# Contents

**Chapter 1: Introduction**  .................. 4  
Using the Help  5  
Recommended Disk Drive List  6

**Chapter 2: Working with the System**  .... 7  
Viewing the Hardware Monitor  11  
Viewing and Managing the System Logs  12  
Configuring the System for UPS Support  14  
NSS-supported UPS Product Families  15

**Chapter 3: Managing the Network Options**  .. 16  
Viewing the Network Settings  18  
Configuring the Network Link IP  19  
Resetting the DHCP Lease on a Link  20  
Viewing VLANs Configured on the NSS  21  
Allowing a VLAN Access to the NSS  22  
Changing a VLAN Configuration  25  
Removing a VLAN’s Access to the NSS  26  
Configuring the NSS Network Identification  27  
Configuring DNS or WINS for Name Resolution  29  
Joining the NSS to a Network Information System (NIS) Domain  31  
Editing Access Control Lists (ACLs) from Windows Explorer: Restrictions  33  
Running Diagnostics of your Physical Links  34  
Configuring the Network Ports  35  
Setting up the Link Bonding & Advertising Modes  36

**Chapter 4: Managing your Storage**  .......... 38  
Choosing a RAID Array Level  42  
Creating a RAID Array  44  
Adding a Disk Drive to an Array  45  
Deleting an Array  47  
Migrating a RAID Array to another Storage Device  48  
Virtualizing Storage within your Network  49  
Exporting Storage to your Network  50  
Creating Virtualized Storage  51  
Unexporting Storage  52  
Volume Management  53  
Creating a Volume  54  
Expanding a Volume  56  
Deleting a Volume  58  
Viewing the Snapshot Reserve Details  59  
Creating a Snapshot for a Volume  61  
Taking a Manual Snapshot of a Volume  63
Windows End Users: Accessing a Snapshot for a Share  64
Volume Encryption Overview  65
Locking an Encrypted Volume  66
Unlocking a Locked Volume  67
Changing the Password for an Encrypted Volume  69
Storage Options  71
Setting the RAID Rebuild Priority  72
Setting the Spin Down Time  73

Chapter 5: Administering Access to the NSS. . . . . . . . . . . . . . . . . . 74
Managing your NSS Users  75
Creating a User Profile  76
Editing a User Profile  78
Integrating Users from an ADS, NTv4, or NIS Domain  80
Deleting a User Profile  81
Working with Groups  82
Creating a Group  83
Changing the Users Assigned to a Group  85
Integrating Groups from an Active Directory, NTv4, or NIS Domain  86
Deleting a Group  87
Managing Volume Quotas  89
Creating Volume Quota for a User or Group  91
Setting up the Grace Period for a Volume Quota  93
Changing a Volume Quota for a User or Group  94
Clearing a Quota  95
Network Filters Overview  96
Defining the Default Network Policy  97
Creating a Network Filter  98
Available Access Filters  100
Deleting a Network Filter  102
Configuring the User/Group Settings  103

Chapter 6: Managing the Shares. . . . . . . . . . . . . . . . . . . . . . . . . . 104
Creating a Share  105
Editing an Existing Share  108
Adding a DFS Shared Folder  110
Restrictions using Microsoft DFS from the NSS  112
Setting up CIFS Access  113
Setting up Network Filesystem (NFS) Access  114
Configuring the NSS for FTP Access  115
Creating or Running a Backup of a Share  117
Creating a Scheduled Backup for a Share  118
Initiating a Backup for a Share  120
Contents

Deleting Backup Images 122

Chapter 7: Managing the Administrator Options 123
- Rebooting or Shutting Down the NSS 124
- Upgrading the NSS Firmware 126
- Restoring the Factory Default Configuration 127
- Managing the NSS Configuration 129
- Saving the Current Configuration 130
- Restoring a Configuration File 132
- Deleting a Configuration File 134
- Configuring the Timing Settings 135
- Configuring SNMP Alerts 137
- Changing the Administrator Password 139

Chapter 8: Accessing the NSS’s Storage 140
- Logging into the CIFS Shares with Administrator Privileges 141
- Windows Users: Accessing the NSS Storage using CIFS/SMB 142
- Windows Users: Accessing the NSS Storage through FTP 143
- Mac Users: Accessing Storage through CIFS/SMB 144
- Mac Users: Accessing Storage through FTP 145
- UNIX/Linux Users: Accessing Storage through NFS 146
- UNIX/Linux Users: Accessing Storage through FTP 147

Chapter 9: Glossary 148

Chapter 10: Troubleshooting 157
- LEDs & Buttons 157
- Repairing a Degraded Array 160
- Working with a Failed Array 162
- Free Bound Aggregation Storage when the Master System Fails 163
- All CIFS Connections were Unexpectedly Ended 164
- Hotplugging the Ethernet Link doesn’t Reset IP or Link Rate 165
- Unable to Create a Share or Quota for a Volume 166
- Cannot access the NSS through FTP 167
- Configuration Page does not Appear in Internet Explorer 168
- Handling an Unexpected (Unclean) Shutdown 170

Appendix A: Support Contact Information 171
Introduction

Thank you for choosing the Linksys Business Series Network Storage System (NSS).

Administering a network can be a difficult job. Finding low-cost ways to simplify your data-management tasks means that you have more resources to dedicate elsewhere. 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 as well as virtualize your storage into one or more logical, redundant storage units or RAID arrays. The NSS uses the most common file-based protocols such as NFS, CIFS, and FTP for file sharing.

Benefits

The NSS offers the following main advantages to your business:

- **Cross-platform File Sharing**: Share files easily and inexpensively across heterogeneous platforms over a cost-effective Ethernet and IP network.

- **Easy Installation and Administration**: With a basic understanding of networking, the NSS is easy to get going and to maintain.

- **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 (Network Storage System) help file provides information about using the configuration interface to configure the NSS. You can access the help topics either through the Help link found in the Manager Menu or by clicking the Help button at the top-right corner of each configuration page.

Audience

The information contained in these 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 some 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, and so on. When you click an option, a sub-menu of related options appears. Clicking a subtopic 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 interface window that you can click to access 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 disk drives, click the Help button for information about the details that appear on the status page.
Recommended Disk Drive List

If you are purchasing disk drives to install in the NSS, please refer to the product support information offered on the LinksysOne website for a list of recommended disk drives.

The decision of which disks to purchase also needs to be made based on the RAID levels you want to create. 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.
Working with the System

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, if an array rebuild is complete, and so on. You can also view the current status of any of the following: storage, shares, backups, volume snapshots, network, power, and system details. Status pages like the System Status page automatically refresh on a regular interval and are very helpful for monitoring the progress of certain processes such as building a RAID.

The following sections provide a detailed explanation of 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 in this area of the System Status page:

- **Error**: These types of messages indicate the most severe problem with the NSS. They are color-coded red and require immediate action. For example, if a disk drive or RAID array is in a failed condition.
• **Warning:** These types of messages indicate there is a problem with the NSS that requires eventual action. They are color-coded orange. 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. They do not require action and are color-coded green. 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. The percentage is color-coded according to the current percentage used:
  - **Green:** 0 to 74%
  - **Orange:** 75-89%
  - **Red:** 90-100%

**Network Status**

The **Network** area displays the following:

- **Link 1 & 2:** The current status of the physical links. The status of the link can be up (color-coded green) or down (color-coded red). If the link is not present, the status appears as "down".
- **Bonding Mode:** Displays how the bonding mode for the physical links has been configured on the **Network Properties** page. (see Setting up the Link Bonding & Advertising Modes)
- **VLANs:** The number of VLANs configured on the NSS.
- **Link 1 IP:** The IP address of the first Ethernet link.
- **Link 2 IP:** The IP address of the second Ethernet link (if installed). If the bonding mode is set to "active backup" or "802.3ad", the two links appear as a single entity (i.e., "Link 1+2 IP").

**Shares Status**

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

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

Backup/Snapshots Status

The Backup/Snapshots area displays the following:

• Snapshots: The total number of volume snapshots configured.
• 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.
  - No Connection: A UPS is not currently connected to the NSS.
  - On Mains: A UPS is connected to the NSS but is not currently being used to power the unit. 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 and is color-coded according to the amount of battery remaining.

• RPSU: The following options are available depending on the current operating condition of the RPSU. For more information about the functioning of the RPSU, refer to the RPSU documentation.
  - No Connection: There is no RPSU installed.
  - Ready: An RPSU is installed and is currently available as a backup power source.
  - Standby/Fault: An RPSU is installed but is in Standby mode, or, the RPSU is installed and has some sort of fault condition. For example, the RPSU is connected to the NSS but is powered off.
  - Active: The RPSU is currently being used to provide backup power to the NSS.
  - Unavailable: The RPSU is currently providing backup power to another device and is not available to provide backup power to the NSS.

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:

- **Voltages**: The current voltage reading for all voltage rails in the system. The reading is color-coded depending on whether 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 (provided that 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. The logs can be stored locally or sent to a remote server on the network. Since local space allocated for log files is limited, the logs are overwritten once the space is filled. Each new event overwrites the oldest event recorded in the file.

To work with the log files:

1. From the Manager Menu, click System ➤ Logs.

   The System Logs page appears.

2. You can view, download, or delete any of the following 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 concatenation of all the log files. You can download and save this file to a location on your network as required.

• **Diagnostics:** A time-stamped log of the cable diagnostic tests run. You can download and save this file.

The following screenshot is an example of the Administrator Log:

![Screen shot of the Administrator Log]

3. 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 name or IP address of the server in the **Remote Log Host** field. Note that the remote server must be running a syslog server.

4. **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.

To set up the UPS:

1. From the Manager Menu, click System ➤ Power.
   
   The System Power page appears.

2. To enable UPS support, select Enable UPS support.

3. Click Update.
NSS-supported UPS Product Families

The NSS supports the following 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
Managing the Network Options

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

### Physical Interfaces

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

- **Link**: The number that appears in this column identifies the link attached to the NSS. It can be either 1 or 2.

- **Status**: The status of the physical link. Options include:
  - **Up**: The link is up (color-coded green) and operational.
  - **Down**: The link is down (color-coded red) and not operational. If a cable is actually 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’s cable diagnostic feature (see Running Diagnostics of your Physical Links) to assist you.

- **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 set 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. If there are two physical links, the link appears as either "1" or "2", or, if the two links are bonded, the number appears as "1+2".
- **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.
- **Tx Pkts**: The total number of IP packets transmitted on the VLAN interface since the last boot.
- **Dropped Pkts**: The total number of IP packets dropped on the VLAN interface since the last boot.
Viewing the Network Settings

The **Network Device Settings** 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, 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.

<table>
<thead>
<tr>
<th>Link</th>
<th>VLAN</th>
<th>Assign Via</th>
<th>IP Address</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1+2</td>
<td></td>
<td>dhcp</td>
<td>192.168.3.101</td>
<td>255.255.255.0</td>
<td>No Gateway Available</td>
<td>Exit</td>
</tr>
<tr>
<td>1+2</td>
<td>500</td>
<td>static</td>
<td>192.168.5.100</td>
<td>255.255.255.0</td>
<td>192.168.5.1</td>
<td>Exit</td>
</tr>
</tbody>
</table>

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

- **Link**: "1+ 2" appears in this column.
- **VLAN**: The ID assigned to the virtual interface. For a physical interface, 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 the DHCP server.
  - **Manual**: A static IP configuration was manually entered through the NSS.
  - **AutoIP**: The interface was configured to use DHCP for IP configuration but no DHCP server was found. Instead the IP address was assigned by the AutoIP protocol.
- **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 need to configure the method for assigning an IP configuration to each physical and virtual interface connected to the NSS.

NOTE: If you hotplug the Ethernet link after the initial installation of the NSS, make sure 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:

1. From the Manager Menu, click Network  ➤  IP.
   The Network IP page appears listing each physical and virtual interface.
2. Click Edit on the row of the interface you want to configure.
   The Network Link Configuration page appears.
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, in dotted-quad notation.
4. Click Update.
Resetting the DHCP Lease on a Link

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

1. From the Manager Menu, click Network → IP.

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

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

   The Network Link Configuration page appears.

3. 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 provided next. 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 configuration changes are required on the NSS.

To view the VLANs currently configured on the NSS:

1. From the **Manager Menu**, click **Network ➪ VLAN**.

   The **VLAN Configuration** page appears.

2. View the following details for each existing VLAN that appears in the **VLAN Configuration** table:
   
   - **Link**: The link on which the VLAN is configured. The status appears as "1+2".
   
   - **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 0 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

To set up a network VLAN to access the NSS:

1. From the Manager Menu, click Network → VLAN.

   The VLAN Configuration page appears.

2. In the New VLAN area of the page, set up the following fields:

   - **Link**: Select the Ethernet link on which you want the VLAN to connect to the NSS. Available options depend on the configuration of your Ethernet link(s).

   - **VLAN**: Enter the ID of the VLAN as it is defined within your network. The range of valid VLAN IDs is from 0 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.

3. Click **Add**.

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

4. Click **OK**.

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

5. Click **Edit** for the VLAN.
The Network Configuration page appears.

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.

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:

1. From the Manager Menu, click Network ➜ VLAN.

   The VLAN Configuration page appears.

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

   The VLAN Configuration page appears.

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

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:

1. From the Manager Menu, click Network ➤ VLAN.
   
   The VLAN Configuration page appears.

2. From the VLAN Configuration table, click Delete for the VLAN you want to remove.
   
   The VLAN disappears from the VLAN Configuration table and no longer has access to 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.

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

- Configure the IP and DNS information.
- Set up your user and group ID ranges on the User/Group Settings page. (see Configuring the User/Group Settings) You cannot make changes to the User or Group ID range after the domain is joined.

To configure the NSS network identity:

1. From the **Manager Menu**, click **Network ➤ Identification**.

   The **Network Identification** page appears.

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.
Warning: If you change the hostname, any current CIFS connections to shares on the NSS will be disconnected.

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.

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.

5. Select the type of network into which you are making the NSS a member from the following 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.
     - **Password**: Enter the password for the administrator account.
   - **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.
     - **Domain Controller**: Enter the hostname or IP address of the domain controller.
     - **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.
     - **Username**: Enter the username of an account that has administrator privileges for this domain.
     - **Password**: Enter the password for the administrator account.

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 (i.e., successful or not successful).
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:

1. From the Manager Menu, click Network ➔ DNS/WINS.

   The Network Name Resolution page appears.

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

   - **Search Domain**: Enter the address of the DNS search domain accessible by the NSS.
   - **Primary DNS Server**: Enter the IP address of the primary DNS server on your network.
   - **Alternate 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. This field is optional.
   - **Alternate WINS Server**: If your network has a secondary WINS server, enter its address. This field is optional.
• **Assign automatically via DHCP:** Select this to assign the IP address 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.

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 you set up or make changes to the NIS domain users and groups ID range on the User/Groups Settings page. (see Configuring the User/Group Settings) This minimizes the risk of collisions of user or group IDs within your network.

To configure the NSS for NIS:

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

The **NIS Configuration** page appears.

2. Select **Enable NIS**.

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

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.

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 Links

The NSS lets you test the physical network cables attached to Ethernet links 1 and 2 for certain fault conditions. You must manually initiate a test to update the results shown on the Network Diagnostics page.

NOTE: When you initiate a test on an Ethernet link, you take down the link for the duration of the test. Any current user connections on the link are dropped. If you have two links installed, any connections through the untested link remain unaffected.

To test the physical link:

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

   The Network Diagnostics page appears.

2. Click Test for the cable you want to test.

   After the test completes, the test results appear in the Link Status area. The test results also appear on the System Status page. If the cable is in sufficient working condition, the link is again accessible to your users.
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 in essence a shortcut to manually defining an equivalent network filter.

To set up the network services:

1. From the Manager Menu, click Network → Ports.

   The Network Ports Configuration page appears.

   ![Network Ports Configuration](image)

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. Note that to access the NSS GUI, 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.

   - **SSL 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.

3. Click *Update*.
Setting up the Link Bonding & Advertising Modes

The Network Properties page is where you configure the bonding mode for the physical Ethernet link(s) attached to the NSS. It also lets you determine how you want to advertise the presence of the NSS within your network.

To configure the network properties:

1. From the Manager Menu, click Network → Properties.

   The Network Properties page appears.

2. To set the bonding mode of your physical links, click one of the following:

   - **802.3ad Link Aggregation (failover and load sharing):** Select this option to aggregate the two Ethernet connections using the IEEE 802.3ad standard. This technology is also known as trunking or bonding.

   - **Active backup (failover):** This is the default option when you first install the NSS or when you restore the factory default settings by resetting the NSS. Select this option to define one link as the active link and one link as the backup. Should the active link become unusable (either disconnected or significantly degraded), the backup link automatically becomes the active link.

3. 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".

4. 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.

5. 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/Bonjour:** The NSS is advertised within the network using Zeroconf/Bonjour.

6. Click **Update**.
Managing your Storage

The Storage Status page is where you can view 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 very helpful for monitoring the progress of certain processes such as checking the condition of a drive.

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.
- **Capacity**: The size of the disk drive.
Chapter 4: Storage

Network Storage System (NSS) Administrator Guide

• **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.
  - **Locate**: Send a locate request to the applicable disk drive. The white disk drive LED on the front of the NSS chassis blinks for the targeted disk drive. (Note that only one locate request can be sent at a time to ensure that you can easily spot the desired disk drive. Disk drives
are numbered from 1 to 4 from left to right on the chassis (when facing the chassis front panel) and correspond with the port number.

- **Cancel Locate**: There is currently a locate request set up for the applicable disk drive. Click **Cancel Locate** to cancel the locate request. This lets you send a locate request for another disk drive.

**RAID Arrays Table**

The **RAID Arrays** table lists each array (either RAID or JBOD) currently configured. The table is made up of the following:

- **Label**: The name assigned to the array.
- **RAID Level**: The configured RAID level.
- **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. The calculation for an array, according to RAID level, is as follows. (Where "n" = the number of drives in the array and "s" = the size of the smallest drive in the array.)
  - JBOD = \( \text{sum(size of each drive)} \)
  - RAID0 = \( n \times s \)
  - RAID1 = \( s \)
  - RAID5 = \( (n-1) \times s \)
  - RAID10 = \( n \times s / 2 \)
- **Status**: The current condition of the RAID array. Options include:
  - **Clean**: The array is in a normal state. This 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 has been removed from the system or has failed. In this state, the array is fully recoverable. This 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 all 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. This status is color-coded orange. During the rebuild, the LED for the disk drive slowly blinks green.
  - **Stopped**: A RAID array has been 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. The table is made up of 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 has been locked and is not currently inaccessible. 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. The USB flash device can be used to save a backup of the configuration file (see Saving the Current Configuration). 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.
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 not technically a RAID level.

The following variables are used in formulas below which explain how 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

**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:** \( m \times n \)
- **Advantages:** Increased read and write performance.
- **Disadvantages:** Decreased reliability. A failure of any component disk in the array causes the entire array to fail.

**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 subsequently replaced, the array must copy the entire contents of a good disk to the new disk. This process is referred to as “resynching”. During a resync, the array continues to be available for reads and writes. When an array contains a failed disk, it is said to be 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 resynching mirrors.

**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 to
reconstruct the data lost when a drive fails in the array. When a failed disk is subsequently 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 synch 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:** \( m \times (n-1) \)
- **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.

**RAID10:** RAID10 is a combination of RAID1 and RAID0. The NSS implements RAID10 as two, 2-disk RAID1 mirrors, which are then used to build a RAID0 array. RAID10 can be thought of as “mirror, then stripe”.

- **Minimum Number of Disks:** 4
- **Total capacity:** \( 2 \times m \)
- **Advantages:** Increased read and write performance; increased reliability; the RAID array can sustain the loss of any single disk without data loss; depending on which disks fail, the array can lose up to two disks without data loss.
- **Disadvantages:** Decreased aggregate storage capacity (you lose half of the storage space)

**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 may 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, it is a good idea to set the Rebuild Priority (see Setting the RAID Rebuild Priority) to determine how you want to allocate the system resources for the rebuild.

NOTE:
When adding disks to an array, we recommend 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.

To create an array:

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

   The RAID page appears:

   ![RAID page screenshot]

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

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

   4. Click Add.

   The RAID creation can take some time to complete (depending on the size of the disks and the selected RAID level). When the build is finished, 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. As long as the array is clean, these disks then become spares.

**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 an array:

1. If not already installed in the chassis, insert the disk in the NSS.
2. From the Manager Menu, click Storage → RAID.

The RAID page appears.

3. In the RAID Arrays table, click Edit for the applicable RAID array.
The RAID Configuration page appears.

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. 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. Note that 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, note that you must assign a new volume as the Home Directory location.

To delete an existing array:

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

   The RAID page appears.

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

   A warning message appears.

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

If you are migrating a RAID array from the NSS to another network NSS, ensure that you coldplug the RAID array (versus hotplug it) into the new system as per the following:

1. Power down the NSS (from which you are removing the RAID array).
2. Remove each of the disk drives that make up the RAID array to be moved.
3. Power down the NSS to which you are migrating the RAID array.
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 (that is, you do not need to install them in the same order or slots that they were installed in the original NSS.

5. When all the disk drives are installed, power up the NSS.
Virtualizing Storage within your Network

The NSS virtualization feature lets you create storage physically located on other network NSS units into one logical storage unit. The recommended network configuration for using virtualization is to use an NSS6000 series to operate as the "master" storage device (the "slave" devices can either be NSS6000 series or NSS4000 series devices). This configuration setup means that you export storage (must be an unused disk drive or configured array) from the slave NSS and then import the storage into the master NSS. The supported RAID level for virtualized storage is JBOD (although the JBOD can consist of concatenated exported arrays).

Currently Exported Storage

The Currently Exported Storage table 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.
- **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.

Currently Imported Storage

For the master NSS to access a disk from another NSS on the network, the network device that contains the storage must first export its storage. Once the exported storage is involved in an array on the master device it appears in the Currently Imported Storage table. Until the exported storage is used to build a JBOD, the storage appears in the list of available disks in the New RAID Device table on the RAID page.

- **Device:** The name of the imported disk or array.
- **Size:** The size of the imported disk or array.
- **Exported by:** The serial number of the network device that exported the storage to the network.
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 as well as is affected by the conditions of the physical unit.

To export storage to the network:

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

2. From the Manager Menu, click Storage ➔ Virtualization.

   The Storage Virtualization page appears.

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

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

5. Click Export.

   The selected disk(s) disappear from the available list of arrays and appears in the Currently Exported Storage table at the top of the page. Follow the steps to create a JBOD from virtualized storage (see Creating Virtualized Storage) to use the exported 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 a NSS6000 series model). The designated master unit then becomes the configuration point for all your storage-related management. Exported storage can be used to create a JBOD, which can then be used 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.

To create a JBOD with exported disks:

1. Log in to the configuration interface from the master unit.
2. From the Manager Menu, click Storage → RAID.
   
   The RAID page appears.

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

3. From the New RAID Device table, click the disks or arrays that you want to include in the JBOD.
4. Select JBOD as the RAID level.
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. Note that you can only unexport storage that has not yet been used.

To unexport a piece of storage:

1. From the **Manager Menu**, click **Storage ➤ Virtualization**.

   The **Storage Virtualization** page appears.

   ![Storage Virtualization Page](image)

   - **Currently Exported Storage**
     - Device | Size       | Imported by | Action
     - SATA3  | 74.53 GB   | None        | Unexport
     - SATA4  | 74.53 GB   | None        | Unexport

   - **Currently Imported Storage**
     - Device | Size       | Exported by
     - None

   - **Export a device**
     - Device | Size | Link
     - None

2. 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 is where you can view the following details about configured volumes, or create additional 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 or GB).
- **% Used**: The amount of space, as a percentage, that is currently used.
- **Crypto**: Whether the volume is encrypted or not.
- **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:

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

   The Storage Volumes page appears.

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 (in MB):** Enter the size for the volume. The unit is in megabytes (MB). The final size of the shared volume will be 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 the volume is created, you can expand the volume but you cannot reduce its size.

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 a volume is created, you cannot change whether it is encrypted or unencrypted. Expect slower Read/Write performance when using encrypted volumes.

4. Enter a password in the Password field using a minimum of eight alphanumeric characters. The password must consist of at least three of the following: lower-case character, upper-case character, number (0-9), or a special character (such as #@*&^). The password must be entered to unlock an encrypted volume when the NSS is started up following a power interruption, shutdown, or reboot, or, if the volume was manually locked through the NSS configuration interface.

WARNING: 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 the password is forgotten, the only way to retrieve the password is if the password was saved in a configuration file. See Restoring the Configuration (see Restoring a Configuration File) for help on this.)

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

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:

1. From the Manager Menu, click Storage ➔ Volumes.
   
   The Volumes page appears.

2. Click Edit for the volume you want to expand.
   
   The Grow File System page appears for the selected volume.

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" and then enter 224 in the **Size** field. **Note:** The system rounds up the total space to the nearest 32 MB boundary.

• **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.

4. Depending on your choice in the previous step, enter the new number in the **Size** field. 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.

5. Click **OK**.
Deleting a Volume

You can choose to delete a volume at any time. **WARNING:** 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 the Home Directory Location to another volume.

To delete a volume:

1. From the Manager Menu, click **Storage ➤ Volumes.**

   The **Storage Volumes** page appears.

2. From the **Existing Volumes** area, click **Delete** for the volume you want to delete.
Viewing the Snapshot Reserve Details

You can configure the NSS6000 series NAS to take snapshots of the data on an existing volume. When you create a snapshot, a backup of each of the shares on the volume is created and is available within the file directory to which the end user has access. The advantage of a snapshot over a backup is that a snapshot is user-accessible and can be used for quick file recovery resulting from end user error (such as, an accidentally deleted file). A backup is only accessible to the administrator through the NSS configuration interface and restoring data through the backup can be timely. Backups are usually used to restore the system from a major system failure.

Snapshots can be taken at various time intervals (such as hourly, daily, and so on). Each time a snapshot is taken, the previous snapshot is overwritten. You can also configure multiple snapshots to occur at different time intervals for the same volume. For example, you might want to capture a snapshot each hour, weekly, and bi-weekly. In this case, the volume has three separate snapshots. Each snapshot is overwritten when the next snapshot of the same frequency is taken. To ensure data integrity, during the creation of the snapshot (the duration is approximately a few seconds), no writes can occur to the share.

The snapshot reserve is the amount of space that you want to allocate to the snapshot on the associated array. Once set, this space is not available for other storage use. The recommended amount of a reserve is generally between 10 to 20% of the total volume size. Note that if the period of time between snapshots is greater, the amount of the reserve should be greater. Or, if there is a heavy amount of activity on the volume, set a higher reserve. This is due to the snapshot reserve being used to store the changes to the volume contents since the last time the snapshot was taken.

NOTE: This feature is only available on the NSS6000 series NAS.
Maintaining Active Snapshots

You can view the list of configured snapshots by displaying the **Storage Snapshots** page. The **Currently Active Snapshots** area lists each snapshot set up for all the volumes on your NSS6000 series NAS.

The following column headings provide details about the snapshot:

- **Volume**: The name of the volume for which the snapshot is set up.
- **Frequency**: The time interval of the snapshot. If the time interval is set up to occur at a certain time of the week, day, or hour, it is also listed. For example, daily @ 10:30 means that the snapshot occurs each day at 10:30 a.m.
- **Size**: The size of the snapshot reserve.
- **Current Usage**: The percent of the space allocated for the snapshot currently taken up by the snapshot.
Creating a Snapshot for a Volume

As part of your backup strategy, you can configure the NSS6000 series NAS to capture snapshots of the data stored on a volume. You can define a snapshot to occur at various frequencies (such as hourly, daily, weekly, and so on). Individual snapshots are overwritten by the subsequent snapshot for the same interval. For example, if you set up an hourly snapshot, the 10:00 a.m. snapshot is replaced by the 11:00 a.m. snapshot (and so on). You can also configure multiple snapshots for the same volume. For example, you might set up an hourly snapshot, another snapshot to occur every four hours, and a daily snapshot. Each of these three snapshots is maintained separately and is only overwritten by the subsequent snapshot of its own frequency type. The snapshot(s) reside in the reserve area allocated for each snapshot. When a snapshot is created, the end user can access it by logging into the NSS with their username and password. Each snapshot appears as a copy of the share accessible by the end user.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>File</td>
<td>12/22/2007 4:20</td>
</tr>
<tr>
<td>snap_03_03_00.00</td>
<td>File Folder</td>
<td>12/22/2007 4:20</td>
</tr>
<tr>
<td>snap_03_03_00.25</td>
<td>File Folder</td>
<td>12/22/2007 4:20</td>
</tr>
</tbody>
</table>

The snapshot reserve is the amount of space that you want to allocate on the array to the snapshot. Once set, this space is not available for other storage use. The recommended amount of a reserve is generally between 10 to 20% of the total volume size. Note that if the period of time between snapshots is greater, the amount of the reserve should be greater. Or, if there is a heavy amount of activity on the volume, set a higher reserve.

NOTE: This feature is only available on NSS6000 series NAS units.

To create a snapshot for a volume:

1. From the Manager Menu, click Storage ➔ Snapshots.
The **Storage Snapshots** page appears.

2. From the **New Snapshot** table, click the volume for which you are creating the snapshot.

3. Depending on the frequency, use the first part of the **Every** field to enter a unit of time. Tab to the second part of the **Every** field, and then click the snapshot frequency (that is, hours or days). For example, set the first part of the field to "7", and the second part to "Days" to take a snapshot once every week.

4. Use the **At:** fields to set up the timing for the snapshot. For example, if the frequency is set to Days, set the hour and minute of the day at which you want the snapshot to be taken. **Note:** When entering the hour, use the 24-hour clock. For example, 3 p.m. should be entered as 15:00. When the frequency is set to Hours, you can only edit the minutes part of the **At:** field.

5. In the **Reserve Size** field, enter the amount of space (in MB) that you want to allocate to the snapshot. This space becomes unavailable for any other storage on the array. Note that you must enter a minimum of 32 MB in this field.

**NOTE:** The snapshot is built at the array level. The **Volume** column currently shows the amount of space left on the array on which the volume is located. To calculate the reserve size, refer to the applicable volume size as listed on the **Volume** page.

6. Click **Add** to save the snapshot.

The snapshot details appear in the **Currently Active Snapshots** area at the top of the page.
Taking a Manual Snapshot of a Volume

There might be times when you want to take a snapshot of a volume that falls outside of the regularly scheduled snapshot times. When you take a snapshot of a volume using the resnap function, the newly taken snapshot overwrites the previously existing one for the specified interval. For example, if you have a snapshot set up to occur hourly and then click Resnap, a new snapshot is built that overwrites the existing hourly snapshot.

**NOTE:** This feature is only available on NSS6000 series NAS units.

To take a manual snapshot:

1. From the Manager Menu, click Storage ➔ Snapshots.

   The Storage Snapshots page appears.

2. Click Resnap next to the volume for which you want to take a snapshot.

   The snapshot takes seconds to complete. To ensure data integrity, no writes can occur to the share until the snapshot is complete.
Windows End Users: Accessing a Snapshot for a Share

After a snapshot is created for a volume, a file folder appears in the end user's file directory for each share to which the end user has access. Snapshots are saved with the name of the share followed by an underscore and then the term "snap". Each file folder contains a subfolder for each snapshot interval (for example, hourly, daily, etc.).

To access a snapshot for a share:

1. There are a variety of ways 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. For example, `\NAS`).
   - Browse for the NSS from the My Network Places window.
   - Map the NSS to a network drive.

   The Log In window appears.

2. Enter your NSS user name and password.

3. Click OK.

   The Windows Explorer window opens with a directory listing of the folders for the shares available on the user's home directory

4. Snapshots are read-only. To work with a snapshot, locate it, take a copy of it, and then place the copy in a working directory.
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.
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:

1. From the Manager Menu, click Storage ➔ Volumes.
   
   The Volumes page appears.

   ![Screenshot of Volumes page with a list of volumes including their location, total space, used space, and encrypted status.

   The Crypto column displays whether the volume is encrypted (Yes) or not encrypted (No).

2. Click Lock to lock the volume.
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:

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

   The Volumes page appears.

2. Click Unlock for the volume you want to unlock.
The **Unlock Volume** page appears.

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

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 (see Creating a Volume). After the volume is created, 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. **WARNING:** 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 the password is forgotten, the only way to retrieve the password is if the password was saved in a configuration file. See Restoring the Configuration (see Restoring a Configuration File) for help on this.)

To change the password on an existing encrypted volume:

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

The **Volumes** page appears.
2. Click **Edit** for the volume you want to change.

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

4. In the **New Password** field, enter the new password. **Note:** The password must be at least eight characters of which at least three of the following characteristics are included: lower-case character, upper-case character, integer (0 to 9), and a special character (such as @#$%^&*).

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

6. Click **Update**.
Storage Options

The Storage Options page lets you define the following:

- **Idle Drive Spin Down**: [see Setting the Spin Down Time](#) Configure the NSS to spin down the disk drives after a predefined time of inactivity.

- **RAID Rebuild Priority**: [see Setting the RAID Rebuild Priority](#) Control how the system prioritizes the RAID rebuild and allocates the system resources based on the current workload and need for responsiveness.

- **Degraded Mode Grace Period**: Set the period of time after which the system automatically shuts down degraded arrays. You can manually restart RAID arrays automatically stopped by using degraded mode management. 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 (via storage virtualization). A system limited to local disks lets you only build up to two, two-disk RAID arrays, but have no spares.
Setting the 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 configure the RAID rebuild priority:

1. From the Manager Menu, click Storage ➤ Options.

   The Storage Options page appears.

2. From the RAID Rebuild Priority menu, select the allocation of CPU processing power to the RAID rebuild task.

   - **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 RAID rebuild when this setting is chosen.

   - **Medium**: This option gives 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. Note that if you are repairing an array, this option leaves the array vulnerable until the rebuild is complete.

3. Click Update.
Setting the Spin Down Time

You can configure the NSS to spin down the disk drives after a predefined time of inactivity. This reduces the power consumption of the system and can possibly increase the lifespan of drives. Because of the potential risks and benefits of spinning down a disk versus leaving it running in an idle condition, we recommend you consult the disk drive manufacturer documentation for the optimum way to handle the disk.

To configure the disk drives for spin down:

1. From the Manager Menu, click Storage ➤ Options.

   The Storage Options page appears.

2. In the Idle Drive Spin Down field, select the period of time that the disk drive must be idle before it is spun down. (Select "Never" to ensure that the drives are never spun down.)

3. Click Update.
Administering Access to the NSS

The Access Status page lets you view 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 like the Access Status page 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.
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 via the NSS configuration interface or imported from an NTv4, Active Directory, or NIS domain. Note that users not created locally via the NSS are read-only. 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.
Creating a User Profile

Depending on your network setup, you might administer users and groups locally or via the domain controller. The NSS configuration interface gives you read-only access to users and groups provided by NTv4, Active Directory, or NIS domains. 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:

1. From the Manager Menu, click Access > Users.

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

2. Click Add to create a user.

   The New User page appears.

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.

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.

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

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.

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.

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

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. Note that 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. If the user profile resides on an ADS, NTv4, or NIS domain, you need to edit the profile from the applicable domain 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:

1. From the Manager Menu, click Access → Users.

   The Configured Users page appears.

   ![Configured Users page](image)

   The existing users appear in the Configured Users table.

2. Select the user from the list, and then click Edit.
The end user’s profile appears in the **Edit User** page.

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

4. Click **Update**.
Integrating Users from an ADS, NTv4, or NIS Domain

Overview

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 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: It is important to 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 should not make changes to the range 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

To delete an existing user profile:

1. From the Manager Menu, click Access ➔ Users.

   The Configured Users page appears.

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, and then click the first user and then 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.
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. Note that each user is assigned a primary group within their user profile. When a user creates a file, the group ownership is automatically set to the user’s primary group. The user’s storage usage is charged to the user’s 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 add a group to file ACL on a CIFS share.

To create a group:

1. From the Manager Menu, click Access ➔ Groups.

The Configured Groups page appears.

2. Click Add.
The New Group page appears.

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.

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.)

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/log on to their computer.

To change the group membership:

1. From the Manager Menu, click Access ➔ Groups.
   
   The Configured Groups page appears.

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

3. Click Edit.
   
   The Edit Group page appears.

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.)

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 are imported into the Configured Groups list. 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:**

It is important to 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 should 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:

1. From the Manager Menu, click Access ➔ Groups.

The Configured Groups page appears.

2. You can delete a group from two locations in the NSS configuration interface:

   - **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, and then click the first group and then 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.
- **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. Defining a user or group’s quota means that 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 below 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 below their soft quota limit.

**NOTE:**
Before you create or edit a quota located on an encrypted volume, make sure the volume is unlocked. You also need to set up the Warn For time for each volume from the Volume 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. Note that 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 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.
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 it is unlocked. You also need to set up the Warn For time for each volume from the Volume 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:

1. From the Manager Menu, click Access → Quota.

   The Volume Quota page appears.

2. Click New Quota.
The **New Volume Quota** page appears.

3. Select the volume on which you want to set the quota from the **New Quota on FS** drop-down list.

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

5. In the **Warning at (MB)** field, enter the threshold of space that, when exceeded, triggers a warning that the quota is close to being used up. 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 below the space set in the **Warning at (MB)** field or they will not be allowed to write further data to the volume. Another way to think about this field is as a "soft quota".

6. In the **Space Limit (MB)** field, enter the amount of space that the user or group has available to use. 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 below the limit by deleting files or have the quota increased.

7. Click **Update**.
Chapter 5: Access

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 user reaches their "soft quota", a warning is issued and the grace period begins. The user then has the amount of time set in the grace period to either reduce the amount of space 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 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:

1. From the Manager Menu, click Access ➤ Quota.
   
   The Filesystem Quota page appears.

2. To set up the grace period, after which 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.

3. Click Update.

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:

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

   The Filesystem Quota page appears.

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

   The Edit Quota page appears.

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

4. Click OK.
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 delete a quota for a user or group:

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

   The Volume Quota page appears.

   Quotas are displayed according to their associated volume.

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 via the various supported protocols.

To view the network filters:

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

   The Network Filters page appears.

2. You can do any of the following:
   
   - Set the default network policy (see Defining the Default Network Policy) to control what happens to traffic not explicitly covered by defined filters.
   
   - View or delete the existing filters (see Network Filters Overview) defined for the NSS from the Active Network Access Filters table.
   
   - Create a new filter (see Creating a Network Filter) based on an IP or MAC address or a range of IP addresses.
Chapter 5: Access
Defining the Default Network Policy

The default network policy is the overarching 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:

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

   The Network Filters page appears.

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.

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 via the specified protocol from the specified IP/MAC address or range of IP addresses.

To add a network filter:

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

   The Network Filters page appears.

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:

   - **An 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.)

   - **A 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).
3. Select the type of filter you want to apply to the IP/MAC address from the **Filter** drop-down menu.

4. Click **Add**.
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.

**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 via all supported protocols.
- **Allow CIFS:** Allow CIFS filesharing access.
- **Allow FTP:** Allow FTP and FTPS access.
- **Allow HTTP:** Allow access to the NSS configuration interface via a Web browser.
- **Allow NFS:** Allow NFS access.
- **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 or 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 via a Web browser. 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 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 or 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 via a Web browser. 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:

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

   The Network Filters page appears.

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 Settings

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 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 will use to store your users’ home directories.

To set up the ID ranges and home directory location:

1. From the Manager Menu, click Access ➤ Options.

   The User/Group Settings page appears.

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 large. 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 be changed.

3. Set the volume that you want to assign as the home directory location for your users via the Home Directory Location field.

4. Click Update.
Managing the Shares

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

There is a limit of about 20 users that you can assign to a share. To assign more than 20 users, assign the applicable users to a group or groups and then assign the group to the share.
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 about 20 users that you can assign to a share. To assign more than 20 users, assign the applicable users to a group or groups and then assign the group (or groups) to the share.

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:

1. From the Manager Menu, click Share ➔ Shares.
2. Click Create New Share.

The New Share page appears.

3. Enter a name for the share in the Share field.
4. From the Location field, select the volume on which you want to configure the share.
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.

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 ensure the **Read-Only** checkbox is deselected.
   - **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.

7. Set up the defaults for how file permissions are set when a file is created using CIFS via the following **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 via 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 via 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 via 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 via CIFS, the group is automatically assigned as the owner’s default group. This group cannot be edited at a later time.
   - **World Readable**: All authenticated users can view the file.
   - **World Writable**: All authenticated users have write permission to the file.

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

9. 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.)

**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.

10. 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 direction of the bracket. The double angled bracket "<" or ">" moves the entire list in the direction of the bracket.)

• **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.

11. 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.

To edit a share:

1. From the Manager Menu, click Share ➔ Shares.
2. Click Edit for the share you want to change.

The Edit Share page appears.

3. Although the Location field lets you make changes to the volume on which the share is located, if you change the location of the share, existing data on the share is NOT migrated. Doing so will orphan existing data.

4. 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).

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.

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 via CIFS, the group is automatically assigned as the owner’s default group. This group cannot be edited at a later time.

- **World Readable**: All authenticated users can view the file.

- **World Writable**: All authenticated users have read-write permissions for the file.

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.
- **FTP**: Enable FTP access to the share.

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.)

- **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.

9. Use the last two tables on 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 direction of the bracket. The double angled bracket "<<" or ">>" moves the entire list in the direction of the bracket.)

- **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.

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 folders as a single set of shares through a familiar, unified folder hierarchy, even when those resources reside on different servers. The NSS can act as a root or leaf. Whichever way you establish the link between the NSS and the DFS, you will have created a transparent link between the NSS and the DFS folders located on remote servers. When you create a DFS folder from a share, note that the user must have privileges set up to access the NSS share. After the user accesses the DFS folder through the NSS share, the user’s access rights to the DFS folder are those assigned for the specific DFS folder.

To add a DFS root directory to a share on the NSS:

1. From the Manager Menu, click Share ➔ Shares.

   The File Shares page appears.

2. Click Edit for the share to which you want to add a folder.

   The Edit Share page appears.

3. Click Add Shared Folder.
The Add Folder page appears.

4. Select one of the following:
   
   - **Add a Folder to DFS**: Select this option to create a DFS root directory. 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 a user clicks this link, they are redirected to the target share on the remote server. Enter any name of up to XX characters.
     
     - **Server Name**: Enter the name of the DFS server on which the target DFS share is located.
     
     - **Share**: Enter the name of the target DFS 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 account with access to the server.
     
     - **Password**: Enter the password for the above account.

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

**NOTE:**

Make sure you review the restrictions and recommendations (see Restrictions using Microsoft DFS from the NSS) 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 tree, 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.

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

1. From the Manager Menu, click Share ➔ CIFS Setup.

   The CIFS Networking Configuration page appears.

2. Enter the amount of time (in seconds) that the CIFS connection can be idle, after which it is disconnected.

3. Click Update.
Chapter 6: Share
Setting up Network Filesystem (NFS) Access

The first step to enable NFS access to the NSS is to enable it globally. You will 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:

1. From the Manager Menu, click Share ➔ NFS Setup.

   The NFS Setup page appears.

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

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 would normally do. Instead they continue immediately after committing the write. This can improve performance if the NSS is heavily used.

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.

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:

1. From the **Manager Menu**, click **Share ➔ FTP Setup**.

   The FTP Setup page appears.

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

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

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

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.

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

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 checked.

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.

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.

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.

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.)

13. 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.
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:

1. From the Manager Menu, click Share → Backup.

2. Click Schedule Backup.

   The Scheduled Backup page appears.

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.)

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.

5. Click Next.
Chapter 6: Share
Creating a Scheduled Backup for a Share

The **Select Backup Schedule** page appears.

6. 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 you select a day that is 28 or less. If you select the 29th, 30th or 31st day, the backup will not run during months that do not contain that day.

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

8. 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.

9. Click **OK**.
Initiating a Backup for a Share

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

To initiate a backup manually:

1. From the Manager Menu, click Share ➔ Backup.

   The Scheduled Backup page appears.

2. Click Run Backup.
The *Run a Backup* page appears.

![Image of Run a Backup page]

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.)

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.

5. 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:

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

   The share's contents appear.

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

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

- Rebooting or Shutting down the system (see Rebooting or Shutting Down the NSS)
- Upgrading the firmware (see Upgrading the NSS Firmware)
- Restoring configuration settings to factory defaults (see Restoring the Factory Default Configuration)
Rebooting or Shutting Down the NSS

In situations where you might need to reboot or shut down the NSS, note that 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 employ a UPS (and optionally an RPSU) to ensure that power to the NSS is never interrupted. Refer to the Troubleshooting topic "Handling an Unexpected Shutdown (see Handling an Unexpected (Unclean) Shutdown)" for more information. During a reboot or shutdown of the NSS, the color and blink rate of the Power LED (see LEDs & Buttons) on the front of the chassis indicates the status of the currently selected process.

To reboot or shut down the NSS:

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

The System Details page appears.

2. Click one of the following:

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

   **NOTE:** Make sure when the system is rebooting that you close the Web browser. 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 by pressing and holding the Reset button on the front of the chassis until the Power LED starts to flash (you must then release it).

   A warning message appears.

3. Click OK to continue.
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

WARNING: When you upgrade the firmware, avoid using a wireless connection to the NSS as wireless connections can be unreliable and cause image corruption. Do not interrupt the power during the firmware upgrade. The system will reboot 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:

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.

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

3. From the Manager Menu, click Admin ➔ Maintenance.
   The System Details page appears.

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

5. Click Upgrade Firmware to initiate the upgrade process.

6. When the firmware upgrade completes, the system automatically reboots. Wait until the Power LED is a solid green before you log back into the configuration interface.

For more information about the behavior of the Power LED, refer to the LEDs & Buttons (see LEDs & Buttons) section.
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 just the network settings so that you can log into the NSS configuration interface.

To reset the NSS:

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

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**.

   - **Reset the Network Settings to Enable you to Access the Configuration Interface**: If there is a problem with the NSS that results in your not being able to access the NSS configuration interface, you might need to reset the network settings. This lets you access the interface and make any further changes 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. Note the following settings are reset to their default:

- **Link Addressing**: DHCP
- **Link Bonding Mode**: Active Backup
- **NSS Hostname**: nas<MAC address of primary link> For example, "nas0123456789ab"
- **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.

⚠️ **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 display the Configuration Manager page, from the Manager Menu, click Admin › Configuration.
Saving the Current Configuration

You can save a copy of the NSS configuration that can be used should 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:

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.

2. From the Manager Menu, click Admin ➔ Configuration.

   The Configuration Manager page appears.

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.

4. Click Update.

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

![Storage Status Page](image)

7. Click **Unmount**.

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

8. 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.
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:

1. From the Manager Menu, click Admin ➔ Configuration.
   The Configuration Manager page appears.

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.

3. From the Stored Configuration Location field, select the volume that contains the saved configuration file.

4. Click Update.

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.

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 may 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.

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

8. Close the Web browser.

After a few minutes the system will reboot.

9. Check the Power LED (see LEDs & Buttons) on the front of the chassis. The Power LED goes to a solid green when the reboot completes.

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

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

12. Click Unmount.

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

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:

1. From the Manager Menu, click Admin ➔ Configuration.

   The Configuration Manager page appears.

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.

3. Click Restore.

   A list of saved configuration files appear.

4. Click Delete for each configuration file you want to remove.
Configuring the Timing Settings

If you are installing the NSS within the Linksys One environment, the NSS time is automatically set via the Linksys NTP server.

When you first configure the NSS, ensure that the NSS has successfully synchronized the time with the NTP server. 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:

1. From the Manager Menu, click Admin ➔ Time.

   The NTP Configuration page appears.

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

3. If your DHCP server is configured to provide NTP settings, then select "Assign automatically via DHCP". If not, you must manually configure the NTP settings. In the NTP Server fields, enter the IP address or hostname for the NTP servers you wish to synchronize. Note that the settings in these fields are also be 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.

4. Click Manually.
5. Enter the date and time in the **Date and Time** fields.
6. Select your timezone from the **Timezone** drop-down menu.
7. Click **Update**.
Chapter 7: Admin
Configuring SNMP Alerts

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

To define SNMP Trap Sinks:

1. From the **Manager Menu**, click **Admin ➔ SNMP**.
   The **SNMP Trapsinks** page appears.

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

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.

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

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 is above temperature threshold, 3) 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.

   - **Snapshot**: When a snapshot reserve is more than 90% full.

   - **Quota**: When a user or group is over their quota.

   - **Backup**: When a backup job completes.
• **UPS:** When any of the following occurs: 1) the UPS goes online, 2) the UPS goes on battery, 3) the battery is low, 4) the NSS establishes contact with the UPS, 5) the NSS loses contact with the UPS (after communication was successfully established), 6) the UPS is about to shut down the system, 7) the UPS battery needs to be replaced, 8) the NSS cannot talk to the UPS.

6. Click **Add**.

   The management station appears in the **Existing SNMP Trap Sinks** list.

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

8. To send a test alert for each of the selected conditions to all configured trap sinks, click **Test All**. To delete an existing SNMP Trap Sink, 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:

1. From the Manager Menu, click Admin ➔ Password.

   The Admin Password Configuration page appears.

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

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

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

5. Click Update.

   The new password is in effect immediately. The next configuration interface page that you access will prompt you for the new password.
Accessing the NSS’s Storage

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:

1. There are a variety of ways to access the CIFS shares on the NSS:
   - 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").
   - Browse for the NSS from the My Network Places window.
   - Map the NSS to a network drive.

   The Login window appears.

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

3. Click OK.

4. As the administrator, you have read-write access to all the shares and all files and folders within those shares. You can delete files (such as backup images) as required.
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:

1. There are a variety of ways 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.

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

3. Click OK.

   The Windows Explorer window opens with a directory listing of the shares accessible by the user.

4. Depending on your privileges to the share, 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: 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. Refer to the online help from the NSS configuration interface for detailed help.

To access the NSS storage using FTP:

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

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

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

3. Depending on your privileges to the share, you can begin using the NSS storage.
Mac Users: Accessing Storage through CIFS/SMB

Mac 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 via CIFS/SMB:

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

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.

3. Click Connect.

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), you need to enter the following: <NSS hostname>/<user name>.

5. Depending on your privileges to the share, you can begin using the NSS storage.
Mac Users: Accessing Storage through FTP

Mac users who have a user profile set up can access any shares to which they have privileges on the NSS storage using FTP.

**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. Refer to the online help from the NSS configuration interface for detailed help.

To access the NSS storage using FTP:

1. Open your FTP client application.
2. Click **Connect**.
3. From your FTP client application, connect to the NSS. You need to enter the IP address or hostname of the NSS. For more information about using your FTP client application, refer to its documentation.
4. Enter your username and password when prompted by your FTP client.
   - When your FTP client has logged in, a list of shares accessible by the user appears as individual directories.
5. Depending on your privileges to the share, you can begin using the NSS storage.
UNIX/Linux Users: Accessing Storage through NFS

UNIX/Linux users can access shares on the NSS via 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.

1. Log into client system as root.
2. Create a mount point directory for the mount if you do not already have one (e.g., mkdir /mnt/nas_share1).
3. Mount the NFS share by typing "mount -t nfs -o nfsvers=3 <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.
4. Log out of the root account.
5. Log into the user account on client system.

You should now have access to the share via the mount point directory on your client. You will have the same privileges to the share as 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:** 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. Refer to the online help from the NSS configuration interface for detailed help.

To access the NSS storage using FTP:

1. Open your FTP client application.
2. Enter the NSS hostname/IP address.
3. Enter any other required settings. If using FPS, ensure that the client is set to use Explicit FTPS. For more help using the FTP client, refer to the FTP client documentation.
4. Enter your username and password when prompted by the FTP client.
5. Depending on your privileges to the share, you can begin using the NSS storage.
Glossary

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: In a NAS, 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.

**Gigabyte (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.

**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 Linksys Business Series NSS product.

**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.

**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...
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: In a NAS, 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 Linksys Business Series 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.
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.

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.

RPSU: Redundant Power Supply Unit. A device, typically rack mountable, that provides instant power should the power fail to a device (such as a network switch or NAS). Implementing an RPSU in a network wiring closet provides a greater degree of availability for devices on the network.

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 NAS 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.
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 Linksys 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 Linksys 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 0–1023.

**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

LEDs & Buttons

The LEDs on the front and back of the NSS chassis help you troubleshoot a variety of conditions on the NSS—from normal operating condition, 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 LED (Front Panel)

The Power LED can be in any of the following states, depending on the current state of the NSS:

- **Solid Yellow**: The NSS is powered on and the boot loader is currently running. The boot loader will run for approximately 10 seconds at the beginning of the startup of the NSS, after which the LED goes to a blinking green.

- **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.

System LED (Front Panel)

The System LED can be in any of the following conditions, depending on the current type of system error on the NSS:
• **Solid Yellow:** The administrator needs to look into the exact error condition through the configuration interface as one of the following has occurred:
  
  - 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.
  - The NSS is running on RPSU due to an internal power supply failure.

• **Solid Red:** There is a critical system failure where both firmware images are corrupt and are not bootable.

• **Off:** There are no system-related problems.

**Reset Button (Front Panel)**

The **Reset** button lets you 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.

**LAN LEDs (Front Panel)**

**Solid Green:** The LAN link is up and running at 1000 link speed, but is currently idle.

**Blinking 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.

**Blinking 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 (Front Panel)**

The LEDs associated with each of the installed disk drives indicate the disk drive activity, error condition, and locate state.

The various states of the green LED indicates the drive activity:
• **Solid Green:** The disk drive is configured but is currently idle.

• **Flicker 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).

The various states of the red LED indicate whether 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.).

• **Off:** The drive is OK.

The various states of the white LED indicate whether there is a locate request currently on the disk drive:

• **Blinking White:** There is a locate request currently on the disk drive (from the *Storage Status* page on the configuration interface). Note: There can only be one locate request set for a disk drive at one time.

• **Off:** The disk drive is not marked by a locate request.

**USB LED (Front Panel)**

**Solid Green:** The USB hard/flash drive is connected and is not safe to remove.

**Blinking Green:** The USB hard/flash drive is connected and is being mounted or unmounted.

**Off:** There is either no USB hard/flash drive connected to the NSS, or, if connected, the USB hard/flash drive is safe to remove.

**UPS LED (Back Panel)**

**Off:** There is either no UPS attached to the NSS or the UPS function has been disabled in the *System Power* page (see Configuring the System for UPS Support) in the configuration interface.

**On:** A UPS is attached to the NSS and the UPS function is enabled in the *System Power* page (see Configuring the System for UPS Support) in the configuration interface.
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 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 will need to 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:

1. If you are replacing a disk, remove the failed drive from the NSS and install the replacement disk.
2. From the Manager Menu, click Storage ➤ RAID.

   The RAID page appears.

   ![RAID page screenshot]

3. In the RAID Arrays table, click Edit for the applicable RAID array.
The RAID Configuration page appears.

4. Available disk drives appear in the listing. Click **Add** to add the disk drive it 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. You can monitor the progress of the rebuild through the **System Status** page.
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:

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.)

2. Reboot the NSS. Make sure you do a safe reboot using the Reboot function (see Rebooting or Shutting Down the NSS) from the System Details page.

3. When the system reboots, log into the configuration interface.

4. From the Manager Menu, click Storage ➔ RAID.

   The RAID page appears. The failed array appears with a status of "Stopped".

5. Click Delete.

   The disk drives used in the failed array become part of the available storage.

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.
Free Bound Aggregation Storage when the Master System Fails

**Problem Scenario:** A storage system is bound to a failed storage system and rejects any bind requests from other systems. The steps to recreate this problem are as follows:

1. Export storage from System A.
2. Import storage from System A to System B.
3. System B crashes and cannot be recovered.
4. System A is "bound" to System B and rejects any new bind requests from other systems.

**Resolution:** To resolve the problem:

1. Unexport the bound storage system (in our example, System A).
2. Re-export the storage system.

   The storage system is now available to be used by another system.
All CIFS Connections were Unexpectedly Ended

Problem: All current CIFS connections to the NSS were unexpectedly severed.

Solution: Check if the hostname set up in the Network Identification page has been changed. Changing the hostname will sever any current CIFS connections to the NSS.
Hotplugging the Ethernet Link doesn’t Reset IP or Link Rate

Problem Scenario: When you disconnect an Ethernet link and reconnect it, the IP address and link rate should reset. For example, if you unplug a cable from the NSS to a 100 Mbps switch and then reconnect the NSS to a 1 Gbps switch, the link is not restored.

Resolution: To resolve the problem:

1. Unplug the desired Ethernet link.
2. Wait at least 15 seconds.
3. Reconnect the link.
4. Wait 10 seconds.

The link should be re-established correctly. You can view the status from the System Status page on the configuration interface.
Unable to Create a Share or Quota for a Volume

**Problem Scenario:** You cannot create a quota or share. 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.

**Resolution:** 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 Location). To resolve the problem:

1. From the Manager Menu, click Storage ➤ Volumes.

2. If the problem is due to the volume being locked, the Unlock button appears next to the volume in the Action column. Click Unlock.

3. Enter the password for the volume.

4. Click OK.

   You should now be able to create a share or quota for the volume.
Cannot access the NSS through FTP

**Problem Scenario:** Users attempt to log into the NSS through FTP but are unable to access their home directory or shares on the NSS.

**Resolution:** There are several configuration settings that must be defined to enable FTP access.

1. From the Manager Menu, click Shares ➤ FTP Setup.

2. Ensure Enable FTP is selected. (You can go through the settings on this page to ensure they are correctly defined.)

3. Close the FTP Setup page.

4. From the Manager Menu, click Shares ➤ Shares.

5. Click Edit for the applicable share.

6. Make sure the FTP protocol is selected, and then click Update.

7. From the Manager Menu, click Access ➤ Network.

8. Make sure there are no filters set up to drop or reject FTP access for the applicable IP or MAC addresses.
Configuration Page does not Appear in Internet Explorer

Problem Scenario: When you click a configuration page, the page does not appear. This is a known caching problem with the Internet Explorer browser.

Resolution: The problem can be resolved by changing the Internet Explorer settings. Note: The following steps describe how to change the settings for Internet Explorer version 6.0. The exact steps for other versions of Internet Explorer might vary slightly.

1. From the Internet Explorer browser window, click Tools ➤ Internet Options.
2. Click General, and then click Settings.
The **Settings** window appears.

3. Under the **Check for newer versions of stored pages:** section, click **Automatically**.

4. Set the **Amount of disk space to use** to 1 MB.

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. 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 two ways: 1) when the NSS powers up, an SNMP trap sends a notification, and 2) when the Administrator first logs into the configuration pages following the shutdown, a message appears. If, after you follow the steps listed below, a problem persists, you might need to restore to factory defaults via the configuration interface and then restore from a USB backup or restore the settings manually.

Following an unclean shutdown of the NSS:

1. Do one of the following:
   - **Review/Edit the System Settings Manually:** Go through each setting, including the time setting to ensure nothing has been negatively altered. If you make changes to the settings, we highly recommend 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 just to restore the system settings from the backup (versus manually going through and checking each system setting).

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".
Support Contact Information

Need to contact Linksys One?
Visit us online for information on the latest products and updates to your existing products at
http://www.Linksys.com

Customer Service Contacts
If you experience problems with any Linksys One product, you can call us at:
1-866-870-5826

For Email Service, submit your requests or questions on-line at www.Linksys.com

(Details on Warranty and RMA issues can be found in the Warranty Information section in the product’s Quick Installation Guide.)

Normal business hours for RMA Customer Service are from 6 AM to 8 PM Pacific Time Monday through Friday, and 8 AM to 5 PM Saturday and Sunday.

Phone: (800) 546-5797 (Option 3)
Fax: (949) 823-3007

For Email Service, submit your requests or questions on-line at www.Linksys.com

Corporate Contacts
Normal business hours are from 8 AM to 5 PM Pacific Time Monday through Friday.
Phone: (949) 261-1288
Fax: (949) 823-3002

Sales Contacts
Normal business hours are from 7 AM to 5 PM Pacific Time Monday through Friday.
Phone: (800) 546-5797 (Option 1)
Fax: (949) 823-3007

For Email Service, submit your requests or questions on-line at www.Linksys.com