



Overland
Storage

SnapServer Manager™

Users Guide

For SnapServers® Using GuardianOS™ Version 7.1



December 2011
10400352-001



©2010-11 Overland Storage, Inc. All rights reserved.

Overland®, Overland Data®, Overland Storage®, LibraryPro®, LoaderXpress®, Multi-SitePAC®, NEO®, NEO Series®, PowerLoader®, Protection OS®, REO®, REO 4000®, REO Series®, Snap Care®, SnapServer®, StorAssure®, and XchangeNOW® are registered trademarks of Overland Storage, Inc.

GuardianOST™, SnapWrite™, Snap Enterprise Data Replicator™, SnapExpansion™, SnapSAN™, and SnapServer Manager™ 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 products 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 7.1

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 users charged with managing SnapServer appliances running GuardianOS 7.1 on their network using SnapServer Manager (SSM). It provides server tasks, tips on maximizing SSM functionality, and user scenarios. SnapServer Manager is usually installed on a network computer in the same SAN as the SnapServers it manages.

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

Product Documentation

The SnapServer Manager product documentation and additional literature are available online, along with the latest release of both the SnapServer Manager and GuardianOS 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 Manager, search for help at:

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

You can email our technical support staff at techsupport@overlandstorage.com or get additional technical support information on the [Contact Us](#) web page:

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

For a complete list of support times depending on the 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 command buttons 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.

Software Updates

The latest release of the GuardianOS software can be obtained from the Downloads and Resources (NAS Solutions) page at the Overland Storage website:

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

Follow the appropriate instructions to download the **latest** software file.

For additional assistance, search at <http://support.overlandstorage.com/>.

Finding More Information

Product documentation related to GuardianOS SnapServers and expansion arrays are listed below. The current versions of all these documents are always available from the Overland Storage NAS Solutions website (<http://docs.overlandstorage.com/snapserver>).

Source	Location	Content
<i>Quick Start Guide</i>	Product Packaging and Web	Provides complete instructions for installing the server into a rack and connecting the server to the network. Also contains links to warranty registration and information.
<i>Quick Start Guide Translations</i>	Web	Quick Start Guide is translated into French, Italian, German, Spanish, and Russian.
<i>EULA</i>	Product Packaging and Web	End User License Agreement for GuardianOS.
<i>Administrator's Guide</i>	Web	Provides an overview of the configuration, maintenance, and troubleshooting of SnapServers, the administration of the CA Antivirus software, the installation of third-party backup agents, and detailed instructions on using the Web Management Interface.
<i>SnapServer Online Help</i>	Web Management Interface via the Overland Website	Basic troubleshooting information embedded in the software with direct links to additional information from the Administrator's Guide.

Electrostatic Discharge Information

A discharge of static electricity can damage static-sensitive devices. Proper packaging and grounding techniques are necessary precautions to prevent damage. To prevent electrostatic damage, observe the following precautions:

- Transport products in static-safe containers such as conductive tubes, bags, or boxes.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free stations.
- Cover the appliance with approved static-dissipating material.
- Use a wrist strap connected to the work surface and properly-grounded tools and equipment.
- Keep the work area free of non-conductive materials such as foam packing materials.
- Make sure you are always properly grounded when touching a static-sensitive component or assembly.
- Avoid touching pins, leads, or circuitry.

Preface

Chapter 1 - Overview

Tips and Requirements	1-1
SnapServer Manager Main Window	1-2
Server Column Status Icons	1-3
Status Column Icons (GuardianOS only)	1-3
Communication Indicators	1-4
Software Update Notification Banner	1-5
Features List	1-5
GuardianOS-Only Features	1-5
Features Common to All Platforms Supported by SSM	1-6
Discovery	1-7
Local Discovery	1-7
Remote Discovery	1-8
Laptop SSM Installation and Remote Server Discovery	1-8
Customizing the SSM Interface	1-9
Server Groups	1-10
The Server Details List	1-12
Usage Scenarios for GuardianOS Servers	1-13
Viewing GuardianOS Server Settings/Generating a Report	1-14
Configuring Multiple GuardianOS Servers/Setting Up Email Notification	1-14
Copying Settings Among GuardianOS Servers	1-14
Scheduling an OS Update for Multiple GuardianOS Servers	1-15

Chapter 2 - Administer Servers

Server Name	2-2
Date/Time	2-3
Admin Password	2-5
Email Notification	2-6
SSH	2-8
UPS	2-8
Windows/SMB	2-10
Apple/AFP	2-12
NFS	2-14
NIS	2-15
FTP/FTPS	2-16
SNMP	2-17
Web	2-19
Shutdown	2-20

Restart	2-21
OS Update	2-21

Chapter 3 - SSM Dialog Box Reference

Server Properties	3-1
Ethernet Indicators (GuardianOS only)	3-2
The Discovery IP Address	3-2
Total Storage Usage (GuardianOS only)	3-3
Remote Servers	3-3
Available Options	3-3
Importing a Remote Server List	3-4
Options	3-4
Specify a Web Browser	3-5
Adjust the Server Offline Timeout Setting	3-5
Display No-Link Status Warnings for Ethernet Ports (GuardianOS only)	3-5
Activate Auto-scanning of All Remote Servers	3-5
Use an HTTP Proxy Server (GuardianOS only)	3-5
Enable Automatic Update Notification (GuardianOS only)	3-6
Administering Servers	3-6
Configure Settings	3-6
View or Copy Settings	3-7
Apply Schedule (Start Later)	3-7
Schedule Operations to Run at a Later Time	3-8
Change a Scheduled Operation	3-8
Apply to Servers	3-8
Available Options	3-9
Improve the Readability of the Display	3-9
Operations Report	3-9
View a Sample Operations Report	3-10
Configure SSM to Automatically Deliver Operations Reports By Email	3-10
Save a Single Copy of an Operations Report	3-10
Current Settings for Servers	3-11
Available Options	3-11
Improve the Readability of the Display	3-12
Set IP Address	3-12
Feature Licensing	3-13
Server Software Updates	3-13

Index

SnapServer Manager (SSM) is a Java-based application that runs on all major client platforms. SSM provides a single screen from which administrators can discover all SnapServers and REO 4600 appliances on their network, and launch an external application or browser for configuration and management. Additionally, SSM can monitor, upgrade, and configure network and administrative settings on one or more GuardianOS servers simultaneously.

This section is divided into sub-sections that provide the key processes and configuration options needed to maximize your usage of SnapServer Manager:

- [Tips and Requirements](#) – Provides technical specifications and tips you need to know before you begin using SSM.
- [SnapServer Manager Main Window](#) – Shows how to select the GuardianOS servers you want to administer with SSM, then navigate to Administration > Administer Servers.
- [Features List](#) – Covers the multiserver and single-server functions available for GuardianOS servers in SSM.
- [Discovery](#) – Explains how SSM discovers and maintains contact with SnapServers and REO 4600 appliances. This section is of particular interest to administrators who plan to install SSM on a laptop.
- [Customizing the SSM Interface](#) – Provides advanced procedures for creating Server Groups and customizing the Server Details list.
- [Usage Scenarios for GuardianOS Servers](#) – Shows common scenarios providing the fastest way to learn how to use SSM.

Tips and Requirements

Consider the following technical tips and requirements when deploying SnapServer Manager on the network.

Normalize Admin Passwords for Server Groups (GuardianOS servers only)

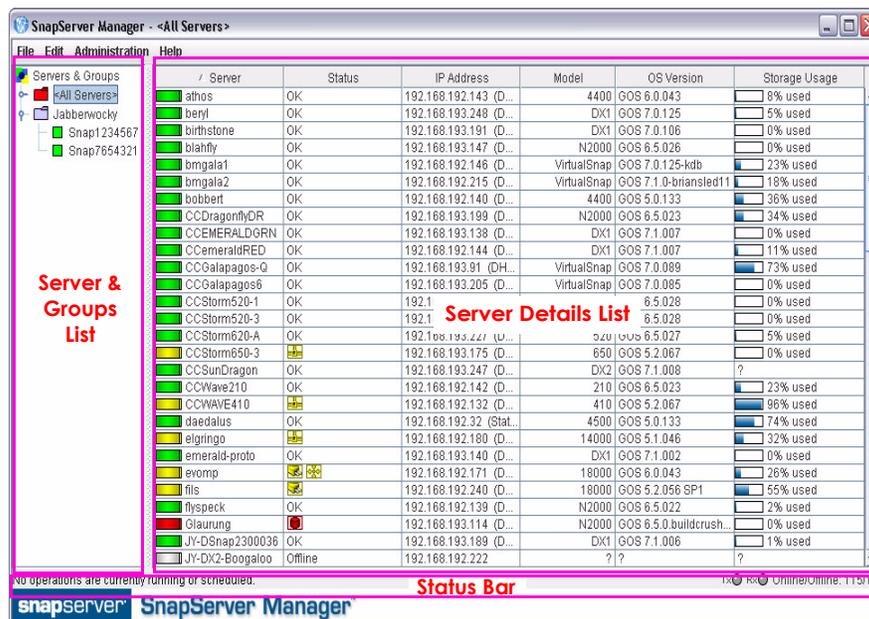
Before you can configure a server group, SnapServer Manager asks for the admin password for each server in the group. If the servers in the group have different passwords for the admin account, you will have to remember and enter the password for each server in the group before you can perform any operations. Normalizing the password for the admin account for each server group allows you to gain administrative access to all servers in the group by entering a single password.

Right-Click vs. Control-Click

This document uses the Windows convention of right-clicking in describing keyboard access to context-sensitive menus. Macintosh users should substitute control-click to achieve the same result.

SnapServer Manager Main Window

The SnapServer Manager main window allows an administrator instant access to all the servers on the network.



The SnapServer Manager main screen is divided into three sections:

- **Server & Groups List** – Located on the left, it provides a collapsible list of servers that can be sorted into groups for easier management.
- **Server Details List** – This largest section in the middle shows detailed information about each GuardianOS server.
- **Status Bar** – Located at the bottom of the screen, it provides specific information about operations, transmissions, and availability.

Because it is a graphical interface, the main screen is able to convey large amounts of information using specialized SSM icons for servers and their statuses.

Server Column Status Icons

The Server Details list of SnapServer Manager has visual cues to the status and health of the servers on your network. The following color scheme applies to all icons you see on the SnapServer Manager main window and any sub-windows that are displayed:

Color	Description
	The server is online.
	One or more status indicators indicate a warning-level condition (GuardianOS only).
	One or more status indicators indicate a fault-level condition (GuardianOS only).
	The server is offline.

Status Column Icons (GuardianOS only)

The Server Details list also uses the following status icons to alert users to the different functions on GuardianOS servers. These icons follow the above color coding alerts and will turn the appropriate color depending on the alert. Any problems will appear in the Status column.

To check the status of a server, double click the server name to open the Properties screen for that server. For information on customizing the Server Details list, see [“Customizing the SSM Interface” on page 1-8](#).

Icon	Description
Drive Status – Indicates whether a drive error has occurred. Double-click the server name to check the specific problem.	
	All disks are OK.
	A disk has failed.
	Disk status is not available (server may be offline).
Ethernet Status – Indicates whether an error has occurred with a NIC. Double click the server name to check the specific problem.	
	All Ethernet ports are OK.
	An Ethernet port has no link.
	An Ethernet port has failed, or one Ethernet port in a bonded pair has no link.
	NIC status is not available (server may be offline).
Power Supply Status – Indicates whether the power to the server has encountered a problem. Double click the server name to check the specific problem.	
	All power supplies are OK.
	A power supply is missing, has failed, or is not plugged in.
	Power supply status is not available (server may be offline).

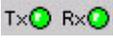
Icon	Description
Fan Status – Indicates whether a fan on the server has encountered a problem. Double click the server name to check the specific problem.	
	All fans are OK.
	A fan is missing or has failed.
	Fan status is not available (server may be offline).
System/CPU Temperature – Indicates whether the server system or CPU temperature has changed to possibly harmful levels. Double click the server name to check the specific problem.	
	System or CPU temperature is OK.
	System or CPU temperature is high.
	System or CPU temperature is critical.
	Temperature status is not available (server may be offline).

For GuardianOS servers, the Server Details list also displays a disk usage icon that shows what percentage of the space on the main volume is being used.

Icon	Description
	Disk Usage – The blue bar indicates how much of the space on the server main volume has been used. The numerical usage percentage is shown to the right.

Communication Indicators

For all supported platforms, the Status Bar displays two LED indicators that monitor the transmission of discovery packets. Discovery packets are used to monitor the status of servers that SSM is monitoring. The LED indicators are located next to the count of online and offline servers at the bottom right of the screen. For more information about discovery packets, please see [“Discovery” on page 1-6](#).

Icon	Description
	<p>Tx stands for “Transmit” and lights whenever SSM sends out a request for discovery information.</p> <p>Rx stands for “Receive” and lights whenever SSM receives a server discovery packet.</p> <p>The mouse over tooltip displays the number of packets transmitted and received, respectively.</p>

Software Update Notification Banner

A banner is displayed across the top of the Server Details area whenever GuardianOS updates are available for discovered servers.

Tip: The Server Software Update Notification feature is enabled by default, but can be disabled from **Edit > Options**.

The **Tell me more** link in the banner opens the Server Software Updates dialog, listing servers for which an update is available, the version of GuardianOS each server is currently running, and the version to which each server could be updated.

Tip: 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.

Features List

SnapServer Manager can be used to discover SnapServers and REO 4600 appliances; however, status monitoring and advanced multiserver and single-server administration functions are available only for GuardianOS SnapServers.

GuardianOS-Only Features

The following functions are available for only GuardianOS SnapServers. For information on how to perform the multiserver operations summarized below, see [“Usage Scenarios for GuardianOS Servers” on page 1-12](#).

Registering One or More Servers

To register multiple GuardianOS servers, select the servers in the SSM screen, and then select **Administration > Register Servers**. A separate browser window opens to a product registration form in which some of your product information may already be entered.

Simultaneous Application of Settings to Server Groups

SnapServer Manager allows administrators to organize servers into functional groups and to apply configuration modifications simultaneously to all GuardianOS servers within a group. For example, administrators can configure domain and other network settings for any number of SnapServers in one operation and be confident the settings are consistently applied across servers.

Comparing Settings Across Servers

SnapServer Manager can compare settings across any number of GuardianOS servers and identify when settings differ among servers. For example, comparing protocol access configuration for a group of servers may reveal that settings are consistent for Windows, NFS, and AFP but that differences exist among servers in HTTP/HTTPS and FTP/FTPS settings.

Assigning IP Addresses to SnapServers on a Network Without a DHCP Server

By default, SnapServers are preconfigured to use DHCP to acquire an IP address at startup. If a SnapServer cannot find a DHCP server on the network, you may not be able to access the server. SSM discovers all SnapServers on its local subnet using a proprietary multicast communication mechanism.

To set a static IP address, right-click the server name in the Server Details list and select **Set IP Address**.

Copying Settings from One Server to One or More Different Servers

SnapServer Manager can copy selected settings (TCP/IP, SNMP, SMB access, etc.) from any GuardianOS server to one or more different GuardianOS servers. See [Chapter 3, “Current Settings for Servers”](#).

Scheduling Operations to Run During Off-peak Hours

Operations can be scheduled to run on multiple GuardianOS servers during off-peak hours. [Chapter 3, “Apply Schedule \(Start Later\)”](#).

Automatic Email Notification of Completed Operations

SnapServer Manager can automatically create and send an operations report (CSV format) upon the completion of any operation. See [Chapter 3, “Operations Report”](#).

Monitoring Server Status

The color coding of server and group names alerts administrators to warning and fault conditions on a server. To view detailed status information, double-click the server row in the SSM screen. See [“Server Column Status Icons” on page 1-3](#).

Software Update Notification

SnapServer Manager is configured to check daily for available updates to the GuardianOS and to display an alert at the top of the Server Details list when updates are available.

To force SSM to check for available updates immediately, click **Administration > Check for Server Software Updates**. SSM will connect to the remote software update server, search for applicable updates for all of the discovered servers, and display them in the Server Software Updates dialog box.

Features Common to All Platforms Supported by SSM

Except where noted, the following single-unit features are available for all platforms supported by SSM.

Discovering Servers on the Network

SnapServer Manager automatically discovers all supported platforms on the same network segment and displays them in the main SSM window. Additionally, SSM discovers servers outside the local network if they have been added to the Remote Servers list. For more information, see [“Discovery” on page 1-6](#).

Launching External Administration

The Web Management Interface(GuardianOS servers and SnapSAN servers) and REO 4600 GUI are browser-based applications that allow you to perform a wide range of administrative tasks on a server-by-server basis. To launch one of these tools, right-click the server name or go to the Administration menu and select **Launch Web Administration**.

Discovery

At startup and once per minute afterward, SnapServer Manager broadcasts a discovery request packet to its local subnet. SnapServers and REO 4600 appliances on the same network segment that receive discovery requests respond with a discovery packet

containing information. All other discovery activity is performed using both direct communication (unicast) and a proprietary multicast communication mechanism that does not impact other systems on the network.

When SSM sends or receives discovery packets, status LEDs at the right on the Status Bar flash according to which activity is taking place. The LED labeled “Tx” flashes whenever SSM sends out a discovery request. The LED labeled “Rx” flashes whenever SSM receives a server discovery information packet.

You can add other SnapServers that reside outside the local network segment by entering their IP addresses in the Remote Server List (**Edit > Remote Servers**).

Tip: *If SSM has not been able to communicate with a discovered GuardianOS SnapServer (for example, the server is offline or has just been started), that server's IP address appears in blue and the Properties screen for that server shows Not Validated next to the IP address. Once SSM has successfully communicated with the server, the text color of the IP address changes to black, and Validated appears on the Properties screen.*

Local Discovery

A *local server* is one that resides on the same network segment as the machine on which SnapServer Manager is installed. GuardianOS SnapServers regularly send multicast discovery information to their local network segment, other platforms broadcast their presence once on startup, and all platforms respond to discovery request broadcasts from SnapServer Manager. SnapServer Manager passively listens for multicast or broadcast discovery information from supported platforms and broadcasts a discovery request packet on the local network segment in three cases: (1) at startup; (2) once per minute; and (3) when the administrator manually refreshes the information by selecting **Edit > Refresh All**.

Remote Discovery

A *remote server* is one that resides on a network segment different than the one on which SSM resides. SSM cannot hear discovery information broadcasts from remote servers until the administrator configures them on the Remote Servers list (see [“Configuring Remote Server Discovery Example” on page 1-7](#)).

SSM regularly queries servers on the Remote Servers list for discovery information. When discovered, remote servers return information about themselves, and remote GuardianOS servers also return information about any other GuardianOS servers on the same network. As a result, only one GuardianOS SnapServer needs to be added per remote network to discover all remote GuardianOS servers. However, for non-GuardianOS platforms, each server must be added individually to the Remote Servers list. Remote SnapServers discovered in this manner display the letter **R** in the Discovery State column of the Server Details list of the SSM screen, along with the name of the discovering Remote Server, if applicable.

Tip: *For instructions on displaying the Discover State column in the SSM screen, see [“The Server Details List.”](#)*

Configuring Remote Server Discovery Example

For example, assume a remote network segment contains six servers:

- REO 4600 running the latest REO 4600 GUI (non-GuardianOS)
- SnapServer DX2 running GuardianOS 7.1
- SnapSAN S2000 running SnapSAN 4.3 (non-GuardianOS)
- SnapServer 410 running GuardianOS 5.2

- SnapServer N2000 running GuardianOS 6.5

To enable SnapServer Manager to discover all these remote servers, the IP address of one of the GuardianOS SnapServers needs to be entered in the Remote Servers List to discover the other two GuardianOS servers. The three non-GuardianOS platforms must be added individually. Using a GuardianOS SnapServer as a remote discovery server makes the administrator's configuration task easier and reduces the network traffic required to refresh server status.

Tip: For full interoperability, Overland recommends that all GuardianOS SnapServers on the network run the same version of the SnapServer software. If you have SnapServers running different versions of GuardianOS on your network, use a server running the **most current** version as the remote discovery server.

Laptop SSM Installation and Remote Server Discovery

Unexpected results may occur in instances where SnapServer Manager is installed on a laptop that is moved from one network segment to another. In this situation, the servers that were previously in SSM's local segment are now in a remote segment, and since no remote server has been designated in that segment, SSM can no longer hear their discovery information broadcasts. Thus, when SSM is started up in the new location, these servers will display as offline.

To Ensure All Servers Display Correctly in the SSM Screen

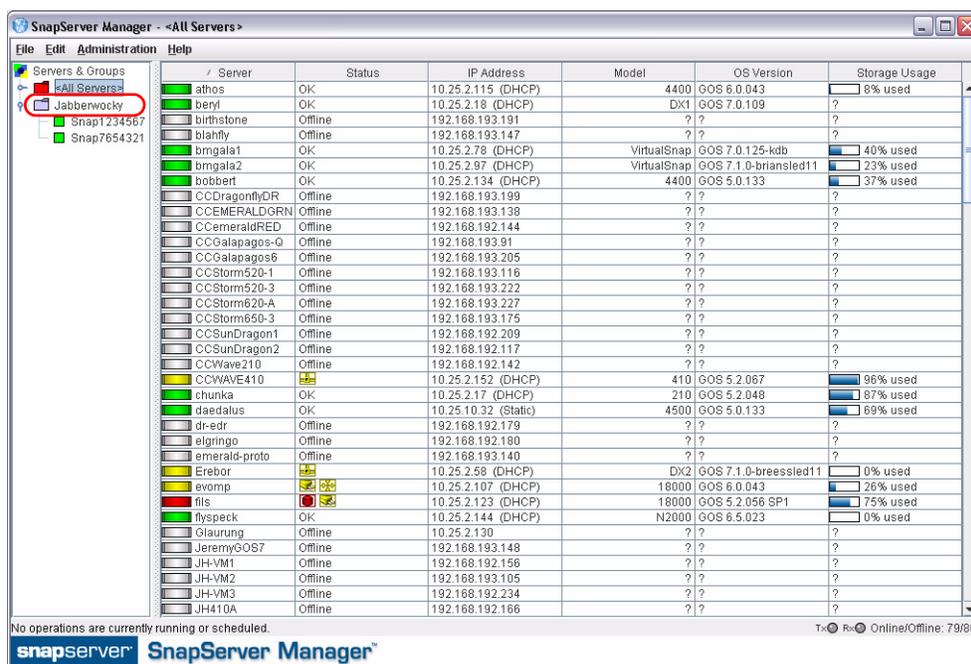
SnapServer Manager offers three methods to ensure all servers display correctly in the SSM screen. The first option is the preferred method (available only if all servers are GuardianOS servers) because this method results in less network traffic than the other options; but any combination of methods can be used to suit your environment.

Procedure	Result
Add one GuardianOS (v. 2.6 or higher) SnapServer from every network segment (including the current local segment) to the Remote Servers List. This option is applicable only if all servers on the remote network are GuardianOS servers.	SSM sends out only a single DRP for each server on the Remote Servers List.
For non-GuardianOS servers, manually add each server to the Remote Servers List.	SSM sends out a single DRP for each server on the Remote Servers List.
From SSM, select Edit > Options . Select the Auto-scan servers not on Remote Server list option, and click OK . This option instructs SSM to directly (and regularly) send DRPs to all previously discovered servers that are neither: (1) specified on the Remote Servers list, nor (2) resident on the same network segment as a server specified on the Remote Servers list.	SSM sends out one DRP for each previously discovered server, resulting in increased network traffic.

Customizing the SSM Interface

At startup, the SnapServer Manager displays all SnapServers and REO 4600 appliances discovered on the local subnet as well as any remote supported platforms configured by the administrator. The default group **<All Servers>** contains all discovered servers. Additional

server groups can be created for easier multiserver administration. Clicking a server group displays only the group's servers in the Server Detail list. Click the group name to show all the servers under the name in the Server Details list.



Tip: The Status Bar indicates the status of any running or scheduled operations. Operations are defined as administrative tasks (for example, changing TCP/IP settings or configuring email notification) that are run concurrently for a group of servers.

Server Groups

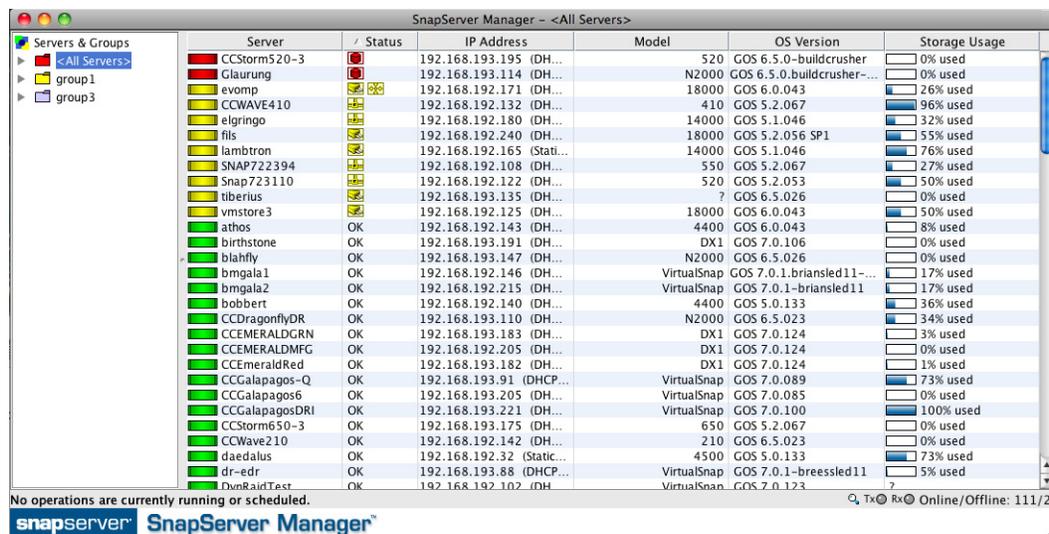
SnapServer Manager allows administrators to organize servers into groups for ease of administration. Different server groupings can be created, saved, and shared with other administrators.

Server Group Color Coding

The folder color of a server group reflects the highest level of alert for any of the servers in the group.

Tip: Only GuardianOS servers display the warning and failure color codes. A group with only non-GuardianOS servers will always be color-coded grey.

The following Mac OS X image shows a server group **group1** that contains multiple servers. The group folder is yellow because one or more GuardianOS servers contain a warning-level condition associated with them. The **<All Servers>** folder above **group1** is red, indicating a failure-level condition on at least one GuardianOS server in that group. A grey folder next to **group3** indicates none of the servers in the group show warning or failure indicators.



Creating, Populating, and Maintaining Server Groups

In creating server groups, you can perform the following operations:

Task	Procedure
To create a new group on the root	Right-click Servers & Groups and select New Group . Enter a unique name in the dialog box that opens and click OK . The new group is added alphabetically to the root of the Servers & Groups tree.
To create a new group inside another group	Right-click a group and select New Group . Enter a unique name in the dialog box that opens and click OK . The new group is nested inside the original group.
To copy multiple servers from the Server Details list to a group	Select one or more servers from the Server Detail list, and do one of the following: <ul style="list-style-type: none"> Right-click a highlighted row and select Copy. Select a group, then right-click and select Paste. Click-and-drag a highlighted row to the group.
To copy the contents of one server group into another server group	Right-click a group and select Copy . Then, right-click the target group and select Paste .
To rename a group	Right-click a group and then select Rename Group . Enter a unique name in the dialog box that opens and click OK .
To delete a group	Right-click a group and then select Delete . In the confirmation dialog box that opens, click Yes .

Saving and Distributing Server Groups

Administrators who manage SnapServers from different machines will want to have the same group structures available from each SSM installation. Server groups can be saved to an XML file by highlighting the group to be saved and selecting **File > Save Groups As**. By default, this file is saved to the home directory for your platform.

For example, on a machine running Windows XP, the default home directory would be similar to the following:

```
C:\Documents and Settings\username\ssm_groups.xml
```

To share groups, copy the XML files to an appropriate directory on any other machines used to manage SnapServers. Alternatively, you can select **File > Open Groups** and navigate to the desired file.

Remove Offline Servers

Select **Edit > Remove Offline Servers** to remove offline servers from groups. An **Include all subgroups** check box on the Confirmation dialog allows you to remove offline servers from the subgroups of the selected group also. The subgroup removal option is checked by default and is disabled (grayed) if the selected group has no subgroups.

The Server Details List

The data displayed in the Server Details list can be customized to accommodate different administrative interests.

Column Definitions

The Server Details list is divided into several different columns. The following table defines the properties shown in these columns:

Column	Description
Server	Lists the names of all discovered servers.
Status	<ul style="list-style-type: none"> • OK – All systems are functioning correctly. • Offline – The server is offline. • Alert Icon – Displays any warning (amber) or fault (red) conditions for the selected GuardianOS server. See the “Status Column Icons (GuardianOS only)” table on page 1-3 for a list and description of the different icons.
IP Address	Displays the IP address and type for the server.
Model	Displays the type of server model (such as, DX1 or N2000)
OS Version	Displays the OS type and version number.
Storage Usage	Shows a percentage bar and the numerical percentage of the amount of storage space used.
OS*	Displays the operating system name of the server.
Number*	Displays the server number of the selected server.
Up Time (D:H:M)*	Displays how long a server has been up and running, in days, hours, and minutes.
Discovery State*	Displays the date and time the listed server’s DRP was sent and received by SSM.

Column	Description
Configured*	Displays whether or not the server has gone through the initial configuration process. Displays yes, no, and partial.
Expansion Units*	Displays the number and type of expansion units attached to a server. For example, if a server has one E2000 unit, the expansion unit column will display “ 1 - E2000 ”.

* These columns not shown in the default display. Must be added manually using the right-click menu.

Customizing the Server Details List

Use the following procedures to customize the information displayed in the Server Details list:

Task	Description
To sort the Server Details list according to a column	Click a column header. The Server Details list sorts according to the contents of the column in ascending order. To sort in descending order, click the column header again.
To resize a column header	Hover the cursor over the right border of the column header you want to resize, and then click and drag the border to the desired width.
To normalize the size and contents of all column headers	Right-click any column header and click Reset Columns . The original factory set columns, properties, and order are restored.
To load a different property into a column	Right-click a column and select a different property.
To create a new column	Right-click a column, and select New Column . The clicked column is duplicated. Right-click the new column, and select a different property (see “Column Definitions”).
To reorder columns	To reorder columns, simply configure the properties into the existing columns in the order you want.
To delete a column	Right-click a column header and select Delete Column .

Usage Scenarios for GuardianOS Servers

This section provides scenarios of the major types of operations you can perform on multiple GuardianOS servers. Operations can be run immediately or be scheduled to run at a later time. SSM can also automatically deliver reports on completed operations by email. Review these scenarios to quickly learn the steps required to perform each of these operations:

- [Viewing GuardianOS Server Settings/Generating a Report](#)
- [Configuring Multiple GuardianOS Servers/Setting Up Email Notification](#)
- [Copying Settings Among GuardianOS Servers](#)
- [Scheduling an OS Update for Multiple GuardianOS Servers](#)

Tip: *If servers within a group have different passwords, you will have to remember and enter each password before you can administer the server group. For ease of administration, configure servers within a group with the same password.*

Viewing GuardianOS Server Settings/Generating a Report

A common problem for administrators is maintaining network and other settings across large groups of servers. This scenario shows how to view and compare settings across a group of servers in a single operation, and then generate a report in CSV format.

1. Select a group of servers.

In the SSM screen, select a group of servers and click **Administer Servers**. After you enter the passwords for the servers, the Administer Servers dialog box opens.

Tip: Configure the servers within a group with the same password.

2. Select one or more tasks.

Administrative tasks are listed in the left-hand pane. Select each setting you want to view, and then click **View/Copy**. The Current Settings for Servers dialog box opens.

3. Run the operation.

Click **Start**. The interface provides feedback on the progress of the operation. Color coding indicates configurations whose settings are identical across servers and those whose settings differ.

4. Generate an Operations Report (optional).

Once SSM retrieves server settings, click **Report** to save the settings to a CSV file.

Configuring Multiple GuardianOS Servers/Setting Up Email Notification

Configuring servers one-by-one is a tedious and error-prone process. This scenario shows how to simultaneously configure multiple SnapServers in a single operation, eliminating unnecessary administrative overhead and assuring consistency of settings across servers.

1. Select a server group.

In the SSM screen, right-click a server group and select **Administer Servers**. After you enter the passwords for the servers, the Administer Servers dialog box opens.

2. Edit settings for one or more tasks.

Administrative tasks are listed in the left-hand pane. Check any task to edit its settings. For example, to edit the administrative password, check **Admin Password**. A check mark appears before the task and its fields become editable, allowing you to modify settings. Select and edit any other tasks, then click **Apply**. The Apply to Servers dialog box opens.

3. Run the operation.

Click **Start Now**. The interface provides feedback on the progress of the operation.

4. Set up automatic delivery of operations reports (optional).

Once SSM applies server settings, click **Report** to open the Operation Report dialog box. Select the **Send e-mail report when operations finish** option, enter the SMTP Server IP address and the email address of at least one recipient, and then click **OK**.

Copying Settings Among GuardianOS Servers

SnapServer Manager allows administrators to apply configuration settings from one server to a group of other servers in a single operation. This scenario shows how to copy specific settings from one (source) server and apply those settings to a (target) group of other servers.

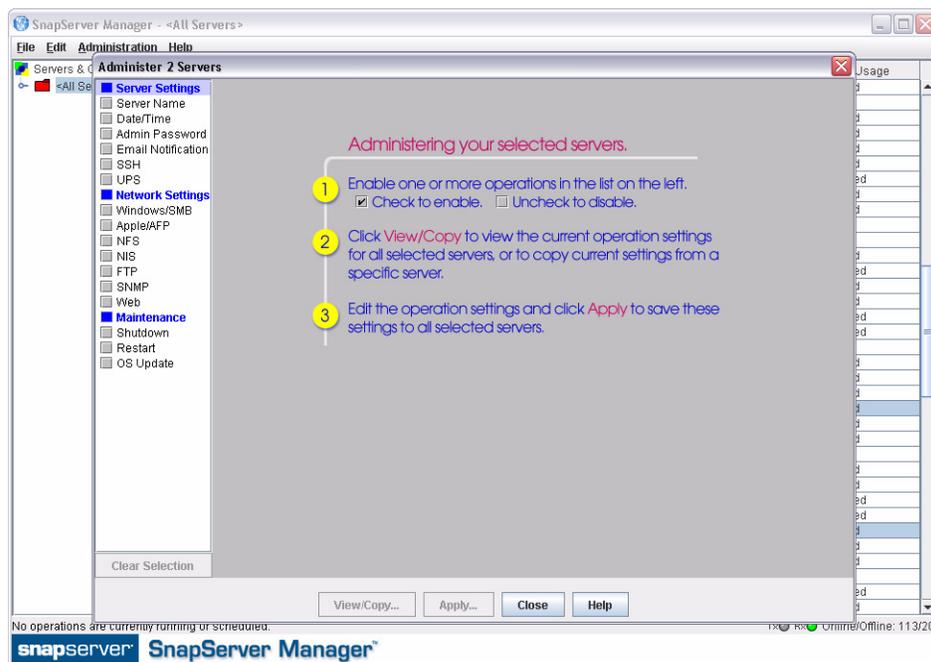
1. Select a server group.
In the SSM screen, right-click a server group and select **Administer Servers**. Make sure the source server is included in the group. After you enter the passwords for the servers, the Administer Servers dialog box opens.
2. Copy specified settings to the Administer Servers window.
In the settings pane to the left, select each setting you want to copy, and then click **View/Copy**. In the Current Settings for Servers window, click **Start**. Once the settings are retrieved, double-click the source server row, and then click **OK** at the confirmation screen. To close the Current Settings for Servers window, click **Close**.
3. Apply the settings to the entire group.
In the Administer Servers window, click **Apply**. In the Apply to Server window, click **Start Now**. The interface provides feedback on the progress of the operation.

Scheduling an OS Update for Multiple GuardianOS Servers

Updating the SnapServer operating system without interrupting client access is difficult to achieve during normal working hours. This scenario shows how to update all GuardianOS SnapServers on your network in a single operation scheduled during off-peak hours.

1. Select a server group.
In the SSM screen, right-click a server group and select **Administer Servers**. After you enter the passwords for the servers, the Administer Servers dialog box opens.
2. Set up the OS Update task.
Select OS Update and if necessary, use the link to download the update file from the SnapServer website to a location accessible to SSM over the network. Click the **Browse** button to navigate to and select the update file. Click **Apply** to open the Apply to Servers dialog box.
3. Schedule the operation to run at a later time.
In the Apply to Servers dialog box, click **Start Later**. In the Apply Schedule dialog box, select an off-peak time to run the operation and click **OK**.
4. Click **Hide** to return to the SSM screen.
Note that the status bar shows the schedule you just set up. You can click this status bar message at any time to view or cancel the operation.

SnapServer Manager provides an easy way to manage single or multiple servers through the Administer Servers configuration screen. It is accessed by highlighting the servers to be configured and selecting **Administration > Administer Servers** from the menu bar:



The screen title bar shows either the name of the server selected or, when performing multiserver administration tasks, the number of servers selected (such as, **Administer 2 Servers**). When you check a feature to configure, a gray screen is displayed showing the available settings along with some basic directions and information.

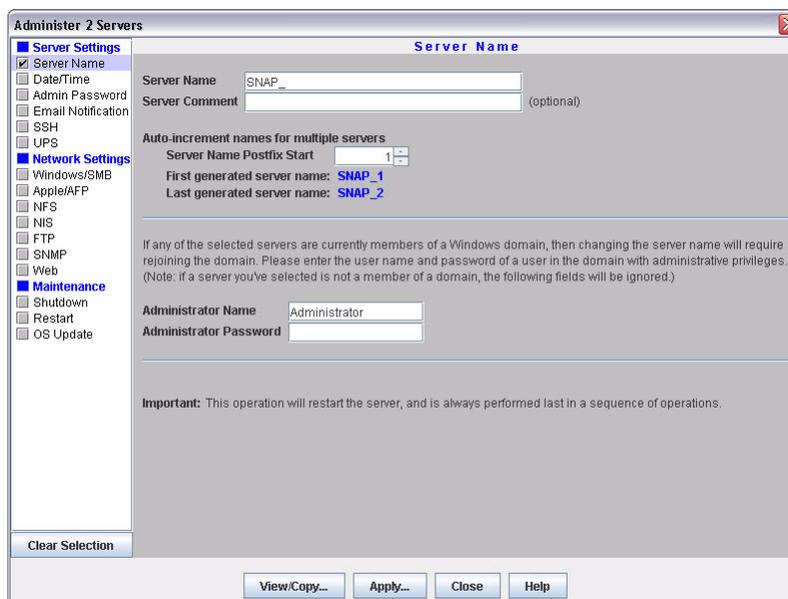
SnapServer Manager makes the following administrative tasks available for multiserver administration.

- **Server Settings** – [Server Name](#), [Date/Time](#), [Admin Password](#), [Email Notification](#), [SSH](#), and [UPS](#).
- **Network Settings** – [Windows/SMB](#), [Apple/AFP](#), [NFS](#), [NIS](#), [FTP/FTPS](#), [SNMP](#), and [Web](#).
- **Maintenance Settings** – [Shutdown](#), [Restart](#), and [OS Update](#).

NOTE: For other tasks, such as storage configuration, use the Web Management Interface.

Server Name

Check the Server Name option to name/rename the servers. If any of the selected servers are currently members of a Windows domain, then you must rejoin the domain.



When configuring a single server, the name you enter in the Server Name field is applied to the server. When configuring multiple servers, the name you enter in the Server Name field is used as the basis for the name of each of the servers in the group, and a number differentiating each server is added by the auto-increment feature.

To change servers that are currently members of a Windows domain, changing the server names will require rejoining the domain. Enter an administrator user name and password of a user in this domain with administrative privileges. If a server that has been selected is not a member of a domain, the administrator name and password fields will be ignored.

Options	Description
Server Name	The default server name is SNAPnnnnnn, where nnnnnn is the unique server number (for example, SNAP242424). SnapServer names are limited to 27 alphanumeric characters. You can also use the dash (-), underscore (_) between characters, and spaces.
Server Comment	Optionally, add a comment (for example, server location) specific to the server. This comment will be displayed in Windows Network Neighborhood.
Server Name Postfix Start	Select the starting number for the suffix of a series of server names that use the same core name.
Administrator Name and Password	The user name and password of a user in the domain with administrative privileges.

To Change a Single Server Name

1. At Administration > Administer Servers, click **Server Name**.
2. Enter the new name in the **Server Name** field and a comment if desired.

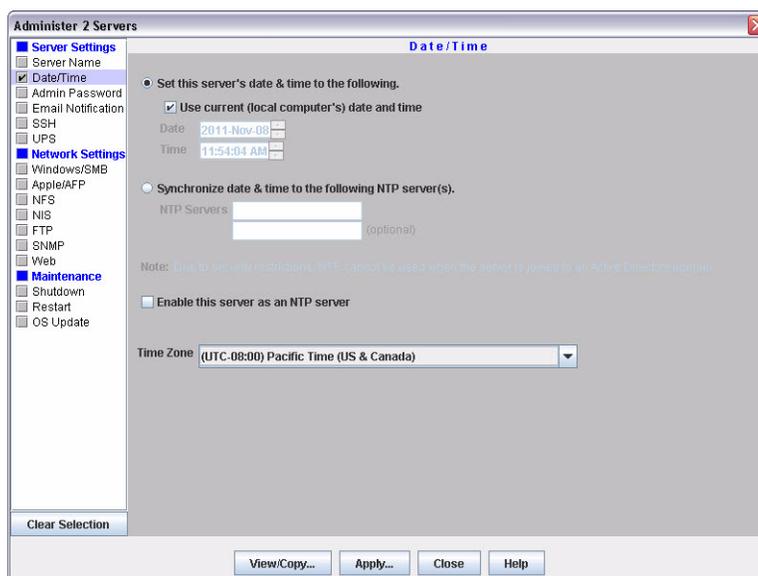
3. Enter an administrator's name and password in the fields provided.
4. Do one of the following:
 - To continue server configuration, select a different task.
 - To apply changes made to all selected tasks, click **Apply**. Then, in the Apply to Servers dialog, click **Start** to begin applying active settings.

To Change Multiple Server Names Using the Auto-increment Feature

1. Enter the base server name in the **Server Name** field.
2. By default, the auto-increment feature starts at one (1). Change this starting number as appropriate.
3. Do one of the following:
 - To continue server configuration, select a different task.
 - To apply changes made to all selected tasks, click **Apply**. Then, in the Apply to Servers dialog, click **Start** to begin applying active settings.

Date/Time

Use this screen to configure date and time settings, to configure the SnapServer as an NTP server, and to set the time zone used.



The time stamp applies when recording server activity in the Event Log (Monitoring tab), when creating or modifying files, and when scheduling snapshot, antivirus, or Snap EDR operations.

Tip: The SnapServer automatically adjusts for Daylight Savings time.

Options	Description
Date & Time	Set either to the local computer (the computer on which SnapServer Manager is installed) or enter manually.
NTP Servers	Network Time Protocol (NTP) sets the date and time to a network server rather than the local computer.
Enable NTP Server	Put a check in this box to enable the SnapServer as an NTP server.
Time Zone	Defaults to UTC



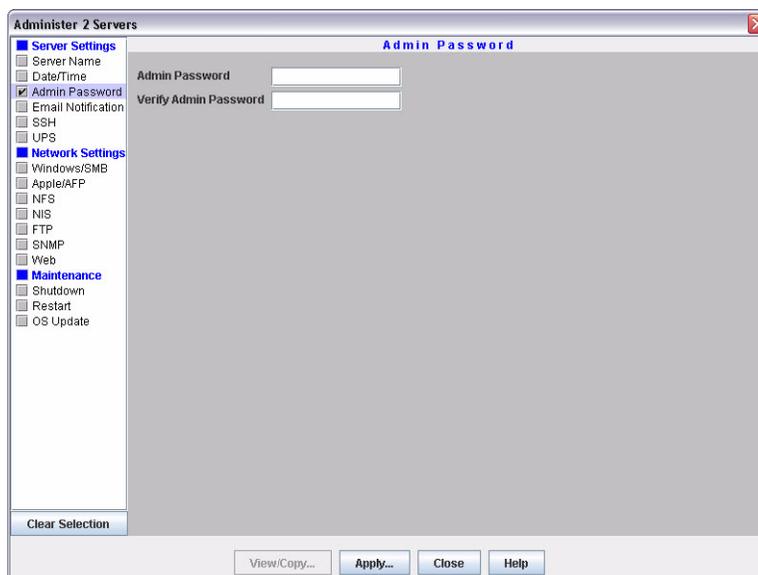
CAUTION: If the current date and time are reset to an earlier date and time, the change does not automatically propagate to any scheduled events you have already set up for snapshot, antivirus, or Snap EDR operations. These operations will continue to run based on the previous date and time settings.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

Configure Date and Time Settings

1. At Administration > Administer Servers, click **Date/Time**.
2. Do one of the following:
 - **Use Computer Settings** – Select **Set this Server's Date & Time to the Following**, then check **Use Current (Local Computer's) Time and Date** to use the current computer's settings, or clear the check box to manually set the time and date.
 - **Sync With NTP Server** – Select **Synchronize Date & Time to the Following NTP Server(s)** to sync servers to the NTP server, then add the server name or IP address in the field provided. This option is only available for use with GuardianOS 4.0 and higher.
3. Select a **Time Zone** from the pull-down menu.
4. Do one of the following:
 - To continue server configuration, select a different task.
 - To apply changes made to all selected tasks, click **Apply**. Then, in the Apply to Servers dialog, click **Start** to begin applying active settings.

Admin Password

This screen is used to manage the administrator-level password for a SnapServer. To prevent unauthorized access to the SnapServer, create a secure password immediately.



Option	Description
Admin Password (and Verify)	The default password for the admin user account is <i>admin</i> . Use up to 15 alphanumeric characters. Passwords are case-sensitive.

To Create a New Admin Password

1. At Administration > Administer Servers, click **Admin Password**.
2. In the fields provided, enter the new password, and then repeat it in the field below to verify the password.
3. Do one of the following:
 - To continue server configuration, select a different task.
 - To apply changes made to all selected tasks, click **Apply**. Then, in the Apply to Servers dialog, click **Start** to begin applying active settings.

Email Notification

NOTE: The Email Notification feature requires GuardianOS 6.0 or higher.

To set up email alerts in response to system events, you will need the SMTP server's IP address or host name and the email address of at least one recipient (four are possible) who is to receive an alert.

Option	Description
Enable Email Notification	To enable email notification, check the Enable Email Notification check 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.
Use Authenticated SMTP	Check this box to require authentication 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.
Use Secure Connection	Check this box to encrypt emails from the SnapServer. STARTTLS and TLS/SSL encryption protocols are supported.
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 to four email addresses to receive the notifications. At least one address is required.

Option	Description
Send email notification for the following events	<p>Check the boxes next to the events you wish to be notified about:</p> <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 – For a RAID 1, 5,6, or 10, it experiences a disk drive failure, a disk drive is removed, or it 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 Migration or Unicode 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 after saving settings	To verify your settings, check the box. After you apply the settings, a test email will be sent to the recipients.

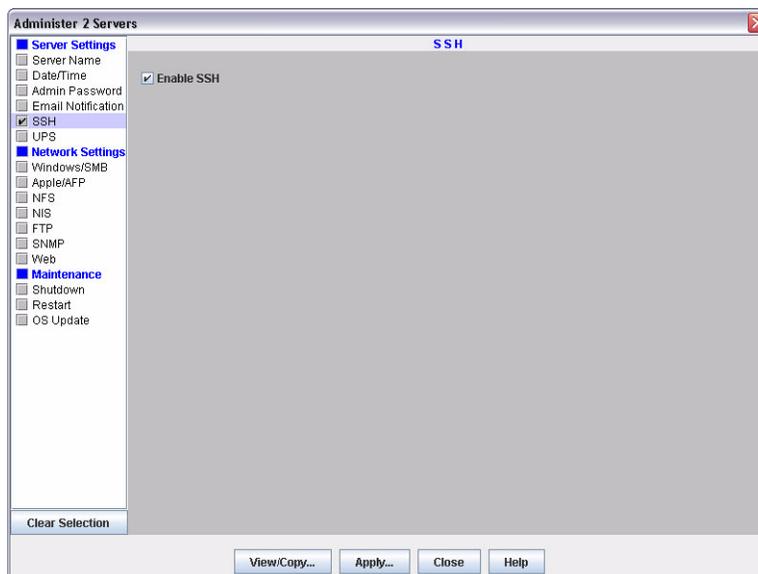
Configure Email Notification

1. At Administration > Administer Servers, click **Email Notification**.
2. Select the **Enable Email Notification** check box.
3. Enter the SMTP server IP address, and either enter a port number for the SMTP server or accept the default.
4. If desired, select **Use Authenticated SMTP** and provide a user name and password to require authentication when the SnapServer sends an email to the SMTP server.
5. If desired, select **Use Secure Connection** if you want the SnapServer emails to be encrypted.
6. Select an **Email Address of Sender**.
Designate an email address from which email notifications are to be sent. The default is **<Use default>**, which uses either *serverName@serverDomain* (if a DNS Domain Name is specified on TCP/IP screen), or *serverName@ServerIP* (if a domain name is not specified) as the default sender email address. To add a new email address, click the Email Address of Sender field and type the desired email address. Alphanumeric characters, except spaces, are accepted.
7. If desired, add up to three more **recipient** email addresses in the fields provided.
8. Select the **server** events of which you want to be notified.
9. Select **Send a test email after saving settings** to verify the configuration.
10. Do one of the following:
 - To continue server configuration, select a different task.

- To apply changes made to all selected tasks, click **Apply**. Then, in the Apply to Servers dialog, click **Start** to begin applying active settings.

SSH

Secure Shell (SSH) is a service that provides remote access to a command line shell that allows the user to perform basic management and update functions outside the GuardianOS Web Management Interface.



CAUTION: SSH is enabled by default. To maintain security, consider disabling SSH when not in use.

To Enable or Disable SSH

1. At Administration > Administer Servers, click **SSH**.
2. The **Enable SSH** check box toggles SSH on and off. Select to enable.
3. Do one of the following:
 - To continue server configuration, select a different task.
 - To apply changes made to all selected tasks, click **Apply**. Then, in the Apply to Servers dialog, click **Start** to begin applying active settings.

UPS

APC®-brand Smart-UPS® series devices allow SnapServers to shut down gracefully in the event of an unexpected power interruption. No configuration of the UPS is required if it is connected directly to a SnapServer via USB.

For a network-based APC UPS device, you must configure UPS support on the SnapServer as described in this section and identify the SnapServer to the APC software. In the APC UPS Web-based user interface, navigate to the Power Chute configuration page, and add the SnapServer's IP address to the client list. If you are using DHCP, entering any IP address on your network will work.

Tip: For SnapServers with a single power supply, only the first procedure applies. The second procedure applies to servers that have dual power supplies.

Configure One (Primary) UPS Device

Complete the following fields and click **Apply**.

Option	Description
Enable UPS Support	Select option to enable or clear to disable UPS support.
Automatically restart server when power is restored	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. This option is available for servers running GuardianOS 4.2 or higher.
Use a single USB-connected UPS device	Select this radio button to use a USB-connected APC UPS device. This option is available for servers running GuardianOS 4.2 or higher.
Use the following network-connected UPS device(s)	Select this radio button to use one or two network-connected APC UPS devices.
IP Address	Enter the IP address of the server on which the network UPS resides.

Option	Description
APC User Name (for authentication)	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.

Configure a Secondary UPS Device

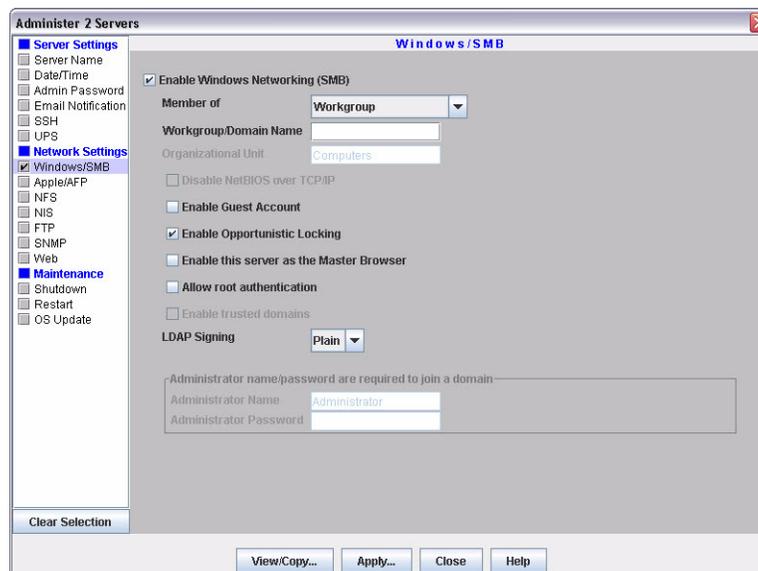
1. At Administration > Administer Servers, click **UPS**.
2. Complete the following fields and click **Apply**.

Option	Description
Secondary UPS Device (optional)	Select to enable (or clear to disable) a secondary UPS device.
IP Address	Enter the IP address of the server where the network UPS resides.
APC User Name (for authentication)	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.
Shutdown server upon receiving a low battery message from	Select one of the following from the drop-down list: <ul style="list-style-type: none"> • Either UPS Device – Select this option to allow shutdown upon receipt of a message from one 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.

Windows/SMB

In addition to joining the SnapServer to a Windows workgroup or Active Directory domain, several other options are available for Windows networking:

- You can enable guest account access to the SnapServer for all Windows clients.
- With ADS domains, you can disable NetBIOS.
- For ADS domains, you must specify a valid user name and password to join the domain.



To Join a Workgroup

Edit settings as described in the following table, and then click **Apply**.

Option	Settings
Enable Windows (SMB)	Select to enable (or clear to disable) access to the server via the SMB protocol.
Member Of	Select Workgroup from this pull-down menu.
Workgroup/Domain Name	Enter the workgroup to which the server belongs.
Enable Guest Account	Select the Enable Guest Account option to allow unknown users 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.
Enable this server as the Master Browser	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.) Select to enable 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.
Allow Root Authentication	Select Allow Root Authentication to allow a root login on the selected server. Available only on servers with OS versions 4.0 and higher.

To Join an Active Directory Domain

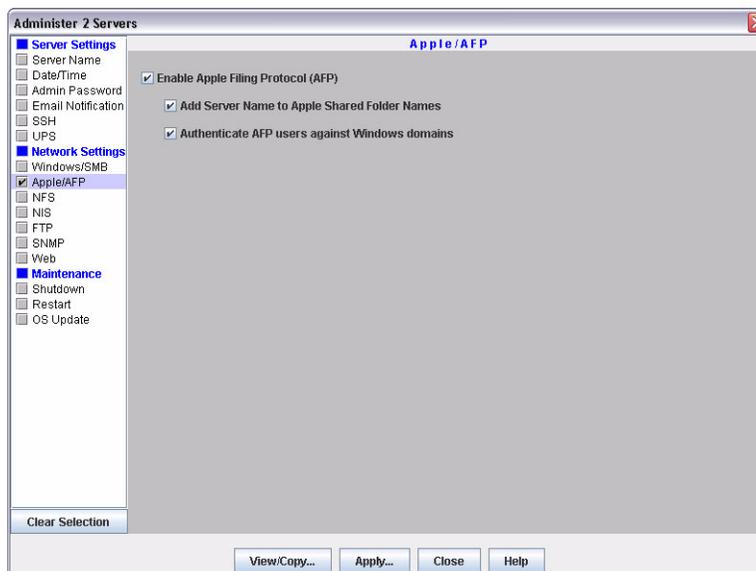
1. At Administration > Administer Servers, click **Windows/SMB**.

2. Edit settings as described in the following table, and then click **Apply**.

Option	Settings
Enable Windows SMB	Select to enable (or clear to disable) access to the server via the SMB protocol.
Member Of	Select Active Directory Domain from this pull-down menu.
Workgroup/Domain Name	The default settings make the SnapServer available in the workgroup named "Workgroup." Enter the domain name to which the server belongs.
Organizational Unit	You must enter the name of the organizational unit within the Active Directory tree in which the SnapServer will appear. By default, the server appears within the container named Computers. To join a sub-level of an organizational unit, enter the path in the following format: <i>/[organizational unit]/[sub-unit1]/[sub-unit1a]</i> .
Disable NetBIOS over TCP/IP	Check the box to disable NetBIOS or clear it to leave NetBIOS enabled.
Enable Guest Account	Select the Enable Guest Account option to allow unknown users 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.
Enable this sever as the Master Browser	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). Select to enable 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.
Allow Root Authentication	Select Allow Root Authentication to allow a root login on the selected server. Available only on servers with OS versions 4.0 and higher.
Enable Trusted Domains	SnapServers recognize trust relationships established between the domain to which the SnapServer is joined and other domains in a Windows environment by default. Check the box to allow this feature. Available only on servers with OS versions 4.0 and higher.
Administrator Name/Password	Enter a user name and password with sufficient administrative privileges to allow a remote computer to join the domain.

Apple/AFP

Macintosh clients connecting over AFP can authenticate to the server as a local user or guest. If the server is joined to an Active Directory domain, AFP clients can also optionally authenticate against the domain (enabled by default). The default settings provide access to Macintosh clients over an AppleTalk or TCP/IP network.



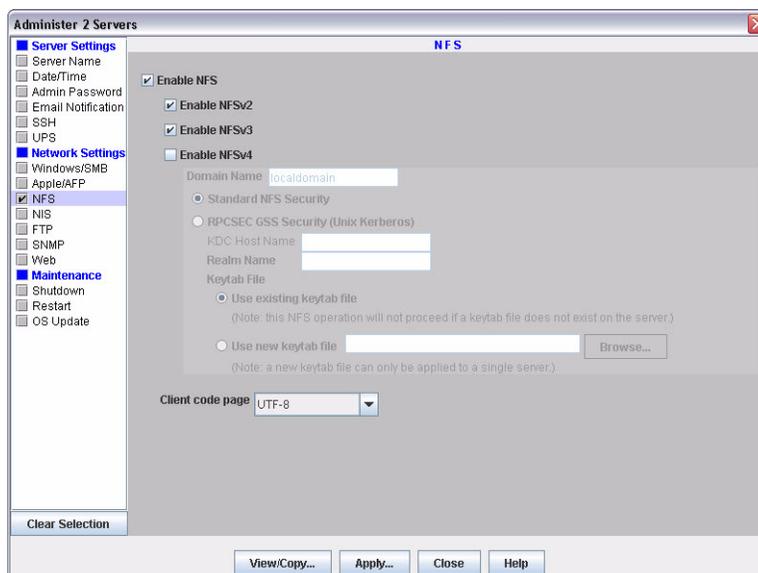
Edit Apple/AFP Settings

1. At Administration > Administer Servers, click **Apple/AFP**.
2. Edit settings as described in the following table, and then click **Apply**.

Options	Usage
Enable Apple Filing Protocol (AFP)	Select to enable (or clear to disable) AFP access.
Add Server Name to Apple Shared Folder Names	Select to show both the server name and share name in the Connect to Server dialog box. Clear the check box to display only the share name.
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's servername. For example: <i>windowsdomain\username</i> or <i>snap12345\username</i> .

NFS

SnapServer supports NFS v2/3/4, each version being individually configurable. Optionally, Kerberos-based security is supported for NFS v4.



Edit NFS Settings

1. At Administration > Administer Servers, click **NFS**.
1. NFS is enabled by default. To disable NFS, uncheck the **Enable NFS** box.
2. Select the versions of NFS that you want to enable (NFS v2, NFS v3, and NFS v4). The **Enable NFS** box must also be checked in order to enable any of the NFS versions.
3. If you enable NFS v4, complete information for the following fields:

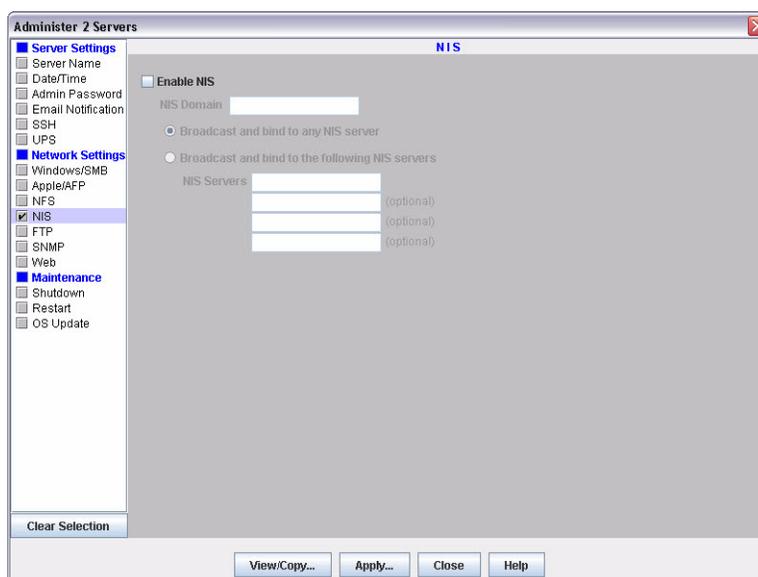
Option	Description
Standard NFS Security	Click this button if you want to use standard NFS security.
RPSEC GSS Security (Unix Kerberos)	Click this button and then complete the following fields if you want to use Unix Kerberos security to authenticate NFS v4 connections: <ul style="list-style-type: none"> • KDC Host Name – Enter the host name or IP address of the Kerberos server. • Realm Name – Enter the Kerberos realm name. • Keytab File – Select Use existing keytab file; or, select Use new keytab file and Browse to locate and upload a keytab file generated for the SnapServer.

4. Use the **Client Code Page** drop-down menu to select a page type. The **Keep current value** option allows you to change the NFS enable-state without changing the code page. This is the default setting for servers that have not had Unicode enabled. You can change the Client Code Page for a server only if Unicode has been enabled. Unicode is always enabled in GuardianOS 6.5 and higher. Use the Web Management Interface to enable Unicode for servers using GuardianOS 6.0 or earlier.

5. Click **Apply**.

NIS

A 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. Thus, you must use the NIS server to make modifications.



To Join an NIS Domain

1. At Administration > Administer Servers, click **NIS**.
2. Edit settings as described in this section, and then click **Apply**.

Option	Description
Enable NIS	Select to enable (or clear to disable) NIS Authentication.
NIS Domain	Enter the NIS domain name.
Broadcast and bind to any NIS server	Select this option to bind to all available NIS servers.
Broadcast and bind to the following NIS servers	Select this option and then enter up to four valid NIS server IP addresses.

NIS Facts

Consider the following facts when configuring NIS access:

You cannot modify NIS user or group accounts locally

You must use the NIS server to make modifications. 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.

Possible conflicts between NIS and SnapServer UIDs/GIDs

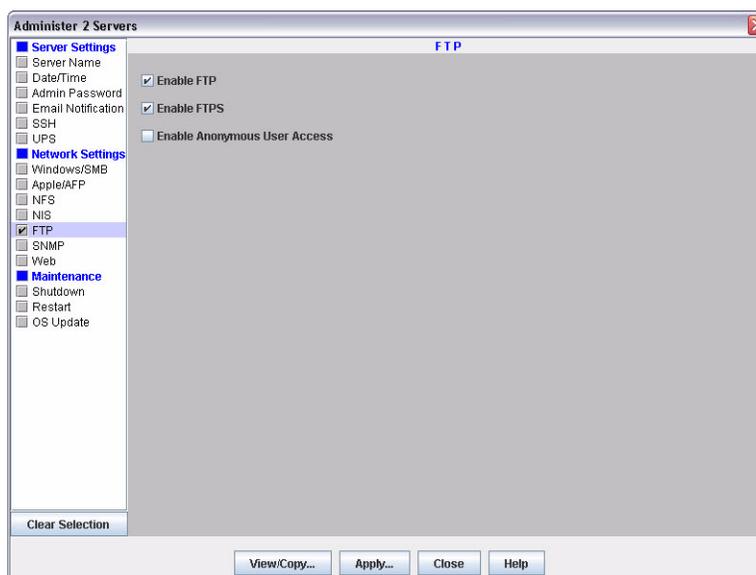
- NIS identifies users by UID, not user name, and although it is possible to have duplicate user names, Overland Storage does not recommend this configuration.
- If you join the SnapServer to an NIS domain, consider the following guidelines
 - The SnapServer does not recognize users or groups who have identification numbers less than 100.
 - Each UID or GID must be unique.
 - You should not define a UID or GID that has been previously assigned, and you cannot define a UID or GID that is currently assigned.

Specify Client Access

As a security measure, list only users who need access, rather than allowing all NFS clients access to SnapServer shares.

FTP/FTPS

FTP/FTPS clients can access the server using local users or the anonymous account. The anonymous user is mapped to the SnapServer's local guest user account. Administrators 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. For more granular control over FTP/FTPS access, administrators must create local user accounts for FTP/FTPS users.



Edit FTP/FTPS Settings

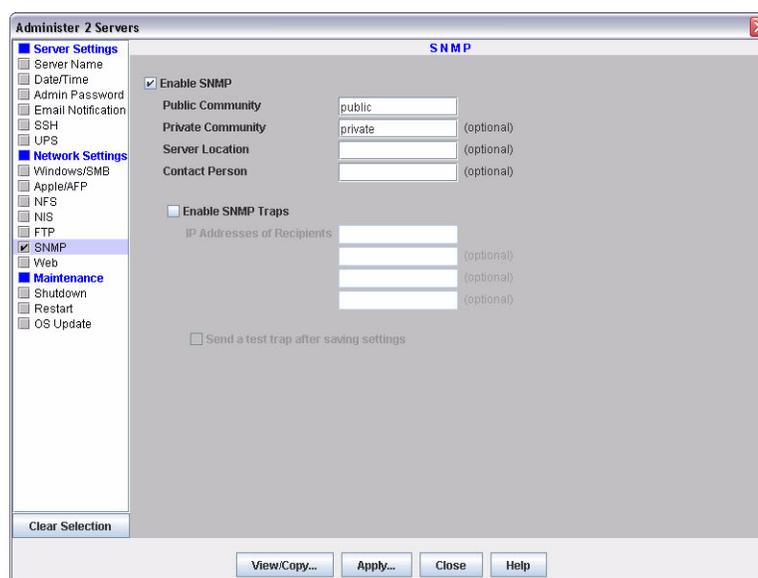
1. At Administration > Administer Servers, click **FTP**.
2. Edit settings as described below, and then click **Apply**.

Option	Settings
Enable FTP	Select to enable (or clear to disable) access to this server via the FTP protocol.

Option	Settings
Enable FTPS	Select to enable (or clear to disable) access to this server via the secure FTPS protocol.
Enable Anonymous User Access	<p>When you allow anonymous user access, FTP/FTPS users employ an email address as the password. When you disallow anonymous access, only FTP/FTPS users who are configured as local SnapServer users can access the server.</p> <ul style="list-style-type: none"> • Select this option to allow users to connect to the server using the anonymous user account. The anonymous user is mapped to the SnapServer's local guest user account. Administrators 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. • Clear this option to prevent anonymous user access. FTP/FTPS users can may still log in via a locally created user name and password.

SNMP

The Simple Network Management Protocol (SNMP) views a network as a collection of cooperating, communicating devices that consists of managers and agents. The SnapServer can act as an SNMP agent. Once SNMP is enabled on a SnapServer, SNMP managers can access management data on the server from MIB-II and the Host Resources MIB.



Supported Network Manager Applications

You can use any network manager application that adheres to the SNMP V2 protocol with SnapServer. The following products have been successfully tested with SnapServers: CA Unicenter TNg, HP Open View, and Tivoli NetView.

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:

- **coldStart** – An SNMP agent has restarted.
- **linkDown** – An Ethernet interface has gone off-line.
- **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.
- **enterpriseSpecific** – SnapServer-generated traps that correspond to the error-level, warning-level, and fatal-error-level traps of the GuardianOS. These traps contain a descriptive message that helps to diagnose a problem.

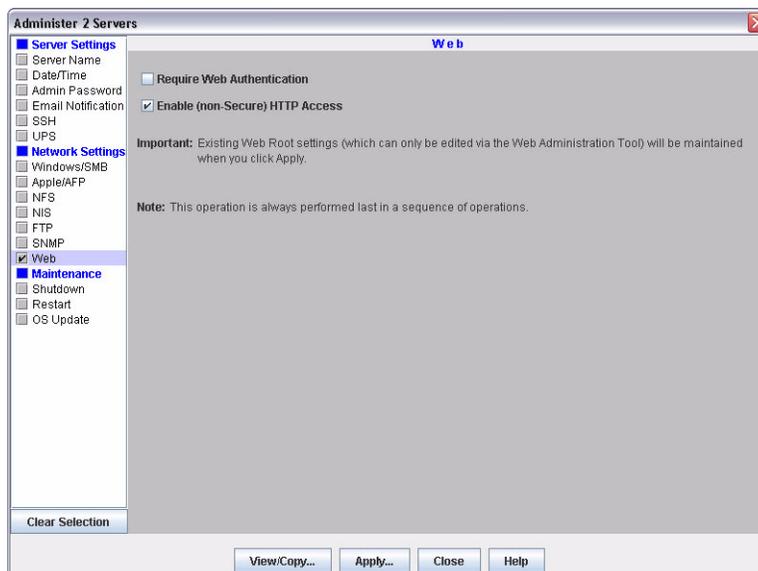
Configure SNMP

1. At Administration > Administer Servers, click **SNMP**.
2. Edit settings as described below, and then click **Apply**.

Option	Description
Enable SNMP	Select to enable (or clear to disable) SNMP.
Public Community	To enable SNMP managers to read data from this server, enter the name of one or more public communities, or accept the default <i>snap_public</i> .
Private Community	To enable SNMP managers to remotely configure this server, enter the name of one or more private communities, or accept the default <i>snap_private</i> . Create unique public and private names. As a precaution against unauthorized access, Overland Storage recommends that you create your own public and private community names.
Server Location	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 Person	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	Select to enable (or clear 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. You can enter up to three additional IP addresses.
Send a Test Trap	Select this option to verify your settings when you apply them.

Web

The Web configuration screen is used to manage authentication and non-secure access to the Web Management Interface.



The Web Management Interface opens when users access a SnapServer using their web browsers. It 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.

The Web Management Interface can be accessed using Microsoft Internet Explorer (7.0 or later), Safari (2.0 or later), Chrome (1.0 or later), or FireFox (3.0 or later).

HTTP and HTTPS are the default protocols used for browser-based access to the server. HTTPS enhances security by encrypting communications between client and server, and cannot be disabled. You can, however, disable HTTP access. Additionally, you can require browser-based clients to authenticate to the server.

Enable Web Authentication

1. At Administration > Administer Servers, click **Web**.
2. Edit the following setting, and then click **OK**.

Option	
Require Web Authentication	Select this option to require HTTPS or HTTP clients to enter a valid user name and password in order to access the server. Clear this option to allow access to the server without authentication.

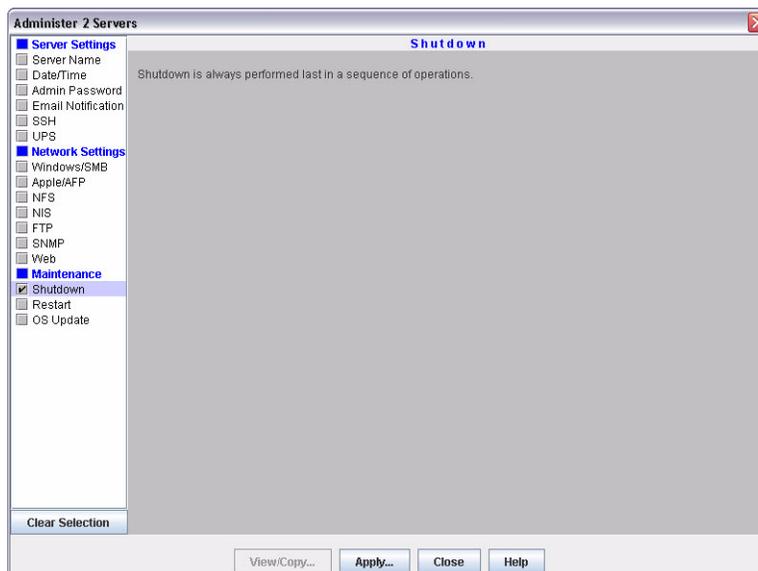
Enable Non-Secure HTTP Access

Edit the following setting, and then click **OK**.

Option	
Enable (non-secure) HTTP access	Select this option to enable HTTP client access to the server. Clear to disable. (HTTPS is always enabled.)
NOTE: To access the CA eTrust Antivirus configuration interface (on the Web Management Interface's Snap Extensions screen), HTTP must be enabled.	

Shutdown

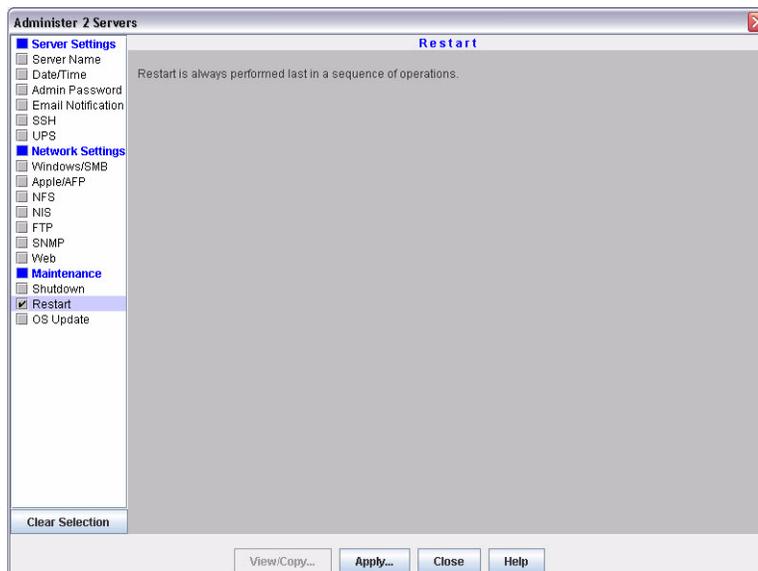
This task shuts down and powers off the servers being administered. There are no options to select or complete. At Administration > Administer Servers, select the **Shutdown** task to activate it, and then click **Yes** to confirm. It is always performed last if more than one operation is selected.



NOTE: If updating the firmware, after clicking Apply, select either Start Now or Start Later. See [“Run the Operations Now” on page 3-8](#) and [“Schedule the Operations to Run Later” on page 3-8](#).

Restart

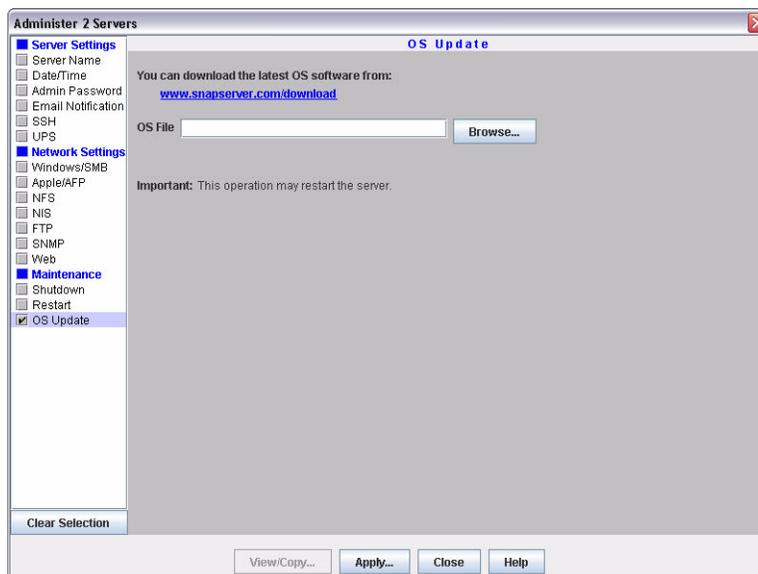
This task restarts the servers being administered. There are no options to select or complete. At Administration > Administer Servers, select the **Restart** task to activate it, and then click **Yes** to confirm. It is always performed last if more than one operation is selected.



NOTE: If updating the OS software, after clicking Apply, select either Start Now or Start Later. See [“Run the Operations Now” on page 3-8](#) and [“Schedule the Operations to Run Later” on page 3-8](#).

OS Update

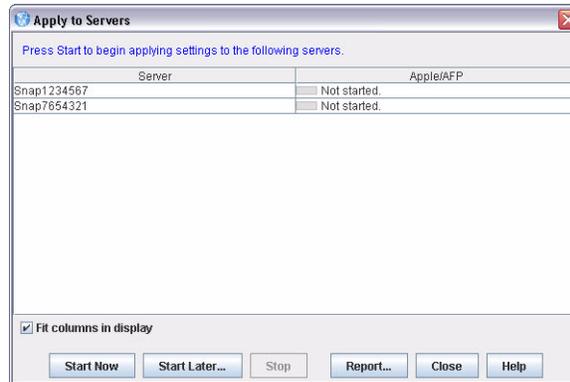
This task updates the GuardianOS (the software that governs the SnapServer’s functionality). It is mutually-exclusive from all other Administration functions.



CAUTION: Do not interrupt this process. You may severely damage the server if you interrupt a software update operation.

Update the GuardianOS Software

1. At Administration > Administer Servers, click **OS Update**.
2. Download the update by clicking the **download link** on the OS Update screen.
3. Follow the **instructions** provided to download the update file.
4. Click **Browse**, locate the file you’ve downloaded, and select it.
5. Click **Apply**.
6. The **Apply to Server** screen opens, listing servers and their update status. Select when to start the update:



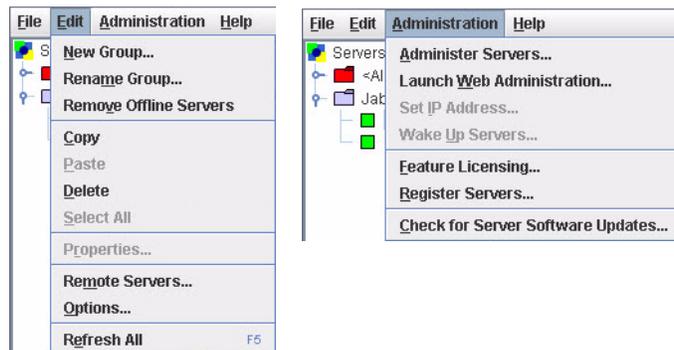
- Click **Start Now** to confirm the OS update. The SnapServer updates the OS and then reboots.
- Click **Start Later** to schedule the update to run at a later time.

NOTE: If you schedule the update for a later time, you will not be able to perform any other operations on the servers being updated until the scheduled update is done.

- Click **Report** to receive a report when the scheduled update is finished.

SSM Dialog Box Reference

This section describes some of the SnapServer Manager dialog boxes and their usage associated with the Edit and Administration menu options:



Edit Menu Dialog Boxes:

While New Group, Rename Group, and Remove Offline Servers have simple dialog boxes, the following menu items have additional options in their dialog boxes:

- [Server Properties](#)
- [Remote Servers](#)
- [Options](#)

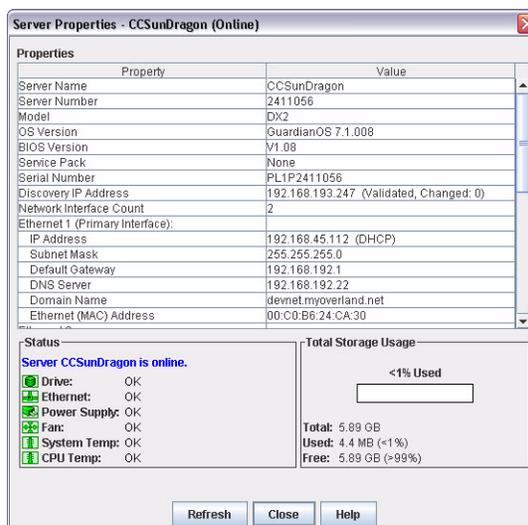
Administration Menu Dialog Boxes:

These special menu and sub-menu options apply to GuardianOS servers only:

- [Administering Servers](#)
 - [Apply Schedule \(Start Later\)](#)
 - [Apply to Servers](#)
 - [Operations Report](#)
 - [Current Settings for Servers](#)
- [Set IP Address](#)
- [Feature Licensing](#)
- [Server Software Updates](#)

Server Properties

The Server Properties dialog box (**Edit > Properties** or right-click server name) provides a summary of server specifications and status data.



Ethernet Indicators (GuardianOS only)

The following table explains the status coding for the Ethernet status indicators.

Status	Description
	All Ethernet connections are operating properly.
 (Only displayed if the no-link status check box is enabled in the Options dialog box)	At least one Ethernet connection has a link error. Possible causes include a loose or faulty cable; or perhaps a problem with a connecting switch or hub. NOTE: SSM cannot distinguish between a NIC that is not in use and a NIC that is disconnected. If you are using only one NIC on a SnapServer, the NIC status will remain yellow.
	At least one Ethernet interface is not functioning.
	Ethernet status is not available (server may be offline).

The Discovery IP Address

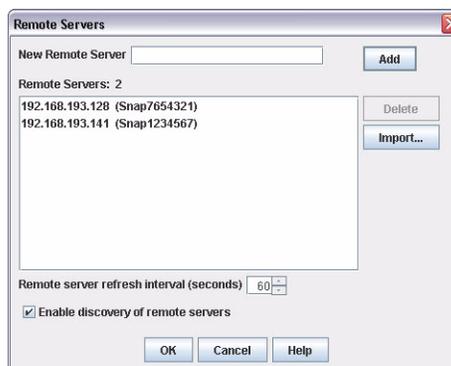
The word *Discovery* is placed next to the IP address used to discover the server. SSM uses this IP address to communicate with the server when performing View/Copy and Apply operations.

Total Storage Usage (GuardianOS only)

The percentage refers only to capacity that has been allocated to existing volumes; unallocated RAID capacity is not included.

Remote Servers

Select **Edit > Remote Servers** to open this dialog box. It is used to add servers that reside outside the network segment on which SnapServer Manager resides. See [“Discovery” on page 1-6](#).



Available Options

These options are available with this dialog box:

Add Remote Servers

Enter the server's IP address or server name in the New Remote Server field and click **Add**.

- If you entered the IP address, it appears in the Remote Servers list box, with the server name in parentheses (if resolved).
- If you entered the server name, it appears in the Remote Servers list box, with the IP address in parentheses (if resolved).
- If SSM cannot find the remote server you entered, **unresolved** appears in the Remote Servers list box.

The current number of remote servers is listed above the Remote Servers list box. The maximum allowed remote servers is 5000.

NOTE: If the remote servers being imported would make the full list greater than 5000 servers, SSM displays a prompt to truncate the list being imported.

Delete a Remote Server

In the Remote Servers list box, select one or more remote servers and click **Delete**.

Adjust the Remote Server Refresh Interval

Adjust the interval to a setting between 30 seconds and 90 seconds.

Toggle Discovery of Remote Servers

Click the **Enable discovery of remote servers** check box.

Importing a Remote Server List

Remote server names and/or IP addresses can be imported from a text file. Within the text file, each server and IP address can be designated either by entering one server per line, or by entering multiple server names separated by a space, a comma, or a semi-colon. Blank lines and lines beginning with the number sign (#) are ignored.

Import a Remote Servers List

Click the **Import** button and navigate to the appropriate text file. Click **OK**.

The remote servers list will be added to the existing list, ignoring duplicate servers.

Options

The Options dialog box allows you to:

- Specify the Web browser that SSM uses.
- Set the period after which a server will be considered offline after receipt of the last discovery packet.
- Specify whether SSM displays a warning if any Ethernet port has no link (GuardianOS only).
- Instruct SSM to directly scan all servers.
- Configure an HTTP proxy server for online registration (GuardianOS only).
- Enable or disable automatic notification of OS updates (GuardianOS only).



Specify a Web Browser

You can specify the Web browser you would like SnapServer Manager to use to display the Web Management Interface and the SSM help system.

- Click **Browse** to navigate to and select the executable for your chosen browser.
- Click **Test** to open this help window in your chosen browser.

Adjust the Server Offline Timeout Setting

SSM constantly updates the server list with fresh data it receives from servers that reside on its local network segment and are specified on the Remote Servers list. SSM considers a server offline if no communication occurs for the specified time-out period. (The default timeout period is 180 seconds.) If SSM receives no communication from a server for 180 seconds, it displays that server as offline in the Server List of the main SSM screen. Adjust this interval to a setting between 120 seconds and 300 seconds as appropriate for your network conditions.

Display No-Link Status Warnings for Ethernet Ports (GuardianOS only)

SSM is set by default to display a warning status if one of a server's Ethernet ports has no link. With this feature activated, you can quickly see all servers with no-link status Ethernet ports (such as, unplugged Ethernet cables). You may wish to disable the no-link status feature if you have servers with only one connected Ethernet port. To disable the feature, uncheck the **Display warning if any of a server's Ethernet ports has no link** check box, and click **OK**.

Activate Auto-scanning of All Remote Servers

When SnapServer Manager is installed on a laptop that is moved from one network segment to another, some remote servers may appear to be offline when they are in fact online. The **Auto-scan servers not on Remote Servers list** option ensures that discovery works properly by sending discovery request packets to each server discovered in a previous session; this solution does, however, increase network traffic. To activate auto-scanning, select the check box and click **OK**.

Use an HTTP Proxy Server (GuardianOS only)

In environments that use an HTTP proxy server for external web-based communication, SSM must be configured to use the proxy for online server registration. Check **Use a proxy server for HTTP communication**, enter the name or IP address of the proxy server in the **Proxy host** field, and enter the port used by the proxy server in the **Proxy port** field.

Enable Automatic Update Notification (GuardianOS only)

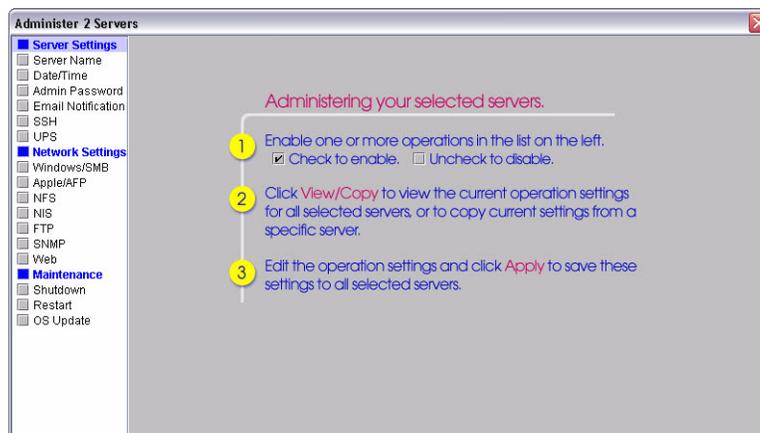
SSM is configured by default to check daily for available updates to the GuardianOS. When an update is found, an alert displays in a banner at the top of the SSM main window. The *Tell me more* link in the banner opens the Server Software Updates dialog, listing servers for which an update is available, the version of GuardianOS each server is currently running, and the version to which each server could update.

Tip: 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* is selected, the server will display the banner after the next check for updates. If *Hide this message* is selected, the server will hide the banner for the update in question until a later version is released.

To disable this feature, uncheck the **Enable Automatic Update Notification** check box and click **OK**.

Administering Servers

Select **Administration > Administer Servers** to open this dialog box. It is the starting point for configuring, viewing, or copying settings for servers running GuardianOS.



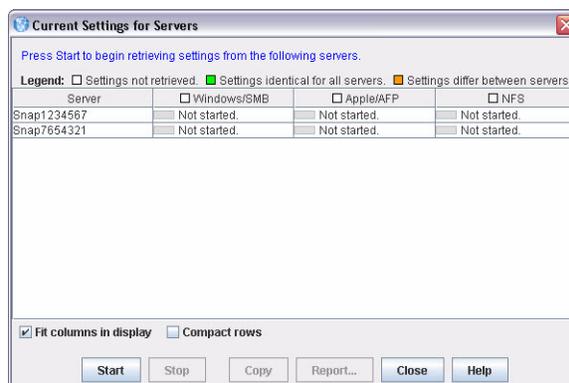
Configure Settings

1. Select a task in the left pane.
A check mark indicates the task is active and its fields are editable.
2. Edit the settings as appropriate.
3. Repeat [Steps 1–2](#) for any other tasks to be modified.
4. When you are finished configuring settings, click **Apply**.
5. In the Apply to Servers dialog, click **Start Now** (or **Start Later**) to begin applying modifications across servers.

NOTE: If you schedule the update for a later time, you will not be able to perform any other operations on the servers being updated until the scheduled update has completed.

View or Copy Settings

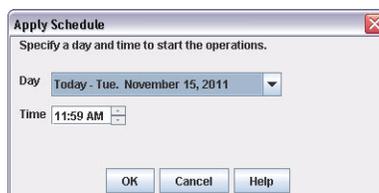
1. Select the **tasks** whose settings you want to view or copy.
A check mark indicates the task is active.
2. Click **View/Copy**.
3. In the Current Server Settings dialog, click **Start** to begin retrieving settings.



4. When copied, close this window to return to the Administer Servers window.
The selected settings will be populated with the copied values.

Apply Schedule (Start Later)

When administering GuardianOS server options (see [“Administering Servers” on page 3-6](#)), clicking **Apply** opens the Apply to Server dialog box with a **Start Later** button located at the bottom. You can use it to schedule a set of operations to run up to one week in the future.



Before scheduling operations, note the following:

- SnapServer Manager **must remain running** – For scheduled operations to take effect at the specified time, SSM must remain running. SSM will display an error message if you attempt to close the application while operations are scheduled.
- **No other operations are possible** – Until a scheduled operation completes, no other changes can occur. SSM allows you to run one set of operations at a time; you cannot start one set of operations on one group of servers, and then run a different set on another group of servers while the first operation is still scheduled or running.

Schedule Operations to Run at a Later Time

1. Select a day and time from the fields provided, and click **OK**.
The **Hide** button appears in the Apply to Servers dialog box.
2. Click **Hide** to return to the main SSM screen.
You can monitor server status and properties, manage server groups, and administer servers using the Web Management Interface, but no other operations can be run until after the scheduled operations are completed.

Change a Scheduled Operation

If a scheduled operation exists, the Status Bar on the screen displays a message similar to the following:

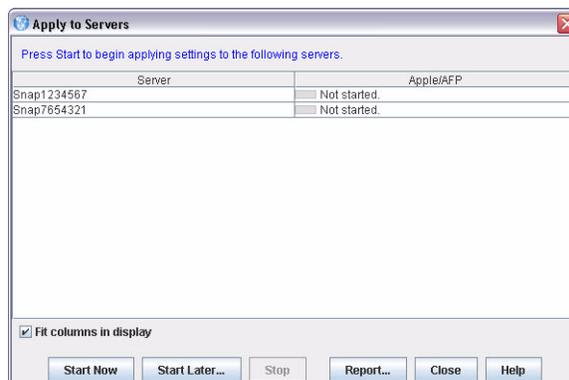
```
Operations are scheduled to run on Monday January 11, 2010 at  
1:57 PM. (Click to view.)
```

Click the message to view or cancel the scheduled operations. After the Apply to Servers screen reopens, you can do one of the following:

- Click **Stop** to cancel the scheduled operations.
- Click **Hide** to return to the main SSM screen.

Apply to Servers

When administering GuardianOS server options (see [“Administering Servers” on page 3-6](#)), clicking **Apply** opens this dialog box. It lists operations to be performed on a group of servers running GuardianOS.



Available Options

The three buttons at the bottom activate the options available with this dialog box:

Run the Operations Now

Click **Start Now**. The interface informs you of the progress (progress bar) and result of the operations.

Schedule the Operations to Run Later

1. Click **Start Later**.
2. In the Apply Schedule dialog box that opens, select a date and time and click **OK**. You return to the Apply to Servers dialog box.
3. Click **Hide** to return to the main screen.

Tip: The status bar in the main screen displays the status of the scheduled operations. While operations are scheduled to run, no other multiserver administration is possible.

Generate an Operations Report

1. Click **Report** to open the Operations Report dialog box.
2. Do one of the following:
 - To set up email report delivery for this and all future operations, complete the fields provided and click **OK**.
 - To save an operations report for this operation only, click **Save Report**.

Improve the Readability of the Display

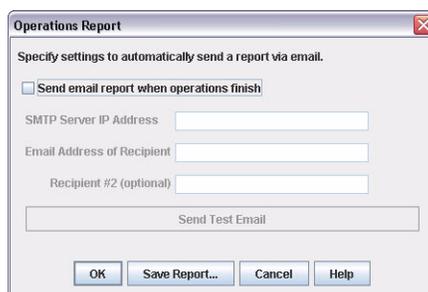
When working with a large number of settings or servers, use the following methods to improve the readability of the display.

Method	Description
Fit Columns in Display	When selected (default), this option resizes column widths to fit in the current size of the window. All columns are visible, but text within columns may be clipped. When deselected, column widths expand to fit the width of its contents, but some columns may not be visible.
Resizing columns	To resize a column, hover the cursor over the border between column headers, and then click and drag to the desired width

Operations Report

When administering GuardianOS server options (see [“Administering Servers” on page 3-6](#)), clicking **Apply** opens the Apply to Servers dialog box with a **Reports** button located at the bottom. Clicking that button opens this dialog box which serves two functions:

- Configuring SSM to automatically deliver an operations report by email.
- Saving an individual operations report as a CSV file.



View a Sample Operations Report

Below is an operations report on changing SSH settings for three servers:

```
SnapServer Manager Report:
All operations completed successfully on Monday January 11, 2011 at
8:29 AM.
Operations started by user jsmith on machine sales/209.219.19.19, on
Monday January 11, 2011 at 8:29 AM.
Server      SSH
Server_1    OK
Server_2    OK
Server_3    OK
```

Configure SSM to Automatically Deliver Operations Reports By Email

Complete the following fields and click **OK**.

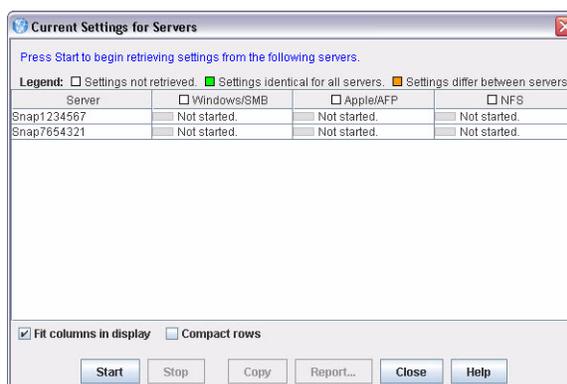
Option	Description
Send Email Report	Select this option to have SSM email all operations reports to the specified recipients.
SMTP Server	Enter the mail server IP address.
Email Addresses	Enter up to two email addresses in the spaces provided.
Send Test Email	Click this button to verify your settings.

Save a Single Copy of an Operations Report

Click **Save Report** to open a Save dialog box and save the report as a CSV file to a location of your choice.

Current Settings for Servers

When administering GuardianOS server options (see [“Administering Servers” on page 3-6](#)), clicking **View/Copy** opens this dialog box. It allows administrators to view and compare settings across a group of servers running GuardianOS. A legend for the headings is displayed at the top.



Available Options

The three buttons at the bottom activate the options available with this dialog box:

View and Compare Settings Across a Group of Servers

Click **Start**. The interface provides feedback on the progress of the operation in the form of a progress bar. The legend indicates where settings differ among servers.

Copy Settings

Select a server row, and then click **Copy**. Close this window to return to the Administer Servers window. The selected settings will be populated with the copied values.

Generate an Operations Report

Once SSM retrieves server settings, the **Report** button becomes available. Click **Report** to save the settings to a CSV file.

Improve the Readability of the Display

When working with a large number of settings or servers, use the following methods to improve the readability of the main display.

Method	Description
Fit Columns in Display	<p>When selected (default), this option resizes column widths to fit in the current size of the window. All columns are visible, but text within columns may be clipped.</p> <p>When deselected, column widths expand to fit the width of its contents, but some columns may not be visible.</p>
Compact Rows	<p>When selected, this option displays only the first text line of each row. All (or most) server rows will be visible, but most text is clipped.</p> <p>When deselected (default), all text lines display, but it may be necessary to use the scroll bars to see some rows and/or columns.</p>
Resizing columns	To resize a column, hover the cursor over the border between column headers, and then click and drag to the desired width

Set IP Address

By default, SnapServers are preconfigured to use DHCP to acquire an IP address at startup. If a SnapServer cannot find a DHCP server on the network, it will default to an address of “ZeroConf,” and you may not be able to see the server on your network. In this case, the Set IP Address feature can be used to assign a fixed IP address to the server.

NOTE: GuardianOS 6.0 and earlier servers will show 10.10.10.10 as the IP address in this case rather than ZeroConf.

Set IP Address is only available for servers that are configured for DHCP and have not received an IP address from a DHCP server.

Set a Server's IP Address

1. In the SSM main screen, select a server.
2. Right-click the server, and select **Set IP Address**.
3. Enter the following required information in the TCP/IP Addressing fields:
 - IP address
 - Subnet mask
4. Optionally, you may also specify the default gateway, domain name server, domain name, and WINS server as appropriate.

Feature Licensing

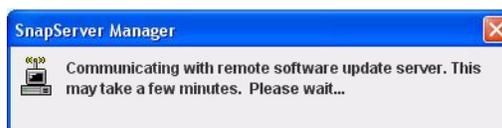
Use the Feature Licensing menu (**Administration > Feature Licensing**) to apply SnapExtension license keys to one or more GuardianOS servers. There is no limit to the number of licenses that can be entered using this dialog box. Click **Enter License**, then enter one or more license keys per line or separated by spaces, and click **OK**. This feature is only available with GuardianOS v 4.0 or later.



The Feature License dialog box does not display any pre-existing SnapExtension licenses. Only licenses that have been applied while the current dialog box is open will be displayed.

Server Software Updates

When you select **Administration > Check for Server Software Updates**, the SnapServer Manager connects with a remote server to determine if any of the GuardianOS servers it is monitoring have new software updates available.



The resulting dialog box lists all of the GuardianOS servers that SSM has discovered that have updates available, and provides the following information about the servers:

Property	Description
Server Name	Name of the SnapServer that has an update available.
Current OS version	Version of GuardianOS currently running on the SnapServer.
Update OS version	Version of GuardianOS that the server can be updated to.

Apply Software Updates

1. To download the available GuardianOS update, click the **Download this software** link.
2. SSM creates a special SSM Server Group called **<Updates Available>**. It contains all the servers for which each update is applicable. Apply the software update to the servers in this folder.

Symbols

> (menu flow indicator) **PR-4**

A

Admin Password option **2-5**
 Administer Servers configuration screen **2-1**
 Administer Servers dialog box **3-6**
 alert definitions **PR-4**
 APC UPS set up **2-8**
 Apply Schedule dialog box **3-7**
 Apply to Servers dialog box **3-8, 3-9**
 Authentication
 NIS domain, joining **2-15**
 Web (http) **2-19**
 auto-scanning from servers **3-5**

B

blue IP address **1-7**

C

CA Unicenter TNg **2-18**
 Client access, configuring
 FTP/FTPS **2-16**
 NFS **2-14**
 Windows (SMB) **2-10**
 communication indicators **1-4**
 compare settings **1-6**
 conventions, typographical **PR-4**
 Current Settings for Servers dialog box **3-11**
 customer support **PR-3**
 customizing the interface **1-9**

D

Date/Time option **2-3**
 default SSM window **1-2**
 default timeout period **3-5**
 Discovery flag **3-2**
 discovery LEDs **1-7**
 discovery request packet **1-7**
 Documents
 related to SnapServers **PR-5**
 Domain, joining
 NIS **2-15**
 download website link **PR-4**

E

electrostatic discharge information **PR-5**
 Email notification of server events, configuring **2-6**
 Email Notifications option **2-6**
 Ethernet port no link **3-5**
 Ethernet status indicators **3-2**

F

firmware update **1-5, 1-6**
 FTP/FTPS **2-16**
 configuring access **2-16**
 FTP/FTPS option **2-16**

G

GuardianOS
 software update **2-22**

H

HP Open View **2-18**
 HTTP proxy **3-5**

I

- icons **1-3**
- import remote server list **3-4**
- Internal temperature, e-mail notification of **2-7**

L

- laptop SSM installation **1-8**
- Launch Web Administration **1-7**
- local server **1-7**

M

- Macintosh
 - enabling Appletalk for **2-12**
- main window **1-2**
- menu flow indicator **PR-4**
- methods ensuring correct server display **1-9**
- Monitoring
 - configuring SNMP alerts **2-18**
 - email notification **2-6**

N

- Network Information Service (NIS)
 - joining an NIS domain **2-15**
- NFS access
 - configuring **2-14**
- NIS option **2-15**

O

- Options dialog box **3-4**
- OS Update option **2-21**
- Overland technical support **PR-3**

P

- product documentation **PR-3**

R

- readability **3-12**
- Reboot
 - setting up alert for **2-7**
- remote server **1-8**
- remote server list import **3-4**

- Remote Servers **1-8**
- Remote Servers dialog box **3-3**
- remove offline servers **1-12**
- Restart option **2-21**
- Resynchronization, setting alert for completion of **2-7**
- Rx **1-4**
- Rx LED **1-7**

S

- scheduled operation message **3-8**
- Secure HTTP. See HTTPS
- Security
 - https encryption **2-20**
 - NIS authentication **2-15**
- Server Details list **1-3, 1-12**
- Server Details screen
 - status icons **1-3**
- Server Details screen icons **1-3**
- server discovery **1-7**
- server groups **1-10**
- server groups XML file **1-12**
- Server Name option **2-2**
- Server Properties dialog box **3-1**
- Server registration
 - performing **1-5**
- Shutdown option **2-20**
- Simple Network Management Protocol. See SNMP
- simultaneous configuration modifications **1-5**
- SMB, configuring **2-10**
- SnapServer Manager
 - description **1-1**
 - main window **1-2**
 - using **1-5**
- SnapServers
 - configuring email notification of server events **2-6**
 - setting e-mail alerts for **2-7**
 - SNMP alerts **2-18**
- SNMP
 - configuring alerts **2-18**
 - overview **2-17**
 - supported NMS applications **2-18**
 - supported traps **2-18**
- SNMP option **2-17**
- software update **PR-3, PR-4**
- SSH options **2-8**
- SSM interface customization **1-9**

SSM on a laptop 1-8
Start Later option 3-7
static IP address, setting 1-6
Status Column icons 1-3

T

technical support PR-3
time zone 2-3
timeout setting 3-5
Tivoli NetView 2-18
Tx 1-4
Tx LED 1-7
typographical conventions PR-4

U

update banner 1-5
Update notification 1-6, 3-6
UPS options 2-8
usage scenarios 1-13
Users
 joining NIS security 2-15

V

Volumes
 capacity reached alert 2-7

W

Web browser choice 3-5
Web Management Interface 1-7
Web option 2-19
Windows
 configuring client access 2-10
Windows/SMB option 2-10

X

XML file, server groups 1-12