displayed by default.


**Figure 7-1: Events page**

The dates are color coded based on the number of events.

View events reported for a month by clicking the previous ( ) and next ( ) buttons on the calendar.


**Figure 7-2: Number of Events on a Day**

Click a date in the calendar to view the number of events reported on that day. After you click a date, the Timeline Graph displays the number of events (as a bubble) reported in an interval of every two hours.

Point to the bubble corresponding to a timeslot to view the number of events reported during that time. The size of the bubble varies based on the number of events.

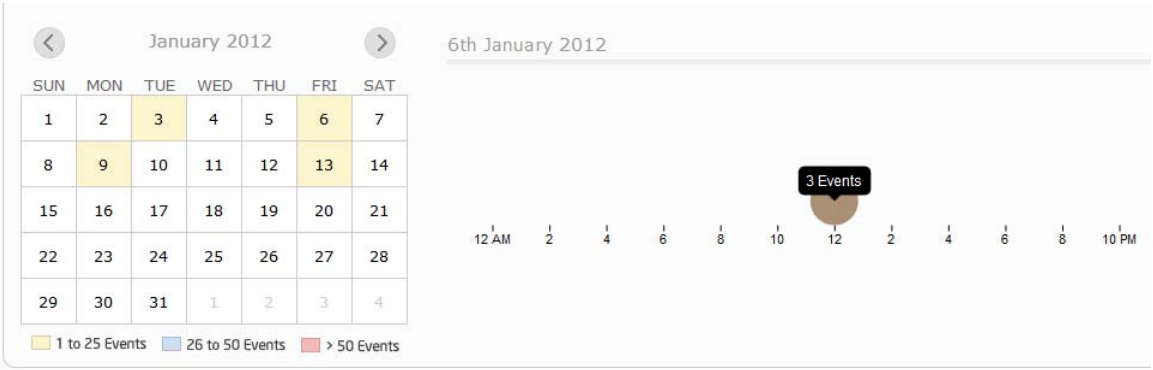


**Figure 7-3: Number of Events in a Timeslot**

Click the bubble to view the events' details such as:

- Time interval of the Timeline Graph
- Severity of the event (informational, warning, or critical)
- Description of the event
- Category (storage, hardware, data protection, or console)
- Date and time at which the event was created

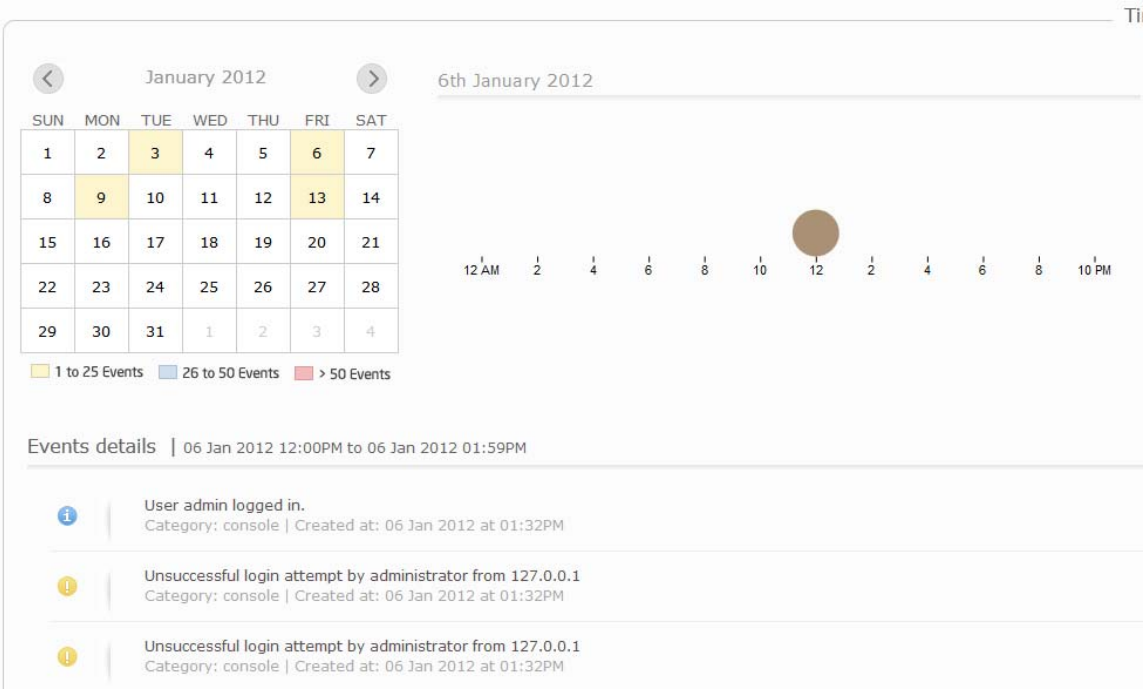


**Figure 7-4: Event's Details**

## 7.2 Actions

The **Actions** tab displays activities performed One Time and in Recurrence. One Time actions are those that are performed once, such as creating and initializing virtual disks in Storage Management. Recurrence actions are scheduled, such as creating consistency points or scheduling patrol read. One Time actions are displayed in a calendar view with a Timeline Graph. Recurrence actions are displayed only in a Timeline Graph. One Time actions are displayed by default when you click the Actions tab.

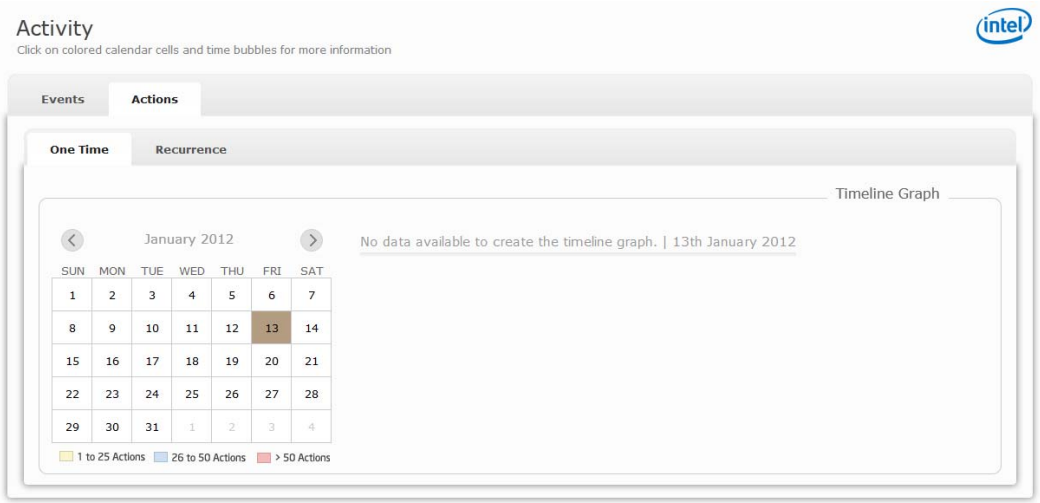


**Figure 7-5: Actions**

### 7.2.1 One Time Actions

The dates are color coded based on the number of actions.

View One Time actions reported for a month by clicking the previous ( ) and next ( ) buttons on the calendar. The calendar displays the number of actions performed each day. Point to a date to view the number of actions created.


**Figure 7-6: Number of One Time Actions on a Day**

Click a date in the calendar to view the number of actions reported on that day. After you click a date, the Timeline Graph displays the number of actions (as a bubble) reported in an interval of every two hours. The size of the bubble varies based on the number of actions.

Point to the bubble corresponding to a timeframe to view the number of actions reported during that time. The size of the bubble varies based on the number of actions.


**Figure 7-7: Number of One Time Actions in a Timeslot**

Click the bubble to view the action's details such as:

- Time interval of the Timeline Graph

- Status of the action (running, completed, or suspended)
- Description of the action
- Date and time at which the action was performed

### 7.2.2 Recurrence

The Recurrence tab displays actions scheduled in the main modules such as Storage Management and CDP, and alerting settings. Each recurrence displays the activity details including the time interval of occurrence, status, and next due date of the activity.

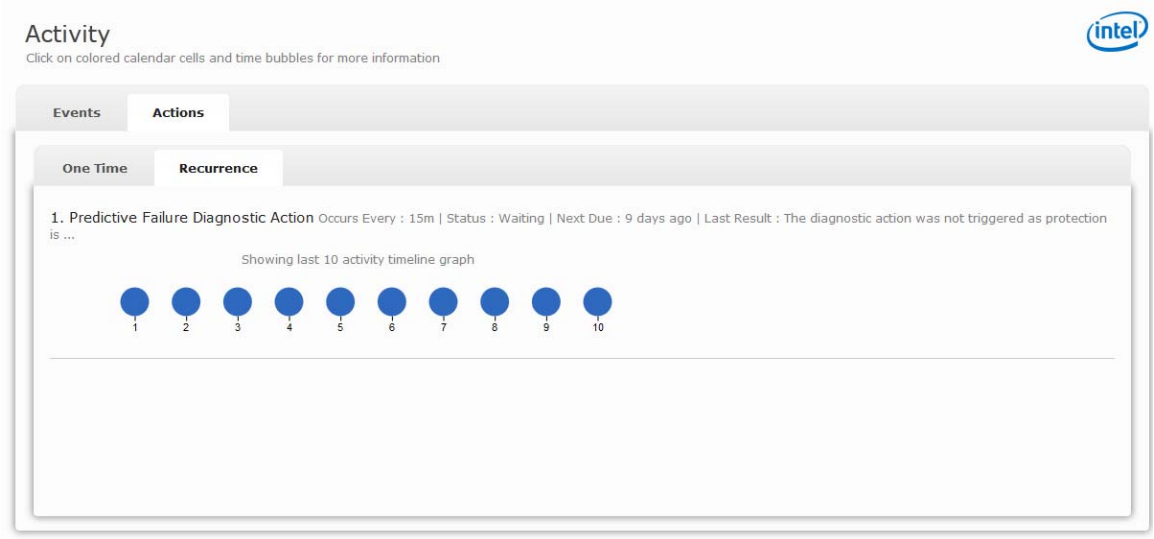


**Figure 7-8: Recurrence Actions**

Point to the bubble corresponding to each action to view the date and time at which the action will be performed.

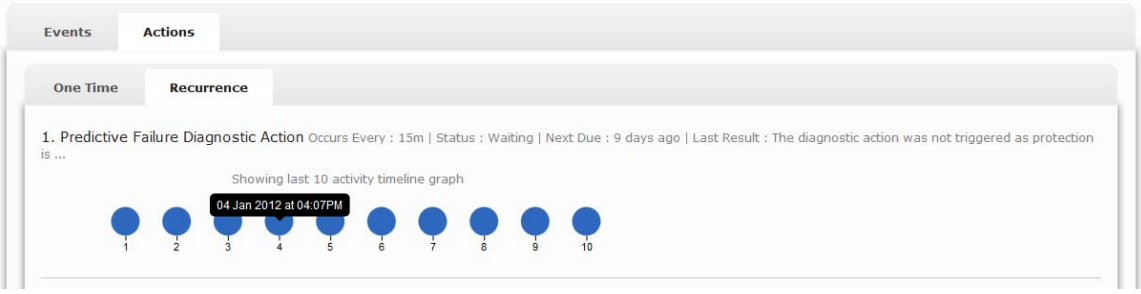


**Figure 7-9: Recurrence Actions Details**

# 8 Settings

The Settings feature available in the main menu refers to the application settings. Intel® Server Continuity Suite (Intel® SCS) provides features to:

- Automatically send event notifications and periodic alerts in email
- Set rules based on which emails are sent
- Clear cache, events, and actions

The settings screen also provides access to the license screen where you can upgrade the license key and support key.

The settings for email, alerts, and rules must be configured the first time Intel® SCS is started.

## 8.1 Configuring Email

Email Configuration provides options to add the administrator's email ID to which event notifications and periodic alerts are sent. The event notifications and periodic alerts are sent to the email address entered in the Email Configuration tab using the **SMTP Server Configuration**.


**Figure 8-1: Email Configuration**

To configure email configuration:

1 Enter the **SMTP Server Configuration** based on your email server settings.

2 Enter the email address to which emails must be sent to in the **To Email** text box.

3 Click **Save**.

The Email Configuration is saved.

4 Click **Send Test Mail**.

If SMTP configuration is correct, a message indicating that the test mail is sent successfully appears on the screen.

## 8.2 Alerting Settings

Alerting enables you to monitor the server remotely by receiving continuous updates in the form of periodic alerts from Intel® SCS.

### 8.2.1 Activating Alerts

The Configure Alerts settings allow you to switch the alert On or Off. Alert must be On to activate sending alerts.

To activate alerts:

1 After configuring the settings, select **Alert** as **On**.

2 Click **Save** to save the alert configurations.

A message indicating that the alert is scheduled successfully appears.

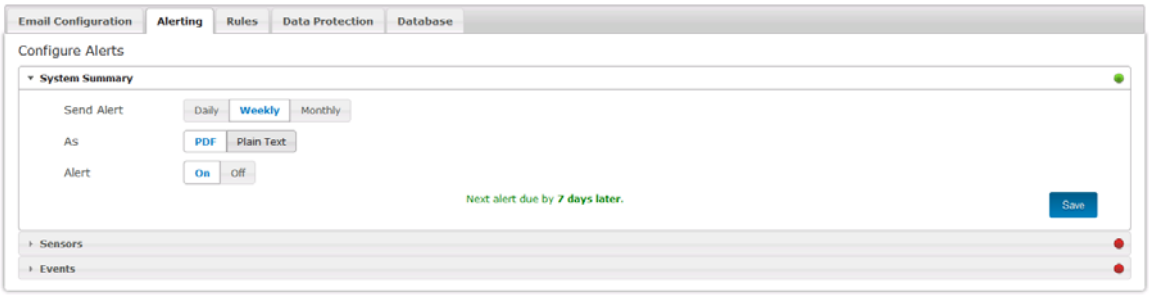


**Figure 8-2: Alert—On**

Once the alert is scheduled successfully, messages as shown in the table appear based on the Send Alert option.

**Table 8-1: Alert Messages**

| Send Alert Option | Message Description | Example |
|---|---|---|
| Daily | The number of hours due for sending the alert. | Next alert due by about 22 hours. |
| Weekly | The number of days due for | Next alert due by 7 days. |

| | | |
|---|---|---|
| | sending the alert. | |
| Monthly | The number of days due for sending the alert. | Next alert due by about 1 month. |

The activated alerts appear in the Activity > Actions > Recurrence tab. For more information, see Recurrence.

The Alerting tab provides options to send periodic alerts for:

- System Summary
- Sensors
- Events

### 8.2.2 System Summary

System Summary alerting settings allow you to:

- Send alerts daily, weekly, or monthly
- Send alerts as PDF or plain text
- Switch alerts On or Off
- Save system summary alerting settings

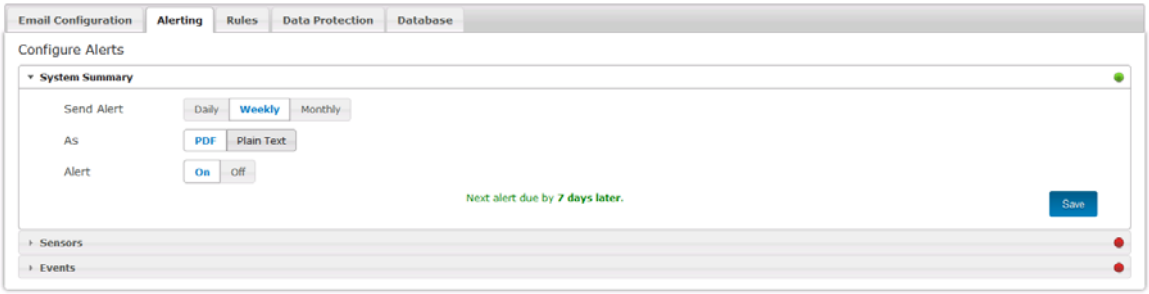


**Figure 8-3: System Summary Alerting Settings**

### 8.2.3 Sensors

Sensors alerting settings allow you to:

- Send alerts for Type—current, voltage, temperature, fans, or all

**Note**: You can choose many types at a time. If you choose all, you will receive alerts about memory, processor, hard drives, and power supply also.

- Send alerts with State—informational, warning, or critical

**Note**: If you choose informational, you will receive all the alerts. If you choose warning, you will receive warning and critical alerts. If you choose critical, you will receive only critical alerts.

- Send alerts daily, weekly, or monthly
- Send alerts as PDF or plain text
- Switch alerts On or Off
- Save sensors alerting settings

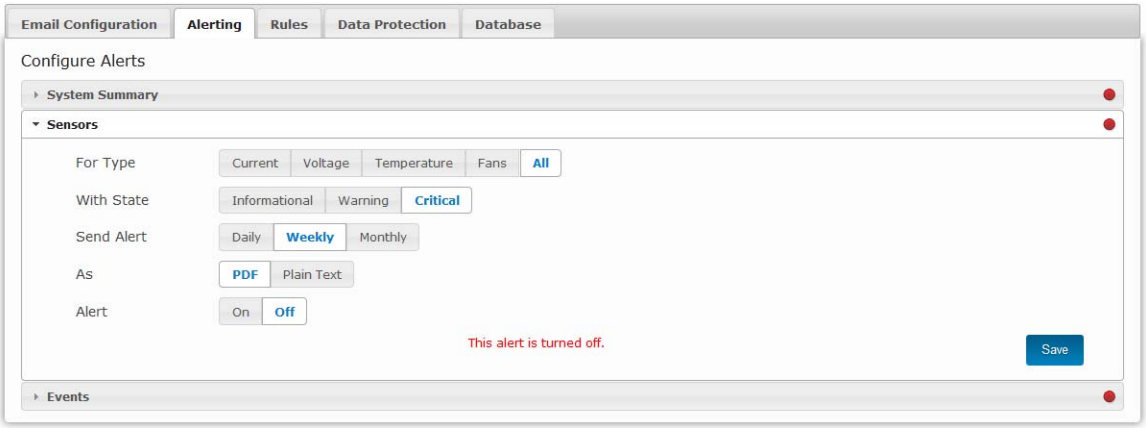


**Figure 8-4: Sensors Alerting Settings**

### 8.2.4 Events

Events alerting settings allow you to:

- Send alerts for Module—hardware, storage, data protection, or console

**Note**: You can choose many modules at a time.

- Send alerts with State—informational, warning, or critical
- Send alerts daily, weekly, or monthly
- Send alerts as PDF or plain text
- Switch alerts On or Off
- Save events alerting settings

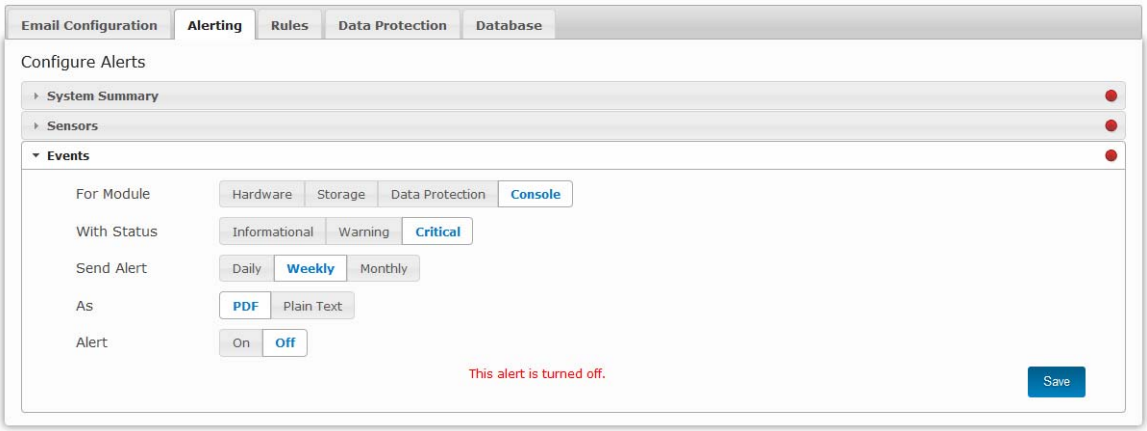


**Figure 8-5: Events Alerting Settings**

## 8.3 Configuring Rules

Rules are configured to send event notifications via email for warning or critical events. You must select the modules for which the event notifications must be sent.

The modules for which you can set the rules are:

- Hardware
- Storage
- Data Protection
- Console

Click on the module name to select or deselect it.

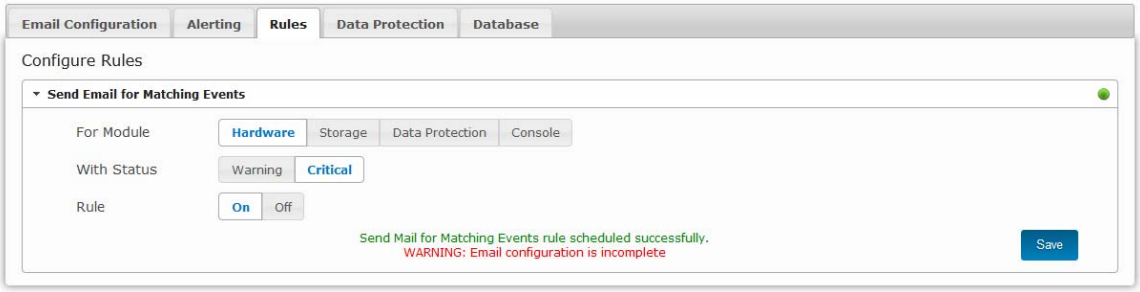


**Figure 8-6: Configuring Rules**

### 8.3.1 Activating Rules

The Configure Rules settings allow you to switch the rules On or Off.

To active rules:

1 After configuring the settings, select **Rule** as **On**.

2 Click **Save**, to save the rules configurations.

A message indicating that the rule is scheduled successfully appears.

Once the rule is scheduled successfully, a message that the rule is active appears.

## 8.4 Data Protection Settings

The Data Protection tab in Settings allows you to:

- Download data protection logs to troubleshoot issues
- Resynchronize protection to synchronize the data in volumes and repository
- Delete repository to change the repository volume

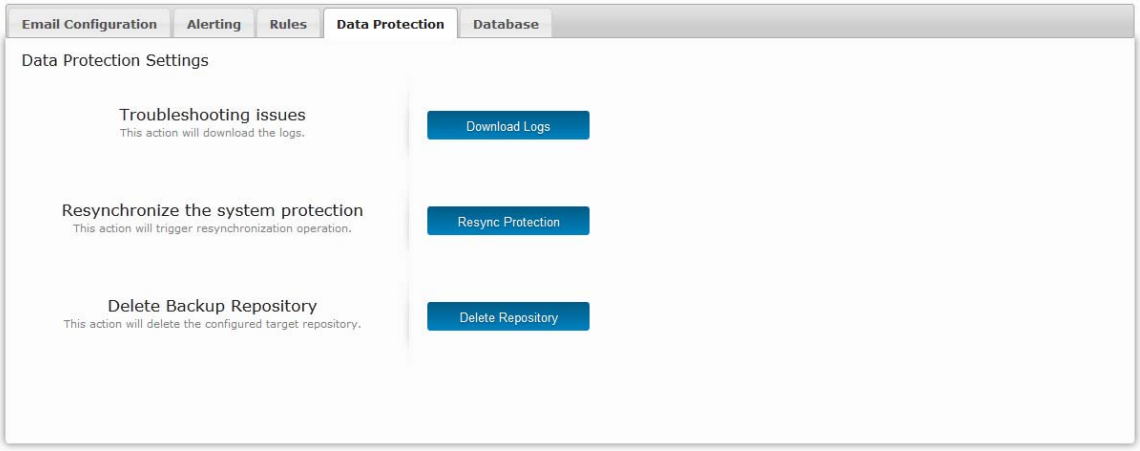


**Figure 8-7: Configuring Data Protection**

### 8.4.1 Download Logs

The Data Protection tab allows you to download the logs created in the Continuous Data Protection module to troubleshoot any issues.

To download and save the logs:

1 Select the **Data Protection** tab.

2 Click the **Download Logs** button.

3 Click **Download** in the screen that appears and save the log file to a location of your choice.

### 8.4.2 Resync Protection

If you resize the source volume, follow the steps below to resume protection.

**Note**: The steps are valid only for extended volume resize. Shrinking volume resize is not supported.

1 Stop the Backup Agent Service. To stop the Backup Agent, click **Start** > **Run** > **services.msc**.

2 In the Backup Agent Service wizard, find Intel® Backup Agent Service and stop that Service.

3 Click **Start** > **My Computer** and right click on **Source Volume Properties**. Note the volume capacity in bytes.

4 Get the respective target volpack. To get the target volpack, execute the command

<*INSTALL_PATH*>\cdp\cdpcli.exe --virtualvolume --op=list

The list of virtual volumes mounted in the system displays.

For example, if the install path is c:\Program Files (x86)\Intel\SCS\, you need to execute the command

c:\Program Files (x86)\Intel\SCS\cdp\cdpcli.exe --virtualvolume --op=list

The list of virtual volumes mounted in the system displays as given below:

- r:\381859e2-4bba-af48-a1cb3d911db4d3b1\f_virtualvolume
- r:\381859e2-4bba-af48-a1cb3d911db4d3b1\e_virtualvolume
- r:\381859e2-4bba-af48-a1cb3d911db4d3b1\c__srv_virtualvolume
- r:\381859e2-4bba-af48-a1cb3d911db4d3b1\c_virtualvolume

5 Resize the target Volpack such that it is either equal to or larger than the source volume by executing the command

cdpcli.exe --virtualvolume --op=resize --devicename=<*device name from the above command*> --size=<*size of modified volume in bytes*> --sizeinbytes

6 Navigate to the Intel® Server Continuity Suite – Data Protection install path and clear the agent cache by issuing the command

drvutil --stopfiltering <*drive letter or mount point*> -deletebitmap

7 Start the Intel® Backup Agent Service.

8 Resume the protected pair for which protection was paused due to volume resize.

9 Click the **Resync Protection** button.

10 Enter the string displayed in the screen in the box provided.

11 Click **Confirm**.

**Note:** Click **Cancel** to exit without resynchronizing.

### 8.4.3 Delete Repository

If you want to create a new repository, the Data Protection tab allows you to delete the backup repository.

**Note:** Ensure important data in the repository is retrieved before deleting the repository.

Select the **Data Protection** tab.

Click the **Delete Repository** button.

Enter the string displayed in the screen in the box provided.

Click **Confirm**.

**Note:** Click **Cancel** to exit without deleting the repository.

## 8.5 Clearing the Database

The database configuration allows you to clear cache, events, and actions stored in the system. This allows you to clear events and actions based on the module and a time period.

### 8.5.1 Clear Cache

The Database tab allows you to clear the console cache stored in the system running Intel® SCS. This action will clear the cache permanently from the system.

To clear cache:

1 Select **Clear Cache** tab from the **Database** tab.

2 Click the **Clear Cache** button.

The Database Action | Settings screen appears.

3 Enter the string displayed in the screen in the box provided.

4 Click **Confirm**.

All the information stored in cache is cleared.

If the string entered is invalid, Database Action | Settings—Invalid Input screen appears.

**Note:** Click **Cancel** to exit without clearing cache.

### 8.5.2 Clear Events

The Database tab allows you to clear Events based on the following classifications:

- Hardware, storage, data protection, console, or all
- 30 days, 60 days, 90 days, or all

To clear events:

1. Select **Clear Events** tab from the **Database** tab.
2. Click the **Clear Events** button.

   The Database Action | Settings screen appears.
3. Enter the string displayed in the screen in the box provided.
4. Click **Confirm**.

   All the events generated till then are cleared.

If the string entered is invalid, Database Action | Settings—Invalid Input screen appears.

**Note:** Click **Cancel** to exit without clearing events.

### 8.5.3 Clear Actions

The actions are displayed in the Activity module.

Actions can be cleared based on the following classifications:

- 30 days, 60 days, 90 days, or all

To clear actions:

1. Select **Clear Actions** tab, from the **Database** tab.
2. Click the **Clear Actions** button.

   The Database Action | Settings screen appears.
3. Enter the string displayed in the screen in the box provided.
4. Click **Confirm**.

   All the actions generated till then are cleared.

If the string entered is invalid, Database Action | Settings—Invalid Input screen appears.

**Note:** Click **Cancel** to exit without clearing actions.

# 9 Events and Actions

All events logged in the server are listed on the Events tab in Intel® Server Continuity Suite (Intel® SCS).

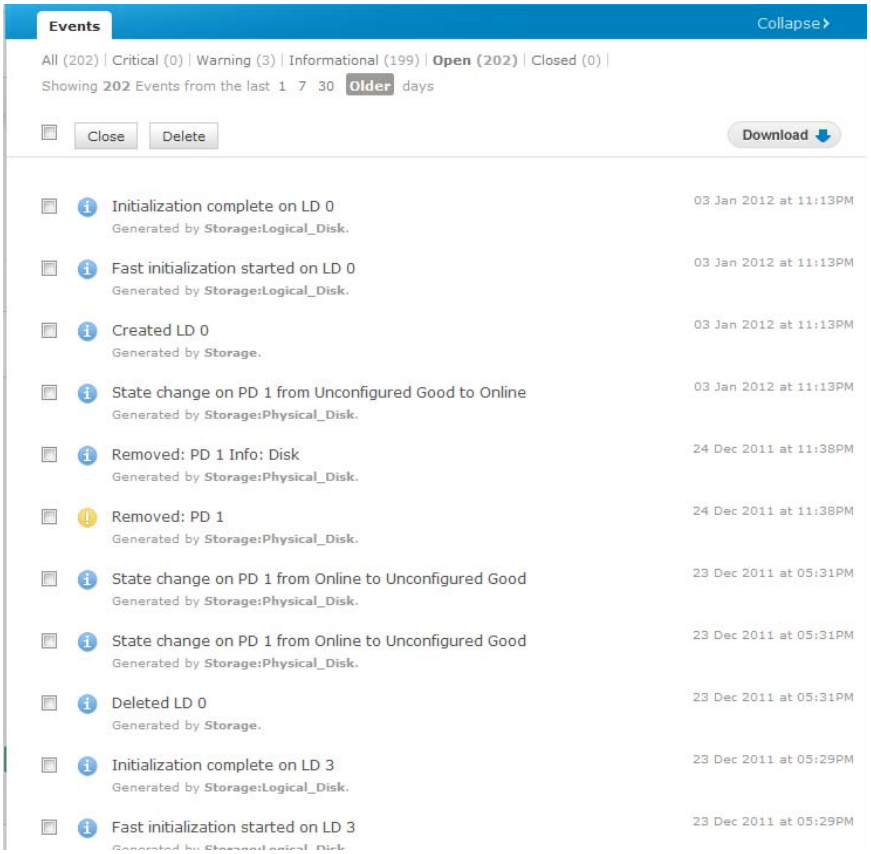


**Figure 9-1: Events Tab**

You can view events of the last 1 day, 7 days, 30 days, or older. Every page in the Events tab displays 15 events. Click Next, Previous, or the page number to view more events. Each event is displayed with the date and time of the event. Based on the state and health, events are classified as:

- Informational
- Warning
- Critical

Informational events are generated when an action is performed in a server with its components are in a healthy state. Warning events are generated when an action fails to execute or when the health of the server components change to a warning state. Critical events are generated when the components are in any of the states that result in critical health state.

### 9.1.1 Viewing Events

Events appear on the tab based on the following categories:

1. Severity
    - All
    - Critical
    - Warning
    - Informational
2. Status
    - Open
    - Closed

By default, the Events screen displays the most recent events in Open state. Click a category to view the list of those events.

You can perform the following operations on events:

- Close
- Delete

**Note:** Users have the option of closing an event to delete it from the log screen.

### 9.1.2 Closing Events

The Closing events option helps you move attended and resolved events, to the closed list.

To close events:

1 Select the events to close, in the Events screen.

2 Click **Close**.

The closed events appear in the closed list. You can delete these events.

### 9.1.3 Deleting Events

You can delete events from the events list.

To delete events:

1 In the Events screen, select the events to delete.

2 Click D**elete**.

The selected events are deleted.

### 9.1.4 Reporting Events

You can configure Intel® SCS to report events automatically using the options in the Alerting tab in the Settings menu:

- Sending as email—based on the severity and status settings, the most recent 250 events are sent in an email.
- Generating a report in PDF—based on the severity and status settings, the most recent 1500 events are provided in PDF format.

#### 9.1.4.1 Sending Events as Email

Intel® SCS provides settings to report events based on the state and severity.

1 In the **Events** tab, click the **Download** button.

2 In the window that appears, click **Send as Email**.

Based on the severity and status settings, the most recent 250 events are emailed to the Email ID configured in settings.

#### 9.1.4.2 Generating a Report in PDF

Using the Settings, users can configure Intel® SCS to send events as email to only one recipient. You can generate a PDF of events and send it to multiple recipients.

1 In the **Events** tab, click the **Download** button.

2 In the window that appears, click **Generate PDF**.

The **Save File** dialog appears.

3 Select the location to save the generated file, and click **Save**.

Based on the severity and status settings, the most recent 1500 events are provided in PDF format and saved in the selected location.

The Events icon on the Intel® title bar displays the total number of events. You can view the events by clicking the icon.

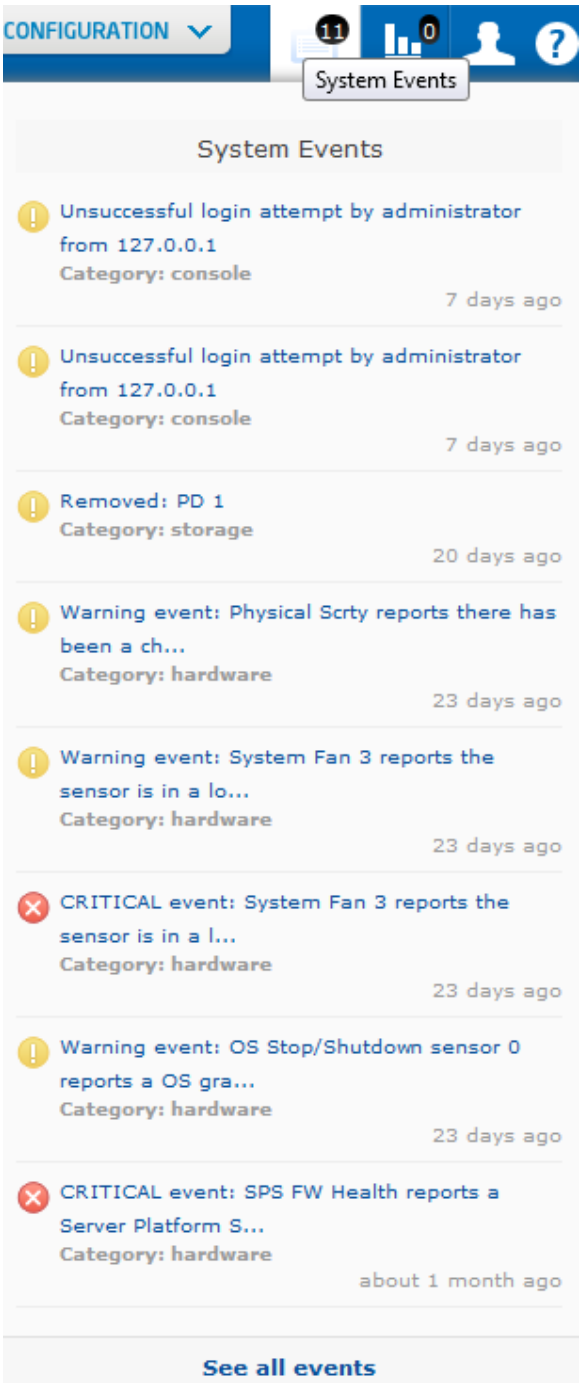


**Figure 9-2: Events List**

### 9.1.5 Viewing Actions

The actions performed in the console are listed in the actions list. The Actions icon on the Intel® title bar displays the total number of actions. You can view the actions by clicking the icon.

Actions appear in the following states:

- Running ( )—activities that are started and are executing appear in this state
- Suspended ( )—activities that are halted or aborted appear in this state
- Completed ( )—activities that are complete appear in this state

For more information on actions, see Actions.

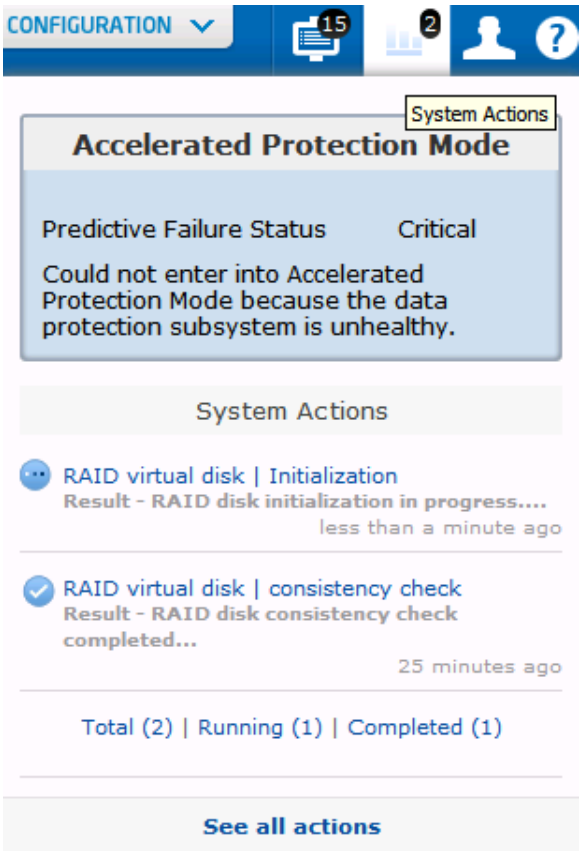


**Figure 9-3: Actions List**

# 10 User Management

Intel® Server Continuity Suite (Intel® SCS) provides tools to add users to access the console and manage users based on roles. The User Management module displays the list of users and allows you to:

- Update your user profile
- Add new users
- View and edit user profile
- Change user role
- Delete users

Click the icon to access User Management.

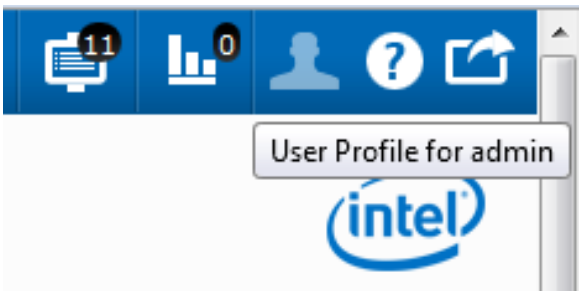


**Figure 10-1: User Management Icon**

## 10.1 Update Your Profile

You can update your profile in the application.

To update your profile:

1 In the **User Management** screen, click the **Your Profile** tab.

**Note**: The username cannot be changed.

2 Update the following details:

- E-mail
- First Name
- Last Name
- Password

3 Retype the password in **Password Again** box.

4 Update the **Role**.

5 Click Save Changes.

**Note:** Click Cancel if you want to exit without updating your profile.

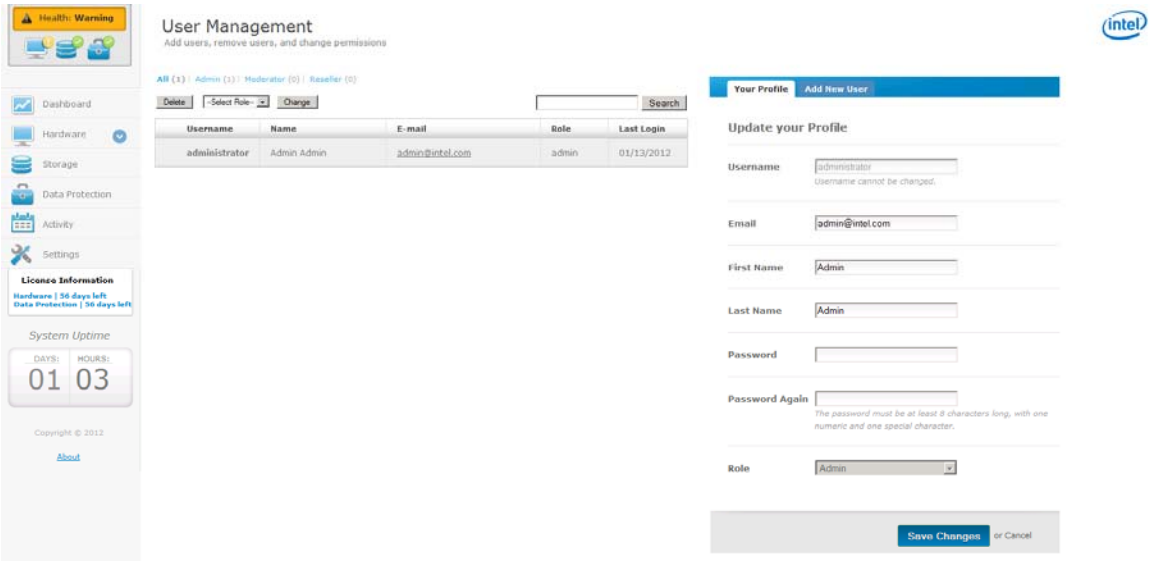


**Figure 10-2: User Management—Your Profile**

## 10.2 Adding New Users

You can add users with three roles:

- Admin—If you log in as an admin, you can perform all the actions in Intel® SCS.
- Moderator—If you log in as a moderator, you can perform only limited actions in Intel® SCS. A few actions that are not available for a moderator are shut down, restart, BMC configuration, clear SEL, delete the repository, delete events, delete actions, and delete RAID volumes.
- Reseller—If you log in as a reseller, you can perform only limited actions in Intel® SCS. A few actions that are not available for a reseller are shut down, restart, BMC configuration, clear SEL, delete the repository, delete events, delete actions, and delete RAID volumes.

To add a user:

1 In the **User Management** screen, click the **Add New User** tab.

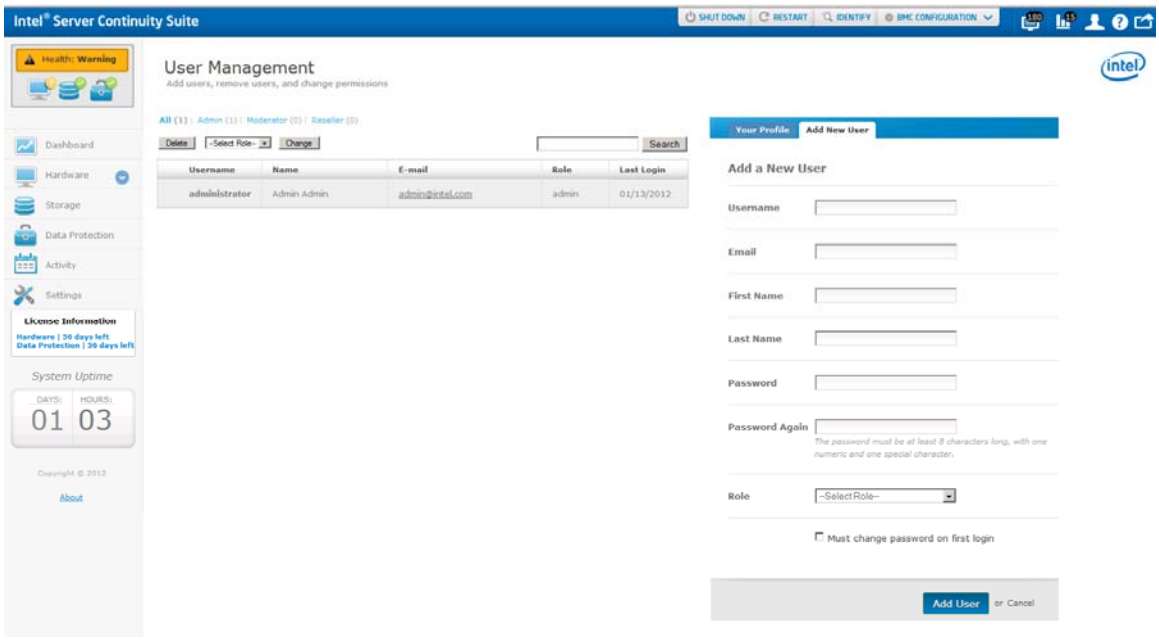


**Figure 10-3: User Management—Your Profile**

2 Enter the following details:

- Username
- E-mail
- First Name
- Last Name
- Password

**Note:** The password should be at least eight characters long and must contain one letter of the English alphabet, one numeric, and one special character.

3 Retype the password in **Password Again** box.

4 Select the **Role**.

5 Select **Must change password on first login** by clicking on the checkbox if you want the user to change the password on first login.

6 Click Add User.

The new user details appear in the users list.

**Note:** Click **Cancel** if you want to exit without adding a new user.

## 10.3 Viewing and Editing User Profile

You can view the user profile and edit the following details of existing users in the Edit Profile tab:

- E-mail
- First Name
- Last Name
- Password
- Role

**Note:** Username cannot be changed.

To edit a profile:

1 In the **User Management** screen, click the user name in the users list.

2 Edit the required parameters.

**Note:** If you change the password, retype the password in **Password Again** box.

3 Click Save Changes.

**Note:** Click **Cancel** if you want to exit without saving changes.

## 10.4 Changing User Role

You can change the role of a user added in the console using the Edit Profile tab or the users list if you log in as an administrator.

**Note**: You cannot change the role of the administrator that was created while installing the application.

To change a user role from the Edit Profile tab:

1 In the **User Management** screen, click on the user name to display the **Edit Profile** tab.

2 Click the **Select Role** drop-down menu.

3 Select the new role.

4 Click Save Changes.

**Note:** Click **Cancel** if you want to exit without saving changes.

To change a user role from users list:

1 In the **User Management** screen, select the user in the users list by clicking on the checkbox.

2 Click the **Select Role** drop-down menu.

3 Select the new role.

4 Click **Change**.

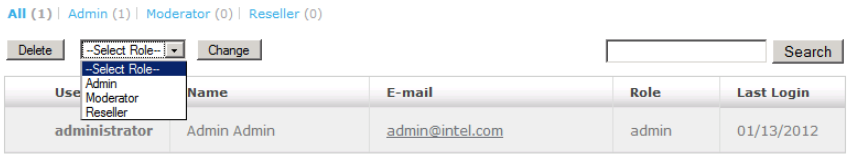


**Figure 10-4: Changing User Role—Users List**

## 10.5 Deleting Users

You can delete an existing user from the application if you log in as an administrator.

To delete a user:

1 In the **User Management** screen, select the user in the users list.

2 Click **Delete**.

The message: User(s) has been deleted appears.

3 Click **OK**.

The selected user is deleted from the users list.

# 11 Contacting Support

If you encounter an issue with your software, please follow the steps below to obtain support:

1. Connect to our support web page for 24x7 support and to get the latest technical support information on all Intel® Enterprise Servers, Storage Platforms, and Management Software. Information available at the support site includes:
   a. Latest BIOS, firmware, drivers, and utilities available through Intel® download center
   b. Product documentation, flash demos, installation guides, and quick start guides.
   c. A searchable knowledgebase of product information that you can access from any page in the support site
2. Utilize the community forums.
3. Chat live with a support person.
4. Contact an Intel® representative using one of the support phone numbers. Charges may apply.

Intel® now offers Channel Program members 24x7 technical phone support+ on Intel® server boards, server chassis, server RAID controller cards, and Intel® Server Management.

+ Requires Login to the Reseller Site to obtain the 24x7 number.

The latest user guide and related documentation are available at http://support.intel.com/support/motherboards/server/scs/.