



Overland
Storage

SnapServer®

Administrator's Guide

For SnapServer or SnapExpansion™ Appliances Running
GuardianOS™ Version 7.5



May 2014
10400541-001



©2008-14 Overland Storage, Inc. All rights reserved.

Overland[®], Overland Data[®], Overland Storage[®], ARCvault[®], DynamicRAID[®], LibraryPro[®], LoaderXpress[®], Multi-SitePAC[®], NEO[®], NEO Series[®], PowerLoader[®], Protection OS[®], REO[®], REO 4000[®], REO Series[®], Snap Appliance[®], Snap Care[®] (EU only), SnapServer[®], StorAssure[®], Ultamus[®], VR2[®], and XchangeNOW[®] are registered trademarks of Overland Storage, Inc.

GuardianOS[™], RAINcloud[™], RapidRebuild[™], SnapDisk[™], SnapEDR[™], Snap Enterprise Data Replicator[™], SnapExpansion[™], SnapSAN[™], SnapScale[™], SnapServer DX Series[™], SnapServer Manager[™], and SnapWrite[™] are trademarks of Overland Storage, Inc.

All other brand names or trademarks are the property of their respective owners.

The names of companies and individuals used in examples are fictitious and intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is coincidental.

PROPRIETARY NOTICE

All information contained in or disclosed by this document is considered proprietary by Overland Storage. By accepting this material the recipient agrees that this material and the information contained therein are held in confidence and in trust and will not be used, reproduced in whole or in part, nor its contents revealed to others, except to meet the purpose for which it was delivered. It is understood that no right is conveyed to reproduce or have reproduced any item herein disclosed without express permission from Overland Storage.

Overland Storage provides this manual as is, without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Overland Storage may make improvements or changes in the product(s) or programs described in this manual at any time. These changes will be incorporated in new editions of this publication.

Overland Storage assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of this manual, nor for any problem that might arise from the use of the information in this manual.

FW 7.5.045

Overland Storage, Inc.
9112 Spectrum Center Blvd.
San Diego, CA 92123
U.S.A.

Tel: 1.877.654.3429 (toll-free U.S.)
Tel: +1.858.571.5555, Option 5 (International)
Fax: +1.858.571.0982 (general)
Fax: +1.858.571.3664 (sales)
www.overlandstorage.com

Audience and Purpose

This guide is intended for system and network administrators charged with installing and maintaining SnapServers DX appliances running GuardianOS 7.5 on their network. It provides information on the installation, configuration, security, and maintenance of SnapServers and SnapExpansion units.

It is assumed that the administrator is familiar with the basic concepts and tasks of multi-platform network administration.

This guide also provides information on the following utilities and software components:

- The GuardianOS 7.5 Web Management Interface
- SnapServer Manager (SSM)
- CA Antivirus software

GuardianOS 7.5 comes preinstalled on all new SnapServer DX-Series appliances. It can also be upgraded from a previously installed version of GuardianOS 7.0 or later.

Product Documentation & Software Updates

SnapServer product documentation and additional literature are available online, along with the latest release of the GuardianOS 7.5 software.

Point your browser to:

<http://docs.overlandstorage.com/snapserver>

Follow the appropriate link on that page to download the latest software file or document. For additional assistance, search at <http://support.overlandstorage.com>.

Overland Technical Support

For help configuring and using your SnapServer, email our technical support staff at:

techsupport@overlandstorage.com.

You can get additional technical support information on the [Contact Support](#) web page at:

<http://docs.overlandstorage.com/support>

For a complete list of support times based on your type of coverage, visit our website at:

<http://docs.overlandstorage.com/care>

Conventions

This document exercises several alerts and typographical conventions.

Alerts

Convention	Description & Usage
 IMPORTANT	An <i>Important</i> note is a type of note that provides information essential to the completion of a task or that can impact the product and its function.
 CAUTION	A <i>Caution</i> contains information that the user needs to know to avoid damaging or permanently deleting data or causing physical damage to the hardware or system.
 WARNING	A <i>Warning</i> contains information concerning personal safety. Failure to follow directions in the warning could result in bodily harm or death.
AVERTISSEMENT	Un Canadien avertissement comme celui-ci contient des informations relatives à la sécurité personnelle. Ignorer les instructions dans l'avertissement peut entraîner des lésions corporelles ou la mort.

Typographical Conventions

Convention	Description & Usage
Button_name	Words in this special boldface font indicate the names of command buttons or pages found in the Web Management Interface.
Ctrl-Alt-r	This type of format details the keys you press simultaneously. In this example, hold down the Ctrl and Alt keys and press the r key.
NOTE	A Note indicates neutral or positive information that emphasizes or supplements important points of the main text. A note supplies information that may apply only in special cases, for example, memory limitations or details that apply to specific program versions.
Menu Flow Indicator (>)	Words with a greater than sign between them indicate the flow of actions to accomplish a task. For example, Setup > Passwords > User indicates that you should press the Setup button, then the Passwords button, and finally the User button to accomplish a task.
<i>Courier Italic</i>	A variable for which you must substitute a value.
Courier Bold	Commands you enter in a command-line interface (CLI).

Information contained in this guide has been reviewed for accuracy, but not for product warranty because of the various environments, operating systems, or settings involved. Information and specifications may change without notice.

Japanese Voluntary Control Council for Interference (VCCI)

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI— A

(Translation: This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.)

Contents

Preface

Chapter 1: Overview

GuardianOS Specifications	2
GuardianOS 7.5 Features	3
Using SnapServer Manager with SnapServer	4
SnapServer Manager Installation	4
Connecting to the Server for the First Time	5
Connect Using the Server Name	5
Connect Using SSM	5
SnapExtensions	6
Wake-on-LAN Support	6
Expansion Units	6

Chapter 2: Server Setup and Options

Initial Setup Wizard	7
General Configuration	9
TCP/IP Configuration	10
RAID Type Selection (DynamicRAID/Traditional RAID)	10
DynamicRAID Setup	13
Traditional RAID Setup	14
Configure Expansion Units	16
Setup Completion	18
Registration Page	19
Server Status and Site Map	19
Hardware Information	21
Scheduling Data Protection Tasks	21
Server Options	23
Server Name	23
Date/Time	24
Secure Shell	25
UPS Protection	27
Print Server	29

Chapter 3: Network Settings

View Network Information	33
TCP/IP Networking Options	35
Configuring Port Properties	37
TCP/IP Configuration Considerations	38
Creating a Bond	40

Deleting a Bond	42
Windows Networking (SMB)	43
Support for Windows Networking (SMB)	44
Support for Windows Network Authentication	45
Configure Windows/SMB Networking	46
Apple Networking (AFP)	49
AFP Configuration Considerations	50
Edit AFP Access	50
NFS Access	51
Assigning Share Access to NFS Users	52
Enable NFS Access to the Server	52
Configure NFSv4 Access	52
LDAP and NIS Domains	54
LDAP vs. NIS Overview	54
Configuring LDAP	55
Configuring NIS	56
FTP/FTPS Access	57
Supported FTP Clients	57
Configure FTP/FTPS Access	57
SNMP Configuration	58
Default Traps	58
Supported Network Manager Applications and MIBs	59
Configure SNMP	59
Web Access	60
Configuring Web Options	61
Home Page Overview	62
Using Web Root to Configure the SnapServer as a Simple Web Server	62
iSNS Configuration	63

Chapter 4: DynamicRAID Storage

Storage Pools	66
Storage Pool Creation	67
Storage Pool Properties	70
View Disks from Storage Pool Properties Page	72
Storage Pool Deletion	73
Parity Management	74
Volumes	76
Volume Creation	76
Volume Properties	78
Volume Deletion	79

Chapter 5: Traditional RAID Storage

Storage Guides	81
Factors in Choosing a RAID Type	81
Local and Global Spares	82
RAID Sets	83
Create RAID Sets	83
Group RAID Sets	86
Change RAID Settings	90
Manage Global Spares	91

Edit RAID Set Properties	92
Volumes	94
Volumes and the Snapshot Pool	95
Volume Creation	95
Volume Properties	98
Quotas	101
Quotas Page	101
Enable/Disable Quotas	102
Add Quotas Wizard	103
Displaying/Changing Quotas	105

Chapter 6: Other Storage Options

Snapshots	109
Creating Snapshots	110
Schedule Snapshots	113
Snapshot Space	114
Snapshot Properties	115
iSCSI Disks	117
Configuring iSCSI Initiators	118
iSCSI Configuration on the SnapServer	119
Create iSCSI Disks	122
Edit an iSCSI Disk	124
Delete an iSCSI Disk	125
Configuring VSS/VDS for iSCSI Disks	125
Disks	129
Replacing Disk Drives	130
Adding Disk Drives	132
Managing Expansion Unit Storage	136
Integrating Orphaned Expansion Units	137

Chapter 7: Security Options

Overview	138
Guidelines for Local Authentication	139
User and Group ID Assignments	140
Security Guides	140
Windows Active Directory Security Guide	141
Entire Volume Security Guide	142
Folder on Volume Security Guide	142
Shares	143
Share Security Overview	143
Create Shares	144
Edit Share Properties	146
Delete Shares	147
Configuring Share Access	147
Local Users	153
Create a User	154
Edit User Properties	155
User Password Policies	156
Assign User to a Group	157
Delete Local User	158

Local Groups	159
Create New Group	159
Edit Group Properties	160
Specify Users in Group	161
Delete Group	162
Security Models	162
Managing Volume Security Models	163
Managing Folder Security Models in Traditional RAID	163
ID Mapping	165
Add Mapping	166
Change Mapping	168
Auto Mapping	171
Remove Mappings	172
Remove Missing ID Mappings	174
Filesystem Updates	175
Home Directories	175
Configure Home Directories	177

Chapter 8: System Monitoring

System Status	179
SnapServer Status	179
Expansion Unit Status	180
Active Users	180
Open Files	181
Event Log	181
Filter the Log	182
Tape	182

Chapter 9: Maintenance

Shutdown and Restart	184
Manually Powering SnapServers On and Off	184
Factory Defaults	184
Disaster Recovery	186
Backing Up Server and Volume Settings	186
SnapDRImage File and Volume-Specific Files	187
System Settings Recovery	188
Volume and Storage Pool Security Settings Recovery	190
Replacing or Cloning a Server	191
Data Import	192
Setting Up a Data Import Job	193
Stopping an Import Job	195
Recreating an Import Job	195
Preserving Permissions	195
OS Update	196
Check for Updates	197
Update the GuardianOS Software	197
Update Notification	197
Last OS Update	198
Support	199
Registering Your Server	199

Maintenance Tools	200
Email Notification	201
Host File Editor	202
Checking Filesystems	203

Chapter 10: Misc. Options

Home Pages	207
Home Page	207
Administration Page	208
SnapExtensions	210
BitTorrent Sync	210
CA Antivirus	212
Snap EDR	212
Snap Finder	213
Snap Finder Properties	214
Change Password	215
Change Your Password	215
Mgmt. Interface Settings	216

Chapter 11: CA Antivirus Software

Antivirus Dependencies	218
Launching the CA Antivirus GUI	219
Launching the CA Antivirus Browser Interface	219
The Local Scanner View	219
Scan Jobs	220
Defining Scan Jobs	220
Running a Manual Scan Job	221
Scheduling a Scan Job	221
Signature Updates	222
Updating SnapServers with Internet Access	222
Updating a SnapServer without Internet Access	223
Distributing Updates from One SnapServer to Another	223
Verifying Download Events	224
Alert Options	225
The Move Directory	225
Log View	226

Appendix A: DynamicRAID Overview

About DynamicRAID	227
Should I use DynamicRAID or Traditional RAID?	228
Setting Up DynamicRAID	230
DynamicRAID Implementation	230
Storage Expansion	230
Snapshots	231
iSCSI Target Volumes	231
Indicators	231
Additional Information on DynamicRAID Sizing	231

Appendix B: Backup Solutions

Backup and Replication Solutions	233
--	-----

Snap Enterprise Data Replicator	233
Snap EDR Usage	234
Configuring Snap EDR for GuardianOS	234
Scheduling Jobs in Snap EDR	235
Backup via SMB, NFS, or AFP	235
Off-the-Shelf Backup Solutions	235
iSCSI Disk Backups	235
Using Backup Exec for VSS-based Snapshots of SnapServer iSCSI Disks	235

Appendix C: Security and Access

Security Model Rules	237
Security Model Directories	238
Security Model Management	239
Special Share Options	239
Hiding Shares	239
Share Level Permissions	240
Where to Place Shares	240
File and Share Access	240
NFS Share Access	240
Snapshot Access	240
Snapshot Shares and On Demand File Recovery	241
Creating a Snapshot Share	241
File-level Security	242
Security Personalities and Security Models	242
Windows ACLs	242

Appendix D: Troubleshooting SnapServers

LED Indicators	244
System Reset Options	246
Performing System Resets Without Network Access	247
Maintenance Mode	247
Networking Issues	247
Miscellaneous Issues	250
Phone Home Support	251

Appendix E: Command Line Interface

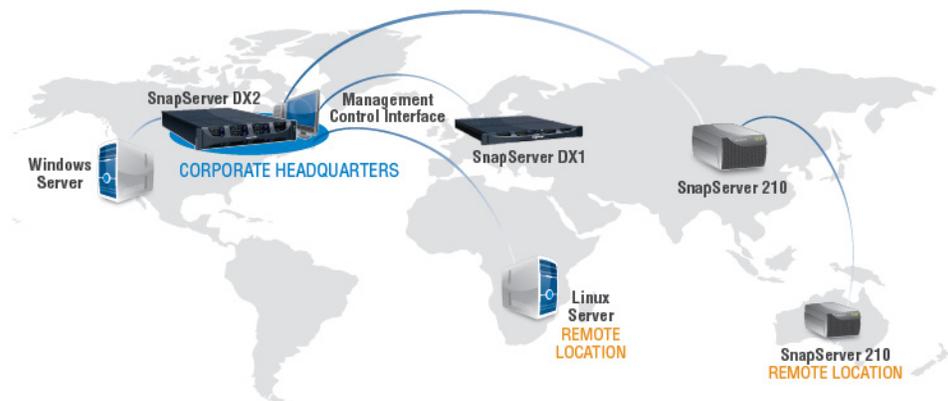
SnapCLI Syntax	252
SnapCLI Procedures	254
SnapCLI Commands	254
Scripts in SnapCLI	260
Running a SnapCLI Script	260
Sample Script	261

Appendix F: GuardianOS Ports

Master Glossary & Acronym List

Index

SnapServer appliances are designed as flexible, low-maintenance network-attached storage (NAS) file servers optimized for performance and efficiency. They run GuardianOS, an operating system built to maximize file I/O throughput across multi-network protocols. To this end, all unnecessary system control and processing functions that are associated with a general-purpose server have been removed.



This guide applies to SnapServer DX appliances, including SnapExpansion units, running GuardianOS version 7.5.

Topics in Overview:

- [GuardianOS Specifications](#)
- [GuardianOS 7.5 Features](#)
- [Using SnapServer Manager with SnapServer](#)
- [Connecting to the Server for the First Time](#)
- [SnapExtensions](#)
- [Wake-on-LAN Support](#)
- [Expansion Units](#)

GuardianOS Specifications

These specifications apply to all devices running GuardianOS 7.5.

Feature	Specification
Network Transport Protocols	<ul style="list-style-type: none"> TCP/IP (Transmission Control Protocol/Internet Protocol) UDP/IP (User Datagram Protocol/Internet Protocol)
Network Block Protocols	iSCSI (Internet Small Computer System Interface)
Network File Protocols	<ul style="list-style-type: none"> Microsoft Networking (CIFS/SMB1/SMB2) Unix Network Filesystem (NFS) 2.0/3.0/4.0 Apple Filing Protocol (AFP) v2.0/v3.1/3.2* Hypertext Transfer Protocol (HTTP/HTTPS) File Transport Protocol (FTP/explicit FTPS such as FTPES or Auth TLS) <p>* AFP v 3.2 ACLs and extended attributes not supported.</p>
Network Client Types	<ul style="list-style-type: none"> Microsoft Windows 2003/2003 R2/2008 SP2/2008 R2 /XP SP3/Vista SP2/7/8/2012 Mac OS X 10.5/10.6/10.7/10.8/10.9 Sun Solaris 10 and 11 HP-UX 11 AIX 5.3/6 Red Hat Enterprise Linux (RHEL) 4.x/5.x/6.x Novell SuSE Linux Enterprise Server (SLES) 10.x/11.x
Network Security	<ul style="list-style-type: none"> CA Antivirus software Microsoft Active Directory Service (ADS) (member server) Unix Network Information Service (NIS) user/group UID/GID translation LDAP user/group UID/GID translation File and Folder Access Control List (ACL) Security for Users and Groups Secure Sockets Layer (SSL v2/3) 128-bit Encryption Target Challenge Handshake Authentication Protocol (CHAP) for iSCSI SMTP Authentication and support for email encryption (STARTTLS and TLS/SSL encryption protocols)
Data Protection	<ul style="list-style-type: none"> Snapshots for immediate or scheduled point-in-time images of the filesystem Support for local backup with Symantec NetBackup/Backup Exec Remote Media Server for Linux Support for network backup with Symantec NetBackup/Backup Exec, CA ARCserve, or EMC NetWorker APC[®] brand Uninterruptible Power Supply (UPS) with Network Management Cards, a USB interface, or a serial interface (with USB-to-Serial adapter) are supported for graceful system shutdown

Feature	Specification
RAID Options with Traditional RAID	<ul style="list-style-type: none"> • RAID 0 (drive striping): Large virtual drive with data striped across all drives of the array to provide maximum performance with no loss in usable capacity. Does not provide data protection. • RAID 1 (drive mirroring): One or more drives duplicate one drive for maximum data protection. Available only on systems with two (2) or more drives. • RAID 5 (drive striping with parity): For each array, the size of one drive is reserved for parity. Provides good performance and space utilization with one-drive fault tolerance. Available only on systems with four (4) or more drives. • RAID 6 (drive striping with two parity drives): Like a RAID 5 except that two drives are used for parity rather than one. Provides moderate performance and reasonable space utilization with two-drive fault tolerance. Available only on systems with four (4) or more drives. • RAID 10 (striped mirroring): A combination of RAID 0 and RAID 1. Provides high performance and fault tolerance. Available only on systems with four (4) or more drives. • Global or local spare support. • Instant Capacity Expansion (ICE): Logically groups RAIDs for dynamic online scalability.
DHCP Support	Supports Dynamic Host Configuration Protocol (DHCP) for automatic assignment of IP addresses
System Management	<ul style="list-style-type: none"> • Browser-based administration tool called the Web Management Interface • SnapCLI for volume system deployment • SnapServer Manager utility (platform independent) • SNMP (MIB II and Host Resource MIB) • User disk quotas for Windows, Unix/Linux, Mac, FTP/FTPS (Traditional RAID only) • Group disk quotas for Unix/Linux (Traditional RAID only) • Environmental monitoring • Email event notification and SNMP trap notification • Data importation (migration)

GuardianOS 7.5 Features

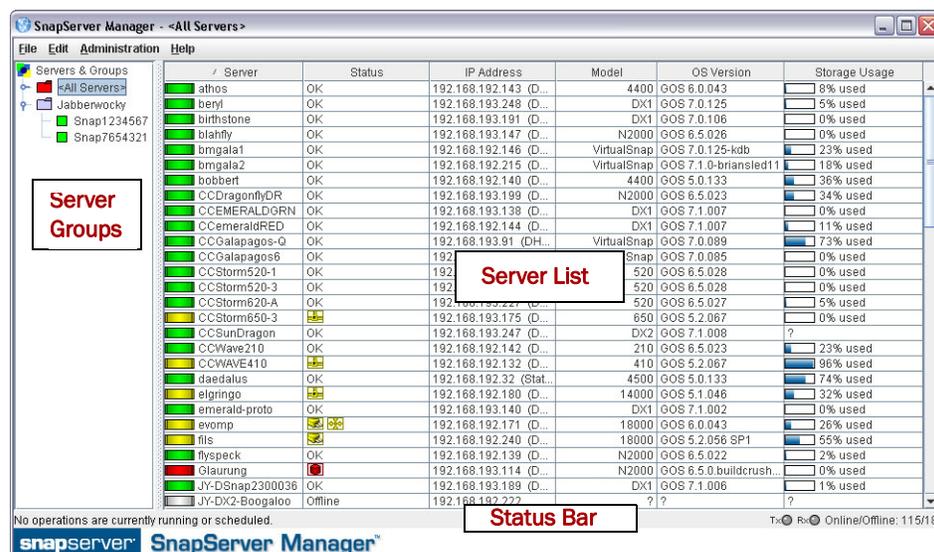
NOTE: For details and descriptions of all the new features and a list of other improvements to the firmware, see the [Product Information Bulletin](#) and the [Release Notes](#) on the Overland SnapServer website.

With the release of the GuardianOS 7.5, the following features and functionality are now available:

Feature	New Functionality
Snapshots Performance Optimization	File write performance is significantly improved when one or more snapshots exist for a volume.
LDAP Integration	Lightweight Directory Access Protocol (LDAP) can be used to look up user/group names and UIDs/GIDs for quota assignment, ID mapping, and home directories.
BitTorrent Sync	BitTorrent Sync can be used to replicate data between the SnapServer and other servers or workstations.
SMB 2.0/2.1	The server supports Server Message Block (SMB) version 2.0/2.1 for improved compatibility and performance for later Windows OS versions.
Windows Security Model	Volumes can be configured with a security model that permits only Windows personality file system permissions (ACLs).

Using SnapServer Manager with SnapServer

SnapServer Manager (SSM) is a Java-based application from Overland Storage that runs on all major client systems. SSM provides a single screen from which administrators can discover all SnapServer servers, REO appliances, SnapSAN arrays, SnapScale clusters, and SnapScale Uninitialized nodes (that is, nodes that are not part of a SnapScale cluster) on their network.



SnapServer Manager Installation

You can download and install SSM by navigating to the Overland Storage NAS website and downloading the [SnapServer Manager executable file](#). SSM can be installed on all client platforms, including Windows, Mac OS X, and Linux.

Refer to the *SnapServer Manager User Guide* for details on discovering and configuring SnapServers.

Connecting to the Server for the First Time

SnapServers are configured to acquire an IP address from a DHCP server. If no DHCP server is found on the network, the SnapServer defaults to an IP address in the range of 169.254.xxx.xxx and is labeled “ZeroConf” in SSM. While you may not be able to see the server on your network, you can discover the SnapServer using either the default server name or the SSM utility. Use the server name method if you are installing one SnapServer on the network. Use SSM if you are installing two or more SnapServers, or if your network does not have IP-to-name resolution services.

Connect Using the Server Name

This procedure requires that name resolution services (via WINS or an equivalent service) be operational.

1. Find the **server name**.

The default server name is “SNAP n ”, where n is the server number. For example, the name of a SnapServer with a server number of 6100191 is SNAP6100191. The server number is a unique, numeric-only string that appears on a label affixed to the top of the server in the left front corner.

2. In a Web browser, enter the **server URL**.

For example, enter `http://SNAP n` (where n is the server name).

3. Press **Enter** to open the **Home** page.

4. Log into the Web Management Interface.

In the login dialog box, enter **admin** as the user name and **admin** as the password, then click **OK**.

5. Complete the **Initial Setup Wizard**.

Connect Using SSM

1. Launch SSM.

SSM discovers all SnapServers on its local network segment and displays their server names, IP addresses, and other status information in the main console. If you do not have a DHCP server, there might be a delay before the server appears on the network.

NOTE: To distinguish multiple SnapServers, you may need to find their default server names as explained in the previous procedure.

2. If using a DHCP server, proceed to [Step 3](#); otherwise, follow these steps to assign an **IP address** to the new server:

- a. In SSM, right-click the **server name**.

- b. Select **Set IP Address**.

- c. Enter an IP address and a subnet mask, then click **OK**.

3. In SSM, right-click the server name and select **Launch Web Administration**.

4. Log into the Web Management Interface.

In the login dialog box, enter **admin** as the user name and **admin** as the password, then click **OK**.

5. Complete the **Initial Setup Wizard**.

At this point, your SnapServer is ready to be configured for your specific environment.

SnapExtensions

SnapExtensions are software applications, agents, and utilities that extend the capabilities of a SnapServer (for additional details, see [SnapExtensions](#) in [Chapter 10](#)). Some SnapExtensions are fully functional out-of-the-box; others may require a download and/or the purchase of a license for full operation. For up-to-date information on feature availability, contact [Overland Storage](#).

Wake-on-LAN Support

Wake-on-LAN, the Ethernet computer networking standard that allows a powered-off computer to be powered on by a network signal, is automatically enabled (and cannot be disabled) for Ethernet 1 (Management) and Ethernet 2 ports. Wake-on-LAN is activated when another computer on the same LAN sends a “magic packet” to the SnapServer using the SnapServer Manager or other program designed to send magic packets. Wake-on-LAN only works for SnapServers and does not work with any expansion units that may be attached to the system.

Expansion Units

To increase the capacity of a SnapServer DX-series server, use one or more SnapExpansion units.



NOTE: If GuardianOS detects an expansion unit that is not integrated with the SnapServer, a message is displayed across the top of the Disks, Admin Home, RAID, and Storage Pool pages with a link to information about the orphaned expansion unit.

The SnapExpansion is a 2U, 12-bay SAS-connected expansion unit for expanding either SnapServer DX1 or DX2 systems. The SnapExpansion supports SAS and SATA hard drives and allows capacity growth by creating additional DynamicRAID storage pools.

- By adding the optional SAS expansion card to the SnapServer DX1, you can attach up to **three** SnapExpansion chassis to grow storage up to 120TB.
- The SnapServer DX2 includes the SAS expansion card that allows for **seven** SnapExpansion chassis to be attached, to scale up to 288TB in total space.

A SnapExpansion is accessed and managed through the SnapServer head unit to which it is connected. The expansion unit has no physical connection to the network.

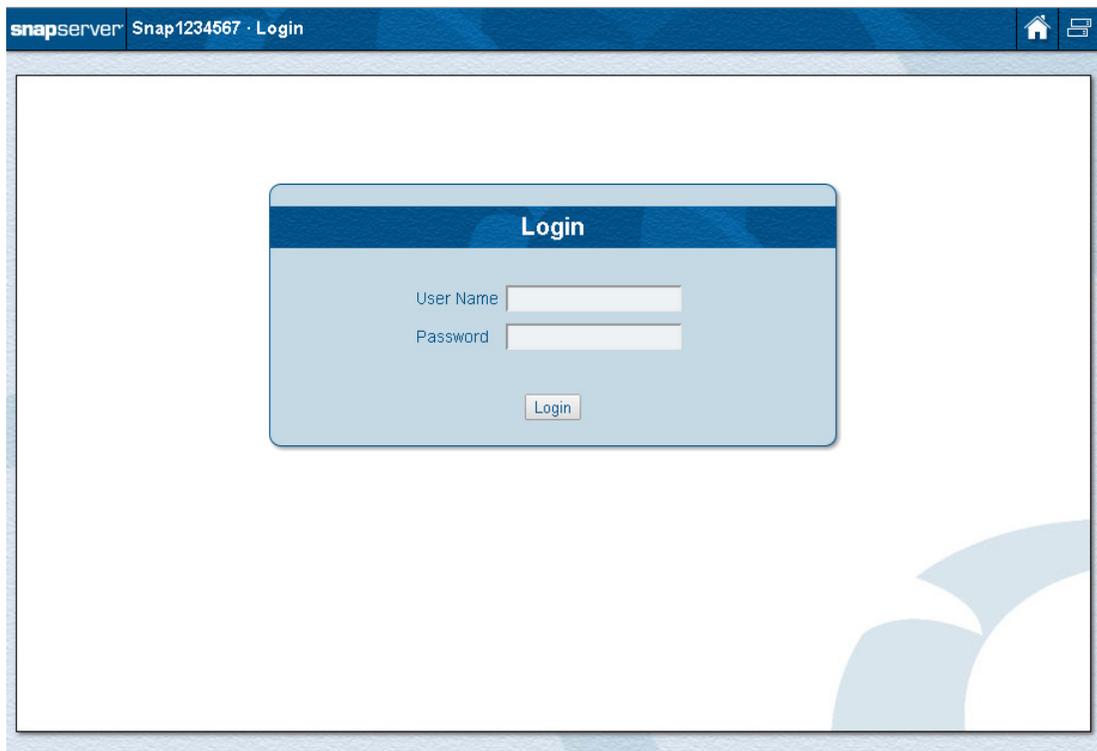
This section covers the initial steps needed to set up and configure a SnapServer running GuardianOS 7.5.

Topics in Server Setup and Options:

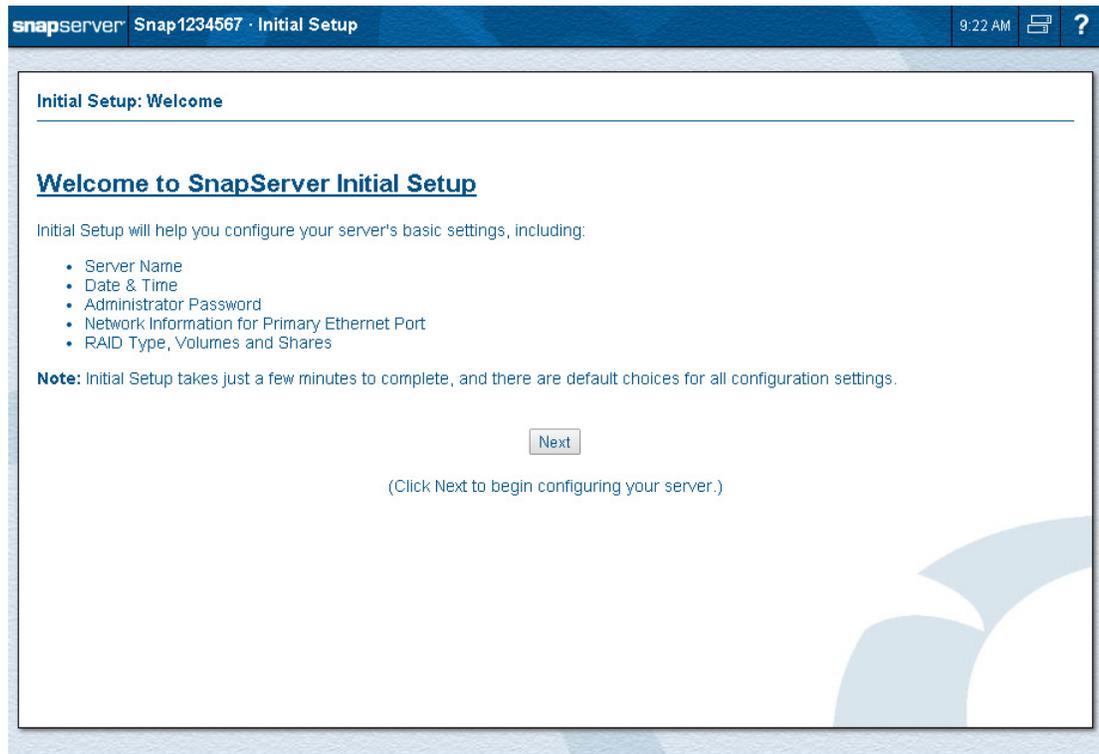
- [Initial Setup Wizard](#)
- [Server Status and Site Map](#)
- [Scheduling Data Protection Tasks](#)
- [Server Options](#)

Initial Setup Wizard

The first time you connect to a SnapServer via the Web Management Interface, you are prompted to log in. Log in using the default administrator user name **admin** and password **admin**.



Once you log in, the Initial Setup Wizard runs displaying the Welcome page.



The Initial Setup Wizard consists of several web pages that help you configure your server's basic settings. The basic pages include:

- [General Configuration](#)
- [TCP/IP Configuration](#)
- [RAID Type Selection \(DynamicRAID/Traditional RAID\)](#)
 - [DynamicRAID Setup](#)
 - [Traditional RAID Setup](#)
- [Configure Expansion Units](#)
- [Setup Completion](#)
- [Registration Page](#)

Click **Next** to start the Initial Setup wizard.

General Configuration

Clicking Next on the Welcome page displays the General Information page of the Initial Setup wizard. This page allows you to change the basic information for the SnapServer. It is recommended that you set your Administrator password at this time to something other than the default.

The screenshot shows the 'Initial Setup: General Information' page. At the top, there's a header with 'snapserver Snap1234567 · Initial Setup' and a clock showing '9:27 AM'. Below the header, the page title is 'Initial Setup: General Information'. The main content area has a heading 'Enter basic information for your server.' followed by a 'Server Name' field containing 'Snap1234567'. Under the 'Date and Time' section, there are fields for 'Date' (2014-03-07), 'Time' (09:24:25 AM), and 'Time Zone' (UTC-08:00 Pacific Time (US & Canada)). A note below these fields states: 'Note: Changing the date, time or time zone may require you to re-login to this Web Management Interface.' The 'Administrator Password' section has two fields: 'Admin Password' and 'Confirm Password', with a note '(Leave blank to keep existing administrator password)'. A red warning message says: 'Warning: You should assign an administrator password if you want to protect your server from unauthorized changes.' At the bottom center, there is a 'Next' button.

1. Enter (or accept) the **Server Name**.

The default server name is `SNAPnnnnnnnn`, where `nnnnnnnn` is the server number. If desired, a unique server name of up to 15 alphanumeric characters can be used. In addition to letters and numbers, you can also use a dash (-) between characters, but spaces are not allowed.

2. Enter (or accept) the **Date/Time Settings**.

The SnapServer time stamp applies when recording server activity in the event log (Monitor Menu), setting the create/modify time on a file, and when scheduling snapshot, antivirus, or Snap Enterprise Data Replicator (EDR) operations. Edit the settings according to local conditions.

NOTE: GuardianOS automatically adjusts for Daylight Saving Time, based on the selected time zone.

3. Change the **Administrator Password**.

The default administrator user name is `admin`, and the default password is also `admin`. To prevent unauthorized access to the SnapServer, enter a new secure password immediately in the fields provided.

NOTE: Passwords consist of 1 to 15 alphanumeric characters and are case-sensitive.

- To continue to the next page, click **Next**.

If you have changed the date, time, or time zone settings in the [General Configuration](#) window above, you may be prompted to log in again before continuing the setup.

TCP/IP Configuration

The next wizard page shows the current TCP/IP information for this SnapServer. All SnapServers come preset to acquire an IP address from a DHCP server.

- If you wish to assign a **static IP** instead of using DHCP, check the box for obtaining a static IP address and enter the following information:
 - The IP address for the SnapServer (required)
 - The subnet mask (required)
 - Any WINS server IP addresses
 - The default gateway IP address
 - The DNS domain name and IP addresses
- Click **Next** to configure the type of RAID storage you want to use.

NOTE: If a Static IP address was entered, the network is restarted automatically (without confirmation from the user) when **Next** is clicked.

RAID Type Selection (DynamicRAID/Traditional RAID)

GuardianOS 7.5 offers the new, powerful DynamicRAID feature that simplifies management of disk additions and replacements in a RAID environment. You can also manually manage the RAID configurations using the Traditional RAID option.

To determine which RAID configuration is appropriate for your needs, see [Should I use DynamicRAID or Traditional RAID?](#) in [Appendix A](#).

1. Click the button to choose either **DynamicRAID** or **Traditional RAID**.

Initial Setup: Configure Storage

Select the type of storage environment that you would like to use on this system.
(Important: Once selected, the storage environment cannot be changed without first deleting all your data.)

DynamicRAID™ (Recommended)

DynamicRAID is a form of RAID developed for GuardianOS which provides simple and flexible storage provisioning. DynamicRAID offers the following benefits over Traditional RAID:

- Flexible Disk Parity - Switch between single-parity and dual-parity dynamically.
- Automatic RAID Creation - New RAID groups are created automatically.
- RAID Expansion - When disks are added to the system, the space is easily incorporated into your existing RAIDs and your data remains accessible.
- Non-Disruptive Disk Upgrades - Migrate an existing RAID array to higher capacity disks without interrupting data access.
- Dynamic Volumes - The size of a volume is adjustable at anytime and can be limited to a specified level.

Traditional RAID

- You manually manage your storage.

Note: With DynamicRAID, the size of a volume is limited to the capacity available in a single physical chassis. If a volume must span across multiple units, or if you need the ability to stripe or mirror data (such as RAID 0, 1, or 10), then you should select Traditional RAID.

[Tell Me More](#) [Next](#)

2. After you have made your selection, click **Next**. You will be prompted to confirm your selection of either **DynamicRAID** or **Traditional RAID**:

Initial Setup: Configure Storage

Important: You have selected a DynamicRAID storage environment. Once selected, the storage environment cannot be changed without first performing a system reset which will delete all of your data.

Are you sure you want DynamicRAID storage?

[Back](#) [Yes, I Want DynamicRAID](#)

Initial Setup: Configure Storage

Important: You have selected a Traditional RAID storage environment. Once selected, the storage environment cannot be changed without first performing a system reset which will delete all of your data.

Are you sure you want Traditional RAID storage? **(Note:** The server will be restarted.)

[Back](#) [Yes, I Want Traditional RAID](#)

3. Click the **Yes option** to continue.

4. Available disks are detected and shown on the **Configure Storage - Detected Disks** page.

Initial Setup: Configure Storage - Detected Disks

Your server's disk slots are fully populated. Click Next to view your storage options.

Detected Disks

Location	Disks Detected	Available Disk Slots
Head Unit Model: VirtualSnap Total disk capacity: 200 GB	4	4

Re-Detect Disks Next

If SnapExpansion units are attached, their available disks are also detected and displayed:

Initial Setup: Configure Storage - Detected Disks

Your server's disk slots are fully populated. Click Next to view your storage options.

Detected Disks

Location	Disks Detected	Available Disk Slots
Head Unit Model: DX2 Total disk capacity: 21.83 TB	12	12
Expansion Unit 1 Model: SE DX Total disk capacity: 30.02 TB	11	12
Expansion Unit 2 Model: SE DX Total disk capacity: 12.74 TB	12	12
Expansion Unit 3 Model: SE DX Total disk capacity: 21.83 TB	12	12
Expansion Unit 4 Model: SE DX Total disk capacity: 6 TB	11	12
Expansion Unit 5 Model: SE DX Total disk capacity: 12.74 TB	12	12
Expansion Unit 6 Model: SE DX Total disk capacity: 22.74 TB	12	12
Expansion Unit 7 Model: SE DX Total disk capacity: 43.66 TB	12	12

Re-Detect Disks Next

NOTE: If you are using expansion units and DynamicRAID, the SnapServer first configures the head unit, then expansion units. For Traditional RAID, the expansion units must be configured separately via **Storage > RAID Sets**.

5. If empty slots exist in either the head or expansion units, new drives can be physically added and then **Re-Detect Disks** clicked to add them to the configuration.

Continue configuring the SnapServer based on the **RAID mode** you selected:

- If you selected **DynamicRAID**, proceed to [DynamicRAID Setup](#) on page 13.
- If you selected **Traditional RAID**, the server will be restarted. Once the server has restarted and you have logged back in, proceed to [Traditional RAID Setup](#) on page 14.

DynamicRAID Setup

The **Configure Storage - Head Unit** page lets you configure your head unit storage by choosing the parity mode and snapshot pool size under DynamicRAID.

Initial Setup: Configure Storage - Head Unit

Use the settings below to create a Storage Pool on your server.
(Note: A volume and share will be created automatically for this Storage Pool.)

Storage Pool configuration is based on these settings:

Pool	Estimated Available Space	Percent of Storage
Data Pool	85.77 GB	80%
Snapshot Pool	21.44 GB	20%

Storage Pool Name:

Parity Mode

Single-parity protection - protects your data in the event of a single disk failure.

Dual-parity protection - uses more disk space than single-parity, yet protects your data in the event of up to 2 disk failures.

Snapshot Pool

If you plan on using snapshots, it is recommended that you reserve at least 20% of your Storage Pool for snapshots. You can adjust the snapshot pool percentage at a later time; however to increase it, you will first need to add more capacity to this Storage Pool.

Percentage of this Storage Pool to reserve for snapshots:

You choose the parity mode to set the data pool size. Options presented are based on the number and available space of disk drives detected in the previous step. See [Parity Management](#) in [Chapter 4](#) for full details.

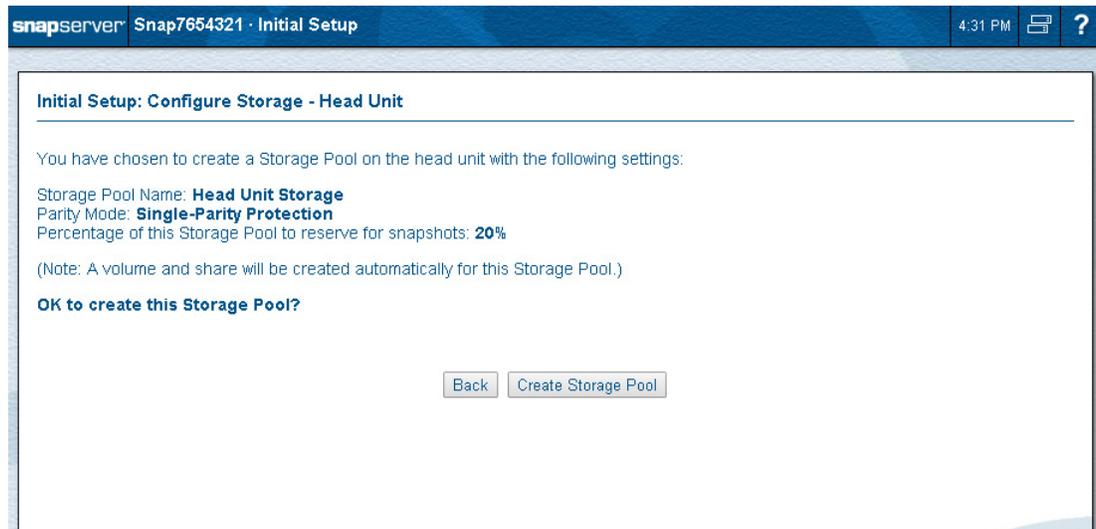
In addition, snapshot space can be reserved using the following guidelines:

- For typical usage, at least 20% snapshot space should be reserved from each storage pool.
- Once snapshot space is set up under DynamicRAID, it can be decreased at any time. However, to increase the size of the snapshot space, either the storage pool must be deleted and re-created, or you must add more storage capacity to your storage pool. See [Snapshots](#) in [Chapter 6](#) for more information.

Configure DynamicRAID Storage

1. Select the **parity mode** from the options provided.
2. Use the drop-down list to choose the size of the **snapshot pool**.
3. After you have made your selections, click **Next**.

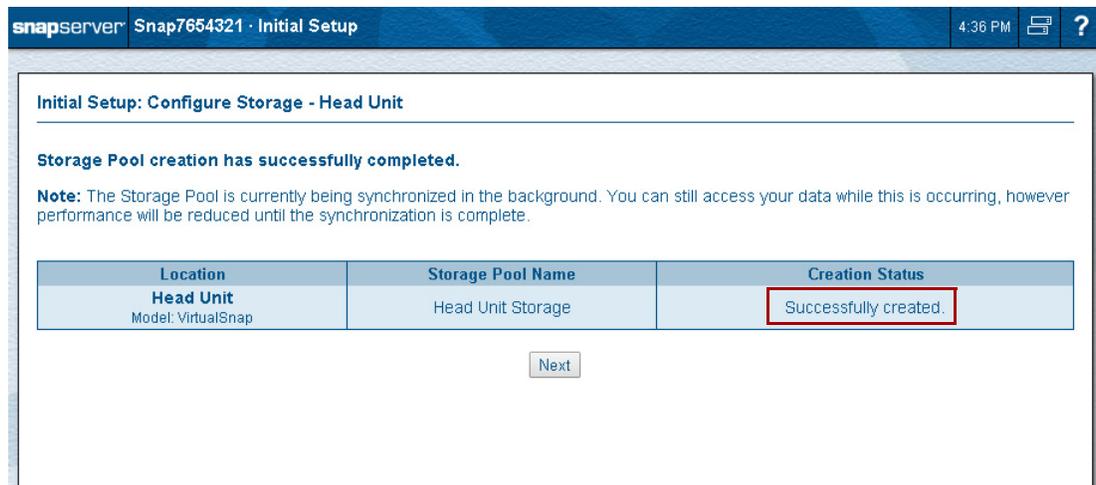
- At the confirmation page, click **Create Storage Pool**.



NOTE: If a disk in the storage pool has previously been used in a different system, it will be reformatted and all data on the disk will be deleted.

The hard drives are configured to create a usable storage pool that can be divided into volumes for different applications or user groups. See [Additional Information on DynamicRAID Sizing](#) in [Appendix A](#) for more details.

- When the storage pool has been successfully created on the head unit, a summary page is shown. Once the **Successfully created** status is shown, click **Next** to continue.



Next steps:

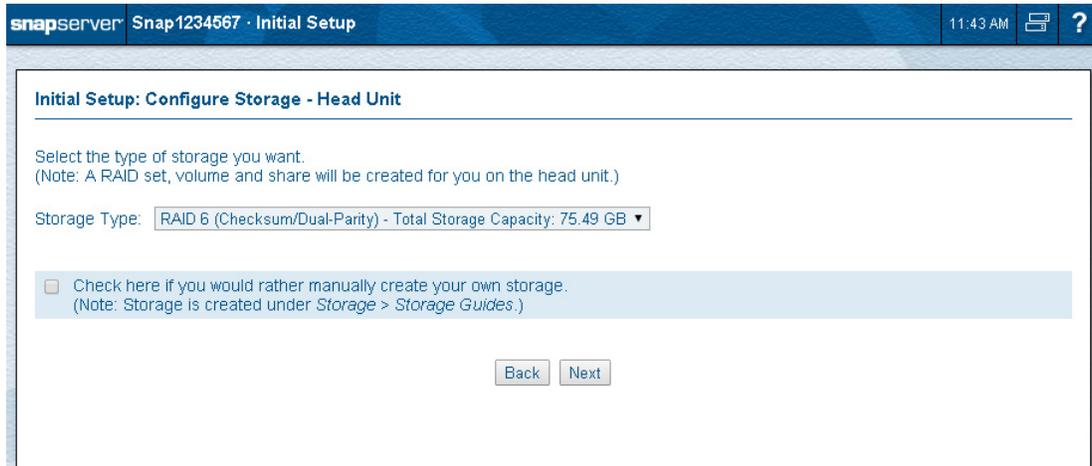
- If you are using SnapExpansion units, their configuration automatically starts next. Continue with [Configure Expansion Units](#) on page 16.
- Otherwise, continue with [Setup Completion](#) on page 18.

Traditional RAID Setup

Once Traditional RAID is selected, the wizard continues with the setup of the head unit.

NOTE: In Traditional RAID, only the head unit is configured during the setup process. If you are using expansion units, they are configured manually after the setup wizard is complete ([Storage > RAID Sets](#)).

The next page lets you manually configure your head unit storage by selecting the RAID type based on the installed disk drives. See [Factors in Choosing a RAID Type](#) in [Chapter 5](#).



Initial Setup: Configure Storage - Head Unit

Select the type of storage you want.
(Note: A RAID set, volume and share will be created for you on the head unit.)

Storage Type: RAID 6 (Checksum/Dual-Parity) - Total Storage Capacity: 75.49 GB

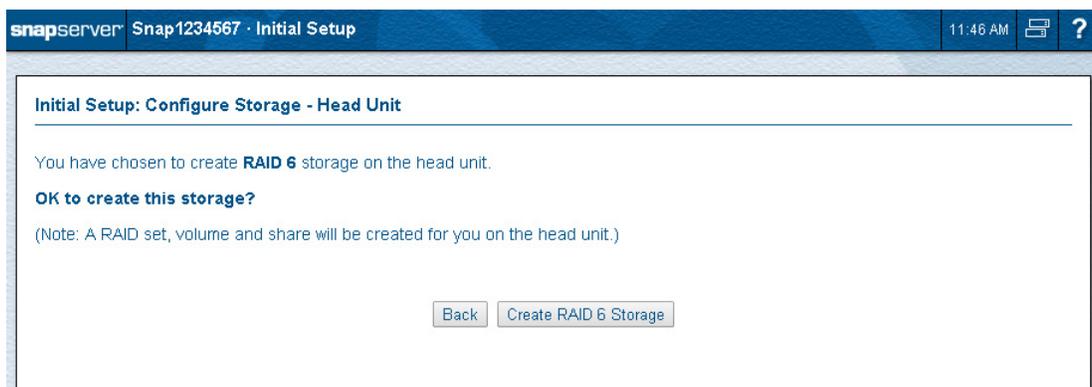
Check here if you would rather manually create your own storage.
(Note: Storage is created under [Storage > Storage Guides](#).)

Back Next

1. Choose **one** of the following:
 - From the drop-down list, select the predefined **storage type** (RAID) available based on units and drives installed.
 - Check the **Check here if you would rather manually create your own storage** checkbox.
2. Click **Next** to accept the settings.

NOTE: If the manual storage creation option was checked, you will be asked to confirm this choice at the next prompt and the wizard exits. You must go to [Storage > Storage Guides](#) to complete the storage setup process.

3. At the confirmation page, click **Create RAID n Storage** to proceed.



Initial Setup: Configure Storage - Head Unit

You have chosen to create **RAID 6** storage on the head unit.

OK to create this storage?

(Note: A RAID set, volume and share will be created for you on the head unit.)

Back Create RAID 6 Storage

A RAID set, volume, and share are all created automatically on the head unit with the default space reserved for snapshots equal to 20% of the volume's size.

Configure Expansion Units

If you are using expansion units with DynamicRAID, the SnapServer will recognize them during the setup process, and you can configure storage pools on them. After the setup is complete, expansion units can be managed via **Storage > Storage Pools**.

NOTE: If you are using Traditional RAID, expansion units can only be configured manually after the setup process is complete (using **Storage > RAID Sets**).

For more information on expansion units, see [Expansion Units](#) in [Chapter 1](#).

1. During the setup of a DynamicRAID system, after the head unit is configured, you are prompted to create the storage pools on the expansion units. Select the **parity mode** and **snapshot pool size** for each expansion unit.

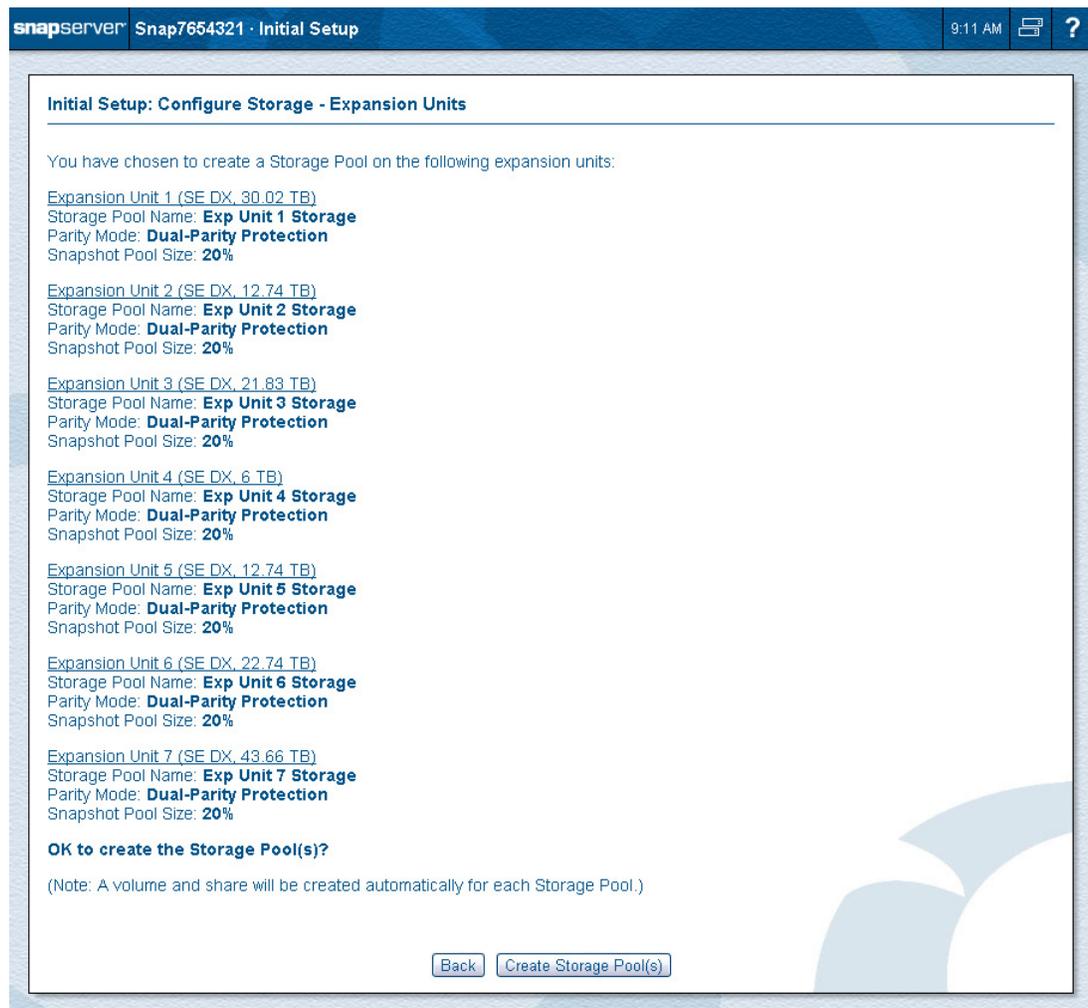
The screenshot shows the 'Initial Setup: Configure Storage - Expansion Units' screen. It features a table with columns for Location, Storage Pool Name, Parity Mode, and Snapshot Pool Size. The table lists the Head Unit and seven Expansion Units (1-7) with their respective models and disk capacities. Each expansion unit has a text input field for the Storage Pool Name, a dropdown menu for Parity Mode (set to 'Dual'), and a dropdown menu for Snapshot Pool Size (set to '20%'). Below the table are 'Back' and 'Next' buttons, and a note: '(Click Next to review and confirm your expansion unit settings.)'

Location	Storage Pool Name	Parity Mode	Snapshot Pool Size
Head Unit Model: DX2 Total disk capacity: 21.83 TB	Head Unit Storage	Dual	20%
Expansion Unit 1 Model: SE DX Total disk capacity: 30.02 TB	Exp Unit 1 Storage	Dual	20%
Expansion Unit 2 Model: SE DX Total disk capacity: 12.74 TB	Exp Unit 2 Storage	Dual	20%
Expansion Unit 3 Model: SE DX Total disk capacity: 21.83 TB	Exp Unit 3 Storage	Dual	20%
Expansion Unit 4 Model: SE DX Total disk capacity: 6 TB	Exp Unit 4 Storage	Dual	20%
Expansion Unit 5 Model: SE DX Total disk capacity: 12.74 TB	Exp Unit 5 Storage	Dual	20%
Expansion Unit 6 Model: SE DX Total disk capacity: 22.74 TB	Exp Unit 6 Storage	Dual	20%
Expansion Unit 7 Model: SE DX Total disk capacity: 43.66 TB	Exp Unit 7 Storage	Dual	20%

(Click Next to review and confirm your expansion unit settings.)

2. Click Next.

3. Review your storage pool configuration. When you are done, click **Create Storage Pools** to create the storage pools on the expansion units (or **Back** to make changes).



A screen appears showing the creation of the storage pools on the expansion units. The creation of the storage pools may take several minutes.

4. When the expansion units' storage pools have been created, click **Next** to continue with the completion steps.

Setup Completion

Once the head unit and all the DynamicRAID expansion units are configured, the **Initial Setup - Complete** page is shown:

Initial Setup: Complete

Your server's storage is ready to use and is configured with the following Storage Pool(s):

Storage Pool	Usable Storage Space
Head Unit Storage	13 TB
Exp Unit 1 Storage	19.56 TB
Exp Unit 2 Storage	7.18 TB
Exp Unit 3 Storage	13.73 TB
Exp Unit 4 Storage	3.84 TB
Exp Unit 5 Storage	7.18 TB
Exp Unit 6 Storage	14.46 TB
Exp Unit 7 Storage	29.01 TB

You can manage Storage Pools under *Storage > Storage Pools*, volumes under *Storage > Volumes* and shares under *Security > Shares*.

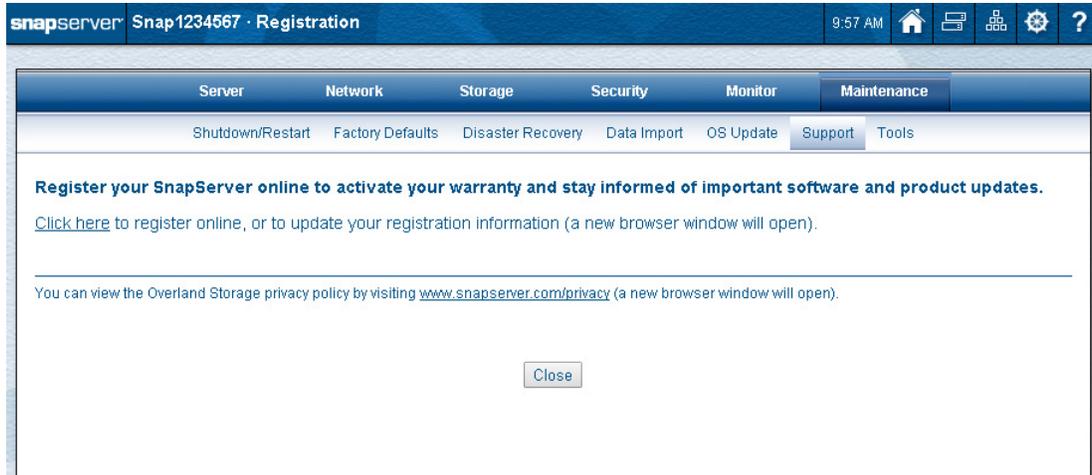
Note: Storage Pool(s) are currently being synchronized in the background. You can still access your data while this is occurring, however performance will be reduced until the synchronization is complete.

The setup process is now complete. Click OK to continue administering the server.

1. Click **OK** to finish the setup process.
Storage Pools will be synchronizing in the background. You can still access your data while this is occurring, however performance will be reduced until the synchronization is complete.
2. If you have changed the **server name**, you will be prompted to **restart**. Click **Restart** to continue.
The server will restart and your browser will automatically reconnect to the server.
Log in again when prompted to do so.
3. You are prompted to **register** your system.
It is important that you register your system to activate the warranty coverage. Proceed to the [Registration Page](#) on [page 19](#).

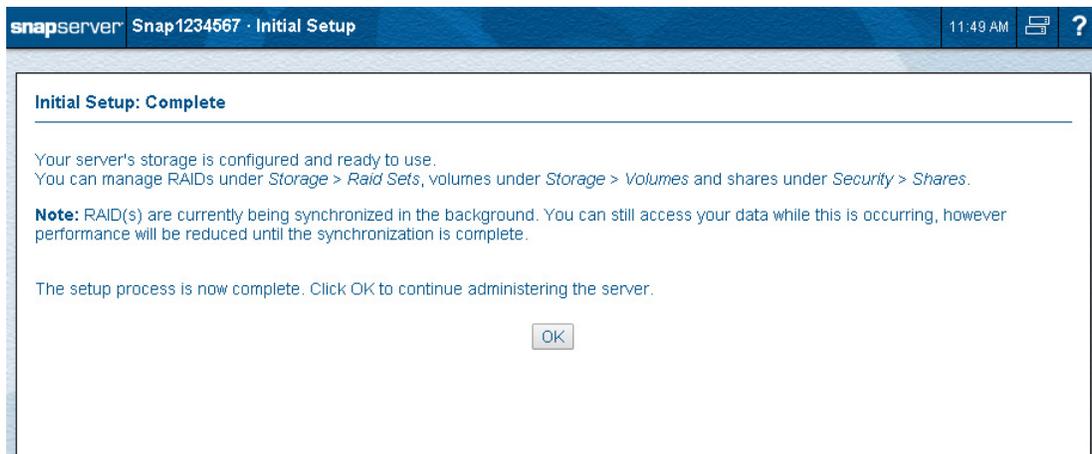
Registration Page

After the setup wizard is done, you are given a chance to register your SnapServer. The **Registration** page appears (this page can also be accessed by clicking **Maintenance > Support > Registration**). Click as indicated to launch the Overland Storage Support website.



 **IMPORTANT:** Because technical and warranty service are not available until your appliance is registered, it is recommended that you do so at this time. Registration is quick and easy.

Once registration is complete, you can check the box to no longer be reminded. Then click **Close** to finish your setup.



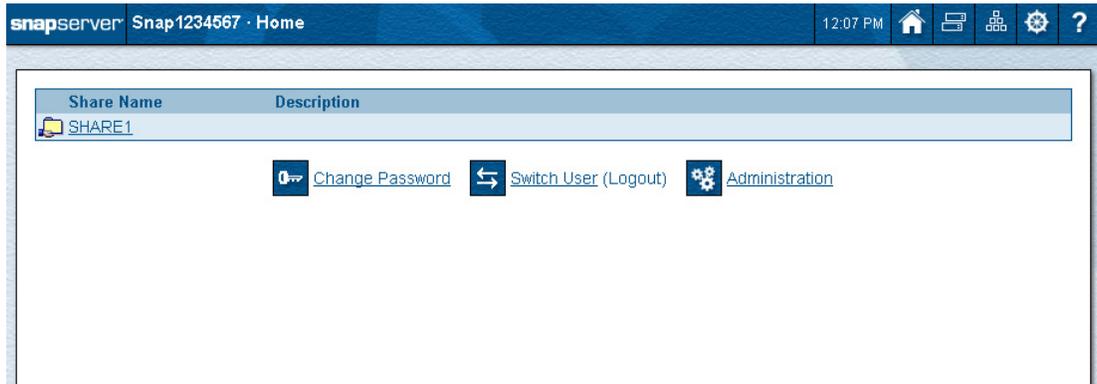
Click **OK** to be taken to the **Admin Home** page.

Server Status and Site Map

SnapServer appliances running GuardianOS 7.5 use a web-based graphical user interface (GUI) called the **Web Management Interface**. It supports most common web browsers, including Internet Explorer 7 and higher, Firefox 3 and higher, Apple Safari 5, and Google Chrome 9 and higher. JavaScript must be enabled in the browser.

When initially connecting to the server with a web browser, the Home page of the Web Management Interface is displayed. This page shows any shares at the top, the three primary options below the shares list, and has special navigation buttons displayed on the right side of the title bar (see the next table).

NOTE: If you haven't gone through the initial setup or authentication is required, you may be prompted to log in when you first access the Web Management Interface.



The **Home** page displays the following icons and options:

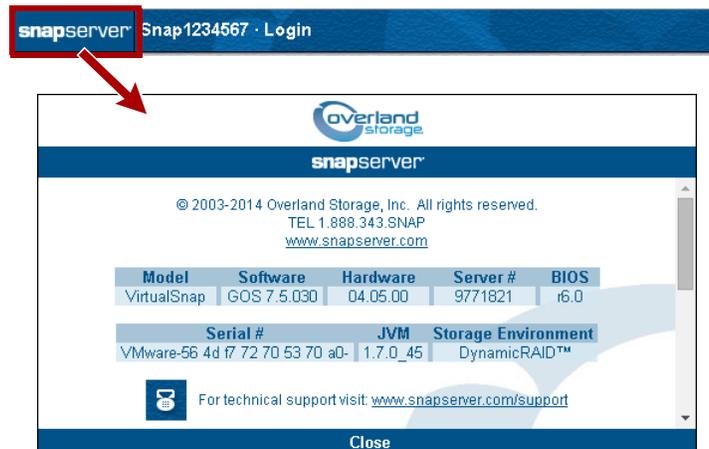
Icons & Options	Description
Change Password 	Click to access the password change page. Passwords are case sensitive. Use up to 15 alphanumeric characters.
Switch User (Logout) 	Click to log out as the current user and open the login dialog box to log in as a different user.
Administration 	Click to administer the server. If you are not yet logged in, you are prompted to do so.
Navigation Buttons	<p>The following Navigation buttons are present in the upper right on every Web Management Interface page:</p> <p>Home – Click this to switch between the Home page and the Admin Home page. If you have not yet logged in to the Admin Home page, only the Home page is available.</p> <p>Snap Finder – Click this to view a list of all SnapServers found on your network and to specify a list of remote servers that will be used to discover SnapServers on other subnets. You can access these servers by clicking the listed name or IP address.</p> <p>SnapExtensions – Click this to view the SnapExtensions page, where you can acquire licenses for and configure third-party applications.</p> <p>Site Map – Click this to view a Site Map of the available options in the Web Management Interface, where you can navigate directly to all the major utility pages. The current page is shown in orange text.</p> <p>Help – Click this to access the online help for the UI page you are viewing.</p>
	
	
	
	
	

Icons & Options	Description
UI Appearance	Click the Mgmt. Interface Settings link in the Site Map to choose a background for the Web Management Interface. You can select either a solid-colored background or a textured-graphic background.

For more information, see [Home Pages](#) in [Chapter 10](#).

Hardware Information

From the Web Management Interface, click the SnapServer logo in the upper left corner to display the pertinent hardware information and contact links and information:

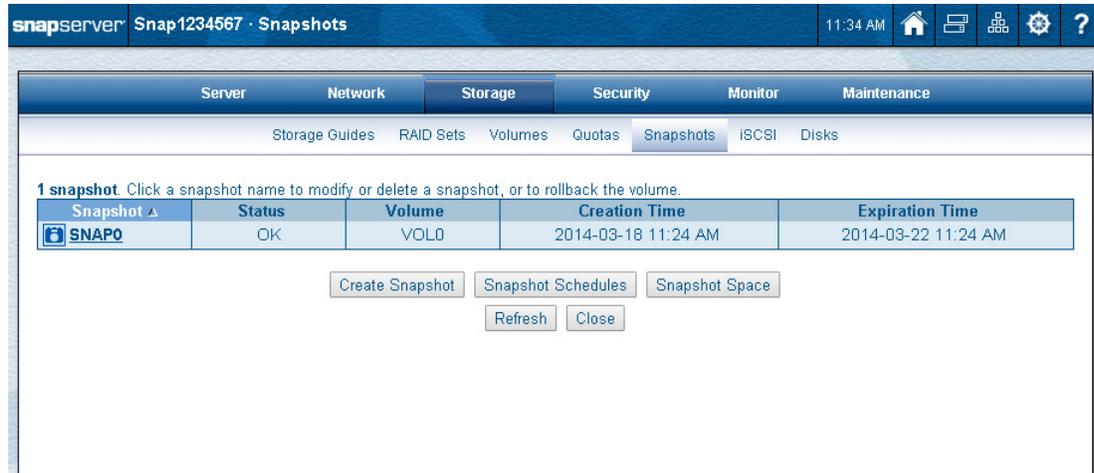


Scroll down to view additional contact information. Click **Close** (or outside the box) to dismiss.

Scheduling Data Protection Tasks

Scheduling backups, snapshots, and antivirus scans, and creating a disaster recovery image preserves your server configuration and protects your data from loss or corruption. Snapshots can be taken to provide a point-in-time image of files and changes to files to help in quickly recovering from accidental deletion or modification, or to facilitate performing an offline tape backup of an active data partition.

Navigate to **Storage > Snapshots** in the browser-based Web Management Interface to create or schedule snapshots.



Snapshots should be taken when the system is idle or under low data traffic. To modify the space available for storing snapshots:

- For DynamicRAID mode, go to **Storage > Storage Pools** and click the storage pool name ([Storage Pool Properties](#) on [page 70](#)).
- For Traditional RAID mode, go to **Storage > Snapshots > Snapshot Space** ([Storage Pools](#) on [page 66](#)).

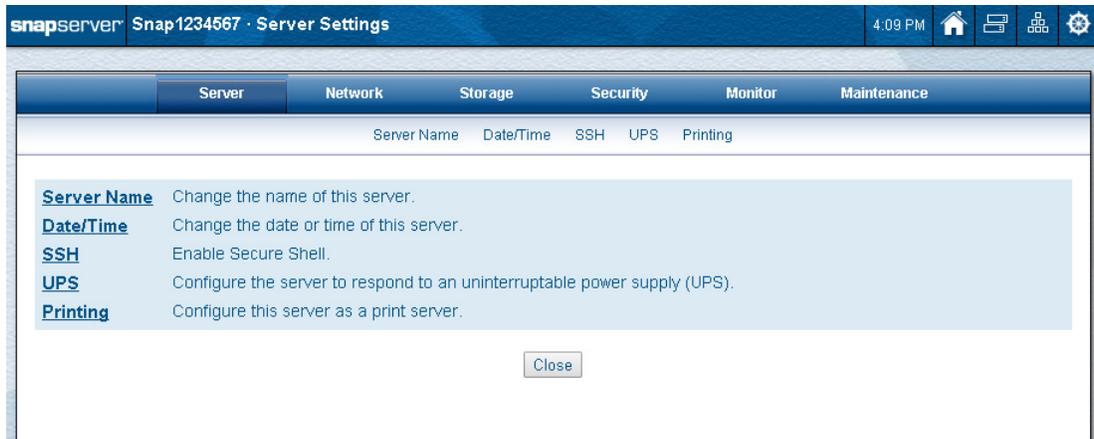
Set up antivirus protection by clicking the **SnapExtensions** icon () and then clicking **CA Antivirus**. Click the checkbox to enable antivirus, and click **OK**. When the configuration link appears, click it to launch the administration user interface for configuration and scheduling of virus scans and virus signature file updates.

Create a disaster recovery image on the **Maintenance > Disaster Recovery** page. This image should be created after the server configuration is complete, and can be used to recover the server or a replacement server to the configured state. See [Disaster Recovery](#) in [Chapter 9](#) for detailed information on creating and using disaster recovery images.

GuardianOS contains built-in support for Snap EDR (trial mode) to synchronize and back up to and from other SnapServers. GuardianOS also supports several third-party backup agents. For information on using these backup methods to help protect your data, see [Backup Solutions](#) in [Appendix B](#).

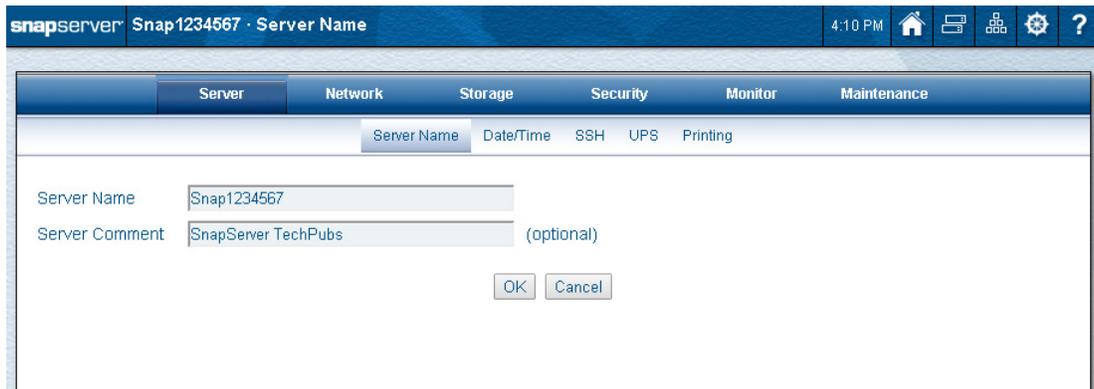
Server Options

By clicking either the Administration link (or using the GuardianOS 7.5 site map link ()), you have immediate access to five editable server options.



Server Name

Use this option to change the server name and add a comment.



1. Edit the following **fields**:

Option	Description
Server Name	<p>The default server name is SNAPnnnnnnn, where nnnnnnn is your server number.</p> <p>For example, the default name for a SnapServer with the serial number 1234567 would be Snap1234567.</p> <p>If desired, enter a unique server name of up to 15 alphanumeric characters. In addition to letters and numbers, you can also use a dash (-) between characters, but spaces are not allowed.</p> <p>NOTE: The server number can be found on the Monitor > System Status page.</p>
Server Comment	Optionally, add a comment (for example, server location) specific to the server.

2. Click **OK** to save the changes.

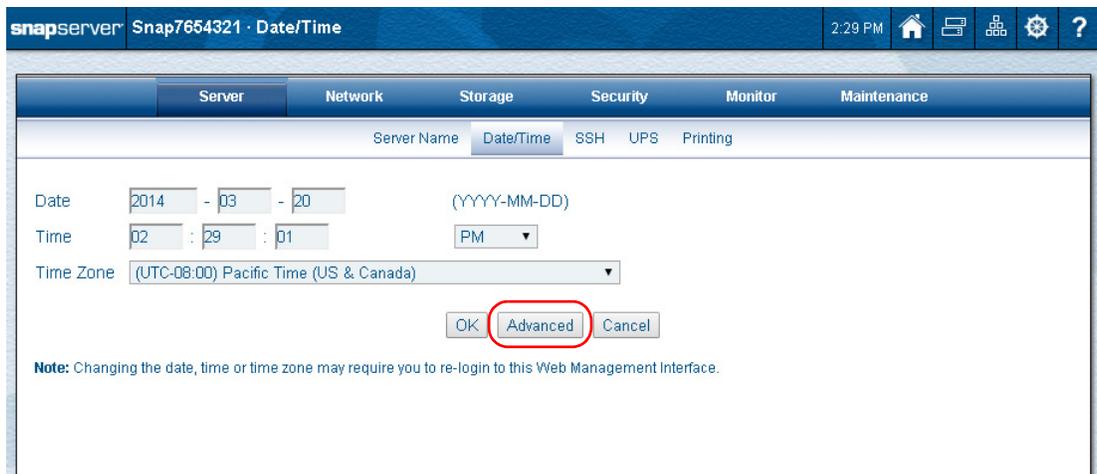
Date/Time

Use this page to configure date and time settings in ISO 8601 formatting. The time stamp applies when recording server activity in the **Event Log (Monitor tab)**, when creating or modifying files, and when scheduling snapshot or antivirus operations.

CAUTION: If the current date and time are reset to an earlier date and time, the change does not automatically propagate to any scheduled events you have already set up for snapshot, antivirus, or Snap EDR operations. These operations will continue to run based on the previous date and time setting. To synchronize these operations with the new date and time settings, you must reschedule each operation.

Configure the Date and Time Settings

If NTP was not selected during the setup process, only the manual configuration is shown:



2:29 PM

Server Network Storage Security Monitor Maintenance

Server Name Date/Time SSH UPS Printing

Date 2014 - 03 - 20 (YYYY-MM-DD)

Time 02 : 29 : 01 PM

Time Zone (UTC-08:00) Pacific Time (US & Canada)

OK Advanced Cancel

Note: Changing the date, time or time zone may require you to re-login to this Web Management Interface.

Click **Advanced** to display all options:



1. Choose to either manually enter or automatically synchronize (using NTP servers) the **date and time**:

- **Manually** – Select the first button, enter the correct date and time in the appropriate fields, and use the drop-down list to choose either AM or PM.
- **Automatically** – Select the second button and enter a valid NTP server IP address or host name. Optionally, enter a second address or name for a second server.

NOTE: For security reasons, NTP cannot be used with Active Directory domains.

2. If automatic synchronization to NTP servers is selected, to use this SnapServer as an NTP server, check the **enable box**.
3. From the drop-down list, select the **time zone**.

NOTE: GuardianOS automatically adjusts for Daylight Saving Time, depending on your time zone.

4. Click **OK**.

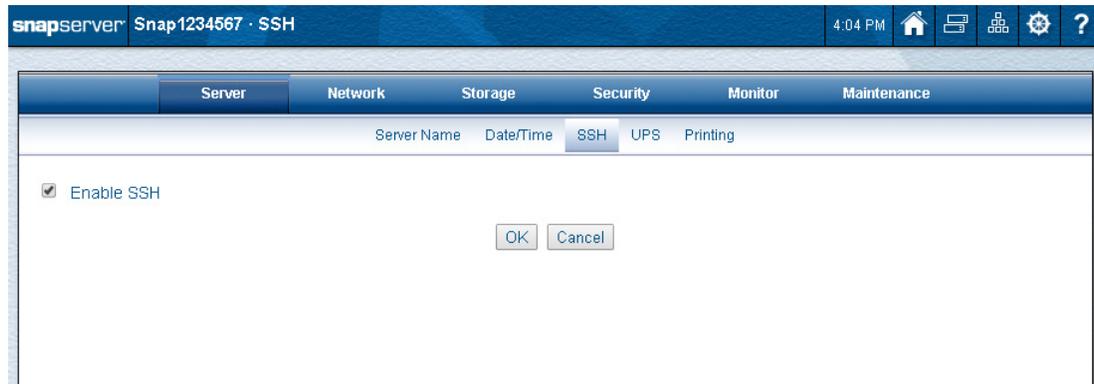
Secure Shell

Secure Shell (SSH) is a service that provides a remote console to access a command line shell that allows the user to perform basic management and update functions outside the GuardianOS Web Management Interface. See [Command Line Interface](#) on [page 252](#) for more information. The SSH implementation requires SSH v2.

NOTE: To maintain security, consider disabling SSH when not in use.

Disable SSH

SSH is enabled by default. To disable SSH, at the **SSH** page, uncheck the **Enable SSH** box, and click **OK**.



Connect to the CLI using SSH

1. Verify that your remote machine has an **SSH client application** installed.
Free or low-cost SSH applications are available from the Internet.
2. Connect to the server using its **IP address**.
Before the Initial Setup Wizard is completed and storage is configured, SnapCLI disables and hides all standard commands and makes only the system command available. See [Before You Begin](#) in [Appendix E](#).
3. Log in as **admin**.

NOTE: SSH v2 is required. If you fail to connect to the server, ensure that your SSH client is configured to connect via SSH v2.

You will automatically be placed in the CLI shell.

UPS Protection

SnapServers support automatic shutdowns when receiving a low-power warning from an APC uninterruptible power supply (UPS). Use this page to manage this feature:

12:20 PM

Server Name Date/Time SSH UPS Printing

You can configure this server to automatically shut down when a low power warning is sent from a USB- or network-based uninterruptible power supply (UPS). Currently, only APC® brand UPS devices* are supported.

Enable UPS Support

Automatically restart server when power is restored or UPS comes back online

Use a single USB-connected UPS device

Use the following network-connected UPS device(s):

Primary UPS Device

IP Address

APC User Name (for authentication)

APC Authentication Phrase

OK Refresh Cancel

*UPS technology copyright © 2001 American Power Conversion Corporation.

NOTE: If you are not using a UPS and your server supports disabling write cache, consider disabling write cache to help protect your data in case of a power outage.

An APC Smart-UPS® series device allows the SnapServer to shut down gracefully in the event of an unexpected power interruption. You can configure the server to automatically shut down when a low power warning is sent from an APC network-enabled or USB-based UPS device (some serial-only APC UPS units are also supported by using the IOGear GUC232A USB to Serial Adapter Cable). To do this, you must enable UPS support on the SnapServer, as described in this section, to listen to the IP address of one or two APC UPS units, and you must supply the proper authentication phrase configured on the UPS. Some SnapServer products have a single power supply, allowing you to attach a single UPS device. Other products have dual power supplies, allowing you to attach two UPS devices.

NOTE: Select a UPS capable of providing power to the SnapServer for at least ten minutes. In addition, in order to allow the SnapServer sufficient time to shut down cleanly, the UPS should be able to provide power for at least five minutes after entering a low battery condition.

Procedure to Configure UPS Protection

1. Complete the following **fields**:

Option	Description
Enable UPS Support	Check the Enable UPS Support check box to enable; leave the check box blank to disable UPS support.
Automatically restart server...	Check this box to automatically restart the server when power has been restored or the UPS comes back online. Leave the check box blank to manually start the server after a power failure.
Use a single USB-connected UPS device	Select this option button to use a USB-connected APC UPS device or serial UPS with USB to serial adapter cable. NOTE: If using a serial UPS with a USB-to-serial adapter cable, reboot the SnapServer after connecting the cable to the server to properly initialize the connection to the UPS.
APC Status	Under the selected UPS connection type, an APC status field will display the following possible values: Unknown, No Connection, Low Battery, On Battery, and Online.
Use the following network-connected UPS devices	Select this option button to use up to two network-connected APC UPS devices.
IP Address	Enter the IP address of the network UPS device.
APC User Name	Enter the APC Administrator user name. NOTE: The APC user name entered must be the APC Administrator name for the UPS (by default, apc).
APC Authentication Phrase	Enter the authentication phrase configured for shutdown behavior on the UPS (in the UPS Web UI, this can be configured in PowerChute settings or, for older firmware, in the User Manager for the administrator user). NOTE: This password phrase is not the same as the user's password.
Secondary UPS device (optional)	Check the Secondary UPS device check box to enable; leave the check box blank to disable secondary UPS support.
Low Battery Alert	Select one of the following: <ul style="list-style-type: none"> • Either UPS Device: Select this option to allow shutdown upon receipt of a message from either of the two specified UPS servers. • Both UPS Devices: Select this option to allow shutdown only upon receipt of one message from each of the two specified UPS servers.

2. Click **OK** to finish.

Print Server

The SnapServer can be configured to emulate a Windows print server for locally-attached USB printers or IPP printing. Client machines connect to the SnapServer over the network and use the printer similarly to using a printer shared by a Windows or CUPS server. You can pause or resume the printer, and monitor or cancel print jobs using the Web Management Interface.



Configuring your as a print server is a two-part process:

- Step 1:** Configure the **printer** on the SnapServer.
- Step 2:** Configure the **client** to print via the SnapServer.

Procedure to Configure the Printer

First, you need to configure the printer connected to the SnapServer.

1. Check **Enable printing support**.
2. Connect a printer to one of the **USB ports** on the SnapServer.
3. Power **ON** the printer.
4. In the SnapServer Web Management Interface, navigate to **Server > Printing**.
A list of currently defined USB printers is displayed.
5. To add the new printer, click **Add Local Printer**.
6. The SnapServer will detect the new printer and show it as an option in the **Local Printer Device** drop-down list. Select that **printer**.
7. **Name** the printer and, if desired, complete Description and Location information.
8. Click **OK**.
The printer will appear in the list on the main printing page.

Procedure to Configure the Client

Next, add the printer to a Windows, Mac, or Linux client, enabling you to print via the SnapServer. The SnapServer supports both Windows SMB and IPP printing protocols.

NOTE: To make printer drivers easily accessible to users, copy them to a share that everyone can access on the SnapServer. The SnapServer cannot be configured to automatically provide printer drivers to clients.

Adding the Network Printer to a Windows Client

Windows offers several methods for adding a printer. Follow your usual printer configuration method to add a printer shared on a SnapServer. When asked to locate the printer:

- To use SMB, enter the SnapServer name or IP address, or browse to the server to choose the printer share.
- To use IPP, enter the exact path as follows in the URL field:
`http://servername:631/printers/sharename`
where *servername* is the name or IP address of your SnapServer and *sharename* is the name of the printer.

NOTE: 631 is the IPP port number.

If you experience difficulty adding the printer, try the following:

1. Navigate to **Start > Run** and enter the server name as follows:
`\\servername`
2. After a delay, you may be prompted for a user name and password. Log in as a user with access to the SnapServer.
3. A Windows Explorer window opens displaying all shares and printers on the server. Right-click the server and choose **Connect**.
4. Follow the instructions to provide the printer driver and complete the setup.

To Add a Network Printer to a Mac OS X Client

Add a printer using your usual method. If you are using SMB, you will need to know the SnapServer name. If you are using IPP, you will need to enter the IP address in the **Type** field and the printer and sharename in the **Queue** field.

To Add a Network Printer to a Linux Client

Add a printer using your usual method. If you are using SMB, you will need to know the SnapServer name. If you are using IPP, enter the exact path as follows in the URL field:

```
http://servername:631/printers/sharename
```

where *servername* is the name or IP address of your SnapServer and *sharename* is the name of the printer.

NOTE: 631 is the IPP port number.

To Monitor Print Jobs Remotely

Pause or resume the printer, and check the status of or cancel print jobs from the SnapServer Web Management Interface.

To Pause the Printer

Use this procedure to pause the printer:

1. Navigate to **Server > Printing**.
2. Click the **Status** link next to your printer to open the **Job Status** window and see your print job queue.

3. Click the **Pause Printer** button to pause all print jobs.

When the printer is paused, the button becomes a **Resume Printer** button, which you can click to resume printing.

To Cancel or Check the Status of Print Jobs

Use this procedure to cancel or check the status of a print job:

1. Navigate to **Server > Printing** and click the **Status** link next to your printer to open the Job Status window and see your print job queue.
2. To cancel a print job, click to put a check in the box next to the job you want to remove and click **Cancel Selected Jobs**. You can select to cancel multiple jobs. If you want to cancel all the listed print jobs, click the **Cancel All Jobs** button. Click the **Refresh** button to update the page with the current list of print jobs.

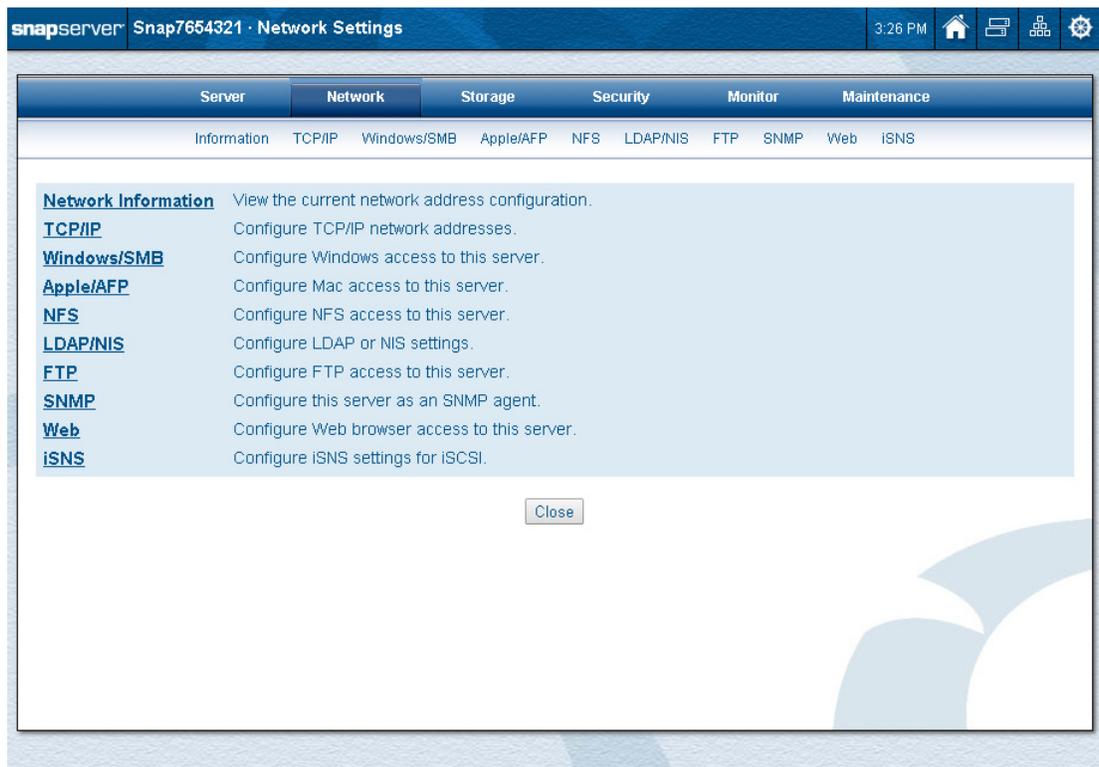
To Delete a Printer

When you remove a printer, remember to remove its information from both the Web Management Interface and the client machines.

1. Disconnect the printer cable from the SnapServer.
2. In the Web Management Interface, navigate to **Server > Printing**. In the list of printers, the status of printer you just removed should appear as **Offline**.
3. Click the printer link to open the **Edit Printer** page, then click the **Delete** button to delete the printer.

This chapter addresses the network options for configuring TCP/IP addressing, network bonding, and access protocols.

SnapServers are preconfigured to use DHCP, to autonegotiate network settings, and to allow access to the server for Windows (CIFS/SMB1/SMB2), Unix (NFS), Mac (AFP), FTP/FTPS, and HTTP/HTTPS clients. Network bonding options allow you to configure the SnapServer for load balancing and failover. Network protocols control which network clients can access the server.



Topics in Network:

- [View Network Information](#)
- [TCP/IP Networking Options](#)
- [Windows Networking \(SMB\)](#)
- [Apple Networking \(AFP\)](#)
- [NFS Access](#)
- [LDAP and NIS Domains](#)
- [FTP/FTPS Access](#)

- [SNMP Configuration](#)
- [Web Access](#)
- [iSNS Configuration](#)

 **IMPORTANT:** The default settings enable access to the SnapServer via all protocols supported by the SnapServer. As a security measure, disable any protocols not in use. For example, if no Mac or FTP clients need access to the SnapServer, disable these protocols in the Web Management Interface.

View Network Information

Browse to **Network > (Network) Information** to access the **Network Information** page that displays the server's current network settings. One column appears for each Ethernet port in use.



Ethernet Interface Information		
Port Name	Ethernet 1 (Primary Interface)	Ethernet 2
Enabled	Yes	Yes
TCP/IP Mode	Static	DHCP
IP Address	10.25.3.35	10.25.3.10
Subnet Mask	255.255.0.0	255.255.0.0
Primary WINS Server	-	-
Secondary WINS Server #1	-	-
Secondary WINS Server #2	-	-
Secondary WINS Server #3	-	-
Ethernet Address	00:0C:29:8B:BF:3D	00:0C:29:8B:BF:47
Speed Status	1000 Mbps (Auto)	1000 Mbps (Auto)
Duplex Status	Full Duplex (Auto)	Full Duplex (Auto)
Bonding Status	Standalone	Standalone
Gateway Information		
Default Gateway	10.25.1.1	
DNS Information		
Domain Name	devnet.myoverland.net	
Primary DNS	10.6.8.34	
Secondary DNS #1	10.6.8.35	
Secondary DNS #2	-	

Field definitions for the **Network Information** page are given in the following table:

Ethernet Interface Information	
Port Name	The names of the Ethernet interfaces.
Enabled	Yes or No.
TCP/IP Mode	DHCP or Static.
IP Address	The unique 32-bit value that identifies the server on a network subnet.

Ethernet Interface Information	
Subnet Mask	Combines with the IP address to identify the subnet on which the server is located.
Primary WINS Server	The Windows Internet Naming Service server which locates network resources in a TCP/IP-based Windows network by automatically configuring and maintaining the name and IP address mapping tables.
Secondary WINS Servers (#1, #2, and #3)	Secondary Windows Internet Naming Service servers. Up to three secondary servers can be used.
Ethernet Address	The unique six-digit hexadecimal (0-9, A-F) number that identifies the Ethernet port.
Speed Status	10 Mbps, 100 Mbps, or 1000 Mbps.
Duplex Status	Half-duplex: two-way data flow, only one way at a time. Full-duplex: two-way data flow simultaneously.
Bonding Status	Standalone, Load Balance (ALB), Failover, Switch Trunking, or Link Aggregation.
Gateway Information	
Default Gateway	The network address of the gateway is the hardware or software that bridges the gap between two otherwise unroutable networks. It allows data to be transferred among computers that are on different subnets.
DNS Information	
Domain Name	The ASCII name that identifies the Internet domain for a group of computers within a network.
Primary DNS	The IP address of the primary Domain Name System server that maintains the list of all host names.
Secondary DNS (#1 and #2)	Up to two secondary Domain Name System servers can be used.

TCP/IP Networking Options

SnapServers ship with one or more Gigabit Ethernet (GbE) ports. The information about those ports is displayed on the primary **TCP/IP Networking** page:

The screenshot shows the SnapServer web interface for TCP/IP Networking. The top navigation bar includes 'Server', 'Network', 'Storage', 'Security', 'Monitor', and 'Maintenance'. Under 'Network', there are sub-tabs for 'Information', 'TCP/IP', 'Windows/SMB', 'Apple/AFP', 'NFS', 'LDAP/NIS', 'FTP', 'SNMP', 'Web', and 'ISNS'. The main content area contains a table with the following data:

Port/Bond	Status	IP Address	Bond Type	Modified
Ethernet 1	OK (Primary Interface)	10.25.3.35 (static)	Standalone	No
Ethernet 2	OK	10.25.3.10 (DHCP)	Standalone	No

Below the table are three buttons: 'OK', 'Create Bond', and 'Cancel'.

The following table for the **TCP/IP Networking** page describes the port information:

Column	Description
Port/Bond	A list of the Ethernet ports or bonds on the server. Click a port or bond name to display or modify configuration details. See Configuring Port Properties on page 37.
Status	<ul style="list-style-type: none"> • OK – Port is connected and active. • No link – Port is not connected. • Failed – Port has failed.
IP Address	<ul style="list-style-type: none"> • The IP address for the NIC or bond if known or not available if unknown. • Whether the IP address was obtained by DHCP or is Static.

Column	Description
Bond Type	<p>NOTE: If you have more than two ports, you can have a mixture of standalone and bonded ports. For example, on a 4-port system, one port can be a standalone and the other three ports can be bonded into a load balanced configuration.</p> <ul style="list-style-type: none"> • Standalone – The default state <i>Standalone</i> is the absence of network bonding and treats each port as a separate interface. • Load Balance (ALB) – An intelligent software adaptive agent repeatedly analyzes the traffic flow from the server and distributes the packets based on destination addresses, evenly distributing network traffic for optimal network performance. All ports in the same ALB configuration need to be connected to the same switch. • Failover – This mode uses one Ethernet port (by default, <i>Ethernet 1</i>) as the primary network interface and a one or more Ethernet ports are held in reserve as the backup interface. Redundant network interfaces ensure that an active port is available at all times. If the primary port fails due to a hardware or cable problem, the second port assumes its network identity. The ports should be connected to different switches (though this is not required). <p>NOTE: Failover mode provides switch fault tolerance, as long as ports are connected to different switches.</p> <ul style="list-style-type: none"> • Switch Trunking – This mode groups multiple physical Ethernet links to create one logical interface. Provides high fault tolerance and fast performance between switches, routers, and servers. Both ports of the bond need to be connected to the same physical or logical switch, and the switch ports must be configured for static link aggregation. • Link Aggregation (802.3ad) – This method of combining or aggregating multiple network connections in parallel is used to increase throughput beyond what a single connection could handle. It also provides a level of redundancy in case one of the links fails. It uses Link Aggregation Control Protocol (LACP), also called dynamic link aggregation, to autonegotiate trunk settings. Both ports of the bond need to be connected to the same switch or logical switch.
Modified	<p>Indicates whether configuration for one or more interfaces has been changed and needs to be applied to take effect:</p> <ul style="list-style-type: none"> • Yes – One or more parameters for the interface have been modified. • No – None of the parameters for the interface have been modified.

Configuring Port Properties

To configure the TCP/IP properties of a specific port or bond, click the name in the table on the **TCP/IP Networking** page. A **TCP/IP Port Properties** page displays the configuration options for the Ethernet port selected.

The screenshot shows the 'SnapServer' interface for 'Snap1234567' on the 'TCP/IP Port Properties' page. The 'Network' tab is active, and the 'TCP/IP' sub-tab is selected. The configuration is for 'Ethernet 1'. The 'Enable Ethernet 1' checkbox is checked. Under 'Use the settings below', the IP Address is 10.25.3.35, Subnet Mask is 255.255.0.0, and Default Gateway is 10.25.1.1. DNS Domain Name is devnet.myoverland.net. Domain Name Servers are 10.6.8.34 and 10.6.8.35. The Speed and Duplex Setting is set to 'Auto'. The 'Primary Interface' checkbox is checked. 'OK' and 'Cancel' buttons are at the bottom.

The following table for the **TCP/IP Port Properties** page describes these options.

Option	Setting	Description
Enable Ethernet <i>n</i>	Checked	By default, all Ethernet ports are enabled, whether they are used or not.
	Unchecked	Ports other than the Primary Interface (by default, <i>Ethernet n</i>) can be disabled by selecting the port and unchecking the Enable Ethernet <i>n</i> box. However, a bonded Ethernet port cannot be disabled, nor can a disabled Ethernet port be placed in bonded mode. NOTE: The primary Ethernet port must always be enabled. GuardianOS will not allow you to disable it.
TCP/IP (DHCP or Static)	DHCP	By default, SnapServers acquire an IP address from the DHCP server on the network.
	Static	Administrators may assign a fixed IP address or other IP settings as needed.

Option	Setting	Description
Speed and Duplex Setting	Auto	The default setting of Auto enables automatic negotiation of the speed and duplex settings based on the physical port connection to a switch. The speed setting establishes the rate of transmission and reception of data. The duplex setting allows the Ethernet port to transmit and receive network packets simultaneously. NOTE: Auto is the only allowable setting for a Gigabit port.
	Fixed Speed & Duplex	Using the drop-down list, the SnapServer may also be set to one of five fixed speed (Mbps)/duplex settings: <ul style="list-style-type: none"> • 10 Half Duplex • 10 Full Duplex • 100 Half Duplex • 100 Full Duplex • 1000 Full Duplex. NOTE: To prevent connectivity problems when changing to a fixed setting, see Changing from Auto to a Fixed Link Setting on page 39 .
Primary Interface	Checked or Unchecked	By default, the primary Ethernet port is Ethernet n and it cannot be disabled. However, the Primary Interface can be changed to a different Ethernet port by selecting the Ethernet port you want as the Primary port and checking the Primary Interface box. The Primary Interface is prioritized for various network configuration parameters that apply to the server as a whole (for example, DNS IP address, hostname, and default gateway). In addition, the IP address of the Primary Interface is preferred to identify the server for various services and circumstances that require a single IP address.

TCP/IP Configuration Considerations

Consider the following guidelines when connecting a SnapServer to the network.

Cabling for Single-Subnet, Multihomed, or Network Bonding Configurations

- For a **Single Subnet** or **Multihomed** Configuration (Standalone) – Standalone treats each port as a separate interface. In a single-subnet configuration, only the primary port is connected to the switch. In a multihomed configuration, each port is cabled to a different switch and the network connections lead to separate subnets.



CAUTION: Do not connect multiple Ethernet ports to the same network segment in Standalone mode, except for iSCSI MPIO configurations. This configuration is not supported by most network file protocols and can lead to unexpected results.

If you connect only one port, use the default primary port (**Ethernet 1**). If you use **Ethernet 2** or any other non-primary port, some services may not function properly.

- For a **Network Bonding** Configuration (Load Balancing, Failover, Switch Trunking, or Link Aggregation) – Network bonding technology treats multiple ports as a single channel, with the network using one IP address for the server.

NOTE: This network bonding configuration is only applicable to SnapServers with more than one Ethernet port. To take advantage of network bonding, all ports in the bonded team must be physically connected to the same network:

- For load balancing, Switch Trunking, or Link Aggregation, these parts are connected to the same switch on the same subnet.
- For failover, these parts are connected to a different switch on the same subnet (in case one switch fails).

Make Sure the Switch is Set to Autonegotiate Speed/Duplex Settings

When the server is shipped from the factory, both ports are set to autonegotiate. This setting allows the SnapServer to base speed and duplex settings on the physical port connection to a switch. Thus, the switch/hub to which the SnapServer is cabled *must* be set to autonegotiate to initially connect to the server; otherwise, network throughput or connectivity to the server may be seriously impacted.

To use fixed duplex settings (not applicable to gigabit), the same fixed setting must be set on the server and switch.

Configure the Switch for Load Balancing

If you select either Switch Trunking or Link Aggregation (802.3ad) network bonding configuration for the Client network bond, be sure the switch is configured correctly for that bonding method **after** configuring the bond on the node. No switch configuration is required for Adaptive Load Balancing (ALB).

Changing from Auto to a Fixed Link Setting

You can configure a fixed link speed and duplex setting on the **Network > TCP/IP Networking** page in the browser-based Web Management Interface. If you change this setting, you must:

1. Configure the **fixed setting** in the Web Management Interface first.
2. Configure the **switch** to the same fixed setting.

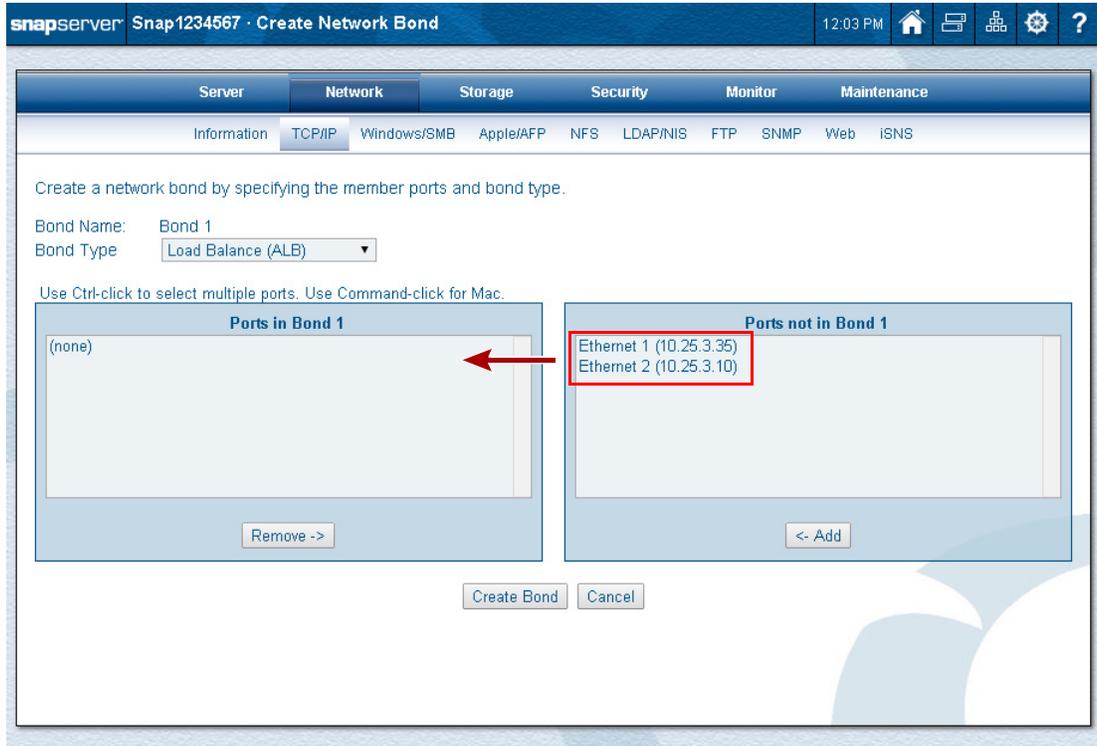


IMPORTANT: If you change the switch setting **before** you change the setting in the Web Management Interface, the SnapServer may not connect to the network. The **Link LED** on the SnapServer front panel will be off or amber if the server is not connected to the network.

Creating a Bond

On a SnapServer with two or more Ethernet ports, a network bond can be created:

1. At the **TCP/IP Networking** page, click **Create Bond**.
2. Using the **Bond Type** drop-down list, select a **bonding type**:



- **Load Balance (ALB)** – enables all selected ports to share the network load.
- **Failover** – enables other selected ports to automatically take over the connection if the primary port fails. Only one port is active at any given time.
- **Switch Trunking or Link Aggregation (802.3ad)** – use either of these two options to group multiple Ethernet ports into one logical Ethernet port for high speed and fault tolerance.

Ports not joined to a bond are configured as **Standalone** and have separate interfaces (one IP address per port).

3. Select the **ports** you want to include in the bond from the **Ports not in Bond n** column and use the **Add** button to move them to the **Ports in Bond n** column.
4. Click **Create Bond**.

The **TCP/IP Networking** page is displayed showing the bond details:

The screenshot shows the SnapServer web interface for TCP/IP Networking. The page title is "Snap1234567 · TCP/IP Networking". The navigation menu includes Server, Network, Storage, Security, Monitor, and Maintenance. Under the Network menu, there are sub-menus for Information, TCP/IP, Windows/SMB, Apple/AFP, NFS, LDAP/NIS, FTP, SNMP, Web, and ISNS. The main content area displays a table with the following data:

Port/Bond	Status	IP Address	Bond Type	Modified
Bond 1	Ethernet 1 - OK Ethernet 2 - OK	10.25.3.35 (static)	Load Balance (ALB)	Created

Below the table are buttons for "OK", "Create Bond", and "Cancel". A red arrow points to the "Created" text in the "Modified" column. Below the buttons, there is a note: "(Important: Click OK to save your changes.)"

- Click **OK** to save the changes.



CAUTION: The changes made require restarting the server's network. Restarting the server's network will disconnect all connected clients.

- At the confirmation/restart page, click **Save Changes**.

The screenshot shows the SnapServer web interface for TCP/IP Networking. The page title is "Snap1234567 · TCP/IP Networking". The navigation menu is the same as in the previous screenshot. The main content area displays a warning message in red text: "Warning: The changes you have made may require restarting the server's network. Restarting the server's network will disconnect all connected clients." Below the warning, it asks "OK to save your TCP/IP changes?". At the bottom, there are buttons for "Save Changes" and "Cancel".



IMPORTANT: You must reconfigure the network switch accordingly if using Switch Trunking or Link Aggregation (802.3ad).

Deleting a Bond

On a SnapServer with an existing bond, the bond can be deleted as follows:

1. At the **TCP/IP Networking** page, click the **bond name** in the table to view the properties page.

snapsrver Snap1234567 · TCP/IP Bond Properties 2:34 PM

Server Network Storage Security Monitor Maintenance

Information TCP/IP Windows/SMB Apple/AFP NFS LDAP/NIS FTP SNMP Web ISNS

Enable Bond 1

Obtain TCP/IP settings from a DHCP server.

Use the settings below:

IP Address: 10.25.3.35

Subnet Mask: 255.255.0.0

WINS Servers: (optional)

Default Gateway: 10.25.1.1 (optional)

DNS Domain Name: devnet.myoverland.net (optional)

Domain Name Servers: 10.6.8.34 (optional), 10.6.8.35 (optional)

Speed and Duplex Setting: Auto

Primary Interface

OK Delete Bond Cancel

2. Click **Delete Bond**.

The **TCP/IP Networking** page is displayed showing the details of the unbonded ports.

snapsrver Snap1234567 · TCP/IP Networking 2:36 PM

Server Network Storage Security Monitor Maintenance

Information TCP/IP Windows/SMB Apple/AFP NFS LDAP/NIS FTP SNMP Web ISNS

Click a Port/Bond name to edit the TCP/IP settings. Click a bond's port members to edit the members.

Port/Bond	Status	IP Address	Bond Type	Modified
Ethernet 1	OK (Primary Interface)	10.25.3.35 (static)	Standalone	Unbonded
Ethernet 2	OK	(not available)	Standalone	Unbonded

OK Create Bond Cancel

(Important: Click OK to save your changes.)

3. Click **OK** to save the changes.



CAUTION: The changes made require restarting the server's network. Restarting the server's network will disconnect all connected clients.

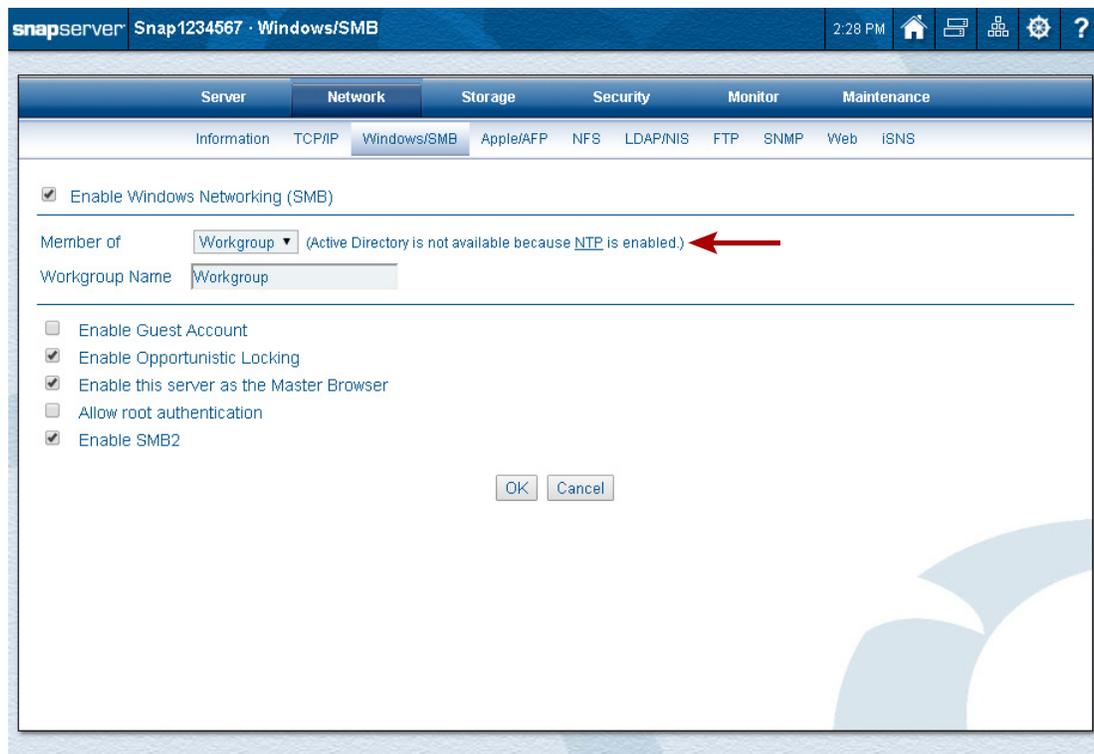
4. At the confirmation/restart page, click **Save Changes**.

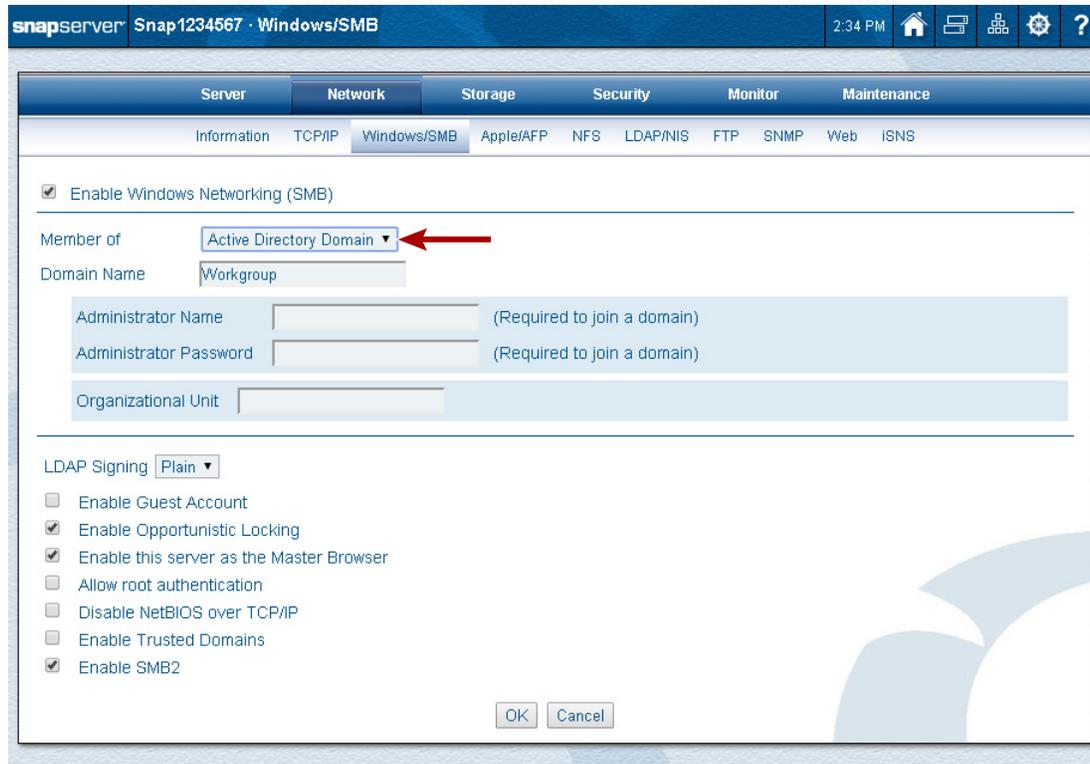


 **IMPORTANT:** You must reconfigure the network switch accordingly if removing Switch Trunking or Link Aggregation (802.3ad).

Windows Networking (SMB)

Windows SMB and security settings are configured on the **Network > Windows/SMB** page of the Web Management Interface. You can configure these settings as a member of a **Workgroup** or an **Active Directory Domain**, as shown in these two screens:





Support for Windows Networking (SMB)

The default settings make the SnapServer available to SMB clients in the workgroup named *Workgroup*. Opportunistic locking is enabled, as is participation in master browser elections.

Consider the following when configuring access for your Windows networking clients:

Support for Microsoft Name Resolution Servers

The SnapServer supports NetBIOS, WINS, and DNS name resolution services. However, when you use a domain name server with a Windows Active Directory (ADS) server, make sure the forward and reverse name lookup are correctly set up. ADS can use a Unix BIND server for DNS as well.

ShareName\$ Support

GuardianOS supports appending the dollar-sign character (\$) to the name of a share in order to hide the share from SMB clients accessing the SnapServer.

NOTE: As with Windows servers, shares ending in '\$' are not truly hidden, but rather are filtered out by the Windows client. As a result, some clients and protocols can still see these shares.

To completely hide shares from visibility from any protocols, the **Security > Shares** page gives you access to a separate and distinct hidden share option that hides a share from SMB, AFP, HTTP, HTTPS, and FTP clients. However, shares are not hidden from NFS clients, which cannot connect to shares that aren't visible. To hide shares from NFS clients, consider disabling NFS access on hidden shares.

For new shares, select **Create Share** and click the **Advanced Share Properties** button to access the Hidden share option. For existing shares, select the share, click **Properties**, and click **Advanced Share Properties** to access the Hidden share option.

Support for Windows Network Authentication

This section summarizes important facts regarding the GuardianOS implementation of Windows network authentication.

Windows Networking Options

Windows environments operate in either workgroup mode, where each server contains a list of local users it authenticates on its own, or Active Directory (ADS) domain mode, where domain controllers centrally authenticate users for all domain members.

Option	Description
Workgroup	In a workgroup environment, users and groups are stored and managed separately on each server in the workgroup.
Active Directory (ADS)	<p>When operating in a Windows Active Directory domain environment, the SnapServer is a member of the domain and the domain controller is the repository of all account information. Client machines are also members of the domain and users log into the domain through their Windows-based client machines. Active Directory domains resolve user authentication and group membership through the domain controller.</p> <p>Once joined to a Windows Active Directory domain, the SnapServer imports and then maintains a current list of the users and groups on the domain. Thus, you must use the domain controller to make modifications to user or group accounts. Changes you make on the domain controller appear automatically on the SnapServer.</p> <p>NOTE: Windows 2000 domain controllers must run SP2 or later.</p>

Kerberos Authentication

Kerberos is a secure method for authenticating a request for a service in a network. Kerberos lets a user request an encrypted “ticket” from an authentication process that can then be used to request a service from a server. The user credentials are always encrypted before they are transmitted over the network.

The SnapServer supports the Microsoft Windows implementation of Kerberos. In Windows Active Directory (ADS), the domain controller is also the directory server, the Kerberos key distribution center (KDC), and the origin of group policies that are applied to the domain.

NOTE: Kerberos requires the server's time to be closely synchronized to the domain controller's time. This means that (1) the server automatically synchronizes its time to the domain controller's and (2) NTP cannot be enabled when joined to an ADS domain.

Interoperability with Active Directory Authentication

The SnapServer supports the Microsoft Windows family of servers that run in ADS mode. Any SnapServer can join Active Directory domains as a member server. References to the SnapServer shares can be added to organizational units (OU) as shared folder objects.

NOTE: Windows 2000 domain controllers must run SP2 or later.

Guest Account Access to the SnapServer

The **Network > Windows/SMB** page in the Web Management Interface contains an option that allows unknown users to access the SnapServer using the guest account.

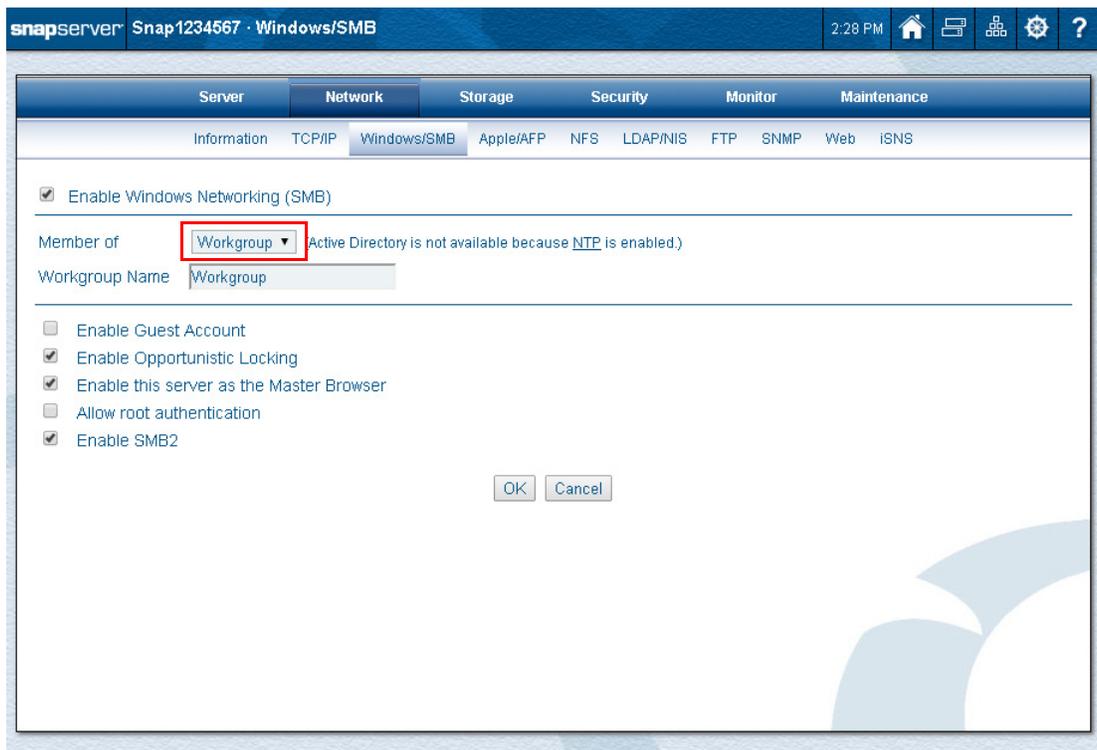
Configure Windows/SMB Networking

Windows SMB and security settings are configured from this page. The server can be configured as part of a Workgroup or an Active Directory Domain.

Before performing the configuration procedures provided here, be sure you are familiar with the information provided in [Support for Windows Networking \(SMB\)](#) and [Support for Windows Network Authentication](#).

To Join a Workgroup

1. Go to **Network > Windows/SMB**.
2. At the Member list, verify that the default **Workgroup** is selected.



3. Edit the **Workgroup** fields shown in the following table:

Option	Settings
Enable Windows SMB	Check the Enable Windows Networking (SMB) checkbox to enable SMB. Clear the checkbox to disable SMB.
Member Of	Verify it is set to Workgroup . NOTE: For the Active Directory Domain option, see To Join an Active Directory Domain .
Workgroup Name	The default settings make the SnapServer available in the workgroup named Workgroup . Enter the workgroup name to which the server belongs.
Enable Guest Account	Check the Enable Guest Account checkbox to allow unknown users or users explicitly logging in as “guest” to access the SnapServer using the guest account. Clear the option to disable this feature.

Option	Settings
Enable Opportunistic Locking	Enabled by default. Opportunistic locking can help server performance if the current user has exclusive access to a file. Clear the checkbox to disable opportunistic locking.
Enable this Server as the Master Browser	Enabled by default. The SnapServer can maintain the master list of all computers belonging to a specific workgroup. (At least one Master Browser must be active per workgroup.) Check the checkbox if you plan to install this server in a Windows environment and you want this server to be able to serve as the Master Browser for a workgroup. Clear the checkbox to disable this feature.
Allow Root Authentication	Check the Allow root authentication checkbox to allow a root login on the selected server. NOTE: The root password is synchronized with the admin password.
Enable SMB2	Enabled by default. Uncheck the box to turn off SMB2 support.

4. Click **OK** to update Windows network settings immediately.

To Join an Active Directory Domain

1. Go to **Network > Windows/SMB**.
2. From the drop-down Member list, select **Active Directory Domain** to view the configuration page.

The screenshot shows the SnapServer configuration interface for Windows/SMB. The top navigation bar includes 'Server', 'Network', 'Storage', 'Security', 'Monitor', and 'Maintenance'. Under 'Network', there are sub-tabs for 'Information', 'TCP/IP', 'Windows/SMB', 'Apple/AFP', 'NFS', 'LDAP/NIS', 'FTP', 'SNMP', 'Web', and 'ISNS'. The 'Windows/SMB' sub-tab is active, and the 'Enable Windows Networking (SMB)' checkbox is checked. The 'Member of' dropdown menu is set to 'Active Directory Domain' and is highlighted with a red box. Below it, the 'Domain Name' field contains 'Workgroup'. There are input fields for 'Administrator Name' and 'Administrator Password', both with '(Required to join a domain)' next to them. The 'Organizational Unit' field is also present. At the bottom, there are 'OK' and 'Cancel' buttons.

3. Edit the **Active Directory Domain** fields shown in the following table:

Option	Description
Enable Windows SMB	Check the Enable Windows Networking (SMB) checkbox to enable SMB. Clear the checkbox to disable SMB.
Member Of	Verify it shows Active Directory Domain .
Domain Name	<p>The default settings make the SnapServer available in the domain named <i>Workgroup</i>. Enter the domain name to which the server belongs.</p> <p>If you join a Windows domain through the Advanced Security option (Security > Security Guides > guide_option), the domain name you entered displays here and can be changed on the next page or the Advanced Security page.</p> <p>NOTE: Windows 2000 domain controllers must run SP2 or later.</p>
Administrator Name and Password	If joining a domain, enter the user name and password of a user with domain join privileges (typically an administrative user).
Organizational Unit	<p>To create a machine account at a different location than the default, enter a name in the Organizational Unit field. By default, this field is blank, signaling the domain controller to use a default name defined within the controller.</p> <p>NOTE: Sub-organizational units can be specified using Full Distinguished Name LDAP syntax or a simple path ([org_unit]/[sub-unit1]/[sub-unit1a])</p>
LDAP Signing	Use the drop-down list to set ADS domain LDAP signing to Plain (no signing), Sign , or Seal , as appropriate for your domain. Default setting is Plain .
Enable Guest Account	Check the Enable Guest Account checkbox to allow unknown users or users explicitly logging in as "guest" to access the SnapServer using the guest account. Clear the option to disable this feature.
Enable Opportunistic Locking	Enabled by default. Opportunistic locking can help performance if the current user has exclusive access to a file. Clear the checkbox to disable opportunistic locking.
Enable this Server as the Master Browser	Enabled by default. The SnapServer can maintain the master list of all computers belonging to a specific workgroup. (At least one Master Browser must be active per workgroup.) Check the checkbox if you plan to install this server in a Windows environment and you want this server to be able to serve as the Master Browser for a workgroup. Clear the checkbox to disable this feature.
Allow Root Authentication	<p>Check the Allow Root Authentication checkbox to allow a root login on the selected server.</p> <p>NOTE: The root password is synchronized with the admin password.</p>
Disable NetBIOS over TCP/IP	<p>Some administrators may wish to disable NetBIOS over TCP/IP. Select the checkbox to disable NetBIOS; clear the checkbox to leave NetBIOS enabled.</p> <p>NOTE: If you disable NetBIOS and you are joining a domain, you must enter the domain name as a fully qualified domain name (for example, actdir.com.companyname.com). A short form such as ActDirDom will not work.</p>

Option	Description
Enable Trusted Domains	<p>SnapServers recognize trust relationships established between the domain to which the SnapServer is joined and other domains in a Windows environment by default. Select the checkbox to toggle this feature.</p> <p>NOTE: SnapServers remember trusted domains. That is, if this feature is disabled and then activated at a later time, the previously downloaded user and group lists, as well as any security permissions assigned to them, will be retained.</p>
Enable SMB2	Enabled by default. Uncheck the box to turn off SMB2 support.

4. Click **OK** to update Windows network settings immediately.

Apple Networking (AFP)

Apple File Protocol (AFP) settings are configured on the **Network > Apple/AFP** page of the Web Management Interface.



The default settings provide access to AFP clients over a TCP/IP network. Mac clients connecting over AFP can log in to the server either as local users on the SnapServer or as Active Directory domain users (if the server belongs to a domain). For more granular control over client access for Mac users who do not belong to a recognized Windows domain, create local user accounts.

NOTE: Mac OS X users can also connect to the SnapServer using Windows networking (SMB).

AFP Configuration Considerations

Consider the following when configuring access for your AFP clients.

Some SnapServer terms may cause confusion for those familiar with Apple terminology:

Term	Definitions
Share	A SnapServer share appears as a Mac volume that can be accessed through the Finder. NOTE: Unlike standard AppleShare servers, SnapServers allow nested shares (folders within folders). As a result, it is possible for some files or directories to appear in more than one share.
Volume	A volume on a SnapServer is a logical partition of a RAID's storage space that contains a filesystem.
Right-click	This document uses the Windows convention in describing keyboard/mouse access to context-sensitive menus. For example, "To rename a group, right-click a group and then choose Rename ." NOTE: Mac users with a single-button should substitute control-click to achieve the same result.

Authenticating Clients Against a Configured Windows Domain

You can authenticate AFP clients against a Windows domain by navigating to **Network > Apple/AFP** and checking the **Authenticate AFP users against Windows domains** box. When domain authentication is enabled, user names will first be authenticated against the Windows domain and then authenticated against the local database. Local and domain users with the same name will connect as the domain user. To force either local or domain authentication, prefix the user name with the name of the domain to authenticate against or the name of the SnapServer. For example:

`mydomain\username` (domain authentication)

`snap12345\username` (local authentication)

Distinguishing Share Names on the Desktop and Finder

By default, the Finder identifies SnapServer shares using only the share name. To display both the share name and the server name, the **Add Server Name To Apple Shared Folder Names** checkbox on the **Network > Apple/AFP** page is enabled by default. This option makes it easier to differentiate between shared folders with the same share name on multiple servers. For example, SHARE1 on SNAP61009 refers to the share named SHARE1 on the SnapServer named SNAP61009.

Edit AFP Access

1. Go to **Network > Apple/AFP**.
2. Edit **settings** as described in the following table:

Options	Usage
Enable Apple Filing Protocol (AFP)	Check the Enable Apple Filing Protocol (AFP) checkbox to enable AFP; leave the checkbox blank to disable AFP access.
Add Server Name to Apple Shared Folder Names	Select this option to identify shares to AFP clients using both the server name and share name. Clear the checkbox to display only the share name.

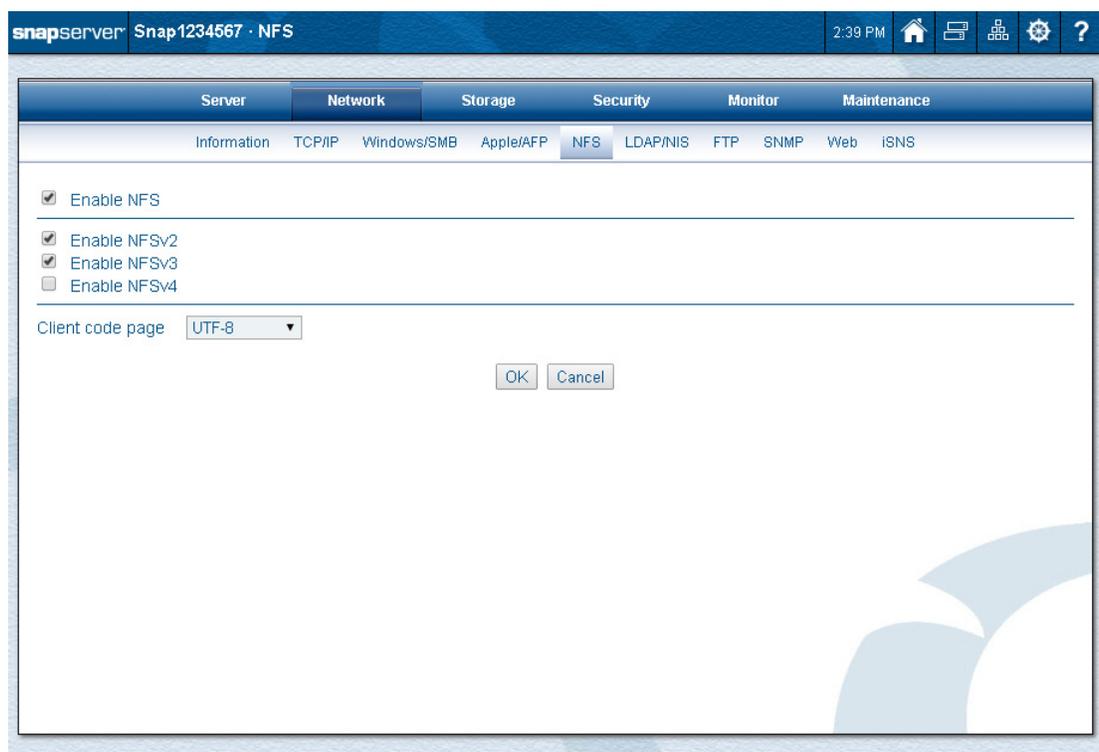
Options	Usage
Authenticate AFP Users Against Windows Domains	Select this option to automatically authenticate AFP users against a Windows domain, if configured. NOTE: By default, users are authenticated against the domain first, then against the local database, so if the same user name exists on both the domain and the SnapServer, the domain user will take precedence. To force an AFP client to log in as either user, prefix the user name with either the Windows domain name or the SnapServer servername. For example: <i>windowsdomain\username</i> or <i>snap12345\username</i>

3. Click **OK** to update network AFP settings immediately.

NFS Access

NFS access to the server is enabled on the **Network > NFS** page of the Web Management Interface. By default, most NFS access is enabled and any NFS client can access the SnapServer through the guest account.

NOTE: Only NFSv2 and v3 are enabled by default. If you wish to enable NFSv4, select the **Enable NFSv4** checkbox on the Network > NFS page.



NFS client access to shares can be specified by navigating to the **Security > Shares** page and clicking the **NFS Access** link next to the share. To ensure proper Unicode representation on the file system, set the client code page to indicate the code page used by NFS clients to represent characters in filenames (usually UTF-8 on modern Unix/Linux-based operating systems).

SnapServers support these versions of the NFS protocol:

Protocol	Version	Source
NFS	2.0, 3.0, 4.0*	RFC 1094, RFC 1813, RFC 3530
Mount	1.0, 2.0, 3.0	RFC 1094 Appendix A, RFC 1813, RFC 3530
Lockd	1.0, 4.0	RFC 1094, RFC1813, RFC 3530

*NFSv4 ACLs are not supported.

Assigning Share Access to NFS Users

The NFS v2/3 protocol does not support user-level share access control, but rather supports host- and subnet-based access control. NFSv4 supports user-level access control via Kerberos configuration, but otherwise uses the same form of host-based access control. On a standard Unix server, share access is configured in an “exports” file. On SnapServers, the exports for each share are configured on the NFS Access page independently of user-based share access for other protocols.

Enable NFS Access to the Server

1. Go to **Network > NFS**.
2. Check the **Enable NFS** checkbox.
3. Check the versions you want to enable.
Select one or more from **NFSv2**, **NFSv3**, and **NFSv4**.
4. Choose the desired **Client code page** from the drop-down list.
Select **UTF-8**, **ISO-8859-1**, **ISO-8859-15**, or **EUC-JP**.
5. Click **OK**.

Configure NFSv4 Access

1. Go to **Network > NFS**.
2. Check the **Enable NFS** and **Enable NFSv4** checkboxes.
A new set of security options are displayed below the **Enable NFSv4** option.

3. Use this table to select the **level of security** you want to apply:

Option	Description
Domain Name	The default domain name “localdomain” is shown in the field. If necessary, you can change it.
	 CAUTION: This setting is used by the NFSv4 IDMAP daemon and must be set to the same value on all NFSv4 clients and servers for proper functionality. If set incorrectly, UID and GID resolution will not work properly.
Security Type	<ul style="list-style-type: none"> • Standard NFS Security – Choose this option if you want to use standard NFS host- and subnet-based security. • RPSEC GSS Security (Unix Kerberos) – Choose this option and complete the fields that appear if you want to use Unix Kerberos security to authenticate NFSv4 connections. <p>NOTE: Kerberos security can only be configured for Unix-based Kerberos implementations. Windows ADS Kerberos is not supported for NFSv4 authentication.</p>

4. If you select **RPSEC GSS Security (Unix Kerberos)** security, complete the options in the table below. Note the following:
- The service will not start unless the TCP/IP domain name is set up exactly the same as the keytab.
 - You must create the NFS and host service entries in the keytab with the fully qualified domain name of the SnapServer.
 - The SnapServer assumes the domain name from the **primary** Ethernet interface. For more information, see [TCP/IP Networking Options](#) on page 35.

Option	Description
KDC Host Name	Enter the host name of the Kerberos server (for example, kerberos-2000.mit.edu).
Realm Name	Enter the Kerberos realm name (For example, ATHENA.MIT.EDU). NOTE: Realm names are conventionally specified in all CAPITAL letters, but this is not required to function correctly.
Key Tab File	Click Browse to locate and upload the Kerberos key tab file (for example, zeus.keytab). NOTE: This file can have any name the administrator wishes to give it. If you do not have a keytab file for the SnapServer: <ul style="list-style-type: none"> - create a host and NFS principle for the SnapServer on the KDC - generate a keytab file - save it to a location the client administering the SnapServer can access.

- Click **OK** to save the configuration.

NOTE: After enabling NFSv4 with Kerberos security, read-write host entries for `gss/krb5`, `gss/krb5i`, and `gss/krb5p` are automatically added to the NFS access entries for each NFS-enabled share.

LDAP and NIS Domains

LDAP and NIS domains are configured on the **Network > LDAP/NIS** page of the Web Management Interface. Choose either LDAP or NIS as the user database type to configure:

LDAP vs. NIS Overview

NIS (Network Information Service) is a client-server directory service protocol for distributing system configuration data such as user and host names between computers on a computer network. The SnapServer can join an NIS domain and function as an NIS client. It

can then read the users and groups maintained by the NIS domain to translate user/group names to UIDs/GIDs for configuration of quotas, ID mapping, and home directories. As such, you must use the NIS server to make modifications.

NOTE: Changes you make on the NIS server do not immediately appear on the SnapServer. It may take up to 10 minutes for changes to be replicated.

LDAP (Lightweight Directory Access Protocol) is an open, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. The SnapServer can be configured to query an LDAP directory for user/group names and UIDs/GIDs for configuration of quotas, ID mapping, and home directories. As such, you must use the LDAP directory to make modifications.

NOTE: SnapServer currently can't be configured to authenticate users against an LDAP directory.

Configuring LDAP

Use this procedure to configure LDAP on your SnapServer:

1. Go to **Network > LDAP/NIS**.

2. From the **User Database Type** drop-down list, select **LDAP**.
3. Check **Enable LDAP**.
4. Edit the **settings** shown in the following table:

Options	Description
LDAP Server	Enter the host name or IP address for the LDAP server.
LDAP Base DN	Click the Search button to locate the Base DN on the LDAP server, or enter the base DN in LDAP syntax such as: cn=accounts,dc=mydir,dc=mydomain,dc=com.
LDAP Bind Type	From the drop-down list, select the LDAP bind type: <ul style="list-style-type: none"> • Anonymous • Simple If Simple is selected, two new fields are shown: Bind DN and Bind Password . Enter the necessary data.

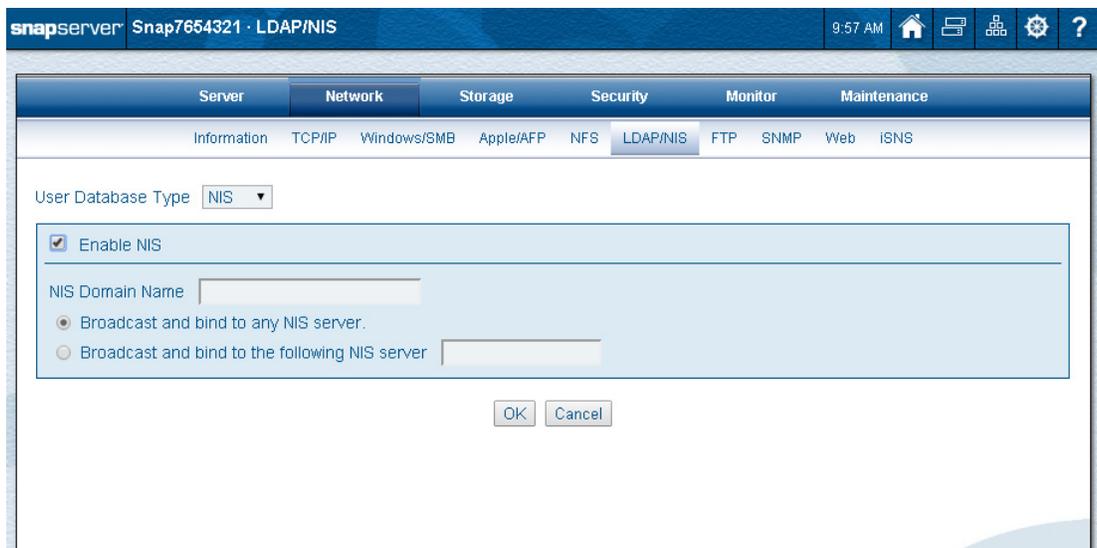
5. Click **OK** to update the settings immediately.
6. If NIS is enabled, you are warned that existing quotas or ID mappings for NIS users will automatically be applied to LDAP users and groups that have the same UID or GID. Click **Enable LDAP**.

Configuring NIS

NOTE: Unless UID/GID assignments are properly handled, NIS users and groups may fail to display properly. For guidelines on integrating compatible SnapServer UIDs, see [User and Group ID Assignments in Chapter 7](#).

NIS uniquely identifies users by UID, not user name, and although it is possible to have duplicate user names, Overland Storage does not support that configuration. To configure NIS on your SnapServer:

1. Go to **Network > LDAP/NIS**.



2. From the **User Database Type** drop-down list, select **NIS**.
3. Check **Enable NIS**.
4. Edit the **settings** shown in the following table:

Options	Description
NIS Domain Name	Enter the NIS domain name.
NIS Server	To bind to an NIS server, select either: <ul style="list-style-type: none"> • Broadcast and Bind to Any NIS server to bind to any available NIS servers. • Broadcast and Bind to the following NIS server and enter the IP address for a specific NIS server in the field provided.

5. Click **OK** to update the settings immediately.
6. If LDAP is enabled, you are warned that existing quotas or ID mappings for LDAP users will automatically be applied to NIS users and groups that have the same UID or GID. Click **Enable NIS**.

FTP/FTPS Access

FTP and FTPS settings are configured on the **Network > FTP** page of the Web Management Interface. FTPS adds encryption to FTP for increased security. By default, FTP and FTPS clients can access the server using the anonymous user account, which is mapped to the SnapServer *guest* user account and *AllUsers* group account. You can set share access and file access for anonymous FTP users by modifying permissions for these accounts. For more granular control over FTP access, you must create local user accounts for FTP users.

For FTPS, it is recommended that your FTPS client application use explicit FTPS (such as, FTPES or Auth TLS).

NOTE: If standard FTP is enabled, only the data channel is encrypted for FTPS connections – the control channel (including user password) is not encrypted. To force FTPS to encrypt the control channel as well, disable standard FTP.

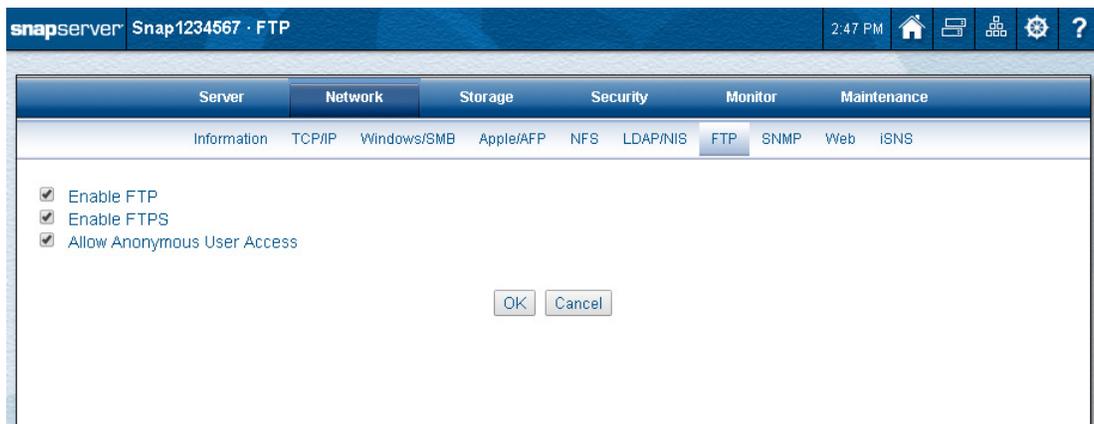
Supported FTP Clients

SnapServers have been tested with the most common FTP clients and work as expected based on the commands required by RFC 959. SnapServers have been proven to work with these products for standard FTP: Internet Explorer 6.0 and later, Safari 2.0 and later, and Firefox 2.0 and later, and Chrome 1.0 and later.

NOTE: Most standard FTP clients do not support FTPS. A client designed to support FTPS is required for FTPS connections.

Configure FTP/FTPS Access

1. Go to **Network > FTP**.



2. Edit the **settings** shown in the following table:

Option	Settings
Enable FTP	Check the Enable FTP checkbox to enable standard FTP services; leave the checkbox blank to disable access to this server via standard FTP.
Enable FTPS	Check the Enable FTPS checkbox to enable FTPS services; leave the checkbox blank to disable access to this server via FTPS.

Option	Settings
Allow Anonymous User Access	<p>When you allow anonymous login, FTP/FTPS users employ an email address as the password. When you disallow anonymous login, only FTP/FTPS users who are configured as local SnapServer users can access the server. Select one of the following access options:</p> <ul style="list-style-type: none"> • Checking the checkbox allows users to connect to the server using the anonymous user account. The anonymous user is mapped to the SnapServer local guest user account. You can set share access for anonymous FTP/FTPS users by granting either read-write (the default access) or read-only access to the guest account on a share-by-share basis. • Leaving the checkbox blank means users cannot log in anonymously but must instead log in via a locally created user name and password.

3. Click **OK** to update the settings immediately.

SNMP Configuration

The SnapServer can act as an SNMP agent. SNMP managers collect data from agents and generate statistics and other monitoring information for administrators. Agents respond to managers and may also send traps, which are alerts that indicate error conditions. The server communicates with SNMP managers in the same community. A community name is a password that authorizes managers and agents to interact. The server only responds to managers that belong to the same public or private community.

Default Traps

A *trap* is a signal from the SnapServer informing an SNMP manager program that an event has occurred. The SnapServer supports the following default traps:

Trap	Initiating Action
coldStart	Whenever SNMP is enabled and the server boots.
linkDown	An Ethernet interface has gone offline.
linkUp	An Ethernet interface has come online.
authenticationFailure	An attempt to query the SNMP agent using an incorrect public or private community string was made, and resulted in a failure.

Trap	Initiating Action
enterpriseSpecific	<p>SnapServer-generated traps that correspond to the error-level, warning-level, and fatal-error-level traps of GuardianOS. These traps contain a descriptive message that helps to diagnose a problem using the following OIDs:</p> <ul style="list-style-type: none"> 1.3.6.1.4.1.6411.2000.1000.1:loglevel 0 syslog messages ("emergency") 1.3.6.1.4.1.6411.2000.1001.1:loglevel 1 syslog messages ("alert") 1.3.6.1.4.1.6411.2000.1002.1:loglevel 2 syslog messages ("critical") 1.3.6.1.4.1.6411.2000.1003.1:loglevel 3 syslog messages ("error") <p>NOTE: There is no Snap-specific MIB that defines traps sent by SnapServers.</p>

Supported Network Manager Applications and MIBs

SnapServers respond to requests for information in MIB-II (RFC 1213) and the Host Resources MIB (RFC 2790 or 1514). You can use any network manager application that adheres to the SNMP V2 protocol with the SnapServer. The following products have been successfully tested with SnapServers: CA Unicenter TNg, HP Open View, and Tivoli NetView.

Configure SNMP

The SNMP configuration page can be found at **Network > SNMP**:

The screenshot displays the SnapServer web interface for configuring SNMP. The main navigation bar includes 'Server', 'Network', 'Storage', 'Security', 'Monitor', and 'Maintenance'. Under 'Network', there are sub-tabs for 'Information', 'TCP/IP', 'Windows/SMB', 'Apple/AFP', 'NFS', 'LDAP/NIS', 'FTP', 'SNMP', 'Web', and 'ISNS'. The 'SNMP' sub-tab is active, showing the following configuration options:

- Enable SNMP
- Read-Only Community:
- Read-Write Community: (optional)
- Location: (optional)
- Contact: (optional)
- Enable SNMP traps
- IP Address 1:
- IP Address 2: (optional)
- IP Address 3: (optional)
- IP Address 4: (optional)
- Send a test trap to listed IP addresses upon saving settings.

At the bottom of the configuration area are 'OK' and 'Cancel' buttons.

Edit settings as described in the following table, and then click **OK**. Once enabled, SNMP managers can access MIB-II and Host Resources MIBs management data on the server.

Option	Description
Enable SNMP	To enable SNMP, check the Enable SNMP checkbox. Leave the check box blank to disable SNMP.
Read-Only Community	To allow SNMP managers to read data from this server, enter a read-only community string or accept the default <i>snap_public</i> . NOTE: As a precaution against unauthorized access, Overland Storage recommends that you create your own community string.
Read-Write Community	While SNMP support is read-only, the optional read-write string is used for compatibility purposes. Enter a read-write community string or accept the default <i>snap_private</i> . NOTE: As a precaution against unauthorized access, Overland Storage recommends that you create your own community string.
Location	Optionally enter information that helps a user identify the physical location of the server. For example, you might include a street address for a small business, a room location such as <i>Floor 37, Room 308</i> , or a position in a rack, such as <i>rack slot 12</i> .
Contact	Optionally enter information that helps a user report problems with the server. For example, you might include the name and title of the system administrator, a telephone number, pager number, or email address.
Enable SNMP Traps	Check the Enable SNMP Traps check box to enable traps. Clear the check box to disable SNMP traps.
IP Address 1-4	Enter the IP address of at least one SNMP manager in the first field as a trap destination. Optionally, you can enter up to three additional IP addresses in fields 2-4.
Send a Test Trap	To verify your settings, check the Send a test trap box, then click OK .

Web Access

HTTP and HTTPS are used for browser-based access to the server via **Home** page, Web Root, or the Web Management Interface. HTTPS enhances security by encrypting communications between client and server, and cannot be disabled. You can, however, disable HTTP access on the **Network > Web** page of the Web Management Interface. Additionally, you can require browser-based clients to authenticate to the server.

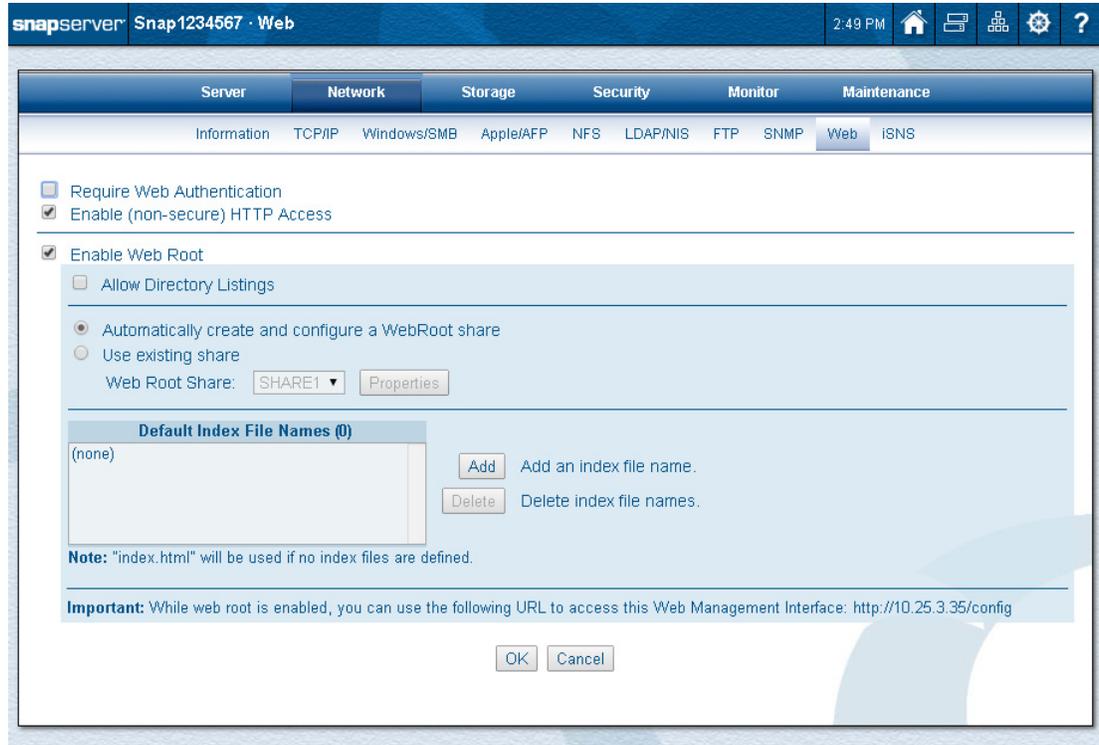
NOTE: To access the CA Antivirus configuration interface (on the [SnapExtensions](#) page), HTTP must be enabled.

GuardianOS supports the following browsers: Internet Explorer 8 or higher, Firefox 3 or higher, Apple Safari 5 or higher, and Google Chrome 9 or higher.

Configuring Web Options

You can configure these options to require web authentication, disable HTTP (non-secure) access, and enable the Web Root feature.

1. Navigate to **Network > Web**.



2. Edit the **settings** shown in the following table:

Option	Description
Require Web Authentication	Check the Require Web Authentication checkbox to require clients to enter a valid user name and password in order to access the server via HTTP/HTTPS. Leave the checkbox blank to allow all HTTP/HTTPS clients access to the server without authentication. NOTE: This option applies to both Home and Web Root modes.
Enable (non-secure) HTTP Access	Check the Enable HTTP Access checkbox to enable non-secure HTTP access. Leave the checkbox blank to disable access to the server via HTTP. NOTE: This option applies to both Home and Web Root modes. To access the CA Antivirus configuration interface, HTTP must be enabled.
Enable Web Root	Check the Enable Web Root checkbox to configure the SnapServer to serve the Web Root directory as the top level web access to the server, and optionally, automatically serve an HTML file inside. When the box is checked, the options described below will appear.

Option	Description
Web Root: Allow Directory Listings	<p>If Allow Directory Listings is checked and no user-defined index pages are configured or present, the browser will open to a page allowing browsing of all directories underneath the Web Root.</p> <p>NOTE: Checking or unchecking this option only affects directory browsing in Web Root. It does not affect access to Home directory browsing.</p>
Web Root: Create and Configure a Share	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Automatically create and configure a Web Root share: A share named "WebRoot" will automatically be created. By default, the share will be hidden from network browsing and will have all network access protocols except HTTP/HTTPS enabled (as such, it can be accessed from a browser as the Web Root but can not be accessed via Home). You can change these settings from the Security > Shares page. • Use existing share: Click the Browse button to locate an existing share you want to use as the Web Root share.
Web Root: Default Index File Names	<p>Files found underneath the Web Root with names matching those in this list will be automatically served to the web browser when present, according to their order in the list. To add a filename, click the Add button, enter the name of one or more index HTML files, then click OK. The file you entered will be shown in the Index Files box.</p> <p>NOTE: If no files are specified, <code>index.html</code> will be automatically loaded if found.</p>

3. Click **OK** to update the settings immediately.

Home Page Overview

The Web Management Interface **Home** page opens when the user accesses a SnapServer using a Web browser, unless the administrator has enabled the Web Root feature (see Using Web Root to Configure the SnapServer as a Simple Web Server). This page displays a list of all shares to which the user has access. Users can navigate the share structure to locate and view or download files, but they cannot modify or upload files.

For users with admin rights, a key icon () appears next to the file/folder in the share. Clicking this icon displays a popup box with security information about the file/folder.

For complete details, see Home Page on [page 207](#).

Using Web Root to Configure the SnapServer as a Simple Web Server

When you enable the Web Root feature from the **Network > Web** page, you can configure your SnapServer to open automatically to an HTML page of your choice when a user enters the following in the browser field:

```
http://[servername] or http://[IP address]
```

In addition, files and directories underneath the directory you specify as the Web Root can be accessed by reference relative to `http://[servername]` without having to reference a specific share. For example, if the Web Root points to the directory *WebRoot* on share *SHARE1*, the file *SHARE1/WebRoot/photos/slideshow.html* can be accessed from a web browser:

```
http://[servername]/photos/slideshow.html
```

The Web Root can also be configured to support directory browsing independent of **Home** page (access through shares).

NOTE: The SnapServer supports direct read-only web access to files. It is not intended for use as an all-purpose Web Server, as it does not support PERL or Java scripting, animations, streaming video, or anything that would require a special application or service running on the server.

To use, map a drive to the share you have designated as the Web Root share and upload your HTML files to the root of the directory, making sure the file names are listed in the Index Files box.

Accessing the Web Management Interface when Web Root is Enabled

By default, when you connect to a SnapServer with Web Root enabled, the browser will load the user-defined HTML page or present a directory listing of the Web Root. To access the Web Management Interface (for example, to perform administrative functions or change a password), enter the following in the browser address field:

```
http://[servername or ip address]/config
```

You will be prompted for your User ID and password, then you will be placed into the Web Management Interface.

If you need to access the **Home** page to browse shares on the server independent of Web Root, enter this in the browser address:

```
http://[servername or ip address]/sadmin/GetWebHome.event
```

iSNS Configuration

Microsoft iSNS Server can be used for the discovery of targets on an iSCSI network. The iSNS software package installs a readme file that contains extensive release notes on bug fixes and current iSNS limitations.



To configure the iSNS settings:

1. Install the iSNS service on a **Windows server**.

Follow the instructions provided in the iSNS readme file. Note the IP address of the server or workstation on which the iSNS service is installed.

2. Configure iSNS on the SnapServer.

On the **Network > iSNS** page, check to select the **Enable iSNS** box, enter the **IP address** of the iSNS workstation, and then click **OK**. The iSNS port default value of 3205 can be changed on this page as well (if changing the port is supported).

3. Configure iSNS in the iSCSI initiator.

Run the initiator software and configure the iSNS service from the **iSNS Servers** tab.

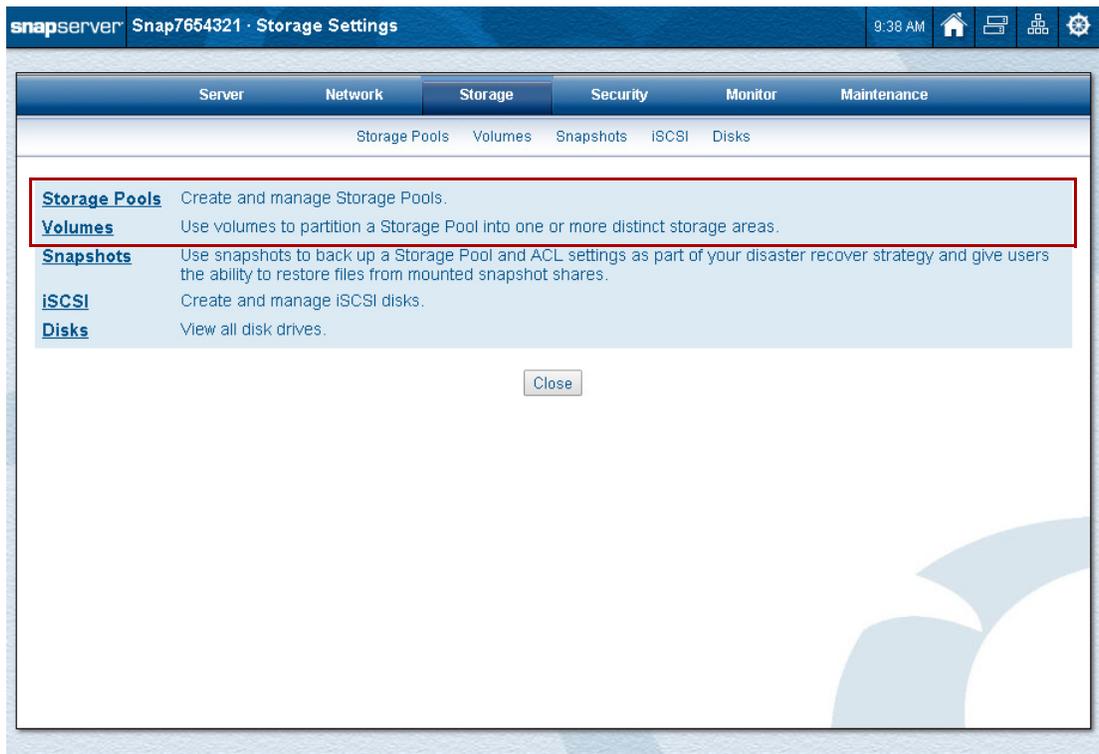
For example, from a Windows client:

- When using the Microsoft initiator, run the Microsoft initiator software, select the iSNS Servers tab, and click **Add**. Enter the name or address of the iSNS server, and then click **OK**.
- When using the QLogic4010/4050 initiator, right-click the QLogic adapter and select **Properties**. Select the Discovery Configuration tab, and check **Perform Discovery**. Check **Use iSNS Server**, enter the server name or IP Address, and click **OK**.

NOTE: After you have completed this procedure, all the iSCSI targets on the SnapServer automatically appear in the Microsoft Initiators target list.

DynamicRAID Storage

This chapter covers the key options of a DynamicRAID configuration used to manage your SnapServer storage pools and volumes with a maximum of flexibility.



To determine which RAID configuration is appropriate for your needs, see [Should I use DynamicRAID or Traditional RAID?](#) in [Appendix A](#).

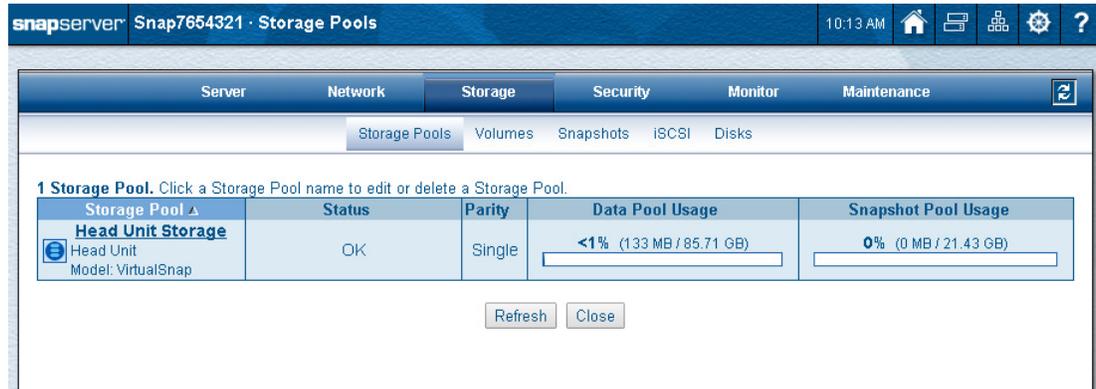
For information on the Traditional RAID configuration option, see [Traditional RAID Storage](#) in [Chapter 5](#). For other storage features, see [Other Storage Options](#) in [Chapter 6](#).

Topics in DynamicRAID Storage:

- [Storage Pools](#)
- [Volumes](#)

Storage Pools

If you selected the DynamicRAID option during the initial setup of your SnapServer, the wizard created a separate storage pool on the head unit and on each attached expansion unit. When you navigate to **Storage > Storage Pools**, an overview of all configured storage pools is shown.

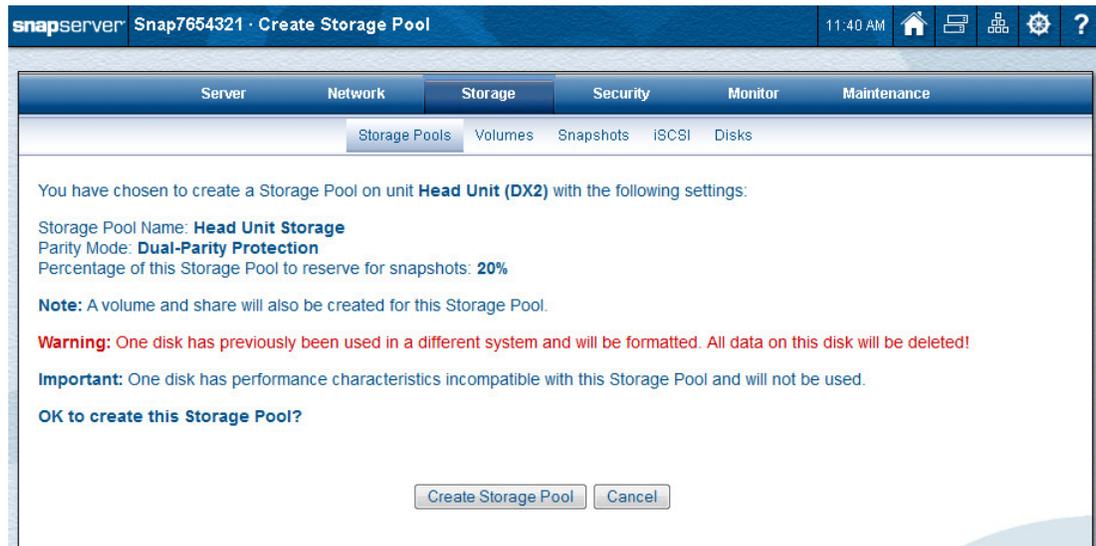


IMPORTANT: A SnapServer head unit or expansion unit supports only **one** storage pool created from its drives and contained within that enclosure. Multiple volumes can be created on that storage pool.

All the disk drives in a chassis (head unit or expansion unit) are part of a single storage pool. If disk drives are added to fill empty slots, they become part of the same storage pool. If a new expansion unit is added, a new storage pool is created on it.

Disk drives that have been previously configured (foreign drives) can be added to a head or expansion unit and are then incorporated into its storage pool. These drives are indicated in the list by the  icon and a message stating that the disk has previously been used in a different system. This includes a drive that has any kind of storage configuration on it (from any machine, including the current one) that is not recognized by the server. This also applies to drives that are current RAID members and may have been removed inadvertently. Upon reinsertion, they will not be automatically incorporated, regardless of whether automatic incorporation of unassigned drives is turned on.

The example below demonstrates the notification of both a disk that has previously been used in a different system, and an incompatible drive.



Storage Pool Creation

Storage pools can be created on head and expansion units that do not yet have pools, one pool per unit, with each pool completely contained within the unit.

During the initial setup process, storage pools are created on the head and expansion units using all disk drives available in each unit. DynamicRAID always maximizes the space available based on both the parity mode type and the snapshot pool size requested.

NOTE: The first detected drive is used as the basis for the drive-size characteristics of the storage pool. All other drives in the storage pool must conform to the size characteristics of the first drive. Otherwise, the drives are not used. See [DynamicRAID Setup](#) in [Chapter 2](#) for more details.

To create a new storage pool, click the link in the **Status** column of the Storage Pool table to open the **Create Storage Pool** page.



CAUTION: When a storage pool is created, any disks in the storage pool that have previously been used in a different system will be reformatted and all data on the disks will be deleted.

At the **Create Storage Pool** page, you can configure these options:

Option	Description
Storage Pool Name	Use this field to enter the name of the storage pool. It can be up to 32 alphanumeric characters and spaces.
Parity Mode	Based on the total number of disks that are available for a storage pool, you can set the parity mode of the storage pool: <ul style="list-style-type: none"> • 1 disk drive – No parity available. • 2 or 3 disk drives – Single-parity protection only. • 4 or more disk drives – Single- or dual-parity protection available. <p>NOTE: Increasing the parity level may require additional disks. You will need to install disks if none are currently available.</p>

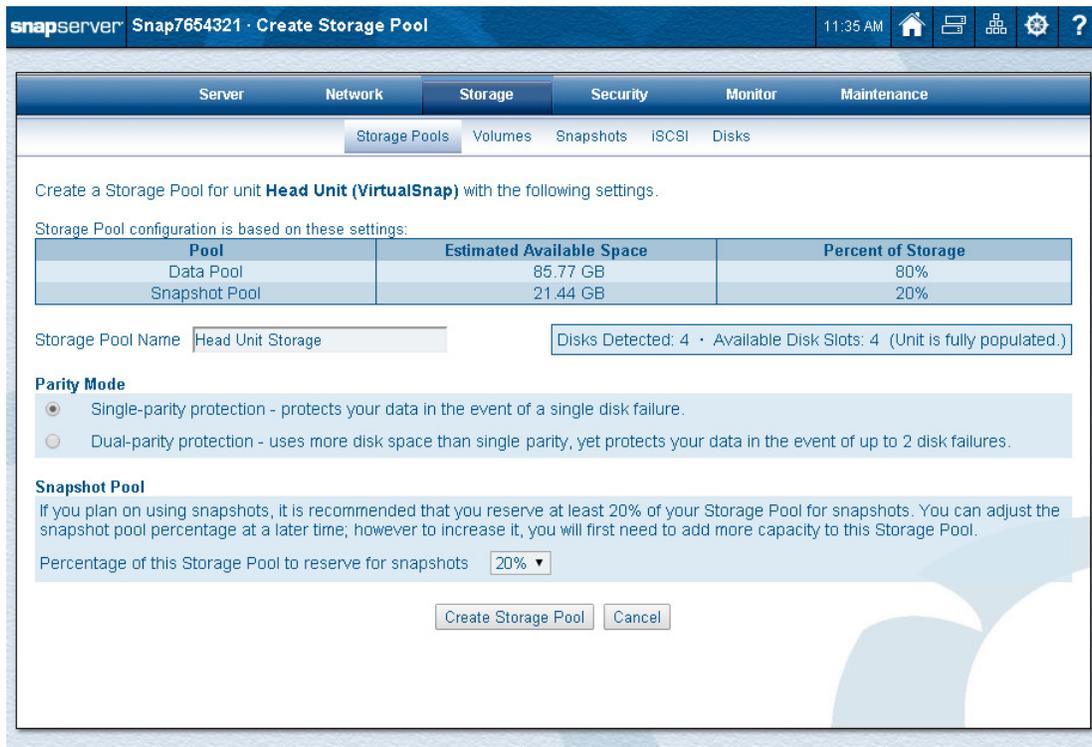
Option	Description
Snapshot Pool	<p>Use the drop-down list to choose a percentage of the storage pool that is reserved for snapshots.</p> <p>For more details about snapshots, refer to Snapshots in Chapter 6.</p> <p>NOTE: Once snapshot space is set up, it can be decreased at any time. To increase the size of the snapshot pool, either the storage pool must be deleted and re-created, or you must add more storage capacity to your storage pool.</p> <p>Default: 20%</p>

Create a Storage Pool

To create a new storage pool (on a unit that doesn't already have a storage pool):



1. At the **Storage Pools** page (**Storage > Storage Pools**), click **No Storage Pool** in the **Status** column.



2. At the **Create Storage Pool** page:
 - Select the desired **parity mode** from the options provided.
 - From the drop-down list, choose the **percentage** of storage pool space reserved for the snapshot.
3. Click **Create Storage Pool**.
4. At the confirmation page, verify your selections and, if everything is correct, click **Create Storage Pool** again. (To make changes, click **Cancel**.)

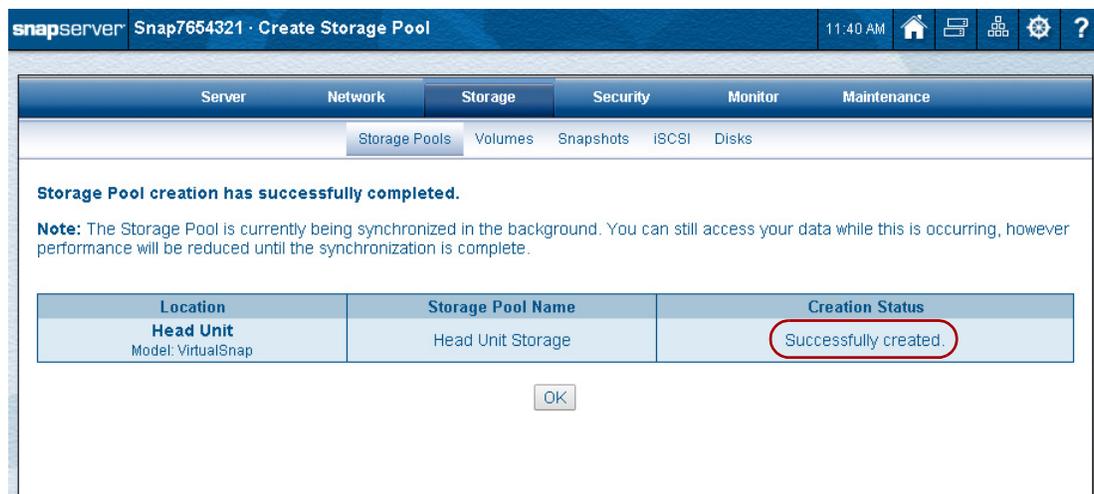


If any disk in a storage pool has previously been used in a different system, a warning appears that it will be reformatted and all data on the disk will be deleted.

If any disk has size characteristics that are incompatible with the other disks in a storage pool, a message appears that this disk will not be used.

While a storage pool is being created, progress is shown in the **Status** column.

5. When a storage pool has been successfully created, click **OK** to continue.



6. You are returned to the **Storage Pools** page where the **Status** shows a resync underway.

The screenshot shows the SnapServer web interface for 'Snap7654321 - Storage Pools'. The 'Storage' tab is selected, and the 'Storage Pools' sub-tab is active. A table displays one storage pool:

Storage Pool	Status	Parity	Data Pool Usage	Snapshot Pool Usage
Head Unit Storage Head Unit Model: VirtualSnap	Resync: 4% complete	Single	<1% (133 MB / 85.71 GB)	0% (0 MB / 21.43 GB)

Below the table are 'Refresh' and 'Close' buttons.

Click **Refresh** now and then to see the current **Status** and to determine when the resync is complete.

IMPORTANT: The new storage pool is currently being synchronized in the background. Do not apply a heavy load to this storage pool until the synchronization operation is complete. Also, unless you are performing necessary tasks using the Web Management Interface, it is recommended to **log out** of the interface during synchronization to give the synchronization operation the full system resources necessary to complete as quickly as possible.

Storage Pool Properties

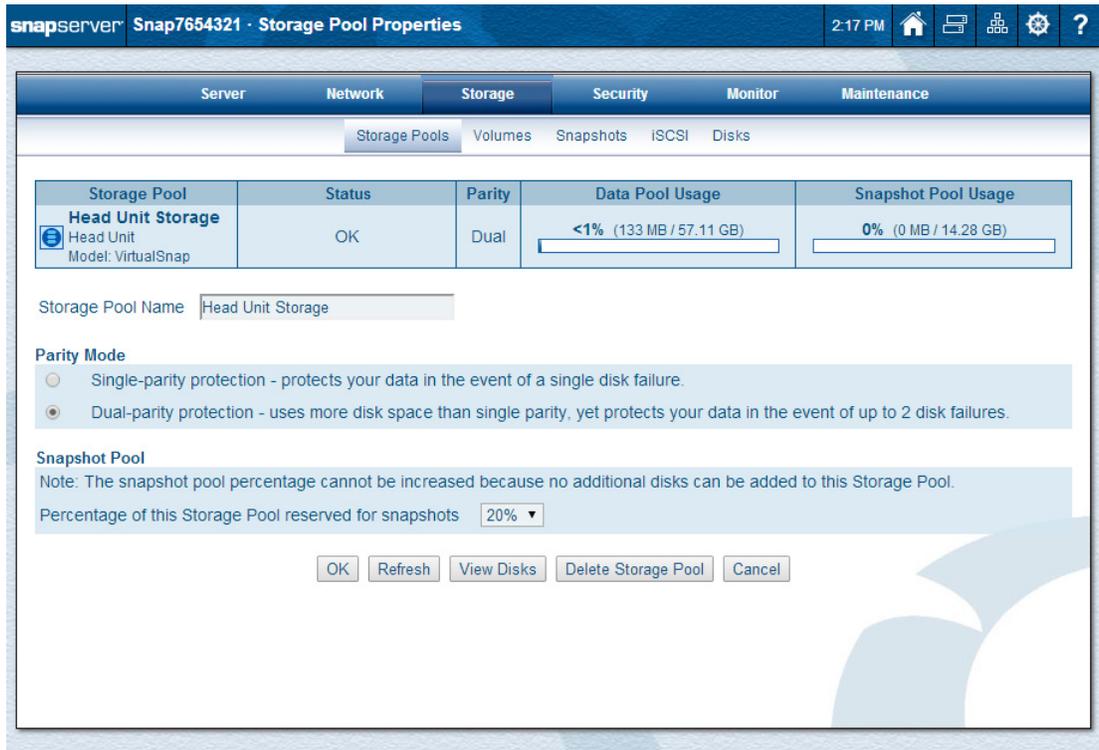
To access the **Storage Pool Properties** page for a storage pool, click the storage pool's name.

The screenshot shows the SnapServer web interface for 'Snap7654321 - Storage Pools'. The 'Storage' tab is selected, and the 'Storage Pools' sub-tab is active. A table displays one storage pool:

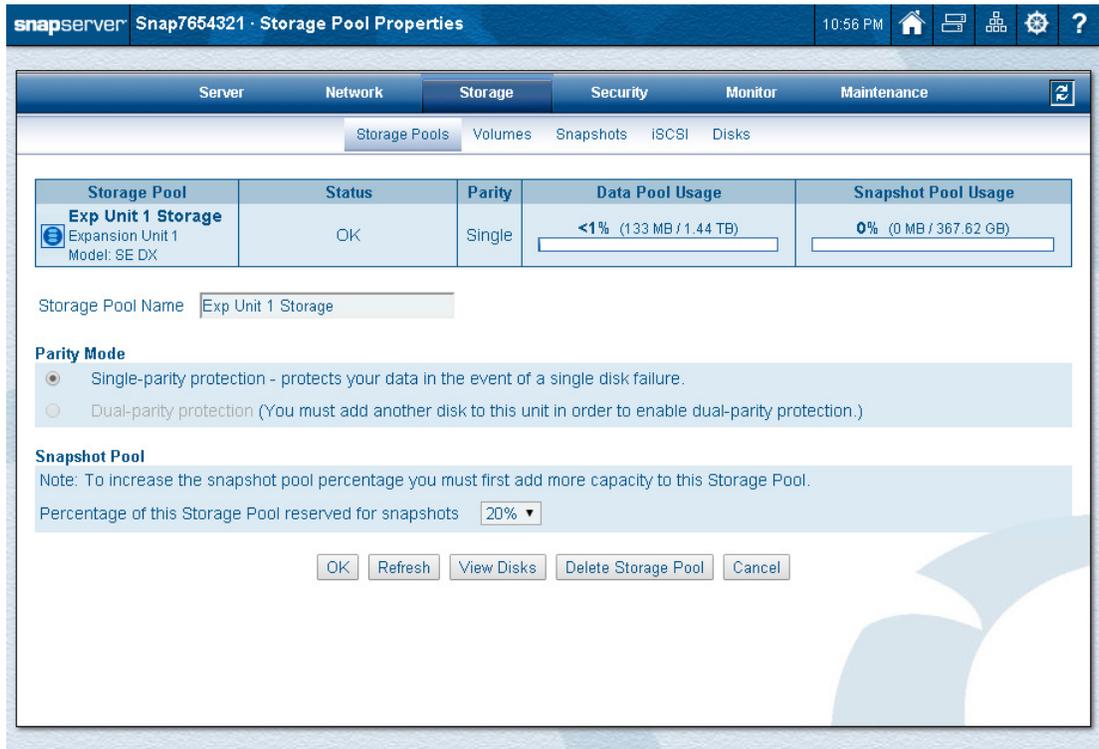
Storage Pool	Status	Parity	Data Pool Usage	Snapshot Pool Usage
Head Unit Storage Head Unit Model: VirtualSnap	OK	Single	<1% (133 MB / 85.71 GB)	0% (0 MB / 21.43 GB)

A red arrow points to the 'Head Unit Storage' link in the first column. Below the table are 'Refresh' and 'Close' buttons.

After you click the head unit storage pool name in the Storage Pool list, the properties page for the head unit is shown:



When you click an expansion unit storage pool name in the Storage Pool list, the properties page for that specific expansion unit is shown:



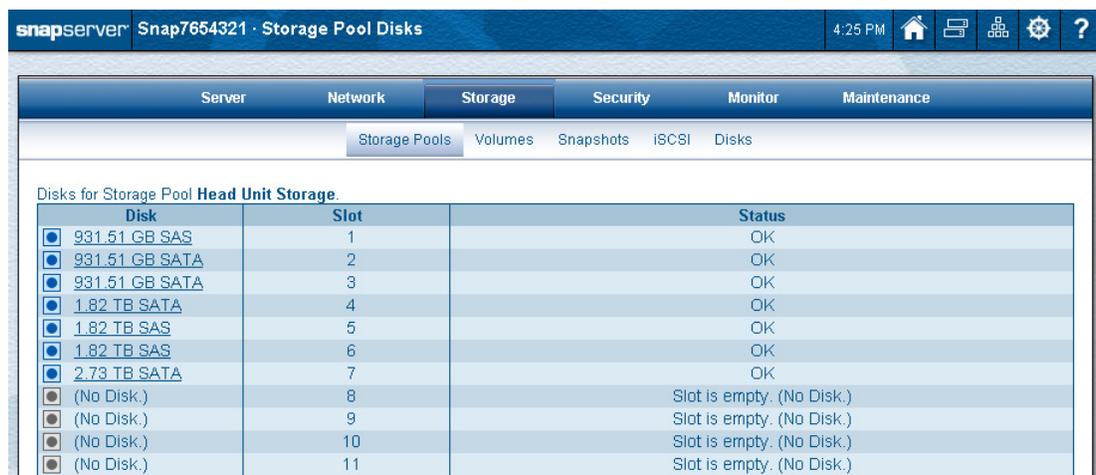
At the **Storage Pool Properties** page, you can edit these options:

Option	Description
Storage Pool Name	Use this field to change the name of the storage pool. It can be up to 32 alphanumeric characters and spaces.
Parity Mode	<p>You can change the Parity Mode. Your options are based on the current setting and available disk drives. For more information on Parity management, see Parity Management on page 74.</p> <p>Possible options include:</p> <ul style="list-style-type: none"> • No parity available. • Single-parity protection only. • Single- or dual-parity protection available. <p>NOTE: Increasing the parity level always requires the addition of an unassigned disk to the storage pool. In addition, it may require the installation of additional disks if none are currently available.</p>
Snapshot Pool	<p>Use the drop-down list to choose a percentage of the storage pool that you want reserved for snapshots. You can only decrease the current reserved space from the Properties page.</p> <p>NOTE: If you grow the storage pool by adding a drive and not changing the parity mode, you can allocate the new space to increase snapshot space.</p> <p>For more details about snapshots, refer to Snapshots in Chapter 6.</p>

If changes are made to the storage pool, a confirmation page is shown. Click **OK** to accept the changes.

View Disks from Storage Pool Properties Page

To view all of the disks in a storage pool, from the **Storage > Storage Pools** page, select a storage pool to open the properties page, then click **View Disks**.



The screenshot shows the SnapServer interface for 'Storage Pool Disks'. The top navigation bar includes 'Server', 'Network', 'Storage', 'Security', 'Monitor', and 'Maintenance'. Under 'Storage', there are sub-tabs for 'Storage Pools', 'Volumes', 'Snapshots', 'iSCSI', and 'Disks'. The main content area displays a table titled 'Disks for Storage Pool Head Unit Storage'.

Disk	Slot	Status
<input checked="" type="checkbox"/> 931.51 GB SAS	1	OK
<input checked="" type="checkbox"/> 931.51 GB SATA	2	OK
<input checked="" type="checkbox"/> 931.51 GB SATA	3	OK
<input checked="" type="checkbox"/> 1.82 TB SATA	4	OK
<input checked="" type="checkbox"/> 1.82 TB SAS	5	OK
<input checked="" type="checkbox"/> 1.82 TB SAS	6	OK
<input checked="" type="checkbox"/> 2.73 TB SATA	7	OK
<input type="checkbox"/> (No Disk.)	8	Slot is empty. (No Disk.)
<input type="checkbox"/> (No Disk.)	9	Slot is empty. (No Disk.)
<input type="checkbox"/> (No Disk.)	10	Slot is empty. (No Disk.)
<input type="checkbox"/> (No Disk.)	11	Slot is empty. (No Disk.)

Any disk that is incompatible is shown with a highlighted message.

Storage Pool Deletion



CAUTION: Deleting a storage pool deletes all volumes and their data on the storage pool. The data cannot be recovered.

Delete a Storage Pool

1. Go to the **Storage > Storage Pools** page.
2. Click the **name** of the storage pool being deleted.
3. At the **Storage Pool Properties** page, click **Delete Storage Pool**.

The screenshot shows the SnapServer interface for the 'Storage Pool Properties' of a storage pool named 'Head Unit Storage'. The page includes a navigation bar with tabs for Server, Network, Storage, Security, Monitor, and Maintenance. Under the Storage tab, there are sub-tabs for Storage Pools, Volumes, Snapshots, iSCSI, and Disks. A table displays the storage pool's status as 'OK', parity as 'Dual', data pool usage as '<1% (133 MB / 57.11 GB)', and snapshot pool usage as '0% (0 MB / 14.28 GB)'. Below the table, the 'Storage Pool Name' is 'Head Unit Storage'. The 'Parity Mode' section has two radio buttons: 'Single-parity protection - protects your data in the event of a single disk failure.' (unselected) and 'Dual-parity protection - uses more disk space than single parity, yet protects your data in the event of up to 2 disk failures.' (selected). The 'Snapshot Pool' section has a note: 'Note: The snapshot pool percentage cannot be increased because no additional disks can be added to this Storage Pool.' and a dropdown menu set to '20%'. At the bottom, there are buttons for 'OK', 'Refresh', 'View Disks', 'Delete Storage Pool' (highlighted with a red circle), and 'Cancel'.

Storage Pool	Status	Parity	Data Pool Usage	Snapshot Pool Usage
Head Unit Storage Head Unit Model: VirtualSnap	OK	Dual	<1% (133 MB / 57.11 GB)	0% (0 MB / 14.28 GB)

Storage Pool Name:

Parity Mode

Single-parity protection - protects your data in the event of a single disk failure.

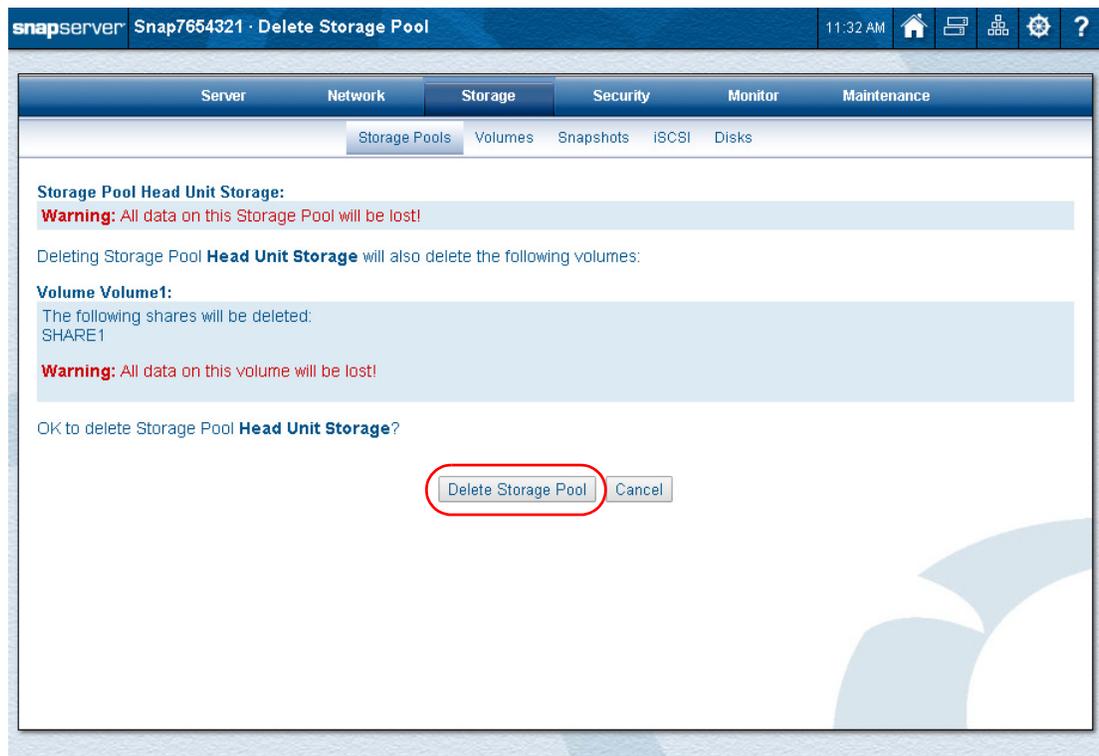
Dual-parity protection - uses more disk space than single parity, yet protects your data in the event of up to 2 disk failures.

Snapshot Pool

Note: The snapshot pool percentage cannot be increased because no additional disks can be added to this Storage Pool.

Percentage of this Storage Pool reserved for snapshots:

4. At the confirmation page, click **Delete Storage Pool** again.



You are returned to the **Storage Pools** page. The Status for the unit should show **No Storage Pool1**. To create a new storage pool, click that link and follow the steps in [Create a Storage Pool](#) on [page 74](#).

Parity Management

Parity is used to achieve redundancy in the SnapServer. If a drive in the array fails, remaining data on the other drives can be combined with the parity data to reconstruct the missing data.

- **Single Parity** – Protects your data in the event of a single disk failure.
- **Dual Parity** – Uses more disk space than single parity, yet protects your data in the event of up to two disk failures.

Parity is usually set when creating a new storage pool. It can also be changed when modifying an existing storage pool to either increase parity (by adding a new drive) or decrease parity (to expand storage space and sacrifice redundancy). Parity and snapshot space are selected by the user according to the best estimate of necessary storage requirements.

A move from dual parity to single parity is allowed at any time, provided the storage pool is healthy. A move from single parity to dual parity is only allowed when a new disk drive is added that is large enough to support the new parity mode. See [Additional Information on DynamicRAID Sizing](#) in [Appendix A](#).

NOTE: A storage pool that was converted from dual parity to single parity cannot be converted back to dual parity until a new disk drive is added. This is due to the extra dual-parity drive that was rolled into the single-parity RAID set.

To Add a Disk Drive to Upgrade Parity

To increase the parity protection of the storage pool, new disk drives are added to empty slots in the unit containing the storage pool. The DynamicRAID will then obtain user input on how you want to use the new, additional space:

Current Number of Unit Disks	Impact of Adding One More Disk
1	Parity is upgraded from no parity to single parity.
2	Dual-parity option is activated: <ul style="list-style-type: none"> • If dual parity selected, system migrates to it. • If single parity is kept, filesystem space is expanded.
3 or more	The filesystem space is expanded and, if dual parity has been selected to replace single parity, migration commences. See Adding Drives on page 75 .

When a new disk drive is added, the Administration pages display a message banner that new drives were detected. At the **Storage > Storage Pools** page, the same message is shown with a clickable link. When you click the link, the **Storage Pool Properties** page is shown where you can then change the parity and snapshot settings for the storage pool to take advantage of the additional space.

NOTE: Disk drives that have been previously configured can be added; they are indicated in the list by the Disk is Foreign icon (🗑️) and a message stating that the disk has previously been used in a different system.

There are no separate spare or global spare disk drives when using the DynamicRAID option. With single parity, if a disk drive fails, a warning is issued and the system reverts to degraded mode with no protection, so that a second drive failure will cause the system to fail. With dual parity, if two disk drives fail, a warning is issued and the system reverts to degraded mode with no protection, so that a third drive failure will cause the system to fail.

Adding Drives. Adding new disks to a storage pool sometimes requires the SnapServer to perform multiple queued operations. During this multi-step resynchronization process, the estimated data pool size will be displayed and may be different than the size currently displayed in the **Data Pool Usage** column. The actual pool size won't be known until the process is complete.

NOTE: New drives added to a storage pool must at least be the same size or larger than the smallest drive in that pool.

Volumes

GuardianOS supports multiple volumes in a storage pool. During the initial creation of your DynamicRAID storage pool, an initial volume was also created. To view that volume (and create other volumes if needed), navigate to **Storage > Volumes**. To access the **Properties** page for a volume, click the volume name.



Clicking the storage pool name will take you to the **Storage Pool Properties** page.

Volume Creation

If a storage pool exists, at the **Volumes** page, you can use the **Create Volume** button to set up a new volume.



Create a New Volume

1. Navigate to **Storage > Volumes**.

2. Click the **Create Volume** button.

3. Choose the **options** for the new volume:

- Select a **storage pool name** from the drop-down list.
- Enter a unique **volume name** of 32 alphanumeric characters and spaces.
- Specify the **maximum size** of the volume:
 - **No limit** – this allows the volume to expand as needed by making available as much (or as little) of the remaining unused space on the storage pool.
 - **Maximum size** – Establish a maximum volume size limit by entering the amount and selecting a unit of measure. The volume then expands in size as needed until it reaches its maximum. If email notification has been enabled, alerts are sent as the maximum is approached. (To enable email notification, see [Email Notification](#) in [Chapter 9](#).)

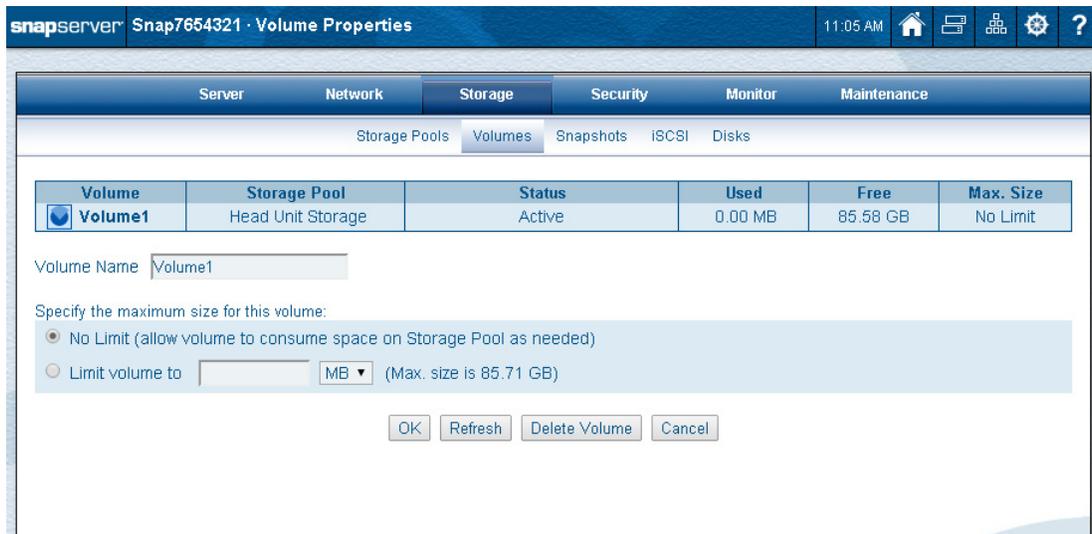
NOTE: If you set the maximum size to less than the current size, the volume is treated as full and no more data can be written to it until the actual space consumed is below the maximum size again.

4. Click the **Create Volume** button on this page to create the volume.

A message appears that the volume has been created. If desired, you can now create a share by clicking the **Create Share** button shown. See [Shares](#) in [Chapter 7](#) for more information about creating shares.

Volume Properties

By clicking the volume name, the **Volume Properties** page is shown that you can use to edit the volume settings.



Edit Volume Properties

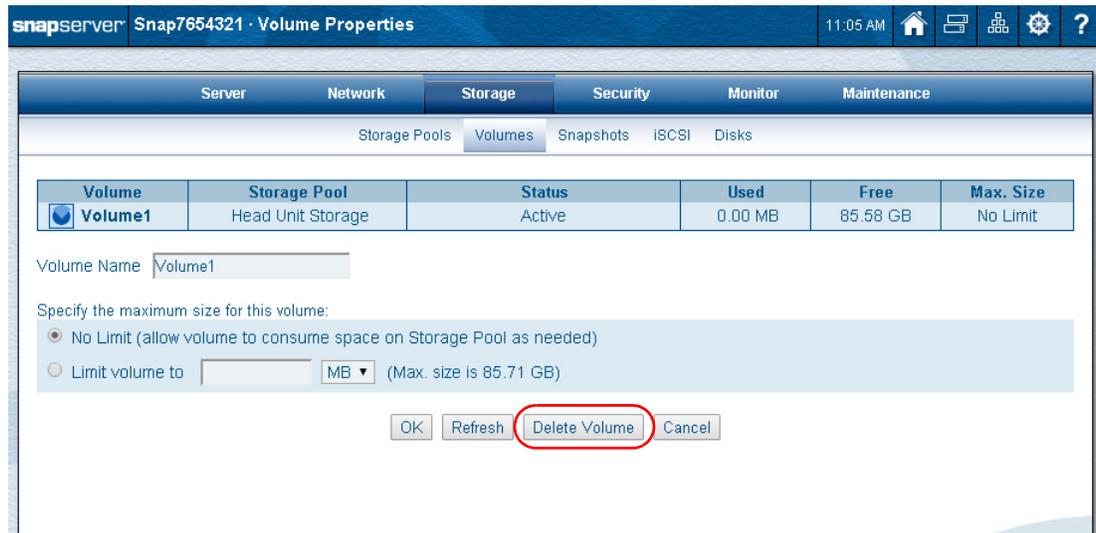
1. Navigate to **Storage > Volumes**.
2. Click the **volume name** in the table.
3. At the **Volume Properties** page, change the **options** desired:
 - Edit the **volume name** using up to 32 alphanumeric characters and spaces.
 - Specify the **maximum size** of the volume:
 - **No Limit** – this allows the volume to expand as needed incorporating the remaining unused space on the storage pool.
 - **Maximum size** – Establish a maximum volume size limit by entering the amount and selecting a unit of measure. The volume then grows in size until it reaches its maximum. If email notification has been enabled, alerts are sent as the maximum is approached. (To enable email notification, see [Email Notification](#) in [Chapter 9](#).)

NOTE: If you set the maximum size to less than the current size, the volume is treated as full and no more data can written to it until the actual space consumed is below the maximum size again.

4. When you are done, click **OK**.

Volume Deletion

To delete a volume, click the **Delete** button on the **Storage > Volumes** page.



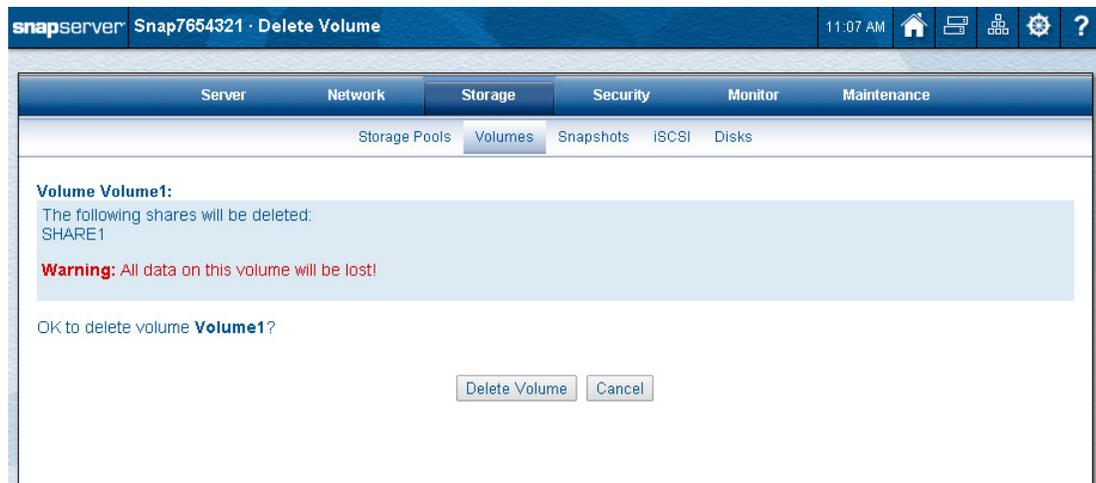
Delete a Volume

1. Navigate to **Storage > Volumes**.
2. Click the **volume name** in the table.
3. At the **Volume Properties** page, click **Delete Volume**.



CAUTION: Deleting a volume deletes all data on the volume.

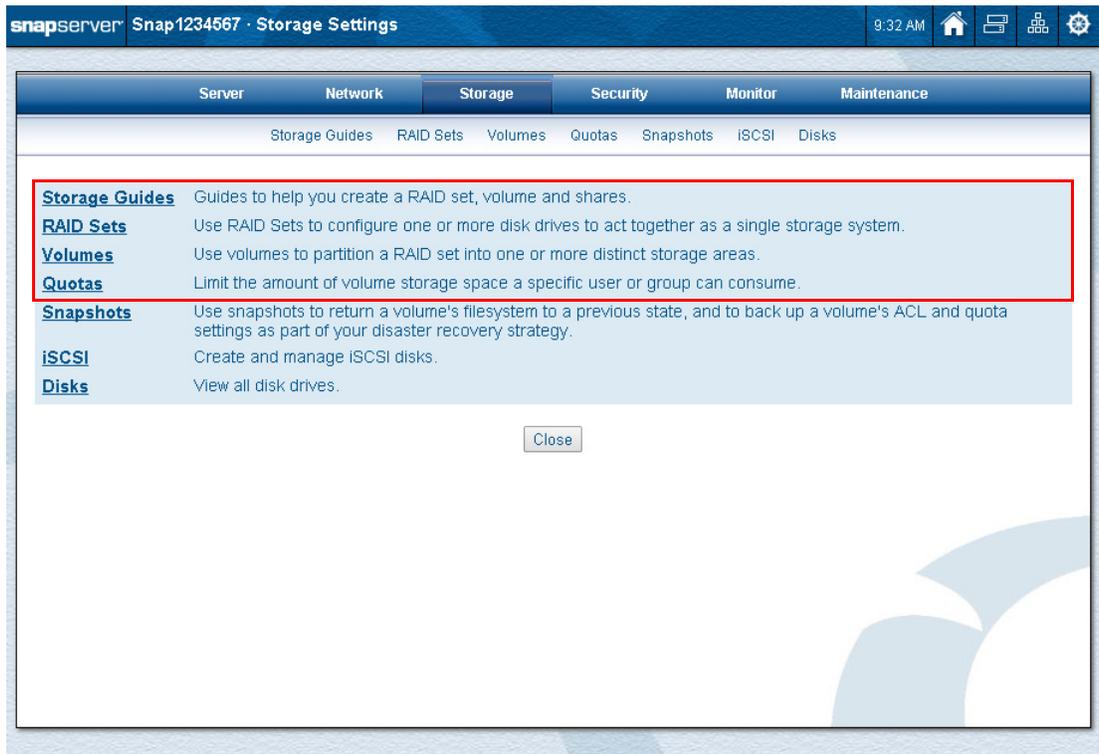
4. At the confirmation page, click **Delete Volume** again.



You are returned to the **Volumes** page. The volume is deleted in the background.

Traditional RAID Storage

This chapter covers the key options of a Traditional RAID configuration. It explains how best to use the Storage Guides and manage your RAID sets, volumes, and quotas.



IMPORTANT: To simplify the management of your SnapServer RAID sets, it is recommended that you use the DynamicRAID option on your server and expansion units.

Using the Traditional RAID option requires you to manually configure and manage RAID sets to meet your specific needs. For simplified storage management and additional configuration options not available in Traditional RAID, use the DynamicRAID option instead. For information on the DynamicRAID configuration option, see [DynamicRAID Storage](#) in [Chapter 4](#). For other storage features, see [Other Storage Options](#) in [Chapter 6](#).

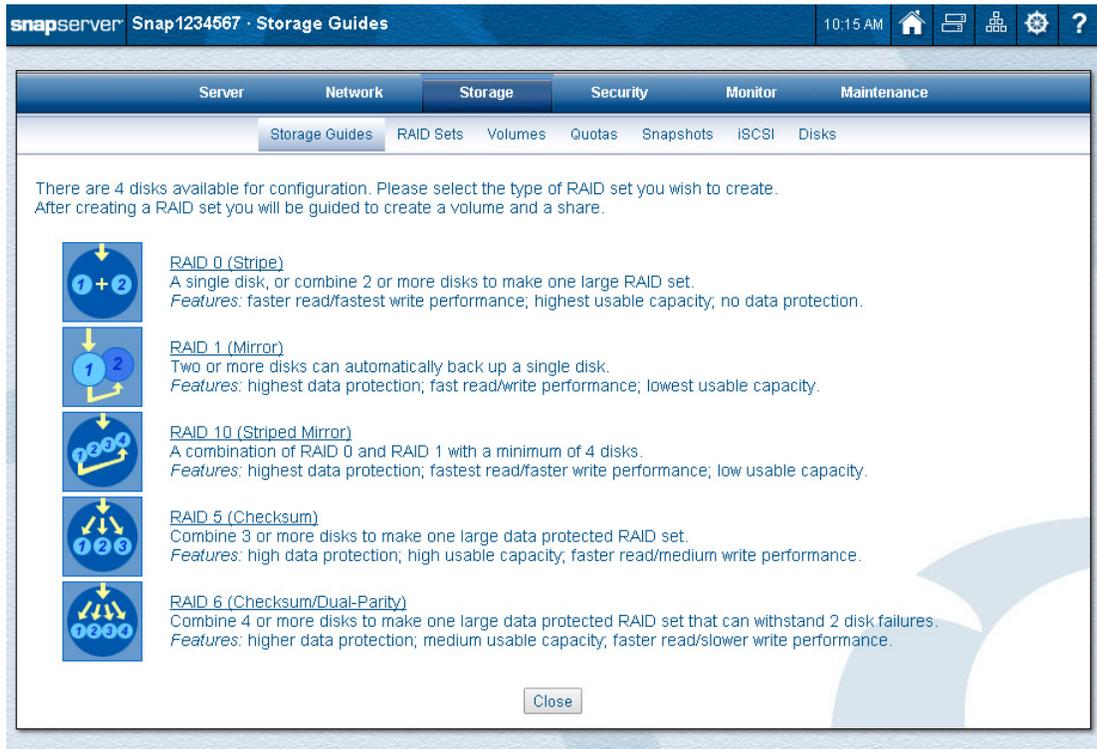
Topics in Traditional RAID Storage

- [Storage Guides](#)
- [RAID Sets](#)
- [Volumes](#)
- [Quotas](#)

Storage Guides

Five different storage guides (wizards) are available for creating a RAID set, volume and share.

NOTE: If you do not have enough disk drives for the more advanced RAID set configurations, they will be grayed out and unavailable.



The basic steps for storage configuration are:

Step 1: Create a RAID set.

Step 2: Create a volume on the new RAID set.

Step 3: Create a share to access files on the new volume.

Factors in Choosing a RAID Type

The type of RAID configuration you choose depends on a number of factors:

- The importance of the data
- Performance requirements
- Drive utilization
- The number of available drives

For example, in configuring the disk drives of a four-drive SnapServer, the decision whether to include a spare in the RAID depends on the value you place on capacity vs. high availability. If capacity is paramount, you would use all drives for storage; if high availability were more important, you would configure one of the drives as a spare.

The following table summarizes the advantages and disadvantages of each type of RAID.

Features	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10
Data Loss Risk	Highest	Lowest	Low	Lower	Very Low
Write Access Speeds	Fastest	Fast	Medium	Slower	Faster
Usable Capacity	Highest	Lowest	High	Medium	Low
Disks Required	1 or more	2 or more	3 or more	4 or more	4 or more
Supports Spares	No	Yes	Yes	Yes	Yes



CAUTION: To reduce exposure to double-drive disk failures on RAID 5, use no more than eight drives in a single RAID set and group smaller RAID sets together. RAID 6 is recommended for RAID sets with more than four drives.

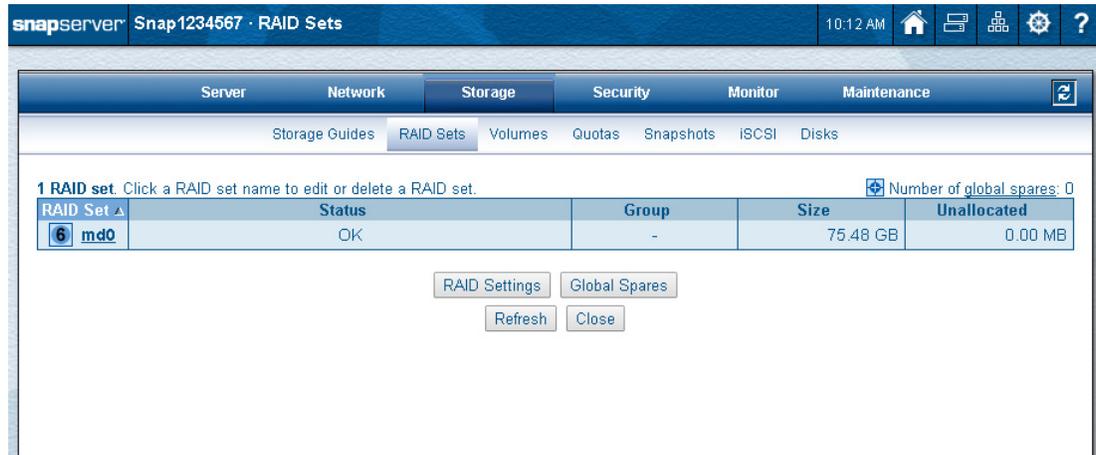
Local and Global Spares

A *spare* is a disk drive that can automatically replace a failed drive in a RAID 1, 5, 6, or 10 set. Designating a disk drive as a spare helps ensure that data is available at all times. If one disk drive in a RAID fails or is not operating properly, the RAID automatically uses the spare to rebuild itself without administrator intervention. SnapServers offer two kinds of spares: local and global.

Item	Description
Definitions	<p>Local (hot) spare – A local (or dedicated) spare is associated with and is available only to a single RAID. Administrators typically create a local spare for RAID sets containing mission-critical data that must always be available.</p> <p>Global (hot) spare – A spare that may be used for any RAID 1, 5, 6, or 10 in the system on any unit (assuming sufficient capacity) as it becomes needed.</p>
Identifying	<p>Spares are identified on the Storage > Disks page using the following icons:</p> <p style="text-align: center;">  Local Spare  Global Spare (GS) </p> <p>Each icon will be associated with a disk in the RAID, identifying that disk as either a local spare or a global spare.</p>
Interaction	<p>When a drive in a RAID fails, the system looks for a spare in the following order:</p> <ol style="list-style-type: none"> 1. If a local spare dedicated to the RAID exists, use the local spare. 2. If no local spare is available, and there is a single global spare of sufficient capacity, use the global spare. 3. If no local spare is available, and two global spares of different capacity are available, use the smaller global spare with sufficient capacity.

RAID Sets

Use the **Storage > RAID Sets** page to manage RAID sets and their options.



From the **RAID Sets** main page, you can do the following:

- **Create RAID Sets** – If unassigned drives exist, a new RAID set can be created by launching a wizard.
- **Group RAID Sets** – If more than one RAID set exists, they can be grouped together.
- **Change RAID Settings** – Change two RAID options:
 - Enable/disable automatic incorporation of unused disks into degraded RAID sets.
 - Enable/disable background disk scans during idle I/O system time.
- **Manage Global Spares** – Add, delete, and configure global spares.
- **Edit RAID Set Properties** – Edit the RAID set properties (click the name to access).

Create RAID Sets

If you choose not to use the Storage Guide wizards to expedite the configuration of your RAID sets, you can manually configure them using these steps:

1. At **Storage > RAID Sets**, click **Create RAID**.

The following page is displayed. Based on the disk drives available, only the supported RAID options have active links. The other options and icons are grayed out.



2. Click the desired **RAID type** name or icon.

The following table summarizes the advantages and disadvantages of each type of RAID:

Features	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10
Data Loss Risk	Highest	Lowest	Low	Lower	Very Low
Write Access Speeds	Fastest	Fast	Medium	Slower	Faster
Usable Capacity	Highest	Lowest	High	Medium	Low
Disks Required	1 or more	2 or more	3 or more	4 or more	4 or more
Supports Hot Spares	No	Yes	Yes	Yes	Yes

CAUTION: To reduce exposure to double-drive disk failures on RAID 5, use no more than eight drives in a single RAID set and group smaller RAID sets together. RAID 6 is recommended for RAIDs with more than four drives.

3. Place a check mark next to the **disks** you want to include in the RAID set.

snapservers Snap1234567 · Create RAID 12:01 PM

Server Network **Storage** Security Monitor Maintenance

Storage Guides RAID Sets Volumes Quotas Snapshots iSCSI Disks

Create RAID set: **RAID 5 (Checksum)**
Select at least 3 of the following disks and click Next. Select at least 4 disks if one is to be used as a spare.

Disk	Location	Status	Usable Space
<input checked="" type="checkbox"/> 50 GB SAS	Head Unit, disk 1	OK	37.75 GB
<input checked="" type="checkbox"/> 50 GB SAS	Head Unit, disk 2	OK	37.75 GB
<input checked="" type="checkbox"/> 50 GB SAS	Head Unit, disk 3	OK	37.75 GB
<input checked="" type="checkbox"/> 50 GB SAS	Head Unit, disk 4	OK	37.75 GB

I do not want a hot spare
 I want a local spare (usable only by this RAID set)
 I want a global spare (usable by any RAID set). (The current number of global spares is: 0)

Back Next Cancel

NOTE: Disks can be from the head unit or any attached expansion unit. However, creating a RAID with disks from different units increases the chance of a multiple-disk RAID failure due to communication issues that may arise between units.

CAUTION: Do not mix drives of different capacity in a RAID 1, 5, 6, or 10 set. Because all drives within a RAID must be the same capacity, using mixed-capacity drives in the same RAID will result in wasted capacity. Also, do not mix drives of different rotational speeds in the same slot column. See [Adding Disk Drives](#) in [Chapter 6](#) for illustrations of supported and unsupported drive configurations.

For example, if a RAID is configured with the drives listed in the following table, some capacity of the larger drives will go unused.

Drive	Raw Capacity	Actual Used Capacity	Usage
Drive 1	750 GB	750 GB	100%
Drive 2	750 GB	750 GB	100%
Drive 4	1 TB	750 GB	75% of 1 TB
Drive 6	2 TB	750 GB	38% of 2 TB

4. Select an **option** for spares:

- **I do not want a hot spare** – No spare will be created.
- **I want a local spare** – A local spare will be usable only by this RAID set.
- **I want a global spare** – A global spare is usable by any RAID set.

For more information about spares, see [Manage Global Spares](#) on [page 91](#).

5. Click **Next**.

Server Network **Storage** Security Monitor Maintenance

Storage Guides RAID Sets Volumes Quotas Snapshots iSCSI Disks

Create RAID set: **RAID 5 (Checksum)**
RAID Set Name: **md0**
Total Storage Capacity: **113.24 GB**

You have chosen the following 4 disks for this RAID set.

Disk	Location	Status	Usable Space	Usage	Type
<input checked="" type="checkbox"/> 50 GB SAS	Head Unit, disk 1	OK	37.75 GB	100%	Active Member
<input checked="" type="checkbox"/> 50 GB SAS	Head Unit, disk 2	OK	37.75 GB	100%	Active Member
<input checked="" type="checkbox"/> 50 GB SAS	Head Unit, disk 3	OK	37.75 GB	100%	Active Member
<input checked="" type="checkbox"/> 50 GB SAS	Head Unit, disk 4	OK	37.75 GB	100%	Active Member

Back Next Cancel

6. Verify your configuration, then click **Next** to create the RAID.

A message appears confirming the successful creation of the RAID set. It details how much storage space is available. The RAID will be syncing in the background.

7. Before you can place any data on this RAID set, you must create a volume. You use the buttons on this page to choose whether you want to create the volume now or later:

- Click **Create Volume Now** to create the volume now by following the procedure outlined in [Volume Creation](#) on [page 95](#).
- Click **Create Volume Later** to be returned to the **RAID Sets** page. You will need to remember to go to the **Volumes** option at a later time to create the required volume.

Group RAID Sets

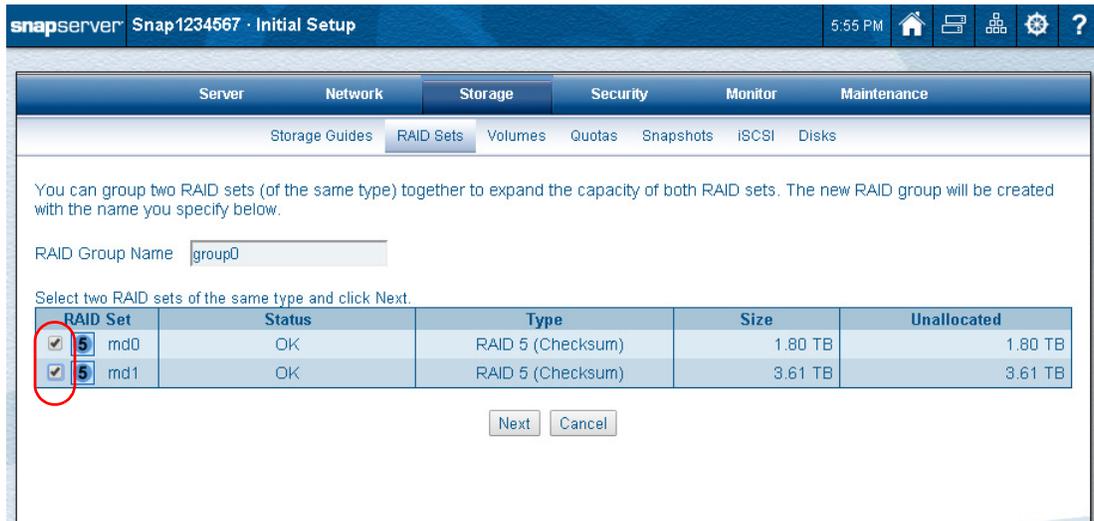
RAIDs can be grouped together to neatly resolve a number of capacity issues. For example, a volume on one RAID nearing full utilization can be expanded using spare capacity on another RAID. The ability to grow volumes beyond the capacity of a single RAID allows administrators to expand a volume without reconfiguring RAID sets and allows users to continue working as usual with no interruption.

Grouped RAID sets must be the same type. For example, you can group two RAID 1 sets or two RAID 5 sets but you cannot group a RAID 1 set and a RAID 5 set.

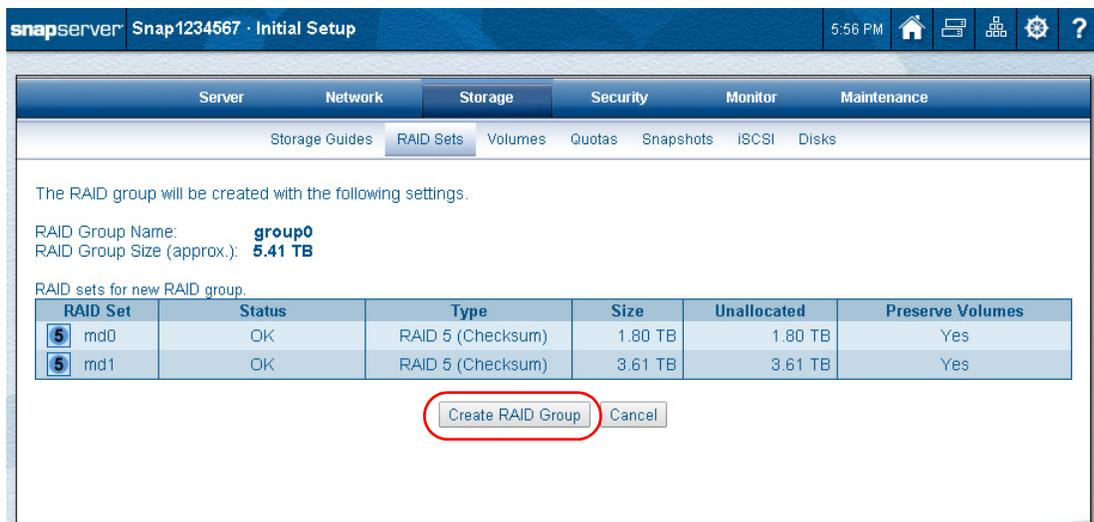
Click the **Group RAID** button to show the Group RAID Sets page.



1. Select (check) the **RAID sets** you want to include in the group and click **Next**.



2. At the confirmation page, click the **Create RAID Group** button to complete the process.



3. At the primary **RAID Sets** page, click the **group name** to see the details of the group.

The screenshot shows the SnapServer web interface. The top navigation bar includes 'Server', 'Network', 'Storage', 'Security', 'Monitor', and 'Maintenance'. Under 'Storage', there are sub-tabs for 'Storage Guides', 'RAID Sets', 'Volumes', 'Quotas', 'Snapshots', 'iSCSI', and 'Disks'. The 'RAID Sets' tab is active, displaying a table for RAID group 'group0'.

RAID Group	Status	Type	Size	Unallocated
group0	Active	RAID 5 (Checksum)	5.41 TB	5.41 TB

Below this table, it says 'RAID sets for RAID group group0.' and shows another table:

RAID Set	Status	Type	Size	Unallocated
md0	OK	RAID 5 (Checksum)	1.80 TB	-
md1	OK	RAID 5 (Checksum)	3.61 TB	-

At the bottom of the RAID sets table, there are buttons for 'Refresh', 'Delete RAID Group', 'Add RAID', and 'Close'.

From this page you can view the status, add another RAID set of the same type to the group, or delete the entire group. The status shows the following information in two tables:

Label	Description
<i>Group Table</i>	
RAID Group	The name of the RAID Group to which the RAID belongs
Status	The current condition of the Group: <ul style="list-style-type: none"> • <i>Active</i> – The group and all its RAID sets is functioning properly. • <i>Resync</i> – A device repair operation is in progress. • <i>Failure</i> – The RAID is offline. • <i>Degraded</i> – A drive has failed or been removed.
Type	Type of RAID configured on members of the group.
Size	The total capacity of the group.
Unallocated	The total storage space in the group not allocated to a volume or snapshot pool.
<i>RAID Set Table</i>	
RAID Set	The name of each RAID set. A symbol of the RAID type is shown to the left of the name. See Disks on page 129 .
Status	The current condition of the RAID: <ul style="list-style-type: none"> • <i>OK</i> – The RAID is functioning properly. • <i>Resync</i> – A device repair operation is in progress. • <i>Failure</i> – The RAID set is offline. • <i>Degraded</i> – A drive has failed or been removed.
Type	Type of RAID configured on the RAID set.
Size	The total capacity of the RAID set.
Unallocated	The total storage space not allocated to a volume or the RAID set's snapshot pool.

Adding an Expansion Unit

In a common scenario, a SnapServer is nearing full utilization. The administrator decides to add an expansion unit. The administrator creates the same RAID type on the expansion unit, groups it with the existing RAID set on the SnapServer, and then expands volume capacity using the new storage from the expansion unit. Clicking the **Expand Volume** button that appears does this automatically (see [Expand Volume Capacity](#) on page 95).

Expansion unit RAID sets are created in the same way as head unit RAID Sets. See [Create RAID Sets](#) on page 83.

Grouping RAIDs with other Grouped RAIDs

Just as RAID sets can be grouped, individual RAID groups can be brought together to form an even larger group.

For example, a SnapServer is running out of capacity. Two 12-drive expansion units are attached to the SnapServer to provide increased capacity. You can configure a RAID on each of the expansion units, then group the two of them together. The resulting RAID group can then be grouped with the RAID set on the SnapServer, allowing network users to take advantage of the full capacity of the head and expansion units with no loss of capacity.

See [Group RAID Sets](#) on page 86.

Deleting Grouped RAIDs



CAUTION: Deleting a RAID group deletes all the RAID sets, volumes, and shares. Any data on those volumes will be lost.

If one RAID set becomes inaccessible for any reason, the entire RAID group containing that RAID set will also become inaccessible. Depending on the cause, the RAID group may or may not be recoverable.

For example, if a RAID group spans a SnapServer and an expansion unit and one of the RAIDs goes down because of a disconnected cable, the RAID group is fully recoverable by reconnecting the cable and rebooting the system. On the other hand, if one of the RAIDs becomes corrupted and remains unrecoverable, the data in the other RAID will also be lost.

See [Delete a RAID Set](#) on page 94.

Snapshot Pools are Combined

When two RAID sets are grouped, the size of the resulting snapshot pool is the sum of each RAID set's formerly separate snapshot pools.

Two RAIDs at a Time Grouping Rule

To group more than two RAID sets, create a RAID group with two RAID sets, then add each remaining RAID set to the RAID group, one at a time.

Change RAID Settings

Click the **RAID Settings** button on the **RAID Sets** page to allow you to enable or disable the automatic incorporation of a disk into a degraded RAID set or a background scan.



Automatic Incorporation of Hot-Swapped Drives

If a RAID (except RAID 0) is running in degraded mode and a raw drive, a non-GuardianOS drive, or an unassigned GuardianOS-partitioned drive is “hot-inserted” into a SnapServer, it can be automatically assigned as a local spare and used to rebuild the degraded RAID. If there are no degraded RAIDs, a hot-inserted non-GuardianOS or unassigned drive will be automatically configured as a global spare. To enable automatic incorporation of unassigned drives, go to the **Storage > RAID Sets** page and click the **RAID Settings** button.

NOTE: Drives that have previously been configured for use in a different RAID set on any SnapServer are not automatically incorporated, regardless of whether automatic incorporation of unassigned drives is turned on. You must manually incorporate and configure these previously used drives.

Background Disk Scan

The background disk scan checks the integrity of RAID data by continuously scanning the disk drives for errors. Each RAID (except RAID 0) has its own background disk scan that is set to run when disk I/O drops to a low level of activity. Once the activity rises above the *idle threshold*, the background scan stops and waits for the activity to fall to the idle threshold again before resuming. As a result, there should be minimal to no impact on performance. Once the disk scan has completed a pass on a given RAID set, it waits a designated period of time before starting again.

The background disk scan is enabled by default. To disable the background disk scan, go to the **Storage > RAID Sets** page and click the **RAID Settings** button. Note the following:

- If the background disk scan is disabled, the SnapServer will still initiate a scan on a RAID if problems are detected on one of the RAID drives.
- The background scan will not run on RAIDs that are degraded, syncing, or rebuilding.

Manage Global Spares

A **spare** is a unused disk drive that can automatically replace a damaged drive in a RAID 1, 5, 6, or 10. Designating a disk drive as a spare helps ensure that data is available at all times. If one disk drive in a RAID fails or is not operating properly, the RAID automatically uses the spare to rebuild itself without administrator intervention. SnapServers offer two kinds of spares: local and global (see [Local and Global Spares](#) on [page 82](#)).

Click the **Global Spares** button to view the **Global Spares** page showing all the disks available for use, or that are in use, as global spares.

The following disks are available for use as (or are currently assigned as) global spares. Global spares are automatically used to replace failed members of RAID sets. Check the disks you want to use as global spares. Uncheck the disks you do not want to use as global spares.

Legend: Disk available for use as global spare Disk currently assigned as global spare

Disk	Location	Status	Usable Space
<input type="checkbox"/> 2.73 TB SATA	Head Unit, disk 7	OK	2.72 TB
<input checked="" type="checkbox"/> 931.51 GB SATA	Exp. Unit 1, disk 1	OK	919.26 GB
<input type="checkbox"/> 931.51 GB SATA	Exp. Unit 1, disk 2	OK	919.26 GB
<input type="checkbox"/> 3.64 TB SATA	Exp. Unit 1, disk 4	OK	3.63 TB

OK Cancel

To enable a disk as a global spare, check the checkbox next to the desired disk and click **OK**. More than one disk can be checked at a time. To disable or delete a disk assigned as a global spare, clear the checkbox next to the disk and click **OK**.

Edit RAID Set Properties

By clicking a RAID set name on the **RAID Sets** main page, details of that particular RAID set are shown on a **RAID Set Properties** page.

The screenshot shows the RAID Set Properties page for RAID set md0. The RAID set is in an OK status, with 3/3 members active and 0/0 spares active. It is part of group0 and has a size of 1.80 TB. The member disks are listed in the following table:

Disk	Location	Status	Usable Space	Action
931.51 GB SAS	Head Unit, disk 1	OK	919.26 GB	Remove
931.51 GB SATA	Head Unit, disk 2	OK	919.26 GB	Remove
931.51 GB SATA	Head Unit, disk 3	OK	919.26 GB	Remove

Number of global spares: 1

Note: This RAID set is a member of a RAID Group and cannot be deleted individually. To delete this RAID set, you must delete the RAID Group [group0](#).

The following table shows details about member drives of that specific RAID:

Label	Description
RAID Set	The name of each RAID.
Status	<p>The current condition of the RAID:</p> <ul style="list-style-type: none"> • <i>OK</i> – The RAID is functioning properly. • <i>OK-Spare Missing</i> – The RAID is functioning properly after a repair and rebuild. Because the local spare was consumed to repair the RAID, it is no longer available as a spare. <p>It is recommended that the original drive that failed be replaced to restore the RAID to its proper configuration and provide the full protection by one or more local spares. Alternately, you can click the link to reset the RAID spare count; however, the RAID will not be able to automatically recover from a drive failure.</p> <ul style="list-style-type: none"> • <i>Resync</i> – A device repair operation is in progress. • <i>Failed</i> – The RAID is offline. • <i>Degraded</i> – A drive has failed or been removed. <p>Number of members in the RAID:</p> <ul style="list-style-type: none"> • <i>Active</i> – Number of non-spare disks in the RAID that have a status of OK. • <i>Configured</i> – Number of non-spare disks with which the RAID was configured.

Label	Description
Group	The name of the RAID Group to which the RAID belongs.
Size	The total capacity of the RAID.
Unallocated	The total storage space not allocated to a volume.



CAUTION: Actions on this page can result in a loss of data. Be sure you have backed up your data before making changes to RAID sets.

From this secondary page, you can:

- Remove an individual RAID disk drive or local spare.
- Add a disk drive.
- Delete the entire RAID set (if not part of a group).

Remove a RAID Drive

From the **RAID Set Properties** page, you can remove a RAID disk drive or local spare by clicking the **Action** link on the far right of disk table. If you are removing a primary RAID disk, you will see a message page warning of RAID running in a degraded mode (with no or reduced parity).

NOTE: The only types of drives that can be removed are local spares, failed drives, or members of a RAID 1, 5, 6, or 10.

Add a Disk Drive as Local Spare to RAID

Clicking the **Add Disk** button at the bottom of the page displays a table of available disk drives.

Select one or more of the following disks to be used as local spares for RAID set **md0**.

Available disks: (Note: RAID set md0 supports only disks with a minimum usable space of 919.26 GB.)

Disk	Location	Status	Usable Space
<input type="checkbox"/> 2.73 TB SATA	Head Unit, disk 7	OK	2.72 TB
<input checked="" type="checkbox"/> 931.51 GB SATA	Exp. Unit 1, disk 2	OK	919.26 GB
<input checked="" type="checkbox"/> 3.64 TB SATA	Exp. Unit 1, disk 4	OK	3.63 TB

Number of global spares: 1

Next Cancel

Check one or more boxes to add disks to the RAID set and click **Next** for the confirmation page.

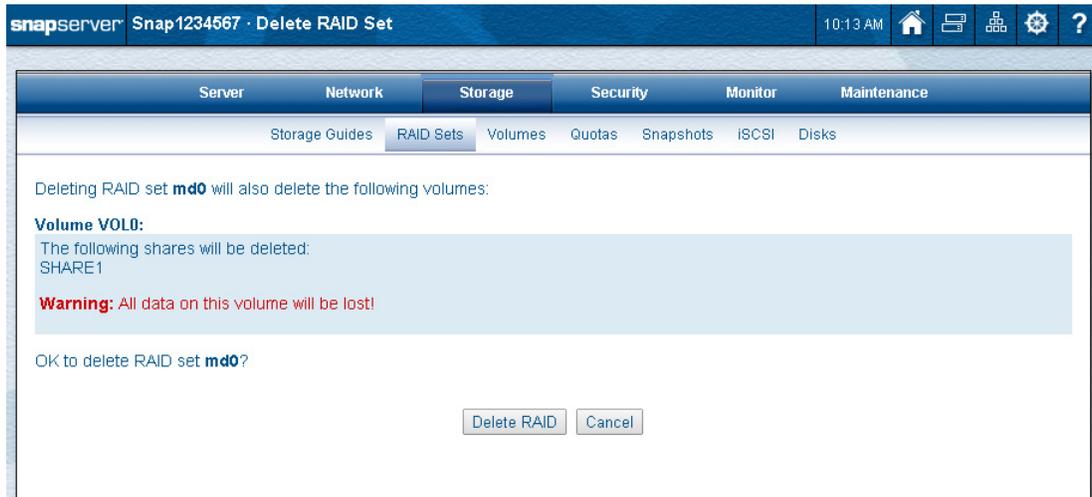
Adding disks is limited based on the type of RAID it is being made a member of:

- Disks cannot be added to a RAID 0.
- Disks can only be added to a RAID 1 as full members.
- Disks can only be added to all other RAID types (5, 6, or 10) as local spares.

NOTE: Disk drives that have been previously configured can be added; they are indicated in the **Storage > Disks** list by the  icon and a message stating that the disk has previously been used in a different system. If you want to use the drive, add it to the RAID as you would any other drive.

Delete a RAID Set

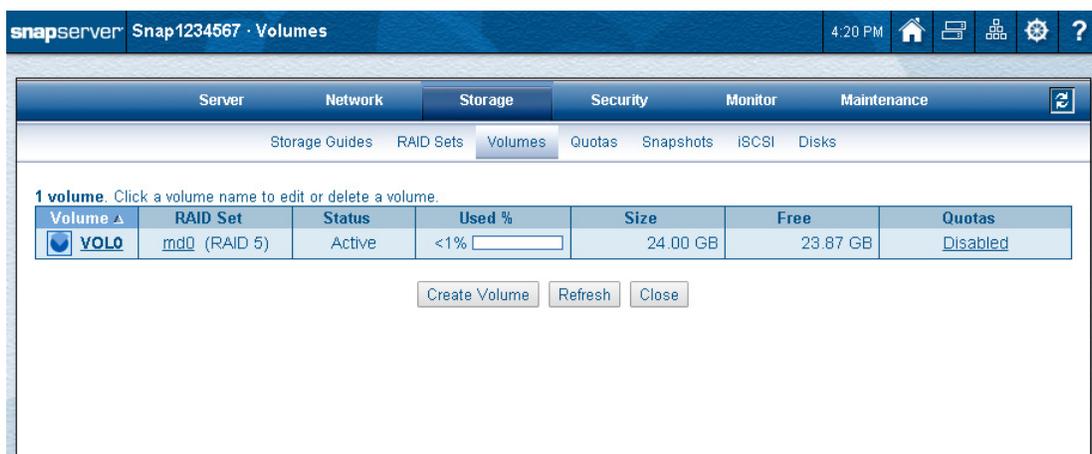
Click the **Delete RAID** button at the bottom to completely delete the RAID set.



This also deletes the Volume and Shares, including any data on them. Click the **Delete RAID** button again to complete the deletion.

Volumes

Use the **Storage > Volumes** page to manage the volumes that have been created on the RAID set.



From this page, you can:

- Create a new volume.
- Edit or delete the volume (by clicking the name).
- Enable/disable quotas on the volume (click the **Quotas** link at far right).

Volumes and the Snapshot Pool

The default capacity settings for the filesystem and future snapshot use are 80% for the filesystem and the remaining 20% for snapshots. You may need to adjust this figure depending on your snapshot strategy or expand the volume to all available space if you plan never to use snapshots. Keep in mind that you can increase or decrease snapshot pool size at any time, but volume space can only be increased. For more information, see [Estimating Snapshot Space Requirements](#) in [Chapter 6](#).

NOTE: GuardianOS snapshots should not be used on volumes that contain iSCSI disks. If a volume will contain one or more iSCSI disks, decrease the Snapshot pool size to zero. For information about creating snapshots of iSCSI disks, see [Configuring VSS/VDS for iSCSI Disks](#) in [Chapter 6](#).

Volume Creation

To create a volume on a RAID set, click the **Create Volume** button on the main page. When manually creating a RAID set, at the end you can click the **Create Volume Now** to launch the same **Create Volume** page.

snapserver Snap1234567 · Create Volume 2:23 PM

Server Network **Storage** Security Monitor Maintenance

Storage Guides RAID Sets **Volumes** Quotas Snapshots iSCSI Disks

Select the RAID set on which to create the new volume, as well as the new volume's name and size.

RAID Set: md0 - RAID 5 (113.23 GB available for volume)

Volume Name: VOLD

Volume Size: 30 GB

Enable Write Cache (not recommended without a configured, online UPS device)

You can reserve some of this new volume (typically around 20%) for storing snapshots. The amount you specify will decrease the volume's total size (as specified above) and increase accordingly the size of the snapshot pool. (The snapshot pool is used by all volumes on a given RAID set.)

Percentage of this volume's size to add to the snapshot pool for RAID set md0: 20%

Current allocation of RAID set md0	
Total size:	113.23 GB
Allocated size (for volumes):	0.00 MB
Snapshot pool size:	0.00 MB

Create Volume Cancel

Create A New Volume (and Share)

1. Navigate to **Storage > Volumes** and click the **Create Volume** button.

2. Configure the **settings** for the new volume:

Label	Description
RAID Set	Use the drop-down menu to select the RAID to be used for the volume.
Volume Name	Enter a name for the volume or accept the default (VOLO). You can use up to 20 alphanumeric characters or hyphens (but not spaces)
Volume Size	Enter the size you want for the volume or accept the default of the full size of the RAID. Use the drop-down list to choose the appropriate unit.
Enable Write Cache	Uncheck the box to turn off write caching if you do NOT have a configured, online UPS device in use.
Snapshot Percentage	Use the drop-down selector to choose the percentage you want to use for snapshots.

3. Click **Create Volume**.

4. At the confirmation page, review the **settings** and click **Create Volume** again to start the configuration.

To prevent data loss, you are cautioned if write caching was enabled without the required UPS in use. Click **Cancel** to return to the **Create Volume** settings page to make changes.



IMPORTANT: If you click **Cancel** to return to the **Create Volume** settings page, note that the settings revert to the defaults with the **Volume Size** reset to the maximum space.

snapserver Snap1234567 · Create Volume 4:19 PM

Server Network **Storage** Security Monitor Maintenance

Storage Guides RAID Sets **Volumes** Quotas Snapshots iSCSI Disks

You have chosen to create a new volume with the following properties:

RAID Set: **md0**
 Volume Name: **VOLO**
 Volume Size: **24 GB**
 Enable Write Cache: **No**

Current allocation of RAID set md0

Total size:	113.23 GB
Allocated size (for volumes):	0.00 MB
Snapshot pool size:	0.00 MB

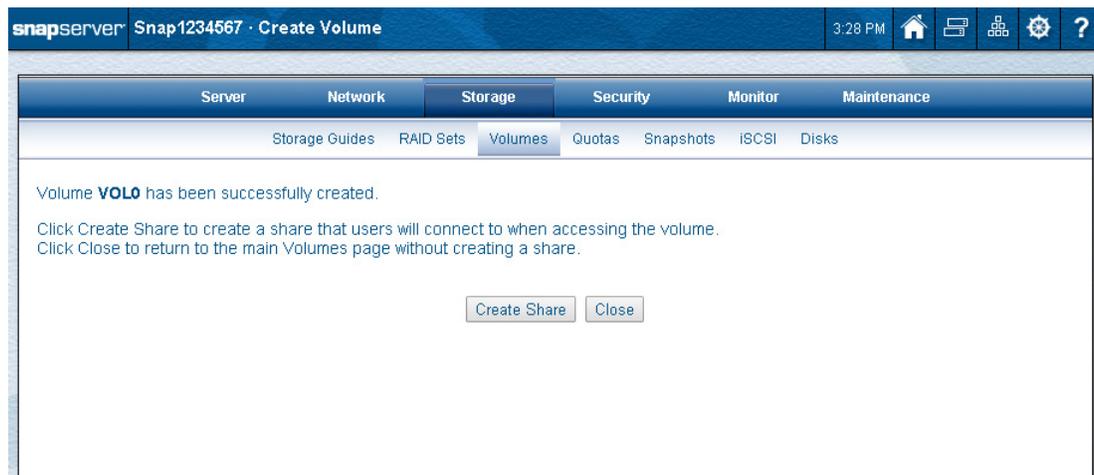
Allocation of RAID set md0 after volume is created

Total size:	113.23 GB
Allocated size (for volumes):	24.00 GB
Unallocated size remaining:	83.23 GB
Snapshot pool size:	6.00 GB

OK to create this volume?

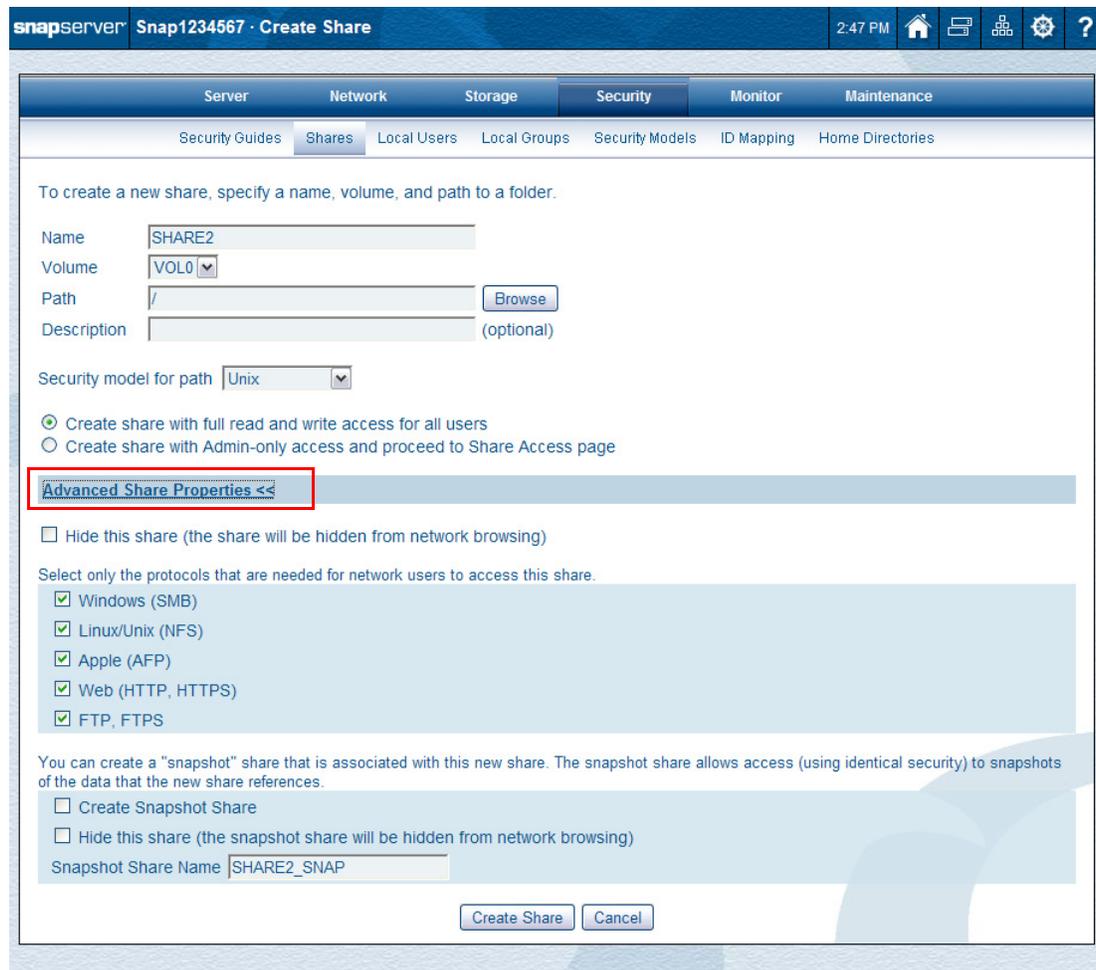
Create Volume Cancel

- At the successful volume creation page, click **Create Share** to provide access to this new volume.



This opens the **Security > Shares** option page so you can create a share pointing to this new volume.

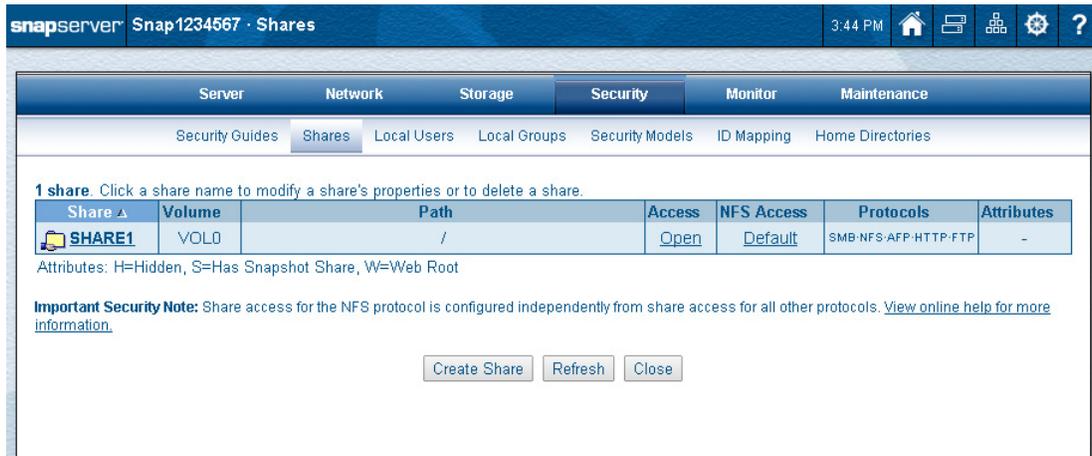
- Enter the appropriate **data**, select the necessary **options**, and then click **Create Share**.



Additional options can be accessed by clicking the **Advanced Share Properties** link at the bottom. See [Shares](#) in [Chapter 7](#) for complete details.

- Click the **Create Share** button again.

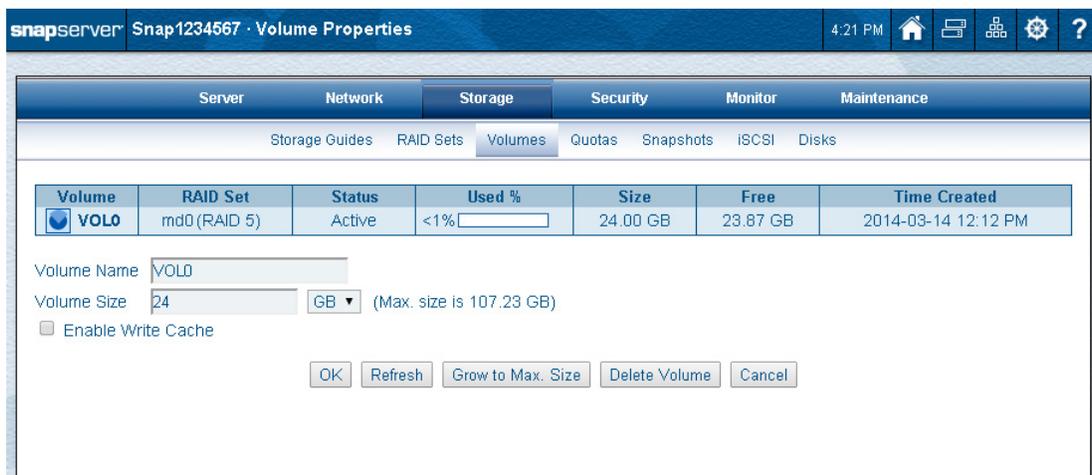
The share is automatically created and shown in the share table.



Volume Properties

By clicking a volume's name on the main **Volumes** page, details of that particular volume are shown on a **Volume Properties** page. From this secondary page, you can:

- Change the volume name.
- Increase the volume size.
- Enable the write cache (only recommended if a UPS system is attached and configured).
- Delete the entire volume.



Rename a Volume

On the **Volume Properties** page, enter the new name starting with an alphanumeric character and using up to 20 alphanumeric characters or hyphens (but not spaces). Then click **OK**.

Expand Volume Capacity

A volume's capacity can be expanded by navigating to the **Storage > Volumes** page and clicking the name of a volume. There are two ways to expand the size of a volume:

- **Adding Unallocated Capacity** – If there is unallocated capacity remaining on the RAID, you can add this capacity to the volume:
 - Change the **Volume Size** to a size less than or equal to the maximum size of the volume.
 - Click the **Grow to Max. Size** button at the bottom, and then click **OK** at the confirmation page.

NOTE: You cannot decrease the size of an existing volume. You can, however, delete the volume and recreate it as a smaller size.

- **Creating a New RAID Set** – If all capacity on the existing RAID set is allocated, and either a sufficient number of drives to create a new RAID set exists, or a RAID set of the same type with excess capacity exists, then the **Expand Volume** button appears. Click this button to create an additional RAID set, group the new RAID set with the existing RAID, and then expand the volume into the space on the new RAID group. This is usually accomplished through the addition of an expansion unit.

NOTE: If you expand the volume onto an existing RAID set with existing volumes, those volumes will be preserved and the expanded volume will only consume the free space on the RAID set.

Configure Volume Write Caching

NOTE: This is not related to write caching on iSCSI disks. For information about configuring write caching on iSCSI disks, see [Write Cache Options with iSCSI Disks](#) in [Chapter 6](#).

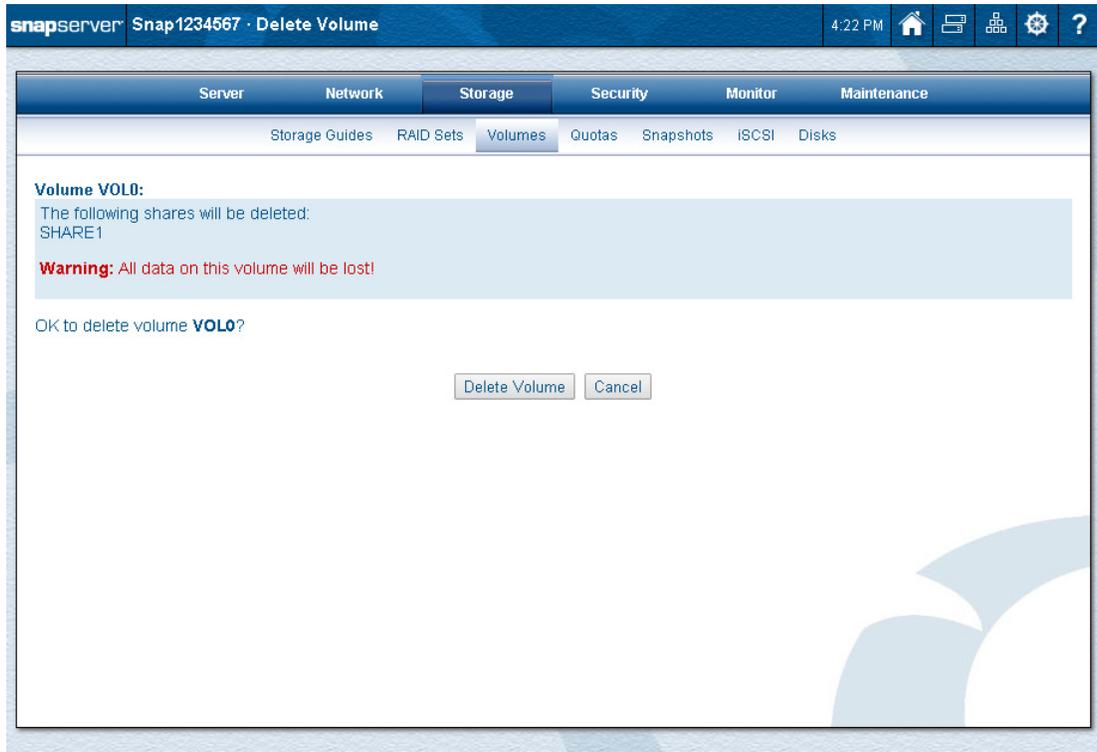
By default, write caching is enabled on all volumes. For systems that do not use a UPS device to help protect data during a power outage, or for applications that require synchronous writes to disk, write cache can be disabled on a volume-by-volume basis. When a volume's write cache is disabled, all data written to the volume bypasses memory buffers and writes directly to disk, helping to protect the data when writes are occurring during a power outage. While disabling write cache does help protect data, it also significantly impacts disk write performance.

NOTE: When write cache is disabled on a volume, disk cache is also disabled on all disk drives that are members of the RAID or RAID group hosting the volume. This can impact performance on other volumes with write cache enabled that are hosted by the same RAID or RAID group.

To enable write caching, verify that a UPS device is attached and configured. Check the **Enable Write Cache** box and click **OK**. To disable, uncheck the box and click **OK**.

Delete a Volume

To delete a volume, go to the **Volume Properties** page and click the **Delete Volume** button. At the confirmation page, click the **Delete Volume** button again.



The volume and all its shares and data are deleted.

Third-Party Applications on Deleted Volumes

Deleting volumes may move or disable certain third-party applications that are installed on the user volume space.

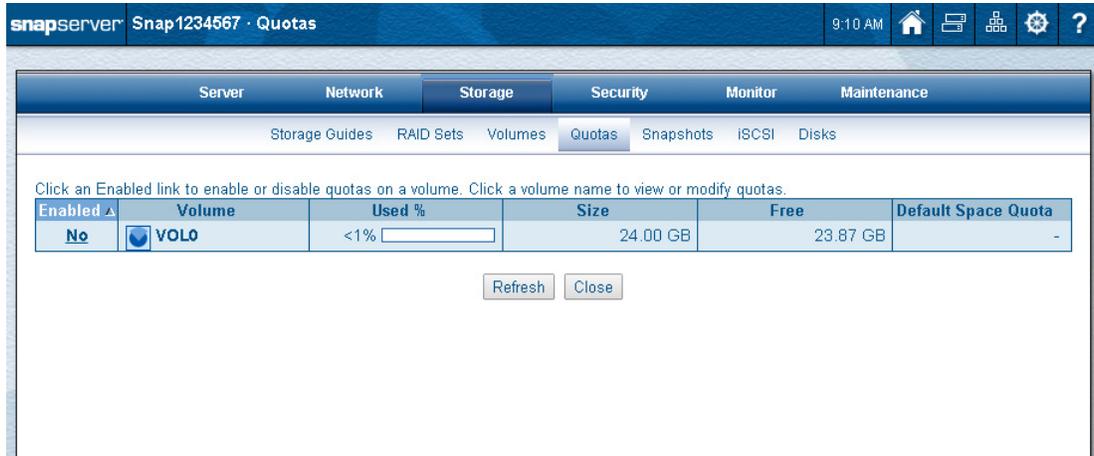
The CA Antivirus software and Snap EDR can reside on one or more volumes. If you delete a volume containing one of these applications, these components will be automatically moved to another volume, or deleted if no other volume or volumes of sufficient space are available. If deleted, CS Antivirus will need to be re-enabled and Snap EDR will need to be reinstalled when a new volume with sufficient space exists.

CA Antivirus. After creating your new storage configuration, you can reenble the antivirus software by navigating to the SnapExtensions page and selecting CA Antivirus. On the next page, check the **Enable** checkbox and click **OK**. The SnapServer reinstalls the antivirus software (using default settings) on the volume with the most available space. However, the installation process does not preserve custom antivirus configuration settings, so make a note of any such settings before deleting a RAID or volume. To reconfigure the antivirus software, click **Configure Antivirus**.

Snap EDR. To reactivate Snap EDR functionality after creating a new volume, download the Snap EDR package from the SnapServer website and install it on the server using the OS Update feature. Then go to the **Misc. > SnapExtensions** page using the Site Map and enable it.

Quotas

Quotas, which are only available in Traditional RAID, are configured in the **Storage > Quotas** screen of the Web Management Interface.



Assigning quotas ensures that no one user or group consumes a disproportionate amount of volume capacity. Quotas also keep tabs on how much space each user, LDAP group, or NIS group is currently consuming on the volume, allowing for precise tracking of usage patterns. You can set individual quotas for any LDAP group, NIS group, Windows domain, or local user known to the SnapServer. Group quotas are available only for LDAP and NIS groups.

For users and groups, there are no preassigned default quotas on the SnapServer. When quotas are enabled on the SnapServer, you can assign a default quota for all users, or allow all users to have unlimited space on the volume. Unless you assign individual user or group quotas, all users and groups will receive the default quota when it is enabled.

In calculating usage, the SnapServer looks at all the files on the server that are owned by a particular user and adds up the file sizes. Every file is owned by the user who created the file and by the primary group to which the user belongs. When a file is copied to the server, its size is applied against both the applicable user, LDAP, and NIS group quotas.

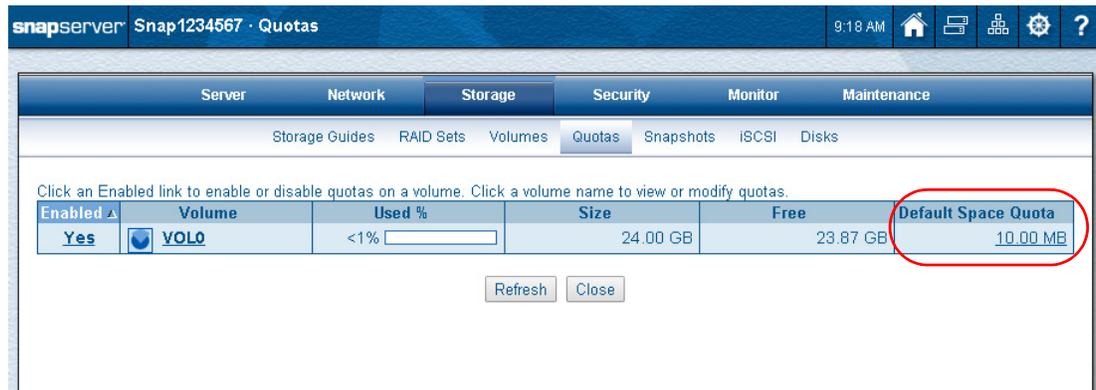
Quotas Page

The Quotas page shows if quotas are enabled on the volumes. From here you can:

- Enable or disable quotas.
- Modify the size of a quota.
- Change the way quotas are displayed.

NOTE: Quotas can also be accessed from **Storage > Volumes** by clicking the link in the Quotas column on the far right.

When a quota is enabled on a volume, the view/modify name link in the **Volume** column is active and a status is shown in the **Default Space Quota** column.



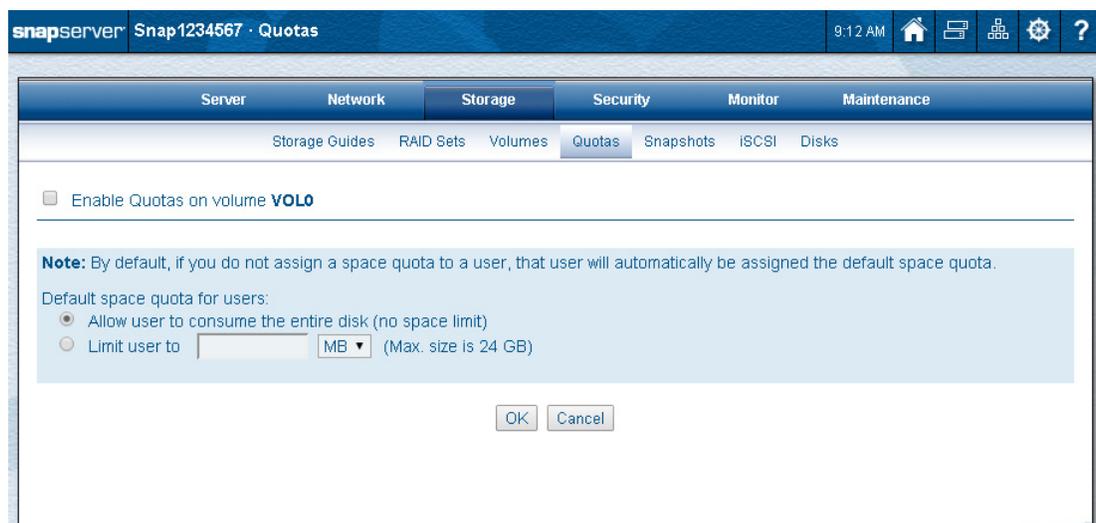
For enabled quotas, the **Default Space Quota** column shows one of the following:

- **An amount** – the default quota size assigned to users in that volume who do not have a specific quota assigned to them.
- **“no limit”** – text displayed when quotas are enabled but no default quota size is configured for users in that volume (users can consume the entire disk).
- **“–” (dash)** – a dash indicates quotas are disabled for that volume.

The **Default Space Quota** amount doubles as a link to access the quota enable/disable page.

Enable/Disable Quotas

From the Quotas default page, you can enable/disable quotas on the volume by clicking the **Yes/No** link in the **Enabled** column on the far left. When you click the link (left-most column in the Quota table), a secondary page is shown for managing the quota properties.



1. Check/uncheck the **Enable Quotas** box to enable/disable quotas.

NOTE: The **Enable Quotas** check box must be checked before changes are accepted.

2. Select one of the two **default quota options** to set the quota applied to users who do not have individual quotas assigned to them.

3. Click **OK** (or **Cancel** to return without changes).

NOTE: The server may require a restart. If so, a warning message is displayed. Click **OK** to proceed.

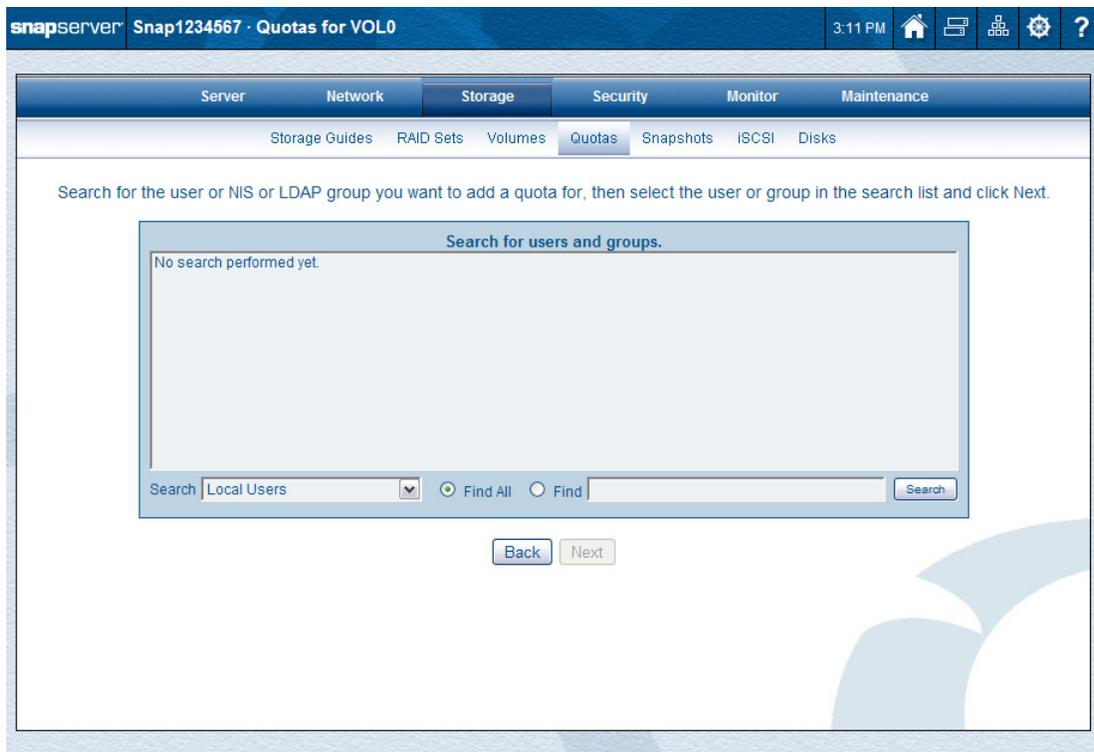
You are returned to the default **Quotas** page.

Add Quotas Wizard

1. Click the volume **name link** on the **Quotas** default page to open the quota search and configuration page for that specific volume.



2. Click **Add Quota** to launch the search wizard.



3. To search for a user, LDAP group, or NIS group, select the **domain** from the **Search** drop-down list, enter the **search string** (or select Find All), and click **Search** at the lower right.

NOTE: For domains that require authentication (showing an "(A)" after the name), after you select the domain name, enter the User Name and Password for that domain.

The screenshot shows a search interface with a dropdown menu set to 'Cardinals Users (A)'. Below the dropdown are two input fields: 'User Name' and 'Password'. A red arrow points to the 'User Name' field.

- Returned results will include all users, LDAP groups, and NIS groups whose name **begins** with the string entered in the **Search** field.
 - The search results returned may be limited. Fine tune your search by using a more specific string to return the names desired.
 - On the rare occasion you need to search for a Windows domain that's not listed ("remote domain"), select a Windows domain from the Search drop-down list through which to search, then enter in the Find box the name of the remote domain, followed by a slash (/) or backslash (\) and the user name for which you are searching (for example, `remote_domain\user_name`). After you click **Search**, an authentication prompt may be presented for the remote domain.
4. From the search results, select the **name** of the appropriate user, LDAP group, or NIS group, and click **Next**.

The screenshot shows the SnapServer Quotas configuration page. The search results are displayed in a window titled 'Search for users and groups.' with the following content:

Local Users (2 found)

Fred
Vicky

At the bottom of the search window, the search field contains 'Local Users' and there are 'Find All' and 'Find' radio buttons. Below the search window are 'Back' and 'Next' buttons.

- At the user quota properties page, select or enter the **quota** desired, and click **OK**.

Quota for user **Local User/Fred** on volume **VOLD0** (VOLD is 24 GB).

Quota	Used	Used (%)
(10 MB)	0.00 MB	0%

User space quota:

- No space limit (user can consume space up to the size of the entire volume)
- Limit to MB (Max. size is 24 GB)
- Use default user space quota (10 MB)

OK Cancel

NOTE: LDAP and NIS groups do not display the third option for a default user quota.

Displaying/Changing Quotas

To display and configure quotas of users or groups that have used space on this volume or have had specific quotas assigned to them from the volume:

- Click the volume **name link** on the **Quotas** default page to open the quota search and configuration page for that volume.
This link is only active for volumes that have quotas enabled.
- Select the sort and view **parameters**.

Change the following fields to specify how quotas are displayed for **VOLD0**. Default user space quota: 10 MB.

Sort by: Name View: Assigned or space used Find All Find Search

No search performed yet.

Add Quota Close

- From the **Sort** drop-down list, choose **Name**, **Limit**, **Used**, or **Used (%)**.

Change the following fields to specify how quotas are displayed for **VOLD0**. Default user space quota: 10 MB.

Sort by: Name View: Assigned or space used Find All Find Search

No search performed yet.

Add Quota Close

- From the **View** drop-down list, choose **Only assigned quotas**, **Only with space used**, **Assigned or space used**, or **> 95% used**.



3. Enter the search string (or select Find All).

When entering a search string:

- Returned results will include all users and groups whose name **begins** with the string entered.
- To search a specific Windows, LDAP, or NIS domain, enter the domain name, followed by a slash (/) or backslash (\) before the search string.
- To search only local user and groups, enter “**local**” followed by a backslash (\) before the search string.
- The search results returned may be limited. Fine tune your search by using a more specific string to return the names desired.

4. Click Search.

A detailed list of users, LDAP groups, or NIS groups that match the parameters:

User or Group (click to edit)	Domain	Limit	Used	Used (%)
nisGroup000	atlanta Groups	no limit	1.67 TB	24%
nisGroup001	atlanta Groups	882.18 GB	442.65 GB	50%
nisGroup002	atlanta Groups	441.09 GB	147.72 GB	33%
nisGroup003	atlanta Groups	641.58 GB	342.43 GB	53%
nisGroup004	atlanta Groups	no limit	1.73 TB	25%
nisGroup005	atlanta Groups	542.88 GB	295.71 GB	54%
nisGroup006	atlanta Groups	705.74 GB	398.36 GB	56%
nisGroup007	atlanta Groups	371.44 GB	334.92 GB	90%
nisGroup008	atlanta Groups	542.88 GB	475.08 GB	87%
nisGroup009	atlanta Groups	no limit	732.20 GB	10%
nisGroup010	atlanta Groups	1,008.20 GB	920.75 GB	91%
nisGroup011	atlanta Groups	no limit	5.37 TB	77%
nisGroup012	atlanta Groups	no limit	1.63 TB	23%
nisGroup013	atlanta Groups	no limit	1.54 TB	22%
nisGroup014	atlanta Groups	1,008.20 GB	858.30 GB	85%
nisGroup015	atlanta Groups	no limit	6.86 TB	99%
nisGroup016	atlanta Groups	415.14 GB	33.52 GB	8%
nisGroup017	atlanta Groups	470.49 GB	378.74 GB	80%
nisGroup018	atlanta Groups	1,008.20 GB	529.67 GB	52%
nisGroup019	atlanta Groups	no limit	4.18 TB	60%
nisGroup020	atlanta Groups	1.15 TB	537.22 GB	45%
nisGroup021	atlanta Groups	no limit	1.63 TB	23%

NOTE: The search results returned may be limited. Fine tune your search by using a more specific string to return the names desired.

Parentheses around a quota limit amount indicates the volume default quota is being used. If the volume's default quota limit is set to “no limit,” then **(no limit)** is displayed. If the volume's default quota limit is set to an actual value, such as 500 GB, then “(500 GB)” is displayed.

No parentheses around the limit amount indicates a specific quota has been assigned that is different from the default value. If the default quota limit is set to “no limit” but a particular user's or group's quota is set to 750 GB, then **750 GB** is shown instead of the default “**(no limit)**.”

The one exception to this is LDAP and NIS groups. They don't use a volume default quota, so **no limit** (without parentheses) is shown.

5. From the search results, select the **name** of the appropriate user, LDAP group, or NIS group from the left column to open the quotas properties page.
6. Select or enter the **quota** desired, and click **OK**.
LDAP and NIS groups do not display the third option for a default user quota.

NOTE: Any changes override the default volume quota for this user, LDAP group, or NIS group.

The main search page is displayed and your changes are reflected here if allowed by your search criteria.

The screenshot shows the SnapServer web interface for Snap7654321. The page title is "Quotas for VOL0". The navigation menu includes Server, Network, Storage, Security, Monitor, and Maintenance. Under Storage, there are sub-menus for Storage Guides, RAID Sets, Volumes, Quotas, Snapshots, iSCSI, and Disks. The main content area shows a search bar with "Sort by" set to "Name" and "View" set to "Assigned or space used". Below the search bar, it says "Quotas: 1 found." and displays a table with the following data:

User or Group (click to edit)	Domain	Limit	Used	Used (%)
hobbiesue	Local Users	100.00 MB	0.00 MB	0% <input type="text"/>

At the bottom of the table, there are three buttons: "Add Quota", "Refresh", and "Close".

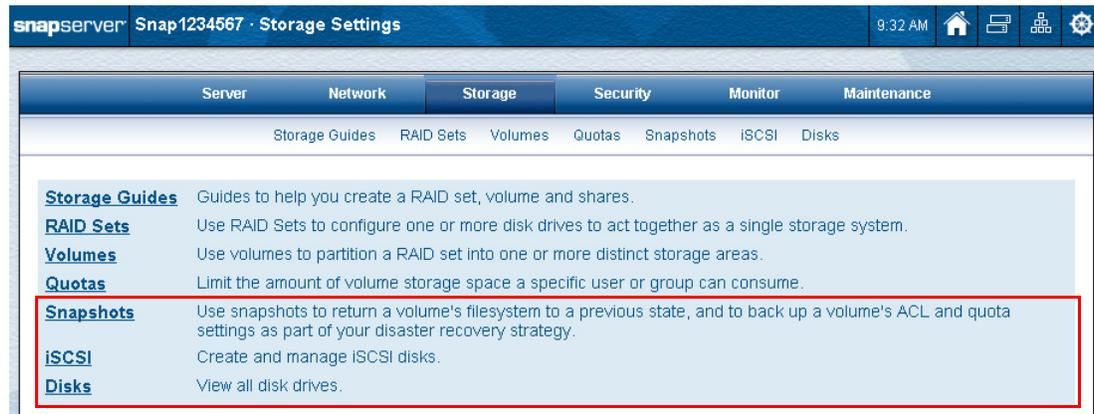
Other Storage Options

Once the RAID sets have been configured using either the DynamicRAID or Traditional RAID options, you can configure the other three storage options for your SnapServer: **Snapshots**, **iSCSI**, and **Disks**.

DynamicRAID Configuration



Traditional RAID Configuration



For information on the DynamicRAID configuration option, see [DynamicRAID Storage in Chapter 4](#). For information on the Traditional RAID configuration option, see [Traditional RAID Storage in Chapter 5](#).

Topics in Other Storage Options:

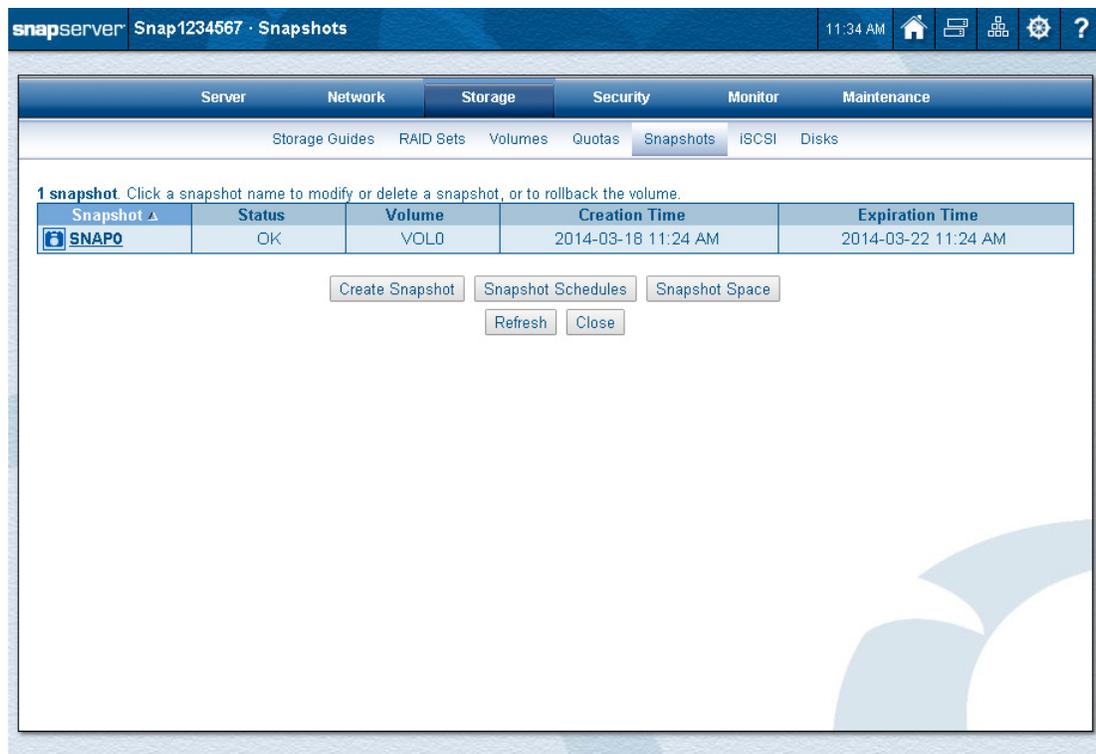
- [Snapshots](#)
- [iSCSI Disks](#)
- [Disks](#)

Snapshots

A *snapshot* is a consistent, stable, point-in-time image of a Traditional RAID volume or DynamicRAID storage pool that can be backed up independent of activity on the live volume or storage pool. Snapshots can also satisfy short-term backup situations such as recovering a file deleted in error, or even restoring an entire filesystem, without resorting to tape. More importantly, snapshots can be incorporated as a central component of your backup strategy to ensure that all data in every backup operation is internally consistent and that no data is overlooked or skipped.

NOTE: The Snapshot feature described here does not apply to snapshots for iSCSI disks. Supported Windows servers can create native snapshots of iSCSI disks using VSS. For more information, see [Configuring VSS/VDS for iSCSI Disks](#) on page 125.

To manage the snapshot options using the SnapServer Web Management Interface, go to **Storage > Snapshots**.



These options are available in the Snapshots section of the Web Management Interface:

Action	Procedure
Create a New Snapshot	<p>Click Create Snapshot. The process involves first defining snapshot parameters, and then scheduling when and how often to run the snapshot.</p> <p>Do not take more snapshots than your system can store, or more than 250 snapshots. Under normal circumstances, between nine and ten snapshots are sufficient to safely back up any system.</p>
Edit a Snapshot Schedule	<p>Click the Snapshot Schedules button, and then click the snapshot name. You can modify all snapshot parameters.</p>

Action	Procedure
Adjust Snapshot Space	NOTE: Traditional RAID only. Click the Snapshot Space button, then click the RAID set name for the snapshot space you want to adjust. You can adjust the amount of space allotted for snapshots on each RAID set or RAID group.
Edit and Delete	Click the snapshot's name to open the Snapshot Properties page. You can edit the snapshot's name and duration, or delete the snapshot.
Roll Back a Snapshot	NOTE: Traditional RAID only. Click the snapshot's name to open the Snapshot Properties page. You can roll back the snapshot to a volume.

NOTE: It is recommended that snapshots be taken when the system is idle or under low data traffic to minimize conflicts.

Clicking the **Refresh** button updates the data shown. This is helpful when waiting for a snapshot to complete.

When single snapshots are originally created or while recurring snapshots are active, a refresh icon (🔄) is displayed to the right on the tab bar. It indicates that the snapshot data in the table is being refreshed every 5 minutes.

Clicking the **Close** button returns you to the **Storage** home page.

NOTE: The presence of one or more snapshots on a volume (Traditional RAID) or storage pool (DynamicRAID) usually has minimal performance impact, but may impact write performance when frequently overwriting file data. Additional snapshots taken of the same volume or storage pool do not have additional impact; in other words, the write performance impact of one snapshot on a volume is the same as the impact of 100 snapshots on the same volume.

Creating Snapshots

Creating a snapshot involves first defining the snapshot and then scheduling the snapshot. For regular data backup purposes, create a recurring snapshot. A recurring snapshot schedule works like a log file rotation, where a certain number of recent snapshots are automatically generated and retained as long as possible, after which the oldest snapshot is discarded. You can also create individual, one-time-only snapshots as needed.

NOTE: If you have created a new volume or have numerous existing snapshots, make sure you have enough space allocated in the snapshot space; otherwise, you will not be able to create the snapshot.

Scheduling Snapshots

Snapshots should ideally be taken when your system is idle. It is recommended that snapshots be taken before a backup is performed. For example, if your backup is scheduled at 4 a.m., schedule the snapshot to be taken at 2 a.m., thereby avoiding system activity and ensuring the snapshot is backed up. See [Schedule Snapshots](#) on [page 113](#) for more information.

Snapshots and Backup Optimization

When you back up a live volume directly, files that reference other files in the system may become out-of sync in relation to each other. The more data you have to back up, the more time is required for the backup operation, and the more likely these events are to occur. By backing up the snapshot rather than the volume itself, you greatly reduce the risk of archiving inconsistent data. See [Schedule Snapshots](#) on [page 113](#) for more information.

Snapshots and iSCSI Disks

Running a GuardianOS snapshot on a volume containing an iSCSI disk will abruptly disconnect any clients attempting to write to the iSCSI disk and the resulting snapshot may contain inconsistent data. Do not use GuardianOS snapshots on a volume containing an iSCSI disk.

To create a native snapshot of an iSCSI disk on Windows systems, use the VSS feature described in [Configuring VSS/VDS for iSCSI Disks](#) on [page 125](#).

Create a Snapshot

1. Navigate to **Storage > Snapshots** and click **Create Snapshot**.

The screenshot shows the 'Create Snapshot' configuration page in the SnapServer web interface. The page is titled 'SnapServer Snap1234567 · Create Snapshot' and shows the 'Storage' tab selected. The 'Snapshots' sub-tab is active, displaying fields for 'Snapshot Name' (SNAP0), 'Source Volume' (VOLD), and options to 'Create Snapshot Now' or 'Create Snapshot Later'. The 'Create Snapshot Later' option is selected, showing a 'Start Date' of 2014-03-18, a 'Start Time' of 12:00 PM, and a 'Repeat Interval' of 10 days. A 'Duration' of 10 days is also set. A 'Create Recovery File' checkbox is present with a note. 'Create Snapshot' and 'Cancel' buttons are at the bottom.

2. Configure the desired **settings**.

- Enter or accept the **Snapshot Name** (20 character maximum).
- Select the **Source Volume/Storage Pool** from the drop-down list.
- Specify **when** to create the snapshot.

Click either the **Create Snapshot Now** button to run the snapshot immediately or the **Create Snapshot Later** button to schedule the Snapshot for a later time. When you select the **Create Snapshot Later** button, a new input section appears below the option. Complete the following:

- Schedule a **Start Date** for the snapshot.
- Choose a **Start Time** to run the snapshot.
- Select either to create the snapshot only once (**One Time**) or to have it **Recurring**.

To repeat a snapshot periodically using the **Recurring** option, specify the repeat interval in hours, days, weeks, or months.

- Specify the **Duration** of the snapshot.

In the **Duration** field, specify how long the snapshot is to be active in hours, days, weeks, or months. The SnapServer automatically deletes the snapshot after this period expires, as long as no older unexpired snapshots exist that depend on it. If any such snapshot exists, its termination date is displayed at the bottom of the page. You must set the duration to a date and time after the displayed date.

- Specify whether to create a recovery file.

If you plan to create a backup from the snapshot and want to save filesystem security configuration and quota consumption and in the backup, check the **Create Recovery File** box. See [Schedule Snapshots](#) on [page 113](#) for more information on coordinating snapshots and backup operations.

3. Click **Create Snapshot**.

If you elected to run the snapshot immediately, it appears in the current snapshots table on the **Snapshot** page.

1 snapshot. Click a snapshot name to modify or delete a snapshot, or to rollback the volume.

Snapshot	Status	Volume	Creation Time	Expiration Time
SNAP0	OK	VOL0	2014-03-18 11:24 AM	2014-03-22 11:24 AM

Buttons: Create Snapshot, Snapshot Schedules, Snapshot Space, Refresh, Close

If you scheduled the snapshot to run at a later time, it appears in the scheduled snapshots table under **Snapshot Schedules**.

1 snapshot schedule. Click a snapshot schedule name to modify or delete a schedule.

Schedule	Storage Pool	Repeat Interval	Next Snapshot Time
SNAP1	Head Unit Storage	One time only.	2014-03-20 2:00 AM

Buttons: Refresh, Close

Accessing Snapshots

After snapshots are created, they can be accessed via a snapshot share. Just as a share provides access to a portion of a live volume (or filesystem), a snapshot share provides access to the same portion of the filesystem on all current snapshots of the volume. The snapshot share's path into snapshots mimics the original share's path into the live volume. The snapshot share is created in the **Shares** section under the **Security** tab. See [Shares](#) in [Chapter 7](#) and [Snapshot Access](#) in [Appendix C](#) for details.

Schedule Snapshots

Like backups, snapshots can be scheduled to recur at a designated time and interval. Part of the initial creation process is to set the time and date when the snapshot will occur or recur.

In addition to synchronizing the backup and snapshot schedules, you must create a share (and snapshot share) to the appropriate directory so that the backup software can access the snapshot. For most backup purposes, the directory specified should be one that points to the root of the volume so that all of the volume's data is backed up and available from the snapshot share.

Step 1: Create a snapshot for each Traditional RAID volume or DynamicRAID storage pool you want to back up.

In the Web Management Interface, navigate to **Storage > Snapshots**, and click **Create Snapshot**. When defining and scheduling the snapshot, consider the following:

- Check the **Create Recovery File** checkbox to ensure that the ACL, extended attributes, and quota information are captured and appended to the snapshot. This step is needed because many backup packages do not back up native ACLs and quotas. Placing this information in a recovery file allows all backup packages to include this information. If the volume needs to be restored from tape, or the entire system needs to be recreated from scratch on a different server, this information may be required to restore all rights and quota information.
- Offset the snapshot and backup schedules such that the backup does not occur until you are sure the snapshot has been created. The snapshot itself does not require much time, but creating the recovery file may take up to 30 minutes, depending on the number of files in the volume.

For example, assuming you schedule nightly backups for a heavily used volume at 3:00 a.m., you might schedule the snapshot of the volume to run every day at 2:30 a.m., allowing half an hour for the snapshot to run to completion.

Step 2: If you have not already done so, create a share for each volume with snapshot share enabled.

In the Web Management Interface, navigate to the **Security > Shares** page, and click **Create Share**. Select the volume you want the share to point to (if you want to create a share to the root of the volume, simply accept the default path). Click **Advanced Share Properties**, then select **Create Snapshot Share**.

Step 3: Set the backup software to archive the latest version of the snapshot.

The SnapServer makes it easy to configure your backup software to automatically archive the most recent snapshot. Simply configure your backup software to copy the contents of the **latest** directory within the snapshot share you created.

For example, assume the snapshot share named *SHARE1_SNAP* contains the following four directories:

```
latest
2014-03-25.120000
2014-03-01.000100
2014-02-17.020200
```

Each directory inside the snapshot share represents a different snapshot. The directory names reflect the date and time the snapshot was created. However, the **latest** directory always points to the latest snapshot (in this case, *2014-02-17.020200*, or February 17th, 2014, at 2:02 a.m.). In this case, configuring the backup software to copy from:

```
\SHARE1_SNAP\latest
```

ensures that the most recently created snapshot is always archived.

Depending on their ability to cross bind mounts, locally-installed backup agents can access the snapshot share in one of two ways:

- via `/shares` (for example, `/shares/SHARE1_SNAP/latest`)
- via `/links` (for example, `/links/SHARE1_SNAP/latest`)

Snapshot Space

Snapshots are stored in a RAID set or storage pool in snapshot space reserved within the RAID set for this purpose. Each RAID set on the system contains its own independent snapshot space. This space contains all snapshot data for all the volumes on the RAID set or storage pool.

The amount of space used on a Traditional RAID can be seen by navigating to **Storage > Snapshots > Snapshot Space**.

The screenshot shows the SnapServer web interface for 'Snap1234567 - Snapshot Space'. The 'Storage' tab is active, and the 'Snapshots' sub-tab is selected. The main content area shows '1 RAID set' and a table for 'RAID Space Allocation' and 'Snapshot Space Usage'.

RAID Set	RAID Space Allocation	Snapshot Space Usage
md0	VOLD: 24.00 GB <Snapshot Space>: 6.00 GB <Unallocated Space>: 83.23 GB <Total Space>: 113.23 GB	0% (4 MB / 6 GB)

Buttons: Refresh, Close

Estimating Snapshot Space Requirements

Snapshot data grows dynamically for as long as a snapshot is active and as long as there is enough space available in the snapshot space to store them. When the snapshot space approaches its capacity (at about 95 percent), the SnapServer deletes the oldest snapshot's data to create space for more recent snapshot data.

By default, 80 percent of RAID set or storage pool capacity is allocated to volumes and 20 percent to snapshot space. You can adjust the amount of snapshot space on the RAID set or storage pool up (assuming unallocated space exists) or down according to your needs. If you find that your snapshot strategy does not require all of the space allocated to the snapshot space by default, consider decreasing snapshot space capacity and reallocating the capacity to the Traditional RAID volumes or data storage in the DynamicRAID storage pool.

Adjusting Snapshot Space Size

The size of the snapshot space can be adjusted at any time. However, under DynamicRAID, to increase the size of the space a new disk drive must be added to the Storage Pool.

To adjust the size of the snapshot space:

- For DynamicRAID, navigate to the **Storage > Storage Pools** page, and then click the **Storage Pool name** for the snapshot space you want to adjust. Using the drop-down list, select the percentage of space you want to reserve on this pool.

- For Traditional RAID, navigate to the **Storage > Snapshots** page, click the **Snapshot Space** button, and then click the **RAID set name** for the snapshot space you want to adjust. Enter the new amount in the **Snapshot Space** field.

The number of snapshots that a RAID set can support is a function of these factors:

- The space reserved for the snapshot data.
- The duration of the snapshots you create.
- The amount and type of write activity to the volume since the snapshot was created.

The following table describes minimum and maximum allocation cases.

Allocate about 10% of RAID set if	Allocate about 25% of RAID set if
<ul style="list-style-type: none"> • Activity is write-light. • Write access patterns are concentrated in a few places. • A small number of Snapshots must be available at any point in time. 	<ul style="list-style-type: none"> • Activity is write-heavy. • Write access patterns are randomized across the volume. • A large number of Snapshots must be available at any point in time.

There are two other processes that may affect the size of the snapshot space:

- **Creating a Traditional RAID Volume** – In the course of creating a new volume, a drop-down list allows you to add a percentage of the capacity being allocated to the new volume to the snapshot space. This feature defaults to 20 percent, the recommended amount of space to reserve for snapshots. If you do not plan to use snapshots with this volume, maximize volume capacity by reducing this percentage to zero; if you do plan to use snapshots, adjust this percentage in accordance with the guidelines discussed in the previous section, [Estimating Snapshot Space Requirements](#) on [page 114](#).
- **Creating a Traditional RAID Group** – When two or more RAID sets are grouped together, their snapshot spaces are added together. For example, if RAID set A with a snapshot space of 50 GB is grouped with RAID set B with a snapshot space of 25 GB, the resulting RAID set group will have a snapshot space of 75 GB. Depending on the purpose you had in mind when grouping the RAID sets, the result of combining the two snapshot spaces may or may not be desirable, and you will need to readjust the size as described previously.

Snapshot Properties

From the **Snapshot** main page table, you can click a snapshot name to access the **Snapshot Properties** page. There you can edit the name and duration, delete the snapshot, or, for Traditional RAID configurations, roll back to a previous state.

Snapshot	Status	Volume	Creation Time	Expiration Time
SNAPO	OK	VOL0	2014-03-18 11:24 AM	2014-03-22 11:24 AM

Snapshot Name:

Duration: days

Buttons: OK, Delete Snapshot, Rollback, Cancel

Edit a Snapshot

You can edit the name and duration by changing the data in the detail fields and clicking **OK**.

Delete a Snapshot

Click the **Delete Snapshot** button and then click it again on the confirmation page. The snapshot is deleted and all its associated data.

Rollback to a Previous State

NOTE: This is only available on a Traditional RAID configuration.

If you need to restore an entire filesystem to a previous state, you can do so without resorting to tape. The snapshot rollback feature allows you to use any archived snapshot to restore an entire filesystem to a previous state simply by selecting the snapshot and clicking the **Rollback** button. During the rollback operation, data on the volume will be inaccessible and changes blocked.



CAUTION: Rolling back a volume cannot be undone and should only be used as a last resort after attempts to restore selected directories or files have failed. Performing a rollback on a volume may disable the antivirus software. If you are using the antivirus software, take the necessary precautions.

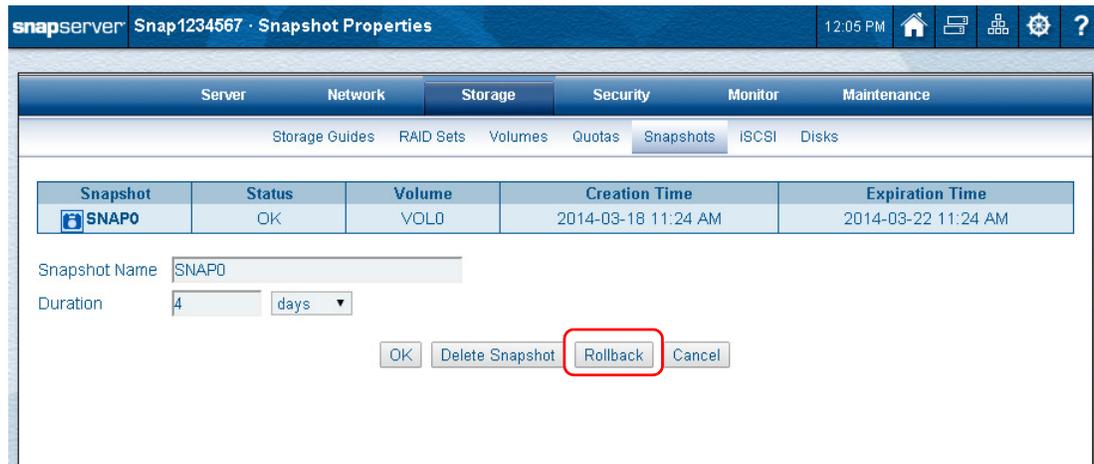
To access the Rollback option, navigate to the **Storage > Snapshots** page.

1 snapshot. Click a snapshot name to modify or delete a snapshot, or to rollback the volume.

Snapshot	Status	Volume	Creation Time	Expiration Time
SNAPO	OK	VOL0	2014-03-18 11:24 AM	2014-03-22 11:24 AM

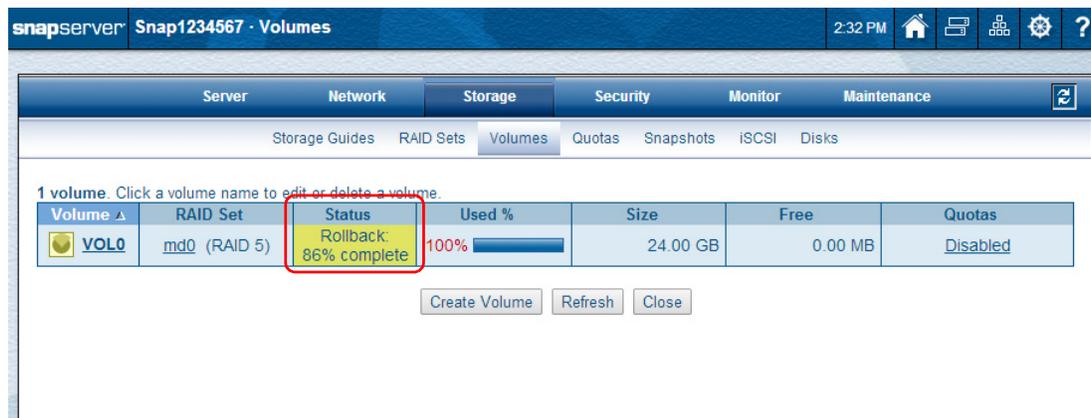
Buttons: Create Snapshot, Snapshot Schedules, Snapshot Space, Refresh, Close

Click the name of the Snapshot you want to use that is shown in the left-most column. At the displayed **Snapshot Properties** page, click the **Rollback** button.



NOTE: If BitTorrent Sync is enabled, it will be disabled and reset to default settings.

At the confirmation page, click the **Rollback** button again. The **Storage > Volumes** page is displayed showing the rollback progress.



IMPORTANT: A rollback can disable Snap EDR and result in its removal. If this occurs, download Snap EDR from the SnapServer website, reinstall it using the OS Update feature, then re-enable and configure it from the SnapExtensions page.

iSCSI Disks

Internet SCSI (iSCSI) is a standard that defines the encapsulation of SCSI packets in Transmission Control Protocol (TCP) and their transmission via IP. On SnapServers, an iSCSI disk is based on an expandable, RAID set-protected volume, but appears to a client machine as a local SCSI drive. This storage virtualization frees the administrator from the physical limitations of direct-attached storage media and allows capacity to be expanded easily as needed. Unlike standard SnapServer volumes, SnapServer iSCSI disks can be formatted by the iSCSI client to accommodate different application requirements.

Connectivity to the iSCSI disk is established using a software package or PCI card, known as an initiator, that must be installed on a client machine. The initiator sees the SnapServer as a “target portal” and an iSCSI disk as a “target.”

To use the SnapServer as an iSCSI target, you need to configure iSCSI on both the client initiating the iSCSI connection, and on the SnapServer. Use the information presented here in conjunction with the documentation supplied with your initiator to install, configure, and connect the iSCSI initiators to the SnapServer.

iSCSI Disk Limitations:

- The size of any iSCSI disk is limited to the size of a single chassis filesystem.
- GuardianOS can maintain up to 256 iSCSI disks.

For Additional Information:

The following resources provide further information you may need to plan and complete your iSCSI implementation.

- **RFC3720: Internet Small Computer System Interface (iSCSI)** – Detailed specification for the iSCSI protocol, available from <http://www.ietf.org>.
- **RFC4171: Internet Storage Name Service (iSNS)** – Detailed specification for the iSNS protocol, available from <http://www.ietf.org>.
- **The Microsoft iSCSI Software Initiator User's Guide** (uguide.doc) – This document is packaged with the initiator download and installs to the default location, usually: C:\Windows\iscsi\uguide.doc. It can also be downloaded from the [Microsoft website](#).
- **The SANSurfer iSCSI HBA CLI Application Users Guide** – This document is available for download on the QLogic website at http://support.qlogic.com/support/drivers_software.asp.
- **The RedHat or Novell (SuSE Linux) websites** – Information on configuring the Linux in-box initiators can be found by searching for *iSCSI* on the RedHat (<http://www.redhat.com>) or Novell (<http://www.novell.com/home/>) websites.
- **The Novell NetWare Administrator's Guide** – This document is available for download on the [Novell website](#).
- **The VMware Server Configuration Guide** – This document is available for download on the [VMware website](#).
- **ReadMe files and Help menus** – For Solaris 10 and operating systems using Open iSCSI (SuSE 10, RedHat 4/5, and CentOS 5), the readme files and help menus provide information on installing and configuring iSCSI.
- **Specifications, Briefs, and White Papers** – The Overland Storage website offers a wide array of informational guides regarding iSCSI and its uses, from product overviews and problem solving for iSCSI, to product specifications and knowledge base articles. For more information about iSCSI and its uses, please browse the Overland Storage website.

Configuring iSCSI Initiators

Overland Storage has qualified a number of software initiators, PCI cards, and drivers to interoperate with SnapScale clusters. Refer to the vendor's documentation to properly install and configure you initiator to connect to the SnapScale iSCSI disks.

iSCSI Configuration on the SnapServer

iSCSI disks are created on the **Storage > iSCSI** page of the Web Management Interface. Before setting up iSCSI disks on your SnapServer, carefully review the following information.



Basic Components of an iSCSI Network

iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances. A basic iSCSI network has two types of devices:

- iSCSI initiators, either software or hardware, resident on hosts (usually servers), that start communications by issuing commands; and
- SCSI Targets, resident on storage devices, that respond to the initiators' requests for data.

The interaction between the initiator and target mandates a server-client model where the initiator and the target communicate with each other using the SCSI command and data set encapsulated over TCP/IP. Overland Storage is one of the first to embed iSCSI target support in its SnapServers.

Isolate iSCSI Disks from Other Resources for Backup Purposes

It is important to isolate iSCSI disks from other resources on the SnapServer for two reasons:

- The filesystem of an iSCSI disk differs fundamentally from the SnapServer native filesystem.
- iSCSI disks are managed from client software rather than the SnapServer Web Management Interface.

For ease of management and particularly for data integrity and backup purposes, either dedicate the entire SnapServer to iSCSI disks, or if the server is to be used with other shared resources, place the iSCSI disk and the other shared resources on separate volumes.

- **Back up an iSCSI Disk from the Client, not the SnapServer** – An iSCSI disk is not accessible from a share and thus cannot be backed up from the SnapServer. The disk can, however, be backed up from the client machine from which the iSCSI disk is managed.

NOTE: While some third-party, agent-based backup packages could *technically* back up an iSCSI disk on the SnapServer, the result would be inconsistent or corrupted backup data if any clients are connected during the operation. Only the client can maintain the filesystem embedded on the iSCSI disk in the consistent state that is required for data integrity.

- **Do Not Use the GuardianOS Snapshots Feature on a Volume or Storage Pool Containing an iSCSI Disk** – Running a GuardianOS snapshot on a volume or storage pool containing an iSCSI disk will abruptly disconnect any clients attempting to write to the server's iSCSI disk, and the resulting snapshot may contain inconsistent data. Supported Windows servers can create a native snapshot of a SnapServer iSCSI disk using VSS (see [Configuring VSS/VDS for iSCSI Disks](#) on page 125 for more information).

iSCSI Multi-Initiator Support

Check the **Support Multiple Initiators** box to allow two or more initiators to simultaneously access a single iSCSI target. Multiple initiator support is designed for use with applications or environments in which clients coordinate with one another to properly write and store data on the target disk. Data corruption becomes possible when multiple initiators write to the same disk in an uncontrolled fashion.

NOTE: RAINcloudOS supports Windows 2003 and Windows 2008 Server failover clustering.

When the box for **Support Multiple Initiators** is checked, a warning message appears:

```
Uncontrolled simultaneous access of multiple initiators to the same
iSCSI target can result in data corruption. Only enable Multi-
Initiator Support if your environment or application supports it.
```

It functions as a reminder that data corruption is possible if this option is used when creating an iSCSI disk.

Write Cache Options with iSCSI Disks

NOTE: This section refers only to iSCSI disks. For information about configuring write cache on GuardianOS volumes on a Traditional RAID configuration, see [Volume Properties in Chapter 5](#).

To ensure the fastest possible write performance, SnapServers can buffer up to 1GB of data to efficiently handle data being transmitted to a SnapServer. This widely accepted method of improving performance is not without some risk. For example, if the SnapServer were to suddenly lose power, data still in cache would be lost.

This risk can be minimized by following industry-standard security precautions, such as keeping servers in a secured location and connecting power supplies to the mains using a network- or USB-based UPS. In most environments, taking these simple precautions virtually eliminates the risk of serious data loss from sudden and unexpected power outages.

Of course, the physical conditions and company policies that guide IT decisions vary widely. Power outages are a common occurrence in some areas, and data protection procedures vary from company to company. Administrators who determine that the risk of data loss, even with security cautions in place, outweighs the significant increase in write performance that write cache provides, can disable this feature for individual iSCSI disks.

When working with write cache for iSCSI disks, note the following:

- Write cache can be disabled on an iSCSI-disk-by-iSCSI-disk basis. Disabling write cache for an iSCSI disk does *not* disable write cache for any other iSCSI disk or any other resources on the SnapServer.
- The write cache for an iSCSI disk can be enabled/disabled any time using the Web Management Interface. However, to change it no active sessions can be connected to the iSCSI disk.

- Disabling write cache for an iSCSI disk does not eliminate *all* potential risk of data loss due to an unexpected loss of power as each disk drive contains its own internal cache of 8 MB or more.

Disconnect iSCSI Disk Initiators before Shutting Down the Server

Shutting down the server while a client initiator is connected to an iSCSI disk appears to the client initiator software as a disk failure and may result in data loss or corruption. Make sure any initiators connected to iSCSI disks are disconnected before shutting down the server.

Ignore Volume is Full Message

When an iSCSI disk is created, the volume or storage pool allocates the specified capacity to the disk. If all volume or storage pool capacity is allocated to the iSCSI disk and email notification is enabled, the SnapServer may generate a **Volume is Full** message. This message indicates only that the volume capacity is fully allocated to the iSCSI disk and is not available to other resources. To determine the status of iSCSI disk storage utilization, use the tools provided on the client machine.

iSCSI Disk Naming Conventions

iSCSI disks are assigned formal IQN names. These appear as the iSCSI device names that the user chooses (or types) when connecting from a client initiator to the SnapServer target, and also on the iSCSI disk details page.

The format of IQN names for GuardianOS iSCSI disks on the SnapServer is:

```
iqn.1997-10.com.SnapServer:[servername]:[diskname]
```

where **[servername]** is the name of the SnapServer, and **[diskname]** is the name of the iSCSI disk on the target SnapServer. For example:

```
iqn.1997-10.com.SnapServer:snap123456:iscsi0
```

NOTE: Users with iSCSI disks created in earlier GuardianOS versions will see a shortened IQN name in the following format:

```
iqn.[servername].[iscsidiskname]
```

The format of IQN names for VSS-based iSCSI disks on the SnapServer is:

```
iqn.1997-10.com.SnapServer:[servername]:[diskname].[nnn]
```

where **[servername]** is the name of the SnapServer, **[diskname]** is the name of the iSCSI disk on the target SnapServer, and **[nnn]** is a sequential number starting from 000. For example:

```
iqn.1997-10.com.SnapServer:snap123456:iscsi0.000
```

The format of IQN names for VDS-based iSCSI disks on the SnapServer is:

```
iqn.1997-10.com.SnapServer:[servername]:[diskname]-snap[n]
```

where **[servername]** is the name of the SnapServer, **[diskname]** is the name of the iSCSI disk on the target SnapServer, and **[n]** is a sequential number starting from 0. For example:

```
iqn.1997-10.com.SnapServer:snap123456:iscsi0-snap0
```

Create iSCSI Disks

Navigate to **Storage > iSCSI** and click **Create iSCSI Disk** to create, edit, or delete iSCSI disks on the SnapServer. Be sure to read [iSCSI Configuration on the SnapServer](#) on [page 119](#) before you begin creating iSCSI disks.

NOTE: You cannot delete or edit an iSCSI disk until all clients have been disconnected from that disk.

The creation process involves first defining iSCSI parameters, then setting up security, and finally confirming your settings.

Step 1: Define the iSCSI parameters.

In the top half of the **Create iSCSI Disk** page, configure the new disk:

Setting Label	Description of Options
iSCSI Disk Name	Accept the default name or enter a new one. Use up to 20 alphanumeric, lowercase characters.
Storage Pool/Volume	Select the pool or volume on which to create the iSCSI disk. For Traditional RAID, if your configuration includes multiple volumes, select a volume to host the iSCSI disk. The page refreshes, displaying the capacity of the selected volume and restoring all fields to default values.
Size	Accept the default size of the space remaining on the selected pool or volume, or enter a smaller size. NOTE: If you plan on creating VSS snapshots of the iSCSI disk, be sure to reserve some of the volume space for the iSCSI snapshot. The required Snap volume space for VSS snapshots is 10% of the size of the iSCSI disk per snapshot.

Setting Label	Description of Options
Enable Write Cache	<p>Selected by default, the write cache option significantly enhances performance. However, if a sudden, unexpected power outage occurs, some data may be lost. For more information on how to treat this option, see Write Cache Options with iSCSI Disks on page 120.</p> <p>NOTE: Disabling a write cache for an iSCSI disk does <i>not</i> disable the write cache for any other iSCSI disk or any other resources on the SnapServer. No active sessions can be connected to the iSCSI disk when enabling or disabling the write cache.</p>
Support Multiple Initiators	<p>Check this box if you want your iSCSI disk to allow multiple initiator connections.</p> <p>NOTE: Data corruption is possible if this option is checked. See iSCSI Multi-Initiator Support on page 120 for more information.</p>

Step 2: If desired, enable CHAP authentication.

In the bottom half of the page, check the **Enable CHAP Logon** box to display the hidden options. Enter a user name and target secret (password) twice. Both are case-sensitive.

- The user name range is 1 to 223 alphanumeric characters.
- The target secret must be a minimum of 12 and a maximum of 16 characters.

Step 3: Confirm your settings.

Click the **Create iSCSI Disk** button. At the confirmation page, verify the settings and click the **Create iSCSI Disk** button again. You are returned to the primary iSCSI page and the new iSCSI disk is displayed in the table there with the following information:

Label	Description
iSCSI Disk	The name of the iSCSI disk.
Storage Pool/Volume	The pool or volume on which the iSCSI disk was created.
Status	<p>Current condition of the iSCSI disk:</p> <ul style="list-style-type: none"> • OK – The iSCSI disk is online and accessible. • Not Mounted – The iSCSI disk is offline.
Active Clients	The number of current sessions.
Authentication	Either CHAP or none.
Size	The size of the iSCSI disk.

Edit an iSCSI Disk

NOTE: You cannot edit an iSCSI disk if an initiator is connected. The hostname and IQN name of all connected initiators are displayed in the table.

After disconnecting all client initiators, click the iSCSI disk name in the table on the **iSCSI** main page to display the **iSCSI Disk Properties** page.

The screenshot shows the 'iSCSI Disk Properties' page for a SnapServer. The page title is 'Snap7654321 - iSCSI Disk Properties'. The navigation tabs include Server, Network, Storage, Security, Monitor, and Maintenance. Under the Storage tab, there are sub-tabs for Storage Pools, Volumes, Snapshots, iSCSI, and Disks. A table lists the iSCSI disk properties:

iSCSI Disk	Storage Pool	Status	Active Clients	iSCSI Disk EUI	Device	Size
iscsi0	Head Unit Storage	OK	0	00c0b61b2d000001	/hd/vol_mnt0/iscsi0	77.00 GB

Below the table, the iSCSI Disk IQN is shown as 'iqn.1997-10.com.snapserver.snap7654321:iscsi0'. The iSCSI Disk Size is set to 77 GB (Max. size is 85.58 GB). There are three checkboxes: 'Enable Write Cache' (unchecked), 'Support Multiple Initiators' (unchecked), and 'Enable CHAP Logon' (checked). A warning message states: 'Warning: Uncontrolled simultaneous access of multiple initiators to the same iSCSI target can result in data corruption. Only enable multi-initiator support if your environment or application supports it.' The CHAP Logon section has fields for 'User Name', 'Target Secret' (with a note '(Minimum 12 characters)'), and 'Confirm Target Secret'. At the bottom, there are buttons for 'OK', 'Delete iSCSI Disk', 'Refresh', and 'Cancel'.

On this page, you can:

- Increase (but not decrease) the size of the iSCSI disk (if space remains).
- Enable or disable the write cache.
- Enable or disable support for multiple initiators.
- Enable or disable the CHAP logon.

Click **OK** to accept the changes (or **Close** to cancel).

CAUTION: The consistency of the internal filesystem on the iSCSI disk is primarily the responsibility of the file and operating systems on the iSCSI client used to format and manage the disk. Growing an iSCSI disk is handled differently by different operating systems and may lead to unexpected results on some client types.

Delete an iSCSI Disk

NOTE: You cannot delete an iSCSI disk if an initiator is connected. The hostname and IQN name of all connected initiators are displayed in the table.

After disconnecting all client initiators, click the iSCSI disk name in the table on the primary **iSCSI** page to display the **iSCSI Disk Properties** page. Click **Delete iSCSI Disk** (which is followed by a confirmation page) to delete the iSCSI disk.

Configuring VSS/VDS for iSCSI Disks

GuardianOS 7.5 provides VSS and VDS hardware providers for support of Microsoft Volume Shadow Copy Services (VSS) and Virtual Disk Service (VDS) for iSCSI disks.

- The VSS hardware provider provides a mechanism for taking application-consistent native snapshots of iSCSI disks without performing full application (or system) shutdown. A snapshot of an iSCSI disk can be automatically created by a backup job run by a VSS-compatible backup application, so that the job backs up the snapshot volume rather than the main production volume.

NOTE: VSS iSCSI snapshots are managed by the Windows client and represent the iSCSI disk, not the Snap volume on which the iSCSI disk resides. They are not related to GuardianOS snapshots as described in [Snapshots on page 109](#). The VSS iSCSI snapshot rollback feature is not currently supported.

- The VDS hardware provider allows administrators to natively manage SnapServer iSCSI disks, using any VDS-compliant management console application.

SnapServers support VSS and VDS on the following platforms:

Platform	VSS	VDS
Windows Server 2003	X	-
Windows Server 2003 R2	X	X
Windows Vista	-	X
Windows Server 2008 R2	X	X

Backing up an iSCSI Disk using VSS Snapshots. Windows VSS-compatible backup applications can create snapshots of SnapServer iSCSI disks to perform consistent backups of application data without stopping the application, using the snapshot instead of the live volume as the backup source.

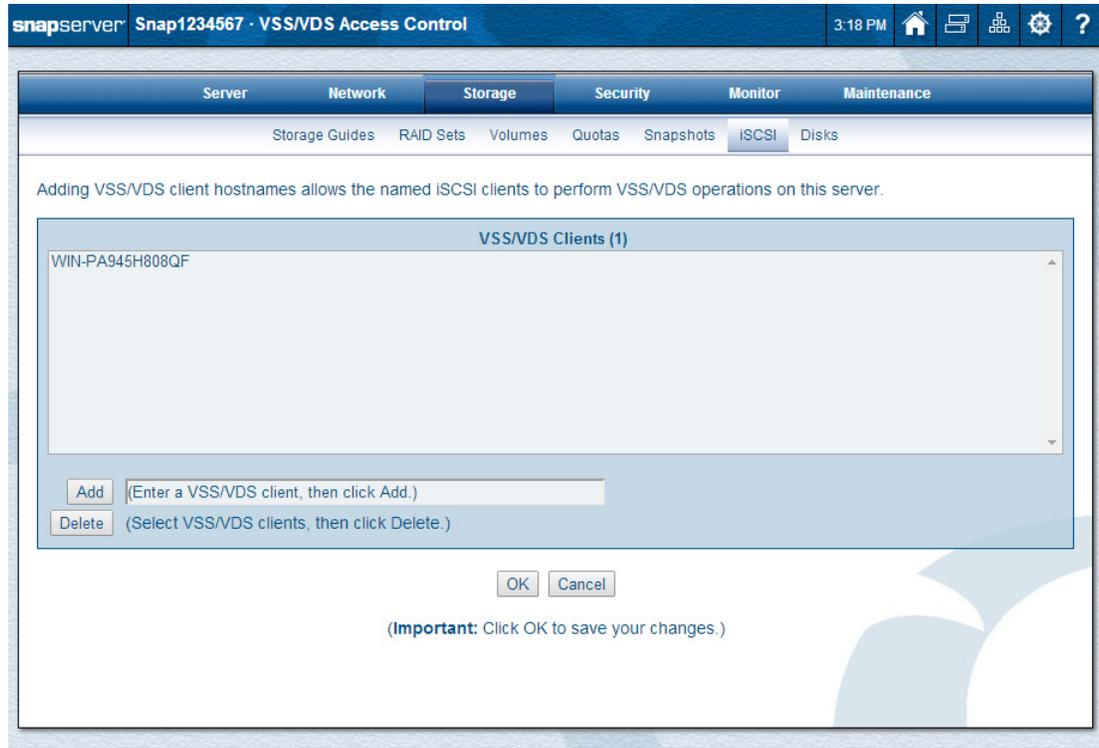
NOTE: To use Symantec Backup Exec as your VSS-compatible backup application, you must first modify the registry of the Backup Exec server and agents.

Each VSS snapshot of an iSCSI target requires additional space on the pool or volume on which the iSCSI disk resides. The required space is 10% of the size of the iSCSI disk per snapshot. If this amount of free space is not available on the pool or volume, the VSS snapshot will not be created and an error will be reported by the SnapServer VSS hardware provider to the Windows event log.

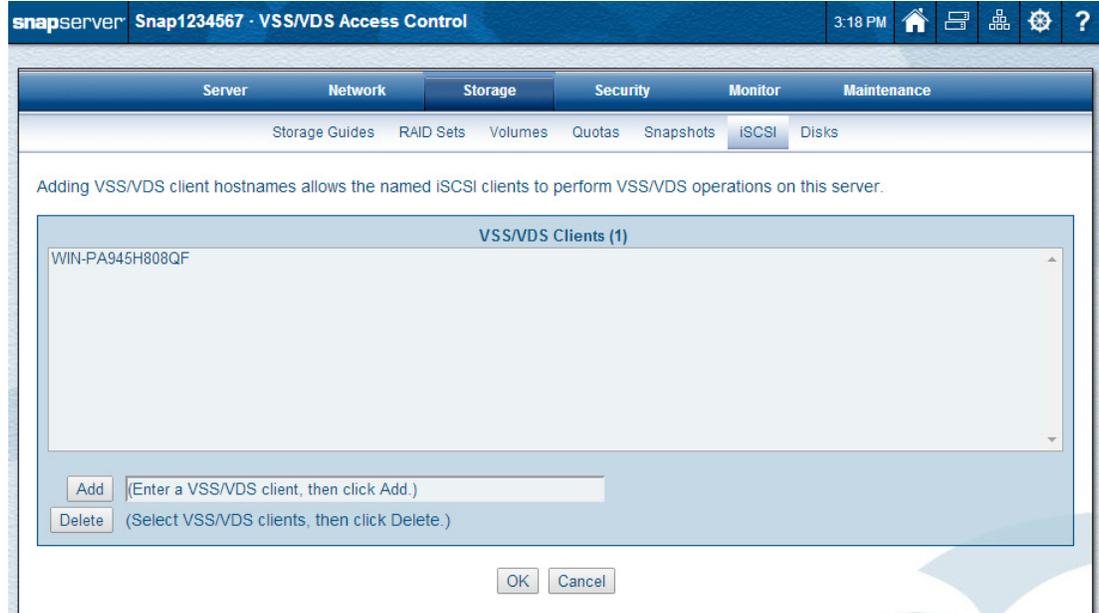
When creating iSCSI disks for later VSS snapshot use, be sure to leave at least 10% of the size of the iSCSI target free on the SnapServer volume.

NOTE: VSS snapshots can only be taken of Windows volumes that fully consume the iSCSI disk. Snapshots of iSCSI disks that contain multiple Windows volumes are not supported.

1. Add the **VSS client** to the SnapServer.
 - a. From the **Storage > iSCSI** page, click the **VSS/VDS Access** button.



- b. Enter a VSS/VDS client and then click **Add**.



- c. Add the **hostname** of the VSS client you wish to grant access and click **Add** (the hostname is not case-sensitive).

The client hostname should appear in the VSS/VDS Clients box.

NOTE: Use the short hostname (*myclientname*) of the client only. Do not use the IP address or fully-qualified name (for example, *myclientname.mydomain.com*).

- d. When you have finished adding VSS clients, click **OK**.

2. Install the **VSS hardware** provider on the Windows iSCSI client.
 - a. Depending on the Windows client, locate *SnapServerToolInstall32.exe* or *SnapServerToolInstall64.exe* on the Overland website:
<http://docs.overlandstorage.com/snapserver>
 - b. Double-click the **executable** (.exe) to run the Installation Wizard on the VSS client and select the VSS/VDS hardware providers option. This will add the SnapServer hardware provider to the Windows iSCSI client.
3. Configure VSS-based **backups** of the iSCSI disk.
 - a. Connect the client **iSCSI initiator** to the Snap iSCSI disk and create a volume (if necessary). Add data or configure applications to use the iSCSI volume for the data repository.
 - b. Configure a VSS-based **backup** of the iSCSI disk. Where applicable, choose to use the SnapServer VSS hardware provider in the backup job configuration. When the backup job is run, the snapshot of the iSCSI disk is automatically created and hosted by the SnapServer as a virtual iSCSI disk (named after the main iSCSI disk with *snap[n]* appended), and the backup application performs the backup using the snapshot iSCSI disk. The snapshot will be deleted after the backup completes.

NOTE: VSS snapshots are not supported on SnapServer iSCSI disks that have been configured into multiple Windows volumes.

Creating and Managing iSCSI LUNs Using VDS

1. Create the **volume** and **RAID set** for the iSCSI disk on the SnapServer using the Web Management Interface (**Storage > Volumes**).

The volume and RAID set must be created on the SnapServer before the iSCSI disk can be created using a VDS application such as Microsoft's *Storage Manager for SANs*.
2. Add **VDS clients** to the SnapServer.
 - a. From the Storage > iSCSI page, click the **VSS/VDS Access** button.
 - b. Click **Add**.
 - c. Add the hostname of the VDS client you wish to grant access and click **Add** (the hostname is not case-sensitive). The client hostname should appear in the VSS/VDS Clients list.

NOTE: Use the short hostname (*myclientname*) of the client only. Do not use the IP address or fully-qualified name (for example, *myclientname.mydomain.com*).
 - d. When you have finished adding VDS clients, click **OK**.
3. Install the **VDS hardware provider** on the Windows client.
 - a. Depending on the Windows client, locate *SnapServerToolInstall32.exe* or *SnapServerToolInstall64.exe* on the Overland website:
<http://docs.overlandstorage.com/snapserver>
 - b. Run the **Installation Wizard** on a VDS client and select the VSS/VDS hardware providers option. This will add the SnapServer hardware provider to the Windows client.
4. Create and configure the **iSCSI disk** using *Storage Manager for SANs* (or other VDS-compliant application).

NOTE: RAID set terminology differs somewhat between GuardianOS and *Storage Manager for SANs*. The following table shows the equivalents:

GuardianOS RAID Set Level	Storage Manager for SANs Equivalent
0	Stripe
1	Mirror
5/6	Stripe with Parity
10	Stripe Mirror

RAID set types listed in *Storage Manager for SANs* when creating an iSCSI disk reflect the types of RAID sets already configured on the SnapServer. Once a RAID set type is selected, the SnapServer automatically chooses a SnapServer RAID set of the selected type and volume to create the iSCSI disk on.

Deleting VSS/VDS Client Access

1. From the **Storage > iSCSI** page, click the **VSS/VDS Access** button.
2. Select the **VSS/VDS client** you want to delete from the VSS/VDS Clients list, and click **Delete**.
3. Click **Yes** to confirm the deletion, then click **OK**.

Disks

The Disks page is a graphic representation of the RAID set or storage pool configuration and disk status on your server. The legend on the **Storage > Disks** page explains the meaning of each disk icon.

The screenshot shows the SnapServer interface for server Snap7654321. The 'Storage' tab is active, and the 'Disks' sub-tab is selected. The page displays a 'Head Unit (VirtualSnap, 200 GB)' with four 50 GB SAS disks. A legend is highlighted with a red box, showing icons for Disk OK, Disk Unused, Disk Too Small, Disk is Foreign, Disk Size Incompatible, Disk Failure, and Empty Slot (No Disk). Below the legend are 'Refresh' and 'Close' buttons, and the text 'DynamicRAID' is displayed in red.

The screenshot shows the SnapServer interface for server Snap1234567. The 'Storage' tab is active, and the 'Disks' sub-tab is selected. The page displays a 'Head Unit (VirtualSnap, 200 GB)' with four 50 GB SAS disks, labeled as md0, md0, md0, and md0. A legend is highlighted with a red box, showing icons for Disk OK, Disk is Foreign, Disk Failure, Empty Slot (No Disk), Local Spare, Global Spare (GS), RAID level, Global Spare, and Unassigned. Below the legend are 'Refresh' and 'Close' buttons, and the text 'Traditional RAID' is displayed in red.

- Click a disk icon (such as ) to view disk details.
- Click a unit's LED icon () to flash the unit's status and drive status LEDs for identification. The LEDs flash amber. Click the LED stop icon () to stop the flashing.

NOTE: The LEDs will continue to flash for five minutes unless stopped. To stop flashing LEDs for all units, click either the master LED stop icon () or link located below the legend.

- Hover the mouse over a RAID set name of one of the drives to display the RAID level next to all the disks within the RAID set (Traditional RAID only).
- Click a RAID set name to view or edit the RAID set (Traditional RAID only).

If expansion arrays are attached to your server, they will also be displayed on this page.

The screenshot shows the SnapServer Administration Console interface. The top navigation bar includes 'Server', 'Network', 'Storage', 'Security', 'Monitor', and 'Maintenance'. The 'Storage' section is active, showing sub-tabs for 'Storage Guides', 'RAID Sets', 'Volumes', 'Quotas', 'Snapshots', 'iSCSI', and 'Disks'. The main content area displays a list of RAID sets and expansion units. Each RAID set is shown with its name, capacity, and a grid of disks with their respective RAID levels and statuses. A legend at the bottom explains the icons used for disk status and RAID levels.

Legend:

- Disk OK
- Disk is Foreign
- Disk Failure
- Empty Slot (No Disk)
- Local Spare
- Global Spare (GS)
- 1, 3, 5, 10** RAID level
- +** Global Spare
- ⚡** Unassigned (---)

[Click here](#) to stop flashing LEDs on all units.

NOTE: If GuardianOS detects an expansion unit that is not integrated with the SnapServer, a message displays across the top of the administration pages with a link to information about the orphaned expansion unit. Also, the orphaned expansion unit will be highlighted on the page.

Replacing Disk Drives

Should a disk drive fail, usually it can be replaced without shutting down the SnapServer appliance (hot-swapped).

A failed disk drive can be removed and replaced anytime if two or more disks are installed in the SnapServer. However, only one disk at a time can be replaced. While dual parity allows two disks to be swapped out simultaneously, they will only be incorporated one at a time.

The following procedures assume that you are installing a new, Overland-approved disk drive as a replacement for a failed drive.

NOTE: Failed drives cannot be added back in to a RAID set.

DynamicRAID Mode

If a disk drive fails in DynamicRAID mode, the Administration page displays a Disk Failure message and an icon with a link to the Disks page. Both the **Storage Pools** and **Storage Pool Properties** pages show the degraded status. If single parity mode is being used, no parity protection message is shown. In dual parity mode, just a degraded status is shown.

NOTE: If a working disk is removed, the same changes occur as when a disk fails.

Once a disk is removed, a new disk can be inserted into any empty slot and DynamicRAID will recognize it as a replacement. The system still shows the storage as degraded but a new message appears on both the **Storage Pools** and **Storage Pool Properties** pages saying **New Disks Detected (click to repair)**. At the same time, **Storage Pool Disks** and **Disks** pages show **OK - New/Unused Disk** in that slot. To add the disk, click the repair link.

NOTE: Disk drives that have been previously configured can be added; they are indicated in the **Storage > Disks** list by the  icon and a message stating that the disk has previously been used in a different system. If you want to use the drive, add it to the RAID as you would any other drive.

If there are no errors, after the new disk is incorporated any LEDs are turned off and statuses are updated.

Traditional RAID Mode

If a disk drive fails in Traditional RAID mode, the Administration page displays a **Disk Failure** message and an icon with a link to the **Disks** page. This section describes how to remove and replace drives in a RAID set of a SnapServer configured in Traditional RAID mode.

When removing a working disk drive, note the following:

- **RAID 0 (nonredundant) set** – Removing a disk drive from a RAID 0 set causes the RAID set to fail. This action renders any data residing on its drives inaccessible and is not recommended. If a RAID 0 disk drive is inadvertently removed, reinserting it should restore file access.
- **RAID 1, 5, 6, or 10 (redundant) set** – Removing a disk drive from a RAID 1, 5, 6, or 10 set places the RAID set into degraded mode. While operating in degraded mode, users can access or even update data. However, the array loses its redundant characteristics until all drives of the array are available and operating properly (except for RAID 6 set, which can tolerate a two-drive failure before it loses redundancy).

NOTE: If you configure a RAID 1, 5, 6, or 10 set with a spare, the array automatically starts rebuilding with the spare when one of the disk drives fails or is removed.

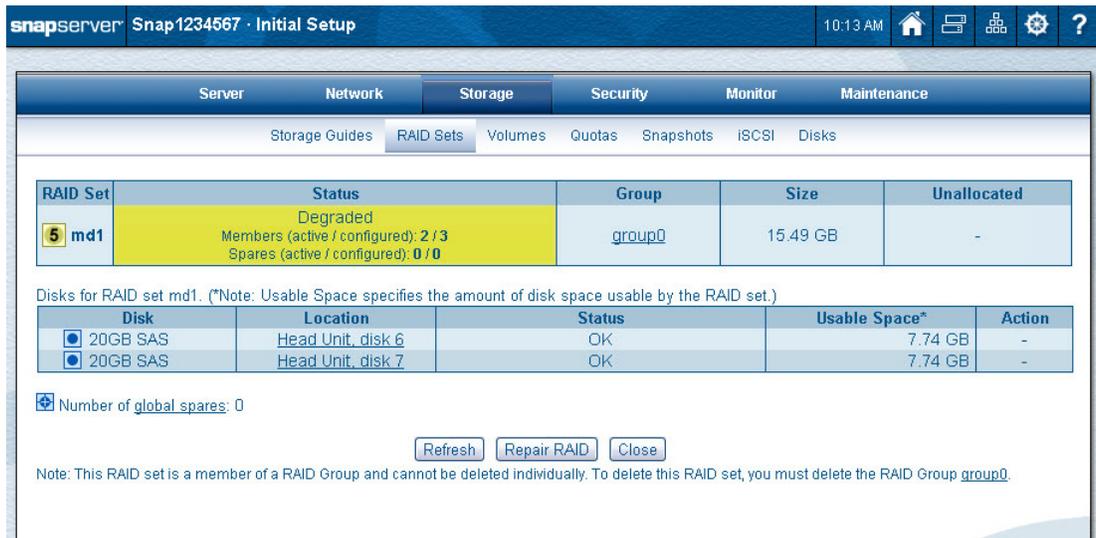
If a disk drive fails, the Traditional RAID Administration page changes to show the Disk storage as Degraded and provides a link to the **RAID Sets** page. Both the **RAID Sets** and **RAID Set Properties** pages show the degraded status.

NOTE: If a working disk is removed, the same changes occur as when a disk fails.

After a fresh drive is inserted, if auto-incorporation is not enabled, you must use the Web Management Interface to add it to a RAID set:

1. Go to **Storage > RAID Sets** and click the **name** of the RAID set with the new drive.
2. Click **Repair RAID**.

3. Select a drive from the list shown, and click **Repair RAID** again to incorporate it into the RAID as a replacement for a failed member drive.



NOTE: The **Repair RAID** button only appears when a drive has failed or been removed, and the RAID is in degraded mode.

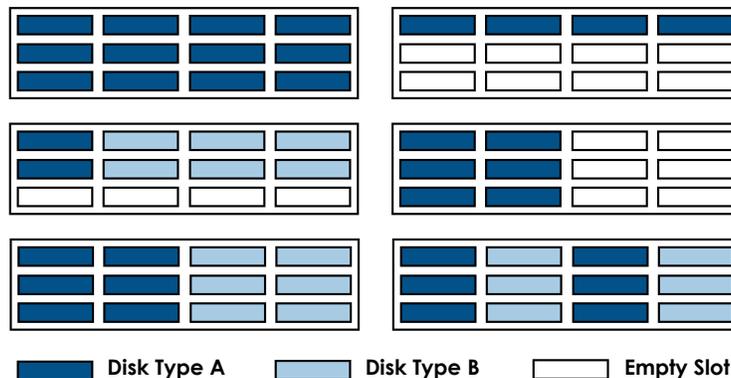
The RAID set status changes to **Resyncing** while the new drive is incorporated into the RAID set. It reads **OK** once the incorporation is complete.

Adding Disk Drives

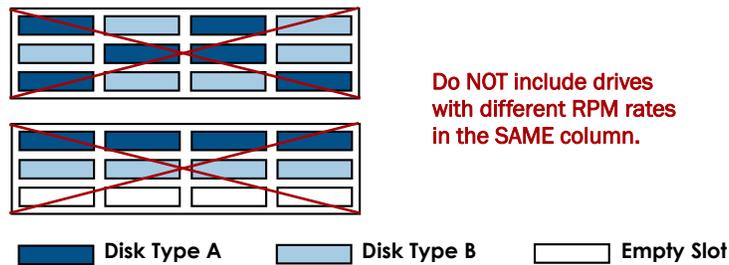
If empty slots are available, you can add an Overland-approved disk drive to expand the storage pool/volume on your SnapServer or SnapExpansion unit.

Drives of different rotational speed (for example, SAS and SATA drives) can be combined in the same server. However, they cannot be combined in the same column, and it is recommended that columns of same-type drives be grouped together. If you are combining drives with different rotational speeds, use the figures below to plan where to place the disk drives.

Recommended Disk Drive Configurations.



Unsupported Disk Drive Combinations.



DynamicRAID Mode

When adding additional disk drives, keep the following in mind:

- While disk sizes within a Storage Pool can vary, the type of disks used must be the same (such as, SAS 7200 RPM or SAS 15K RPM).
- If a non-compatible disk of a different partition size is added to a Storage Pool, it is indicated in the **Storage > Disks** list by the  icon.
- If only a single disk is in a Storage Pool, the second disk added must be of equal or greater size.
- A move from dual parity to single parity is allowed at any time, provided the storage pool is healthy. A move from single parity to dual parity is only allowed when a new disk drive is added that is large enough to support the new parity mode.

To add a new disk drive to a DynamicRAID:

1. Insert the **drive** into an empty SnapServer slot.

It appears in the **Storage > Disks** map as “Disk Unused” (for a new disk) or “Disk is Foreign” (reused, clean disk). A “New disk detected” banner is shown.

NOTE: Disk drives that have been previously configured can be added; they are indicated in the **Storage > Disks** list by the  icon (Disk is Foreign) and a message stating that the disk has previously been used in a different system and all data will be deleted. If you want to use the drive, continue to add it to the RAID as you would any other drive.

2. Click the **link** in the banner (or navigate to the **Storage > Storage Pools** page).
3. In the **Status** column, click the link to open the **Storage Pool Properties** page.
4. At the bottom of the properties page, verify or change the **Parity Mode** and **Snapshot Pool** settings.

Pending Changes: (Click OK to review & confirm)		Data Pool Usage (New)	Snapshot Pool Usage (New)
· Incorporate 1 new disk.		<1% (133 MB / 1.46 TB)	0% (0 MB / 374 GB)

The following new disk has been detected.

Disk	Slot	Status
 279GB SAS	9	OK - New / unused disk.

Storage Pool Name

5. Click **OK** to continue.
6. At the confirmation page, click **Save Changes**.

- At the success notice page, click **OK**.

To speed up the storage pool synchronization, it is recommended that you exit the Web Management Interface.



Traditional RAID Mode

This section describes how to safely add drives to an existing RAID 1, 5, 6, or 10 set. On SnapServers, after a fresh drive is inserted into a drive bay, if auto-incorporate is not enabled (see [Automatic Incorporation of Hot-Swapped Drives](#) in [Chapter 5](#)), you must use the Web Management Interface (**Storage > RAID Sets**) to add it to a RAID set.

- RAID 0 set (nonredundant)** – You cannot add a drive to a RAID 0 set. To reconfigure a RAID 0 set, you must delete the RAID set and then recreate it.
- RAID 1 set (redundant)** – You can add a new drive to a RAID 1 set as either a spare or as a new member. Adding a disk drive to a RAID 1 set does not add storage capacity. The new member simply creates an additional copy of the original drive.
- RAID 5, 6, or 10 set (redundant)** – You can add an new drive as a spare to a RAID 5, 6, or 10 set. However, you cannot add a new drive as a new member.

To add a new disk drive as a **Local Spare** for a Traditional RAID set:

- Insert the **drive** into an empty SnapServer slot.

It appears in the **Storage > Disks** map as “Disk Unused” (for a new disk) or “Disk is Foreign” (reused, clean disk).

NOTE: Disk drives that have been previously configured as part of a RAID can be added. They are indicated in the **Storage > Disks** list by the  icon and a message stating that the disk has previously been used in a different system (foreign). If you want to use the drive, add it to the RAID as you would any other drive.

- Navigate to the **Storage > RAID Sets** page.
- Click the **name** of the RAID set to which you want to add a drive.
- On the RAID set page that opens, click **Add Disk**.
If you are adding to a RAID 1 set, select either **Spare** or **Member** at the top of the page.
- From the Available Disks list, select one or more **drives** to add to the configuration, and then click **Next**.
- On the confirmation page, click **Add Disk**.
The disk is added as a Local Spare to the selected RAID set.

To add a new disk drive as a **Global Spare** for a Traditional RAID set:

1. Insert the **drive** into an empty SnapServer slot.

It appears in the **Storage > Disks** map as “Disk Unused” (for a new disk) or “Disk is Foreign” (reused, clean disk).

NOTE: Disk drives that have been previously configured as part of a RAID can be added. They are indicated in the **Storage > Disks** list by the  icon and a message stating that the disk has previously been used in a different system (foreign). If you want to use the drive, add it to the RAID as you would any other drive.

2. Navigate to the **Storage > RAID Sets** page.
3. Click **Global Spares**.
4. From the Available Disks list, select one or more **drives** to add to as Global Spares, and then click **OK**.

The disk is added as a Global Spare.

To remove the drive as a Global Spare, use the same process but uncheck the box in the **Available Disks** list.

Reintegrate Orphaned Disk Drives

An orphaned disk drive can occur in either of the following circumstances:

- A working drive from a RAID set is accidentally removed from the server
- The RAID set or system is started with a drive missing.

In either case, the drive becomes suspect and is considered an orphan. To remedy the problem, click the RAID set name on the **Storage > RAID Sets** page, and then click the **Repair** link next to the drive in question.

Managing Expansion Unit Storage

The **Storage > Disks** page displays the head unit and any expansion units attached to the head unit. For more information about the **Disks** page, see [Disks](#) on page 129.

Move the mouse over a RAID Set name to highlight its disks. Click a disk icon to view disk details. Click to flash (for approx. 5 minutes) a unit's LEDs for identification. (Click to stop flashing LEDs.)

Head Unit (DX2, 4.55 TB)			
1 md0 931.51 GB SATA	2 md0 1.82 TB SATA	3 md0 931.51 GB SATA	4 md0 931.51 GB SATA
5 --- (No Disk)	6 --- (No Disk)	7 --- (No Disk)	8 --- (No Disk)
9 --- (No Disk)	10 --- (No Disk)	11 --- (No Disk)	12 --- (No Disk)

Expansion Unit 1 (SE DX, 2.18 TB)			
1 md1 558.91 GB SAS	2 md1 558.91 GB SAS	3 md1 558.91 GB SAS	4 md1 558.91 GB SAS
5 --- (No Disk)	6 --- (No Disk)	7 --- (No Disk)	8 --- (No Disk)
9 --- (No Disk)	10 --- (No Disk)	11 --- (No Disk)	12 --- (No Disk)

Expansion Unit 2 (SE DX, 2.18 TB)			
1 md2 558.91 GB SAS	2 md2 558.91 GB SAS	3 md2 558.91 GB SAS	4 md2 558.91 GB SAS
5 --- (No Disk)	6 --- (No Disk)	7 --- (No Disk)	8 --- (No Disk)
9 --- (No Disk)	10 --- (No Disk)	11 --- (No Disk)	12 --- (No Disk)

Expansion Unit 3 (SE DX, 2.18 TB)			
1 md2 558.91 GB SAS	2 md2 558.91 GB SAS	3 md2 558.91 GB SAS	4 md2 558.91 GB SAS
5 --- (No Disk)	6 --- (No Disk)	7 --- (No Disk)	8 --- (No Disk)
9 --- (No Disk)	10 --- (No Disk)	11 --- (No Disk)	12 --- (No Disk)

Legend: Disk OK Disk is Foreign Disk Failure Empty Slot (No Disk) Local Spare Global Spare (GS)
 RAID level Global Spare Unassigned (---)

[Click here to stop flashing LEDs on all units.](#)

Refresh Close

The disk drives of expansion units are completely integrated into the head unit's logic. Their access is determined by the type of RAID system being used.

DynamicRAID

Each unit in the SnapServer system has its own storage pool which DynamicRAID manages.

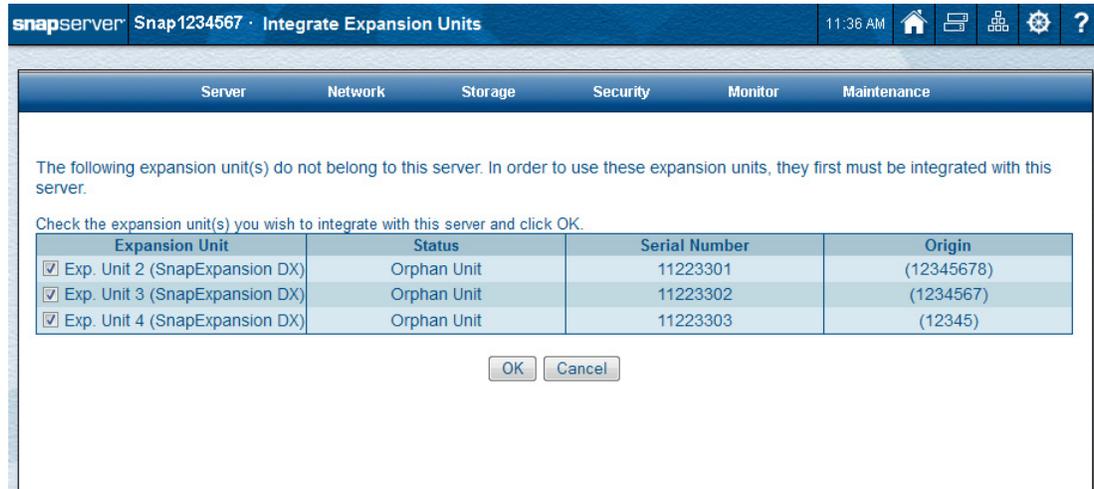
Traditional RAID

The head unit and expansion disk drives can be combined as necessary. For example, to create one large RAID set, you could delete the existing RAID sets on both the head unit and the expansion unit, then combine all drives into one high-capacity storage system.

This configuration of one large RAID reduces administrative complexity and overhead, but the failure of any one unit in the system (due to a cable coming loose, for example) will render the entire RAID set inaccessible. This configuration also increases the potential for multiple drive failures in a single RAID set.

Integrating Orphaned Expansion Units

Expansion units that have been discovered by GuardianOS (for example, are newly connected to the SnapServer) but have not been integrated with the SnapServer are listed on the Orphan Expansion Units Table accessed by the message link in the banner at the top of the administration pages.



The information shown is covered in the following table:

Property	Description
Expansion Unit	A description of the unit
Status	The status of the unit (for example, Orphan Unit)
Serial Number	The expansion unit's serial number
Origin	The serial number of the server with which the expansion unit was last incorporated

If you want to use the expansion unit with the SnapServer, check the box next to the orphaned expansion unit you want to integrate, and click **OK**.

 **CAUTION:** Before integrating an orphaned expansion unit, be sure that it is compatible with the SnapServer. For example, the expansion is unconfigured or configured for the same RAID mode (Traditional RAID or DynamicRAID) as the SnapServer itself.

This section covers Security options for users, groups, shares, and file access.

Topics in Security Options

- [Overview](#)
- [Security Guides](#)
- [Shares](#)
- [Local Users](#)
- [Local Groups](#)
- [Security Models](#)
- [ID Mapping](#)
- [Home Directories](#)

Overview

The Security options control access to the SnapServer and its data.



SnapServer authentication validates a user’s identity by requiring the user to provide a registered login name (User ID) and corresponding password. The server ships with predefined local users and groups that allow administrative (admin) and guest user access to the server via all protocols.

Administrators may choose to join the SnapServer to a Windows Active Directory domain, and CIFS/SMB and AFP clients can then authenticate to the server using their domain credentials. To accommodate NFS clients, the SnapServer can also join an LDAP or NIS domain, and the SnapServer can look up user IDs (UIDs) and group IDs (GIDs) maintained by the domain for configuration of quotas and ID mapping. For authentication control beyond the guest account, Mac and FTP client login credentials can be created locally on the server. See [User and Group ID Assignments](#) on page 140.

SnapServer default security configuration provides one share to the entire volume. All network protocols for the share are enabled, and all users are granted read-write permission to the share via the guest account. By default, the `guest` user is disabled in SMB but enabled for HTTP, AFP, and FTP.

Network clients can initially access the server using the guest account, but if you require a higher degree of control over individual access to the filesystem for these clients, you must create local accounts (or use Windows Active Directory security for CIFS/SMB and AFP clients).

Local users or groups are created using the **Security > Local Users** and **Security > Local Groups** pages in the Web Management Interface. Local users are also used for administrative access to the server through the server's Web Management Interface, SnapServer Manager, or SSH.

A local user or group is one that is defined locally on the SnapServer using the Web Management Interface. The default users and groups listed below cannot be modified or deleted.

- **admin** – The local user admin account is used to log into the Web Management Interface. The default password for the admin account is also *admin*.
- **guest** – The local user guest account requires no password.
- **admingrp** – The Admin group account includes the default admin user account. Any local user accounts created with admin rights are also automatically added to this group.

Guidelines for Local Authentication

These password authentication guidelines are for both users and groups.

Duplicating Client Login Credentials for Local Users and Groups. To simplify user access for Windows Workgroup or Mac clients, duplicate their local client log on credentials on the SnapServer by creating local accounts on the SnapServer that match those used to log on to client workstations. This strategy allows users to bypass the login procedure when accessing the SnapServer.



CAUTION: This strategy applies only to local users. Do not use duplicate domain user credentials if joined to an Active Directory domain.

Default Local Users and Groups . Default users *admin* and *guest* appear in the list of users on the **Local Users** page, and the default group *admingrp* appears in the list of groups on the **Local Groups** page. However, they cannot be deleted or modified (although the admin password can be changed).

Changing Local UIDs or GIDs. The SnapServer automatically assigns and manages UIDs and GIDs. Because you may need to assign a specific ID to a local user or group in order to match your existing UID/GID assignments, the SnapServer makes these fields editable.

Password Policies. To provide additional authentication security, set password character requirements, password expiration dates, and lockout rules for local users.

Local users can also be individually exempted from password expiration and character requirement policies. The built-in *admin* user is exempt from all password policies.

Local Account Management Tools. The SnapServer offers the following tools for creating, modifying, and editing local user and group accounts.

Function	Navigation Path
Local User Management	Navigate to the Security > Local Users page, from which you can create, view, edit, and delete local users. You can also set user password policy, including password character requirements, maximum number of allowed log on failures, and password expiration settings.
Local Group Management	Navigate to the Security > Local Groups page, from which you can create, view, edit, and delete local groups.

User and Group ID Assignments

The SnapServer uses the POSIX standard to assign UIDs or GIDs, in which each user and group must have a unique ID. This requirement applies to all users and groups on the SnapServer, including LDAP, NIS, Windows Active Directory, and local users and groups.

If you join the SnapServer to a Windows, LDAP, or NIS domain, IDs are assigned using available IDs only. Consider the following when creating and configuring users and groups:

- UIDs and GIDs from 0 to 100 are unavailable for use. If you try to assign a UID or GID that is less than 101 to a local user, you will get an error message.
- When the server automatically generates UIDs or GIDs for imported Windows domain users or groups, UIDs or GIDs that are already in use by local, LDAP, and NIS users will be skipped.
- When LDAP or NIS domain users and groups are imported, the SnapServer will discard any UIDs that are less than 101 or are in conflict with UIDs already in use by local or Windows domain users and groups.

The `nfsnobody` and `nobody` user IDs (UID 65534 and 65535, respectively) and GIDs are reserved. They are not mappable to other IDs, nor is another ID mappable to `nfsnobody` or `nobody`.

Security Guides

Security Guides are special wizards to guide you through:

- Setting up Windows Active Directory security.
- Giving users or groups share-level access to an entire volume.
- Giving users or groups share-level access to a folder on a volume.



Windows Active Directory Security Guide

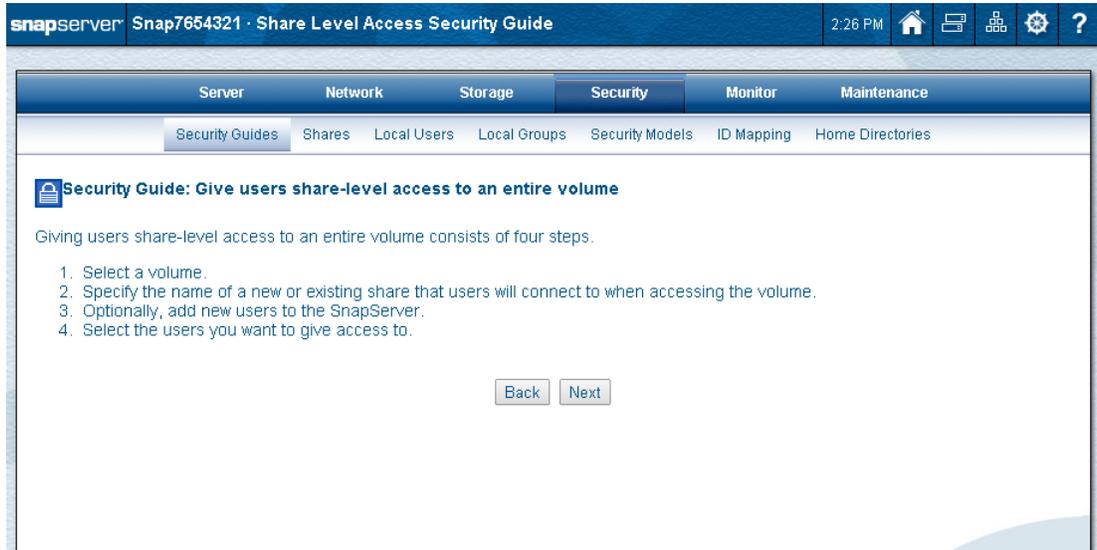
NOTE: This option is only available if NTP is disabled.

This wizard guides you through the setup of Windows Active Directory on your server.



Entire Volume Security Guide

This wizard guides you through the four steps it takes to give share-level access to a folder on a volume.



Folder on Volume Security Guide

This wizard guides you through the five steps it takes to give share-level access to an entire volume.



Shares

SnapServer provides integration with existing Windows Active Directory Domain or Unix LDAP or NIS user and group databases. At the share level, administrators can assign read-write or read-only share access to individual Windows and local users and groups for Windows/SMB, AFP, FTP, and HTTP. Administrators can also edit the NFS exports file to control how shares are exported to NFS client machines.

1 share. Click a share name to modify a share's properties or to delete a share.

Share	Volume	Path	Access	NFS Access	Protocols	Attributes
SHARE1	VOL0	/	Open	Default	SMB-NFS-AFP-HTTP-FTP	-

Attributes: H=Hidden, S=Has Snapshot Share, W=Web Root

Important Security Note: Share access for the NFS protocol is configured independently from share access for all other protocols. [View online help for more information.](#)

[Create Share](#) [Refresh](#) [Close](#)

Share Security Overview

SnapServers support file access in Windows, Unix, and Apple networks, as well as access via FTP and HTTP. New shares are created by default with full read-write access to all users, subject to the filesystem permissions on the share target directory (see [File-level Security in Appendix C](#)).

The first step to securing a SnapServer is to specify access at the individual share level. Administrators can assign read-write or read-only share access to individual Windows (and local) users and groups.

For more details and information about using Shares, see [Security and Access in Appendix C](#).

Create Shares

To create a new share, you need, at a minimum, to specify the share name, volume, and folder path.

The screenshot shows the SnapServer web interface for creating a share. The page title is "SnapServer Snap1234567 · Create Share". The navigation menu includes Server, Network, Storage, Security (selected), Monitor, and Maintenance. The Security menu is expanded to show Security Guides, Shares (selected), Local Users, Local Groups, Security Models, ID Mapping, and Home Directories.

The main content area contains the following fields and options:

- Name:** SHARE2
- Volume:** VOL0
- Path:** / (with a "Browse" button)
- Description:** (optional)
- Security model for path:** Unix
- Create share with full read and write access for all users
- Create share with Admin-only access and proceed to Share Access page
- Advanced Share Properties <<** (highlighted with a red box)
- Hide this share (the share will be hidden from network browsing)
- Select only the protocols that are needed for network users to access this share.
 - Windows (SMB)
 - Linux/Unix (NFS)
 - Apple (AFP)
 - Web (HTTP, HTTPS)
 - FTP, FTPS
- You can create a "snapshot" share that is associated with this new share. The snapshot share allows access (using identical security) to snapshots of the data that the new share references.
 - Create Snapshot Share
 - Hide this share (the snapshot share will be hidden from network browsing)
 - Snapshot Share Name: SHARE2_SNAP
- Buttons: Create Share, Cancel

By clicking the Advanced Share Properties link, additional options are displayed. Use these options to hide the share from network browsing, select the protocols supported, and create a snapshot share associated with this share.

Create a Share

Creating a share involves selecting the volume, security model, and directory path for the share and then defining share attributes and network access protocols.

1. Accept the default **share name** or enter a new one.
To ensure compatibility with all protocols, share names are limited to 27 alphanumeric characters (including spaces).
2. Choose the **volume** from the drop-down list.
3. Select from the following **path options**:
 - **To create a share to the entire volume** – The current Path field defaults to the root path of the volume. Do nothing if this is the desired configuration.

- **To create a share to a folder on the volume** – Browse to the folder you want to which you want to point the share, click the folder name, and click **OK**.

NOTE: If you want to create a new folder inside any other folder, type the folder name into **New Folder Name** and click **Create Folder**.

4. If desired, enter a **description** to clarify the purpose of the share.
5. Choose a **security model** by selecting either **Windows/Unix**, **Windows**, or **Unix** from the drop-down list.

The **security model** option is only available under the following circumstances:

- **Traditional RAID** – When pointing the share at the root of a volume or one directory down from the root of the volume.
- **DynamicRAID** – When pointing the share to the root of a volume.

If available, the option defaults to the current security model at the specified path. If changed to a different security model, the change will propagate to all files and subdirectories underneath. For more information, see [Security Models](#) on [page 162](#).

6. Choose the user-based **share access** option desired for Windows/SMB, AFP, FTP, and HTTP users:
 - **Create share with full read and write access for all users**
 - **Create share with Admin-only access and proceed to Share Access page**

For more information, see [Share Access Behaviors](#) on [page 148](#).

NOTE: If selecting **Create share with Admin-only** access and if the share has NFS enabled, be sure to configure the NFS Access settings afterward.

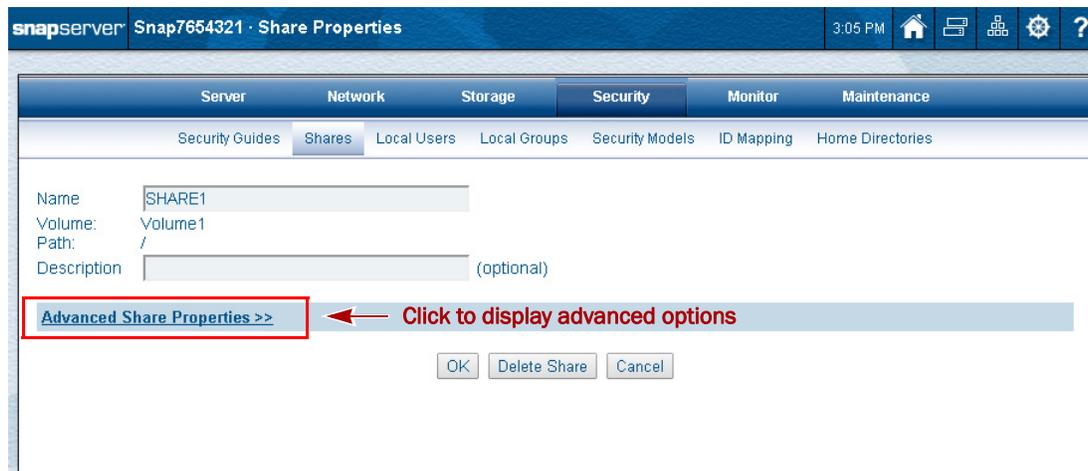
7. To further configure the share, click **Advanced Share Properties**, and enter any of the following:

Option	Description
Hide this Share	Select this option if you want the share to be hidden from network browsing using SMB, HTTP/HTTPS, AFP, and FTP (but not NFS) protocols.
Protocols	Select the access protocols for the share: Windows (SMB) , Linux/Unix (NFS) , Apple (AFP) , Web (HTTP, HTTPS) , and FTP, FTPS . Check all that apply.
Snapshot Share	To create a snapshot share, check the Create Snapshot Share box. Optionally, do either of the following: <ul style="list-style-type: none"> • To hide the snapshot share from the SMB, HTTP, AFP, and FTP protocols, check the Hide Snapshot Share box. • If desired, enter a unique name for the Snapshot Share Name field. Use up to 27 alphanumeric characters (including hyphens and spaces).

8. Click **Create Share** to complete the process.

Edit Share Properties

Once a share has been created, you can change its name, description and the advanced properties. To edit the properties, go to **Security > Shares > *share_name* > Share Properties**.



You cannot change the **Volume** or **Path**. If you need to change the volume, you must delete the share and create a new one on another volume.

Options are shown in this table:

Option	Description
Name	Accept the default share name or enter a new one. If you change the default, observe the following guidelines: <ul style="list-style-type: none"> • Make sure the share name is unique to this server • To ensure compatibility with all protocols, share names are limited to 27 alphanumeric characters (including hyphens and spaces).
Description	If desired, enter a description of the share. This is an opportunity to clarify the purpose of the share.
Hide this share	Select this option if you want the share to be hidden from network browsing.
Protocols	Select the access protocols for the share: Windows (SMB) , Linux/Unix (NFS) , Apple (AFP) , Web (HTTP, HTTPS) , and FTP, FTPS . Check all that apply.
Snapshot Share	The option that displays depends on whether a snapshot share currently exists. <p>To create a snapshot share, check the Create Snapshot Share box.</p> <ul style="list-style-type: none"> • If desired, enter a unique name for the Snapshot Share Name field. Use up to 27 alphanumeric characters (including hyphens and spaces). • To hide the snapshot share from the SMB, HTTP, AFP, and FTP protocols, select the Hide Snapshot Share checkbox. <p>To remove a snapshot share, do the following:</p> <ul style="list-style-type: none"> • Check the Remove Snapshot Share box.

Delete Shares

To delete a share, go to **Security > Shares > Share Properties** (displayed by clicking the share name).

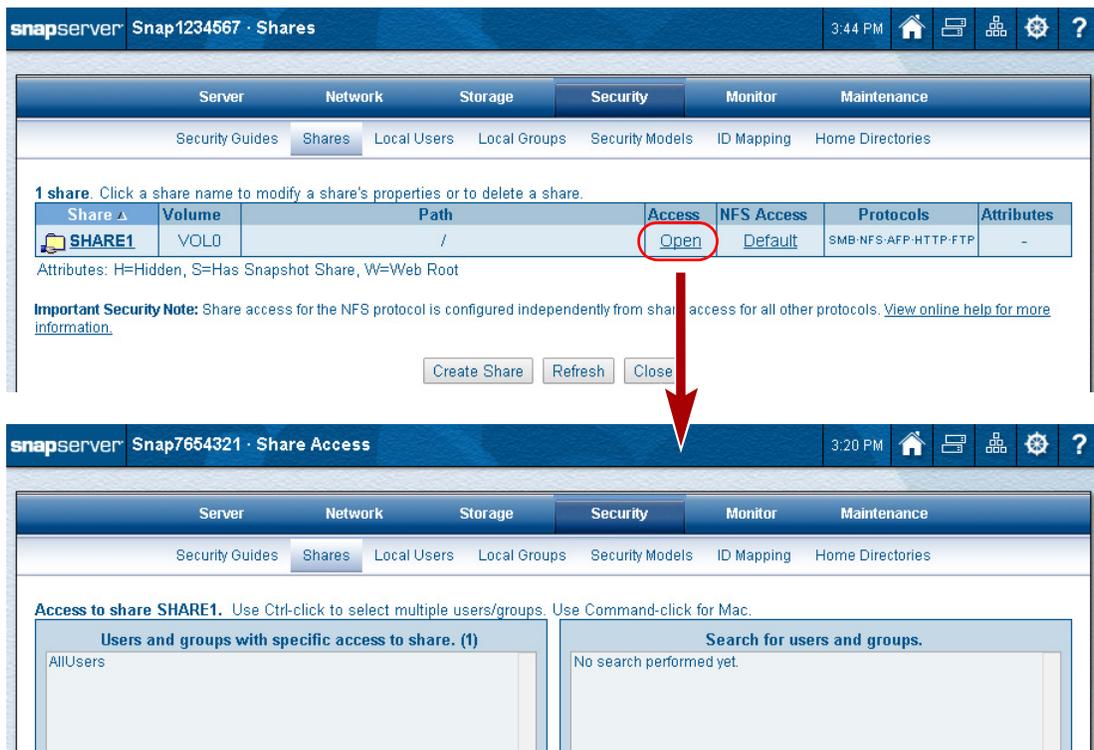
1. Click the **Delete Share** button at the bottom.
2. At the **Delete Share** confirmation page, click the **Delete Share** button again.



Configuring Share Access

In **Security > Shares**, in the **Access** column, click the access link next to the share you want to configure. The **Share Access** page displays. You can set access levels for the share, as well as grant or deny access to specific users and groups.

NOTE: To add a new user to a share, you must first create the user, then add that user to the share. Please see [Local Users](#) on page 153 for information on creating new users.



Share Access Behaviors

Administrators tasked with devising security policies for the SnapServer will find the following share access behaviors informative:

- **Share access defaults to full control** – The default permission granted to users and groups when they are granted access to the share is full control. You may restrict selected users and groups to read-only access.
- **User-based share access permissions are cumulative** – An SMB, AFP, FTP, or HTTP user's effective permissions for a resource are the sum of the permissions that you assign to the individual user account and to all of the groups to which the user belongs in the **Share Access** page. For example, if a user has read-only permission to the share, but is also a member of a group that has been given full-access permission to the share, the user gets full access to the share.
- **NFS access permissions are not cumulative** – An NFS user's access level is based on the permission in the NFS access list that most specifically applies. For example, if a user connects to a share over NFS from IP address 192.168.0.1, and the NFS access for the share gives read-write access to "*" (All NFS clients) and read-only access to 192.168.0.1, the user will get read-only access.
- **Interaction between share-level and file-level access permissions** – When both share-level and file-level permissions apply to a user action, the more restrictive of the two applies (see [File-level Security](#) in [Appendix C](#)). Consider the following examples:
Example A: More restrictive file-level access is given precedence over more permissive share-level access.

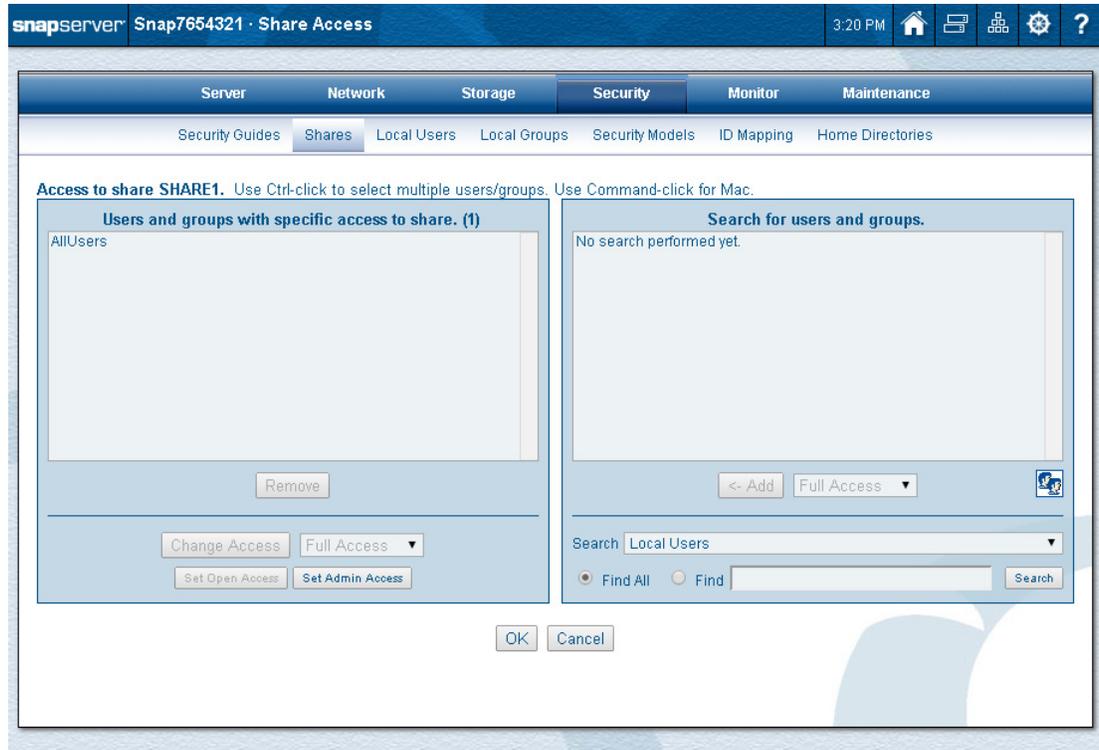
Share Level	File Level	Result
Full control	Read-only to File A	Full control over all directories and files in SHARE1 except where a more restrictive file-level permission applies. The user has read-only access to File A.

Example B: More restrictive share-level access is given precedence over more permissive file-level access.

Share Level	File Level	Result
Read-only	Full control to File B	Read-only access to all directories and files in SHARE1, <i>including</i> where a less restrictive file-level permission applies. The user has read-only access to File B.

Setting User-based Share Access Permissions

Share permissions for Windows, Apple, FTP, and HTTP users are configured from **Security > Shares** by clicking the link in the **Access** column of the share you want to configure. Share permissions for NFS are configured and enforced independently. See [NFS Access for Shares](#) on [page 151](#) for more information.



User-based share access permissions apply to users connecting over SMB, AFP, FTP, or HTTP. Users and groups with assigned share access permissions appear in the list on the left (**Users and groups with specific access to share**). To search for those without assigned access, use the field on the right (**Search for users and groups**).

The default permission granted to users and groups when they are granted access to the share is **Full** access. You may restrict selected users and groups to **Read-only** access.

Share-Level Access Permissions

Full access	Users can read, write, modify, create, or delete files and folders within the share.
Read-only	Users can navigate the share directory structure and view files.

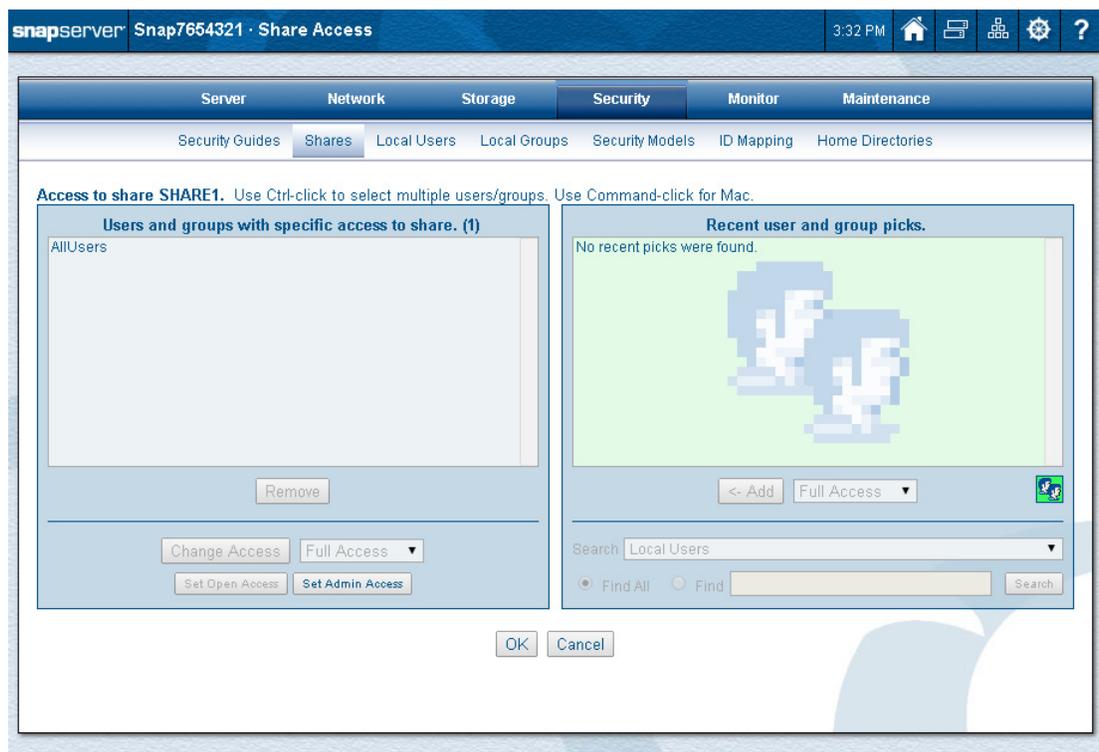
1. Display the **Share Access** page (**Security > Shares > access_link**).
2. To **add** share access permissions for a user or group:
 - a. At the bottom, using the drop-down list, select the **domain** or **local user/group list** to search.

NOTE: For domains that require authentication (showing an “(A)” after the name), after selecting the domain name, enter the User Name and Password for that domain. The user name and password can be for any user in the domain and are used to retrieve basic information (like the user & group lists) from the domain.

- b. Enter the **search string** (or select **Find All**).
When entering a search string:

- Returned results will include all users and groups whose name **begins** with the string entered in the Search field.
 - The search results returned may be limited. Fine tune your search by using a more specific string to return the names desired.
 - On the rare occasion you need to search for a domain that's not listed ("remote domain"), select a domain from the Search drop-down list through which to search, then enter in the Find box the name of the remote domain, followed by a slash (/) or backslash (\) and the user name for which you are searching (for example, `remote_domain\user_name`).
- c. Click **Search** to display any matches.
After you click Search, another authentication prompt may be presented to authenticate with the remote domain.
 - d. Select one or more **names** in the list.
Users that already have access are shown in purple font with a plus sign (+) in front of their name.
 - e. Choose either **Full Access** or **Read Only** from the drop-down list.
 - f. Click **Add**.

NOTE: To display recent user or group picks, click the **faces** (👤) icon. A list with a green background is displayed. Click the now green icon to return to the normal search box.



3. To **remove** share access permissions for a user or group:
 - a. Select one or more **users or groups** in the left box.
 - b. Click **Remove**.

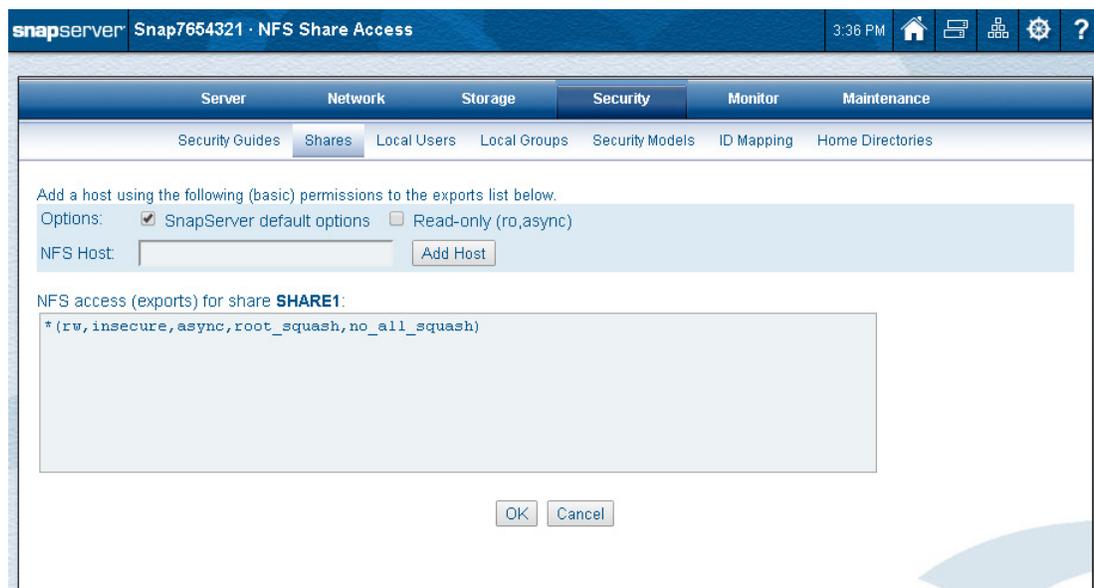
4. To change **access permissions** for a user or group, select one or more users or groups in the left box, then select either **Full Access** or **Read Only** from the drop-down list, and click the **Change Access** button.
5. To quickly specify either Open or Admin-only **access** for the entire share, click either the **Set Open Access** or **Set Admin Access** button.
6. Click **OK** to save share permissions.

NFS Access for Shares

NOTE: Multiple shares pointing to the same target directory must have the same NFS access settings. The Web Management Interface applies the same NFS access for all shares pointing to the same directory.

To configure NFS access, click the link shown in the **NFS Access** column for the share you want to configure. You can configure NFS access to the share using standard Linux “exports” file syntax.

On the **Shares** page, click the name of the access type listed in the NFS Access column to open the **NFS Share Access** page.



The NFS Access text box is a window into the client access entries in GuardianOS’s *exports* file. This file serves as the access control list for filesystems that may be exported to NFS clients. You can use the **Add Host** controls as described below to assist in making entries to the file, or you can directly edit the text box. After all entries are made, click **OK** to return to the **Shares** page.

NOTE: The syntax used in this file is equivalent to standard Linux exports file syntax. If the SnapServer detects any errors in syntax, a warning message appears. You can choose to correct or ignore the error warning.

The Exports File Default Options. The default entry provides read-write access to all NFS clients (including NFSv4, if Kerberos security is not enabled).

```
* (rw, insecure, async, root_squash, no_all_squash)
```

The entry options are explained in the following table:

Entry Code	Meaning
Asterisk	All NFS clients
ro	The directory is shared read only (ro).
rw	The client machine will have read and write (rw) access to the directory.
insecure	Turns off the options that require requests to originate on an Internet port less than IPPORT_RESERVED (1024).
root_squash	Forces users connected as root to interact as the "nobody" user (UID 65534). This is the GuardianOS default.
no_root_squash	no_root_squash means that if root is logged in on your client machine, it will have root privileges over the exported filesystem. By default, any file request made by user root on the client machine is treated as if it is made by user nobody on the server. (Exactly which UID the request is mapped to depends on the UID of user nobody on the server, not the client.) If no_root_squash is selected, then root on the client machine will have the same level of access to the files on the system as root on the server. This can have serious security implications, although it may be necessary if you want to perform any administrative work on the client machine that involves the exported directories. You should not specify this option without a good reason.
async	Tells a client machine that a file write is complete – that is, has been written to stable storage – when NFS has finished handing the write over to the filesystem.
no_all_squash	Allows non-root users to access the nfs export with their own privileges.

Configuring Export Strings for NFSv4 with Kerberos Security. Share access for NFSv4 clients can be enforced either by the traditional NFS host method (described in [The Exports File Default Options](#) on page 151) or via Kerberos.

If Kerberos is enabled, access is applied uniformly to all Kerberos-authenticated NFSv4 clients connected using the matching Kerberos option. Host-based access as described in The SnapServer Exports File Default Options still applies to NFSv2 and v3 clients when Kerberos is enabled, but it does not apply to NFSv4 clients.

When Unix Kerberos security is enabled for NFSv4, the following entries are automatically added to the NFS Access settings for each NFS-enabled share:

```
gss/krb5(rw,insecure,async,root_squash,no_all_squash)
gss/krb5i(rw,insecure,async,root_squash,no_all_squash)
gss/krb5p(rw,insecure,async,root_squash,no_all_squash)
```

These give read-write access to Kerberos-authenticated NFSv4 users connecting via:

- Standard Kerberos (**gss/krb5**)
- Kerberos with data integrity checksumming (**gss/krb5i**)
- Kerberos with protection/encryption (**gss/krb5p**).

These entries can be independently removed, added, and modified on each NFS-enabled share.

Using the Add Host Controls. Follow these steps:

1. Select **one** of the following options:
 - **SnapServer Default Options** – Inserts the default options as described above
 - **Read Only** – Inserts the read only option only
 - **Both** – Inserts default options, but substitutes read only for read/write
2. Do **one** of the following in the NFS host text box:
 - **To apply the options to all NFS hosts** – Leave this field blank
 - **To apply the options to specific hosts** – Enter one or more IP addresses.
3. Click **Add Host**.

Local Users

The **Local Users** page (**Security > Local Users**) provides all the options to manage local users. Local users are users that are known only to the server being accessed. Each server running GuardianOS comes with two predefined users: admin and guest. The admin user has full Administrator rights. Go to **Security > Local Users** to view settings or make changes.

The screenshot shows the SnapServer web interface for managing local users. The top navigation bar includes 'Server', 'Network', 'Storage', 'Security' (selected), 'Monitor', and 'Maintenance'. Below this, a sub-navigation bar lists 'Security Guides', 'Shares', 'Local Users' (selected), 'Local Groups', 'Security Models', 'ID Mapping', and 'Home Directories'. The main content area contains the following text: 'Local users are users that are known only to this server. After you create local users, you can give them access to shares from the Shares page. To modify a user's settings, select the user name and then click the button on the right.' Below this text is a table with two columns: 'Local Users (2)' and 'Actions'. The table lists 'admin (A)' and 'guest'. The 'Actions' column contains buttons for 'Properties', 'Groups', and 'Delete'. A legend at the bottom left of the table states '(A=User has Admin rights, D=User login is disabled.)'. At the bottom of the interface are buttons for 'Create User', 'Password Policy', and 'Close'.

Local Users (2)	Actions
admin (A)	Properties: Modify a user's properties (name, password, admin rights). Groups: Specify which local groups a user belongs to. Delete: Delete a user.
guest	

(A=User has Admin rights, D=User login is disabled.)

Create User Password Policy Close

Create a User

Click the **Create** button to create a new user on this server. Enter the user data, select any special options, and click the **Create User** button again.

The screenshot shows the 'Create Local User' page in the SnapServer web interface. The page title is 'SnapServer Snap7654321 - Create Local User'. The navigation menu includes Server, Network, Storage, Security (selected), Monitor, and Maintenance. The sub-menu includes Security Guides, Shares, Local Users (selected), Local Groups, Security Models, ID Mapping, and Home Directories. The main content area contains the following form:

To create a new user, specify a name, password and user ID (UID).

Name:

Full Name: (optional)

Password:

Confirm Password:

User ID (UID):

Disable user login

Grant admin rights to this user (A local user with admin rights will be able to access this Web Management Interface.)

Create a Local User

1. On the **Local Users** page, click **Create**.
2. On the **Create Local User** page that opens, enter the requested **information**:

Option	Description
Name	Use up to 31 alphanumeric characters and the underscore.
Full Name	Use up to 49 alphanumeric characters (includes spaces). Input in this field is optional.
Password	Passwords are case-sensitive. Use up to 15 alphanumeric characters without spaces.
Password Verify	Type the chosen password again for verification.
User ID (UID)	Displays the user identification number assigned to this user. Alter as necessary. For information on available UID ranges, see User and Group ID Assignments on page 140 .
Disable User Login	Select this checkbox to disable the user login. The user's information will remain in the system, but login rights are denied. The user login can be re-enabled by clearing the checkbox. This box can also be used to enable a user locked out by the <i>Disable login after n attempts</i> password policy.
Exempt from Password Expiration and Character Requirements	This checkbox is only visible if Password Policy is enabled. Select this checkbox to exempt this user from password expiration and character requirement policies.
Grant Admin Rights To This User	Select this checkbox to allow the user access to the Web Management Interface and SSH (for access to the CLI and backup agent installation).

3. Click **Create User** again to create the user account.

Edit User Properties

Highlight a user and click the **Properties** button to open the **Local User Properties** page to make changes to the user's full name, password, or user ID (UID). Note that the UID cannot be changed for the built-in admin user.

The screenshot shows the 'Local User Properties' page for a user named 'Fred'. The page has a navigation bar with tabs for Server, Network, Storage, Security, Monitor, and Maintenance. Under the Security tab, there are sub-tabs for Security Guides, Shares, Local Users, Local Groups, Security Models, ID Mapping, and Home Directories. The 'Local Users' sub-tab is active. The form contains the following fields and options:

- Name: Fred
- Full Name: Fredrick Sandstone (optional)
- Password: (blank)
- Confirm Password: (blank)
- User ID (UID): 18001
- Disable user login
- Exempt this user from password expiration and character requirements. (highlighted with a red box and arrow, with text 'Only shown if Password Policy enabled')
- Grant admin rights to this user. (A local user with admin rights will be able to access this Web Management Interface.)

At the bottom of the form are 'OK' and 'Cancel' buttons.

To Edit Local User Properties

1. On the **Security > Local Users** page, select the **user** you want to edit, and click **Properties**.
2. On the **Local User Properties** page that opens, enter or change the following **information**:

NOTE: The name cannot be changed. If a user must be renamed, delete and re-create the user with the same UID.

Option	Description
Full Name	Use up to 49 alphanumeric characters (includes spaces). Input in this field is optional.
Password	Passwords are case-sensitive. Use up to 15 alphanumeric characters. Leave this field blank to keep the existing password.
Password Verify	Type the chosen password again for verification. Leave this field blank to keep the existing password.
User ID (UID)	Displays the user identification number assigned to this user. Alter as necessary. For information on available UID ranges, see User and Group ID Assignments on page 140 . NOTE: Changing a user's UID may alter filesystem access permissions that apply to that UID. In addition, any existing permissions for a UID previously assigned to a user that are changed to a different UID may become active if another user is created with the same UID. Carefully consider security configuration on existing files and directories before changing the UID of a user.

Option	Description
Disable User Login	Select this checkbox to disable the user login. The user's information will remain in the system, but login rights will be denied. The user login can be re-enabled by deselecting the checkbox. This checkbox can also be used to enable a user locked out by the <i>Disable login after n attempts</i> password policy.
Exempt from Password Expiration and Character Requirements	NOTE: This option is only visible if Password Policy is enabled. Select this checkbox to exempt this user from password expiration and character requirement policies.
Grant Admin Rights To This User	Select this checkbox to allow the user access to the Web Management Interface and SSH (for access to the CLI and backup agent installation).

3. Click **OK**.

User Password Policies

NOTE: Local users can be individually exempted from password expiration and character requirements. This may be necessary for some special users, such as users configured to perform backups. See [Create a Local User on page 154](#) for procedures to set password policy for local users. Also, the built-in *admin* user is automatically exempt from all password policies.

Click the **Password Policy** button to make changes to all the local user password settings.

snapserver Snap7654321 - Local Users Password Policy 8:58 AM

Server Network Storage **Security** Monitor Maintenance

Security Guides Shares **Local Users** Local Groups Security Models ID Mapping Home Directories

Specify the password policy for all local users. (Note: The built-in *admin* user is exempt from all password policies.)

Enable Password Policy

Character requirements: None

Minimum number of characters: 4

Disable login after: attempts.

Re-enable a disabled login after: minutes.

Expire password after: days.

OK Cancel

Set Password Policy for Local Users

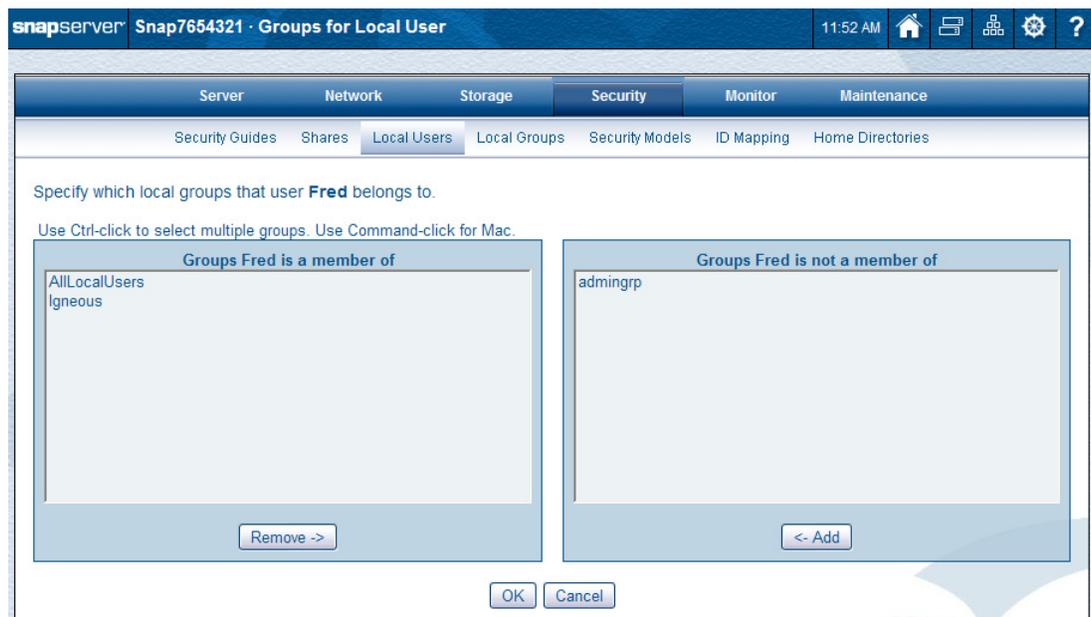
1. On the **Security > Local Users** page, click the **Password Policy** button.
2. On the **Local Users Password Policy** page, check the **Enable Password Policy** box.
3. Enter the following **information**:

Option	Description
Character Requirements	Select the alpha/numeric/special character requirements for the password from the drop-down list.
Minimum Number of Characters	Check the checkbox to enable the policy, then enter the minimum number of characters required for the password.
Disable Login After <i>n</i> Attempts	Check the checkbox to enable the policy, then enter the number of times a user can fail to login before the system locks the user out. NOTE: To unlock a user, clear the Disable User Login checkbox for the user in the Local Users page.
Re-enable a Disabled Login After <i>n</i> Minutes	If you have defined a limit to the number of times a user can fail to log in, you can also check this checkbox and enter a time period after which the system will allow the user to log in again. NOTE: This will save the administrator from having to manually re-enable the user.
Expire Password After <i>n</i> Days	Check the checkbox to enable the policy, then enter the number of days before the password must be changed. NOTE: Local users with expired passwords can change their passwords at: <a href="http://<servername>/changepassword">http://<servername>/changepassword .

4. Click **OK** to save the settings.

Assign User to a Group

Use the **Groups for Local Users** page (**Security > Local Users > Groups**) to make changes to a local group membership.



Add or Remove Users from Groups

1. On the **Groups for Local User** page, select a **user**.
2. Click **Groups**.
The group settings for the selected user are shown.
3. To make a **change**:
 - To add the user to a group, from the group list on the right, select a **group name** and click **<-Add**.
 - To delete the user from a group, from the group list on the left, select the **group name** and click **Remove->**.
4. Click **OK** to save your changes.

Delete Local User

On the **Local Users** page, click the **Delete** button to remove a user.

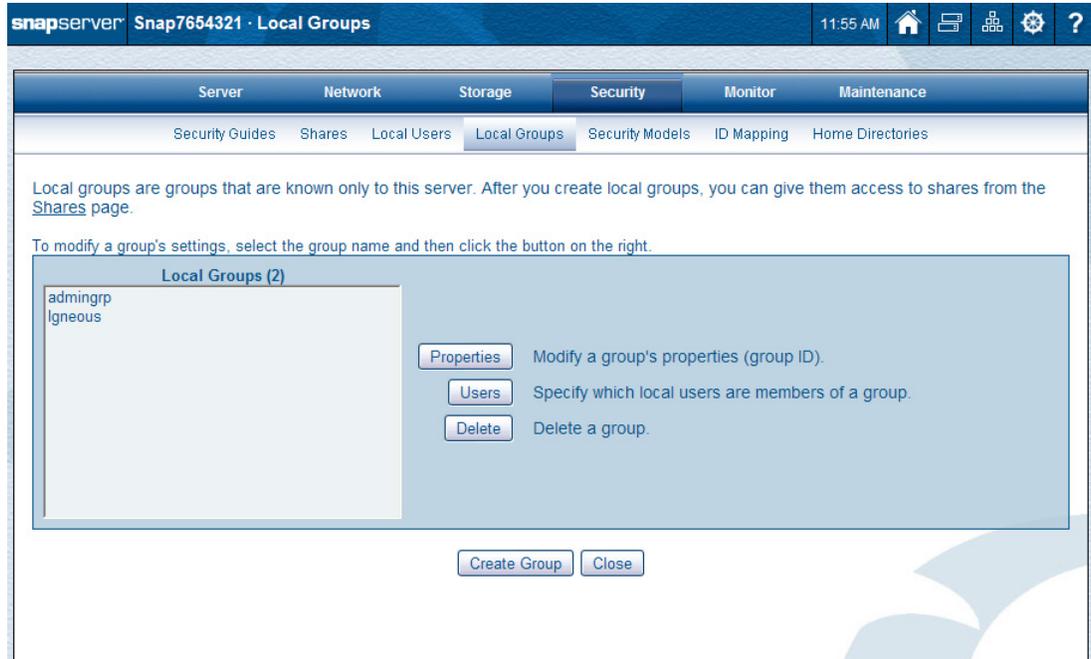


Delete a Local User

1. On the **Security > Local Users** page, select the **user** to be deleted.
2. Click the **Delete User** button.
3. The confirmation page will display. Click **Delete User** to delete the selected user (or click **Cancel**).

Local Groups

The **Local Groups** page (**Security > Local Groups**) provides all the options to manage local groups. Local groups are groups of local users that are known only to the server being accessed. Each server running GuardianOS comes with one predefined group: **admingrp**.



Create New Group

Click the **Create** button to open the **Create Local Group** page to configure a new group on this server.



Create a New Local Group

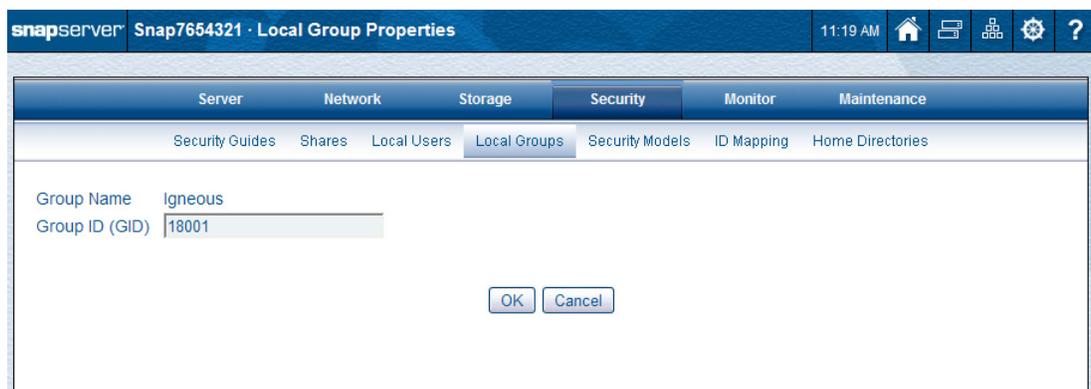
1. On the **Security > Local Groups** page, click **Create**.
2. On the **Create Local Group** page that opens, enter the following information:

Option	Description
Group Name	Use up to 31 alphanumeric characters and the underscore.
Group ID (GID)	Displays the user identification number assigned to this user. Alter as necessary. For information on available UID ranges, see User and Group ID Assignments on page 140 .

3. Click **Create Group** when finished. The **Users for Local Group** page is displayed, allowing you to add other users to your new local group.
4. Click **Close** to save your changes.

Edit Group Properties

Use the **Properties** button to open the **Local Group Properties** page to make changes to the options there.



Edit Local Group Properties

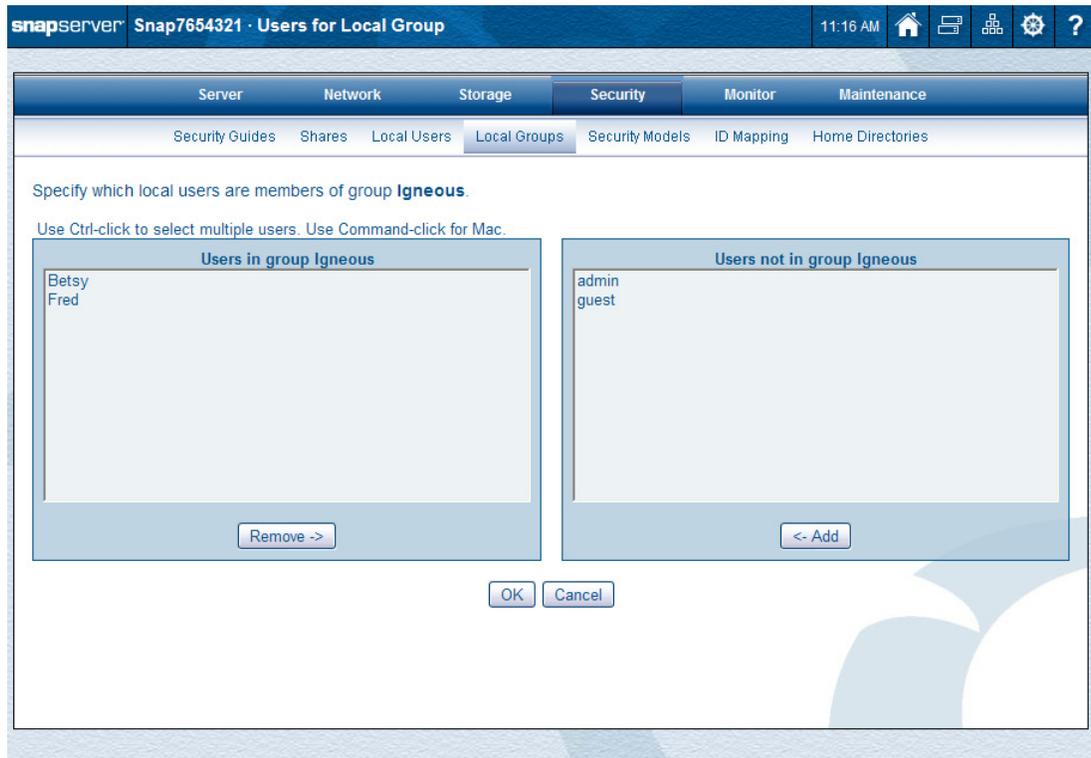
1. On the **Security > Local Groups** page, select the **group** you want to edit, and click **Properties**.
2. On the page that opens, you can only change the **GID**.
For information on available UID ranges, see [User and Group ID Assignments](#) on [page 140](#).

NOTE: Changing a group's GID may alter filesystem access permissions that apply to that GID. In addition, any existing permissions for a GID previously assigned to a group that are changed to a different GID may become active if another group is created with the same GID. Carefully consider security configuration on existing files and directories before changing the GID of a group.

3. Click **OK**.

Specify Users in Group

Click the **Users** button on the **Local Groups** page to make changes to a local group membership.



Add or Remove Users in a Group

1. On the **Security > Local Groups** page, select the **group** you want to edit, and click **Users**.

NOTE: This same **Users for Local Group** page is also shown after creating a new group (**Create Group**) so you can add users immediately.

2. To make a **change**:
 - To add the user to a group, from the group list on the right, select a **user name** and click **<-Add**.
 - To delete the user from a group, from the group list on the left, select the **user name** and click **Remove->**.
3. Click **OK** to save your changes.

Delete Group

On the **Local Groups** page, click the **Delete** button to remove a group.

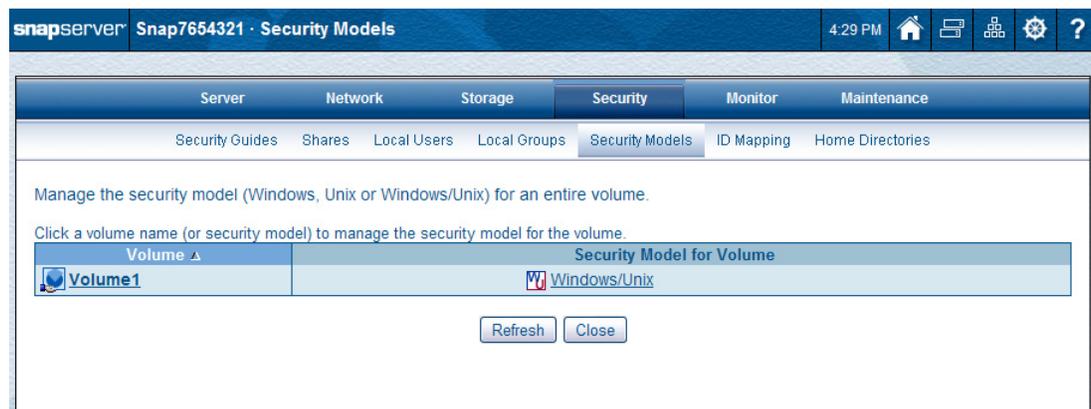


Delete a Group

1. On the **Local Groups** page, select the **group** to be deleted, and click **Delete**. The delete confirmation page is displayed.
2. Click **Delete Group** to delete the selected group (or **Cancel** to cancel the deletion).

Security Models

The **Security Models** page (**Security > Security Models**) provides all the options to manage the types of file-level security that can be set on files and directories.



There are three file-level security models that can be used by a SnapServer: **Windows/Unix**, **Windows**, and **Unix**. In Traditional RAID, the security model can be configured on volumes and the folders created in the root of the volumes. In DynamicRAID, the security model only can be configured on the volumes.

The security model determines the rules regarding which security personality is present on files and folders created by the various protocols and clients, and whether the personality of files and folders can be changed by changing permissions.

Folders created in a volume default to the security model of that volume. The folder's security model may differ from the personality of the folders (for example, folders with a Windows/Unix security may have a Unix personality).

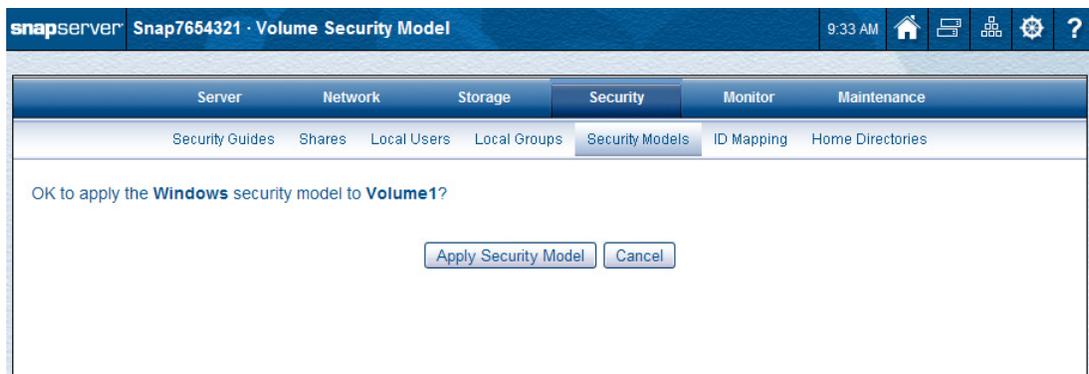
For more information about Security Models, see [Security and Access](#) in [Appendix C](#).

Managing Volume Security Models

1. Select **Security > Security Models**.
2. Click the **security model name**.
The **Volume Security Model** page opens.



3. From the drop-down list, select the **security model type** desired, and click **OK**.
4. At the confirmation message, click **Apply Security Model**.



If there are files and directories under the volume, you are prompted whether you want to recursively apply the change. This resets permissions on all files and directories to make them accessible by all users, and configured for the Windows personality (Windows and Windows/UNIX security models) or UNIX personality (UNIX security model). When done, the main page displays a conversion status.

Managing Folder Security Models in Traditional RAID

NOTE: This is only available with Traditional RAID.

1. Select **Security > Security Models**.

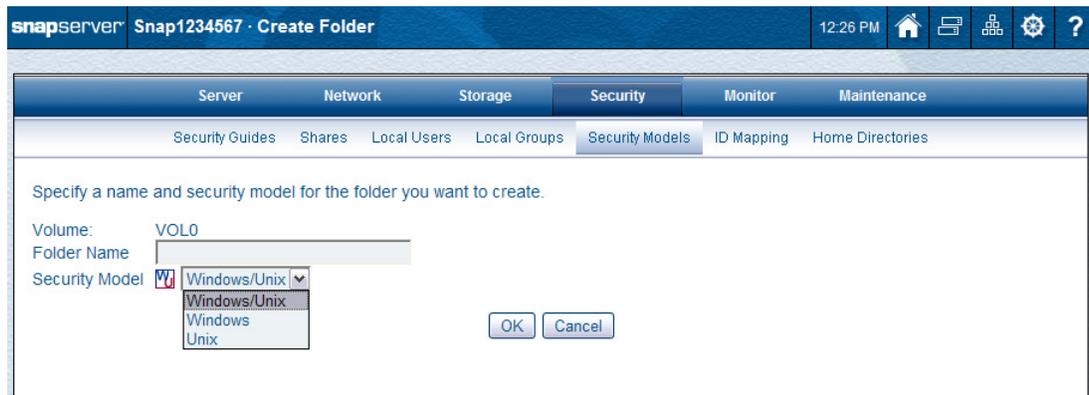
2. Click the **volume name**.



3. At the **Security Models** folder page, do one of the following:

- **Create a new folder** with a specific security model:

Click **Create Folder**, enter the **folder name**, select the **security model type** from the drop-down list, and click **OK**.



- **Change the security model** of a folder:

Click the security model **icon** (**W/U**, **W**, or **U**) of the folder, select the **security model type** from the drop-down list, and click **OK**. At the confirmation message, click **Apply Security Model**.

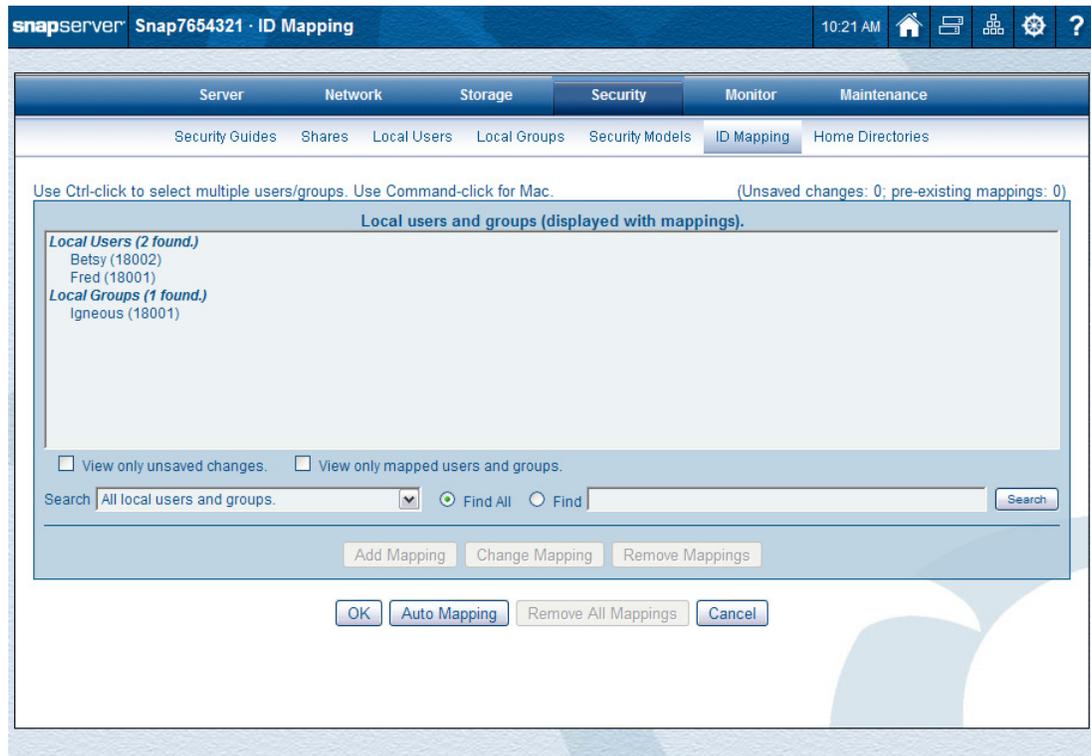


NOTE: If there are files and directories under the volume, you are prompted whether you want to recursively apply the change.

4. At the results page, click **Close**.

ID Mapping

ID mapping allows users and groups that exist on Windows domains to share user and group IDs with local, LDAP, or NIS users and groups. This results in the same permissions and quota consumption applying to both users and groups in an ID-mapped pair. This information is accessed and configured using the **Security > ID Mapping** page:



Example: John Smith is a local user on a SnapServer, as well as having a user ID on a Windows domain. John's quota for the SnapServer has been set to 200 MB. The administrator of the SnapServer maps the Windows domain user's UID for John Smith to the local UID for John Smith, giving both users access to John's 200 MB.

Select a local, LDAP, or NIS user or group from the displayed list on the default page. You can then click **Add Mapping** to map the user's UID or group's GID to that of a Windows domain user or group. **Change Mapping** is used to change existing mappings. **Remove Mappings** removes one or more mappings while **Remove All Mappings** removes all mappings that had been previously established.

To simplify the discovery of a desired user or group to manage their ID mapping search options are presented at the bottom of the selection pages. On the search results page, you can narrow the list by using the following options:

- Check **View only unsaved changes** to display only mapping changes that have not yet been applied.
- Check **View only mapped users and groups** to display only local or NIS users and groups that have been mapped to a Windows domain user or group.

Add Mapping

NOTE: Adding or changing an ID mapping requires that the server be joined to a Windows Active Directory domain.

1. If the desired user or group to be mapped to **does not appear** in the default page list, use the **search option** to locate them.

Local Groups (1 found)
Igneous (18001)

View only unsaved changes. View only mapped users and groups.

Search All local users and groups. Find All Find

- a. Using the Search drop-down list, select a **list** to search.
 - b. Do **one** of the following:
 - Select **Find** and enter the exact **name** (or a string with a wildcard "*" before or after).
 - Select **Find All**.
 - c. Click **Search** to display any matches.
2. Select a **user or group** from the **Local users and groups (displayed with mappings)** list field.
 3. Click **Add Mapping**.
 4. At the **Add Mapping** page, select the Windows domain **user or group list**, and click **Search**.
 - To search for a specific user or group, use either **Find All** or a **Find** search string (wildcard "*" before or after string is allowed).

Enter Parameters

Search NATIONALPARKS Users. Find All Find

- For domains that **REQUIRE** authentication (showing an **(A)** after the name), select the domain name, enter the **User Name** and **Password** for that domain, and use either **Find All** or a **Find** search string (wildcard "*" before or after string is allowed).

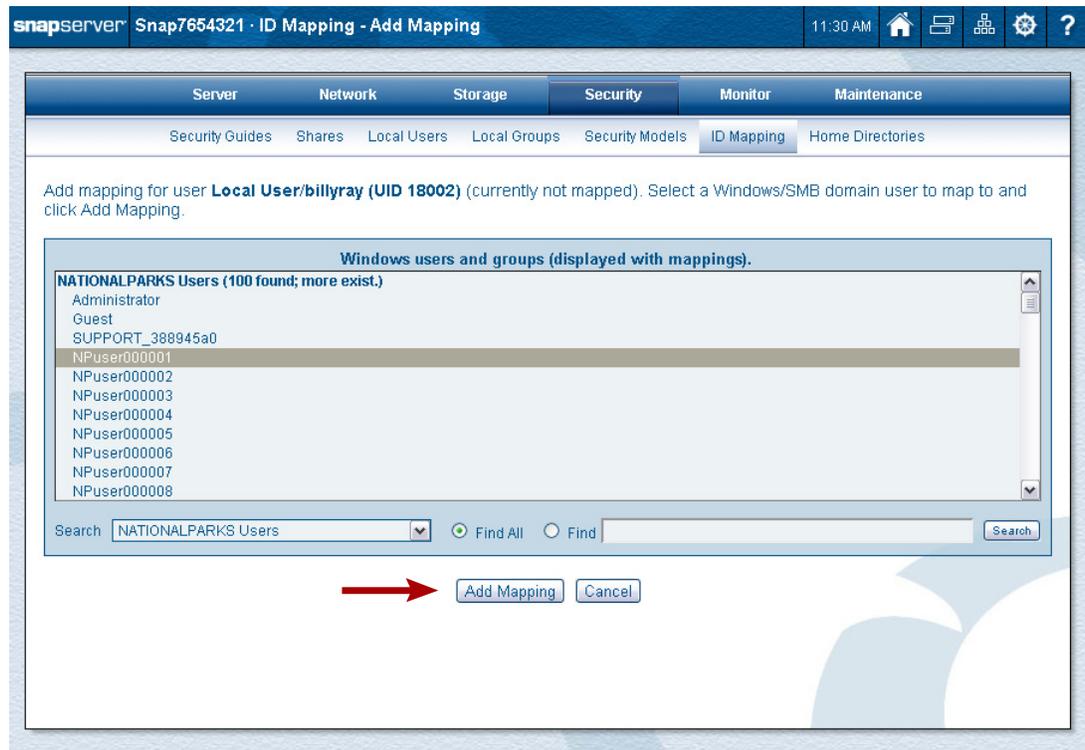
Enter Parameters

Search Cardinals Users (A). Find All Find

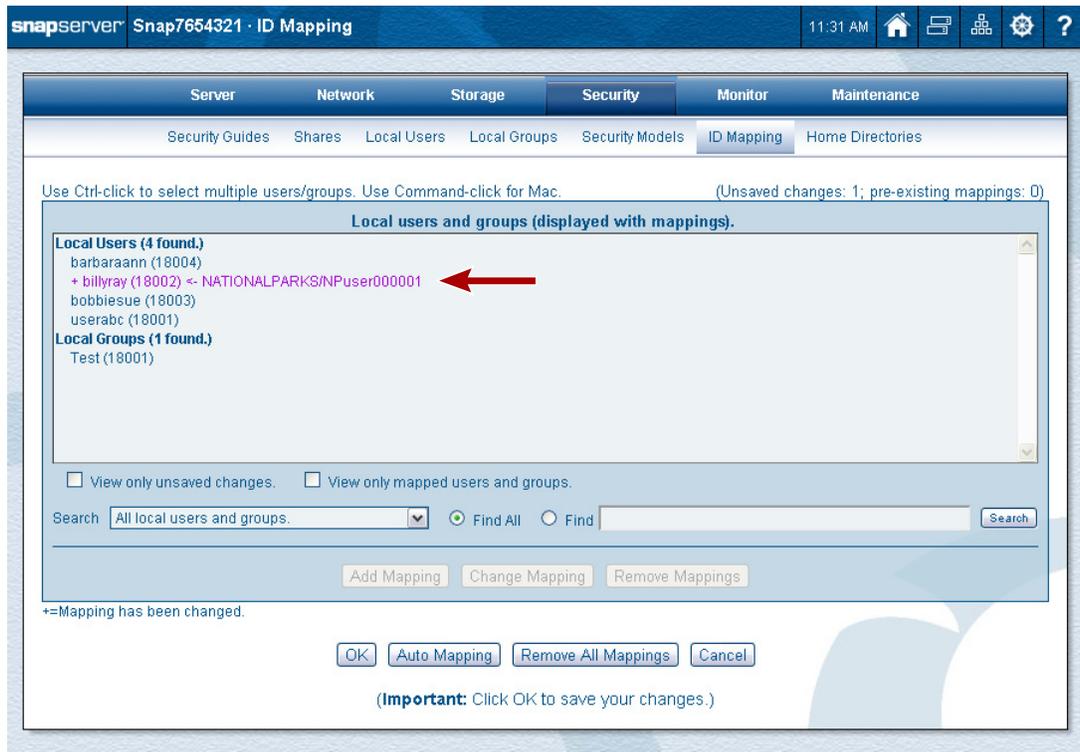
User Name

Password

- On the rare occasion you need to search for a Windows domain that's not listed (“remote domain”), select a Windows domain from the **Search** drop-down list through which to search, then enter in the **Find** field the name of the remote domain, followed by a slash (/) or backslash (\) and the user name for which you are searching (for example, **remote_domain\user_name**). After you click **Search**, you may get another authentication prompt to authenticate with the remote domain.
5. From the search results, select the Windows/SMB domain user you want to map the local or NIS user to, and click **Add Mapping**.



The mapping result is shown on the default page.



Check **View only unsaved changes** to display only changes that have not yet been applied. Check **View only mapped users and groups** to display only local or NIS users or groups that have been mapped to a Windows domain user or group.

6. Repeat [Steps 1–5](#) to add **other mappings**.
7. Save your **changes**:
 - a. Click **OK** to save changes (or **Cancel** to reset).
 - b. At the confirmation page, click **Save Changes**.
 - c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.
See [Filesystem Updates](#) on [page 175](#) for more details.

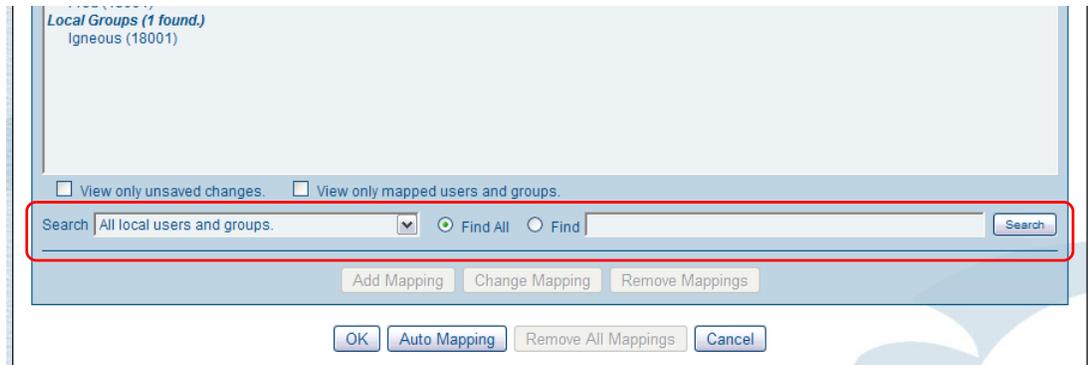


IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

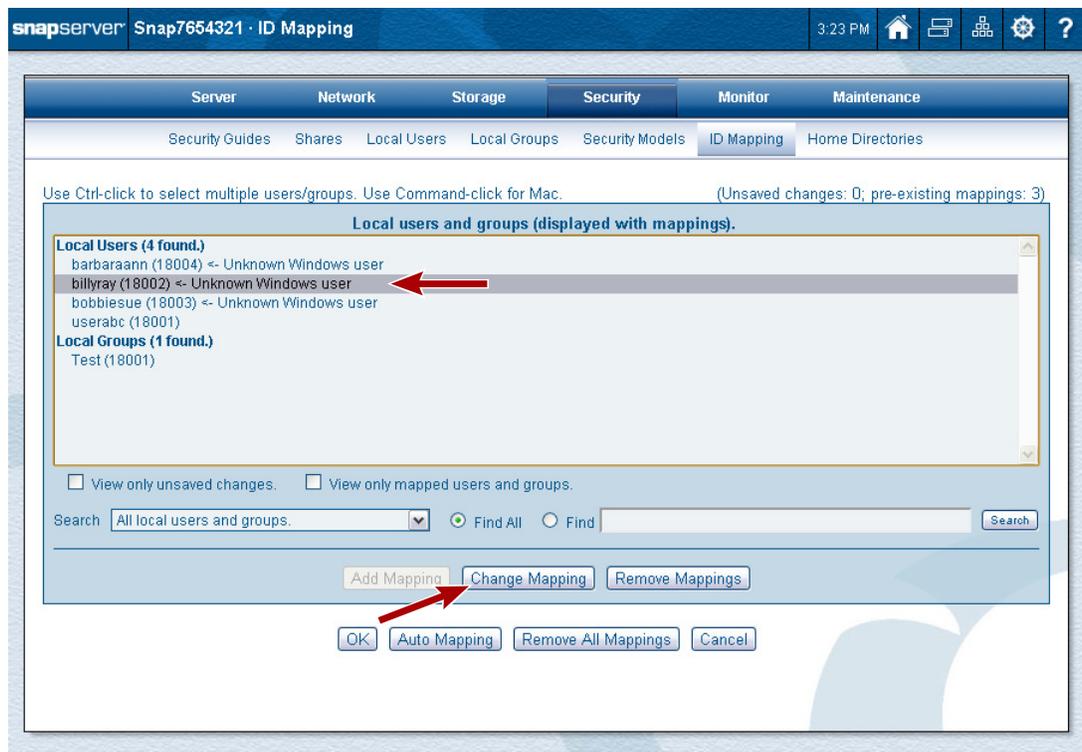
Change Mapping

To re-map a mapped local or NIS user or group to a different Windows domain user or group:

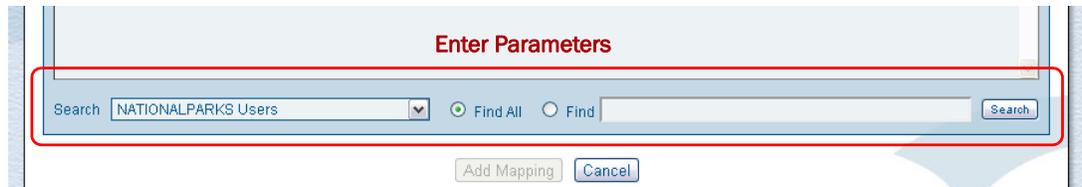
1. If the desired user or group to be mapped to **does not appear** in the default page list, use the **search option** to locate them.



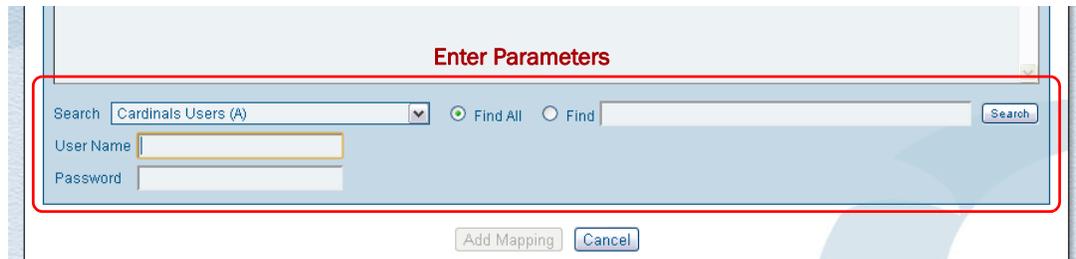
- a. Using the Search drop-down list, select a **list** to search.
 - b. Do **one** of the following:
 - Select **Find** and enter the exact **name** (or a string with a wildcard "*" before or after).
 - Select **Find All**.
 - c. Click **Search** to display any matches.
2. Select a **mapped user or group** to be changed, and click **Change Mapping**.



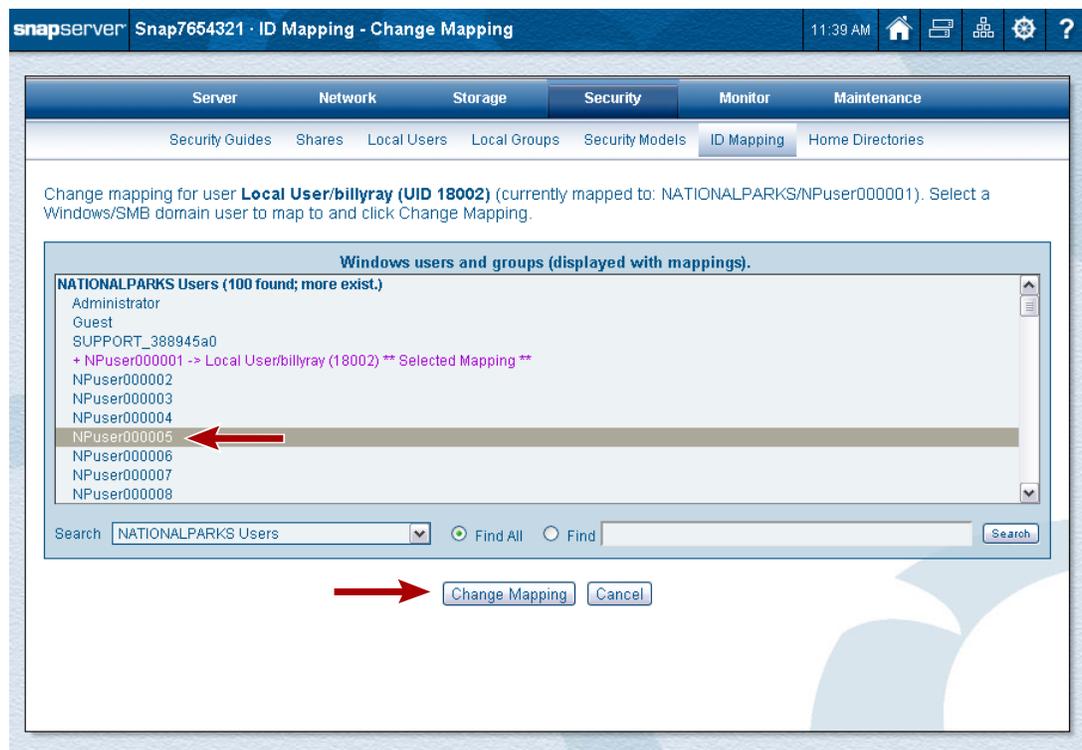
3. At the **Change Mapping** page, select the Windows domain **user or group list**, and click **Search**.
 - To search for a specific user or group, use either **Find All** or a **Find** search string (wildcard "*" before or after string is allowed).



- For domains that **REQUIRE** authentication (showing an **(A)** after the name), select the domain name, enter the **User Name** and **Password** for that domain, and use either **Find All** or a **Find** search string (wildcard "*" before or after string is allowed).



- On the rare occasion you need to search for a Windows domain that's not listed ("remote domain"), select a Windows domain from the **Search** drop-down list through which to search, then enter in the **Find** field the name of the remote domain, followed by a slash (/) or backslash (\) and the user name for which you are searching (for example, **remote_domain\user_name**). After you click **Search**, you may get another authentication prompt to authenticate with the remote domain.
4. From the search results, select a new Windows/SMB domain user to map to and click **Change Mapping**.



5. Repeat **Steps 1–4** until all **changes** are made.

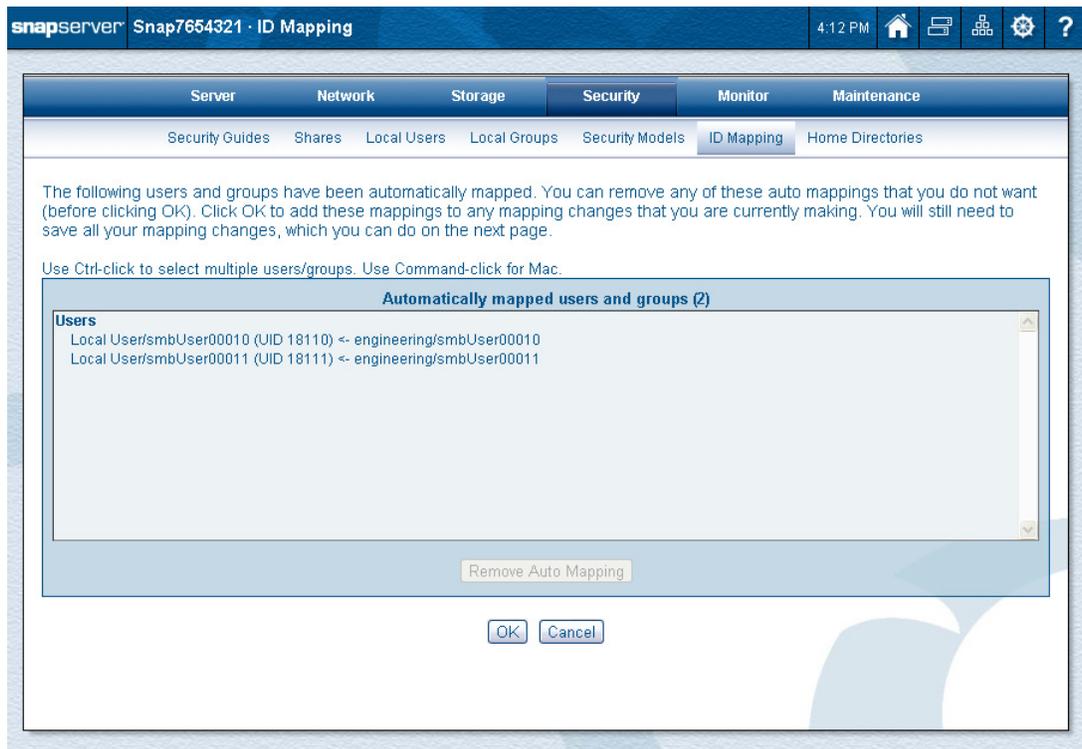
6. Save your **changes**:
 - a. Click **OK** to save changes (or **Cancel** to reset).
 - b. At the confirmation page, click **Save Changes**.
 - c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.
See [Filesystem Updates](#) on page 175 for more details.



IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Auto Mapping

1. Click **Auto Mapping** to generate a list of Windows domain users/groups that have the same name as your local, LDAP, or NIS users and groups:
Domain, local, LDAP, and NIS user and group lists are compared. The matches are automatically queued. Users and groups already mapped will not be affected.
2. At the confirmation page, click **View Auto Mappings** to continue.
A page is displayed summarizing your changes.



3. Save your **changes**:
 - a. Click **OK** to save changes (or **Cancel** to reset).
 - b. At the confirmation page, click **Save Changes**.

- c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.

See [Filesystem Updates](#) on [page 175](#) for more details.



IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Remove Mappings

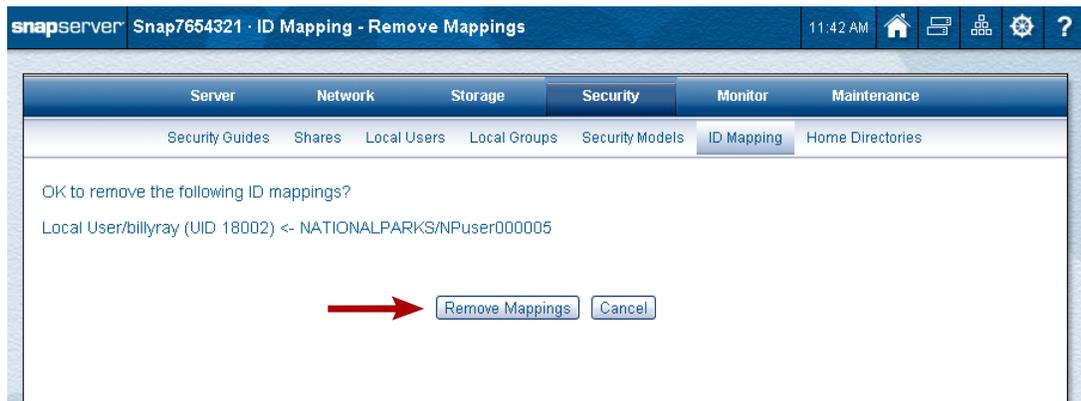
User mappings can be removed individually or all at once. Once removed, they can not be restored but must be added back using [Add Mapping](#) on [page 166](#). You also have the option to update the filesystem after removing the ID mappings.

Remove a Mapping

1. At the default page, select one or more users/groups you wish to unmap and click **Remove Mappings**.

If necessary, check **View only mapped users and groups** to display only local or NIS users or groups that have been mapped to make it easier to find ones to remove.

2. At the **ID Mapping - Remove Mappings** page, verify the users/groups on the list, and click **Remove Mappings**.



The mappings are removed and the default page is displayed.

3. Repeat [Steps 1–2](#) until all **changes** are made.
4. Save your **changes**:
 - a. Click **OK** to save changes (or **Cancel** to reset).
 - b. At the confirmation page, click **Save Changes**.
 - c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.

See [Filesystem Updates](#) on [page 175](#) for more details.



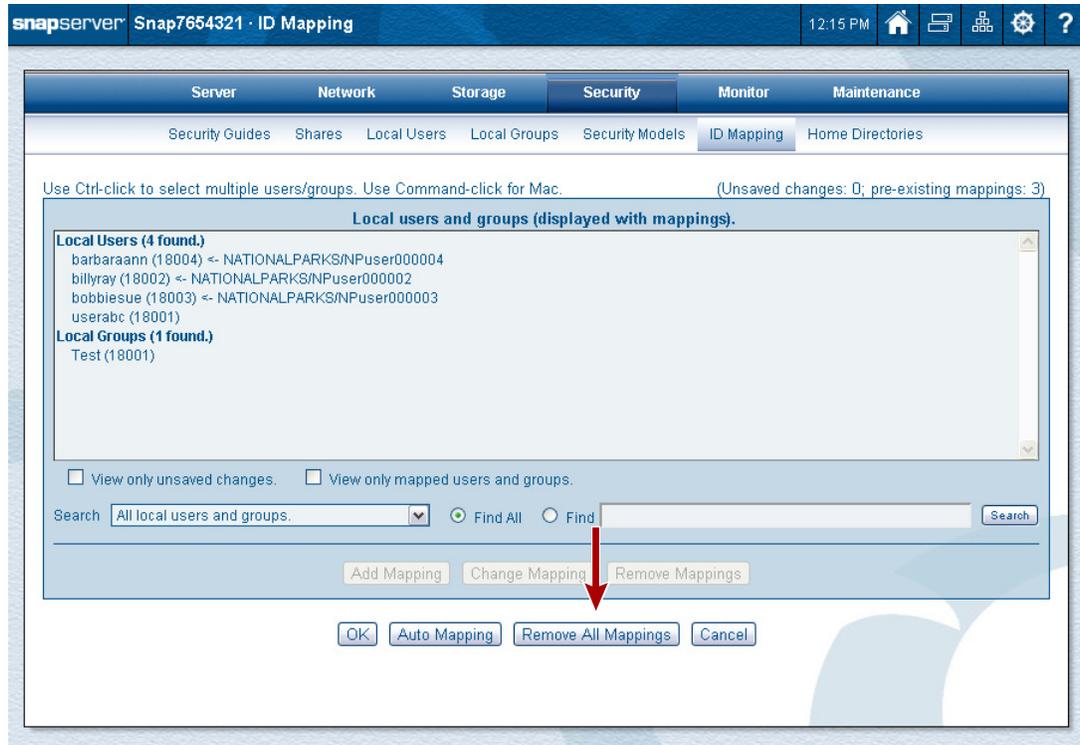
IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Remove All Mappings

The **Remove All Mappings** button allows you to remove all ID mappings on the SnapServer. Click this only if you want to remove all ID mappings. If there are no mappings, the button is grayed out.

1. At the default page, without highlighting any users or groups, click the **Remove All Mappings** button.

Check **View only unsaved changes** to display only mapping changes that have not yet been applied. Check **View only mapped users and groups** to display only local or NIS users/groups that have been mapped to a Windows domain user or group.



2. A confirmation page appears. Click **Remove All Mappings**.
3. Save your **changes**:
 - a. Click **OK** to save changes (or **Cancel** to reset).
 - b. At the confirmation page, click **Save Changes**.
 - c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.

See [Filesystem Updates](#) on [page 175](#) for more details.



IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Remove Missing ID Mappings

If the SnapServer has mappings for users or groups that no longer exist, the following warning message may be displayed at the top of the main **ID Mapping** page:



1. Click the **Click here** link in the warning message to display the following page:



2. Click **Remove Missing Mappings** to clear them from the system. A confirmation is shown on the **ID Mapping** main page.



3. Click **OK** to save changes.

Filesystem Updates

After making any changes to ID mappings, you are presented with a filesystem update option page, where you can choose either **Update Filesystem** or **Do Not Update Filesystem** options.

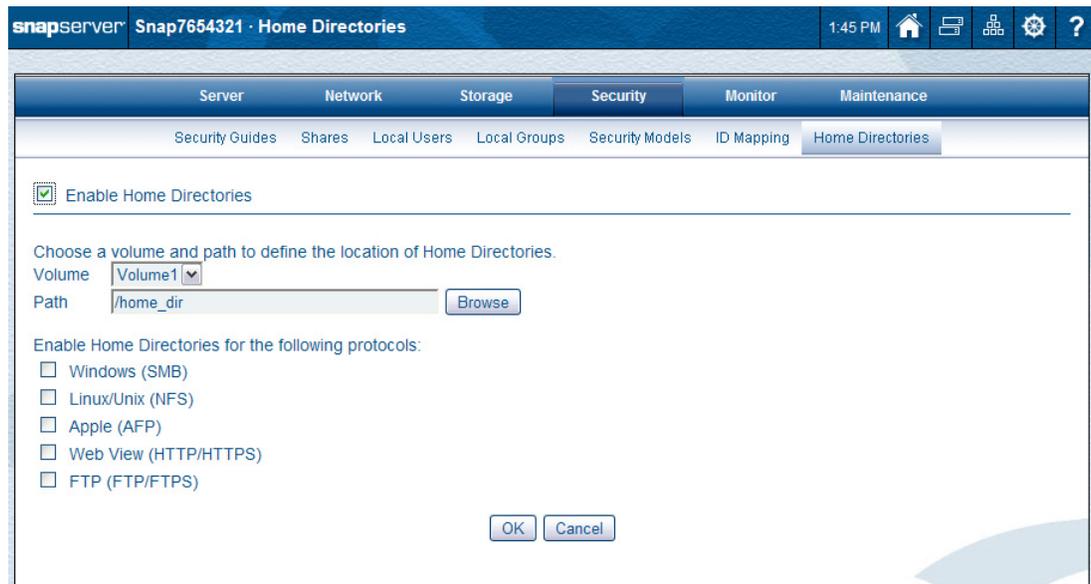


If you choose **Update Filesystem**, UID and GID ownership on files and SIDs in ACLs will be updated to reflect the ID mapping operation.

IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Home Directories

To enable Home Directories, go to **Security > Home Directories** and check **Enable Home Directories**. Choose the volume, path, and protocols you want.



The Home Directories feature creates a private directory for every local or Windows domain user that accesses the system. When enabling Home Directories (from the **Security > Home Directories** page), the administrator creates or selects a directory to serve as the home directory root. When a user logs in to the server for the first time after the administrator has

enabled Home Directories, a new directory named after the user is automatically created inside the home directory root, and is configured to be accessible only to the specific user and the administrator.

Depending on the protocol, home directories are accessed by users either via a user-specific share, or via a common share pointing to the home directory root.

Home directories are supported for SMB, NFS, AFP, HTTP/HTTPS, and FTP/FTPS. They are accessed by clients in the following manner:

- For SMB, AFP, and HTTP/HTTPS, users are presented with a virtual share named after the user name. The virtual share is visible and accessible only to the user. Users are not limited only to their virtual shares; all other shares on the server continue to be accessible in the usual fashion.
- For NFS, the home directory is exported. When a user mounts the home directory root, all home directories will be visible inside the root, but the user's home directory will be accessible only by the user and the administrator.

NOTE: If desired, Unix clients can be configured to use a Snap Home Directory as the local user's system home directory. Configure the client to mount the home directory root for all users, and then configure each user account on the client to use the user-specific directory on the SnapServer as the user's home directory.

- For FTP/FTPS, local users will automatically be placed in their private home directory when they log in. Access to the home directory is facilitated through a share pointing to a parent directory of the home directory, so users can still change to the top-level directory to access other shares.

If **ID Mapping** (see [page 165](#)) is enabled, domain users and local users mapped to the same user will be directed to the domain user's home directory. In some cases, data in the local user's home directory will be copied to the domain user's home directory:

- If a local user home directory accumulates files before the local and domain users are mapped, and if the domain user's home directory is empty, the local user's files will be copied to the domain user's home directory the first time the local user connects after the users are mapped.
- If both the local and domain user home directories accumulate files before the local and domain users are mapped, the files in the local user's home directory will not be copied to the domain user's home directory.

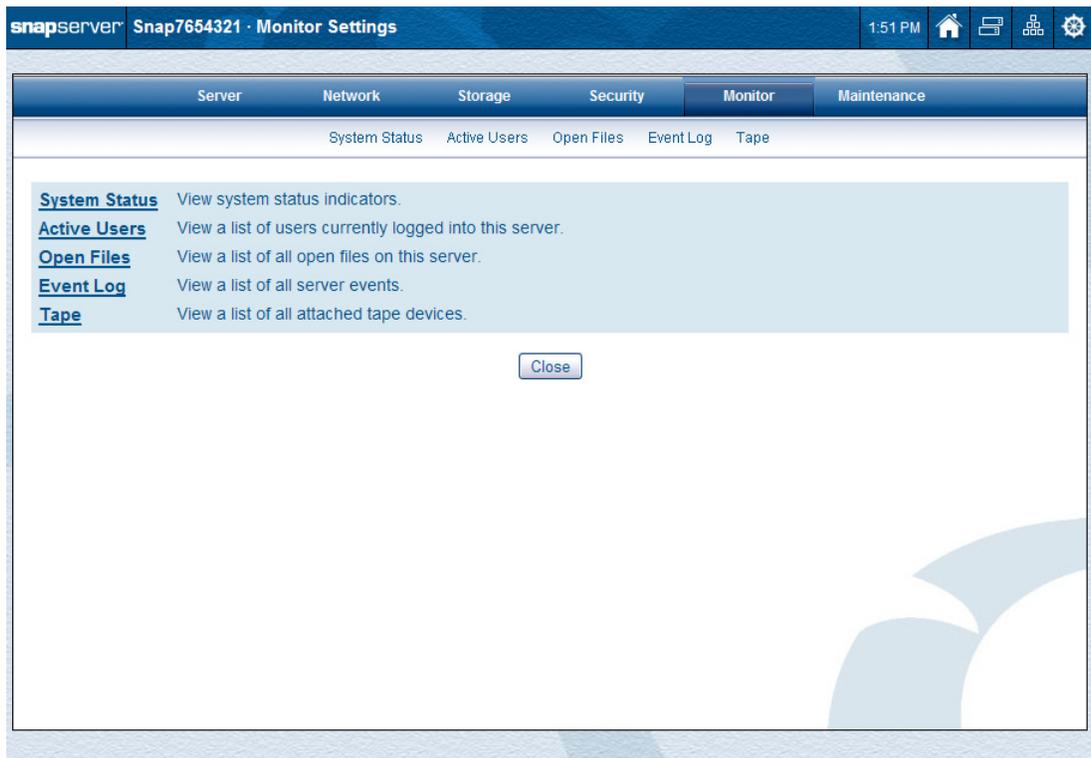
Configure Home Directories

Complete the following fields and click **OK**.

Field	Description
Enable Home Directories	Check to enable Home Directories for local users. Remove the check to disable.
Volume	Select the volume where the Home Directories will be located. NOTE: Be sure the volume you select has enough disk space. Once Home Directories are placed, they cannot be moved.
Path	Provide the path to the Home Directories or click Browse to create a new folder. The default path is <code>/home_dir/</code> .
Enable Protocols	Check each of the protocols where Home Directories will be enabled.

NOTE: Do not put Home Directories on a volume that might be deleted. If you delete the volume, you will also delete the Home Directories.

This chapter addresses the options for monitoring the SnapServer. Here you can view the system status and other activities.



Topics in System Monitoring:

- [System Status](#)
- [Active Users](#)
- [Open Files](#)
- [Event Log](#)
- [Tape](#)

System Status

Use the **System Status** page (**Monitor > System Status**) to assess the status of the SnapServer and any attached expansion units.



SnapServer Status

The following status fields will be displayed for the SnapServer (head unit). Any critical messages are displayed in a **red font**.

Field	Description
Server Name	Current name of the server. The default server name is SNAPnnnnnn, where nnnnnn is your server number (for example, SNAP112358).
Server Model	Server model (such as SnapServer DX1).
OS Version	The version of GuardianOS currently loaded on the SnapServer.
Server Number	Number derived from the MAC address on Ethernet 1 port, used as part of the default server name.
Serial Number	Unique number assigned to the SnapServer.
Uptime	The amount of time the server has been up (since the last reboot) in "days:hours:minutes" format.
Memory	Amount of system RAM.
CPU (n)	The type of central processing unit for the server's different CPUs. If more than one CPU exists, each is listed separately.
Ethernet 1	Details on the server's primary Ethernet connection.

Field	Description
Ethernet 2	If it exists, details on the server's secondary Ethernet connection.
Ethernet <i>n</i>	If an optional Ethernet card is installed, details on the server's other Ethernet connections are shown.
Ambient Temp.	The temperature of the space inside the chassis.
CPU Temp.	Current CPU temperature.
Power Supply	The status of power supply modules
Fan Status	The status of fan modules.

Expansion Unit Status

The following status fields will be displayed for each expansion unit.

Field	Description
Expansion Unit	EXTN1, EXTN2, etc.
Expansion Model	SnapServer Expansion S50, etc.
Serial Number	The serial number of the expansion unit
Ambient Temperature	The temperature of the space around the expansion unit.
Power Supply	The status of the power supply
Fan Status	The status of fan modules.

Click **Refresh** to update the information. Click **Close** to return to the main **Monitor** page.

Active Users

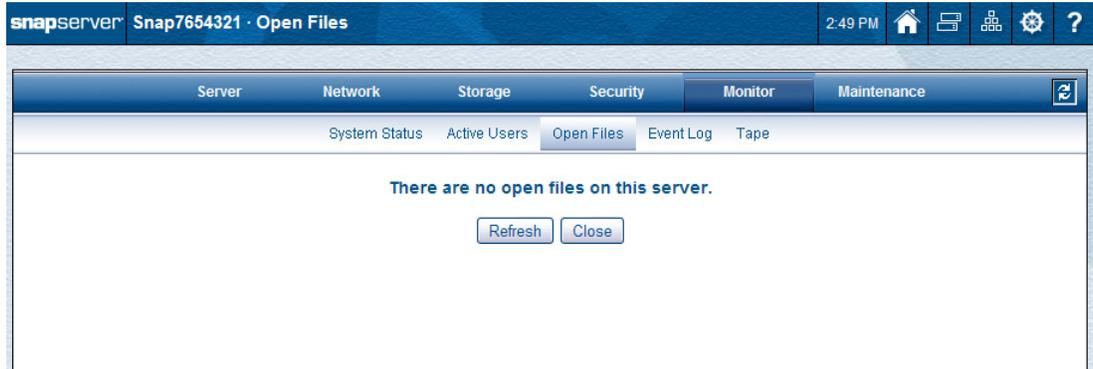
Use this page to view read-only details on the active users logged on to the server. Information available on this page includes user names of all active users, their workstation names, authorization, the number of open files they have on the share, the protocol, and when they logged on. Columns can be sorted in ascending or descending order by clicking the column head.

NOTE: Active users are not displayed for HTTP or NFS.



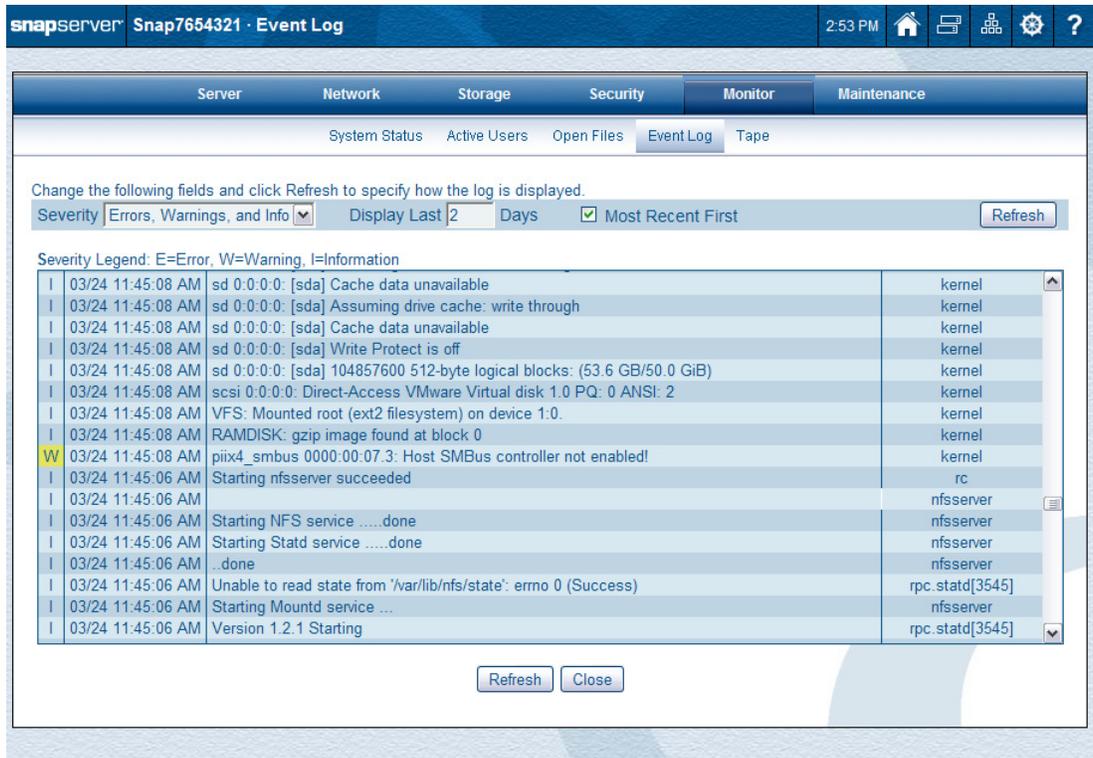
Open Files

Use this page to view read-only details on the open files in use on this server.



Event Log

Use the **Event Log** page to view a log of operations performed on the server.



Entries are color coded according to severity as described in the following table:

Background Color	Entry Type
Red 	Errors (E)
Yellow 	Warning (W)

Background Color	Entry Type
(no color)	Informational or Unclassified (I)

Filter the Log

Edit the following fields as appropriate, then click **Refresh**.

Option	Description
Severity	Select the type of entries you want to view.
Display Last <i>n</i> Days	Enter the number of days' entries (24-hour periods) you want to view
Most Recent First	Select to start the list with the most recent entry, deselect to start the list with the oldest entry.

Tape

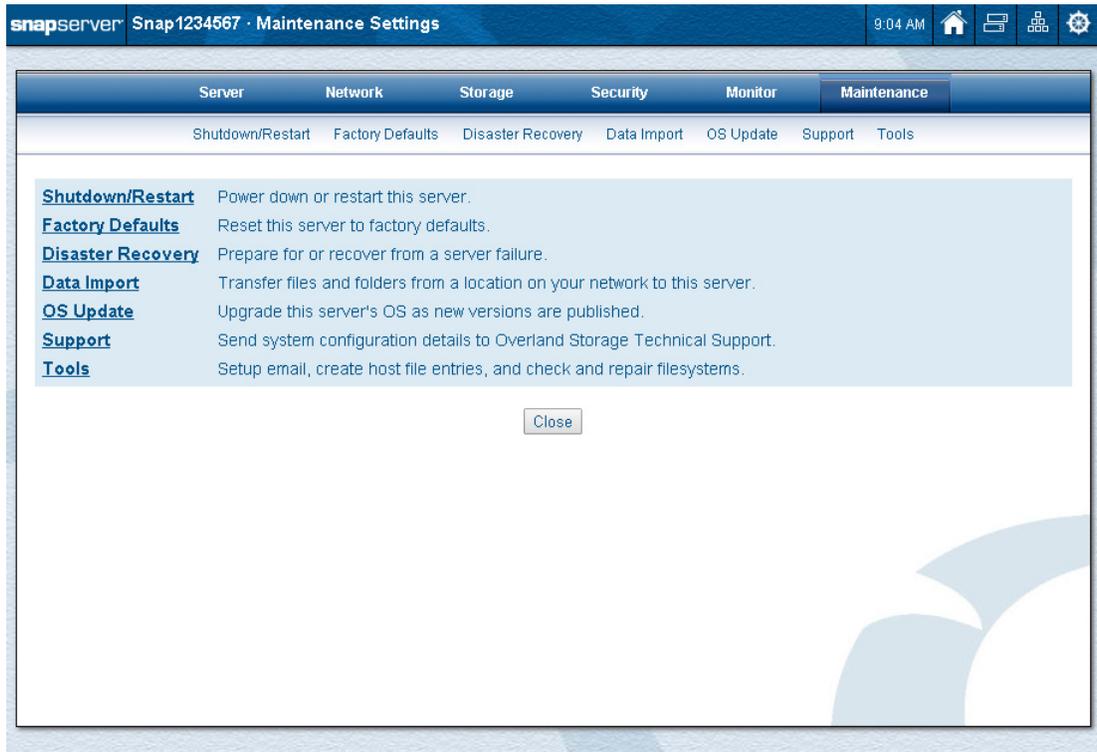
Use the **Tape** page to monitor and view read-only details on the SCSI and USB tape devices attached to the server.



Information presented on this page includes:

Field	Description
Device Model	The manufacturer's model for the device.
Device Type	Type of tape device: either Sequential-Access (tape drive) or Medium-Changer (for example, robotic arm for a tape library).
Device Name	Name of the device node to which the device is bound.
Connection	Identifies the connection type: SCSI or USB.
Bus	Bus number indicating which physical interface (for example, SCSI card) the device is connected to.
ID	ID number (SCSI only)
LUN	LUN identifier (SCSI only)

Clicking the **Maintenance** tab on the Web Management Interface displays seven options used to maintain your SnapServer appliance and the GuardianOS 7.5 software. The **Tools** option has four subpages of options.

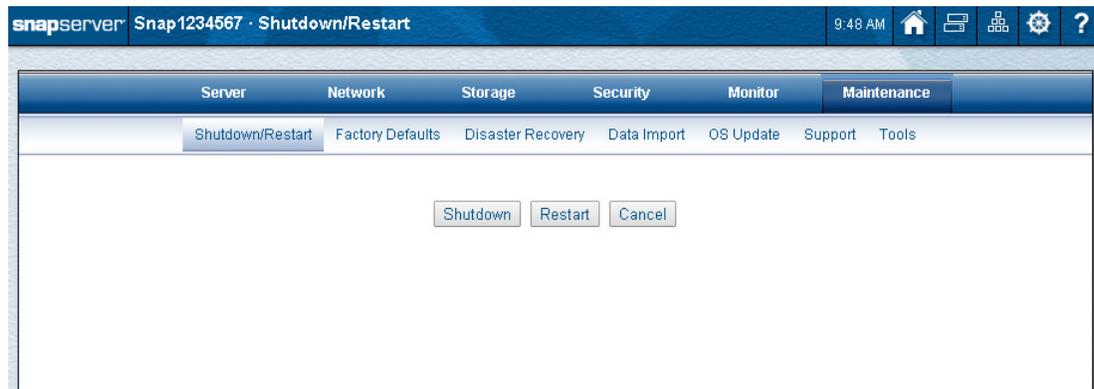


Topics in Web Management Interface

- [Shutdown and Restart](#)
- [Factory Defaults](#)
- [Disaster Recovery](#)
- [Data Import](#)
- [OS Update](#)
- [Support](#)
- [Maintenance Tools](#)
 - [Email Notification](#)
 - [Host File Editor](#)
 - [To Check the Filesystem on a Volume](#)
 - [To Check the Root Filesystem](#)

Shutdown and Restart

Use the **Shutdown/Restart** page to reboot or shut down the server.



Click one of the following buttons:

- **Shutdown** – Shuts down and powers off the server.
- **Restart** – Reboots the server via a controlled shutdown and restart.

The selected process begins immediately.

Manually Powering SnapServers On and Off



CAUTION: To prevent possible data corruption or loss, make sure all users are disconnected from the SnapServer before powering down the server.

The power button on the front of the server can be used to turn the server ON or OFF if necessary:

- To turn the server ON, press the power button on the front of the server. The server takes a few minutes to initialize. A green system/status LED indicates that the system is up and running.
- To turn the server OFF, press and release the power button to begin the shutdown process. Do not depress this button for more than four seconds.

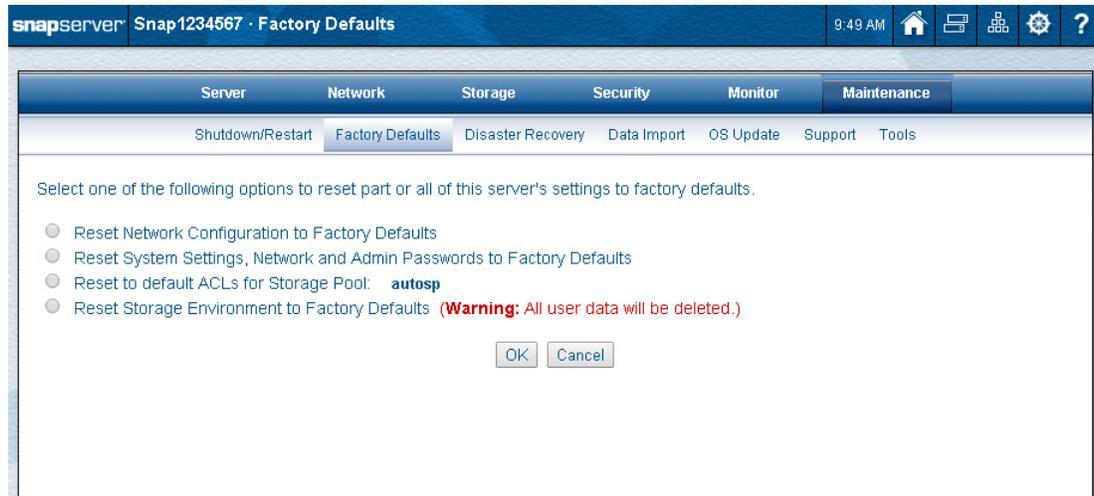
NOTE: SnapServers have a persistent power state. When a physical loss of power occurs, the SnapServer returns to the same operation it had when the power went out. Therefore, if the system is powered down prior to a power loss, it will remain powered down when the power is restored.

Factory Defaults

GuardianOS allows you to reset different components of the system back to the original factory defaults. You can reset some or all of the factory settings using the different options available on the **Factory Defaults** page.



CAUTION: Each reset option requires a restart of the server. To prevent possible data corruption or loss, make sure all users are disconnected from the SnapServer before proceeding.



Navigate to the **Maintenance > Factory Defaults** page in the Web Management Interface, select one of the following options, and then click **OK**:

- **Reset Network Configuration To Factory Defaults** – Returns TCP/IP and other network protocol settings to factory defaults.
- **Reset System Settings, Network, and Admin Passwords To Factory Defaults** – Returns the admin and root passwords to the default value, returns TCP/IP and other network protocol settings to factory defaults, eliminates all shares to all volumes, and returns settings for server name, date and time, users, groups, Windows and NIS domain memberships, quotas, and the activation and configuration of CA Antivirus to factory default values. Storage configuration and data is retained.

When the server finishes rebooting, the Login dialog box opens. Enter the default admin password of **admin**, and click **OK**. The Initial Setup Wizard runs, allowing you to reset the server name, admin password, and IP address.

NOTE: Resetting system settings will disable Snap EDR. After reset, you will need to uninstall, reinstall, and reconfigure Snap EDR.

- **Reset To Default ACLs For Volume: <volume name>** – Resets the file and directory security on selected volumes. Volumes are all set to the Windows/Unix security model. All files and directories are set to the Windows personality with a Windows ACL that gives full access to Administrators, read access to Everyone, file/directory create access to Everyone (for directories), and full access to the owner (owners are retained in the reset operation).

NOTE: Rebooting or shutting down the server in the middle of an ACL reset will halt the operation, and it will not recommence on reboot.

- **Reset Storage Environment to Factory Defaults** – Storage configuration is reset and the Initial Setup Wizard is displayed when the SnapServer is restarted.



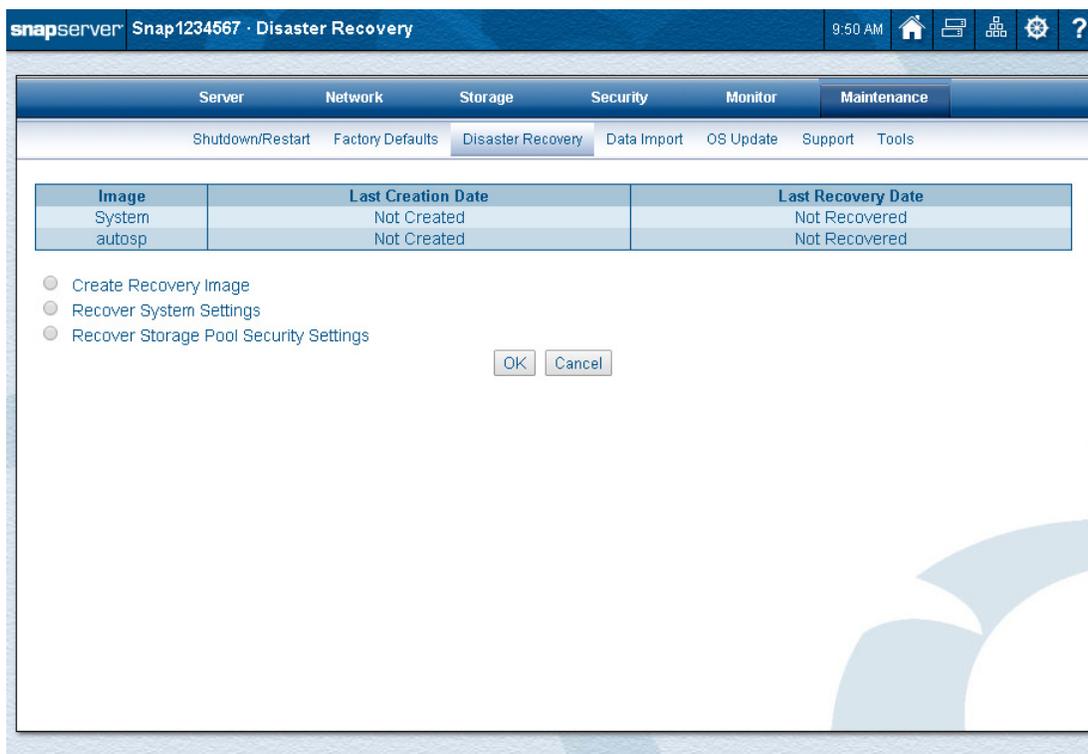
CAUTION: ALL USER DATA WILL BE DELETED on the SnapServer when this option is selected. A confirmation page will be displayed, and the admin password must be entered before the process begins.

NOTE: Use this option to change your RAID configuration standard from DynamicRAID to Traditional RAID or vice versa.

Disaster Recovery

Disaster recovery entails creating the files you need to recover a SnapServer configuration, such as network and RAID configurations, together with volume-specific information, such as ACLs and quota settings.

NOTE: Disaster recovery does not include user data. Backups of user data must be configured and managed separately; see [Backup Solutions \(Appendix B\)](#) for information on backup options.



Disaster recovery also encompasses what to do if all access to the data on a SnapServer is cut off due to a hardware or software failure. Focus is placed on these procedures:

- Reinstalling the SnapServer operating system (GuardianOS).
- Restoring the SnapServer to its original configuration with data intact.

These files are then used to restore any SnapServer to its original state. The disaster recovery feature can also be used to clone one server to another by restoring the disaster recovery image from one server to another server.

Backing Up Server and Volume Settings

In addition to backing up the data stored on the SnapServer, you may also back up the server's system and volume settings. The **Disaster Recovery** page allows you to create the files you need to restore these settings:

- Server-specific settings such as network, RAID, volume and share configurations, local user and group lists, snapshot schedules, and Snap EDR Management Console settings (if applicable).
- Volume-specific settings such as ACLs, extended attributes, and quota settings.

For information about scheduling these tasks, see [Scheduling Data Protection Tasks](#) in [Chapter 2](#).

SnapDRImage File and Volume-Specific Files

Details on the SnapServer disaster recovery files and the information they contain are as follows:

- **SnapDRImage** – The SnapServer disaster recovery image saves server-specific settings such as network, RAID, volume and share configuration, local user and group lists, and snapshot schedules, and Snap EDR Management Console settings (if applicable). There is one SnapDRImage file per server, residing in the `.os_private` directory on the root of the first volume in Traditional RAID, or on the root of the first volume on the first storage pool in Dynamic RAID.

NOTE: The SnapDRImage file is in binary form and can be safely used only with the SnapServer Disaster Recovery tool. Other tools will not work and may compromise the integrity of the file.

- **Volume-specific files** – These files, named *backup.acl*, *backup.qta.groups*, and *backup.qta.users*, preserve volume-specific settings such as ACLs, extended attributes, and quota settings. One set of these files exists per volume, and are located as follows:
 - In Traditional RAID, the volume settings specific to each volume are stored in the `.os_private` directory on the root of each volume.
 - In DynamicRAID, the volume settings for an entire storage pool are stored in the `.os_private` directory on the first volume of the storage pool.



CAUTION: The Create Recovery Files option in the snapshot feature automatically updates the volume-specific files when the snapshot is taken. If you do not use snapshots to back up a volume to tape, you must manually regenerate these files whenever you change ACL or quota information to ensure that you are backing up the most current volume settings.

Creating the SnapDRImage and Volume Files

Creating a SnapDRImage that covers the scope of your server's configuration is essential to a successful disaster recovery operation. Create a disaster recovery image on the **Disaster Recovery** page. This DRImage should be created after server configuration is complete, and can be used to recover the server or a replacement server to the configured state.

Before you create the disaster recovery files, make sure you have completed the following activities:

- You have completely configured the SnapServer. If you subsequently make any major changes to the configuration of your server, you must repeat the procedures described in this section to have an up-to-date SnapDRImage.

NOTE: You may want to record, in an off-server location, the following information about the configuration of your server: (1) the server name; (2) the number of RAID; (3) the number of volumes; and (4) the size of each volume. If the disaster recovery fails, having this information may be useful in recreating the original configuration of the server.

- You have devised and implemented a data backup strategy. It is recommended that you make a backup of your system regularly, from the root of the share for each volume, and store it in an off-server location. This ensures that the most current data is backed up and available for use with a disaster recovery.

Use the following procedure to create and secure the disaster recovery files:

Step 1: Create the disaster recovery files.

Navigate to the **Maintenance > Disaster Recovery** page. Select the **Create Recovery Image** button and click **OK** to create the SnapDRImage file and the volume files in a single operation.

Step 2: Copy the files to a safe place off the server.

Once the recovery image has been made, click the **Download Recovery Image** button to download the SnapDRImage file to a safe location on another server or backup medium. (See [SnapDRImage File and Volume-Specific Files](#) on [page 187](#) for file names and paths.) This strategy ensures that if the filesystem on the SnapServer is corrupted, the image file will be available to restore server settings.

The DRImage is also automatically placed in the root of the first user volume. These files will be copied to tape as part of your regular backup procedures.

Step 3: Back up volume-specific files with scheduled data backups.

Ensure the `.os_private` directory on each volume is included in your backup configuration so the volume-specific files are written to tape as part of your regular volume backup procedures.

System Settings Recovery

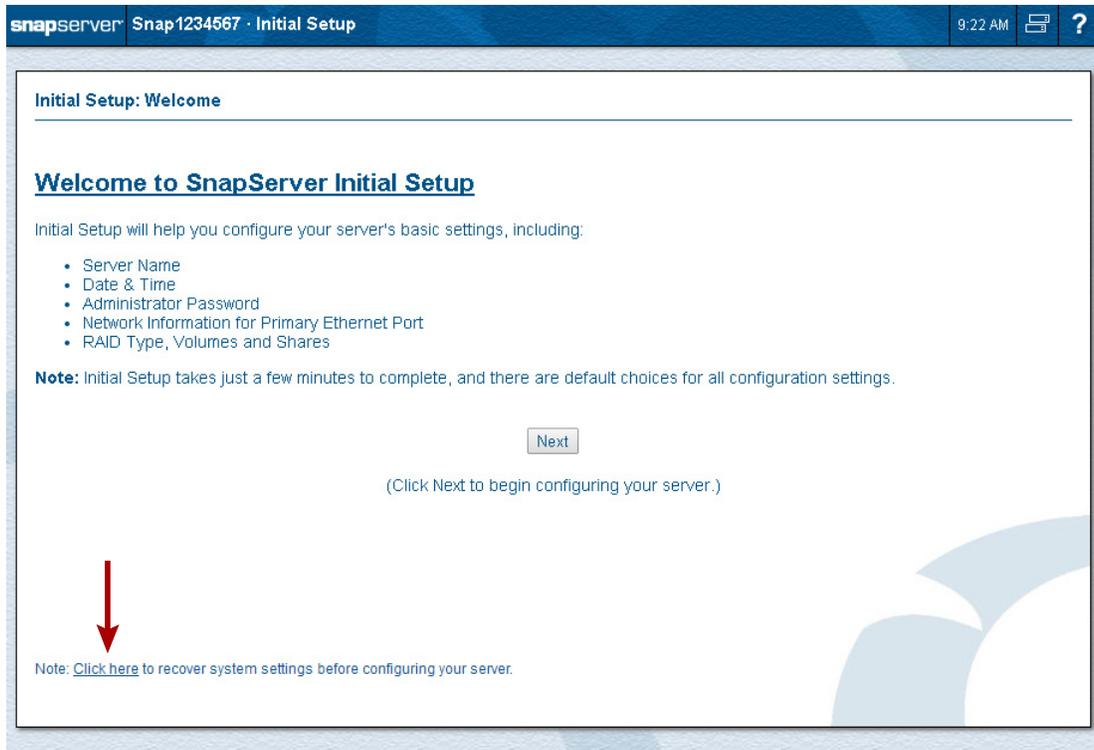
System settings include all network, user, share, and storage configuration, and can only be performed on an uninitialized server as a replacement or clone. If system settings must be restored to a configured server, contact technical support to perform a fresh install of the OS to put it back in the uninitialized default state.



CAUTION: A fresh install of the OS and return to the uninitialized default state will destroy all existing data on the server.

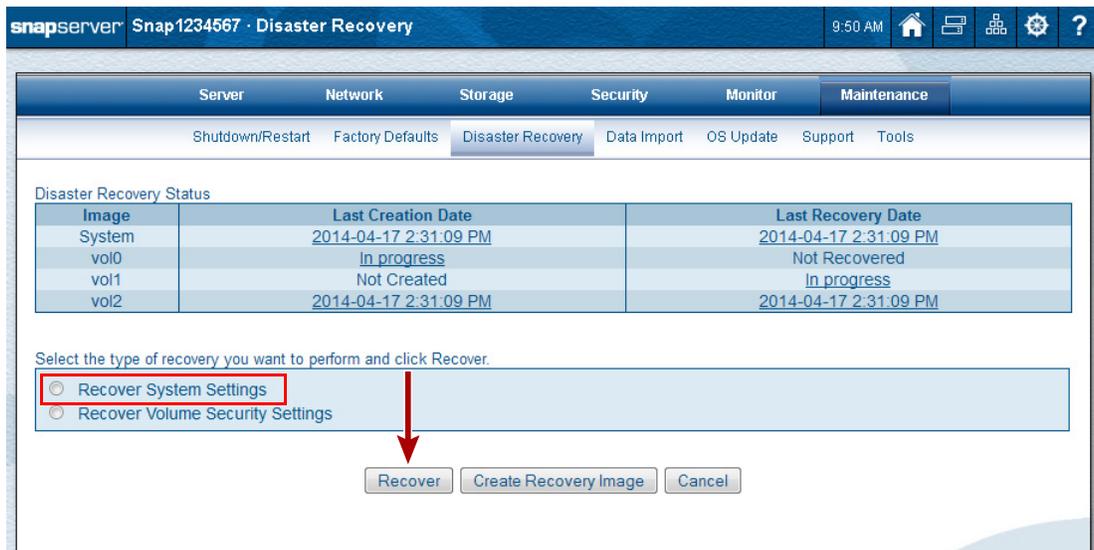
Recovering System Settings

1. Click the **link** on the **Initial Setup Welcome** page:



This link launches the **Disaster Recovery** page.

- At the **Disaster Recovery** page, select the **Recover System Settings** option and click **Recover** to open the Server Recovery page.



CAUTION: Do not try to navigate back from this page during the recovery process. Activity is restricted to this page so that the recovery operation is not interrupted which might result in a loss of data.

- At the **Server Recovery** page, use the **Browse** button to navigate to the SnapDRImage file.

4. Click **Recover** to start the operation.
5. If the recovery file contains **Snap EDR application settings**, you are asked if you want to include those settings. Check the settings you want to recover, and click **Recover**.
After recovery completes, the server restarts.
6. After the server restarts, log in to **Administration**, navigate to **Network > Windows/SMB**, and, if necessary, rejoin the Windows domain.

The server is now available for additional configuration, data restore from tape backup, and volume or storage pool security recovery. If any configuration operations failed, view the recovery log on the **Disaster Recovery** page.

Volume and Storage Pool Security Settings Recovery

Volume and storage pool security settings include file system security and quota settings for each volume, and is only available on configured servers with volume, data, and user configuration in place. Recovery requires the backup.acl, backup.qta.groups, and backup.qta.users files to be present in the .os_private directory on each volume or storage pool on which you wish to recover security settings.

Recovering Security Settings on a Volume or Storage Pool

1. If necessary, restore **user data** from tape backups to **each** volume you want to recover. Ensure the correct backup.acl, backup.qta.groups, and backup.qta.users files matching the data are placed in the .os_private directory on each of the volumes.
2. Connect to the **Administration** page and navigate to **Maintenance > Disaster Recovery**.

The screenshot shows the SnapServer Administration interface. The top navigation bar includes 'snapserver', 'Snap1234567 · Disaster Recovery', and a clock showing '9:50 AM'. Below the navigation bar, there are tabs for 'Server', 'Network', 'Storage', 'Security', 'Monitor', and 'Maintenance'. Under the 'Maintenance' tab, there are sub-tabs: 'Shutdown/Restart', 'Factory Defaults', 'Disaster Recovery', 'Data Import', 'OS Update', 'Support', and 'Tools'. The 'Disaster Recovery' sub-tab is active, showing a 'Disaster Recovery Status' section with a table:

Image	Last Creation Date	Last Recovery Date
System	2014-04-17 2:31:09 PM	2014-04-17 2:31:09 PM
vol0	In progress	Not Recovered
vol1	Not Created	In progress
vol2	2014-04-17 2:31:09 PM	2014-04-17 2:31:09 PM

Below the table, there is a section titled 'Select the type of recovery you want to perform and click Recover.' with two radio buttons: 'Recover System Settings (Not available because the server has already been configured.)' and 'Recover Storage Pool Security Settings' (which is selected and highlighted with a red box). At the bottom, there are three buttons: 'Recover', 'Create Recovery Image', and 'Cancel'.

3. Select the **Recover Volume Security Settings** button and click **Recover**.
4. Select the **volume** you want to restore.
The creation date of the recovery file on a volume indicates when the recovery files were generated. Volumes that do not have recovery files in .os_private appear as unavailable.
5. Click **Recover** to start the operation and follow the onscreen instructions.
6. After recovery completes, check the **recovery log** for the volume on the **Disaster Recovery** page if there were any errors.

7. Repeat [Steps 3–6](#) to recover any **additional** volumes.

Replacing or Cloning a Server

Disaster Recovery combined with restore from backup can be used to recover configuration to a replacement server or to clone a server's configuration to another server.



IMPORTANT: When recovering configuration to a server replacing a failed server, Overland Storage strongly recommends that you contact a technical service representative before proceeding.

When recovering configuration, any third-party license keys you have not purchased through Overland Storage are lost. If you have installed data replication or management utilities such as Snap EDR, you will need to re-install and/or relicense them for use with the new server. You will also need to reschedule snapshots and reconfigure CA Antivirus.

Replacing or Cloning a Server

1. Recover **system settings** as described in [Recovering System Settings](#) on [page 188](#).
2. Recover **volume or storage pool security settings** as described in [Recovering Security Settings on a Volume or Storage Pool](#) on [page 190](#).
Be sure to restore the backup.acl, backup.qta.groups, and backup.qta.users files matching the user data to the .os_private directory on each volume you want to restore.
3. If necessary, reconfigure or reschedule the following items:
 - Reconfigure your **Snap EDR** settings.
 - Reconfigure your **CA Antivirus** settings.
 - Reschedule your **snapshot** times.

Data Import

Use the **Data Import** page to import (migrate) data from a legacy SnapServer or other computer that supports CIFS or NFS (v2 or v3) to a new SnapServer. This feature can be used to copy or move files and folders from a server on the network (Source) to your SnapServer (Target). To access the **Data Import** utility, navigate to **Maintenance > Data Import**.

If an error is encountered during the import (for example, a file or folder is locked and cannot be imported), the utility records the error in a log, and continues the operation. When the import is completed, the administrator can view the log of import errors. Once the errors have been corrected, the administrator returns to the main page, and recreates the import. With the exception of the password, all fields will still be populated with the specifications of the last job.

The following import options can be specified:

- Copy or move data
- Include subfolders
- Overwrite existing files
- Preserve the original permissions settings

NOTE: If you elect to preserve original permissions settings, be sure to review [Preserving Permissions on page 195](#).

- Verify imported data

NOTE: If you elect to verify imported data, all data will be read twice, once for import and once for comparison to the copied data. This could be a lengthy process.

Setting Up a Data Import Job

Before setting up a data import job, be sure to specify a user identity for the operation that will have full access to all files on the source, regardless of permissions set:

- For Windows import, specify an administrator or member of the Windows server/domain administrators group.
- For NFSv2/3 import, consider using the user root, and configuring the NFS export on the source to `no_root_squash` for the IP Address of the SnapServer for the duration of the import.

To create a data import job, perform the following procedure:

NOTE: Only one import job can run at a time.

1. On the **Data Import** page, complete the required **information** for both the source (legacy server) and target (SnapServer).

Option	Description
Source	
Network Protocol	<p>Protocol that the SnapServer uses to connect to the source server. Select:</p> <ul style="list-style-type: none"> • Windows (SMB) for Windows servers or GuardianOS servers with source data on a Windows root directory (default) <p>NOTE: If you are importing via SMB, SMB must also be enabled on the target SnapServer (go to Network > Windows/SMB to enable SMB in GuardianOS).</p> <ul style="list-style-type: none"> • NFS v2/3 for Unix/Linux-based servers or GuardianOS servers with source data on a Unix root directory
User Identification	<ul style="list-style-type: none"> • If Windows was selected as the protocol, provide the Auth. (Authentication) Name and Password (Windows user name and password to log in to the server over SMB). • If NFS was selected as the protocol, provide the User Name (SnapServer local user name or NIS user, representing the UID used to perform the operation over NFS).
Host	Enter the name or IP address of the source computer you are importing data from.
Share/Export	<p>Specify the Windows share or NFS export on the source server containing the data you want to import.</p> <p>NOTE: Wildcards are not supported when specifying the source share to import.</p>
Path	<p>Enter the path to the file or folder you want to import. If you are importing the entire share, you can leave the source Path field blank.</p> <p>NOTE: Wildcards are not supported when specifying the path to import.</p>
Target	
Volume	Specify the volume on the target SnapServer where you want the data imported.
Path	Specify the path to the target SnapServer where you want the data imported.

Option	Description
Options	
Import Type	Options for the import data are to Copy (source data is maintained) or Move (source data is removed during copy). If Verify imported data is enabled, the Move option removes the original data after the verification is complete. The default is Copy . NOTE: If you select to Move rather than Copy data, it is strongly recommended that you also select to Verify imported data .
Include All Sub-folders	If the folder you select for import contains sub-folders, selecting this option will import all files and folders underneath this folder (checked by default). If disabled, <i>only</i> the files directly in this folder will be imported.
Overwrite Existing Target Files & Folders	If files/folders on the target share identical names with files/folders on the source, checking this option overwrites those files/folders during import (checked by default.)
Preserve File/Folder Permissions	Selecting this option will retain the source permissions when the files/folders are imported to the SnapServer target (unchecked by default). NOTE: Before selecting this option, be sure to review Preserving Permissions on page 195 .
Verify Imported Data	Selecting this option will cause all source data to be read twice, once to write to the target SnapServer and once to perform a binary comparison with the data written to the SnapServer (unchecked by default). If enabled, and if the Import Type is Move , files on the source will only be removed after verification. Otherwise, files will be removed immediately during the copying of them to the SnapServer. If you select to move files rather than copy them, it is strongly recommended that you enable the Verify imported data option. If a file mismatch occurs during verification, the target file is moved to a <code>data_import_verify_failures</code> directory on the root of the same volume. Check the failed file to determine the problem, then run the import again with Overwrite Existing Target Files & Folders deselected (so you don't re-copy files that have already been copied and verified). NOTE: Depending upon how much data is being imported, verifying imported data can be a lengthy process.
Email Notification	Clicking the email notification link will take you to the Email Notification page (for more information, see Email Notification on page 201). Fill in notification information and check the box next to Administrative Operation Event in order to receive an email when the import operation is complete.

- Once you have completed the import information, click the **Start Import** button to begin the import. You can see the progress of the import, an estimated time until completion, and the Import log on the **Data Import** page as it is compiling.
- When the import is complete, click the **View Log** button to see details of all errors. Click the **Data Import Error Log** link to download the entire log.

Stopping an Import Job

To stop the import at any time, click the **Stop Import** button on the **Data Import** page. If a file was in the process of being copied, the partially-copied file on the target will be removed.

Recreating an Import Job

The Data Import log records all errors that occurred during import. You can import files and folders that were not imported during the original job because of an error condition (for example, the file was locked).

1. Review the **Data Import** errors log and correct all error conditions.
2. Reopen the **Data Import** page. All fields (except the password) for the last import will still be visible on the page.
3. Click **Start Import** to run the import again. By default, all files will be re-imported. If you want only to import those files that failed to import the first time, you can disable the **Overwrite existing target files** option. However, make sure that any problematic files during the first import are deleted from the target SnapServer so they will be re-imported.

NOTE: If an import failed, it is strongly recommended that you enable the [Verify imported data](#) option for the re-importation.

Preserving Permissions

The types of permissions retained will differ, depending on which import scenario is applied.

Importing from a Windows Security Model to a Windows Root Directory

If you are importing from a Windows server (or other type of server that follows the Windows security model) to a Windows personality directory on a SnapServer, permissions will be retained exactly as they exist on the source. However, as is the case when moving files with permissions between Windows servers, permissions for users that are unknown on the target server will be retained but not enforced. This includes permissions for:

- Local users on the source machine.
- Domain users for domains unknown to the SnapServer (for example, trusted domains, if the SnapServer is not configured to support trusted domains).
- Certain built-in Windows users and groups.

Importing from a Unix Security Model to a Unix Root directory

If you are importing from a Unix server to a Unix personality directory, Unix permissions for UIDs/GIDs are copied exactly from source to target; thus, identities of the users and groups will be best retained if the SnapServer belongs to the same NIS domain as the Unix server.

Importing Between Conflicting Security Models

When importing from a Unix source to a Windows root directory, Unix permissions will be retained and the security personality on the resulting files and directories will be Unix.

However, when importing from a Windows source to a Unix root directory, permissions cannot be retained (since Unix root directories are required to be Unix personality throughout). Files and directories will inherit the Unix personality and will have a set of default Unix permissions.

Importing from a GuardianOS Server

When importing from one GuardianOS server to another, it is recommended that you maintain the same security model on the target server that you have on the source.

- If your source server uses a Windows root directory and has permissions assigned to Windows domain users, use a Windows connection for import. Windows permissions will be retained exactly as they are on the source, with the same enforcement limitations for unknown users as for import from Windows servers (see [Importing from a Windows Security Model to a Windows Root Directory](#) on page 195).

NOTE: If importing from a pre-5.0 GuardianOS server, Windows permissions will be retained verbatim, but may have different meaning due to the differences between the pre-5.0 POSIX ACL security model and the Windows security model introduced in 5.0.

- If your source server uses a Unix root directory and has permissions assigned to local or NIS users, use an NFS connection for import.

NOTE: Local users that have Unix permissions on the source will not be created on the target with the same UIDs.

OS Update

Use this page to install updates to GuardianOS and other installed software. The GuardianOS can be configured here to automatically check for updates to GuardianOS and Snap EDR.

snapservers Snap7654321 · OS Update 8:42 AM

Server Network Storage Security Monitor Maintenance

Shutdown/Restart Factory Defaults Disaster Recovery Data Import OS Update Support Tools

Software updates can be downloaded from the SnapServer [software update website](#).

Specify a software update file below and then click Upload File to upload the file to your server.
Important: Please do not interrupt this upload process.

Current GOS Version: 7.5.025

Software Update File: No file chosen

Note: Click the Upload File button only once. The browser may take several seconds or more to process the file upload request.

Last OS Update: Completed successfully on 2014-04-07 11:01 AM.

Information about the last GuardianOS update is listed at the bottom of the page, and may include the status of the update, product and version, and the completion time.

 **CAUTION:** Do not interrupt the update process. You may severely damage the server if you interrupt a software update operation before it is complete.

Check for Updates

Click the **Check for Updates** button to force the server to immediately search for applicable updates. If an update is available, it will be displayed with information about the update and include a link to download the software to a local computer for upgrade use.



Update the GuardianOS Software

1. Click the **Check for Updates** button.

If an update is available, follow the instructions on the page.

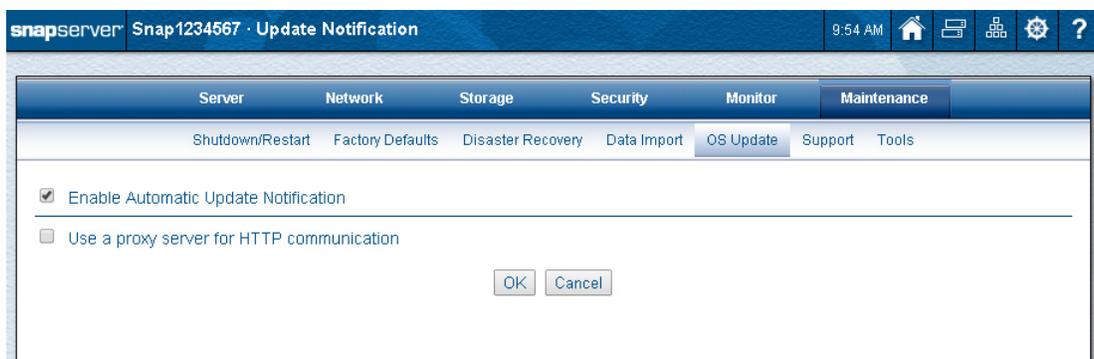
NOTE: If the server does not have access to the Internet, download the latest GuardianOS image or other software package from the [Overland Storage website](#).

2. On the **OS Update** page, click **Choose File**, locate the file to be uploaded, and select it.
3. Click **Upload File** to start the upload to the server.

Only click the button once. Some browsers show the percent of the upload progress in their bottom status bar. The SnapServer uploads the software package and then prompts you to reboot the server to perform the upgrade. Click **Restart for Update** (or click **Cancel** to abort the update).

Update Notification

You can configure GuardianOS to display an alert when GuardianOS or Snap EDR updates are available for the server.



When enabled, the SnapServer checks weekly for GuardianOS or Snap EDR updates that are applicable to the server. If updates are available, a banner alert will display just below the menu bar on the Web Management Interface pages.

NOTE: You can choose to hide the banner by clicking the *Remind me later* or *Hide this message* link on the banner. If *Remind me later*, the server will display the banner after the next check for updates; if *Hide this message*, the server will hide the banner for the update in question until a later version is released.

Configuring Update Notification

1. Click the **Update Notification** button.
2. Click to put a check in the **Enable Automatic Update Notification** check box.
3. If your environment requires using a **proxy server** for external web-based communication:
 - a. Check the **Use a proxy server for HTTP communication** checkbox.
 - b. Complete the **Proxy Host** and **Proxy Port** fields.
4. Click **OK**.

Last OS Update

At the bottom of the **OS Update** page is a **Last OS Update** link. Click this link to view the status of the last update applied to the server.

snapservers Snap1234567 · OS Update 3:56 PM

Server Network Storage Security Monitor Maintenance

Shutdown/Restart Factory Defaults Disaster Recovery Data Import OS Update Support Tools

Software updates can be downloaded from the SnapServer [software update website](#).

Specify a software update file below and then click Upload File to upload the file to your server.
Important: Please do not interrupt this upload process.

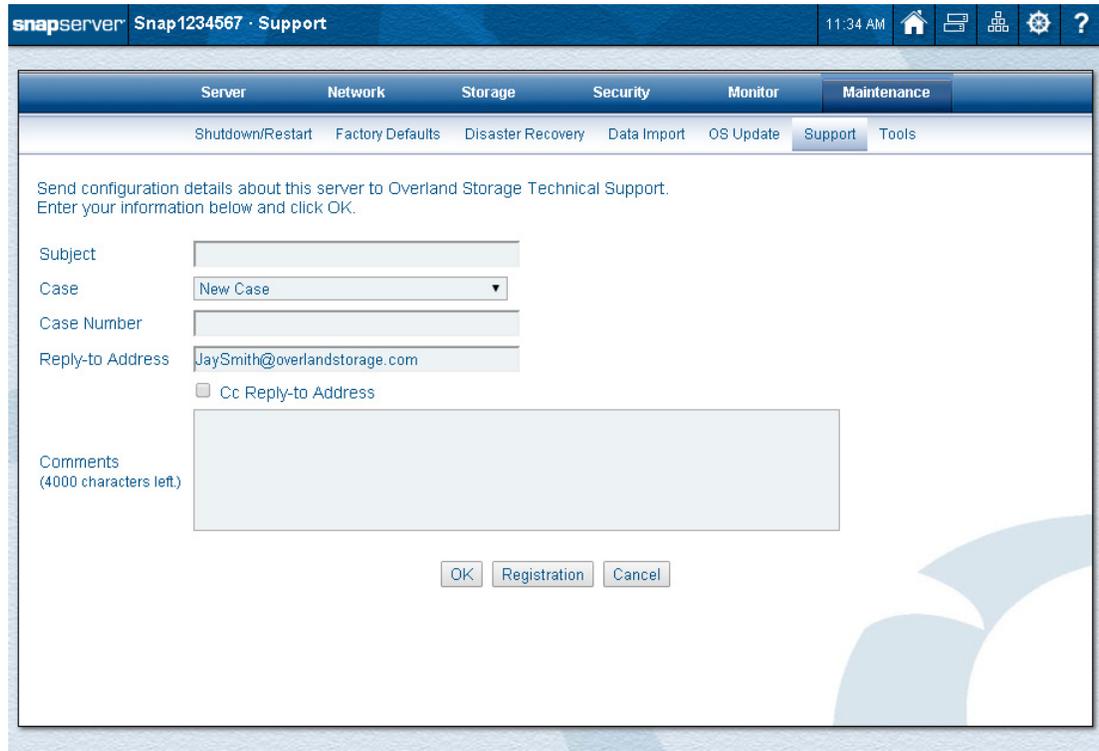
Current GOS Version: 7.5.030
Software Update File: No file chosen

Note: Click the Upload File button only once. The browser may take several seconds or more to process the file upload request.

Last OS Update: Completed successfully on 2014-04-21 11:55 AM.

Support

The **Support** page provides an easy way to contact Overland Technical Support.



The screenshot shows the SnapServer web interface. At the top, there is a navigation bar with the SnapServer logo, the server ID 'Snap1234567', and the title 'Support'. The time is 11:34 AM. Below the navigation bar, there are tabs for 'Server', 'Network', 'Storage', 'Security', 'Monitor', and 'Maintenance'. Under the 'Maintenance' tab, there are sub-tabs for 'Shutdown/Restart', 'Factory Defaults', 'Disaster Recovery', 'Data Import', 'OS Update', 'Support', and 'Tools'. The 'Support' sub-tab is active. The main content area contains the following text: 'Send configuration details about this server to Overland Storage Technical Support. Enter your information below and click OK.' Below this text are several input fields: 'Subject' (text box), 'Case' (dropdown menu with 'New Case' selected), 'Case Number' (text box), 'Reply-to Address' (text box with 'JaySmith@overlandstorage.com' entered), and a checkbox for 'Cc Reply-to Address'. There is also a large text area for 'Comments (4000 characters left)'. At the bottom of the form are three buttons: 'OK', 'Registration', and 'Cancel'.

Once your SnapServer has been registered, Phone Home Support becomes available for use. Phone Home Support emails system logs and files that contain information useful for troubleshooting purposes to Overland Storage technical support. See [Phone Home Support](#) in [Appendix D](#).

Registering Your Server

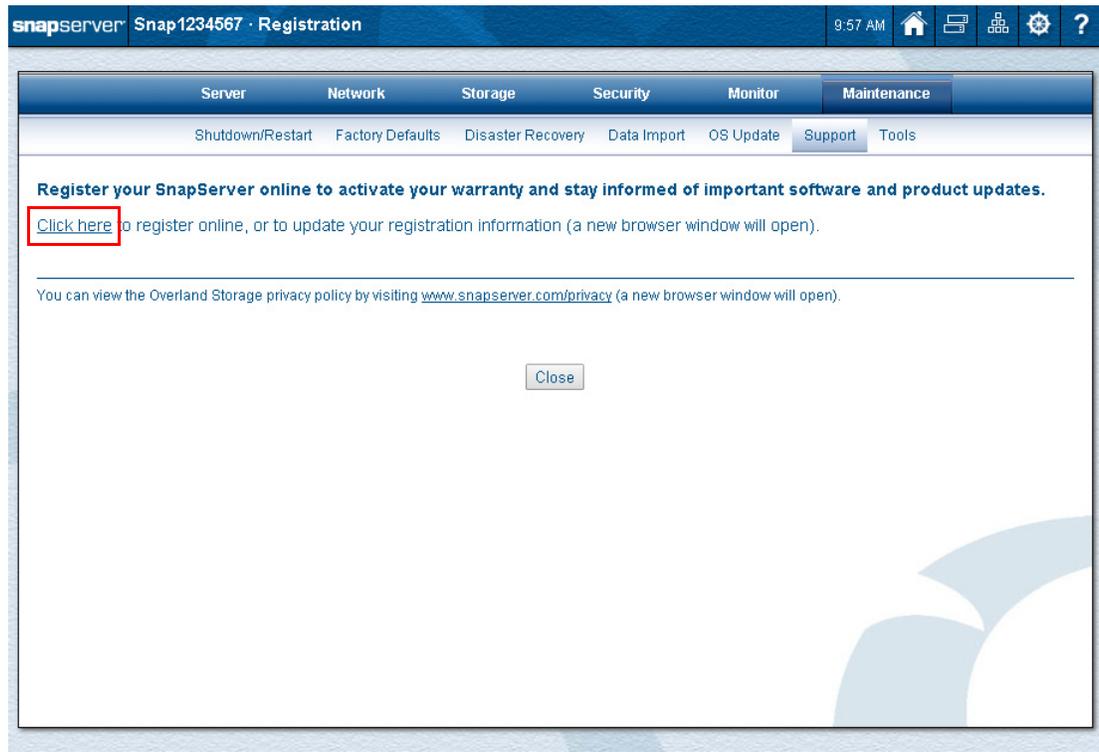
Registering your server activates your warranty and allows you to create and track service requests. Registration also provides access to GuardianOS upgrades, third-party software, and exclusive promotional offers.

NOTE: Warranty information is available at <http://docs.overlandstorage.com/support>

To Register Your Server

NOTE: To use this feature, access to the external Internet is required.

Go to **Maintenance > Support > Registration** and click the **Click here** link to launch the online registration page. Use your Overland credentials to access the **Registration** page.



The same page is also used to update your registration information. Once you have registered, you will receive a confirmation email.

Maintenance Tools

The tools under this Maintenance subheading provide general-purpose server maintenance for both volume and root filesystems.

Email Notification

To configure the server to send email alerts in response to system events, navigate to the **Maintenance > Tools > Email Notification** page. To set up email alerts, you will need: (1) the SMTP server's IP address; and (2) the email address of each recipient to receive an alert.

The screenshot shows the 'Email Notification' configuration page in the SnapServer web interface. The page is titled 'SnapServer Snap1234567 · Email Notification' and includes a navigation menu with options like Server, Network, Storage, Security, Monitor, and Maintenance. The 'Tools' sub-menu is active, showing options like Shutdown/Restart, Factory Defaults, Disaster Recovery, Data Import, OS Update, Support, and Tools. The main configuration area includes:

- Enable Email Notification
- SMTP Server: (Host name or IP address)
- SMTP Port: (Port number for SMTP server)
- Use Authenticated SMTP
- Use Secure Connection
- Email Address of Sender:
 - Use default: Snap1234567@devnet.myoverland.net
 - Use specific:
- Email Addresses of Recipients:
 - (optional)
 - (optional)
 - (optional)
- Send email notification for the following events:
 - Server shutdown/restart
 - RAID Set event
 - Volume is full
 - Hardware event
 - Printing event
 - Administrative operation event
 - License event
- Send a test email to listed email addresses upon saving settings.

Buttons for 'OK' and 'Cancel' are located at the bottom right of the configuration area.

Configuring Email Notification

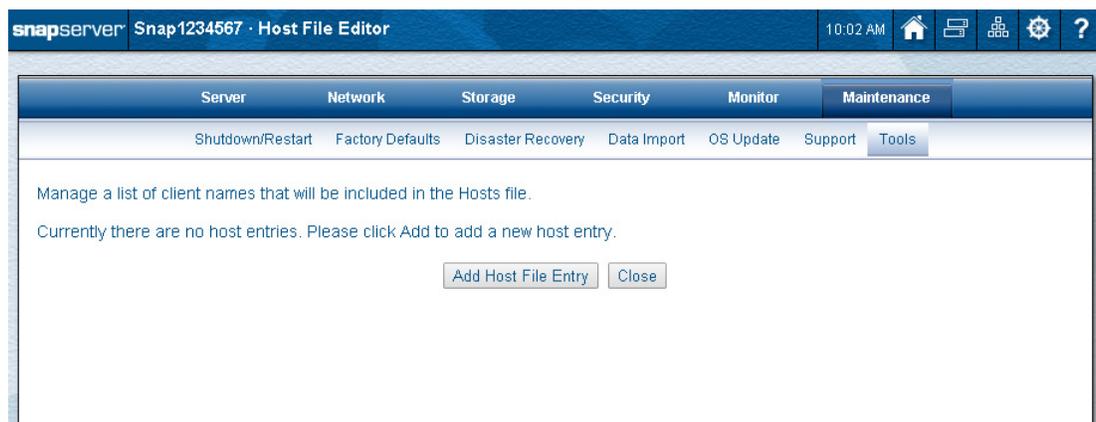
Edit settings as described in the following table, and then click **OK**.

Option	Description
Enable Email Notification	To enable email notification, check the Enable Email Notification box.
SMTP Server	Enter a valid SMTP server IP address or host name.
SMTP Port	Enter a port number for the SMTP server or accept the default. the default is 25.
Use Authenticated SMTP	Check this box to authenticate when an email is sent to the SMTP server by the SnapServer. Provide an authentication User Name and Password in the fields that appear when the feature is enabled. The types of methods supported (in order) are CRAM-MD5, LOGIN, and PLAIN.
Use Secure Connection	Check this box to encrypt emails from the SnapServer. STARTTLS and TLS/SSL encryption protocols are supported.

Option	Description
Email Address of Sender:	Choose: <ul style="list-style-type: none"> The default address (<i>servername@domain</i>) where the <i>domain</i> is the DNS domain name. If there is no DNS domain name, then the server's IP address for Eth0 will be used (<i>servername@ipaddress</i>) Specify a specific sender.
Email Addresses of Recipients	Enter one or more email addresses to receive the notifications. One address is required. Three additional email addresses can be added.
Send Email Notification	Check the boxes next to the events you wish to be notified about: <ul style="list-style-type: none"> Server shutdown/restart – The server shuts down or reboots due to an automatic or manual process. RAID Set event – (1) A RAID 1 or 5 experiences a disk drive failure or a disk drive is removed; or (2) A RAID 1 or 5 configures a spare or a new disk drive as a member. Volume is Full – Storage space on a volume reaches 95% utilization. Hardware event – The internal temperature for the server exceeds its maximum operating temperature or other hardware problems. Printing event – A printer error occurs (for example, the printer is out of paper). Administrative operation event – A Data Import operation has finished or experienced an error. License event – One of the trial licenses included on the SnapServer is about to expire. A notification email will be sent 14 days before the license expires. One day before the license expires another email will be sent. It is recommended that, if you are not acquiring a license key for the SnapExtension that is expiring, you turn off the SnapExtension.
Send a Test Email	To verify your settings, check Send a test email to listed email addresses upon saving settings , then click OK .

Host File Editor

Use this page to identify external hosts in the SnapServer hosts file. This page allows you to supply a hostname-to-IP address mapping that persists across system reboots.



Click **Add Host File Entry**, complete the fields as described on the following table, and then click **Add Host File Entry** again.

Use this table to complete the options shown:

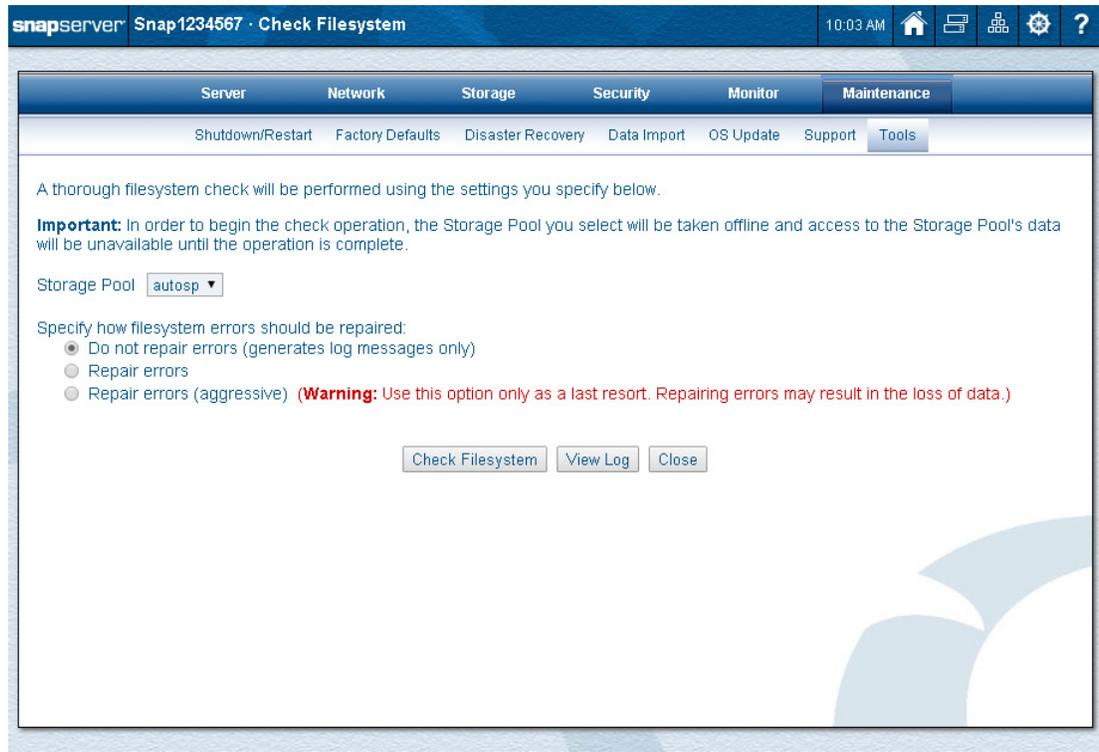
Option	Description
IP Address	The IP address of the external host.
Host Name	Enter the fully qualified hostname for the external host, using the format: <i>myserver.mydomain.com</i> . NOTE: Some applications may require that you enter either one or both of these fields. See the OEM documentation to determine requirements.
Alias (optional)	Enter an optional abbreviated address for the external host, using the format: <i>myserver</i> . NOTE: Some applications may require that you enter either one or both of these fields. See the OEM documentation to determine requirements.

Checking Filesystems

Filesystems on individual volumes can be checked for errors and repaired, if necessary. The root volume filesystem can also be checked, and any errors found will automatically be repaired. Because GuardianOS automatically checks the root volume for errors if any of a number of triggers occurs (for example, a power outage or failure of the volume to mount), it is recommended that the root filesystem check feature only be used when directed by a Technical Support representative.

To Check the Filesystem on a Volume

Checking Filesystems (**Maintenance > Tools > Check Filesystem**) provides a thorough filesystem check on the volume.



 **IMPORTANT:** To begin the check operation, the volume you select is taken offline and access to the volume's data is unavailable until the operation is complete.

1. In **Maintenance > Tools**, click **Check Filesystem**.
2. From the drop-down list, select the **volume** (Traditional RAID) or **storage pool** (DynamicRAID) to be checked.
3. Choose the **type** of repair operation:
 - **Do not repair errors (generates log messages only)** – Checks for errors, but does not repair them. It is recommended that you do this periodically, especially following a power outage or any other unconventional incident.
 - **Repair errors** – Repairs standard filesystem errors. It is recommended that you run this level if you suspect filesystem damage may have occurred (for example, if a previous **Do not repair errors** operation reported filesystem errors).
 - **Repair errors (aggressive)** – Attempts to repair severe filesystem corruption.

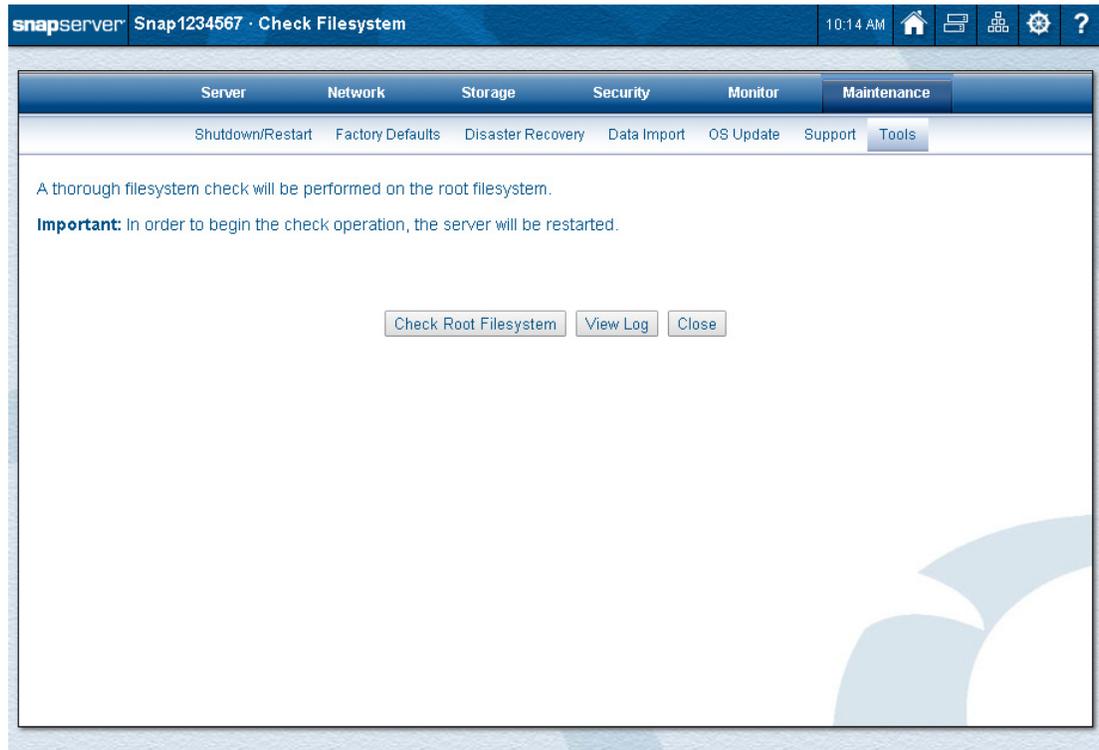
 **CAUTION:** It is only recommended that you run this level if you have been advised to do so by SnapServer Technical Support, or if **Repair errors** has failed to solve the problem and you are willing to risk loss of data.

4. Click **Check Filesystem**.
Checking a filesystem may require a reboot of the server in some circumstances. If prompted that a reboot is required, click **Yes**.

5. To view a log of the results, click the **View Log** button after the filesystem check completes.

To Check the Root Filesystem

Checking the Root Filesystem (**Maintenance > Tools > Check Root Filesystem**) provides a thorough filesystem check on the root.



 **CAUTION:** Checking the root filesystem requires a reboot of the server.

1. In **Maintenance > Tools**, click **Check Root Filesystem**.
2. On the page that opens, click the **Check Root Filesystem** button.
3. Click **Yes** when informed that a reboot is required.
4. After the server reboots, to view a log of the results, click the **View Log** button.

The GuardianOS site map provides links to all the web pages that make up the Web Management Interface. It also provides, in the last column, special links to higher level options and processes which is the focus of this chapter.

These options are also directly navigable from the various menus in the Web Management Interface, and Home, Snap Finder, SnapExtensions, Site Map, and Help are accessible from any page by clicking their respective icon in the top right corner of the screen (see the table in Chapter 2, “Server Status and Site Map,” on page 19).

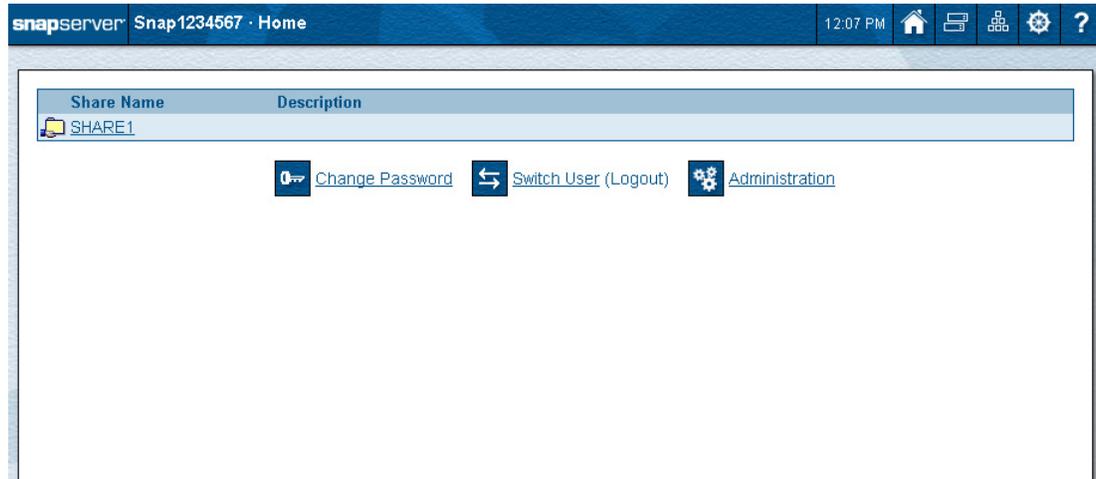
snapserver						
Server	Network	Storage	Security	Monitor	Maintenance	Misc.
Server Name	Information	Storage Guides	Security Guides	System Status	Shutdown/Restart	Administration
Date/Time	TCP/IP	RAID Sets	Shares	Active Users	Factory Defaults	Home
SSH	Windows/SMB	> Create RAID	> Create Share	Open Files	Disaster Recovery	SnapExtensions
UPS	Apple/AFP	> RAID Settings	Local Users	Event Log	Data Import	Snap Finder
Printing	NFS	> Global Spares	> Create Local User	Tape	OS Update	> Snap Finder Properties
	LDAP/NIS	Volumes	> Password Policy		> Update Notification	Change Password
	FTP	> Create Volume	Local Groups		> Check for Updates	Mgmt. Interface Settings
	SNMP	Quotas	> Create Local Group		> OS Update Status	
	Web	Snapshots	Security Models		Support	
	ISNS	> Create Snapshot	ID Mapping		> Registration	
		> Snapshot Schedules	Home Directories		Tools	
		> Snapshot Space			> Email Notification	
		iSCSI			> Host File Editor	
		> Create iSCSI Disk			> Add Host	
		> VSS/VDS Access Control			> Check Filesystem	
		Disks			> Check Root Filesystem	

Topics in Misc. Options

- [Home Pages](#)
 - [Home Page](#)
 - [Administration Page](#)
- [SnapExtensions](#)
 - [BitTorrent Sync](#)
 - [CA Antivirus](#)
 - [Snap EDR](#)
- [Snap Finder](#)
 - [Snap Finder Properties](#)
- [Change Password](#)
- [Mgmt. Interface Settings](#)

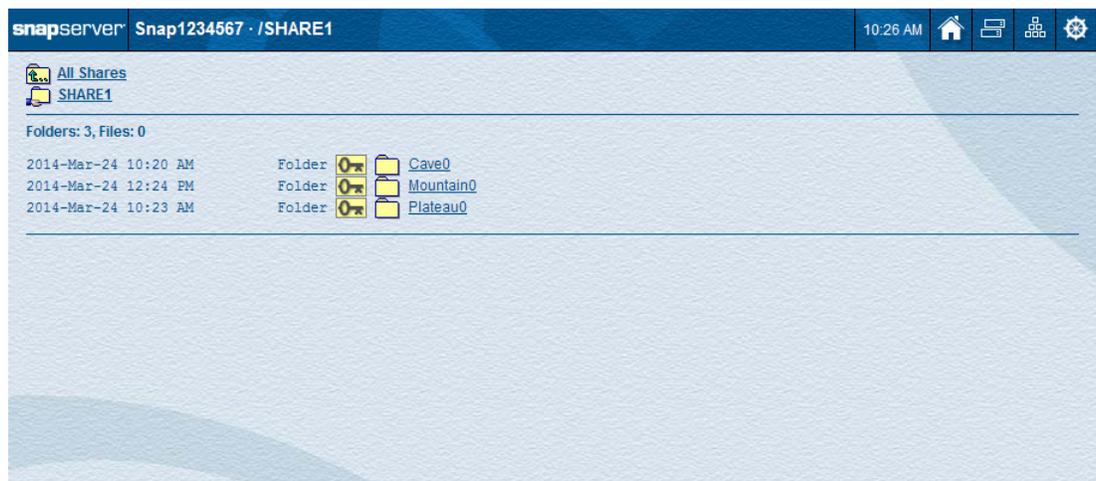
Home Pages

When you first launch the GuardianOS Web Management Interface, the **Home** page is displayed showing any existing shares and three options. Once logged in using the **Administration** link, you can switch between the **Home** page and the **Administration** page using the Home page () icon on the button bar.



Home Page

The Web Management Interface **Home** page displays a list of all shares to which the user has access and three options. Users can navigate the share structure to locate and view or download files without logging in but they cannot modify or upload files.



For users with admin rights, a key icon () appears next to the file/folder on the share. Clicking this icon displays a popup box with security information about the file/folder.

This page also provides three key administrative function links:

- **Change Password** () – Takes you to the **Change Password** page where you can change your administration password. Enter your **User Name** and **Current Password** for access. See [Change Password](#) on [page 215](#).

Enter your user name, current and new passwords, and then click OK.

Important: Passwords are case-sensitive.

User Name

Current Password

New Password

Confirm New Password

OK Cancel

- **Switch User (Logout)** (↔) – Automatically logs out the current user and displays the **Login** page for the new user to gain access to the SnapServer.

Login

User Name

Password

Login

- **Administration** (⚙️) – Displays the **Administration** page (see [Administration Page](#) on page 208). You will be prompted to log in if you have not already done so.

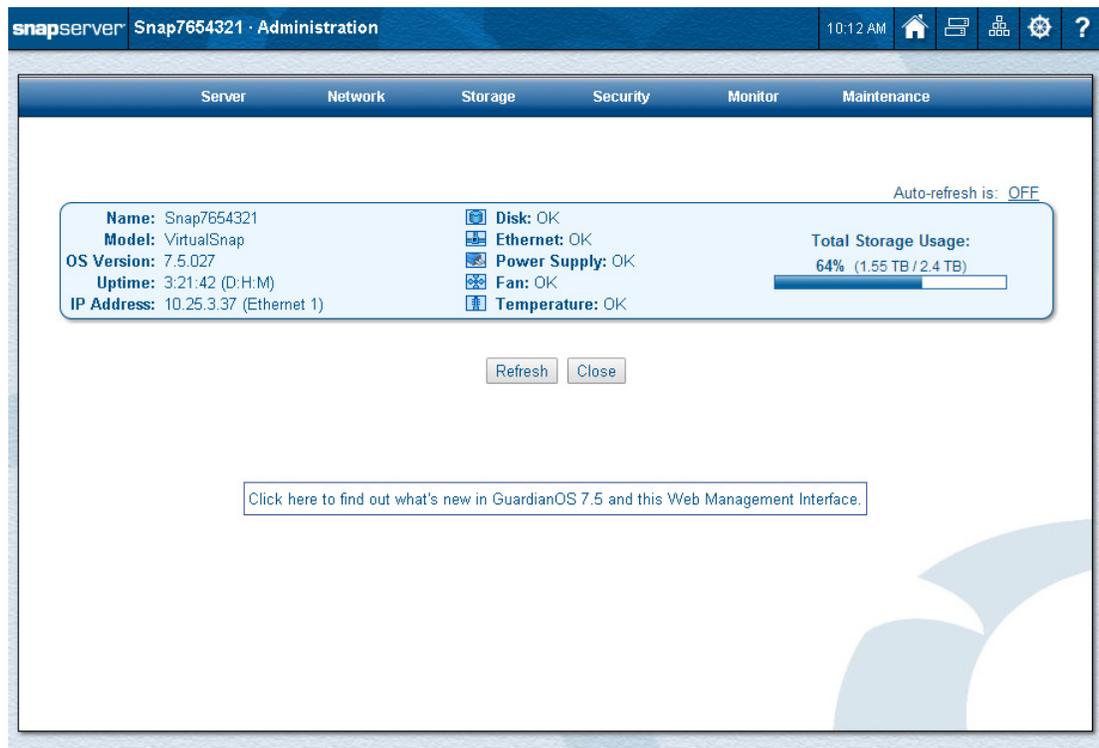
If any of the following conditions are present, you may not be able to access the Home page:

- **Require Web Authentication** is enabled (via **Network > Web > Require Web Authentication**) and you do not have a valid user name and password on the server.
- The server has not completed the **Initial Setup Wizard** (if this is the case, you will not be able to access the **Administration** page of the Web Management Interface either).
- **Web Root** is enabled (via **Network > Web > Enable Web Root**).

Administration Page

The **Administration** page is accessible by clicking either the **Administration** link in the Site Map or the Administration (⚙️) or Home page (🏠) icons on the **Home** page. If web root is enabled, it can also be accessed directly by entering the address `http://servername/sadmin` in a web

browser. It provides a high-level view of the SnapServer status, the amount of total storage being used, and a link to find out what's new in GuardianOS by accessing online help. The tabs at the top provide access to the various functions and features of the GuardianOS.



The **Auto-refresh** link on the right just above the Server Status box lets you select **ON** or **OFF**. When Auto-refresh is **ON**, the site information is automatically refreshed every 5 minutes, and an Auto-refresh icon (🔄) is displayed on the right corner just above the Server Status Box. Click the icon (or **Refresh**) to manually refresh the information.



From the **Administration** page, clicking  takes you to the **Home** page.

SnapExtensions

The SnapExtensions icon () opens the SnapExtensions page. This page is used to manage the SnapExtensions installed on your SnapServer.



If any SnapExtensions are installed, you can click the SnapExtension name in the left column of the table to display the management page for that extension.

BitTorrent Sync

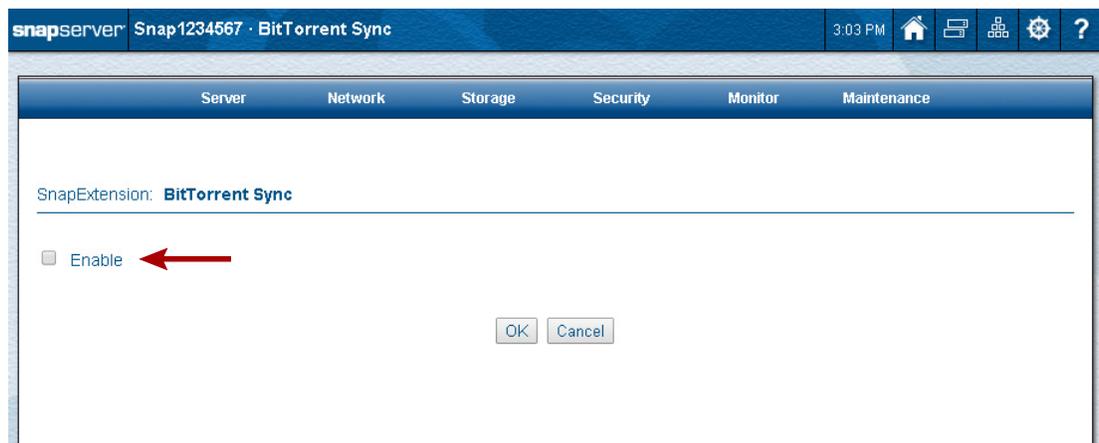


CAUTION: BitTorrent Sync bypasses share and file security. Be sure to only share data that is intended to be accessible by any user with the folder secret.

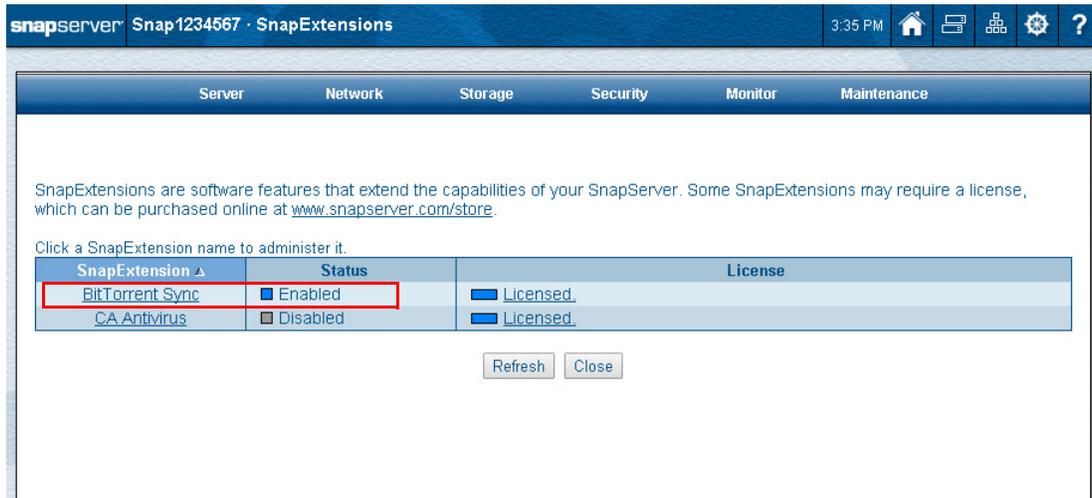
NOTE: Cookies must be enabled on your browser for BitTorrent Sync to work.

BitTorrent Sync (BTSync) is a SnapExtension that is preloaded on SnapServer. It lets you share and sync an unlimited number of files and folders of any size across multiple platforms. For more information, visit <http://www.bittorrent.com/sync>.

1. On the **SnapExtensions** page, click the **BitTorrent Sync** name in the table to access the configuration page.
2. At the next page, check **Enable** and click **OK**.



3. At the following page, to accept the BitTorrent Terms of Use, End User License Agreement (EULA), and Privacy Policy so you can run BitTorrent Sync, click **I Accept**.
4. When returned to the **BitTorrent Sync** page, use the **Configure BitTorrent Sync** link to configure it for your use.
Once enabled, you can return later to configure BitTorrent Sync by clicking **BitTorrent Sync** on the **SnapExtensions** page or on the Site Map.
5. When done, click **OK** to fully enable it.



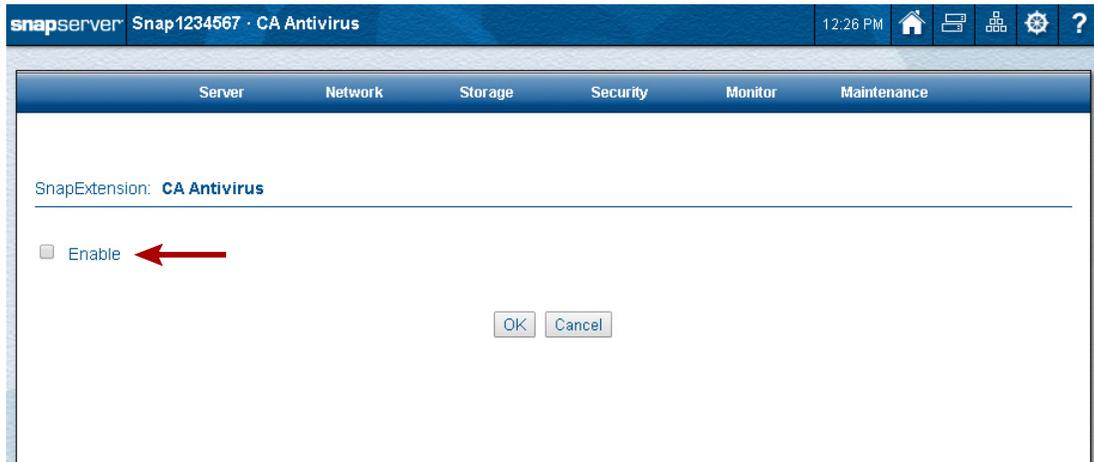
NOTE: To turn off (disable) the BitTorrent Sync feature, uncheck the BitTorrent Sync box.

BitTorrent Considerations

- For the most recent information and details on configuration and use, refer to the BitTorrent Sync documentation (available on their web site).
- In addition to Desktop and Server platforms, there are BitTorrent Sync mobile apps to make synced documents available on iOS, Android, Windows Phone 8, and Kindle Fire systems. Refer to the BitTorrent Sync documentation (available on their web site) for details on configuration and use of BitTorrent Sync on mobile apps.
- BitTorrent Sync can't be used to replicate snapshots because it requires the ability to write to the sync location (and snapshots are read only).
- BitTorrent Sync installs as a hidden directory on a volume (Traditional RAID) or storage pool (DynamicRAID). If the volume or storage pool is deleted or rolled back from a snapshot, the SnapServer attempts to automatically relocate the BitTorrent Sync install directory to another volume or storage pool. If there are no more volumes or storage pools, or if none can be found that are large enough, BitTorrent Sync is disabled and cannot be re-enabled until a suitable volume or storage pool becomes available. Once re-enabled, BitTorrent Sync must be completely reconfigured again.

CA Antivirus

For **CA Antivirus**, click the box to enable it.



For more information, see [Chapter 11 - CA Antivirus Software](#).

Snap EDR

For **SnapEDR**, at the **Configuration** page, select either to configure it as the Management Console or as an Agent of another Management Console. If configuring it as an Agent, enter the **Name or IP of the Management Console**.



After SnapEDR finishes its configuration, the Management Console screen is shown on the Configuration page:



Snap Finder

Snap Finder () is a powerful tool that lists all the SnapServer and REO 4600 appliances on your network and on a remote network segment if so configured, and shows the current status. Click the server name (if you have server name resolution) or IP address of a server to access it through the Web Management Interface.

NOTE: You can sort the columns (ascending or descending order) by clicking the column head.

Server	Status	IP Address	OS Version	Model	Number	Avail Cap.	Total Cap.
at-ros40Diamond	Online	10.25.12.60	ROS 4.0.0.autobuild_Mar04@10:40	-	-	3.42 GB	3.99 GB
beryl	OK	10.25.2.189	GOS 7.2.130	DX1	2300028	4.34 TB	4.34 TB
BlueBottle	OK	10.25.6.18	GOS 7.5.0.jwinfieldsled11	DX2	2415534	7.18 TB	7.18 TB
bm-diamond	Online	10.25.12.230	ROS 4.0.0.briansled11	-	-	28.44 GB	30.89 GB
bmgos5	OK	10.25.2.49	GOS 7.5.0.briansled11	VirtualSnap	15459346	6.08 GB	6.09 GB
bmgos6	OK	10.25.6.33	GOS 7.5.0.briansled11	VirtualSnap	5900192	5.40 GB	6.09 GB
bmgos7	OK	10.25.2.155	GOS 7.5.0.briansled11	VirtualSnap	13478958	6.09 GB	6.09 GB
bmgos8	OK	10.25.2.230	GOS 7.2.130	VirtualSnap	15922671	5.59 GB	6.09 GB
bobbert	OK	10.25.2.178	GOS 5.0.133	4400	1723986	128.16 GB	280.71 GB
CB-110-SJSE	OK	10.25.3.59	GOS 6.5.029	110	2252267	548.71 GB	549.00 GB
CB-Meadowhawk	OK	10.25.2.108	GOS 7.2.128	DX2	2415100	449.41 GB	449.87 GB
CB-Sundragon	OK	10.25.15.60	GOS 7.2.128	DX2	2413126	892.05 GB	1.39 TB
CCCloudDX2	Online	10.25.17.230	ROS 4.1.0.steph-sles11-kdb	-	-	19.23 TB	21.58 TB
CCWAVE410	OK	10.25.2.152	GOS 5.2.067	410	2250681	527.00 GB	836.12 GB
CCWave412	OK	10.25.17.87	GOS 6.5.029	410	2277760	3.39 TB	4.36 TB
CLW240	Online	10.25.12.240	GOS 4.1.021	-	-	6.29 TB	6.39 TB
daedalus	OK	10.25.10.32	GOS 7.2.117	DX1	2302760	1.40 TB	2.00 TB
devqa	OK	10.25.11.2	GOS 6.5.029	N2000	730062	2.68 TB	2.70 TB
JH-VM1	OK	10.25.3.30	GOS 7.2.114	VirtualSnap	2198929	106.61 GB	107.01 GB
kimCluster	Online	10.25.12.46	ROS 4.1.0.kpdevel	-	-	3.06 GB	3.99 GB
lambtron	OK	10.25.10.165	GOS 7.2.117	DX1	2301024	1.18 TB	2.00 TB
LittleJim	Online	10.25.12.85	ROS 4.1.0.jwinfieldsled11	-	-	7.78 TB	7.79 TB
MarcScale	Online	10.25.12.30	ROS 4.1.0.mdorsasled11	-	-	5.66 TB	5.67 TB
MDorsa-N2000	OK	10.25.2.77	GOS 6.5.022	N2000	730054	1.87 TB	1.93 TB
MDorsa-VM	OK	10.25.2.44	GOS 7.2.0-mdorsasled11	VirtualSnap	5269698	2.36 GB	2.36 GB
MyHWCluater	Online	10.25.12.10	ROS 4.1.0.mfsdev1	-	-	8.97 TB	10.64 TB
MyVMCluater	Online	10.25.12.15	ROS 4.0.0.mfsdev1	-	-	38.84 GB	110.74 GB

The following table details the columns in the table:

Identification	Description
Server	Current name of the server. The default server name is SNAPnnnnnnn, where nnnnnnn is your server number (for example, SNAP1234567).
Status	The status of the server (for example, OK, fan failure, or power failure).
IP Address	The IP address of the server.
OS Version	The version of GuardianOS currently loaded on the SnapServer.
Model	The SnapServer model.
Number	The Server Number derived from the MAC address of the primary Ethernet port, used as part of the default server name.
Avail Cap.	The available capacity on the server.
Total Cap.	The total capacity on the server.

NOTE: To enable remote discovery of SnapServers on a different subnet or to display a warning icon for servers with an enabled Ethernet port that has no link, click the **Properties** button at the bottom to open the **Snap Finder Properties** page. For details, go to [Snap Finder Properties](#) on page 214.

Snap Finder Properties

Anyone with administrative privileges can view or edit the Snap Finder properties. Click the **Properties** button to access the **Snap Finder Properties** page.

The screenshot shows the 'Snap Finder Properties' configuration page. At the top, the browser title is 'snapserver Snap1234567 - Snap Finder Properties'. The page includes a navigation bar with icons for home, search, and help, and a clock showing 12:30 PM. The main content area contains the following elements:

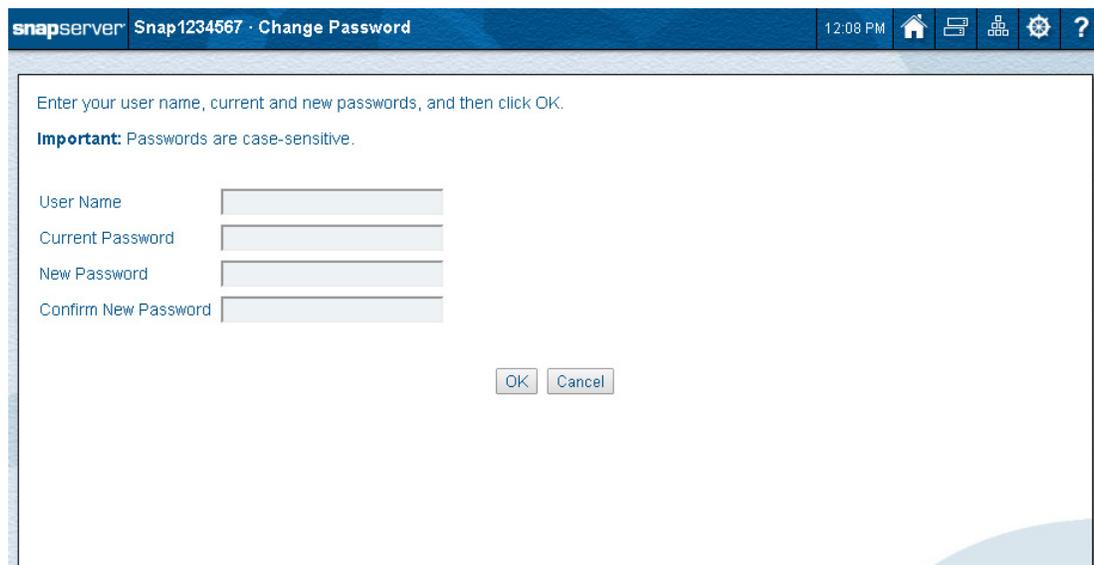
- A checkbox labeled 'Display a warning if any of a server's Ethernet ports have no link.' which is currently unchecked.
- Text explaining that remote discovery servers are SnapServers outside the local network segment, and adding them provides a list of discovered servers.
- A **Note:** 'It may take several minutes for the remote servers to be scanned.'
- A checked checkbox labeled 'Enable Remote Server Discovery'.
- A list box titled 'Remote Discovery Servers (0)' containing '(none)'. Below the list box are 'Add' and 'Delete' buttons.
- At the bottom, there are 'OK' and 'Cancel' buttons.

From this screen you can select to display a warning icon for servers with an enabled Ethernet port that has no link and enable remote discovery of SnapServers on a different subnet. Complete the following fields and then click **OK** to save your changes and return to the Snap Finder screen:

Option	Description
Display a warning...	Check this box to display a warning icon in the Status column for any servers that have an enabled Ethernet port with no link. By default, this box is unchecked.
Enable Remote Server Discovery	Check this box to enable remote discovery of SnapServers on a different subnet.
Add	To add a server, enter the server's host name or IP Address in the field to the right of the Add button, and click Add to incorporate it into the list of Remote Discovery Servers.
Delete	To delete a server, select a server in the Remote Discovery Servers field and click Delete .

Change Password

To enhance the security of your SnapServer, it is recommended that users change their passwords regularly using the **Change Password** page (**Home > Change Password**).



Enter your user name, current and new passwords, and then click OK.

Important: Passwords are case-sensitive.

User Name

Current Password

New Password

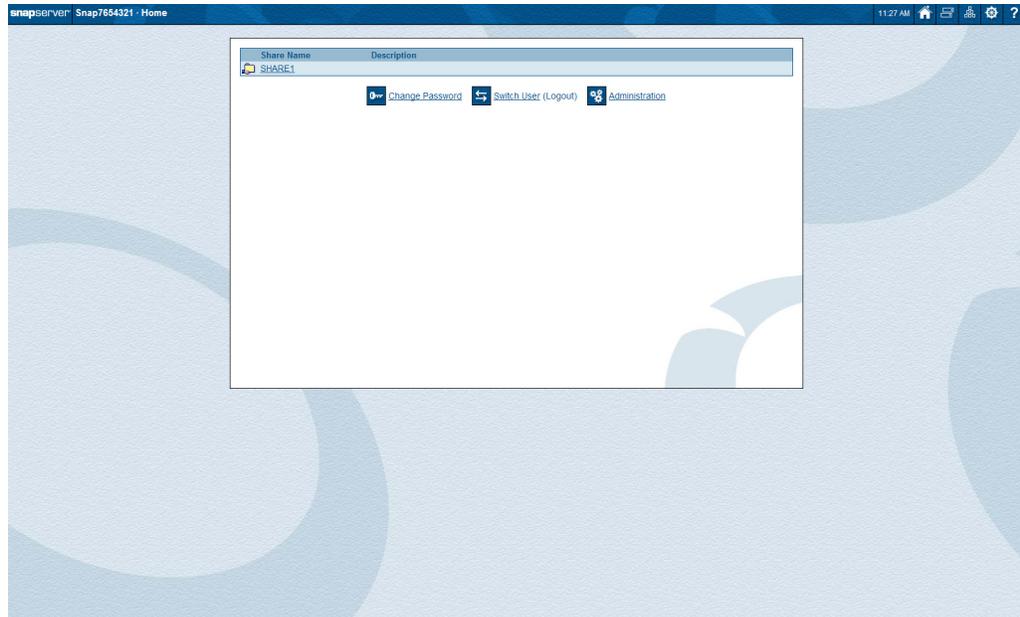
Confirm New Password

Change Your Password

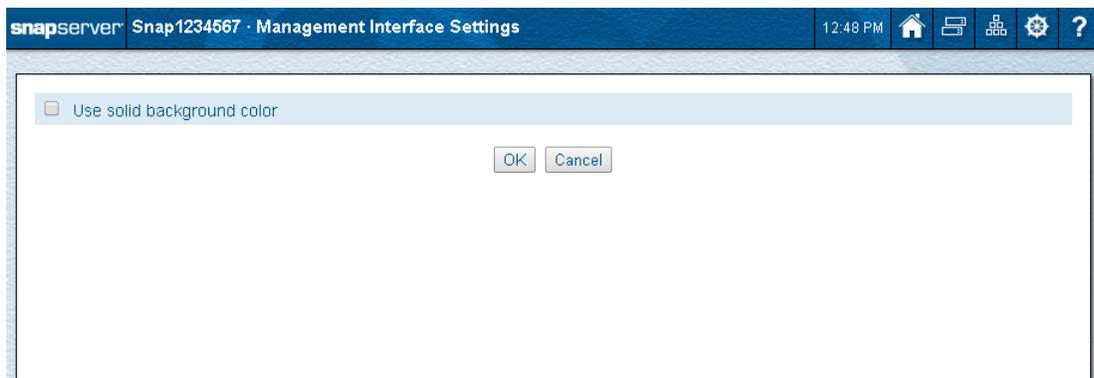
1. On the **Home** page, click the **Change Password** link ().
2. At the **Change Password** page, enter your **User Name** and **Current Password**.
3. Enter and confirm your **new password**.
Passwords are case-sensitive. Use up to 15 alphanumeric characters without spaces.
4. Click **OK**.

Mgmt. Interface Settings

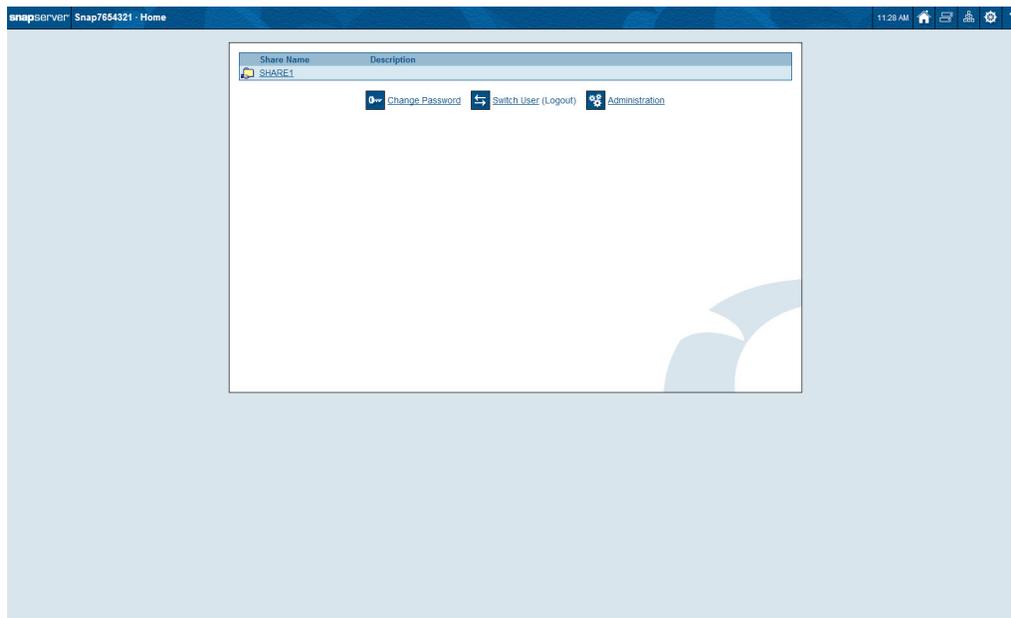
The Web Management Interface default background is light blue with the stylized “O” symbols on a textured blue background:



This can be changed to a solid blue background on the Web Management Interface Settings page by clicking the Site Map icon (⚙️) to access **Management Interface Settings**.



Check the **Use solid background color** and click **OK** to change to the solid background:



To convert back to the stylized background, clear the checkbox.

The CA Antivirus software is preinstalled on all GuardianOS SnapServers. By default, the software is enabled on most SnapServers, but no scan jobs or signature updates have been scheduled. (The server will, however, check for signature updates whenever the server boots.) These and other antivirus configuration and management tasks are performed using the CA Antivirus GUI, accessed from the **SnapExtensions > CA Antivirus** page of the Web Management Interface. This section outlines the major steps in configuring the antivirus software. See the GUI online help for detailed descriptions of all options.

Topics in CA Antivirus Software:

- [Antivirus Dependencies](#)
- [Launching the CA Antivirus GUI](#)
- [The Local Scanner View](#)
- [Scan Jobs](#)
- [Signature Updates](#)
- [Alert Options](#)
- [The Move Directory](#)
- [Log View](#)

NOTE: Antivirus functions or options not relevant to the SnapServer have been disabled in the CA Antivirus configuration GUI.

Antivirus Dependencies

The SnapServer implementation of CA Antivirus software includes the following features:

HTTP Access and Antivirus Configuration . To access the CA Antivirus configuration interface, HTTP must be enabled on the **Network > Web** page.

Resetting the Server Date and Time. If the current server date and time are changed to an earlier date and time (**Server > Date/Time**), the change does not automatically propagate to any scheduled antivirus operations. To synchronize scheduled antivirus operations with the new date and time settings, you must reschedule each operation.

NOTE: New jobs may be affected by the time change. Be sure to check that new jobs have been executed if a date or time change has been made to the server.

Storage Configuration and the Antivirus Software . The antivirus software resides on the largest volume (that existed at the time the software was installed). If you delete this volume, the CA Antivirus software will also be deleted. The SnapServer automatically reinstalls the antivirus software on the largest remaining volume on the system.

NOTE: The antivirus re-installation process does not preserve custom antivirus configuration settings. Make a note of any such settings before deleting a volume.

Launching the CA Antivirus GUI

The CA Antivirus software on SnapServers is enabled by default. Some situations, such as deleting a volume or performing an upgrade procedure, may require you to re-enable the software. To learn how the antivirus software interacts with other GuardianOS software components, see [Antivirus Dependencies](#) on [page 218](#).

NOTE: Antivirus functions or options not relevant to the SnapServer have been disabled in the configuration GUI;

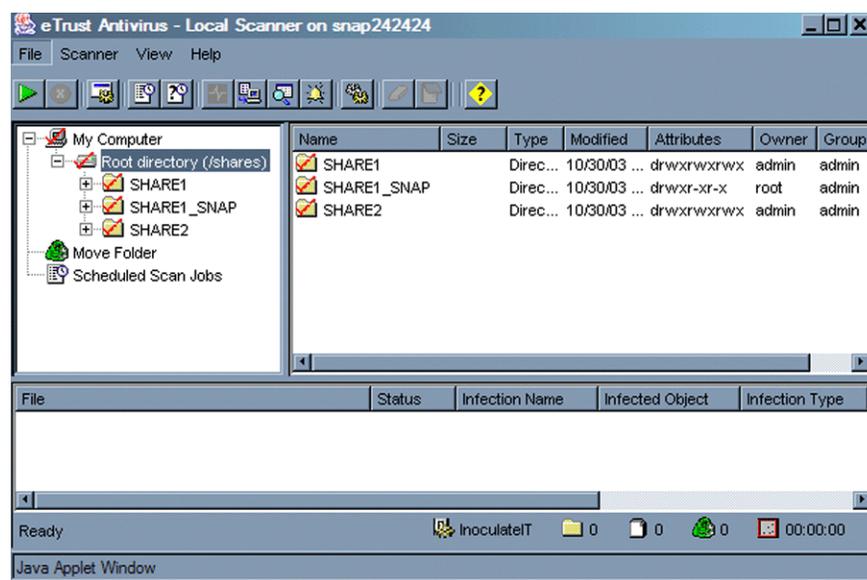
Launching the CA Antivirus Browser Interface

The first time you connect to the CA Antivirus GUI, it may take from 30 seconds to several minutes for the application to load, depending on the speed of your connection.

1. If you need to enable the antivirus software, go to **SnapExtensions > CA Antivirus**, click the checkbox next to **Enable**, and click **OK**.
2. Click the **Configure Antivirus** link. The splash page opens first, followed momentarily by the GUI login dialog box.
3. Enter the same administrative user name and password (case-sensitive) you have established for the GuardianOS Web Management Interface, and then click **Login**. The antivirus GUI box opens.

The Local Scanner View

Use the **Local Scanner** view to scan a SnapServer for infected drives, folders, files, or disks on demand.



Component	Description
Root Directory	Displays the directory structure of the SnapServer. As in Windows Explorer, click folder icons to navigate the structure and display subfolders and files in the right-hand pane.
Move Folder	May contain infected files. The administrator can instruct the software to automatically move infected files to this directory. For more information, see Scan Jobs on page 220 .
Scheduled Scan Jobs	Scan Jobs you schedule appear in this folder. For more information, see Scheduling a Scan Job on page 221 .

Scan Jobs

You can run scan jobs on demand or you can configure scan jobs to run periodically. This section outlines the process of configuring and running manual and scheduled scans. For detailed descriptions of all scanning options, see the CA Antivirus online help.

NOTE: You may not want to include Snapshot shares as part of your virus scan. Because access to an archived version of the filesystem provided by a snapshot share is read-only, you cannot treat or move any infected file; you would have to delete the entire snapshot to effect a cure. A more useful approach is to always scan your filesystem for viruses before running a snapshot. Adjust your antivirus scan schedule to synchronize with your snapshot schedule so that any infected files are cured (repaired) or removed before the snapshot is scheduled to run.

Defining Scan Jobs

This section provides an overview of the major choices available in configuring scan jobs. Access these options by selecting **Local Scanner Options** from the Scanner Menu.

Choosing an Infection Treatment (Scan Tab)

You can instruct the software to perform one of the following file actions when an infected file is found:

File Actions	Description
Report Only	(Default) Reports when an infection is found.
Delete File	Deletes an infected file.
Rename File	Renames an infected file with an AVB extension. Infected files with the same name are given incremental extensions (for example, FILE.O.AVB, FILE.1.AVB, and so on). After a file is renamed with an AVB-type of extension, it is not scanned subsequently.
Move File	Moves an infected file from its current directory to the Move directory for quarantine.
Cure File	Attempts to cure an infected file automatically. Choosing this setting enables the File Options button. Click this button to display the Cure Action Options and specify how the Cure File option performs.

NOTE: The *System Cure* option is not available on SnapServers.

Setting the Type of Files to Scan (Selections tab)

Use the Selections tab options to choose the types of objects to scan, the types of file extensions to include or exclude from a scan, and the types of compressed files to scan.

- **File Extensions** – You can choose to scan files regardless of extension, or select specific types of extensions to include or exclude.
- **Compressed Files** – To scan compressed files, select the **Scan Compressed Files** checkbox, and then click **Choose Type** to specify the compressed file extension types.

Filtering File Information for Logs (Manual Scans Only)

You can specify the types of events that are written to a log. Check the **Infected files** option to put information in the log about files that are found to be infected. Check the **Clean files** option to put information in the log about files that are scanned and are not infected. Check the **Skipped files** option to put information in the log about files that have been excluded from the scan.

Running a Manual Scan Job

Before running a local scan job, confirm that the scanner options are correctly configured as described in the previous section [Defining Scan Jobs](#) on [page 220](#).

Step 1: In Local Scanner View, select the folders you want to scan.

The left-hand pane displays the directory structure of the SnapServer. A red check mark on a folder or file indicates that it is selected for scanning. (By default, all directories and files are selected for scanning.) Click folders or files to toggle file/folder selection on or off.

Step 2: Run the scan.

Select **Scanner > Start Scanning**. The interface is unavailable for further configuration while the scan is in progress. The scan results display in the lower pane of the Local Scanner View, and the action taken with each file is listed in the Status column.

Scheduling a Scan Job

A scan job is configured and scheduled in the **Schedule New Scan Job** dialog box. To open this dialog box, select the **Scanner > Schedule Scan Job > Create** command.

Step 1: Set scan options in the Scan and Selection tabs.

These options are summarized in [Defining Scan Jobs](#) on [page 220](#).

Step 2: Schedule the scan.

The Schedule tab allows you to set a start date and a repeat interval for the scan.

Step 3: Select the directories to scan.

The Directories tab lists all paths that currently exist on the server. You can remove or add new paths as desired. You can also use the Exclude Directories tab to achieve the same result.

Step 4: Click OK.

You can view scheduled scan jobs by clicking the **Scheduled Scan Jobs** folder in the Local Scanner View. To edit a job, right-click it and select **Options**.

Signature Updates

Signature updates contain the latest versions of the signature files that recognize the latest infections. They also contain the latest engine versions, which do the work of looking for infections. Signature updates are made available on a regular basis by Computer Associates.

These updates are cumulative, so they contain everything from all previous file updates, plus the newest information on the latest infections. If you have missed a recent update, you only need to collect the latest signature file to have the most up-to-date protection.

SnapServers are preconfigured to download signature updates from the CA FTP site at <ftp://ftpav.ca.com/pub/inoculan/scaneng>. By default, no signature updates are scheduled. The antivirus software will, however, check for signature updates whenever the server is powered on. To update SnapServers that do not have Internet access, the following methods are available:

Method	Description
FTP	Use FTP to download the update files from the Computer Associates FTP site. You can also use FTP to distribute signature updates from one SnapServer (or any FTP server) to another. NOTE: When using FTP, the user name and password are passed as clear text.
UNC	Use UNC to distribute signature updates from one SnapServer to another (or from any arbitrary SMB or Windows server). Note that for UNC to work, you must have the Enable Guest Account option enabled (Network > Windows/SMB) on the SnapServer on which the signature updates reside. NOTE: Alternatively, you can distribute updates to SnapServers from any Windows/SMB server. If using this method, make sure the guest account on the chosen server exists, is enabled, and has a blank password.
Local Path	As part of the procedure to provide signature updates to the SnapServer with no Internet access, you can connect to a local path relative to the root (for example, <code>/shares/SHARE1/virusdefs</code>). Note that the path to the share is case-sensitive.

Updating SnapServers with Internet Access

If your SnapServers have direct access to the Internet, you only need to schedule the downloads to set up automatic signature updates. If access to the Internet is routed through a proxy server, you may also need to specify the name of the proxy server. Both procedures are explained below:

To Schedule Signature Update Downloads

1. Choose **Scanner > Signature Update Options**.
2. On the Schedule tab, click **Enable Scheduled Download**. Select the initial download date and time, then select how often to repeat the download.
3. Click **OK**.

To Specify a Proxy Server

1. Navigate to **Scanner > Signature Update Options**, and click the **Incoming** tab.
2. Select **FTP** in the list box, then click **Edit**.

3. In the Proxy Name field, enter the IP address of the proxy server, then click **OK**.

Updating a SnapServer without Internet Access

If you have SnapServers that do not have Internet access, use the following procedures to download the signature files to a machine with Internet access and then copy them to the SnapServer.

NOTE: When retrieving signature updates, the antivirus software attempts to connect to all the sites in the site list in the order they are listed. To avoid delays or superfluous error messages, delete the default FTP option from the list on SnapServers that have no Internet access.

1. Using a workstation with Internet access, go to <ftp://ftpav.ca.com/pub/inoculan/scaneng> and download the following **files**.
 - All ***.tar** files containing the word *Linux*, for example, *fi_Linux_i386.tar* and *ii_Linux_i386.tar*
 - All ***.txt** files containing the string *Sig*, for example, *Siglist.txt* and *Siglist2.txt*
2. Using a method appropriate to your environment, copy the **update files** to the SnapServer.
3. Navigate to **Scanner > Signature Update Options**, and click the **Incoming** tab.
4. Click the **Add** button, then select **Local Path** from the Method drop-down list.
5. In the Path field, enter the path to the directory on the server on which the update file resides. If you are using a SnapServer, the path would be similar to the following:
`/shares/SHARE1/sigfiles`
where *SHARE1/sigfiles* is the share path to the directory containing the signature update files.
6. Click **OK**. The path appears in the list box.
7. Click **Download Now**.

Distributing Updates from One SnapServer to Another

When retrieving signature updates, the antivirus software attempts to connect to all the sites in the site list in the order listed. To avoid delays or superfluous error messages, delete the default FTP option from the list on SnapServers without Internet access.

If you have more than one SnapServer with no Internet access, you can perform the previous procedure on just one of them (or any Windows/SMB server), and then configure your other SnapServers to get the update from that server automatically via SMB by specifying the UNC of the server containing the signature files.

The following conditions must be met in order to distribute updates using UNC:

- The correct **Signature files** must have been downloaded to the root of the share being used for updates.
- The server containing the Signature updates must have the Guest account enabled (**Network > Windows/SMB**) in GuardianOS. For other SMB/CIFS servers, the Guest account must have no password, and there may be additional requirements (for example, Windows servers must allow anonymous connections).
- The share and Signature files must be accessible to the **Guest account**.
- The **server name** used in the UNC must be resolvable by the server running CA Antivirus.

To Distribute Files via UNC

1. Navigate to **Scanner > Signature Update Options**, and click the **Incoming** tab.
2. Click the **Add** button, and select **UNC** in the Method list box.
3. Enter the path to the SnapServer (or Windows/SMB server) to which the update files have been downloaded (see previous procedure) using the following format:
`\\server_name\share_name`
where *server_name* is the name of the server, and *share_name* is the name of the share providing access to the files. (On a SnapServer, the update files must reside on the root of the share.)
4. Click **OK**. The path you entered appears in the **Download Sources** list box.
5. Click **Download Now**.

To Distribute Files via FTP

If you have more than one SnapServer with no Internet access, you can perform the FTP download procedure on just one of them (or any FTP server), and then configure your other SnapServers to get the signature updates from that server automatically via FTP.

1. Navigate to **Scanner > Signature Update Options**, and click the **Incoming** tab.
2. Click the **Add** button, and select **FTP** in the **Method** list box.
3. Enter the following **information** regarding the server on which the update file resides as follows:
 - In the Host Name field, enter the **IP address**.
 - In the User Name and Password fields, enter the admin **user name and password**.
 - In the Remote Path field, enter the **path** to the directory in which the file resides. If you are using a SnapServer, the path would be similar to the following:

```
/shares/SHARE1/sigfiles
```

where *SHARE1/sigfiles* is the share path to the directory containing the signature update files.

4. Click **OK**. The path you entered appears in the Download Sources list box.
5. Click **Download Now**.

Verifying Download Events

Use the following procedure to verify download and distribution events.

1. Select **View > Log Viewer**.
2. In the left-hand pane, select **Distribution Events**. Distribution events are listed in the upper right-hand pane in chronological order.
3. Select a distribution event. The details of the distribution event display in the lower pane.

Alert Options

Alert options allow you to tailor the notification information that is provided to the Alert Manager, cut down on message traffic, and minimize the dissemination of notifications that are not critical. To set alert options, select **Alert Options** from the Scanner menu. The Alert Options dialog box contains the following tabs:

Tab	Description
Report	Use the Alert Report options to specify where to send notification information, and the Report Criteria options to manage how frequently messages from the General Event Log are reported. NOTE: The Local Alert Manager option is not supported on SnapServers.
Alert Filter	Use the Alert Filter options to manage notification severity levels, and to determine what types of messages should be passed to the Alert Manager. NOTE: In the Custom Notification Module, the <i>Realtime Server</i> and <i>Admin server</i> settings have no effect on SnapServers.

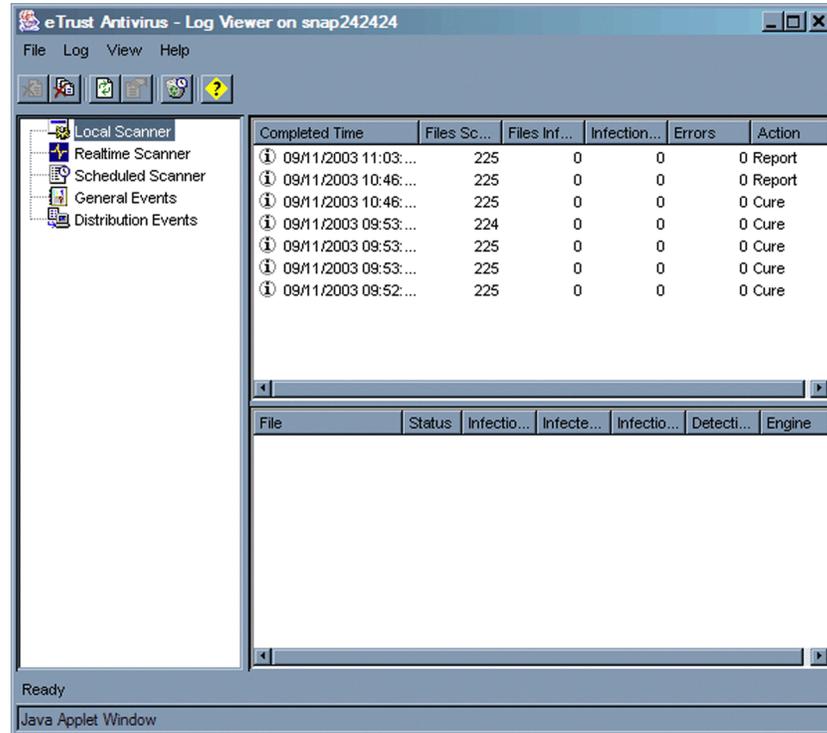
The Move Directory

You can configure scans to move infected files to the move folder (**Scanner > Local Scanner** options). To view infected files, click the **Move** directory on the left-hand pane of the Local Scanner View. To manage a moved file, right-click the file and select from the following options:

Option	Description
Restore	This option removes the file from the Move Folder and restores it to its original location with its original name and type.
Restore as	This option displays a dialog box that allows you to change the directory location and file name. You can rename a file and isolate it safely in a different location. You may want to use this option, for example, if you do not have another source for the data and you need to look at the file. Or you may have a file that you want to analyze. NOTE: To restore a file to a different directory, you must prepend the path to the directory with the string <code>"/shares."</code> For example, to restore a file to the <code>SHARE1/sales</code> directory, enter the path as follows: <code>/shares/SHARE1/sales</code>
Restore and Cure	This option allows you to restore the selected item back to the original folder it was in, and cure it. This option is useful if you update the signature files after items have been put in the Move folder. If a cure is provided that you did not have available, you can get the latest signature update and use this option to restore and cure an infected item.
Delete	This option deletes the infected file; no warning or confirmation message is displayed.

Log View

The Log View provides easy access to detailed information on scan, distribution, and other events. To access this view select **Log View** from the View menu.



Option	Description
Local Scanner	Displays summary information about scan jobs that have run.
RealTime Scanner	Not supported.
Scheduled Scanner	Displays summary information on scheduled scans that have run.
General Events	Displays the Event log for a given day. Click a date to view all events that occurred that day.
Distribution Events	Displays distribution events by date. Click a date to view detailed information on the distribution event in the lower pane.

DynamicRAID Overview

You can configure your SnapServer in either DynamicRAID or Traditional RAID mode. The following section details the benefits of DynamicRAID, as well as providing guidelines to help you choose the mode that is best for your needs.

DynamicRAID is a powerful feature that simplifies storage management and provides additional configuration options not available in Traditional RAID. A SnapServer can be purchased with any amount of initial storage (or number of drives), and more capacity can be added over time by inserting or replacing drives. Volumes can be added and removed at will, and all volumes share the same underlying pool of storage.



IMPORTANT: A SnapServer head unit or expansion unit supports only one storage pool created from its drives and contained within that enclosure. Multiple volumes can be created on that storage pool.

Topics in DynamicRAID:

- [About DynamicRAID](#)
 - [Should I use DynamicRAID or Traditional RAID?](#)
 - [Features Comparisons: DynamicRAID and Traditional RAID](#)
- [Setting Up DynamicRAID](#)
 - [DynamicRAID Implementation](#)
- [Additional Information on DynamicRAID Sizing](#)

About DynamicRAID

- To increase the capacity of the storage pool when the SnapServer is fully populated, you can replace drives, one at a time, with larger-capacity drives. Replacing drives can only be done when the DynamicRAID is healthy.
- DynamicRAID has two forms – one with single parity (protects your data against a single drive failure) and one with dual parity (protects your data against two simultaneous drive failures). The parity model can be changed over time.
- Volumes on DynamicRAID are virtual and may be created almost instantaneously. They all share the same underlying pool of storage, so there is no need to worry about the size of the volume when created. At the administrator's discretion, volumes may be constrained in size so they cannot consume more than a defined limit. This limit can be adjusted or removed as required.

- DynamicRAID is comparable to Traditional RAID for both file-level and block-level access. All of its features apply equally to both file sharing and iSCSI volumes created on the SnapServer NAS system. DynamicRAID uses clear visible indicators on the drive bays to illustrate what can or cannot be done to that bay, thus reducing user error and negating the need for any required skill set or training for operation. Anyone can easily manage and maintain an expandable storage system.

Should I use DynamicRAID or Traditional RAID?

Use the following guidelines and the table on below to help determine which RAID mode is right for you.

Step 1: Determine how much time and effort you want to spend managing your RAID configuration.

- If you have **little or no time** to manage your RAID solution, choose DynamicRAID.
- If you want to have more **direct control** over your storage configuration, conduct **manual tuning**, and **manually manage the RAID array**, choose Traditional RAID.

Step 2: Determine what kind of storage configuration you need.

- **Will storage requirements in your environment change over time?**

If so, DynamicRAID provides you with the flexibility to respond to these changing needs. For example, you can upgrade smaller drives to larger drives one by one. These drives will be automatically incorporated and will share the same storage pool.

If you plan to add disk drives, you can take advantage of the ability to change parity when you do so. You can optimize parity based on the number of drives inserted into the system. You can either increase parity by adding a new drive, or decrease the parity setting to expand storage space (and sacrifice redundancy).

- Do you want to aggregate all disk storage on the head unit and attached expansions?
If you do, choose Traditional RAID.
- **Do you need to use local or global spare drives?**
If you do, choose Traditional RAID.
- **Do you need to use user or group quotas?**
If you do, choose Traditional RAID.

Step 3: Will you need to choose your RAID type?

If it is necessary for you to choose your specific RAID type, select Traditional RAID. For example, you may want maximum speed but no redundancy, and thus want RAID 0.

For more information on RAID types, see the [GuardianOS Specifications](#) table in [Chapter 1](#), as well as [Factors in Choosing a RAID Type](#) in [Chapter 5](#).

The following table summarizes some of the prospective decision factors in choosing DynamicRAID or Traditional RAID. This list is not exhaustive.

Choosing DynamicRAID or Traditional RAID

Feature	DynamicRAID	Traditional RAID
I need a simple, scalable, flexible RAID solution that takes little or no effort to manage.	X	
I need to easily add more storage capacity as needed.	X	
I need to be able to change the parity level over time.	X	
I need to be able to adjust volume size as needed.	X	
I need to be able to optimize parity based on the number of drives inserted into the system.	X	
I need the SnapServer to configure and manage the RAID array size and parity.	X	
I need to manually configure the RAID array.		X
I need to manually tune my storage system for specific needs, such as RAID levels and/or storage types.		X
I need user or group quotas.		X
I need to mix different drives in the same chassis, and then group these different drives together to make a homogeneous RAID.		X
I need the filesystem to span multiple chassis.		X
I need local and global spares.		X
I need to do snapshot rollbacks.		X

Features Comparisons: DynamicRAID and Traditional RAID

The following table compares the features of these two RAID types:

Feature	DynamicRAID	Traditional RAID
RAID Levels	Single- or dual-parity options that can be changed dynamically.	Manually created RAID sets 0, 1, 5, 6, or 10. Must delete and recreate to change.
RAID Creation	Automatic after selection of parity. Snapshot space is configured by the user.	Manual selection of drives, RAID set level, and snapshot space.
RAID Expansion	Can be expanded by adding drives to the SnapServer.	Can be grouped with other RAID sets to increase the space available to volumes.
Mixed Drive Capacities	Additional capacity on larger drives can be utilized within the constraints of single- or dual parity protection. Additional capacity on larger drives can be utilized if there are enough larger drives to satisfy the parity configuration of DynamicRAID.	Only the capacity equivalent to the smallest drive is used on each drive in the RAID set.
Mixed Drive Types	All drives in a given Storage Pool must be the same type of drive (for example, SAS 15K).	Different types of drives can be mixed in a head unit or expansion unit (using different RAID sets and volumes).
Volumes	Volumes consume space directly from the storage pool as data is placed on the volume, and allocated as needed.	Volumes allocate from the RAID upon creation of the volume, and volumes must be manually grown to increase space for data as needed.

Feature	DynamicRAID	Traditional RAID
Snapshots	Snapshots are by Storage Pool and can be mounted for individual file recovery.	Snapshots are by volume and can be mounted for either individual file recovery or volume rollback.
Data Storage Capacity	Data storage capacity for all volumes on a storage pool is limited by the size of the storage pool and/or the maximum size that is set on each volume.	Limited by the storage size on the head unit plus all the expansion units.
Filesystem Spanning	Filesystem is limited to a given Storage Pool.	Filesystem can span multiple RAIDs concatenated together using Instant Capacity Expansion (ICE) and RAID grouping.
Quotas/Size Limits	Volume size limits can be either specified or unlimited.	User and Group quotas can be specified for each volume.

Setting Up DynamicRAID

These are the high-level steps to configuring DynamicRAID:

1. During setup, after selecting DynamicRAID, all available **disk drives** on the SnapServer are detected and displayed.
2. Select the **parity** setting:
 - One disk drive – No parity protection only.
 - Two or three disk drives – Single-parity protection only.
 - Four or more disk drives – Choose either single- or dual-parity protection.

The software wizard configures the SnapServer based on the parity selected.
3. Use the following **options** to fine-tune the configuration:
 - **Storage > Storage Pools** (see [Storage Pools](#) in [Chapter 4](#))
 - **Storage > Volumes** (see [Volumes](#) in [Chapter 4](#))
 - **Security > Shares** (see [Shares](#) in [Chapter 7](#))

DynamicRAID Implementation

DynamicRAID streamlines the storage management experience. During the initial setup, when making the RAID Type Selection, choose DynamicRAID and the type of parity desired. The SnapServer automatically configures the RAID array, and the user may optimize the parity according to the number of drives inserted into the system. A storage pool is then created that can be divided into volumes for different applications or user groups. These steps are described in detail in the following sections.

Storage Expansion

During the setup process, storage pools are created on the head unit and each expansion unit using all disk drives available in that unit. More capacity can be added to a SnapServer over time by inserting or replacing drives, then adjusting Storage Pool properties. Volumes can be added and removed at will, and all volumes share the same underlying pool of storage.

When adding drives to a storage pool, the Web Management Interface displays the estimated time required until the new drive will be available for storing data, and an estimate of the final capacity that will be available when it is ready. Once the drive has been added to the Storage Pool, any of the following may take place to maximize capacity:

- The filesystem may be expanded to cover the available space (see [Edit Volume Properties](#) in [Chapter 4](#)).
- The snapshot space may be expanded (see [Adjusting Snapshot Space Size](#) in [Chapter 6](#)).
- Both the filesystem and snapshot space may be expanded within a unit. However, the storage pool on one unit cannot be expanded to a different unit.
- Neither the filesystem nor snapshot space are expanded, but the parity is increased (see [To Add a Disk Drive to Upgrade Parity](#) in [Chapter 4](#)).

When a drive is replaced in the storage pool, DynamicRAID rechecks its size to determine if it is now larger than before the replacement. This way, drives in a DynamicRAID can be replaced with larger drives one at a time, and once enough drives have been replaced with larger drives to support the storage pool's parity setting, the additional space in the larger drives will become available.

Snapshots

DynamicRAID utilizes current GuardianOS technology and snapshots the entire storage pool. Provisioning for snapshots can be increased as the storage pool is grown to ensure the percentage of storage reserved remains consistent. The directories inside the snapshot that represent volumes can be shared individually by the administrator, rather than all at once, to provide a level of access control.

iSCSI Target Volumes

All iSCSI targets use current SnapServer technology. DynamicRAID maintains the iSCSI volumes on the storage pool in a location that is not visible to users.

Indicators

Drives can be inserted into the SnapServer NAS system at any time unless the user is specifically instructed not to do so.

Each drive bay has an associated indicator which can be either red, amber, or green. Indicators show the state of the storage pool. See [LED Indicators](#) in [Appendix D](#).

Additional Information on DynamicRAID Sizing

All the drives in a chassis are considered part of a single storage pool on that unit and are dynamically configured as such. The first drive detected in the storage pool is used as the basis for the drive-size characteristics of the storage pool. These characteristics center around whether the drive space can be evenly divided into either 300 or 500 GB-sized partitions.

For example, a large capacity drive (such as 1 TB and 2 TB SATA drives) will use 500 GB partitions for the storage pool while a smaller capacity drive (such as 300 GB and 600 GB SAS drives) will use 300 GB partitions. Then, all the other drives in the storage pool (or added later) are configured using the same partition sizing.

Drives of different overall capacity may be added to the same storage pool as long as they have the same partition sizing (such as, 300 GB). However, the extra space on larger drives will only be available to the storage pool if there are enough larger drives to satisfy the storage pool's parity setting using the extra space. Otherwise, the extra space will not be available to the storage pool until more drives are added with the same larger capacity.

For example, adding a 3 TB SATA drive to a group of three 1 TB drives with single parity only adds 1 TB (2x500 GB) of space for a total of 4 TB. The extra 2 TB of space on the 3 TB drive is not available until enough 3 TB drives are added to satisfy parity. Adding two more 3 TB drives opens up the additional 2 TB (4x500 GB) of space on all the 3 TB drives. The total storage pool then expands to 12 TB.

For more information on DynamicRAID, go to <http://docs.overlandstorage.com/dynamicraid>.

This appendix provides a brief description of the supported backup solutions and the Snap Enterprise Data Replicator (Snap EDR) software.

Topics in Backup Solutions:

- [Backup and Replication Solutions](#)
- [Snap Enterprise Data Replicator](#)
- [Backup via SMB, NFS, or AFP](#)
- [Off-the-Shelf Backup Solutions](#)
- [iSCSI Disk Backups](#)

Backup and Replication Solutions

GuardianOS supports several backup methods, including third-party off-the-shelf backup applications and applications that have been customized and integrated with GuardianOS on the SnapServer.

- Data and security metadata backup and replication can be performed using the built-in Snap EDR.
- Backup over network file protocols can be performed using various backup packages that can access the server via SMB, NFS, or AFP.
- Backup from the server or to a tape attached to the server can be performed using supported backup agents and media libraries installed on the server.

Snap Enterprise Data Replicator

Snap EDR provides server-to-server synchronization by moving, copying, or replicating the contents of a share from one server to another share on one or more different servers. It comes preinstalled on SnapServers and activates a 45-day free trial if configured as a Management Console.

Snap EDR consists of a Management Console and a collection of Agents. The Management Console is installed on a central system. It coordinates and logs the following data transfer activities carried out by the distributed Agents:

- Replicates files between any two systems including SnapServers, SnapScale clusters, and Windows, Linux, and Mac Agents.
- Transfers files from one source host to one or more target hosts.
- Transfers files from multiple hosts to a single target host, and stores the files on a local disk or locally attached storage device.

- Backs up data from remote hosts to a central host with locally-attached storage.
- Restores data from a central storage location to the remote hosts from which the data was originally retrieved.

Snap EDR Usage

The Snap Enterprise Data Replicator software distribution comes preinstalled on the SnapServer but must first be installed in SnapExtensions and then configured before it's available for use.

All other Snap EDR installations (including another machine running as the Management Console that the server registers to, other Agents that register to a Snap EDR Management Console running on the server, or other Agents replicating to/from the server) need to be able to resolve the SnapServer server name to its IP address in order to interoperate properly with the server. This can be accomplished via a DNS host record, local hosts file entries, or other name resolution services in the environment.

Configuring Snap EDR for GuardianOS

To configure the server as a Snap EDR Management Console or an Agent:

1. Click the **SnapExtensions** icon located in the upper right corner of the Web Management Interface.
2. If necessary, install the **software package**:
 - a. Run the **installation routine** from SnapExtensions. SnapExtensions displays a Snap EDR link and the status **Not Installed**.
 - b. Click the **Snap EDR link** and confirm the installation. Wait for the installation to complete. The SnapExtensions page then displays the Snap EDR Configuration link.
3. Click the **link** to launch the Management Console/Agent configuration page.
4. Select either the **Configure as the Management Console** or **Configure as the Agent** button.

NOTE: If you are configuring the server as an Agent, you must provide the server name (for a SnapServer) or cluster management name of the Management Console (for a SnapScale). The server must be able to resolve the server name of the Management Console to the correct IP address.

5. Once the server is configured, select the following **options** from the page that appears:

Option	Description
Click here to configure jobs	Opens the Management Console where jobs can be scheduled.
Stop Service	Stops all services.
Restart Service	Restarts all services.

 **CAUTION:** Use only if you have encountered a problem, and customer support advises you to restart the service. Any jobs currently running will stop and will not resume when you restart the service.

Scheduling Jobs in Snap EDR

To schedule jobs, click the **Snap EDR** link in the Site Map (under **Misc.**).

For complete information on scheduling jobs in Snap EDR, see the *Snap EDR Administrator's Guide*.

Backup via SMB, NFS, or AFP

A SnapServer can be backed up via standard file server access.

In this configuration, the backup server is set up to use SMB, NFS, or AFP to connect to the server, examine the file system, and then back up the data onto itself. No special agents or media servers are needed.

Off-the-Shelf Backup Solutions

Special Application Notes for installing the backup agent or media servers can be found on the Overland SnapServer Support website (<http://docs.overlandstorage.com/snapserver>).

NOTE: The backup packages shown in the Application Notes do not support the backup of Windows ACLs. If Windows ACL backup is critical, Overland Storage strongly recommends you create a SnapServer disaster recovery image (see *Creating the SnapDRImage and Volume Files* in Chapter 9) before you perform a backup.

iSCSI Disk Backups

iSCSI disks can be backed up from iSCSI clients using any standard backup application on the client operating system. These backups run independently of the SnapServer since the client backs up the contents of the iSCSI disk as if the iSCSI disk were a local hard disk.

Windows clients can make backups of VSS-based snapshots of iSCSI disks using VSS-compatible backup applications. See *iSCSI Disks* in Chapter 6 for instructions.

Using Backup Exec for VSS-based Snapshots of SnapServer iSCSI Disks

To configure Backup Exec to take native VSS snapshots of SnapServer iSCSI disks using Backup Exec's *Advanced Open File* or *Advanced Disk-Based Backup* feature, you must first add a Windows registry entry to the systems running the Backup Exec Server and all of the Backup Exec agents backing up iSCSI disks.

After the Backup Exec Server or agent has been installed, modify the registry to add the SnapServer as a Backup Exec VSS provider:

1. Run the following **command**:

```
regedit
```

2. Navigate to the following **key**:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec For Windows\Backup Exec\Engine\Misc\VSSProviders]
```

- Underneath VSSProviders are other keys numbered sequentially from 0 to some number. Create a new key in VSSProviders named after the highest key value plus 1 (such as, if the highest key value is 9, create a new key value 10).

For example:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec For Windows\Backup Exec\Engine\Misc\VSSProviders]\10
```

- Inside the new key, create three string values:

VALUE NAME	VALUE DATA
ID	{759c7754-6994-46c9-9cf9-c34ac63a0689}
Name	SnapServer VSS Hardware Provider
Version	5.2

- Close `regedit`.

The SnapServer VSS Provider should now be available to Backup Exec to use for VSS-based backups. Return to **iSCSI Disk Backups** main page.

This appendix provides additional information and configuration options about securing and accessing shares and files on the SnapServer. The SnapServer GuardianOS supports share-, file-, and directory-level permissions for all local and Windows domain users and groups.

File and directory security can be configured using either Windows NTFS-style security or classic Unix-style security. The type of security present on a file or directory is its “security personality”.

A computer security model is a scheme for specifying and enforcing security policies.

Files and directories are stored on the server on volumes (or the directories underneath) with a configured “security model.” The security model on the volume governs the permitted security personalities, the default personalities, and the ability to change personalities on child files and directories.

Security models can be configured on volumes in either DynamicRAID and Traditional RAID mode. For DynamicRAID, the security models can only be on the top-level volumes. With Traditional RAID, the directories immediately underneath the top-level volume directory can also be configured with a security model and are known as “security model directories”.

The default security model on newly-created volumes is always Windows/Unix. It can be changed to a Windows or Unix security model.

Topics in Shares and File Access:

- [Security Model Rules](#)
- [Security Model Directories](#)
- [Security Model Management](#)
- [Special Share Options](#)
- [File and Share Access](#)
- [File-level Security](#)

Security Model Rules

Files and directories created by clients inside security models acquire the security personality and permissions according to the rules of the chosen security model.

Windows/Unix Security Model:

- Files and directories created by SMB clients will have the Windows security personality. Permissions will either be inherited according to the ACL of the parent directory (if Windows) or will receive a default ACL that grants the user full access only (if the parent is Unix or has no inheritable permissions).
- Files and directories created by non-SMB clients will have the Unix personality. Unix permissions will be as set by the client (per the user’s local umask on the client).

- The security personality of a file or directory can be changed by any user with sufficient rights to change permissions or ownership. If a client of one security personality changes permissions or ownership of a file or directory of a different personality, the personality will change to match the personality of the client protocol (for example, if an NFS client changes Unix permissions on a Windows file, the file will change to the Unix personality).

Windows Security Model:

- All files and directories will have the Windows security personality. Permissions will be inherited according to the ACL of the parent directory.
- The permissions of a file or directory can be changed by any Windows SMB user with sufficient rights to change permissions or ownership. Permissions cannot be changed by NFS, AFP, or FTP clients.
- The personality of files and directories cannot be changed on a Windows security model. All files and directories always have the Windows personality with a Windows ACL. Standard Unix permissions will appear as `777 (rwxrwxrwx)`, but only the permissions in the Windows ACL will be enforced.

Unix Security Model:

- Files and directories created by non-SMB clients will have the Unix personality. Unix permissions will be as set by the client (per the user's local umask on the client).
- Files and directories created by SMB clients will have the Unix personality. Unix permissions will be set to a default.
- The personality of files and directories cannot be changed on a Unix security model. All files and directories always have the Unix personality.

Security Model Directories

With Traditional RAID, a security model can be configured on directories immediately underneath the top-level volume directory.

Default ownership differs according to the method used to create the security model directory:

- **From the client** – For Unix personality directories, the owner and owning group will be according to the logged-in user. For Windows personality directories, the owner will be the logged-in user, or “Administrators” for directories created by Domain Admins or members of the local `admingrp`.
- **From the Web Management Interface** – For Unix personality directories, the user and group owner will be `admin` and `admingrp`. For Windows personality directories, the owner will be the local `admingrp` (“Administrators”).

Security models and permissions differ according to the method used to create the security model directory:

- **From the client:** If SMB, permissions will either be according to ACL inheritance (if the parent volume root directory has the Windows security model) or *Full Access* to the owning user only. Permissions for directories created by all other protocols will be set by the client (per the client's umask).
- **From the Web Management Interface:**
 - If created in a Unix volume, permissions are `777 (rwxrwxrwx)`.
 - If created in a Windows/Unix volume, permissions allows all users to create, delete, and change permissions on files created inside the security model, and grants full control to administrators.

Security Model Management

Changes to a security model can optionally be propagated with the corresponding personality and default permission to all files and directories underneath the security model.

When **setting** the security model:

- For Traditional RAID, which permits security models to be set on both volumes and directories immediately underneath volumes, you can mix security models on the volume.
- For DynamicRAID, only a single security model can be set on the entire volume at the root level but not the directories immediately underneath the volume.

When **changing** the security model:

- If changing from Windows to Unix, all files and directories will be changed to be owned by *admin* and *admingrp*, with Unix permissions of *777(rwxrwxrwx)*.
- If changing from Unix to Windows, files and directories will be changed to default permissions that allow all users the ability to create and manage their own files and directories and to access other users' files and directories.

Special Share Options

The basic setup and configuration of shares on a SnapServer is handled on the **Security > Shares** page (see [Chapter 7, Security Options](#)). This section covers more details about the special options and features of share security on your SnapServer:

- [Hiding Shares](#)
- [Share Level Permissions](#)
- [Where to Place Shares](#)

Hiding Shares

There are three ways a share can be hidden in GuardianOS:

- Name the share with a dollar-sign (\$) at the end. This is the traditional Windows method of hiding shares; however, it does not truly hide the share since Windows clients themselves filter the shares from share lists. Other protocols can still see dollar-sign shares.
- Hide the share from all protocols (except NFS) by navigating to **Security > Shares > Create Share > Advanced Share Properties** and selecting the **Hide this Share** checkbox, or by selecting a share, clicking to expand **Advanced Share Properties**, and selecting the **Hide this Share** checkbox. When a share is hidden this way, the share is invisible to clients, and must be explicitly specified to gain access.

NOTE: Hidden shares are not hidden from NFS, which cannot access invisible shares. To hide shares from NFS, consider disabling NFS access to the hidden shares.

- Disable individual protocol access to certain shares by navigating to **Security > Shares > Create Share > Advanced Share Properties** and enabling/disabling specific protocols, or by selecting a share, clicking to expand **Advanced Share Properties**, and enabling or disabling specific protocols.

Share Level Permissions

Share-level permissions on GuardianOS are applied cumulatively. For example, if the user “jdoe” has Read-Only share access and belongs to the group “sales”, which has Read/Write share access, the result is that the user “jdoe” will have Read/Write share access.

NOTE: Share-level permissions only apply to non-NFS protocols. NFS access is configured independently by navigating to the Security > Shares page, selecting from the table the NFS Access level for the share, and modifying the client access as desired. See [NFS Share Access](#) on page 240.

Where to Place Shares

For security and backup purposes, it is recommended that administrators restrict access to shares at the root of a volume to administrators only. After initialization, all SnapServers have a default share named *SHARE1* that points to the root of the default volume *VOL0* (Traditional RAID) or *Volume1* (DynamicRAID). The share to the root of the volume should only be used by administrators as a “door” into the rest of the directory structure so that, in the event that permissions on a child directory are inadvertently altered to disallow administrative access, access from the root share is not affected. This also allows one root share to be targeted when performing backups of the server. If it is necessary to have the root of the volume accessible, using the Hidden option helps ensure only those that need access to that share can access it.

File and Share Access

The shares feature also controls access by other users and groups. This section provides information on setting up the shares options to allow proper access to the files.

NFS Share Access

When controlling share access for NFS clients, administrators limit client access to the shares independently of share level permissions that apply to other protocols. Access is controlled on a per-share basis. To set the NFS access, navigate to **Security > Shares**. In the Shares table, click in the **NFS Access** column of the share you want to modify. Changes made on this page affect the NFS “exports” file within GuardianOS.



CAUTION: If there are multiple shares to the same directory on the disk, and those shares permit access via NFS, they must all have the same NFS export configuration. This is enforced when configuring NFS access to the overlapping shares.

Snapshot Access

Snapshots are accessed via a snapshot share. Just as a share provides access to a portion of a live volume (or filesystem), a snapshot share provides access to the same portion of the filesystem on all current snapshots of the volume. The snapshot share’s path into snapshots mimics the original share’s path into the live volume.

Snapshot Shares and On Demand File Recovery

A *snapshot share* is a read-only copy of a live share that provides users with direct access to versions of their files archived locally on the SnapServer via a snapshot. Users who wish to view or recover an earlier version of a file can retrieve it on demand without administrator intervention.

Snapshot shares are created during the course of creating a share, or thereafter by navigating to the Snapshots page and clicking the name of a snapshot. For instructions on accessing snapshot shares, see [Shares](#) in [Chapter 7](#).

Creating a Snapshot Share

You create a snapshot share by selecting the **Create Snapshot Share** option on the **Security > Shares > (share_name) > Share Properties** page, under the **Advanced Share Properties** link.

For example, assume you create a share to a directory called *sales*, and you select the **Create Snapshot Share** option. When you connect to the server via a file browser or use the **Misc. > Home** link in the Site Map, two shares display:

```
SALES
SALES_SNAP
```

The first share provides access to the live volume, and the second share provides access to any archived snapshots. Other than read-write settings (snapshots are read-only), a snapshot share inherits access privileges from its associated live-volume share.

NOTE: The same share folders appear on the Home page when you connect to the SnapServer using a Web browser. However, the snapshot share folder does not provide access to the snapshot; it always appear to be empty. You can prevent the snapshot share from displaying on this Home page by selecting the **Hide Snapshot Share** option when creating or editing a share.

Accessing Snapshots Within the Snapshot Share

A snapshot share contains a series of directories. Each directory inside the snapshot share represents a different snapshot. The directory names reflect the date and time the snapshot was created.

For example, assume the snapshot share named *Sales_SNAP* contains the following four directories:

```
latest
2014-02-25.120000
2014-03-01.000100
2014-03-07.020200
```

The *latest* directory always points to the most recent snapshot (in this case, **2014-03-07.020200**, or March 7th, 2014, at 2:02 a.m.). A user may view an individual file as it existed at a previous point in time or even roll back to a previous version of the file by creating a file copy to the current live volume.

NOTE: The latest subdirectory is very useful for setting up backup jobs, as the name of the directory is always the same and always points to the latest available snapshot.

Depending on their ability to cross bind mounts, locally-installed backup agents can access the snapshot share in one of two ways:

- via `/shares` (for example, `/shares/SHARE1_SNAP/latest`)
- via `/links` (for example, `/links/SHARE1_SNAP/latest`)

File-level Security

GuardianOS supports two “personalities” of filesystem security on files and directories:

- **Windows ACLs:** Windows NTFS-style filesystem permissions. Windows ACLs fully support the semantics of NTFS ACLs, including configuration, enforcement, and inheritance models (not including the behavior of some built-in Windows users and groups).
- **Unix:** Traditional Unix permissions (rwx) for owner, group owner, and other.

By default, volumes are created with the Windows/Unix security model (Windows-style ACLs for files created by SMB clients and Unix-style permissions for files created by other protocols and processes), and allow all users to create, delete, and configure permissions on their own files and to access files and directories created by other users.

Security Personalities and Security Models

The security personality of a file or directory is dependent on the security model of the root directory or volume in which the file or directory exists.

Files and directories in a Windows/Unix security model can have either a Windows or Unix security personality, depending on the network protocol used to create the file or change permissions on it. Files in a Windows security model always have the Windows security personality and permissions can only be set by Windows SMB clients. Files in a Unix security model always have the Unix security personality and permissions can only be set by non-SMB clients.

Windows ACLs

GuardianOS fully supports Windows NTFS-style filesystem ACLs, including configuration, enforcement, and inheritance models. Inside Windows/Unix and Windows security models, files created and managed by Windows clients have the Windows security personality and behave just as they would on a Windows server. Clients can use the standard Windows Explorer interface to set directory and file permissions for local and Windows domain users and groups on the SnapServer.

Permissions are enforced for the specified users in the same manner for all client protocols, including non-SMB clients that normally have the Unix security personality. However, if a non-SMB client changes permissions or ownership on a Windows personality file or directory (or deletes and recreates it) inside a Windows/UNIX security model, the personality will change to Unix with the Unix permissions specified by the client.

NOTE: Group membership of NFS clients is established by configuring the local client's user account or the LDAP or NIS domain. Group membership of SnapServer local users or users ID-mapped to domain users is not observed by NFS clients. Therefore, ACL permissions applied to groups may not apply as expected to NFS clients.

Default File and Folder Permissions

When a file or directory is created by an SMB client, the owner of the file is the user who created the file (except for files created by local or domain administrators, in which case the owner will be the **Administrators** group, mapped to the local **admingrp**). The ACL is inherited per the inheritance ACEs on the parent directory's ACL. The owner of a file or directory always implicitly has the ability to change permissions, regardless of the permissions established in the ACL. In addition, members of the SnapServer local admin group, as well as members of Domain Admins (if the server is configured to belong to a domain) always implicitly have *take ownership* and *change ownership* permissions.

Setting File and Directory Access Permissions and Inheritance (Windows)

Access permissions for files and directories with the Windows security personality are set using the standard Windows Explorer interface. GuardianOS supports:

- All standard generic and advanced access permissions that can be assigned by Windows clients.
- All levels of inheritance that can be assigned to an ACE in a directory ACL from a Windows client.
- Automatic inheritance from parent directories, as well as the ability to disable automatic inheritance from parents.
- Special assignment and inheritance of the CREATOR OWNER, CREATOR GROUP, Users, Authenticated Users, and Administrators built-in users and groups.

Procedure to set file and directory access permissions and inheritance in Windows:

1. Using a Windows client, **map a drive** to the SnapServer, logging in as a user with change permissions for the target file or directory.
2. Right-click the file or directory, choose **Properties**, and then select the **Security** tab.
3. Use the **Windows security tools** to add or delete users and groups, to modify their permissions, and to set inheritance rules.

Troubleshooting SnapServers

Basic techniques for identifying and resolving common hardware and networking issues are described here.

Topics in Troubleshooting SnapServers

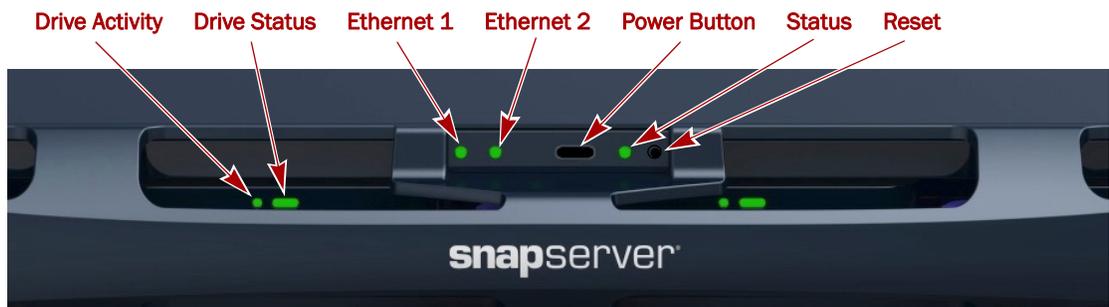
- [LED Indicators](#)
- [System Reset Options](#)
- [Maintenance Mode](#)
- [Networking Issues](#)
- [Miscellaneous Issues](#)
- [Phone Home Support](#)

LED Indicators

LED indicators provide information on the status of basic connectivity, disk drives, fan modules, and power supply modules.

SnapServer DX1

The SnapServer DX1 has two network LEDs (Ethernet 1, left; Ethernet 2, right) and one status LED. Each drive has two disk LEDs (Drive Activity and Drive Status). There is a Power button and a Reset button, as shown in the following illustration:



SnapServer DX2

The SnapServer DX2 has one network LED (Ethernet) and one system status LED on the Power Panel located on the right flange, along with a Power button and a Reset button. Each drive has two disk LEDs (Drive Activity and Drive Status) as shown in the following illustration:



SnapExpansion

The SnapExpansion has one network LED (Ethernet) and one system status LED on the Power Panel located on the right flange, along with a Power button. Each drive has two disk LEDs (Drive Activity and Drive Status) as shown in the following illustration:



The Power button is an override option only as the SnapServer head unit manages the power to all attached expansion units. To use the Power button to shut down the expansion unit, press and hold it for four seconds.

Drive Status LEDs

The following LED behavior can be observed when the SnapServer is ON.

Device State	LED State
No Disk Drive in Bay	Off
Normal Operation	Solid green
Unit Identification Indicator	Flashing amber *
RAID in Degraded Mode/Rebuilding [†]	Flashing green/amber
Failed	Flashing red
Unusable	Solid amber

* When the Unit Identification Indicator is turned on, all drive LEDs and the system/status LED flash amber.

† All member drives of a RAID flash green/amber when the RAID is degraded and throughout the entire rebuild process when the RAID is being repaired with a new drive. Do not remove the drive during this time.

Drive Activity LEDs

Device State	LED State
Powered OFF / No Activity	Off
Drive Activity	Flashing green

Network LEDs

Device State	LED State
Powered OFF	Off
Link Up (SnapServer Powered ON)	Solid green
Link Down	Off

Server Status LEDs

Device State	LED State
Powered OFF	Off
Unit Identification Indicator	Flashing amber *
Booting	Solid amber
Normal Operation	Solid green
Shutting down	Flashing green
Maintenance Mode	Flashing green/amber

* When the Unit Identification Indicator is turned on, all drive LEDs and the system/status LED flash amber.

Power Supply Status LED

Device State	LED State
Normal Operation	Solid green
Standby	Solid red
Power Failure	Off
Fan Failure	Blinking red

System Reset Options

Often the first thing to try in resolving anomalous behavior on a SnapServer is to reset the server to factory defaults using the Web Management Interface. See [Factory Defaults](#) in [Chapter 9](#).

Performing System Resets Without Network Access

Should Web Management Interface access to the server be lost, the **Reset** button can be used to reset server settings and reestablish connectivity. This option is also useful should you forget the admin password.

On the SnapServer DX1, the **Reset** button is accessed via a small hole next to the **Power** button on the front of the server at the top. On the DX2, the hole is located at the bottom of the Power panel on the right flange. Verify that the server is fully booted (as indicated by the system/status LED). Using the end of a straightened paper clip or the fine point of an instrument, press in and hold the **Reset** button for a few seconds.

The system will reboot after about a minute. As a part of the reset and reboot process, the SnapServer does the following:

- Clears user-defined TCP/IP settings such as DHCP configuration.
- Resets the server name to its default setting (**SNAP<server_number>**).
- Resets network speed and bonding settings to their defaults.
- Resets the Administrator password to the default (**admin**).
- Resets the web server to allow HTTP access.

Maintenance Mode

The SnapServer may enter Maintenance Mode (system/status LED blinking amber and green) when GuardianOS has been compromised and is in need of repair or re-installation. The two functions available in Maintenance Mode should only be used under the direction of Overland Technical Support:

- **Repair** – Reapplies the GuardianOSImage, but preserves system settings.
- **Fresh install** – Reinstalls GuardianOS, overwriting any previous configurations and destroying all disk partitions.



CAUTION: Because of significant changes introduced in GuardianOS 7.5, a fresh install of GuardianOS 7.5 should not be performed on a SnapServer running an older version of GuardianOS. Failure to follow this guideline can result in total failure of the SnapServer to start, even into Maintenance Mode. The Fresh install option should only be performed with the same version of GuardianOS currently installed on the SnapServer, and only under the direction of Overland Technical Support.

NOTE: To install GuardianOS, you must obtain the appropriate GuardianOS image file. This file is available for download by entitled users from the SnapServer support site: <http://docs.overlandstorage.com/SnapServer>

Networking Issues

These are some of the networking issues you may encounter when using your SnapServer.

The Server Cannot Be Accessed Over Network

Inaccessibility may be caused by a number of reasons. To resolve this issue, use one of the following methods:

- Verify that you have the correct IP address of the server, and try to connect again.

- Verify that the LED for the primary Ethernet port is lit. (This light indicates network connectivity.) If the light is not lit, perform the following:
 - The most likely cause is the physical connection. Check for a loose or damaged cable, or poor connections in the port connector.
 - This problem may also be caused by a mismatch between the settings on the switch or hub and the settings on the SnapServer Ethernet port. These settings must match. To resolve the problem, make sure the port settings on the hub or switch match the settings for the primary port as configured on the **Network > TCP/IP** page of the Web Management Interface. Use the autonegotiate setting on both the switch and the server port.

You Have No Access to SnapServer via HTTP

When trying to access the SnapServer via HTTP, the Web browser times out. However, the server can be accessed using the ping command or Windows Explorer.

- HTTP and HTTPS are both enabled by default on SnapServers. Try typing HTTPS in the Web address rather than HTTP. If you are able to access the server via HTTPS, you can re-enable HTTP on the **Network > Web** page.
- If you cannot access the server via HTTPS, try resetting the server as described on [Performing System Resets Without Network Access](#) on [page 247](#).

Access Denied Message Appears after Configuring Microsoft Domain Security

Customers who have configured local users and local groups with the same name as their domain users and groups can have security conflicts if they integrate with Microsoft Domain Security. The SnapServer will authenticate the users as local SnapServer users before authenticating through the Domain. However, the Domain users/groups may be the ones that had been granted access to the shares.

Be careful not to add local users or groups that are duplicates of those that are found on the Windows domain controller.

The SnapServer Does Not Operate Properly on a Network Running Gigabit-Full-Duplex

For Gigabit Ethernet to operate properly, both the switch and the SnapServer primary Ethernet port must be set to **Auto** (autonegotiate). Any other setting will result in unexpected behavior and reduced performance.

The Network Does Not Have a DHCP Server and SnapServer IP Address Is Unknown

Install SnapServer Manager (available from the SnapServer [support page](#) on the Overland Storage website) onto a client workstation on the same subnet as the SnapServer. You can then use the utility to discover all SnapServers on that network segment, and to assign static IP addresses as necessary.

Problems Occur with Domain Controller Authentication

You are receiving the following errors in your error log:

```
SMB: Domain Controller unavailable
```

```
SMB: Username not connected to Domain Controller
```

This means that either your Domain Controller is down, or the SnapServer is unable to reach it. Because it cannot communicate with the Domain Controller, it is not able to authenticate the user. Check to make sure the Domain Controller is online, is consistently reachable via the network, and that users can authenticate to the Domain Controller.

You Start Your SnapServer but Cannot See It on Network

Ensure that the Ethernet cable is connected securely to both the network port and the server's primary Ethernet port. Also, check to see that the Link light on the front of the SnapServer is lit (solid green). If the Link light is off, this is normally caused by a mismatch between the switch/hub and the Ethernet port on the SnapServer. To resolve this problem, verify that all settings (if using multiple Ethernet ports) on the switch/hub match the setting on the server. When the server is shipped from the factory, both ports are set to autonegotiate. Therefore, the switch/hub *must* be set to autonegotiate to initially connect to the server.

SnapServers are configured by default to acquire an IP address from a DHCP server. If no DHCP server is found on the network, the SnapServer defaults to an IP address in the range of 169.254.xxx.xxx and is labeled ZeroConf in SSM. While you may not be able to see the server on your network, you can discover the SnapServer using either the default server name or the SSM utility (available at our external download site:

<http://www.overlandstorage.com/SSM>)

Use the server name method if you are installing one SnapServer on the network. Use SSM if you are installing two or more SnapServers, or if your network does not have IP-to-name resolution services.

You Try to Mount to a Share on Your SnapServer from Your Linux Workstation and You Receive an RPC Timeout Message

Check the firewall configuration to your Linux workstation. Be sure you have not blocked the ability to receive TCP or User Datagram Protocol (UDP) communications. If problems persist, contact Overland Storage Technical Support.

You Receive an Access Denied Message When Attempting to Mount a Share on Your SnapServer from a Linux Workstation

If you are logged in as **root** on your workstation and NFS is enabled on your SnapServer, this message can be misleading, causing you to look for security issues, when in fact it could be a command syntax issue. For example, the common Linux mount command:

```
mount 192.168.32.124:SHARE1 /mnt
```

is missing a forward slash (/) in the command following the IP address. This returns an Access Denied message. The correct syntax should be the following (added slash shown in **red**):

```
mount 192.168.32.124: /SHARE1 /mnt
```

NOTE: The share name is case-sensitive.

You Cannot Log in as Root to SnapServer

GuardianOS allows you to log in as root over SMB. If this operation has failed or you have trouble logging in, be sure that you have enabled root login in the **Network > Windows/SMB** page. Also note that the root account password is tied to the admin account password. If you cannot log in as root, change the password for the admin account on the **Network > Windows/SMB** page. Use the admin password to log in as root.

You Are Unable to See Your Domain Users When Trying to Set Up Windows Security Permissions on File Folders

The SnapServer running GuardianOS has joined the Active Directory domain properly, and you can see the domain users when you set Share permissions from the browser-based Web Management Interface.

Make sure the Windows client (PC) you are trying to set permissions from is assigned a valid DNS server. You can check your Windows client using the `ipconfig` command from a command prompt.

Miscellaneous Issues

These are some miscellaneous issues you may encounter when using your SnapServer.

You Backed Up Your Snapshot Share, Are Now Attempting to Restore It, and Operation Fails

A snapshot share is read-only. You can restore the data to a read-write accessible share.

A Problem Occurred While Booting. The System is Offline and the System/Status LED is Blinking Amber and Green

The SnapServer has booted into Maintenance (Recovery) Mode. This may be due to a boot failure in the previous boot attempt. Try booting again. If the server still returns to Maintenance Mode, contact Overland Technical Support.

Power to the SnapServer Is Unexpectedly Cut Off Due to a Power Outage

Overland Storage recommends that you use an uninterruptible power supply (UPS) with the SnapServer. If you did not have a UPS attached to the server at the time of the power outage, do the following:

1. Remove the power cables.
2. Once the power is restored and stabilized, turn the power supplies back on and reboot the server.

Once the SnapServer boots, it begins resynchronizing the RAIDs if necessary. You can use the server during the resynchronization, but performance will be a little slower than normal. Do not remove drives, however, while the server is resynchronizing the RAID.

The Server Is Not Responding to File Requests or Configuration Commands

Call your SnapServer technical support representative.

You Have Problems Seeing the Tape Library Tape Device, Not the Robotic Arm

When you have problems seeing the actual tape device rather than the robotic arm, it is most likely due to the Tape Loader being configured for Sequential Access. Change the Tape Loader to Random or Mixed Mode.

The Admin Password to the Web Management Interface Is Not Available

You can perform a limited reset to defaults, which includes the admin password, then use the Web Management Interface to set a new password. See [Performing System Resets Without Network Access](#) on page 247.

You Cannot Delete Files or Folders From an iSCSI Disk

If an iSCSI disk is mounted to a folder, not a letter drive, in Windows you will not be able to delete files and folders inside that mount point. The Windows Recycle Bin does not understand mount points, so to avoid this problem either mount iSCSI disks to letter drives on your Windows OS, or hold down the shift key while deleting folders or files.

Phone Home Support

Once your SnapServer has been registered, Phone Home Support becomes available for use. Phone Home Support emails system logs and files that contain information useful for troubleshooting purposes to Overland Storage Technical Support. You can use the **Maintenance > Support** page to open a new case with technical support; or, in the course of working to resolve an issue, a technical support representative may ask you to fill out and submit this page. If a case is already in progress, you will need to enter the case number provided by the technical support representative.

NOTE: Phone Home Support interacts with two fields on the **Maintenance > Tools > Email Notification** page. To use Phone Home Support, you must first enter a valid SMTP server IP address on the Email Notification page. The first email address listed in the Recipients field automatically populates the Reply-to Address field on the **Support** page.

Complete the following fields as appropriate, then click **OK**:

Text Field	Description
Subject*	Enter a concise description that identifies the issue.
Case*	Select <i>New Case</i> if you are emailing technical support for the first time. Select <i>Existing Case</i> if you have previously contacted technical support concerning the issue.
Case Number	If you selected <i>Existing Case</i> above, enter the case number provided by technical support.
Reply-to Address*	This field defaults to the first email address entered as a recipient on the Server > Email Notification page. If necessary, enter at least one email address that will serve as the contact email address for this issue. To receive a copy of the email and system information attachment, check the Cc Reply-to Address box.
Comments*	Enter additional information that will assist in the resolution of the problem.

*Required option.

Command Line Interface

GuardianOS includes a command line interface (SnapCLI) that is accessible through SSH. Using the CLI, users can access information about most of the SnapServer configuration parameters and perform configuration and maintenance functions without using the GuardianOS Web Management Interface or SSM.

 **IMPORTANT:** Some administrative tasks must still be performed using the Web Management Interface. The CLI is intended as a convenient way to perform some functions; it is not intended as an alternative to using the Web Management Interface.

Before You Begin

Before the storage type is configured to DynamicRAID or Traditional RAID, SnapCLI disables all standard commands and makes only the `system` command available. This command is available *only* before storage is configured, and has the following arguments:

Command	Arguments and Options	Descriptions
system	type	<code>type=DynamicRAID</code> Specify DynamicRAID mode
		<code>type=Traditional-RAID</code> Specify Traditional RAID mode
	force	<code>yes</code> Bypass confirmation prompt

Thus, the following command string:

```
system type=Traditional-RAID force=yes
```

sets the storage type to Traditional RAID and bypasses the confirmation prompt.

Once the `system` command is run and the storage type is chosen, SnapCLI unlocks the rest of the standard commands. A reboot is required if Traditional RAID is chosen as the storage type.

Topics in Command Line Interface

- [SnapCLI Syntax](#)
- [SnapCLI Commands](#)
- [Scripts in SnapCLI](#)

SnapCLI Syntax

SnapCLI command syntax uses three parameters: **COMMANDS**, **ARGUMENTS**, and **OPTIONS**. To generate commands in SnapCLI, use the following syntax:

```
COMMAND [ARGUMENT] [OPTIONS]
```

where **COMMAND** is the name of one of the SnapCLI commands, **ARGUMENT** is an action available for that command, and **OPTIONS** are additional parameters for the command.

Once logged into the CLI, there are several ways of displaying information about available parameters.

Type	To
?	see an overview of the CLI, with a list of available commands and a description of command syntax.
{command} help	see a description of that particular command's function and a list of options available for the command.
tab	finish the command you have started to type (such as, tab-complete).
{command} tab	list any arguments and/or options available for that command.

For example, to see a list of available commands once you have logged into SnapCLI, type “?” at the prompt.

To see a description of a specific command, type the command name (for example, date) + “help” or “?”:

Command	Arguments and Options	Descriptions
date	timezones	- list available time zones
	get	- get server date/time
	set [OPTIONS]	- set server date/time
	- [day=1-31]	- day of month
	- [month=1-12]	- month of year
	- [year=1900-current]	- year
	- [hour=0-23]	- hour
	- [minute=0-59]	- minutes
	- [second=0-59]	- seconds
	- [timezone=1- 40]	- timezone (use the command date timezones to get a list of timezones)

In this instance, to set the date to October 27, 2011, enter:

```
date set day=27 month=10 year=2011
```

NOTE: If, instead of typing the word **date**, you had typed **d + [tab]**, the word would have been completed for you. If you entered **d + [tab] + [tab]**, the word would have been completed and the available options displayed.

Suppose, instead of **date**, you typed the command **web**. Two arguments would be available, one with options:

Command	Arguments and Options	Descriptions
web	get	- get WEB properties

Command	Arguments and Options	Descriptions
	<code>set [OPTIONS]</code>	- set WEB properties
	- <code>require-webview-auth=(yes no)</code>	- require HTTP/HTTPS clients to authenticate in order to access the server
	- <code>non-secure-http=(yes no)</code>	- enable/disable non-secure HTTP access

Thus, the following command string:

```
web set require-webview-auth=yes non-secure-http=no
```

sets HTTP/HTTPS properties on the SnapServer to require clients to authenticate in order to access the server and to disable non-secure HTTP access.

SnapCLI Procedures

Use these procedures to access and exit SnapCLI.

Logging into SnapCLI

1. Make sure your client has an SSH v2 client application installed.

NOTE: Free or low-cost SSH applications are available from the Internet.

2. Connect to the server using its name or IP address, and log in as *admin* (or any other member of *admingrp*).

You will automatically be placed in the CLI shell.

NOTE: SSH v2 is required. If you fail to connect to the server, ensure that your SSH client is configured to connect via SSH v2.

Exiting SnapCLI

To exit SnapCLI, type `exit`. The SSH session will close.

SnapCLI Commands

The following table presents a list of the available SnapCLI commands and a brief description of the function of each.

Command	Description
<code>activeusers</code>	Display active users
<code>apple get</code>	Display apple network settings
<code>apple set</code>	Update apple network settings
<code>clear</code>	Clear the page
<code>date get</code>	Get the current date/timezone information
<code>date set</code>	Set the current date/timezone information

Command	Description
date timezones	List the available timezones (used in conjunction with the date set command)
diskunits	Get status information of all the disk units on the server
domain get	Get the domains known to the SnapServer and their properties
domain list	List the domains known to the SnapServer
dri create	Create a Disaster Recovery Image (dri)
dri recover system	Restore a Disaster Recovery Image (dri)
dri recover volume	Restore a Disaster Recovery Volume Image (dri)
email get	Get email notification settings
email set	Set email notification settings
event clear	Clear all events in the System Event Log
event get	Display the System Event Log
exit	Quit the command line, log off, and exit ssh/bash session. NOTE: If user has started another shell, the command 'exit' will return them to the SnapServer command line shell.
factorydefaults	Reset the SnapServer settings back to the factory defaults, will reboot
fscheck	Check or repair the user or root filesystem
ftp get	Get the current ftp settings, including anonymous user access
ftp set	Set the current ftp settings, including anonymous user access
globalspares list	List global spares
globalspares remove	Remove a disk from the global spares list
globalspares add	Add a disk to the global spares list
group create	Create a local group
group delete	Delete a local group
group get	Get available groups with their associated information
group list	List available groups
group set	Change the properties of a local group
group member add	Add a group member to a local group
group member delete	Delete a group member from a local group
group members get	Get a list of the members of a local group
group members list	List the members of a local group
history	Print the history of commands typed into the SnapServer command line
homedirs get	Get Home Directory configuration information
homedirs set	Set Home Directory configuration information
hostfile add	Add a host file entry

Command	Description
hostfile delete	Delete a host file entry
hostfile get	Get information for a specific host file entry
hostfile set	Set information for a specific host file entry
hostfile list	List all host file entries
idmap auto map	View/Save auto-generated ID mappings
idmap count	Count number of ID mappings
idmap group get	Get ID mapping for a (windows domain) group
idmap group remove	Remove ID mapping for a (windows domain) group
idmap group set	Set ID mapping for a (windows domain) group to a local or NIS group
idmap list	List all ID mappings
idmap remove all	Remove all ID mappings
idmap update files	Update filesystem for ID mapping changes
idmap update status	View status of ID mapping update filesystem operation
idmap user get	Get ID mapping for a (windows domain) user
idmap user remove	Remove ID mapping for a (windows domain) user
idmap user set	Set ID mapping for a (windows domain) user to a local or NIS user
iscsi create	Create an iscsi disk
iscsi delete	Delete an iscsi disk
iscsi get	Get iscsi disk properties
iscsi set	Set iscsi disk properties
isns get	Get configuration settings for iSNS server
isns set	Set configuration settings for iSNS server
jumboframe get	Get jumbo frame settings for all interfaces
jumboframe list	List jumbo frame settings for all interfaces
jumboframe set	Set jumbo frame settings for all interfaces
less	With a file name, this command allows the user to view any file on the system. It should only be used for 'text' files.
name get	Get the name of the SnapServer
name set	Set the name of the SnapServer
netinfo	Get information about the Ethernet interface
nfs get	Get SnapServer NFS Properties
nfs set	Set SnapServer NFS Properties
nis get	Get current NIS settings
nis set	Set current NIS settings
ntp get	Get NTP client settings
ntp set	Set NTP client settings
ntp_server get	Get NTP Server settings
ntp_server set	Set NTP Server settings

Command	Description
openfiles	List the Open Files
osupdate get	Display status of last OS update
osupdate load	Perform an OS update
passwordpolicy get	Display Password Policy settings and status
passwordpolicy set	Update Password Policy settings
phonehome	Send configuration details to SnapServer Technical Support
proxy get	Display the HTTP proxy properties
proxy set	Set the HTTP proxy properties
quit	Quit the command line, log off, and exit the ssh/bash session
quota list	List user or group quotas for a volume
quota get	Get quota settings for a volume
quota set	Set quota settings for a volume
quota group get	Get volume quota limit & usage for a specific group
quota group set	Set volume quota limit & usage for a specific group
quota user get	Get volume quota limit & usage for a specific user
quota user set	Set volume quota limit & usage for a specific user
reboot	Reboot the SnapServer
securitymodel get	Get the security model on a SnapServer Volume
securitymodel set	Set the security model on a SnapServer Volume
share create	Create a share
share delete	Delete a share
share get	View a share
share rename	Rename a share
share set	Modify a share
share list	List available shares
share access get	Get access list for the share
share access set	Set access list for the share
share access delete	Delete access permission of the specified user/group for the share
share nfsaccess get	Get NFS access permission of the host for the specified share
share nfsaccess set	Set NFS access permission of the host for the specified share
share nfsaccess delete	Delete NFS access permission of the host for the specified share
shutdown	Shutdown the SnapServer
slidingwindow get	Get sliding window settings for a specific interface
slidingwindow set	Set sliding window settings for a specific interface
slidingwindow list	List sliding window settings for all interfaces

Command	Description
snapex	Perform a control operation on the snap extension
snapshot create later	Create a new snapshot schedule
snapshot get	Get snapshot properties
snapshot set	Set properties for the specified snapshot
snapshot list	Get list of snapshots
snapshot create now	Create a new one time snapshot to be run immediately
snapshot delete	Delete specified snapshot
snapshot sched delete	Delete specified snapshot schedule
snapshot sched get	Get specified snapshot schedule
snapshot sched set	Set specified snapshot schedule
snapshot sched list	List current snapshot schedules
snapshot pool get	Get snapshot pool properties
snapshot pool set	Set snapshot pool properties
snapshot pool list	List current snapshot pools
snapshot rollback	Start a rollback for the specified snapshot
snmp get	Get SNMP parameters
snmp set	Set SNMP parameters
ssh get	Get current SSH settings
ssh set	Enable and Disable SSH. NOTE: Turning off SSH while running the command line will 'kick' the user off the system and they won't be able to log back into the command line until SSH is re-enabled via the SnapServer Web Management Interface.
syslog all	Create a tar file of syswrapper and all third-party logs
syslog edr	Create a tar file of Snap EDR logs
syslog s2s	Create a tar file of S2Sv2 logs
syslog syswrapper	Create a tar file of syswrapper only
system type	Available only before storage is configured. Specifies storage type.
system type force	Available only before storage is configured. Allows you to bypass the confirmation prompt.
systemstatus	Get system status information for the server
tape list	List the SCSI tape devices
tape settings get	Display current SCSI tape device settings
tape settings set	Update SCSI tape device settings
tcpip get	Get TCP/IP parameters
tcpip set	Set TCP/IP parameters. NOTE: Changing the parameters of the Ethernet interface over which the user is currently running the SSH/command line session may result in the user being disconnected.

Command	Description
tcpip create bond	Create a bond and set TCP/IP properties.
tcpip delete bond	Remove a TCP/IP bond.
updatenotification get	Get update notification properties
updatenotification set	Set update notification properties
updatenotification check	Check to see if updates are available
ups get	Get UPS settings and status
ups set	Set UPS settings
user create	Create a local user
user delete	Delete a local user
user get	Get available users with their associated information
user list	List available users
user set	Change the properties of a local user
user lock	Lock the specified user.
user unlock	Unlock the specified user.
version	Display current version information, including the Server Number. NOTE: This is the same information displayed in the Web Management Interface "About" box
volume list	List of the volumes defined on the SnapServer
volume get	Get a specific volume's properties
volume create	Create a new logical volume
volume edit	Edit an existing logical volume
volume delete	Delete a logical volume
volume write-cache	Enable or disable write cache on a volume.
vxxaccess list	List hostnames with VSS/VDS access
vxxaccess add	Add hostname of VSS/VDS client requiring access to this server
vxxaccess delete	Delete access for a VSS/VDS client hostname
web get	Get current HTTP Web access settings
web set	Enable or Disable HTTP access to Web Management Interface
windows domain-filter	Allows the user to limit the number of domain users and groups that the server imports from the Active Directory domain, by restricting the import to a specific organizational unit as well as to specific domain users and groups.

The following commands are available only in Traditional RAID:

Command	Description
raid list	List available raids
raid create	Create a raid set

Command	Description
raid delete	Delete a raid set
raid get	Get raid set properties
raid add disk	Add a disk to a raid set
raid remove disk	Remove a disk from a raid set
raid repair	Repair a degraded raid set
raidsettings get	Get auto-incorporation and back-round disk settings
raidsettings set	Set the auto-incorporation and background disk properties
raid-speed-limit get	Get the current setting for the RAID sync speed limit.
raid-speed-limit set	Change the maximum RAID sync or resync speed. Use with caution.

The following commands are available only in DynamicRAID:

Command	Description
storagepool create	Create a new storage pool
storagepool edit	Edit an existing storagepool
storagepool get	Get storagepool properties
storagepool list	List available storagepools
storagepool repair	Repair an existing storagepool
storagepool delete	Delete a storage pool

Scripts in SnapCLI

Administrative tasks can be automated with shell scripts that call SnapCLI commands.

Running a SnapCLI Script

1. Create the script and put it in a share on the local server.
 - Be sure to use an application that is compatible with the standard Unix text file format (for example, vi). Avoid using Windows clients to create or edit scripts.
 - Place the script in a share that will never be part of a delete script.
2. Log in to the SnapCLI (see [Logging into SnapCLI](#) on [page 254](#) for instructions).
3. Type `osshell` to get a bash prompt (#).
4. At the prompt, make sure the script is executable by typing the following and pressing **Enter**:

```
chmod +x/shares/[sharename]/[scriptname]
```

where **sharename** is the name of the share where you put the script and **scriptname** is the name of the script.

- To run the script, type the path again, and press **Enter**:
`/shares/[sharename]/[scriptname]`

Sample Script

Following is an example script that can be used to create and remove users, groups, and shares:

```
#!/bin/sh

#####
# Copyright 2003-2007 Overland Storage, Inc. All rights reserved. #
# Permission is granted to use this code provided that it #
# retains the above copyright notice. ##
#####
CLI=/bin/cli
USER=myuser
PASSWORD=myuserpass
GROUP=mygroup
SHARE=myshare
VOLUME=VOL0

# usage: 'mkuser <user_name> <password>'
mkuser()
{

Create a User

# if the user does not exist then create it
if ! $CLI user get user-name="$1" > /dev/null 2>&1; then
echo "Creating user '$1' ..."
$CLI user create user-name="$1" password="$2" > /dev/null 2>&1
if [ $? -ne 0 ]; then
echo "Creation of user '$1' failed."
return 1
fi
else
echo "User '$1' already exists."
fi

return 0
}

# usage: 'mgroup <group_name>'
mkgroup()
{
```

Create a Group

```
# if the group does not exist then create it
if ! $CLI group get group-name="$1" > /dev/null 2>&1; then
    echo "Creating group '$1' ..."
    $CLI group create group-name="$1" > /dev/null 2>&1
    if [ $? -ne 0 ]; then
        echo "Creation of group '$1' failed."
    fi
else
    echo "Group '$1' already exists."
fi

return 0
}
```

```
# usage: 'adduser2group <user_name> <group_name>'
adduser2group()
{
```

Add the User to the Group

```
# if both the user and the group exist add the user as a member of this group
if $CLI user get user-name="$1" > /dev/null 2>&1; then
if $CLI group get group-name="$2" > /dev/null 2>&1; then
    echo "Adding user '$1' to group '$2' ..."
    $CLI group member add user-name="$1" group-name="$2" > /dev/null 2>&1
    if [ $? -ne 0 ]; then
        echo "Adding user '$1' to group '$2' failed."
    fi
else
    echo "Group '$2' does not exist."
fi
else
    echo "User '$1' does not exist."
fi

return 0
}
```

```
# usage: 'mkshare <share_name> <share_volume>'
mkshare()
{
```

Create a Share

```
# if the share does not exist create it
if ! $CLI share get share-name="$1" > /dev/null 2>&1; then
    echo "Creating share '$1' ..."
    $CLI share create share-name="$1" share-volume="$2" > /dev/null 2>&1
    if [ $? -ne 0 ]; then
        echo "Creating share '$1' failed."
    fi
else
    echo "Share '$1' already exists."
fi

return 0
}
```

```
# usage: 'rmuser <user_name>'
rmuser()
{
```

Delete the User

```
# if the user exists then delete it
if $CLI user get user-name="$1" > /dev/null 2>&1; then
    echo "Deleting user '$1' ..."
    $CLI user delete user-name="$1" > /dev/null 2>&1
else
    echo "User '$1' does not exist."
fi
```

```

        if [ $? -ne 0 ]; then
            echo "Deletion of user '$1' failed."
        fi
    return 1
    fi
else
    echo "User '$1' does not exist."
fi
return 0
}

```

```

# usage: 'rmgroup <group_name>'
rmgroup()
{

```

Delete the Group

```

# if the group exists then delete it
if $CLI group get group-name="$1" > /dev/null 2>&1; then
echo "Deleting group '$1' ..."
    $CLI group delete group-name="$1" > /dev/null 2>&1
    if [ $? -ne 0 ]; then
        echo "Deletion of group '$1' failed."
    fi
return 1
fi
else
    echo "Group '$1P' does not exist."
fi
return 0
}

```

```

# usage: 'rmshare <share_name>'
rmshare()
{

```

Delete the Share

```

# if the share exists delete it
if $CLI share get share-name="$1" > /dev/null 2>&1; then
echo "Deleting share '$1' ..."
    $CLI share delete share-name="$1" > /dev/null 2>&1
    if [ $? -ne 0 ]; then
        echo "Deletion of share '$1' failed."
    fi
return 1
fi
else
    echo "Share '$1' does not exist."
fi
return 0
}

```

Create a User, Group, and Share; Then Add the User to the Group

```

#####
#   Main   #
#####

# create a user, a group and a share and add the user to the group
mkuser "$USER" "$PASSWORD"
mkgroup "$GROUP"
adduser2group "$USER" "$GROUP"
mkshare "$SHARE" "$VOLUME"

#remove the group, the user and the share
rmgroup "$GROUP"
rmuser "$USER"
rmshare "$SHARE"

```


GuardianOS Ports

The following table outlines the ports used in GuardianOS.

Port #	Layer	GOS Feature	Name	Comment
1	DDP		rtmp	Routing Table Management Protocol
1	TCP & UDP		tcpmux	TCP port service multiplexer
2	DDP		nbp	Name Binding Protocol
21	TCP & UDP	Network > FTP	ftp	File Transfer Protocol (FTP) port; sometimes used by File Service Protocol (FSP)
22	TCP & UDP	Server > SSH	ssh	Secure Shell (SSH) service
25	TCP & UDP	Server > Email Notification	smtp	Simple Mail Transfer Protocol (SMTP)
67	TCP & UDP	Network > TCP/IP	bootps	Bootstrap Protocol (BOOTP) services; also used by Dynamic Host Configuration Protocol (DHCP) services
68	TCP & UDP	Network > TCP/IP	bootpc	Bootstrap (BOOTP) client; also used by Dynamic Host Control Protocol (DHCP) clients
80	TCP & UDP	Web Management Interface	http	HyperText Transfer Protocol (HTTP) for World Wide Web (WWW) services
81	TCP	Web Management Interface	HTTP	Hypertext Transport Protocol
88	TCP & UDP	Network > NFS	Kerberos	Kerberos Security (NFSv4)
111	TCP & UDP	<ul style="list-style-type: none"> • Networking > NFS • Assist • SnapServer Manager 	sunrpc	Remote Procedure Call (RPC) Protocol for remote command execution, used by Network Filesystem (NFS) and SnapServer Manager
123	TCP & UDP	Server > Date/Time > Advanced	ntp	Network Time Protocol (NTP)
137	TCP & UDP	Network > Windows/SMB	netbios-ns	NETBIOS Name Services used in Red Hat Enterprise Linux by Samba
138	TCP & UDP	Network > Windows/SMB	netbios-dgm	NETBIOS Datagram Services used in Red Hat Enterprise Linux by Samba
139	TCP & UDP	Network > Windows/SMB	netbios-ssn	NETBIOS Session Services used in Red Hat Enterprise Linux by Samba
161	TCP & UDP	Network > SNMP	snmp	Simple Network Management Protocol (SNMP)

Port #	Layer	GOS Feature	Name	Comment
162	TCP & UDP	Network > SNMP	snmptrap	Traps for SNMP
389	TCP & UDP	Network > Windows/SMB	ldap	Lightweight Directory Access Protocol (LDAP)
443	TCP & UDP	<ul style="list-style-type: none"> Web Management Interface SnapServer Manager SnapExtensions > Snap EDR 	https	Secure Hypertext Transfer Protocol (HTTP).
445	TCP & UDP	Network > Windows/SMB	microsoft-ds	Server Message Block (SMB) over TCP/IP
515	TCP	Server > Printing		LPD (Linux Printer Daemon)/LPR (Linux Printer Remote)
631	TCP & UDP	Server > Printing		IPP (Internet Printing Protocol)/CUPS (Common Unix Printing System)
852	TCP	Network > NFS		Used by rpc.mountd
882	UDP	<ul style="list-style-type: none"> Snap Finder SnapServer Manager 	Sysbroker	Broadcast Discovery
933	UDP	Network > NFS		Used by rpc.statd
936	UDP	Network > NFS		Used by rpc.statd
939	TCP	Network > NFS		Used by rpc.statd
957	UDP	Assist		Used by assistrecv
959	TCP	Assist		Used by assistrecv
2005	TCP	SnapExtensions	SnapExtensions	Bridge from Servlet to Snap Extension framework
2049	TCP & UDP	Network > NFS	nfs [nfsd]	Network Filesystem (NFS)
2050	UDP	Network > NFS	mountd	
2051	UDP	Network > NFS	lockd	
2599	UDP	<ul style="list-style-type: none"> Snap Finder SnapServer Manager 	Sysbroker	Multicast Discovery
3052	TCP	Server > UPS		Port for monitoring UPS status
3205	TCP	Network > iSCSI	iSNS	
3260	TCP	Network > iSCSI	iSCSI	
8001	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications
8002	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications
8003	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications
8005	TCP	Web Management Interface	tomcat	Tomcat Shutdown port
8008	TCP & UDP	Web Management Interface	http-alt	Tomcat - Apache Bridge
9049	TCP	Sysbroker		Sysbroker Shutdown Port

Port #	Layer	GOS Feature	Name	Comment
9050	TCP	Sysbroker		Sysbroker RPC Port
10001	TCP	Snap Extension	Snap Extension	Shutdown Port
12000	TCP & UDP	Network > Apple/AFP	afp2overtcp	Second NIC
12168	TCP	CA Antivirus	inoweb	Admin Interface
16384	UDP		Sysbroker	Random Port
16388	UDP		Sysbroker	Random Port
24066	TCP		poolmgr	Used by /bin/poolmgr
32780	TCP	Web Management Interface	tomcat	Random Port
32781	TCP	Web Management Interface	tomcat	Random Port
49221	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications Port
49229	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications Port
1024 - 65535	TCP & UDP	<ul style="list-style-type: none"> • Network > NFS • Network > FTP 	NFS FTP (passive)	Dynamically allocated in runtime for user connections

Master Glossary & Acronym List

NOTE: This is a general Overland Storage glossary and acronym list. Not all items may be found in this document or be used by this product.

1000BASE-T

1000BASE-T (also known as IEEE 802.3ab) is a standard for gigabit Ethernet over copper wiring. It requires, at a minimum, Category 5 cable (the same as 100BASE-TX), but Category 5e (Category 5 enhanced) and Category 6 cable may also be used and are often recommended. 1000BASE-T requires all four pairs to be present and is far less tolerant of poorly installed wiring than 100BASE-TX.

Address

An address is a data structure or logical convention used to identify a unique entity, such as a particular process or network device.

Algorithm

A sequence of steps designed to solve a problem or execute a process.

ATA

Short for *Advanced Technology Attachment*. A standard interface for connecting storage devices to a PC.

Authentication

The validation of a user's identity by requiring the user to provide a registered login name and corresponding password.

Autonegotiation

An Ethernet feature that automatically negotiates the fastest Ethernet speed and duplex setting between a port and a hub or switch. This is the default setting and is recommended.

Autosensing

An Ethernet feature that automatically senses the current Ethernet speed setting.

Bar Code

The machine-readable representation of a product code. Bar codes are read by a scanner that passes over the code and registers the product code. The width of black lines and white spaces between varies. Combinations of lines and spaces represent characters. Overland uses 3-of-9 code (Code 39) where each character is represented by 9 bars, 3 of which are wide.

Bus or Channel

A common physical path composed of wires or other media, across which signals are sent from one part of a computer to another. A channel is a means of transferring data between modules and adapters, or between an adapter and SCSI devices. A channel topology network consists of a single cable trunk that connects one workstation to the next in a daisy-chain configuration. All nodes share the same medium, and only one node can broadcast messages at a time.

CA

Short for *Certificate Authority*. A trusted third-party in a network that issues and manages security credentials.

Cat 5 Cable

Short for *Category 5*, it is network cabling that consists of four twisted pairs of copper wire terminated by 8P8C modular connectors. CAT 5 cabling supports frequencies up to 100 MHz and speeds up to 100 Mbps. It can be used for ATM, token ring, 100BASE-T, and 10BASE-T networking.

Cat 5 is based on the EIA/TIA 568 Commercial Building Telecommunications Wiring Standard developed by the Electronics Industries Association as requested by the Computer Communications Industry Association in 1985.

Cat 6 Cable

Short for *Category 6*, it is network cabling that consists of four twisted pairs of copper wire terminated by 8P8C modular connectors made to higher standards that help reduce noise caused by crosstalk and system noise. The ANSI/TIA-568-B.2-1 specification states the cable may be made with 22 to 24 AWG gauge wire, so long as the cable meets the specified testing standards.

It is designed for Gigabit Ethernet that is backward compatible with the Category 5/5e and Category 3 cable standards. Cat 6 features more stringent specifications for crosstalk and system noise. The cable standard provides performance of up to 250 MHz and is suitable for 10BASE-T, 100BASE-TX, and 1000BASE-T (Gigabit Ethernet).

Channel

A communications path between two computers or devices.

Checksum

The result of adding a group of data items that are used for checking the group. The data items can be either numerals or other character strings treated as numerals during the checksum calculation. The checksum value verifies that communication between two devices is successful.

CIFS

Short for *Common Internet Filesystem*. Also known as [SMB](#). The default Windows protocol for communication between computers. A specification for an Internet file access protocol that complements HTTP and FTP.

daemon

A process that runs in the background.

default gateway

The router used when there is otherwise no known route to a given subnet.

DHCP

Short for *Dynamic Host Configuration Protocol*. A communications protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a computer network. Each system that connects to the Internet/intranet needs a unique IP address.

Disaster Recovery

A strategy that allows a company to return to normal activities after a catastrophic interruption. Through failover to a parallel system or by restoration of the failed system, disaster recovery restores the system to its normal operating mode.

DNS

Short for *Domain Name Service*. A network service that translates domain names into IP addresses using a server that maintains a mapping of all host names and IP addresses. Normally, this mapping is maintained by the system administrator, but some servers support dynamic mappings.

Domain

A set of network resources in Windows 2000/2003/2008, such as users and groups of users. A domain may also include multiple servers on the network. To gain access to these network resources, the user logs into the domain.

Domain Name

The ASCII name that identifies the domain for a group of computers within a network.

Ethernet

The most widely installed LAN technology. 100BASE-T Ethernet provides transmission speeds of up to 100 Mbps. Fast Ethernet or 1000BASE-T provides transmission speeds up to 1000 Mbps and is typically used for LAN backbone systems, supporting workstations with 100BASE-T cards. Gigabit Ethernet (GbE) provides an even higher level of backbone support at 1000 Mbps (one Gigabit or one billion bits per second).

Ethernet Address

The unique six-digit hexadecimal (0-9, A-F) number that identifies the Ethernet interface.

Ethernet Port

The port on a network card to provide Ethernet access to the computer.

Event

Any significant occurrence or error in the system that may require notifying a system administrator or adding an entry to a log.

Expansion Slot

Area in a computer that accepts additional input/output boards to increase the capability of the computer.

Failover

A strategy that enables one Ethernet port to assume the role of another port if the first port fails. When the port comes back online, the original identities are restored. Failover is possible only in a multi-Ethernet configuration.

Failover/Failback

A combination of Failover and Failback. When a preferred path becomes unavailable, another path is used to route I/O until the preferred path is restored. In this case I/O will “fail back” to the preferred path once it is available again.

Fibre Channel

Fibre Channel (FC) is a gigabit-speed network technology which transports SCSI commands over Fibre Channel networks. Fibre Channel was primarily concerned with simplifying the connections and increasing distances, but later designers added the goals of connecting SCSI disk storage, providing higher speeds and far greater numbers of connected devices.

Firmware

Software stored in read-only memory (ROM) or programmable ROM (PROM). Firmware is often responsible for the behavior of a system when it is first switched on.

FTP

Short for *File Transfer Protocol*. A standard Internet protocol that provides a way to exchange files between computers on the Internet.

Full-duplex

A type of transmission that allows communicating systems to both transmit and receive data simultaneously.

Gateway

The hardware or software that bridges the gap between two network subnets. It allows data to be transferred among computers that are on different subnets.

Gigabit Ethernet

Also known as GigE or GbE, this Ethernet standard uses a one Gigahertz (1000 Hz) clock rate to move data.

HBA

Short for *Host Bus Adapter*. An HBA is an I/O adapter that sits between the host computer's bus and the Fibre Channel loop and manages the transfer of information between the two channels. In order to minimize the impact on host processor performance, the HBA performs many low-level interface functions automatically or with minimal processor involvement.

Half-duplex

A type of transmission that transfers data in one way at a time.

Hidden Share

A share that restricts the display of the share via the Windows (SMB), Web Home (HTTP/HTTPS), FTP, and AFP protocols. See also [SMB](#).

Host Name

The unique name by which a computer is known on a network. It is used to identify the computer in electronic information interchange.

Hot Swapping

The ability to remove and add disk drives to a system without the need to power down or interrupt client access to filesystems. Not all components are hot-swappable. Please read installation and maintenance instructions carefully.

HTTP

Short for *Hypertext Transfer Protocol*. An application protocol for transferring files (text, graphic images, sound, video, and other multimedia files) over TCP/IP on the World Wide Web.

HTTPS

Short for *Hypertext Transfer Protocol Secure*. The HTTP protocol using a Secure Sockets Layer (SSL). SSL provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.

Inheritance

In Windows permissions, inheritance is the concept that when permissions for a folder are defined, any subfolders within the defined folder inherit its permissions. This means an administrator need not assign permissions for subfolders as long as identical permissions are desired. Inheritance greatly reduces administrative overhead and also results in greater consistency in access permission management.

Initiator Device

An iSCSI system component that originates an I/O command over an I/O bus or network. An initiator issues the commands; a *target* receives them.

An initiator normally runs on a host computer. It may be either a software driver or a hardware plug-in card, often called a Host Bus Adapter (HBA). A software initiator uses one of the computer's Ethernet ports for its physical connection, whereas the HBA will have its own dedicated port.

Software initiators are readily available for most host operating systems. Hardware initiators are not widely used, although they may be useful in very high performance applications or if 10 Gigabit Ethernet support is required.

I/O (Input/Output)

The operation of transferring data to or from a device, typically through an interface protocol like CIFS, NFS, or HTTP.

IP

Short for *Internet Protocol*. The unique 32-bit value that identifies the location of the server. This address consists of a network address, optional subnetwork address, and host address. It displays as four addresses ranging from 1 to 255 separated by periods.

IQN

Short for *iSCSI Qualified Name*. A name format used in the iSCSI protocol. Initiators and targets have IP addresses, just like any other network entity. They are also identified using an iSCSI name, called the iSCSI Qualified Name (IQN). The IQN should be unique worldwide. It is made up of a number of components, specifying the date, identifying the vendor in reverse format, and then uniquely identifying the initiator or target. An example of an IQN is:

```
iqn.2001-04.com.example:storage:diskarray-sn-123456789
```

Since these IQNs are rather unwieldy, initiators and targets also use short, user friendly names (sometimes called alias names or just aliases).

iSCSI

Short for *Internet SCSI*. iSCSI is an IP-based storage networking standard for linking data storage facilities. iSCSI is a standard that defines the encapsulation of SCSI packets in TCP and then routing it using IP. It allows block-level storage data to be transported over widely used IP networks.

iSNS Server

Short for *Internet Storage Name Service Server*. A protocol enabling the automatic discovery, configuration, and management of iSCSI devices on a TCP/IP network.

Kerberos

A secure method for authenticating a request for a service used by ADS. Kerberos lets a user request an encrypted “ticket” from an authentication process that can then be used to request a service from a server. The user credentials are always encrypted before they are transmitted over the network.

In Windows 2000/XP, the domain controller is the Kerberos server. The Kerberos key distribution center (KDC) and the origin of group policies are applied to the domain.

LAN

Short for *Local Area Network*. A network connecting computers in a relatively small area such as a building.

LCD

Short for *Liquid Crystal Display*. An electronic device that uses liquid crystal to display messages.

LED

Short for *Light-Emitting Diode*. An LED is a type of diode that emits light when current passes through it. Visible LEDs are used as indicator lights on electronic devices.

Linux

A UNIX-like operating system that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive UNIX systems.

Load Balancing

A process available only in multi-Ethernet configurations. The Ethernet port transmission load is distributed among two or more network ports (assuming the cards are configured for load balancing). An intelligent software adaptive agent repeatedly analyzes the traffic flow from the server and distributes the packets based on destination addresses.

MAC Address

Short for *Media Access Control address*, a hardware address that uniquely identifies each node of a network. In the Open Systems Interconnection (OSI) model, one of two sublayers of the Data Link Control layer concerned with sharing the physical connection to the network among several computers. Each Ethernet port has a unique MAC address.

MD5 Algorithm

MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods.

MIB

Short for *Management Information Base*. A formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of SNMP.

Mirroring

Used in RAID 1 and 10, a process of storing data on one disk and copying it to one or more disks, creating a redundant storage solution. RAID 1 is the most secure method of storing mission-critical data.

Mounted

A filesystem that is available.

MPIO

Short for *Multipath Input/Output*. A multipath solution built into Microsoft server-grade iSCSI operating systems.

MTU

Short for *Maximum Transfer Unit*. It is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network.

NIC

Short for *Network Interface Card*. A board that provides network communication capabilities to and from a computer.

NIS

Short for *Network Information Service*. It is a client–server directory service protocol for distributing system configuration data such as user and host names between computers on a computer network. Sun Microsystems developed the NIS; the technology is licensed to virtually all other Unix vendors.

NTFS

Short for *New Technology File System*. The standard file system used by Windows NT and later versions of the Windows operating system.

NTP

Short for *Network Time Protocol*. A protocol for synchronizing the system clocks of computers over a packet-switched network.

NVRAM

Abbreviation of *Non-Volatile Random Access Memory*, a type of memory that retains its contents when power is turned off.

Permissions

A security category, such as no access, read-only, or read-write, that determines what operations a user or group can perform on folders or files.

PoP

Short for *Proof of Purchase*. The number used to obtain a license key for an upgrade to third-party applications.

Portal

A target's IP address together with its TCP port number used in iSCSI systems.

POSIX

Short for *Portable Operating System Interface*. A set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to develop programs that could run on multiple platforms without the need to recode.

Protocol

A standardized set of rules that specifies the format, timing, sequencing, and/or error checking for data transmissions.

PTP

Short for *Point-to-Point*. PTP is the common mode of attachment to a single host. PTP is sometimes used to attach to a Fibre Channel switch for [SAN](#) connectivity.

Quota

A limit on the amount of storage space on a volume that a specific user or NIS group can consume.

Router

A router is a device that enables connectivity between Ethernet network segments.

SAN

Short for *Storage Area Network*. Data storage connected to a network that provides network clients access to data using block level protocols. To the clients, the data storage devices appear local rather than remote. An iSCSI SAN is sometimes referred to as an IP-SAN.

SAS

Short for *Serial Attached SCSI*. It is a point-to-point serial protocol that replaces parallel SCSI bus technology (multi-drop) and uses the standard SCSI command set. It has no termination issues, supports up to 16,384 devices (using expanders), and eliminates clock skew. It consists of an Initiator that originates device service requests, a Target containing logical units that receives device service requests, and a Service Delivery Subsystem that transmits information between the Initiator and the Target.

Session

When an initiator wants to establish a connection with a target, it establishes what is known as an iSCSI session. A session consists of one or more TCP/IP connections between an initiator and a target. Sessions are normally established (or re-established) automatically when the host computer starts up, although they also can be established (and broken) manually.

SMB

Short for *Server Message Block*. A protocol for Windows clients. SMB uses the TCP/IP protocol. It is viewed as a complement to the existing Internet application protocols such as FTP and HTTP. With SMB, you can access local server files, obtain read-write privileges to local server files, share files with other clients, and restore connections automatically if the network fails.

SMTP

Short for *Simple Mail Transfer Protocol*. A TCP/IP protocol used for sending and receiving email.

SNMP

Short for *Simple Network Management Protocol*. A system to monitor and manage network devices such as computers, routers, bridges, and hubs. SNMP views a network as a collection of cooperating, communicating devices, consisting of managers and agents.

SSH

Short for *Secure Shell*. A service that provides a remote console for special system administration and customer support access to the server. SSH is similar to telnet but more secure, providing strong encryption so that no passwords cross the network in clear text.

SSL

Short for *Secure Sockets Layer*. A protocol for managing the security of a message sent on the Internet. It is a type of technology that provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.

Standalone

A network bonding mode which treats each port as a separate interface. This configuration should be used only in multihomed environments in which network storage resources must reside on two separate subnets.

Static IP Address

An IP address defined by the system administrator rather than by an automated system, such as DHCP.

Storage Area Network

See [SAN](#).

Subnet Mask

A portion of a network that shares a common address component. On TCP/IP networks, subnets are all devices with IP addresses that have the same prefix.

Target

A target is a device (peripheral) that responds to an operation requested by an initiator (host system). Although peripherals are generally targets, a peripheral may be required to act temporarily as an initiator for some commands (for example, SCSI COPY command).

Targets are embedded in iSCSI storage controllers. They are the software that makes the RAID storage available to host computers, making it appear just like any other sort of disk drive.

TCP/IP

Short for *Transmission Control Protocol/Internet Protocol*. The basic protocol used for data transmission over the Internet.

Trap

A signal from a device informing an SNMP management program that an event has occurred.

U

A standard unit of measure for designating the height in computer enclosures and rack cabinets. One U equals 1.75 inches. For example, a 3U server chassis is 5.25 inches high.

UDP

Short for *User Datagram Protocol*. A communications protocol for sending messages between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol but, unlike TCP, does not guarantee reliability or ordering of data packets.

UPS

Short for *Uninterruptible Power Supply*. A device that allows a computer to keep running for a short time when the primary power source is lost. It also provides protection from power surges. A UPS device contains a battery that starts when the device senses a loss of power from the primary source.

URL

Short for *Uniform Resource Locator*. A Web address.

USB Port

USB is short for *Universal Serial Bus*. A USB port is a hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer, and telephony devices.

Web Management Interface

A Web-based utility used for configuration and ongoing maintenance, such as monitoring server conditions, configuring email alerts for key events, or for SNMP management.

Windows Domain Authentication

Windows-based networks use a domain controller to store user credentials. The domain controller can validate all authentication requests on behalf of other systems in the domain. The domain controller can also generate encrypted challenges to test the validity of user credentials. Other systems use encrypted challenges to respond to CIFS/SMB clients that request access to a share.

WINS

Short for *Windows Internet Naming Service*. The server that locates network resources in a TCP/IP-based Windows network by automatically configuring and maintaining the name and IP address mapping tables.

Workgroup

A collection of computers that are grouped for sharing resources such as data and peripherals over a LAN. Each workgroup is identified by a unique name.

Symbols

> (menu flow indicator) **iv**

A

access

problems with **247**

Access Denied message **248**

ACLs

backing up **187**

resetting to defaults **185**

setting file-level permissions (Windows) **243**

Active Directory

and name resolution servers **44**

joining Active Directory domain **47**

SnapServer interoperability with **45**

admin password

default **139**

resetting forgotten **185, 250**

Administration page **208**

administration password **207**

AFP terminology **50**

AFP, see *Mac OS*

alert definitions **iv**

Antivirus

dependencies on other software components **218**

distributing updates **223**

excluding snapshots from **220**

HTTP requirement **218**

launching configuration GUI **219**

scan job configuration **220**

using logs **226**

Application Notes **235**

Authentication

default settings **139**

HTTPS/HTTP **60**

Kerberos **45**

LDAP domain **55**

NIS domain **54**

automatic incorporation, and previously configured drives **90**

automatic shutdown **27**

B

background disk scan **90**

backup

coordinating with snapshots **113**

inability to back up iSCSI disks **111, 119**

iSCSI disks **119**

of server and volume settings **186**

off-the-shelf solutions **235**

backup.acl **187**

backup.qta.groups **187**

backup.qta.users **187**

BitTorrent Sync **210**

C

CA Antivirus **212, 218**

CA Unicenter TNg **59**

change password **207, 215**

changing server name **23**

CLI connection via SSH **25**

client access, configuring

Apple **49**

FTP **57**

HTTPS/HTTP **60**

NFS **51**

Command Line Interface **252**

running scripts **260**

syntax **252**

connecting

to SnapServers **5**

conventions, typographical **iv**

create new share **95**

create new volume **95**

CUPS server 29
customer support iii

D

data import 192
data protection tasks 21
date and time settings 24
defaults
 admin password 139
 TCP/IP 35
directories, home 175
Disaster Recovery
 backing up server and volume settings 186
 creating recovery files 187
discovering server name 5
disk drives
 adding
 in DynamicRAID 67, 75, 230
 in Traditional RAID 93
 automatic incorporation 90
 and previously configured drives 90
 detecting 12
 hot swap 130
 incompatible 67
 LED indicators 245
 previously configured 67, 230
 in different system 14, 67
 in Traditional RAID 94
 reintegrating orphaned 135
 replacing 130
disk icons 75, 129
Disk is Foreign icon 75
domain search
 authentication required 104, 149, 166, 170
download software web link iii
drive rotational speeds 85
drive-size characteristics, DynamicRAID 231
dual parity 130
dynamic volumes 229
DynamicRAID 65
 compared to Traditional RAID 229
 drive indicators 231
 how it works 230
 implementation 230
 storage pools 66
 volumes 76

E

email notification of server events 201
Ethernet, see *Gigabit Ethernet*
Expand Volume button 99
expansion units 6
 adding to Traditional RAID 89
 configuring initial setup of 16
 DynamicRAID usage 71
 integrating orphans 137
 SnapExpansion usage 6
 Traditional RAID usage 89
exports file, NFS 143

F

failover, see *Network bonding*
file/folder security information 207
files, setting permissions for 242
FTP
 configuring access 54

G

GID 140
Gigabit Ethernet
 autonegotiation required 38
global hot spares 82
Global Spare 135
Groups
 creating local 159
 file-level access for 242
GuardianOS
 ports 265
 specifications 2
 updating 197

H

hardware information screen 21
Head Unit properties page 71
home directories 175
Home page 62, 207
home pages 207, 208
hot spares 82
hot swap
 and automatic incorporation of disks 90
 disk drive 130

HP Open View **59**

HTTPS/HTTP

configuring **60**

I

ID mapping **165**

increase capacity **6**

Initial Setup

configuring storage

expansion units **16**

in DynamicRAID **13**

in Traditional RAID **14**

wizard **7**

integrate expansion units **137**

internal temperature, e-mail notification of **202**

IP address

setting **37**

using SSM to discover **5**

IPP port number

Linux **30**

Windows **30**

iSCSI disks **117**

and DynamicRAID **231**

backing up **125**

configuring iSNS **63**

creating **122**

LUNs **128**

multi-initiator support **120**

write cache options **120**

iSNS **63**

K

Kerberos **45**

key icon **207**

L

LDAP domains **55**

LEDs

disk drive indicators **245**

in DynamicRAID **231**

network **246**

power/unit status **246**

system/status **246**

understanding **244**

Link Aggregation (802.3ad) **36**

load balancing, configuring server for **37**

local groups **159**

local hot spares **82**

login

SnapServer **7**

to antivirus GUI **219**

M

Mac OS

configuring client access **49**

Finder **50**

Macintosh, supported OS versions **2**

maintenance

data import **192**

disaster recovery **186**

factory defaults **184**

OS update **196**

shutdown and restart **184**

support **199**

tools **200**

managing snapshots **109**

mapping, ID **165**

menu flow indicator **iv**

mixed drive capacities **229**

mixed drive types **229**

monitoring

system **178**

tape **182**

Multihomed configurations **38**

N

network

access **32**

bonding, cabling requirements for **39**

current settings **33**

LED indicators **246**

problems with access **247**

reset to factory defaults **185**

NFS

access **51**

configuring **51**

exports file **143**

read-only share access **52**

share-level permissions **151**

NIS domains **54**

O

- orphaned disk drive **135**
- orphaned disk drives **135**
- OS update **196**
- Overland technical support **iii**

P

- parity
 - adding disk drives to upgrade **75**
 - configuring DynamicRAID **230**
 - disk drive failure
 - dual **75**
 - single **75**
 - increasing protection **75**
 - management **74**
 - options **229**
 - Parity Mode **67, 72**
 - Parity Mode change **133**
 - removing a drive **133**
- parity, dual **130**
- password
 - changing **215**
 - default for admin account **139**
 - unlock **157**
- password expiration **139**
- paths
 - for backing up snapshots **113**
 - for distributing antivirus updates **223, 224**
 - for restoring a “cured” file **225**
- permissions
 - share- and file-level interaction **148**
 - file-level, default behavior **242**
- Phone home support **251**
- power/status LED **246**
- Print Server **29**
 - adding a printer **29**
 - canceling print jobs **31**
 - configure the printer **29**
 - deleting a printer **31**
 - IPP port number, Linux **30**
 - IPP port number, Windows **30**
 - monitoring print jobs **30**
 - pausing the printer **30**
- product documentation **iii**

Q

- Quota
 - Sort drop-down list **105**
 - View drop-down list **106**
- Quotas
 - adding **105**
 - backing up configuration **187**
 - defaults **101**
 - displaying **105**
 - properties **102**
 - usage calculation **101**

R

- RAID
 - adding disk drives to **93**
 - choosing **81**
 - creating new **83**
 - effect of deleting on antivirus software **218**
 - grouped
 - deleting **89**
 - grouping **86**
 - multiple RAIDs **89**
 - with other grouped RAIDs **89**
 - scrubber **90**
 - sets
 - creating new **83**
 - grouping **86**
 - screen **83**
 - settings **90**
 - Traditional RAID and replacement disks **93**
 - type selection **10**
 - reboot, setting up alert for **202**
 - reduced parity with Traditional RAID **93**
 - remote SnapServer discovery **214**
 - replacing disk drives **130**
 - replication **233**
 - reset options **246**
 - restart **184**
 - resynchronization, setting alert for completion of **202**
 - rotational speeds of drives **85**
-
- S**
 - Secure Shell (SSH) **25**
 - security
 - guides **140**

- models **162**
 - resetting default ACLs for volumes **185**
 - shares **143**
 - Windows ACLs **242**
 - server
 - and volume settings, backing up **186**
 - changing server name **23**
 - discovering server name **5**
 - options **23**
 - registration, via Web Management Interface **199**
 - status **19**
 - Shares **143**
 - backing up configuration **187**
 - delete **147**
 - edit properties **146**
 - shares with Admin rights **207**
 - shutdown **184**
 - Simple Network Management Protocol, see *SNMP*
 - Single-subnet configuration **38**
 - site map **19, 206**
 - server links **23**
 - SMB **43**
 - SMTP methods supported **201**
 - Snap EDR **212, 233**
 - Snap Finder **213**
 - SnapCLI **252**
 - running scripts **260**
 - syntax **252**
 - SnapDRImage **187**
 - SnapExpansion **6**
 - SnapExtensions
 - BitTorrent **210**
 - CA Antivirus **212, 218**
 - main page **210**
 - Snap EDR **212**
 - SnapServers
 - configuring email notification of server events **201**
 - connecting to **5**
 - setting e-mail alerts for **202**
 - snapshot
 - access **240**
 - autobackup of volume settings **187**
 - combined pools **89**
 - coordinating with backup jobs **113**
 - estimating storage requirements for **114**
 - excluding from antivirus scans **220**
 - excluding iSCSI Disks from **120**
 - managing **109**
 - shares **241**
 - ways to adjust pool size **114**
 - snapshot share **241**
 - SNMP configuration **60**
 - SNMP configuration page **59**
 - software update **iii**
 - specifications, GuardianOS **2**
 - speed/duplex options **38**
 - standalone **38**
 - storage
 - guides **81**
 - pools **66**
 - and incompatible disk drives **67**
 - creating initial **13**
 - RAID Sets screen **83**
 - Volumes screen **94**
 - storage pools
 - and expansion units **71**
 - support **199**
 - switch user (logout) **208**
 - system monitor **178**
 - system reset **246**
 - system/status LED **246**
- ## T
- tape monitor **182**
 - TCP/IP
 - configuring **37**
 - initial configuration **10**
 - options **35**
 - technical support **iii**
 - terminology for AFP **50**
 - Tivoli NetView **59**
 - tools **200**
 - Traditional RAID **80, 138**
 - adding disk drives **93**
 - and expansion units **89**
 - compared to DynamicRAID **229**
 - quotas **101**
 - RAID sets **81**
 - shares **81**
 - storage guides **81**
 - volumes **81**
 - troubleshooting **244**
 - typographical conventions **iv**

U

UID **140**

Uninterruptable Power Supplies (UPS) **27**

unlock a user password **157**

updates to GuardianOS **196**

UPS

 configuring **27**

 enabling support for **27**

 low-power warning **27**

users

 creating local **154**

 file-level access for **242**

write cache **98, 120**

V

volumes

 and DynamicRAID **76**

 and Traditional RAID **94**

 backing up configuration **186**

 capacity reached alert **202**

 dynamic **229**

 effect of deleting on antivirus software **218**

 expanding capacity of **98**

 Properties screen **98**

 quotas **230**

 screen **94**

 size limits **230**

W

Wake-on-LAN Support **6**

Web Management Interface, overview **19**

Web Root **62**

Web Server **62**

Windows

 enabling guest account access **46, 48**

 guest account access **45**

 issues with PDC **248**

 name resolution server support **44**

 networking (SMB) **43**

 security, joining

 active directory domain **47**

 see also *Active Directory*

 see also *Authentication*

Windows Active Directory **45**

 setup **141**

 Shares **143**