ADMINISTRATION GUIDE

Cisco Small Business

NSS3000 Series Network Storage System

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2008 Cisco Systems, Inc. All rights reserved.

Contents

Introduction

Thank you for choosing the Cisco Small Business Network Storage System (NSS).

The NSS is a Network Attached Storage (NAS) unit that appears as a native file server for the various clients within your network, including Windows, Apple Macintosh, UNIX, and Linux platforms. The biggest benefit to your users is that they can now access data that might be stored across different physical platforms as simply as if it were on their own computers. The NSS provides a single repository that is completely dedicated to storage, ensuring the integrity, reliability, and accessibility of your data for a relatively low cost.

The NSS lets you install up to four physical disk drives. The NSS uses the most common file-based protocols such as NFS, CIFS, and FTP for file sharing.

Benefits

The NSS offers these main advantages to your business:

- **Cross-platform File Sharing**: Share files easily and inexpensively across different platforms over a cost-effective Ethernet and IP network.
- **Easy Installation and Administration**: With a basic understanding of networking, the NSS is easily configured, managed, and made available to all of users on your network.
- **Data Consolidation**: Centralize data to reduce management costs and maximize your investment in existing hardware. This also means better data security.

Using the Help

The NSS help file provides information about using the configuration interface to configure the NSS.

Audience

The information contained in the help pages is intended for use by network administrators. It assumes a basic understanding of storage-related concepts, including RAID, filesystems, and networking.

About the NSS Configuration Interface

The NSS configuration interface contains basic navigation features to help you as you configure the NSS.

- **Manager Menu**: The Manager Menu forms the left side of the configuration interface window. It contains the menu options that represent the major configuration areas for the NSS. For example, System, Network, Share, Storage. When you click an option, a sub-menu of related options appears. Clicking a topic opens the associated topic in the **Topic** page in the right side of the window.
- **Topic Page**: When you select a topic from the **Manager Menu**, the configuration page for that topic appears in the right side of the window.

Getting Help

There are two buttons on the NSS configuration window that you can click to access the help:

- From the **Manager Menu** click **Help** to display the full online Administrator Guide. Use the navigation tools within the help to find information for your chosen topic.
- A context-sensitive help button appears in the upper-right corner of the topic page. Click it to display help on the specific configuration area. For example, if the current configuration topic is about the status of your system, click the **Help** button for information about the details that appear on the **System Status** page.

Refreshing the GUI Pages

Although certain GUI pages automatically refresh at a preselected time interval, some pages do not refresh until they are reselected. The best way to manually refresh a GUI page is to reselect it through the options in the **Manager Menu** on the left side of the GUI window. For example, to refresh the NTP Configuration page, from the **Manager Menu,** click **Admin** and then click **Time**.

We recommend that you do not use the Refresh button on the Web browser toolbar as this can cause data issues.

Using the Quick Setup Wizards to Configure the NSS

There are three wizards available from the Manager Menu of the configuration interface. Select the wizard and then follow the onscreen instructions.

- **Initial Setup**: Automatically appears when you log into the configuration interface for the first time. Although you can access it at any time from the **Manager Menu**, if you have saved any configuration settings before you run the wizard, running the wizard will erase any saved data.

  For example, if you configure a RAID and then run the wizard, the RAID will be deleted. The NSS then reboots and the wizard steps you through the basic configuration to create a RAID, volume, share, user, to set the **Home Directory** location, set the time, and so on.

- **IP Camera Options**: The FTP and CIFS wizards let you set up the NSS to store videos from IP surveillance cameras. The type of wizard you choose depends on the way the camera transfers the video clips.

  NOTE You only need to run the wizard once and then you must configure each camera to output the video to the configured share.

  When running either of the wizards make sure that you create a RAID array, a volume, and any users that you want to grant access to the surveillance videos. After running the wizard you must map a network drive to the share on the PC running the camera utility and configure the camera utility to save the video to this mapped network drive.

- **FTP**: Run this wizard if the cameras are set up to transfer motion-triggered clips through FTP. Running the wizard creates a single user and FTP share for the cameras. The videos are then saved within the FTP share which contains a subfolder dedicated to each camera. After you run the wizard, you must configure each camera to output the video to the configured NSS share. Use the information summarized on the last page of the wizard to set up the cameras through their configuration interface.
- **CIFS**: Run this wizard if the cameras have a Windows utility program that lets you save the streaming video to a local drive (or in this case, the NSS) and then view the video from its saved location. The wizard creates a single user and share for all cameras that are configured to stream video to the Windows camera utility program. After you run the wizard, you must map the network drive from the PC that runs the Windows utility program to the CIFS share and then set up the utility to save to the mapped network drive.

Approved Vendor List for Drives

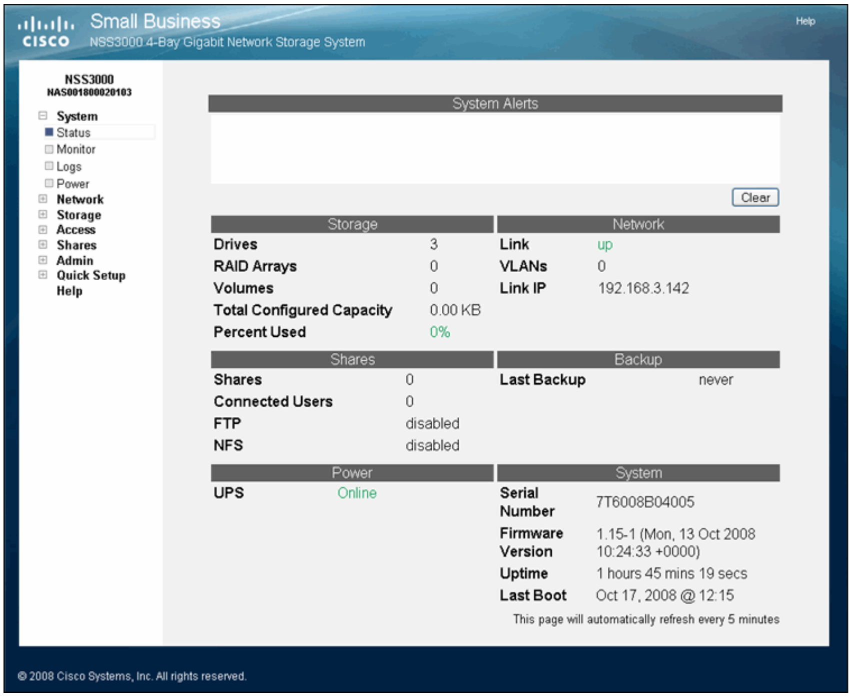
If you are purchasing disk drives to install in the NSS, see the Approved Vendor List at www.cisco.com/go/smallbiz for a list of recommended disk drives.

When you select a disk drive, consider the type of RAID levels required to service your business needs. For example, if you are creating a RAID (versus a JBOD), make sure that each of the disks used in the array have the same disk capacity. The RAID is built using the capacity of the smallest disk in the array.

Managing the System

The NSS3000 lets you view status details from two locations: the LCD panel on the front of the chassis, or from the **Configuration Interface**. See ”About the NSS Configuration Interface” on page 2. The LCD lets you view some of the status information such as the hostname, IP address, netmask system alerts, RAID status, volume status, cable diagnostics, time and date, firmware version and firmware upgrade status, and bootup and shutdown status.

The **System Status** page provides an overview of the current operating condition of the NSS. For example, you can view system alert messages such as if a disk drive is failing or has failed, if a volume is approaching its full capacity, and if an array rebuild is complete. You can also view the current status of any of the following: storage, shares, backups, network, power, and system details. Status pages like the **System Status** page automatically refresh on a regular interval and are helpful for monitoring the progress of certain processes such as building a RAID.



Storage		Network	
Drives	3	Link	up
RAID Arrays	0	VLANs	0
Volumes	0	Link IP	192.168.3.142
Total Configured Capacity	0.00 KB		
Percent Used	0%		

Shares		Backup	
Shares	0	Last Backup	never
Connected Users	0		
FTP	disabled		
NFS	disabled		

Power		System	
UPS	Online	Serial Number	7T6008B04005
		Firmware Version	1.15-1 (Mon, 13 Oct 2008 10:24:33 +0000)
		Uptime	1 hours 45 mins 19 secs
		Last Boot	Oct 17, 2008 @ 12:15

This page will automatically refresh every 5 minutes

The following sections describe the information that appears on the **System Status** page.

System Alerts

The **System Alerts** section shows any system messages issued since the last time they were cleared. Messages can range in severity from informational to immediate action required.

There are three type of alerts that can appear:

- **Error**: Indicates the most severe types of problems with the NSS. They require immediate action. For example, if a disk drive or RAID array is in a failed condition.
- **Warning**: Indicates that there is a problem with the NSS that requires eventual action. For example, if the amount of storage used for a volume is over 90%.
- **Notification**: These types of messages are simply to advise of changes to the NSS. For example, the RAID rebuild is complete.

Storage Status

The **Storage** area displays details about the configured storage on the NSS, including:

- **Drives**: The number of physical disk drives installed.
- **RAID Arrays**: The number of configured RAID arrays.
- **Volumes**: The number of configured volumes.
- **Total Configured Capacity**: The total aggregate size of all configured volumes.
- **Percent Used**: The total amount of the configured capacity used.

Network Status

The **Network** area displays the following:

- **Link**: The current status of the Ethernet link. The only status that is visible is if the link is up. If the link is down, you cannot access the Configuration Manager.
- **VLANs**: The number of VLANs configured on the NSS.
- **Link IP**: The IP address of the Ethernet link.

Shares Status

The **Shares** area displays status for the following:

- **Shares**: The number of configured shares.
- **Connected Users**: The total number of user sessions currently connected to the NSS.
- **FTP**: The FTP access state (enabled or disabled).
- **NFS**: The NFS access state (enabled or disabled).

Backup Status

The **Backup** area displays the following:

- **Last Backup**: The date and time of the last backup run. If a backup has never been run on the system, the word "never" appears.

Power Status

The **Power** area displays the following:

- **UPS**: The following options are available depending on the current operating condition of the UPS. For more information about the functioning of the UPS, refer to the UPS documentation.
  - **Disabled**: A UPS is not currently connected to the NSS or is not enabled.
  - **Online**: A UPS is connected to the NSS and is enabled. The NSS is deriving power from the mains power.
  - **On Battery (%)**: The NSS is currently deriving its power from the UPS battery. The percentage of power still available is also listed.

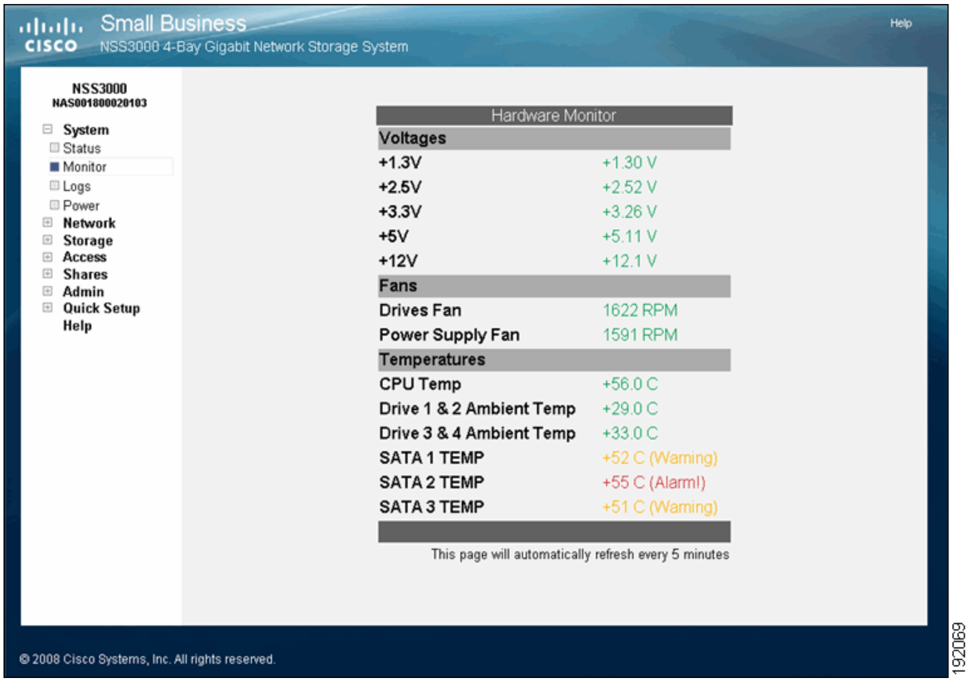
System Status

The **System** area displays the following:

- **Serial Number**: The serial number of the NSS.
- **Firmware Version**: The current version and date of the firmware installed on the NSS.
- **Uptime**: The number of days the NSS has been running since it was last rebooted.
- **Last Boot**: The date when the NSS was last rebooted.

Viewing the Hardware Monitor

The **Hardware Monitor** page displays details about the following physical conditions related to the NSS:



Hardware Monitor	
Voltages	
+1.3V	+1.30 V
+2.5V	+2.52 V
+3.3V	+3.26 V
+5V	+5.11 V
+12V	+12.1 V
Fans	
Drives Fan	1622 RPM
Power Supply Fan	1591 RPM
Temperatures	
CPU Temp	+56.0 C
Drive 1 & 2 Ambient Temp	+29.0 C
Drive 3 & 4 Ambient Temp	+33.0 C
SATA 1 TEMP	+52 C (Warning)
SATA 2 TEMP	+55 C (Alarm!)
SATA 3 TEMP	+51 C (Warning)

This page will automatically refresh every 5 minutes

© 2008 Cisco Systems, Inc. All rights reserved.

- **Voltages**: The current voltage reading for all voltage rails in the system. The reading is color-coded depending on if the voltage level is within specification (green) or out of specification and in need of attention (red).
- **Fans**: The fan speed for each chassis fan. If the fan has stalled, the reading is color-coded red. Normal fan operation is color-coded green.
- **Temperatures**: The NSS has temperature sensors located at various parts of the chassis. Temperature readings are done from these sensors as well as from any installed disks (if the disk has an internal temperature sensor).
  - If a disk does not have a temperature sensor, the reading appears as "unavailable".
  - If the temperature of the system or disks is over or under the ideal temperature, the temperature is color-coded red. When the temperature is within the normal range the color-coding is green.

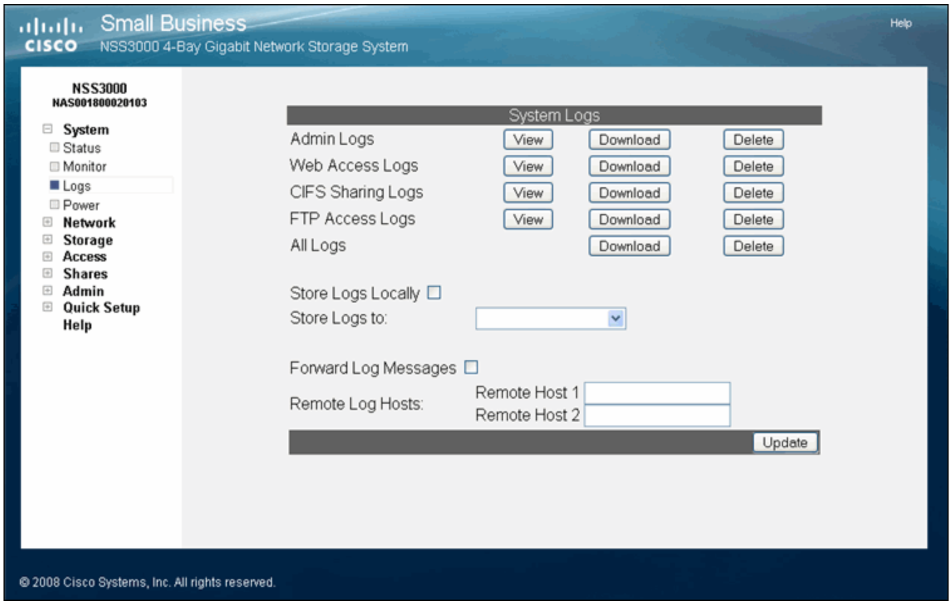
Viewing and Managing the System Logs

The NSS captures various types of information into log files, such as user access details. You can store the logs locally or on a remote server on the network. Since local space allocated for log files is limited, the logs are overwritten once the space is filled.

To work with the log files:

STEP 1 From the **Manager Menu**, click **System** ➔ **Logs**.

The **System Logs** page appears.

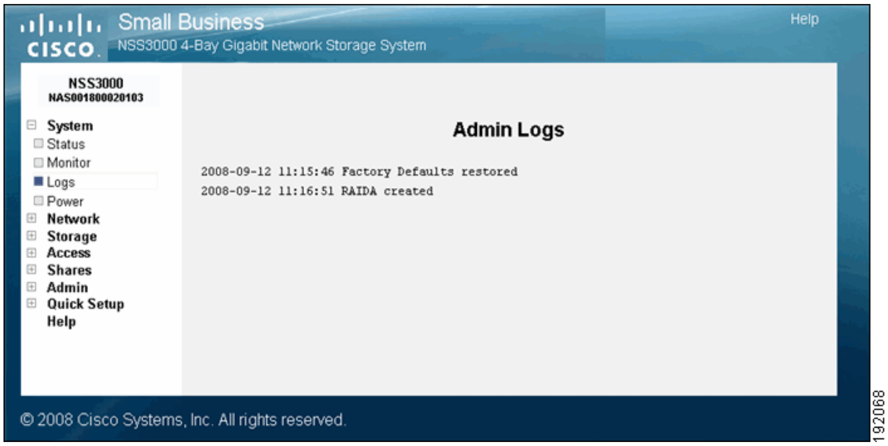

Small Business
CISCO
NSS3000 4-Bay Gigabit Network Storage System
Help
NSS3000
NAS001800020103
System
Status
Monitor
Logs
Power
Network
Storage
Access
Shares
Admin
Quick Setup
Help
System Logs
Admin Logs View Download Delete
Web Access Logs View Download Delete
CIFS Sharing Logs View Download Delete
FTP Access Logs View Download Delete
All Logs Download Delete
Store Logs Locally □
Store Logs to:
Forward Log Messages □
Remote Log Hosts: Remote Host 1 Remote Host 2
Update
© 2008 Cisco Systems, Inc. All rights reserved.
192067

You can view, download, or delete these types of log files:

- **Admin**: A full list of time-stamped actions that were initiated through the NSS configuration interface.
- **Web Access**: This log displays IP addresses of the systems that accessed the NSS configuration interface and the date and time of the authentication requests. This information helps you detect unauthorized attempts to access the NSS configuration interface.
- **CIFS Sharing**: A time-stamped event log of events initiated by users accessing shares through CIFS.

- **FTP Access**: A time-stamped log of FTP actions, including user logins, file transfers, and user logouts.
- **All Logs**: A list of all the log files. You can download and save this file.

This is an example of the **Administrator Log** window:



Admin Logs

```
2008-09-12 11:15:46 Factory Defaults restored
2008-09-12 11:16:51 RAIDA created
```

STEP 2 Choose where you want to store the log files:

- **Locally**: To store the log files on the NSS, select **Store Logs Locally**, and then select the volume to which you want to store the logs from the options in the **Store Logs to** drop-down menu.
- **Remotely**: To store the log files on a remote server, select **Forward Log Messages**, and then enter the hostname or IP address of the server in one or both of the **Remote Log Host** fields. (If you set up two remote hosts, the log file is sent to both servers.) Note that the remote server must be running a syslog server.

STEP 3 Click **Update**.

Configuring the System for UPS Support

You can set up the NSS to use an uninterruptible power supply (UPS) if one is connected directly to the UPS port on the NSS. The **Power Status** page provides an overview of the current power condition of the NSS.

NOTE When the UPS power goes to low battery, a signal is sent through the USB port on the NSS and a shutdown of the NSS is initiated. Make sure that the UPS has enough reserve power to sustain the NSS through the shutdown (approximately 5 minutes)

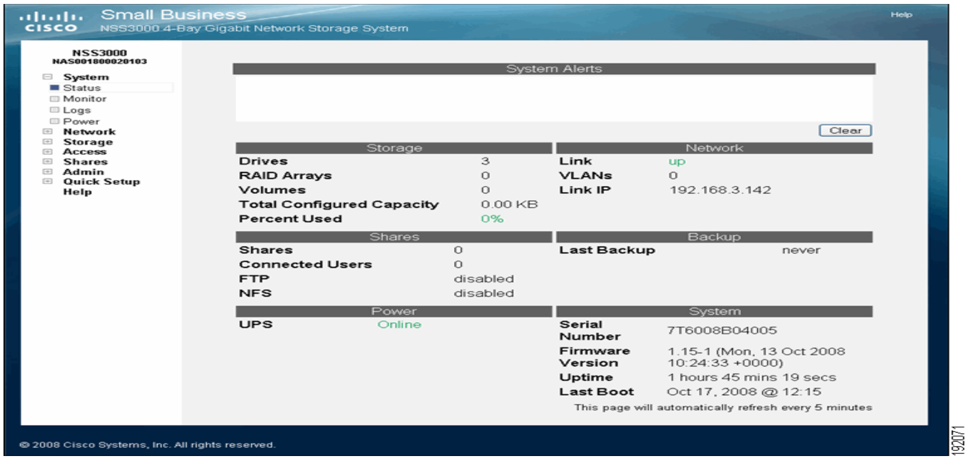
The Power area displays the following:

- **AC Status:** The following options are available depending on the current operating condition of the UPS. For more information about the functioning of the UPS, refer to the UPS documentation.
- **Disconnected**: A UPS is not currently connected to the NSS or has not yet been enabled.
- **Online**: A UPS is connected to the NSS and is enabled. The NSS is deriving power from the mains power.
- **On Battery**: The NSS is currently deriving its power from the UPS battery.
- **Battery Status**: The percentage of power still available is also listed and is color-coded according to the amount of battery remaining.

To enable the UPS:

STEP 1 From the **Manager Menu**, click **System** ➜ **Power**.

The **System Power** page appears.



Storage	
Drives	3
RAID Arrays	0
Volumes	0
Total Configured Capacity	0.00 KB
Percent Used	0%

Network	
Link	up
VLANs	0
Link IP	192.168.3.142

Shares	
Shares	0
Connected Users	0
FTP	disabled
NFS	disabled

Backup	
Last Backup	never

Power	
UPS	Online

System	
Serial Number	7T6008B04005
Firmware Version	1.15-1 (Mon, 13 Oct 2008 10:24:33 +0000)
Uptime	1 hours 45 mins 19 secs
Last Boot	Oct 17, 2008 @ 12:15

This page will automatically refresh every 5 minutes

© 2008 Cisco Systems, Inc. All rights reserved.

STEP 2 Select **Enable UPS support**.

STEP 3 Click **Update**.

NSS-Supported UPS Product Families

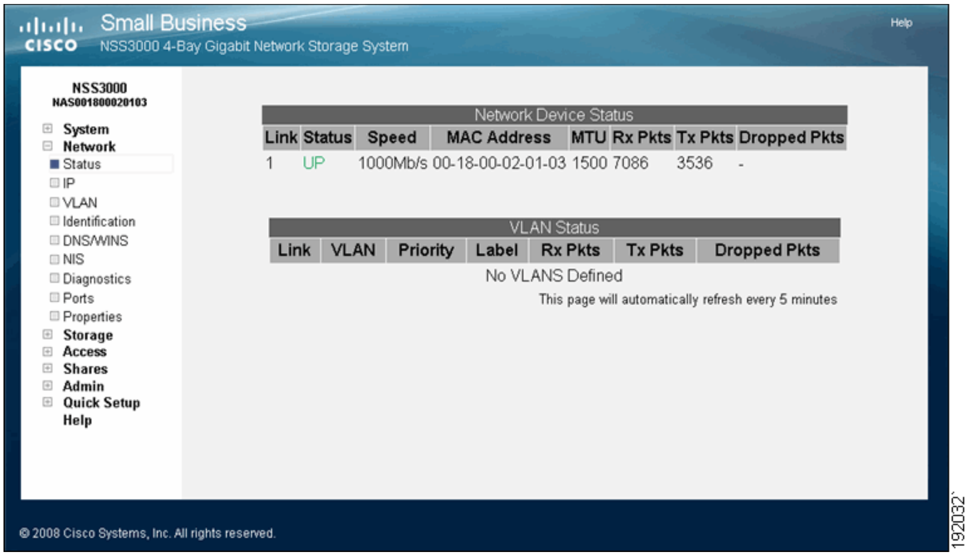
The NSS supports these UPS product families:

- APC Back-UPS Pro USB
- APC Back-UPS RS USB
- APC Back-UPS USB
- APC Back-UPS LS USB
- APC Back-UPS ES/CyberFort 350
- APC Smart-UPS USB

3

Adding the NSS to your Network

The **Network Device Status** page displays the current status of the NSS physical and virtual network interfaces.



Network Device Status

Link	Status	Speed	MAC Address	MTU	Rx Pkts	Tx Pkts	Dropped Pkts
1	UP	1000Mb/s	00-18-00-02-01-03	1500	7086	3536	-

VLAN Status

Link	VLAN	Priority	Label	Rx Pkts	Tx Pkts	Dropped Pkts

No VLANS Defined

This page will automatically refresh every 5 minutes

© 2008 Cisco Systems, Inc. All rights reserved.

Physical Interfaces

The **Network Device Status** table displays the current status of the physical Ethernet link connected to the NSS.

- **Link**: The number of the physical link attached to the NSS. The number appears as 1.
- **Status**: The status of the physical link.
- **Dropped Pkts**: The total number of IP packets dropped on the VLAN interface since the last boot.

- **Status**: The status of the physical link. Options include:
  - **Up**: The link is up (color-coded green) and is operational.
  - **Down**: The link is down (color-coded red) and not operational. If a cable is connected to the Ethernet port, check the cable integrity and the status of the device (switch, router, or computer) at the other end of the cable. You can use the NSS cable diagnostic feature to assist you. See "Running Diagnostics of your Physical Link from the Configuration Interface" on page 32.

    If the link is down, this status is not visible since you cannot access the **Configuration Manager**.
- **Speed**: The configured speed, in Mbps, of the physical link. Options include: 10 Mbps, 100 Mbps, 1000 Mbps.
- **MAC Address**: The Ethernet MAC address for the link.
- **MTU**: The Maximum Transmission Unit (MTU) in bytes defined for the link. This is set either manually from the Network Properties page or via the DHCP server.
- **Rx Pkts**: The total number of IP packets received since the last boot.
- **Tx Pkts**: The total number of IP packets transmitted since the last boot.
- **Dropped Pkts**: The total number of IP packets dropped since the last boot.

Virtual Interfaces

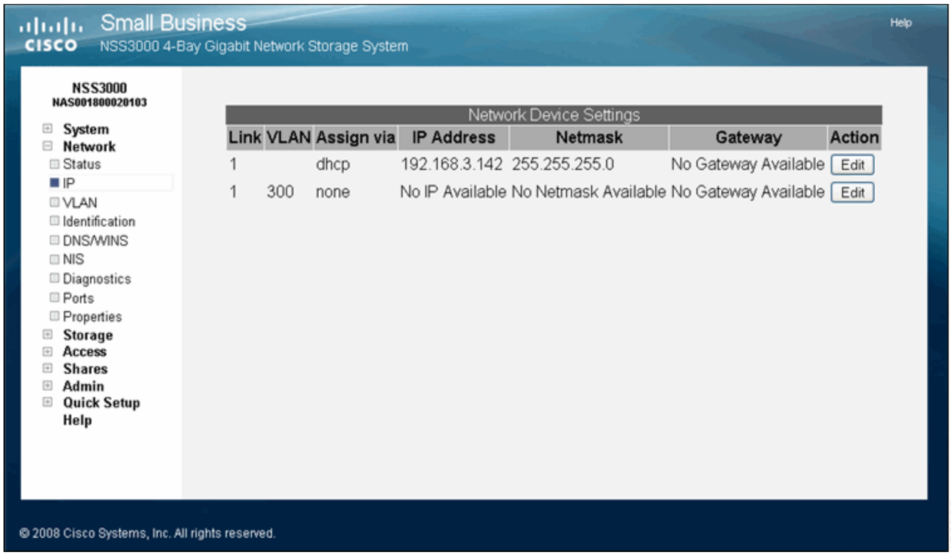
The **VLAN Status** area of the **Network Status** page displays the current status and details regarding each configured VLAN.

- **Link**: The number that appears in this column identifies the physical link on which the VLAN is configured.
- **VLAN**: The VLAN number.
- **Priority**: The 802.1p priority set for the VLAN. Options include 0 through 7 (0 being best effort data and 7 being network critical data).
- **Label**: The text description defined for the VLAN.
- **Rx Pkts**: The total number of IP packets received on the VLAN interface since the last boot.

Viewing the Network IP Settings.

The **Network Device IP** page displays information about the physical and virtual interfaces currently configured on the NSS.

NOTE If you hotplug the Ethernet link after the initial installation of the NSS, make sure that you wait 15 seconds between the time you unplug the cable and then plug it back in. The NSS displays the correct new settings within 10 seconds.



Network Device Settings

Link	VLAN	Assign via	IP Address	Netmask	Gateway	Action
1		dhcp	192.168.3.142	255.255.255.0	No Gateway Available	Edit
1	300	none	No IP Available	No Netmask Available	No Gateway Available	Edit

To display the **Network Device IP** page, from the **Manager Menu**, click **Network** ➔ **IP**. The **Network Device Settings** table displays the following:

- **Link**: The number of the physical link attached to the NSS. It appears as 1.
- **VLAN**: The ID assigned to the virtual interface. For physical interfaces, this column is blank.
- **Assign via**: The method used to assign an IP configuration to the physical or virtual interface. Options include:
  - **DHCP**: The IP configuration was assigned by a DHCP server. Or, if the interface was configured to use DHCP for IP configuration but no DHCP server was found, the IP address was assigned by the AutoIP protocol.

  - **Static**: A static IP configuration was manually entered through the NSS configuration interface.
- **IP Address**: The IP address for the physical or virtual interface.
- **Netmask**: The netmask for the physical or virtual interface.
- **Gateway**: The address of the gateway for the physical or virtual interface.

Configuring the Network Link IP

You must configure the method for assigning an IP configuration to each interface connected to the NSS.

NOTE If you hotplug the Ethernet link after the initial installation of the NSS, make sure that you wait 15 seconds between the time you unplug the cable and then plug it back in. The NSS displays the correct new settings within 10 seconds.

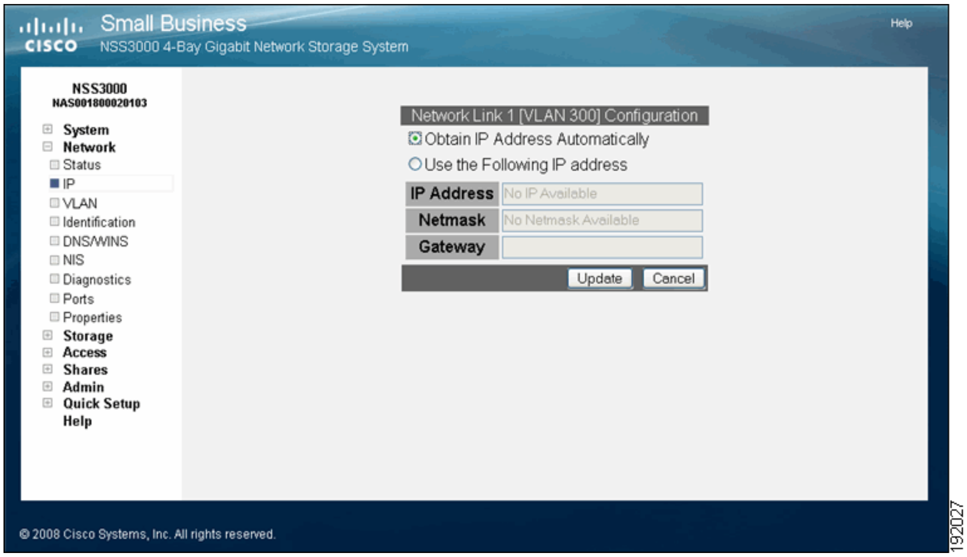
To set the IP address allocation method for an interface:

STEP 1 From the **Manager Menu**, click **Network** ➡ **IP**.

The **Network IP** page appears listing each interface.

STEP 2 Click **Edit** on the row of the interface you want to configure.

The **Network Link Configuration** page appears.



Network Link 1 [VLAN 300] Configuration

● Obtain IP Address Automatically
○ Use the Following IP address

IP Address	No IP Available
Netmask	No Netmask Available
Gateway	

STEP 3 Select one of the following:

- **Obtain IP Address Automatically**: Use a DHCP server to retrieve the IP address, netmask, and gateway address for the interface.
- **Use the Following IP Address**: Enter the IP configuration details manually for the IP address, netmask, and gateway, in dotted-quad notation (i.e., set of four digits separated by periods where each digit is in the range of 0-255.

STEP 4 Click **Update**.

Resetting the DHCP Lease on a Link

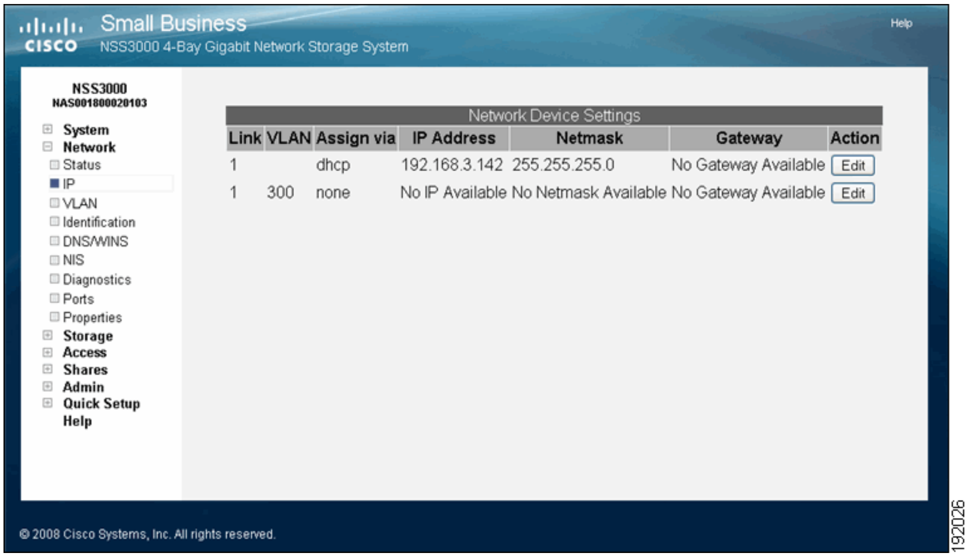
You can force a renewal of the DHCP lease on the physical link or VLAN that is configured for DHCP:

STEP 1 From the **Manager Menu**, click **Network** ➔ **IP**.

The **Network IP** page appears listing each physical and virtual interface.

STEP 2 Click **Edit** on the row of the link IP you want to reset.

The **Network Link Configuration** page appears.



Network Device Settings

Link	VLAN	Assign via	IP Address	Netmask	Gateway	Action
1		dhcp	192.168.3.142	255.255.255.0	No Gateway Available	Edit
1	300	none	No IP Available	No Netmask Available	No Gateway Available	Edit

STEP 4 Click **Update**.

Viewing VLANs Configured on the NSS

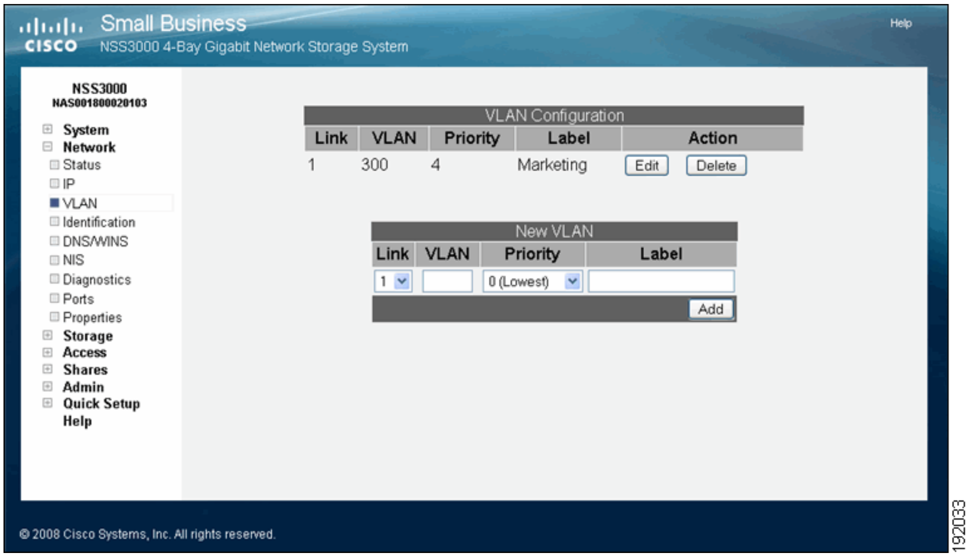
When you first display the **Network VLAN** page, the currently configured VLANs appear. Configuring a VLAN to connect to the NSS depends if it is trunk-based or port-based.

- To configure a trunk-based VLAN, follow the steps to allow a VLAN to access the NSS. See "Allowing a VLAN Access to the NSS" on page 21.
- To configure a port-based VLAN, configure the switch to assign the port to which the NSS is connected to the desired VLAN. In this case, no NSS configuration changes are required.

To view the VLANs currently configured on the NSS:

STEP 1 From the **Manager Menu**, click **Network** ➡ **VLAN.**

The **VLAN Configuration** page appears.



VLAN Configuration

Link	VLAN	Priority	Label	Action
1	300	4	Marketing	Edit Delete

New VLAN

Link	VLAN	Priority	Label
1		0 (Lowest)	

Add

STEP 2 View the following details for each existing VLAN that appears in the **VLAN Configuration** table:

- **Link**: The physical link attached to the NSS. The number appears as 1.
- **VLAN**: The ID of the VLAN. This is configured when the VLAN is added to the NSS and should match the ID of the VLAN as it is configured in your network. The range of valid VLAN IDs is from 1 to 4095.
- **Priority**: The quality of service (QoS) as defined in the IEEE 802.1p standard for the VLAN traffic. VLAN Ethernet frames contain a three-bit priority tag ranging from 0 to 7 (where 0 is best effort and 7 is network-critical traffic).
- **Label**: A text description for the VLAN (for example, "Data," "Voice," "Video," and so on). This description is used solely as a reference within the NSS interface and does not affect its operation.

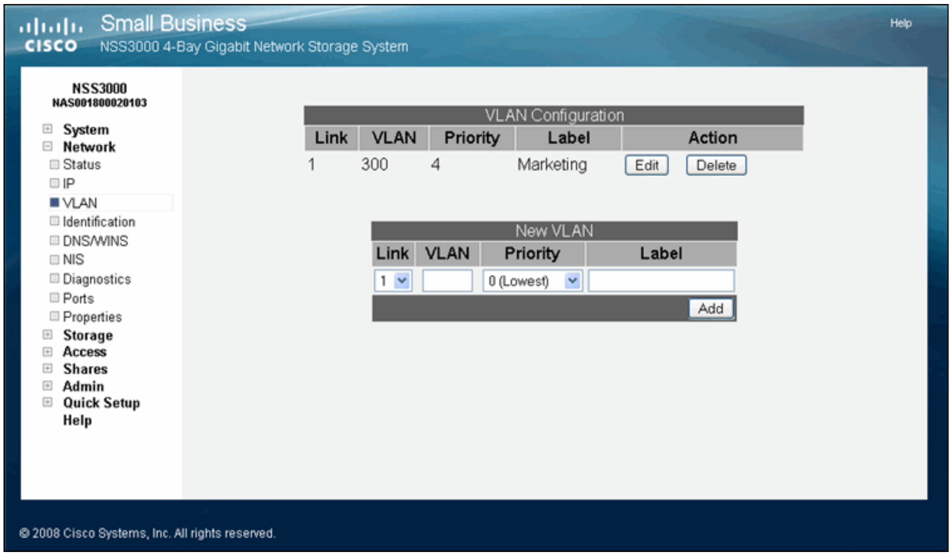
Allowing a VLAN Access to the NSS

Configuring a VLAN to connect to the NSS depends if it is trunk-based or port-based. To configure a trunk-based VLAN, follow the steps in this section. To configure a port-based VLAN, configure the switch to assign the port to which the NSS is connected to the desired VLAN. In this case, no NSS configuration changes are required.

To set up a network VLAN to access the NSS:

STEP 1 From the **Manager Menu**, click **Network** ➡ **VLAN**.

The **VLAN Configuration** page appears.



VLAN Configuration

Link	VLAN	Priority	Label	Action
1	300	4	Marketing	Edit Delete

New VLAN

Link	VLAN	Priority	Label
1		0 (Lowest)	

Add

STEP 2 Under **New VLAN**, configure the following fields:

- **Link**: This shows as "1" for the Ethernet link.
- **VLAN**: Enter the ID of the VLAN as it is defined within your network. The range of valid VLAN IDs is from 1 to 4095.
- **Priority**: Select the QoS priority for the VLAN traffic as it is defined for your network. Valid options range from 0 to 7 (as defined by the IEEE 802.1p standard). VLAN Ethernet frames contain a three-bit priority tag ranging from 0 to 7 (where 0 is best effort and 7 is network-critical traffic).

- **Label**: Enter a text description for the VLAN (for example, "Data", "Voice", "Video", etc.). It can be made up of alphanumeric characters. Note that this description is used solely as a reference within the NSS interface and does not affect its operation.

STEP 3 Click **Add**.

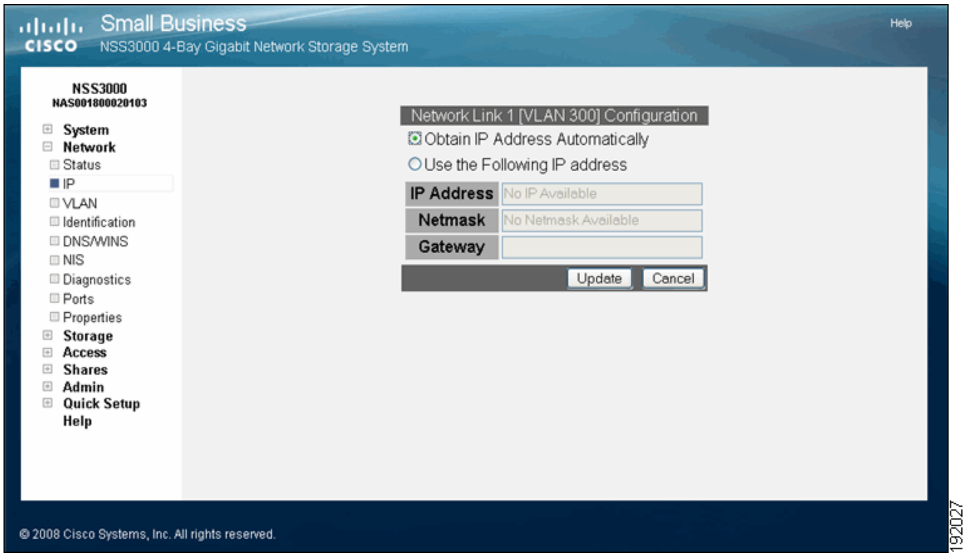
The newly added VLAN appears in the **VLAN Configuration** table. A message appears to advise that the VLAN does not take effect until you configure the IP address.

STEP 4 Click **OK**.

The **Network IP** page appears. The newly added VLAN appears in the list.

STEP 5 Click Edit for the VLAN you need to configure.

The **Network Configuration** page appears.



Network Link 1 [VLAN 300] Configuration

● Obtain IP Address Automatically

○ Use the Following IP address

IP Address	No IP Available
Netmask	No Netmask Available
Gateway	

STEP 6 Click one of the following, depending on how you want to assign the VLAN IP addressing:

- **Obtain IP Address Automatically**: Use a DHCP server to retrieve the IP address, netmask address, and gateway address for the VLAN.
- **Use the Following IP address**: Enter the IP configuration details manually.

STEP 7 Click **Update**.

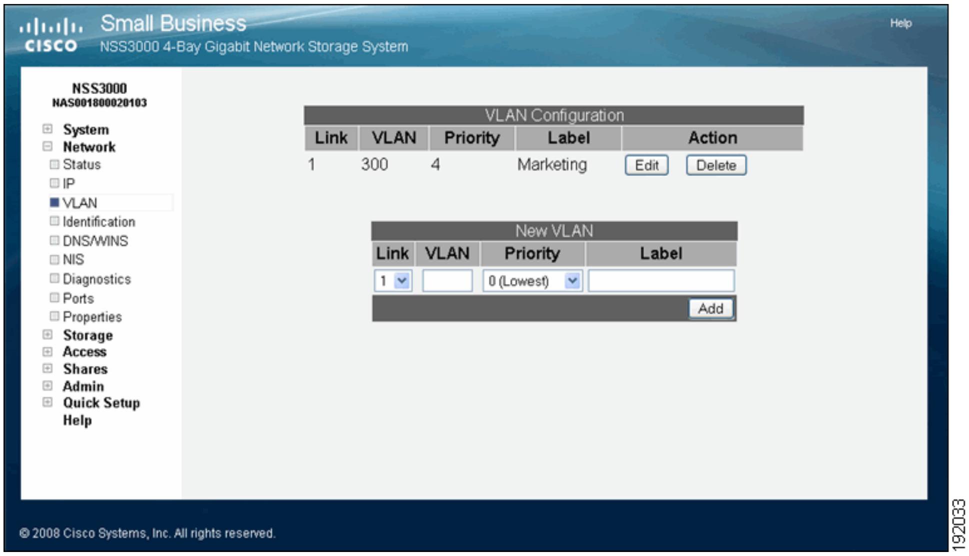
Changing a VLAN Configuration

After you set up a VLAN to access the NSS, you can change its configuration details.

To edit a VLAN configuration:

STEP 1 From the **Manager Menu**, click **Network** ➡ **VLAN**.

The **VLAN Configuration** page appears.



VLAN Configuration

Link	VLAN	Priority	Label	Action
1	300	4	Marketing	Edit Delete

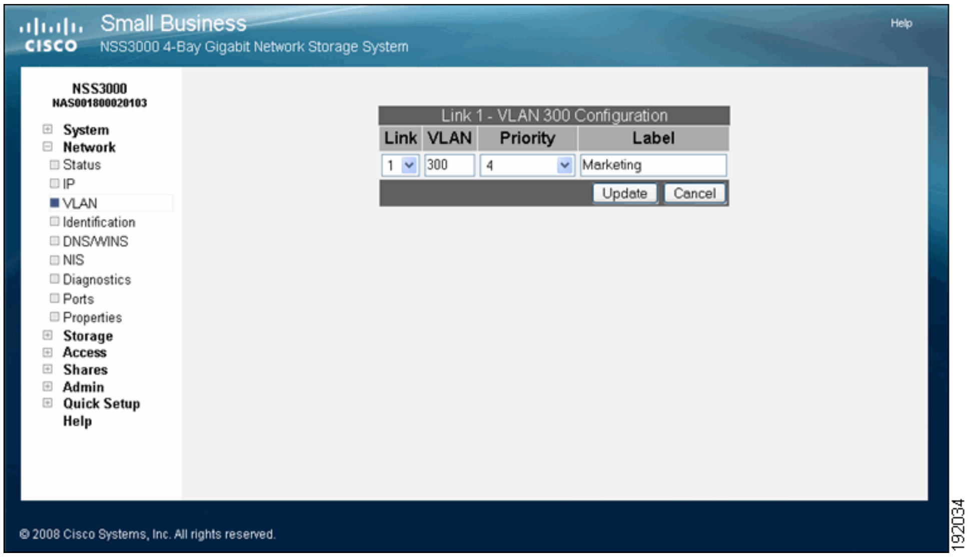
New VLAN

Link	VLAN	Priority	Label
1		0 (Lowest)	

Add

STEP 2 Click **Edit** for the VLAN you want to change.

The **Edit VLAN** page appears.



Link 1 - VLAN 300 Configuration

Link	VLAN	Priority	Label
1	300	4	Marketing

STEP 3 Make changes to any of the VLAN configuration fields as required.

STEP 4 Click **Update**.

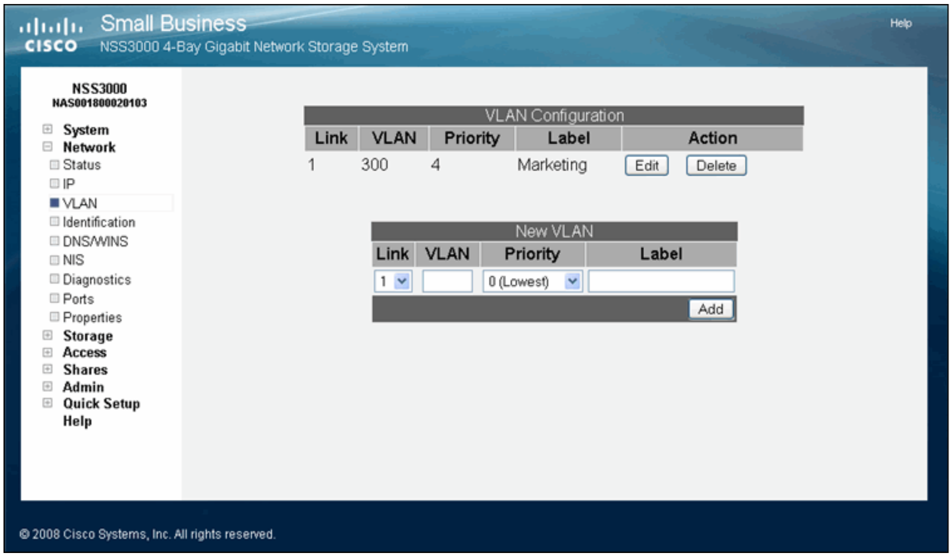
Removing a VLAN's Access to the NSS

All connected VLANs appear when you first display the VLAN Configuration page. You can delete the connection between a VLAN and the NSS. Note that deleting the VLAN only affects the VLAN's ability to access the NSS. It does not impact the VLANs operation within your network.

To disconnect a VLAN's access to the NSS:

STEP 1 From the **Manager Menu**, click **Network** ➔ **VLAN**.

The **VLAN Configuration** page appears.



VLAN Configuration

Link	VLAN	Priority	Label	Action
1	300	4	Marketing	Edit Delete

New VLAN

Link	VLAN	Priority	Label
1		0 (Lowest)	

192033

STEP 2 From the **VLAN Configuration** table, click **Delete** for the VLAN you want to remove.

The VLAN disappears from the **VLAN Configuration** table and can no longer access the NSS.

Configuring the NSS Network Identification

The **Network Identification** page is where you configure the network identity of the NSS, including the hostname and domain membership.

Before you join the NSS to an NTv4 or Active Directory Service (ADS) domain, do the following:

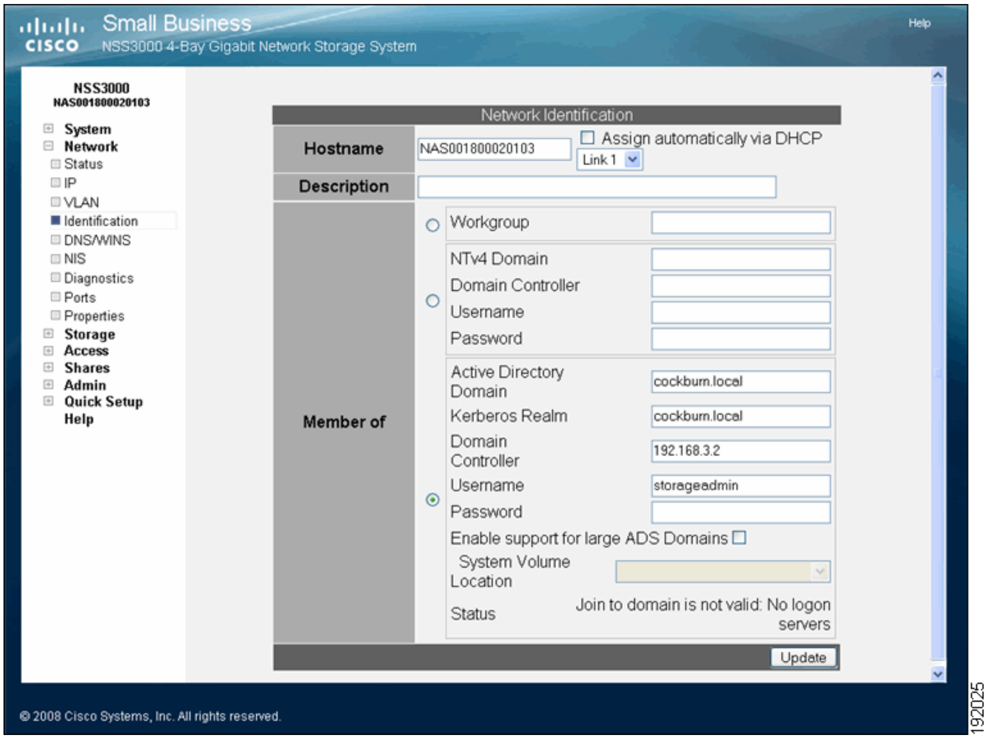
- Configure the IP and DNS information.
- Configure the NTP Server to synchronizing with ADS server.
- Set up your user and group ID ranges on the **User/Group Settings** page (from the **Manager Menu**, click **Access** and then **Options**). If you make a change to the range after the you join the domain, you must rejoin the NSS to the domain after the change is made.

- Set up the **Home Directory Location** on the **User/Group Settings** page. This is used for both domain users and local users.

To configure the NSS network identity:

STEP 1 From the **Manager Menu**, click **Network ➡ Identification**.

The **Network Identification** page appears.



Network Identification

Hostname: NAS001800020103 □ Assign automatically via DHCP Link 1

Description:

Member of:

○ Workgroup:

○ NTv4 Domain:
Domain Controller:
Username:
Password:

● Active Directory Domain: cockburn.local
Kerberos Realm: cockburn.local
Domain Controller: 192.168.3.2
Username: storageadmin
Password:
Enable support for large ADS Domains □
System Volume Location:
Status: Join to domain is not valid: No logon servers

STEP 2 In the **Hostname** field, enter the name you want to use for the NSS. Note any special naming restrictions or conventions enforced by the domain(s) into which the NSS is being joined.

CAUTION If you change the hostname, any current CIFS connections to shares on the NSS are disconnected.

STEP 3 To assign the hostname for the NSS using the DHCP server, select **Assign automatically via DHCP.** If the DHCP server is not available or if it is not configured to supply a hostname, the NSS hostname is assigned using the information entered in the Hostname field.

STEP 4 In the **Description** field, enter the textual description for the NSS as you want it to appear in the file manager window for your users.

STEP 5 Select the type of network into which you are making the NSS a member from the these options:

- **Workgroup**: Make the NSS part of a peer-to-peer network.
- **NTv4 Domain**: Make the NSS a part of a pre-Windows 2000 domain. If you select this option, set up the following fields:
  - **NTv4 Domain**: Enter the domain name.
  - **Domain Controller**: Enter the hostname or IP address of the domain controller.
  - **Username**: Enter the username of an account that has administrator privileges for this domain. Note: The username cannot contain the "%" character.
  - **Password**: Enter the password for the administrator account. This password is cleared each time you click Update. You must re-enter the password each time you edit the fields on this page to ensure the rejoin of the domain is successful.
- **Member of Active Directory domain**: Make the NSS part of an Active Directory (ADS) domain. If you select this option, set up the following fields:
  - **Active Directory Domain**: Enter the domain name. Note that you might have to use the DNS fully qualified domain name. For example, "domain.com" versus just "domain."
  - **Kerberos Realm**: Enter the name of your Kerberos realm. If you are not sure what to enter here, enter the domain name. In most standard Windows domain installations, this is the correct value. Note that you might have to use the fully qualified domain name for the **Kerberos Realm** fields. For example, "domain.com" versus just "domain".
  - **Domain Controlle**r: Enter the hostname or IP address of the domain controller.
  - **Username**: Enter the username of an account that has administrator privileges for this domain. Note: The username cannot contain the "%" character.

- **Password**: Enter the password for the administrator account. This password is cleared each time you click Update. You must re-enter the domain password each time you edit fields on this page to ensure the rejoin of the domain is successful.
- **Enable Support for Large ADS Domains**: Check this option to connect the NSS to an ADS domain that has more than 1000 users and groups. ((This is the sum of the individual users and individual groups.).

  It can take up to 5 minutes to complete the domain join for large ADS domains. When the NSS initially joins the domain, there might be a delay of several minutes until the domain users and groups appear in the user interface. This delay only occurs after the join. Any changes that you make to the users and groups on the domain controller (additions or deletions) can take up to one hour to appear in the user interface.

  NOTE The NSS3000 supports ADS domains of up to 8,000 users and groups. If you connect the NSS to an ADS domain larger than this, you might have problems making CIFS connections to the NSS.

- **System Volume Location**: If you checked the **Enable Support for Large ADS Domains** field, you must then select the RAID array on which to store the system cache files associated with the ADS domain join. The RAID array that you choose must have at least 512 MB of available space. Note that If you delete the RAID array on which the system volume is located, leave the domain by switching to workgroup mode, and then delete the RAID array.

STEP 6 Click **Update**.

If you configured the NSS to join a domain, when you click Update, the domain join occurs. The NSS configuration interface displays the status of the domain join (successful or not successful).

NOTE If you are joined to a domain and make changes to the fields on this page, make sure that you re-enter the domain password as the NSS automatically rejoins the domain when you click **Update**.

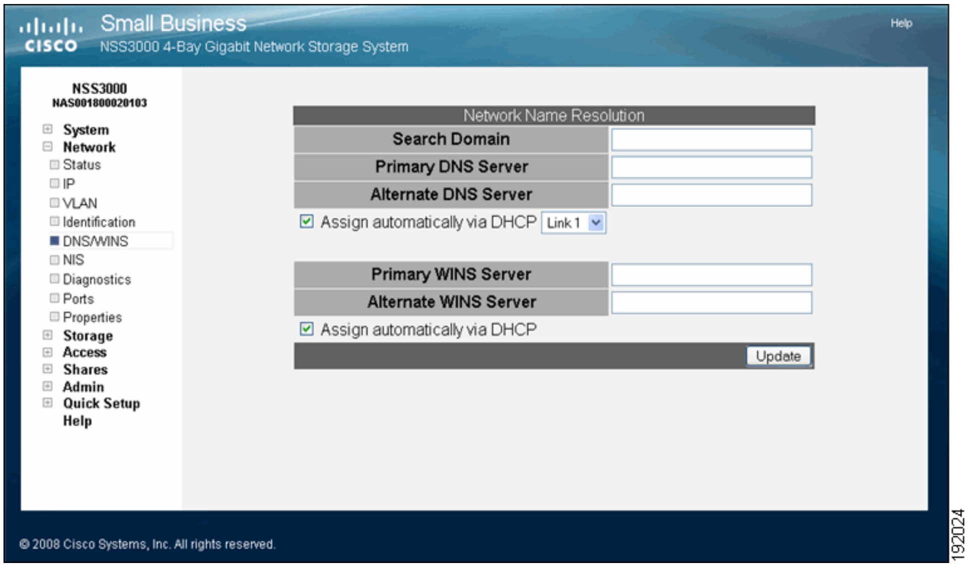
Configuring DNS or WINS for Name Resolution

Within a network, DNS and WINS are used to translate hostnames into IP addresses. For example, the hostname "myserver" might translate to 172.1.135.6. Configuring how the NSS works with name resolution depends on what type of servers exist within your network.

To configure the DNS or WINS server addresses for your network:

STEP 1 From the **Manager Men**u, click **Network** ➜ **DNS/WINS**.

The **Network Name Resolution** page appears.



Network Name Resolution

Search Domain	
Primary DNS Server	
Alternate DNS Server	

☑ Assign automatically via DHCP Link 1

Primary WINS Server	
Alternate WINS Server	

☑ Assign automatically via DHCP

STEP 2 Based on your network setup, configure the following fields:

- **Search Domain**: Enter the address of the DNS search domain accessible by the NSS. For example, "mycompany.com".
- **Primary DNS Server**: Enter the IP address of the primary DNS server on your network.
- A**lternate DNS Server**: Enter the IP address of a second DNS server to be used should the primary DNS server become unavailable. This field is optional.
- **Assign automatically via DHCP**: Select this to assign the IP address for the DNS server using the DHCP server. If the DHCP server cannot be found or

times out, the DNS server IP address is assigned the IP address manually entered in the **Primary** or **Alternate DNS Server** fields.

- **Primary WINS server**: If your network has a WINS server, enter its address or hostname. This field is optional.
- **Alternate WINS server**: If your network has a secondary WINS server, enter its address or hostname. This field is optional.
- **Assign automatically via DHCP**: Select this to assign the IP address or hostname for the WINS server using the DHCP server

  If the DHCP server cannot be found or times out, the DNS server IP address is assigned the IP address manually entered in the **Primary** or **Alternate WINS Server** fields.

STEP 3 Click **Update**.

Joining the NSS to a Network Information System (NIS) Domain

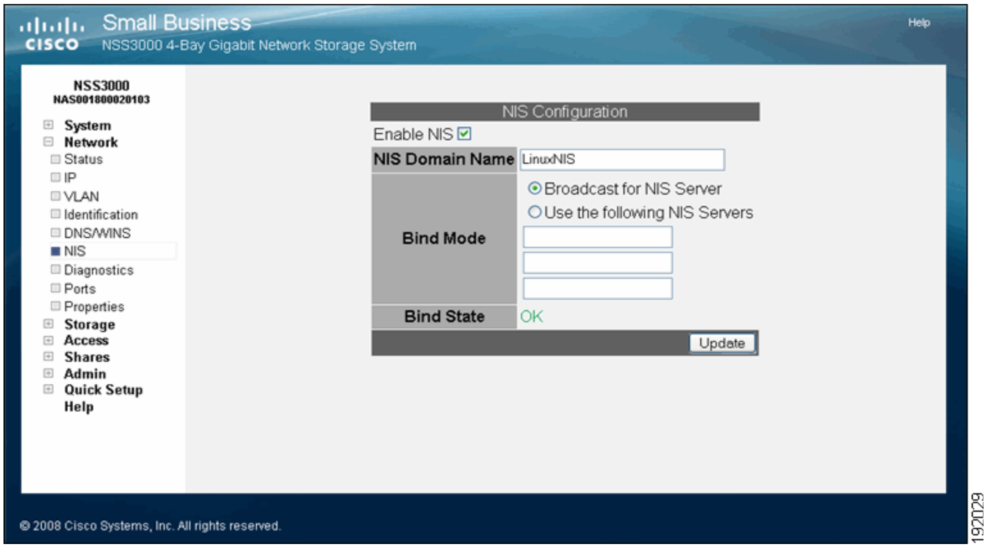
To join the NSS to a NIS domain, you need to configure and enable it.

NOTE Before you join a NIS domain, make sure that you set up or make changes to the NIS domain users and groups ID range on the User/Groups Settings page. This minimizes the risk of collisions of user or group IDs within your network.

To configure the NSS for NIS:

STEP 1 From the **Manager Menu**, click **Network** ➔ **NIS**.

The **NIS Configuration** page appears.



NIS Configuration

Enable NIS ☑

NIS Domain Name	LinuxNIS
Bind Mode	● Broadcast for NIS Server ○ Use the following NIS Servers
Bind State	OK

© 2008 Cisco Systems, Inc. All rights reserved.

STEP 2 Select **Enable NIS**.

STEP 3 Enter the NIS domain name in the **NIS Domain Name** field.

STEP 4 Set the bind state by clicking one of the following:

- **Broadcast for NIS Server**: Click this option to have the NSS search until it finds the NIS server on the network.
- **Use the following NIS Servers**: To manually identify the NIS server you want the NSS to use, click this option, and then enter the address of up to three different NIS servers.

The **Bind State** field shows the current bind status of the NSS. Options include: "Invalid" (the NSS is not joined to an NIS domain), or "Enabled" (the NSS is successfully joined to a NIS domain).

STEP 5 Click **Update**.

Editing Access Control Lists (ACLs) from Windows Explorer: Restrictions

Access Control Lists (ACLs) are used to set user and group access privileges for specific files and folders stored on the NSS. There are certain restrictions to be aware of as you work with ACLs through Windows Explorer:

- **Group versus User ACLs**: You can only set up an ACL for individual users. You cannot set up a group ACL.
- **NIS domain**: You cannot create or edit ACLs for NIS domain users; they do not appear in the Security tab in Windows Explorer.

Running Diagnostics of your Physical Link from the Configuration Interface

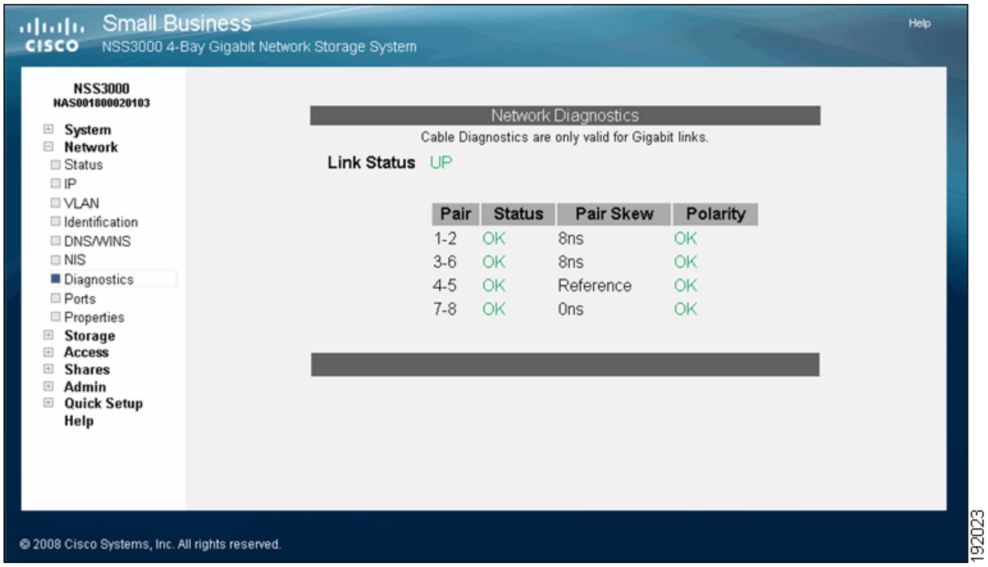
The NSS lets you test the physical network cable attached to the Ethernet link for certain fault conditions. You can either run the test through the Configuration Interface or from the LCD panel on the front of the chassis. The test automatically runs each time you display the Network Diagnostics page or when you display the Ethernet Cable screen from the LCD. Running this test does not affect the use of the link in any way.

NOTE The diagnostics test is only supported when the NSS is connected to a Gigabit Ethernet switch.

To test the physical link from the Configuration Interface:

STEP 1 From the **Manager Menu**, click **Network** ➔ **Diagnostics**.

The **Network Diagnostics** page appears.



Network Diagnostics

Cable Diagnostics are only valid for Gigabit links.

Link Status UP

Pair	Status	Pair Skew	Polarity
1-2	OK	8ns	OK
3-6	OK	8ns	OK
4-5	OK	Reference	OK
7-8	OK	0ns	OK

STEP 2 View the **Link Status** area for the test result or view the **Ethernet Cable** screen from the LCD panel. If the link is down, you cannot access the **Configuration Manager.**

Running Cable Diagnostics from the LCD

To test the physical link from the LCD:

STEP 1 Press and hold down the **Display** button on the front of the chassis until the **Ethernet Cable** screen appears.

STEP 2 If the link is up, the panel displays the status of the cable. If the link is down, after a few seconds the test starts.

After the test completes, the status of the cable appears. If the link is up, the status appears as OK. If there is a problem with the link, the status is reported according to the pairs within the cable.

These are the possible test results (because of screen space limitations, each page shows two sets of cable pairs):

- **Short**: If the pair has a short, the message appears as "pair a-b short@ Xm" (where "a" and "b" are the numbers of the pair, "X" is the location in the cable where the short was found, and "m" stands for metres).

- **Open**: If the cable has an open, the message appears as "pair a-b open@ Xm (where "a" and "b" are the numbers of the pair, "X" is the location in the cable where the open was found, and "m" stands for meters).
- **Disconnected**: If the cable shows an open at the minimum measurable distance, it is assumed that the cable is not connected. The message "Cable is not connected" appears.

The cable diagnostic test only runs the first time you display the **Cable Diagnostics** screen. To rerun the test, scroll through the LCD pages until you redisplay the **Cable Diagnostics** screen.

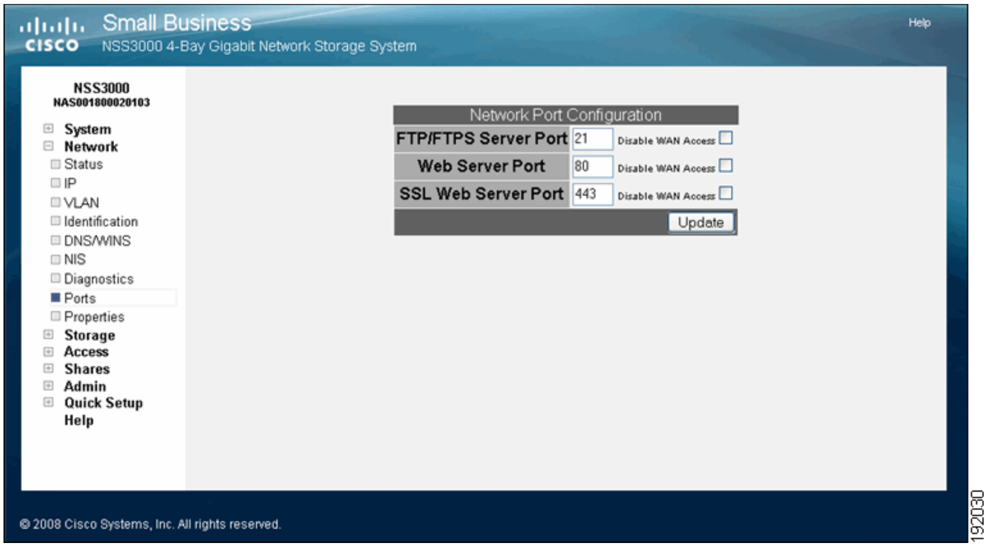
Configuring the Network Ports

By default the NSS runs network services on their well known (IETF defined) port numbers. You can change the port on which any particular service runs. When you disable WAN access for a given service, only hosts on the same subnet as the NSS may connect to that service. This is a shortcut to manually defining an equivalent network filter.

To set up the network services:

STEP 1 From the **Manager Menu**, click **Network** ➡ **Ports**.

The **Network Ports Configuration** page appears.



Network Port Configuration		
FTP/FTPS Server Port	21	Disable WAN Access □
Web Server Port	80	Disable WAN Access □
SSL Web Server Port	443	Disable WAN Access □

STEP 2 Change the port assignment for any of the following service types:

- **FTP/FTPS Port**: The well-known port setting is 21. Select **Disable WAN Access** to disallow FTP and FTPS protocol access to the NSS from a WAN.
- **Web Server Port**: The well-known port setting is 80.

  To access the NSS configuration interface, you must have either the HTTP port or HTTPS port enabled. Select **Disable WAN Access** to disallow HTTP protocol access to the NSS from a WAN.
- S**SL Web Server Port**: The well-known port setting is 443. Select **Disable WAN Access** to disallow HTTPS protocol access to the NSS from a WAN.

STEP 3 Click **Update**.

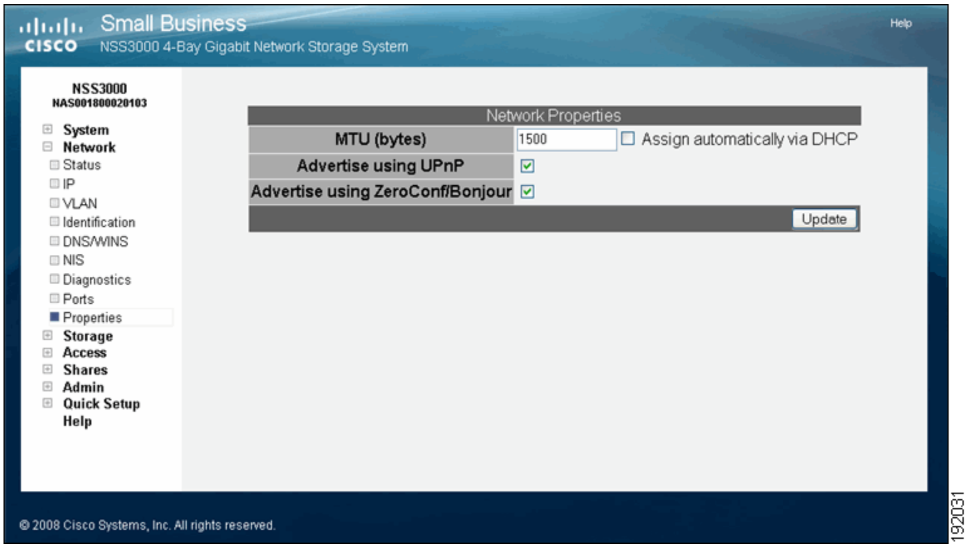
Setting up the Ethernet Frame Size & Advertising Modes

The **Network Properties** page lets you set the Ethernet frame size and determine how you want to advertise the presence of the NSS within your network.

To configure the network properties:

STEP 1 From the **Manager Menu**, click **Network** ➡ **Properties**.

The **Network Properties** page appears.



Network Properties

MTU (bytes)	1500	□ Assign automatically via DHCP
Advertise using UPnP	☑	
Advertise using ZeroConf/Bonjour	☑	

Update

STEP 2 Set the Maximum Transmission Unit (MTU), in bytes, in the **MTU** field. This is the largest Ethernet frame that your network can handle. The default MTU size is 1500 bytes. MTU sizes greater than 1500 bytes are considered "jumbo frames".

STEP 3 To assign the link MTU size automatically using the DHCP server, click **Assign automatically via DHCP**. In this case, the value entered in the MTU field is used as a backup if the DHCP server does not provide an MTU value or if the server cannot be reached.

STEP 4 Based on your network requirements, enable any of the following:

- **Advertise using UPnP**: The NSS is advertised within the network using UPnP.
- **Advertise using Zeroconf/Bonjou**r: The NSS is advertised within the network using Zeroconf/Bonjour.

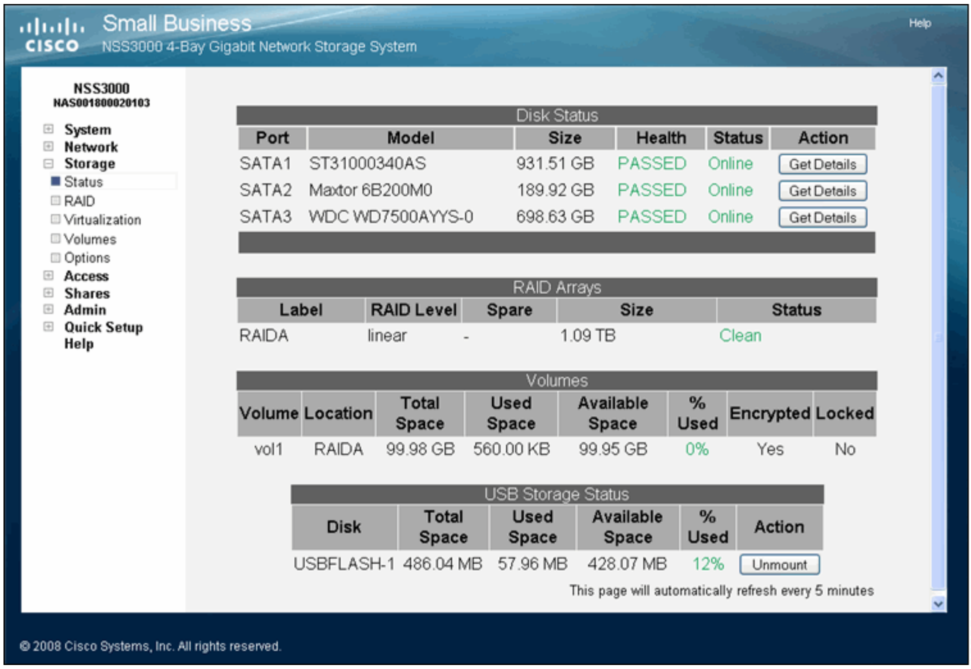
STEP 5 Click **Update**.

4

Configuring your Storage

The **Storage Status** page shows the current state of the disk drives, arrays, and volumes currently installed or exported to the NSS. You can also view the S.M.A.R.T. health report for each physical disk. To display the **Storage Status** page, from the **Manager Menu**, click **Storage** ➡ **Status**. Status pages like the **Storage Status** page automatically refresh on a regular interval and are helpful for monitoring the progress of certain processes such as checking the condition of a drive.

The LCD on the front of the chassis also lets you view the state of the RAID arrays and volumes.



Disk Status

Port	Model	Size	Health	Status	Action
SATA1	ST31000340AS	931.51 GB	PASSED	Online	Get Details
SATA2	Maxtor 6B200M0	189.92 GB	PASSED	Online	Get Details
SATA3	WDC WD7500AYYS-0	698.63 GB	PASSED	Online	Get Details

RAID Arrays

Label	RAID Level	Spare	Size	Status
RAIDA	linear	-	1.09 TB	Clean

Volumes

Volume	Location	Total Space	Used Space	Available Space	% Used	Encrypted	Locked
vol1	RAIDA	99.98 GB	560.00 KB	99.95 GB	0%	Yes	No

USB Storage Status

Disk	Total Space	Used Space	Available Space	% Used	Action
USBFLASH-1	486.04 MB	57.96 MB	428.07 MB	12%	Unmount

This page will automatically refresh every 5 minutes

Storage Status Tables

The **Storage Status** page include the following tables:

Disk Status Table

The **Disk Status** table lists each of the physical disks installed in the NSS. The table is made up of the following columns:

- **Port**: The port number on the NSS in which the disk is installed.
- **Model**: The model of the disk drive. This information is read from the disk drive.
- **Size**: The size of the disk drive.
- **Health**: The system monitors each disk drive and reports the condition of the disk drive. Options include:
  - **Passed**: The disk drive has passed the S.M.A.R.T. test and is considered fully operational. The Error LED on the disk drive is off.
  - **Failing**: The disk drive has failed the S.M.A.R.T. test and is predicated to fail. The red Error LED on the disk drive is blinking.
  - **Failed**: The disk drive is not operational (has failed). The red Error LED on the disk drive is on solid.
- **Status**: The state of use for the disk drive. Options include:
  - **Online**: The disk drive is spun up.
  - **Standby**: The disk drive is idle and is spun down.
  - **Offline**: The disk drive is failed.
- **Action**: There are available action buttons associated with each installed disk drive:
  - **Get Details**: View the current, detailed S.M.A.R.T. report for the disk drive.

RAID Arrays Table

The **RAID Arrays** table lists each array (either RAID or JBOD) currently configured. It includes the following:

- **Label**: The name assigned to the array.
- **RAID Level**: The configured RAID level.
- **Spare**: Indicates if the RAID has a spare or not.
- **Size**: The size allocated for the array. The amount of available storage for an array depends on the number of drives in the array, the size of the smallest drive, as well as the RAID level assigned.
- **Status**: The current condition of the RAID array. Options include:
    - **Clean**: The array is in a normal state. The status is color-coded green.
    - **Degraded**: For RAID arrays with redundancy (i.e., RAID levels 1, 5, 10), one or more of the redundant disk drives is removed from the system or is failed. In this state, the array is fully recoverable. The status is color-coded orange.
    - **Failed**: One or more disk drives have been removed or are unrecoverable from a RAID0 or a JBOD array. For RAID levels 1, 5, 10, it indicates a loss of the redundant disks in the array plus at least one more drive. In this state, the array is unrecoverable.
    - **Rebuilding**: A RAID level with redundancy is being rebuilt. Note that during a rebuild, the RAID array is still fully usable. The status is color-coded orange. During the rebuild, the disk drive LED slowly blinks green.
    - **Stopped**: A RAID array was stopped by the system (through degraded mode management) due to it being in degraded mode for the amount of time configured in the **Storage Options** page. Volumes associated with a stopped array are unmounted and unusable. To start the RAID array, click the **Start** button.

Volumes Table

The **Volumes** table provides a list of the existing volumes. It includes the following:

- **Location**: The name of the RAID array on which the volume is configured.
- **Volume**: The name assigned to the volume.
- **Total Space**: The amount of space configured for the volume.
- **Used Space**: The amount of space used on the volume.
- **Avail. Space**: The amount of unused space on the volume.
- **% Used**: The percentage of available space that is used.
- **Encrypted**: Whether the volume is encrypted or unencrypted.
- **Locked**: The encrypted volume is locked and is not accessible. To make the volume accessible, the volume must be unlocked.

USB Storage Status

If you mount a USB flash device by inserting it into the AUX-1 port on the front of the chassis, the **USB Storage Status** table appears. If there is no USB flash device mounted, the **USB Storage Status** table does not appear. You can use the USB flash device to save a backup of the configuration file. When you finish using the USB flash device, click Unmount before you remove it from the AUX-1 port. (The AUX-1 LED on the front of the chassis must be off before you can safely remove the USB flash device.) If you remove the USB flash device in a mounted state, you risk corrupting the files or filesystem.

The **USB Storage Status** table provides the following details about the mounted USB flash device:

- **Disk**: The type of disk in this case is the USB flash.
- **Total Space**: The total amount of space (both used and available) on the USB flash device.
- **Used Space**: The amount of space taken up on the USB flash device.
- **Available Space**: The amount of unused space on the USB flash device.
- **%Used**: The percentage of space used on the USB flash device.
- **Action**: The Unmount button unmounts the USB flash device so that it can be safely removed from the AUX-1 port.

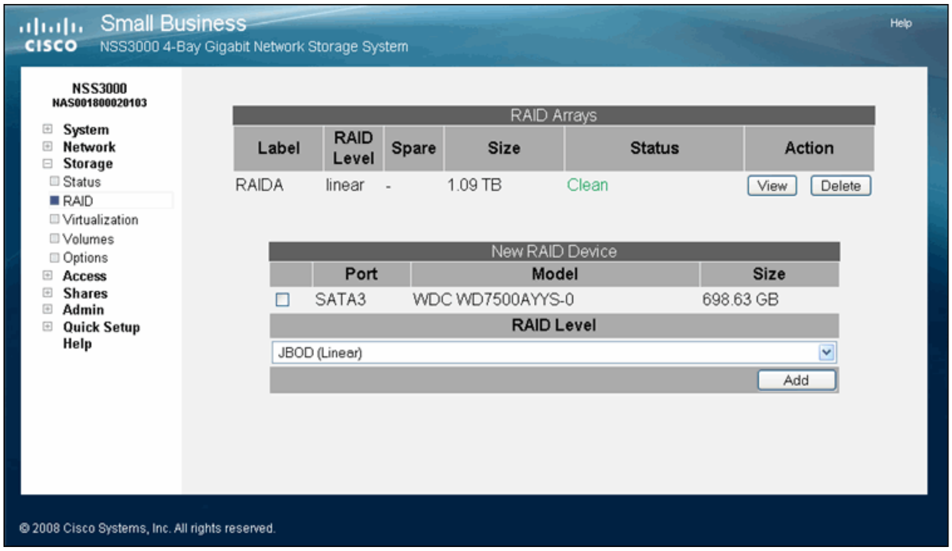
Managing RAID Arrays

RAID is an acronym for Redundant Array of Inexpensive Disks. In storage environments, a RAID array uses multiple physical disk drives to create a single logical unit from which data can be shared or replicated between the drives. A RAID array also simplifies the data management as the data appears in one logical unit. Choosing to store your data using a RAID array gives you the benefit of speed and performance; storage capacity; decreased downtime costs and increased availability; fault tolerance; and higher data security.

The LCD on the front of the chassis lets you view the RAID level (i.e., JBOD, 0,1,5,10), the state of the RAID (i.e., clean, degraded, rebuild, failed or stopped), and the percent completion of the RAID rebuild if in progress.

About the RAID Arrays Page

The RAID Arrays page is where you manage the local RAID and JBOD arrays. To display the **RAID Arrays** page, from the **Manager Menu**, click **Storage** ➡ **RAID**.



RAID Arrays

Label	RAID Level	Spare	Size	Status	Action
RAIDA	linear	-	1.09 TB	Clean	View Delete

New RAID Device

	Port	Model	Size
□	SATA3	WDC WD7500AYYS-0	698.63 GB

RAID Level

JBOD (Linear)

Add

Choosing a RAID Array Level

RAID (Redundant Array of Inexpensive Disks) is a technology that enables multiple low-cost hard drives to be used together in a way that increases performance and/or reliability compared to that of a single drive. The component devices in a RAID array appear as a single logical storage device. There are various types of RAID, referred to as RAID levels. Some RAID levels increase the performance of the array, some increase the reliability, and others do a mixture of both. The NSS supports the following RAID levels: 0, 1, 5 and 10. The NSS also supports JBOD (Just a Bunch of Disks), which is technically not a RAID level.

These variables are used in the formulas used to calculate the total capacity of each RAID level:

- m: capacity of the smallest disk in the array
- n: number of disks in the array

Stripe (RAID0): RAID0 stripes the data written to the array across the component disks. The data is broken into chunks and each chunk is written to a different disk. Reads and writes to each disk occur in parallel, speeding up the total read and write performance of the array.

- Minimum Number of Disks: 2
- Total capacity: m * n
- Advantages: Increased read and write performance.
- Disadvantages: Decreased reliability. A failure of any component disk in the array causes the entire array to fail.

Mirror (RAID1): RAID1 writes the same data to each disk in the array. The disks are referred to as mirrors because each one mirrors the data stored on the others. As long as one disk in the array is intact, all data can be read back from the array. If a disk fails in the array and is then replaced, the array must copy the entire contents of a good disk to the new disk. This process is referred to as resyncing. During a resync, the array continues to be available for reads and writes. When an array contains a failed disk, it is operating in degraded mode. This reflects the decreased performance and reliability of the array when it is missing disks.

- Minimum Number of Disks: 2
- Total capacity: m
- Advantages: Increased reliability. The array can sustain the loss of all but one disk without any data loss. Each mirror disk added to the array

increases the reliability (for example, a two-disk RAID1 is half as likely to fail, a three-disk RAID1 is one-third as likely to fail, and so on). Increased read performance.

- Disadvantages: Decreased aggregate storage capacity (each mirror disk does not contribute to the total capacity of the array). Decreased write performance. I/O intensive when resyncing mirrors.

Mirror + Spare (RAID1): RAID1 plus a hot spare.

- Minimum Number of Disks: 3
- Total capacity: m
- Advantages: The hot spare can be used in case of a failure to either disk in the mirrored pair.

Parity (RAID5): RAID5 stripes data written to the array like RAID0, except that, unlike RAID0, RAID5 generates parity information that also gets striped across the array. This parity information is used during the reconstruction of the lost data when a drive fails in the array.

When a failed disk is then replaced, the array must regenerate and rewrite the parity information of the array. This process is referred to as “rebuilding”. During a rebuild, the array continues to be available for reads and writes. If the parity information in the array gets out of sync with the data in the array, usually as the result of an unexpected loss of power to the system, the array must be rebuilt. Like RAID1, if a disk is missing from the array, the array is said to be operating in “degraded” mode.

- Minimum Number of Disks: 3
- Total capacity: m * (n-1)
- Advantages: Increased reliability. The RAID array can sustain the loss of any single disk without any data loss. Increased read and write performance.
- Disadvantages: Decreased aggregate storage capacity (you lose the equivalent capacity of a single disk). CPU intensive calculation of parity, especially during rebuild operation. I/O intensive during rebuild operation.

Parity + Spare (RAID5): RAID5 with a hot spare.

- Minimum Number of Disks: 4
- Total capacity: m * (n-1)
- Advantages: The hot spare is available in case of a failure of one of the disks in the array.

JBOD: JBOD lets you combine multiple disks of mixed capacities into a single logical storage device. The capacity of the JBOD array is the sum of the total capacities of the individual component disks (that is, it does not have the limitation of RAID0 where you lose some capacity when using mixed sized disks). JBOD offers no performance increase compared to the component disks. It has lower reliability than the component disks, as the failure of a single disk results, in general, in the failure of the whole array. Depending on how you create volumes on the JBOD array, you might be able to recover data when one or more disks in the JBOD fail. This, however, is not guaranteed.

- Minimum Number of Disks: 1
- Total capacity: sum of capacities of component disks.
- Advantages: Maximal storage capacity, especially when using mixed size disks.
- Disadvantages: Decreased reliability.

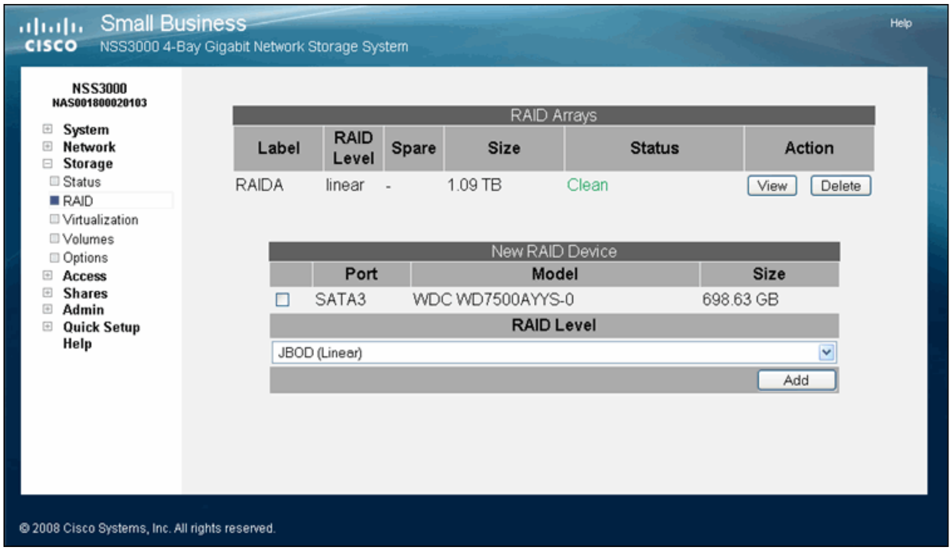
Creating a RAID Array

After you install the physical disks, you can create the RAID arrays. Before you create a RAID array, either for the first time, or when you are rebuilding it as a result of failed disks in the array, set the rebuild priority to determine how you want to allocate the system resources for the rebuild. To set the rebuild priority, see ”Storage Options” on page 29.

NOTE When adding disks to an array, we recommend that you use the same model of disk with the same capacity. With the exception of a JBOD, RAIDs are configured to use the maximum of the smallest disk capacity in the array for each additional disk in the array. For example, if you install two, 250 GB disks and one 500 GB disk in a RAID0 array, the total capacity is only 750 GB.

STEP 1 From the **Manager Menu,** click **Storage** ➔ **RAID**.

The **RAID** page appears.



RAID Arrays

Label	RAID Level	Spare	Size	Status	Action
RAIDA	linear	-	1.09 TB	Clean	View Delete

New RAID Device

	Port	Model	Size
□	SATA3	WDC WD7500AAYS-0	698.63 GB

RAID Level: JBOD (Linear)

Add

192051

STEP 2 The available disks appear in the **New RAID Device** table. Select each disk that you want to include in the array.

STEP 3 From the **RAID Level** drop-down menu, click the RAID level of the RAID array that you want to create.

STEP 4 Click **Add**.

NOTE Creating a RAID can take some time to complete depending on the disk sizes and the selected RAID level. You can monitor the progress of the RAID build from the **Storage Status** page. When the build finishes, the array appears in the **RAID Arrays** table. The disks used in the array are no longer available for creating additional arrays.

Adding a Disk Drive to an Array

You can add additional disks to an existing RAID1, RAID5, and RAID10 array. As long as the array is clean, these disks then become spares.

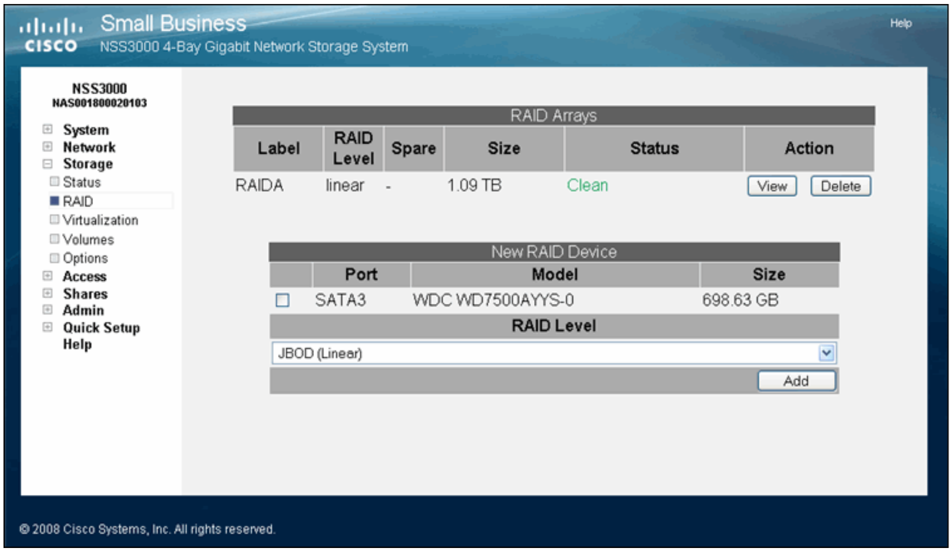
NOTE When adding disks to an array, we recommend that you use the same model of disk with the same capacity. The new disk must have at least the same capacity of the smallest disk currently in the array. With the exception of a JBOD, RAIDs are configured to use the maximum of the smallest disk capacity in the array for each additional disk in the array. For example, if you install two, 250 GB disks and one 500 GB disk, the total capacity is 750 GB.

To add a disk to an array:

STEP 1 If not already installed in the chassis, insert the disk into the NSS.

STEP 2 From the **Manager Menu**, click **Storage** ➜ **RAID**.

The **RAID** page appears.



RAID Arrays

Label	RAID Level	Spare	Size	Status	Action
RAIDA	linear	-	1.09 TB	Clean	View Delete

New RAID Device

	Port	Model	Size
□	SATA3	WDC WD7500AYYS-0	698.63 GB

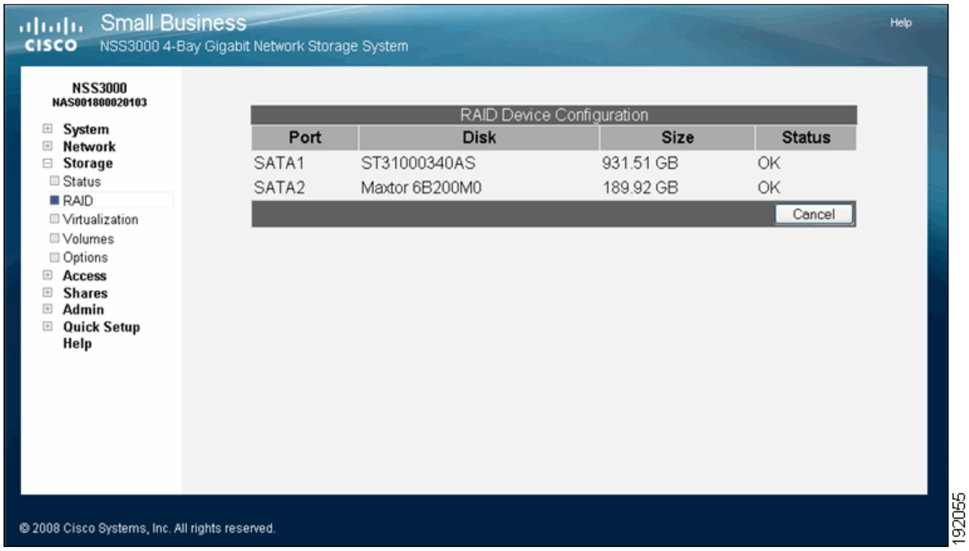
RAID Level

JBOD (Linear)

Add

STEP 3 In the **RAID Arrays** table, click **Edit** for the applicable RAID array.

The **RAID Device Configuration** page appears.



RAID Device Configuration

Port	Disk	Size	Status
SATA1	ST31000340AS	931.51 GB	OK
SATA2	Maxtor 6B200M0	189.92 GB	OK

All available disk drives appear in the listing.

STEP 4 Click **Add** to add the disk drive to the array.

- If the disk drive is added to a functional array, the disk drive becomes a hot spare.
- If the disk drive is added to a degraded array, the RAID array is rebuilt. While the rebuild continues, you can still use the array. After the rebuild process completes, the disk becomes part of the redundant storage. You can monitor the progress of the rebuild through the **System Status** page.

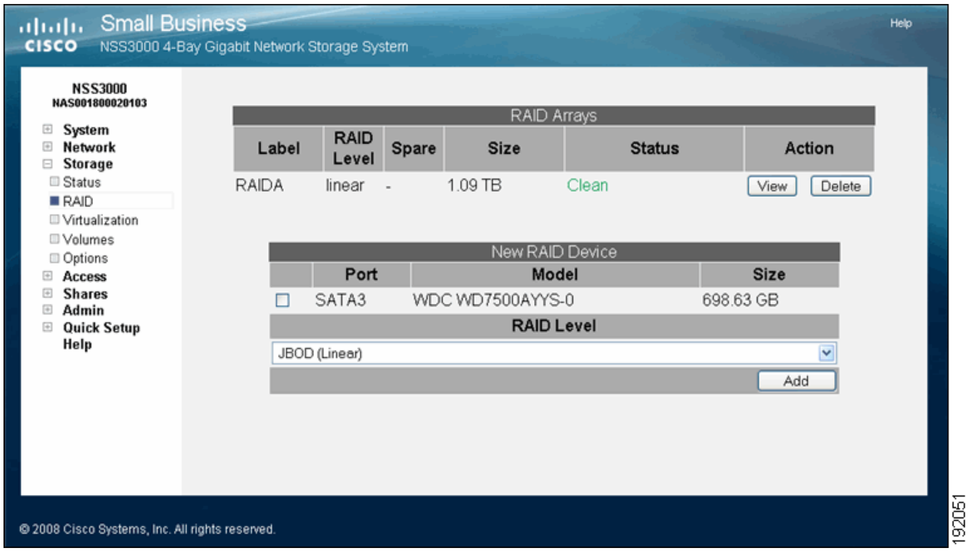
Deleting an Array

You can remove an existing array and release the disks used in the array back into available storage. Deleting an array also deletes any existing data on the array (including the volumes, shares, and quotas). If you delete an array that contains the volume that is used as the location of your users' Home Directories, you must assign a new volume as the **Home Directory** location.

To delete an existing array:

STEP 1 From the **Manager Menu**, click **Storage** ➡ **RAID**.

The **RAID** page appears.



RAID Arrays

Label	RAID Level	Spare	Size	Status	Action
RAIDA	linear	-	1.09 TB	Clean	View Delete

New RAID Device

	Port	Model	Size
□	SATA3	WDC WD7500AYYS-0	698.63 GB

RAID Level: JBOD (Linear)

Add

STEP 2 Click **Delete** in the row of the RAID array that you want to delete.

A warning message appears.

STEP 3 To continue, click **OK**.

The deleted array disappears from the list of existing arrays. The disks used in the array are released back into available storage and appear in the **New RAID Device** table.

Migrating a RAID Array to another Storage Device

After you build a RAID array, you can migrate it to a different NSS3000 as required (you cannot migrate a RAID to or from the NSS4000 or NSS6000). If you are migrating a RAID array from the NSS3000 or to another network NSS3000, make sure that you power down the RAID array (versus hot-plugging it) before migrating it into the new system.

To migrate a RAID array:

STEP 1 Power down the NSS (from which you are removing the RAID array).

STEP 2 Remove each of the disk drives that make up the RAID array to be moved.

STEP 3 Power down the NSS to which you are migrating the RAID array.

STEP 4 Insert each of the disk drives in the RAID array into the new NSS.

NOTE You can install the drives into the new NSS in any order. You do not need to install them in the same order or slots that they were installed in the original NSS.

STEP 5 When all the disk drives are installed, power up the NSS.

STEP 6 If any local users were assigned permissions to shares on the RAID array, you must either save the configuration from the original RAID array device and then upload it to the new NSS, or manually reconfigure the users and their share permissions.

Virtualizing Storage within your Network

NOTE After you configure a virtual RAID, you cannot migrate the disks used for that RAID to another NSS. You also cannot export storage from a device that uses imported storage.

Currently Exported Storage

When you display the **Storage Virtualization** page, the **Currently Exported Storage** table appears. It shows the details for any exported disks or arrays:

- **Device**: The name of the exported disk or array.
- **Size**: The size of the exported storage.
- **Exported As**: The serial number of the exported NSS.

- **Imported by**: The serial number of the NSS that has imported the storage. If the exported disk or array has not yet been imported by the master NSS, "None" appears in this column.
- **Action**: Click the **Unexport** button to stop the NSS from exporting the associated drive or array. This frees up the drive or array for use in local RAID arrays.

Exporting Storage to your Network

If you have multiple NSS units in your network, you can easily export the storage to form a large, logical storage unit that can be managed from the master NSS. The first step in creating virtualized storage is to export the disk(s) or array to the network. Note that when you export storage, you need to consider how things like rebooting an NSS might impact users of the virtualized storage. While the logical storage is controlled from the master NSS, the physical device (including the disk drives) is still controlled through the slave's configuration interface and is affected by the conditions of the physical unit.

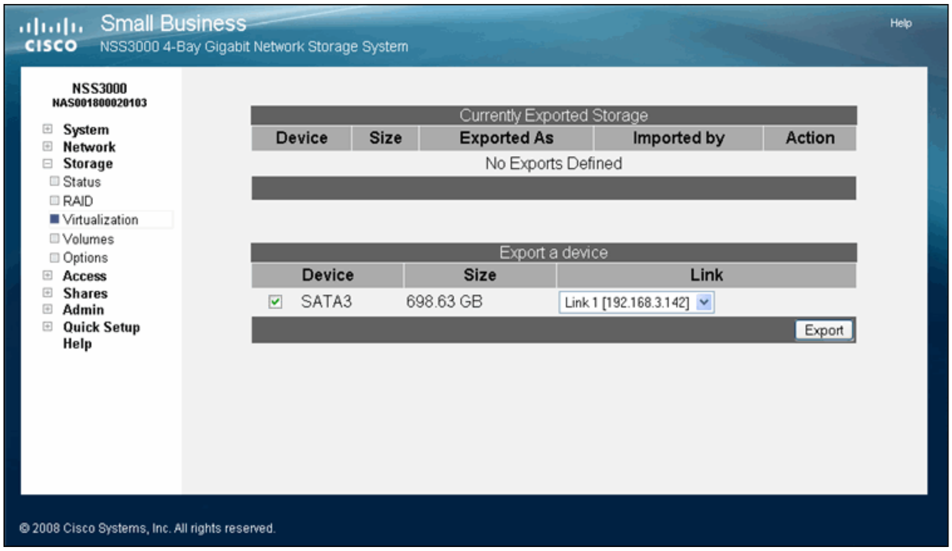
⚠ CAUTION After you configure a virtual RAID, you cannot migrate the disks used for that RAID to another NSS. You also cannot export storage from a device that uses imported storage.

To export storage to the network:

STEP 1 Log into the configuration interface for the device from which you are exporting storage.

STEP 2 From the **Manager Menu**, click **Storage** ➔ **Virtualization**

The **Storage Virtualization** page appears.



Currently Exported Storage

Device	Size	Exported As	Imported by	Action
No Exports Defined				

Export a device

	Device	Size	Link
☑	SATA3	698.63 GB	Link 1 [192.168.3.142]

STEP 3 From the **Export a device** area, select each device that you want to export from the list of available devices.

STEP 4 From the **Link** field, select the physical link that you want to use to export the storage.

STEP 5 Click **Export**.

STEP 6 The selected disk(s) disappear from the available list of arrays and appear in the **Currently Exported Storage** table at the top of the page. To use the exported storage, follow the steps in the next section, Creating Virtualized Storage.

Creating Virtualized Storage

After you export storage from a slave storage unit, it becomes available to other storage units in your network. The recommended way to use virtualized storage is to assign a master storage unit (the master must be an NSS6000 series model). The designated master unit then becomes the configuration point for all your storage-related management. You can use the exported storage to create a JBOD, which you can then use to set up volumes and shares.

Keep in mind that although the storage is managed through the master unit, the physical device that contains the exported storage is still managed through the applicable slave unit. If you affect the physical disk drives (e.g., shut down the power to the unit), this affects any logical storage built using those disk drives.

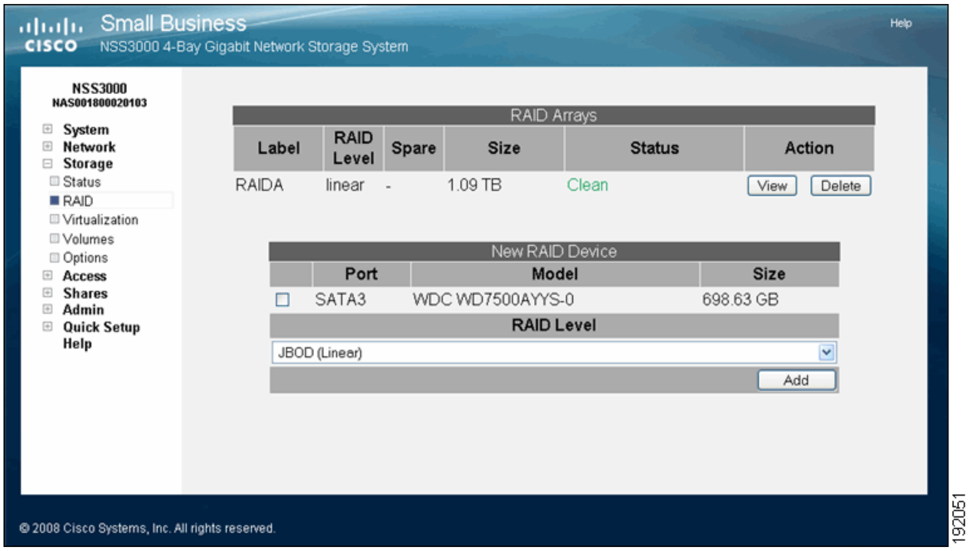
NOTE After you configure a virtual RAID, you cannot migrate the disks used for that RAID to another NSS. You also cannot export storage from a device that uses imported storage.

To create a JBOD with exported disks:

STEP 1 Log in to the configuration interface from the master NSS6000 series unit.

STEP 2 From the **Manager Menu**, click ***Storage*** → **RAID**.

The **RAID** page appears.



RAID Arrays

Label	RAID Level	Spare	Size	Status	Action
RAIDA	linear	-	1.09 TB	Clean	View Delete

New RAID Device

	Port	Model	Size
□	SATA3	WDC WD7500AAYS-0	698.63 GB

RAID Level: JBOD (Linear)

Add

Exported disks from other NSS units in the network appear in the **New RAID Device** table.

STEP 3 From the **New RAID Device** table, click the disks or arrays that you want to include in the JBOD.

STEP 4 Select **JBOD** as the RAID level.

STEP 5 Click **Add**.

The JBOD appears in the **RAID Arrays** listing. You can now create volumes from the virtualized JBOD.

Unexporting Storage

You can choose to unexport pieces of the storage currently exported to the network.You can only unexport storage that has not yet been used.

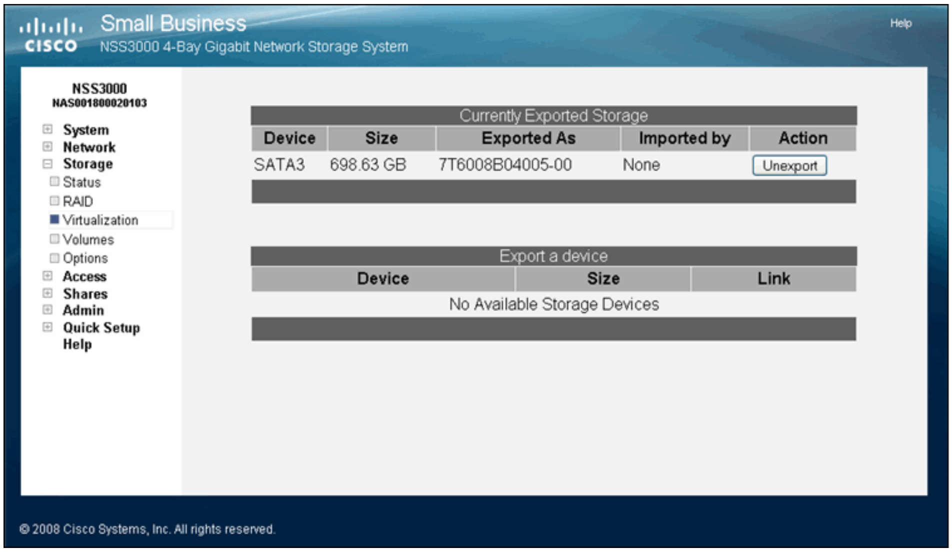
To unexport a piece of storage:

STEP 1 From the Master device, delete any RAID arrays associated with the storage you want to unexport. See ”Deleting an Array” on page 11.

STEP 2 Display the **Configuration Interface** for the slave device that contains the storage you want to unexport.

STEP 3 From the Manager Menu, click **Storage** ➡ **Virtualization**.

The **Storage Virtualization** page appears.



Currently Exported Storage

Device	Size	Exported As	Imported by	Action
SATA3	698.63 GB	7T6008B04005-00	None	Unexport

Export a device

Device	Size	Link
No Available Storage Devices		

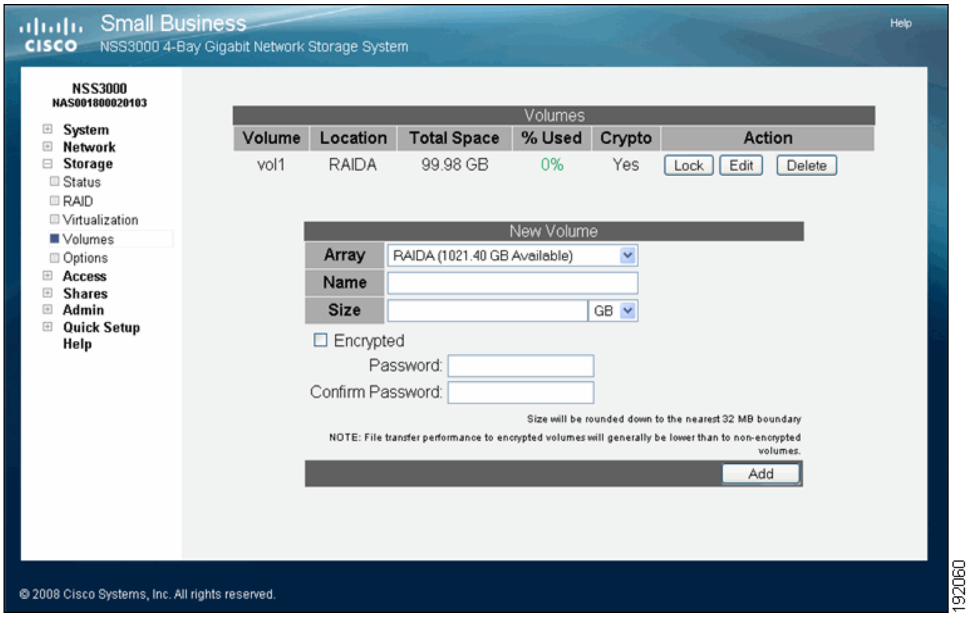
STEP 4 Click **Unexport** for the device you want to release from the network.

The disk drive(s) or array no longer appears in the **Currently Exported Storage** list. It now appears in the **Export a device** list and is again available for use.

Volume Management

A volume is a way to partition storage space available on an array. The **Storage Volumes** page shows the following details about configured volumes or create additional volumes.

The LCD lets you view the existing volumes and the percentage of space used.



Volumes

Volume	Location	Total Space	% Used	Crypto	Action
vol1	RAIDA	99.98 GB	0%	Yes	Lock Edit Delete

New Volume

Array	RAIDA (1021.40 GB Available)
Name	
Size	GB

☐ Encrypted

Password:

Confirm Password:

Size will be rounded down to the nearest 32 MB boundary

NOTE: File transfer performance to encrypted volumes will generally be lower than to non-encrypted volumes.

The Volumes table displays the following:

- **Volume**: The name of the volume.
- **Location**: The array on which the volume is located.
- **Total Space**: The amount of space allocated for the volume (in MB, GB, or TB).
- **% Used**: The amount of space, as a percentage, that is currently used.
- **Crypto**: Whether the volume is encrypted or not. Note that file transfer performance to encrypted volumes is generally lower than to non-encrypted volumes.

- **Action**: Click **Edit** to make changes to the current volume. Click **Delete** to remove the volume (and any saved data on the volume) from the array. If the volume is encrypted, you can either click **Unlock** to unlock it and make it usable, or click **Lock** to manually lock it.

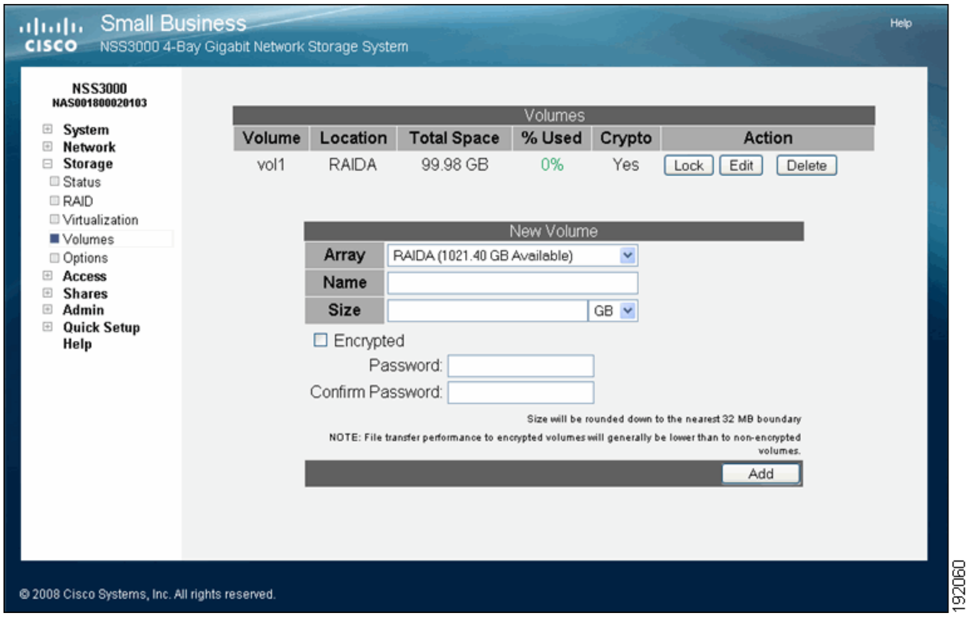
Creating a Volume

After you define at least one RAID array, you can create a volume. You need to create at least one volume before you can create users, groups, or shares.

To create a volume:

STEP 1 From the **Manager Menu**, click **Storage** ➔ **Volumes**.

The **Storage Volumes** page appears.



Volumes

Volume	Location	Total Space	% Used	Crypto	Action
vol1	RAIDA	99.98 GB	0%	Yes	Lock Edit Delete

New Volume

Array	RAIDA (1021.40 GB Available)
Name	
Size	GB

□ Encrypted

Password:

Confirm Password:

Size will be rounded down to the nearest 32 MB boundary

NOTE: File transfer performance to encrypted volumes will generally be lower than to non-encrypted volumes.

STEP 2 From the **New Volume** area, set up the following fields:

- **Array**: Click the drop-down menu to select the array on which you want to create the volume.

- **Name**: Enter the name you want to give the volume. The volume name must consist of at least one alphanumeric character, must begin with a letter, but cannot contain any spaces.
- **Size**: Enter the size for the volume, and then select the unit from the drop-down menu. The final size of the shared volume is less than the size you enter in this field due to filesystem overhead. The minimum volume size is 32 MB. Volume sizes are rounded down to the nearest 32 MB increment.

NOTE Once you create the volume, you can expand it but you cannot reduce its size.

STEP 3 To encrypt the volume, select **Encrypted**. To create an unencrypted volume, go to step 6.

NOTE You can encrypt the volume only when the volume is first created. After you create a volume, you cannot change whether it is encrypted or unencrypted. to The file transfer performance for encrypted volumes is generally lower than for non-encrypted volumes.

STEP 4 Enter a password in the **Password** field.

The password must be entered to unlock an encrypted volume when the NSS is started up following a power interruption, shutdown, or rebooted, or, if the volume was manually locked through the NSS configuration interface. The password can be any alphanumeric characters (with the exception of the ";" |", and "&"). It cannot contain any spaces and must be a minimum of one character (no maximum).

CAUTION Because you need the password to decrypt a locked volume, keep a secure backup of the password to ensure that it is accessible when required. There is no way to unlock the volume without the password. (If you forget the password, the only way to unlock the volume is if a known password was saved in a configuration file. You can then restore the configuration, and then use that password to unlock the volume. See ”Restoring a Configuration File” on page 62.

STEP 5 Re-enter the password in the **Confirm Password** field.

STEP 6 Click **Add**.

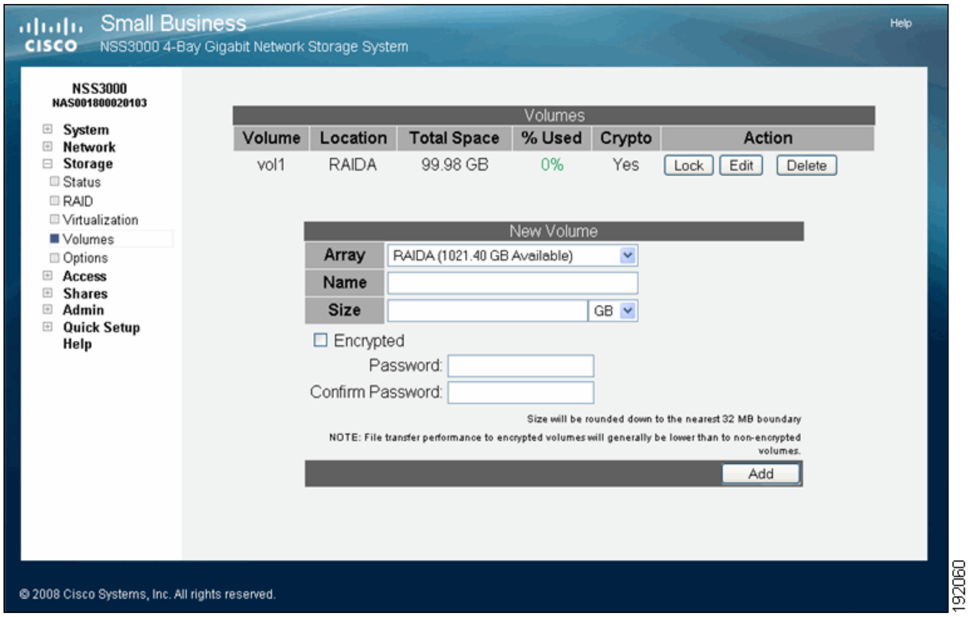
Expanding a Volume

After a volume is created, you can increase its size, provided there is available space on the array.

To increase the size of a volume:

STEP 1 From the **Manager Menu**, click **Storage** ➡ **Volumes**.

The **Volumes** page appears.



Volumes

Volume	Location	Total Space	% Used	Crypto	Action
vol1	RAIDA	99.98 GB	0%	Yes	Lock Edit Delete

New Volume

Array	RAIDA (1021.40 GB Available)
Name	
Size	GB

□ Encrypted

Password:

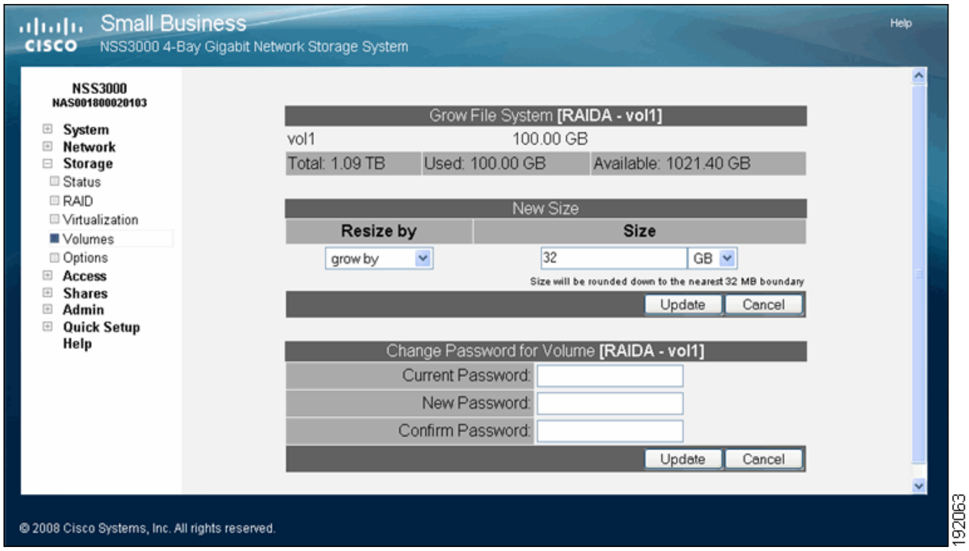
Confirm Password:

Size will be rounded down to the nearest 32 MB boundary

NOTE: File transfer performance to encrypted volumes will generally be lower than to non-encrypted volumes.

Add

STEP 2 Click **Edit** for the volume you want to expand.



Grow File System [RAIDA - vol1]

vol1 100.00 GB

Total: 1.09 TB | Used: 100.00 GB | Available: 1021.40 GB

New Size

Resize by	Size
grow by	32 GB

Size will be rounded down to the nearest 32 MB boundary

Change Password for Volume [RAIDA - vol1]

Current Password:

New Password:

Confirm Password:

The **Grow File System** page appears for the selected volume.

STEP 3 In the **Resize** by field, select one of the following:

- **Grow By**: Select this option to add the space allocated in the **Size** field to the existing space for the volume. For example, if the volume currently has 224 MB of space and you want to add another 224 MB, select "**Grow By**", then enter 224 in the Size field, and then set the unit field to MB.
- **Resulting Size**: Select this option to resize the volume to the space entered in the Size field. For example, if the volume currently has 224 MB of space and you want it to have 928 MB, select "**Resulting Size**", and then enter 928 in the **Size** field.

NOTE The system rounds up the total space to the nearest 32 MB boundary.

STEP 4 Depending on your choice in the previous step, enter the new number in the **Size** field, and then select the unit from the drop-down menu. If you selected "**Grow By**", the new number is added to the existing volume size. If you selected "**Resulting Size**", the new number becomes the total size for the volume.

STEP 5 Click **OK**.

Deleting a Volume

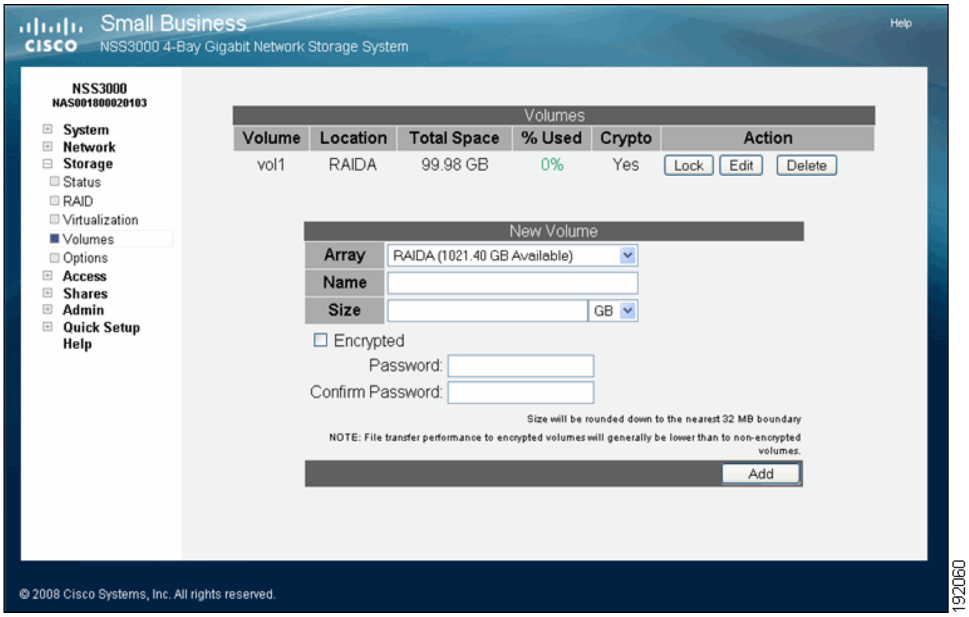
You can choose to delete a volume at any time.

CAUTION Deleting the volume removes any shares or data currently saved to that volume. If the volume was assigned as the users' **Home Directory Location**, you must reassign it to another volume.

To delete a volume:

STEP 1 From the **Manager Menu**, click **Storage ➔ Volumes**.

The **Storage Volumes** page appears.



Volumes

Volume	Location	Total Space	% Used	Crypto	Action
vol1	RAIDA	99.98 GB	0%	Yes	Lock Edit Delete

New Volume

Array	RAIDA (1021.40 GB Available)
Name	
Size	GB

□ Encrypted

Password:

Confirm Password:

Size will be rounded down to the nearest 32 MB boundary

NOTE: File transfer performance to encrypted volumes will generally be lower than to non-encrypted volumes.

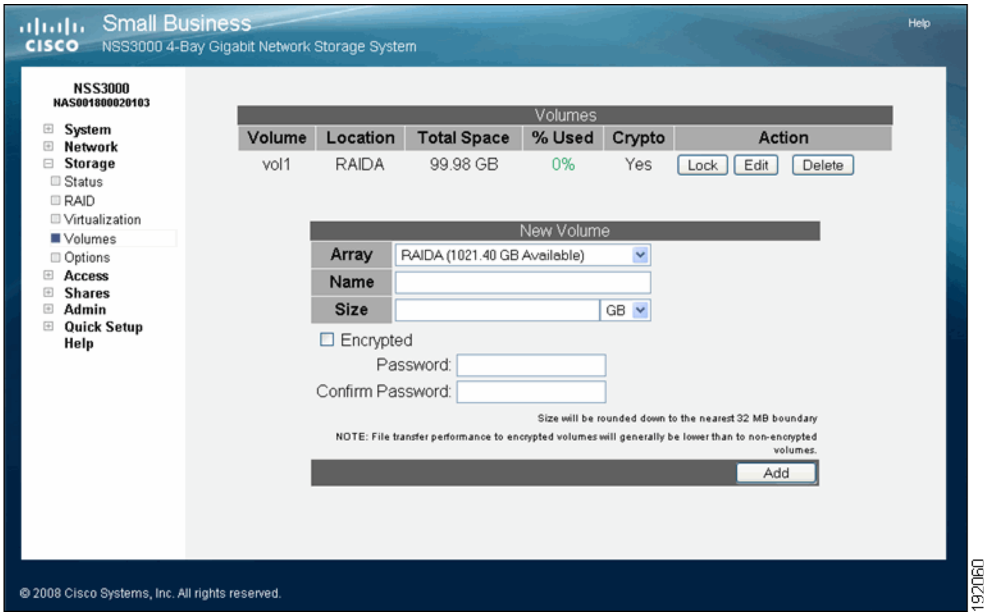
Add

STEP 2 From the Volumes area, click **Delete** for the volume you want to delete.

Volume Encryption Overview

The **Volumes page** lists both the encrypted and unencrypted volumes and lets you create a volume, and lock, unlock, or change the password for encrypted volumes.

NOTE File transfer performance to encrypted volumes is generally lower than non-encrypted volumes.



Volumes

Volume	Location	Total Space	% Used	Crypto	Action
vol1	RAIDA	99.98 GB	0%	Yes	Lock Edit Delete

New Volume

Array	RAIDA (1021.40 GB Available)
Name	
Size	GB

□ Encrypted

Password:

Confirm Password:

Size will be rounded down to the nearest 32 MB boundary

NOTE: File transfer performance to encrypted volumes will generally be lower than to non-encrypted volumes.

Add

© 2008 Cisco Systems, Inc. All rights reserved.

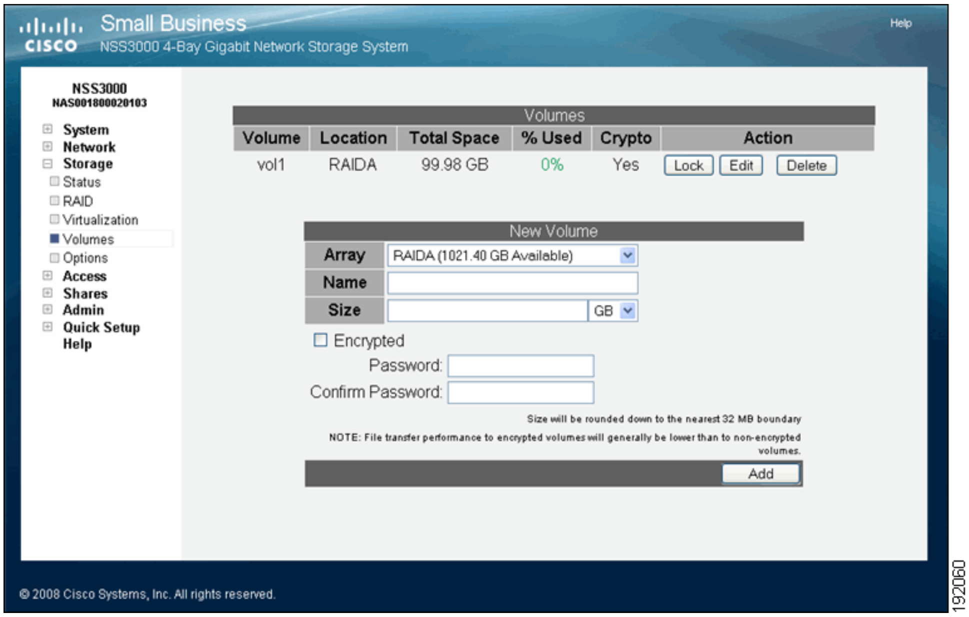
Locking an Encrypted Volume

You can manually lock an encrypted volume at any time. Locking a volume means that it becomes unmounted and is unusable (you cannot create or use shares stored on the locked volume). This provides an extra layer of security against the theft of data.

To lock a volume:

STEP 1 From the **Manager Menu**, click **Storage** ➜ **Volumes**.

The **Volumes** page appears.



Volumes

Volume	Location	Total Space	% Used	Crypto	Action
vol1	RAIDA	99.98 GB	0%	Yes	Lock Edit Delete

New Volume

Array	RAIDA (1021.40 GB Available)
Name	
Size	GB

□ Encrypted

Password:

Confirm Password:

Size will be rounded down to the nearest 32 MB boundary

NOTE: File transfer performance to encrypted volumes will generally be lower than to non-encrypted volumes.

Add

The **Crypto** column shows if the volume is encrypted (Yes) or not encrypted (No).

STEP 2 Click **Lock** to lock the volume.

NOTE The encrypted volume is locked automatically when the NSS is reboot or if a power outage occurs.

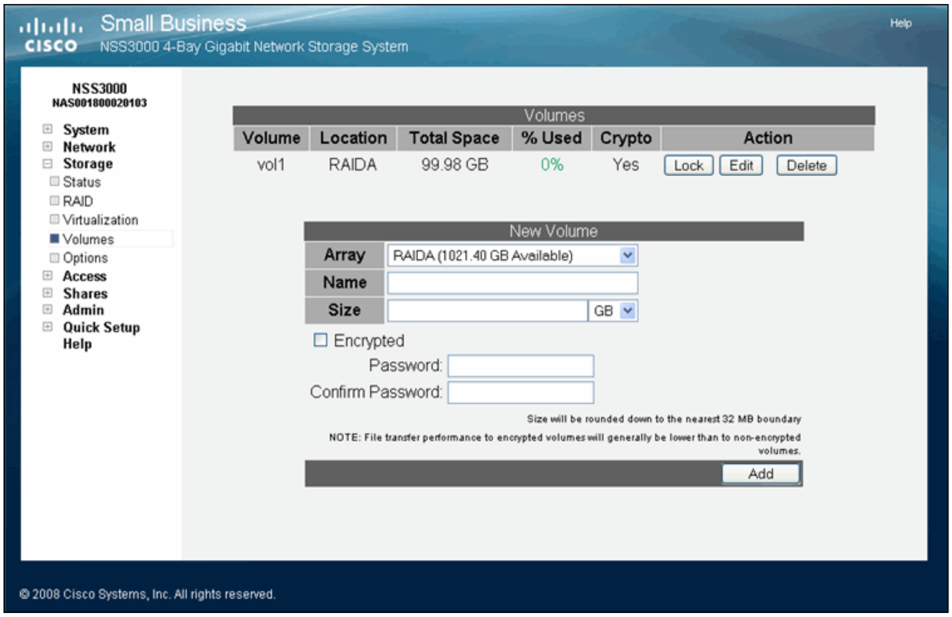
Unlocking a Locked Volume

When an encrypted volume is locked, either automatically as a result of the NSS being rebooted or manually locked through the configuration interface, you must unlock it before it can be used for tasks such as creating shares or quotas.

To unlock a volume:

STEP 1 From the **Manager Menu**, click **Storage** ➡ **Volumes**.

The **Volumes** page appears.



Volumes

Volume	Location	Total Space	% Used	Crypto	Action
vol1	RAIDA	99.98 GB	0%	Yes	Lock Edit Delete

New Volume

Array	RAIDA (1021.40 GB Available)
Name	
Size	GB

□ Encrypted

Password:

Confirm Password:

Size will be rounded down to the nearest 32 MB boundary

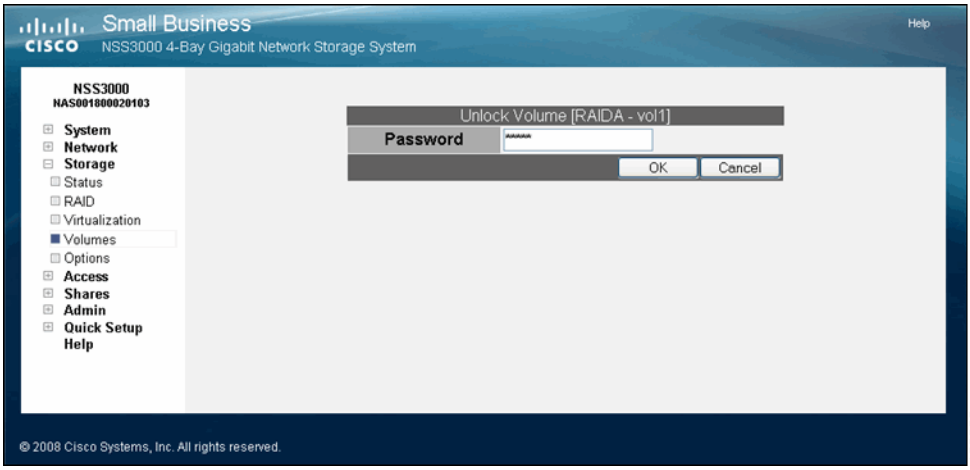
NOTE: File transfer performance to encrypted volumes will generally be lower than to non-encrypted volumes.

Add

192060

STEP 2 Click **Unlock** for the volume you want to unlock.

The **Unlock Volume** page appears.



Unlock Volume [RAIDA - vol1]

Password: *****

OK Cancel

192066

STEP 3 Enter the password for the volume in the **Password** field.

STEP 4 Click **OK**.

The **Volume Encryption** page appears. The volume is now unlocked.

Changing the Password for an Encrypted Volume

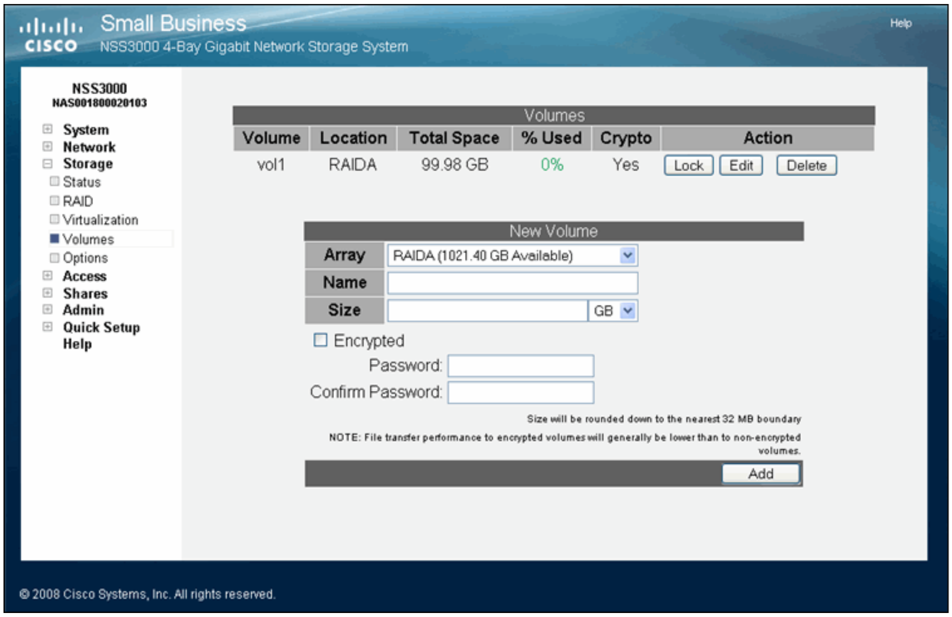
A password must be set up when you create an encrypted volume. After you create a volume, you can change the password at any time. The password must be entered under two conditions: when the NSS is started up after a power interruption, or, the volume has been manually locked.

⚠ **CAUTION** Because the password is required to de-crypt a locked volume, keep a backup of the password to ensure that it is accessible when required. There is no way to unlock the volume without the password. (If you forget the password, the only way to unlock the volume is if there is a known password saved in a configuration file. See ”Restoring a Configuration File” on page 62.

To change the password on an existing encrypted volume:

STEP 1 From the **Manager Menu**, click **Storage** ➜ **Volumes**.

The **Volumes** page appears.



Volumes

Volume	Location	Total Space	% Used	Crypto	Action
vol1	RAIDA	99.98 GB	0%	Yes	Lock Edit Delete

New Volume

Array	RAIDA (1021.40 GB Available)
Name	
Size	GB

☐ Encrypted

Password:

Confirm Password:

Size will be rounded down to the nearest 32 MB boundary

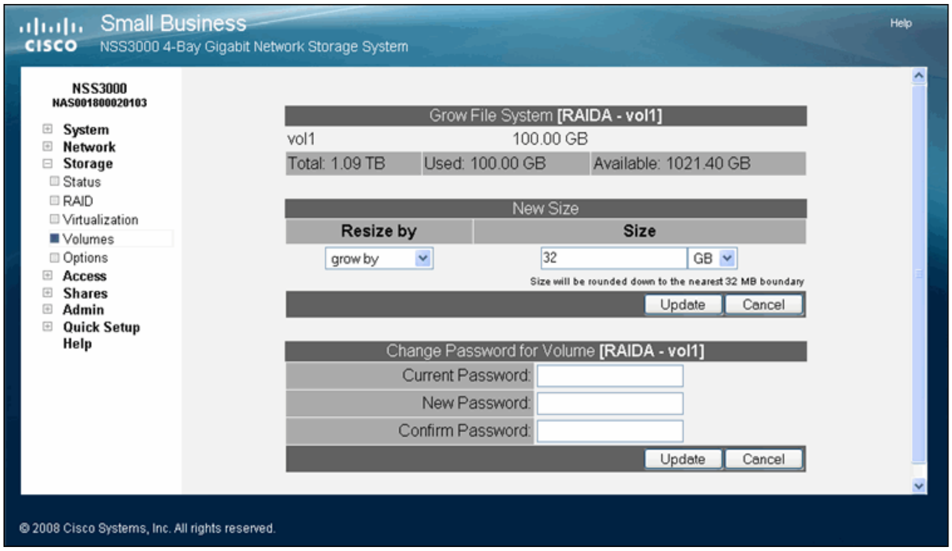
NOTE: File transfer performance to encrypted volumes will generally be lower than to non-encrypted volumes.

Add

192060

STEP 2 Click **Edit** for the volume you want to change.

The **Edit Volume** page appears.



Grow File System **[RAIDA - vol1]**

vol1	100.00 GB	
Total: 1.09 TB	Used: 100.00 GB	Available: 1021.40 GB

New Size

Resize by	Size
grow by	32 GB

Size will be rounded down to the nearest 32 MB boundary

Update Cancel

Change Password for Volume **[RAIDA - vol1]**

Current Password:

New Password:

Confirm Password:

Update Cancel

192063

STEP 3 In **Current Password** field, enter the password.

STEP 4 In the **New Password** field, enter the new password. The password can be any alphanumeric characters (with the exception of the ";" |", and "&"). It cannot contain any spaces and must be a minimum of one character (no maximum).

STEP 5 Re-enter the new password in the **Confirm Password** field.

STEP 6 Click **Update**.

Storage Options

The **Storage Options** page lets you define the following:

- **Idle Drive Spin Down**: Configure the NSS to spin down the disk drives after a predefined time of inactivity. You can select the period of time that the disk drive must be idle before it is spun down.
- **RAID Rebuild Priority**: During normal operation, the CPU switches between tasks to service all active tasks on the system. Creating a RAID array or rebuilding an existing array can take up a significant amount of the available percentage of CPU processing power. You can control how the system prioritizes the rebuild and allocates the system's resources based on your system's current workload and need for responsiveness.

  To set the RAID rebuild priority, choose one of the following options from the RAID Rebuild Priority field:

  - **High**: The CPU focuses on the RAID rebuilding process. This setting allows for the fastest possible RAID rebuild at the expense of other system tasks. File-sharing throughput is adversely affected during a RAID rebuild when this setting is chosen.
  - **Medium**: Provides a balance between the rebuild process and other system tasks. The rebuild process takes longer than if it was set to High.
  - **Low**: The CPU focuses on other tasks versus the RAID rebuild process. This results in a longer rebuild time on a busy system. However, if the workload on the system is low, the CPU services the rebuild process well. If you are repairing an array, this option leaves the array the most vulnerable of all the options as it takes the longest for the rebuild to complete.
- **Degraded Mode Grace Period**: Set the period of time after which the system automatically shuts down degraded arrays. You can manually restart a RAID array that has been automatically stopped by the degraded

mode management feature. Warning messages are sent out periodically while the RAID array is degraded.

- **Enable Global Spares**: Allow RAID arrays defined in the system to share spare drives. If this option is disabled, a RAID array can only use a spare that has been added to that particular array. If this option is enabled, spare drives added to one RAID array may be reallocated by the NSS to another RAID array.

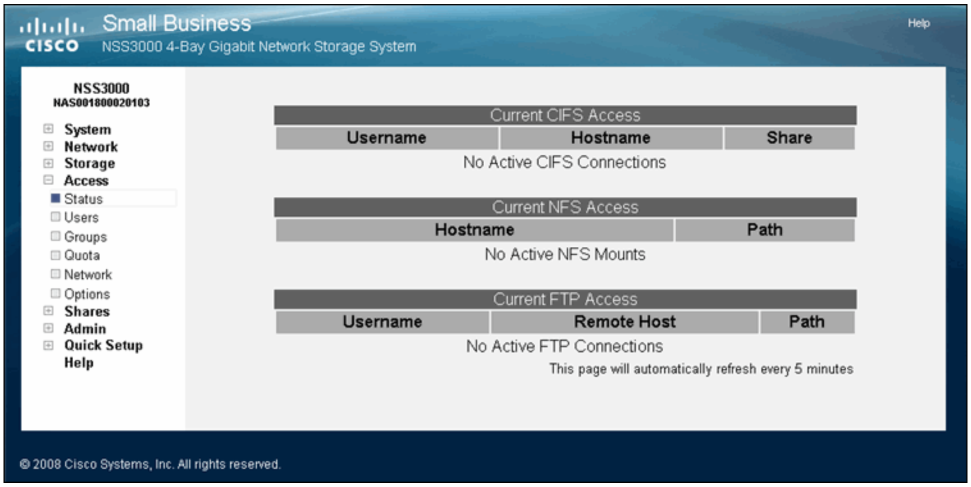
  For example, if RAID A is a two-drive RAID1 that is not degraded and RAID B is a degraded two-drive RAID1, if you add a spare drive to RAID A, the NSS automatically +gives the spare drive to RAID B to enable RAID B to resync. This option is only relevant when you use network disks (through storage virtualization). A system limited to local disks lets you only build up to two, two-disk RAID arrays, but have no spares.

NOTE If you make changes to any of the storage options, click **Update**.

5

Setting up End-User Access

The **Access Status** page shows the current end-user connections to the NSS, grouped by the file-sharing protocol used. The page displays the username, the name of the host from which the user is currently connected, and the share or path that the user is accessing. Status pages automatically refresh on a regular interval and are very helpful for monitoring the progress of certain processes such as the current end-user connections to the NSS.



Current CIFS Access

Username	Hostname	Share

No Active CIFS Connections

Current NFS Access

Hostname	Path

No Active NFS Mounts

Current FTP Access

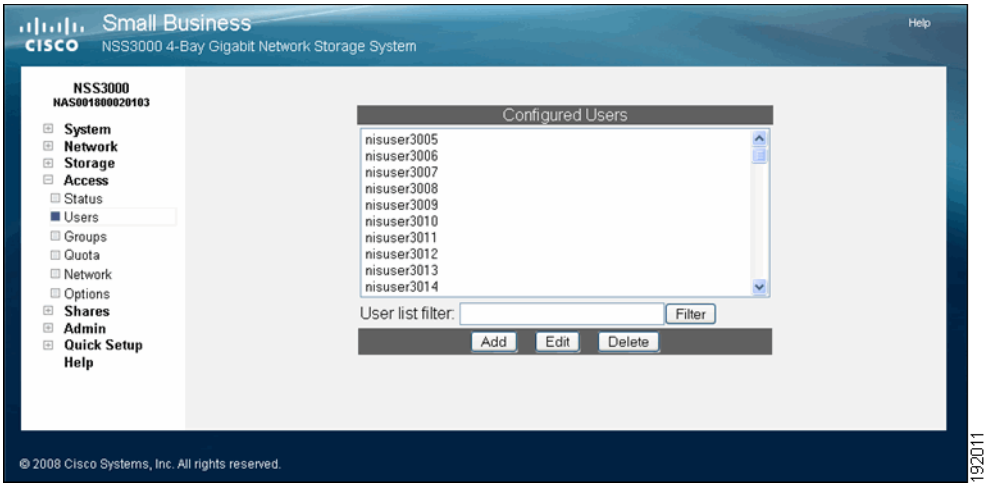
Username	Remote Host	Path

No Active FTP Connections

This page will automatically refresh every 5 minutes

Managing your NSS Users

You can create, view, and maintain the list of users who can access the NSS. The **Configured Users** page displays the **Configured Users** table. This table lists each defined user whether the user was created locally through the NSS configuration interface or imported from an NTv4, Active Directory, or NIS domain. Users not created locally through the NSS are read-only with the exception of the email address field which you can update directly through the **NSS Configuration Manager.** Once a user profile is created, you cannot rename the username. To rename an existing user profile, delete the user profile and then create a new one. User profiles are maintained by the administrator. Users cannot make changes to their passwords.



To limit the entries in the User list, perform a substring search by entering the desired search string in the **User List Filter** field, and then click **Filter.** (For example, enter "ea" to display any list items that contain "ea" such as "Sean" or "BillyJean".) To clear the filter, delete the contents of the **User List Filter** field, and then click **Filter.**

Creating a User Profile

Depending on your network setup, you might administer users and groups locally or through the domain controller. The NSS configuration interface gives you read-only access to users provided by NTv4, Active Directory, or NIS domains (with the exception of being able to edit the email address). You can also create and manage local users from the NSS configuration interface. Before you can create a user profile, you must configure the volume you want to use as the home directory location for your users on the **Access Options** page (from the **Manager Menu**, click **Access** ➜ **Options**).

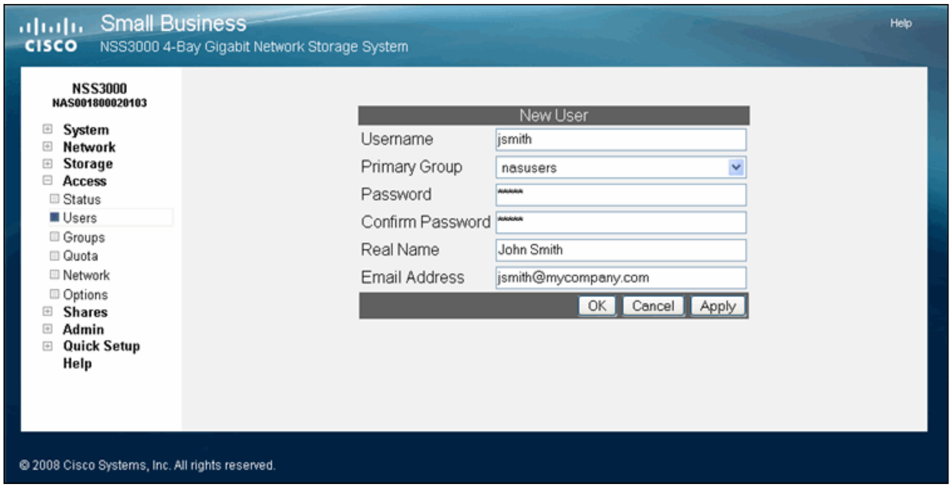
To add a local user:

STEP 1 From the **Manager Menu**, click **Access** ➜ **Users**.

The **Configured Users** window appears. Users created from the NSS configuration interface and provided by the ADS, NTv4, or NIS domain appear in the **Configured Users** table.

STEP 2 Click **Add** to create a user.

The **New User** page appears.



New User

Username	jsmith
Primary Group	nasusers
Password	*****
Confirm Password	*****
Real Name	John Smith
Email Address	jsmith@mycompany.com

STEP 3 In the **Username** field, type the username. The name must be made up of alphanumeric characters (that is, a-z, 0-9), any case, to a maximum of 32 characters. This field is required.

STEP 4 Select the group you want to assign as the user's primary group from the **Primary Group** field. If there are no groups configured, the only available choice is the default group "nasusers". This field is required.

NOTE Although you can assign the user to multiple groups (through the **Add Group** or **Edit Group** page), the primary group is the group against which quota charges for the user's storage usage are made and is the group that defines the group ownership for all files created by the user. The primary group applies to users set up locally on the NSS. A domain user's primary group is set up from the domain and is not derived from the Primary Group field in the NSS user profile.

STEP 5 Assign a password by entering any valid (ASCII table) characters in the **Password** field. The password is required.

STEP 6 To verify the password, re-enter it in the **Confirm Password** field.

NOTE All password changes to end-user accounts set up through the NSS configuration pages must be made by the administrator.

STEP 7 To record the user's full name, enter it in the **Real Name** field. This field is optional. Note that you cannot enter the "/" character in this field.

STEP 8 To record the user's email address, enter it in the **Email Address** field. This field is optional.

STEP 9 Click **OK** to create the user and exit the **New User** page. Click **Apply** to create the user and then add another new user.

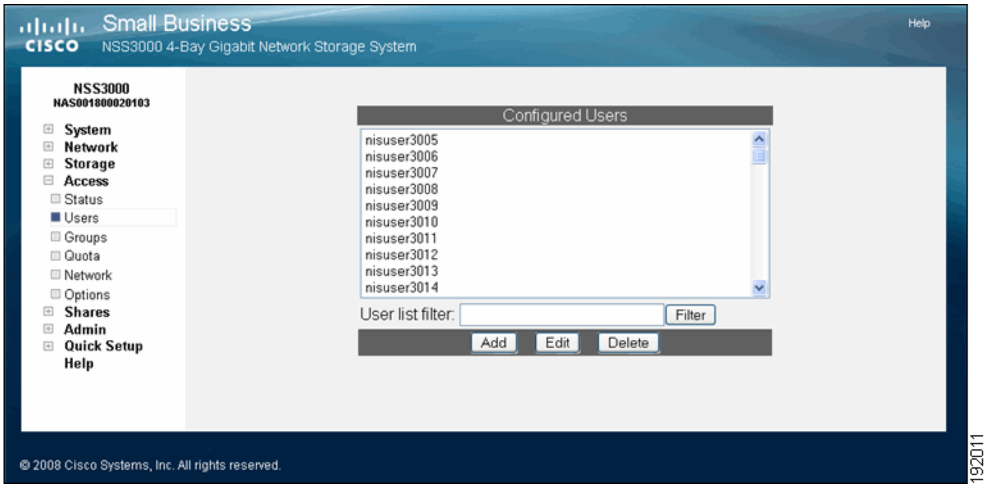
Editing a User Profile

You can change certain aspects of the user's profile. Once you create a username, the only way to "rename" that user is to delete the existing user profile and then create a new one. Domain user profiles are read-only except for the email address which you can add or edit directly from the **NSS Configuration Manager**. All password changes for end-user accounts set up directly through the NSS configuration pages must be done by the Administrator.

To edit an existing user profile:

STEP 1 From the **Manager Menu**, click **Access** ➡ **Users**.

The **Configured Users** page appears.

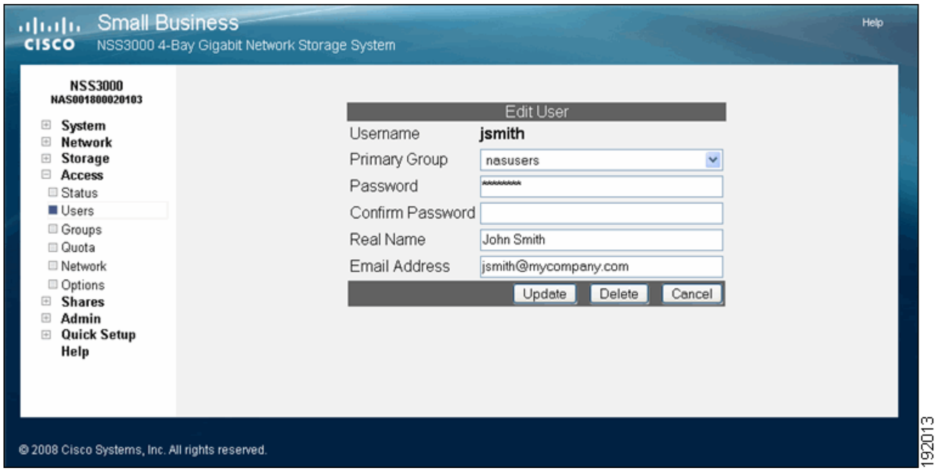


nisuser3005
nisuser3006
nisuser3007
nisuser3008
nisuser3009
nisuser3010
nisuser3011
nisuser3012
nisuser3013
nisuser3014

The existing users appear in the **Configured Users** table.

STEP 2 Select the user from the list, and then click **Edit**. To limit the entries in the **User** list, perform a substring search by entering the desired search string in the **User List Filter** field, and then clicking **Filter**. (For example, enter "ea" to display any list items that contain "ea" such as "Sean" or "BillyJean".)

The end user's profile appears in the **Edit User** page.



Edit User

Username jsmith

Primary Group nasusers

Password ********

Confirm Password

Real Name John Smith

Email Address jsmith@mycompany.com

STEP 3 The username is read-only. You can make changes to any of the other fields in the user's profile.

STEP 4 Click **Update**.

Integrating Users from an ADS, NTv4, or NIS Domain

When the NSS is joined to an ADS, NTv4, or NIS domain, a list of existing domain users is imported into the **Configured Users** list. You can view the entire user list from the **Configured Users** page but can only edit or delete locally created users (not domain users). The one exception to this is that you can edit the email address directly from the Configuration Manager. The naming conventions use the NetBIOS format with the domain name as a prefix of the username. The primary group for users set up within the ADS, NTv4 or NIS domain is taken from the user's domain profile versus the **Primary Group** field in the NSS user profile.

NOTE Set up your User and Group ID ranges before you join the NSS to an ADS, NTv4, or NIS domain. After you join the NSS to a domain, you do not make any changes to the ranges as this might lead to an ID collision.

Logging into the NSS as a Local User

When the NSS is joined to an NTv4 or ADS domain, local users must prefix their username with the hostname of the NSS. Users who log in without the hostname prefix are automatically assumed to be domain users. For example, if the NSS hostname is "NASadmin" and the local username is "bob", the user would need to log in as "NASadmin\bob" in the login dialog.

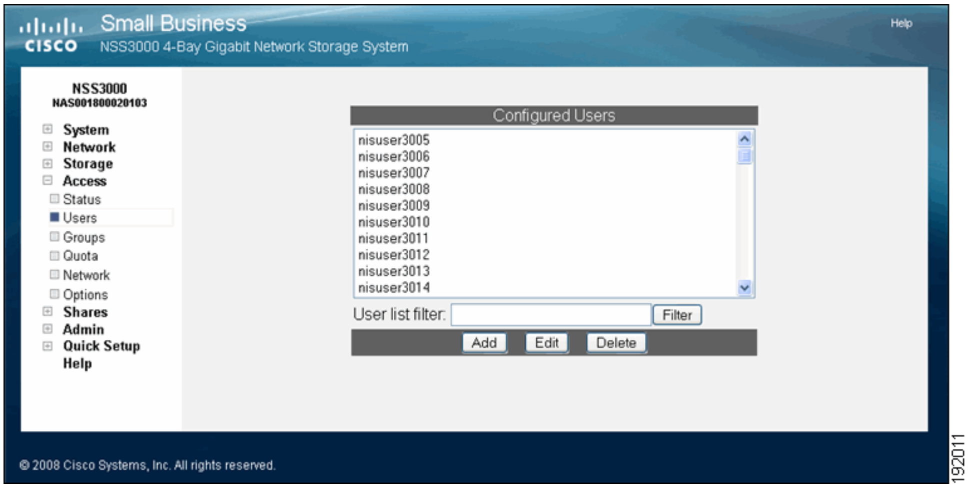
Deleting a User Profile

You can delete user profiles that were created through the NSS. When you delete a user profile, the user’s home directory and any files or folders created by the user on the various shares are not deleted. As an administrator, you can log into CIFS using the administrator account to delete the user’s data as required.

To delete an existing user profile:

STEP 1 From the **Manager Menu**, click **Access** ➜ **Users**.

The **Configured Users** page appears.



STEP 2 Click the username and then click **Delete**. To delete multiple users, use the following mouse-key combinations:

- **Shift-click**: To select a contiguous group of users that you want to delete, hold down the **Shift** key, then click the first user, and then the last user in the series. Click **Delete** to delete the highlighted users.
- **Ctrl-click**: To select a non-contiguous group of users that you want to delete, hold down the **Ctrl** key, and then click each user from the list. Click **Delete** to delete the highlighted users.

The selected user(s) disappear from the list of available users.

Working with Groups

Groups are an easy way to manage users with the same storage needs and privileges. A group consists of one or more users. You can add or remove users from a group at any time. The user's primary group (the group to which quota charges for storage usage are applied) is set up in the **Primary Group** field of the user's profile.

A group called "nasusers" is automatically created when you first install the NSS. This group is the default primary group when you create new users.

To limit the entries in the **Group** list, perform a substring search by entering the desired search string in the **Group List Filter** field, and then clicking **Filter**. (For example, enter "ea" to display any list items that contain "ea" such as "Sean" or "BillyJean".) To clear the filter, delete the contents of the **Group List Filter** field, and then click **Filter**.

Creating a Group

Groups let you specify the share access privileges for a set of users. After you create a group, you can define the group's access privileges on a per-share basis. You can add or remove users to and from the group at any time.

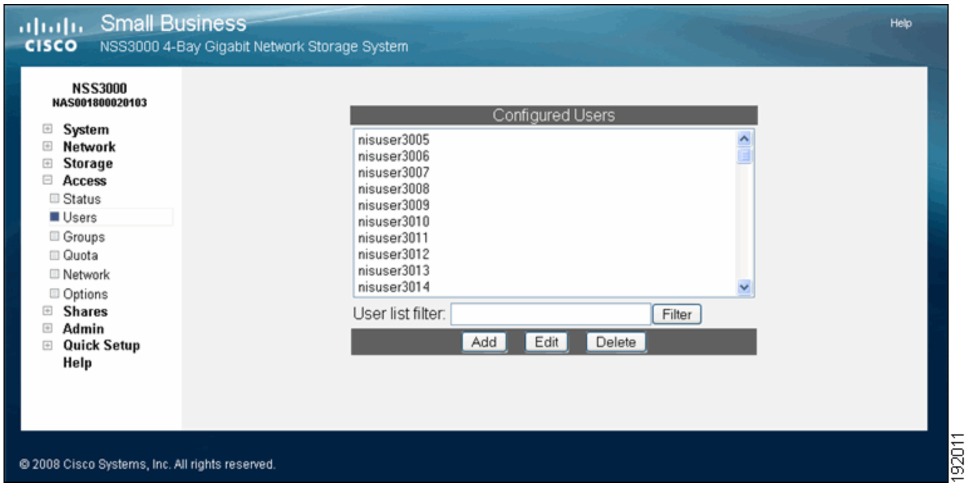
Users are assigned a primary group within their user profile. When users create a file, the group ownership is automatically set to their primary group. The storage usage is charged to their primary group for the purposes of volume quota accounting. Group membership, other than the primary group, is defined in either the **Add Group** or **Edit Group** page and is used only to control access to shares and files.

NOTE You cannot grant security privileges to a group for a CIFS share through an ACL.

To create a group:

STEP 1 From the **Manager Menu**, click **Access** ➡ **Groups**.

The **Configured Groups** page appears.



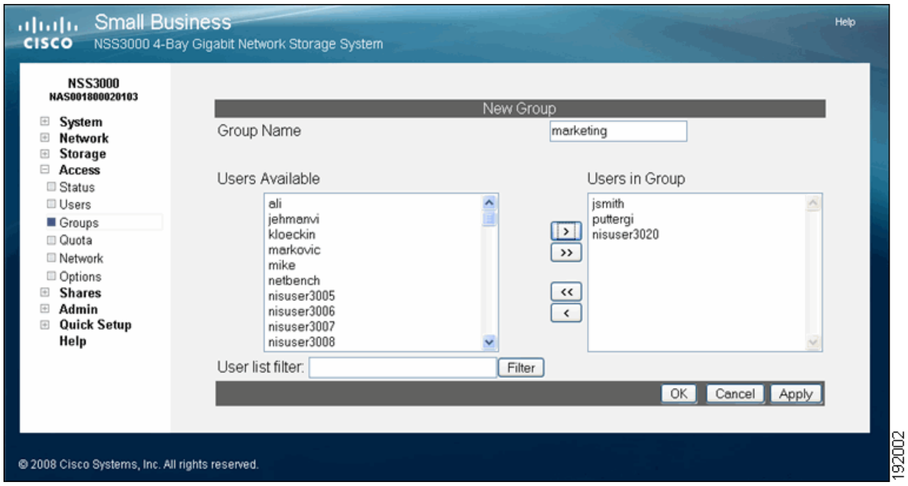
Configured Users

nisuser3005
nisuser3006
nisuser3007
nisuser3008
nisuser3009
nisuser3010
nisuser3011
nisuser3012
nisuser3013
nisuser3014

User list filter:

STEP 2 Click **Add**.

The **New Group** page appears.



New Group

Group Name: marketing

Users Available:
ali
jehmanvi
kloeckin
markovic
mike
netbench
nisuser3005
nisuser3006
nisuser3007
nisuser3008

Users in Group:
jsmith
puttergi
nisuser3020

User list filter:

STEP 3 In the **Group Name** field, type the name you want to assign to the group. The name can only contain lower-case alphanumeric characters and underscores (i.e., a-z, 0-9, _) to a maximum of 32 characters.

STEP 4 Move the users you want to assign to the group from the **Users Available** list to the **Users in Group** list. Note that a user can be assigned to multiple groups. (The single angled bracket "<" or ">" moves the selection in the direction of the bracket. The double angled bracket "<<" or ">>" moves the entire list in the direction of the bracket.) To limit the entries in the **Users Available** list, perform a substring search by entering the desired search string in the **User List Filter** field, and then clicking Filter. (For example, enter "ea" to display any list items that contain "ea" such as "Sean" or "BillyJean".)

STEP 5 Click **OK** to save the current group and display the **Configured Groups** page. Click **Apply** to save the current group and remain in the **New Group** page to add another group.

Changing the Users Assigned to a Group

After you create a group, you can delete or add to the list of users that belong to that group.

NOTE When you delete an end user from a group, the end user must log out of their client machine before the change takes effect. This means that users no longer assigned to a group maintain full group privileges (i.e., access to shares) until they log off or log on to their computer.

To change the group membership:

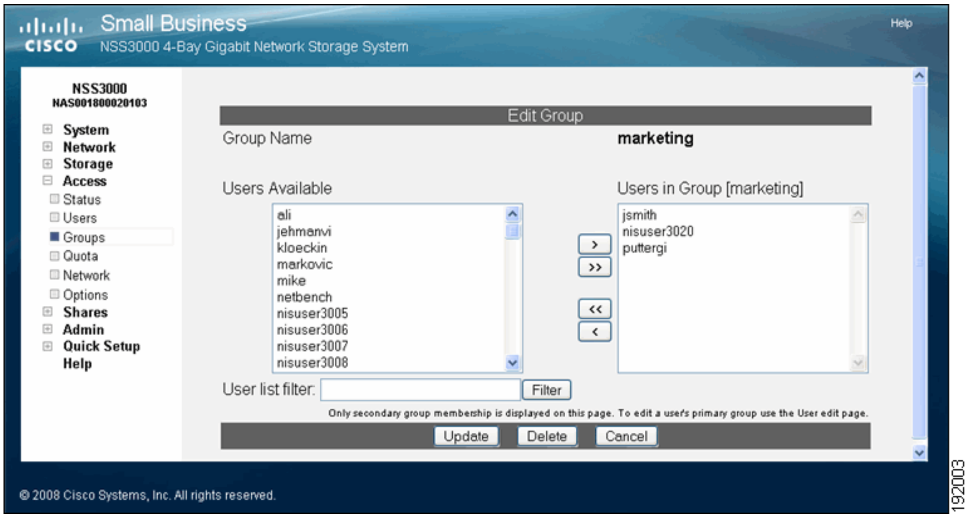
STEP 1 From the **Manager Menu**, click **Access** ➜ **Groups**.

The **Configured Groups** page appears.

STEP 2 From the list of configured groups, select the group that you want to change.

STEP 3 Click **Edit**.

The **Edit Group** page appears.



Edit Group

Group Name marketing

Users Available: ali, jehmanvi, kloeckin, markovic, mike, netbench, nisuser3005, nisuser3006, nisuser3007, nisuser3008

Users in Group [marketing]: jsmith, nisuser3020, puttergi

User list filter:

Only secondary group membership is displayed on this page. To edit a user's primary group use the User edit page.

STEP 4 Set up the **Users in Group** list as required. (The single angled bracket "<" or ">" moves the selection in the direction of the bracket. The double angled bracket "<<" or ">>" moves the entire list in the direction of the bracket.)

STEP 5 Click **Update**.

Integrating Groups from an Active Directory, NTv4, or NIS Domain

When the NSS is joined to an Active Directory, NTv4, or NIS domain, domain groups only appear on the **Shares** page (they do not appear in the list of configured groups). Group membership for imported domain groups are read-only. The naming conventions use the NetBIOS format with the domain name as a prefix of the group name. For example, "DOMAINNAME\GroupName"

NOTE Set up your User and Group ID ranges before you join the NSS to an ADS, NTv4, or NIS domain. After you join the NSS to a domain, do not make changes to the range as this might lead to an ID collision.

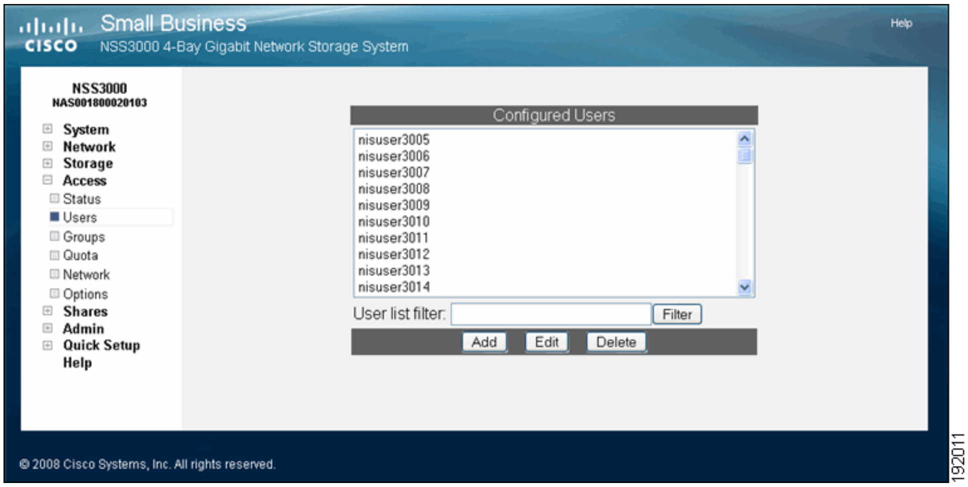
Deleting a Group

When you delete a group, the group is automatically removed from having access to any configured shares.

To delete a group:

STEP 1 From the **Manager Menu**, click **Access** ➡ **Groups**.

The **Configured Groups** page appears.



nisuser3005
nisuser3006
nisuser3007
nisuser3008
nisuser3009
nisuser3010
nisuser3011
nisuser3012
nisuser3013
nisuser3014

User list filter:

STEP 2 Before you can delete a group, you must remove any assigned users.

STEP 3 You can delete a group from the **Groups** page and **Edit Groups** page.

- To delete a group from the **Groups** page:

  Highlight the group you want to delete from the **Configured Groups** table, and then click **Delete**. To delete multiple groups, use the following key-mouse combination:

  - **Shift-click**: To select a contiguous list of groups that you want to delete, hold down the **Shift** key, then click the first group, and then the last group in the series. Click **Delete** to delete the highlighted groups.
  - **Ctrl-click**: To select a non-contiguous set of groups that you want to delete, hold down the **Ctrl** key, and then click each group from the list. Click **Delete** to delete the highlighted groups.

- To dele a group from the **Edit Groups** page

  Select the group you want to edit, and then click **Edit**. The **Edit Groups** page appears. Click **Delete** to remove the group.

Managing Volume Quotas

You can set up specific space limits for each user or group who has write access to a volume. When you define a user or group's quota you can set a space limit (referred to as a soft quota) that, when reached, sends a warning to the administrator and initiates a countdown of the defined grace period. The user has the amount of time in the grace period to reduce the amount of space used to under the soft quota limit. Users who do not reduce the space in the allotted grace period, or who reach their hard quota limit, no longer have write access to the volume until they reduce their usage to under their soft quota limit.

When a user creates, modifies or deletes a file on a volume, there is a small delay before the usage is updated on the **Filesystem Quota** page. This delay is due to the caching in the filesystem used to provide high performance.

NOTE Before you create or edit a quota located on an encrypted volume, make sure that the volume is unlocked. You also need to set up the **Warn For** time for each volume from the **Filesystem Quota** page. The **Warn For** time only affects individual quota that was created after the **Warn For** time was set.

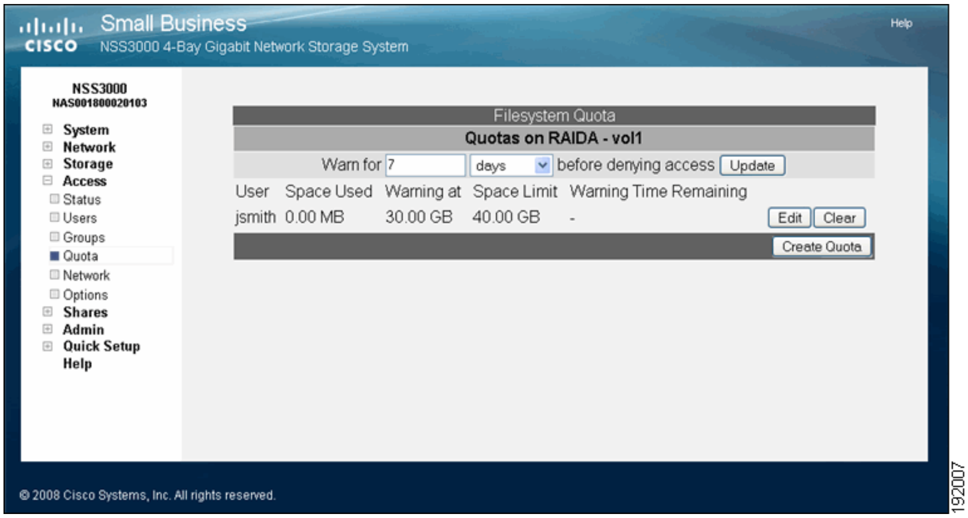
Changing the User's Primary Group

Quotas are charged to the group assigned as the user's primary group at the time of file creation. If the user's primary group changes, files created under the previous group continue to be charged against that group. If the user's primary group changes while the user is connected to the NSS, the previous primary group continues to be the group charged until the user's connection is closed. The new primary group becomes the group charged only after the connection is re-opened.

NOTE If the user is created within a domain, the primary group defined is in the user profile from the domain, not the **Primary Group** field in the NSS user profile.

About the Volume Quota Page

The **Volume Quota** page is where you manage user and group quotas for each volume. To display the **Volume Quota** page, from the **Manager Menu**, click **Access** ➡ **Quota**.



Filesystem Quota

Quotas on RAIDA - vol1

Warn for 7 days before denying access

User	Space Used	Warning at	Space Limit	Warning Time Remaining
jsmith	0.00 MB	30.00 GB	40.00 GB	-

Creating Volume Quota for a User or Group

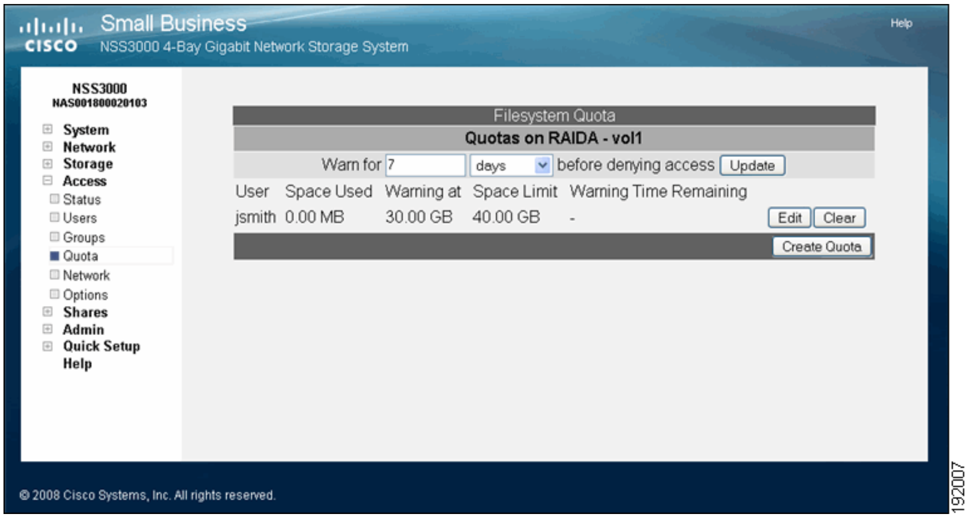
You can set up a quota on a volume for each user or group. This quota limits the user or group to the allocated amount of space within the volume. To give certain users or groups assigned to a volume full access to the space on the volume, do not create a quota for that user or group.

NOTE Before you can create quota on an encrypted volume, make sure that it is unlocked. You also need to set up the **Warn For** time for each volume from the **Filesystem Quota** page. The **Warn For** time only affects individual quota that was created after the **Warn For** time was set.

To create a quota for a user or group:

STEP 1 From the **Manager Menu**, click **Access** ➜ **Quota**.

The **Filesystem Quota** page appears.



Filesystem Quota

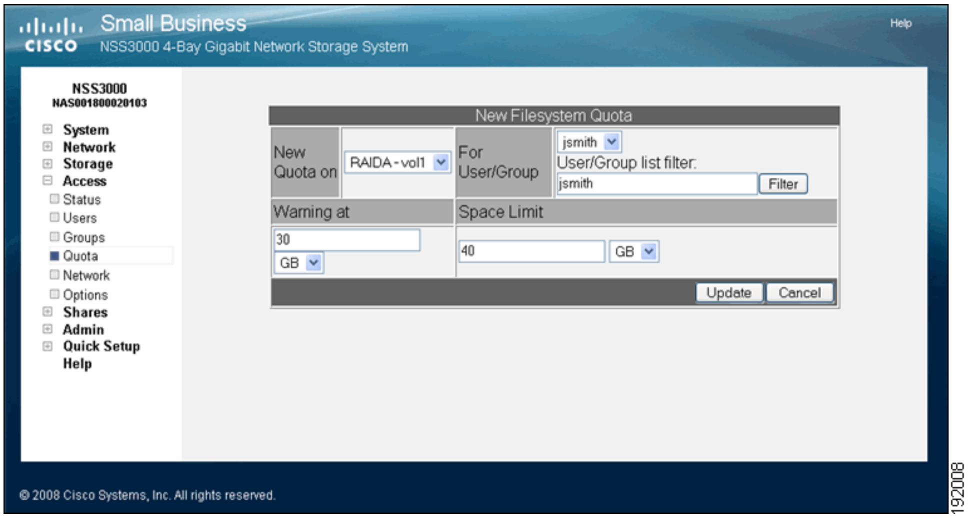
Quotas on RAIDA - vol1

Warn for 7 days before denying access

User	Space Used	Warning at	Space Limit	Warning Time Remaining
jsmith	0.00 MB	30.00 GB	40.00 GB	-

STEP 2 Click **Create Quota**.

The **New Filesystem Quota** page appears.



New Filesystem Quota

New Quota on	RAIDA - vol1	For User/Group	jsmith User/Group list filter: jsmith
Warning at		Space Limit	
30 GB		40 GB	

STEP 3 Select the volume on which you want to set the quota from the **New Quota on** drop-down list. To limit the entries in the User/Group list, perform a substring search by entering the desired search string in the **User/Group List Filter** field, and then clicking **Filter**. (For example, enter "ea" to display any list items that contain "ea" such as "Sean" or "BillyJean".)

STEP 4 Select the user or group for which you are creating the quota from the **For User/ Group** drop-down list.

STEP 5 In the **Warning at** field, enter the threshold of space that, when exceeded, triggers a warning that the quota is close to being used up. Select the size unit from the drop-down menu.

When the threshold is exceeded, the grace period set up for the volume begins. The user has the amount of time set in the grace period to reduce the amount of space used to under the space set in the **Warning at** field or they are not allowed to write further data to the volume. Another way to think about this field is as a “soft quota".

STEP 6 In the **Space Limit** field, enter the amount of space that the user or group has available to use, and then select the size unit from the drop-down menu. Another way to think about this field is as the "hard quota". If the user reaches the space limit, the user can no longer write data to the volume until they either reduce the amount of space used to under the limit by deleting files or have the quota increased.

STEP 7 Click **Update**.

Setting up the Grace Period for a Volume Quota

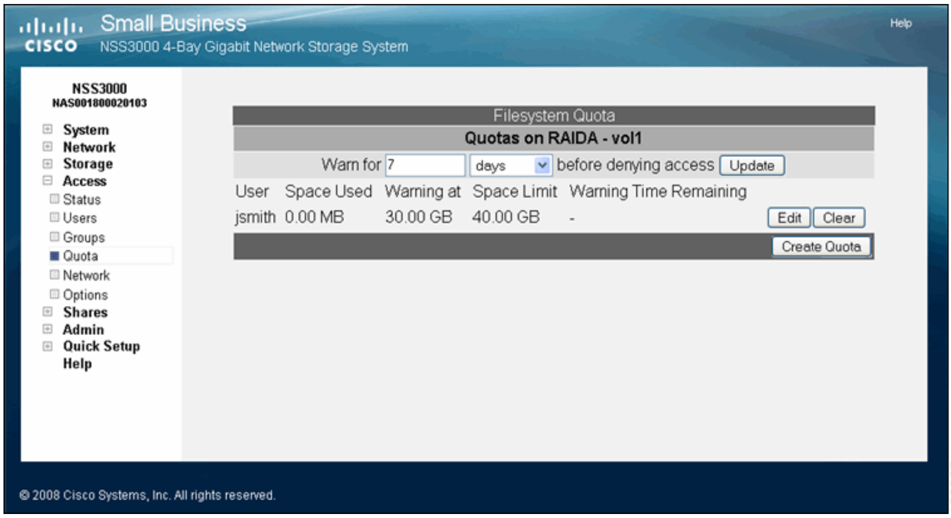
You can set up a limit on the amount of space available to your users or groups. This limit can be set as a soft quota and hard quota. When the users reach their "soft quota", a warning is issued and the grace period begins. Users then have the amount of time set in the grace period to either reduce the amount of spaced used by deleting files, or have the quota increased. If the amount of space is not reduced before the grace period expires or the user reaches the hard quota, the user is automatically denied write access to the volume.

NOTE Before you create quotas for a user or group, make sure that you set up the **Warn For** time for each volume from the **Filesystem Quota** page. The **Warn For** time only affects individual quota that was created after the **Warn For** time was set.

To set up the grace period for a volume:

STEP 1 From the **Manager Menu**, click **Access** ➜ **Quota**.

The **Filesystem Quota** page appears.



Filesystem Quota

Quotas on RAIDA - vol1

Warn for 7 days before denying access

User	Space Used	Warning at	Space Limit	Warning Time Remaining
jsmith	0.00 MB	30.00 GB	40.00 GB	-

STEP 2 To set up the grace period, and if the soft limit set for the user or group is still exceeded, the user or group is denied write access, enter the time period in the **Warn for <time period> before denying access** field. Enter the number in the first part of the field, and the time unit in the second part of the field. For example, to

warn the user or group that they have reached their soft limit and have three days to reduce it, enter "3" and then select "days". Normally, when the quota is under the limit, it appears in black type. When a user reaches their soft quota limit, the amount listed on **Filesystem Quota** page turns red.

STEP 3 Click **Update**.

STEP 4 Repeat steps 2 and 3 for each applicable volume.

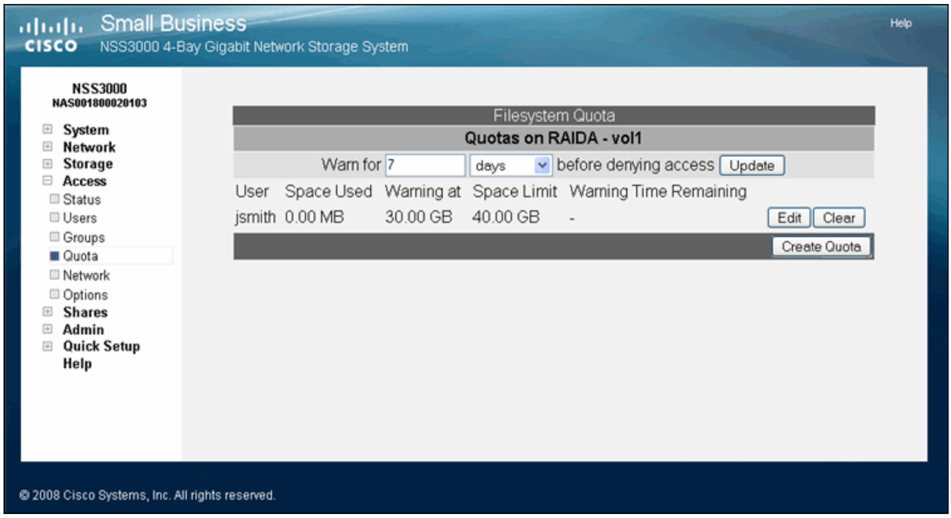
Changing a Volume Quota for a User or Group

After a quota is created, you can increase or decrease it. You can also change the limit at which the user or group receives a warning message and the grace period begins.

To change the quota limit or warning limit:

STEP 1 From the **Manager Menu**, click **Access** ➡ **Quota**.

The **Filesystem Quota** page appears.



Filesystem Quota

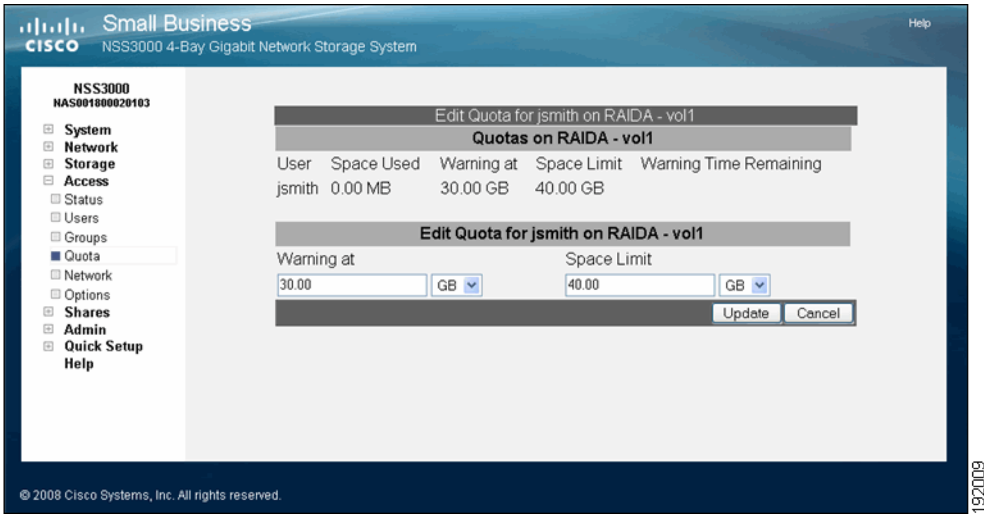
Quotas on RAIDA - vol1

Warn for 7 days before denying access

User	Space Used	Warning at	Space Limit	Warning Time Remaining
jsmith	0.00 MB	30.00 GB	40.00 GB	-

STEP 2 Click **Edit** for the user or group for which you want to change the quota.

The **Edit Quota** page appears.



Edit Quota for jsmith on RAIDA - vol1

Quotas on RAIDA - vol1

User	Space Used	Warning at	Space Limit	Warning Time Remaining
jsmith	0.00 MB	30.00 GB	40.00 GB	

Edit Quota for jsmith on RAIDA - vol1

Warning at: 30.00 GB

Space Limit: 40.00 GB

STEP 3 Make the required changes to the soft (warning) or hard quota (space limit) limits.

STEP 4 Click **Update**.

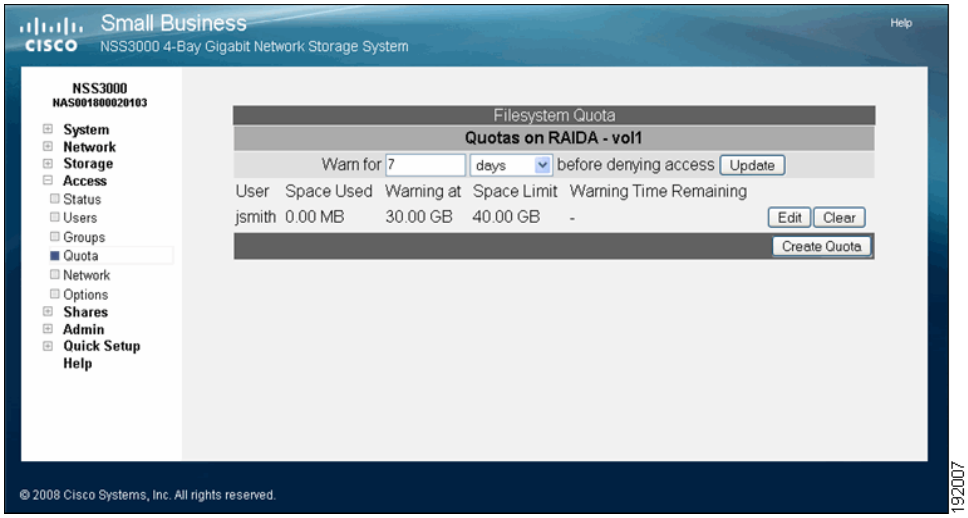
Clearing a Quota

After a quota has been set up, you can clear it. Clearing a quota means that the user or group no longer has a space limitation on their use of the associated volume (other than the actual unused storage space on the volume).

To clear a quota for a user or group:

STEP 1 From the **Manager Menu**, click **Access** ➔ **Quota**.

The **Filesystem Quota** page appears.



Filesystem Quota

Quotas on RAIDA - vol1

Warn for 7 days before denying access

User	Space Used	Warning at	Space Limit	Warning Time Remaining
jsmith	0.00 MB	30.00 GB	40.00 GB	-

Quotas are displayed according to their associated volume.

STEP 2 Click **Clear** for the user or group whose quota you want to remove.

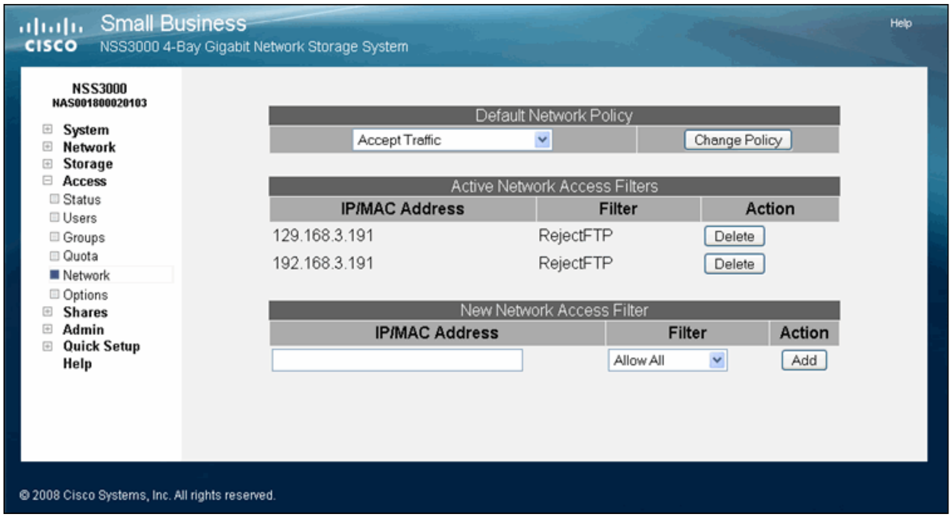
Network Filters Overview

In addition to providing storage for your data, the NSS provides a configurable firewall to protect that data. Defining network filters lets you specify which network hosts have access to the NSS through the various supported protocols.

To view the network filters:

STEP 1 From the **Manager Menu**, click **Access** ➜ **Network**.

The **Network Filters** page appears.



Default Network Policy

Accept Traffic

Active Network Access Filters

IP/MAC Address	Filter	Action
129.168.3.191	RejectFTP	Delete
192.168.3.191	RejectFTP	Delete

New Network Access Filter

IP/MAC Address	Filter	Action
	Allow All	Add

STEP 2 You can do any of the following:

- Set the **Default Network Policy** to control what happens to traffic not explicitly covered by defined filters. See "Defining the Default Network Policy" on page 21.
- View or delete the existing filters defined for the NSS from the **Active Network Access Filters** table. See "Network Filters Overview" on page 20.
- Create a new filter based on an **IP/MAC Address** or a range of IP addresses. See "Creating a Network Filter" on page 23.

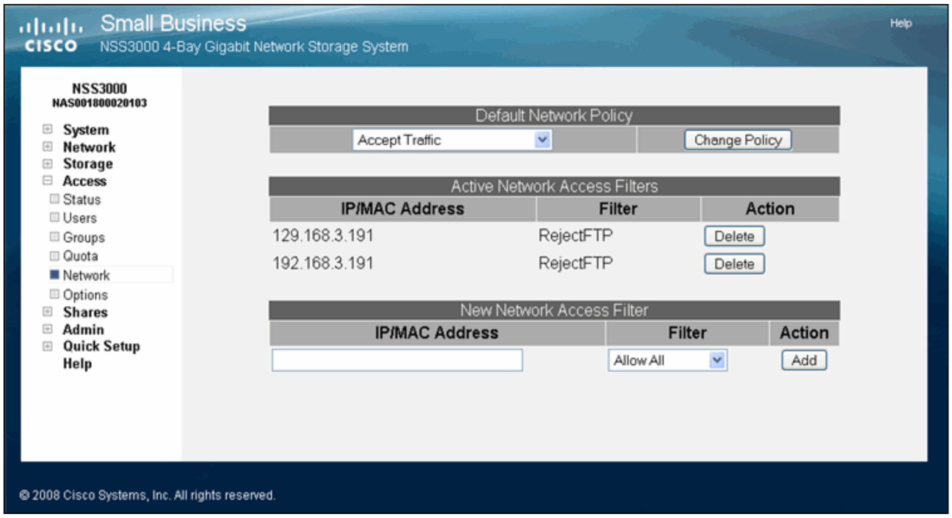
Defining the Default Network Policy

The default network policy is the policy that defines the gateway for communication to the NSS. It specifies how traffic that is not covered by defined filters is handled. The default policy can be defined to either accept or reject such traffic.

To define the default network policy:

STEP 1 From the **Manager Menu**, click **Access** ➡ **Network**.

The **Network Filters** page appears.



Default Network Policy: Accept Traffic

Active Network Access Filters

IP/MAC Address	Filter	Action
129.168.3.191	RejectFTP	Delete
192.168.3.191	RejectFTP	Delete

New Network Access Filter

IP/MAC Address	Filter	Action
	Allow All	Add

192004

STEP 2 From the **Default Network Policy** drop-down menu, click one of the following:

- **Accept Traffic**: Allow the NSS to communicate with all initiating hosts. Select this option if you have a limited number of systems that you want to disallow. When you set up your individual filters, select those filters that "disallow" (i.e., drop or reject) certain types of connections. For example, you might want to disallow CIFS connections but allow all other types.
- **Drop Traffic**: Disallow the NSS from communicating with any initiating systems. Select this option if you have a limited number of systems that you want to allow to communicate with the NSS. When you set up your filters, select those filters that "allow" certain types of connections. For example, you might only want to allow FTP connections.

NOTE If you set the default policy to **Drop** and you want to enable FTP connections, make sure you set the FTP connection type on the host to "active". (If you set the connection type to "passive" you can connect to the NSS but are not able to list, transfer the data, and so on.)

STEP 3 Click **Change Policy**.

Creating a Network Filter

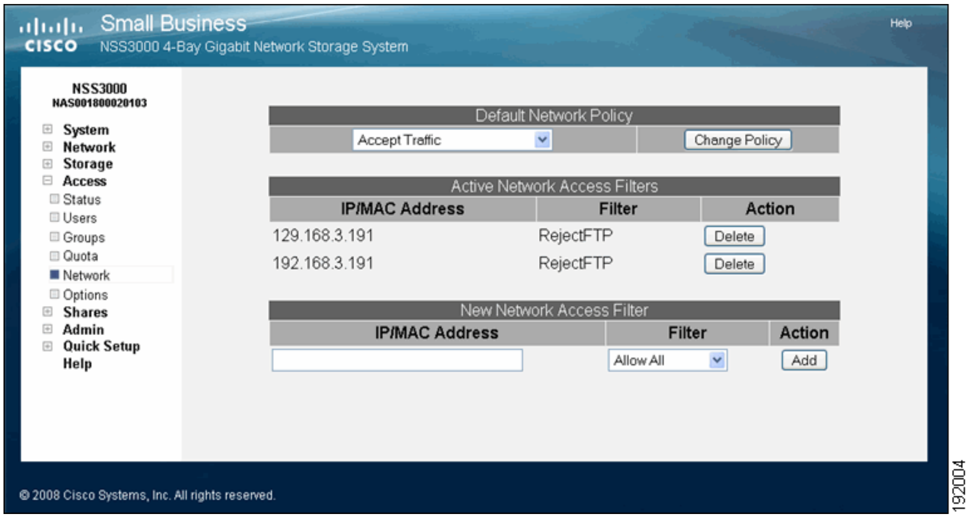
The **Active Network Access Filters** table on the **Network Filters** page displays currently defined filters. These filters control if access to the NSS from specified hosts is granted or denied on a per-protocol basis. Each device in your network is assigned a fixed 48-bit MAC address and changeable 32-bit IP address. When you define a filter, it grants or denies access through the specified protocol from the specified IP/MAC address or range of IP addresses.

NOTE When you define a new filter, any existing connections that would normally be denied by this rule remain in tact. These connections are denied during the next attempt to connect to the NSS.

To add a network filter:

STEP 1 From the **Manager Menu**, click **Access** ➔ **Network**.

The **Network Filters** page appears.



Default Network Policy: Accept Traffic

Active Network Access Filters

IP/MAC Address	Filter	Action
129.168.3.191	RejectFTP	Delete
192.168.3.191	RejectFTP	Delete

New Network Access Filter

IP/MAC Address	Filter	Action
	Allow All	Add

STEP 2 From the **New Network Access Filter** table, type the **IP/MAC address** to which you are applying the filter, in the **IP/MAC Address** field. You can also enter addresses for the following:

- **IP Address Range**: Type the range according to the following format: first address-last address. (Where the first IP address in the range is entered first, followed by a hyphen, and then the last IP address in the range.)
- **Subnet**: Enter the subnet to set a filter for all the addresses within the subnet. The format should appear as shown in the following example: 192.168.1.0/24 (where the digits following the slash represent the number of bits in the network portion of the IP address).

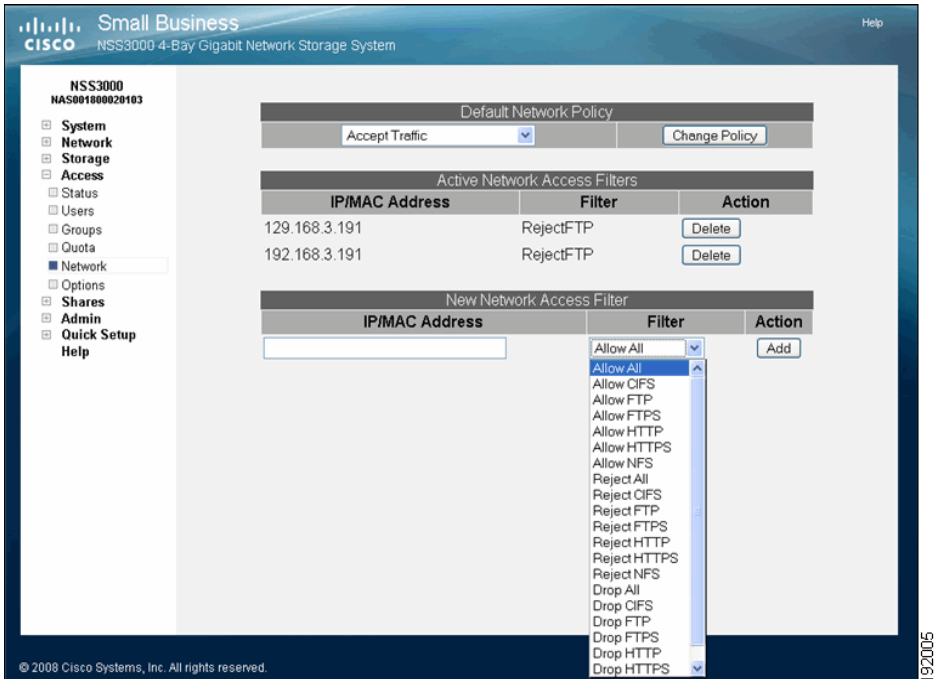
STEP 3 From the **Filter** drop-down menu, select the type of filter you want to apply to the IP/MAC address.

STEP 4 Click **Add**.

Any connections that apply to the new filter rule are affected by the rule during the next connection attempt.

Available Access Filters

When you configure network filters, determine which protocols can or cannot access the NSS. To display the list of available filters, click the drop-down arrow next to the **Filter** field on the **Network Filters** page.



Active Network Access Filters

IP/MAC Address	Filter	Action
129.168.3.191	RejectFTP	Delete
192.168.3.191	RejectFTP	Delete

NOTE **Rejecting versus Dropping Traffic**: When incoming traffic matches a "reject" filter, the NSS drops the traffic and then sends a notice to the initiating system of the denial of service. When incoming traffic matches a "drop" filter, the NSS drops the traffic but no notice is sent to the initiating system.

- **Allow All**: This is the default filter. It tells the NSS to accept traffic through all supported protocols.
- **Allow CIFS**: Allow CIFS filesharing access.
- **Allow FTP**: Allow FTP access.
- **Allow FTPS**: Allow FTPS access.
- **Allow HTTP**: Allow access to the NSS configuration interface through a Web browser through HTTP.
- **Allow HTTPS**: Allow access to the NSS configuration interface through a Web browser through HTTPS.
- **Allow NFS**: Allow NFS access.
- **Reject All**: Reject traffic through all supported protocols.
- **Reject CIFS**: Do not allow CIFS filesharing access. The NSS informs the system initiating the connection about the denial of service.
- **Reject FTP**: Do not allow FTP traffic. The NSS informs the system initiating the connection about the denial of service.
- **Reject FTPS**: Do not allow FTPS traffic. The NSS informs the system initiating the connection about the denial of service.
- **Reject HTTP**: Do not allow access to the NSS configuration interface through a Web browser through HTTP. The NSS informs the system initiating the connection about the denial of service.
- **Reject HTTPS**: Do not allow access to the NSS configuration interface through a Web browser through HTTPS. The NSS informs the system initiating the connection about the denial of service.
- **Reject NFS**: Do not allow NFS filesharing access. The NSS informs the system initiating the connection about the denial of service.

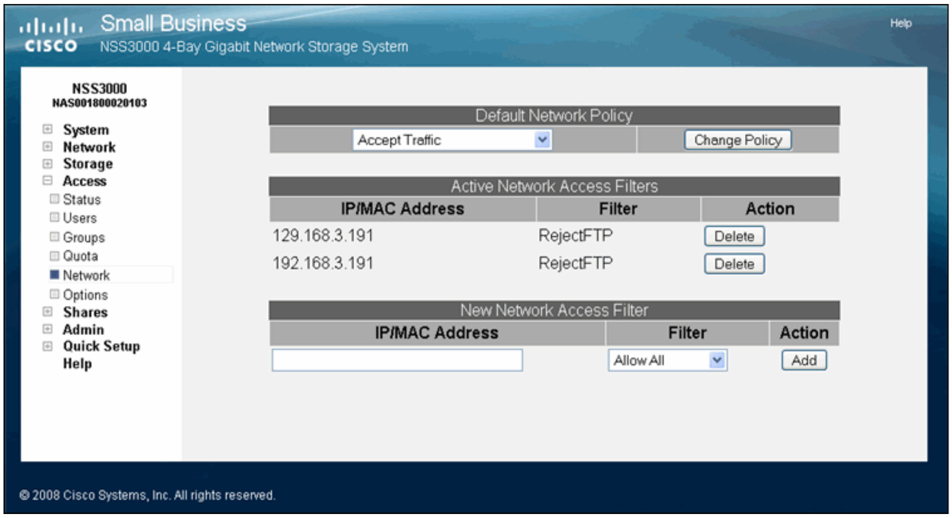
- **Drop All**: Do not allow access from any of the supported protocols. The NSS does not inform the system initiating the connection about the denial of service.
- **Drop CIFS**: Do not allow CIFS filesharing access. The NSS does not inform the system initiating the connection about the denial of service.
- **Drop FTP**: Do not allow FTP traffic. The NSS does not inform the system initiating the connection about the denial of service.
- **Drop FTPS**: Do not allow FTPS traffic. The NSS does not inform the system initiating the connection about the denial of service.
- **Drop HTTP**: Do not allow access to the NSS configuration interface through a Web browser through HTTP. The NSS does not inform the system initiating the connection about the denial of service.
- **Drop HTTPS**: Do not allow access to the NSS configuration interface through a Web browser through HTTPS. The NSS does not inform the system initiating the connection about the denial of service.
- **Drop NFS**: Do not allow NFS filesharing access. The NSS does not inform the system initiating the connection about the denial of service.

Deleting a Network Filter

To delete a network filter:

STEP 1 From the **Manager Menu**, click **Access** ➡ **Network**.

The **Network Filters** page appears.



Default Network Policy

Accept Traffic	Change Policy

Active Network Access Filters

IP/MAC Address	Filter	Action
129.168.3.191	RejectFTP	Delete
192.168.3.191	RejectFTP	Delete

New Network Access Filter

IP/MAC Address	Filter	Action
	Allow All	Add

STEP 2 The **Active Network Access Filters** table lists the existing filters. To delete a filter, click **Delete** for the filter you want to remove.

The filter disappears from the list. The filter is no longer active.

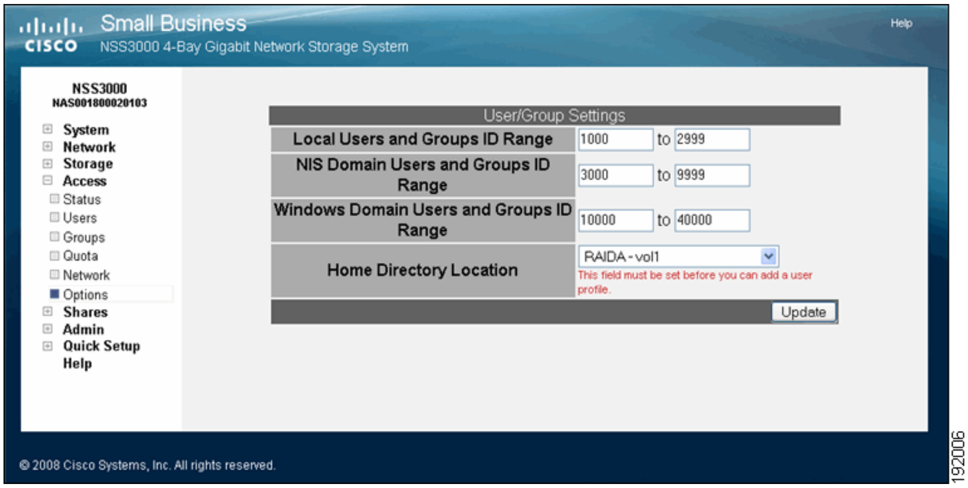
Configuring the User/Group Ranges and Home Directory Location

To avoid conflicts between your user and group IDs, it is important to set up the ranges for the various types of users and groups (i.e., local, NIS domain, and Windows domain). The ID range should be set up before you create any local users or join a NIS, NTv4, or ADS domain as you should not change the range after the domain has been joined. In addition to setting the ID ranges, you also need to define which volume you are using to store your users' home directories.

To set up the ID ranges and home directory location:

STEP 1 From the **Manager Menu**, click **Access** ➡ **Options**.

The **User/Group Settings** page appears.



User/Group Settings

Local Users and Groups ID Range	1000 to 2999
NIS Domain Users and Groups ID Range	3000 to 9999
Windows Domain Users and Groups ID Range	10000 to 40000
Home Directory Location	RAIDA - vol1 This field must be set before you can add a user profile.

STEP 2 Set up the following ID Ranges:

- **Local Users and Groups ID Range**: This ID range applies to any users or groups created from the NSS configuration interface. When you create a user or group, the ID assigned is in this range. Make sure the range you set does not conflict with the NIS or Windows domain ranges.
- **NIS Domain Users and Groups ID Range**: This ID range should match the range of IDs defined in your NIS domain and not conflict with the local or Windows ID range. Set this range before you join the NSS to the NIS domain.
- **Windows Domain Users and Groups ID Range**: This ID range must be at least 10,000 in size. Users and groups from your NTv4 and ADS domain are mapped to local user or group IDs within this range. It is important to set this range before you join the NTv4 or ADS domain. After you join the NTv4 or ADS domain, the ID range should not change.

STEP 3 Set the volume that you want to assign as the home directory location for your users through the **Home Directory Location** field. The hostname must start with a letter (it can be any character after that) and be a minimum of one character (no maximum).

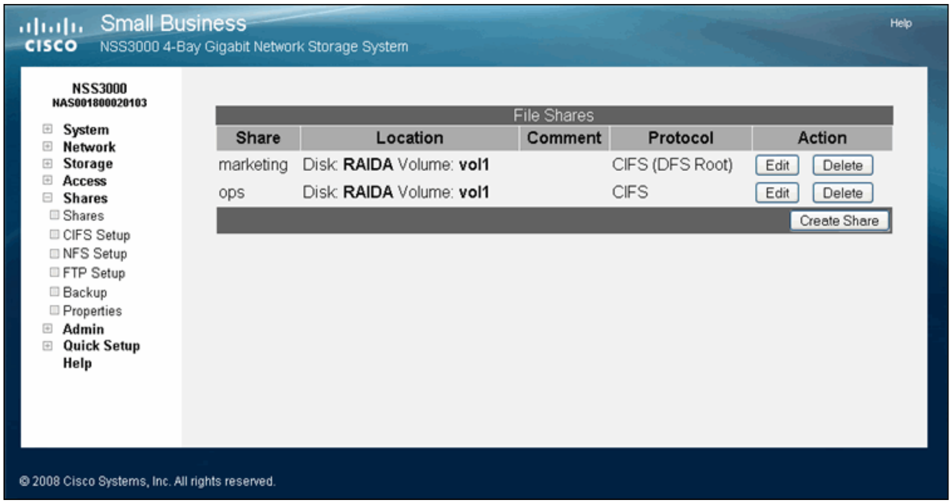
STEP 4 Click **Update**.

6

Managing the Shares

To display a list of your defined file shares, from the **Manager Menu,** click **Shares ➡ Shares**. The **File Shares** page displays read-only details about the shares currently defined on the NSS. You can add new shares by clicking the **Create Share** button.

There is a limit of 21 users and groups (the combined total) that you can assign access privileges to a share. If you have a number of users that exceeds the limitation, assign the applicable users to a group or groups and then assign the group to the share. There is no limit to the number of users that you can assign to an individual group.



File Shares

Share	Location	Comment	Protocol	Action
marketing	Disk: **RAIDA** Volume: **vol1**		CIFS (DFS Root)	Edit Delete
ops	Disk: **RAIDA** Volume: **vol1**		CIFS	Edit Delete

Create Share

192047

Creating a Share

After you define at least one volume, you can create the shares that can be accessed by your users when they log into the NSS. There is a limit of 21 users and groups (the combined total) that you can assign access privileges to a share. If you have a number of users that exceeds the limitation, assign the applicable users to a group or groups and then assign the group to the share. There is no limit to the number of users that you can assign to an individual group.

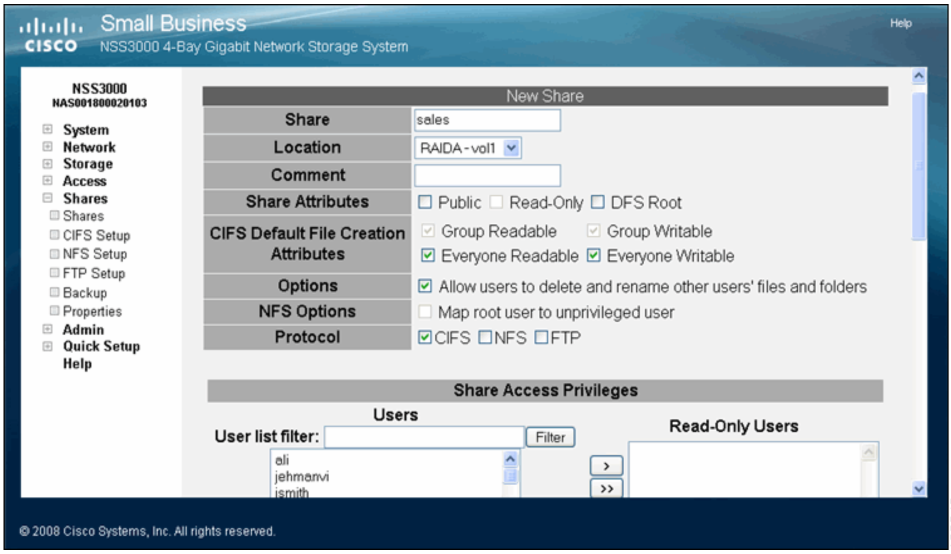
NOTE You cannot create a share on a locked volume. If the volume is locked, go to the Volume page, and unlock the volume.

To add a share:

STEP 1 From the **Manager Menu**, click **Shares** ➡ **Shares**.

STEP 2 Click **Create Share**.

The **New Share** page appears.



New Share

Share	sales
Location	RAIDA - vol1
Comment	
Share Attributes	□ Public □ Read-Only □ DFS Root
CIFS Default File Creation Attributes	☑ Group Readable ☑ Group Writable ☑ Everyone Readable ☑ Everyone Writable
Options	☑ Allow users to delete and rename other users' files and folders
NFS Options	□ Map root user to unprivileged user
Protocol	☑ CIFS □ NFS □ FTP

Share Access Privileges

Users

User list filter:

ali
jehmanvi
jsmith

Read-Only Users

© 2008 Cisco Systems, Inc. All rights reserved.

STEP 3 In the **Share** field, enter a name for the share.

STEP 4 From the **Location** field, select the volume on which you want to configure the share.

STEP 5 Add a description or comment about the share in the **Comment** field. This comment appears when you browse the NSS from My Network Places (as the tooltip when you hover over the share, or if you select the **Details viewing** mode). This field is optional.

STEP 6 Click the **Share Attributes** options to configure the share as public and if public, read-only. (These settings are optional.)

- **Public**: Enable all users to access the share.
  - To make an NFS share world readable/writable, select this checkbox, and verify that the Read-Only checkbox is also deselected.
  - To make an NFS share world readable, select this checkbox, and verify that the Read-Only checkbox is selected.
- **Read-Only**: If the share is configured as a public share, allow the users read-only access to the share. Users can access and view the share but cannot write to the share. (For NFS shares, see to the information in the **Public** field.)
- **DFS Root:** Set the share to be a Microsoft DFS root. Note: The share must be set as a DFS root when it is created. You cannot set it as a DFS root after it is created or revert a DFS root share to be a regular share. When you set this option, the **CIFS Default File Creation Attributes** and **Protocol** checkboxes are greyed out as they are not relevant. To add shared folder links to the root. See ”Adding a DFS Shared Folder” on page 37.

STEP 7 Set up the defaults for how file permissions are set when a file is created using CIFS through these **CIFS File Creation Attributes** checkboxes:

- **Group Readable**: Members of the group assigned to the file have read permission. The group is assigned during file creation. For files created through NFS, the owner can manually set the group permissions when the file is created and can edit them at a later time. For files created through CIFS, the group is automatically assigned as the owner’s default group. This group cannot be edited at a later time.
- **Group Writable**: Members of the group assigned to the file have write permission. The group is assigned during file creation. For files created through NFS, the owner can manually set the group permissions when the file is created and can edit them at a later time. For files created through CIFS, the group is automatically assigned as the owner’s default group. This group cannot be edited at a later time.

- **Everyone Readable**: All authenticated users can view the file.
- **Everyone Writable**: All authenticated users have write permission to the file.

STEP 8 From the **Options** field, set the **Allow users to delete or rename other users' files and folders** checkbox as required. This field determines whether users who are assigned to a share can delete or rename files or folders within that share that they do not own.

It is important to consider interoperability with applications such as MS Word 2007 and Photoshop. For example, if this field is not selected and you gave a user write permissions to a file and that user tried to open, edit, and save the file, the save would fail because Word sets up a temporary file and then attempts to delete it and replace it with the new version. Not all applications work this way. It is important to consider the applications used by your users to determine how you want to set this field.

- **Select this field**: By selecting this field, users with write permissions can rename or delete files or folders within the assigned share even though they are not the owners of the files or folders.
- **Deselect this field:** Users cannot rename or delete a file or folder within the assigned share unless they are the owners of the file or folder.

NOTE Any subfolders created through CIFS behave according to the current setting of the Allow users to delete or rename other users' files or folders field. If a subfolder is created through NFS or FTP, it behaves as though this field is selected until this field is changed. These subfolders then behave according to the current setting.

STEP 9 From the **Protocol** field, click the checkboxes to select the protocols that can be used to access the share:

- **CIFS**: Enable CIFS access to the share.
- **NFS**: Enable NFS access to the share. (To allow NFS access to the share, the NSS must also be configured to allow NFS access.)
- **FTP**: Enable FTP access to the share. (To allow FTP access to the share, the NSS must also be configured to allow FTP access.)

STEP 10 To assign users access to the share, move the users into one of the following boxes. (The single angled bracket "<" or ">" moves the selection in the direction of the bracket. The double angled bracket "<<" or ">>" moves the entire list in the direction of the bracket.) To limit the entries in the **Users** list, enter the desired search string in the **User List Filter** field, and then click **Filter**.

NOTE Setting individual user and group permissions on NFS shares only works when joined to an NIS domain.

- **Read-Only Users**: These users have read-only access to the share.
- **Read-Write Users**: These users have full read-write access to the share.

STEP 11 To assign a group access to the share, move the users into one of the following boxes. (The single angled bracket "<" or ">" moves the selection in the direction of the bracket. The double angled bracket "<<" or ">>" moves the entire list in the direction of the bracket.) To limit the entries in the **Groups** list, perform a substring search by entering the desired search string in the **Group List Filter** field, and then clicking Filter. (For example, enter "ea" to display any list items that contain "ea" such as "Sean" or "BillyJean".)

- **Read-Only Groups**: These groups have read-only access to the share.
- **Read-Write Groups**: These groups have full read-write access to the share.

STEP 12 Click **OK**.

Editing an Existing Share

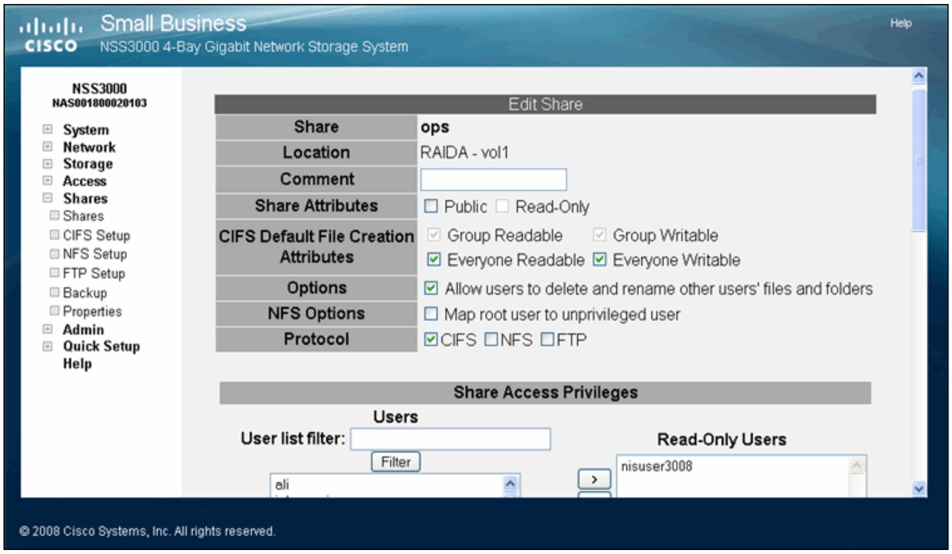
After a share is created, you can make changes to it, such as changing user or group permissions, changing the share attributes, and adding a DFS shared folder for shares set up to be a DFS root. There is a limit of 21 users and groups (the combined total) that you can assign access privileges to a share. If you have a number of users that exceeds the limitation, assign the applicable users to a group or groups and then assign the group to the share. There is no limit to the number of users that you can assign to an individual group.

To edit a share:

STEP 1 From the **Manager Menu**, click **Shares** ➜ **Shares**.

STEP 2 Click **Edit** for the share you want to change.

The **Edit Share** page appears.



Edit Share

Share	ops
Location	RAIDA - vol1
Comment	
Share Attributes	□ Public □ Read-Only
CIFS Default File Creation Attributes	☑ Group Readable ☑ Group Writable ☑ Everyone Readable ☑ Everyone Writable
Options	☑ Allow users to delete and rename other users' files and folders
NFS Options	□ Map root user to unprivileged user
Protocol	☑CIFS □NFS □FTP

Share Access Privileges

Users

User list filter:

Filter

ali

Read-Only Users

nisuser3008

STEP 3 You can change the comment from the **Comment field** as required. This comment appears when you browse the NSS from My Network Places (as the tooltip when you hover over the share, or if you select the **Details viewing** mode).

STEP 4 Change the setting for the **Allow users to delete or rename other users' files and folders** field as required. This field determines whether users who are assigned to a share can delete or rename files or folders within that share that they do not own.

It is important to consider interoperability with applications such as MS Word 2007 and Photoshop. For example, if this field is not selected and you gave a user write permissions to a file and that user tried to open, edit, and save the file, the save would fail because Word sets up a temporary file and then attempts to delete it and replace it with the new version. Not all applications work this way. It is important to consider the applications used by your users to determine how you want to set this field.

- **Select this field**: By selecting this field, users with write permissions can rename or delete files or folders within the assigned share even though they are not the owners of the files or folders.

- **Deselect this field**: Users cannot rename or delete a file or folder within the assigned share unless they are the owners of the file or folder.

NOTE Any subfolders created through CIFS behave according to the current setting of the Allow users to delete or rename other users' files or folders field. If a subfolder is created through NFS or FTP, it behaves as though this field is selected until this field is changed. These subfolders then behave according to the current setting.

STEP 5 The **Share attributes** checkbox determines if the share is read-only or if users can write to the share:

- **Public**: All users can write to the share.
- **Read-Only**: Users can view the share as read-only.

STEP 6 Set up the defaults for how file permissions are set when the file is created in the following **CIFS File Creation Attributes** checkboxes:

- **Group Readable**: Members of the group assigned to the file have read-only permissions. The group is assigned during file creation. For NFS files, the owner can manually set the group permissions when the file is created and can edit them at a later time. For CIFS files, the group is automatically assigned as the owner's default group. This group cannot be edited at a later time.
- **Group Writable**: Members of the group assigned to the file have read-write permissions. The group is assigned during file creation. For NFS files, the owner can edit the group ownership of a file. For files created through CIFS, the group is automatically assigned as the owner's default group. This group cannot be edited at a later time.
- **Everyone Readable**: All authenticated users can view the file.
- **Everyone Writable**: All authenticated users have read-write permissions for the file.

STEP 7 From the **Protocol** field, click the checkboxes to select the protocols that can be used to access the share:

- **CIFS**: Enable CIFS access the share.
- **NFS**: Enable NFS access the share. (To allow NFS access to the share, the NSS must also be configured to allow NFS access.)

- **FTP**: Enable FTP access to the share. (To allow FTP access to the share, the NSS must also be configured to allow NFS access.)

STEP 8 Move any usernames that you want to have access to the share from the **User** list into one of the following boxes. (The single angled bracket "<" or ">" moves the selection in the direction of the bracket. The double angled bracket "<<" or ">>" moves the entire list in the direction of the bracket.) To limit the entries in the **Users** list, perform a substring search by entering the desired search string in the User List Filter field, and then clicking Filter. (For example, enter "ea" to display any list items that contain "ea" such as "Sean" or "BillyJean".)

- **Read-Only Users**: Usernames that appear in this list have read-only access to the share.
- **Read-Write Users**: Usernames that appear in this list have read-write access to the share.

STEP 9 Use the last two tables in the window to set up your group permissions for the share. Move any groups that you want to have access to the share from the left side of the page into one of the following. (The single angled bracket "<" or ">" moves the selection in the direction of the bracket. The double angled bracket "<<" or ">>" moves the entire list in the direction of the bracket.) To limit the entries in the **Groups** list, enter the desired search string in the **Group List Filter** field, and then click **Filter**.

- **Read-Only Groups**: Groups that appear in this list have read-only access to the share.
- **Read-Write Groups**: Groups that appear in this list have full read-write access to the share.

STEP 10 Click **OK**.

Adding a DFS Shared Folder

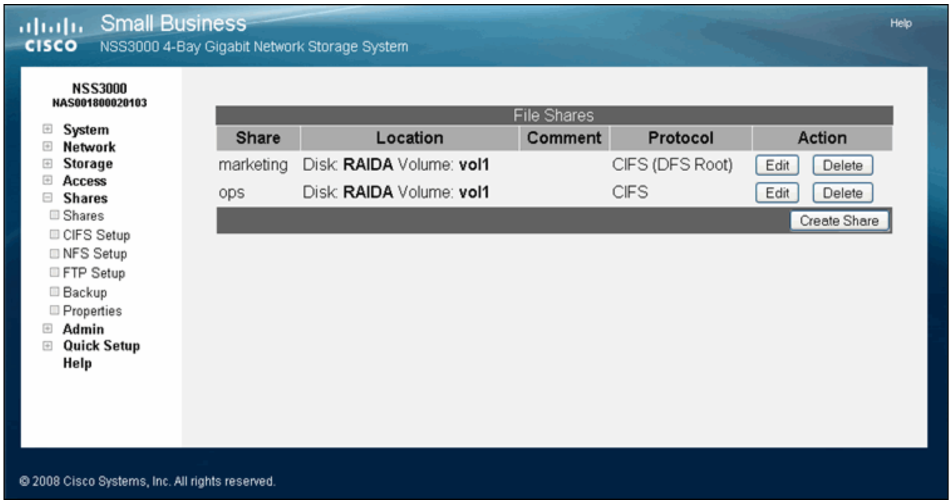
Microsoft DFS lets users within your network easily access data stored on multiple remote computers. Through DFS, your users can view and access shares through a familiar, unified folder hierarchy, even when those resources are located on different servers. The NSS can act as a DFS root or leaf. When acting as a root, the share on the NSS contains subfolders that link to the various shares on remote systems, referred to as "DFS shared folders". When you create a DFS shared folder from a share, the user must have privileges set up to access that share on the remote system. After the user accesses the DFS shared folder through the NSS DFS root share, the user's rights to the DFS shared folder are those assigned to the corresponding target share on the remote system.

To add a DFS root directory to a share that has been set as a DFS root on the NSS:

STEP 1 Make sure that the share is created with the **DFS Root** option selected. You cannot set a share as a DFS root after it has been created. For more information, see "Creating a Share" on page 30.

STEP 2 From the **Manager Menu**, click **Shares** ➡ **Shares**.

The **File Shares** page appears.

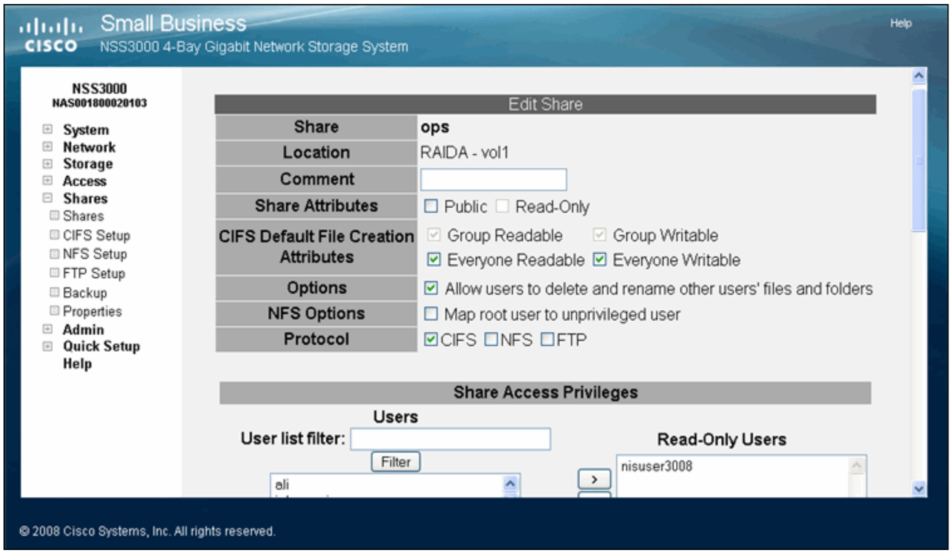


File Shares

Share	Location	Comment	Protocol	Action
marketing	Disk: **RAIDA** Volume: **vol1**		CIFS (DFS Root)	Edit Delete
ops	Disk: **RAIDA** Volume: **vol1**		CIFS	Edit Delete

STEP 3 Click **Edit** for the share to which you want to add a folder.

The **Edit Share** page appears.



Edit Share

Share	ops
Location	RAIDA - vol1
Comment	
Share Attributes	□ Public □ Read-Only
CIFS Default File Creation Attributes	☑ Group Readable ☑ Group Writable ☑ Everyone Readable ☑ Everyone Writable
Options	☑ Allow users to delete and rename other users' files and folders
NFS Options	□ Map root user to unprivileged user
Protocol	☑CIFS □NFS □FTP

Share Access Privileges

Users

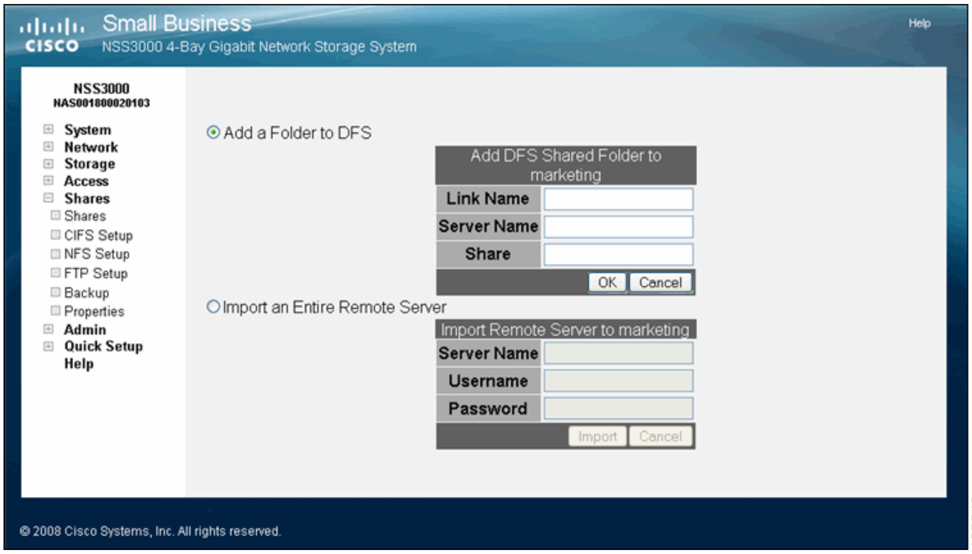
User list filter:

Read-Only Users

ali

nisuser3008

STEP 4 Click **Add Shared Folder.**



● Add a Folder to DFS

Add DFS Shared Folder to marketing

Link Name	
Server Name	
Share	

○ Import an Entire Remote Server

Import Remote Server to marketing

Server Name	
Username	
Password	

STEP 5 Select one of the following:

- **Add a Folder to DFS**: Select this option to create a single DFS shared folder. Fill in the following fields from the **Add DFS Shared Folder** table:
  - **Link Name**: This is the name of the link that appears as a folder within the share. When users click this link, they are redirected to the target share on the remote server. Enter any name of up to 255 characters.
  - **Server Name**: Enter the name of the remote server on which the target share is located.
  - **Share**: Enter the name of the target share.
- **Import an Entire Remote Server**: Select this option to automatically create links for all shares on the remote server. Fill in the following fields from the **Import Remote Server** table:
  - **Server Name**: Enter the name of the remote server.
  - **Username**: Enter the username of the account with access to the server.
  - **Password**: Enter the password for the above account.

STEP 6 If you are adding a folder to DFS, click **OK**. If you are importing a remote server, click Import.

NOTE Make sure that you review the restrictions and recommendations for using Microsoft DFS from the NSS.

Restrictions using Microsoft DFS from the NSS

To use DFS folders from the NSS, it is important to understand the limitations or restrictions involved and how to best configure your system:

- **User Credentials must be Recognized by the Remote Server**: Re-direction to a remote file-server is only successful if the current user credentials (i.e., the user's NSS username and password) are recognized by the remote server. Microsoft DFS (MSDFS) operates optimally if the PC-user's login username and password are recognized as valid on all file servers being accessed. Otherwise, an authentication error occurs and the user may not be able to re-authenticate with different user credentials. As a workaround in a non-domain (workgroup) environment, pre-map a file-share to each file server that needs special user credentials (other than the logged-in username and password). In this case, the MSDFS redirect proceeds smoothly because the PC-client already has an established session with the target file-server. When the user’s login is different on the DFS leaf than the DFS root, they can pre-login to the leaf. When they then login to the root, they can access the linked DFS share.

- **Windows Operating System Version**: MSDFS is not supported by Windows 98 clients.
- **Windows Clients must be Restarted**: After you set up a DFS root, any Windows clients that were connected must be restarted.

Setting up CIFS Access

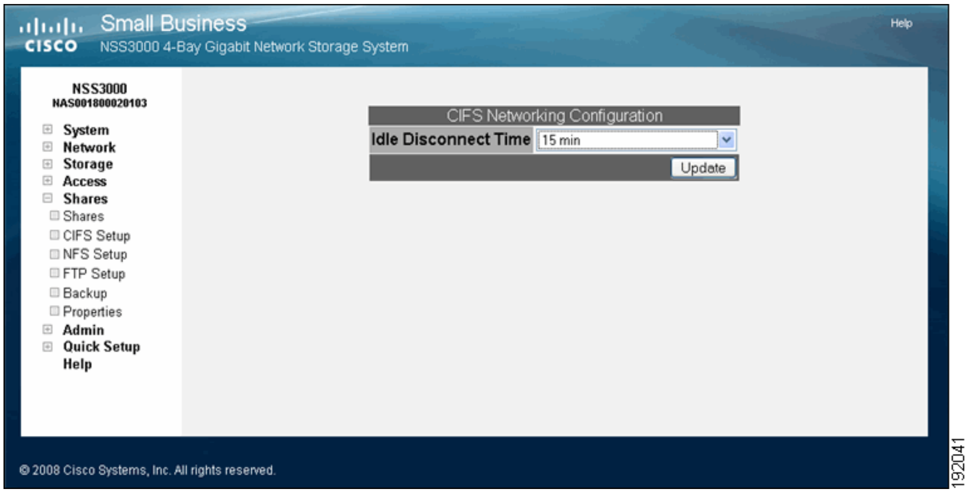
Although you cannot globally disable CIFS as you can for NFS and FTP, you can allow or disallow CIFS access on a per-share basis. The CIFS Networking Configuration page lets you specify the length of time CIFS connections to the NSS can be idle before being automatically disconnected.

NOTE The CIFS idle disconnect only works correctly for Windows and Linux clients. Mac clients are not disconnected despite being idle for more than the configured timeout.

To set up the idle disconnect time for a CIFS connection to the NSS:

STEP 1 From the **Manager Menu**, click **Shares** ➡ **CIFS Setup**.

The **CIFS Networking Configuration** page appears.



CIFS Networking Configuration

Idle Disconnect Time: 15 min

STEP 2 From the drop down box, select the amount of time that the CIFS connection can be idle, after which it is disconnected.

STEP 3 Click **Update**.

Setting up Network Filesystem (NFS) Access

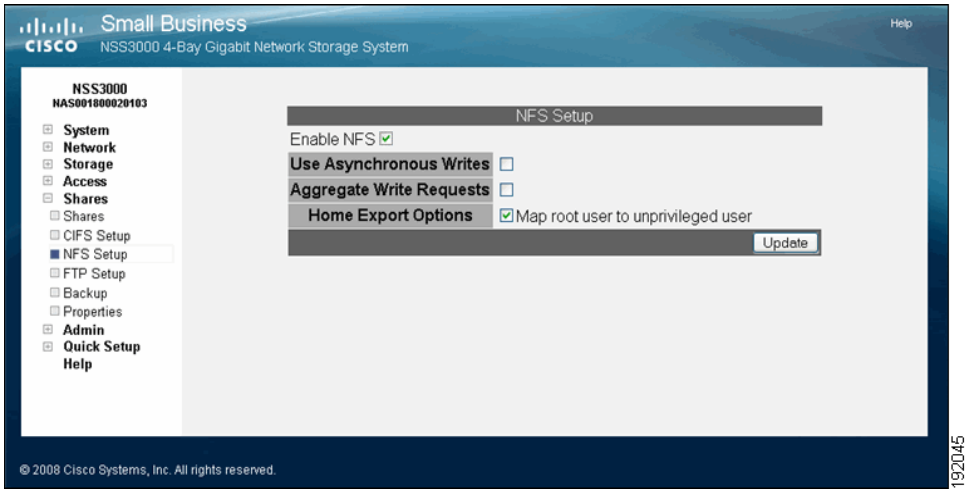
The first step to enable NFS access to the NSS is to enable it globally. You then need to enable it on a per-share basis.

NOTE The NSS only supports NFSv3.

To set up global NFS access to the NSS:

STEP 1 From the **Manager Menu**, click **Shares** ➜ **NFS Setup**.

The **NFS Setup** page appears.



NFS Setup

Enable NFS ☑

Use Asynchronous Writes □

Aggregate Write Requests □

Home Export Options ☑ Map root user to unprivileged user

Update

STEP 2 To enable NFS support, click **Enable NFS**. This checkbox activates the other NFS configuration options on this page.

STEP 3 To enable the optional asynchronous write option, click **Use Asynchronous Writes**. Asynchronous writes allow applications running on the NFS client to not block until write requests are complete on the NSS as they normally would. Instead they continue immediately after committing the write. This can improve performance if the NSS is heavily used.

STEP 4 If asynchronous writes is enabled, you can enable aggregate write requests by selecting **Aggregate Write Requests** checkbox. When enabled, NFS write requests are "bulked" and sent in a batch. When disabled, the write requests are sent immediately. The benefit of enabling this feature is that it is more efficient. The downside of enabling this feature is that there is a potential for permanent data loss should the NSS suffer an unexpected power loss or if the NFS client crashes.

STEP 5 Click **Update**.

Configuring the NSS for FTP Access

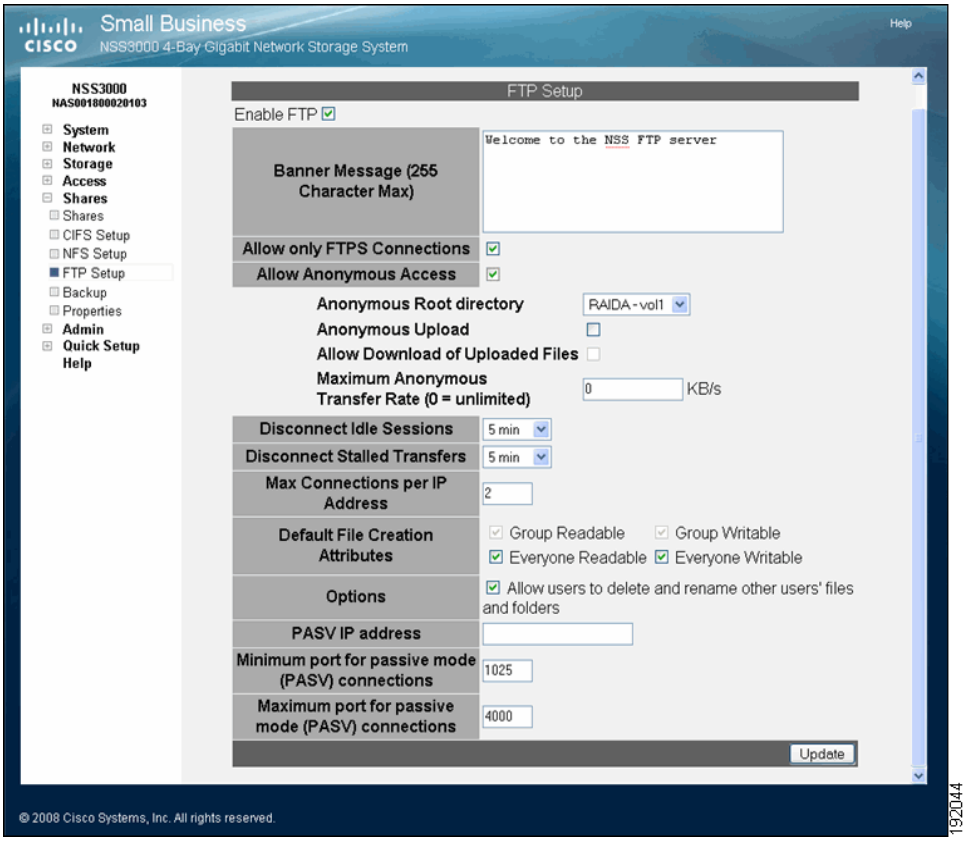
You can configure the NSS to allow the FTP protocol to be used for file transfers between the NSS over the Internet. The NSS supports both FTP (faster but not as secure) and FTPS (not as fast as FTP but more secure). Note that the NSS only supports Explicit FTPS (versus Implicit FTPS). The NSS does not support SFTP. After you globally enable FTP access, you can allow or disallow FTP access on a per-share basis.

NOTE The default setting is to disable FTP access. You must enable FTP access before your users can access the NSS storage through FTP regardless of their per-share settings.

To set up the FTP protocol:

STEP 1 From the **Manager Menu**, click **Shares** ➡ **FTP Setup**.

The **FTP Setup** page appears.



Enable FTP ☑

Banner Message (255 Character Max)	Welcome to the NSS FTP server
Allow only FTPS Connections	☑
Allow Anonymous Access	☑
Anonymous Root directory	RAIDA-vol1
Anonymous Upload	□
Allow Download of Uploaded Files	□
Maximum Anonymous Transfer Rate (0 = unlimited)	0 KB/s
Disconnect Idle Sessions	5 min
Disconnect Stalled Transfers	5 min
Max Connections per IP Address	2
Default File Creation Attributes	☑ Group Readable ☑ Group Writable ☑ Everyone Readable ☑ Everyone Writable
Options	☑ Allow users to delete and rename other users' files and folders
PASV IP address	
Minimum port for passive mode (PASV) connections	1025
Maximum port for passive mode (PASV) connections	4000

STEP 2 To enable FTP, click **Enable FTP**. This enables both FTP and FTPS access and activates the remaining FTP configuration settings on this page.

STEP 3 In the **Banner Message** box, enter a message that appears when a user first connects to the NSS.

STEP 4 To allow only file transfers using FTPS (FTP over SSL), click **Allow only FTPS Connections** (make sure the **Allow Anonymous Access** checkbox is deselected).

STEP 5 To allow anonymous FTP access, click **Allow Anonymous Access**.

STEP 6 If you allow anonymous access, select the volume that you want to set as the anonymous root directory from the **Anonymous Root Directory** drop-down menu.

STEP 7 To allow anonymous users to have write access to the NSS, click **Anonymous Upload**.

STEP 8 To allow anonymous users to download files that have been uploaded by other anonymous users, make sure the **Allow Download of Uploaded Files** checkbox is selected.

STEP 9 To set a maximum transfer rate for anonymous users, enter it in KB/s in the **Maximum Anonymous Transfer Rate** field. For no maximum, set the rate as 0.

STEP 10 To disconnect the FTP connection after a period of time when the connection is idle, select the number of minutes in the **Disconnect Idle Sessions** drop-down menu.

STEP 11 To disconnect an FTP connection after a certain length of time has passed during a file transfer, select the number of minutes in the **Disconnect Stalled Transfers** drop-down menu.

STEP 12 To set the maximum number of FTP connections that can be made from a single client IP address, enter the number in the **Max Connections per IP Address** field. (To leave this as an unlimited number of connections, leave this field blank.) The maximum FTP connections cannot exceed the maximum FTP connections allowed by the connection profile. See ”Configuring the Connection Profile” on page 51. For example, if you set the connection profile to Standard, the maximum FTP connections is two.

STEP 13 Set up the defaults for how file permissions are set when a file is created using **FTP through the following Default File Creation Attributes** checkboxes. Note that unlike CIFS permissions which are set on a share-by-share basis, the FTP permissions are global to all files and folders created through FTP regardless of the share to which they are assigned.

- **Group Readable**: Members of the user who created the file or folder’s primary group have read permission.
- **Group Writable**: Members of the user who created the file or folder’s primary group have write permission.
- **Everyone Readable**: All authenticated users can view the file.
- **Everyone Writable**: All authenticated users have write permission to the file.

STEP 14 Set the **Allow users to delete or rename other users’ files and folders** field as required. This field determines if users who have write permission to a share can delete or rename files or folders within that share that they do not own.

It is important to consider interoperability with applications such as MS Word 2007 and Photoshop. For example, if this field is not selected and you gave a user write permissions to a file and that user tried to open, edit, and save the file, the save would fail because Word sets up a temporary file and then attempts to delete it and replace it with the new version. Not all applications work this way. It is important to consider the applications used by your users to determine how you want to set this field.

- **Select this field**: By selecting this field, users with write permissions can rename or delete files or folders within the assigned share even though they are not the owners of the files or folders.
- **Deselect this field**: Users cannot rename or delete a file or folder within the assigned share unless they are the owners of the file or folder.

NOTE Unlike the setting on the **Shares Setup** page, this setting is global, not per share. All files within folders created through FTP act according to this setting, regardless of the share they are created in.

STEP 15 If you want clients to access the NSS through **Passive Mode FTP** through a firewall and/or router, enter the router's WAN IP address in the **PASV IP Address** field. Continue with the next step.

NOTE Passive Mode FTP through a router only works on a single interface. If you have VLANs defined, choose which interface to access through FTP.

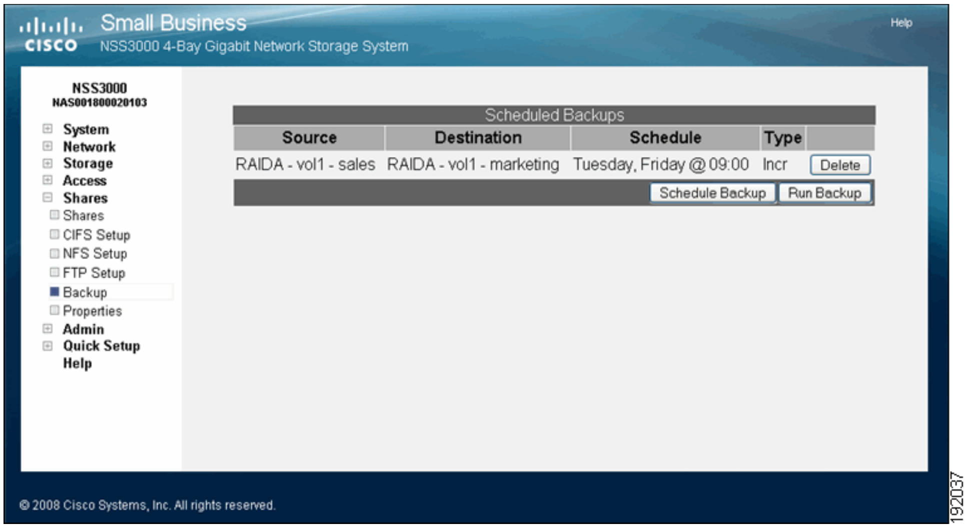
STEP 16 If you are setting up **Passive Mode FTP**, set up the passive mode range:

- **Minimum port for passive mode (PASV) connections**: If your network has FTP connections that pass through a firewall, set the minimum port for the port range. The default is 1025.
- **Maximum port for passive mode (PASV) connections**: Set the maximum port number for the port range. The default is 4000. Ensure your router is configured to forward the entire configured Passive Mode FTP port range to the NSS.

STEP 17 Click **Update**.

Creating or Running a Backup of a Share

The **Scheduled Backup** page displays any backups that have been configured. It lets you schedule further backups or initiate a manual backup.



Scheduled Backups

Source	Destination	Schedule	Type	
RAIDA - vol1 - sales	RAIDA - vol1 - marketing	Tuesday, Friday @ 09:00	Incr	Delete

Creating a Scheduled Backup for a Share

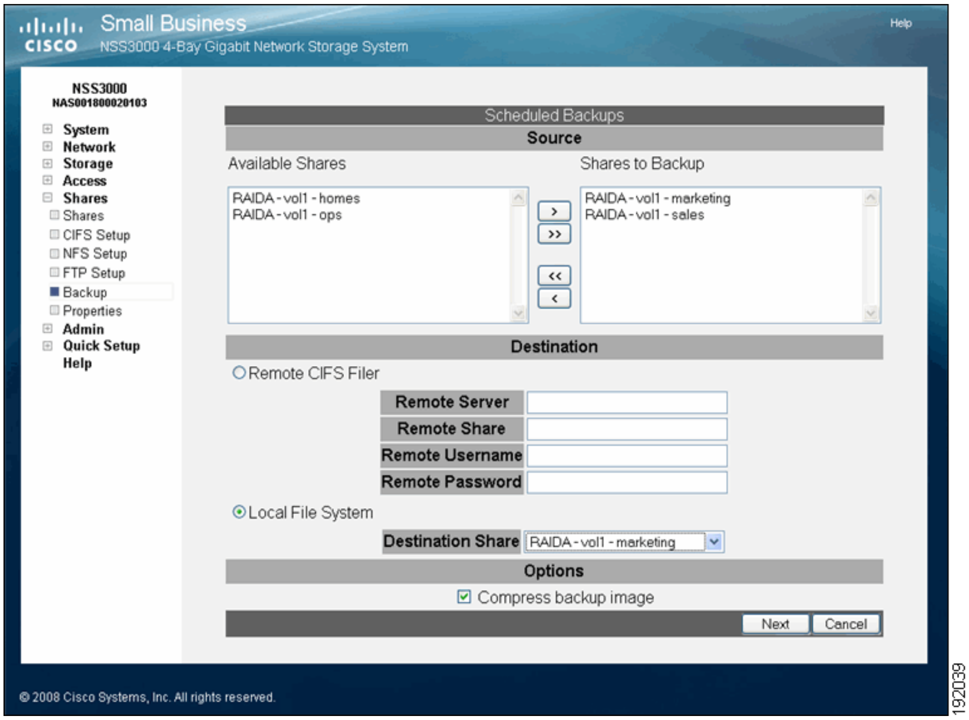
You can quickly configure a backup to run at a scheduled time interval for a share or group of shares. The backup can be saved to a remote CIFS server or to another share on the NSS.

To set up a scheduled backup:

STEP 1 From the **Manager Menu**, click **Shares** ➜ **Backup**.

STEP 2 Click **Schedule Backup**.

The **Scheduled Backups** page appears.



Scheduled Backups

Source

Available Shares	Shares to Backup
RAIDA - vol1 - homes RAIDA - vol1 - ops	RAIDA - vol1 - marketing RAIDA - vol1 - sales

Destination

○ Remote CIFS Filer

Remote Server	
Remote Share	
Remote Username	
Remote Password	

● Local File System

Destination Share: RAIDA - vol1 - marketing

Options

☑ Compress backup image

STEP 3 Move the shares you want to include in the backup from the **Available Shares** list to the **Shares to Backup** list. (The single angled bracket "<" or ">" moves the selection in the direction of the bracket. The double angled bracket "<<" or ">>" moves the entire list in the direction of the bracket.)

STEP 4 Click one of the following to determine the destination for the backup:

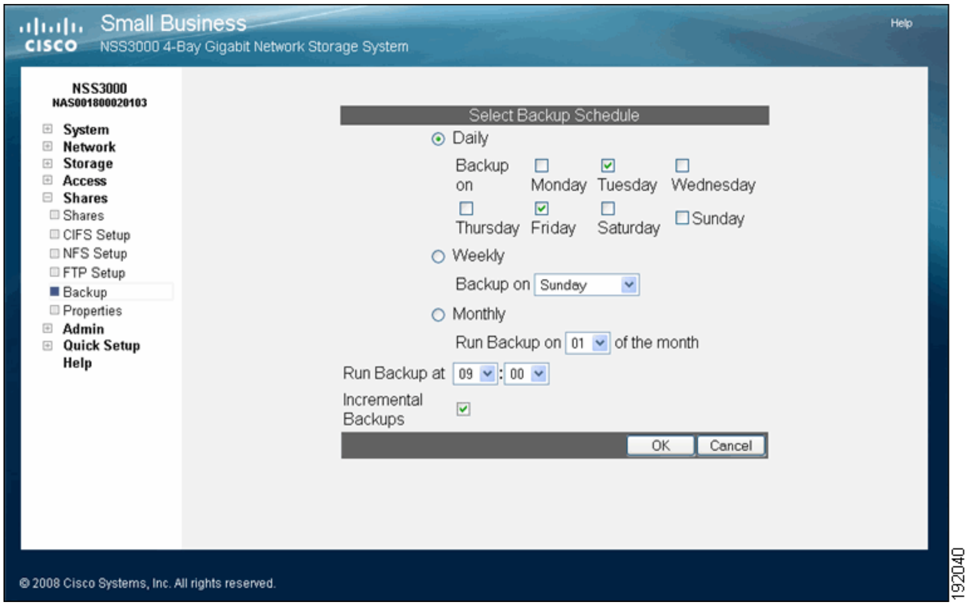
- **Remote CIFS Filer**: To save the backup on a remote CIFS server, click this option and then configure the hostname of the remote server, the remote share, as well as the login credentials to that share.
- **Local File System**: Select the share on which you want to store the backup.

STEP 5 To create a compressed backup, check **Compress backup image**.

Compressed backup images are smaller than non-compressed images but take longer to create.

STEP 6 Click **Next**.

The **Select Backup Schedule** page appears.



Select Backup Schedule

● Daily

Backup on ☐ Monday ☑ Tuesday ☐ Wednesday ☐ Thursday ☑ Friday ☐ Saturday ☐ Sunday

○ Weekly

Backup on Sunday

○ Monthly

Run Backup on 01 of the month

Run Backup at 09 : 00

Incremental Backups ☑

OK Cancel

STEP 7 Select the backup frequency as one of the following:

- **Daily**: Select each day on which you want the backup to occur.
- **Weekly**: Select the day of the week on which you want the backup to occur.
- **Monthly**: Select the day of the month on which you want the backup to occur. Make sure that you select a day that is 28 or less. If you select the 29th, 30th or 31st day, the backup does not run during months that do not contain that day.

STEP 8 In the **Run Backup at** field, set up the specific time (hour:minute) at which time the backup occurs. When setting the hour, use the 24-hour clock.

STEP 9 To set up a backup that backs up just the changes made to the share since the last backup, click **Incremental Backups**. Leave it unchecked to take a full backup of the share each time the backup is run.

STEP 10 Click **OK**.

Initiating a Backup for a Share

You can initiate a backup on a share or group of shares at any time. You can save the backup to a remote CIFS server or to another share on the NSS.

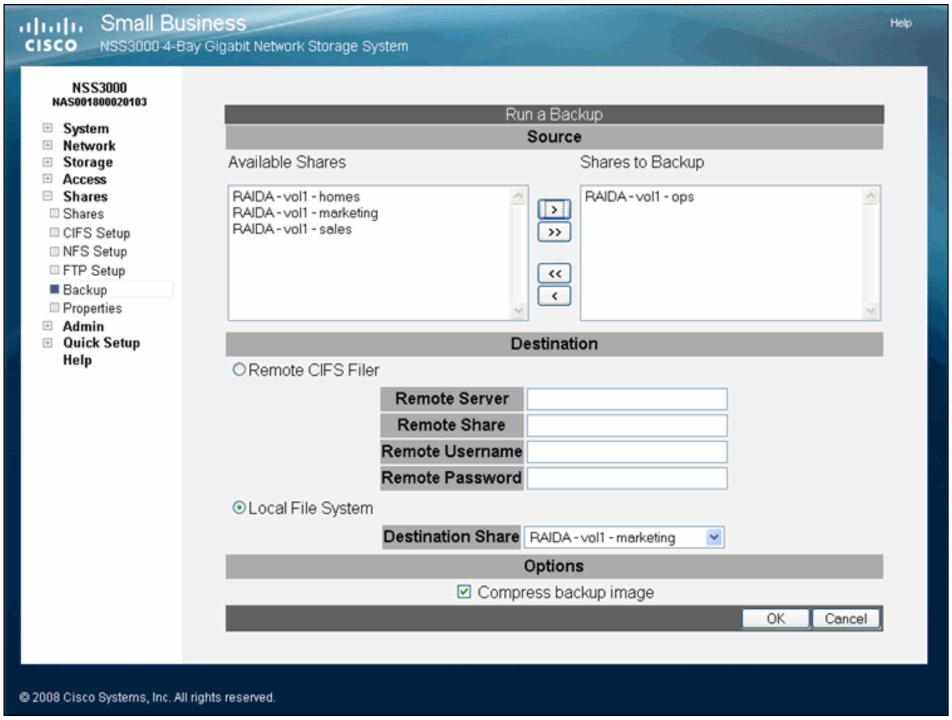
To initiate a backup manually:

STEP 1 From the **Manager Menu**, click **Shares** ➡ **Backup**.

The **Scheduled Backups** page appears.

STEP 2 Click **Run Backup**.

The **Run a Backup** page appears.



Run a Backup

Source

Available Shares: RAIDA - vol1 - homes, RAIDA - vol1 - marketing, RAIDA - vol1 - sales

Shares to Backup: RAIDA - vol1 - ops

Destination

○ Remote CIFS Filer

Remote Server	
Remote Share	
Remote Username	
Remote Password	

● Local File System

Destination Share: RAIDA - vol1 - marketing

Options

☑ Compress backup image

STEP 3 Move the shares you want to include in the backup from the **Available Shares** list to the **Shares to Backup** list. (The single angled bracket "<" or ">" moves the selection in the direction of the bracket. The double angled bracket "<<" or ">>" moves the entire list in the direction of the bracket.)

STEP 4 Click one of the following to determine the destination for the backup:

- **Remote CIFS Filer**: To save the backup on a remote CIFS server, click this option and then configure the hostname of the remote server, the remote share, as well as the login information to that share.
- **Local File System**: Select the share on which you want to store the backup.

STEP 5 To create a compressed backup, check **Compress backup image**.

NOTE Compressed backup images are smaller than non-compressed images but take longer to create.

STEP 6 Click **OK** to initiate the backup. A message appears when the backup is complete.

Deleting Backup Images

Each time the backup job runs for a CIFS share or group of CIFS shares, the backup image is saved to the local share (if configured for backups). To remove these images, you must have administrator privileges.

To delete a backup image from a local CIFS share:

STEP 1 Login to the share using the "admin" username together with the password configured for the administrator.

STEP 2 Go to the "backup" folder and delete the backup images (they appear as .tar.gz files) as required.

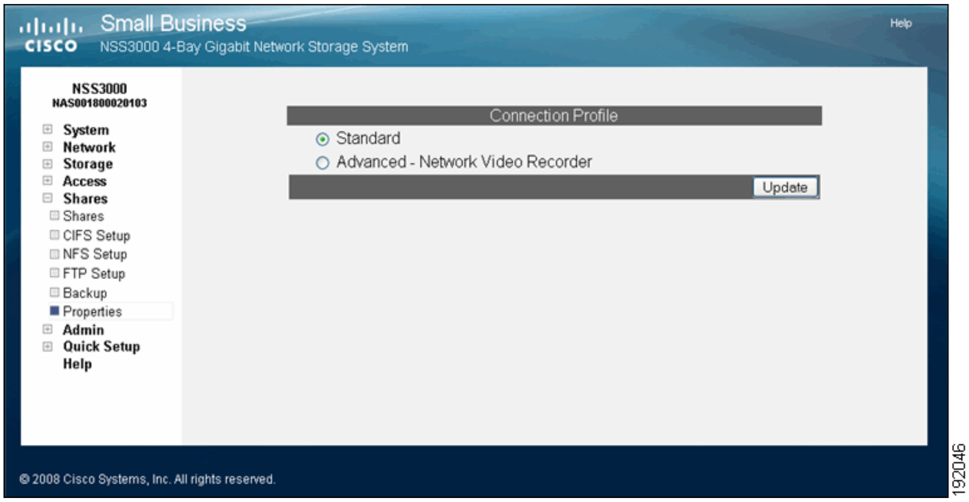
Configuring the Connection Profile

The NSS has a default connection profile (maximum number of simultaneous CIFS and FTP connections) that is appropriate for normal filesharing use. If you use the NSS primarily to store security images and have more than two IP cameras accessing the NSS at one time, you can set the connection profile to allow a greater number of simultaneous FTP connections and less simultaneous CIFS connections. The number of connections possible is different between the different NSS models.

To configure the connection profile:

STEP 1 From the **Manager Menu**, click **Shares ➜ Properties**.

The **Connection Profile** page appears.



Connection Profile

● Standard

○ Advanced - Network Video Recorder

Update

STEP 2 Select one of the following:

- **Standard**: This is the default setting. It allows up to 2 FTP and 15 CIFS simultaneous connections to the NSS.
- **Advanced - Network Video Recorder**: Select this option to allow up to 16 FTP and 8 CIFS simultaneous connections to the NSS.

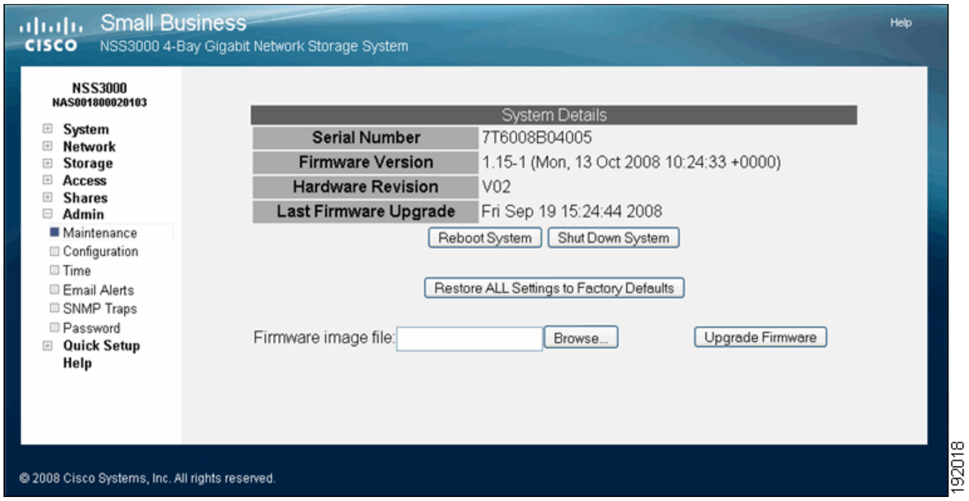
STEP 3 Click **Update**.

7

Managing the NSS

There are a number of maintenance tasks that you can do from the **System Details** page.

The LCDs on the front of the chassis lets you view the current time and date of the system, the firmware version and last upgrade date, and the status of the firmware upgrade.



System Details	
Serial Number	7T6008B04005
Firmware Version	1.15-1 (Mon, 13 Oct 2008 10:24:33 +0000)
Hardware Revision	V02
Last Firmware Upgrade	Fri Sep 19 15:24:44 2008

Firmware image file:

- Rebooting or Shutting down the system. See ”Rebooting or Shutting Down the NSS” on page 54.
- Upgrading the firmware. See ”Upgrading the NSS Firmware” on page 55.
- Restoring configuration settings to factory defaults. See ”Restoring the Factory Default Configuration” on page 57.

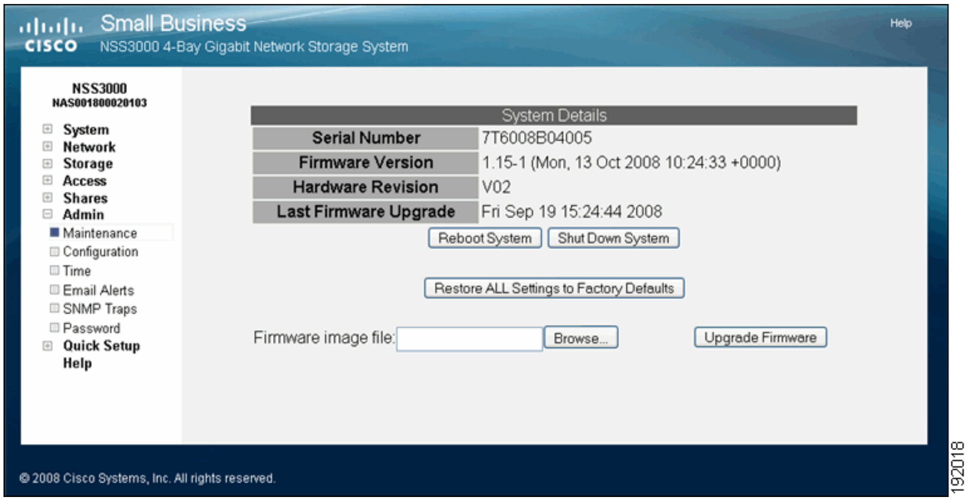
Rebooting or Shutting Down the NSS

In situations where you might need to reboot or shut down the NSS, doing so disconnects all active user sessions. If the power to the NSS is interrupted unexpectedly (i.e., an unclean shutdown), your system settings might become corrupted. It is highly recommended that you use a UPS to ensure that power to the NSS is never interrupted. See ”Handling an Unexpected (Unclean) Shutdown” on page 105. During a reboot or shutdown of the NSS, the color and blink rate of the Power LED on the front of the chassis indicates the status of the currently selected process.

To reboot or shut down the NSS:

STEP 1 From the **Manager Menu**, click **Admin** ➜ **Maintenance**.

The **System Details** page appears.



System Details	
Serial Number	7T6008B04005
Firmware Version	1.15-1 (Mon, 13 Oct 2008 10:24:33 +0000)
Hardware Revision	V02
Last Firmware Upgrade	Fri Sep 19 15:24:44 2008

STEP 2 Click one of the following:

- **Reboot System**: Power down and power up the system.

  Make sure that you close the Web browser when the system is rebooting. If you refresh the configuration interface Web page during the reboot process, the system inadvertently initiates another reboot.

- **Shut Down System**: This does a "clean" shutdown of the NSS. You can also shut down the NSS to:
  - **Restore the network setting system defaults**: You need to do this if the configuration interface becomes inaccessible. To reset the network setting system defaults, shut down the NSS, power it off, hold down the **Reset** button, and then power up the NSS. When you see the Power LED blink yellow rapidly, release the **Reset** button. The network settings are restored to factory defaults.
  - **Reset the box**: Press and hold the **Reset** button while the system is running until the PowerLED begins to blink green. Release the button.

A warning message appears.

STEP 3 Click **OK** to continue.

STEP 4 You can view the Power LED on the front of the chassis during the reboot or shutdown process. It changes to indicate the current status of the process. When the NSS is fully powered up, the Power LED is solid green. When the shutdown is complete, the Power LED is off. You need to unlock any encrypted volumes following any reboot or power up of the NSS.

Upgrading the NSS Firmware

Before you start the firmware upgrade, note the following:

- The firmware must be upgraded from an external source to the NSS. You cannot install firmware that is saved to a disk on the NSS. If a copy of the firmware is saved to a disk on the NSS, make sure you copy it to another location (such as onto a PC) before you attempt to upgrade it.
- The firmware must be compatible with the NSS platform.
- The firmware must be newer than the version currently installed. The system does not support downgrades.
- The firmware must be installed in a specific order if upgrading within a virtualized setup.

CAUTION When you upgrade the firmware, avoid using a wireless connection to the NSS. Wireless connections can sometimes be unreliable and cause image corruption. Do not interrupt the power during the firmware upgrade. The system reboots after the firmware upgrade is completed. Wait until the Power LED goes back to solid green before you log in and use the configuration interface.

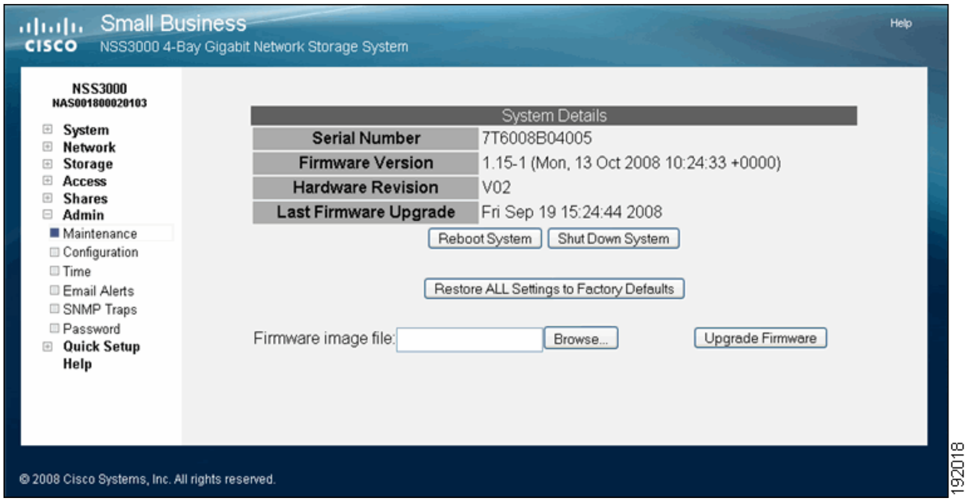
To upgrade the firmware:

STEP 1 Back up the system configuration file on a USB flash device before you upgrade the firmware. It is a good idea to back up the configuration file daily.

STEP 2 Download the latest image from the support website to your local computer.

STEP 3 From the **Manager Menu**, click **Admin** ➡ **Maintenance**.

The **System Details** page appears.



System Details

Serial Number	7T6008B04005
Firmware Version	1.15-1 (Mon, 13 Oct 2008 10:24:33 +0000)
Hardware Revision	V02
Last Firmware Upgrade	Fri Sep 19 15:24:44 2008

Firmware image file:

STEP 4 In the **Firmware image file:** field, either enter the location of the firmware file, or click **Browse** to locate it.

STEP 5 Click **Upgrade Firmware** to initiate the upgrade process. During the upgrade, the Power LED alternates from yellow to green. You can view the status of the firmware upgrade through the LCD on the front of the chassis.

STEP 6 When the firmware upgrade completes, the system automatically reboots. Wait until the Power Button LED is solid green before you log back into the configuration interface. If the upgrade is not successful, a message appears. (The Power Button LED appears solid yellow until you click **OK** after which the system reboots with the current version of the firmware.) For more information about the LED, see ”Power Button LED” on page 93.

STEP 7 After the firmware upgrade is complete, we recommend that you clear your browser cache before you reconnect to the administrator interface.

Restoring the Factory Default Configuration

There are two ways to restore configuration settings when you run into a problem with the NSS: preserve the specific storage configuration but restore everything else to factory defaults, or reset only the network settings so that you can log into the NSS configuration interface.

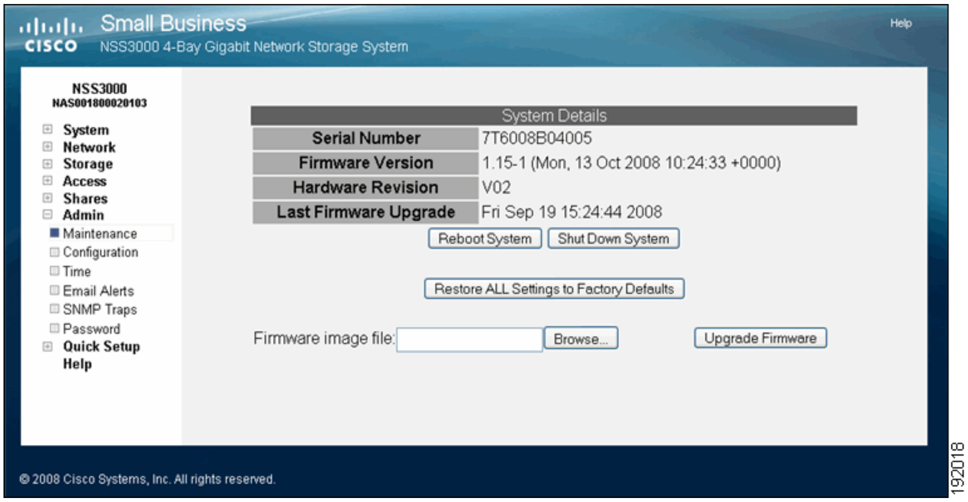
CAUTION If you restore the full factory defaults to an NSS in a virtualized setup, you will break any virtualized RAIDs.

To reset the NSS:

STEP 1 From the **Manager Menu**, click **Admin** ➔ **Maintenance**.

STEP 2 Depending on the nature of the problem, choose one of the following ways to reset the configuration:

- Delete the entire configuration with the exception of the storage details: When you reset the configuration through the configuration interface, the RAID, volume, share, and quota configuration is maintained. All other configuration details are restored to factory defaults. Click **Restore All Settings to Factory Defaults**.



System Details	
Serial Number	7T6008B04005
Firmware Version	1.15-1 (Mon, 13 Oct 2008 10:24:33 +0000)
Hardware Revision	V02
Last Firmware Upgrade	Fri Sep 19 15:24:44 2008

Firmware image file:

- **Reset All Settings to Factory Defaults**: If you cannot access the NSS configuration interface, you might need to reset the network settings. This option lets you access the interface and make the changes required to resolve the problem.

  To reset the network settings, first shut down the system and power it off. Press and hold the recessed **Reset** button on the front panel of the chassis, and then apply power to the system. Wait until you see the Power LED on the front of the chassis flash yellow rapidly, and then release the **Reset** button.The following settings are reset to their default:

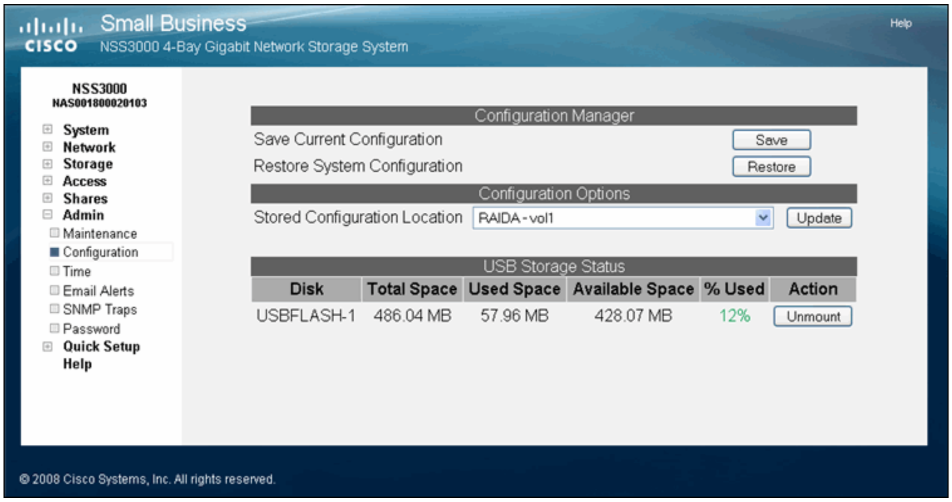
  - **Link Addressing**: DHCP
  - **NSS Hostname**: nas<MAC address of primary link> For example, "nas0123456789ab"
  - **Network Ports**: The network ports are reset to their default. See ”Configuring the Network Ports” on page 34.
  - **VLANs**: All configured VLANs are deleted.
  - **ADS Server**: ADS server settings are cleared.
  - **DNS**: DNS settings are cleared.
  - **Administrator Password**: admin
  - **Network Filters**: cleared
  - **Network Default Policy**: Accept All
  - **MTU Size**: 1500

Managing the NSS Configuration

You can save the current configuration settings within a configuration file that can be used to restore the settings at a later time. You can choose to save the configuration file to a volume on the NSS or you can save the file to a USB flash device that is inserted into the AUX-1 port on the front of the chassis. When you save the configuration file, it is time and date stamped and becomes available in the list of available configuration files when you click the **Restore** button from the **Configuration Manager** page. After you mount the USB flash device by inserting it into the AUX-1 port, make sure you unmount the USB flash device before you remove it. (To unmount the USB flash device, display the **Storage Status** page and then click **Unmount**.)

To display the **Configuration Manager** page, from the **Manager Menu**, click **Admin** ➡ **Configuration**.

The **Configuration Manager** page appears.



Configuration Manager

Save Current Configuration

Restore System Configuration

Configuration Options

Stored Configuration Location: RAIDA - vol1

USB Storage Status

Disk	Total Space	Used Space	Available Space	% Used	Action
USBFLASH-1	486.04 MB	57.96 MB	428.07 MB	12%	Unmount

192016

Saving the Current Configuration

You can save a copy of the NSS configuration that can be used if you need to restore the settings at a later time. When you save the configuration file, it saves a date-stamped version of the current configuration settings to the specified volume on the NSS. You can choose to save the current configuration settings to a specified volume on the NSS or you can save the file to a USB flash device inserted into the AUX-1 port.

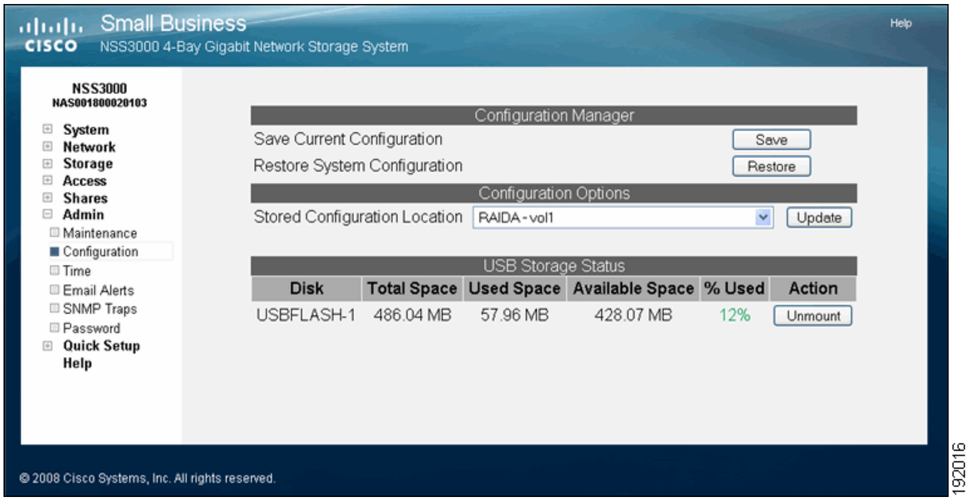
NOTE If you restore a configuration file that was saved in an older version of the NSS firmware than the current version, check the settings after you restore the file to ensure they were updated correctly.

To save the current configuration:

STEP 1 If you are saving the configuration file to a USB flash device, insert a USB flash device into the AUX-1 port on the NSS chassis.

STEP 2 From the **Manager Menu**, click **Admin** ➜ **Configuration**.

The **Configuration Manager** page appears.



Configuration Manager

Save Current Configuration

Restore System Configuration

Configuration Options

Stored Configuration Location: RAIDA - vol1

USB Storage Status

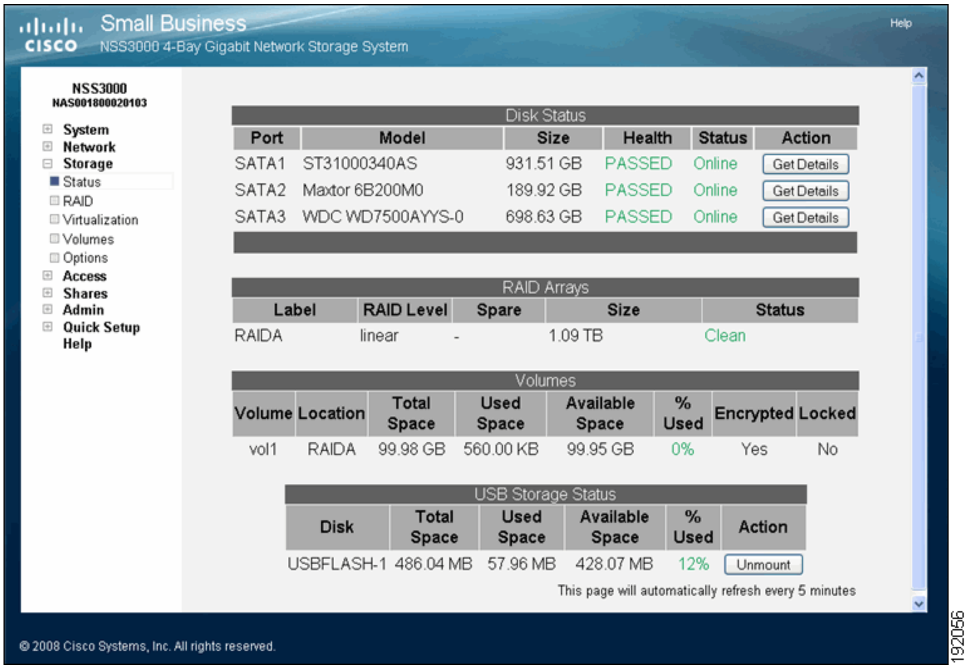
Disk	Total Space	Used Space	Available Space	% Used	Action
USBFLASH-1	486.04 MB	57.96 MB	428.07 MB	12%	Unmount

STEP 3 Select the location where the backup is saved from the **Stored Configuration Location** drop-down menu. To save the configuration file to a USB flash device, select the AUX-1 port as the location. You can then copy the configuration file from the USB flash device to another location on your network.

STEP 4 Click **Update**.

STEP 5 Click **Save** to save the configuration settings. If the configuration file does not successfully save to the specified volume, check the volume to ensure that it is not locked.

STEP 6 If you saved the file to the USB flash device, open the **Storage Status** page.



Disk Status

Port	Model	Size	Health	Status	Action
SATA1	ST31000340AS	931.51 GB	PASSED	Online	Get Details
SATA2	Maxtor 6B200M0	189.92 GB	PASSED	Online	Get Details
SATA3	WDC WD7500AYYS-0	698.63 GB	PASSED	Online	Get Details

RAID Arrays

Label	RAID Level	Spare	Size	Status
RAIDA	linear	-	1.09 TB	Clean

Volumes

Volume	Location	Total Space	Used Space	Available Space	% Used	Encrypted	Locked
vol1	RAIDA	99.98 GB	560.00 KB	99.95 GB	0%	Yes	No

USB Storage Status

Disk	Total Space	Used Space	Available Space	% Used	Action
USBFLASH-1	486.04 MB	57.96 MB	428.07 MB	12%	Unmount

This page will automatically refresh every 5 minutes

STEP 7 Click **Unmount**.

NOTE Removing the USB flash device in a mounted state can cause file or filesystem corruption.

STEP 8 When the AUX-1 LED on the chassis is off, you can safely remove the unmounted USB flash device from the AUX-1 port.

Restoring a Configuration File

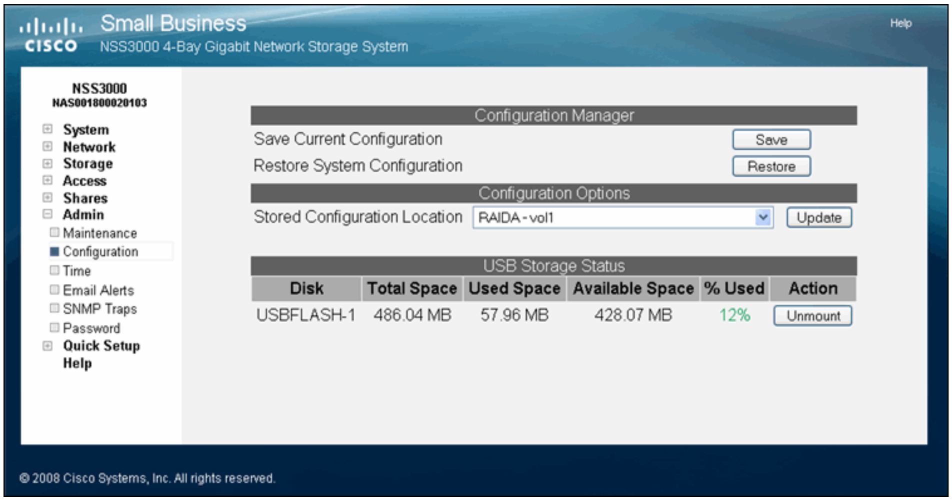
You can easily overwrite the current configuration settings with the configuration settings in a saved configuration file.

NOTE If you restore a configuration file that was saved in an older version of the NSS firmware than the current version, check the settings after you restore the file to ensure they were updated correctly.

To restore a configuration file:

STEP 1 From the **Manager Menu,** click **Admin** ➜ **Configuration**.

The **Configuration Manager** page appears.



Configuration Manager

Save Current Configuration

Restore System Configuration

Configuration Options

Stored Configuration Location: RAIDA - vol1

USB Storage Status

Disk	Total Space	Used Space	Available Space	% Used	Action
USBFLASH-1	486.04 MB	57.96 MB	428.07 MB	12%	Unmount

192016

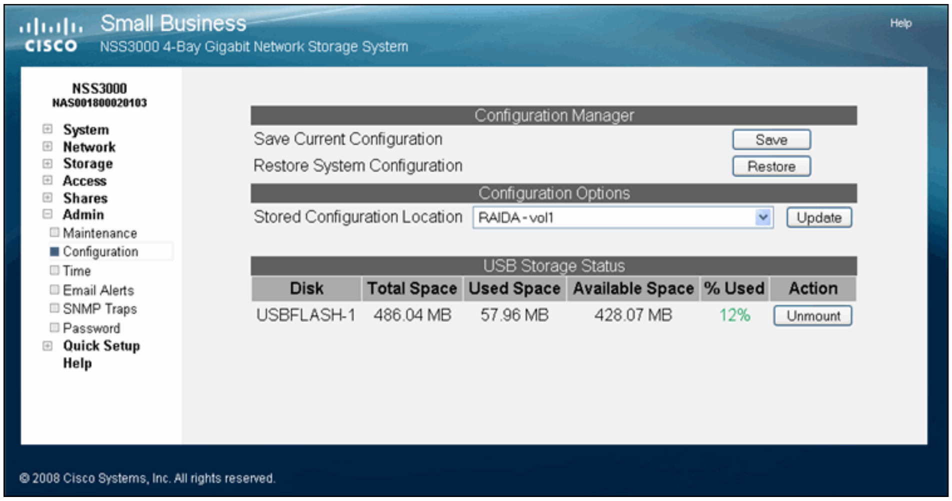
STEP 2 If the configuration file is not located on a volume in the NSS, copy it onto a USB flash device and then insert the USB flash device into the AUX-1 port.

STEP 3 From the **Stored Configuration Location** field, select the location of the saved configuration file.

STEP 4 Click **Update**.

STEP 5 Click **Restore**.

A list of saved configuration files appear. Each saved configuration file is named according to the time and date it was saved. The naming format is: HH.MM.SS.NN.DD.YY.tar.gz where HH = hour, MM=minute, SS=second, NN=month, DD=day, and YY=year.



Configuration Manager

Save Current Configuration [Save]

Restore System Configuration [Restore]

Configuration Options

Stored Configuration Location: RAIDA - vol1 [Update]

USB Storage Status

Disk	Total Space	Used Space	Available Space	% Used	Action
USBFLASH-1	486.04 MB	57.96 MB	428.07 MB	12%	Unmount

STEP 6 Set **Restore Volume Encryption Password** depending on whether you want to include the encryption keys for the encrypted volumes in the restore.

The NSS configuration backup includes a backup of the encryption header for all the encrypted volumes (the encryption header contains an encrypted version of the encryption key used to encrypt the volume data. Including it in the configuration backup does not decrease the security of the encryption because this same header would be available to any attacker with physical access to the system). You can choose to restore these keys or not, depending on the reason you are doing the restore. If the encryption header on an encrypted volume becomes corrupted, restoring the header might allow you to unlock the volume. Also, if you have forgotten the password, you can restore the encryption header. This lets you revert to the volume password as it was when the configuration file was saved.

STEP 7 Click **Full Restore** for the configuration file you want to restore.

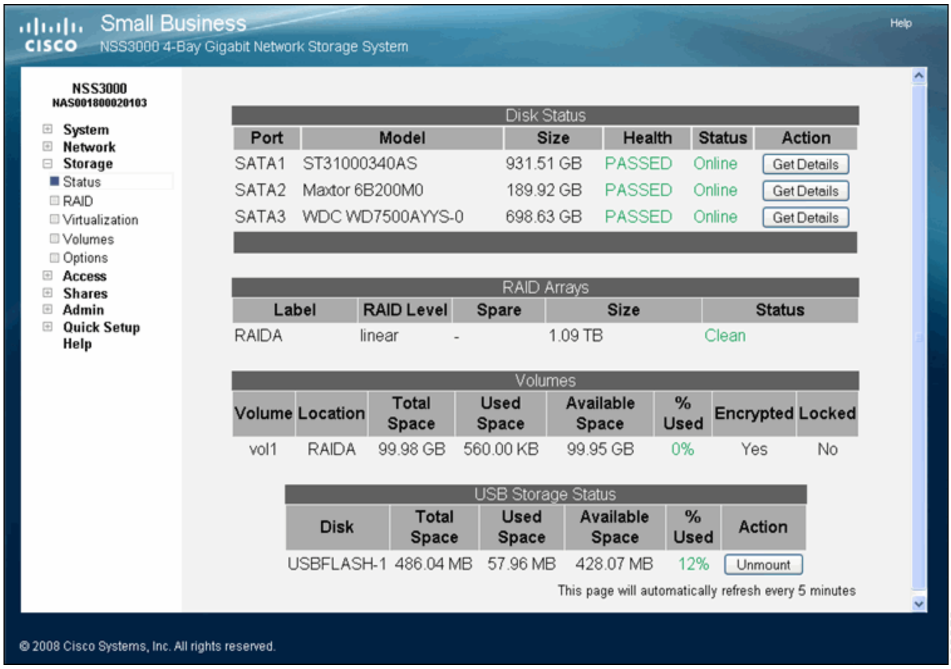
STEP 8 Close the Web browser.

After a few minutes the system reboots.

STEP 9 Check the Power LED on the front of the chassis. The Power LED goes to a solid green when the reboot completes.

STEP 10 Log back into the configuration interface. You need to unlock any encrypted volumes to make them available for storage purposes.

STEP 11 If you saved the file to the USB flash device, display the **Storage Status** page.



Disk Status

Port	Model	Size	Health	Status	Action
SATA1	ST31000340AS	931.51 GB	PASSED	Online	Get Details
SATA2	Maxtor 6B200M0	189.92 GB	PASSED	Online	Get Details
SATA3	WDC WD7500AYYS-0	698.63 GB	PASSED	Online	Get Details

RAID Arrays

Label	RAID Level	Spare	Size	Status
RAIDA	linear	-	1.09 TB	Clean

Volumes

Volume	Location	Total Space	Used Space	Available Space	% Used	Encrypted	Locked
vol1	RAIDA	99.98 GB	560.00 KB	99.95 GB	0%	Yes	No

USB Storage Status

Disk	Total Space	Used Space	Available Space	% Used	Action
USBFLASH-1	486.04 MB	57.96 MB	428.07 MB	12%	Unmount

This page will automatically refresh every 5 minutes

STEP 12 Click **Unmount**.

NOTE Removing the USB flash device in a mounted state means that you risk causing file or filesystem corruption.

STEP 13 When the AUX-1 LED on the front of the chassis is off, you can safely remove the unmounted USB flash device from the AUX-1 port.

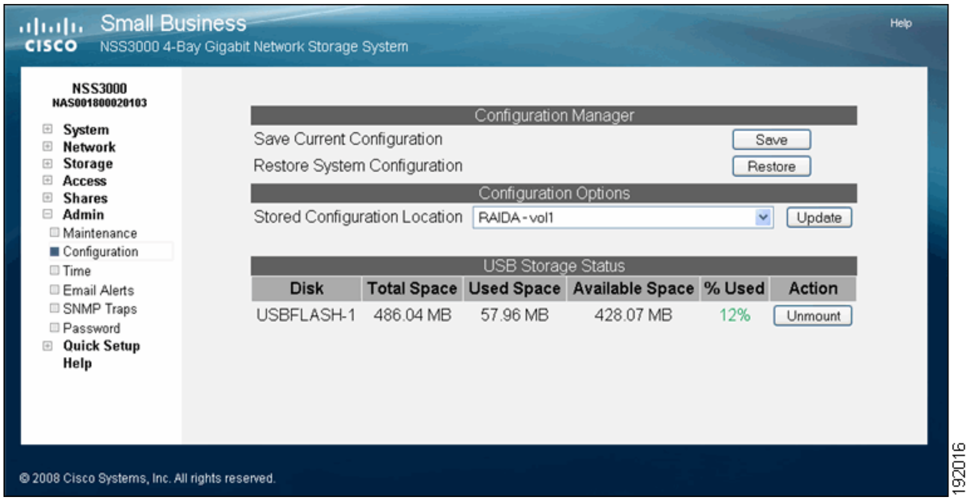
Deleting a Configuration File

Each time you save a configuration file, a copy of it is time and date stamped and saved to the specified location. You can choose to delete a configuration file.

To delete a configuration file:

STEP 1 From the **Manager Menu**, click **Admin** ➜ **Configuration**.

The **Configuration Manager** page appears.



Stored Configuration Location: RAIDA - vol1

Disk	Total Space	Used Space	Available Space	% Used	Action
USBFLASH-1	486.04 MB	57.96 MB	428.07 MB	12%	Unmount

STEP 2 If the configuration file is located in a location on your network, install it onto a USB flash device and then insert the USB flash device into the AUX-1 port on the front of the NSS chassis.

STEP 3 Click **Restore**.

A list of saved configuration files appear.

STEP 4 Click **Delete** for each configuration file you want to remove.

Configuring the Timing Settings

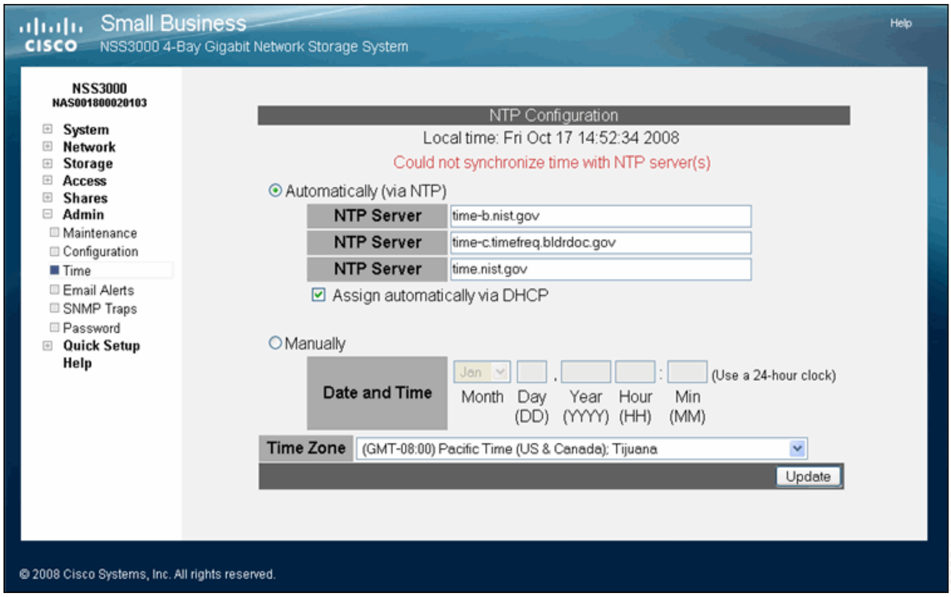
When you first configure the NSS, ensure that the NSS has successfully synchronized the time with the NTP server. When the NSS is synchronizing with the NTP time server, the "Synchronizing time with NTP server" message appears and the **Update** button is grayed out. After the synchronization is complete, you can manually refresh the page by reselecting the **NTP Configuration** page from the **Manager Menu**. If the synchronization failed, the following occurs:

- An error message stating "Could not synchronize with NTP server(s)" appears in the **NTP Configuration** page.
- The system alert message "Could not synchronize with NTP server(s)" appears in the System Status page.
- If the SNMP traps are configured, an SNMP trap message is sent.

To configure the time settings for the NSS:

STEP 1 From the **Manager Menu**, click **Admin** ➡ **Time**.

The **NTP Configuration** page appears.



NTP Configuration

Local time: Fri Oct 17 14:52:34 2008

Could not synchronize time with NTP server(s)

● Automatically (via NTP)

NTP Server	time-b.nist.gov
NTP Server	time-c.timefreq.bldrdoc.gov
NTP Server	time.nist.gov

☑ Assign automatically via DHCP

○ Manually

Date and Time	Jan Month	Day (DD)	Year (YYYY)	Hour (HH)	Min (MM)	(Use a 24-hour clock)

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

STEP 2 To use an NTP server to maintain the NSS time, click **Automatically (via NTP)**. To assign the time manually, skip to step 4.

STEP 3 If your DHCP server is configured to provide NTP settings, select "**Assign automatically through DHCP**". If not, manually configure the NTP settings. In the **NTP Server** fields, enter the IP address or hostname for the NTP servers you want to synchronize. The settings in these fields are also used as a fallback if you chose to get NTP settings from your DHCP server. The NTP servers can be located on your network or can be public NTP servers located on the Internet. Skip to step 6.

STEP 4 Click **Manually**.

STEP 5 Enter the date and time in the **Date and Time** fields.

STEP 6 Select your time zone from the **Time Zone** drop-down menu.

STEP 7 Click **Update**.

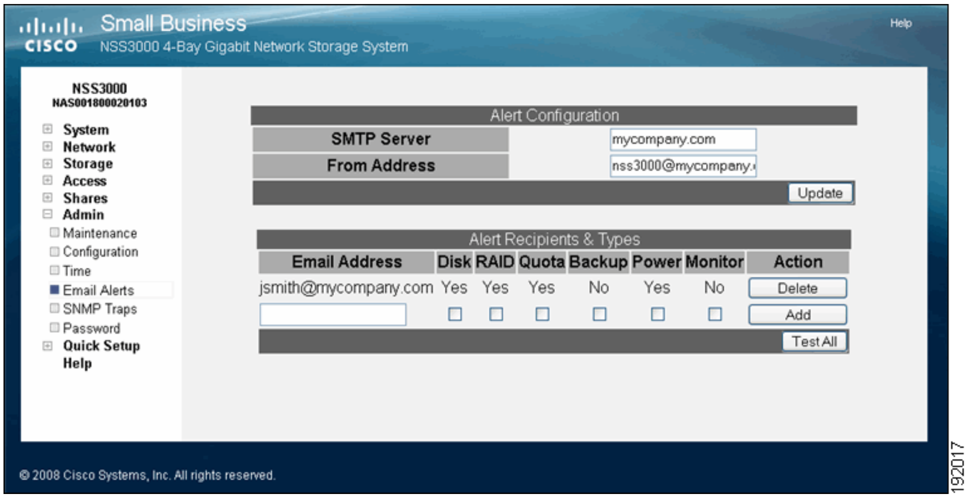
Configuring the Email Alerts for a Recipient

You can create a list of users that will receive email alerts when changes occur to the NSS. Changes can include configuration changes (such as the addition of a volume), physical changes (such as the removal or insertion of a disk), and changes of state (such as a loss of power). You can customize the user’s email profile to suit the user’s specific "need-to-know" requirements.

To configure the NSS for email alerts:

STEP 1 From the **Manager Menu**, click **Admin** ➡ **Email Alerts**.

The **Email Alerts** page appears.



Alert Configuration

SMTP Server	mycompany.com
From Address	nss3000@mycompany.(

Alert Recipients & Types

Email Address	Disk	RAID	Quota	Backup	Power	Monitor	Action
jsmith@mycompany.com	Yes	Yes	Yes	No	Yes	No	Delete
	□	□	□	□	□	□	Add

STEP 2 Enter the SMTP server IP address or name in the **SMTP Server** field.

STEP 3 In the **From Address** field, enter the email address that you want to appear in the from: field of the email header of each email alert.

STEP 4 Click **Update**.

STEP 5 To add a new email account, define the following fields in the **Alert Recipients & Types** area:

- **Email Address**: Enter the user's email address.
- **Disk**: Check this option to notify the user when a change occurs to the disks installed in the NSS.
- **RAID**: Check this option to notify the user when a change occurs to a RAID array.
- **Quota**: Check this option to notify the user when a change occurs to a quota.
- **Backup**: Check this option to notify the user when a backup is run.
- **Power**: Check this option to notify the user when there is a change of state of the UPS.
- **Monitor**: Check this option to notify the user when there is an event tracked through the hardware monitor (i.e., voltages, fans, and temperatures) that falls out of specification.

STEP 6 Click **Add.** Click **Test All** to send a test notification for all checked options to the defined recipients.

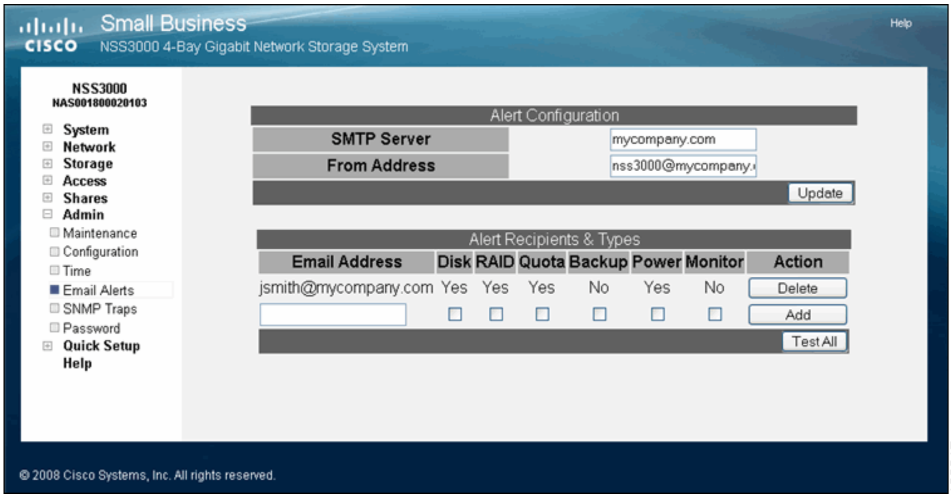
Changing the Email Alerts for a Recipient

After you define a recipient to receive email alerts, you can only edit the alert profile by first deleting the existing profile and then recreating it.

To edit the email alerts:

STEP 1 From the **Manager Menu**, click **Admin** ➡ **Email Alerts**.

The **Email Alerts** page appears.



Alert Configuration

SMTP Server	mycompany.com
From Address	nss3000@mycompany.(

Alert Recipients & Types

Email Address	Disk	RAID	Quota	Backup	Power	Monitor	Action
jsmith@mycompany.com	Yes	Yes	Yes	No	Yes	No	Delete
	□	□	□	□	□	□	Add

STEP 2 Click **Delete** for the applicable email recipient.

STEP 3 Recreate the email recipient.

STEP 4 Click **Add.** Click **Test All** to send a test notification for all checked options to the defined recipients.

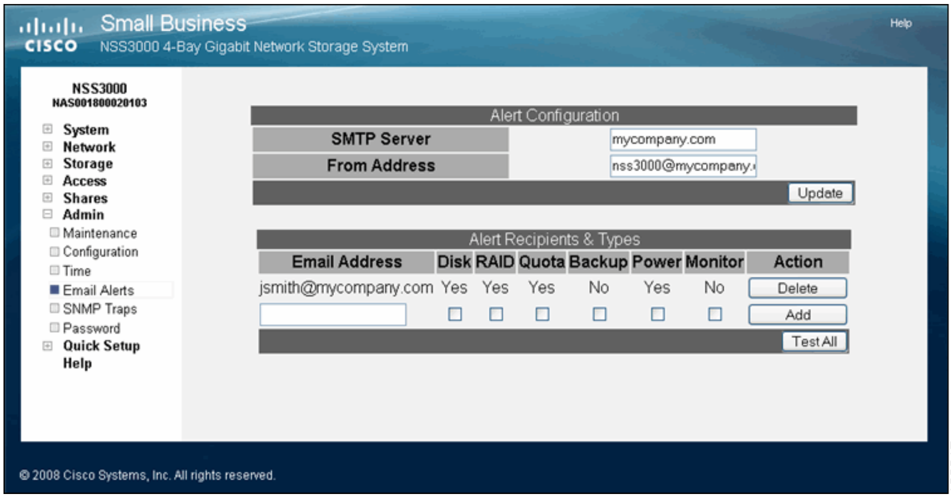
Deleting an Email Alert Recipient Profile

To stop sending all email alerts to a user, you can delete the profile at any time. This is also one of the steps you must take if you want to make changes to the types of email alerts the user receives.

To delete the email alerts:

STEP 1 From the **Manager Menu**, click **Admin** ➡ **Email Alerts**.

The **Email Alerts** page appears.



Alert Configuration

SMTP Server	mycompany.com
From Address	nss3000@mycompany.

Update

Alert Recipients & Types

Email Address	Disk	RAID	Quota	Backup	Power	Monitor	Action
jsmith@mycompany.com	Yes	Yes	Yes	No	Yes	No	Delete
	□	□	□	□	□	□	Add

Test All

192017

STEP 2 Click **Delete** for the applicable email recipient.

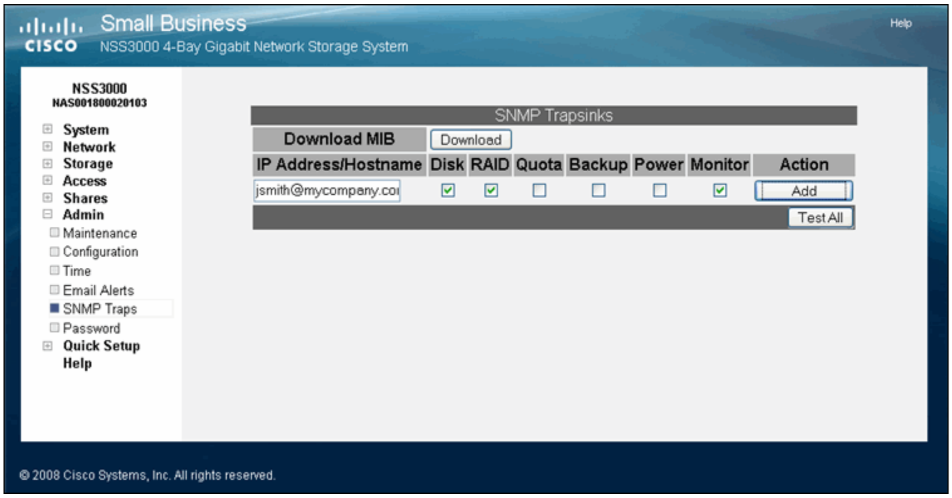
Configuring SNMP Alerts

The NSS can send SNMP traps to alert you of various system events. If you download and install the NSS SNMP MIB, you get a more human readable version of alerts displayed on your SNMP management station.

To define **SNMP Trapsinks**:

STEP 1 From the **Manager Menu**, click **Admin** ➡ **SNMP**.

The **SNMP Trapsinks** page appears.



SNMP Trapsinks

Download MIB	Download						
IP Address/Hostname	Disk	RAID	Quota	Backup	Power	Monitor	Action
jsmith@mycompany.co	☑	☑	□	□	□	☑	Add
							Test All

STEP 2 To install the NSS MIB on your management station, click **Download**.

STEP 3 Save and install the MIB to your management station. For more information on installing and integrating the NSS MIB into your management station, refer to the management station documentation.

STEP 4 Enter the IP address or hostname for the management station to which you want to send the alerts.

STEP 5 Select the checkbox for each type of trap sink for which you want to send alerts to the SNMP server.

You can set up an alert for any of the following:

- **Disk**: When the following occurs: 1) a drive is predicted to fail by S.M.A.R.T., 2) a drive fails, 3) a drive is above temperature threshold, 4) a volume is more than 90% full.
- **RAID**: When any of the following occurs: 1) a RAID goes into a degraded state, 2) a RAID is in a degraded state and will be deactivated (the alert advises the time at which the RAID will be deactivated), 3) a RAID goes into a failed state, 4) a RAID is deactivated, 5) a RAID is rebuilt, 6) a RAID is created.
- **Quota**: When a user or group is over their quota.
- **Backup**: When a backup job completes.
- **Power**: When there is a change in the state of the UPS.
- **Monitor**: When there is an event tracked through the hardware monitor (i.e., voltages, fans, and temperatures) that falls out of specification.

STEP 6 Click **Add**.

The management station appears in the **Existing SNMP Trapsinks** list.

STEP 7 Repeat steps 4 through 6 for each SNMP server address to which you want to send alerts.

STEP 8 To send a test alert for each of the selected conditions to all configured trapsinks, click **Test All**. To delete an existing SNMP Trapsink, click **Delete**.

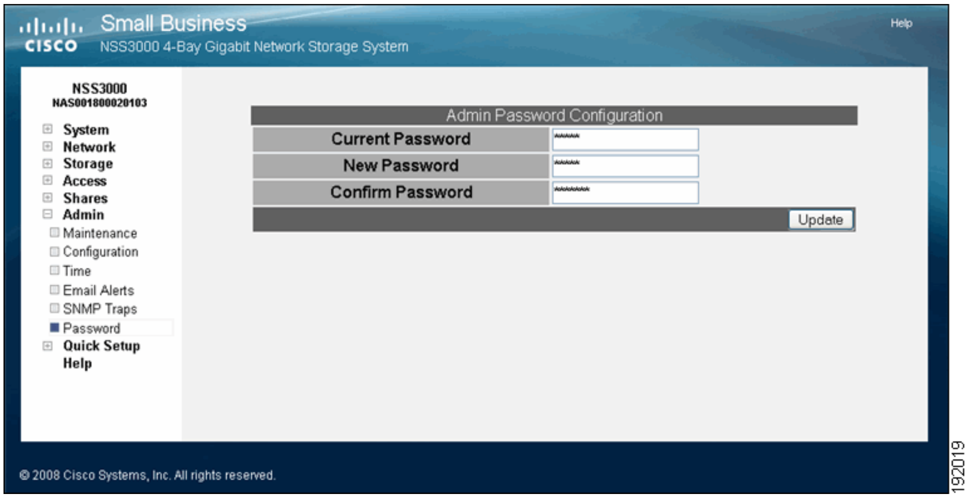
Changing the Administrator Password

You should change the administrator password from the default to ensure that only authorized individuals can access the NSS configuration interface. If you forget the administrator password, you can only reset it by pressing the **Reset** button on the NSS chassis and restoring the factory defaults. The default password is "admin".

To set up the administrator password:

STEP 1 From the **Manager Menu**, click **Admin** ➜ **Password**.

The **Admin Password Configuration** page appears.



Admin Password Configuration

Current Password	*****
New Password	*****
Confirm Password	*******

STEP 2 Enter the current password in the **Current Password** field.

STEP 3 Enter the new password in the **New Password** field.

STEP 4 Re-enter the new password in the **Confirm Password** field.

STEP 5 Click **Update**.

The new password takes effect immediately. The next configuration interface page that you access prompts you for the new password.

End User Access

Logging into a Share

End users, using a Windows, UNIX, Linux, or Mac computer can easily access NSS storage. Once the end user logs into the NSS using their username and password, the shares to which the end user has read or read-write privileges appear. The NSS supports three file-sharing protocols: CIFS, NFS, and FTP. The steps to access the NSS storage depend on which file-sharing protocol the end user chooses to use: CIFS, NFS, or FTP as well as the end user's operating system.

Logging into the CIFS Shares with Administrator Privileges

To log into CIFS shares with administrator privileges:

STEP 1 There are a variety of ways to access the CIFS shares on the NSS. As the administrator, you also have read-write access to a hidden share called "storage". This share gives access to all data on the system (including user home directories). As the administrator, you can read, write, and delete all files and folders regardless of who owns them. For this reason, make sure that you change the default administrator password.

- From the **My Computer** window, type the NSS \\<**hostname**> or <**IP address** > in the Address bar. (Where the <hostname> refers to your NSS hostname and <**IP address** > refers to the IP address of your NSS. For example, "\\NAS0123456789ab" or "\\192.168.1.2".) To access the hidden storage folder, type the hostname or IP address followed by "\storage". For example, "\\NAS0123456789ab\storage".
- Browse for the NSS from the **My Network Places** window. To access the hidden storage folder, make sure that you add "\storage" to the address.
- Map the NSS to a network drive. To access the hidden storage folder, make sure that you add "\storage" to the address.

The **Login** window appears.

STEP 2 Enter the user name "admin" and then enter your administrator password.

STEP 3 Click **OK**.

Windows Users: Accessing the NSS Storage using CIFS/SMB

Windows users who have a user profile set up can access any shares to which they have privileges on the NSS storage using CIFS/SMB.

To access the NSS storage using CIFS/SMB:

STEP 1 Choose one of these options to access the NSS.

- From the **My Computer** window, type \\<**hostname**> or \\<**IP address**> in the Address bar. (Where the <**hostname**> refers to your NSS hostname and <**IP address**> refers to your NSS IP address. For example, "\\NAS0123456789ab or \\192.168.1.2".)
- Browse for the NSS from the **My Network Places** window.
- Map the NSS to a network drive.

The **Login** window appears.

STEP 2 If your user profile is set up locally (that is, through the NSS configuration interface) and the NSS is part of a Windows domain, in the **User name** field, enter the following: <NSS hostname>\<username>. If your user profile is set up through the domain or the NSS is not joined to a domain, you do not need to enter the NSS hostname before your user name. (Just enter your user name and then your password.)

STEP 3 Click **OK**.

The **Windows Explorer** window opens with a directory listing of the available shares.

STEP 4 Depending on your share privileges, you can begin using the NSS storage.

Windows Users: Accessing the NSS Storage through FTP

Windows users who have a user profile set up can access any shares to which they have privileges on the NSS storage using CIFS/SMB or FTP. Note that when using FTP to access the NSS storage, users cannot rename folders. To rename a folder, use CIFS or NFS if enabled on the share.

NOTE Before your end users can access the shares on the NSS using FTP, the NSS must have FTP access enabled and the individual share must be set up to allow FTP access.

To access the NSS storage using FTP:

STEP 1 From your FTP client application, connect to the NSS. Enter the IP address or hostname of the NSS. For more information about using your FTP client application, refer to its documentation.

STEP 2 Enter your username and password when prompted by your FTP client.

When your FTP client has logged in, a list of accessible shares appears as individual directories.

STEP 3 Depending on your share privileges, you can begin using the NSS storage.

Mac Users: Accessing Storage through CIFS/SMB

Mac users who have a user profile can access any shares to which they have privileges on the NSS storage using CIFS/SMB.

To access the NSS storage through CIFS/SMB:

STEP 1 From the **Finder's Go** menu, click **Connect to Server**.

STEP 2 Enter "smb://<hostname or IP address of the NSS>/<sharename>. (Where the information in the brackets is meant to be replaced with the applicable information. Do not type the brackets.)

Click the "+" sign to save the NSS address to the Favorite Servers list so that the next time you log in you just need to select the address from the list.

STEP 3 Click **Connect**.

STEP 4 When the **Login** window appears, enter your username and password. If your user profile is set up locally (that is, through the NSS configuration interface and not through the ADS or NTv4 domain) and the NSS is joined to a domain, you need to enter the following: <NSS hostname>\<user name>. If the NSS is not joined to a domain, just enter the username.

STEP 5 Depending on your share privileges, you can begin using the NSS storage.

Mac Users: Accessing Storage through FTP

Mac users who have a user profile can access any shares to which they have privileges on the NSS storage using FTP. However, they cannot rename folders when using FTP to access the NSS storage. To rename a folder, use CIFS or NFS if it is enabled on the share.

NOTE Before your end users can access the shares on the NSS using FTP, the NSS must have FTP access enabled and the individual share must be set up to allow FTP access.

To access the NSS storage using FTP:

STEP 1 Open your FTP client application.

STEP 2 Click **Connect**.

STEP 3 From your FTP client application, connect to the NSS. Enter the IP address or hostname of the NSS. For more information about using your FTP client application, refer to its documentation.

STEP 4 Enter your username and password when prompted by your FTP client.

When your FTP client has logged in, a list of accessible shares appears as individual directories.

STEP 5 Depending on your share privileges, you can begin using the NSS storage.

UNIX/Linux Users: Accessing Storage through NFS

UNIX and Linux users can access shares on the NSS through NFS. Due to the way that the NSS implements NFS file access privileges, only NFSv3 is supported. In order for NFS access privileges to work correctly, you must have the NSS joined to an NIS domain.

NOTE You must have root privileges to your client system to create an NFS mount. Before an end user can access the shares on the NSS through NFS, NFS must be enabled on the NSS and the individual share set up to allow NFS access.

To access the NSS storage through FTP:

STEP 1 Log into the client system as root.

STEP 2 Create a mount point directory for the mount if you do not already have one (e.g., mkdir /mnt/nas_share1).

STEP 3 Mount the NFS share by typing "mount -v -t nfs -o nfsvers=3,rsize=32768,wsize=32768 <IP address/hostname>:<mount point path on NSS> <mount point path on client>". The mount point path on the NSS appears in the **Shares** page.

STEP 4 Log out of the root account.

STEP 5 Log into the user account on the client system.

You can now access the share though the mount point directory on your client. You have the share privileges as are defined for the NSS.

UNIX/Linux Users: Accessing Storage through FTP

UNIX and Linux users who have a user profile set up can access any shares to which they have privileges on the NSS storage using NFS or FTP. Note that when using FTP to access the NSS storage, users cannot rename folders. To rename a folder, use CIFS or NFS if enabled on the share.

NOTE Before your end users can access the shares on the NSS using FTP, the NSS network filters must be set up to allow FTP access. The individual share must be also be set up to allow FTP access.

To access the NSS storage using FTP:

STEP 1 Open your FTP client application.

STEP 2 Enter the **NSS hostname/IP address**.

STEP 3 Enter any other required settings. If using FTPS, ensure that the client is set to use Explicit FTPS. For more help using the FTP client, refer to the FTP client documentation.

STEP 4 Enter your username and password when prompted by the FTP client.

STEP 5 Depending on your share privileges, you can begin using the NSS storage.

Glossary of Storage-related Terms and Acronyms

A

ACL: Access Control List. Used within network security systems to allow selective use of services. An Access Control List is used to control access to, and denial of, services. It lists the services available with a corresponding list of the hosts permitted to use the service.

Active Directory: A Microsoft directory service for use in Windows environments. Administrators use Active Directory to assign enterprise wide policies, deploy programs to many computers, and apply critical updates to an entire organization. Active Directory functions much like an online phone book, storing information about resources on the network while providing a means of centrally organizing, managing, and controlling access to these resources.

AES (Advanced Encryption Standard): A block cipher adopted as an encryption standard by the U.S. government.

Aggregation: The act of collecting something together. In Network Storage Aggregation, you can put together pieces of networked storage into one, logical storage unit.

B

Bonjour: Apple's version of the Zeroconf. Used to automatically configure devices and discover services on an IP network, Bonjour is the most widely used implementation of Zeroconf. On the Mac, Bonjour lets Safari Web browser users find the Zeroconf-enabled Web servers in the network. Web servers are widely used not just for HTML pages, but function as control panels for a variety of network devices such as routers and Webcams. There is also a Bonjour plug-in for Internet Explorer which is used to discover Bonjour-enabled network printers and devices. (It was originally named Rendezvous.)

C

CIFS: Common Internet Filesystem. A protocol that evolved out of SMB (Server Message Block). CIFS is an application-level network protocol mainly used to share files, printers, serial ports, and miscellaneous communications between nodes on a network. It also provides an authenticated Inter-process communication mechanism. It is mainly used by Microsoft Windows-equipped computers.

Coldplug: Often taken to mean the opposite of hotplugging. In other words, the inability of a computer system to add or remove hardware without powering the system down.

D

DAS: Direct Attached Storage. Also referred as Server Attached Storage and Captive Storage. The storage device (such as disk drive or RAID array) is directly attached to a computer. The computer uses various adapters and standardized protocols, such as SCSI and Fibre Channel, to access the storage device.

DFS: Distributed Filesystem. This system, developed by Microsoft, lets you build a hierarchical view of multiple file servers and shares on the network.

DHCP: Dynamic Host Configuration Protocol. Software that dynamically assigns IP addresses to devices on a TCP/IP network. DHCP software typically runs in servers and is also found in network devices such as ISDN routers and modem routers that allow multiple users access to the Internet. Newer DHCP servers dynamically update the DNS servers after making assignments.

DiffServ (Differentiated Services): A scalable IP Layer 3 method for classifying, managing network traffic, and providing QoS (Quality of Service) guarantees on an IP network. DiffServ is often used to provide low-latency, guaranteed service to time-sensitive network traffic like voice or video while concurrently providing best-effort traffic guarantees to non-time sensitive Web traffic (such as email) or file transfers.

Disk Quotas: For NAS devices, a limit set by a network administrator that restricts certain aspects of filesystem usage. There are four types of disk quotas: 1) Usage (or block) quota sets a limit on the amount of storage space (measured in MB or GB) that connected users or groups can use, 2) File (or inode) quota sets a limit for a specific number of directories or files that connected users or groups can use, 3) Usage or File quotas are considered Hard quotas, 4) Soft quota is a way, set by the administrator, to define a warning level that alerts users that they are nearing their specified hard quota limit.

Disk Tax/Disk Overhead: The limitation of hard disk drive (HDD) capacity when specific RAID configurations that use mirroring or redundancy are applied to an array.

DNS: Domain Name System (or Service or Server). An Internet service that translates domain names into IP addresses. While domain names are alphabetic and easier to remember, the Internet uses IP addresses. When you use a domain name, a DNS service must translate the name into the corresponding IP address. The DNS system is its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain: The name that identifies a computer connected to the Internet. For example, www.google.com. The "www." refers to the connection to the World Wide Web; the middle portion of a domain name is usually the name of the company that owns the computer (in this case, Google). The final portion of a domain name tells you what kind of site is served by this machine. In this case, .com means this is a commercial site. Other categories include: .net, .org, .edu, .fr, .uk, etc. All devices sharing a common part of the IP address share that domain.

dotted quad: This refers to the IP address number.The dotted quad is a unique number format made up of four parts separated by dots. For example, 116.112.96.2.

E

ext2: Second extended filesystem. A native filesystem for the Linux kernel. It was initially designed to replace the extended filesystem (ext). It is fast enough that it is used as the benchmarking standard. Although ext2 is not a journaling filesystem, its successor, ext3, provides journaling and is almost completely compatible with ext2.

ext3: Third Extended Filesystem. A journalled filesystem that is commonly used by the Linux operating system. Unlike its predecessor, ext2, the journaling support alleviates lengthy filesystem checks (fsck) at bootup after a sudden system crash, reset, or power loss. It is the default filesystem for many popular Linux distributions.

F

FAT32: File Allocation Table. Microsoft developed this partially patented filesystem for MS-DOS. It is the primary filesystem for consumer versions of Microsoft Windows up to and including Windows Me. Because it is considered relatively simple, the FAT filesystem is supported by virtually all existing operating systems for personal computers. This ubiquity makes it an ideal format for floppy disks and solid-state memory cards, and a convenient way of sharing data between disparate operating systems installed on the same computer (a dual boot environment). The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process. Defragmentation is one solution to this, but is often a lengthy process in itself and has to be repeated regularly to keep the FAT filesystem clean. To overcome the volume size limit of FAT16, while still allowing DOS real-mode code to handle the format without unnecessarily reducing the available conventional memory, Microsoft decided to implement a newer generation of FAT, known as FAT32, with cluster counts held in a 32-bit field, of which 28 bits are currently used.

File Sharing Protocol: A high-level network protocol that provides the structure and language for file requests between clients and servers, including the commands for opening, reading, writing and closing files across the network. It may also provide access to the directory services. It is sometimes referred to as a "client/server protocol" and functions at the application layer (layer 7 of the OSI model). In order for a client to have access to multiple servers running different operating systems, either the client supports the file sharing protocol of each operating system or the server supports the file sharing protocol of each client. Software that adds this capability is very common and allows interoperability between Windows, Macintosh, NetWare and Unix platforms. Examples of file sharing protocols include: CIFS/SMB (Windows), and NFS (UNIX).

FTP: File Transfer Protocol. FTP is a standard Internet protocol that uses the Internet's TCP/IP protocols to exchange files between computers on the Internet. FTP can be used to transfer, download, and upload files individually or in batch form.

FTPS: File Transfer Protocol over SSL. FTPS is similar to the standard FTP but because it operates over an encrypted link (SSL), it is a more secure way to transfer files over the Internet. The NSS supports Explicit FTPS (versus Implicit FTPS). Explicit FTPS is named for the command issued to indicate that TLS security should be used. This is the preferred method according to the RFC defining FTP over TLS. The client connects to the server port 21 and starts an unencrypted FTP session as normal, but requests that TLS security be used and performs the appropriate handshake before sending any sensitive data.

G

Gigabit: Also Gbit or Gb. A unit of information or data storage equivalent to 1,000,000,000 (1 billion) bits.

Gigabtye (GB): A unit of information or data storage equivalent to 1,000,000,000 (1 billion) bytes.

H

High Availability: A term applied to a class of electronic devices where a system design protocol has been applied and implemented to ensure a higher/improved degree of operational continuity during a given measurement period.

Hotplug: The ability to add or remove hardware without first powering down the system.

I

IEEE 802.1ad: Protocols that provide separate instances of MAC services to multiple independent users on a bridged LAN (local area network) in a way that does not require cooperation among the users, but does require a minimum of cooperation between users and the MAC service provider.

IEEE 802.1p: An IEEE standard that provides quality of service (QoS) in 802-based networks at the MAC level. 802.1p uses three bits (defined in 802.1q) to allow switches to reorder packets based on priority level (traffic class expediting and dynamic multicast filtering). It also defines the Generic Attributes Registration Protocol (GARP) and the GARP VLAN Registration Protocol (GVRP). GARP lets client stations request membership in a multicast domain, and GVRP lets them register into a VLAN. Eight different classes of service are available, expressed through three extra bits on the Ethernet Frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE however has made some broad recommendations. 802.1p is used within the IEEE 802.1D and IEEE 802.1Q standards.

IEEE 802.1Q: An Ethernet, Layer 2 standard for providing VLAN identification and QoS (Quality of Service) levels for devices on a network. This is achieved by adding four bytes to the Ethernet frame header of a data packet (three bits of which assign up to eight priority or QoS levels and 12 bits identify up to 4096 VLANs).

IEEE 802.1X: Standard for port-based network access control that authenticates devices attached to a LAN port. This standard establishes connection to a network and its connected resources if authentication is approved, and conversely, prevents access to the network if authentication fails. An authentication server resides in each Cisco Small Business NSS product.

J

JBOD: Just a Bunch of Disks. Multiple hard disk drives (HDDs) that are combined into a single virtual drive. In a JBOD configured array, each drive can be a different size or capacity (this storage method can be used to turn two or more odd-sized hard drives into one useful drive). There is no redundancy provided with a JBOD and the failure of one disk in the array usually results in the loss of the data stored on the JBOD.

Journaling Filesystem: A fault-resilient filesystem that provides data integrity because updates to directories and bitmaps are constantly written to a serial log on disk before the original disk log is updated. If the system fails, a full journaling filesystem restores the data on the disk to its pre-crash configuration. It also recovers unsaved data and stores it in the location where it would have gone if the computer had not crashed. This type of system is beneficial for mission-critical systems. A physical journal logs verbatim copies of blocks that will be written later (for example, ext3) as compared with a logical journal that logs metadata changes in a special, more compact format. Logical journals can improve performance by reducing the amount of data that needs to be read from and written to the journal in large, metadata-heavy operations (for example, deleting a large directory tree). XFS keeps a logical journal.

L

LCD: Stands for Liquid Crystal Display and is a display technology that uses liquid crystals that flow like liquid and bend light. The LCD appears on the front of the NSS3000 chassis and can be used to determine various status details about the NSS3000.

LDAP (Lightweight Directory Access Protocol): A protocol that lets users find organizations, workgroups, other users, network resources (such as directories, volumes, files) or peripheral devices (such as printers and NAS devices) on a local network, in a intranet or on the Internet without knowing the specific domain where they reside. A single LDAP directory can be mirrored on multiple servers that can be periodically synchronized.

Link Aggregation Group: (LAG) A computer networking term used to describe using multiple Ethernet network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port. Other terms for this also include "ethernet trunk", "NIC teaming", "port teaming", "port trunking", "NIC bonding" and "link aggregate group" (LAG), and is based on a networking standard known as "IEEE 802.3ad".

M

MDFS (Microsoft Distributed Filesystem): see DFS.

Mirroring: For NAS devices, the automated process of simultaneously writing data to two (or more) hard disk drives. Mirroring creates a redundant repository of data, such that if one of the hard disk drives (HDD) fails, the redundant drive continues to provide access to the stored data for connected users. Network administrators can then replace the failed drive with a new drive that can be re-mirrored to the good drive. RAID level 1 uses mirroring.

MTBF (Mean Time Between Failures): A measurement of hardware product reliability typically indicated in thousands, tens of thousands, or hundreds of thousands of operational hours between failures. It is most often defined as the average time between failures. MTBF can be derived from extensive and time intensive testing of the working product, calculated from actual product field performance (depending on the product, its market, its usage, and the ability to retrieve accurate usage data), or from a calculated prediction based on known factors. Manufacturers provide MTBF as a reference of the product’s, or its subcomponent’s reliability. Customers can use the MTBF to determine their service needs to maintain or replace the product.

N

NAS (Network Attached Storage): A data storage device on a computer network to provide a centralized repository of data that can be shared and accessed by other end-users or workgroups on the network. The Cisco Small Business NSS products are NAS devices.

NFS: Network Filesystem. A protocol suite developed and licensed by Sun Microsystems that allows different makes of computers running different operating systems to share files and disk storage.

NIS: Network Information Service (formerly known as Yellow Pages). A system by which one machine (the master) holds the Ethernet addresses of other machines (the servants). NIS is an insecure alternative to DNS.

NTFS: New Technology Filesystem. Windows NT standard filesystem and its descendants: Windows 2000, Windows XP, Windows Server 2003 and Windows Vista. NTFS replaced Microsoft's previous FAT filesystem, used in MS-DOS and early versions of Windows, and offers improvements over FAT such as improved support for metadata and the use of advanced data structures to improve performance, reliability and disk space utilization plus additional extensions such as security access control lists and filesystem journaling.

P

Parity: A way to attach additional binary digits to data blocks that lets a NAS controller monitor if data has been lost or overwritten after it has been moved from one place to another in a storage array or among networked computers.

PSU: Power Supply Unit. A device or system external to or within the NSS that supplies electrical power to the device or group of devices.

R

RADIUS (Remote Authentication Dial-in User Service): An authentication, authorization, and accounting protocol to access a network locally or remotely. RADIUS uses a RADIUS server that resides in the local network or as an offsite, leased resource/service to perform the authentication and authorization functions.

RAID: Redundant Array of Inexpensive or Independent Disks. In storage environments, a RAID uses multiple physical disk drives to create a single logical unit from which data can be shared or replicated between the drives. There are various RAID levels (or ways to define how the disks work together). Each level provides one or more of increased data integrity, fault-tolerance, and throughput or capacity. The types of RAID levels and combinations of these levels is constantly changing as new methods and technologies continue to improve. Currently, the NSS offers the choice of five different RAID levels (including JBOD) with two options for adding a hot spare to an existing RAID level.

S

SAN (Storage Area Network): A network of storage and server devices typically found in large, enterprise environments with high volume or high data traffic requirements. SANs are architected to be scalable so that computer storage devices (such as disk array controllers, tape libraries, and servers) can be added and incorporated into the system. A SAN lets computers connect to hard disk drives and tape drives on a network as though they were locally attached devices. A SAN can contain a single NAS device or numerous NAS devices.

SAS (Serial Attached SCSI): A computer bus technology and serial communication protocol to transfer data to and from hard disk drives and CD-ROMs. Used in large enterprise environments to replace legacy, parallel, SCSI solutions, because SAS attains much higher transfer speeds, and has backwards-compatibility with SATA. SAS uses serial communication to establish connectivity to other SAS devices and uses SCSI commands for file transfer.

SATA: Serial ATA. A computer bus technology that evolved from the Parallel ATA physical storage interface. Like PATA, SATA is an IDE (Integrated Drive Electronics) drive, designed for transfer of data to and from a hard disk. Serial ATA is a serial link -- a single cable with a minimum of four wires creates a point-to-point connection between devices. Transfer rates for Serial ATA begin at 150 MBps. One of the main design advantages of Serial ATA is that the thinner serial cables facilitate more efficient airflow inside a form factor and also allow for smaller chassis designs. The IDE cables used in parallel ATA systems are bulkier than Serial ATA cables and can only extend to 40cm long, while Serial ATA cables can extend up to one meter.

SATA II: A followup set of specifications to the original SATA specifications. The SATA II enhancements are delivered in increments. The first increment, called SATA II: Extensions to SATA 1.0. was released in 2002 and focused on the immediate needs for the server and network storage segments. Additional increments of the specification will focus on enhanced cabling, fan-out and failover capabilities and next generation signaling speeds. In spring 2003, two incremental developments were announced: a SATA II Port Multiplier specification release candidate and the completion and pending adoption of the SATA II Cables and Connectors Volume 1 specification.

SFTP: Secure File Transfer Protocol. A network protocol designed by the IETF to provide secure file transfer and manipulation facilities over the secure shell (SSH) protocol. This protocol is NOT supported by the NSS. (It does support FTPS.)

S.M.A.R.T. : Self-Monitoring Analysis and Reporting Technology. This industry-standard technology was developed by a number of major hard disk drive manufacturers to try to increase the reliability of drives. Using this technology, the NSS can predict the future failure of hard disk drives. The NSS uses the advanced diagnostics within the S.M.A.R.T. system to monitor the internal operations of a drive. It can then send an early warning for about 70% of all hard drive errors, such as disk performance, faulty sectors, recalibration, CRC errors, drive spin-up time, drive heads, distance between the heads and the disk platters, drive temperature, and characteristics of the media, motor, and servomechanisms. This lets the administrator repair or replace the drive before any data is lost or damaged.

SMB (Server Message Block): An application-level networking protocol that gives shared access to files, serial ports, printers, and other data transfer between nodes on a network. SMB can also be used to access different subnets over the Internet. Computers on a network that don’t share their individual hard disk drives, use SMB to gain access to shared drives, volumes, files, printers, or other devices on a network. It is mainly used by Microsoft Windows-enabled computers.

SMTP (Simple Mail Transfer Protocol): The standard protocol for sending emails over the Internet typically used in conjunction with POP or IMAP mail servers so that end users can receive, save, and store email.

Snapshot: A copy of a set of files, volumes, or directories as they were at a particular point in time. The Cisco NSS uses snapshots to back up the shares located on a volume in such a way that end users can recover their own files without having to ask the administrator to restore a backup. So for files that are on a volume for which snapshots are set up, a snapshot folder is created for each share on the volume. End users can revert to older versions of files by browsing the snapshot folder and finding a version of the desired file. The snapshots can be set for hourly, daily, and weekly intervals.

SSH (Secure Shell): A protocol and group of standards that provide confidentiality and integrity of data as it is exchanged between two or more computers or from a storage/server device to an accessing computer. SSH uses encryption and authentication codes to establish a secure communication channel. It is most often used to log into a remote computer or other device to execute commands.

SSL: Secure Sockets Layer. SSL is a protocol used to transmit files over the Internet using a private key to encrypt the data. SSL was originally developed by Netscape and is now an industry standard. The NSS supports FTPS which is FTP over SSL.

Striping: A method of concatenating multiple disk drives into one logical storage unit. Striping involves partitioning each drive's storage space into stripes which may be as small as one sector (512 bytes) or as large as several megabytes. These stripes are then interleaved round-robin, so that the combined space is composed alternately of stripes from each drive. In effect, the storage space of the drives is shuffled like a deck of cards. The type of application environment, I/O or data intensive, determines whether large or small stripes should be used.

T

Terabyte (TB): For data storage capacity usage, terabyte is equal to 1024 gigabytes.

TFTP (Trivial File Transfer Protocol): A simple file transfer protocol used to transfer small files between hosts on a network. TFTP works like a very basic form of FTP.

TLS: Transport Layer Security. A security protocol from the IETF that is based on the Secure Sockets Layer (SSL) 3.0 protocol developed by Netscape. TLS uses digital certificates to authenticate the user and the network. The TLS client uses the public key from the server to encrypt a random number and send it back to the server. The random number, combined with additional random numbers previously sent to each other, is used to generate a secret session key to encrypt the subsequent message exchange.

U

UPnP: Universal Plug and Play. A family of protocols from the UPnP Forum that automatically configure devices, discovering services and providing peer-to-peer data transfer over an IP network. Like Zeroconf, UPnP uses link-local addressing for IP assignment and provides service discovery. Unlike Zeroconf, UPnP uses a different protocol. If a device does not have an IP address and there is no DHCP server in the network, UPnP employs link-local addressing to create an IP address. Software such as Windows Media Connect uses UPnP to stream audio and video over the network. Several UPnP standards are employed including the Simple Service Discovery Protocol (SSDP) for finding devices and UPnP AV Architecture, MediaServer and MediaRenderer for streaming. UPnP can open router ports to let a device, external to the network, contact a network device.

UPS: Uninterruptible Power Supply. A device that provides battery backup when the electrical power fails or drops to an unacceptable voltage level. Small UPS systems provide power for a few minutes; enough to power down the computer in an orderly manner, while larger systems have enough battery for several hours.

V

Virtualization: The creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources. The Cisco NSS refers to virtualization as a way of aggregating storage between devices. Virtualized storage occurs when storage is exported to the network as a disk drive or an array and is then imported by a master NSS. The master NSS then uses the newly imported storage to create a single JBOD.

VLAN: Virtual Local Area Network (LAN). A logical group of user stations, servers, and other network devices that appear to be on the same LAN, regardless of their physical location. You can use the MAC addresses or IP addresses to interconnect the workstations on the LAN. You can access and control the switches directly from a console port or via the LAN using IP.

W

Well Known Ports: IANA assigns TCP and UDP port numbers to specific uses. The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.The Ports that are popular (well known) are those in the range 0 to 1023.

WINS: Windows Internet Naming Service. This is part of the Microsoft Windows NT Server. It manages the association of workstation names and locations with Internet addresses. The user or an administrator does not have to be involved in each configuration change.

X

XFS: A high-performance journaling filesystem created by Silicon Graphics for their IRIX operating system. XFS has been merged into the mainline Linux 2.4 and 2.6 kernels, making it almost universally available on Linux systems. Installation programs for the SuSE, Gentoo, Mandriva, Slackware, Zenwalk, Fedora, Ubuntu and Debian Linux distributions all offer XFS as a choice of filesystem. FreeBSD gained read-only support for XFS in December 2005 and in June 2006 experimental write support was introduced to FreeBSD-7.0-CURRENT.

Z

Zeroconf: An IETF (Internet Engineering Task Force) specification that lets IP network devices automatically configure themselves and be discovered without manual intervention. Zeroconf can also manually assign an IP address and alternate host name to a device, as required. Once assigned, Zeroconf lets users and applications readily discover the service it offers. Apple’s Bonjour is the major implementation of Zeroconf.

Troubleshooting

NSS LEDs

The LEDs on the front of the NSS chassis help you troubleshoot a variety of conditions on the NSS---from normal operating conditions, alerts, to serious error conditions. The **Reset** button lets you restore the network defaults in situations where you can no longer log into the configuration interface.

Power Button LED

The **Power Button LED** shows whether the NSS is receiving power and is functioning properly. These are the LED colors and their meanings:

- **Solid Yellow**: The NSS is powered on and the boot loader is currently running. The boot loader runs for approximately 10 seconds when the NSS first starts up, and then the LED blinks green.

  This condition also occurs if the upgrade of the firmware process fails (although in this case, the LED remains in a solid yellow condition until the user clicks **OK** from the **System Details** page following an unsuccessful upload. After the user clicks **OK**, the system reboots using the current version of the firmware.

- **Blinking Yellow**: The network configuration factory defaults are being reset. When resetting the network defaults, hold down the **Reset** button until you see the **Power** LED flash yellow rapidly.
- **Solid Green**: The NSS is powered up and finished booting.
- **Blinking Green**: The NSS is either booting up or shutting down.
- **Alternating Yellow & Green**: The firmware update is currently in progress.
- **Off**: The NSS is either disconnected from a power source or has finished the shutdown process and can be safely disconnected from a power source.

You can also use the **Power Button** LED to perform a graceful shutdown or hard shutdown of the NSS:

- **To perform a graceful shutdown**: Press the **Power** button and hold for about 1 to 2 seconds to trigger a graceful shutdown of the NSS.
- **To perform a hard shutdown**: Press the **Power** button and hold for about eight seconds. Choose this option only if the NSS is not responding to a graceful shutdown

System LED

The **System (SYS)** LED indicates that a system error has occurred on the NSS. These are the LED colors and their meanings:

- **Solid Yellow**: Indicates one of these error conditions. You can view the error through the NSS configuration interface.
  - A volume is more than 90% full.
  - A disk drive has failed or is about to fail.
  - A fan has stalled.
  - The system temperature is above the maximum threshold.
  - The temperature of a disk drive is above the maximum threshold.
  - A voltage rail is above or below specification.
  - The NSS is running on UPS due to a mains power failure.
- **Solid Red**: Indicates a critical system failure. The system could not boot due to a corrupted firmware image.
- **Off**: There are no system-related problems

LAN LED

The **LAN LED** shows the status of the Ethernet link. These are the LED colors and their meanings:

- **Solid Green**: The LAN link is up and running at 1000 link speed, but is currently idle.
- **Flickering Green**: The LAN link is up and running at 1000 link speed and is currently active. The LED flickers off with activity.
- **Solid Yellow**: The LAN link is up and running at 10/100 link speed, but is currently idle.
- **Flickering Yellow**: The LAN link is up and running at 10/100 link speed and is currently active. The LED flickers off with activity.
- **Off**: No LAN link is detected.

Hard Disk Drive LEDs

The **ACT** and **Error** LEDs shows the status of the installed disk drives.

ACT LED

The **ACT** LED states indicates drive activity. These are the LED colors and their meanings.

- **Solid Green**: The disk drive is configured but is currently idle.
- **Flickering Green**: The disk drive is configured, active, and not rebuilding. Flickers off with activity.
- **Blinking Green**: The disk drive is configured and a RAID array is currently rebuilding to the disk drive.
- **Off**: The disk drive is not configured (not part of a RAID or JBOD array and not exported).

ERR LED

The **ERR** LED states indicates that the disk drive is in an error condition. These are the LED colors and their meanings

- **Solid Red**: The disk drive is in a failed state.
- **Blinking Red**: The disk drive is predicated to fail (via S.M.A.R.T.). We recommend that you replace the disk drive to avoid the loss of data.
- **Off**: The drive is OK.

Off: There is either no UPS attached to the NSS or the UPS function has been disabled in the **System Power** page in the configuration interface.

On: A UPS is attached to the NSS and the UPS function is enabled in the **System Power** page in the configuration interface.

Reset Button

Use the **Reset** button to restore the network setting system defaults or to reset the box. The **Reset** button is located to the left of the display button on the front panel of the NSS. You might need to use a pen or the end of a straightened paperclip to press the button.

- **To restore the network setting system defaults**

  Shut down the NSS, press the **Reset** button, and then power up the NSS. When you see the **Power** LED blink yellow rapidly, release the **Reset** button. The network settings are restored to the factory defaults.

- **To reset the NSS**

  Press and hold the **Reset** button while the system is running until the **Power** LED blinks green. Release the **Reset** button.

The various states of the Error LED indicate that the disk drive is in an error condition:

- **Solid Red**: The disk drive is in a failed state.
- **Blinking Red**: The disk drive is predicated to fail (via S.M.A.R.T.). We recommend that you replace the disk drive to avoid the loss of data.
- **Off**: The drive is OK.

Off: There is either no UPS attached to the NSS or the UPS function has been disabled in the System Power page in the configuration interface.

On: A UPS is attached to the NSS and the UPS function is enabled in the System Power page in the configuration interface.

For more information about the UPS, see ”Configuring the System for UPS Support” on page 12.

Using the NSS3000 LCD Panel

The LCD panel on the front of the chassis lets you view various aspects of the system such as the status of the configured RAIDs, volumes, the status of the bootup, and so on. To step through the available options, press the **Display** button. Each time you press the **Display** button, the next screen appears. Because of the screen space limitations within many of the available screens, the information appears on multiple pages.

For example, the **Home** screen has two pages (page 1 shows the hostname and IP, and the second page shows the hostname and netmask). When you display a screen, the first page appears. Subsequent pages appear after a few seconds and continue to automatically scroll through the pages until you press the **Display** button.

The LCD panel displays these screen options:

- **Bootup Screen**: During the bootup of the NSS, the LCD panel displays its progress.
- **Home Screen**: Displays the current hostname, IP address, and netmask of the system.
- **System Alerts**: Displays the system alerts (two per page) in order from most recent to the oldest. Fordetailed information about the system alerts, see ”System Alerts” on page 6.

- **RAID Status**: Displays details for the configured RAID arrays in the system. You can view the type of the RAID array (J=JBOD, 0,1,5,10), the state of the RAID (i.e., clean, degraded, rebuild, failed, and stopped), and the percentage complete of the RAID rebuild (if currently in progress).
- **Volume Status** :Displays the configured volumes and the percentage of space used. Each volume appears with the RAID on which it is configured followed by the volume name. For example, A:volB (which indicates that Volume B is located on RAID A).
- **Cable Diagnostics**: Displays the status of the Ethernet cable If the link is working properly, the link status appears as **OK**. If there is a problem with the link, the status is reported according to the pairs within the cable. These messages can appear:
  - **Short:** If the pair has a short, the message appears as "pair a-b short@ Xm" (where "a" and "b" are the numbers of the pair, "X" is the location in the cable where the short was found, and "m" stands for metres).
  - **Open**: If the cable has an open, the message appears as "pair a-b open@ Xm (where "a" and "b" are the numbers of the pair, "X" is the location in the cable where the open was found, and "m" stands for metres).
  - **Disconnected**: If the cable shows an open at the minimum measurable distance, it is assumed that the cable is not connected. The message "Cable is not connected" appears.

  The cable diagnostic test only runs the first time you display the **Cable Diagnostics** screen. To rerun the test, scroll through the LCD screens until you see the **Cable Diagnostics** screen appear again.
- **Firmware Version/Update Date**: Displays the version of the firmware and the date that the last firmware upgrade was completed.
- **Firmware Upgrade**: Displays the progress of the firmware upgrade. When you display this screen, a diagnostic test is automatically run (This screen only appears when performing a firmware upgrade)
- **System Time/Date**: Displays the current time and date for the system. The time appears using the 24-hour clock. The date appears as the day of the week, the month as a three-character abbreviation, and the year.
  For example, 21:45, Wed, Dec 12, 2008.
- **Shutdown Screen**: During the shutdown of the NSS, the LCD panel displays the progress of the shutdown.

- **Network Factory Defaults Restore**: During the restoration of the default network configuration the LCD panel displays that the network is being restored and is changing the settings to the default settings.

Repairing a Degraded Array

If a RAID level 1, 5, or 10 is in a degraded state (that is, a redundant disk drive has failed), you can replace the failed disk drive(s). (You might be able to use some of the data on a JBOD if there are volumes that do not span across the failed disk. Otherwise, you must rebuild the JBOD after you replace the disk.) If an array with no redundancy has a failed disk drive, you must delete the array, replace the disk drive, and then recreate the array.

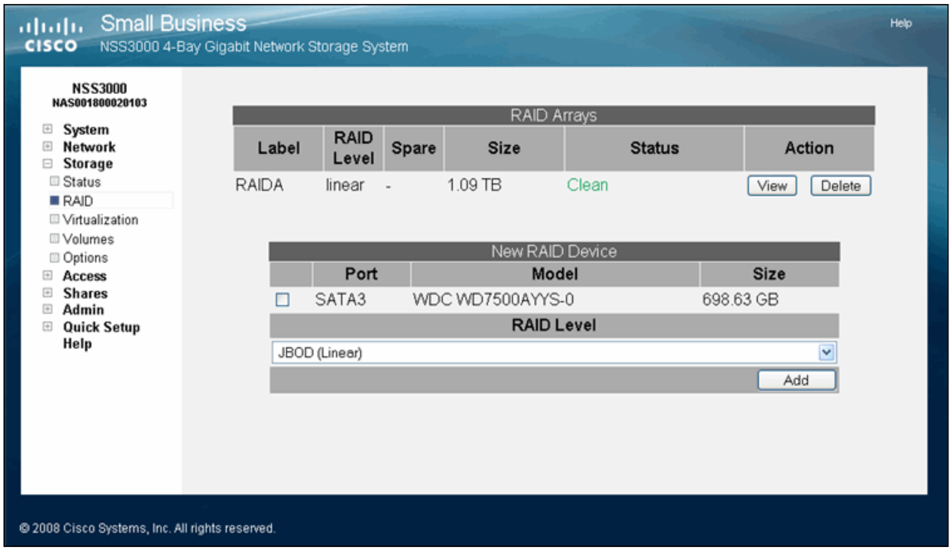
NOTE When adding disks to an array, we recommend you use the same model of disk with the same capacity. The new disk must have at least the same capacity of the smallest disk currently in the array. With the exception of a JBOD, RAIDs are configured to use the maximum of the smallest disk capacity in the array for each additional disk in the array. For example, if you install two, 250 GB disks and one 500 GB disk, the total capacity is 750 GB.

To add a disk to a degraded array:

STEP 1 If you are replacing a disk, remove the failed drive from the NSS and install the replacement disk.

STEP 2 From the **Manager Menu**, click **Storage** ➜ **RAID**.

The **RAID** page appears.



RAID Arrays

Label	RAID Level	Spare	Size	Status	Action
RAIDA	linear	-	1.09 TB	Clean	View Delete

New RAID Device

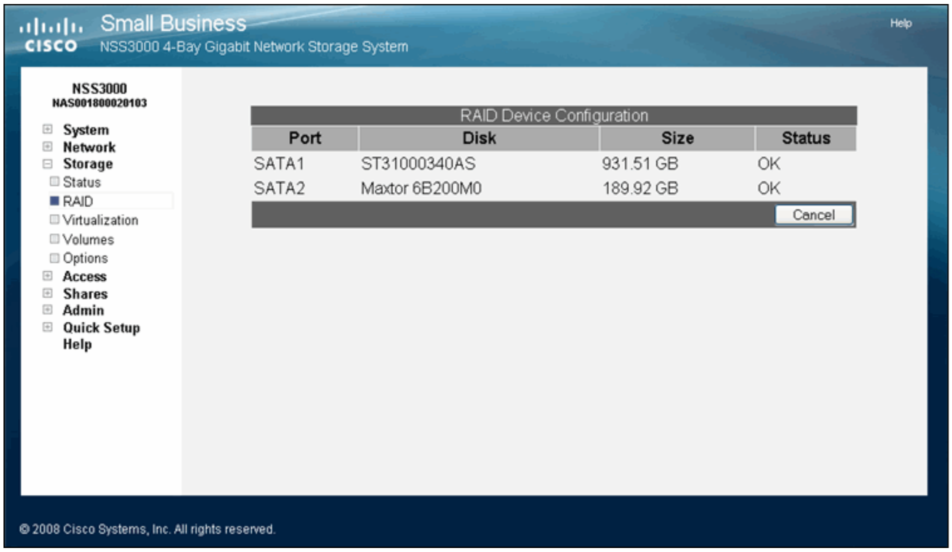
	Port	Model	Size
□	SATA3	WDC WD7500AAYS-0	698.63 GB

RAID Level: JBOD (Linear)

Add

STEP 3 In the **RAID Arrays** table, click **Edit** for the applicable RAID array.

The **RAID Configuration** page appears.



RAID Device Configuration

Port	Disk	Size	Status
SATA1	ST31000340AS	931.51 GB	OK
SATA2	Maxtor 6B200M0	189.92 GB	OK

Cancel

STEP 4 Available disk drives appear in the listing. Click **Add** to add the disk drive to the array.

The **RAID array** is rebuilt for the added or changed redundant disk drive. While the rebuild continues, the array can still be used. After the rebuild process completes, the disk becomes part of the redundant storage.

Working with a Failed Array

If a RAID is in a failed state, the data on the array is not recoverable. You need to delete the array, replace the disk drive, and then configure a new array.

To create an array when an array fails:

STEP 1 Remove the failed drive from the NSS and install the replacement disk. (This step can be done out of order as long as it is installed before you configure the new array.)

STEP 2 Reboot the NSS. Make sure that you do a safe reboot using the Reboot function. See ”Rebooting or Shutting Down the NSS” on page 54.

STEP 3 When the system reboots, log back into the configuration interface.

STEP 4 From the **Manager** Menu, click **Storage** ➜ **RAID**.

The **RAID** page appears. The failed array appears with a status of "Stopped".

STEP 5 Click **Delete**.

The disk drives used in the failed array become part of the available storage.

STEP 6 Create a new array as required.

Once built, you can set up the volumes, shares, and quotas for the array. If the failed array contained the volume used as the **Home Directory** Location, set the location to the volume you want to use.

Firmware Attempt is Unsuccessful

If a problem occurs when updating the firmware, check the following:

- If a copy of the firmware is saved to a disk on the NSS, make sure that you copied it to another location (such as onto a PC). You cannot install firmware that is saved to a disk on the NSS.

- Verify that the firmware is compatible with the NSS platform.
- Verify that the firmware is newer than the version that is currently installed. The system does not support downgrades.
- If you are upgrading within a virtualized setup, make sure that you installed the firmware in the order described in ”Upgrading the NSS Firmware” on page 55.

To update the firmware after a failed attempt:

STEP 1 Click **OK** when the message appears from the **System Details** page that the firmware upgrade was not successful.

The system automatically reboots using the current firmware version. The **Power** LED blinks green and then goes solid green when the reboot completes.

STEP 2 Go through the steps to upgrade the firmware.

Free Bound Virtualized Storage when the Master System Fails

A storage system is bound to a failed storage system and rejects any bind requests from other systems.

Follow these steps to recreate the problem:

STEP 1 Export storage from System A.

STEP 2 Import storage from System A to System B.

STEP 3 System B crashes and cannot be recovered.

STEP 4 System A is "bound" to System B and rejects any new bind requests from other systems.

To resolve the problem:

STEP 1 Unexport the bound storage system (in our example, System A).

STEP 2 Re-export the storage system.

The storage system is now available to be used by another system.

All CIFS Connections were Unexpectedly Ended

If all current CIFS connections to the NSS were unexpectedly severed, check to see if the the hostname the **Network Identification** page was changed. Changing the hostname severs any current CIFS connections to the NSS.

To resolve the problem, change the name back to the original hostname.

Hotplugging the Ethernet Link doesn’t Reset IP or Link Rate

When you disconnect the Ethernet link and reconnect it, the IP address and link rate does not reset. For example, if you unplug a cable from the NSS to a 100 Mbps switch and then reconnect the NSS to a 1 Gps switch, the link is not restored.

To resolve the problem:

STEP 1 Unplug the Ethernet link.

STEP 2 Wait at least 15 seconds.

STEP 3 Reconnect the link.

STEP 4 Wait 10 seconds.

The link is re-established. You can view the status from the **System Status** page on the configuration interface.

Unable to Create a Share or Quota for a Volume

When you attempt to create a share, the volume does not appear in the **Location** field. When you try to create a quota, the quota is not successfully added for the volume.

The problem is likely caused by the volume being locked. An encrypted volume is automatically locked whenever the NSS is rebooted or is manually locked through the configuration interface. As long as the volume is locked, you cannot use the volume to create shares or quotas (you can however, set up the **Home Directory**).

To resolve the problem:

STEP 1 From the **Manager Menu**, click **Storage** ➡ **Volumes.**

If the problem is due to the volume being locked, the **Unlock** button appears next to the volume in the **Action** column.

STEP 2 Click **Unlock**.

STEP 3 Enter the password for the volume.

STEP 4 Click **OK**.

You can now be create a share or quota for the volume.

Cannot Access the NSS through FTP

Users attempt to log into the NSS through FTP but are unable to access their home directory or shares on the NSS.

To resolve the problem, you need to configure these settings to enable FTP access:

STEP 1 From the **Manager Menu**, click **Shares** ➡ **FTP Setup**.

STEP 2 Make sure that **Enable FTP** is selected. (You can go through the settings on this page to ensure they are correctly defined.)

STEP 3 Close the **FTP Setup** page.

STEP 4 From the **Manager Menu**, click **Shares** ➡ **Shares**.

STEP 5 Click **Edit** for the applicable share.

STEP 6 Make sure the **FTP protocol** is selected, and then click **Update.**

STEP 7 From the **Manager Menu**, click **Access** ➡ **Network.**

STEP 8 Make sure there are no filters set up to drop or reject FTP access for the applicable IP or MAC addresses.

Cannot Rename a Folder through FTP

Users attempt to log into the NSS through FTP but are unable to rename a folder. Renaming of folders is not a supported FTP standard.

To rename a folder, users must log into the NSS through NFS or CIFS (provided that these are supported protocols).

Configuration Page Does not Appear in Internet Explorer

If you click a configuration page and the page does not appear, this is a caching problem with the Internet Explorer browser.

Follow these steps to resolve the problem (These steps only apply to Internet Explorer version 6.0. The steps for other versions might vary slightly):

STEP 1 From the **Internet Explorer** browser window, click **Tools** ➡ **Internet Options**.

STEP 2 Click **General**, and then click **Settings**.

The **Settings** window appears.

STEP 3 Under the **Check for newer versions of stored pages**: section, click **Automatically**.

STEP 4 Set the Amount of disk space to use to 1 MB.

STEP 5 Click **OK**.

Handling an Unexpected (Unclean) Shutdown

The best way to shut down the NSS is to use the **Shut Down** command from the **System Details** page on the configuration interface or by using the **Power** button on the front of the chassis.

If the power to the NSS is unexpectedly disrupted, causing the NSS to do an unclean shutdown, the system settings (including time) might be altered. The Administrator is notified of the unclean shutdown in three possible ways:

- When the NSS powers up, an SNMP trap sends a notification.
- When the Administrator first logs into the configuration pages following the shutdown, a message appears.
- An email is sent to the defined email address if the Administrator is set up to receive an email for power loss. .

Following an unclean shutdown of the NSS:

STEP 1 Do one of the following:

- **Review/Edit the System Settings Manually**: Go through each setting, including the time setting to make sure that nothing has been negatively altered. If you make changes to the settings, we highly recommend that you take a USB backup.
- **Back up the System Settings from a USB Backup**: If you have a valid backup on a USB flash device, it might be easier to restore the system settings from the backup (versus manually going through and checking each system setting).

STEP 2 If you attempt either of the above unsuccessfully, restore the configuration settings back to the factory defaults, and then either restore the configuration settings from a USB flash device backup or manually edit the settings.

NOTE The factory default administrator password is "admin".

Boosting the Performance of NFS Transfers

You can substantially improve the NFS performance by increasing the size of read and write buffers on the client. These buffers are sized at 4 KB by default but can be changed at mount time.

For example: mount -v -t nfs 192.168.1.1:/mnt/RAIDA/vol1/share1 /mnt/client -o nfsvers=3,rsize=32768,wsize=32768

where:

- 192.168.1.1 is the IP address of the NSS system
- /mnt/RAIDA/vol1/share1 is the path to the share

- /mnt/client is the mount point on the client
- The size of the read and write buffers is 32 KB.

B

Environmental Specifications

NSS3000

Device Dimensions	3.23 x 11.38” x 9.21” (82 x 289 x 234 mm)
Unit Weight	7.28 lb. (3.3 kg)
Power	60W, 12V external AC power
Certification	FCC Class B
Operating Temp	41 to 104°F(5 to 40°C)
Storage Temp	-4 to 158°F(-20 to 70°C)
Operating Humidity	10 to 90%, Relative non-condensing
Storage Humidity	10 to 95%, Relative non-condensing

C

Support Contacts

Support contact information for this product is available on Cisco.com at this location:

www.cisco.com/go/smallbiz

D

Additional Information

Regulatory Compliance and Safety Information

Regulatory Compliance and Safety Information for this product is available on Cisco.com at this location:

www.cisco.com/go/smallbiz

Warranty

Warranty information that applies to this product is available on Cisco.com at this location:

www.cisco.com/go/smallbiz

End User License Agreement (EULA)

Licensing information that applies to this product is available on Cisco.com at this location:

www.cisco.com/go/smallbiz