Cisco Video Surveillance Storage System Administration Guide

Release 1.6.1
Revised: December 09, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24603-05

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Video Surveillance Storage System Administration Guide
©2012-2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Purpose

This document describes the operation and functions of the Management Console for Cisco Video Surveillance Storage System components.

Audience

This document is intended for Cisco Service Engineers and Cisco Video Surveillance Storage System Administrators.

Revision History

Table 1 Revision History

Date	Change Summary
February, 2012	Initial draft.

Table 1 Revision History (continued)

Date	Change Summary
April, 2013	• Added the "Integrating External Storage Volumes Into Cisco VSM" section for Release 7.0 and 7.0.1 and the Cisco Multiservices Platform (Cisco MSP) servers. • Added notes stating that "Only SATA disk drives are supported with the Cisco Video Surveillance Storage System. SAS, SSD and iSCSI are not supported."
December, 2013	Revised the "Integrating External Storage Volumes Into Cisco VSM" for release 7.2 and the Cisco Connected Safety and Security UCS Platform Series servers. Revised storage support notes to specify that "SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher."

Organization

Chapter	Description
Chapter 1, "Basic Setup"	Describes the features accessible from the QuickStart page.
Chapter 2, "Quick Start"	Describes a Product description, the Getting Started procedures, and the QuickStart Configuration Checklist to configure your system. Also includes i nstructions to integrate the external storage system in the Cisco Video Surveillance system.
Chapter 3, "Home Screen"	Describes the features accessible from the Home Screen page.
Chapter 4, "RAID Information"	Describes the features accessible from the RAID Information page.
Chapter 5, "System Information"	Describes the features accessible from the System Information page.
Chapter 6, "Configure RAID"	Describes the features accessible from the RAID Configuration page.
Chapter 7, "Volume Configuration"	Describes the features accessible from the Volume Configuration page.
Chapter 8, "Host Access Configuration"	Describes the features accessible from the Host Access Configuration page.
Chapter 9, "Power Settings"	Describes the features accessible from the Power Settings page.
Chapter 10, "System Administration"	Describes the features accessible from the System Administration page.
Chapter 11, "Network Configuration"	Describes the features accessible from the Network Configuration page.
Chapter 12, "Technical Support"	Explains how to contact Cisco Technical Support.
Appendix A, "RAID Levels"	Describes the RAID levels available on Cisco Video Surveillance Storage System components.
Appendix B, "AutoMAID"	Describes AutoMAID power saving technology.

Safety Precautions

This manual covers safety precautions for the Cisco Video Surveillance Storage System, including the CPS-SS-4RU and the CPS-SS-4RU-EX.

Cisco Video Surveillance Storage System products contain hazardous materials:

- Only Trained Operators may remove certain field-replaceable units (FRU's).
- Only trained Service Engineers are authorized to disassemble any other part of the unit, and only when the unit is powered off.

Caution **Static Charge Precautions**
Computer components and disk s are sensitive to static charge. Take precautions to earth any electrostatic charge from your person before and while handling components with your hands or any tools. Please use the anti-static wrist-strap shipped with each Cisco Video Surveillance Storage System product.

Caution **Lifting Precautions**
Ensure correct lifting methods are used when handling Cisco Video Surveillance Storage System products. Special care should be taken when removing Cisco Video Surveillance Storage System products from their packaging and positioning them into their operational location.

Caution **Securing Rack Mounts**
Ensure the mounting rack is stable with wall anchors and/or stabilizing legs, and that the floor supporting the rack has sufficient strength for the overall weight loading.

Caution **Rack-mounting Cisco Video Surveillance Storage System Components**
When installing Cisco Video Surveillance Storage System products as rack-mounted components, ensure that all Cisco-supplied mounting fixtures are secure. **DO NOT** mount any unit exclusively by the front ears. All bolts and screws should be fully tightened. Failure to comply with this may result in a Cisco Video Surveillance Storage System unit not being fully supported in the rack and could lead to the product dropping out of the rack causing personal injury or falling onto other rack components.

Warning **Cisco Video Surveillance Storage System products contain hazardous materials. Only a Trained Operator may remove certain field-replaceable units (FRU's). Only trained Service Engineers are authorized to disassemble any other part of the unit, and only when the unit is powered off.**

Warning **There are multiple power connections. Remove all power leads completely to isolate the power. Always use the IEC power cords supplied with Cisco Video Surveillance Storage System products.**

Warning **THERE IS RISK OF EXPLOSION IF BATTERY IS REPLACED WITH INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS PRINTED ON THE BATTERY, OR IN COMPLIANCE WITH LOCAL REGULATIONS.**

Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

Related Documentation

Use one of the following methods to access the Cisco Video Surveillance (Cisco VSM) documentation:

- Refer to the following documents for instructions to install and administer the Cisco Video Surveillance Storage System (CPS-SS-4RU and CPS-SS-4RU-EX).
  - Cisco Video Surveillance Storage System (main documentation page)
  - Data Sheet
  - Installation Guide
  - Administration Guide (this guide)
- Go to the Cisco Video Surveillance documentation web site.
- See the Cisco Video Surveillance 7 Documentation Roadmap for descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Basic Setup

This guide is designed to help you get your Cisco Video Surveillance Storage System components up and running in a short amount of time. It provides basic setup instructions and complete system configuration details. It does not cover the physical features or rack installation instructions for the storage system. For that information, see the *Cisco Video Surveillance Storage System Hardware Installation Guide*.

This guide describes the Management Console (GUI) and its features and functions used to access and configure Cisco Video Surveillance Storage System components from a web-based interface.

All Cisco Video Surveillance Storage System components have a common operating system and nearly identical Management Consoles. Therefore, this guide is appropriate for all Cisco Video Surveillance Storage System components.

This guide covers all of the features that can be accessed through the Management Console. However, because Cisco Video Surveillance Storage System components are shipped preconfigured, only the basic setup procedures in this chapter are needed for most installations.

Basic setup consists of the following procedures:

- Initial Network Address Setup
- Set Up the System
- Set Date and Time

Note These instructions assume that you are setting up one storage unit or one storage unit/expansion unit pair. If you are setting up more than one, you must perform these procedures for each system.

Initial Network Address Setup

Before you can configure your Cisco Video Surveillance Storage System component through the Management Console, you must assign a unique IP address to it's management port (**MGMT** on CPS-SS-4RU units) and enter the proper gateway and DNS settings.

Configure the Cisco Video Surveillance Storage System Component IP Address

There are two methods to set the IP address of you Cisco Video Surveillance Storage System unit. The first method is using the Web GUI of these storage systems. The second method is to use the Serial Port interface of these systems. The Web GUI is the preferred method.

Add a Route to Access the Desired IP Address

Adding a route doesn't change the IP address of the unit; it simply maps a path to the unit's existing IP address. This method requires your workstation to be directly connected to the same Ethernet network that the unit's management port (**Net 0** or **MGMT**) is connected to.

To add a route to access the IP address of the unit's RAID Controllers, you must have access to the command line interface or a terminal window.

Note The IP addresses 10.11.12.13 and 10.11.12.14 are the system defaults.

Step 1 At the command prompt, enter the information according to your OS:

- Windows: `route add 10.11.12.13 mask 255.255.255.255 <workstationIPaddress>`
- Linux: `/sbin/route add 10.11.12.13/32 gw <workstationIPaddress>`
- Solaris: `route add 10.11.12.13 mask 255.255.255.255 <workstationIPaddress>`

where <*workstationIPaddress*> is the IP address of the workstation you are using.

Step 2 To add a path to the second controller, repeat Step 1, but replace the first IP address with `10.11.12.14`.

Step 3 Open a Web browser. and enter the IP address **10.11.12.13** or **10.11.12.14** (if a second RAID controller is also present). You can access the Web GUI interface of the system with either of these two IP addresses. The Home page of the system should be displayed with this access.

Step 4 Click the **Configure Network** tab on the left hand side of the Home page.

Step 5 In the Configure Network page, you can set a Static IP address and subnet mask, Gateway IP address, and DNS IP address.

Step 6 Click **Save and Apply Changes**.

Use the Serial Port to Change the IP Address

To use the serial port on your Cisco Video Surveillance Storage System component to configure the IP address, you must directly connect your computer to the unit using the supplied Mini-DIN cable. You must also have a terminal emulation program installed on the computer.

Step 1 Connect the serial cable to your computer's serial (or COM) port.

Step 2 Connect the other end of the serial cable to the Cisco unit's serial port.

Step 3 Open the terminal emulation program and set up a new connection. It should be 115,200 bits per second, 8 data bits, 1 stop bit, no parity bits, and no flow control.

Step 4 Activate the serial connection to the unit.

The system management console is displayed.

Step 5 Using the arrow buttons on your keyboard, navigate to **Configure network** and press Enter.

The Network Menu is displayed.

Step 6 Navigate to **Set static IP address** and press Enter.

Step 7 In the dialog box, enter the IP address and press Enter.

The new IP address is saved.

Step 8 Navigate to **Apply new settings** and press Enter.

Accept the EULA

Step 1 Launch a web browser (Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, etc.).

Step 2 In the browser's address field, enter the IP address of the unit.

Step 3 Press **Enter** or click the browser's **Go** button.

The login screen for the unit is displayed.

Note The login screen varies depending on the type of unit you are connected to. However, the **Click Here to Login** button is always displayed.

Step 4 Click the **Click Here to Login** button to log in to the unit.

The Cisco End-User Software License Agreement screen is displayed.

Step 5 Read the EULA, check the box at the end to indicate your agreement, then click the **I Agree** button.

A message is displayed, indicating that you have agreed to the terms of the EULA.

Note In order to access the full functionality of the unit, you *must* agree to the terms of the EULA.

Note After you have agreed to the terms of the EULA, the Cisco End-User Software License Agreement screen will not be displayed again unless you select **Tech Support > EULA** (see End-User License Agreement, page 12-1).

Set Up the System

Once you accept the EULA, the Management Console displays the Quick Start Configuration Checklist, which guides you through the process of getting your system set up. The items on the Quick Start Configuration Checklist are:

- Security
- System Name
- Network Settings
- Array Configuration
- Volume Configuration and Access

Each item in the list displays its status on the Quick Start Configuration Checklist. If an item has a green check mark next to it, that item has been completed with a recommended setting. If an item has a red exclamation point next to it, that item has either not been completed or has an unrecommended setting. The Quick Start Configuration Checklist is only displayed automatically the first time you log in to a system, though it can always be accessed by going to **Quick Start > Check List**.

Security

To protect the integrity of the unit, it is strongly recommended that you at least create a password for the ADMIN account. This prevents unauthorized personnel from making changes to the unit's configuration.

To change security settings, click the **Change Security Settings** button. This takes you to the Password Configuration page.

Step 1 Next to **Change "ADMIN" login password requirement to**, select **Required**.

Step 2 Enter the password into the **New Password** and **Confirm Password** fields. Passwords should be eight characters or longer and can contain both letters and numbers, but not special characters or punctuation.

Step 3 Click **Set ADMIN Password**.

A message is displayed, informing you that the password has been set.

Step 4 Select **Quick Start > Check List** to return to the Quick Start Configuration Checklist.

Passwords take effect immediately. The next time you try to access a configuration page, the Management Console will ask you to enter the user name and password to gain access. Both fields are case-sensitive, and user names must be entered in all capitals ("ADMIN" or "USER").

For more information about the Password Configuration page, see Security Settings, page 11-4.

System Name

Although the system comes preconfigured with a name, it is recommended that you change it to a name more suitable to your environment.

Step 1 In the **RAID system name** field, type the name. You are limited to a maximum of 63 characters.

Step 2 Click **Set System Name**.

A message is displayed, letting you know that the setting has been changed.

Step 3 Click the **Back** button to return to the Quick Start Configuration Checklist.

Network Settings

It is recommended that you confirm your network settings to make sure that they will work with your local area network (LAN) setup. To do so, click the **Change Network Settings** button. This takes you to the Configure Network Settings page.

Note These instructions are for configuring the system management port only.

Step 1 Make sure that the following settings for the **Management** port (for CPS-SS-4RU units) are appropriate for your network:

- **Port Settings**: For most networks, the default setting of **Auto Speed, Auto Duplex** is recommended. However, if your LAN switch doesn't support auto-negotiation, you can "force" one or both settings. The options are:

  Auto Speed, Auto Duplex
  Auto Speed, Fixed Full Duplex
  Auto Speed, Fixed Half Duplex
  Fixed to 100Mbit Full Duplex
  Fixed to 100Mbit Half Duplex
  Fixed to 10Mbit Full Duplex
  Fixed to 10Mbit Half Duplex

- **Assign IP Address**: You can choose whether to **Use DHCP** (Dynamic Host Configuration Protocol) or **Use Static IP**.

  If you select **Use DHCP**, then no other configuration is needed.

  Note NOTE: In order to use DHCP, your network must be configured for DHCP. If it is not, you *must* use a static IP address.

  If you select **Use Static IP**, then you must fill in the **Static IP Address** and **Subnet Mask**. If you wish to use a time server (see Configure Time and Date, page 11-3), you may also wish to fill in values for **Gateway**, **Primary DNS**, and **Secondary DNS**.

Step 2 Repeat Step 1 for the second controller.

Step 3 After making changes, do one of the following:

- Click **Save Configuration**. The new network settings will take effect after the next unit restart.
- Click **Save & Apply Changes**. The new network settings will take effect immediately.

Step 4 Select **Quick Start > Check List** to return to the Quick Start Configuration Checklist.

For more information about configuring network settings, see Configure Network Settings, page 11-1.

Array Configuration

RAID arrays must be set up before volumes (where data is stored) can be assigned to them. To set up RAID arrays, click the **Change Array Configuration** button. This takes you to the Basic Quick Start page.

If you want control over more parameters, click the **Expert** tab to be taken to the Expert Quick Start page (see Expert Quick Start Array Configuration, page 1-7).

Note For complete control over RAID configuration, volume configuration, logical unit number (LUN) mapping, and host access, see Create a New RAID Array, page 6-1, Create a Logical Volume, page 7-1, Map Logical Volumes, page 7-4, and Host Access Configuration, page 8-1.

Basic Quick Start Array Configuration

Arrays are limited to the disks physically contained in a single Cisco Video Surveillance Storage System component.

Note If the system you are setting up is a storage unit/expansion unit pair, you are first asked to select the unit that you wish to configure. Select the unit you wish to configure, then click **Next**. When you are finished, you can configure the second enclosure by repeating this procedure.

The Basic Quick Start configuration page is displayed.

Note Only SATA disk drives can be used in the RAID array. SAS and SSD are not supported. If your Cisco Video Surveillance Storage System component contains a mixture of disk drive types, the Basic Quick Start configuration page will have two or three Quick Start Options sections, one for each drive type. Choose only the SATA option.

Step 1 Using the drop-down lists, set the following parameters:

- **Number of arrays**: Choose the number of RAID sets that you wish to create. The maximum number depends on the number of disks detected in the unit.
- **Select RAID level**: Choose the RAID level that all RAID sets will be configured for. You can choose from the following:

  RAID 0 (striped)
  RAID 1 (mirrored)
  RAID 4 (parity)
  RAID 5 (rotating parity)
  RAID 6 (rotating dual parity)

  Note For more information on RAID levels, see Appendix A, "RAID Levels".

- **Number of pool spares**: Choose the number of spare disks that will be available to use as backups in case a RAID disk fails. The maximum number of pool spares depends on the number of disks detected in the unit.
- **Number of volumes per array**: This setting controls whether or not each RAID array will be further divided into two or more smaller volumes. The default setting is **1**. The number of volumes per array can be anywhere from **1** to **10**.
- **Limit volume size to less than 2TB**: This option is unchecked by default. If your hosts do not support volumes of more than 2TB in size, check this option.

Step 2 Click **Next**.

The New Configuration Preview page is displayed.

Step 3 Ensure that the settings for **Arrays**, **Volumes**, **Pool Spares**, and **Volume Access** are correct.

Step 4 If all settings are acceptable, select the confirmation check box, then click the **Quickstart** button.

Caution If any arrays or volumes have already been configured on the unit, the Management Console displays a warning dialog. If you wish to continue, click the check box and select **Confirm Quickstart Configure**. If you do not wish to continue, click **CANCEL Quickstart**.

Note Although your volumes are available immediately, Quickstart continues to run in the background. The Quickstart operation may take as much as several hours to complete, depending on the size and number of the disk drives in the unit. You can check the progress of the operation by going to **RAID Information > Progress**.

Step 5 Select **Quick Start > Check List** to return to the Quick Start Configuration Checklist.

Step 6 Proceed to Volume Configuration and Access, page 1-9.

Expert Quick Start Array Configuration

Arrays are limited to the disks physically contained in a single Cisco Video Surveillance Storage System component.

Note If the system you are setting up is a storage unit/expansion unit pair, you are first asked to select the unit that you wish to configure. Select the unit you wish to configure, then click **Next**. When you are finished, you can configure the second enclosure by repeating this procedure.

The Expert Quick Start configuration page is displayed.

Note Only SATA disk drives can be used in the RAID array. SAS and SSD are not supported. If your Cisco Video Surveillance Storage System component contains a mixture of disk drive types, the Basic Quick Start configuration page will have two or three Quick Start Options sections, one for each drive type. Choose only the SATA option.

Step 1 Using the drop-down lists, set the following parameters:

- **Number of arrays**: Choose the number of RAID sets that you wish to create. The maximum number depends on the number of disks detected in the unit.
- **Select RAID level**: Choose the RAID level that all RAID sets will be configured for. You can choose from the following:

  RAID 0 (striped)
  RAID 1 (mirrored)
  RAID 4 (parity)
  RAID 5 (rotating parity)
  RAID 6 (rotating dual parity)

  Note For more information on RAID levels, see Appendix A, “RAID Levels”.

- **Number of pool spares**: Choose the number of spare disks that will be available to use as backups in case a RAID disk fails. The maximum number of pool spares depends on the number of disks detected in the unit.
- **Number of volumes per array**: This setting controls whether or not each RAID array will be further divided into two or more smaller volumes. The default setting is **1**. The number of volumes per array can be anywhere from **1** to **10**.
- **Limit volume size to less than 2TB**: This option is unchecked by default. If your hosts do not support volumes of more than 2TB in size, check this option.

Step 2 Using the drop-down lists, set the following parameters under Advanced Options:

- **Select stripe size**: The default stripe size is **128Kbytes**. You can choose to use smaller stripes by selecting **64Kbytes**, **32Kbytes**, or **16Kbytes**.
- **Select host connection type**: By default, this setting is set to **Fibre/SAS/10Ge iSCSI (multi-path)**, which maps all logical unit numbers (LUNs) to all available Fibre Channel/SAS-to-Host/10GbE iSCSI ports. If you wish to change the mapping, select one of the following:

  Note SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher.

  None (leave unmapped): The LUNs will not be associated with any ports on the unit and will not be available to the host. You can later manually assign each LUN to one or more ports using the procedure under Volume Configuration and Access, page 1-9 or **Configure Volumes > Map Volume** (see Map Logical Volumes, page 7-4).

  Fibre/SAS/10Ge iSCSI (non-redundant): Assigns each LUN to a single available Fibre Channel port.

  Fibre/SAS/10Ge iSCSI (multi-path): Assigns LUNs to all available Fibre Channel/SAS/10Gb iSCSI ports (requires multipathing software).

  iSCSI (non-redundant): Not supported.

  iSCSI (multi-path): Not supported.
- **Select default host access**: This setting defaults to **Read/Write**. This will allow all attached hosts to access all volumes on this unit.
- **Online Create**: When this box is checked, volumes on this unit will be available immediately, with RAID creation continuing in the background. This does, however, slow down the RAID creation process. You can speed up the creation process by unchecking this box, in which case volumes will be unavailable until RAID creation is complete.
- Leave free space on each array for future volumes/expansion: By default, the volumes will take up all of the space in the RAID arrays. This setting lets you keep a percentage of the RAID array space free for additional volumes or expansion of current volumes. Select **0%**, **10%**, **25%**, **50%**, or **75%**.

Step 3 Click **Next**.

The New Configuration Preview page is displayed.

Step 4 Ensure that the settings for **Arrays**, **Volumes**, **Pool Spares**, and **Volume Access** are correct.

Step 5 If all settings are acceptable, select **Check this checkbox to confirm**, then click the **Quickstart** button.

Caution If any arrays or volumes have already been configured on the unit, the Management Console displays a warning dialog. If you wish to continue, click the check box and select **Confirm Quickstart Configure**. If you do not wish to continue, click **CANCEL Quickstart**.

Note The Quickstart operation may take as much as several hours to complete, depending on the size and number of the disk drives in the unit. You can check the progress of the operation by going to **RAID Information > Progress**.

Step 6 Select **Quick Start > Check List** to return to the Quick Start Configuration Checklist.

Step 7 Proceed to Volume Configuration and Access, page 1-9.

Volume Configuration and Access

Although default volume and host access configuration is performed during Basic or Expert Quick Start, you may wish to change settings for individual volumes. To do so, click the **Change Volume Mapping** button. This takes you to the Map Logical Volumes page.

Find the volume that you wish to change, then click its **Next** button in the far right column.

- You can change the volume's LUN mapping by selecting a new LUN in the drop-down list.
- You can chance the volume's **Default Access** privileges by selecting the button under **Deny** (hosts cannot access this volume unless specifically configured to do so), **Read** (hosts are able to read, but not alter, this volume unless specifically configured to do so), or **R/W** (hosts have full read and write privileges to this volume).

  Note NOTE: To ensure integrity of data, it is recommended that you change this setting to **Deny**.

- You can change the **Group Default** access privileges by checking the **Use Default** check box (host groups use the **Default Access** setting) or by selecting the button under **Deny** (host groups cannot access this volume unless specifically configured to do so), **Read** (host groups are able to read, but not alter, this volume unless specifically configured to do so), or **R/W** (host groups have full read and write privileges to this volume).
- You can change the access privileges for host groups and individual hosts by checking the **Use Default** check box (host uses the Default Access setting; host group uses the Group Default setting) or by selecting the buttons under **Deny** (host or host group cannot access this volume), **Read** (host or host group is able to read, but not alter, this volume), or **R/W** (host or host group has full read and write privileges to this volume).

After making any changes, click the **Apply Changes** button. A message is displayed, informing you that changes to the volume have been made.

For more information about volumes, see Chapter 7, "Volume Configuration". For more information about host access, see Chapter 8, "Host Access Configuration".

When the Quick Start Checklist is Complete

When you have finished configuring the settings listed on the Quick Start Configuration Check List, do the following:

Step 1 Scroll to the bottom of the list.

Step 2 Uncheck the **Show the configuration checklist on home page** check box.

Step 3 Click **Close Checklist**. You are taken to the Home page (see Chapter 3, "Home Screen").

Set Date and Time

It is important to set the date and time so that events in the event log (see Event Log, page 5-7) and SNMP traps (see SNMP/SYSLOG Settings, page 11-2) show the correct time stamp.

- In the Management Console, select **Configure Network > Date & Time**. The Configure Time and Date page is displayed.

There are two ways to set the unit's time and date: manually and automatically.

To Set the Time and Date Manually

Step 1 Enter the time in the **Time entered in 'hh:mm:ss' format** field.

Note The time entered in the **Time entered in 'hh:mm:ss' format** field will be set when the **Save Settings** button is clicked. Therefore, it is suggested that you enter the time rounded to the next five minute mark, then click **Save Settings** when the entered time is reached.

Step 2 Enter the date using the **Date** drop-down lists.

Step 3 Select the **Timezone relative to GMT (GMT offset)** using the drop-down list.

Step 4 Click **Save Settings**.

To Set the Time and Date Automatically

Note For automatic time setting to work, you may have to configure the Gateway setting for your network. See Configure Network Settings, page 11-1 for more information.

Step 1 Select the **Timezone relative to GMT (GMT offset)** using the drop-down list.

Step 2 Next to **Time server IP address to use for auto time and date configure**, do one of the following:

- Select **Use IP address from list** and select a time server IP address from the drop-down list.
- Select **Use entered IP address** and enter the IP address of a known time server into the text box.

Step 3 Next to **Time server protocol**, select either **Daytime** or **SNTP**.

Step 4 If you entered a time server IP address in Step 2 and selected **Daytime** in Step 3, select the **Time server time and date format** using the drop-down list.

Note If you do not know the format of the time server data, click the **Retrieve Time Server Data** button. The data is retrieved and displayed next to **Data retrieved from contacting the daytime server**. Use this data to choose the proper format in the **Time server time and date format** dropdown list.

Step 5 If you wish the unit to contact the time server every twenty-four hours to update the time and date, select the check box next to **Set system time and date by the time server every 24 hours**.

Step 6 Click **Save Settings**.

Step 7 If you wish to update the time immediately, click the **Contact Time Server To Auto Configure Time And Date** button. The time and date are updated immediately.

CHAPTER 2

Quick Start

When you click the **Quick Start** button in the navigation pane, you are taken to the Basic Configure RAID System page. The navigation bar across the top contains links to this section's subpages.

- **Basic** links to Basic Quick Start
- **Expert** links to Expert Quick Start
- **Check List** links to Check List

This chapter also contains the Integrating External Storage Volumes Into Cisco VSM section that describes how to integrate the Cisco Video Surveillance Storage Systems (CPS-SS-4RU and CPS-SS-4RU-EX) into a Cisco VSM Release 7.2 and higher deployment using an integration script.

Basic Quick Start

Clicking **Quick Start** takes you to the Basic Configure RAID System page, which lets you quickly and easily configure RAID arrays and volumes for your system. This is an excellent tool for getting started with a new storage system (see Set Up the System, page 1-3).

Caution If arrays or volumes have already been configured on the unit, this tool will erase all existing data. It is recommended that this tool ONLY be used when first setting up the unit.

Arrays are limited to the disks physically contained in a single Cisco Video Surveillance Storage System component.

Note If the system you are setting up is a storage unit/expansion unit pair, you are first asked to select the unit that you wish to configure. Select the unit you wish to configure, then click **Next**. When you are finished, you can configure the second enclosure by repeating this procedure.

The Basic Quick Start configuration page is displayed.

Note Only SATA disk drives can be used in the RAID array. SAS and SSD are not supported. If your Cisco Video Surveillance Storage System component contains a mixture of disk drive types, the Basic Quick Start configuration page will have two or three Quick Start Options sections, one for each drive type. Choose only the SATA option.

Step 1 Using the drop-down lists, set the following parameters:

- **Number of arrays**: Choose the number of RAID sets that you wish to create. The maximum number depends on the number of disks detected in the unit.
- **Select RAID level**: Choose the RAID level that all RAID sets will be configured for. You can choose from the following:

  RAID 0 (striped)
  RAID 1 (mirrored)
  RAID 4 (parity)
  RAID 5 (rotating parity)
  RAID 6 (rotating dual parity)

  Note For more information on RAID levels, see Appendix A, "RAID Levels".

- **Number of pool spares**: Choose the number of spare disks that will be available to use as backups in case a RAID disk fails. The maximum number of pool spares depends on the number of disks detected in the unit.
- **Number of volumes per array**: This setting controls whether or not each RAID array will be further divided into two or more smaller volumes. The default setting is **1**. The number of volumes per array can be anywhere from **1** to **10**.
- **Limit volume size to less than 2TB**: This option is unchecked by default. If your hosts do not support volumes of more than 2TB in size, check this option.

Step 2 Click **Next**.

The New Configuration Preview page is displayed.

Step 3 Ensure that the settings for **Arrays**, **Volumes**, **Pool Spares**, and **Volume Access** are correct.

Step 4 If all settings are acceptable, select the confirmation check box, then click the **Quickstart** button.

Caution If any arrays or volumes have already been configured on the unit, the Management Console displays a warning dialog. If you wish to continue, click the check box and select **Confirm Quickstart Configure**. If you do not wish to continue, click **CANCEL Quickstart**.

Note Although your volumes are available immediately, Quickstart continues to run in the background. The Quickstart operation may take as much as several hours to complete, depending on the size and number of the disk drives in the unit. You can check the progress of the operation by going to **RAID Information > Progress**.

Expert Quick Start

Arrays are limited to the disks physically contained in a single Cisco Video Surveillance Storage System component.

Note If the system you are setting up is a storage unit/expansion unit pair, you are first asked to select the unit that you wish to configure. Select the unit you wish to configure, then click **Next**. When you are finished, you can configure the second enclosure by repeating this procedure.

The Expert Quick Start configuration page is displayed.

Note Only SATA disk drives can be used in the RAID array. SAS and SSD are not supported. If your Cisco Video Surveillance Storage System component contains a mixture of disk drive types, the Basic Quick Start configuration page will have two or three Quick Start Options sections, one for each drive type. Choose only the SATA option.

Step 1 Using the drop-down lists, set the following parameters:

- **Number of arrays**: Choose the number of RAID sets that you wish to create. The maximum number depends on the number of disks detected in the unit.
- **Select RAID level**: Choose the RAID level that all RAID sets will be configured for. You can choose from the following:

  RAID 0 (striped)
  RAID 1 (mirrored)
  RAID 4 (parity)
  RAID 5 (rotating parity)
  RAID 6 (rotating dual parity)

  Note For more information on RAID levels, see Appendix A, "RAID Levels".

- **Number of pool spares**: Choose the number of spare disks that will be available to use as backups in case a RAID disk fails. The maximum number of pool spares depends on the number of disks detected in the unit.
- **Number of volumes per array**: This setting controls whether or not each RAID array will be further divided into two or more smaller volumes. The default setting is **1**. The number of volumes per array can be anywhere from **1** to **10**.
- **Limit volume size to less than 2TB**: This option is unchecked by default. If your hosts do not support volumes of more than 2TB in size, check this option.
- **Select stripe size**: The default stripe size is **128Kbytes**. You can choose to use smaller stripes by selecting **64Kbytes**, **32Kbytes**, or **16Kbytes**.
- **Select host connection type**: By default, this setting is set to **Fibre/SAS/10Ge iSCSI (multi-path)**, which maps all logical unit numbers (LUNs) to all available Fibre Channel/SAS/10GbE iSCSI ports. If you wish to change the mapping, select one of the following:

Note SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher.

None (leave unmapped): The LUNs will not be associated with any ports on the unit and will not be available to the host. You can later manually assign each LUN to one or more ports using **Configure Volumes > Map Volume** (see Map Logical Volumes, page 7-4).

Fibre/SAS/10Ge iSCSI (non-redundant): Assigns each LUN to a single available Fibre Channel/SAS/10Gb iSCSI port.

Fibre/SAS/10Ge iSCSI (multi-path): Assigns LUNs to all available Fibre Channel/SAS/10Gb iSCSI ports (requires multipathing software).

iSCSI (non-redundant): Assigns each LUN to a single available iSCSI port.

iSCSI (multi-path): Assigns LUNs to all available iSCSI ports (requires multipathing software).

- **Select default host access**: This setting defaults to **Read/Write**. This will allow all attached hosts to access all volumes on this unit. If you wish to restrict host access to this unit, change this setting to **Deny**, then use the procedure under Manage Hosts, page 8-3 to assign **Read** or **R/W** access to specific hosts.

  To ensure integrity and security of data, it is recommended that you change this setting to **Deny**.
- **Online Create**: When this box is checked, volumes on this unit will be available immediately, with RAID creation continuing in the background. This does, however, slow down the RAID creation process. You can speed up the creation process by unchecking this box, in which case volumes will be unavailable until RAID creation is complete.
- **Leave free space on each array for future volumes/expansion**: Be default, the volumes will take up all of the space in the RAID arrays. This setting lets you keep a percentage of the RAID array space free for additional volumes or expansion of current volumes. Select **0%**, **10%**, **25%**, **50%**, or **75%**.

Step 2 Click **Next**.

The New Configuration Preview page is displayed.

Step 3 Ensure that the settings for **Arrays**, **Volumes**, **Pool Spares**, and **Volume Access** are correct.

Step 4 If all settings are acceptable, select **Check this checkbox to confirm**, then click the **Quickstart** button.

Caution If any arrays or volumes have already been configured on the unit, the Management Console displays a warning dialog. If you wish to continue, click the check box and select **Confirm Quickstart Configure**. If you do not wish to continue, click **CANCEL Quickstart**.

Note The Quickstart operation may take as much as several hours to complete, depending on the size and number of the disk drives in the unit. You can check the progress of the operation by going to **RAID Information > Progress**.

Check List

Clicking **Quick Start > Check List** takes you to the Configuration Checklist page, which contains links to pages in the Management Console that should be configured when the unit is first installed.

The items on the Quick Start Configuration Checklist are:

- **Security** (see Security Settings, page 11-4)
- **System Name** (see Configure Enclosures, page 10-3)
- **Network Settings** (see Configure Network Settings, page 11-1)
- **Array Configuration** (see Create a New RAID Array, page 6-1)
- **Volume Configuration and Access** (see Create a Logical Volume, page 7-1)

Each item in the list displays its status on the Quick Start Configuration Checklist. If an item has a green check mark next to it, that item has been completed with a recommended setting. If an item has a red exclamation point next to it, that item has either not been completed or has an unrecommended setting. For more information see Set Up the System, page 1-3.

Integrating External Storage Volumes Into Cisco VSM

The CPS-SS-4RU and CPS-SS-4RU-EX systems provide external storage volumes to the Cisco Video Surveillance servers. This external storage is in addition to the internal storage available in the Cisco VSM server.

To use these external storage systems with a Cisco VSM, you must integrate the external system by running a script on the Cisco VSM server. See the following topics for more information:

Note See the Release Notes for Cisco Video Surveillance Manager for information on supported servers and platforms, such as the Cisco Connected Safety and Security UCS Platform Series servers.

Understanding the Integration Script

The CPS-SS system is configured to provide the full capacity of a given RAID array (with 2TB or 3TB drives) to the Cisco VSM server as a single volume. For example, if you have a RAID-5 set of 10 drives with 3TB, then the entire ~25TB is provided as a single volume; the single volume appears to the Cisco VSM server as a single hard drive (e.g. sdc, sdd, sde).

The `setup_external_storage.sh` script splits the single storage volume into two partitions of equal size, formats the partitions, mounts them, and integrates them into Cisco VSM.

The `setup_external_storage.sh` script offers the following options:

Table 2-1 Script Options

Script	Purpose
No parameters	Run the script with no parameters (for example, **setup_external_storage.sh**) to discover any connected fibre channel devices and create the new media partitions for use by Cisco VSM. See the "Integration Procedure" section on page 2-7 for more information.
Restore	Include the restore option (for example, **setup_external_storage.sh restore**) to retrieve and restore any media partitions that were previously configured on the disk so they can be used again. No new partitions are created using this restore option. Use this option only if the following previously occurred: • The script was previously run and the external storage partitions were successfully configured. • The Cisco VSM system software recovery procedure was executed (which removes the partitions from the Cisco VSM configuration). See the "Example Integration Script with Restore Option" section on page 2-11 for more information.
Help	Include the restore option (for example, **`setup_external_storage -h`**) to view more information about the script options and version. See the "Integration Procedure" section on page 2-7 for more information.

Requirements

The `setup_external_storage.sh` script requires the following:

Table 2-2 Script Requirements

Requirements	Complete? (✓)
A Cisco Connected Safety and Security UCS Platform Series server running Cisco Video Surveillance release 7.2 or higher.	❑
The Cisco Video Surveillance Storage System must be configured with one or more RAID array to provide storage for video recording by a Cisco Video Surveillance server. • A Cisco VSM server or virtual machine will exclusively access the volumes for each RAID array, (even though a VSM server can access the volumes multiple RAID arrays). The Storage System must be configured with multiple RAID arrays so that it can support multiple Cisco VSM servers. • The RAID array should be configured with a single RAID volume. The `setup_external_storage.sh` script will create partitions on the RAID volume as video repositories for VSM.	❑
A Cisco Video Surveillance Storage System must be connected to the Cisco VSM server. **Note** If the Fibre Channel (FC) connection is not present when the script is run, the external storage will not be detected and not integrated into Cisco VSM. The script can be run again after the FC cable connection is established. The FC port LEDs indicate the connection status. **Note** Disconnecting the FC cable during normal operation removes the access by Cisco VSM to the external storage volumes. The `/media` mount points remain intact, however, and are not deleted form the server and Cisco VSM configuration. The script does not include a delete option for the external storage volumes.	❑
The `setup_external_storage.sh` script file. To download the script, go to the Cisco Video Surveillance software download page and select **Standalone Tools**. http://software.cisco.com/download/type.html?mdfid=282976740&i=rm	❑

Integration Procedure

Complete the following procedure to display the commands and output to view the server filesystem and partitions, display the script help, run the integration script and verify the results.

Note This example executes the integration script without options. If partitions were previously created, and the Cisco VSM system software was recovered (which deletes any partitions) use the recovery option as described in the "Example Integration Script with Restore Option" section on page 2-11.

Tip See the "Understanding the Integration Script" section on page 2-6 for more information.

Procedure

Step 1 Prepare for the external storage integration:

a. Verify the requirements are complete.

See the "Requirements" section on page 2-7.

b. Copy the integration script to the Cisco VSM server as the "localadmin" user.

c. Run the following command to copy the files to the /usr/BWhttpd/sbin/ directory.

localadmin@vsm-server ~]$ **sudo cp setup_external_storage.sh /usr/BWhttpd/sbin/**

d. Change the user to `root`.

```
localadmin@vsm-server ~]$ sudo su -
[root@vsm-server ~]#
```

e. Verify that the fiber channel controller module `lpfc` is installed in the system:

[root@vsm-server ~]# **modprobe -l -a lpfc**

For example:

```
[root@vsm-server ~]# modprobe -l  -a lpfc
kernel/drivers/scsi/lpfc/lpfc.ko
```

Note The `lpfc` module is included in Media Servers that were factory installed with Cisco VSM.

f. Connect the fiber channel cable from the external storage array to the Cisco VSM server.

g. Reboot the server so it boots with the storage attached.

Step 2 (Optional) Display the Cisco VSM release details (to verify support per the "Requirements") and the current filesystem disk space usage:

a. Display the Cisco VSM build details to verify the release is supported:

```
[root@vsm-server ~]# cat /etc/Cisco-release
PRODUCT="VSM"
RELEASE="7.2.0"
OSVER=""
GOLD_DISK="VSM 7.2.0-cd15"
BUILDDATE="Sun Aug 25 10:37:12 PDT 2013"
```

b. Display the filesystem disk space usage (in human readable format):

```
[root@vsm-server ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sdb1             7.9G  2.2G  5.4G  29% /
/dev/sdb7              50G  570M   47G   2% /mysql/data
/dev/sdb5             7.9G  2.8G  4.7G  38% /usr/BWhttpd
/dev/sdb3              32G  173M   30G   1% /var
/dev/sda1             146M   17M  122M  12% /boot
tmpfs                 4.0G  4.0K  4.0G   1% /dev/shm
/dev/sdc1             5.4T  8.2M  5.4T   1% /media1
```

Step 3 (Optional) Display the **help** output for command options and other information:

```
[root@vsm-server ~]# /usr/BWhttpd/sbin/setup_external_storage.sh help

setup_external_storage  will configure external storage volumes for
    use by  VSM 7.x.   It is currently optimized for RAID volumes
    configure in 10 drive, RAID 5 arrays (9+1).
```

```
    All other configurations are not supported and would cause
    performance impacts.

usage:
   setup_external_storage [noprompt|restore|help|]
     where
        noprompt    will destroy all partitioning and data on external
                    volumes without any prompting

            without argument it will look for existing partition
            and prompt the user if and only if partitioning info
            exists.

            version: 1.0     date: 11/06/2013
```

Step 4 Execute the **setup_external_storage.sh** integration script from the `/usr/BWhttpd/sbin/` directory to discover any connected fibre channel devices and create the new media partitions for use by Cisco VSM.

The command syntax is:

[root@vsm-server ~]# */usr*/**BWhttpd/sbin/setup_external_storage.sh**

Note After running the script, the newly created `/media` partitions are available for recording in Cisco VSM, without needing to reboot the server.

Note In the following example, the script is run without options, which creates new partitions. See the "Example Integration Script with Restore Option" section on page 2-11 if previously configured partitions need to be restored.

For example:

```
[root@vsm-server ~]# /usr/BWhttpd/sbin/setup_external_storage.sh
user friendly !!!

get_external_storage_devices
using the next  MEDIA_PART_NUMBER = 1
WARNING:  /dev/disk/by-id/scsi-36000402006d812907fbf9a1d00000000 has partitioning and
or data
WARNING:  It appears the external storage has existing partitioning and
          possibly video data.  Continuing will erase any data on external
          partitions.
Are you sure you want to proceed? [yes/no]
yes
====== Creating Partition Tables ======================
DEVICE /dev/disk/by-id/scsi-36000402006d812907fbf9a1d00000000

create_partition_table /dev/disk/by-id/scsi-36000402006d812907fbf9a1d00000000
parted /dev/disk/by-id/scsi-36000402006d812907fbf9a1d00000000 mklabel gpt
Warning: The existing disk label on /dev/sdd will be destroyed and all data on this
disk will be
lost. Do you want to continue?
parted: invalid token: gpt
Yes/No? Yes
New disk label type?  [gpt]?
Information: Don't forget to update /etc/fstab, if necessary.

======= Creating Partitions ========================
create_partitions_on_device /dev/disk/by-id/scsi-36000402006d812907fbf9a1d00000000
stripe size = 18432
```

```
START_S=34  SIZE_S=10
number of partitions: 2
stripe size = 18432
START_S=36864  SIZE_S=13502366MB
parted /dev/disk/by-id/scsi-36000402006d812907fbf9a1d00000000 mkpart primary xfs
36864s 27652884479s
Information: Don't forget to update /etc/fstab, if necessary.

stripe size = 18432
START_S=27652884480  SIZE_S=13502366MB
parted /dev/disk/by-id/scsi-36000402006d812907fbf9a1d00000000 mkpart primary xfs
27652884480s 100%
Information: Don't forget to update /etc/fstab, if necessary.

======= Formating Partitions and ====================
======= Creating fstab entries, mount pts =======

format_partitions_on_device /dev/disk/by-id/scsi-36000402006d812907fbf9a1d00000000
format partition: /dev/sdd1
log stripe unit specified, using v2 logs
format partition: /dev/sdd2
log stripe unit specified, using v2 logs
update_fstab_device_mount_log UUID=d7844df6-eda7-4acc-b317-36c0412b90fe /media2
update_device_name /dev/sdd 1 /media2
parted /dev/sdd name 1 /media2
Information: Don't forget to update /etc/fstab, if necessary.

update_fstab_device_mount_log UUID=6e68759b-8b6f-4036-a859-36571460b753 /media3
update_device_name /dev/sdd 2 /media3
parted /dev/sdd name 2 /media3
Information: Don't forget to update /etc/fstab, if necessary.

Configuring VSMS
cisco           0:off   1:off   2:on    3:on    4:on    5:on    6:off
cisco_kernelTweaks      0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Step 5 Verify that the filesystem disk space usage and external storage partitions are correct.

a. Display the filesystem disk space usage (the **-h** option displays the results in human readable format):

```
[root@vsm-server ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sdb1             7.9G  2.2G  5.4G  29% /
/dev/sdb7              50G  570M   47G   2% /mysql/data
/dev/sdb5             7.9G  2.8G  4.7G  38% /usr/BWhttpd
/dev/sdb3              32G  171M   30G   1% /var
/dev/sda1             146M   17M  122M  12% /boot
tmpfs                 4.0G  4.0K  4.0G   1% /dev/shm
/dev/sdc1             5.4T  8.2M  5.4T   1% /media1
/dev/sdd1              13T  8.2M   13T   1% /media2
/dev/sdd2              12T  8.2M   12T   1% /media3
```

b. Display the available disks and disk partitions. The file system unique ID and its mount point are displayed from the list of configured partitions:

```
[root@vsm-server ~]# diff /etc/fstab /etc/fstab.orig
12,13d11
< UUID=d7844df6-eda7-4acc-b317-36c0412b90fe /media2         xfs
rw,noatime,nodiratime,logbufs=2  1 2
< UUID=6e68759b-8b6f-4036-a859-36571460b753 /media3         xfs
rw,noatime,nodiratime,logbufs=2  1 2
```

Example Integration Script with Restore Option

The **restore** option retrieves and restores any media partitions that were previously configured on the disk so they can be used again.

This option is used after the Cisco VSM system software is recovered, since the recovery process deletes any Cisco VSM storage partitions from the Cisco VSM configuration.

Tip See the "Understanding the Integration Script" section on page 2-6 for more information.

Procedure

Step 1 Restore the Cisco VSM system software.

See the Cisco Video Surveillance Manager Recovery Guide (UCS Platform) for more information.

Step 2 Complete the procedure to "Integration Procedure" section on page 2-7, except use the **restore** option to the integration script.

Tip See the "Understanding the Integration Script" section on page 2-6 for more information.

For example:

```
[root@vsm-server /]# /root/BWhttpd/sbin/setup_external_storage restore
restore

get_external_storage_devices
======= Creating fstab entries, mount pts =======
update_fstab_device_mount_log UUID=d7844df6-eda7-4acc-b317-36c0412b90fe /media2
update_device_name /dev/sdd 1 /media2
parted /dev/sdd name 1 /media2
Information: Don't forget to update /etc/fstab, if necessary.

update_fstab_device_mount_log UUID=6e68759b-8b6f-4036-a859-36571460b753 /media3
update_device_name /dev/sdd 2 /media3
parted /dev/sdd name 2 /media3
Information: Don't forget to update /etc/fstab, if necessary.

Configuring VSMS
cisco           0:off   1:off   2:on    3:on    4:on    5:on    6:off
cisco_kernelTweaks      0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Step 3 Verify the results by listing the contents of each partition.

The following examples uses the **-al** option to list all results in long format.:

```
[root@vsm-server /]# ls -al /media2
total 8
drwxr-xr-x  6 root   root    103 Nov 26 17:29 .
drwxr-xr-x 27 nobody nobody 4096 Nov 26 18:00 ..
drwxrwxr-x  3 root   root     21 Nov 26 17:29 10000
drwxrwxr-x  3 root   root     21 Nov 26 17:29 10001
drwxrwxr-x  3 root   root     21 Nov 26 17:29 10004
```

```
drwxrwxr-x  3 root   root     21 Nov 26 17:29 10008
-rw-rw-rw-  1 root   root      0 Nov 26 17:14 getstoragestatus
-rw-rw-rw-  1 root   root      0 Nov 26 12:25 systemstoragestatus

[root@vsm-server /]# ls -al /media3
total 8
drwxr-xr-x  6 root   root    103 Nov 26 17:29 .
drwxr-xr-x 27 nobody nobody 4096 Nov 26 18:00 ..
drwxrwxr-x  3 root   root     21 Nov 26 17:29 10002
drwxrwxr-x  3 root   root     21 Nov 26 17:29 10003
drwxrwxr-x  3 root   root     21 Nov 26 17:29 10005
drwxrwxr-x  3 root   root     21 Nov 26 17:29 10009
-rw-rw-rw-  1 root   root      0 Nov 26 17:14 getstoragestatus
-rw-rw-rw-  1 root   root      0 Nov 26 12:25 systemstoragestatus
```

CHAPTER 3

Home Screen

This chapter deals with the following topics:

Logging In

When you enter the IP address of your Cisco Video Surveillance Storage System component into the address field of your web browser, the login page displays. The appearance of this page varies depending on which Cisco Video Surveillance Storage System component you are logging in to, but **Click Here to Login** is always displayed.

Clicking the **Click Here to Login** button does one of two things:

- If no password has been set up for the USER account (see Security Settings, page 11-4), clicking the **Click Here to Login** button takes you to the Home page (see Home Page, page 3-2).
- If a USER password has been set up, clicking **Click Here to Login** opens a security dialog. Enter the user name and password for either the USER or ADMIN account to be taken to the Home page.

If you log in as ADMIN, you have access to all pages within the Management Console. If you log in as USER, you have access to all information and status pages in the Management Console, but are denied access to configuration pages.

Note Both the user name and password fields are case-sensitive. User names must be entered in all capitals ("ADMIN" or "USER").

Navigation and Status

The main menu is located on the left side of each page and links to each section of the Management Console for the Cisco Video Surveillance Storage System component. Each section (except the Home and Log Off pages) also has a navigation bar across the top. These are different for each section of the Management Console.

- The upper right corner of the GUI displays a unit status indicator. When the unit is operating within specifications, this indicator displays “ALL OK” with a green check mark.
- When an environmental reading is outside of specified limits, but no failure has yet occurred, this indicator displays “WARNING” with a red exclamation point.
- When a module fails, this indicator displays “FAILURE” with a red X.

  Click the “WARNING” or “FAILURE” indicator to be taken to the Summary of System Problems page (see Summary of System Problems, page 5-7 for more information).

When an array has been rebuilt or data has been lost after the unit has recovered from a failure, the indicator displays a red exclamation point next to the “ALL OK” indicator. Click the exclamation point to be taken to the Lost Data/Bad Blocks page (see Lost Data/Bad Blocks, page 6-6) or the Acknowledge Rebuild page (see Acknowledge Rebuild, page 6-7).

Home Page

The Home page provides a quick summary of the state of your Cisco Video Surveillance Storage System component and all of its modules. Its appearance depends on whether you are connecting to a single storage unit or to a storage unit/expansion unit pair.

Single Storage Unit

When you are viewing a single storage unit, the Home page displays a diagram of the unit with icons for each component. Each icon indicates the associated component’s current status. Generally:

- A green status bar indicates that the associated component is functioning correctly.
- A flashing red status bar indicates that the associated component has failed or is indicating a fault.

Some icons can indicate additional states, depending on the component:

- Black text above a **Controller** icon indicates the controller through which you are currently accessing the system’s Management Console. The other controller is indicated by gray text above the icon. To switch between the two, click the icon with the gray text.
- Text beneath each **Controller** icon indicates the current temperature of that RAID Controller.
- The **Alarm** icon is normally gray, but turns red when the audible alarm sounds (see Audible Alarm, page 10-2 and Summary of System Problems, page 5-7).
- **Disk** icons can indicate numerous states:

  Disk not present: A grayed out icon with a grayed out status bar indicates that no drive is installed in that slot.

  Disk not configured: A gray status bar indicates that the drive is functioning, but is not assigned to an array and is not designated as a spare.

  Array disk, functioning normally: A green status bar indicates that the drive is functioning and is part of a RAID array (see RAID Array Information, page 4-1). The text below it indicates which RAID array it belongs to and which RAID Controller that array is assigned to.

  Spare disk: A blue status bar indicates that the drive is functioning and is designated as a spare, which will be used to rebuild RAID arrays when other drives fail (see Add Hot Spare, page 6-4, Delete Hot Spare, page 6-5, and Configure Hot Spare Mode, page 6-6). The text below it indicates whether it is a “Pool Spare” (which can be used by any RAID array) or a dedicated spare (assigned to a specific RAID array).

Disk idle: A green "Zzz" on a disk icon indicates that the drive is in low-power mode (see Chapter 9, "Power Settings").

Disk inaccessible: A red status bar indicates that the drive is functioning, but the RAID array to which it belongs is currently inaccessible.

Disk in critical array: A status bar alternating amber and red indicates that the drive is functioning, but is part of a RAID array that is in a critical state (see RAID Array Information, page 4-1).

Disk failed: A red icon with a flashing red status bar indicates that the drive has failed.

Spare added to array: A moving green status bar indicates that this disk was a spare, but is being added to the array. Data from the missing drive is being rebuilt and saved onto this disk.

Array rebuilding: A status bar alternating green and amber indicates that the drive is functioning and is part of a RAID array that is being rebuilt.

Additionally, clicking on any **Disk** icon takes you to that drive's Disk Information detail page (see Disk Information Detail Page, page 4-6).

- On units with active drive drawers (CPS-SS-4RU and CPS-SS-4RU-EX), each drawer has a lock icon:
  - A closed lock icon with a green status bar indicates that the drawer is locked.
  - An open lock icon with a yellow status bar indicates that the drawer is unlocked.

Storage Unit with Attached Expansion Unit

When you are viewing a storage system with an attached expansion unit, the Home page displays a summary diagram of each enclosure, with icons for each subsystem. Each icon indicates the status of the components within each subsystem. Generally:

- A green status bar indicates that the associated component is functioning correctly.
- A flashing red status bar indicates that the associated component has failed or is indicating a fault.

Some icons can indicate additional states, depending on the subsystem:

- The text beneath the **Enclosure** icon indicates whether the unit is online or offline.
- The **Arrays** icon can indicate several states:

  Fault tolerant array: A green status bar indicates that all RAID arrays are functioning correctly and are fault tolerant.

  Array under construction: A moving green status bar indicates that one or more RAID arrays are being constructed.

  Array critical: A status bar alternating amber and red indicates that one or more RAID arrays are in a critical state.

  Array rebuilding: A status bar alternating green and amber indicates that one or more RAID arrays are being rebuilt.

  Array offline: A red icon with a flashing red status bar indicates that one or more RAID arrays are offline or have failed.

- The **Net status**, **Host status**, and **Exp status** (**in** or **out**) icons can indicate several states:

  Green indicates that the host/port is connected.

  Gray indicates that the host/port is not connected or is offline.

  Amber indicates that the host/port is connected, but no volumes have been mapped to it.

Red indicates that the host/port is on a failed RAID Controller.

Additionally, each icon (except **Exp status**) is a link to its associated subsystem:

- The **Enclosure** icon links to the status page for that physical unit, which is identical to the status page for a single unit (see Single Storage Unit, page 3-2).
- The **Fans**, **PSUs**, and **Controller** icons link to the Environmental Information page (see Environmental Information, page 5-2).
- The **Disks** icon links to the Disk Information page (see Disk Information, page 4-5).
- The **Arrays** icon links to the RAID Array Information page (see RAID Array Information, page 4-1).
- The **Net status** icons link to the Network Information page (see Network Information, page 5-3).
- The **Host status** icons link to the Fibre Information page, SAS Information page, 10Ge Information page, or iSCSI Information page, depending on which type of connection you are using (see Fibre Channel Information, page 4-7 or SAS Information, page 4-8).

Note SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher.

Alarms and Warnings

When a failure occurs, the top of the Home page contains an alarm statement and two extra buttons: the **Problem Summary** button and the **Silence Alarm** button.

- Clicking the **Problem Summary** button takes you to the Summary of System Problems page (see Summary of System Problems, page 5-7).
- Clicking the **Silence Alarm** button silences the audible alarm on the unit. A message is displayed, indicating that the alarm has been silenced. Click the **Back** button on the message to return to the Home page.

Note If further problems occur, the audible alarm will sound again.

When an array has been rebuilt following a failure, the top of the Home page contains a rebuild statement and the **Acknowledge Array Reconstruction** button. Click the **Acknowledge Array Reconstruction** button to acknowledge the rebuilt array. A message is displayed, stating that the rebuild has been acknowledged (see Acknowledge Rebuild, page 6-7).

When data in an array has been lost following a failure, the top of the Home page contains a data loss statement and the **Acknowledge Lost Data Warning** button. Click the **Acknowledge Lost Data Warning** button to acknowledge the data loss. A message is displayed, stating that the data loss has been acknowledged (see Lost Data/Bad Blocks, page 6-6).

CHAPTER 4

RAID Information

When you click the **RAID Information** button in the navigation pane, you are taken to the RAID Array Information page. The navigation bar across the top contains links to this section's subpages.

- **RAID Array** links to RAID Array Information
- **Progress** links to RAID Array Utility Progress
- **Volumes** links to Configured Logical Volumes
- **Disk Drives** links to Disk Information
- **Disk Stats** links to Disk Statistics
- **Fibre Info** links to Fibre Channel Information
- **Host Stats** links to Host Statistics
- **System Nav** links to System Hierarchal View

RAID Array Information

Clicking **RAID Information** takes you to the RAID Array Information page, which displays summary information for each array that has been configured on the unit. This includes arrays that are being constructed or rebuilt. There is an information block for each array, which contains the following information:

Item	Description
Title Bar	The Array name, Array number, and Enclosure.
Array name	The user-defined name of the array. If no name has been assigned, this item defaults to "Array #*n*", where *n* is the **Array number**. The name can be changed on the Rename RAID Arrays page (see Rename RAID Arrays, page 6-3).
Array number	Reference number, normally given in order of creation.
Enclosure	Reference number of the unit that houses the disks that make up this array. "Enclosure 0" is the main unit; "Enclosure 1" is the expansion unit.
Configured owner	Displays the RAID Controller to which this array has been assigned. This can be changed on the RAID Array Ownership page (see RAID Array Ownership, page 6-4).

Item	Description
Current owner	Displays the RAID Controller that is currently controlling this array. This may differ from Configured owner if the assigned RAID Controller is restarting or has failed.
Array status/health	Displays the current status of the RAID array: fault tolerant, not fault tolerant, constructing, critical, rebuilding, or offline. If an array verification is currently being performed (see Verify RAID Arrays, page 10-5), the progress of the scan is also displayed here.
RAID level	Displays the RAID level that this array is configured for. See Appendix A, "RAID Levels" for more information.
Disk type	Displays the type of disk (SATA, SAS, or SSD) and its speed in revolutions per minute (RPMs). **Note** SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher.
Array capacity	Displays the total data storage space of the array, in true terabytes (TB) followed by binary terabytes (TiB).
No. of members	The number of disks that make up the array.
No. of spares	The total number of spares available for the array. This includes both pool spares and dedicated spares. New spares can be added on the Add Hot Spare page (see Appendix 6, "Add Hot Spare").
No. of volumes	The number of configured volumes in this array.
Data stripe size	The size of the individual data stripes in this array.
Cache memory	Indicates whether the cache is enabled, its mirroring status, its streaming mode, and its FUA status.
Cache size	The total size of the cache, in megabytes (MB).
Rebuild priority	Displays the configured rebuild priority, ranging from Lowest to Highest. This controls the amount of resources that a RAID Controller assigns to rebuilding the array versus handling host data requests. See Configure Rebuild Priority, page 10-5 for more information.
Verify utility	Displays the user-configured verification tests for this array, as well as how often they are run. Verification tests are configured on the RAID Array Verify page (see Verify RAID Arrays, page 10-5).
Verify due	The date and time of the next scheduled verification, formatted as "Day-of-week DD-Mmm-YYYY HH:MM". If the verification is scheduled to begin within a few hours, this will display "[Verification test] will start shortly". If the verification is currently running, it will display "[Verification test] is currently active". A RAID array verification can be initiated at any time by going to the RAID Array Verify page and clicking the **Execute Verify Utility NOW** button (see Verify RAID Arrays, page 10-5).
Number of reads	Displays number of reads from the array.
Number of writes	Displays number of writes to the array.
Created	Displays the date and time that the array was created, formatted as "Day-of-Week DD-Mmm-YYYY HH:MM".

The bottom area displays the array status icon, the Array status/health, and the Array capacity. The array status icon can indicate several states:

- A green status bar indicates that all RAID arrays are functioning correctly and are fault-tolerant.
- A moving green status bar indicates that one or more RAID arrays are being constructed.
- A status bar alternating yellow and red indicates that one or more RAID arrays are in a critical state.
- A status bar alternating green and yellow indicates that one or more RAID arrays are being rebuilt.
- A red icon with a flashing red status bar indicates that one or more RAID arrays are offline or have failed.

New arrays can be created on the Create a New RAID Array page (see Create a New RAID Array, page 6-1). Arrays can be deleted on the Delete a RAID Array page (see Delete a RAID Array, page 6-3).

RAID Array Utility Progress

Clicking **RAID Information > Progress** takes you to the RAID Array Utilities Progress page, which displays the progress of active RAID array utilities.

Processes that can be viewed on this page are:

- Array construction (see Create a New RAID Array, page 6-1)
- Array reconstruction (see Acknowledge Rebuild, page 6-7)
- Surface scan (see Verify RAID Arrays, page 10-5)
- Parity scrub (see Verify RAID Arrays, page 10-5)

Configured Logical Volumes

Clicking **RAID Information > Volumes** takes you to the Configured Logical Volumes page, which displays the configured volumes for each array.

Volume Details displays the volume name, the array to which it is assigned, the number of the controller to which the array is assigned, the unit that the array is in, and the total capacity of the volume.

- The volume name can be changed on the Rename Logical Volumes page (see Rename Logical Volumes, page 7-4).
- If there is room left in the array, the total capacity of the volume can be expanded on the Expand a Logical Volume page (see Expand a Logical Volume, page 7-2).

The **Fibre** (or **SAS** or **10GE**) columns display the host port configurations and LUN mappings.

- The LUN mappings can be changed on the Map Logical Volumes page (see Map Logical Volumes, page 7-4).

Clicking the **Next** button takes you to a detail page for that volume.

The upper area displays the same information as on the previous page. The lower area displays details for host access: the Default Access, Groups (if any), and individual hosts.

The **Type** column indicates the kind of host link (Fibre/SAS/10GE or iSCSI) and its status: green for connected, yellow for connected but with no LUNs assigned, and gray for disconnected or offline.

The **Host** column displays the host number or name, its type, and its connection.

The **Access** column displays the kind of access the host has to the volume: **None**, **Read**, or **Read/Write**. Access can be changed on the Host Access page (see Host Access, page 8-3).

Volumes are created on the Add Volume page (see Create a Logical Volume, page 7-1) and deleted on the Delete Volume page (see Delete a Logical Volume, page 7-3).

Volume Access Summary

If you click the **Click here to view volume access summary** link at the bottom of the main Configured Logical Volumes page, it takes you to a summary page that displays which hosts have access to which volumes. There are columns for Type, Host, and each configured volume in the system. There are rows for Default Access, Groups (if any), and each Host connection.

The icons in the volume columns indicate the access privileges each host has to that volume:

- No icon indicates no access.
- A green icon on a gray background indicates Read/Write access.
- An amber icon on a gray background indicates Read/Write access, but that the host is not connected to a port with a logical unit number (LUN) mapping.
- A gray icon on a gray background indicates Read/Write access, but that the host is disconnected or offline.
- A green icon on a green background indicates Read Only access.
- An amber icon on a green background indicates Read Only access, but that the host is not connected to a port with a logical unit number (LUN) mapping.
- A gray icon on a green background indicates Read Only access, but that the host is disconnected or offline.

Clicking the gray arrow button on the left takes you back to the main Configured Logical Volumes page.

Detailed Volume Layout

Clicking the **Click here to view detailed volume layout** link at the bottom of the Configured Logical Volumes page takes you to this page, which shows the free space left in each array (if any), the size of each volume, the percentage of the total array that the volume takes up, and the volume's relative position within the array.

The information sections are arranged by array. Each array's section displays a status icon, the array name, the array number, the controller number, the total capacity, and a list of any free areas in the array (see RAID Array Information, page 4-1 for more information). If there is no free space in the array, a message is displayed in place of the list.

Below each array's information section are sections for each volume in the array. These display the following information:

Field Name	Description
Title bar	The volume ID and array name.
Volume name	The user-defined name of the volume.
Volume capacity	Displays the total data storage space of the array, in megabytes (MB), true gigabytes (GB), and binary gigabytes (GiB).

Field Name	Description
% of total array used	Displays the percentage of the array capacity that this volume uses.
Number of bad blocks	Displays the number of blocks in the volume that cannot be read or written to because of disk media errors.
LUN mapping	Displays a link: "Click to view". Clicking the link takes you to the volume's detail page.
Volume serial number	Displays the volume's unique serial number.
Volume created	Displays the date and time that the volume was created, formatted as "Day of Week DD-Mon-YYYY HH:MM".

The darker area below the listed items displays the name of the array that the volume belongs to, the controller number, and the **Volume capacity**.

The bottom area contains a bar which represents the percentage of the array's capacity that the volume uses, as well as the volume's relative position within the array.

Disk Information

Clicking **RAID Information > Disk Drives** takes you to the Disk Information page, which shows all of the disk drives in the system and displays information about each disk.

The **Disk** column displays the disk number and a disk icon. Clicking the disk icon takes you to a detail page for that disk (see Disk Information Detail Page, page 4-6).

The disk icon can indicate various states:

- **Disk not present**: A grayed out icon with a grayed out status bar indicates that no drive is installed in that slot.
- **Disk not configured**: A gray status bar indicates that the drive is functioning, but is not assigned to an array and is not designated as a spare.
- **Array disk, functioning normally**: A green status bar indicates that the drive is functioning and is part of a RAID array (see RAID Array Information, page 4-1). The text below it indicates which RAID array it belongs to and which RAID Controller that array is assigned to.
- **Spare disk**: A blue status bar indicates that the drive is functioning and is designated as a spare, which will be used to rebuild RAID arrays when other drives fail (see Add Hot Spare, page 6-4, Delete Hot Spare, page 6-5, and Configure Hot Spare Mode, page 6-6). The text below it indicates whether it is a "Pool Spare" (which can be used by any RAID array) or a dedicated spare (assigned to a specific RAID array).
- **Disk idle**: A green "Zzz" on a disk icon indicates that the drive is in low-power mode (see Chapter 9, "Power Settings").
- **Disk inaccessible**: A red status bar indicates that the drive is functioning, but the RAID array to which it belongs is currently inaccessible.
- **Disk in critical array**: A status bar alternating amber and red indicates that the drive is functioning, but is part of a RAID array that is in a critical state (see RAID Array Information, page 4-1).
- **Disk failed**: A red icon with a flashing red status bar indicates that the drive has failed.
- **Spare added to array**: A moving green status bar indicates that this disk was a spare, but is being added to the array. Data from the missing drive is being rebuilt and saved onto this disk.

- **Array rebuilding**: A status bar alternating green and amber indicates that the drive is functioning and is part of a RAID array that is being rebuilt.

The **Status** column displays the array that the disk belongs to, the controller number, and the AutoMAID status of the disk (see Chapter 9, "Power Settings").

The **Details** column lists the following information:

- **Model** is the manufacturer's model number for the drive.
- **Capacity** is the raw data storage capacity of the drive, in megabytes (MB).
- **Serial Number** is the manufacturer's serial number for the drive.
- **Firmware** is the firmware that the drive is currently running.

Disk Information Detail Page

When you click a disk icon on the Disk Information page or an information icon on the Disk Statistics page (see Disk Statistics, page 4-7), you are taken to the detail page for that particular disk. The following information is displayed:

Field Name	Description
Status	Displays the array that the disk belongs to, the controller number, and the disk's status icon.
Capacity	Displays the raw data storage capacity of the drive, in megabytes (MB).
Type	Displays the type of disk (SAS, SATA, or SSD) and it's speed in revolutions per minute (RPMs).
Model	Displays the manufacturer's model number for the disk drive.
Serial Number	Displays the manufacturer's serial number for the drive.
Firmware	Displays the firmware that the drive is currently running.
Read IOs	Displays the number of reads executed on the drive because of array access by attached hosts.
Write IOs	Displays the number of writes executed on the drive because of array access by attached hosts.
Other IOs	Displays the number of disk input/output operations (I/Os) executed on the drive that are not because of array access, but are directly from the RAID Controller.
R/W Transfer Retries	Displays the number of times that the RAID Controller has had to retry a read or write operation on a block of data on this drive due to data transfer problems.
R/W Media Retries	Displays the number of times that the RAID Controller has had to retry a read or write operation on a block of data on this drive due to disk media problems.
Bad blocks	Displays the number of blocks on the drive that cannot be read or written to because of disk media errors.
AutoMAID Status	Displays the current AutoMAID level of the disk, if any (see Chapter 9, "Power Settings").
Qualified by	Shows who qualified the drive for use in Cisco Video Surveillance Storage System components. If the disk is unqualified, this row is not displayed.

Clicking **Previous** or **Next** takes you to other disk's detail pages.

Disk Statistics

Clicking **RAID Information > Disk Stats** takes you to the Disk Statistics page, which displays data on how often individual disks have been accessed and how many retries have been performed in data recovery attempts.

The **Disk Number** column displays the disk number, the controller to which it belongs, and an information icon. Hover the mouse over the information icon for a pop-up dialog that displays that disk's information. Click the icon to be taken to that disk's detail page (see Disk Information Detail Page, page 4-6).

The IOs column displays the number of input/output operations (I/Os) performed on the disk.

- **Read** indicates the number of times the drive has been read because of host array access.
- **Write** indicates the number of times the drive has been written to because of host array access.
- **Others** indicates the number of times that the drive has been accessed by the RAID Controller directly. Examples include array creation, array rebuilds, and verifications.

The **Transfer Retries** column displays the number of times (for **Read** and **Write** operations, respectively) that the RAID Controller has had to retry an I/O operation due to data transfer problems.

The **Media Retries** column displays the number of times (for **Read** and **Write** operations, respectively) that the RAID Controller has had to retry an I/O operation due to disk media problems.

Fibre Channel Information

Clicking **RAID Information > Fibre Info** takes you to the Fibre Channel Information page, which provides an information summary for each Fibre Channel port on each RAID Controller in the system. The information is arranged by controller and host port. For each, the following information is displayed:

Field Label	Description
Fibre Port Name	The World Wide Port Name (WWPN) of the Fibre Channel port.
Fibre Node Name	The World Wide Node Name (WWNN) of the Fibre Channel node. This is the address of the enclosure, which is able to support multiple ports.
Fibre Loop State	Displays the status of the Fibre Channel Loop, either up or down. It also displays the loop speed in gigabits per second (Gb/s).
SFP Information	Displays the make and model of the installed SFPs (see the Cisco Video Surveillance Storage System Hardware Manual for more information).
Topology	Displays the current Fibre Channel topology, either Loop or Point-to-Point (P2P). It also indicates whether the topology is full-fabric.
Loop ID	Shows the loop address if the port is in loop mode.
Port ID	Shows the ID if the port is in point-to-point mode.
Link Speed	Shows the current Fibre Channel link speed in gigabits per second (Gb/s).

These settings can be configured or changed on the Configure Fibre page (see Configure Fibre Channel Host Access, page 8-1).

Host connectivity is also shown at the bottom of this page:

- The **Status** column icons can indicate several states:

  Green indicates that the host is connected.

  Gray indicates that the host is not connected or is offline.

  Amber indicates that the host is connected, but no volumes have been mapped to it.

  Red indicates that the host is on a failed RAID Controller.
- The **Port ID** column shows the port ID for connected hosts.
- The **Host Name** column shows the default or user-configured name of the host (see Manage Hosts, page 8-3).
- The **C*N*:H*N*** columns show which host ports on which controllers the host is connected to. The number after **C** indicates the RAID Controller; the number after **H** indicates the host port on that RAID Controller. For instance, **C0:H1** is host port 1 on RAID Controller 0.

SAS Information

Note SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher.

If your Cisco Video Surveillance Storage System system is configured for SAS-to-Host connectivity, clicking **RAID Information > SAS Info** takes you to the SAS Information page, which provides an information summary for each SAS-to-Host port on each RAID Controller in the system. The information is arranged by controller and host port. For each, the following information is displayed:

Field Label	Description
SAS Port ID	The World Wide Port Name (WWPN) of the SAS port.
SAS Node Name	The World Wide Node Name (WWNN) of the SAS node. This is the address of the enclosure, which is able to support multiple ports.
Link Speed	Shows the current SAS link speed in gigabits per second (Gb/s) and the number of operating lanes. If the link is not operating, displays “Port Down”.
TCP Port	Displays the status of each physical SAS connection, either Up, Down, or Disabled.

These settings can be configured or changed on the Configure SAS page.

Host connectivity is also shown at the bottom of this page:

- The **Status** column icons can indicate several states:

  Green indicates that the host is connected.

  Gray indicates that the host is not connected or is offline.

  Amber indicates that the host is connected, but no volumes have been mapped to it.

Red indicates that the host is on a failed RAID Controller.

- The **Host Name** column shows the default or user-configured name of the host (see Manage Hosts, page 8-3).
- The **C*N*:H*N*** columns show which host ports on which controllers the host is connected to. The number after **C** indicates the RAID Controller; the number after **H** indicates the net port on that RAID Controller. For instance, **C0:H1** is net port 1 on RAID Controller 0.

Host Statistics

Clicking **RAID Information > Host Status** takes you to the Host Statistics page, which displays I/O, block, and reset statistics for each host port. The information is arranged by controller.

The **Controller** column lists the host ports for each controller.

The **IOs** column displays the number of input/output operations (I/Os) performed through the port.

- **Read** indicates the number of times that a read operation has been performed through the port.
- **Write** indicates the number of times that a write operation has been performed through the port.
- **Others** indicates the number of times an RAID Controller initiated I/O operation has been performed through the port. Examples include array creation, rebuilding, and verification.

The **Blocks** column displays the number of 512-byte data blocks that have been accessed by a **Read** or **Write** I/O operation through the host.

The **Resets** column displays the number of times that a logical unit (LUN) or a Port has been reset according to the host communication management protocol.

System Hierarchal View

Clicking **RAID Information > System Nav** takes you to the System Hierarchal View page, which gives an overview of the configured arrays, volumes, and array member disks in a hierarchal view. Clicking the "**+**" icon next to an item expands it to list its components.

Clicking an icon displays information related to the component:

- Unit: Displays a system information summary (see Summary Information, page 5-1).
- Array: Displays the RAID array information (see RAID Array Information, page 4-1).
- Progress: Displays the progress of any running utilities (see RAID Array Utility Progress, page 4-3).
- Disk: Displays that disk's detail page (see Disk Information Detail Page, page 4-6).
- Volume: Displays information specific to the volume, but in a format similar to the Detailed Volume Layout page (see Detailed Volume Layout, page 4-4).

CHAPTER 5

System Information

When you click the **System Information** button in the navigation pane, you are taken to the System Information Summary page. The navigation bar across the top contains links to this section's subpages.

- **System Info** links to Summary Information
- **Enviro Info** links to Environmental Information
- **Network Info** links to Network Information
- **Network Services** links to Network Services
- **Network Stats** links to Network Statistics
- **Problems** links to Summary of System Problems
- **Event Log** links to Event Log
- **Multi View** links to Multiple View HTML Builder
- **Key** links to Icon Key

Summary Information

Clicking **System Information** takes you to the Summary Information page, which displays information about the storage system's main unit.

Note Only the main unit's information is displayed.

The displayed information includes the following:

Field Label	Description
System	The storage unit's family model (CPS-SS-4RU).
System ID	The unit's unique system identifier.
System Mode	Displays the controller failover configuration.
Active Controllers	Displays the number of active RAID Controllers in the system.
Enclosure Type	Displays the physical attributes of the system, including its U-height.
Host fibre/SAS/10Ge iSCSI connection	Displays the configuration of the Fibre Channel, SAS-to-Host, or 10GbE iSCSI connection.

Field Label	Description
Host iSCSI connection	Displays the configuration of the iSCSI connection.
System Time	Displays the current date and time according to the unit's internal clock.
Controller Status	Displays the current status of each RAID Controller (Up or Down) as well as which controller is primary (Master or Slave, see RAID Array Ownership, page 6-4)
Controller up time	Displays the total amount of time that each RAID Controller has been running continuously.
Firmware revision	Displays the firmware version that each RAID Controller is running.
Boot Loader revision	Displays the revision number of the boot loader.
Emergency revision	Displays the version number of code used for alternative system booting. Booting the system into Emergency mode allows you to upload a main firmware file if the main firmware gets corrupted during upload or if it contains a bug that prevents the normal uploading of new firmware.
Controller Serial Number	Displays the serial number of each RAID Controller.
Cache	Indicates the total cache size in megabytes (MB), whether the cache is enabled, its mirroring status, its streaming mode, and its FUA status.

Environmental Information

Clicking **System Information > Enviro Info** takes you to the Environmental Information page, which displays the values of various environmental sensors throughout the unit. Each item displays its status (**OK** or **FAULT**) and related information, if any. The information is arranged by component, and different units will display this information in different arrangements.

If an expansion unit is attached to the main unit, a **Next Enclosure >** link is displayed. Click it to be taken to the Environmental Information page for the expansion unit.

For power supply units (**PSU 0** and **PSU 1**), the following information is displayed:

- **State**: The overall status of the power supply unit.
- **Temperature**: The current temperature of the power supply unit.
- **Blower*N***: The current RPMs of the designated PSU fan.
- For CPS-SS-4RU and CPS-SS-4RU-EX units, the following additional information is displayed:
  - **3V3/12V Current**: The electrical current being supplied from each output of the PSU.
  - **PSU Power**: The power of the PSU in Watts.

For RAID Controllers and Expansion Controllers (**Controller 0** and **Controller 1**), the following information is displayed:

- ***XX* rail voltage**: The voltage of each rail in the Controller.
- **CPU core voltage**: The core voltage of the Controller's central processing unit (CPU).
- For CPS-SS-4RU-EX expansion units, the following additional information is displayed:
  - **Controller temperature**: The current temperature of the Expansion Controller.
- For CPS-SS-4RU units, the following additional information is displayed:

  - **Pcb/CPU/SAS/EXP temperature**: The current temperature of the printed circuit board, CPU, expansion port controller, and expander in the RAID Controller.
  - **Battery status**: The charge status of the cache battery.

For CPS-SS-4RU units, the following information for the active drive drawers (**Pod *N***) is displayed:

- **Power Module A/B**: The status of power modules A and B in the active drive drawer.
- **Front Panel Blower 0**: The current RPMs of the fan in the front of the active drive drawer.
- **Rear Blower 0/1**: The current RPMs of the fan in the back of the active drive drawer.
- **Power Pod Internals**: The status of internal power components in the active drive drawer.
- **Pod Temp (Exp A B)**: The current temperature of each expander (A and B) in the active drive drawer.
- **Pod Temp (Pcb A B)**: The current temperature of each printed circuit board (A and B) in the active drive drawer.

For CPS-SS-4RU-EX expansion units, the following information for the active drive drawers (**Pod *N***) is displayed:

- **Power Module A/B**: The status of power modules A and B in the active drive drawer.
- **Front Panel Blower 0**: The current RPMs of the fan in the front of the active drive drawer.
- **Rear Blower 0/1**: The current RPMs of the fan in the back of the active drive drawer.
- **Pod Temp (Back/Front)**: The current active drive drawer temperature, as measured at the front and the back of the drawer, respectively.

If a **FAULT** occurs in a field-replaceable module, refer to the unit's Hardware Manual for instructions on how to replace the module. If a **FAULT** occurs in a component that is not field-replaceable, contact Technical Support for instructions (see Chapter 12, "Technical Support").

Network Information

Clicking **System Information > Network Info** takes you to the Network Information page, which displays LAN information for both the management and iSCSI network ports. This information is arranged by RAID Controller and then by port.

On CPS-SS-4RU units, the Management Console connection is provided by the dedicated Management port.

Note SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher.

Regardless of the unit being examined, this page provides the same information about each port:

Field Label	Description
Port Status	Displays the current speed and duplex setting for the port. If the port is not active, "Link Down" is displayed.
IP address assignment	Indicates whether the port's IP address is assigned automatically ("DHCP") or manually ("Static IP").
Port IP address	Displays the current IP address of the port.

Field Label	Description
Subnet mask	Displays the current subnet mask.
Gateway IP address	Displays the configured gateway IP address.
Primary DNS IP address	Displays the IP address of the primary domain name service (DNS) server. This setting only applies to the management port (**Net 0** or **Management**).
Secondary DNS IP address	Displays the IP address of the secondary (backup) DNS server. This setting only applies to the management port (**Net 0** or **Management**) and is not required.
Hostname	Displays the default or user-assigned host name of the port.
Ethernet address	Displays the physical ethernet (MAC) address of the port.
Port Mode	Displays the speed and duplex configuration settings for the port, either automatic or fixed.
Jumbo Frames	Indicates whether or not jumbo frame usage has been enabled for the iSCSI port. This setting does not apply to the **Management** port on a CPS-SS-4RU.

These settings can be configured or changed as follows:

- For CPS-SS-4RU units, the settings for the **Management** port are configured on the Configure Network Settings page (see Configure Network Settings, page 11-1).

Network Services

Clicking **System Information > Network Services** takes you to the Network Services page, which provides information about various network and system services. It displays the following information:

E-Alerts

E-Alerts	
Item	**Contents**
When to send E-alerts	Indicates when alert emails are sent: on errors; on warnings and errors; on information, warnings, and errors; or for all events. It can also be set to Disabled, meaning that no email alerts are sent.
Send automatic status emails	Indicates how often status emails are sent: every day, every two days, every four days, weekly, or monthly. It can also be set to Disabled, meaning that no email status updates are sent.
Recipient email address *N*	The email addresses that alerts and statuses are sent to.
Sender email address	The email address that alerts and statuses are sent from.
Friendly name	The user-defined “friendly” name of the system.
SMTP server	The IP address or DNS name of the SMTP email server.
Current emailer status	Indicates how many emails are queued to be sent.

SNMP Traps

SNMP Traps	
Item	**Contents**
IP address *N* for SNMP traps	The IP address that SNMP traps will be sent to. One or two IP address can be specified.
Community string	The SNMP password. By default, this is “public”.
Trap version	The type of SNMP trap that is sent: SNMPv1 (abbreviated “1”) or SNMPv2c (abbreviated “2c”).
Test String	Text that is sent to test the SNMP trap.
When to send SNMP traps	Indicates when SNMP traps are sent: on errors; on warnings and errors; on information, warnings, and errors; or for all events. It can also be set to Disabled, meaning that no SNMP traps are sent.

SNMP trap settings are configured on the SNMP/SYSLOG Settings page (see SNMP/SYSLOG Settings, page 11-2).

Time Server

Time Server	
Item	**Contents**
Auto set time and date	Indicates whether the time and date are configured to be automatically updated by a time server.
Timer Server Protocol	The method by which the time server updates the unit’s time and date: Daytime or SNTP.
Selected time server	The IP address of the time server.
Daytime server date and time format	The date and time format used by the Daytime time server. Not applicable if an SNTP time server is used.
Retrieved daytime server data	The retrieved data from the Daytime time server. Not applicable if an SNTP time server is used.

Time server settings are configured on the Configure Time and Date page (see Configure Time and Date, page 11-3).

Security

Security	
Item	**Contents**
ADMIN account login	Indicates whether or not a password is required for the ADMIN account. If a password is required, but the default password has not been changed, “Password is default” is displayed.

USER account login	Indicates whether or not a password is required for the USER account. If a password is required, but the default password has not been changed, “Password is default” is displayed.
GUI mode	Indicates the current Management Console restrictions. If there are none, “Full GUI access” is displayed.

Security settings are configured on the Password Configuration page (see Security Settings, page 11-4).

SSL

SSL	
Item	**Contents**
SSL certificate	Indicates the type of SSL certificate currently in use, and also provides a download link for the current certificate.
SSL mode	Indicates what kinds of browser connections are allowed for the storage unit: “HTTP only”, “HTTPS only”, and “HTTPS or HTTP”.
Certificate mode	Indicates the current certificate mode.

SSL settings are configured on the SSL Configuration page (see SSL Configuration, page 11-5).

GUI Settings

GUI Settings	
Item	**Contents**
Webpage refresh	The current page auto-refresh setting.
Colored array text	Indicates whether different arrays are displayed with different colored text.
JavaScript enhancements	Indicates whether JavaScript is currently being used in the GUI.
JavaScript RAID icon info	Indicates whether JavaScript is being used for RAID icon help.
Reduce scrolling by using submenus	Indicates whether optional submenus are being used in the GUI.
Reduce scrolling by showing less info	Indicates whether pages are displayed with reduced information.

GUI settings are configured on the GUI Settings page (see GUI Settings, page 11-6).

Network Statistics

Clicking **System Information > Network Stats** takes you to the Network Statistics page, which displays information about network packets. The information is arranged by controller and port. The information provided for each controller and port is as follows:

- **Transmitted Packets**: The number of packets transmitted by the port.
- **Transmitted Errors**: The number of transmission errors reported by the port.
- **Received Packets**: The number of packets received by the port.
- **Received Errors**: The number of reception errors reported by the port.

Summary of System Problems

Clicking **System Information > Problems**, the "Failure" indicator in the upper right corner of any page, or the **Problem Summary** button on the Home page takes you to the Summary of System Problems page, which displays a list of any current problems that the unit is experiencing.

Each problem that the unit is experiencing is listed, with a **Number** indicating its order of occurrence and a **Description** that gives a summary of the problem and the component that it is related to.

Clicking the **Beacon** button causes the LEDs on the front of the unit to flash for one minute. This can help in locating a specific unit in a large installation where multiple Cisco Video Surveillance Storage System units are located.

Clicking the **Silence Alarm** button causes the audible alarm on the unit to stop sounding.

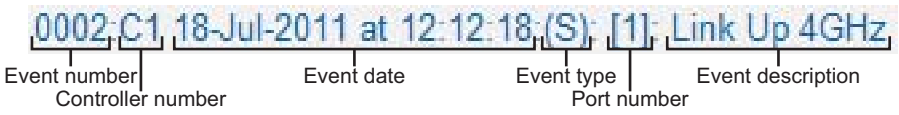
Note If further problems occur, the audible alarm will sound again.

More information about each problem can be obtained by going to the information page for the indicated component (see Chapter 4, "RAID Information" and other sections in this chapter).

Event Log

Clicking **System Information > Event Log** takes you to the Event Log page, which displays the event log for the unit. This log can be used to find information about configuration changes, data errors, hardware failures, and other events experienced by the storage unit (and expansion unit, if present).

Event log entries follow a standard format:



- Event number: The reference number for the event, in reverse order of occurrence (event 0000 is the most recent event).
- Controller number: The RAID Controller that the event is related to.
- Event date: The date and time of the event's occurrence, in "dd-mmm-yyyy at hh:mm:ss" format.
- Event type: The broad category that the event falls into:

  - Errors (**E**) are serious problems that likely require user intervention and may compromise data. Examples include a failed disk, a RAID Controller going offline, or a fan problem.
  - Warnings (**W**) are problems that may indicate an imminent failure, but are themselves unlikely to compromise data. Examples include excessive temperature, firmware errors, or disk block failures.
  - Information (**I**) events indicate items of interest to the user. Examples include RAID array creation or deletion, verification scan start and stop, or a new disk being inserted.
  - System (**S**) events are lower-level information events. Examples include port status, IP address changes, or RAID array initialization messages.
- Port number: For events that pertain to a particular port, the number of the port.
- Event description: A brief description of the event.

The event log can be filtered and formatted using the controls under **Display Options**:

- **Filter by Controller**: Show events for **Controller 0**, **Controller 1**, or both RAID Controllers.
- **Filter by Date**: Show events from the last day, week, or month; or show all entries.
- **Filter by Importance**: Show only error events (**E**); errors and warnings (**E** & **W**); errors, warnings, and information events (**E**, **W**, **I**); or all events (**E**, **W**, **I**, **S**).
- **Date Format**: Show dates in one of three formats:
  - **dd-mmm-yyyy at hh:mm:ss** (international format, the default)
  - **dd/mm/yyyy hh:mm:ss** (European format)
  - **mm/dd/yyyy hh:mm:ss** (North American format)
- **Show event icons**: Display icons for each event category at the beginning of each event entry. Icons are color coded: pink for system events, blue for information events, yellow for warnings, and red for errors. This option is deselected by default.

Note If Show event icons is selected, the Event type is not displayed after the Event date.

- **Show controller colours**: Display events for Controller 0 in black and events for Controller 1 in blue. This option is selected by default.

General Configuration

Clicking the **General Configuration** link on the Event Log page displays a text-based summary of the current system configuration.

Volume and Host Access

Clicking the **Volumes & Host Access** link displays a text-based volume mapping and host access summary.

Disk Configuration

Clicking the **Disk Configuration** link displays a text-based summary of disk information.

Download Event Log Files

You can download the Event Log, General Configuration, Volumes & Host Access, and Disk Information files in text format by clicking the **Download log/config dump as text** link. You can download them as an HTML file by clicking the HTML link in parentheses next to it.

Multiple View HTML Builder

Clicking **System Information > Multi View** takes you to the Multiple View HTML Builder page. From this page, you can create an HTML page that displays a summary of multiple Cisco Video Surveillance Storage System units. You can do this in several ways:

- You can enter an IP address range in the **From IP address** and **To IP address** fields and click the **Scan A Range** button.
- You can scan the entire subnet for Cisco Video Surveillance Storage System units by clicking the **Scan The Subnet** button.
- You can enter the IP addresses of up to sixteen individual Cisco Video Surveillance Storage System units and up to four discrete IP address ranges, then click the **Build Multiple View Page** button.

Whichever method you choose, a link page is displayed after the button is clicked. Depending on the number of Cisco Video Surveillance Storage System units being displayed, this page may take as much as a few minutes to be displayed. Click the **Click here to display the multiple view page** to view an HTML page with a summary of all of the units you asked to have displayed.

Note Alternatively, you can right-click the **Click here to display the multiple view page** and select **Save Target As** or **Save Link As** to save the HTML summary to your computer.

The multiple view page shows a summary of each scanned device. This summary includes RAID status, fan status, PSU status, overall status, system type, unit serial number, firmware revision, total storage capacity, the number of configured arrays, the number of spare disk drives, and the time and date of the scan. Clicking the IP address or the summary takes you to the Login page for that unit.

Icon Key

Clicking **System Information > Key** takes you to the Key page, which displays a legend of the various icons used throughout the Cisco Video Surveillance Storage System Management Console.

System Health Monitoring

The CPS-SS-4RU allows the health of a system to be monitored in four different ways:

- The automated email health notification function can be enabled when a unit is deployed.
- The system provides visual clues through LEDs and the Web GUI.
- An audio alarm is available to determine the overall health of the system.
- The systems logs contain a running total of all events that have occurred on the unit related to power, such as supplies, network, and thermals.

CHAPTER 6

Configure RAID

When you click the **Configure RAID** button in the navigation pane, you are taken to the Create a New RAID Array page. The navigation bar across the top contains links to this section's subpages.

- **Add Array** links to Create a New RAID Array
- **Rename Array** links to Rename RAID Arrays
- **Delete Array** links to Delete a RAID Array
- **Array Owner** links to RAID Array Ownership
- **Add Spare** links to Add Hot Spare
- **Delete Spare** links to Delete Hot Spare
- **Spare Mode** links to Configure Hot Spare Mode
- **Lost Data** links to Lost Data/Bad Blocks
- **Rebuild Ack** links to Acknowledge Rebuild

Create a New RAID Array

Clicking **Configure RAID** takes you to the Create a New RAID Array page, which allows you to create RAID arrays from two or more unused disks.

Note If your Cisco Video Surveillance Storage System component has an attached expansion unit, you are first prompted to select which unit the new RAID array will be built on. Select the enclosure and click **Next** to be taken to the New Array Configuration tool.

When you have selected the desired enclosure, or if your Cisco Video Surveillance Storage System is a single unit, the New Array Configuration tool is displayed. The disks in the unit are represented in a similar fashion to the unit summary diagram on the Home page (see Chapter 3, "Home Screen").

Regardless of the kind of Cisco Video Surveillance Storage System unit you are working with, the New Array Configuration tool asks for the following information:

- **Array name**: Enter a name for the array. Array names can be up to 63 characters in length. If this field is left blank, a default array name ("Array #*N*") will be assigned.

Note Array names can be changed on the Rename RAID Arrays page (see Rename RAID Arrays, page 6-3).

- **Select RAID level**: Choose the RAID level that the array will be configured for. You can choose from the following:

  RAID 0 (striped)
  RAID 1 (mirrored)
  RAID 4 (parity)
  RAID 5 (rotating parity) (default)
  RAID 6 (rotating dual parity)

  Note RAID 10 is also available by selecting RAID 1 (mirrored) and using an even number of drives, with a minimum of four.

  Note For more information on RAID levels, see Appendix A, "RAID Levels".

- **Select stripe size**: The default stripe size is **128Kbytes**. You can choose to use smaller stripes by selecting **64Kbytes**, **32Kbytes**, or **16Kbytes**.
- **Select array owner**: Select the RAID Controller that will be primarily responsible for accessing and monitoring this array. Choose **Controller 0** (the default) or **Controller 1**.
- **Online Create**: When this box is checked (the default), volumes on this array will be available immediately, with RAID creation continuing in the background. This does, however, slow down the RAID creation process. You can speed up the creation process by unchecking this box, in which case volumes will be unavailable until RAID creation is complete.
- **DiskN**: Select the check box beneath each disk that you wish to include in this array.

  Note On CPS-SS-4RU units, there is a section below the Create RAID Set button that allows you to select a section of disks all at once. On a CPS-SS-4RU unit, click the check box next to **Pod0/1/2 left pair** or **Pod0/1/2 right pair**, or any combination, then click **Refresh** page. The disks in the left half and/or right half of each selected active drive drawer are selected.

When you have entered all necessary information and selected the desired disks, click **Create RAID Set**. You are immediately taken to the Configure Logical Volume page (see Create a Logical Volume, page 7-1). The message "Array has been successfully configured" is displayed at the top of the page, along with an additional message:

- If you selected Online Create, the message displayed is "Performance will be degraded until verification is completed".
- If you did not select Online Create, the message displayed is "Volumes will not be accessible until initialisation is completed".

Note If at any time you wish to return the New RAID Configuration Tool to its initial state, click **Reset**.

The array construction process takes many hours, depending on how many disks are in the array and on whether you selected **Online Create** in the New Array Configuration tool. You can check the progress of array construction by clicking **RAID Information > Progress** (see RAID Array Utility Progress, page 4-3).

Rename RAID Arrays

Clicking **Configure RAID > Rename Array** takes you to the Rename RAID Arrays page. Each array is displayed in a separate section, which includes the Array name, Array number, RAID level, Number of members, array icon, array status, and array capacity. For information on these items, see RAID Array Information, page 4-1.

To rename one or more arrays, do the following:

Step 1 Enter the new name into the **Enter new name** field.

Note NOTE: If you leave one or more **Enter new name** fields blank, those arrays retain their previous names.

Step 2 Click **Save Settings**.

The arrays are immediately renamed.

Note If at any time you wish to return the Rename RAID Arrays page to its initial state, click **Reset**.

Delete a RAID Array

Clicking **Configure RAID > Delete Array** takes you to the Delete a RAID Array page. Each array is displayed in a separate section, which includes the Array name, Array number, RAID level, Number of members, array icon, array status, and array capacity. For information on these items, see RAID Array Information, page 4-1.

Note RAID arrays cannot be deleted if they contain volumes. If you try to delete an array that contains volumes, a message is displayed, telling you to delete the volumes first. See Delete a Logical Volume, page 7-3.

To delete a RAID array, do the following:

Step 1 Select the array you wish to delete by clicking the button next to the array icon.

Step 2 Click **Delete RAID Array**.

A confirmation page is displayed, asking you to confirm that you wish to delete the array.

Step 3 Do one of the following:

- To cancel the delete operation, click **CANCEL Delete**.
- To delete the array, click the confirmation check box, then click **Confirm Delete Command**.

A message is displayed, informing you that the array has been deleted. Click the **Back** button to go to the Home page.

RAID Array Ownership

Clicking **Configure RAID > Array Owner** takes you to the RAID Array Ownership page.

Each array is displayed in a separate section, which includes the Array name, Array number, RAID level, Number of members, array icon, and array capacity. For information on these items, see RAID Array Information, page 4-1.

Each section also displays **Controller *N*** selection buttons. The selected button indicates which controller the array is currently assigned to.

To assign an array to a different controller, do the following:

Step 1 Click the selection button next to the desired controller.

Step 2 Click **Save Changes**.

A message is displayed, informing you that the settings have been updated. Click the **Back** button to return to the RAID Array Ownership page.

Note Any conflicting LUNs will be set to “unmapped”.

Add Hot Spare

Clicking **Configure RAID > Add Spare** takes you to the Add Hot Spare page, which allows you to designated specific disk drives as “spares” which will be used to reconstruct RAID arrays when array disks fail.

Note If your Cisco Video Surveillance Storage System component has an attached expansion unit, you are first prompted to select which unit the new spare is in. Select the enclosure and click **Next** to be taken to the Add Hot Spare tool.

When you have selected the desired enclosure, or if your Cisco Video Surveillance Storage System is a single unit, the Add Hot Spare tool is displayed. The disks in the unit are represented in a similar fashion to the unit summary diagram on the Home page (see Home Page, page 3-2).

To designate an unused disk as a Pool Spare (a disk that can be used by any array in the unit), do the following:

Step 1 Next to **Add spare disk(s) to**, select **Enclosure** (this is the default).

Step 2 Select the check box beneath each disk that you wish to designate as a Pool Spare.

Step 3 Click the **Add Hot Spare** button.

A message is displayed, informing you that the new Pool Spares have been added.

Step 4 Click the **Back** button to return to the Add Hot Spare page.

To designate an unused disk as a Dedicated Spare (a disk that is assigned as a spare for a specific array), do the following:

Step 1 Next to **Add spare disk(s) to**, select the ***Array Name***.

Step 2 Select the check box beneath each disk that you wish to designate as a Dedicated Spare for that array.

Note All disks selected will be added to the same array, as selected in step 1. To add disks to multiple arrays, you must repeat steps 1 and 2 for each.

Step 3 Click the **Add Hot Spare** button.

A message is displayed, informing you that the new Dedicated Spares have been added.

Step 4 Click the **Back** button to return to the Add Hot Spare page.

The new spares now appear in the system diagram with a blue bar (see Single Storage Unit, page 3-2).

Note If at any time you wish to return the Add Hot Spare page to its initial state, click **Reset**.

Delete Hot Spare

Clicking **Configure RAID > Delete Spare** takes you to the Delete Hot Spares page, which allows you to remove the "spare" designation from a disk and return it to unused status.

Note If your Cisco Video Surveillance Storage System component has an attached expansion unit, you are first prompted to select which unit the spare is in. Select the enclosure and click **Next** to be taken to the Delete Hot Spares tool.

When you have selected the desired enclosure, or if your Cisco Video Surveillance Storage System is a single unit, the Delete Hot Spares tool is displayed. The disks in the unit are represented in a similar fashion to the unit summary diagram on the Home page (see Home Page, page 3-2).

To delete one or more spares, do the following:

Step 1 Click the check box below the spare or spares that you wish to return to the unused state.

Note On CPS-SS-4RU units, there is a section below the **Delete Hot Spare** button that allows you to select a section of disks all at once. On a CPS-SS-4RU unit, click the check box next to **Pod0/1/2 left pair** or **Pod0/1/2 right pair**, or any combination, then click **Refresh page**. All of the spare disks in the left half and/or right half of each selected active drive drawer are selected.

Step 2 Click **Delete Hot Spare**.

A message is displayed, informing you that the spares have been deleted and are now unassigned.

Step 3 Click the **Back** button to return to the Delete Hot Spares page.

Note If at any time you wish to return the Delete Hot Spares page to its initial state, click **Reset**.

Configure Hot Spare Mode

Clicking **Configure RAID > Spare Mode** takes you to the Configure Hot Spare Mode page.

To change the Hot Spare Mode setting, do the following:

Step 1 Select one of the two options:

- **Inserted disks automatically used as hot spares**: This is the default setting. New disk drives, when inserted into a drive slot and recognized by the system, are automatically configured as pool spares.
- **Inserted disks must be manually configured as hot spares**: When this setting is active, new disk drives are configured as unused disks which are available for use in a RAID array or as either pool or dedicated spares.

Step 2 Click **Set Spare Mode**.

A message is displayed, informing you that the setting has been updated.

Step 3 Click the **Back** button to return to the Set Hot Spare Mode page.

Lost Data/Bad Blocks

Clicking **Configure RAID > Lost Data** takes you to the Lost Data/Bad Blocks page. In RAID 0 arrays, data is lost if any of the component disks fail or develop errors. In RAID 1, RAID 4, and RAID 5 arrays, data is only lost if two or more component disks fail or develop errors simultaneously. In RAID 6 arrays, data is only lost if three or more component disks fail or develop errors simultaneously See Appendix A, "RAID Levels" for more information.

Click the **Acknowledge Lost Data Warning** button to acknowledge the warning. A message is displayed, confirming the acknowledgement. Click the **Back** button to return to the Lost Data/Bad Blocks page.

Note After acknowledging lost data, it is STRONGLY RECOMMENDED that you run an array verification immediately. See Verify RAID Arrays, page 10-5 for instructions.

Note NOTE: Lost data warnings also appear on the Home page and can be acknowledged from there (see Alarms and Warnings, page 3-4).

Acknowledge Rebuild

Clicking **Configure RAID > Rebuild Ack** takes you to the Acknowledge Rebuild page. When a RAID array has been rebuilt after a component disk failure, this page displays a warning and allows you to acknowledge that you have seen it.

Click the **Acknowledge RAID Array Reconstruction** button to acknowledge the rebuild. A message is displayed, confirming the acknowledgement. Click the **Back** button to return to the Acknowledge Rebuild page.

Note RAID array reconstruction warnings also appear on the Home page and can be acknowledged from there (see Alarms and Warnings, page 3-4).

RAID 6 Configuration

The default configuration of the hard drive bundle from the factory is RAID 5 set comprised of ten disk drives. To change the RAID 5 set to a RAID 6 set, perform the following steps using the GUI:

Procedure

Step 1 Identify the RAID 5 set to be modified and delete it.

Step 2 Select a set of ten unconfigured disk drives.

Step 3 Create RAID 6 set using the ten drives. Leave the default stripe size.

Step 4 Create a single LUN inside the new RAID 6 set.

Step 5 Expose the new LUN through the external interfaces by selecting a unique LUN ID number.

Step 6 (Optional) Repeat Steps 1 to 5 to change additional RAID 5 sets to RAID 6 sets.

CHAPTER 7

Volume Configuration

When you click the **Configure Volumes** button in the navigation pane, you are taken to the Create a Logical Volume page. The navigation bar across the top contains links to this section's subpages.

- **Add Volume** links to Create a Logical Volume
- **Expand Volume** links to Expand a Logical Volume
- **Delete Volume** links to Delete a Logical Volume
- **Rename Volume** links to Rename Logical Volumes
- **Map Volume** links to Map Logical Volumes

Create a Logical Volume

Clicking **Configure Volume** takes you to the Create a Logical Volume page, which allows you to create logical volumes that act like disk partitions on RAID arrays in your system.

To add a new volume, do the following:

Step 1 Select an array and click the **Next** button to be taken to the volume creation tool.

Step 2 Enter the following information:

- **Enter the name for the new volume**: If this is the first volume configured for this array, then the name defaults to the name of the array. If there are already volumes on the array, then the name is blank. Enter a name for the volume. This can be up to 63 characters long.
- **Enter the size of the new volume in *X***: The value of this field defaults to all of the remaining space left on the array. The units defaults to true gigabytes (GB), but this can be changed using the **Change Units** button. Enter the desired size of the new volume.
- **Limit volume size to less than 2TB**: This option is unchecked by default. If your hosts do not support volumes of more than 2 terabytes (TB) in size, check this option.

Note If you select this option, the value entered in **Enter the size of the new volume in *X*** must not exceed 2TB, or else the volume will not be built and an error message will appear.

Step 3 When you have entered all of the required information, click **Create Volume**.

A message is displayed, informing you that the volume as been created, and you are prompted to assign a logical unit number (LUN) and host port access.

Step 4 In the Volume LUN Mapping section, assign a logical unit number (LUN) for each port that the volume will be accessed through. Check the **Use same LUN for all ports of the same type** check box to have all Fibre Channel, SAS-to-Host, 10GbE, or iSCSI ports use the same LUN mapping.

Note SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher.

Step 5 Set the **Default Access** (applied to new or unknown hosts) by selecting **Deny**, **Read**, or **R/W**:

- Select **Deny** to prevent all new or unknown hosts from accessing the volume. This is the default setting.

Note It is recommended to leave the **Default Access** setting as **Deny** and then grant access to specific hosts as necessary. This prevents unconfigured hosts from modifying existing data.

- Select **Read** to allow read-only access to the volume for all new or unknown hosts.
- Select **R/W** to allow read/write access to the volume for all new or unknown hosts.

Step 6 If at least one host group has been created (see Manage Host Groups, page 8-2), set the **Group Default** by checking or unchecking the box in the **Use Default** column:

- If **Use Default** is checked, this setting is the same as **Default Access**. This is the default setting.
- If **Use Default** is unchecked, this setting overrides the **Default Access** setting. You can select **Deny**, **Read**, or **R/W** as the default for all host groups.

Step 7 Set access privileges for individual hosts by checking or unchecking the box in the **Use Default** column:

- If **Use Default** is checked, the host or host group will use the **Group Default** setting (if the host is part of a group) or the **Default Access** setting (if the host is not part of a group). This is the default setting.
- If **Use Default** is unchecked, this setting overrides the **Group Default** and **Default Access** settings. Select **Deny**, **Read**, or **R/W** to set the access privileges for the specific host.

Step 8 When you have finished assigning host access privileges, click **Apply Changes**.

A message is displayed, indicating that the settings have been saved.

Note If at any time you wish to return the volume mapping page to its initial state, click **Reset**.

Note For more information about host access, see Chapter 8, “Host Access Configuration”.

Expand a Logical Volume

Clicking **Configure Volume > Expand Volume** takes you to the Expand a Logical Volume page. This page lists each array in the system and all volumes in each array. Scroll down to see all arrays and volumes.

The array information section lists the array name, array number, array owner, enclosure, and total capacity. See RAID Array Information, page 4-1 for more information.

If there is free space on the array, this section displays the total amount of space taken up by existing volumes, plus the percentage of the array's total capacity used. If there is no space on the array, a message to that effect is displayed.

Each volume's information section lists the volume ID, array name, volume name, volume capacity, the percentage of the array that the volume uses, the number of bad blocks, the volume serial number, the date that the volume was created, and a link to the logical unit number (LUN) mapping information (see Map Logical Volumes, page 7-4).

To expand a volume, do the following:

Step 1 Enter a new volume size in true gigabytes (GB) in the **GB** field.

Step 2 Click **Expand Volume**.

A confirmation screen is displayed.

Step 3 Do one of the following:

- To cancel the volume expansion, click **CANCEL Expand**.

  A message is displayed, stating that the operation has been cancelled.

- To proceed with the volume expansion, check the confirmation check box and click **Confirm Expand Command**.

  A message is displayed, confirming that the volume has been expanded.

Step 4 Click the **Back** button to return to the Expand a Logical Volume page.

Delete a Logical Volume

Clicking **Configure Volume > Delete Volume** takes you to the Delete a Logical Volume page. This page lists each array in the system and all volumes in each array. Scroll down to see all arrays and volumes.

The array information section lists the array name, array number, array owner, enclosure, and total capacity. See RAID Array Information, page 4-1 for more information. If there is free space on the array, this section displays the total amount of space taken up by existing volumes, plus the percentage of the array's total capacity used.

Each volume's information section lists the volume ID, array name, volume name, volume capacity, the percentage of the array that the volume uses, the number of bad blocks, the volume serial number, the date that the volume was created, and a link to the logical unit number (LUN) mapping information (see Map Logical Volumes, page 7-4).

To delete a volume, do the following:

Step 1 Click the **Delete Volume** button in the volume's information area.

A confirmation screen is displayed.

Step 2 Do one of the following:

- To cancel the volume deletion, click the **CANCEL Delete** button.

A message is displayed, stating that the operation has been cancelled.

- To delete the volume, click the confirmation check box and then click **Confirm Delete Command**.

  A message is displayed, confirming that the volume has been deleted.

Step 3 Click the **Back** button to return to the Delete a Logical Volume page.

Rename Logical Volumes

Clicking **Configure Volume > Rename Volume** takes you to the Rename Logical Volumes page.

Each volume information section lists the volume number, current volume name, the array the volume belongs to, the controller that the array is assigned to, the enclosure, the volume's capacity, and the volumes host port assignments (see Configured Logical Volumes, page 4-3).

To rename a volume, do the following:

Step 1 Enter the new volume name in the **New Name** field (default is the current volume name).

Step 2 Click **Save Settings**.

Note If at any time you wish to return the Rename Logical Volumes page to its initial state, click **Reset**.

Map Logical Volumes

Clicking **Configure Volumes > Map Volume** takes you to the Map Logical Volumes page.

Each volume information section lists the volume number, current volume name, the array the volume belongs to, the controller that the array is assigned to, the enclosure, the volume's capacity, and the volumes host port assignments (see Configured Logical Volumes, page 4-3).

Caution Changes are made immediately. Changing the LUN of a volume in use could cause your Operating System to crash or lose communication with the volume.

To map a volume to a logical unit number (LUN), do the following:

Step 1 Click the **Next** button next to the volume you wish to map.

The volume mapping tools are displayed.

Step 2 In the Volume LUN Mapping section, assign a logical unit number (LUN) for each port that the volume will be accessed through. Check the **Use same LUN for all ports of the same type** check box to have all Fibre Channel, SAS-to-Host, 10GbE, or iSCSI ports use the same LUN mapping.

Note SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher.

Step 3 Set the **Default Access** (applied to new or unknown hosts) by selecting **Deny**, **Read**, or **R/W**:

- Select **Deny** to prevent all new or unknown hosts from accessing the volume. This is the default setting.

Note NOTE: It is recommended to leave the **Default Access** setting as **Deny** and then grant access to specific hosts as necessary. This prevents unconfigured hosts from modifying existing data.

- Select **Read** to allow read-only access to the volume for all new or unknown hosts.
- Select **R/W** to allow read/write access to the volume for all new or unknown hosts.

Step 4 If at least one host group has been created (see Manage Host Groups, page 8-2), set the **Group Default** by checking or unchecking the box in the **Use Default** column:

- If **Use Default** is checked, this setting is the same as **Default Access**. This is the default setting.
- If **Use Default** is unchecked, this setting overrides the **Default Access** setting. You can select **Deny**, **Read**, or **R/W** as the default for all host groups.

Step 5 Set access privileges for individual hosts by checking or unchecking the box in the **Use Default** column:

- If **Use Default** is checked, the host or host group will use the **Group Default** setting (if the host is part of a group) or the **Default Access** setting (if the host is not part of a group). This is the default setting.
- If **Use Default** is unchecked, this setting overrides the **Group Default** and **Default Access** settings. Select **Deny**, **Read**, or **R/W** to set the access privileges for the specific host.

Step 6 When you have finished assigning host access privileges, click **Apply Changes**.

A message is displayed, indicating that the settings have been saved.

Note If at any time you wish to return the Map Logical Volumes page to its initial state, click **Reset**.

Note For more information about host access, see Chapter 8, “Host Access Configuration”.

CHAPTER 8

Host Access Configuration

When you click the **Configure Host Access** button in the navigation pane, you are taken to the Configure Fibre page. The navigation bar across the top contains links to this section's subpages.

- **Fibre** links to Configure Fibre Channel Host Access
- **Groups** links to Manage Host Groups
- **Hosts** links to Manage Hosts
- **Access** links to Host Access

Note On units configured for SAS-to-Host, the **Fibre** tab is replaced by a **SAS** tab, which links to Configure SAS Host Access.

Note SAS drives are not supported with the Cisco Video Surveillance Storage System. iSCSI is supported on Cisco Video Surveillance Systems (VSM) deployed as a Virtual Machine for VSM releases 7.2 or higher.

Note On units configured for 10Gb Ethernet iSCSI, the **Fibre** tab is replaced by a **10Ge** tab which links to Configure 10GbE iSCSI Host Access.

Configure Fibre Channel Host Access

Clicking **Configure Host Access** takes you to the Configure Fibre page, which allows you to change settings for each Fibre Channel host port on each RAID Controller.

OnCPS-SS-4RU units, the current status is shown in the **Current status** row.

The information is arranged by Controller and then by host port:

- **Current Status**: On CPS-SS-4RU units, lists the link status (up or down), link speed, and topology.
- **Topology**: The Fibre Channel topology, either Loop or Point-to-Point. Select **Loop**, **Point-to-point**, or **AUTO** (the default).
- **Loop ID**: The loop address if the port is in loop mode. Select an ID number from **0** to **126**, or **AUTO** (the default).
- **Link speed**: The Fibre Channel link speed in gigabits per second (Gb/s). Select **2Gbit**, **4Gbit**, **8Gbit**, or **AUTO** (the default).

- **Frame size**: The data payload size of each packet. Select **512**, **1024**, **2048** (the default), or **2112**.
- **Host port cleanup**: This option is only used in full-fabric topologies where RSCN notification in enabled on the connected Fibre switch. Select **No** if you are not using a full-fabric topology or if RSCN notification is disabled. Select **Yes** if you are using a full-fabric topology with RSCN notification.

Note RSCN notification is a switch function which can inform other devices on the FC fabric that a host has been disconnected without logging off. When **Yes** is selected for this setting, the Cisco storage unit registers with the switch to receive RSCN notifications; upon being notified that a host has disconnected, it immediately logs that host off and updates the status of the host to indicate that it is offline. When **No** is selected, the Cisco Video Surveillance Storage System unit receives no notification of hosts that go offline without logging off; disconnected hosts can still show as being connected to the Cisco storage unit.

When you have selected the desired new settings, do one of the following:

- Click **Save Configuration**. The settings are saved and are applied after the system is restarted (see Reboot System, page 10-3).
- Click **Save and Apply Changes**. The settings are saved and applied immediately.

Note If at any time you wish to return the Configure Fibre page to its initial state, click **Reset**.

Manage Host Groups

Clicking **Configure Host Access > Groups** takes you to the Manage Groups page, which allows you to create access control groups. Access control groups provide a set of hosts with common access rights.

To add an access control group, do the following:

Step 1 Click the **Add Group** button.

The new group is displayed as a new line in the group list.

Step 2 Under **Group Name**, edit the default name if you wish, then press **Apply changes**.

Step 3 To add hosts to the list, click the **Edit hosts** link.

A list of hosts is displayed.

Step 4 For each host you want to include in the group, click the **Include** check box.

Step 5 Click **Apply changes**.

A message is displayed, informing you that the host group settings have been updated.

Step 6 Click the **Back** button to return to the Manage Groups page.

Note If at any time you wish to return the Manage Groups page to its initial state, click **Reset**.

Manage Hosts

Clicking **Configure Host Access > Hosts** takes you to the Manage Hosts page, which lets you add, rename, remove, and configure settings for host groups and individual hosts.

- The **Host Name** field, which defaults to the host's address, can be edited to give the host a "friendly" name.
- The **Remove** check box can be checked to remove unconnected hosts (designated by a gray icon under Type) that are no longer relevant.

After changing the **Host Name** or checking a **Remove** check box, click **Apply changes**.

Further information about each host is available by clicking the **Details** link. **Group Membership** can be changed by clicking a button next to a group name and clicking **Apply changes**.

Note If at any time you wish to return the Manage Hosts page to its initial state, click **Reset**.

Host Access

Clicking **Configure Host Access > Access** takes you to the Host Access page, which lets you configure volume access to specific hosts. It also lets you set the defaults for group host access and all host access.

The host access links are arranged in order, starting with Default Access, then each Group and its hosts, and then any hosts that are not in a group.

The Default Access setting controls access by new or unknown hosts. The Group Default setting applies to host groups and overrides the Default Access setting. If you click the **Access** link for Default Access or for Group Default under a group name, you are presented with three columns for each volume on the unit: **Deny**, **Read**, and **R/W**.

Settings for individual hosts override the Default Access and Group Default settings. Each **Access** link takes you to the host access configuration page for that host or category. If you click the **Access** link for a specific host, you are presented with four columns for each volume on the unit: **Default**, **Deny**, **Read**, and **R/W**.

To change host access settings, do the following:

Step 1 For each listed Volume, select **Default** (for a specific host), **Deny**, **Read**, or **R/W** access.

Step 2 When you have set the desired access privilege for the host or the desired default access privilege, click **Apply Changes**.

A message is displayed, informing you that the settings have been updated.

Step 3 Click the **Back** button to return to the Host Access page.

Note If at any time you wish to return the Host Access page to its initial state, click **Reset**.

CHAPTER 9

Power Settings

When you click the **Power Settings** button in the navigation pane, you are taken to the AutoMAID Statistics page. The navigation bar across the top contains links to this section's subpages.

- **AutoMAID Statistics** links to AutoMAID Statistics
- **AutoMAID Config** links to Configure AutoMAID Settings

AutoMAID Statistics

Clicking **Power Settings** takes you to the AutoMAID Statistics page, which shows you details about the disk drives' AutoMAID power savings. For more information about AutoMAID, see Appendix B, "AutoMAID".

The AutoMAID Statistics page reports power savings over the past 96 hours. The exact reporting period is shown above the **Clear Statistics** button. The statistics listed are:

- **Array name**: The name of each array in the unit, plus a row for unused and spare disks. There is also a **Total** line that summarizes statistics across all disk drives.

  Note This list can include names of arrays that no longer exist, but did exist at any time during the reporting period.

- **Disk Time at MAID Level**: The percentage of time during the reporting period that the drives in each array or category have been at the specified AutoMAID level:
  - **Active**: The percentage of time that the drives have been active and at full power.
  - **Idle**: The percentage of time that the drives' read/write heads have been parked (AutoMAID level 1).
  - **Slow**: The percentage of time that the drives' disk platters have been spun down to a slower speed (AutoMAID level 2).
  - **Stopped**: The percentage of time that the drives' disk platters have been spun down completely (AutoMAID level 3).
  - **Off**: The percentage of time that the drives' electronics have been completely powered down (AutoMAID level 4).

  Note Not all disk drives support AutoMAID levels 1, 2, or 4.

- **AutoMAID Efficiency**: Displays the percentage of maximum efficiency that the drives in each array or category have achieved. If all drives were Off for the entire reporting period, this number is 100%.

Note NOTE: An AutoMAID Efficiency percentage of 100% does NOT mean that no energy is being used, just that the maximum efficiency level has been achieved.

You can clear the statistics for the reporting period by clicking the **Clear Statistics** button. The AutoMAID statistics for the past 96 hours are cleared, and new statistics are recorded beginning immediately.

Configure AutoMAID Settings

Clicking **Power Settings > AutoMAID Config** takes you to the Configure AutoMAID Settings page, which allows you to specify when disk drives should enter each AutoMAID level. It also lets you specify times and days of the week when AutoMAID is disabled in order to maximize data accessibility. For more information about AutoMAID, see Appendix B, "AutoMAID".

There are three sections: Default RAID Array AutoMAID Settings, Default Pool Spares/Unassigned AutoMAID Settings, and RAID Array Specific Settings.

Default RAID Array AutoMAID Settings controls the default AutoMAID settings for all disk drives assigned as array members or dedicated array spares. There is one row for each AutoMAID level, and each row has four columns:

- **Power Level**: Displays each AutoMAID level: Level 1 (parked heads), Level 2 (slow disk rotation), Level 3 (stopped disk rotation), and Level 4 (drives powered off).
- **Current Setting**: Displays the amount of time that the system is currently set to wait before activating that AutoMAID level.
- **New Setting**: Displays drop-down lists with the possible settings for each AutoMAID level:
  - Level 1: **never** (the default), **2 mins**, or **5 mins**.
  - Level 2: **never** (the default), **10 mins**, **20 mins**, **30 mins**, **40 mins**, **50 mins**, or **60 mins**.
  - Level 3: **never** (the default), **15 mins**, **30 mins**, **1 hr**, **1.5 hrs**, or **2 hrs**.
  - Level 4: **never** (the default), **20 mins**, **30 mins**, **1 hr**, **1.5 hrs**, or **2 hrs**.

Note Any AutoMAID levels set to **never** will be ignored by the system.

Note If any drives are set to use AutoMAID Level 3 or 4, host timeout values (set for the host HBA either through the HBA BIOS or a management application) should be set to a default of between 120 and 150 seconds to avoid the host requests timing out before the disk drives can power on and spin up to full speed.

- **Supported by**: Displays the number of disk drives out of the total that support each AutoMAID level.

Note Disk drives that do not support a specific AutoMAID level will stay at a previous, usable level until the system reaches an AutoMAID level that drive supports.

AUTOMaid can be scheduled using the following settings:

- **AutoMAID Schedule**: Check the check box to disable AutoMAID during critical hours when high data accessibility is required.
- **Critical hours**: Use this section to schedule the critical hours during which AutoMAID will be disabled. Use the drop-down lists to select the beginning and ending time, and use the check boxes to select specific days of the week.

Default Pool Spares/Unassigned AutoMAID Settings controls the AutoMAID settings for all pool spare (but not dedicated spare) disks and all disks that are currently unassigned as either spares or array members.

- **Pool Spares/Unassigned**: Use the drop-down list to select the AutoMAID level you wish pool spares and unassigned disks to go to:
  - **Never** (the default)
  - **Level 1 — Park heads after 2 minutes**
  - **Level 2 — Reduce disk speed after 10 minutes**
  - **Level 3 — Stop disks spinning after 15 minutes**
  - **Level 4 — Power off disks after 20 minutes**

After you have made your selections in both the Default RAID Array AutoMAID Settings section and the Default Pool Spares/Unassigned AutoMAID Settings section, click the **Save Settings** button. A message is displayed, informing you that the settings have been changed. Click the **Back** button to return to the Configure AutoMAID Settings page.

In the RAID Array Specific Settings section, the default setting is **Default**. Click the **Customize** link to set AutoMAID settings for an individual array. Choose the settings in this section exactly as you would in the Default RAID Array AutoMAID Settings section, then click **Save Current Settings**. A message is displayed, informing you that the new power settings have been saved.

If you wish to return an array to default settings, click **Reset Default Settings**. A message is displayed, informing you that the new power settings have been saved.

CHAPTER 10

System Administration

When you click the **System Admin** button in the navigation pane, you are taken to the Configure Cache page. The navigation bar across the top contains links to this section's subpages.

- **Cache** links to Configure Cache
- **Alarm** links to Audible Alarm
- **Enclosure Config** links to Configure Enclosures
- **Reboot** links to Reboot System
- **Rebuild Rate** links to Configure Rebuild Priority
- **Verify Config** links to Verify RAID Arrays
- **System Mode** links to System Mode
- **Settings** links to Download/Upload System Settings
- **Update Firmware** links to Update Firmware

Configure Cache

Clicking **System Admin** takes you to the Configure Cache page, which allows you to configure settings for the unit's cache memory.

Cache memory holds data that is being written to one or more disks, which enables the RAID Controller to confirm that a command has been completed before the data has been written to disk.

In the event of a power interruption during an unfinished write operation, the cache memory has a battery backup which allows the cache to hold data for up to 72 hours. When the power is restored to the unit, the RAID Controller will automatically complete any write operations using the data held in the cache.

The Configure Cache page displays the current cache settings and lets you configure them:

- **Current write cache state**: Shows whether the cache is currently enabled or disabled, mirrored, and in streaming mode, plus its "force unit access" (FUA) status and the size of the cache in megabytes (MB) for each RAID Controller.
- Manually override current write cache status: Normally, when the cache is enabled or disabled, the unit must be rebooted for it to take effect. Using this check box, you can force the cache to become Enabled (if it is disabled) or Disabled (if it is enabled) without rebooting the system.
- Desired write cache state: By default, this is **Enabled**. Select the desired setting (**Enabled** or **Disabled**).

- **Allow attached host to override write cache configuration**: Some hosts can issue commands that force the cache to not be used. To allow this, check this check box. To prevent it, leave the box unchecked (the default setting).
- **Ignore force unit access (FUA) bit**: Some SCSI commands contain a "force unit access" (FUA) bit, which forces the unit to bypass cache memory and perform read and write operations directly from and to the disks. Check this check box to ignore the FUA bit and always use the cache memory for command execution. Uncheck it (the default setting) to allow the FUA bit to bypass cache memory.
- **Enable cache mirroring**: On Cisco Video Surveillance Storage System components in a dual-controller active-active failover mode (see System Mode, page 10-6), this setting is enabled by default. It tells the system to duplicate the contents of the cache of one RAID Controller to the other, thus ensuring that cache contents are not lost in the event of a controller failure. Uncheck the box to disable cache mirroring (not recommended).

Caution If cache mirroring is turned off, data stored in the write cache may be lost if a RAID Controller fails.

- **Write/Read cache streaming mode**: When the cache streaming mode is active, the system continuously flushes the cache memory, which provides maximum cache buffering to protect against delayed command responses. When the streaming mode is not active, the system runs with a full cache, which helps reduce disk access and maximizes random I/O performance.

  Check this box to activate streaming mode. Uncheck it (the default) to deactivate streaming mode.
- **Cache optimization setting**: Select the cache setting that fits the kind of data and method of data access that your system uses most often:
  - **Random access**: This setting is best for systems that access a large number of files or many different areas of its volumes, such as systems with many individual users or that house frequently accessed databases.
  - **Mixed sequential/random** (default): This setting is best for systems that are "mixed use", sometimes accessing many smaller files and sometimes accessing a few larger files.
  - **Sequential access**: This setting is best for systems that access a small number of large files sequentially, such as an archive of manuscripts or videos.

  This setting can be changed in real-time. We encourage you to experiment with this setting to determine which configuration works best for your environment.

When you have selected the desired settings, click the **Save settings** button. A message is displayed, informing you that the settings have been updated. Click the **Back** button to be returned to the Configure Cache page.

Note If at any time you wish to return the Configure Cache page to its initial state, click **Reset**.

Audible Alarm

Clicking **System Admin > Alarm** takes you to the Audible Alarm page, which allows you to silence or sound the audible alarm on the unit.

If the alarm is sounding, click **Silence the Audible Alarm** to silence the alarm. (To find out why the alarm is sounding, click the notification in the upper right corner to be taken to the Problem Summary page. See Summary of System Problems, page 5-7 for more information.)

Note If further problems occur, the audible alarm will sound again.

If the alarm is not sounding, click **Re-Sound the Audible Alarm** to sound the alarm (if a problem is present—see Summary of System Problems, page 5-7).

Configure Enclosures

Clicking **System Admin > Enclosures Config** takes you to the Configure Enclosures page, which allows you to name each unit in your storage system.

To change the name of a unit, enter the new name in the **Friendly Name** field and click **Submit**. A message is displayed, informing you that the new name is saved. Click the **Back** button to return to the Configure Enclosures page.

Clicking the **Beacon** button causes the LEDs on the front of the unit to flash for one minute. This can help in locating a specific unit in a large installation where multiple Cisco Video Surveillance Storage System components are located.

Reboot System

Clicking **System Admin > Reboot** takes you to the Reboot System page, which enables you to restart or shut down the system.

Reboot RAID

The Reboot RAID System section has three options:

- **Rolling Restart**: For dual-controller units with certain configurations, this allows you to restart the RAID Controllers without losing host connectivity or data transfer capability. During a rolling restart, each RAID Controller reboots individually.

  For a rolling restart to be performed, both RAID Controllers must be fully operational and have the same firmware version (see Update Firmware, page 10-9), and the system must be in mode that supports controller failover (Active-Active or All Ports All LUNs—see System Mode, page 10-6). If one or more of these conditions is not met, the **Rolling Restart** option is grayed out.

  Note In order to avoid host connection timeout during a rolling restart, disk timeouts for all hardware and virtual servers should be set to 150 seconds.

  Note On single-controller units, this option does not appear.

- **System Reboot** (default): This option executes a full restart of the system. While the system is rebooting, the unit is offline, and arrays and volumes are inaccessible. Therefore, hosts should be safely shut down or disconnected before performing a System Reboot. After the system has finished rebooting, the arrays and volumes are once again accessible.

- **System Shutdown**: This option flushes the cache data to the disks and shuts down the system. Therefore, hosts should be safely shut down or disconnected before performing a System Shutdown. System Shutdown does NOT turn the system completely off; the power supply units (PSUs) are still active, and fans may still run. To completely power off the system, or to bring the system back on line after a shutdown, follow the instructions in the system's Hardware Manual.

To perform a reboot or shutdown:

Step 1 Select the desired reboot option.

Step 2 Check the confirmation box.

Step 3 Click **Execute NOW** to reboot the system.

A message is displayed, informing you that the reboot or shutdown sequence is in progress.

Step 4 When the unit is back online, click the **Back** button to return to the Reboot System page.

Note While a rolling restart or reboot operation is in progress, the system status icon may indicate a FAILURE. The FAILURE message will clear once the system is fully restarted.

Controller Maintenance

The Controller Maintenance section allows you to take a RAID Controller offline for maintenance or diagnostic purposes. It also allows you to test failover settings (see System Mode, page 10-6) before deploying the system into your production environment. The RAID Controller that is currently being used to access the Cisco Video Surveillance Storage System Management Console is noted by the text "(current)" after it.

Note Taking the "current" RAID Controller offline can cause the Management Console to become unresponsive for up to a minute as the host connections are passed to the other controller.

To take a RAID Controller offline:

Step 1 Select the RAID Controller to be taken offline.

Step 2 Check the confirmation box.

Step 3 Click **Execute NOW**.

The selected RAID Controller is taken offline, and control of the arrays is passed to the other RAID Controller (if the unit has two controllers and is in an Active-Active or All Ports All LUNs mode—see System Mode, page 10-6).

Step 4 Click the **Back** button to be returned to the Reboot System page.

To re-enable the RAID Controller:

Step 1 Click the button next to **Re-enable controller *N***.

Step 2 Check the confirmation box.

Step 3 Click **Execute NOW**.

The RAID Controller is put back on line.

Step 4 Click the **Back** button to return to the Reboot System page.

Power Restoration Policy

On CPS-SS-4RU units, the Power Restoration Policy section controls how the unit behaves after A/C power has been restored after an interruption (due to power failure or the removal of the power cords).

- **Boot immediately after power is restored**: After power is restored, the unit automatically starts up. This is the default setting.
- **Remain unpowered until the controller push-switch (SW0) is pressed**: After power is restored, the unit will not start up until the **SW0** switch on either RAID Controller is pressed. This switch must be pressed for approximately 4 seconds to start the unit, then released as soon as the unit begins to power up.

Select the desired power restoration policy and click **Save Configuration**. A message is displayed, informing you that the settings has been saved. Click the **Back** button to return to the Reboot System page.

Configure Rebuild Priority

Clicking **System Admin > Rebuild Rate** takes you to the Configure Rebuild Priority page, which lets you customize the amount of system I/O time dedicated to rebuilding critical arrays.

There are five rebuild rates, arranged from **Lowest** to **Highest**. The default setting is **Medium**.

When there is high host activity, less spare I/O time is available, which can result in longer rebuild times. In this situation, it may become necessary to increase the rebuild priority so that arrays are rebuilt more quickly.

Select the desired rebuild rate and click **Set Rebuild Priority**. A message is displayed, informing you that the setting has been saved. Click the **Back** button to return to the Configure Rebuild Priority page.

Caution Your data is vulnerable while an array is critical. Depending on RAID level, any further disk failures could mean your data becomes unavailable to your host.

Verify RAID Arrays

Clicking **System Admin > Verify Config** takes you to the RAID Array Verify page, which lets you configure the method and frequency of RAID array verification.

Schedule RAID Array Verification

To set up a RAID array verification schedule, configure the following settings:

- **Select verify utility to use**: There are two different verification utilities available: **Surface scan** and **Parity scrub**.
  - **Surface scan** (default) reads all blocks on each disk drive in the array to ensure their integrity. If it encounters a bad block, it will quarantine that block and rebuild it using mirrored data (for RAID 1 or 10) or parity data (for RAID 4, 5 or 6).

    Note NOTE: If bad data blocks occur on arrays configured as RAID 0, Surface scan will not be able to rebuild the data.

  - **Parity scrub** (available for RAID 4, 5, and 6) reads all array data and ensures that the parity data is intact. If it encounters a parity inconsistency, it will correct the inconsistency. **Parity scrub** also rebuilds bad data blocks in a similar fashion to **Surface scan**.

  If you do not wish RAID array verification to be scheduled, select **None**.
- **Verify interval**: This settings tells the unit how often to automatically run the selected verification utility. You can select **1 week** (the default), **2 weeks**, or **4 weeks**.
- **Verify schedule**: Use the drop-down lists to select the day of the week and the time of day to begin running the selected verification utility. This allows you to schedule the verification for a time when data activity is low.

When you have configured the verification schedule, click **Save Settings**. A message is displayed, informing you that the settings have been updated. Click the **Back** button to return to the RAID Array Verify page.

When a verification utility is running, you can check its progress on the RAID Array Utility Progress page (see RAID Array Utility Progress, page 4-3).

Start or Stop RAID Array Verification Immediately

- To perform a RAID array verification immediately, select the verification tool (**Surface scan** or **Parity scrub**) and click **Execute verify utility NOW**. A message is displayed, informing you that the verification utility will begin shortly. Click the **Back** button to return to the RAID Array Verify page.

  Progress can monitored on the RAID Array Utility Progress page (see RAID Array Utility Progress, page 4-3).
- To stop a RAID array verification in progress (for instance, if it is negatively impacting host I/O performance), click the **Stop Verification** button. A message is displayed, informing you that the verification will soon be stopped. Click the **Back** button to return to the RAID Array Verify page.

System Mode

Clicking **System Admin > System Mode** takes you to the System Mode page, where you can configure the failover mode for the unit.

"Failover" is the term used for when one RAID Controller takes over the host connections and array control of the other RAID Controller when that controller fails. There are several ways to implement failover, depending on whether the storage area network (SAN) uses switches, multiple host ports, and/or hostbased multipathing software.

Caution If the unit is in Single Controller or Dual Controller Non-Redundant (DCNR) mode, or if cache mirroring is not enabled (see Configure Cache, page 10-1), data stored in the write cache may be lost if a RAID Controller fails.

Note If the System Mode is changed, volumes may become temporarily inaccessible. If this occurs, you must remap them (see Map Logical Volumes, page 7-4).

The possible settings for System Mode are:

- **Single Controller mode** (default): In this mode, only one RAID Controller is active, and failure of this controller makes all arrays and volumes inaccessible. This is the only possible setting on single-controller units, but it is possible to set a dual-controller unit to Single Controller mode.
- **Dual Controller Non-Redundant mode (DCNR)**: In this mode, both controllers are active, but each controller operates as an independent node, and all ports are independent from each other. Volumes can only be mapped to ports on the controller that owns the array. They become inaccessible if the controller fails.

  Note NOTE: Although DCNR mode does not allow failover, overall system performance may increase slightly.

- **2-port Active-Active mode (2 ports active)**: In this mode, each controller operates as an independent node, but only one port is active on each controller. The second port operates in passive mode. Port **0** is active on controller 0, and port **1** is active on controller 1. Volumes are mapped to the active port on their owning controller. When one controller fails, the passive port on the other controller activates and takes over the host port functions of the failed controller. In a switched environment, failover is completely transparent to the hosts. This mode is suitable for customers who want to be able to handle controller failover, but do not have multipathing software.

  Note For failover to occur, hosts must be connected to the same numbered port on both controllers.

  Note iSCSI connections (1Gb/s and 10Gb/s) do not failover in this mode. Should a controller fail, volumes accessed through an iSCSI network will become inaccessible. To configure failover for iSCSI, use **All Ports All LUNs mode**.

- **4-port Active-Active mode (4 ports active)**: In this mode, each controller operates as an independent node, and all ports are active. Port **0** is the primary port on controller 0, and port **1** is the primary port on controller 1. Volumes must be mapped to at least one port on its owning controller and to the secondary port on the other controller. When one controller fails, the secondary port on the other controller takes on the host address of the primary port on the failed controller, allowing host I/O to continue; the host sees the storage become active through its second path.

  Note For failover to occur, hosts to be connected to both ports on their owning controller and to the secondary port on the other controller.

Note If a host is connected to both ports on any one controller, the host must be running multipathing software.

Note iSCSI connections (1Gb/s and 10Gb/s) do not failover in this mode. Should a controller fail, volumes accessed through an iSCSI network will become inaccessible. To configure failover for iSCSI, use **All Ports All LUNs mode**.

- **All Ports All LUNs mode (all ports active)**: In this mode, the entire system operates as a single node. Volumes can be mapped to any or all ports on both controllers. When a controller fails, the ports on that controller become inaccessible. However, if the volumes are mapped to ports on the other controller as well, they remain accessible to the host, which sees the storage become active through its second path.

  Note For hosts to continue to have access to the LUNs after a controller failure or during a rolling restart, each volume should be mapped to at least one port on each controller (see Map Logical Volumes, page 7-4) and each host must have an active path to at least one port on each controller. Volumes mapped to only one controller become inaccessible if that controller fails or if a rolling restart is executed.

  Note Because this mode presents up to eight paths to configured volumes, the host must be running multipathing software.

  Note This is the only mode in which redundancy is available for all network types (Fibre Channel, SAS, 10GbE iSCSI, and 1GbE iSCSI).

Select the desired System Mode and click **Save System Mode**. A message is displayed, informing you that the setting has been saved.

When the setting is saved, click **System Admin > Reboot** and perform a **System Reboot** (see Reboot System, page 10-3).

Note If the System Mode setting is changed, but the system is not rebooted, the new mode will not take effect until the unit is next rebooted.

Note NOTE: If the System Mode is changed, volume mappings may also change. Always check the volume mappings (see Configured Logical Volumes, page 4-3) after changing the System Mode.

Download/Upload System Settings

Clicking **System Admin > Settings** takes you to the Download & Upload System Settings page, where you can download a file with the current controller settings or upload a new controller settings file to the system.

Caution Because improper or incorrect settings in the settings file can prevent the unit from being accessible on the network, *always* verify the contents of a settings.dat file—both manually (by opening it as a text file) and by using the **Verify Settings File** button—before uploading and installing it.

To download the current settings.dat file, click the **Click to download controller settings** link and save the file to your computer according to the method of your operating system.

To upload a new settings.dat file to the system, do the following:

Step 1 Click **Browse** and navigate to the file according to the method of your operating system. (If you select a wrong file, click **Clear Selection** and try again.)

Step 2 When the file's path is displayed in the **Select file** field, click **Verify Settings File** to validate the settings.dat file.

Note If you wish to see more detail, check the **Advanced debugging mode** check box before clicking **Verify Settings File**.

A Settings File Processing Report is displayed. Errors are shown in red text.

Step 3 If there are errors, fix them in the settings.dat file and repeat Step 1.

Step 4 Click **Upload and Install Settings**.

The settings.dat file is automatically installed, although some settings will only take effect after a system restart (see Reboot System, page 10-3).

Update Firmware

Clicking **System Admin > Update Firmware** takes you to the Update Firmware page, which allows you to upload new RAID Controller firmware and emergency firmware.

Firmware updates are periodically released to introduce new features or to solve firmware-related issues.

To upload a new firmware file, do the following:

Step 1 Ensure that both RAID Controllers on the unit are up and running (if applicable).

Step 2 On the Update Firmware page, click **Browse** and navigate to the extracted firmware file according to the method of your operating system. (If you select the wrong file, click **Clear File Selection** and try again.)

Step 3 When the file's path is displayed in the **Select file** field, click **Upload Firmware**.

Note The firmware file may take several minutes to be sent over the network. You will see NO response from the browser while this is happening.

Step 4 If the progress window is not displayed automatically, click the **Click this text ...** link.

The progress bar shows the progress of the installation. When the installation is complete, the message "Firmware update finished, status - 'Microcode Updated OK'" is displayed:

Step 5 Click the **Return to GUI** button to be taken to the Reboot System page (see Reboot System, page 10-3).

Step 6 Restart the system using a **Rolling Restart** (if available) or a **System Reboot**.

Step 7 When the reboot has completed, verify that the update was successful:

a. Go to **System Information > System Info** and check that the **Firmware revision** and **Build Loader revision** for both controllers are updated.

b. If hosts were shut down or disconnected for the system reboot (see Reboot System, page 10-3), reconnect them to the storage unit.

c. Ensure that your volumes are visible and working as expected.

Step 8 Update the emergency firmware, if required:

Note This does not require a reboot and can safely be carried out at any time.

a. Check your current **Emergency revision** on the System Information > System Info page.

b. If an emergency firmware update is required, upload it using Step 2 through Step 5.

CHAPTER 11

Network Configuration

When you click the **Configure Network** button in the navigation pane, you are taken to the Configure Network Settings page. The navigation bar across the top contains links to this section's subpages.

- **Network Settings** links to Configure Network Settings
- **SNMP Syslog** links to SNMP/SYSLOG Settings
- **Date & Time** links to Configure Time and Date
- **Security** links to Security Settings
- **SSL** links to SSL Configuration
- **GUI Settings** links to GUI Settings

Configure Network Settings

Clicking **Configure Network** takes you to the Configure Network Settings page, which allows you to configure all of the settings on each network port.

The information is arranged by controller and then by port. **Current status** indicates whether the link is up or down. If the link is up, it displays the current link speed and duplex mode setting.

For each port, you can configure the following settings:

- **Port Settings**: For most networks, the default setting of **Auto Speed, Auto Duplex** is recommended. However, if your LAN switch does not support auto-negotiation, you can "force" one or both settings. The options are:

  Auto Speed, Auto Duplex
  Auto Speed, Fixed Full Duplex
  Auto Speed, Fixed Half Duplex
  Fixed to 100Mbit Full Duplex
  Fixed to 100Mbit Half Duplex
  Fixed to 10Mbit Full Duplex
  Fixed to 10Mbit Half Duplex

- **Hostname**: This defaults to the host's address. Enter a "friendly" host name for the port, if desired.
- **Assign IP Address**: You can choose whether to **Use DHCP** (Dynamic Host Configuration Protocol, the default) or **Use Static IP**.

  If you select Use DHCP, then no other configuration is needed.

Note NOTE: In order to use DHCP, your network must be configured for DHCP. If it is not, you MUST use a static IP address.

If you select **Use Static IP**, then you must fill in the **Static IP Address** and **Subnet Mask**. If you wish to use a time server (see Configure Time and Date, page 11-3), you should also fill in values for **Gateway**, **Primary DNS**, and **Secondary DNS**.

When you have selected the desired new settings, do one of the following:

- Click **Save Configuration**. The settings are saved and are applied after the system is restarted (see Reboot System, page 10-3).
- Click **Save and Apply Changes**. The settings are saved and applied immediately.

Note If at any time you wish to return the Configure Network Settings page to its initial state, click **Reset**.

SNMP/SYSLOG Settings

Clicking **Configure Network > SNMP Syslog** takes you to the SNMP/SYSLOG Settings page, which allows you to configure settings for SNMP traps and system log (SYSLOG) messages.

Caution SNMP and SYSLOG both use UDP messaging which does not have guaranteed delivery. You may miss critical messages concerning the storage unit.

Information captured by an SNMP trap or a SYSLOG message is sent to an SNMP Network Management Station or system log.

Note If you use SNMP traps, you must parse the trap MIB (Management Information Base) into your application. Use the **MIB** links in the Help section at the bottom of the page to download the MIB for SNMP v1 and v2c.

Note NOTE: Only SNMP traps are available; there is no general SNMP management capability in the unit.

To set up SNMP traps, configure the following settings:

- **SNMP server IP address *N***: Enter the IP address that SNMP traps will be sent to. One or two IP address can be specified. The default is “Not Configured”.
- **Community string**: Enter the SNMP Network Management Server password. By default, this is “public”.
- **Trap version**: Select the type of SNMP trap that is to be sent: **SNMPv1** (the default) or **SNMPv2c**.
- **When to send SNMP traps**: Using the drop-down list, select what kinds of events (see Event Log, page 5-7) will be sent as SNMP traps. There are five options: **Do not send SNMP traps** (the default), **Send SNMP traps for errors only**, **Send SNMP traps for warnings and errors**, **Send SNMP traps for information, warnings and errors**, and **Send SNMP traps for all events**.

To set up SYSLOG messages, configure the following settings:

- **SYSLOG server IP address**: Enter the IP address of the host running the SYSLOG service that will receive the SYSLOG messages.
- **SYSLOG server UDP port**: Enter the UDP port number that the management station is listening to. The default is 514.
- **SYSLOG Facility**: Using the drop-down list, select the designation for the part of the system the SYSLOG message originates from. This is defined by the SYSLOG protocol. Options will vary depending on your operating system.
- **When to send a SYSLOG message**: Using the drop-down list, select what kinds of events (see Event Log, page 5-7) will be sent in SYSLOG messages. There are five options: **Do not send SYSLOG messages** (the default), **Send SYSLOG messages for errors only**, **Send SYSLOG messages for warnings and errors**, **Send SYSLOG messages for information, warnings and errors**, and **Send SYSLOG messages for all events**.

When you have configured the SNMP and SYSLOG settings, click **Save Settings**. A message is displayed, informing you that the settings have been updated. Click the **Back** button to return to the SNMP/SYSLOG Settings page.

Note If at any time you wish to return the SNMP/SYSLOG Settings page to its initial state, click **Reset**.

To test your settings, enter a test phrase (default "test string") in the **Test String** field, then click **Test SNMP** or **Test SYSLOG**. A message is displayed, informing you that the test string has been sent, and the management station or SYSLOG file will receive the test string within a few minutes. Click the **Back** button to return to the SNMP/SYSLOG Settings page.

Configure Time and Date

Clicking **Configure Network > Date and Time** takes you to the Configure Time and Date page, which lets you set the time and date used by the unit's internal clock. This can be done manually or automatically.

To Set the Time and Date Manually

Step 1 Enter the time in the **Time entered in 'hh:mm:ss' format** field.

Note The time entered in the **Time entered in 'hh:mm:ss' format** field will be set when the **Save Settings** button is clicked. Therefore, it is suggested that you enter the time rounded to the next five minute mark, then click **Save Settings** when the entered time is reached.

Step 2 Enter the date using the **Date** drop-down lists.

Step 3 Select the **Timezone relative to GMT (GMT offset)** using the drop-down list.

Step 4 Click **Save Settings**.

To Set the Time and Date Automatically

Note For automatic time setting to work, you may have to configure the Gateway setting for your network. See Configure Network Settings, page 11-1 for more information.

Step 1 Select the **Timezone relative to GMT (GMT offset)** using the drop-down list.

Step 2 Next to **Time server IP address to use for auto time and date configure**, do one of the following:

- Select **Use IP address from list** and select a time server IP address from the drop-down list.
- Select **Use entered IP address** and enter the IP address of a known time server into the text box.

Step 3 Next to **Time server protocol**, select either **Daytime** or **SNTP**.

Step 4 If you entered a time server IP address in Step 2 and selected **Daytime** in Step 3, select the **Time server time and date format** using the drop-down list.

Note If you do not know the format of the time server data, click the **Retrieve Time Server Data** button. The data is retrieved and displayed next to **Data retrieved from contacting the daytime server**. Use this data to choose the proper format in the **Time server time and date format** dropdown list.

Step 5 If you wish the unit to contact the time server every twenty-four hours to update the time and date, select the check box next to **Set system time and date by the time server every 24 hours**.

Step 6 Click **Save Settings**.

Step 7 If you wish to update the time immediately, click the **Contact Time Server To Auto Configure Time And Date** button. The time and date are updated immediately.

Security Settings

Clicking **Configure Network > Security** takes you to the Password Configuration page, which lets you set passwords for the administrator-level (ADMIN) and user-level (USER) accounts.

Caution RESETTING TO FACTORY DEFAULTS WILL RESET THE PASSWORDS.

This page displays the following information for configuring system login:

- **Current "ADMIN"/"USER" login password requirements**: Indicates whether a password is currently required for the ADMIN or USER account, respectively.
- **Change "ADMIN"/"USER" login password requirement to**: Select **NOT Required** (the default) to disable password-protected login. Select **Required** to enable password-protected login.
- **Login user name is fixed to**: Displays the account user name: **ADMIN** or **USER**.
- **Current Password**: Enter the current account password to make changes. If password-protected login is currently disabled for this account, this item is not displayed.
- **New Password**: Enter the new account password. Passwords should be eight characters or longer and can contain both letters and numbers, but not special characters or punctuation.

- **Confirm Password**: Re-enter the password you entered for **New Password**. The two fields must match exactly.

To save the new password settings for the administrator account, click **Set ADMIN Password**. To save the new password settings for the user account, click **Set USER Password**. In either case, a message is displayed, indicating that the settings have been changed. Click the **Back** button to return to the Password Configuration page.

Note NOTE: Before you can configure security settings for the USER account, you must first configure and apply security settings for the ADMIN account.

The Connected Host Access section lets you configure the option to allow hosts that are connected to the storage area network (SAN) to provision the storage system directly, without requiring the ADMIN password. This feature requires compatible storage management software to be installed on the host. This section displays the following information:

- **Current host trust setting**: The current level at which SAN-connected hosts can access the storage system without the ADMIN password.
- **Change host trust setting to**: Select one of the four levels:
  - **None**: Host-based management access is disabled.
  - **Read-only**: Hosts can read information about the RAID storage system, but cannot provision storage.
  - **Limited** (default): Hosts can create new volumes, and expand or delete any volumes to which they have read/write access.
  - **Full**: Hosts can create new volumes, modify volume access rights, and expand or delete any volumes on the RAID system.

Click **Set Host Trust Setting** to save your changes. A message is displayed, indicating that the settings have been changed. Click the **Back** button to return to the Password Configuration page.

Caution If untrusted users have administrative access to hosts on the storage area network (SAN), we strongly recommend that you set this option to **None**.

SSL Configuration

Clicking **Configure Network > SSL** takes you to the SSL Configuration page, which allows you to set up Secure Sockets Layer (SSL) encryption between the storage system and the browser accessing the system's Management Console.

The Configure SSL section displays the following information:

- **SSL status**: The current SSL configuration. Also shows any certificate problems and a download link for the current root CA certificate (when applicable).

  Note It is recommended that you download the root CA certificate and add it to your browser's trusted certificate list to avoid certificate errors when connecting via HTTPS.

- **SSL mode**: The type of browser connection allowed by the RAID system. Select the desired option:

  - **HTTP only** (the default): Disables SSL or HTTPS connection.
  - **HTTPS only**: Enables SSL/HTTPS connection and disables unsecured (HTTP) connection.
  - **HTTPS and HTTP**: Allows both SSL/HTTPS and unsecured HTTP connections.

The Configure Certificate and Key (Advanced) section displays the following information:

- **Dynamic certificate**: This is the default mode. The SSL key and certificate are automatically generated at startup and signed with the default Cisco root CA certificate.
- **Dynamic certificate inherited from uploaded CA root**: The SSL key and certificate are automatically generated at startup and signed with the uploaded root CA certificate. To select this mode, you must provide and select files for the **Certificate** and **Key** by clicking **Browse** and navigating to the files according to the method of your operating system. CA certificate and SSL key files must be in PEM or DER format.
- **Use uploaded certificate and key**: Uses the uploaded certificate and key (PEM or DER format) as long as both files are valid. On dual-controller systems, you must provide different files for each controller.

To save SSL settings, click **Save Configuration**. A message is displayed, indicating that the settings have been changed. Click the **Back** button to return to the SSL Configuration page.

GUI Settings

Clicking **Configure Network > GUI Settings** takes you to the GUI Settings page, which allows you to configure Management Console options.

This page contains the following settings:

- **Enable GUI enhancements (requires Javascript)**: This option is enabled by default. If your browser does not support JavaScript, or if the JavaScript enhancements cause browser problems, disable this option.

  Note Sometimes, JavaScript errors can prevent user login. If this occurs, enter `http://<IPaddress>/admin/guiprefs.asp` into the browser's address bar to load this page directly. JavaScript can then be turned off and login reattempted.

- **Enable persistent tooltips (requires Javascript)**: This option is disabled by default. Enable this option to display pop-up tool tips when the mouse pointer is hovered over an icon. This option requires that the **Enable GUI enhancements** option is enabled.
- **Minimize page scrolling by using submenus where appropriate**: This option is disabled by default. Enable this option to show a summary submenu of links on certain pages. This submenu reduces the need to scroll on long pages.

  Note Enabling this option may change the way in which you are able to access certain features. In such cases, the instructions in this Administration Guide may not match your experience.

- **Minimize page scrolling by showing less information**: This option is disabled by default. Enable this option to show only essential information on each page.

Note Enabling this option may hide certain features from view or change the way in which you are able to access them. In such cases, the instructions in this Administration Guide may not match your experience.

- **Highlight array text using different colors**: This option is enabled by default. Text displayed below disk icons is color-coded by array to aid in visual identification of array members. Disable this option if you wish to display all disk text in black.
- **Select the units you wish to use for volume and free space entry**: The default setting for this option is **Gigabytes (GB)**. Select a different option, if desired. The five options are: **Megabytes (MB)**, **Gigabytes (GB)**, **Percentage of array size (%)**, **Binary Megabytes (MiB)**, and **Binary Gigabytes (GiB)**.
- **Web page auto refresh (10 to 120 secs)**: This option is enabled and set to **30** seconds by default. When no links or buttons are clicked in the Management Console for this length of time, the page is automatically refreshed with updated information from the unit. Disable this option to stop pages from automatically refreshing. Change the number in the **Auto refresh time** field to make automatic page refresh happen more or less often.

To save settings changes, click **Save Settings**. A message is displayed, indicating that the settings have been changed. Click the **Back** button to return to the GUI Settings page.

CHAPTER 12

Technical Support

When you click the **Technical Support** button in the navigation pane, you are taken to the Technical Support page. The navigation bar across the top contains links to this section's subpages.

- **Contact Details** links to Contact Details
- **End User License** links to End-User License Agreement**.**

Contact Details

Clicking **Contact Details** takes you to the Technical Support page, which provides two options for contacting Technical Support.

This page displays URLs for TAC support and telephone numbers for contacting Technical Support.

End-User License Agreement

Clicking **Technical Support > End User License** takes you to the End-User License Agreement page. You must accept the EULA the first time you log into the unit (see Accept the EULA, page 1-3).

APPENDIX A

RAID Levels

The RAID arrays in Cisco storage systems can be configured in various RAID levels. Except where noted below, all RAID levels require a minimum of two disk drives. The levels available are:

RAID 0

RAID level 0 provides data striping. Blocks of data from each file are spread out across multiple disk drives. It does not provide redundancy. This improves the speed of both read and write operations, but does not provide fault tolerance. If one drive fails, all data in the array is lost.

RAID 1

RAID level 1 provides disk mirroring. Files are written identically to two or more disk drives. If one drive fails, the other drive still contains the data. This also improves the speed of read operations, but not write operations.

RAID 10

RAID level 10 is a combination of RAID levels 0 and 1. Data is both striped and mirrored. RAID level 10 is used whenever an even number of drives (minimum of four) is selected for a RAID 1 array.

RAID 4

RAID level 4 provides block level striping similar to RAID level 0, but with a dedicated parity disk. If a data disk fails, the parity data is used to recreate the data on the failed disk. Because there is only one parity disk, this RAID level can slow down write operations.

RAID 5

RAID level 5 provides data striping at the byte level and also stripe error correction information. Parity data, instead of being stored on only one disk, is distributed among all disks in the array. This level provides excellent performance and good fault tolerance. It is one of the most popular implementations of RAID.

RAID 6

RAID level 6 provides block level data striping with parity data distributed across all disks. For additional redundancy, each block of parity data exists on two disks in the array instead of only one. RAID level 6 requires a minimum of four disk drives.

Note RAID levels 2 and 3 are not available on Cisco storage systems.

APPENDIX B

AutoMAID

AutoMAID is a disk drive power management system. MAID stands for Massive Array of Idle Disks. When disk drives are not in use, AutoMAID puts them into one of several power saving states. Disks are still accessible, however, and are automatically brought back up to full power levels when data needs to be accessed.

Note Not all disk drives support all levels of AutoMAID. Disks that do not support a specific AutoMAID level will stay at a previous, usable level until the system reaches an AutoMAID level that the disk supports (see Configure AutoMAID Settings, page 9-2).

Note If any drives are set to use AutoMAID Level 3 or 4, host timeout values (set for the host HBA either through the HBA BIOS or a management application) should be set to a default of between 120 and 150 seconds to avoid the host requests timing out before the disk drives can power on and spin up to full speed.

AutoMAID Level 1

At AutoMAID level 1, the read/write heads of the disk drives are parked. If access to the disk is requested when it is at AutoMAID level 1, the disk is fully powered and data is accessible in under a second. AutoMAID level 1 provides a 15–20% energy savings.

AutoMAID Level 2

At AutoMAID level 2, the read/write heads of the disk drives remain parked, and disk rotation slows down. If access to the disk is requested when it is at AutoMAID level 2, the disk is fully powered and data is accessible in approximately 15 seconds. AutoMAID level 2 provides a 35–45% energy savings.

AutoMAID Level 3

At AutoMAID level 3, the read/write heads of the disk drives remain parked, and disk rotation stops. If access to the disk is requested when it is at AutoMAID level 3, the disk is fully powered and data is available in approximately 30–45 seconds. AutoMAID level 3 provides a 60–70% energy savings.

AutoMAID Level 4

At AutoMAID level 4, the electronics in the disk are powered off. If access to the disk is requested when it is at AutoMAID level 4, the disk is fully powered and data is available in approximately 45–60 seconds. AutoMAID level 4 provides up to an 87% energy savings.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

S

T

U

V

W