NETGEAR ReadyNAS User Guide

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10320-01
v1.0
October 2007

Technical Support

Registration on the website or over the phone is required before you can use our telephone support service. The phone numbers for worldwide regional customer support centers are on the Warranty and Support Information card that came with your product.

Go to *http://kbserver.netgear.com* for product updates and Web support.

Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, X-RAID, FrontView, RAIDar, RAIDiator, Network Storage Processor, and NSP are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Certificate of the Manufacturer/Importer

It is hereby certified that the ReadyNAS Network Attached Storage has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß dasReadyNAS Network Attached Storage gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Product and Publication Details

Model Number:	
Publication Date:	October 2007
Product Family:	Network Storage
Product Name:	ReadyNAS Network Attached Storage
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10320-01
Publication Version Number:	1.0

Contents

NETGEAR ReadyNAS User Guide

About This Manual

Chapter 1
Configuring Your ReadyNAS

Chapter 2
Accessing Shares from Your Operating System

Chapter 3
Maintenance and Administration

Appendix A
RAID Levels Simplified

Appendix B
Input Field Format

Appendix C
Glossary

Index

About This Manual

Congratulations on your purchase of a ReadyNAS Network Attached Storage system from NETGEAR, Inc. If you have not already done so, please read the printed *Installation Guide* provided with your product and the *ReadyNAS Setup Manual* on the *Installation CD.*

The *ReadyNAS Setup Manual* takes you step-by-step through the FrontView Setup Wizard and quickly prepares the ReadyNAS for your network. The *NETGEAR® ReadyNAS User Guide* explains each of the available options in detail, including many of the advanced options not described during the Setup Wizard process. The manual includes:

Chapter 1, "Configuring Your ReadyNAS," describes all the menus and tabs available in the FrontView Advanced Control mode.

Chapter 2, "Accessing Shares from Your Operating System." If you have already configured the ReadyNAS and you need help in accessing the shares on the ReadyNAS, skip to this chapter.

Chapter 3, "Maintenance and Administration":

- If a disk fails, learn about the proper procedure for replacing the failed disk in "Replacing a Failed Disk."
- If you need to reinstall the firmware or reset the system back to the factory default configuration, see "Resetting Your System (System Switch)" for an explanation of both.
- "Changing User Passwords" covers users other than administrators can access FrontView to change their password.

Appendix A, "RAID Levels Simplified," explains the RAID levels that the ReadyNAS supports.

Appendix B, "Input Field Format," covers questions on what constitutes a valid input for hostname, workgroup, or password.

Appendix C, "Glossary," provides definitions for some of the technical terminologies used in this document.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompts, CLI text, code
italic	URL links

- **Formats.** This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Tip: This format is used to highlight a procedure that will save time or resources.

Warning: Ignoring this type of note might result in a malfunction or damage to the equipment.

Danger: This is a safety warning. Failure to take heed of this notice might result in personal injury or death.

- **Scope.** This manual is written for the ReadyNAS according to these specifications:

Product Version	1.0
Manual Publication Date	October 2007

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forward or backward through the manual one page at a time.
- A ☰ button that displays the table of contents and a ☷ button that displays an index. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print This Manual

To print this manual, you can choose one of the following options, according to your needs.

- **Printing a page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.
- **Printing from PDF**. Your computer must have the free Adobe Acrobat Reader installed for you to view and print PDF files. The Acrobat Reader is available on the Adobe website at *http://www.adobe.com*.
  – **Printing a PDF chapter.** Use the **PDF of This Chapter** link at the top left of any page.
    - Click the **PDF of This Chapter** link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
    - Click the print icon in the upper left corner of your browser window.

  – **Printing a PDF version of the complete manual**. Use the **Complete PDF Manual** link at the top left of any page.
    - Click the **Complete PDF Manual** link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

- Click the print icon in the upper left corner of your browser window.

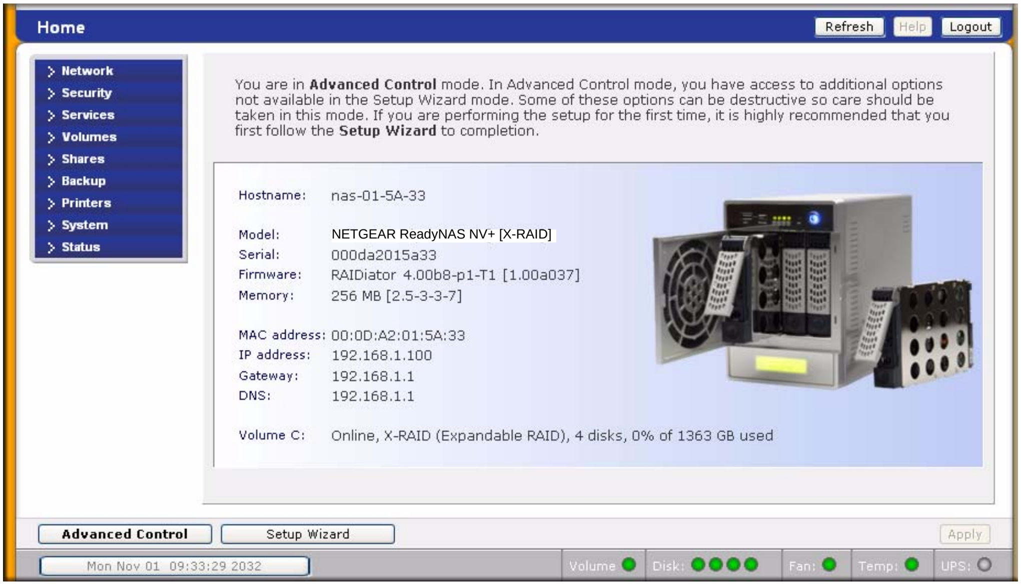
Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Part Number	Version Number	Date	Description
202-10320-01	1.0	Oct. 2007	First publication

Chapter 1
Configuring Your ReadyNAS

The FrontView Advanced Control mode shows all of the settings available in the Setup Wizard plus some more advanced features. The basic network settings and other, optional, more advanced features are included in this chapter.



You are in **Advanced Control** mode. In Advanced Control mode, you have access to additional options not available in the Setup Wizard mode. Some of these options can be destructive so care should be taken in this mode. If you are performing the setup for the first time, it is highly recommended that you first follow the **Setup Wizard** to completion.

Hostname: nas-01-5A-33

Model: NETGEAR ReadyNAS NV+ [X-RAID]
Serial: 000da2015a33
Firmware: RAIDiator 4.00b8-p1-T1 [1.00a037]
Memory: 256 MB [2.5-3-3-7]

MAC address: 00:0D:A2:01:5A:33
IP address: 192.168.1.100
Gateway: 192.168.1.1
DNS: 192.168.1.1

Volume C: Online, X-RAID (Expandable RAID), 4 disks, 0% of 1363 GB used

Figure 1-1

When you first switch to this mode, you see the menus on the left that allow you to quickly jump to the screen you want.

As you click the menu buttons, you notice a similar theme across all screens. At the top right corner is the command bar that typically provides options to return to the Home screen, refresh the browser window, display Help where available, or to log out of this session. For security reasons, **Logout** acts only as a reminder to close the current browser session, which is necessary to securely log out.

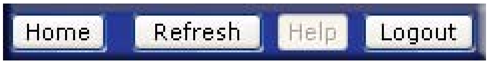


Figure 1-2

Toward the bottom left, there are two buttons that allow you to switch back and forth between the Setup Wizard mode and the Advanced Control mode. At the bottom of the screen is the status bar including the date button on the left which, which clicked, links you to the Clock screen. The status lights to the right give a quick glimpse of the system device status.

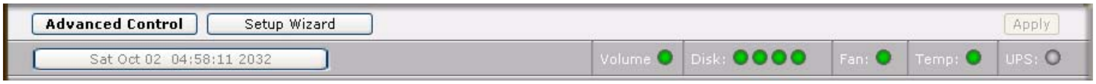


Figure 1-3

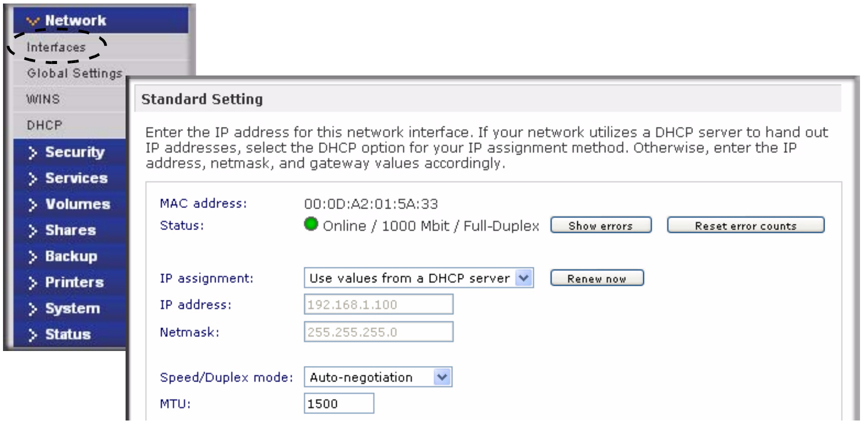
Move the mouse pointer over the status light to display device information, or click a status light to display the status in more detail. Above the Status Lights is the **Apply** button. Use this to save any changes on the current screen.

You can access your Network settings by selecting Network from the main menu. From the Network menu, you can then navigate to your basic network settings screens such as Interfaces, Global Settings, WINS and DHCP.

Specifying Your Ethernet Connection Settings

Select Network > Interfaces, and then select the Ethernet tab to specify network interface-specific settings for Standard Settings, VLAN Settings and Performance Settings.

In the **Standard Setting** section, you can specify the IP address, network mask, speed/duplex mode, and MTU settings. In most networks where a DHCP server is enabled, you can simply specify the **Use values from a DHCP server** option to automatically set the IP address and network mask.



Standard Setting

Enter the IP address for this network interface. If your network utilizes a DHCP server to hand out IP addresses, select the DHCP option for your IP assignment method. Otherwise, enter the IP address, netmask, and gateway values accordingly.

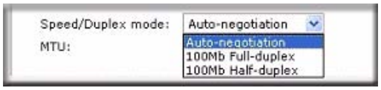
MAC address: 00:0D:A2:01:5A:33
Status: ● Online / 1000 Mbit / Full-Duplex

IP assignment: Use values from a DHCP server
IP address: 192.168.1.100
Netmask: 255.255.255.0

Speed/Duplex mode: Auto-negotiation
MTU: 1500

Figure 1-4

- **IP Assignment.** Select either **Use values from a DHCP server** or **Use values below.**
  - If you elect to assign the IP address using **Use values from a DHCP server**, NETGEAR advises that you set the lease time on the DHCP server/router to a value of at least a day. Otherwise, you might notice that the ReadyNAS IP address changes even when ReadyNAS has been powered down for only a few minutes. Most DHCP servers allow you to assign a static IP address for specified MAC addresses. If you have this option, this would be a good way to ensure your ReadyNAS maintains the same IP address even in DHCP mode.
  - If you assign a static IP address by selecting **Use values below**, be aware that the browser will lose connection to the ReadyNAS device after the IP address has been changed. To reconnect after assigning a static IP address, open RAIDar and click **Rescan** to locate the device, and then reconnect.
- **Speed/Duplex Mode**. If you have a managed switch that works best if the devices are forced to a particular speed or duplex mode, you can select the setting you want. NETGEAR advises that you keep the setting in an Auto-negotiation mode otherwise.

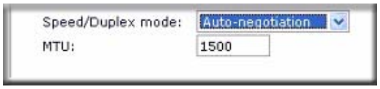


Speed/Duplex mode: Auto-negotiation

MTU:

Figure 1-5

- **MTU**. In some network environments, changing the default MTU value can fix throughput problems. NETGEAR advises that you leave the default setting otherwise.

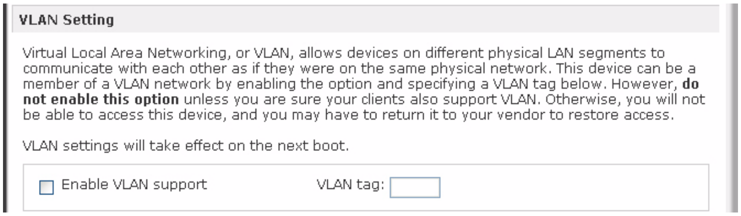


Speed/Duplex mode: Auto-negotiation

MTU: 1500

Figure 1-6

In the VLAN **Settings** (Virtual Local Area Network) area, you can specify whether to allow devices residing on different segments of a LAN to appear in the same segment or, conversely, to allow devices on the same switch to behave as through they belong to a different LAN.



VLAN Setting

Virtual Local Area Networking, or VLAN, allows devices on different physical LAN segments to communicate with each other as if they were on the same physical network. This device can be a member of a VLAN network by enabling the option and specifying a VLAN tag below. However, **do not enable this option** unless you are sure your clients also support VLAN. Otherwise, you will not be able to access this device, and you may have to return it to your vendor to restore access.

VLAN settings will take effect on the next boot.

☐ Enable VLAN support VLAN tag:

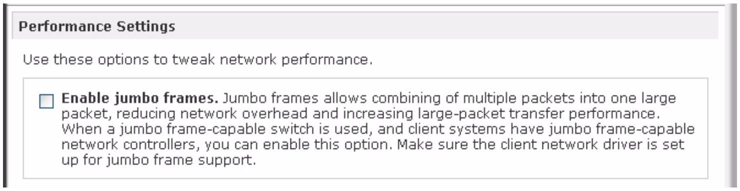
Figure 1-7

If you wish to use the ReadyNAS in a VLAN environment, select the **Enable VLAN support** check box, and enter a numeric VLAN tag. You need to reboot the ReadyNAS for the VLAN function to take effect.

Warning: Do not enable VLAN support unless you are sure that your clients also support VLAN. Otherwise, you can lose network access to the ReadyNAS, and you might need to reinstall the firmware to disable the VLAN setting.

In the **Performance Setting** area, the Enable jumbo frames option allows you to optimize the ReadyNAS for large data transfers such as multiple streams of video playback. Select this option if your NIC and your gigabit switch support jumbo frames.

Note: The ReadyNAS supports a 7936 byte frame size, so for optimal performance, a switch capable of this frame size or larger should also be used.


Performance Settings

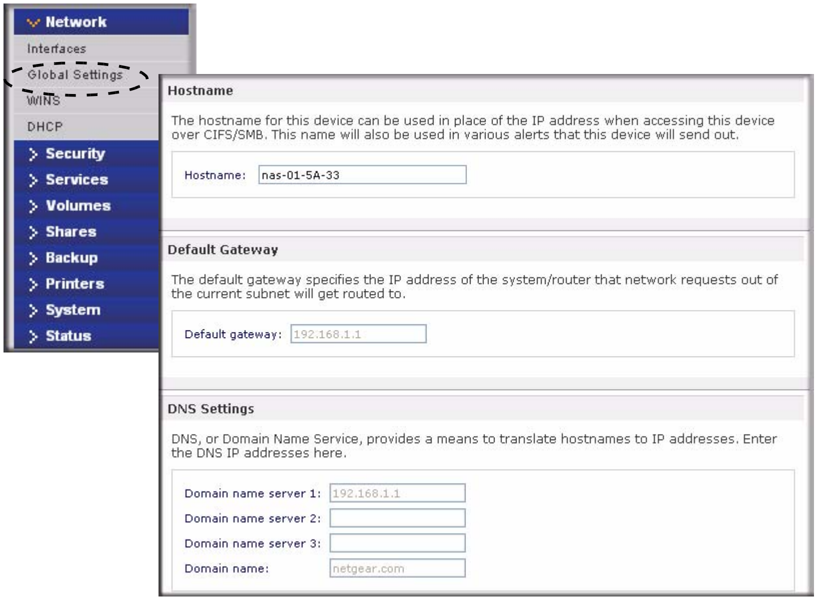
Use these options to tweak network performance.

□ **Enable jumbo frames.** Jumbo frames allows combining of multiple packets into one large packet, reducing network overhead and increasing large-packet transfer performance. When a jumbo frame-capable switch is used, and client systems have jumbo frame-capable network controllers, you can enable this option. Make sure the client network driver is set up for jumbo frame support.

Figure 1-8

If your ReadyNAS device comes with multiple Ethernet interfaces, you will see a separate configuration tab for each interface.

Global Network Settings



Hostname

The hostname for this device can be used in place of the IP address when accessing this device over CIFS/SMB. This name will also be used in various alerts that this device will send out.

Hostname: nas-01-5A-33

Default Gateway

The default gateway specifies the IP address of the system/router that network requests out of the current subnet will get routed to.

Default gateway: 192.168.1.1

DNS Settings

DNS, or Domain Name Service, provides a means to translate hostnames to IP addresses. Enter the DNS IP addresses here.

Domain name server 1: 192.168.1.1
Domain name server 2:
Domain name server 3:
Domain name: netgear.com

Figure 1-9

Hostname

The Hostname you specify is used to advertise the ReadyNAS on your network. You can use the hostname to address the ReadyNAS in place of the IP address when accessing the ReadyNAS from Windows, or over OS X using SMB. This is also the name that appears in the RAIDar scan list.

The default hostname is **nas-** followed by the last three bytes of your primary MAC address.

Default Gateway

The Default Gateway specifies the IP address of the system where your network traffic is routed if the destination is outside your subnet. In most homes and smaller offices, this is the IP address of the router connected to the cable modem or your DSL service.

If you selected the DHCP option in the Ethernet or Wireless tab, the Default Gateway field is automatically populated with the setting from your DHCP server. If you selected the Static option, you can manually specify the IP addresses of the default gateway server here.

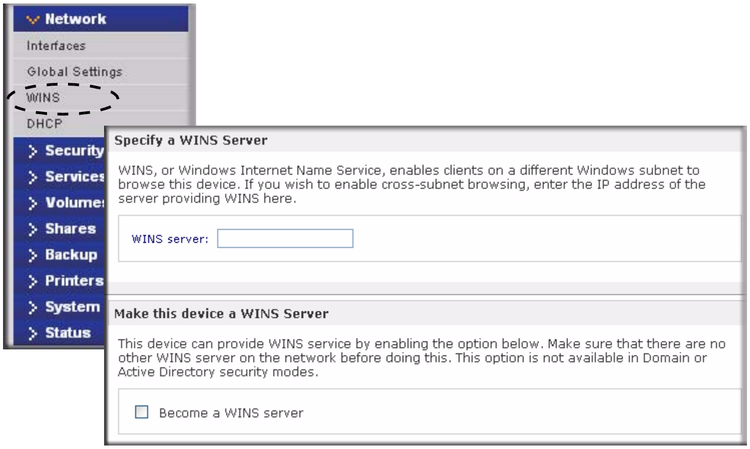
DNS Settings

The DNS area allows you to specify up to three Domain Name Service servers for hostname resolution. The DNS service translates host names into IP addresses.

If you selected the DHCP option in the Ethernet or Wireless tab, the Domain Name Server fields are automatically populated with the DNS settings from your DHCP server. If you selected the Static option, you can manually specify the IP addresses of the DNS servers and the domain name here.

WINS

The WINS option allows you to specify the IP address of the WINS (Windows Internet Naming Service) server. A WINS server is typically a Windows server on the network that allows the ReadyNAS or other devices on the network to be browsed from other subnets.



Specify a WINS Server

WINS, or Windows Internet Name Service, enables clients on a different Windows subnet to browse this device. If you wish to enable cross-subnet browsing, enter the IP address of the server providing WINS here.

WINS server:

Make this device a WINS Server

This device can provide WINS service by enabling the option below. Make sure that there are no other WINS server on the network before doing this. This option is not available in Domain or Active Directory security modes.

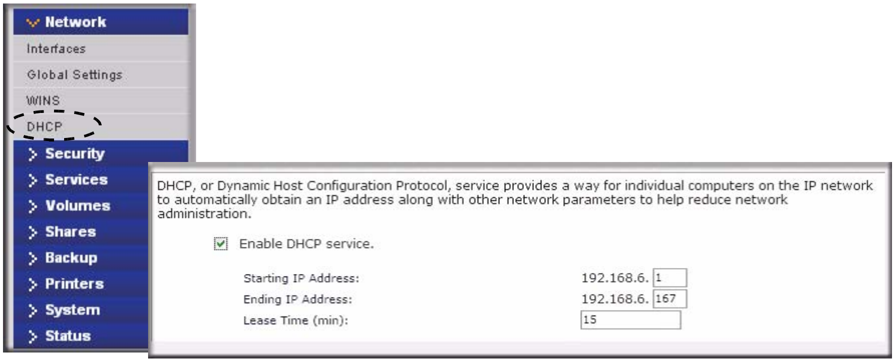
☐ Become a WINS server

Figure 1-10

If you do not have an existing WINS server, you can designate the ReadyNAS to be one. Simply select the **Become a WINS server** check box, and configure your Windows PC to specify the ReadyNAS IP address as the WINS server. This can be useful if you wish to browse by hostname across multiple subnets (for example, over VPN).

DHCP

The DHCP tab allows you to specify this device as a DHCP (Dynamic Host Configuration Protocol) server. DHCP service simplifies management of a network by dynamically assigning IP addresses to new clients on the network.



DHCP, or Dynamic Host Configuration Protocol, service provides a way for individual computers on the IP network to automatically obtain an IP address along with other network parameters to help reduce network administration.

☑ Enable DHCP service.

Starting IP Address: 192.168.6. 1
Ending IP Address: 192.168.6. 167
Lease Time (min): 15

Figure 1-11

Select the **Enable DHCP service** check box if you want the ReadyNAS device to act as a DHCP server. This is convenient in networks where DHCP service is not already available.

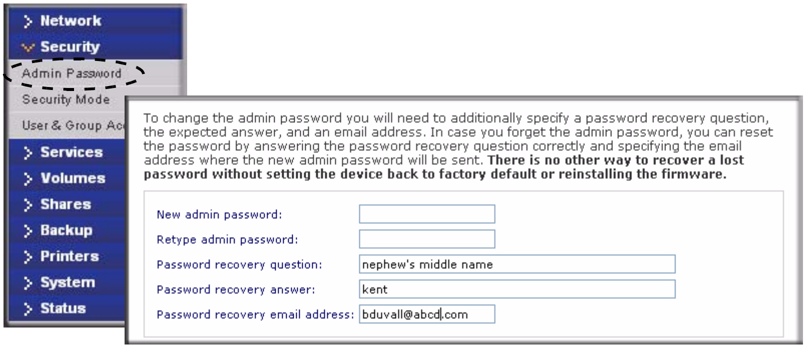
Note: These options are available only if this device is not already using a DHCP address. Enabling DHCP service on a network already utilizing another DHCP server will result in conflicts. If you wish to use this device as a DHCP server, make sure to specify static addresses in the Ethernet and DNS tabs.

Setting Up Security

The Security tab allows you to set the administrator password, administer security, and set up the password recovery feature on the ReadyNAS.

Admin Password

The Admin Password tab allows you to change the administrator user password. The administrator user is the only user that can access FrontView, and this user has administrative privileges when accessing shares. Be sure to set a password different from the default password, and make sure that this password is kept in a safe place. Anyone who obtains this password can effectively change or erase the data on the ReadyNAS.



To change the admin password you will need to additionally specify a password recovery question, the expected answer, and an email address. In case you forget the admin password, you can reset the password by answering the password recovery question correctly and specifying the email address where the new admin password will be sent. **There is no other way to recover a lost password without setting the device back to factory default or reinstalling the firmware.**

New admin password:

Retype admin password:

Password recovery question: nephew's middle name

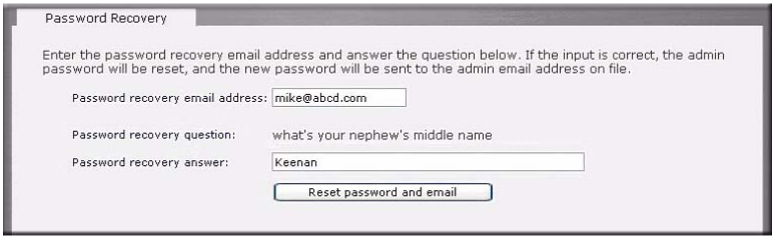
Password recovery answer: kent

Password recovery email address: bduvall@abcd.com

Figure 1-12

Note: In User or Domain security mode, you can use the admin account to log in to a Windows share, and perform maintenance on any file or folder in that share. The admin user also has permission to access all user private home shares to perform backups.

As a safeguard, you are requested to enter a password recovery question, the expected answer, and an e-mail address. If, in the future, you forget the password, you can go to **https://**<*ReadyNAS ip_address*>**/password_recovery**. Successfully answering the questions there resets the Admin Password, and that new password is sent to the e-mail address you enter on this screen.



Enter the password recovery email address and answer the question below. If the input is correct, the admin password will be reset, and the new password will be sent to the admin email address on file.

Password recovery email address: mike@abcd.com

Password recovery question: what's your nephew's middle name

Password recovery answer: Keenan

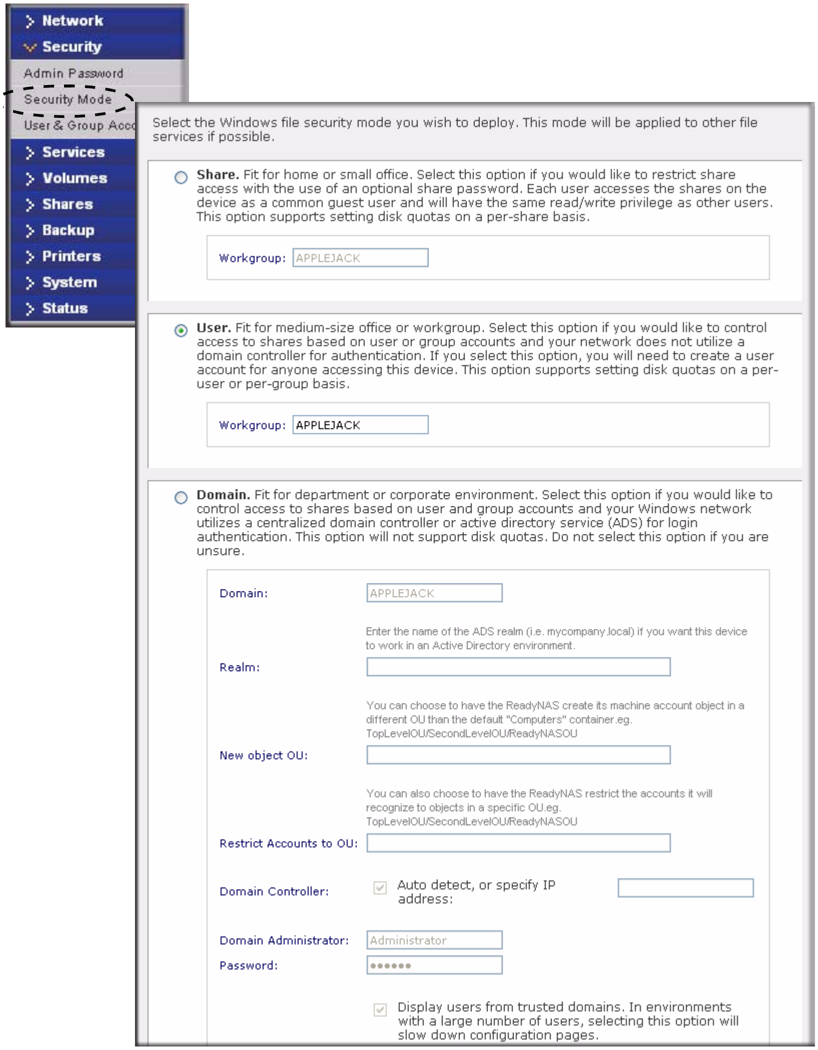
Figure 1-13

Security Mode

The ReadyNAS device offers three security options for your network environment. Select the most appropriate option based on the required level of security and your current network authentication scheme.

- **Share.** The Share security mode is suitable for most home and small office environments, providing a simple way for people in a trusted environment to share files without the necessity of setting up separate user and group accounts. Shares that you create in this environment can be password protected if you want.
- **User.** A more appropriate selection for the medium-size office or workgroup environment is the User security mode. This mode allows you to set up user and group accounts to allow for more specific share access restrictions. Access to shares requires proper login authentication, and you can specify which users and/or groups you wish to offer access. As an example, you might want to restrict company financial data to just users belonging to one particular group. In this security mode, the administrator need to set up and maintain user and group accounts on the ReadyNAS device itself. In addition, each user account is automatically set up with a private home share on the ReadyNAS.
- **Domain.** The Domain security mode is most appropriate for larger department or corporate environments, where a centralized Windows-based domain controller or active directory server is present. The ReadyNAS device integrates in this environment by creating a trusted relationship with the domain/ADS authentication server and allowing all user authentications to occur there, eliminating the need for separate account administration on the device itself. Also, in this security mode, each domain/ADS user is automatically set up with a private home share on the ReadyNAS.

Note: The FrontView management system slows down in proportion to the number of users in the domain. NETGEAR advises that you do not use the ReadyNAS in a domain environment with more than 1000 users.



Select the Windows file security mode you wish to deploy. This mode will be applied to other file services if possible.

○ **Share.** Fit for home or small office. Select this option if you would like to restrict share access with the use of an optional share password. Each user accesses the shares on the device as a common guest user and will have the same read/write privilege as other users. This option supports setting disk quotas on a per-share basis.

Workgroup: APPLEJACK

● **User.** Fit for medium-size office or workgroup. Select this option if you would like to control access to shares based on user or group accounts and your network does not utilize a domain controller for authentication. If you select this option, you will need to create a user account for anyone accessing this device. This option supports setting disk quotas on a per-user or per-group basis.

Workgroup: APPLEJACK

○ **Domain.** Fit for department or corporate environment. Select this option if you would like to control access to shares based on user and group accounts and your Windows network utilizes a centralized domain controller or active directory service (ADS) for login authentication. This option will not support disk quotas. Do not select this option if you are unsure.

Domain: APPLEJACK

Enter the name of the ADS realm (i.e. mycompany.local) if you want this device to work in an Active Directory environment.

Realm:

You can choose to have the ReadyNAS create its machine account object in a different OU than the default "Computers" container.eg. TopLevelOU/SecondLevelOU/ReadyNASOU

New object OU:

You can also choose to have the ReadyNAS restrict the accounts it will recognize to objects in a specific OU.eg. TopLevelOU/SecondLevelOU/ReadyNASOU

Restrict Accounts to OU:

Domain Controller: ☑ Auto detect, or specify IP address:

Domain Administrator: Administrator

Password: ••••••

☑ Display users from trusted domains. In environments with a large number of users, selecting this option will slow down configuration pages.

Figure 1-14

Share Security Mode

The **Share** Security Mode is the easiest security option to set up and is adequate for home or small offices. Select this option if you want to restrict share access with the use of an optional share password. Each user accesses the shares on the device as a common guest user and has the same read/write privilege as other users. This option supports setting disk quotas on a per-share basis.

You need to specify a workgroup only if you wish to change it from the default. A valid workgroup name must conform to the following restrictions:

- The name must consist of characters a–z, A–Z, 0–9, and the symbols _ (underscore), – (dash), and. (period).
- The name must start with a letter.
- The name length mst be 15 characters or less.

User Security Mode

This option is ideal for medium-size offices or workgroups. Select this option if you would like to control access to shares based on user or group accounts and if your network does not utilize a domain controller for authentication. If you select this option, you will need to create a user account for anyone accessing this device. This option supports setting disk quotas on a per-user or per-group basis.

In User security mode, you specify a workgroup name, and create user and group accounts. You have control over how much disk space is allocated for each user or group.

Each user is given a home share on the ReadyNAS device that the user can use to keep private data such as backups of the user's PC. This home share is accessible only by that user and the administrator in order to perform backups of the private shares. The option to automatically generate the private home share is controlled in the Accounts/Preferences tab, and you can disable it if you wish.

Note: Private user shares are accessible only by users using CIFS (Windows) or AppleTalk file protocols.

To set up the ReadyNAS for this security mode, you need the following information:

- Workgroup name
- Group names you wish to create (for example, Marketing, Sales, Engineering)
- User names you wish to create (plus e-mail addresses if you will be setting disk quotas)
- Amount of disk space you want to allocate to users and groups (optional)

To change or set a workgroup name:

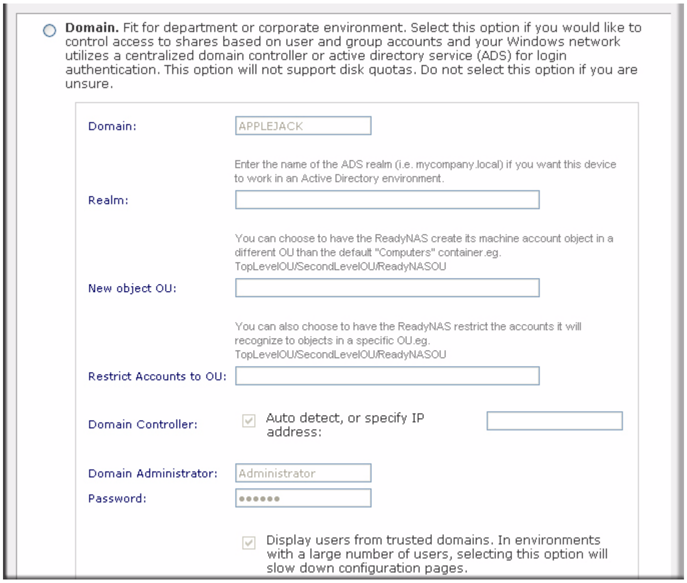
1. Select the **User** radio button.
2. Enter the name you want to use in the **Workgroup** field in the **User** section. The name can be the workgroup name that is already used on your Windows network.

3. Click **Apply** to save your changes.

Domain Security Mode

If you choose the Domain security mode option, you need to create a trusted relationship with the domain controller or the active directory server (ADS) that will act as the authentication server for the ReadyNAS device. You need the following information:

- Domain name
- Domain administrator login
- Domain administrator password
- If using ADS:
  - DNS name of the ADS realm
  - OU (Organization Unit). You can specify nested OUs by separating OU entries with commas. The lowest level OU must be specified first.



○ **Domain.** Fit for department or corporate environment. Select this option if you would like to control access to shares based on user and group accounts and your Windows network utilizes a centralized domain controller or active directory service (ADS) for login authentication. This option will not support disk quotas. Do not select this option if you are unsure.

Domain: APPLEJACK

Enter the name of the ADS realm (i.e. mycompany.local) if you want this device to work in an Active Directory environment.

Realm:

You can choose to have the ReadyNAS create its machine account object in a different OU than the default "Computers" container.eg. TopLevelOU/SecondLevelOU/ReadyNASOU

New object OU:

You can also choose to have the ReadyNAS restrict the accounts it will recognize to objects in a specific OU.eg. TopLevelOU/SecondLevelOU/ReadyNASOU

Restrict Accounts to OU:

Domain Controller: ☑ Auto detect, or specify IP address:

Domain Administrator: Administrator

Password: ●●●●●●

☑ Display users from trusted domains. In environments with a large number of users, selecting this option will slow down configuration pages.

Figure 1-15

You can elect to have the ReadyNAS automatically auto-detect the domain controller, or you can specify the IP address. Sometimes auto-detect fails, and you need to supply the IP address of the domain controller to join the domain.

If you have a large number of users in your domain, you may want to clear the **Display users from trusted domains...** check box. The FrontView management system might slow down to an unusable state.

Note: NETGEAR does not recommend the use of the ReadyNAS in a domain environment with more than 1000 users at this time.

Click **Apply** to join the domain. If Auto-detection is successful, users and groups from the domain now have login access to the shares on this device.

Accounts are managed on the domain controller. The ReadyNAS simply pulls the account information from the controller and displays it in the Accounts tab screen if you have the **Display users from trusted domains**… option enabled. If you wish, you can assign a disk quota to the domain users and groups. If e-mail addresses are specified, users are automatically notified when approaching and reaching their quotas.

Setting Up User and Group Accounts

In the **User & Group Accounts** security mode, the Accounts tab screen allows you to manage user and group accounts on the ReadyNAS.

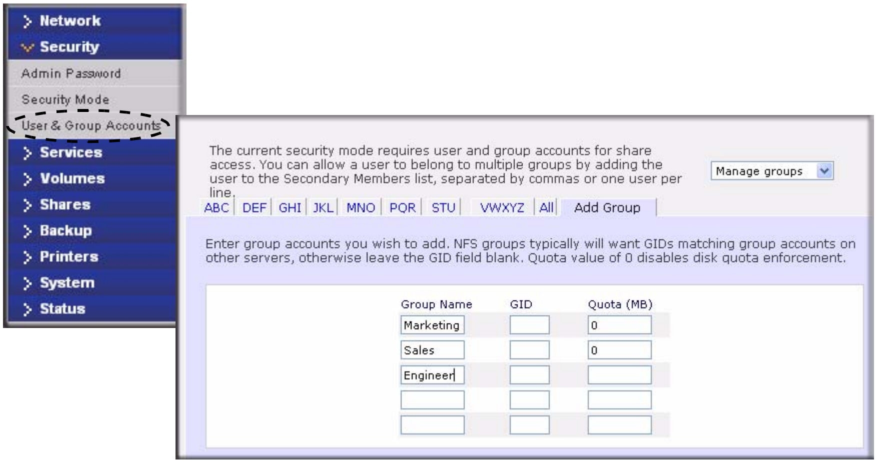
Managing Groups

To add a new group:

1. Select **Manage Groups** from the drop-down menu in the upper right corner.
2. Select the **Add Group** tab if it is not already selected. You can add up to five groups at a time. If you expect to have just one big set of users for one group, you can forego adding a new group and accept the default users group.
3. Click **Apply** to save your settings.

If you want, a user can belong to multiple groups. Once you have created user accounts, you can specify secondary groups that the user can belong to. This allows for finer-grain settings for share access. For instance, you can have user Joe in the Marketing group also belong to the Sales group so Joe can access shares restricted to only the Marketing and Sales groups.

While adding a new group, you can specify the amount of disk space you wish to allocate that group by setting a disk quota. A value of 0 denotes no limit. You can also set the Group ID, or GID, of the group that you are adding. You can leave this field blank and let the system automatically assign this value unless you wish to match your GID to your NFS clients.



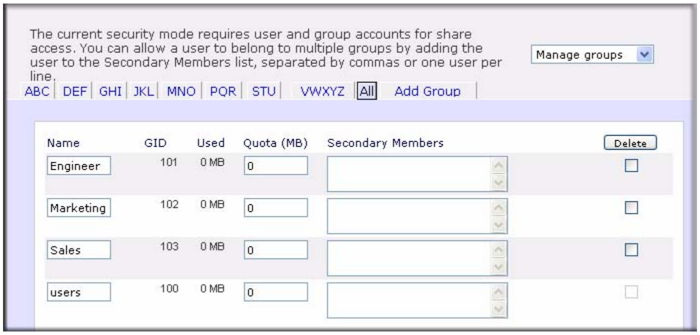
The current security mode requires user and group accounts for share access. You can allow a user to belong to multiple groups by adding the user to the Secondary Members list, separated by commas or one user per line.

Enter group accounts you wish to add. NFS groups typically will want GIDs matching group accounts on other servers, otherwise leave the GID field blank. Quota value of 0 disables disk quota enforcement.

Group Name	GID	Quota (MB)
Marketing		0
Sales		0
Engineer		

Figure 1-16

After adding your groups, you can view or change your groups by clicking the alphabetical index tab, or click **All** to list all groups.

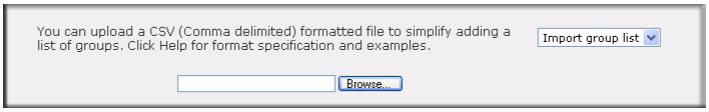

Manage groups
ABC | DEF | GHI | JKL | MNO | PQR | STU | VWXYZ | All | Add Group
Delete

The current security mode requires user and group accounts for share access. You can allow a user to belong to multiple groups by adding the user to the Secondary Members list, separated by commas or one user per line.

Name	GID	Used	Quota (MB)	Secondary Members	Delete
Engineer	101	0 MB	0		□
Marketing	102	0 MB	0		□
Sales	103	0 MB	0		□
users	100	0 MB	0		□

Figure 1-17

If you wish to add a large number of groups, select **Import group list** from the pull-down menu.



You can upload a CSV (Comma delimited) formatted file to simplify adding a list of groups. Click Help for format specification and examples.

Figure 1-18

You can upload a CSV (Comma Separated Value) formatted file containing the group account information. The format of the file is:

```
name1,gid1,quota1,member11:member12:member13
name2,gid2,quota2,member21:member22:member23
```

```
name3,gid3,quota3,member31:member32:member33
                              :
```

Please note the following:

- Spaces around commas are ignored.
- The name field is required.
- Quota is set to default if not specified.
- GID is automatically generated if not specified.
- Empty fields are replaced with account defaults.
- Group members are optional.

Examples of acceptable formats are as follows (note that you can omit follow-on commas and fields if you wish to accept the system defaults for those fields, or you can leave the fields empty):

```
flintstones
```

In this example, the group `flintstones` is created with an automatically assigned GID and default quota.

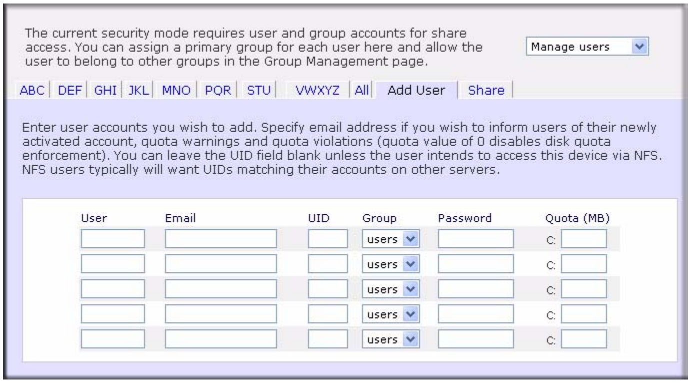
```
rubble,1007,5000,barney:betty
```

In this example, the group `rubble` has a GID of 1007, a quota of 5000 MB, with members `barney` and `betty`.

Managing Users

To manage user accounts:

1. Select **Manage Users** from the drop-down menu.
2. Click the **Add User** tab to add a new user. You can add up to five users at a time. For each user, add the following information:
   - User name,
   - E-mail address
   - User ID
   - Select a group from the **Group** pull-down menu.
   - Password
   - Disk quota.
3. Click **Apply** to save your settings.



The current security mode requires user and group accounts for share access. You can assign a primary group for each user here and allow the user to belong to other groups in the Group Management page.

Manage users

ABC | DEF | GHI | JKL | MNO | PQR | STU | VWXYZ | All | Add User | Share

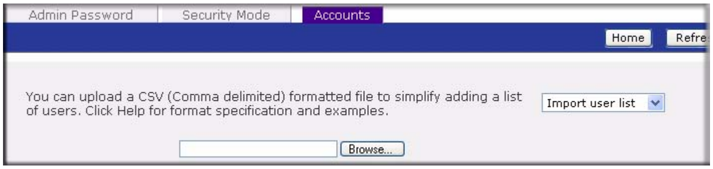
Enter user accounts you wish to add. Specify email address if you wish to inform users of their newly activated account, quota warnings and quota violations (quota value of 0 disables disk quota enforcement). You can leave the UID field blank unless the user intends to access this device via NFS. NFS users typically will want UIDs matching their accounts on other servers.

User	Email	UID	Group	Password	Quota (MB)
			users		C:
			users		C:
			users		C:
			users		C:
			users		C:

Figure 1-19

Only the user name and password fields are required; however, you should specify a user e-mail address if you intend to set up disk quotas. Without an e-mail address, the user will not be warned when disk usage approaches the specified disk quota limit. If you do not wish to assign a disk quota, enter 0.

If you wish to add a large number of users, select **Import user list** from the pull-down menu.



You can upload a CSV (Comma delimited) formatted file to simplify adding a list of users. Click Help for format specification and examples.

Import user list

Figure 1-20

Here, you can upload a CSV (Comma Separated Value) formatted file containing the user account information. The format of the file is:

```
name1,password1,group1,email1,uid1,quota1
name2,password2,group2,email2,uid2,quota2
name3,password3,group3,email3,uid3,quota3
                    :
```

Please note the following:

- Spaces around commas are ignored.
- The name and password fields are required.
- If a listed group account does not exist, it is automatically created.
- Group and quota are set to the defaults if not specified.
- E-mail notification is not sent to the user if the field is omitted or left blank.

- UID is automatically generated if not specified.
- Empty fields are replaced with account defaults.

Examples of acceptable formats are as follows (note that you can omit follow-on commas and fields if you wish to accept the system defaults for those fields, or you can leave the fields empty):

```
fred,hello123
```

In this example, user **fred** has a password set to **hello123**, belongs to the default group, receives no e-mail notification, has a UID assigned automatically, and has a default quota.

```
barney,23stone,,barney@bedrock.com
```

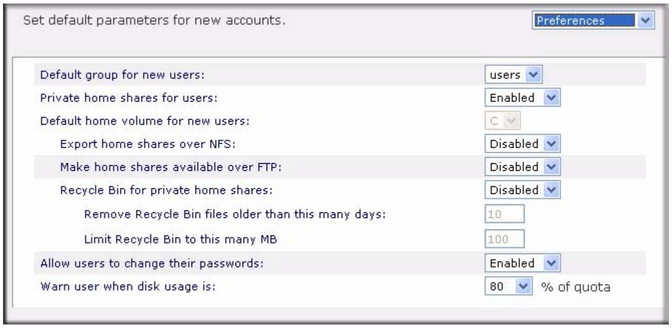
In this example, user **barney** has a password set to **23stone**, belongs to the default group, receives e-mail notification sent to barney@bedrock.com, has a UID assigned automatically, and has a default quota.

```
wilma,imhiswif,ourgroup,wilma@bedrock.com,225,50
```

In this example, user **wilma** has a password **imhiswif**, belongs to the group **ourgroup**, receives e-mail notification sent to wilma@bedrock.com, has a UID set to 225, and a quota set to 50 MB.

Setting Accounts Preferences

You can set various account defaults by selecting **Preferences** option from the pull-down menu.



Set default parameters for new accounts. Preferences

Default group for new users: users
Private home shares for users: Enabled
Default home volume for new users: C
Export home shares over NFS: Disabled
Make home shares available over FTP: Disabled
Recycle Bin for private home shares: Disabled
Remove Recycle Bin files older than this many days: 10
Limit Recycle Bin to this many MB: 100
Allow users to change their passwords: Enabled
Warn user when disk usage is: 80 % of quota

Figure 1-21

Selecting Services for Share Access

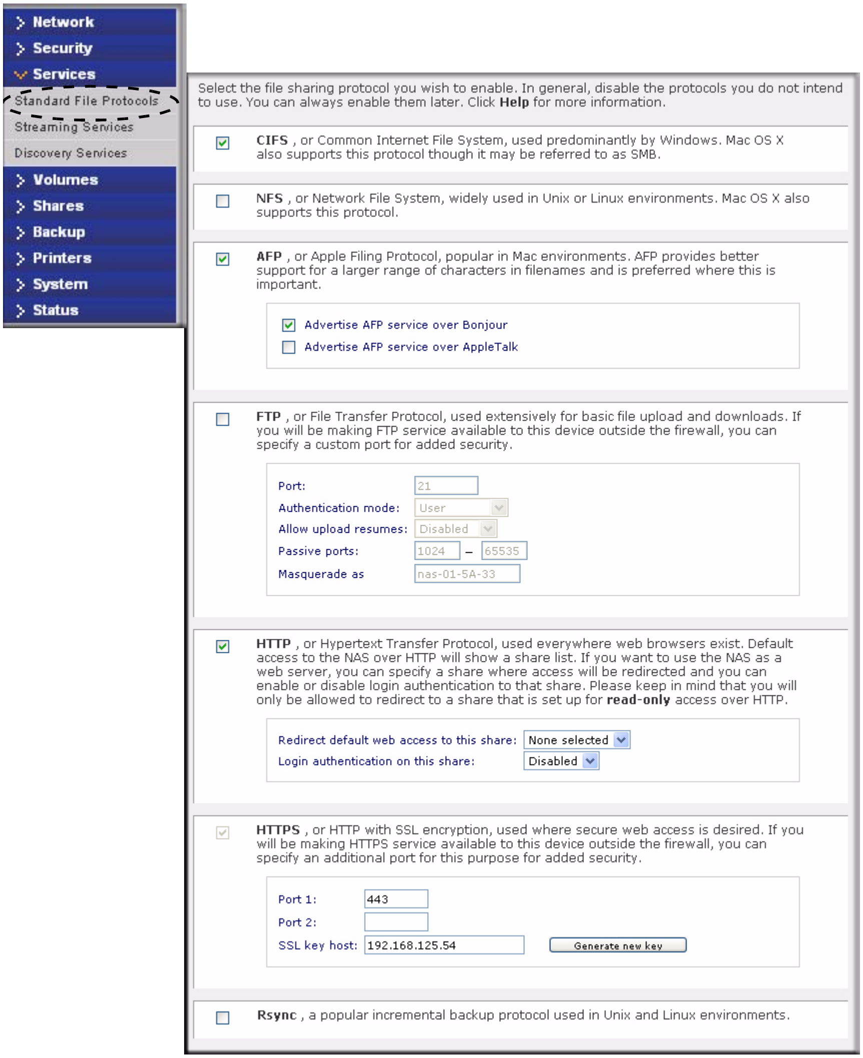
The Services screen allows you to manage various services for share access. This in effect controls the type of clients you wish to allow access to the ReadyNAS. Three types of services are available: Standard File Protocols, Streaming Services, and Discovery Services. These different services are explained in the following sections.

Standard File Protocols

The standard file protocols are common file-sharing services that allow your workstation clients to transfer files to and from the ReadyNAS using built-in file manager-over-network file protocols supported by the client operating system. The available services are:

- **CIFS** (Common Internet File Service). Sometimes referred to as SMB. This protocol is used mainly by Microsoft Windows clients, and sometimes by Mac OS X clients. Under Windows, when you click on My Network Places Network Neighborhood, you are going across CIFS. This service is enabled by default and cannot be disabled.
- **NFS** (Network File Service). NFS is used by Linux and Unix clients. Mac OS 9/X users can access NFS shares as well through console shell access. The ReadyNAS supports NFS v3 over UDP and TCP.
- **AFP** (Apple File Protocol). Mac OS 9 and OS X works best using this protocol as it handles an extensive character set. However, in mixed PC and Mac environments, it is advisable to use CIFS/SMB, unless enhanced character set support is necessary on the Mac.The ReadyNAS supports AFP 3.1.
- **FTP** (File Transfer Protocol). Widely used in public file upload and download sites. ReadyNAS supports anonymous or user access for FTP clients, regardless of the security mode selected. If you wish, you can elect to set up port forwarding to nonstandard ports for better security when accessing files over the Internet.
- **HTTP** (Hypertext Transfer Protocol). Used by Web browsers. ReadyNAS supports HTTP file manager, allowing Web browsers to read and write to shares using the Web browser. This service can be disabled in lieu of HTTPS to allow for a more secure transmission of passwords and data. With the option to redirect default Web access to a specified share, you can transparently force access to **http://readynas_ip** to **http://readynas_ip/share**. This is useful if you do not want to expose your default share listing page to outsiders. All you need in the target share is an index file such as index.htm or index.html. You have the option of enabling or disabling login authentication to this share.
- **HTTPS** (HTTP with SSL encryption). This service is enabled by default and cannot be disabled. Access to FrontView is strictly through HTTPS for this reason. If you want remote Web access to FrontView or your HTTPS shares, you can specify a nonstandard port (default is 443) that you can forward on your router for better security. You can also regenerate the SSL key based on the hostname or IP address that users will use to address the ReadyNAS. This allows you to bypass the default dummy certificate warnings whenever users access the ReadyNAS over HTTPS.
- **Rsync**. An extremely popular and efficient form of incremental backup made popular in the Linux platform but now available for various other Unix systems as well as Windows and

Mac. Enabling rsync service on the ReadyNAS allows clients to use rsync to initiate backups to and from the ReadyNAS.



Select the file sharing protocol you wish to enable. In general, disable the protocols you do not intend to use. You can always enable them later. Click **Help** for more information.

☑ **CIFS** , or Common Internet File System, used predominantly by Windows. Mac OS X also supports this protocol though it may be referred to as SMB.

□ **NFS** , or Network File System, widely used in Unix or Linux environments. Mac OS X also supports this protocol.

☑ **AFP** , or Apple Filing Protocol, popular in Mac environments. AFP provides better support for a larger range of characters in filenames and is preferred where this is important.

☑ Advertise AFP service over Bonjour
□ Advertise AFP service over AppleTalk

□ **FTP** , or File Transfer Protocol, used extensively for basic file upload and downloads. If you will be making FTP service available to this device outside the firewall, you can specify a custom port for added security.

Port: 21
Authentication mode: User
Allow upload resumes: Disabled
Passive ports: 1024 – 65535
Masquerade as nas-01-5A-33

☑ **HTTP** , or Hypertext Transfer Protocol, used everywhere web browsers exist. Default access to the NAS over HTTP will show a share list. If you want to use the NAS as a web server, you can specify a share where access will be redirected and you can enable or disable login authentication to that share. Please keep in mind that you will only be allowed to redirect to a share that is set up for **read-only** access over HTTP.

Redirect default web access to this share: None selected
Login authentication on this share: Disabled

☑ **HTTPS** , or HTTP with SSL encryption, used where secure web access is desired. If you will be making HTTPS service available to this device outside the firewall, you can specify an additional port for this purpose for added security.

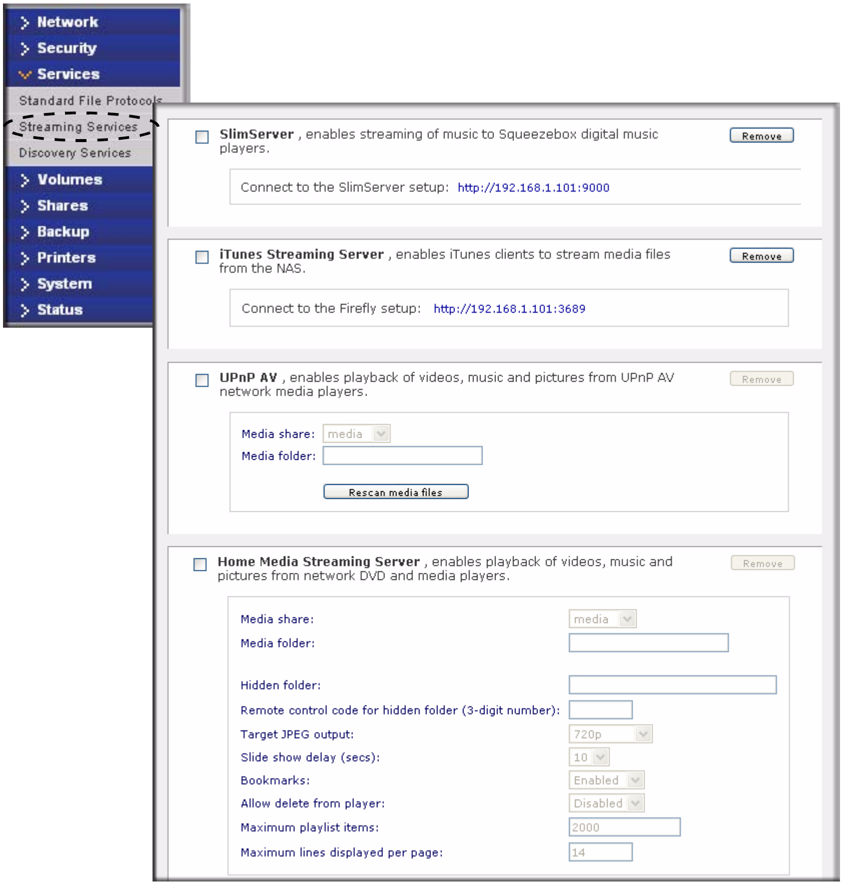
Port 1: 443
Port 2:
SSL key host: 192.168.125.54

□ **Rsync** , a popular incremental backup protocol used in Unix and Linux environments.

Figure 1-22

Streaming Services

The built-in streaming services on the ReadyNAS allow you to stream multi-media content directly from the ReadyNAS, without the need to have your PC or Mac powered on.



□ **SlimServer** , enables streaming of music to Squeezebox digital music players.

Connect to the SlimServer setup: http://192.168.1.101:9000

□ **iTunes Streaming Server** , enables iTunes clients to stream media files from the NAS.

Connect to the Firefly setup: http://192.168.1.101:3689

□ **UPnP AV** , enables playback of videos, music and pictures from UPnP AV network media players.

Media share: media
Media folder:

□ **Home Media Streaming Server** , enables playback of videos, music and pictures from network DVD and media players.

Media share:	media
Media folder:	
Hidden folder:	
Remote control code for hidden folder (3-digit number):	
Target JPEG output:	720p
Slide show delay (secs):	10
Bookmarks:	Enabled
Allow delete from player:	Disabled
Maximum playlist items:	2000
Maximum lines displayed per page:	14

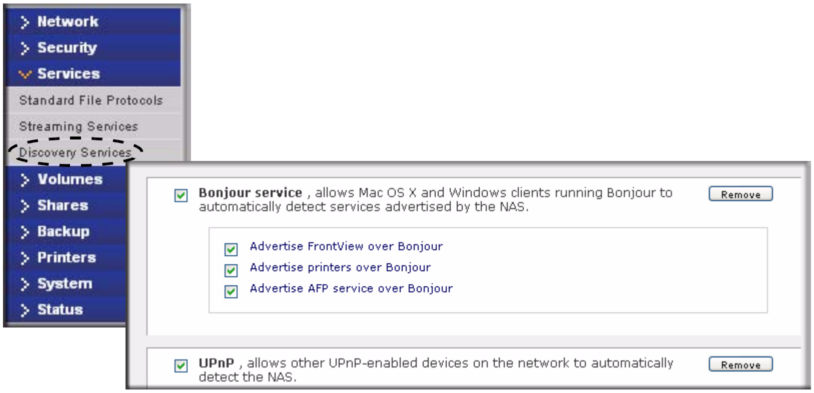
Figure 1-23

- **SlimServer** provides music streaming to the popular Squeezebox music players from Slim Devices. You can click the http setup link for more detailed configuration options.
- **iTunes Streaming Server** enables iTunes clients to stream media files straight from the ReadyNAS. You can click the http setup link for more detailed configuration options.
- **UPnP AV** provides media streaming service to stand-alone networked home media adapters and networked DVD players that support the UPnP AV protocol or are Digital Living Network Alliance (DLNA) standard compliant. The ReadyNAS comes with a reserved media share that is advertised and recognized by the players. Simply copy your media files to the Videos, Music, and Pictures folders in that share to display them on your player. If you wish, you can specify a different media path where your files reside.

- **Home Media Streaming Server** provides streaming of videos, music, and pictures to popular networked DVD players. The streaming players often utilize the streaming client developed by Syabas. Similar to UPnP AV, this service is used to stream videos, music, and pictures from the reserved media share to these adapters. If you wish to change the location where the media files are stored, you can specify a different share and folder path. Note that this path is shared between the UPnP AV and this service.

Discovery Services

- **Bonjour service** provides a simple way of discovering various services on the ReadyNAS. Bonjour currently provides an easy way to connect to FrontView, IPP printing, and AFP services. OS X has built-in Bonjour support, and you can download Bonjour for Windows from Apple's website.
- **UPnP** provides a means for UPnP-enabled clients to discover the ReadyNAS on your LAN.



☑ **Bonjour service** , allows Mac OS X and Windows clients running Bonjour to automatically detect services advertised by the NAS.

☑ Advertise FrontView over Bonjour

☑ Advertise printers over Bonjour

☑ Advertise AFP service over Bonjour

☑ **UPnP** , allows other UPnP-enabled devices on the network to automatically detect the NAS.

Figure 1-24

Understanding Volume Management

The ReadyNAS family consists of two RAID volume technologies: Flex-RAID, utilizing the industry-standard RAID levels 0, 1, and 5; and X-RAID, NETGEAR-patented expandable RAID technology. Your system defaults to one or the other; however, you can switch between the two modes through a factory default reset process described in "Resetting Your System (System Switch)" on page 3-6."

There are advantages to both technologies.

- **Flex-RAID:**
  - The default volume can be deleted and re-created, with or without the snapshot reserved space.
  - Hot spare disk is supported.
  - Full volume management is available—you can create a volume utilizing RAID level 0, 1, or 5, specify the size of the volume, delete a disk from a volume, assign a hot spare, and so on.
  - Multiple volumes are supported, each with a different RAID level, snapshot schedule and disk quota definition.
  - Each disk can be replaced, one by one, then rebuilt; after the last disk is replaced, another data volume utilizing the newly added capacity can be configured.
- **X-RAID:**
  - One-volume technology, but supports volume expansion, either by with the addition of more disks or the replacement of an existing disk with larger capacity disks.
  - You can start out with one disk, and add up to three more disks when you need them or can afford them.
  - Volume management is automatic. Add a second disk, and it becomes a mirror to the first. Add a third disk and your capacity doubles; add a fourth, and your capacity triples—the expansion occurring while redundancy is maintained.
  - In the future, you will be able to replace disks, one at a time, have each one finish rebuilding and, after the last disk is replaced, your volume will automatically expand to utilize the new capacity.

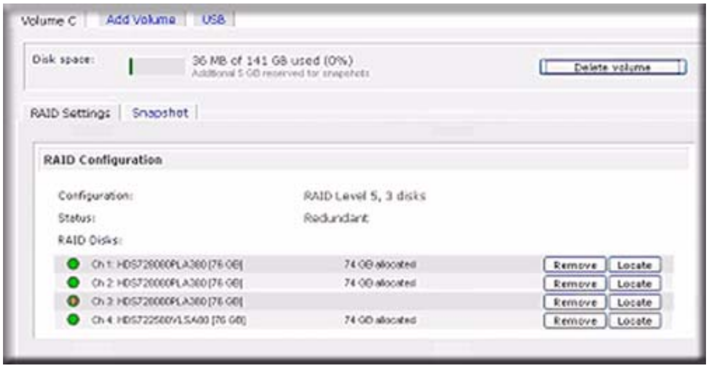
Volume Management for Flex-RAID

If you want to reconfigure the default volume C, split it into multiple volumes, specify a different RAID level, or specify a larger reserved space for snapshots, you need to reconfigure your volume. The first step is to delete the existing volume you want to replace.

Deleting a Volume

To delete a volume, select the **Volume** tab of the volume you wish to delete (if there are multiple volumes) and click **Delete Volume (**in this case only **Volume C** is configured).

Warning: Make sure that you back up the files you wish to keep before deleting a volume. All shares, files, and snapshots residing on that volume *will be deleted are non-recoverable!*



Disk space: 36 MB of 141 GB used (0%)
Additional 5 GB reserved for snapshots

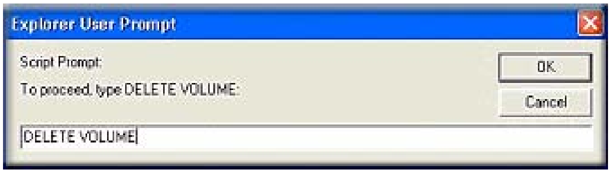
RAID Configuration

Configuration: RAID Level 5, 3 disks
Status: Redundant
RAID Disks:

● Ch 1: HDS728080PLA380 [76 GB] 74 GB allocated
● Ch 2: HDS728080PLA380 [76 GB] 74 GB allocated
● Ch 3: HDS728080PLA380 [76 GB]
● Ch 4: HDS722580VLSA80 [76 GB] 74 GB allocated

Figure 1-25

You are asked to confirm your intention by typing **DELETE VOLUME**.



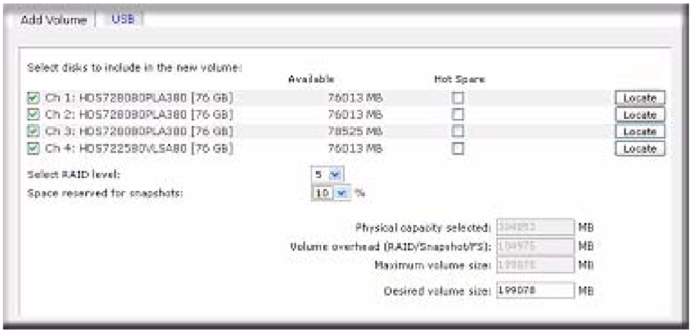
Script Prompt:
To proceed, type DELETE VOLUME:

DELETE VOLUME

Figure 1-26

Adding a Volume

After deleting the volume, Add Volume tab displays listing the available configurable space on the hard disks. All the disks are selected by default. You can elect to specify a hot spare disk if you wish. A hot spare remains in standby mode and automatically regenerates the data from a failed disk from the volume. A hot spare disk is available for RAID level 1 and RAID level 5 only if there are enough disks to fulfill the required minimum plus one.



Select disks to include in the new volume:

	Available	Hot Spare
☑ Ch 1: HDS728080PLA380 [76 GB]	76013 MB	□
☑ Ch 2: HDS728080PLA380 [76 GB]	76013 MB	□
☑ Ch 3: HDS728080PLA380 [76 GB]	78525 MB	□
☑ Ch 4: HDS722580VLSA80 [76 GB]	76013 MB	□

Select RAID level: 5

Space reserved for snapshots: 10 %

Physical capacity selected: 304053 MB

Volume overhead (RAID/Snapshot/FS): 104975 MB

Maximum volume size: 199078 MB

Desired volume size: 199078 MB

Figure 1-27

To add a volume:

1. Select the hard disks. In this example, we select the first three disks and elect not to specify any of them as a hot spare.

2. Select the RAID level. RAID level determines how the redundancy, capacity utilization, and performance are implemented for the volume. See Appendix A, “RAID Levels Simplified,” for more information. Typically in a configuration of three or more disks, RAID level 5 is recommended.

   In our example, we selected RAID level 5 for the three selected disks.

3. Specify the reserve space for a snapshot. Next, select the percentage of the volume you wish to allocate for snapshots. You can specify 0 if you wish to disable snapshot capability, or you can specify a percentage in 5 percent increments from 5 to 50 percent.

   The percentage represents the amount of data you think changes while the snapshot is active. This typically depends on how often you schedule your snapshot to occur (see “Taking and Scheduling Snapshots” on page 1-28), and the maximum amount of data (plus padding) you think changes during that time. Make sure to allocate enough space for a worst case as the snapshot becomes unusable when its reserved space runs out.

   In our example, we selected 10 percent of the volume to be reserved for snapshots.

   Note: If you do not reserve any space for snapshots, the snapshot tab is not displayed in the Volume tab.

4. Specify the desired volume size**.** After you specify the volume parameters, enter the appropriate volume size—if you wish to configure a smaller volume size than the maximum displayed. The resulting volume will be approximately the size that is specified.

In our example, we kept the maximum size that was calculated.

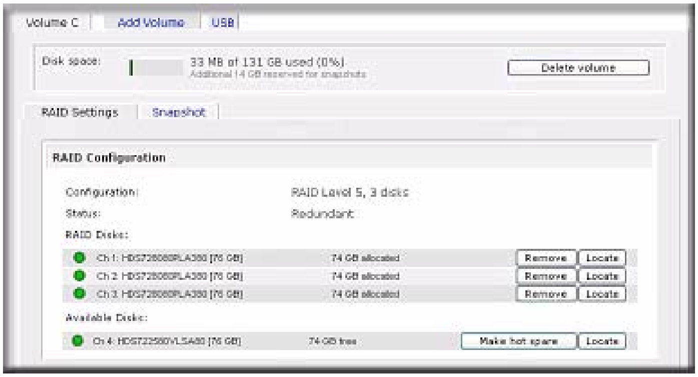
5. Click **Apply,** and wait for the instruction to reboot the system. It typically takes about 1 minute before you are notified to reboot.

   After rebooting, you are notified by e-mail when the volume has been added. Use RAIDar to reconnect to the NAS device.

RAID Settings

After you have added a volume, you can return to the Volume tab and click the RAID Settings tab to display the current RAID information and configuration options for the volume.

Notice that the disk on Channel 4 that we did not configure is listed in the Available Disks section. We can add this disk as a hot spare by clicking **Make hot spare**.



Disk space: 33 MB of 131 GB used (0%)
Additional 14 GB reserved for snapshots

RAID Configuration

Configuration: RAID Level 5, 3 disks

Status: Redundant

RAID Disks:

● Ch 1: HDS728080PLA380 [76 GB] 74 GB allocated

● Ch 2: HDS728080PLA380 [76 GB] 74 GB allocated

● Ch 3: HDS728080PLA380 [76 GB] 74 GB allocated

Available Disks:

● Ch 4: HDS722580VLSA80 [76 GB] 74 GB free

Figure 1-28

We can also remove a disk from the volume by clicking **Remove**. The volume will still be available but in a non-redundant state. An additional disk failure would render this volume unusable.

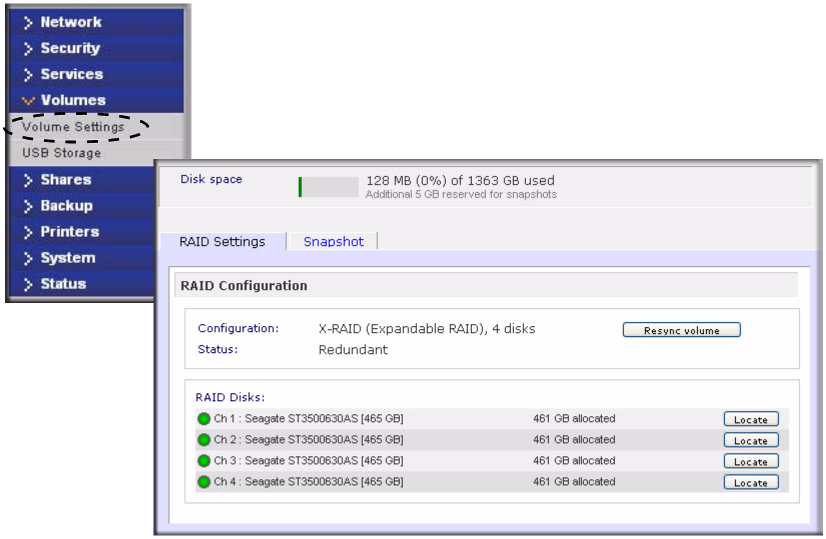
➡	**Note:** The Remove operation is a maintenance feature. NETGEAR recommends that you do not use it in a live environment. Its function is equivalent to hot-removing the disk or simulating a disk failure.

The Locate option is a way to verify that a disk is correctly situated in the expected disk slot. Clicking **Locate** causes disk LED to blink for 15 seconds.

Volume Management for X-RAID

The X-RAID technology offers a simplified approach to volume management. X-RAID works on the premise that what most people want to do with their data volume over time is either adding redundancy or expanding it without the headaches usually associated with doing that. By using simple rules, X-RAID is able to hide all the complexities yet provide volume management features previously available only in enterprise-level storage solutions.

- **X-RAID Redundancy Overhead**. To maintain redundancy from disk failure, X-RAID requires a one-disk overhead. In a two-disk X-RAID volume, the usable capacity is one disk. In a three-disk X-RAID volume, the usable capacity is two disks. In a four-disk X-RAID volume, the usable capacity is three disks.
- **X-RAID has One Data Volume**. X-RAID devices have only one data volume. This volume encompasses one to four disks, utilizing the capacity of the smallest disk from each disk. For instance, if you had one 80 GB disk and two 250 GB disks, only 80 GB from each disk is used in the volume. (The leftover space on the 250 GB disks is reclaimed only when the 80 GB disk is replaced with a 250 GB or greater capacity disk. See "Replacing All Your Disks for More Capacity" on page 1-27.")



Disk space 128 MB (0%) of 1363 GB used
Additional 5 GB reserved for snapshots

RAID Configuration

Configuration: X-RAID (Expandable RAID), 4 disks
Status: Redundant

RAID Disks:

● Ch 1 : Seagate ST3500630AS [465 GB]	461 GB allocated
● Ch 2 : Seagate ST3500630AS [465 GB]	461 GB allocated
● Ch 3 : Seagate ST3500630AS [465 GB]	461 GB allocated
● Ch 4 : Seagate ST3500630AS [465 GB]	461 GB allocated

Figure 1-29

Adding a Second Disk for Redundancy

A one-disk X-RAID device has no redundancy and provides no protection from a disk failure. However, if and when you feel the need for redundancy, simply power down the device, add a new disk with at least the capacity of the first disk, and power on. Depending on the size of the disk, within a few hours, your data volume will be fully redundant. The process occurs in the background, so access to the ReadyNAS is not interrupted.

Adding a Third and Fourth Disk for More Capacity

At a certain point, you will want more capacity. With typical RAID volumes, you have to back up your data to another system (with enough space), add a new disk, reformat your RAID volume, and restore your data back to the new RAID volume.

Not so with X-RAID. Simply add the third disk using the ReadyNAS hot-swap trays. If you are adding multiple disks at the same time, or if your ReadyNAS is not hot-swap capable, power down the ReadyNAS, add the disk(s), and power back on. The X-RAID device initializes and scans the newly added disk(s) for bad sectors in the background. You can continue working normally without any lag in performance. When the process finishes, you will be alerted by e-mail to reboot the device.

During the boot process, your data volume will be expanded. This process typically takes about 15 to 30 minutes per disk to several hours or longer, depending on the size of your disks, or the quantity of data on your volume. A 250 GB disk takes approximately 30 minutes. Access to the ReadyNAS is not permitted during this time. You will be notified by e-mail when the process is complete.

After you receive your e-mail, the ReadyNAS will have been expanded with the capacity from your new disk(s).

Replacing All Your Disks for More Capacity

A year or so down the line when you find the need more disk space, and 600 GB disks are available at an attractive price, you can expand your volume capacity by replacing the existing disks. Keep in mind that you must power down several times to replace out your old disks.

First, power down the ReadyNAS, replace the first disk with the large-capacity disk, and then reboot. If your ReadyNAS supports hot-swapping, you can hot-swap the disk without powering down. The ReadyNAS will detect that a new disk was put in place and resynchronizes the disk with data from the removed disk. This process takes several hours, depending on disk capacity. The disk is initialized and scanned for bad sectors first before the rsync process is started. The total time from the start of initialization to the end of resynchronization can be around 5 hours or more, depending on disk capacity. You will be notified by e-mail upon completion.

Upon completion, power down, replace the second disk with another large-capacity disk, and reboot. This process is the same as for the first disk; repeat this process for the third and fourth disks, as well.

When you receive a completion notification for the fourth disk, reboot the ReadyNAS. During reboot, volume capacity is expanded with the additional capacity from each disk. For instance, if you replaced four 250GB disks with four 600GB disks, the capacity of the volume increases by approximately 350GB x 3 (the fourth disk is reserved for parity). The expansion process takes several hours depending on the expanded capacity, and you will be notified by e-mail when the process is complete. There is no access to the ReadyNAS during this time.

Changing between X-RAID and Flex-RAID Modes

You can switch between X-RAID and Flex-X-RAID modes. The process involves setting the ReadyNAS to the factory default and using RAIDar to configure the volume during a 10-minute delay window during boot. See Chapter 3, “Resetting Your System (System Switch) for more information.

Snapshots

The Volume screen allows you to schedule and take snapshots. You can visualize a snapshot as a frozen image of a volume at the time you take the snapshot. Snapshots are typically used for backups, during which time the original volume can continue to operate normally. As primary storage becomes larger, offline backups tend to become increasingly difficult as backup time increases beyond offline hours. Snapshots allow backups to occur without the need to take your systems offline.

Snapshots also can be used as temporary backups. For example, if a file on the NAS device becomes infected with a virus, the uninfected file can be restored from a prior snapshot taken before the attack.

Taking and Scheduling Snapshots

To take or schedule a snapshot:

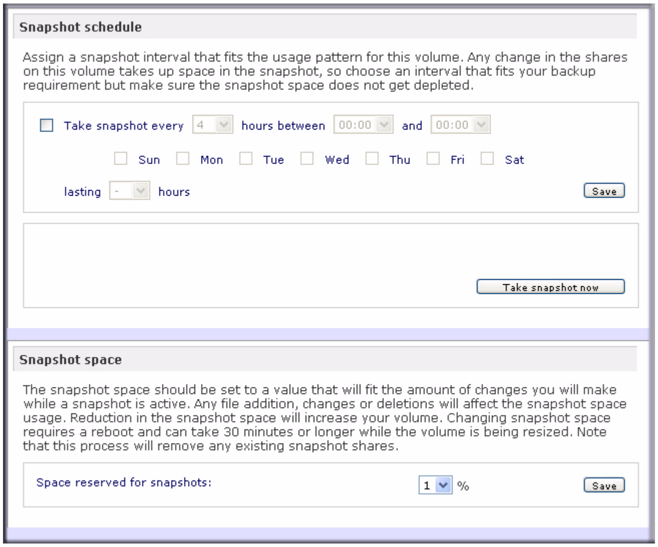
1. Click the Snapshot tab The Snapshot screen will display.

   You can specify how often a snapshot should be taken. Snapshots can be scheduled in intervals from once every 4 hours to once a week.

> ➡ **Note:** If you do not see a Snapshot tab within your volume tab, you did not reserve any space for snapshots when you added the volume. The ReadyNAS ships with a snapshot reserved space of 5 GB.

2. Specify the frequency and the days that you wish to schedule a snapshot:

- If you specify a start and end time of 00:00, ReadyNAS will take one snapshot at midnight. A start time of 00:00 and an end time of 23:00 will set snapshots to be taken between midnight and 11 pm the next day at the interval you specify. Once you save the snapshot schedule, the time of the next snapshot is displayed. When the next snapshot is taken, the previous one is replaced.



Snapshot schedule

Assign a snapshot interval that fits the usage pattern for this volume. Any change in the shares on this volume takes up space in the snapshot, so choose an interval that fits your backup requirement but make sure the snapshot space does not get depleted.

☐ Take snapshot every 4 hours between 00:00 and 00:00

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

lasting - hours

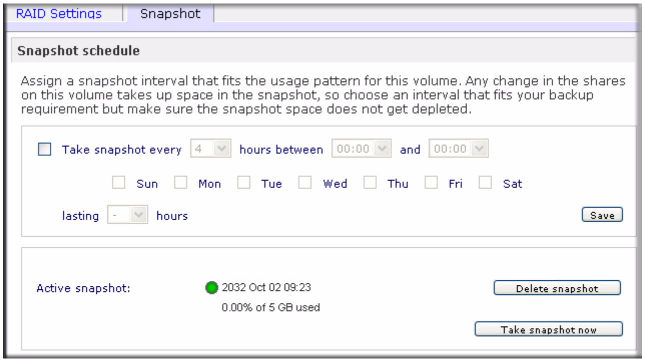
Snapshot space

The snapshot space should be set to a value that will fit the amount of changes you will make while a snapshot is active. Any file addition, changes or deletions will affect the snapshot space usage. Reduction in the snapshot space will increase your volume. Changing snapshot space requires a reboot and can take 30 minutes or longer while the volume is being resized. Note that this process will remove any existing snapshot shares.

Space reserved for snapshots: 1 %

Figure 1-30

- If you prefer, you can manually take a snapshot by clicking **Take Snapshot Now**.



Snapshot schedule

Assign a snapshot interval that fits the usage pattern for this volume. Any change in the shares on this volume takes up space in the snapshot, so choose an interval that fits your backup requirement but make sure the snapshot space does not get depleted.

☐ Take snapshot every 4 hours between 00:00 and 00:00

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

lasting - hours

Active snapshot: ● 2032 Oct 02 09:23
0.00% of 5 GB used

Figure 1-31

You can also specify how long a snapshot should last. If you will be using snapshots for backups, you can schedule the snapshot to last slightly longer than the expected duration of the backup. Having an active snapshot can affect the write performance to the ReadyNAS, so deactivating it when it is not needed might be advantageous in write-intensive environments.

When a snapshot is taken, snapshots of shares appear in your browse list alongside the original shares, except the snapshot share names have **-snap** appended to the original share names. For example, a snapshot taken of a share backup is available as **backup-snap**.

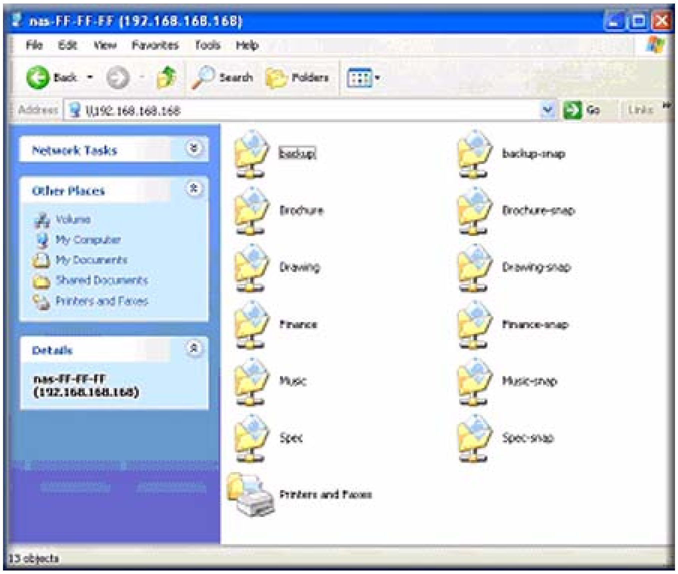
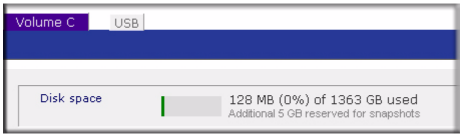


Figure 1-32

You can traverse a snapshot share just as you would a normal share except that the snapshot share is read-only. If you wish, you can select a detailed listing to show the snapshot time in the **Description** field.

Snapshots can expire when the reserved snapshot space is filled. The snapshot mechanism keeps track of data that has been changed from the original volume starting at the point when the snapshot is taken. All these changes are kept in the reserved snapshot space on the volume. The **Disk space** utilization field on the Volume screen shows how much space has been reserved for snapshots.



Disk space 128 MB (0%) of 1363 GB used
Additional 5 GB reserved for snapshots

Figure 1-33

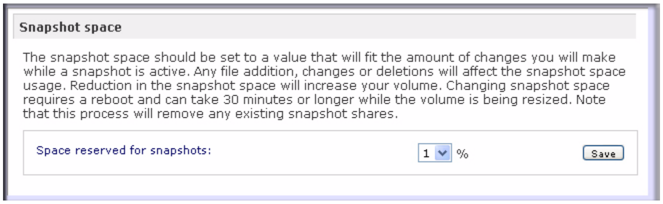
After the snapshot is taken, if changes on the volume exceed this reserved space, the snapshot is invalidated and can no longer be used.

Note: Changes that occupy space in the reserved snapshot space include new file creation, modifications, and deletions; for instance, any time you delete a 1MB file, the change caused by the deletion uses up 1MB of reserved space.

When the snapshot does become invalidated, an e-mail alert is sent and the status reflected on the **Snapshot** screen. The snapshot is no longer usable at this stage.

Resizing Snapshot Space

If you are constantly getting snapshot invalidation alerts, you might want to either increase the frequency of the snapshot or consider increasing the reserved snapshot space. To do this, or to eliminate your existing snapshot space (thus increasing your usable volume space), you can specify the snapshot space you want in the Snapshot Space section. Simply select a value from the pull-down menu and click **Save**. Your snapshot space will be limited to approximately 100GB.



Snapshot space

The snapshot space should be set to a value that will fit the amount of changes you will make while a snapshot is active. Any file addition, changes or deletions will affect the snapshot space usage. Reduction in the snapshot space will increase your volume. Changing snapshot space requires a reboot and can take 30 minutes or longer while the volume is being resized. Note that this process will remove any existing snapshot shares.

Space reserved for snapshots: 1 %

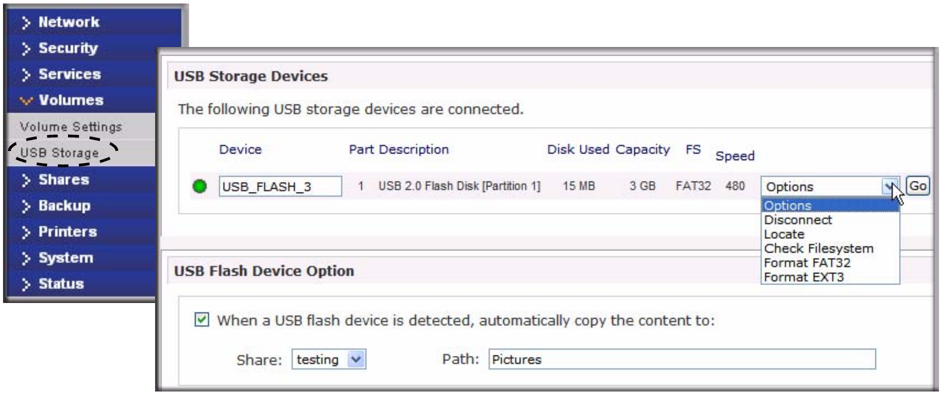
Figure 1-34

Resizing the snapshot space will occur offline and can take a while depending on your data volume size and the number of files in your volume. Expanding the snapshot space reduces your data volume size, and reducing the snapshot space expands it.

Note: Because of the way snapshots work, you will encounter a drop in write performance when a snapshot is active. If your environment requires the highest throughput in performance, the active snapshot should be deleted, or you should set a limit on how long the snapshot should be live.

USB Storage

The USB tab displays the USB disk and flash devices connected to the ReadyNAS, and offers various options for these devices. A flash device appears as **USB_FLASH_1** and a disk device appears as **USB_HDD_1**. If you have multiple devices, they appear appended by an increasing device number; for example, **USB_HDD_2**. If the device contains multiple partitions, the partitions are listed beneath the main device entry.



USB Storage Devices

The following USB storage devices are connected.

Device	Part Description	Disk Used	Capacity	FS	Speed
● USB_FLASH_3	1 USB 2.0 Flash Disk [Partition 1]	15 MB	3 GB	FAT32	480

USB Flash Device Option

☑ When a USB flash device is detected, automatically copy the content to:

Share: testing Path: Pictures

Figure 1-35

Partitions on the storage devices must be one of the following file system formats:

- FAT32
- NTFS
- Ext2
- Ext3

To the right of the access icons are command options for the device. The following commands are available:

Disconnect	This option prepares the USB partition for disconnection by correctly unmounting the file system. In most cases, you can safely disconnect the device without first unmounting; however, the Disconnect command ensures that any data still in the write cache is written out to the disks and that the file system is properly closed. The Disconnect option unmounts all partitions on the device. Once disconnected, physically remove and re-connect to the ReadyNAS to regain access the USB device,.
Locate	In cases where you attach multiple storage devices and wish to determine which device corresponds to the device listing, the Locate command causes the device LED to blink, if present.

Format FAT32	This option formats the device as a FAT32 file system. FAT32 format is easily recognizable by most newer Windows, Linux, and Unix operating systems.
Format EXT3	This option formats the device as an EXT3 file system. Select this option if you will be accessing the USB device mainly from Linux systems or ReadyNAS devices. The advantage of EXT3 over FAT32 is that file ownership and mode information can be retained using this format, whereas this capability is not there with FAT32. Although not natively present in the base operating system, Ext3 support for Windows and OS X can be added. The installation images can be downloaded from the Web.

When the USB device is unmounted, you have the option of renaming it. The next time the same device is connected, it will use the new name rather than the default **USB_FLASH_n** or **USB_HDD_n** naming scheme.

The USB storage shares are listed in the Share screen, and access restrictions can be specified there. The share names reflect the USB device names.

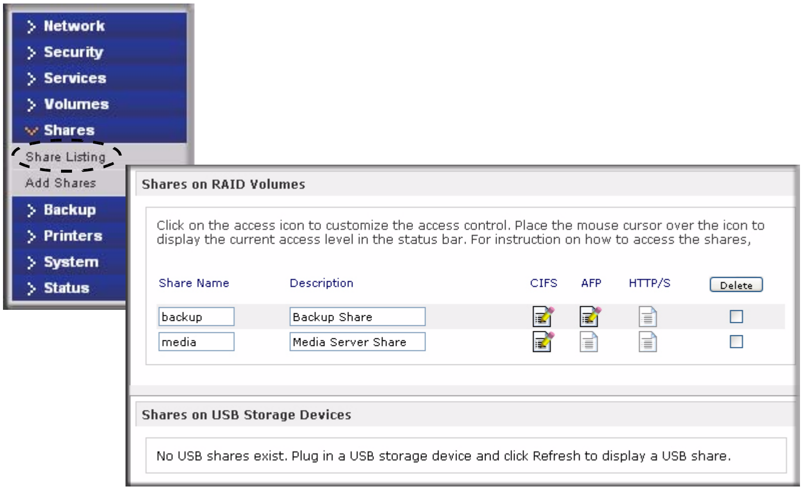
USB Flash Device Option

Toward the lower portion of the USB Storage screen is the USB Flash Device Option section (see Figure 1-35 on page 1-32). There, you can elect to copy the content of a USB flash device automatically on connection to a specified share. Files are copied into a unique timestamp folder to prevent overwriting previous contents. This is useful for uploading pictures from digital cameras and music from MP3 players without needing to power on a PC.

In User security mode, an additional option to set the ownership of the copied files is available.

Managing Your Shares

The Shares menu provides all the options pertaining to share services for the ReadyNAS device. This entails share management (including data and print shares), volume management, and share service management.



Shares on RAID Volumes

Click on the access icon to customize the access control. Place the mouse cursor over the icon to display the current access level in the status bar. For instruction on how to access the shares,

Share Name	Description	CIFS	AFP	HTTP/S	Delete
backup	Backup Share				☐
media	Media Server Share				☐

Shares on USB Storage Devices

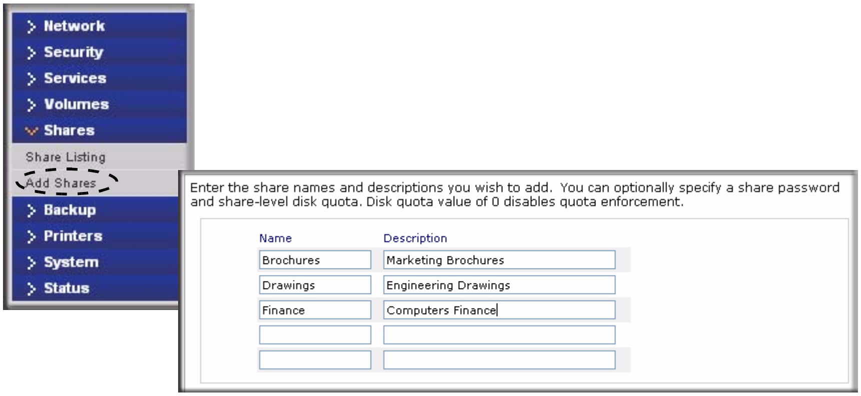
No USB shares exist. Plug in a USB storage device and click Refresh to display a USB share.

Figure 1-36

Adding Shares

To add a share:

1. From the main menu, select Volumes > Volume Settings. If more than one volume is configured, click on the volume you wish to add the share.
2. Select Add Shares. Add Shares has two views, depending on the security mode. In the Add Shares screen, enter the share name, description and, optionally, the password and disk quota. (The share password and share disk quota are available only in the security mode).



Enter the share names and descriptions you wish to add. You can optionally specify a share password and share-level disk quota. Disk quota value of 0 disables quota enforcement.

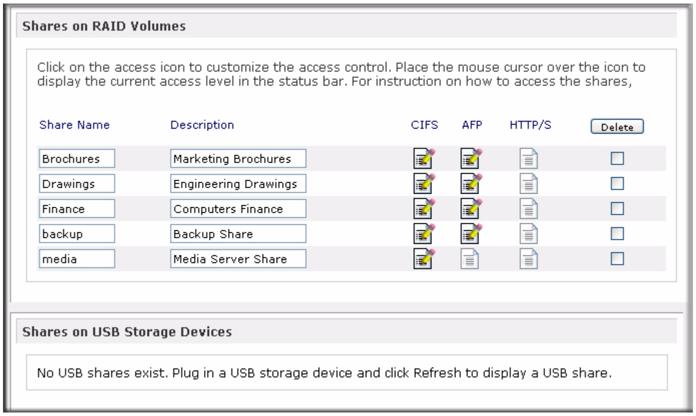
Name	Description
Brochures	Marketing Brochures
Drawings	Engineering Drawings
Finance	Computers Finance

Figure 1-37

In the User or Domain security modes, the Add Share tab consists only of fields for the share name and description. Password and disk quotas are account-specific. In either case, you can add up to five shares at a time. Once you finish adding the shares, refer to Chapter 2, "Accessing Shares from Your Operating System for instructions on how to access them from different client interfaces.

Managing Shares

Once you have added shares, you can manually fine-tune share access by selecting Share List. This screen has two views, one for Share Security mode and one for User and Domain mode. They are similar except for the password and disk quota prompts which appear only in Share mode.



Shares on RAID Volumes

Click on the access icon to customize the access control. Place the mouse cursor over the icon to display the current access level in the status bar. For instruction on how to access the shares,

Share Name	Description	CIFS	AFP	HTTP/S	Delete
Brochures	Marketing Brochures	✎	✎	🗋	□
Drawings	Engineering Drawings	✎	✎	🗋	□
Finance	Computers Finance	✎	✎	🗋	□
backup	Backup Share	✎	✎	🗋	□
media	Media Server Share	✎	🗋	🗋	□

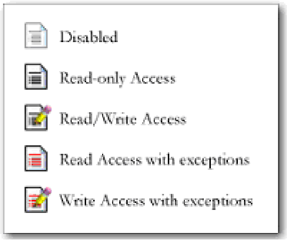
Shares on USB Storage Devices

No USB shares exist. Plug in a USB storage device and click Refresh to display a USB share.

Figure 1-38

If you want to delete a share, select the check box on the far right of the share listing and click **Delete**.

The columns to the left of the Delete check box represent the services that are currently available. The access icons in those columns summarize the status of the service and the access rights to the share for each of the services. Move the mouse pointer over the access icons to view the access settings.



- 🗋 Disabled
- 🗎 Read-only Access
- ✎ Read/Write Access
- 🗎 Read Access with exceptions
- ✎ Write Access with exceptions

Figure 1-39

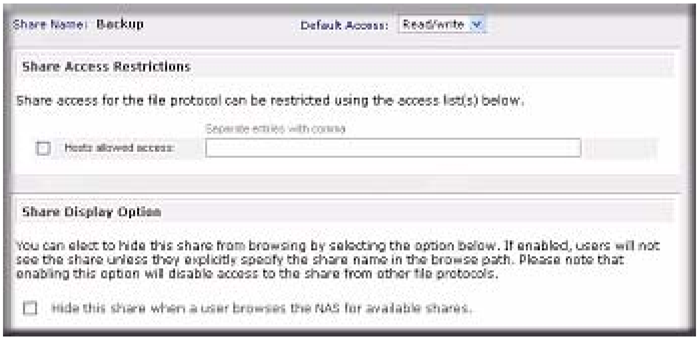
The settings are as follows:

- **Disabled.** Access to this share is disabled.
- **Read-only Access.** Access to this share is read-only.
- **Read/Write Access**. Access to this share is read/write.
- **Read Access with exceptions**. Either (1) access to this share is read-only and allowed only for specified hosts, (2) access is read-only except for one or more users or groups that are granted read/write permission, or (3) access is disabled except for one or more users or groups that are granted read-only privilege.
- **Write Access with exceptions** – Either (1) access to this share is read/write and allowed only for specified hosts, (2) access is read/write except for one or more users or groups that are restricted to read-only access, or (3) access is disabled except for one or more users or groups that are granted read/write privilege.

You can click on the access icons to display the Share Options screen, where you can set the access rules for each file protocol. Keep in mind that access options differ between protocols.

Setting Share Access in Share Mode

In Share mode, the CIFS (Windows) share options screen looks like the following:



Share Name: Backup

Default Access: Read/write

Share Access Restrictions

Share access for the file protocol can be restricted using the access list(s) below.

Separate entries with comma

□ Hosts allowed access:

Share Display Option

You can elect to hide this share from browsing by selecting the option below. If enabled, users will not see the share unless they explicitly specify the share name in the browse path. Please note that enabling this option will disable access to the share from other file protocols.

□ Hide this share when a user browses the NAS for available shares.

Figure 1-40

To set share access:

1. Select the Default Access from the pull-down menu at the top.
2. Select the **Hosts allowed access** check box and specify one or more hosts that you wish to restrict access to in the adjacent field.

For example, select **read-only** for Default Access and list the hosts you wish to allow access to. Access from all other hosts will be denied. To allow only host 192.168.2.101 read-only access to the share, specify the following:

- Default: **Read-only**
- Hosts allowed access: **192.168.2.101**

Multiple hosts can be separated with commas (see Appendix B, “Input Field Format” for information about valid host formats.) For example, if you wish to limit share access to particular hosts, you can enter host IP addresses or valid DNS hostnames in the **Host allowed access** field. In addition, you can enter a range of hosts using common IP range expressions such as:

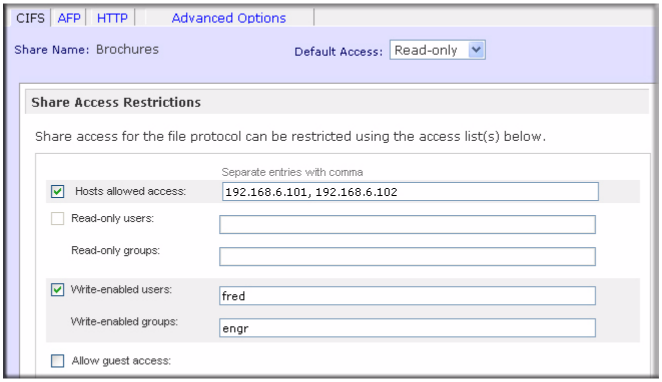
192.168.2., 192.168.2.0/255.255.255.0, 192.168.2.0/24

These designations all allow hosts with IP addresses 192.168.2.1 through 192.168.2.254.

Toward the bottom of the CIFS screen are the Share Display Option, Recycle Bin, and Advanced CIFS Permissions. Refer to the descriptions for these options in the sections that follow.

Setting Share Access in User and Domain Modes

In User or Domain modes, the CIFS screen looks like the following (note the addition of Read-only and Write-enabled user and group fields)



Share Name: Brochures

Default Access: Read-only

Share Access Restrictions

Share access for the file protocol can be restricted using the access list(s) below.

Separate entries with comma

☑ Hosts allowed access: 192.168.6.101, 192.168.6.102

□ Read-only users:

Read-only groups:

☑ Write-enabled users: fred

Write-enabled groups: engr

□ Allow guest access:

Figure 1-41

Share Access Restriction. If you wish to limit share access to particular users and/or groups, you can enter their names in the **Read-only users, Read-only groups, Write-enabled users,** and **Write-enabled group** fields. The names must be valid accounts, either on the ReadyNAS or on the domain controller.

For instance, if you wish to allow read-only access to all and read/write access only user **fred** and group **engr**, you would set the following:

- Default: **Read-only**
- Write-enabled users: **fred**
- Write-enabled groups: **engr**

If you wish to limit this access only to hosts 192.168.2.101 and 192.168.2.102, set the following:

- Default: **Read-only**
- Hosts allowed access: **192.168.2.101, 192.168.2.102**
- Write-enabled users: **fred**
- Write-enabled groups: **engr**

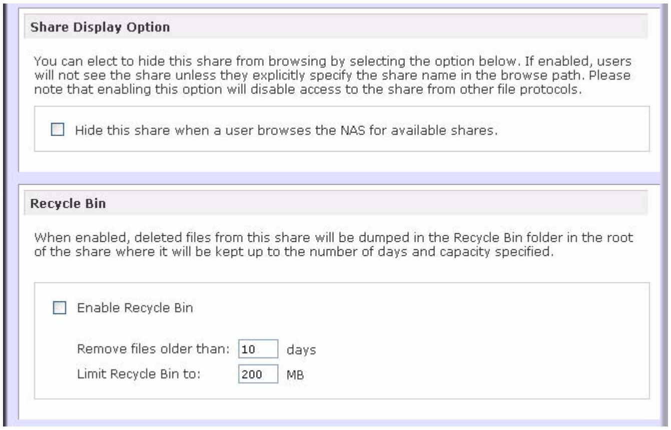
If you wish to specify some users and groups for read-only access and some for read/write access, and disallow all other users and groups, enter the following:

- Default: **Disabled**
- Hosts allowed access: **192.168.2.101, 192.168.2.102**
- Read-only users: **mary, joe**
- Read-only groups: **marketing, finance**
- Write-enabled users: **fred**
- Write-enabled groups: **engr**

Note that access control differs slightly from service to service.

Share Display Option. Restricting access to a share does not prevent users from seeing the share in the browse list. In certain instances, you might not want this, such as for backup shares that you might want to prevent users from seeing.

To hide a share, select the **Hide this share…** check box. Users who have access to this share must specify the path explicitly. For example, to access a hidden share, enter **\\host\share** in the Windows Explorer address bar.



Share Display Option

You can elect to hide this share from browsing by selecting the option below. If enabled, users will not see the share unless they explicitly specify the share name in the browse path. Please note that enabling this option will disable access to the share from other file protocols.

☐ Hide this share when a user browses the NAS for available shares.

Recycle Bin

When enabled, deleted files from this share will be dumped in the Recycle Bin folder in the root of the share where it will be kept up to the number of days and capacity specified.

☐ Enable Recycle Bin

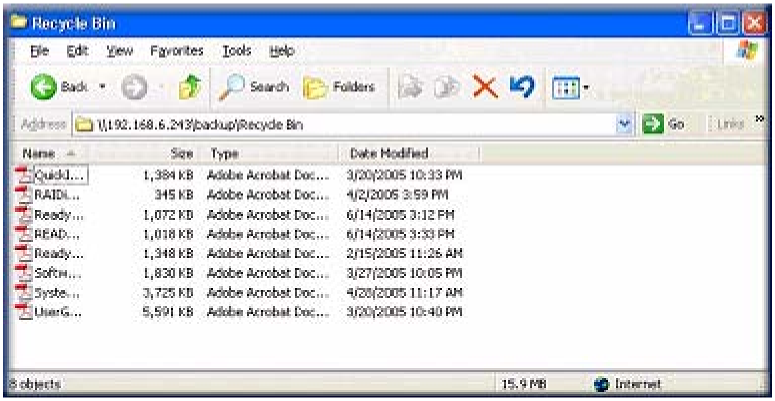
Remove files older than: 10 days

Limit Recycle Bin to: 200 MB

Figure 1-42

Recycle Bin. The ReadyNAS can have a Recycle Bin for each share for Windows users. The **Enable Recycle Bin** option is shown at the bottom of the CIFS screen.

When this check box is selected, whenever you delete a file, the file gets inserted into the Recycle Bin folder in the share rather than being permanently deleted. This allows for a grace period during which users can restore deleted files.



Address: \\192.168.6.243\backup\Recycle Bin

Name	Size	Type	Date Modified
QuickI...	1,384 KB	Adobe Acrobat Doc...	3/20/2005 10:33 PM
RAIDi...	345 KB	Adobe Acrobat Doc...	4/2/2005 3:59 PM
Ready...	1,072 KB	Adobe Acrobat Doc...	6/14/2005 3:12 PM
READ...	1,018 KB	Adobe Acrobat Doc...	6/14/2005 3:33 PM
Ready...	1,348 KB	Adobe Acrobat Doc...	2/15/2005 11:26 AM
Softw...	1,830 KB	Adobe Acrobat Doc...	3/27/2005 10:05 PM
Syste...	3,725 KB	Adobe Acrobat Doc...	4/28/2005 11:17 AM
UserG...	5,591 KB	Adobe Acrobat Doc...	3/20/2005 10:40 PM

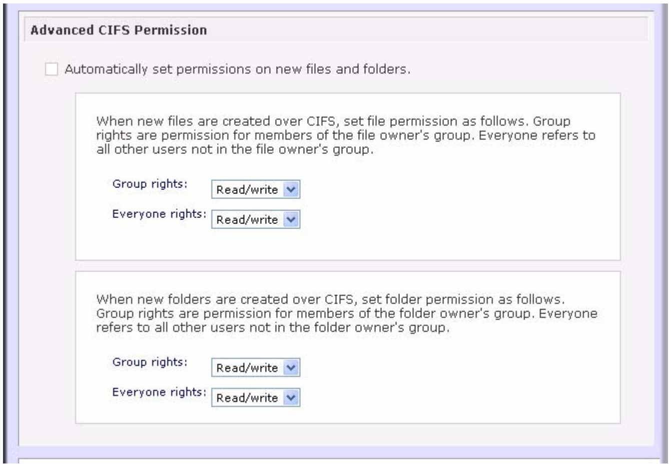
8 objects 15.9 MB Internet

Figure 1-43

You can specify how long to keep the files in the Recycle Bin and how large the Recycle Bin can get before files get permanently erased.

Advanced CIFS Permission. The Advanced CIFS Permission section offers options for setting the default permission of new files and folders created through CIFS. The default permission of newly created files is read/write for the owner and owner’s group and read-only for others (that is, everyone). Permission for newly created folders is read/write for everyone. If the default does not satisfy your security requirement, you can change it here.

Opportunistic locking (often referred to as oplocks) enhances CIFS performance by allowing files residing on the NAS to be cached locally on the Windows client, thus eliminating network latency when the files are constantly accessed.



Advanced CIFS Permission

□ Automatically set permissions on new files and folders.

When new files are created over CIFS, set file permission as follows. Group rights are permission for members of the file owner's group. Everyone refers to all other users not in the file owner's group.

Group rights: Read/write

Everyone rights: Read/write

When new folders are created over CIFS, set folder permission as follows. Group rights are permission for members of the folder owner's group. Everyone refers to all other users not in the folder owner's group.

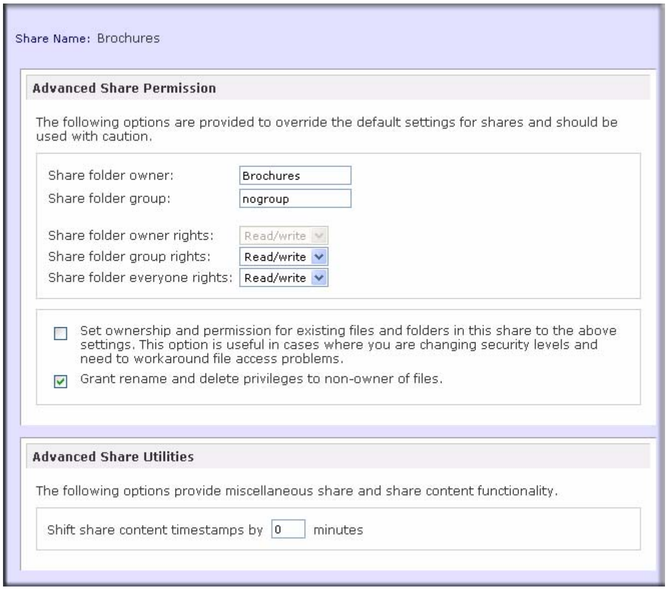
Group rights: Read/write

Everyone rights: Read/write

Figure 1-44

Advanced Options

The Advanced Options tab offers advanced low-level file manipulation options that can affect remote file access through all file protocol interfaces. Care should be taken before you use these options as anything that changes ownership and permissions might not be easily reversible.



Share Name: Brochures

Advanced Share Permission

The following options are provided to override the default settings for shares and should be used with caution.

Share folder owner: Brochures
Share folder group: nogroup

Share folder owner rights: Read/write
Share folder group rights: Read/write
Share folder everyone rights: Read/write

☐ Set ownership and permission for existing files and folders in this share to the above settings. This option is useful in cases where you are changing security levels and need to workaround file access problems.

☑ Grant rename and delete privileges to non-owner of files.

Advanced Share Utilities

The following options provide miscellaneous share and share content functionality.

Shift share content timestamps by 0 minutes

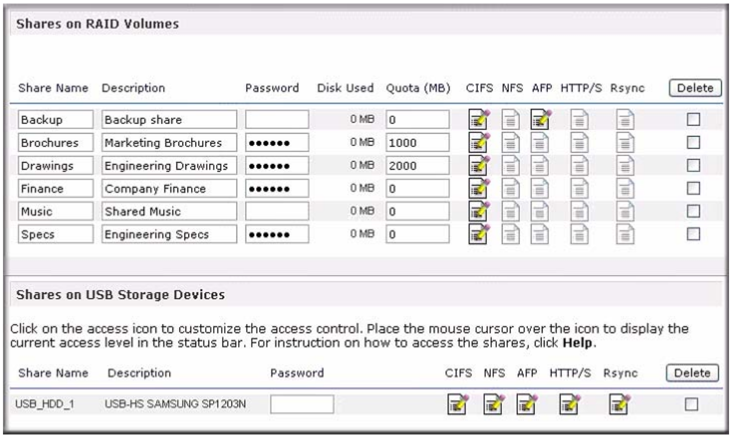
Figure 1-45

Advanced Share Permission. The Advanced Share Permission section offers the options to override the default ownership and permission of the share folder on the embedded file system and to permeate these settings to all files and folders residing on the selected share. The **Set ownership and permission for existing files and folders** option performs a one-time change. Depending on the size of the share, this can take a while to finish.

You can also grant rename and delete privilege to non-owners of the files option. In a collaborative environment, you might want to enable this option. In a more security-conscious environment, you might want to disable this option.

USB Shares

USB storage devices are shared using the name of the device appended with the partition number. You can change the base device name in Volumes > USB Storage, if you want. The ReadyNAS attempts to remember the name as long as there is a unique ID associated with the USB device so that the next time the device is connected, the same share name(s) will be available. Share access restrictions are not saved across disconnects, however.



Shares on RAID Volumes

Share Name	Description	Password	Disk Used	Quota (MB)	CIFS	NFS	AFP	HTTP/S	Rsync	Delete
Backup	Backup share		0 MB	0	✎	📄	✎	📄	📄	□
Brochures	Marketing Brochures	••••••	0 MB	1000	✎	📄	📄	📄	📄	□
Drawings	Engineering Drawings	••••••	0 MB	2000	✎	📄	📄	📄	📄	□
Finance	Company Finance	••••••	0 MB	0	✎	📄	📄	📄	📄	□
Music	Shared Music		0 MB	0	✎	📄	📄	📄	📄	□
Specs	Engineering Specs	••••••	0 MB	0	✎	📄	📄	📄	📄	□

Shares on USB Storage Devices

Click on the access icon to customize the access control. Place the mouse cursor over the icon to display the current access level in the status bar. For instruction on how to access the shares, click **Help**.

Share Name	Description	Password	CIFS	NFS	AFP	HTTP/S	Rsync	Delete
USB_HDD_1	USB-HS SAMSUNG SP1203N		✎	✎	✎	✎	✎	□

Figure 1-46

Note: Although access authorization is based on user login in non-Share mode, files saved on the USB device, regardless of the user account, are with UID 0. This is to allow easy sharing of the USB device with other ReadyNAS and PC systems.

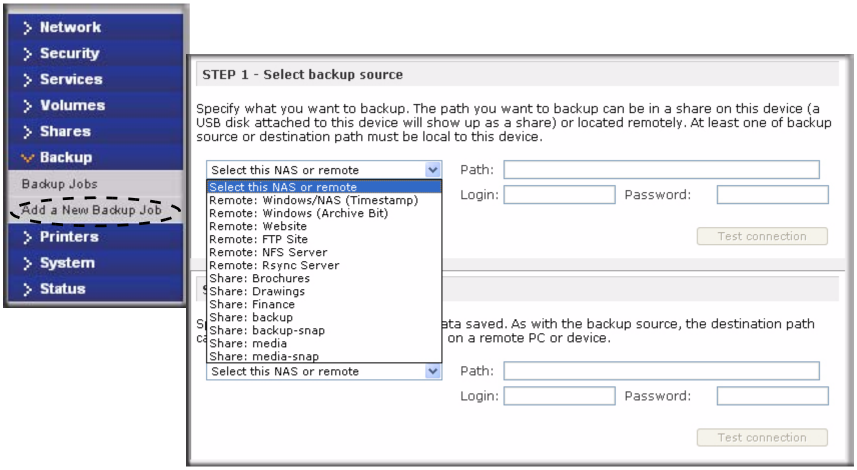
Configuring Backup Jobs

The Backup Manager integrated with the ReadyNAS allows the ReadyNAS to act as a powerful backup appliance. Backup tasks can be controlled directly from the ReadyNAS without the need for a client-based backup application.

With the flexibility to support incremental backups over CIFS/SMB, NFS, and rsync protocols, and full backups over FTP and HTTP protocols, the ReadyNAS can act as a simple central repository for both home and office environments. And with multiple ReadyNAS systems, you can set up one ReadyNAS to back up another directly.

Adding a New Backup Job

To create a new backup job, select **Add a New Backup Job**. A 4-step procedure screen for creating a job displays.



STEP 1 - Select backup source

Specify what you want to backup. The path you want to backup can be in a share on this device (a USB disk attached to this device will show up as a share) or located remotely. At least one of backup source or destination path must be local to this device.

Figure 1-47

Step 1 – Select Backup Source

The backup source can be located remotely, or it can be a public or a private home share, or all home shares on the ReadyNAS.

A USB device appears as a share, so if you want to back up a USB device, select a share name. If you want to back up data from a remote source, select from one of the following:

- **Windows/NAS (Timestamp)**. Select this if you wish to back up a share from a Windows PC. Incremental backups use timestamps to determine whether files should be backed up.
- **Windows/NAS (Archive Bit)**. Select this if you wish to back up a share from a Windows PC. Incremental backups use the archive bit of files, similar to Windows, to determine whether they should be backed up.
- **Website**. Select this if you wish to back up a website or a website directory. The backed up files include files in the default index file and all associated files, as well as all index file links to web page image files.
- **FTP site**. Select this if you wish to back up an FTP site or a path from that site.
- **NFS server**. Select this option if you wish to back up from a Linux or UNIX server across NFS. Mac OS X users can also use this option by setting up a NFS share from the console terminal.

- **Rsync server**. Select this if you wish to perform backups from a rsync server. Rsync was originally available for Linux and other flavors of UNIX, but has lately become popular under Windows and Mac for its efficient use of incremental file transfers. This is the preferred backup method between two ReadyNAS devices.

Once you have selected a backup source, you can enter the path from that source. If you selected a ReadyNAS share, you can either leave the path blank to backup the entire share, or enter a folder path. Note that you should use forward slashes (/), in place of backslashes (\).

If you selected a remote source, each remote protocol uses a slightly different notation for the path. If the path field is empty, selecting the remote source in the pull-down menu shows an example format of the path. Following are some examples:

- Examples of an FTP path:

  ftp://myserver/mypath/mydir

  ftp://myserver/mypath/mydir/myfile

- Examples of a website path:

  http://www.mywebsite.com

  http://192.168.0.101/mypath/mydir

- Examples of a Windows or remote NAS path:

  //myserver/myshare

  //myserver/myshare/myfolder

  //192.168.0.101/myshare/myfolder

- Examples of an NFS path:

  myserver:/mypath

  192.168.0.101:/mypath/myfolder

- Examples of a Rsync path:

  myserver::mymodule/mypath

  192.168.0.101::mymodule/mypath

- Examples of a local path:

  myfolder

  media/Videos

  My Folder

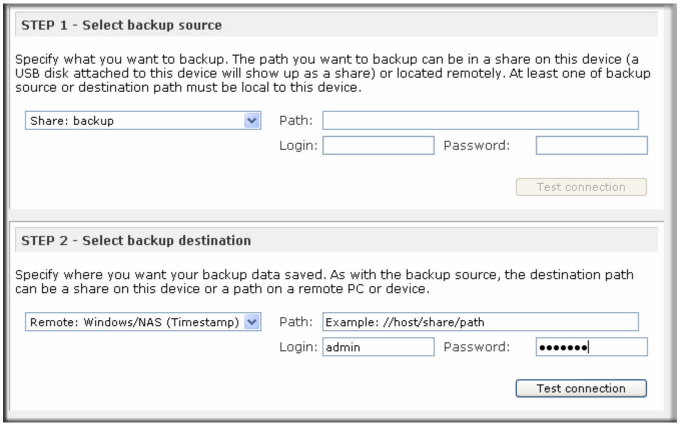
My Documents/My Pictures

With a remote source, you might need to enter a login and password to access the share. If you are accessing a password-protected share on a remote ReadyNAS server configured for Share security mode, enter the name of the share name for login.

To make sure that you have proper access to the backup source, click **Test Connection** before continuing.

Step 2 – Select Backup Destination

The Step 2 process is almost identical to Step 1 except that you are now specifying the backup destination. If you selected a remote backup source, you need to select a public or a private home share on the ReadyNAS (either the source or destination must be local to the ReadyNAS). If you selected a ReadyNAS share for the source, you can either enter another local ReadyNAS share for the destination, or you can specify a remote backup destination.



STEP 1 - Select backup source

Specify what you want to backup. The path you want to backup can be in a share on this device (a USB disk attached to this device will show up as a share) or located remotely. At least one of backup source or destination path must be local to this device.

Share: backup
Path:
Login:
Password:

STEP 2 - Select backup destination

Specify where you want your backup data saved. As with the backup source, the destination path can be a share on this device or a path on a remote PC or device.

Remote: Windows/NAS (Timestamp)
Path: Example: //host/share/path
Login: admin
Password: •••••••

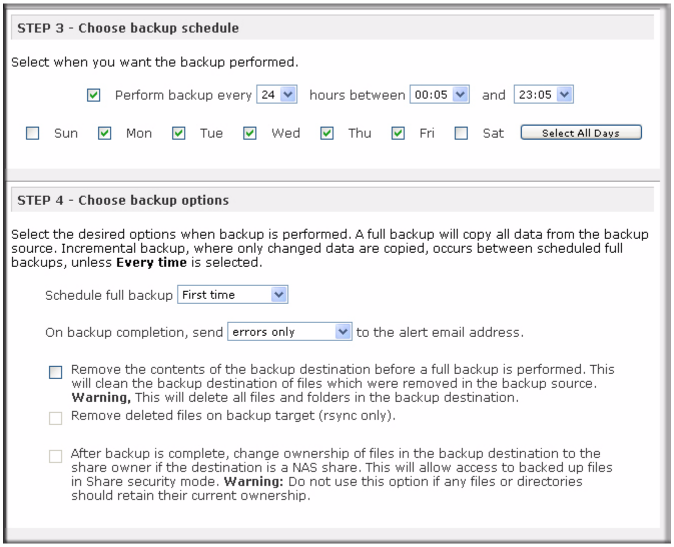
Figure 1-48

The remote backup destination can be a Windows PC/ReadyNAS system, an NFS server, or a rsync server. Note that you can select **rsync** for a remote ReadyNAS if it is configured to serve data over rsync.

Step 3 – Choose Backup Schedule

You can select a backup schedule as frequently as once every 4 hours daily or just once a week. The backup schedule is offset by 5 minutes from the hour to allow you to schedule snapshots on the hour (snapshots are almost instantaneous) and perform backups of those snapshots (see “Snapshots” on page 1-28 to set up a snapshot schedule).

If you wish, you can elect not to schedule the backup job so that you can invoke it manually instead by clearing (deselecting) the **Perform backup every...** check box. (You might want to do this if your ReadyNAS has a backup button.)



STEP 3 - Choose backup schedule

Select when you want the backup performed.

☑ Perform backup every 24 hours between 00:05 and 23:05

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

STEP 4 - Choose backup options

Select the desired options when backup is performed. A full backup will copy all data from the backup source. Incremental backup, where only changed data are copied, occurs between scheduled full backups, unless **Every time** is selected.

Schedule full backup First time

On backup completion, send errors only to the alert email address.

□ Remove the contents of the backup destination before a full backup is performed. This will clean the backup destination of files which were removed in the backup source. **Warning,** This will delete all files and folders in the backup destination.

□ Remove deleted files on backup target (rsync only).

□ After backup is complete, change ownership of files in the backup destination to the share owner if the destination is a NAS share. This will allow access to backed up files in Share security mode. **Warning:** Do not use this option if any files or directories should retain their current ownership.

Figure 1-49

Step 4 – Choose Backup Options

In this last step, you can set up how you want backups to be performed. To set up a backup schedule:

1. **Schedule a full backup**. Select when you want full backups to be performed. You can elect to do this just the first time, every week, every 2 weeks, every 3 weeks, every 4 weeks, or every time this backup job is invoked.

   The first full backup is performed at the next scheduled occurrence of the backup depending on the schedule you specify, and the next full backup is performed at the weekly interval you choose calculated from this first backup. Incremental backup is performed between the full backup cycles.

   Backups of a Web or FTP site only have the option to do a full backup every time.

2. **Send a backup log**. Backup logs can be sent to the users on the Alert contact list when the backup is complete. It is a good idea to select this option to make sure that files are backed up

as expected. You can elect to send only errors encountered during backup, full backup logs consisting of file listings (can be large), or status and errors (status refers to completion status).

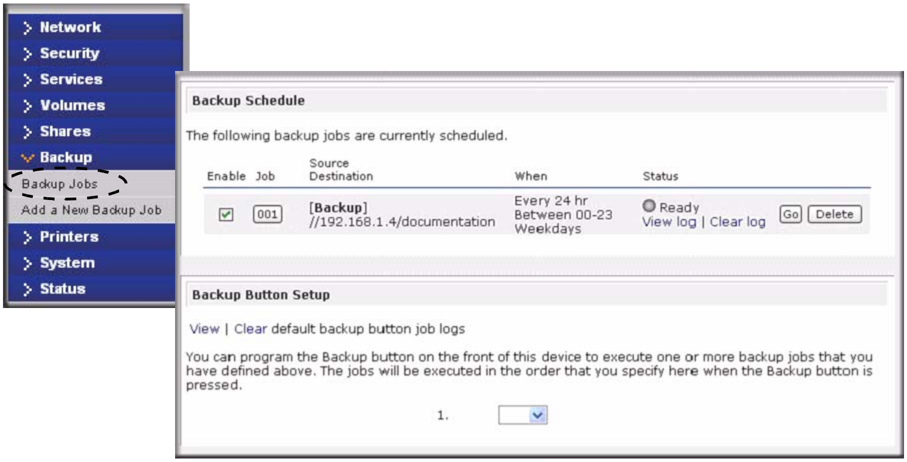
➡	**Note:** Backup log e-mails are restricted to approximately 10K lines. To view the full backup log (regardless of length), select Status > Logs and click the **Download All Logs** link.

3. **Remove files from backup destination**. Select if you want to erase the destination path contents before the backup is performed. Be careful not to reverse your backup source and destination as doing so can delete your source files for good. It is safer to not select this option unless your device is running low on space. Do experiment with a test share to make sure you understand this option.
4. **Remove deleted files on backup target for rsync**. By default, files deleted in the backup source will not get deleted in the backup destination. With rsync, you have the option of simulating mirror mode by removing files in the backup destination deleted from the backup source since the last backup. Select this option if you wish to do this. Experiment with a test share to make sure that you understand this option.
5. **Change ownership of backup files**. The Backup Manager attempts to maintain original file ownership whenever possible; however, this might cause problems in Share Security mode when backup files are accessed. To work around this, you have the option of automatically changing the ownership of the backed-up files to match the ownership of the share. This allows anyone who can access the backup share to have full access to the backed-up files.
6. Click **Apply** to save your settings.

Before trusting your backup job to a schedule, it is a good practice to manually perform the backup to make sure that access to the remote backup source or destination is granted, and that the backup job can be done within the backup frequency you selected. This can be done after you save the backup job.

Viewing the Backup Schedule

After saving the backup job, a new job appears in the Backup Schedule section of the Backup Jobs screen.



Backup Schedule

The following backup jobs are currently scheduled.

Enable	Job	Source Destination	When	Status	
☑	001	[Backup] //192.168.1.4/documentation	Every 24 hr Between 00-23 Weekdays	○ Ready View log | Clear log	Go Delete

Backup Button Setup

View | Clear default backup button job logs

You can program the Backup button on the front of this device to execute one or more backup jobs that you have defined above. The jobs will be executed in the order that you specify here when the Backup button is pressed.

1.

Figure 1-50

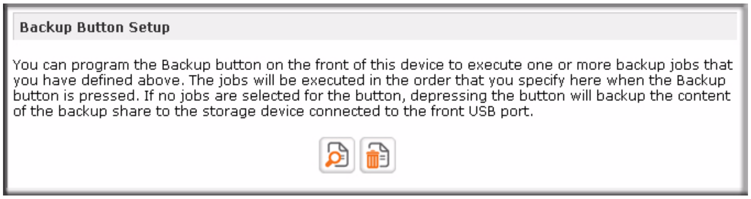
A summary of the backup jobs that have been scheduled are shown; jobs are numbered beginning at 001.

To manage your backup jobs:

1. Click the Job number icon to modify the selected backup job.
2. Enable or disable job scheduling by selecting/clearing the **Enable** check box. Disabling the job does not delete the job, but removes it from the automatic scheduling queue.
3. Click **Delete** to permanently remove the job.
4. Click **Go** to manually start the backup job. The status changes when the backup starts, when an error is encountered, or when the job has finished.
5. Select the **View Log** link to check a detailed status of the backup.
6. click **Clear Logs** to refresh and clear the current log detail.

Programming the Backup Button

On ReadyNAS systems that have the Backup Button feature, you can program the button to execute one or more pre-defined backup jobs (see "Backing Up the ReadyNAS to a USB Drive" on page 3-9 for more information).



Backup Button Setup

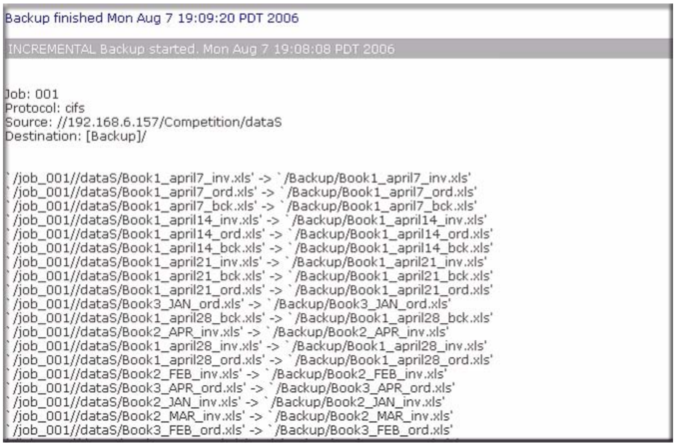
You can program the Backup button on the front of this device to execute one or more backup jobs that you have defined above. The jobs will be executed in the order that you specify here when the Backup button is pressed. If no jobs are selected for the button, depressing the button will backup the content of the backup share to the storage device connected to the front USB port.

Figure 1-51

Simply select the backup jobs in the order that you want them run and click **Apply**. Pressing the Backup Button once starts the job(s).

Viewing the Backup Log

You can view the backup log while the job is in progress or after it has finished.



```
Backup finished Mon Aug 7 19:09:20 PDT 2006

INCREMENTAL Backup started. Mon Aug 7 19:08:08 PDT 2006


Job: 001
Protocol: cifs
Source: //192.168.6.157/Competition/dataS
Destination: [Backup]/


` /job_001//dataS/Book1_april7_inv.xls' -> ` /Backup/Book1_april7_inv.xls'
` /job_001//dataS/Book1_april7_ord.xls' -> ` /Backup/Book1_april7_ord.xls'
` /job_001//dataS/Book1_april7_bck.xls' -> ` /Backup/Book1_april7_bck.xls'
` /job_001//dataS/Book1_april14_inv.xls' -> ` /Backup/Book1_april14_inv.xls'
` /job_001//dataS/Book1_april14_ord.xls' -> ` /Backup/Book1_april14_ord.xls'
` /job_001//dataS/Book1_april14_bck.xls' -> ` /Backup/Book1_april14_bck.xls'
` /job_001//dataS/Book1_april21_inv.xls' -> ` /Backup/Book1_april21_inv.xls'
` /job_001//dataS/Book1_april21_bck.xls' -> ` /Backup/Book1_april21_bck.xls'
` /job_001//dataS/Book1_april21_ord.xls' -> ` /Backup/Book1_april21_ord.xls'
` /job_001//dataS/Book3_JAN_ord.xls' -> ` /Backup/Book3_JAN_ord.xls'
` /job_001//dataS/Book1_april28_bck.xls' -> ` /Backup/Book1_april28_bck.xls'
` /job_001//dataS/Book2_APR_inv.xls' -> ` /Backup/Book2_APR_inv.xls'
` /job_001//dataS/Book1_april28_inv.xls' -> ` /Backup/Book1_april28_inv.xls'
` /job_001//dataS/Book1_april28_ord.xls' -> ` /Backup/Book1_april28_ord.xls'
` /job_001//dataS/Book2_FEB_inv.xls' -> ` /Backup/Book2_FEB_inv.xls'
` /job_001//dataS/Book3_APR_ord.xls' -> ` /Backup/Book3_APR_ord.xls'
` /job_001//dataS/Book2_JAN_inv.xls' -> ` /Backup/Book2_JAN_inv.xls'
` /job_001//dataS/Book2_MAR_inv.xls' -> ` /Backup/Book2_MAR_inv.xls'
` /job_001//dataS/Book3_FEB_ord.xls' -> ` /Backup/Book3_FEB_ord.xls'
```

Figure 1-52

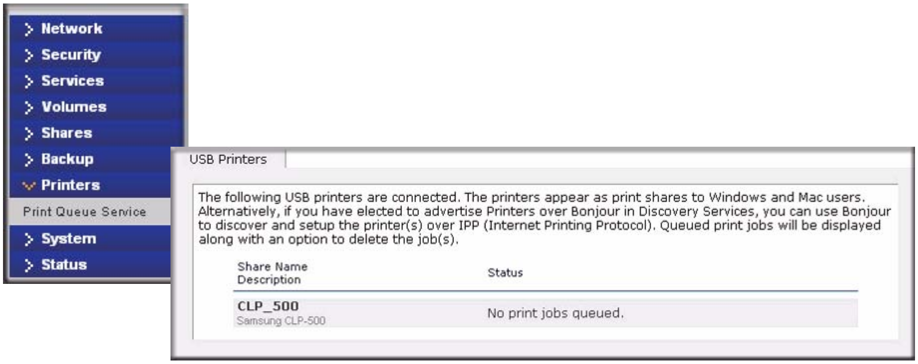
The log format might differ depending on the backup source and destination type that was selected, but you can see when the job was started and finished, and whether it was completed successfully or with errors.

Editing a Backup Job

To edit a backup job, you can either click the 3-digit job number button in the Backup Jobs screen, or you can click the **Edit Backup Job** link while viewing that job log. You can then make appropriate changes or adjustments to the job.

Setting Up Printers

The ReadyNAS device supports automatic recognition of USB printers. If you have not already done so, you can connect a printer now, wait a few seconds, and click **Refresh** to display detected printers. The print share name automatically reflects the manufacturer and model of your printer and is listed in the USB Printers section of the Print Queue service screen.



The following USB printers are connected. The printers appear as print shares to Windows and Mac users. Alternatively, if you have elected to advertise Printers over Bonjour in Discovery Services, you can use Bonjour to discover and setup the printer(s) over IPP (Internet Printing Protocol). Queued print jobs will be displayed along with an option to delete the job(s).

Share Name Description	Status
CLP_500 Samsung CLP-500	No print jobs queued.

Figure 1-53

Print Shares over CIFS/SMB

The ReadyNAS can act as a print server for up to two USB printers for your Windows or Mac clients.

To set up a printer in Windows:

1. Click **Browse** in RAIDar or simply enter \\hostname in the Windows Explorer address bar to list all data and printer shares on the ReadyNAS.
2. Double-click the printer icon to assign a Windows driver.

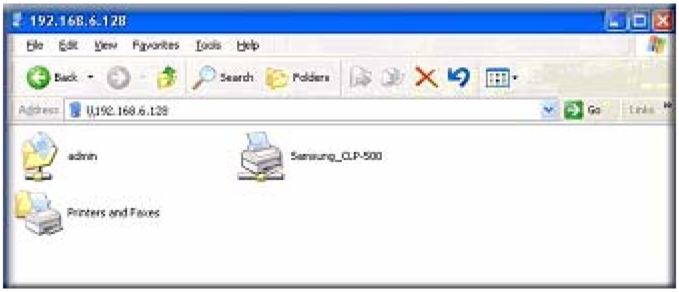


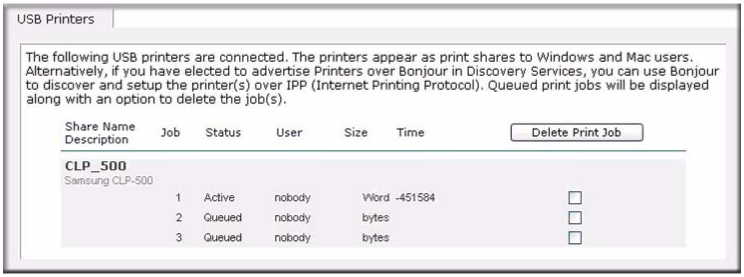
Figure 1-54

IPP Printing

The ReadyNAS also supports the IETF standard Internet Printing Protocol (IPP) over HTTP. Any client supporting IPP printing (IPP is available natively on the latest Windows XP OS and OS X) can now use this protocol to utilize printers connected to the ReadyNAS. The simplest way to utilize IPP printing is to use Bonjour to discover and set up the print queue. Bonjour is built into OS X and can be installed on Windows computers (Bonjour for Windows is available for download from the Apple website at *http://www.apple.com/macosx/features/bonjour/*).

Managing Print Queues

From time to time, printers might run out of ink or paper, or simply jam up, forcing you to deal with the print jobs stuck in a queue. The ReadyNAS has a built-in print queue management to handle this. Simply select the USB Printers tab or click **Refresh** to display the printers and the jobs queued up for any “stuck” printers.



USB Printers

The following USB printers are connected. The printers appear as print shares to Windows and Mac users. Alternatively, if you have elected to advertise Printers over Bonjour in Discovery Services, you can use Bonjour to discover and setup the printer(s) over IPP (Internet Printing Protocol). Queued print jobs will be displayed along with an option to delete the job(s).

Share Name Description	Job	Status	User	Size	Time	Delete Print Job
CLP_500 Samsung CLP-500						
	1	Active	nobody	Word -451584		□
	2	Queued	nobody	bytes		□
	3	Queued	nobody	bytes		□

Figure 1-55

Select the radio button next to the print job and click **Delete Print Job** to remove a job (or all jobs) from the print queue.

Managing Your ReadyNAS System

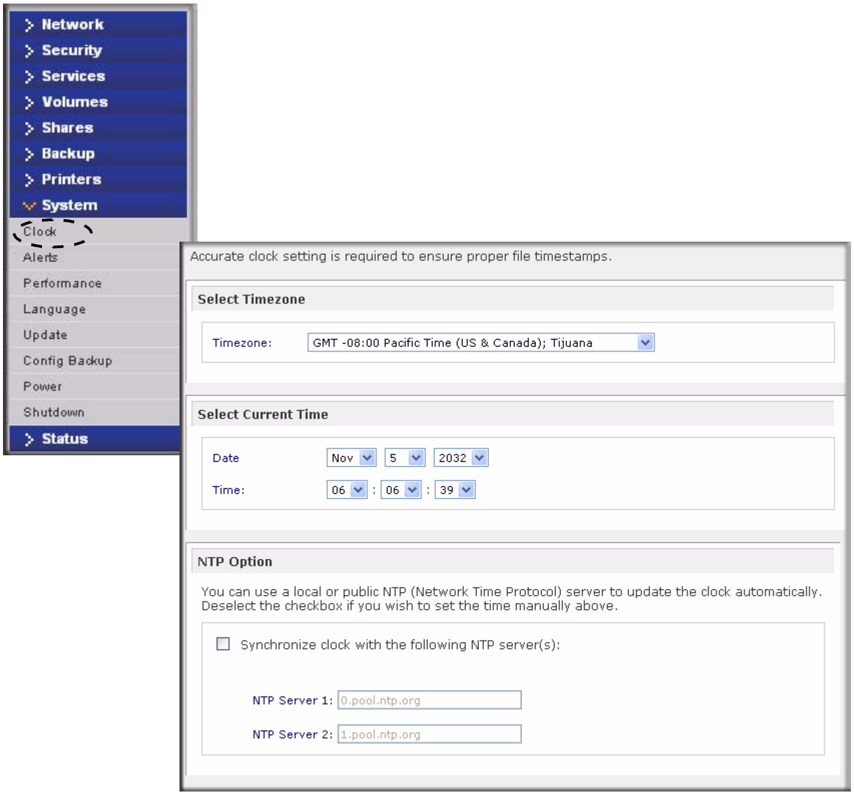
To set up and manage your ReadyNAS effectively, make sure that you review the settings in the following sections, and implement any necessary modifications or updates.

Clock

An accurate time setting on the Clock screen is required to ensure proper file timestamps. You can access the Clock screen by selecting System > Clock from the main menu.

System Time

The Select Timezone section and the Select Current Time section of the Clock screen allow you to set the Timezone, and the Date and Time.



Accurate clock setting is required to ensure proper file timestamps.

Select Timezone

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

Select Current Time

Date Nov 5 2032

Time: 06 : 06 : 39

NTP Option

You can use a local or public NTP (Network Time Protocol) server to update the clock automatically. Deselect the checkbox if you wish to set the time manually above.

□ Synchronize clock with the following NTP server(s):

NTP Server 1: 0.pool.ntp.org

NTP Server 2: 1.pool.ntp.org

Figure 1-56

NTP Option

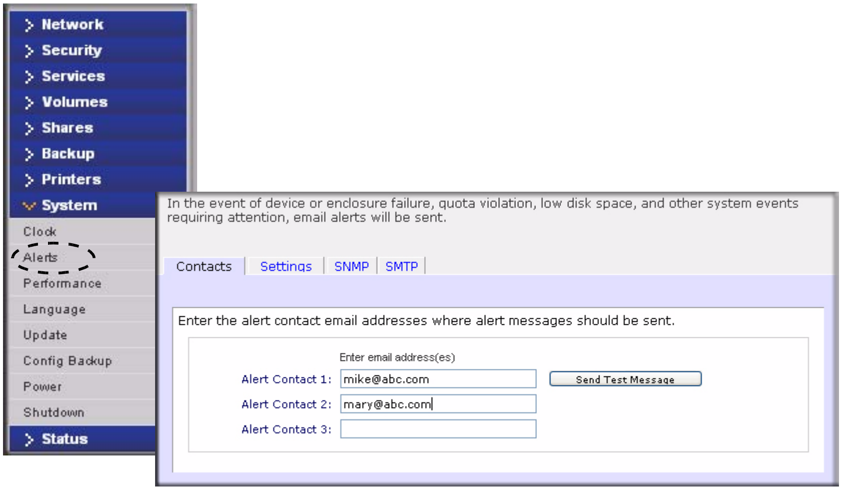
You can elect to synchronize the system time on the device with a remote NTP (Network Time Protocol) server. You can elect to keep the default servers or enter up to two NTP servers closer to your locale. You can find an available public NTP servers by searching the Web.

Alerts

In the event of a device or an enclosure failure, a quota violation, low-disk space warning, and other system events requiring your attention, e-mail alerts are sent. The Alerts screen is accessed by selecting System > Alerts from the main menu.

Alerts Contacts

The Contacts tab allows you to specify up to three e-mail addresses where system alerts will be sent. The ReadyNAS device has a robust system monitoring feature and sends e-mail alerts if something appears to be wrong or when a device has failed. Make sure to enter a primary e-mail address and a backup one if possible.



In the event of device or enclosure failure, quota violation, low disk space, and other system events requiring attention, email alerts will be sent.

Enter the alert contact email addresses where alert messages should be sent.

Enter email address(es)

Alert Contact 1: mike@abc.com

Alert Contact 2: mary@abc.com

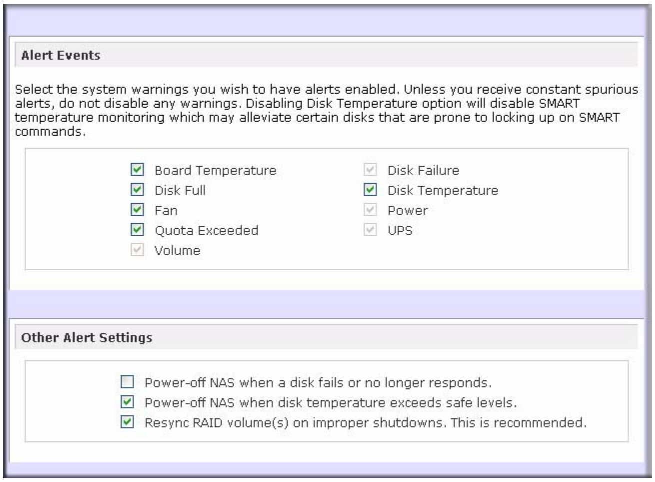
Alert Contact 3:

Figure 1-57

Some e-mail addresses can be tied to a mobile phone. This is a great way to monitor the device when you are away from your desk.

Alerts Settings

This ReadyNAS device has been preconfigured with mandatory and optional alerts for various system device warnings and failures. The Settings tab allows you to control the settings for the optional alerts.



Alert Events

Select the system warnings you wish to have alerts enabled. Unless you receive constant spurious alerts, do not disable any warnings. Disabling Disk Temperature option will disable SMART temperature monitoring which may alleviate certain disks that are prone to locking up on SMART commands.

☑ Board Temperature
☑ Disk Full
☑ Fan
☑ Quota Exceeded
☑ Volume
☑ Disk Failure
☑ Disk Temperature
☑ Power
☑ UPS

Other Alert Settings

□ Power-off NAS when a disk fails or no longer responds.
☑ Power-off NAS when disk temperature exceeds safe levels.
☑ Resync RAID volume(s) on improper shutdowns. This is recommended.

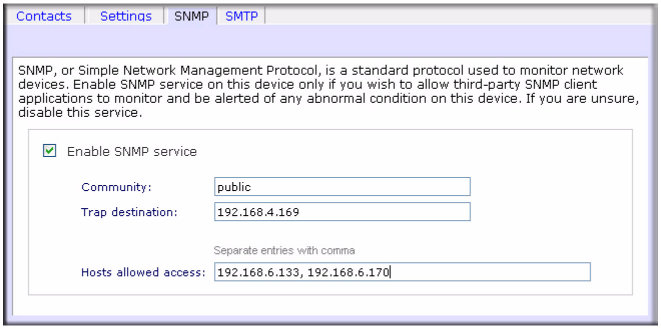
Figure 1-58

NETGEAR strongly recommends that you keep all alerts enabled; however, you might choose to disable an alert if you are aware of a problem and wish to temporarily disable it.

At the bottom of the screen in the Other Alert Settings section, there are a couple of additional options of note. Selecting the **Power-off NAS when a disk fails or no longer responds** option gracefully powers off the ReadyNAS if a disk failure or a disk remove event is detected. Selecting the **Power-off NAS when disk temperature exceeds safe level** gracefully powers off the ReadyNAS when the disk temperature exceeds the nominal range.

SNMP

If you utilize an SNMP management system such as HP OpenView or CA UniCenter to monitor devices on your network, you can set up the ReadyNAS device to work within this infrastructure.



SNMP, or Simple Network Management Protocol, is a standard protocol used to monitor network devices. Enable SNMP service on this device only if you wish to allow third-party SNMP client applications to monitor and be alerted of any abnormal condition on this device. If you are unsure, disable this service.

☑ Enable SNMP service

Community: public

Trap destination: 192.168.4.169

Separate entries with comma

Hosts allowed access: 192.168.6.133, 192.168.6.170

Figure 1-59

To set up SNMP service:

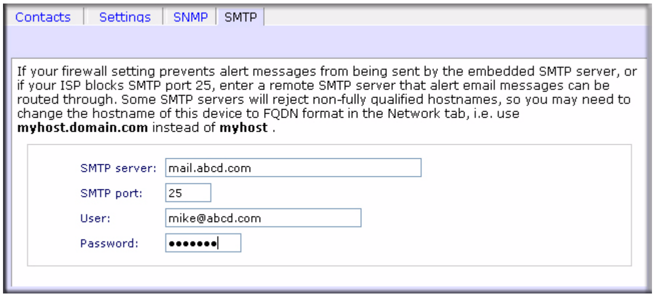
1. Select the SNMP tab to display the SNMP settings.
2. Select the **Enable SNMP service** check box. You can leave the **Community** field set to **public**, or specify a private name if you have opted for a more segregated monitoring scheme.
3. Enter a host name or an IP address in the **Trap destination** field. This is where all trap messages will be sent. The following system events generate a trap:
   - Abnormal power voltage
   - Abnormal board enclosure temperature
   - Fan failure
   - UPS connected
   - UPS detected power failure
   - RAID disk sync started and finished
   - RAID disk added, removed, and failure
   - Snapshot invalidated
4. If you wish to limit SNMP access to only a secure list of hosts, specify the hosts in the **Hosts allowed access** field.
5. Click **Apply** to save your settings.

When you have saved the SNMP settings on the ReadyNAS, you can import the NETGEAR SNMP MIB to your SNMP client application. The NETGEAR MIB can be obtained from the included *Installation CD* or downloaded from the NETGEAR Support site at *http://www.netgear.com/support*.

SMTP

The ReadyNAS device has a built-in e-mail message transfer agent (MTA) that is set up to send alert e-mail messages from the device. Some corporate environments, however, might have a firewall that blocks untrusted MTAs from sending out messages.

If you were unable to receive the test message from the Alerts Settings tab, it might have been blocked by the firewall. In that case, specify an appropriate SMTP server in this tab.



If your firewall setting prevents alert messages from being sent by the embedded SMTP server, or if your ISP blocks SMTP port 25, enter a remote SMTP server that alert email messages can be routed through. Some SMTP servers will reject non-fully qualified hostnames, so you may need to change the hostname of this device to FQDN format in the Network tab, i.e. use **myhost.domain.com** instead of **myhost** .

SMTP server: mail.abcd.com

SMTP port: 25

User: mike@abcd.com

Password: •••••••

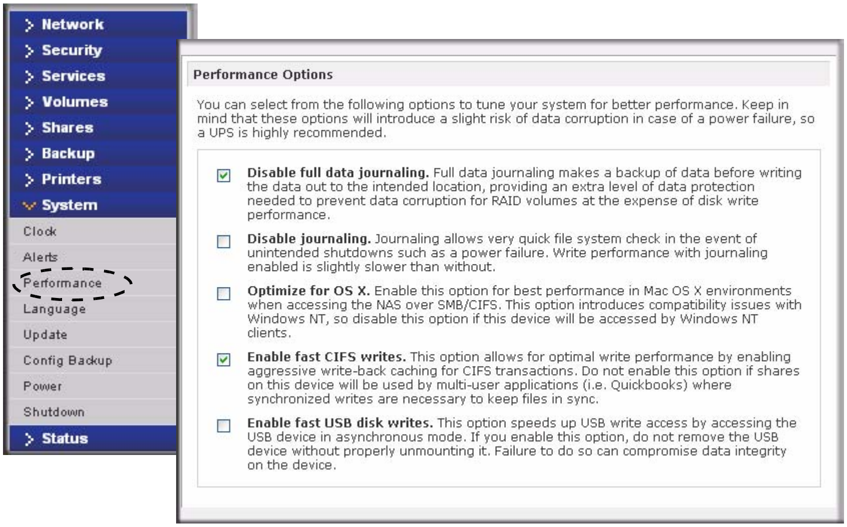
Figure 1-60

Internet Service Providers (ISPs) for home might also block untrusted MTAs. Furthermore, they might allow you to specify their SMTP server but requires that you enter a user login and password to send out e-mail—this is common with most DSL services. If this is the case, simply enter the user name and password in the fields provided.

Performance

If you wish to tweak the system performance, select Performance from the main menu. Note that some of the settings suggest that you utilize an Uninterruptible Power Supply (UPS) before enabling that option:

- NETGEAR recommends that you select the **Disable full data journaling** only if the NAS has UPS protection. Without battery backup, there is a small chance that parity written to a disk in a RAID set might become out of sync with the data disks if a power failure suddenly occurs, possibly causing incorrect data to be recovered if one disk fails. Without full data journaling, disk write performance increases substantially.



Performance Options

You can select from the following options to tune your system for better performance. Keep in mind that these options will introduce a slight risk of data corruption in case of a power failure, so a UPS is highly recommended.

☑ **Disable full data journaling.** Full data journaling makes a backup of data before writing the data out to the intended location, providing an extra level of data protection needed to prevent data corruption for RAID volumes at the expense of disk write performance.

□ **Disable journaling.** Journaling allows very quick file system check in the event of unintended shutdowns such as a power failure. Write performance with journaling enabled is slightly slower than without.

□ **Optimize for OS X.** Enable this option for best performance in Mac OS X environments when accessing the NAS over SMB/CIFS. This option introduces compatibility issues with Windows NT, so disable this option if this device will be accessed by Windows NT clients.

☑ **Enable fast CIFS writes.** This option allows for optimal write performance by enabling aggressive write-back caching for CIFS transactions. Do not enable this option if shares on this device will be used by multi-user applications (i.e. Quickbooks) where synchronized writes are necessary to keep files in sync.

□ **Enable fast USB disk writes.** This option speeds up USB write access by accessing the USB device in asynchronous mode. If you enable this option, do not remove the USB device without properly unmounting it. Failure to do so can compromise data integrity on the device.

Figure 1-61

- Select **Disable journaling** if you understand the consequences of this action, and you do not mind a long file system check (only after unexpected power failures). File system journaling allows disk checks of only a few seconds verses possibly an hour or longer without journaling. Disabling journaling improves disk write performance slightly.

➡	**Note:** You can buy a UPS with USB monitoring at a very reasonable cost. By safely allowing the performance options to be checked, you can effectively double your write performance and provide uninterrupted service of your ReadyNAS for a very low price.

- The **Optimize for OS X** option provides the best performance in Mac OS X environments when connected to the ReadyNAS through the SMB/CIFS protocol. This option, however, introduces compatibility issues with Windows NT 4.0; do not enable this option if this device will be accessed by Windows NT 4.0 clients.
- The **Enable fast CIFS writes** option allows for fast write performance by enabling aggressive write-back caching over CIFS. Do not enable this option in multi-user application environments such as Quick Books where synchronized writes are necessary to keep files in sync.
- The **Force CIFS filename case-sensitivity** option provides substantial performance improvement when you access CIFS shares when many files are being copied; however, before enabling this option, understand the ramifications.

- Since Windows runs in case-insensitive mode, one side-effect of enabling this option is that two file names with different cases (for example, ABC and abc) appear as two files but, when you open one file, the other file might actually open.
- Another effect of this option is that, in Explorer, you now need to enter the exact case for search strings for the Find option (that is, searching for "abc" no longer returns file "ABC").
- Some Windows applications that assume case-insensitive operations (for example, **BackupExec**) may have problems. Do not enable this option if you have clients accessing the NAS running Windows NT/95 or earlier.

- The **Enable fast USB disk writes** option speeds up USB write access by allowing access to the USB device in asynchronous mode. If you enable this option, do not remove the USB device without properly unmounting it. Failure to do so can compromise data integrity on the device.

Adding a UPS for Performance

Adding a UPS to the NAS is an easy way to protect against power failures, but as mentioned in "Performance" on page 1-56, a UPS can also safely allow for a more aggressive performance setting. Simply connect the NAS power cable to the UPS, and connect the UPS USB monitoring cable between the UPS and the NAS. The UPS is detected automatically and shows up in the Status bar. You can move the mouse pointer over the UPS LED icon to display the current UPS information and battery life.

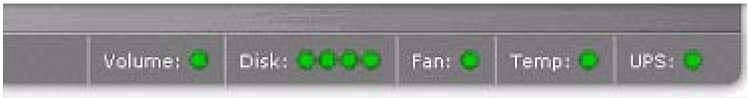


Figure 1-62

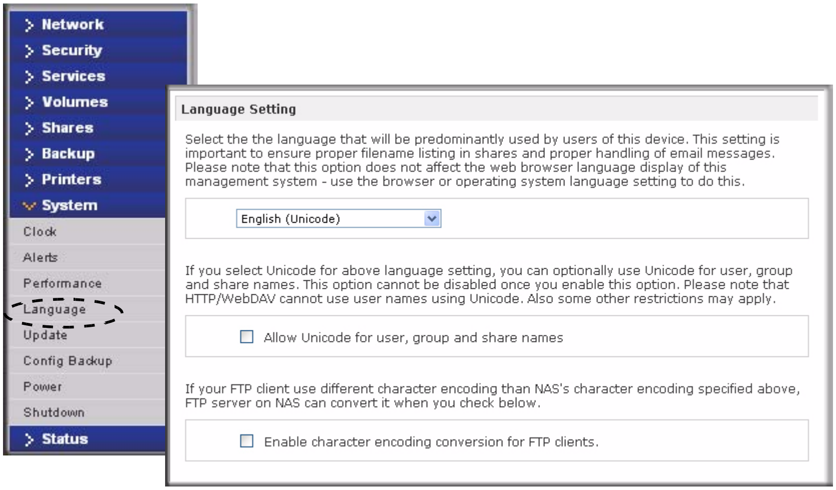
Note: Note that alert notification and automatic system optimization is available only with UPS that utilizes a USB monitoring interface.

You are notified by e-mail whenever the status of the UPS changes; for example, when a power failure forces the UPS to be in battery mode or when the battery is low. When the battery is low, the NAS device automatically shuts down safely.

Make sure to adjust the optimization settings in the Performance screen if you wish to take advantage of the available options.

Language

The Language Setting screen offers the option of setting the ReadyNAS device to the appropriate character set for file names.



Language Setting

Select the the language that will be predominantly used by users of this device. This setting is important to ensure proper filename listing in shares and proper handling of email messages. Please note that this option does not affect the web browser language display of this management system - use the browser or operating system language setting to do this.

English (Unicode)

If you select Unicode for above language setting, you can optionally use Unicode for user, group and share names. This option cannot be disabled once you enable this option. Please note that HTTP/WebDAV cannot use user names using Unicode. Also some other restrictions may apply.

□ Allow Unicode for user, group and share names

If your FTP client use different character encoding than NAS's character encoding specified above, FTP server on NAS can convert it when you check below.

□ Enable character encoding conversion for FTP clients.

Figure 1-63

For example, selecting Japanese allows you to share files with Japanese names in Windows Explorer.

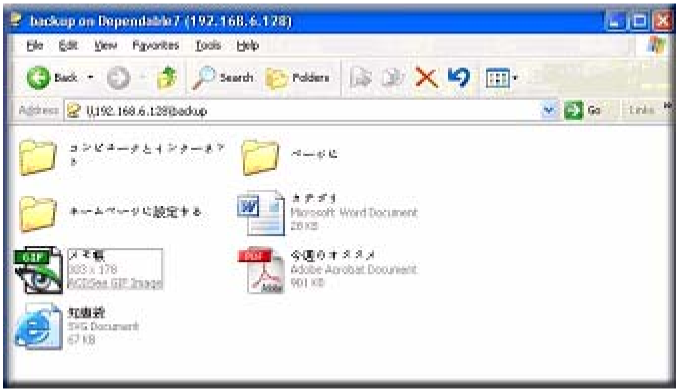


Figure 1-64

It is best to select the appropriate language based on the region where the device will be operated.

Note: This option does not set the web browser language display—browser settings must be done using the browser language option.

If you wish, you can select the **Allow Unicode for user, group and share names** check box to allow for greater flexibility in non-English speaking regions. This option, once selected, cannot be reversed.

Note: HTTP and WebDAV access do not work with Unicode user names. Other restrictions might exist.

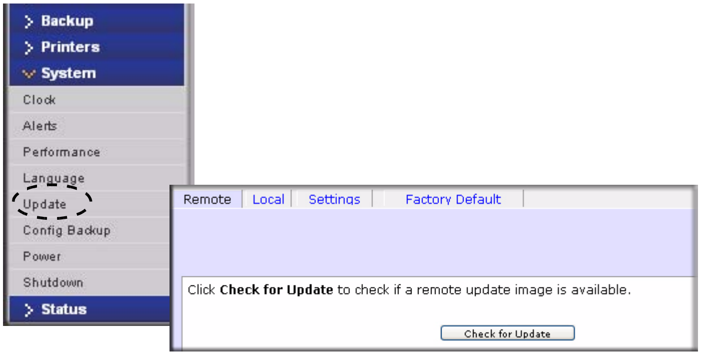
If your FTP client uses different character encoding from the NAS character encoding specified in Unicode, the NAS FTP server will convert it if you select the **Enable character encoding conversion for FTP clients** check box.

Updating ReadyNAS

The ReadyNAS device offers the option of upgrading the operating firmware either automatically using the Remote Update option or by manually loading an update image downloaded from the NETGEAR Support website.

Remote Update

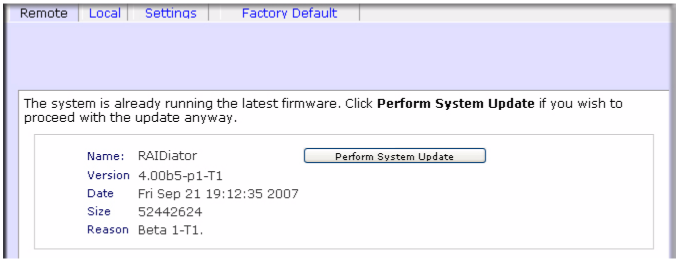
The preferred and quicker method if the ReadyNAS has Internet access is the Remote update option. Select Update from the main menu and then select the Remote tab. Click **Check for Updates** to check for updates on the NETGEAR update server.



Click **Check for Update** to check if a remote update image is available.

Figure 1-65

If you wish to continue, click **Perform System Update**. After the update image has been downloaded, you will be asked to reboot the system. The update process updates only the firmware image and does not modify your data volume. However, it is always a good idea to back up your important data whenever you perform an update.



The system is already running the latest firmware. Click **Perform System Update** if you wish to proceed with the update anyway.

Name:	RAIDiator
Version	4.00b5-p1-T1
Date	Fri Sep 21 19:12:35 2007
Size	52442624
Reason	Beta 1-T1.

Figure 1-66

Local Update

When the ReadyNAS device is not connected to the Internet, or Internet access is blocked, you can download an update file from the Support site and upload that file to the ReadyNAS by selecting the Local update tab. The update file can be a RAIDiator firmware image or an add-on package.

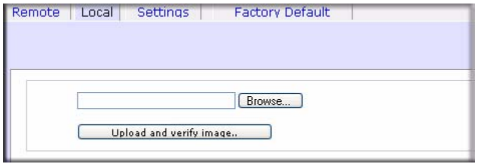


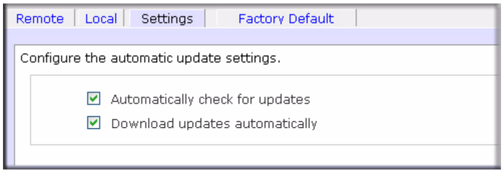
Figure 1-67

Click **Browse** to select the update file and then click **Upload and verify image**. The process takes several minutes after which you are requested to reboot the system and proceed with the upgrade.

⚠	**Warning:** ***Do not*** click the browser Refresh button during the update process.

Settings

If you do have a reliable Internet connection, you can enable the automatic update check and download options in the Settings tab.



Configure the automatic update settings.

☑ Automatically check for updates

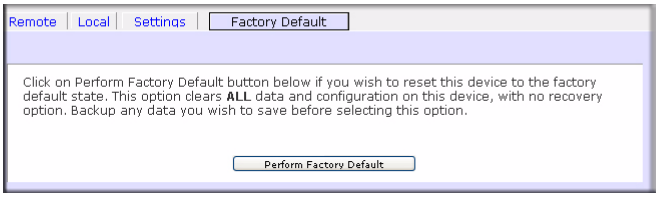
☑ Download updates automatically

Figure 1-68

If you select the **Automatically check for updates** check box, the ReadyNAS does not download the actual firmware update, but notifies you when an update is available. If you select the **Download updates automatically** check box, the update image is downloaded, and you are notified by e-mail to reboot the device to perform the update.

Factory Default

The Factory Default tab allows you to reset the ReadyNAS device back to its factory default state. Choose this option carefully as ***All Data Will Be Lost*** unless you back up any data that you wish to keep prior to clicking **Perform Factory Default**.



Click on Perform Factory Default button below if you wish to reset this device to the factory default state. This option clears **ALL** data and configuration on this device, with no recovery option. Backup any data you wish to save before selecting this option.

Figure 1-69

If you select this option, you are asked to confirm the command by typing: **FACTORY.**

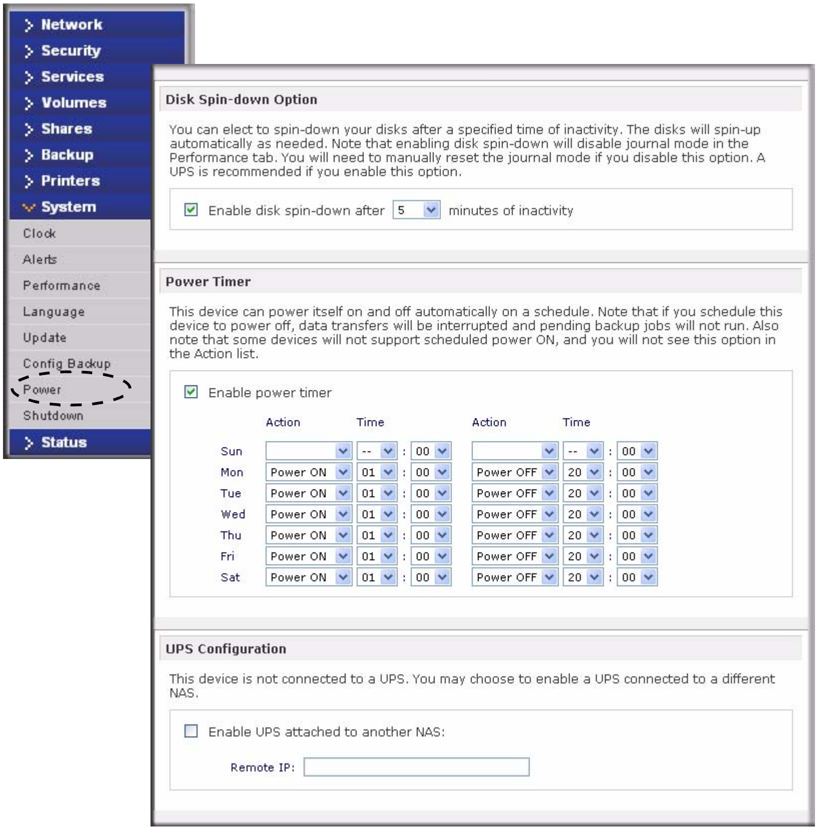
⚠	**Warning:** Resetting to Factory Default erases everything, including data shares, volume(s), user and group accounts, and configuration information. There is no way to recover after you confirm this command.

Power Management

The ReadyNAS offers a couple of power management options to reduce system power consumption, both while the system is in use and when it is not in use.

Disk Spin-Down Option

You can elect to spin down your ReadyNAS disks after a specified time of inactivity. The disks will spin up as needed. To enable spin-down mode, select the **Enable disk spin-down after...** check box, and specify the minutes of inactivity before spin up.



Disk Spin-down Option

You can elect to spin-down your disks after a specified time of inactivity. The disks will spin-up automatically as needed. Note that enabling disk spin-down will disable journal mode in the Performance tab. You will need to manually reset the journal mode if you disable this option. A UPS is recommended if you enable this option.

☑ Enable disk spin-down after 5 minutes of inactivity

Power Timer

This device can power itself on and off automatically on a schedule. Note that if you schedule this device to power off, data transfers will be interrupted and pending backup jobs will not run. Also note that some devices will not support scheduled power ON, and you will not see this option in the Action list.

☑ Enable power timer

	Action	Time	Action	Time
Sun		-- : 00		-- : 00
Mon	Power ON	01 : 00	Power OFF	20 : 00
Tue	Power ON	01 : 00	Power OFF	20 : 00
Wed	Power ON	01 : 00	Power OFF	20 : 00
Thu	Power ON	01 : 00	Power OFF	20 : 00
Fri	Power ON	01 : 00	Power OFF	20 : 00
Sat	Power ON	01 : 00	Power OFF	20 : 00

UPS Configuration

This device is not connected to a UPS. You may choose to enable a UPS connected to a different NAS.

☐ Enable UPS attached to another NAS:

Remote IP:

Figure 1-70

Note: Enabling disk spin-down disables journal mode. Once enabled, if you decide to disable disk spin-down, you need to manually re-enable journal mode if desired. NETGEAR recommends UPS if you utilize this option.

Power Timer

The ReadyNAS can be scheduled to power off and power back on (on certain models) automatically (see Figure 1-70). Select the **Enable power timer** check box and enter the action and time. (The **Power ON** option is available on the ReadyNAS NV through an add-on package.)[1] The **Power ON** option does not appear if the ReadyNAS hardware does not support this feature.

➡ **Note:** When the ReadyNAS is powered off, any file transfers and backup jobs are interrupted, and backup jobs scheduled during the power off state do not run.

UPS Configuration

If this device is not connection to a UPS device, you may ele4ct to enable a UPS connection to another NAS device. Select the **Enable UPS attached to another NAS** check box and enter the IP Address in the **Remote IP** field. NETGEAR recommends that you enable this feature if you have enabled the Disk Spin-Down option.

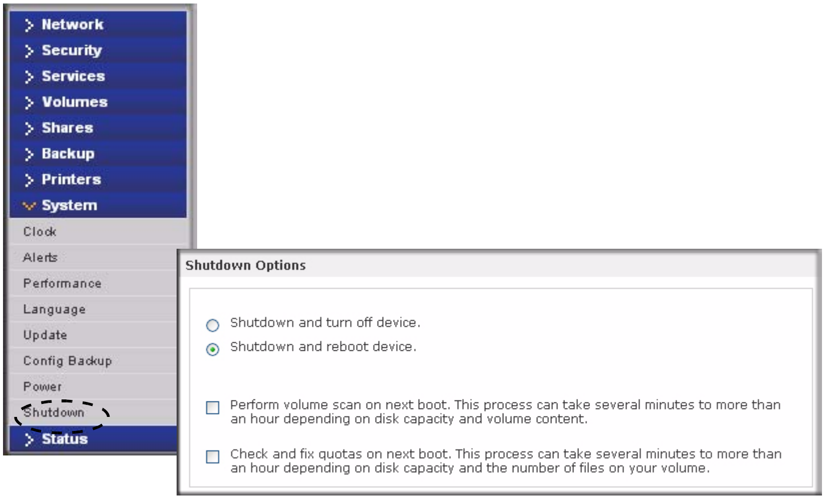
If you use this option, the ReadyNAS is shut down automatically when a battery-low condition is detected on a UPS connected to another ReadyNAS. This is useful when a UPS is shared by multiple ReadyNAS units, even though only one ReadyNAS is monitoring the battery status.

As an option, the ReadyNAS can remotely monitor the UPS when connected to a PC running Network UPS Tools (NUT). For more information about NUT, see *http://www.networkupstools.org.*

Shutdown

The Shutdown Options screen offers the option to either power off or reboot the ReadyNAS device. You also have the option of performing either a full file system check or a quota check on the next boot. Both these options can take several minutes to several hours depending on the size of your volume and the number of files in the volume. You do not need to select these options unless you suspect there might be data or quota integrity problems.

[1] Please refer to the Release Notes for RAIDiator 3 on the NETGEAR Support site for more information.



Shutdown Options

○ Shutdown and turn off device.

● Shutdown and reboot device.

□ Perform volume scan on next boot. This process can take several minutes to more than an hour depending on disk capacity and volume content.

□ Check and fix quotas on next boot. This process can take several minutes to more than an hour depending on disk capacity and the number of files on your volume.

Figure 1-71

When you reboot or shut down the ReadyNAS, you must close the browser window and use RAIDar to reconnect to FrontView.

Chapter 2
Accessing Shares from Your Operating System

This chapter presents examples of how shares on the ReadyNAS device can be accessed by the various operating systems. If you have problems accessing your shares, make sure to enable the corresponding service by selecting Shares > Share Listing screen. Also make sure that the default access of the share is set to Read-only or Read/write.

Windows

To see a share listing in Windows, either click Browse in RAIDar or enter \\<***hostname***> or \\<***ip_address***> in the Explorer address bar. Hostname is the NAS hostname assigned in the Network tab. The default hostname is set to **nas-** followed by the last three hex bytes of the device MAC address.

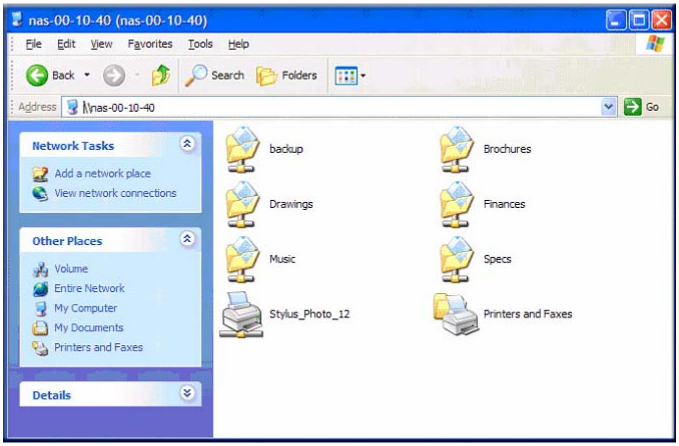


Figure 2-1

To access the share in Windows, specify the hostname followed by the share name in the Explorer address bar, for example: \\<***hostname***>**backup**, as follows:

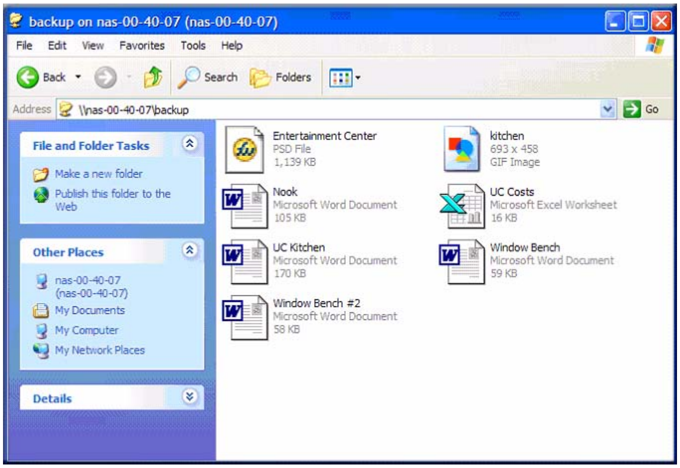


Figure 2-2

MAC OS X

To access the same share over AFP with OS X, select Network from the Finder Go > Network menu.

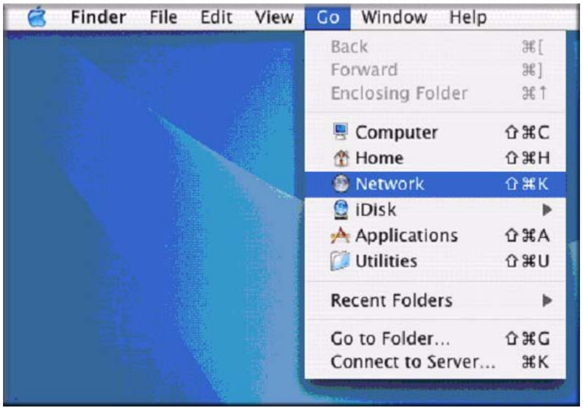


Figure 2-3

From here, there are two ways to access your AFP share, depending on how you have chosen to advertise your AFP share.

AFP over Bonjour

To access the AFP share advertised over Bonjour on Mac OS X, select Network from the Finder Go menu to see a listing of available networks.

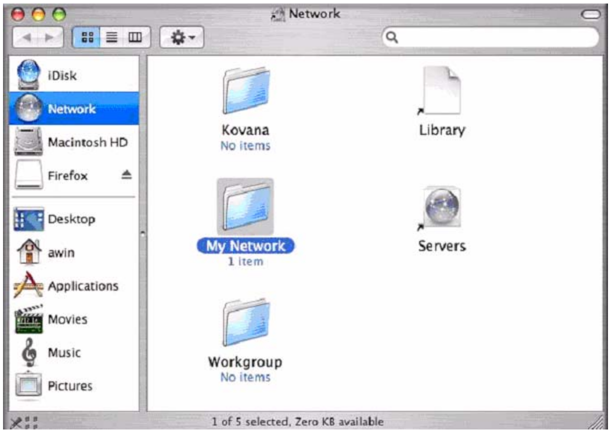
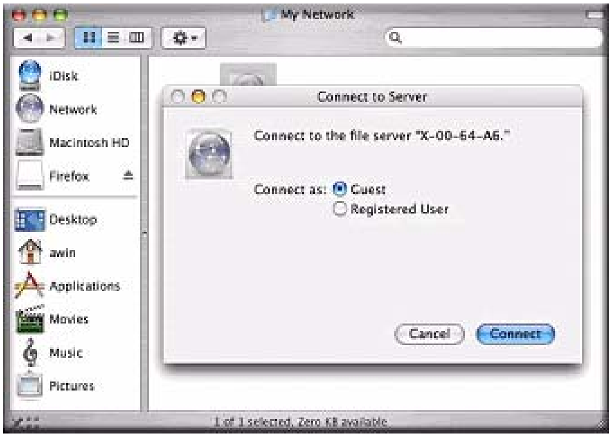


Figure 2-4

Open the My Network folder to display the ReadyNAS hostname.

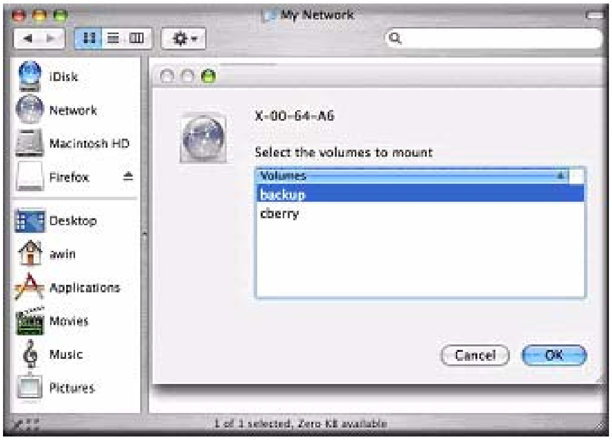


Connect to the file server "X-00-64-A6."

Connect as: ● Guest
○ Registered User

Figure 2-5

In Share security mode, select the **Guest** radio button to access the shares and click **Connect**. In User or Domain security mode, enter the user name and password you wish to use to connect to the ReadyNAS.



X-00-64-A6

Select the volumes to mount

Volumes
backup
cberry

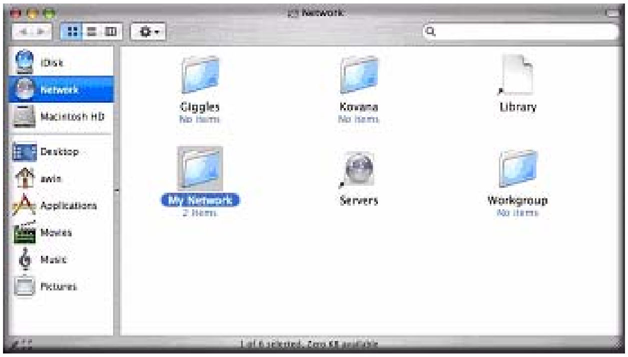
1 of 1 selected, Zero KB available

Figure 2-6

From the Volumes field, select the share you want to access and click **OK.**

AFP over AppleTalk

If you chose to advertise your AFP service over AppleTalk, a listing of available networks is displayed.



1 of 6 selected, Zero KB available

Figure 2-7

Open the My Network folder to display the ReadyNAS hostname. Select the one that has the hostname only. You are prompted with a connection box.

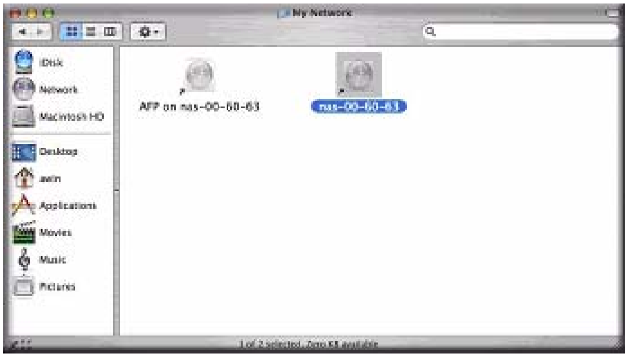
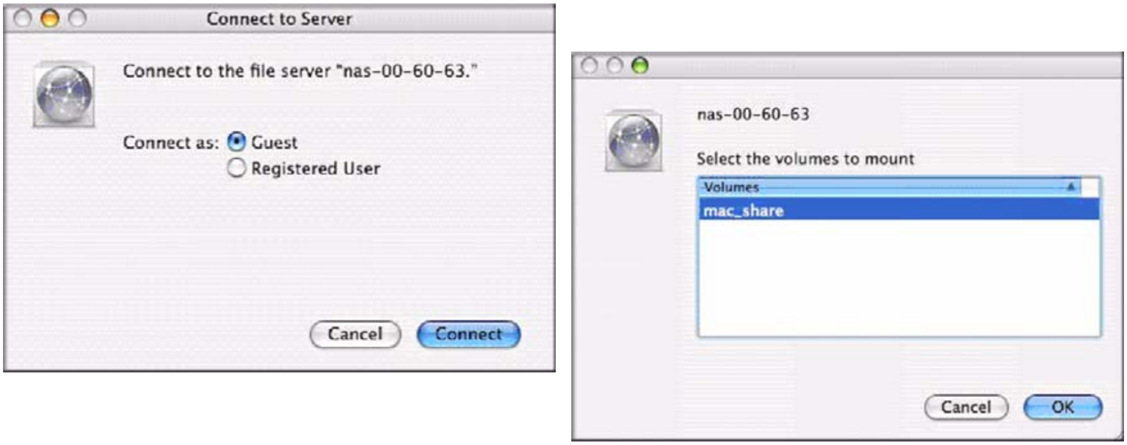


Figure 2-8

Select **Guest** and click **Connect.** Then, select the share you want to connect to and click **OK.**



Connect to the file server "nas-00-60-63."

Connect as: ● Guest
○ Registered User

nas-00-60-63

Select the volumes to mount

mac_share

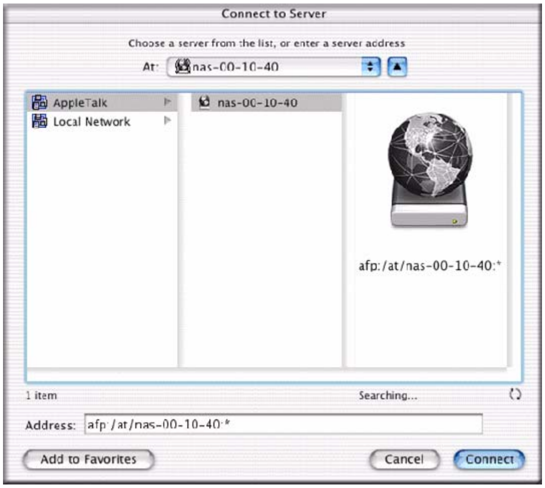
Figure 2-9

In Share security mode, you need to specify only the user name and password—if you have set up a password for your share. If you have not set up a user name, enter the share name in place of the user name. In User or Domain security mode, enter the user name and password you wish to use to connect to the ReadyNAS.

You should see the same file listing as you would in Windows Explorer.

MAC OS 9

To access the same share under Mac OS 9, select Connect to Server from the Finder menu, choose the NAS device entry from the AppleTalk section, and click **Connec**t.



Connect to Server

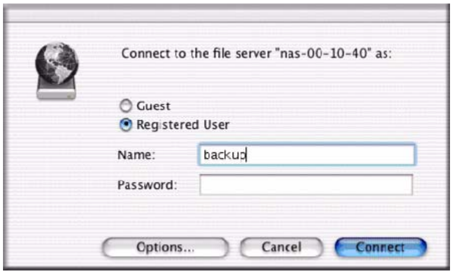
Choose a server from the list, or enter a server address

At: nas-00-10-40

Address: afp:/at/nas-00-10-40:*

Figure 2-10

When you are prompted to log in, enter the **share name** and **password** if the ReadyNAS is configured for Share security mode, otherwise enter a valid **user account** and **password** otherwise, and click **Connect.**



Connect to the file server "nas-00-10-40" as:

○ Guest

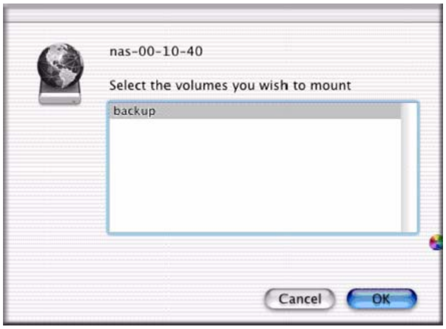
● Registered User

Name: backup

Password:

Figure 2-11

If no share password is set in Share mode, you can select the **Guest** radio button and leave the **password** field blank. If your login is successful, are given a listing of one or more shares. Select the share you wish to connect to and click **OK**.



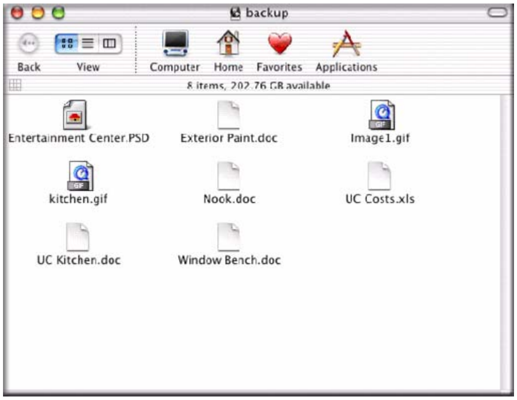
nas-00-10-40

Select the volumes you wish to mount

backup

Figure 2-12

You should see the same files in the share that you do in Windows Explorer.



8 items, 202.76 GB available

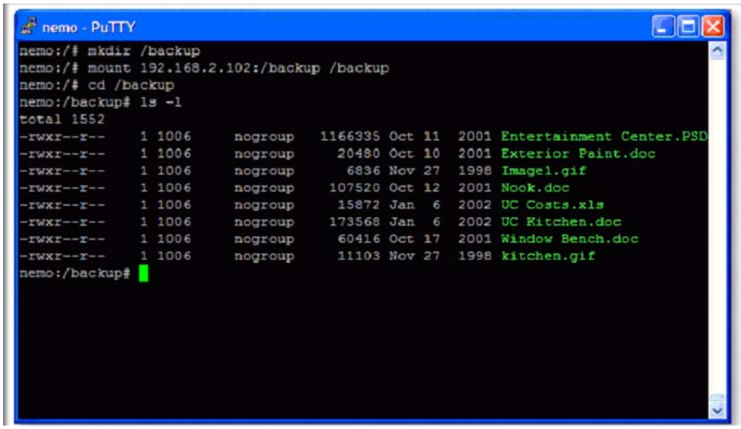
Figure 2-13

Linux/Unix

To access this share from a Linux or Unix client, you will need to mount the share over NFS by entering:

mount <*ipaddr*>:/<*backup /backup*>

where **backup** is the share name. Running the **ls** command in the mounted path displays the share content.



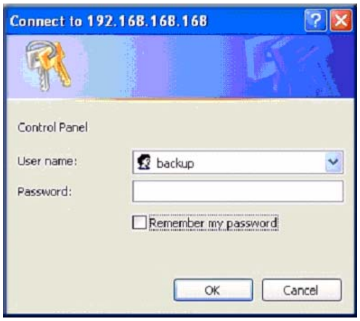
```
nemo:/# mkdir /backup
nemo:/# mount 192.168.2.102:/backup /backup
nemo:/# cd /backup
nemo:/backup# ls -l
total 1552
-rwxr--r--    1 1006     nogroup  1166335 Oct 11  2001 Entertainment Center.PSD
-rwxr--r--    1 1006     nogroup    20480 Oct 10  2001 Exterior Paint.doc
-rwxr--r--    1 1006     nogroup     6836 Nov 27  1998 Image1.gif
-rwxr--r--    1 1006     nogroup   107520 Oct 12  2001 Nook.doc
-rwxr--r--    1 1006     nogroup    15872 Jan  6  2002 UC Costs.xls
-rwxr--r--    1 1006     nogroup   173568 Jan  6  2002 UC Kitchen.doc
-rwxr--r--    1 1006     nogroup    60416 Oct 17  2001 Window Bench.doc
-rwxr--r--    1 1006     nogroup    11103 Nov 27  1998 kitchen.gif
nemo:/backup#
```

Figure 2-14

➡	**Note:** The ReadyNAS does not support NIS as it is unable to correlate NIS information with CIFS logins. In mixed environments where you want CIFS and NFS integration, you can set the security to User mode and manually specify the UID and GID of the user and group accounts to match your NIS or other Linux/Unix server settings. The ReadyNAS can import a comma-delimited file containing the user and group information to coordinate Linux/Unix login settings (see "Managing Users" on page 1-15 for more information).

Web Browser

To access the same share using a Web browser, enter **http://<*ipaddr*>** in the browser address bar. You can use **https** if you want a secure encrypted connection. You will be prompted to log in.



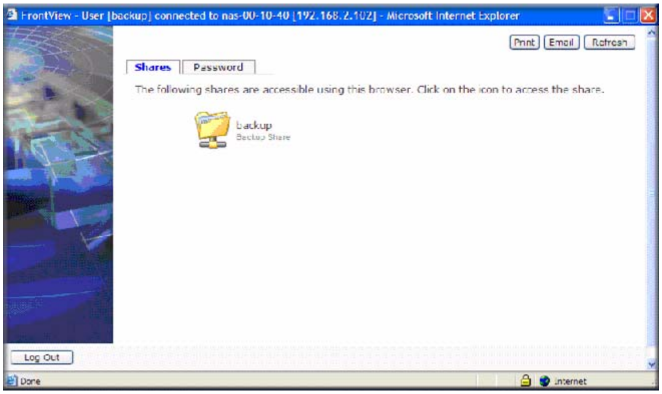
User name: backup

Password:

□ Remember my password

Figure 2-15

If the ReadyNAS is in Share security mode, enter the share name and share password. Otherwise, log in with a valid user name and password if the ReadyNAS is in User or Domain mode.



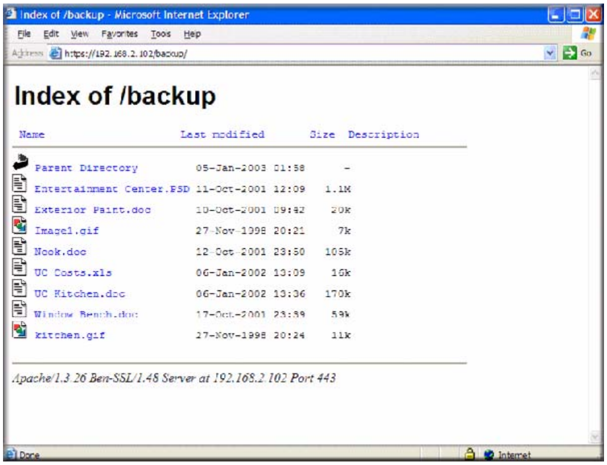
FrontView - User [backup] connected to nas-00-10-40 [192.168.2.102] - Microsoft Internet Explorer

The following shares are accessible using this browser. Click on the icon to access the share.

backup
Backup Share

Figure 2-16

If the Share access is read-only, only the file manager displays.



Index of /backup - Microsoft Internet Explorer

Address https://192.168.2.102/backup/

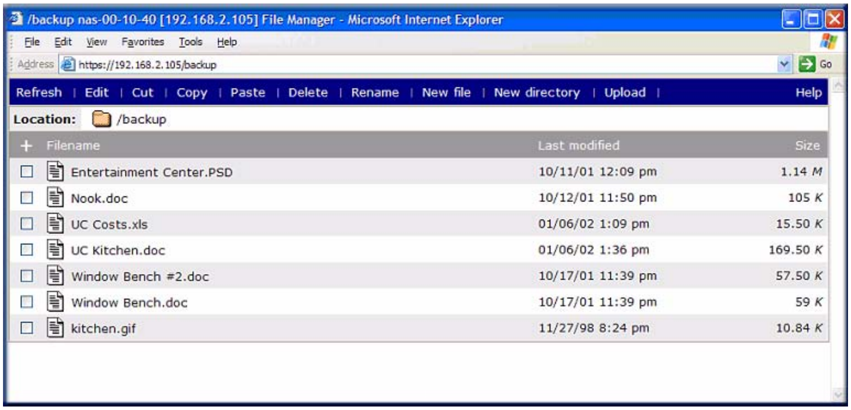
Index of /backup

```
Name                          Last modified      Size  Description
Parent Directory              05-Jan-2003 01:58     -
Entertainment Center.PSD      11-Oct-2001 12:09   1.1M
Exterior Paint.doc            10-Oct-2001 09:42    20k
Image1.gif                    27-Nov-1998 20:21     7k
Nook.doc                      12-Oct-2001 23:50   105k
UC Costs.xls                  06-Jan-2002 13:09    16k
UC Kitchen.doc                06-Jan-2002 13:36   170k
Window Bench.doc              17-Oct-2001 23:39    59k
kitchen.gif                   27-Nov-1998 20:24    11k
```

Apache/1.3.26 Ben-SSL/1.48 Server at 192.168.2.102 Port 443

Figure 2-17

If the Share is also writable, the file manager displays options for creating, modifying, and deleting files, as follows.


/backup nas-00-10-40 [192.168.2.105] File Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
Refresh | Edit | Cut | Copy | Paste | Delete | Rename | New file | New directory | Upload |
Help

https://192.168.2.105/backup

Location: /backup

	Filename	Last modified	Size
□	Entertainment Center.PSD	10/11/01 12:09 pm	1.14 *M*
□	Nook.doc	10/12/01 11:50 pm	105 *K*
□	UC Costs.xls	01/06/02 1:09 pm	15.50 *K*
□	UC Kitchen.doc	01/06/02 1:36 pm	169.50 *K*
□	Window Bench #2.doc	10/17/01 11:39 pm	57.50 *K*
□	Window Bench.doc	10/17/01 11:39 pm	59 *K*
□	kitchen.gif	11/27/98 8:24 pm	10.84 *K*

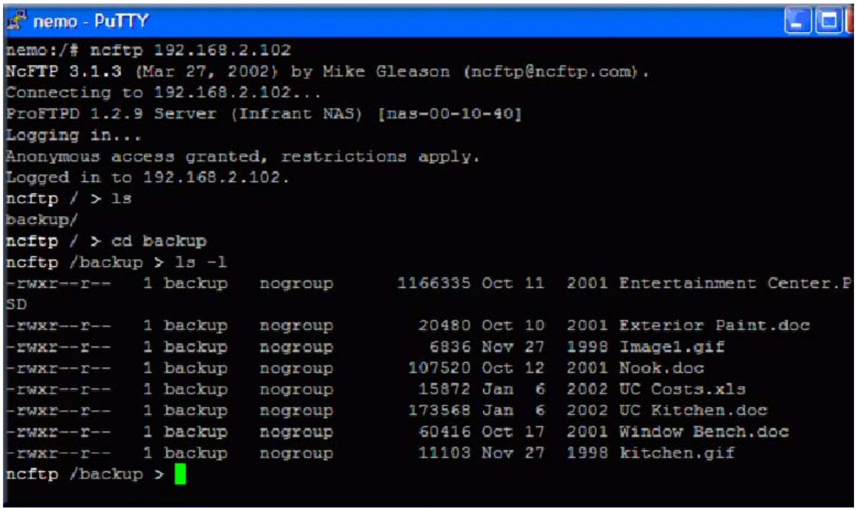
Figure 2-18

One useful application for a Web share is to set up an internal company website. You can copy HTML files to the Web share using Windows, Mac, NFS, or HTTP. When you set HTTP access to read-only, html files, including *index.htm* and *index.html*, can be viewed using any web browser.

➡	**Note:** Files created under the Web file manager can be deleted only under this file manager. The only exception is for the admin user; the admin user can change or delete any files created through the web. Files not created from this file manager can be modified within the file manager but cannot be deleted here.

FTP/FTPS

To access the share via FTP in Share security mode, log in as “anonymous” and use your e-mail address for the password.



```
nemo:/# ncftp 192.168.2.102
NcFTP 3.1.3 (Mar 27, 2002) by Mike Gleason (ncftp@ncftp.com).
Connecting to 192.168.2.102...
ProFTPD 1.2.9 Server (Infrant NAS) [nas-00-10-40]
Logging in...
Anonymous access granted, restrictions apply.
Logged in to 192.168.2.102.
ncftp / > ls
backup/
ncftp / > cd backup
ncftp /backup > ls -l
-rwxr--r--    1 backup   nogroup      1166335 Oct 11  2001 Entertainment Center.P
SD
-rwxr--r--    1 backup   nogroup        20480 Oct 10  2001 Exterior Paint.doc
-rwxr--r--    1 backup   nogroup         6836 Nov 27  1998 Image1.gif
-rwxr--r--    1 backup   nogroup       107520 Oct 12  2001 Nook.doc
-rwxr--r--    1 backup   nogroup        15872 Jan  6  2002 UC Costs.xls
-rwxr--r--    1 backup   nogroup       173568 Jan  6  2002 UC Kitchen.doc
-rwxr--r--    1 backup   nogroup        60416 Oct 17  2001 Window Bench.doc
-rwxr--r--    1 backup   nogroup        11103 Nov 27  1998 kitchen.gif
ncftp /backup > 
```

Figure 2-19

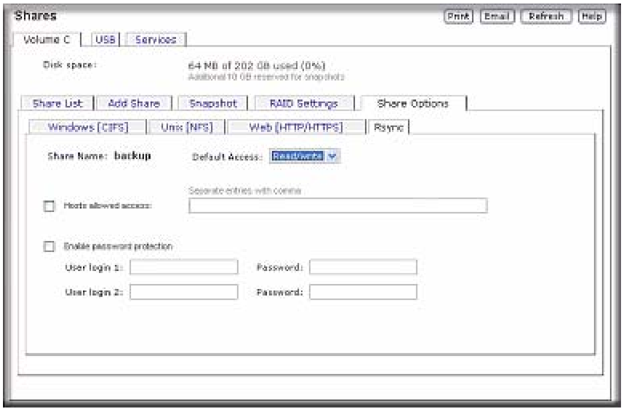
➡	**Note:** Enabling FTP access in Share mode opens up the share to anyone on your network who has an FTP client. NETGEAR recommends that you enable FTP access only to shares you are comfortable making public on your network.

⚠	**Warning:** Disk usage using FTP in Share mode ***does not*** count towards the share disk quota, so carefully choose how you advertise an FTP share.

To access the share in User or Domain security mode, use the appropriate user login and password used to access the ReadyNAS. For better security, use an FTPS (FTP-SSL) client to connect to the ReadyNAS FTP service. With FTPS, both the password and data are encrypted.

Rsync

Access to the share through rsync is identical regardless of the security mode. If you specified a user or password in the rsync share access tab, you will need to specify this when accessing the rsync share. Unlike other protocols, rsync uses arbitrary user name and password that is specific only for rsync access. The user account you specify does not need to exist on the ReadyNAS or a domain controller.



Disk space: 64 MB of 202 GB used (0%)
Additional 10 GB reserved for snapshots

Share Name: backup
Default Access: Read/write

Separate entries with comma
□ Hosts allowed access:

□ Enable password protection
User login 1: Password:
User login 2: Password:

Figure 2-20

Here is an example of a way for a Linux client to list the content of a ReadyNAS rsync share with no user name and password defined:

# rsync <*ipaddr*>::backup

To recursively copy the content of a share to /tmp:

# rsync -a <*ipaddr*>::backup /tmp

To do the same except with a login **user** and password **hello**, enter:

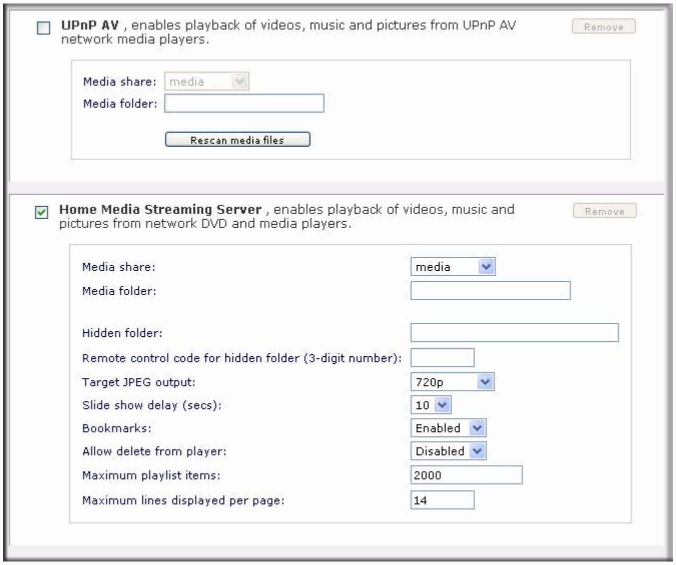
# rsync -a user@<*ipaddr*>::backup /tmp
Password: *****

Note: The ReadyNAS does not support Rsync over SSH.

Networked DVD Players and UPnP AV Media Adapters

Networked DVD players and UPnP AV Media adapters detect the ReadyNAS if either the Home Media Streaming Server or the UPnP AV services are enabled. The content of the Streaming Services media share on the ReadyNAS is available to these players for playback.[1] Multiple players can be connected to the ReadyNAS and can play the media files concurrently.

Make sure that you enable the appropriate service in the Services tab before invoking the service.



☐ **UPnP AV** , enables playback of videos, music and pictures from UPnP AV network media players.

Media share: media

Media folder:

☑ **Home Media Streaming Server** , enables playback of videos, music and pictures from network DVD and media players.

Media share: media

Media folder:

Hidden folder:

Remote control code for hidden folder (3-digit number):

Target JPEG output: 720p

Slide show delay (secs): 10

Bookmarks: Enabled

Allow delete from player: Disabled

Maximum playlist items: 2000

Maximum lines displayed per page: 14

Figure 2-21

Consult the Device Compatibility list for information about which DVD players and media adapters work with the ReadyNAS.

[1] Consult the player manual for information on the file formats that it supports.

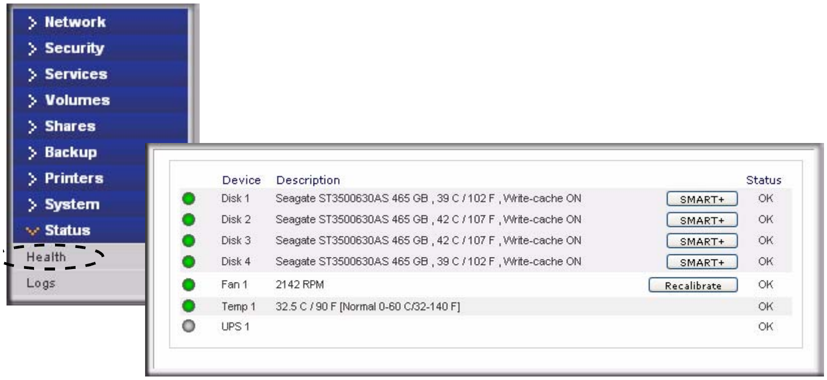
Chapter 3
Maintenance and Administration

Viewing System Status

The Status menu contains links to the Health screen and Logs screen that provide system status information.

Health

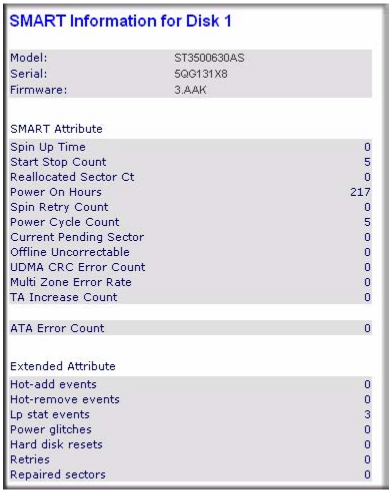
The Health screen displays the status of each disk, and the fan, temperature, and UPS status in detail. When available, normal expected values are provided.



	Device	Description		Status
●	Disk 1	Seagate ST3500630AS 465 GB , 39 C / 102 F , Write-cache ON	SMART+	OK
●	Disk 2	Seagate ST3500630AS 465 GB , 42 C / 107 F , Write-cache ON	SMART+	OK
●	Disk 3	Seagate ST3500630AS 465 GB , 42 C / 107 F , Write-cache ON	SMART+	OK
●	Disk 4	Seagate ST3500630AS 465 GB , 39 C / 102 F , Write-cache ON	SMART+	OK
●	Fan 1	2142 RPM	Recalibrate	OK
●	Temp 1	32.5 C / 90 F [Normal 0-60 C/32-140 F]		OK
○	UPS 1			OK

Figure 3-1

For each disk, you can click **SMART+** (Self-Monitoring, Analysis and Reporting Technology) to display the content of the internal disk log.



SMART Information for Disk 1

Model:	ST3500630AS
Serial:	5QG131X8
Firmware:	3.AAK

SMART Attribute	
Spin Up Time	0
Start Stop Count	5
Reallocated Sector Ct	0
Power On Hours	217
Spin Retry Count	0
Power Cycle Count	5
Current Pending Sector	0
Offline Uncorrectable	0
UDMA CRC Error Count	0
Multi Zone Error Rate	0
TA Increase Count	0
ATA Error Count	0

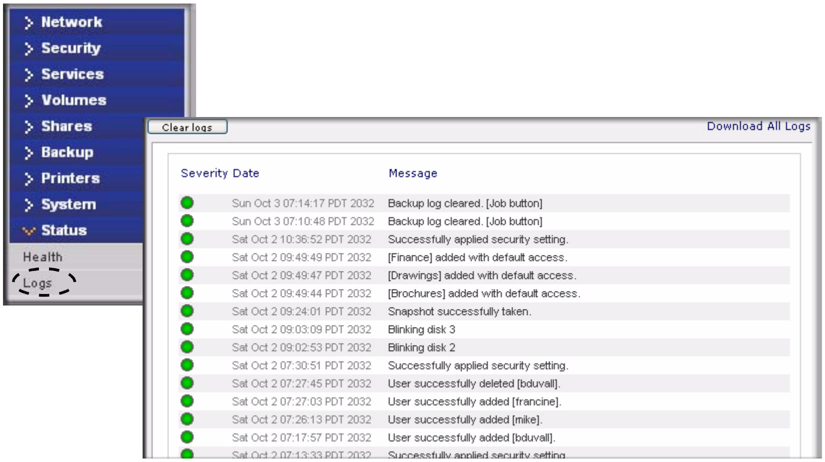
Extended Attribute	
Hot-add events	0
Hot-remove events	0
Lp stat events	3
Power glitches	0
Hard disk resets	0
Retries	0
Repaired sectors	0

Figure 3-2

To recalibrate the fan, click **Recalibrate.**

Logs

Select Status > Logs to access the Clear Logs screen. The Clear Logs screen provides information about the status of management tasks, including a timestamp.



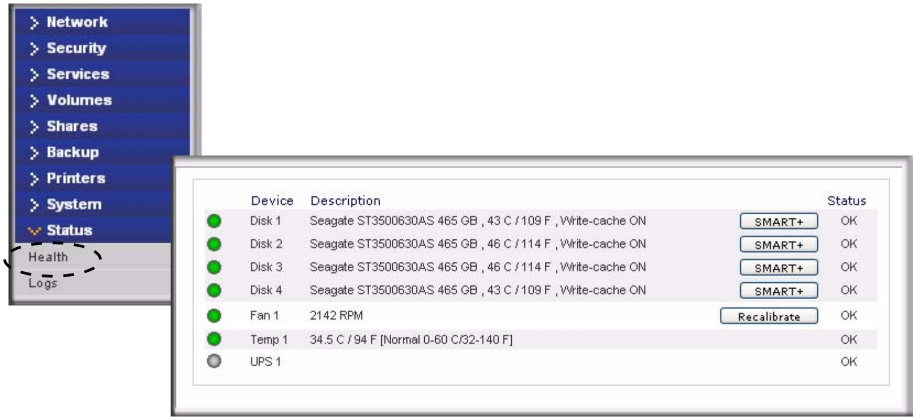
Severity	Date	Message
●	Sun Oct 3 07:14:17 PDT 2032	Backup log cleared. [Job button]
●	Sun Oct 3 07:10:48 PDT 2032	Backup log cleared. [Job button]
●	Sat Oct 2 10:36:52 PDT 2032	Successfully applied security setting.
●	Sat Oct 2 09:49:49 PDT 2032	[Finance] added with default access.
●	Sat Oct 2 09:49:47 PDT 2032	[Drawings] added with default access.
●	Sat Oct 2 09:49:44 PDT 2032	[Brochures] added with default access.
●	Sat Oct 2 09:24:01 PDT 2032	Snapshot successfully taken.
●	Sat Oct 2 09:03:09 PDT 2032	Blinking disk 3
●	Sat Oct 2 09:02:53 PDT 2032	Blinking disk 2
●	Sat Oct 2 07:30:51 PDT 2032	Successfully applied security setting.
●	Sat Oct 2 07:27:45 PDT 2032	User successfully deleted [bduvall].
●	Sat Oct 2 07:27:03 PDT 2032	User successfully added [francine].
●	Sat Oct 2 07:26:13 PDT 2032	User successfully added [mike].
●	Sat Oct 2 07:17:57 PDT 2032	User successfully added [bduvall].
●	Sat Oct 2 07:13:33 PDT 2032	Successfully applied security setting

Figure 3-3

The **Download All Logs** link is available in case you need to analyze low-level log information. If you click this link, a zip of all the logs is provided.

Replacing a Failed Disk

When a disk fails in your ReadyNAS device, you are notified of the failure by e-mail. The failed disk location can be seen in the FrontView status bar at the bottom by selecting Status > Health.



	Device	Description		Status
●	Disk 1	Seagate ST3500630AS 465 GB , 43 C / 109 F , Write-cache ON	SMART+	OK
●	Disk 2	Seagate ST3500630AS 465 GB , 46 C / 114 F , Write-cache ON	SMART+	OK
●	Disk 3	Seagate ST3500630AS 465 GB , 46 C / 114 F , Write-cache ON	SMART+	OK
●	Disk 4	Seagate ST3500630AS 465 GB , 43 C / 109 F , Write-cache ON	SMART+	OK
●	Fan 1	2142 RPM	Recalibrate	OK
●	Temp 1	34.5 C / 94 F [Normal 0-60 C/32-140 F]		OK
○	UPS 1			OK

Figure 3-4

On the front of the ReadyNAS device, a failed disk is identified by an amber LED. The left most LED is disk channel 1; the next one is disk channel 2; and so on. Take note of the failed channel.

Ordering a Replacement Disk

On the main menu, select Status > Health. Take note of the disk vendor and model utilized on your ReadyNAS system. It is best to replace a failed disk with the same disk model. Contact the disk vendor, and arrange to have the disk replaced if the disk is still under warranty. A disk RMA from the vendor requires that you provide the serial number of the disk. To locate the serial number, open the case and take out the failed disk (see the following sections for replacement instructions for your disk model).

If the disk is no longer under warranty, you can obtain a disk of the same capacity or larger from your ReadyNAS retailer.

Replacing a Failed Disk on the ReadyNAS NV+

When a Disk Status LED blinks slowly, it is an indication of a failed disk. ReadyNAS NV+ supports hotswap bays, so there is no need to power down the device.

To replace the disk:

1. Open the disk tray door.
2. Press the button under the failed disk. The latch pops out.

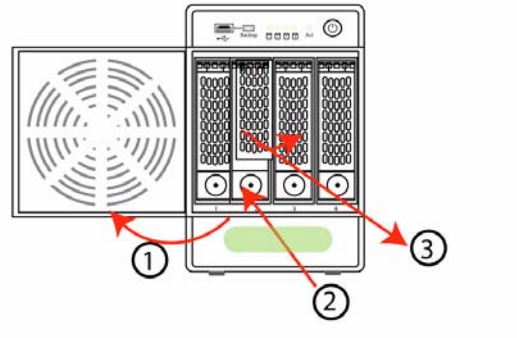


Figure 3-5

3. Pull out the disk tray and remove the screws.
4. Replace the failed disk, reassemble, and slide the disk tray back in. Make sure that the hard disk connectors are facing away from you when you reassemble the disk.

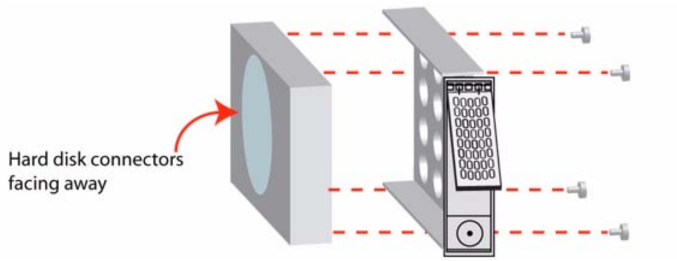


Figure 3-6

The ReadyNAS system performs RAID synchronization in the background, and notifies you by e-mail when synchronization is complete.

Replacing the Failed Disk on the ReadyNAS 1100

The Disk Status LED corresponding to the failed disk blinks slowly. The ReadyNAS1100 supports hotswap disk trays; you do not need to power down the device.

To replace a failed disk:

1. Press disk tray button; the latch pops out.
2. Pull out the disk tray.

3. Replace the failed disk by placing the disk in the disk tray and sliding the disk tray back into the device.

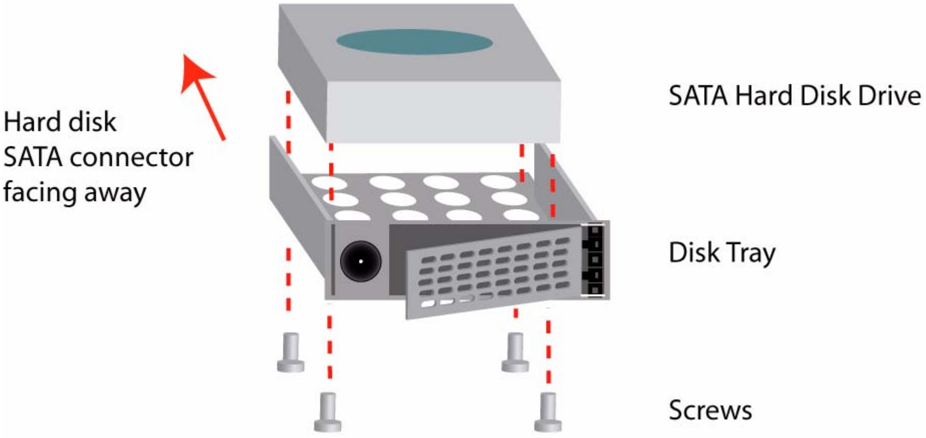


Figure 3-7

Replacing the Failed Disk on the ReadyNAS 600/X6

On the ReadyNAS 600/X6 system, shut down the ReadyNAS and open up the enclosure as instructed in the *Installation Guide*. If you view the disks from the front of the enclosure, the left-most disk is channel 1; the next disk is channel 2; and so on.

On the ReadyNAS 600/X6, Rev A, system, remove the drive cage and disconnect the power and SATA cable from the failed disk. Insert the new replacement disk, reconnect the cables, insert the drive cage, and secure the enclosure.

⚠	**Warning:** When replacing the cables, make sure that the connectors fit square-on and securely. After the drive cage is re-inserted, double-check the connectors to make sure that they have not come loose. Loose connections can cause spurious drive failure events that can render the data volume inoperable.

On the ReadyNAS 600/X6, Rev B, system, you can replace the failed disk in power-off mode by removing the disk from the top and sliding the new disk into place.

On ReadyNAS systems with hot-swap drive bays, you do not need to power off the ReadyNAS to replace a failed disk. You can replace the disk while the system is on. After removing the failed disk, wait at least 10 seconds until the disk LED blinks, and then insert the new disk.

Resynchronizing the Volume

If you had to power off to replace the failed disk, turn on the power on the ReadyNAS.

The RAID volume automatically resynchronizes with the new disk in the background. The process takes several hours depending on disk size. During the resync process, the ReadyNAS can be used as normal, although access will be slower until the volume is finished resynchronizing.

You will be notified by e-mail when the resync process is complete.

Resetting Your System (System Switch)

Refer to the *Installation Guide* included in the shipping box (a PDF of the *Installation Guide* is also on your *Installation CD*) for the location of the System Reset switch on the back of the ReadyNAS.

The System Reset switch allows you to perform three functions:

1. Reinstall the ReadyNAS firmware.
2. Reset the ReadyNAS back to the factory default settings.
3. Change between X-RAID and Flex-RAID mode.

Typically, you should not need to resort to options (1) and (2) unless you exhausted all other means of recovering your system. You might want to reinstall the ReadyNAS firmware as a first step, if the ReadyNAS had been working normally but a configuration change makes it inaccessible. If this does not work or you wish to set the ReadyNAS back to a factory default state, you can do so following these instructions below:

- **To re-install the ReadyNAS firmware:** Use a paper clip to depress the switch while the system is off. Continue to depress the reset switch while powering on the system for approximately 5 seconds until the disk LEDs flash ***once*** to signify that the command has been accepted. The firmware installation takes several minutes to complete. The Status LED in the front will be solid green when the process is complete. The installation does not affect the data on the ReadyNAS.

⚠	**Warning:** Make sure that you do not continue to press the reset switch after the LEDS flash once, otherwise a Factory Default will occur that erases your data. (see below)

- **To set the ReadyNAS device to Factory Default**: Use the same process, except you must hold the System Reset switch for 30 seconds after powering on the system. You will see the disk LEDs flash for a ***second*** time to signify that the command has been accepted.

> ⚠ **Warning:** This process reinstalls the firmware and resets all disk configurations, ***wiping out any data*** you might have on the NAS.

- **To change between X-RAID and Flex-RAID mode**: Perform a Factory Default using the method described in the previous bullet. Changing RAID modes does not preserve your data, so make sure to perform a backup before doing this. During the boot process after a Factory Default, there is a 10-minute window during which you can use RAIDar to select the volume setup you want. RAIDar will display your ReadyNAS with **Setup** in the Info column. (It might take a couple of minutes for RAIDar to display this.)Then, click **Setup** to display the Volume Setup screen.

Configuring RAID on the ReadyNAS 1100 and NV+

Your ReadyNAS comes in one of three configurations:

- Diskless system with X-RAID (expandable volume).
- System with pre-installed disks in X-RAID (expandable volume).
- System with pre-installed disks in RAID 0/1/5 (flexible volume).

The following figure illustrates the default configuration with redundancy in your ReadyNAS NV+.

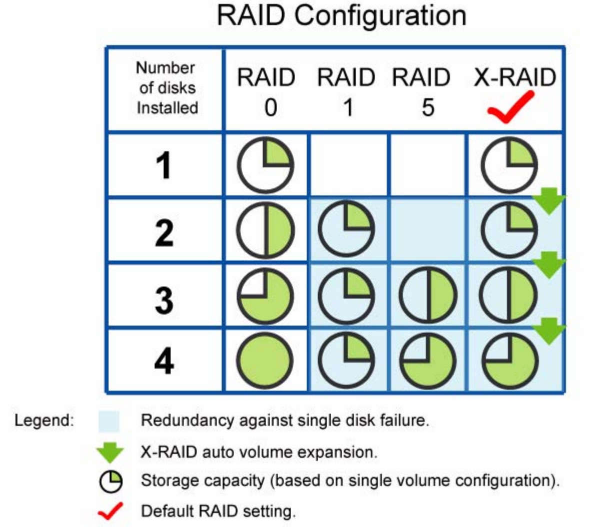

RAID Configuration
Number of disks Installed
RAID 0
RAID 1
RAID 5
X-RAID
1
2
3
4
Legend:
Redundancy against single disk failure.
X-RAID auto volume expansion.
Storage capacity (based on single volume configuration).
Default RAID setting.

Figure 3-8

You can switch between the X-RAID Expandable Volume mode and the RAID 0/1/5 Flexible Volume mode only if you want to change the default configuration. It is not necessary to perform this procedure every time you boot up the system. The device remains in the selected mode until explicitly changed.

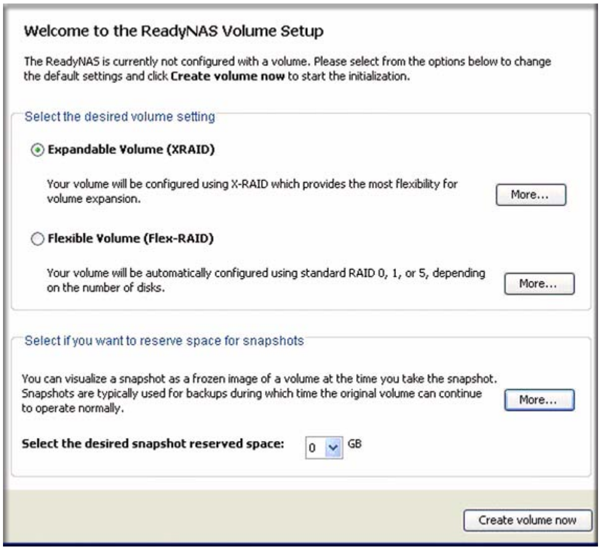
⚠	**Warning:** Performing a Factory Default will erase all your data on the hard disks.

To reconfigure your RAID setup:

1. Power off the device.
2. Use a paper clip or push pin to press the System Reset switch. Press the System Reset switch for 30 seconds while powering on the device.

   The four LEDs will flash for approximately 30 seconds.
3. When the LEDS are on, but not flashing, release the reset switch.

4. Open RAIDar. RAIDar will prompt you to click **Setup.** The ReadyNAS Volume Setup screen displays.



Welcome to the ReadyNAS Volume Setup

The ReadyNAS is currently not configured with a volume. Please select from the options below to change the default settings and click **Create volume now** to start the initialization.

Select the desired volume setting

● **Expandable Volume (XRAID)**

Your volume will be configured using X-RAID which provides the most flexibility for volume expansion.

○ **Flexible Volume (Flex-RAID)**

Your volume will be automatically configured using standard RAID 0, 1, or 5, depending on the number of disks.

Select if you want to reserve space for snapshots

You can visualize a snapshot as a frozen image of a volume at the time you take the snapshot. Snapshots are typically used for backups during which time the original volume can continue to operate normally.

Select the desired snapshot reserved space: 0 GB

Figure 3-9

5. Select either the **Expandable Volume (X-RAID)** or the **Volume (RAID 0,1,5)** radio button and click **Create Volume Now.** The volume and initialization process begins.

⚠	**Warning:** If no action is taken within 10 minutes, the system defaults to X-RAID with 5GB reserved for snapshots.

⚠	**Warning:** Before beginning any of these activities, make sure to back up all important data.

Backing Up the ReadyNAS to a USB Drive

The following sections describe how to back up and remove disks from the ReadyNAS systems.

ReadyNAS1100 Backup

On the ReadyNAS1100, the Backup button is associated with the USB Port at the front of the system. By default, the Backup button copies the data from the Backup share onto the USB disk connected to the USB port at the front of the device (as shown in the following figure).

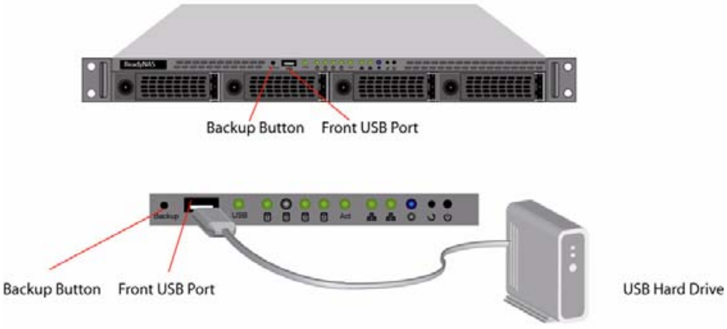


Figure 3-10

ReadyNAS NV+ Backup

On the ReadyNAS NV+, the Backup button is associated with the USB port at the front of the system. By default, the Backup button copies the data from the Backup share onto the USB disk connected to the USB port at the front of the device (as shown in the following figure).

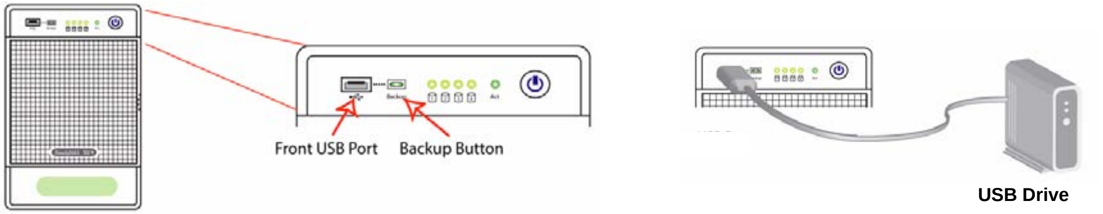


Figure 3-11

You can easily program backups in the FrontView Backup menu to back up one or more predefined backup jobs.

⚠	**Warning:** Make sure that you have a USB hard drive attached to the front USB Port ***before*** pressing the Backup button.

Removing the System Module from the ReadyNAS 1100

To access the system module and remove it from the ReadyNAS1100:

1. Power off the unit and remove the screws.
2. Lift up the latch.
3. Pull the system module forward; it slides out easily.

The illustration on the right shows the ReadyNAS1100 with the system module removed.

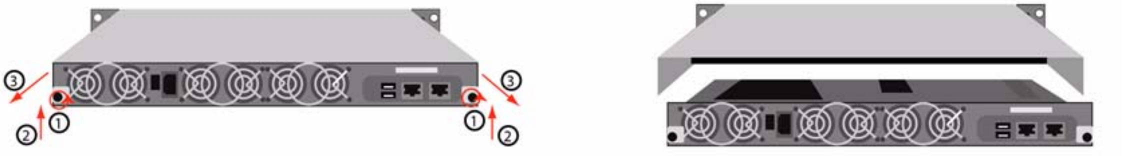
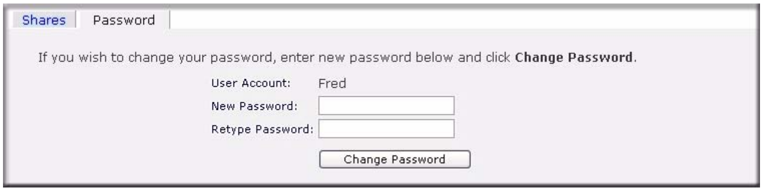


Figure 3-12

Changing User Passwords

There are two ways in which user passwords can be changed in the User security mode. The first way is for the administrator to change the passwords by selecting Security > User & Group Accounts and then selecting **Manage Users** from the pull-down menu. The other and preferred way is to allow users to change their own passwords. This relieves the administrator from this task and encourages users to change their passwords on a more regular basis for enhanced security.

Users can use the Web browser and their existing password to log in to **https://<*ip_addr*>/** to access the Web share listing page. Then select the Password tab, and follow the prompts to set a new password



If you wish to change your password, enter new password below and click **Change Password**.

User Account: Fred

New Password:

Retype Password:

Figure 3-13

In Share and Domain security mode, the Password tab does not appear.

⇨	**Note:** User passwords in Domain mode must be set on the domain or ADS server.

Appendix A
RAID Levels Simplified

RAID can be somewhat daunting; this appendix helps to simplify RAID.

RAID is an acronym for Redundant Array of Independent Disks. Basically, if properly configured, it can store data on multiple disks in a way that if one disk fails, the data can still be accessed from one or more remaining disks. A RAID level selects how data is kept redundant, the most popular ones being levels 0, 1, and 5. Contrary to the RAID acronym, RAID level 0 does not provide any redundancy.

RAID Level 0

RAID level 0 provides the best write performance of all the RAID levels as it stripes data across all disks so that data can be written to all disks in parallel. Unfortunately, it is not redundant, so if one disk fails, the entire volume fails. RAID level 0 can be configured with one or more disks, and its capacity is the size of the smallest disk in the RAID set multiplied by the number of disks in the set. For example, a four-disk RAID 0 yields the capacity of all four disks, assuming they are identical in size.

RAID Level 1

RAID level 1 consists of two or more disks, all disks other than the first being an exact mirror of the first. RAID level 1 can sustain disk failure up to the total number of disks in the RAID set minus one. For example, a two-disk RAID 1 volume can sustain a one-disk failure and continue running. A three-disk RAID 1 volume can sustain up to two disk failures. If a disk fails, the data is retrieved from the surviving disk. Unfortunately, RAID 1 capacity utilization is not optimal in a configuration of three or more disks. The capacity is limited to the size of the smallest disk in the RAID set.

RAID Level 5

RAID level 5 provides the best balance of capacity and performance while providing data redundancy. RAID 5 provides redundancy by striping data across three or more disks and keeping the parity information on one of the disks in each stripe. In case of disk failure, the surviving disks and the parity disk are used to reconstruct the lost data, providing data transparently to the user application. When the failed disk has been replaced with a good disk, the reconstructed data is written out to the new disk; when the reconstruction (or sometimes referred as RESYNC) process is complete, the volume returns to a redundant state. The capacity of a RAID 5 volume is the smallest disk in the RAID set multiplied by one less than the number of disks in the RAID set. For example, a four-disk RAID 5 set provides the capacity of three disks, assuming all four disks are identical in size.

RAID Level X (X-RAID)

RAID level X, or **X-RAID**, is similar to RAID level 5, as it is optimized for large sequential access for the best possible media streaming performance. The X also refers to its natural volume eXpandability. In X-RAID mode, with one disk, the volume is non-redundant and has the capacity of the single disk. By adding a second disk, the capacity remains the same, but the data is now mirrored between the two disks. With redundancy, your data is not lost if a disk fails. Adding a third disk doubles the capacity while maintaining redundancy. Adding a fourth disk triples the capacity with redundancy. The process of volume expansion is automatic. When a disk has been added, you are notified of the steps being taken, and you are notified when you need to reboot to continue with the expansion process.

Appendix B
Input Field Format

Domain or Workgroup Name

A valid domain or workgroup name must conform to the following restrictions:

- Name must consist only of characters a–z, A–Z, 0–9, and the symbols _ (underscore), - (hyphen), and . (period).
- Name must start with a letter.
- Name length must be 15 characters or less.

Host

A valid IP address or a host name.

Host Name

A valid host name must conform to the following restrictions:

- Name must consist only of characters a–z, A–Z, 0–9, and the symbols - (hyphen) and . (period).
- Name must start with a letter.
- A short host name length must be 15 characters or less.
- A fully-qualified domain name (FQDN) must have no more than 63 characters in each section separated by . (period), and cannot end with a - (hyphen). Example of a valid FQDN: firstpart.secondpart.thirdpart.com.

ReadyNAS Host Name

A valid host name except the first part or short host name must be 15 characters or less due to the NetBIOS name length restriction.

Host Expression

A valid host expression is either a valid host or the common IP expression form specifying a range of addresses in a network, for example:

- 192.168.2.
- 192.168.2.0/255.255.255.0
- 192.168.2.0/24

Share Name

- Name must consist only of characters a–z, A–Z, 0–9, and the symbols - (hyphen) and . (period).
- Name cannot be an existing user name.
- Name cannot end in **-snap**.
- Name cannot be any one of the following reserved names:

  ```
  bin boot cdrom dev etc floppy frontview home initrd lib lost+found mnt
  opt proc root sbin tmp usr var admin administrator images language
  quota.user quota.group shares global homes printers diag c d e f g h i
  j
  ```
- Share name can contain Unicode characters if this option is specified in the Language tab.

Share Password

- The password can be any character except for ' (single quote).
- Share passwords are limited to 8 characters.

SNMP Community

- Name must only consist of characters a–z, A–Z, 0–9, and the symbols _ (underscore), - (hyphen) and . (period).
- Name must start with a letter.
- Name length must be 32 characters or less.

User or Group Name

- Name must only consist of characters a–z, A–Z, 0–9, and the symbols _ (underscore), - (hyphen), @, and . (period).
- Name cannot be an existing share name.
- Name can contain Unicode characters if this option is specified in the Language tab.

User Password

- The password can be any character except for ' (single quote).

Appendix C
Glossary

AFP AppleTalk Filing Protocol\ is the standard way Mac OS 9 and earlier versions share files across the network.

CIFS Common Internet File System, a standard protocol that Windows users use to share files across the network. Mac OS X also has the capability to share files using CIFS.

FTP File Transfer Protocol, a common protocol adopted by many OS to enable remote file download and upload for public sharing.

HTTP Hypertext Transfer Protocol, the protocol Web browsers use to connect to Web servers for file access, typically Web pages.

HTTPS HTTP with SSL encryption is used where secure Web access is desired.

NFS Network File System, a common way Unix and Linux systems share files by making remote file systems appear to reside locally.

Quota Amount of volume space allocated to a particular user or group account, or to a particular share. The user, group, or share with a set quota cannot exceed disk usage beyond this limit. Quota is typically specified to ensure that no one user, group, or share abuses the available storage space.

RAID Redundant Array of Independent Disks. Basically it is a method of storing data on multiple disks in a way that if one disk fails, data can still be accessed from the other disks. A RAID level selects how data will be kept redundant, the most popular of which are levels 0, 1, and 5. Contrary to the RAID acronym, RAID level 0 does not provide any redundancy. For more information, see Appendix A, “RAID Levels Simplified.”.

Share A folder on a NAS volume that can be shared among different network file services such as CIFS for Windows, AFP (AppleTalk File Protocol) for Macs, NFS for Unix/ Linux, FTP, and HTTP. Access to the share can be customized on a user or group or host-level basis.

Snapshot An instantaneous, non-changing, read-only image of a volume. Snapshots are useful for backups.While a snapshot is being taken, the original volume can continue to operate normally. Snapshots can also be utilized as a temporary backup in case of viruses. Files can be restored from the snapshot volume if current files are corrupted.

Volume A file system built on top of a RAID set. This file system consists of shares that are made available through various network file services.

X-RAID NETGEAR patent-pending Expandable RAID technology.

Index