ReadyNAS 2100 User Manual

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134 USA

202-10504-01
v1.1
June 2009

© 2009 by NETGEAR, Inc. All rights reserved.

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, X-RAID2, 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 2100 Network Attached Storage System 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 2100 Network Attached Storage System 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 A category (business use only) 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:	2100
Publication Date:	June 2009
Product Family:	Network Storage
Product Name:	ReadyNAS 2100 Network Attached Storage System
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10504-01
Publication Version Number:	1.1

Contents

About This Manual

Conventions and Formats ix

User Manual Revision History x

Chapter 1
Getting Acquainted

What is the ReadyNAS 2100? 1-1

The Benefits of X-RAID2 1-2

Introducing the Status Displays, Ports, and Drive Bay 1-2

Front Panel 1-2

Disk Tray Release and Tray Latch 1-3

Control Panel 1-3

Rear Panel 1-5

Initial Setup 1-5

Default IP Address, Login Name, and Password 1-6

The RAIDar Setup Utility 1-6

The FrontView Management Console 1-7

Chapter 2
Managing Your ReadyNAS 2100

Customizing Network Settings 2-1

Ethernet Interfaces 2-2

Global Network Settings 2-6

WINS 2-7

DHCP 2-7

Route: A Manual Routing Table 2-8

Updating the Admin Password 2-8

Selecting Services for Share Access 2-10

Standard File Protocols 2-10

Discovery Services 2-12

Understanding Volume Management 2-13

Advantages of X-RAID2 and Flex-RAID 2-13
Volume Management for Flex-RAID 2-14
Volume Management for X-RAID2 2-17
Working with iSCSI Target Volumes 2-19
Working with USB Volumes 2-20
Adjusting System Settings 2-22
Clock, System Time, and NTP Options 2-23
Alerts, Alert Contacts, Alert Settings, SNMP, and SMTP 2-23
Language Settings 2-27
Updating ReadyNAS 2100 2-28
Configuration Backup 2-30

Chapter 3
Managing User Access

Understanding Share Security Access Modes 3-1
User Security Mode 3-2
Domain Security Mode 3-4
Setting Up User and Group Accounts 3-5
Managing Groups 3-6
Managing Users 3-8
Setting Accounts Preferences 3-10
Changing User Passwords 3-10
Managing Shares 3-11
Adding Shares 3-11
Managing Shares 3-12
Share Access from a Web Browser 3-18
FTP/FTPS 3-19
Rsync 3-20
Remote Access 3-21
ReadyNAS Remote 3-21
Remote FTP Access 3-23
Remote HTTP Access 3-25

Chapter 4
Securing Your Data

Configuring Backup Jobs 4-1
Adding a New Backup Job 4-1

Viewing the Backup Schedule 4-7
Programming the Backup Button 4-8
Viewing the Backup Log 4-8
Editing a Backup Job 4-9
MAC OS X Time Machine Backup 4-9
Snapshots 4-9
Backing Up the ReadyNAS to a USB Drive 4-13
Back Up to the Web with the ReadyNAS Vault Service 4-14

Chapter 5
Optimizing Performance and Maintaining the System

Optimizing Performance 5-1
Adding a UPS 5-2
Power Management 5-3
Disk Spin-Down Option 5-3
Power Timer 5-4
Configuring UPS Battery Low Shutdown 5-4
Wake-On-LAN 5-4
Viewing System Status 5-5
Health 5-5
Logs 5-6
Control Panel Status and Diagnostic Information 5-7
Shutdown 5-8
Replacing a Failed Disk 5-9
Choosing a Replacement Disk 5-10
Replacing a Failed Disk 5-10
Resynchronizing the Volume 5-11
Using the System Diagnostic Boot Menu 5-12
Use the OS REINSTALL Option to Re-install the Firmware 5-13
Using the Boot Menu to Format a RAID Volume 5-14

Appendix A
Default Settings

Appendix B
Share Access from MAC and Linux Systems

MAC OS X B-1

AFP over Bonjour B-2
AFP over AppleTalk B-3
MAC OS 9 ..... B-5
Accessing Shares from Linux/Unix B-7
Appendix C
X-RAID2 and RAID
The Benefits of X-RAID2 ..... C-1
X-RAID2 Is Auto-Expandable RAID C-1
Simplified Redundancy C-1
Easy Volume Expansion C-2
Overview of RAID C-2
RAID Basics C-3
RAID Levels C-3
Index

About This Manual

The *NETGEAR® ReadyNAS 2100 User Manual* describes how to configure and troubleshoot a ReadyNAS 2100 system. The information in this manual is intended for readers with intermediate computer and networking skills.

Conventions and Formats

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 note highlights information of importance or special interest.

Tip: This note highlights a procedure that will save time or resources.

Warning: This note warns against a malfunction or damage to the equipment.

Danger: This safety warning warns against personal injury or death.

User Manual Revision History

Part Number	Version Number	Publication Date	Description
202-10504-01	1.0	May 2009	First publication
202-10504-01	1.1	June 2009	Update to align with features changes added to initial release firmware.

Chapter 1
Getting Acquainted

This chapter provides an overview of the features and capabilities of the ReadyNAS 2100. It also covers the unit's physical features, main software, and initial setup steps.

Topics discussed in this chapter include:

- "What is the ReadyNAS 2100?"
- "The Benefits of X-RAID2"
- "Introducing the Status Displays, Ports, and Drive Bay"
- "Initial Setup"
- "The RAIDar Setup Utility"
- "The FrontView Management Console"

What is the ReadyNAS 2100?

NETGEAR ReadyNAS gigabit network storage products provide small and medium sized businesses with easy-to-use, high-performance network attached storage solutions to share and protect critical data. Housed in a compact rack mount form factor, the ReadyNAS 2100 supports up to four SATA I or SATA II hard drives via lockable, hot-swappable disk trays. Three USB 2.0 ports enable the connection of USB drives. Based on current drive capacities, the ReadyNAS provides up to 8TB of network attached storage that can easily be expanded as larger capacity drives become available.

ReadyNAS enables users across the LAN, WAN, or over the Internet to back up and share data from Windows, Macintosh, and Linux systems. ReadyNAS offers extensible robust high-availability data protection. Its fail-safe features include dual redundant Gigabit Ethernet ports, support for RAID 0, 1, 5, plus hot spare, and NETGEAR's proprietary X-RAID2™ for automatic volume expansion. You can also allocate iSCSI target volumes on a ReadyNAS 2100.

ReadyNAS includes a built-in FrontView Web based graphical user interface and setup wizard for ease-of-use and setup. ReadyNAS continually monitors the entire system for abnormal situations or part failures. Status indicators in the hardware and software provide quick system status readings. It e-mails the network administrator alerts about critical changes in the system. Also, developers can use the Frontview Add-on SDK to uniquely extend ReadyNAS capabilities.

The NETGEAR ReadyNAS Community web site is *http://readynas.com*, where you will find reviews of new features, tutorials, software updates, documentation, an active user forum and much more. For a full list of what is new compared with existing ReadyNAS systems, see *ReadyNAS Specifications* on ReadyNAS.com.

The Benefits of X-RAID2

X-RAID2 is a proven patent-pending technology that is available only on ReadyNAS. The ReadyNAS 2100 supports both X-RAID2, the second generation version of X-RAID, and RAID 0/1/5.

A major advantage of X-RAID2 is its ability to automatically expand to include the full space of new disks. When as little as two of your disks have extra capacity, the data volume will automatically expand its capacity. The capacity of the data volume increases every time you add a larger disk, regardless of the capacity of the other disks in the system. X-RAID2 lets you do this without reformatting your disks and shuffling your data back and forth. The process occurs in the background, so access to the ReadyNAS 2100 is not interrupted. Furthermore, X-RAID2 supports multiple parity which provides protection against two simultaneous disk failures. For more on X-RAID2 and RAID, see Appendix C, “X-RAID2 and RAID”.

Introducing the Status Displays, Ports, and Drive Bay

This section introduces the ReadyNAS display, ports, and drive bays.

Front Panel

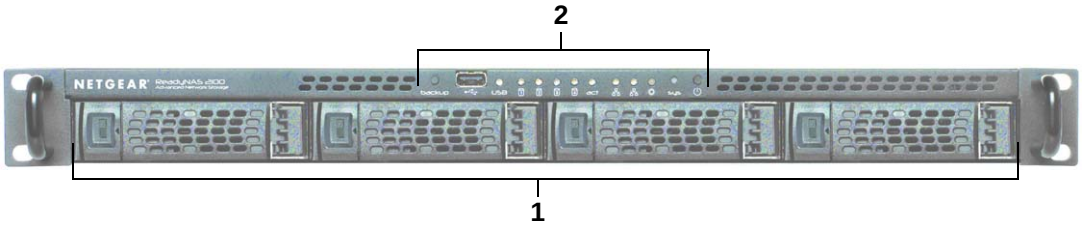


Figure 1-1

1. Drive bays.
2. Control Panel.

Disk Tray Release and Tray Latch

The disk tray features a lockable push switch activated pop-out release.

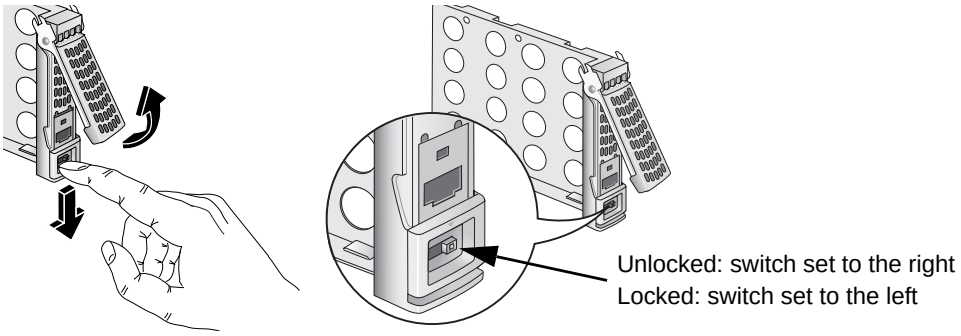


Figure 1-2

To prevent easy removal of the disk, set the recessed tray lock: left is locked; right is unlocked.

Control Panel

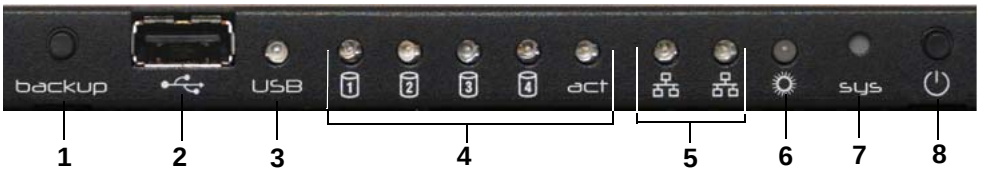


Figure 1-3

The function of each Control Panel item is described in the following table:

Table 1-1. LED Descriptions

Item	Activity	Description
1. Backup Button.	Push button	Backup: Push to initiate FrontView scheduled backup jobs. Diagnostics: See *"Control Panel Status and Diagnostic Information"* on page 5-7.
2. Front USB Port.	USB Port	Connect a USB drive.

Table 1-1. LED Descriptions (continued)

Item	Activity	Description
3. USB Status LED.	On (Green) Blinking (Green) Off	On: A USB device is mounted. Blink: USB device dismounting *or* FrontView scheduled backup running. Off: USB device dismounted.
4. Disk LEDs .	On (Green) Blink (Green) Off	On: Disk installed Blink: • Slow blink: Disk synchronization *or* disk failure. • Fast blink for 10 seconds: Power button just pushed. • Panic blink: Warning that power button pressed & held. • "Marching" LEDs: Volume expansion in progress. Off: No disk installed.
5. Activity LED.	On/Blinking (Green) Off	One or more disks being accessed.
6. LAN1 LAN2 Ports.	On (Green) Blinking Off	On green: The LAN port is linked. Blinking: Data communications activity. Off: The LAN port is disconnected.
7. Power Status LED.	On (Blue) Blinking Off	On: The unit is powered on. Blinking: The unit is powering on or powering off. Off: Power is not supplied to the unit.
8. SYS Reset Button.	Recessed push button, activated with a pen tip or paper clip	Power cycle the ReadyNAS 2100. Also provides access to the diagnostic startup menu. For diagnostics, see *"Control Panel Status and Diagnostic Information"* on page 5-7.
9. Power Button and LED	Push button On (Blue) Blinking Off	Power button actions: • **Press once:** Power the system on. • **Press twice - preferred shutdown:** When the system is running, initiate preferred shutdown. After the first press, the system displays the graceful shutdown blink pattern on the LEDs. After the second button press, the system initiates the shutdown. • **Press and hold - forced shutdown:** If the unit is hung, press and hold the power button for 5 seconds to force shutdown. LED On: Power is supplied to the ReadyNAS 2100. LED Blink: The ReadyNAS 2100 is booting. LED Off: The system is powered off.

Rear Panel

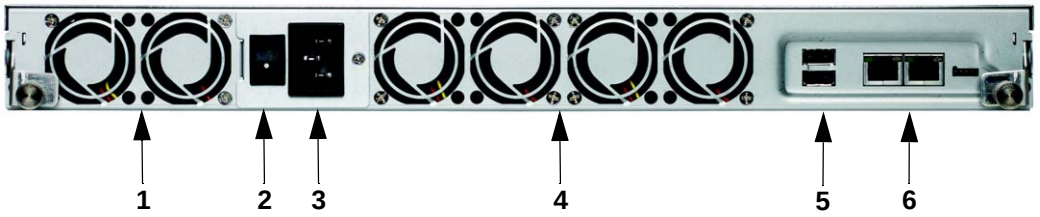


Figure 1-4

1. System exhaust fans.
2. Power on off switch.
3. Power cable socket.
4. Disk exhaust fans.
5. Two USB ports.
6. LAN1 and LAN2 gigabit Ethernet ports.

Initial Setup

Follow the instructions in the NETGEAR Installation Guide that came with your unit to install it. An electronic copy of the installation guide is on the product CD, on the NETGEAR web site, and on *http://readynas.com*.

The initial setup estimated completion time is 20 minutes.

	Note: A diskless unit requires installing disks and initializing RAID before proceeding. Go to *http://www.readynas.com/hcl* for a list of supported disks. Refer to "Using the Boot Menu to Format a RAID Volume" on page 5-14 for instructions on installing disks and configuring RAID.

Refer to *Appendix B, "Share Access from MAC and Linux Systems"* for instructions on accessing shares from Linux and various versions of the MAC OS.

Default IP Address, Login Name, and Password

The default IP configuration is set to DHCP; if the unit does not get an IP address, it defaults to 192.168.168.168. The default administrator user name is **admin** with the default password being **netgear1** (case sensitive).

Note: The RAIDar utility can discover any ReadyNAS on the network without needing its IP address and does not require authentication to access a ReadyNAS.

The RAIDar Setup Utility

The RAIDar utility enables easy setup and management of all your ReadyNAS units.

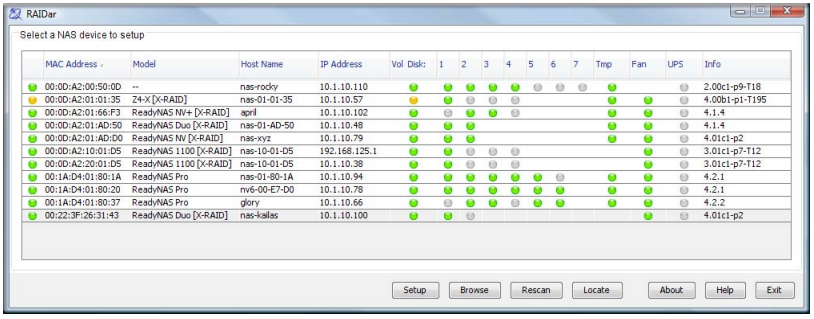


Figure 1-5

It discovers the units in the network, and makes it easy to see the status of the units, and connect to the FrontView management console you use to manage any ReadyNAS on your network.

The FrontView Management Console

The FrontView management console operates in two modes: Setup Wizard mode, and Advanced Control mode. When the unit is in its factory default state, FrontView is in Setup Wizard mode.

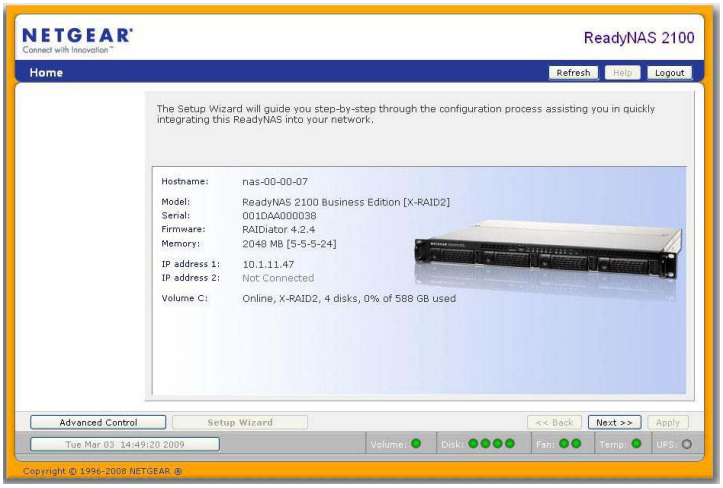


Figure 1-6

Use the wizard to perform the initial configuration of the unit.

The FrontView Advanced Control mode provides access to all the available settings.

Figure 1-7

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

The bar at the top provides options to return to the Home screen, refresh the browser window, display Help where available, or to log out of this session.

Figure 1-8

At the bottom of the screen is the status bar including the date button on the left which, when clicked takes you to the Clock screen. The status lights to the right give a quick glimpse of the system device status.

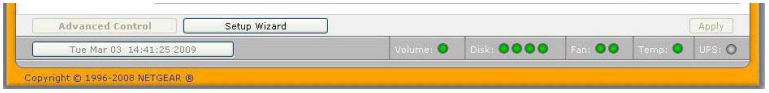


Figure 1-9

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, which you use to save any changes on the current screen.

Chapter 2
Managing Your ReadyNAS 2100

Setting up and managing the ReadyNAS 2100 Network Attached Storage System in your network is described in this chapter. This chapter contains the following sections:

- "Customizing Network Settings"
- "Updating the Admin Password"
- "Selecting Services for Share Access"
- "Understanding Volume Management"
- "Adjusting System Settings"
- "Configuration Backup"

Customizing Network Settings

Access network settings by via the Advanced Control button, and selecting >Network from the main menu. From the Network menu, you can then navigate to your basic network settings screens such as Interfaces, Gateway, DNS, WINS, DHCP, and Route options.

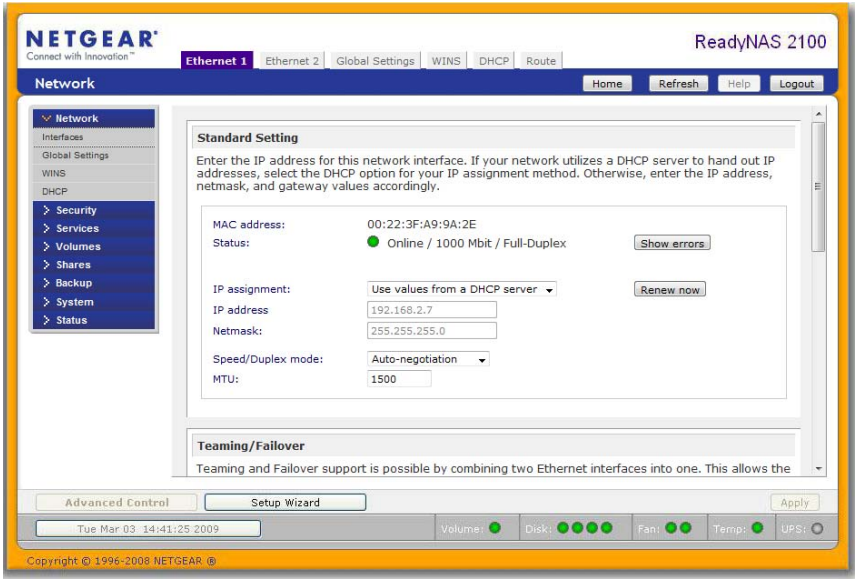


Figure 2-1

Ethernet Interfaces

Select Network > Interfaces > Ethernet 1 /Ethernet 2 tab pages to specify network interface-specific settings for Standard Settings, Teaming/Failover, VLAN, and Performance Settings.

Standard Setting

In this 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.

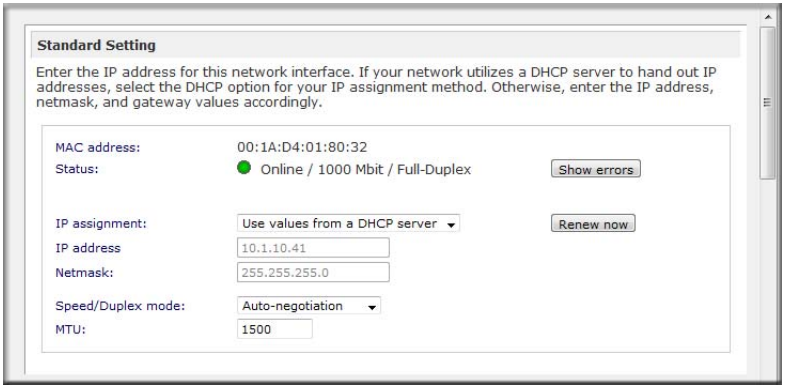


Figure 2-2

- **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 IP address of the unit changes even when it 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 2100 maintains the same IP address even in DHCP mode.

Tip: Consider reserving an IP address for the MAC address of this Ethernet interface in your DHCP server (or router). This will give you the stability of a fixed IP address without the effort of maintaining static addresses.

  - If you assign a static IP address by selecting **Use values below**, be aware that the browser will lose connection to the ReadyNAS 2100 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 (Only applies to 10/100 connections)**. 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.

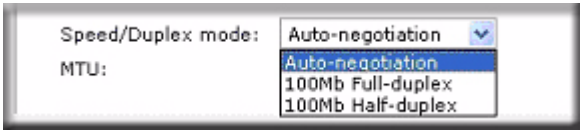


Figure 2-3

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

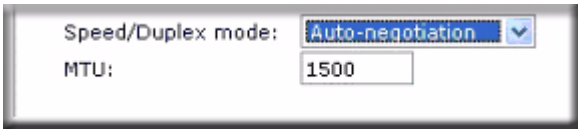


Figure 2-4

Teaming/Failover

In this section, you can select the desired bonding mode. Network teaming provides a way to aggregate the two network interfaces into a single logical teamed, or bonded, interface. The teamed interface can provide for enhanced aggregate performance over a logical single interface while allowing for fail-over support that reduces the number of single points of failure in the network.

If you plan to use the Teaming/Failover option, connect both interfaces, configure the Teaming/Failover options on the Ethernet 1 tab page, then configure the other options for Ethernet 1 and Ethernet 2 accordingly.

	Note: If you plan to reserve an IP address in your DHCP server for the ReadyNAS and will use the Teaming/Failover option, complete the ReadyNAS bonding of the Ethernet interfaces before updating the DHCP server address reservation table.

The following teaming/fail over options are available.

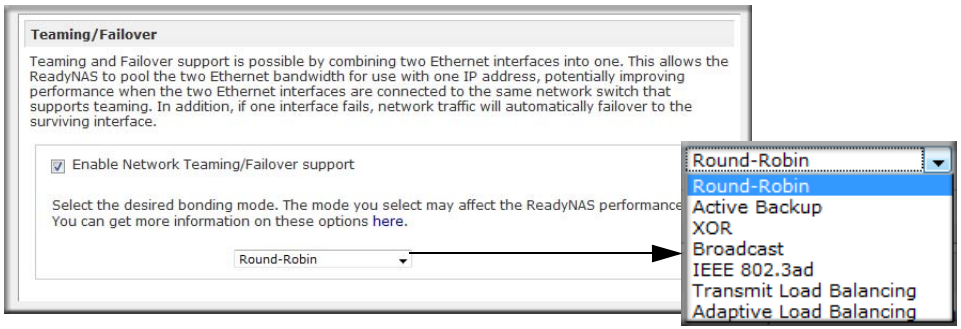


Figure 2-5

Note: To get the full performance benefit of an option, provision servers with dual Ethernet interfaces, and verify that the LAN switch supports the feature that a ReadyNAS teaming option may require. A mismatch between the LAN switch and a ReadyNAS teaming option could degrade the throughput of the ReadyNAS.

- **Round-Robin**: Transmit packets in sequential order from the first available interface to the next. This mode provides load balancing and fault tolerance.
- **Active Backup**: Only one interface in the bond is active. A different interface becomes active if, and only if, the active interface fails. The MAC address of the bonded interface is externally visible on only one port to avoid confusing the switch.
- **XOR**: Transmit based on the default simple transmit hash policy (one, or the other but not both). This mode provides load balancing and fault tolerance.
- **Broadcast**: Transmit everything on all slave interfaces. This mode provides fault tolerance.
- **IEEE 802.3ad LACP**: Creates aggregation groups that share the same speed and duplex settings. Utilizes all interfaces in the active aggregator according to the 802.3ad specification.

Note: To use this option, the switch to which the ReadyNAS connects must support IEEE 802.3ad LACP dynamic link aggregation. If the switch supports this feature, this is the recommended option.

- **Transmit Load Balancing**: Channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each interface. Incoming traffic is received by the current interface. If the receiving interface fails, another interface takes over the MAC address of the failed receiving interface.

- **Adaptive Load Balancing**: Includes Transmit Load Balancing plus Receive Load Balancing for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation.

VLAN Settings (Virtual Local Area Network)

In this section, 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.

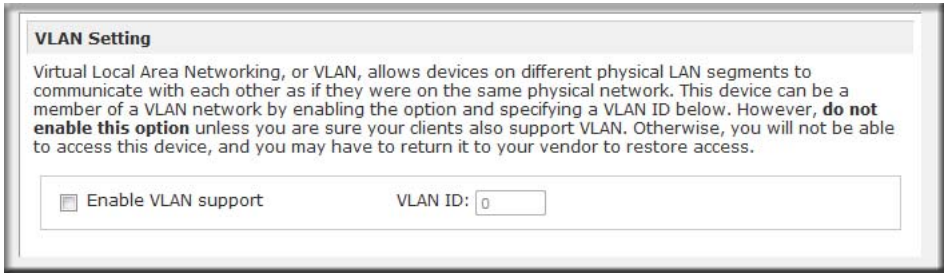


Figure 2-6

If you wish to use the ReadyNAS 2100 in a VLAN environment, select the **Enable VLAN support** check box, and enter a numeric VLAN ID. You need to reboot the ReadyNAS 2100 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 unit, and you might need to reinstall the firmware to disable the VLAN setting.

Performance Settings

In this section, you can the Enable jumbo frames option allows you to optimize the ReadyNAS 2100 for large data transfers such as multiple streams of video playback.

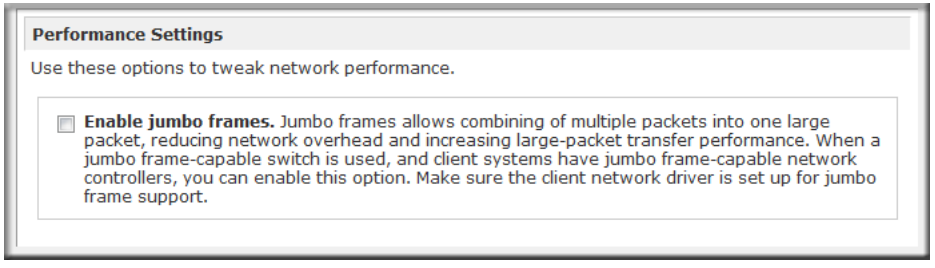


Figure 2-7

Note: Use this option only if your NIC and your gigabit switch support jumbo frames. The ReadyNAS 2100 supports a 9000 byte frame size. For optimal performance, a switch capable of this frame size or larger should be used.

Global Network Settings

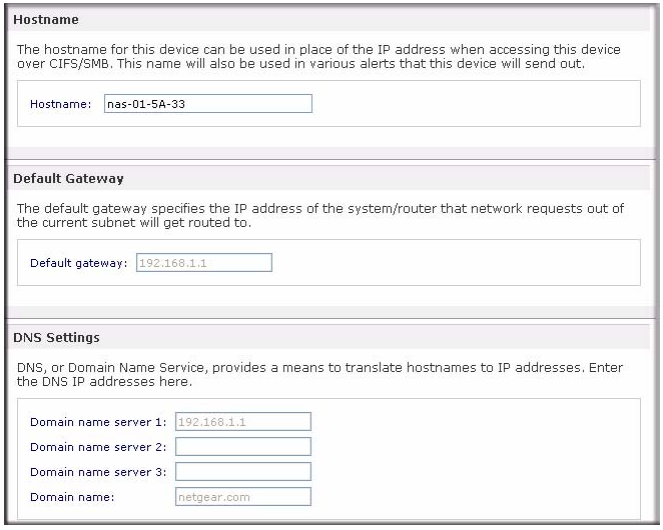


Figure 2-8

Hostname

The Hostname you specify is used to advertise the ReadyNAS 2100 on your network. You can use the hostname to address the ReadyNAS 2100 in place of the IP address when accessing the ReadyNAS 2100 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

A WINS (Windows Internet Naming Service) server allows the ReadyNAS 2100 or other devices on the network to be browsed from other subnets. This can be useful if you wish to browse by hostname across multiple subnets (for example, over VPN).

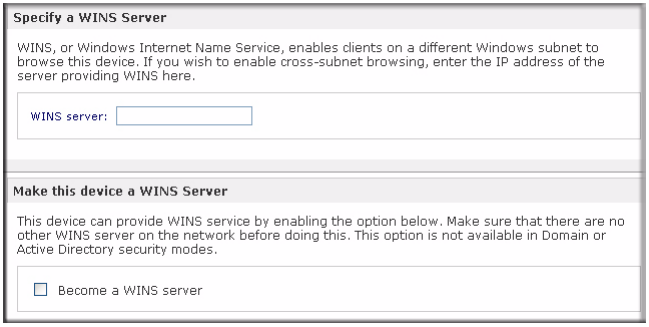


Figure 2-9

You can specify the WINS server IP address, or you make the ReadyNAS your WINS server.

DHCP

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

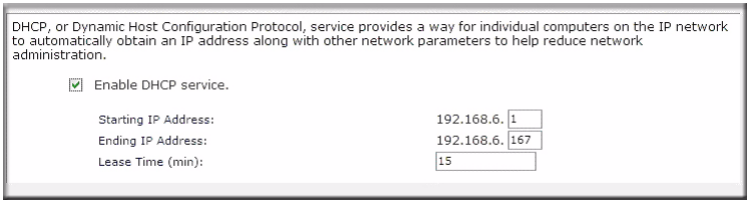


Figure 2-10

Select the **Enable DHCP service** check box if you want the ReadyNAS 2100 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 that can disable network access. If you wish to use this device as a DHCP server, make sure to specify static addresses in the Ethernet and DNS tabs.

Route: A Manual Routing Table

The Route tab allows you to specify a manual routing table for each Ethernet interface. You can use this option to optimize performance. For example, you could configure a manual routing table to assure that these Ethernet interfaces were directly routed over a fiber backbone to assure that the unit would not experience the traffic congestion that can build up on a gigabit segment.

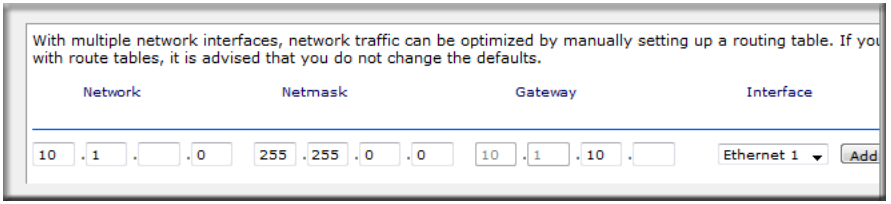


Figure 2-11

Updating the Admin Password

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

	Note: The RAIDar utility includes a discovery mechanism that enables it to find any ReadyNAS on the network without needing to know its IP address. Also, RAIDar does not require a user name and password to monitor a ReadyNAS.

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 change or erase the data on the ReadyNAS.

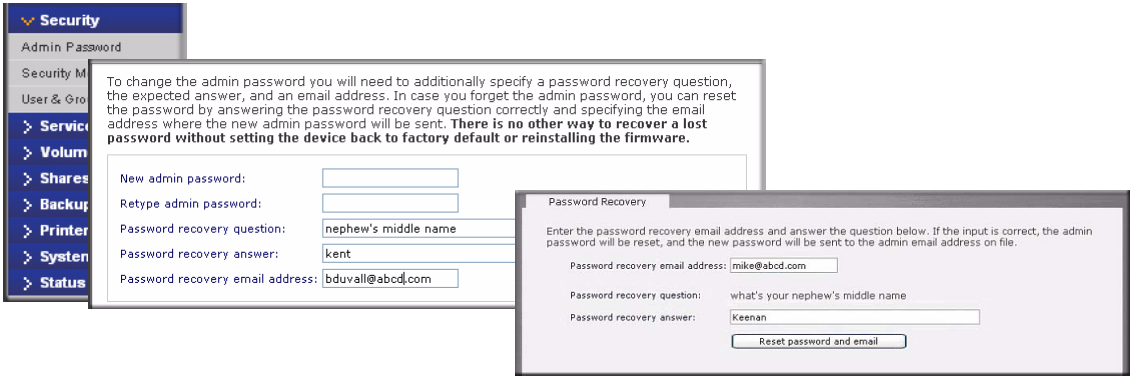


Figure 2-12

	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 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, which is sent to the e-mail address you enter on this screen.

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 2100.

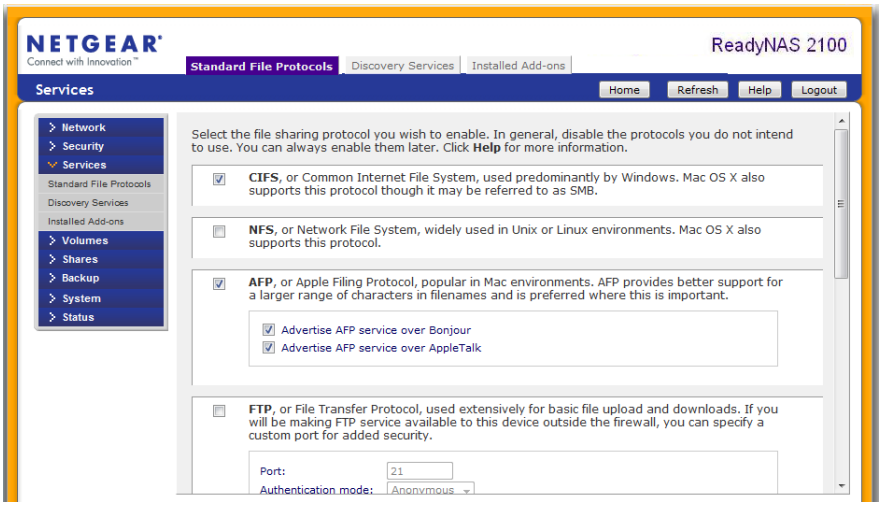


Figure 2-13

Three types of services are available: Standard File Protocols, Discovery Services, and Installed Add-ins such as streaming 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 2100 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 2100 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 2100 supports AFP 3.1.
- **FTP** (File Transfer Protocol). Widely used in public file upload and download sites. ReadyNAS 2100 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 2100 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 2100. This allows you to bypass the default dummy certificate warnings whenever users access the ReadyNAS 2100 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 2100 allows clients to use rsync to initiate backups to and from the ReadyNAS 2100.

Discovery Services

Bonjour and UPnP discovery services are included with theReadyNAS 2100. Additional services that you download and install from www.readynas.com are listed in the Add-ons tab page.

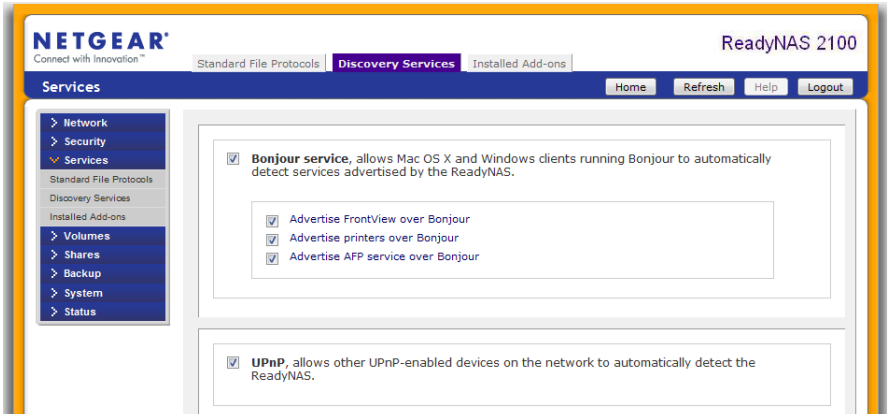


Figure 2-14

- **Bonjour service** provides a simple way of discovering various services on the ReadyNAS 2100. 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 2100 on your LAN.

Understanding Volume Management

The ReadyNAS 2100 family offers two RAID volume technologies: Flex-RAID, utilizing the industry-standard RAID levels 0, 1, and 5; and X-RAID2, the NETGEAR-patented expandable RAID technology.

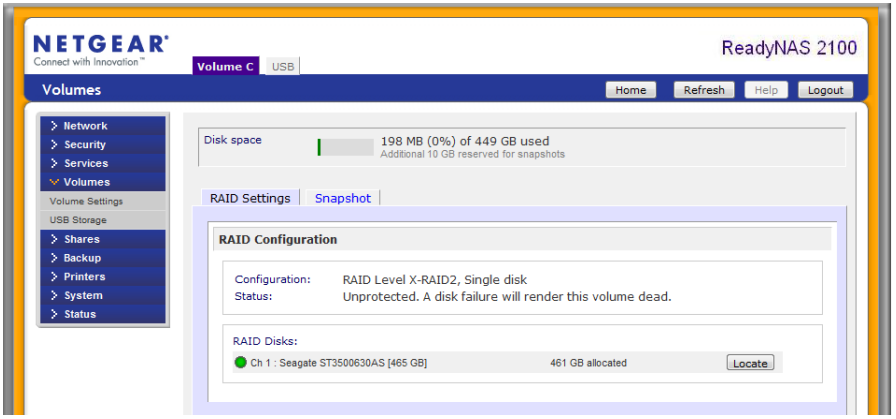


Figure 2-15

Your system comes preconfigured with X-RAID2. However, you can switch between the two modes through a factory default reset process described in *"Using the Boot Menu to Format a RAID Volume"* on page 5-14." For more on X-RAID2 and RAID, see Appendix C, "X-RAID2 and RAID".

Advantages of X-RAID2 and Flex-RAID

There are advantages to both technologies.

- **Flex-RAID:**
  - The default volume can be deleted and re-created, with or without snapshot reserved space.
  - Hot spare disk is supported.
  - Full volume management is available. You can create RAID level 0, 1, or 5 volumes, specify the volume size, 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 using the newly added capacity can be configured.

- **X-RAID2:**
  - One-volume technology, but supports volume expansion, either with the addition of more disks or the replacement of existing disks with larger capacity disks.
  - You can start out with one disk, and add more disks as 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 new redundant space becomes available, your volume will automatically expand to utilize the new capacity.

Volume Management for Flex-RAID

If you want to reconfigure the default Flex-RAID 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 and are non-recoverable!*

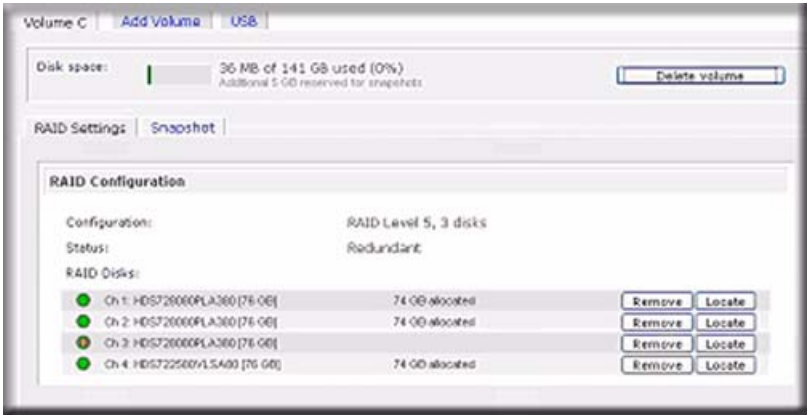


Figure 2-16

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

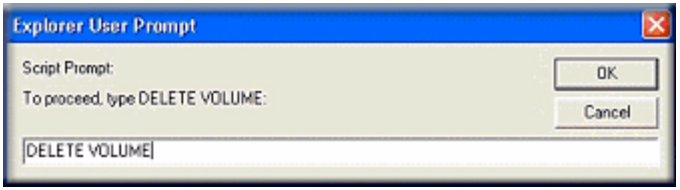


Figure 2-17

Adding a Volume

After deleting the volume, the Add Volume tab lists the available configurable space on the hard disks. All the disks are selected by default. You can 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.

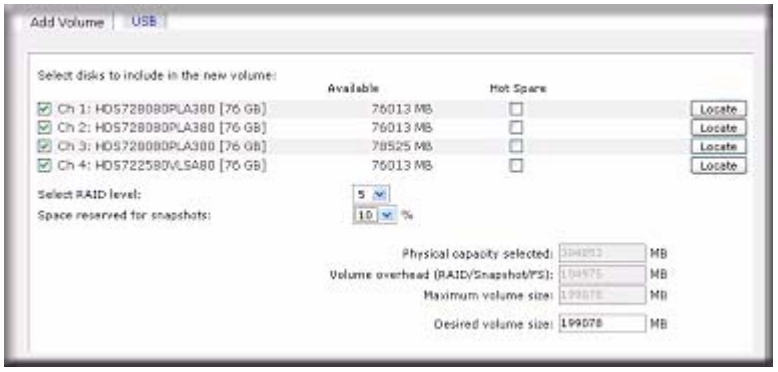


Figure 2-18

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. 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 *"Snapshots"* on page 4-9), 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.
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 ReadyNAS.

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**.

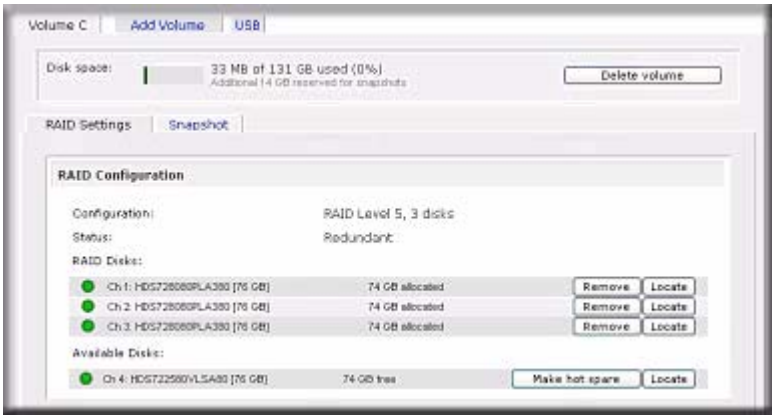


Figure 2-19

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-RAID2

Most people want to either add redundancy or expand their data volume. X-RAID2 enables this without the headaches usually associated with doing so.

Adding a Second Disk for Redundancy

A one-disk X-RAID2 device has no redundancy and provides no protection from a disk failure. However, if and when you feel the need for redundancy, simply add a new disk with at least the capacity of the first disk. 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 2100 is not interrupted.

Adding More Disks

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-RAID2. 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-RAID2 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.

Reboot the ReadyNAS to initiate the background expansion. You can continue using the ReadyNAS while the expansion proceeds. You will get an email notice when the expansion completes.

After you receive your e-mail, the ReadyNAS 2100 will have been expanded with the capacity from your new disk(s).

Replacing Disks for More Capacity

When you need more disk space and larger disks are available at an attractive price, you can expand your volume capacity by replacing the existing disks.

The ReadyNAS 2100 supports hot-swapping, so you can swap disks without powering down. Replace the first disk, and the ReadyNAS will detect that a new disk was put in place and resynchronizes the disk with data from the removed disk. This process can take 30 minutes or longer, depending on disk capacity, but you can use the ReadyNAS while the new disk synchronizes. Upon completion, replace the second disk with another large-capacity disk, allow that disk to synchronize. X-RAID2 lets you expand the volume when a minimum of two disks are replaced. At one time, you cannot replace disks that add up to more than the current volume capacity. When you have replaced the desired number of disks, simply reboot the ReadyNAS to initiate the background expansion. You can continue using the ReadyNAS while the expansion proceeds. You will get an email notice when the expansion completes.

Changing between X-RAID2 and Flex-RAID Modes

You can switch between X-RAID2 and Flex-X-RAID modes. The process involves setting the ReadyNAS 2100 to the factory default and using RAIDar to configure the volume during a 10-minute delay window during boot. Setting the ReadyNAS 2100 to the factory default setting will erase all its data. See “Using the Boot Menu to Format a RAID Volume” on page 5-14 for more information.

Working with iSCSI Target Volumes

The iSCSI target service enables you to create one or more iSCSI target volumes on the ReadyNAS.

The iSCSI (Internet SCSI) protocol allows clients called initiators to send SCSI commands to SCSI storage devices called targets on remote servers. It is a popular Storage Area Network (SAN) protocol, allowing organizations to consolidate storage into data center storage arrays while providing hosts such as databases and web servers with the illusion of locally-attached disks. Unlike Fibre Channel, which requires special-purpose cabling, iSCSI can be run over long distances using existing network infrastructure.

An iSCSI initiator sends SCSI commands over an IP network to an iSCSI target. Software to provide an iSCSI initiator is available for most mainstream operating systems. Unlike network file services where you access files in network share folders, the iSCSI target presents itself as a virtual block device and can be treated like a locally attached disk to the client system acting as the iSCSI initiator. Windows for instance could run FAT32 or NTFS on the iSCSI target device, and treat the device as though it was locally attached.

To configure an iSCSI target volume on the ReadyNAS, go to Volumes > Volume Settings > iSCSI.

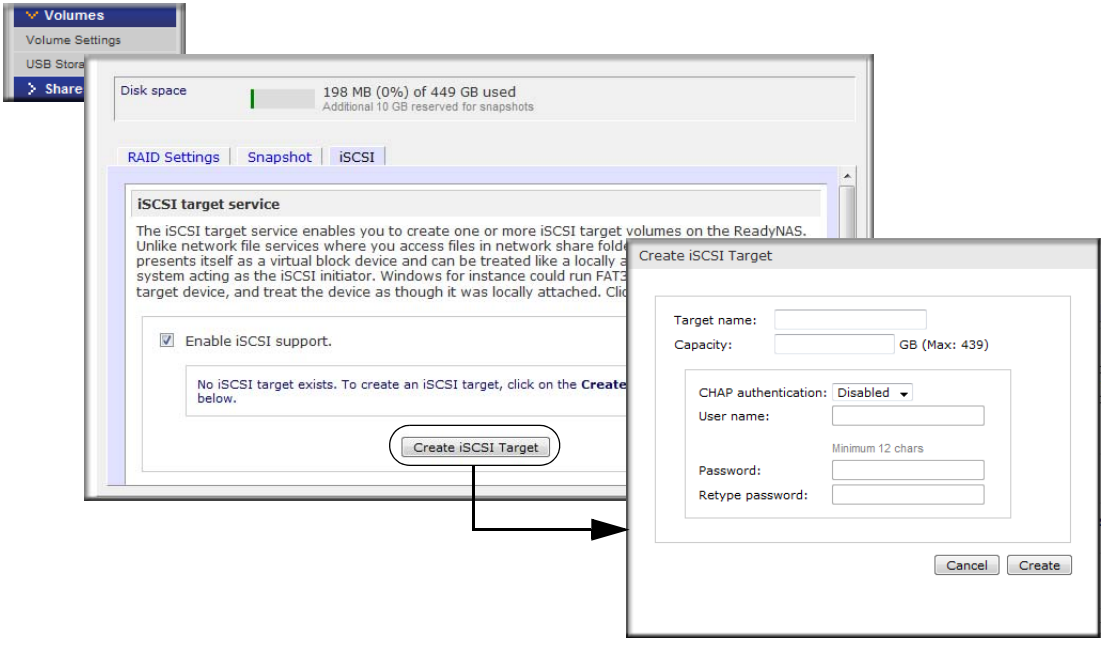


Figure 2-20

To enable iSCSI support, click **Create iSCSI Target**, and enter the desired name of the target and the capacity you wish to reserve for this target device. Maximum capacity is slightly less than the full free space on the ReadyNAS. If you wish to enable authentication for access, enable CHAP authentication and specify the user name and password. The password needs to be at least 12 characters long.

Go to *http://readynas.com/iSCSI* on ReadyNAS.com for instructions on setting up iSCSI access from various operating systems.

Working with USB Volumes

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 USB tab displays the USB disk and flash devices connected to the ReadyNAS 2100, 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.

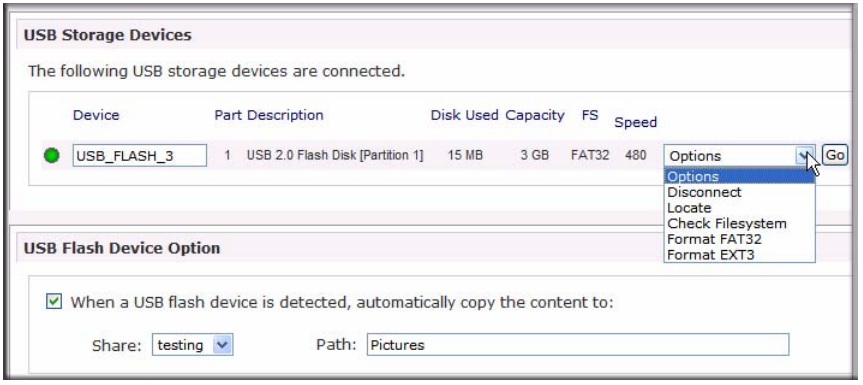


Figure 2-21

Partitions on the storage devices must be one of the following file system formats: FAT32, NTFS, Ext2, or Ext3.

To the right of the access icons are command options. 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.

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 2-21 on page 2-20). 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.

USB Volume Name and Access Rights Persistence Across Mount/Dismounts

The ReadyNAS 2100 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.

Figure 2-22

Note: Even when access authorization is based on user login, files on a USB device, are saved with UID 0 regardless of the user account. This is to allow easy sharing of the USB device with other ReadyNAS and PC systems.

Adjusting System Settings

Use the System menu to adjust the system settings.

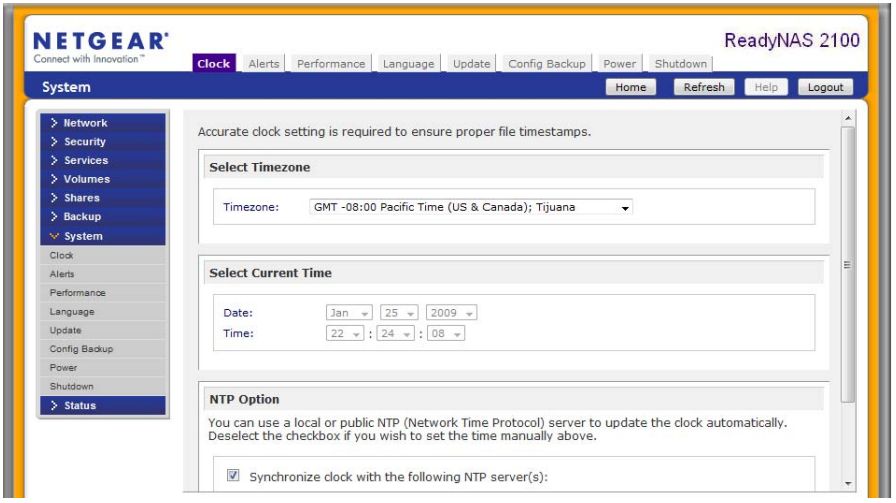


Figure 2-23

System settings include clock, alert, performance, language, firmware update, configuration backup/restore, power, and shutdown settings.

Clock, System Time, and NTP Options

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.

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. 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, Alert Contacts, Alert Settings, SNMP, and SMTP

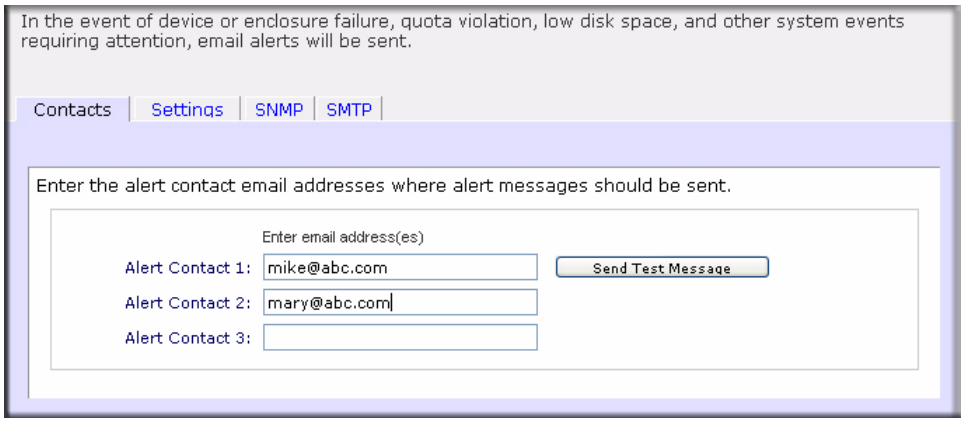


Figure 2-24

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.

Contacts

The Contacts tab allows you to specify up to three e-mail addresses where system alerts will be sent. The ReadyNAS 2100 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.

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.

Settings

This ReadyNAS 2100 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.

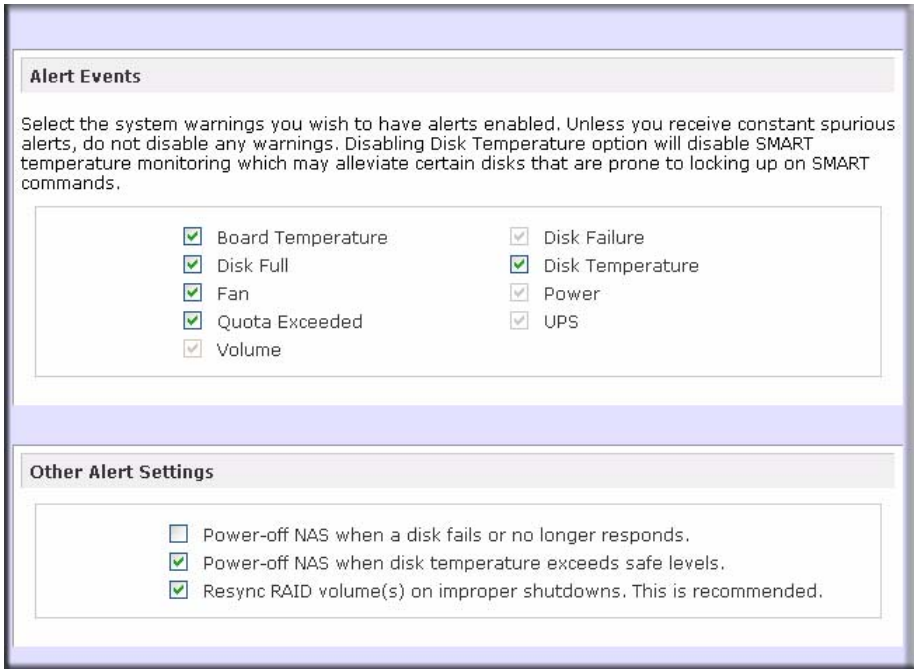


Figure 2-25

You should 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 2100 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 2100 when the disk temperature exceeds the nominal range.

SNMP

If you use an SNMP management system such as HP OpenView or CA UniCenter to monitor devices on your network, you can set up the ReadyNAS 2100 device to work with this infrastructure.

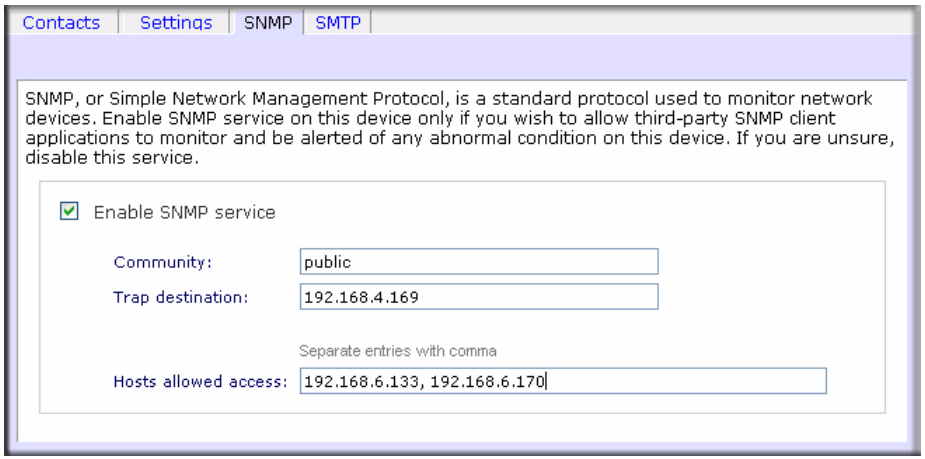


Figure 2-26

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 2100, 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 2100 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.

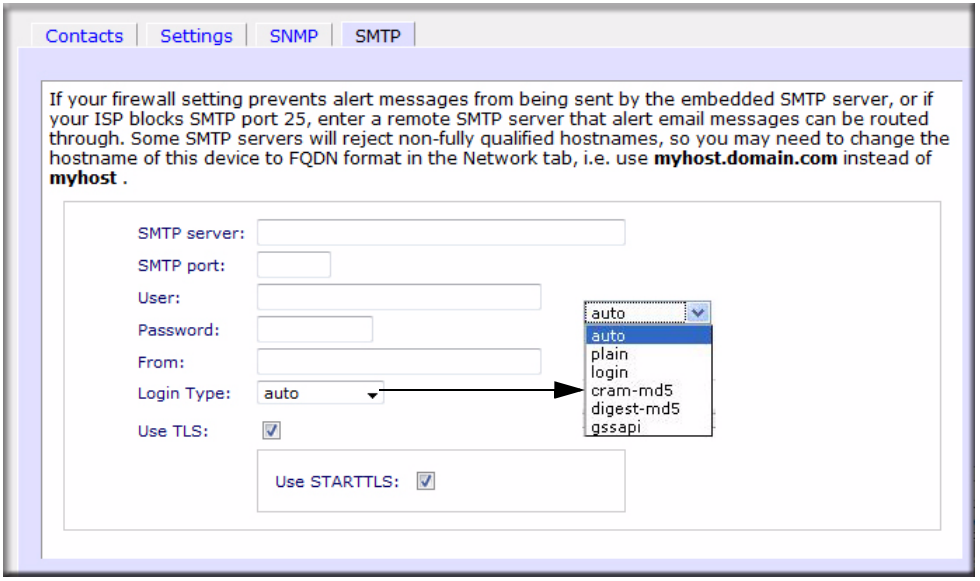


Figure 2-27

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 (see "Hostname" on page 2-6), i.e. use myhost.domain.com instead of myhost.

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.

The TLS option allows the SMTP server and client to use transport-layer security to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers, and may be required by the SMTP server you are using.

Language Settings

The Language Setting screen offers the option of setting the ReadyNAS 2100 device to the appropriate character set for file names.

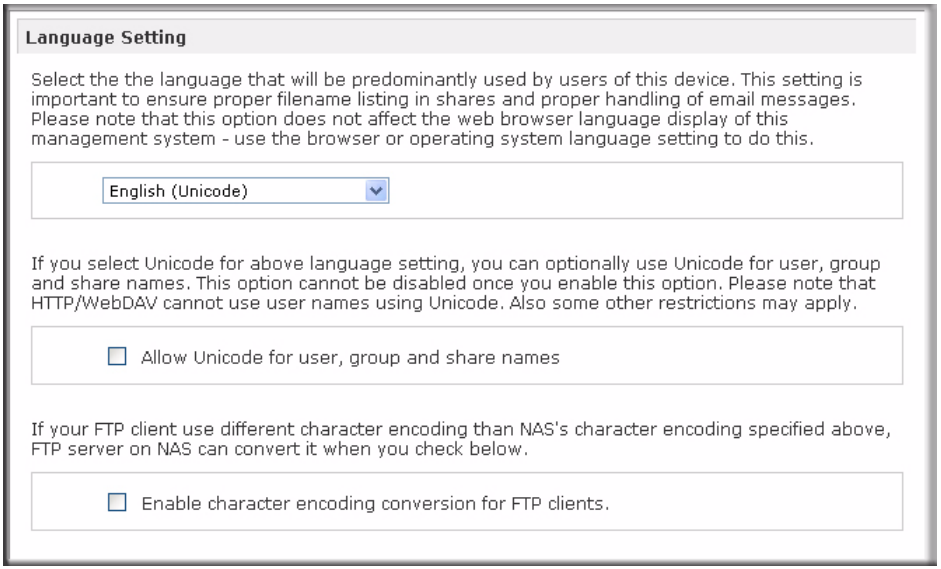


Figure 2-28

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

Figure 2-29

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 2100

The ReadyNAS 2100 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 website.

Updating from the NETGEAR Web Site

If the ReadyNAS 2100 has Internet access the easiest update option is the Remote option. The update process updates only the firmware image and does not modify your data volume. However, it is always a good practice to back up your data before you perform an update.

To use the Remote option, select Update from the main menu and then click the **Remote** tab. Click **Check for Updates** to check for updates on the NETGEAR update server.

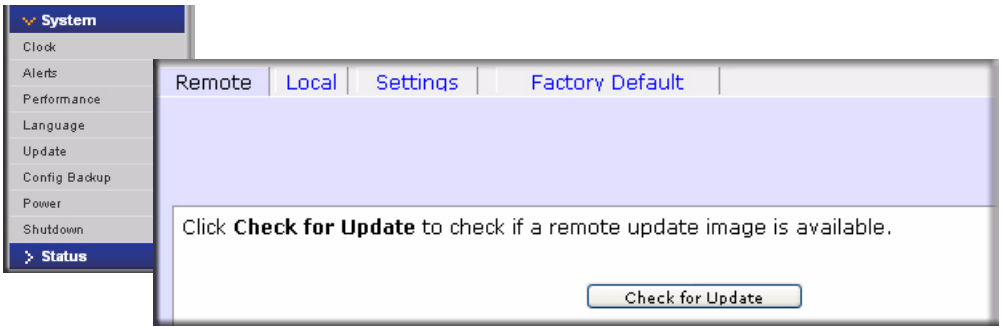


Figure 2-30

When prompted, click **Perform System Update**. After the update image has been downloaded, you will be asked to reboot the system. .

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

Updating from a Local Drive

When the ReadyNAS 2100 is not connected to the Internet, or Internet access is blocked, you can download an updated RAIDiator firmware image from *http://www.readynas.com* and upload that file. The process takes several minutes after which you are requested to reboot the system and proceed with the upgrade

Configuring Automatic Update Settings

You can enable the automatic update check and download options in the Settings tab. If you select the **Automatically check for updates** check box, the ReadyNAS 2100 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.

Restoring the Factory Default Settings

The Factory Default tab allows you to reset the ReadyNAS 2100 device back to its factory default state.

	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.

Back up the data and configuration information that you wish to keep prior to using this option.

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

Configuration Backup

Backup and restore ReadyNAS configurations to preserve settings to safeguard the configurations or to replicate settings onto other ReadyNAS devices. Use the configuration backup to save your configuration so that if you ever have to reset the unit to its factory default settings, you can simply restore all your settings from the configuration backup.

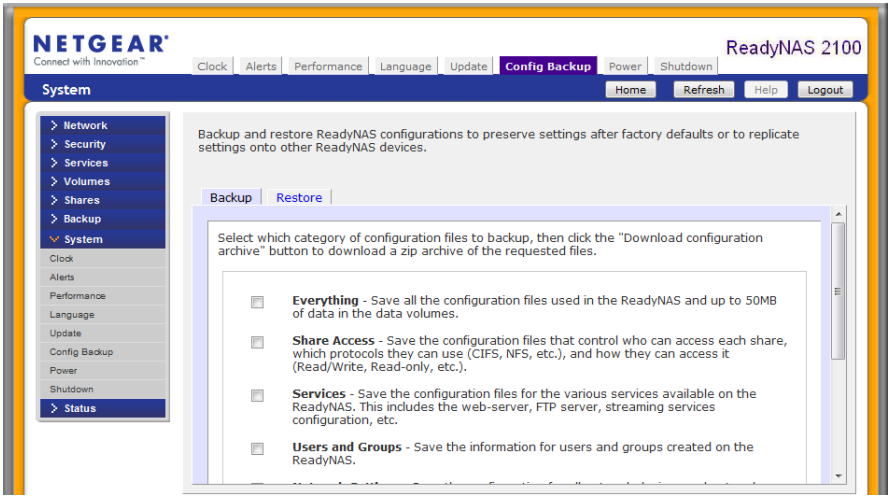


Figure 2-31

Click **Backup** then Select which category of configuration files to backup, then click the "Download configuration archive" button to download a zip archive of the requested files. Use the Restore tab to browse for a configuration backup you would like to restore. You can also use this feature to replicate a standard configuration across a number of units.

Chapter 3
Managing User Access

Setting up and managing the ReadyNAS 2100 Network Attached Storage System in your network is described in this chapter. This chapter contains the following sections:

- "Understanding Share Security Access Modes"
- "Setting Up User and Group Accounts"
- "Changing User Passwords"
- "Managing Shares"
- "Share Access from a Web Browser"
- "FTP/FTPS"
- "Rsync"
- "Remote Access"

Understanding Share Security Access Modes

The ReadyNAS 2100 offers User and Domain security access options.

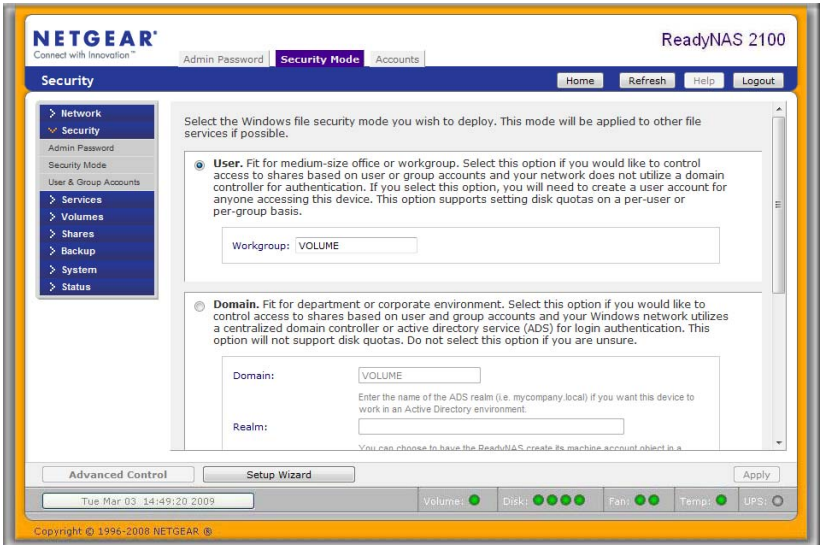


Figure 3-1

Select the most appropriate option based on the required level of security and your current network authentication scheme.

- **User.** User security mode is the recommended selection for the small and medium-size office or workgroup environments. This mode allows you to set up share access restrictions based on user and group accounts. 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.
- **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.

User Security Mode

This option is ideal for small and 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.

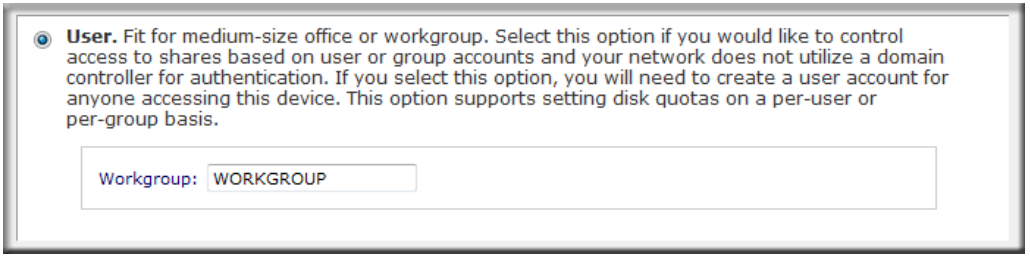


Figure 3-2

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 2100 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), AFP (Mac), and FTP/S protocols.

To set up the ReadyNAS 2100 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 2100.

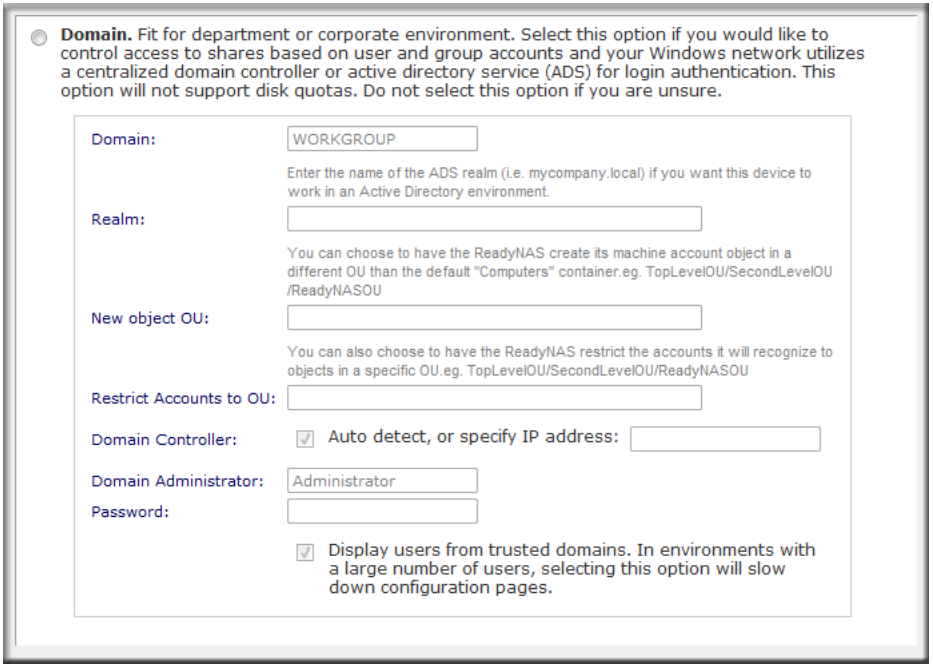


Figure 3-3

You need the following information:

- Domain name.
- Domain administrator login.
- Domain administrator password.
- If using ADS, you will need:
  - 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.

You can elect to have the ReadyNAS 2100 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: At this time you can use of the ReadyNAS 2100 in a domain environment that serves up to 32,000 users.

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 2100 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 2100.

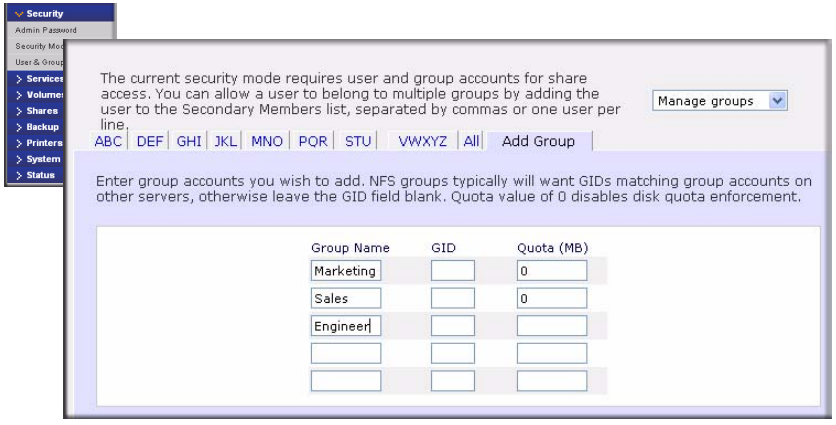


Figure 3-4

Managing Groups

To add a new group:

1. Select **Manage Groups** from the drop-down menu in the upper right corner.

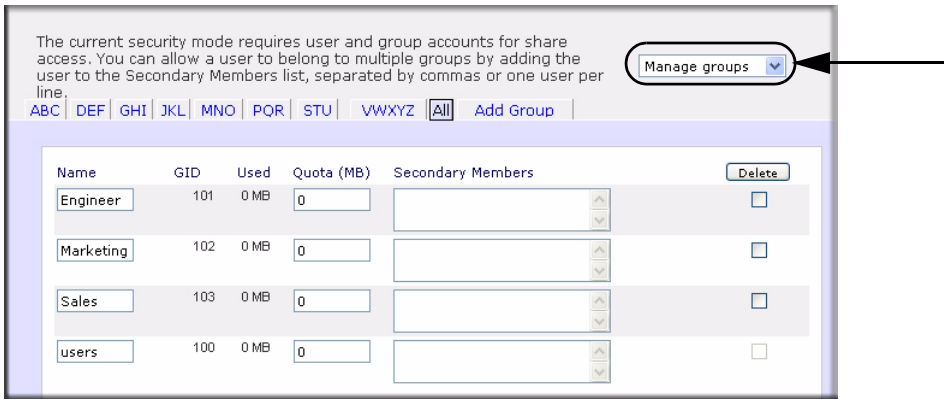


Figure 3-5

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.

You can view or change your groups by clicking the alphabetical index tab, or click **All** to list all groups. If you wish to add a large number of groups, select **Import group list** from the pull-down menu, and browse to locate the file containing the group list. 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.

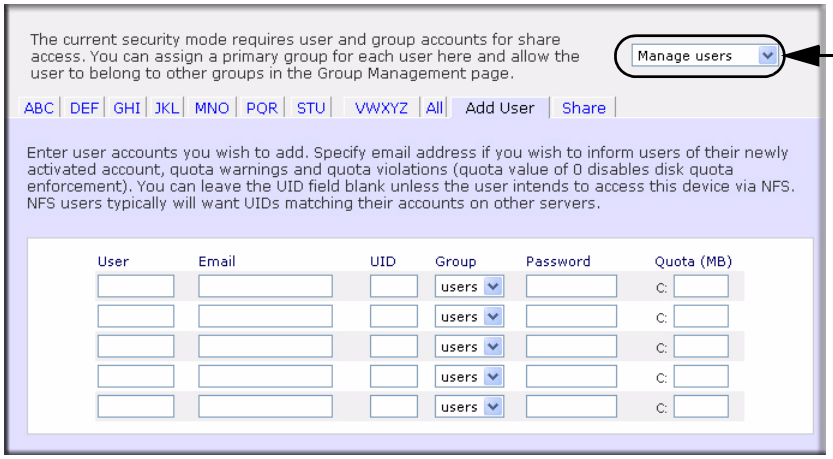


Figure 3-6

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.

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 and browse to locate the file containing the group list. 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.

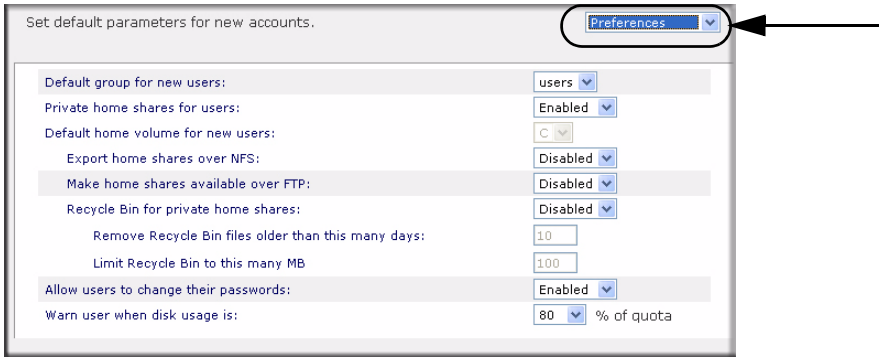


Figure 3-7

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.

Figure 3-8

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.

Managing Shares

Shares enable you to organize the information stored on a volume, and administer who has access to that information. For example, generic policies and forms like blank expense reports everyone should be able to access, compared with sensitive data like financial information only the finance group should be able to access.

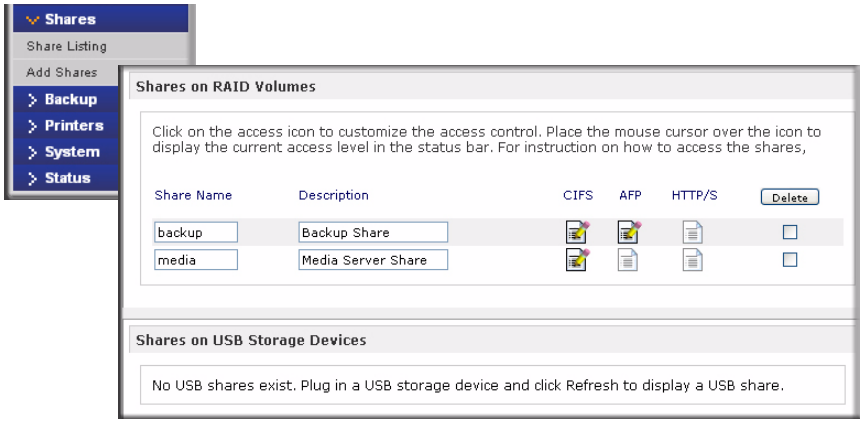


Figure 3-9

The Shares menu provides all the options pertaining to share services for the ReadyNAS 2100 device. This entails share management (including data and print shares), volume management, and share service management.

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. Enter the share name and description.

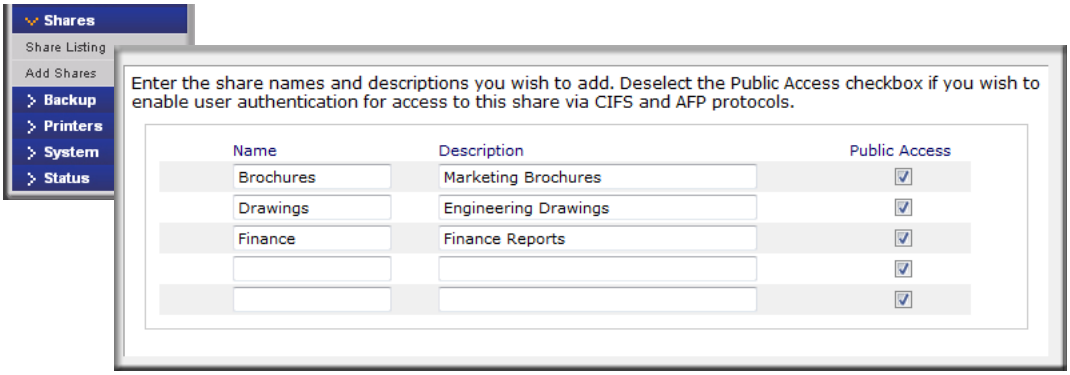


Figure 3-10

	Note: Enabling Public Access means the Guest account has access to the share.

Once you finish adding the shares, refer to Appendix B, “Share Access from MAC and Linux Systems”” 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.

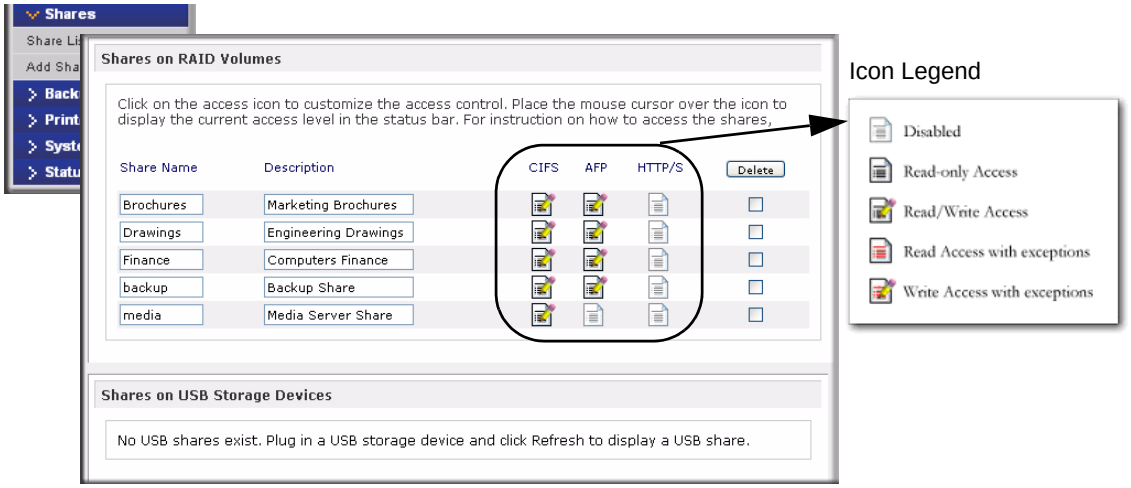


Figure 3-11

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.

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.

To delete a share, select the check box on the far right of the share listing and click **Delete**.

Setting Share Access

Access the CIFS Share Access Restrictions screen by clicking on the file system icon.

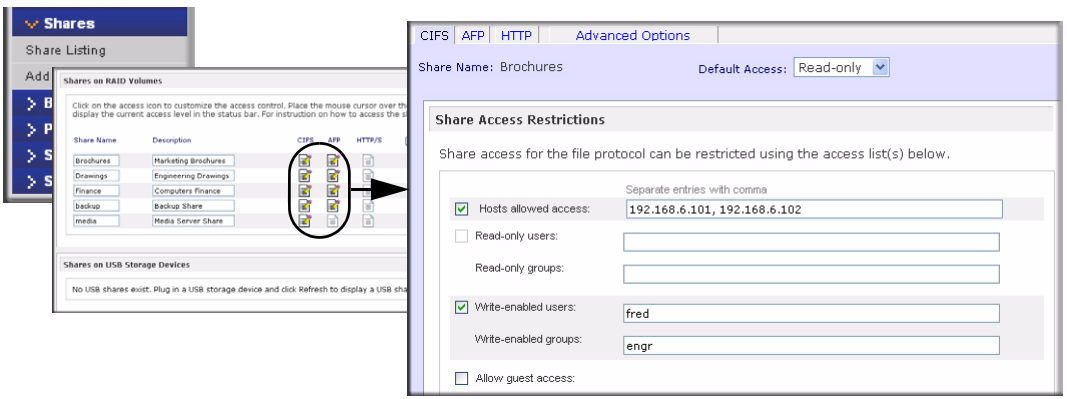


Figure 3-12

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 network storage or on the domain controller. Note that access control differs slightly from service to service.

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**

If you wish to grant guests access to this share, check the **Allow guest access** checkbox.

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.

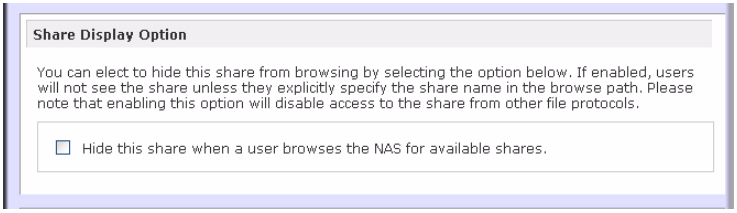


Figure 3-13

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.

Recycle Bin. The ReadyNAS 2100 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.

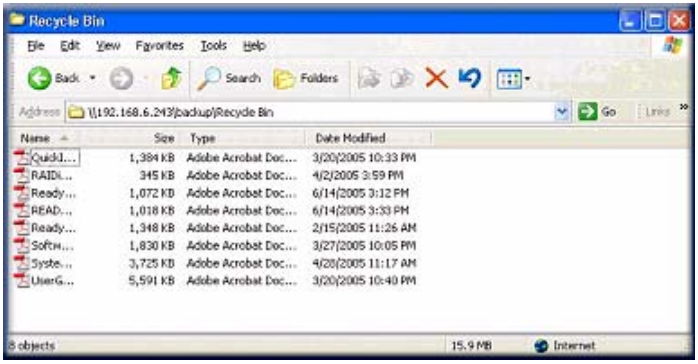


Figure 3-14

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.

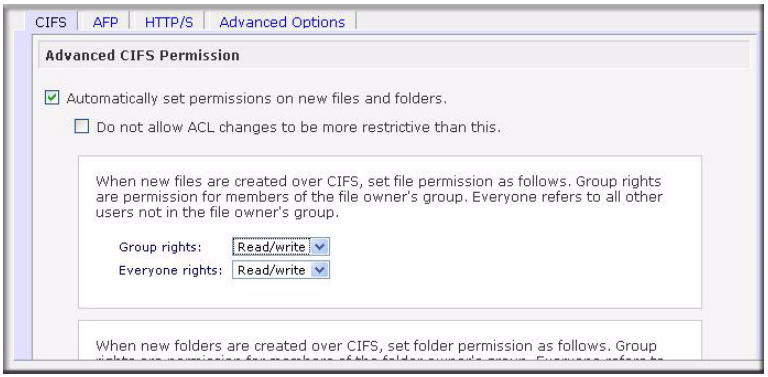


Figure 3-15

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.

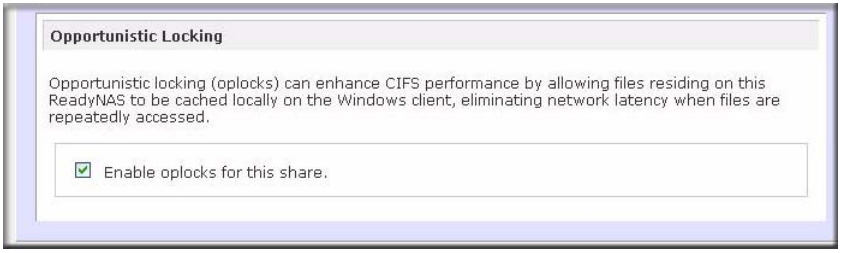


Figure 3-16

Advanced Options

The Advanced Options tab offers advanced low-level file manipulation options that can affect 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.

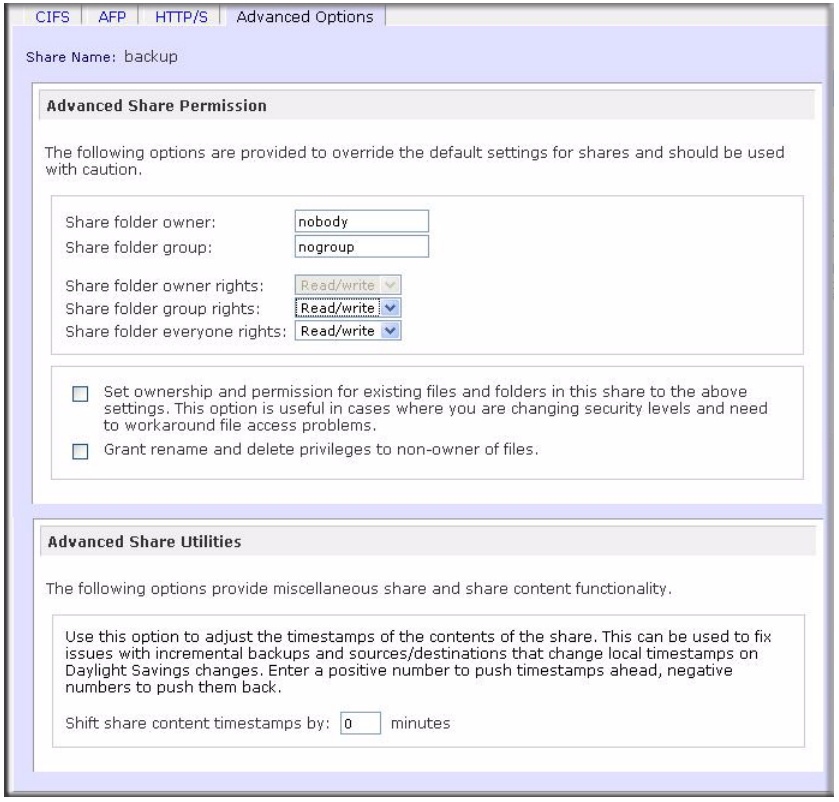


Figure 3-17

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, disable this option.

Share Access from a 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.

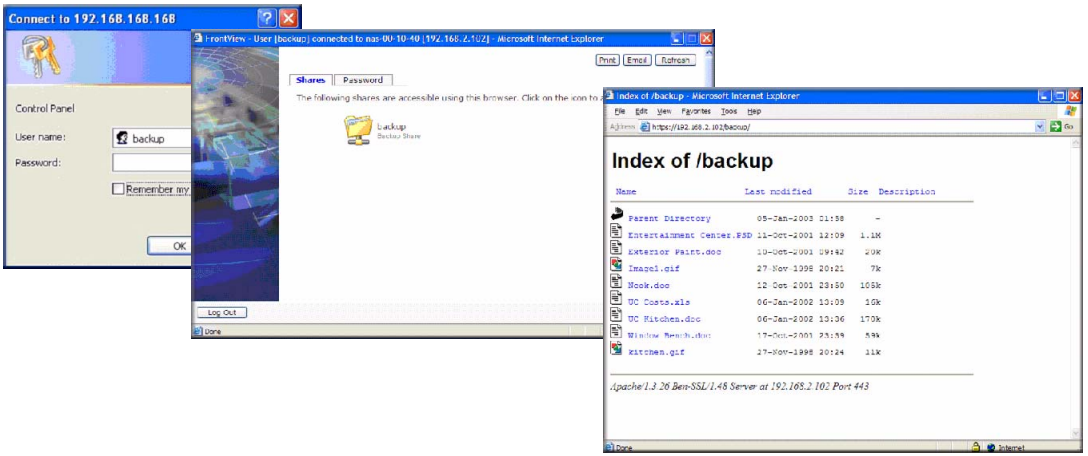


Figure 3-18

Log in with a valid user name and password. If the Share access is read-only, only the file manager displays. If the Share is also writable, the file manager displays options for creating, modifying, and deleting files, as follows.

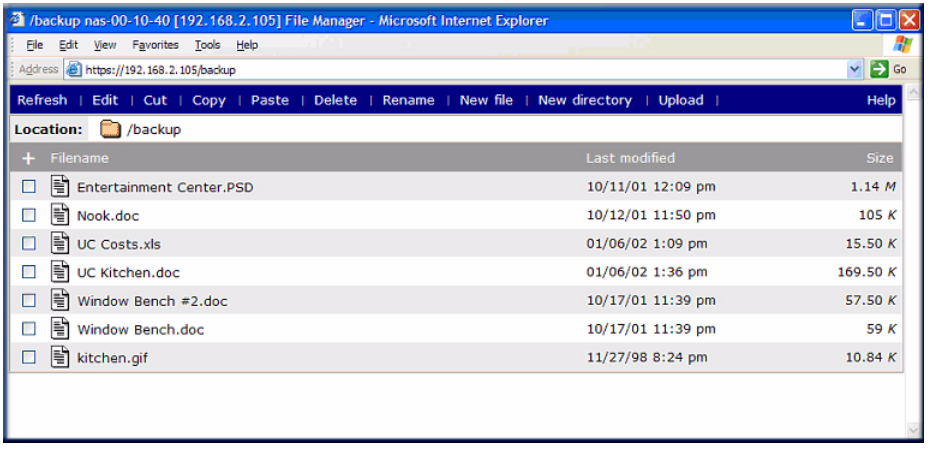


Figure 3-19

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 when accessed via HTTP/S through a browser. The only exception is for the admin user. The admin user can change or delete any files created over the web via any protocol. 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.

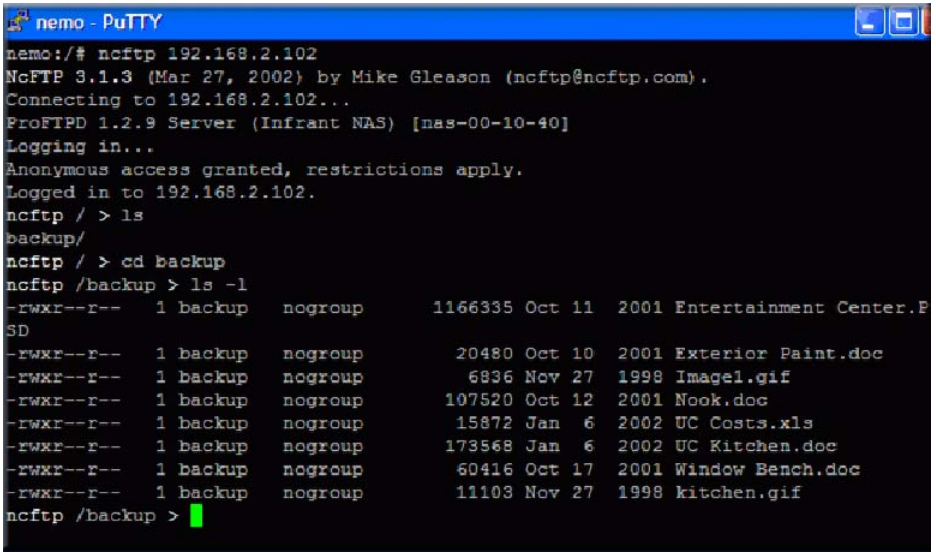


Figure 3-20

To access the share, 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.

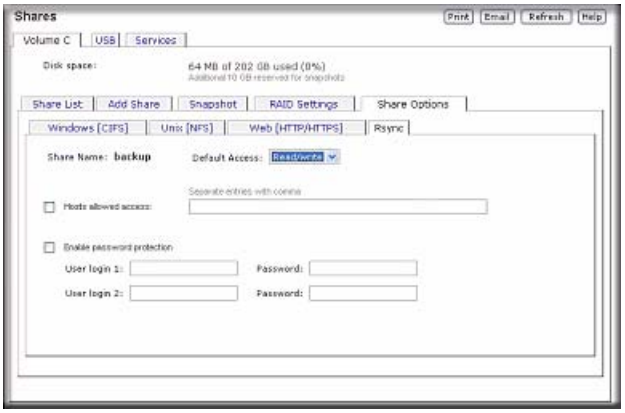


Figure 3-21

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: ***

Remote Access

You can remotely access your ReadyNAS 2100 from the Internet via the ReadyNAS remote feature, or via the FTP and HTTP protocols. This section provides instructions for enabling remote access to your ReadyNAS 2100.

ReadyNAS Remote

ReadyNAS Remote is a web based service that enables drag & drop file transfers from the Windows File Explorer or the Mac Finder over CIFS/SMB. All file permissions and share security settings are retained as if you were on the LAN. All data are transmitted securely over an encrypted tunnel. The setup and use of ReadyNAS Remote is intuitively easy.

Follow these steps to enable ReadyNAS Remote:

1. Install the ReadyNAS Remote client software for Mac or PC. The PC screens are shown below but the Mac steps are nearly identical.

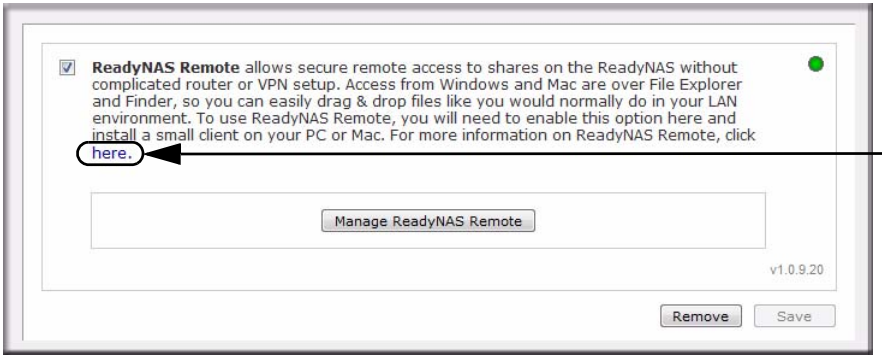


Figure 3-22

a. Log in to FrontView and go to > **Services** > **ReadyNAS Remote**.

b. Click the "*here*" link (http://www.readynas.com/?p=1435) to download the client software from ReadyNAS.com and view the setup tutorial.

c. Install the ReadyNAS Remote client software.

	Note: Desktop firewall software can block the ReadyNAS Remote client. If the PC or Mac is running firewall software like Norton, Zone Alarm, or Kaspersky, you will need to configure your desktop firewall to give permission to the ReadyNAS Remote client software.

2. Click the link in the ReadyNAS Remote client software to create a ReadyNAS Remote account.A popup notice displays upon successful registration with the ReadyNAS Remote web service.

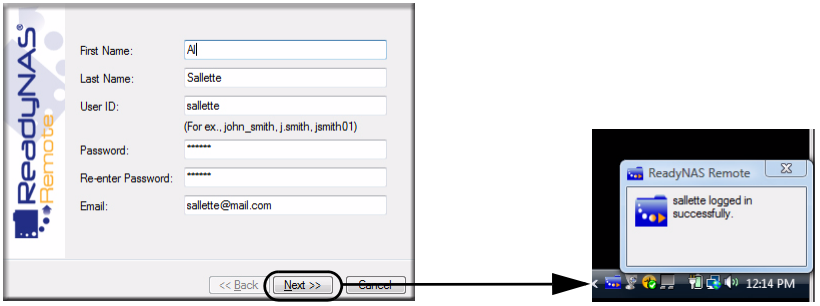


Figure 3-23

3. Use FrontView to enable the ReadyNAS Remote feature, and identify the ReadyNAS Remote accounts that you will permit to access your ReadyNAS shares.

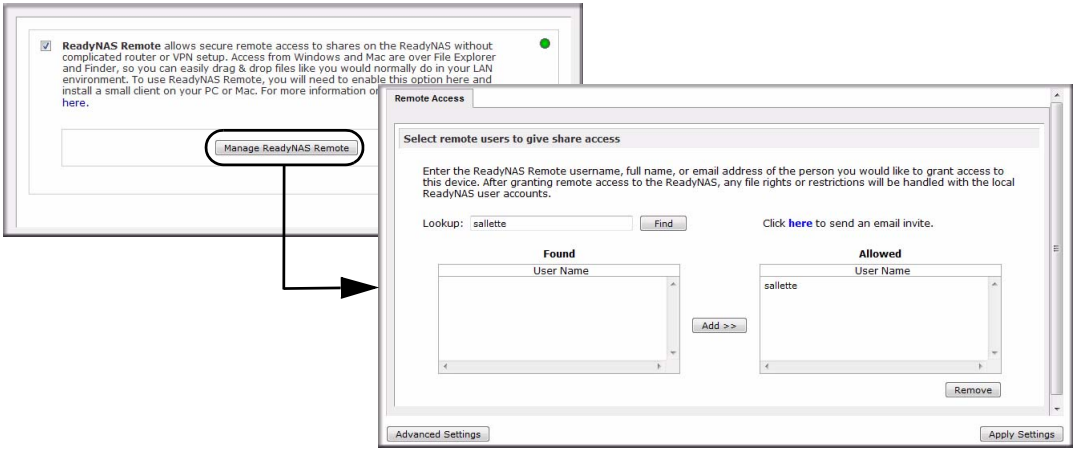


Figure 3-24

4. Use the ReadyNAS Remote client to log in to the ReadyNAS.

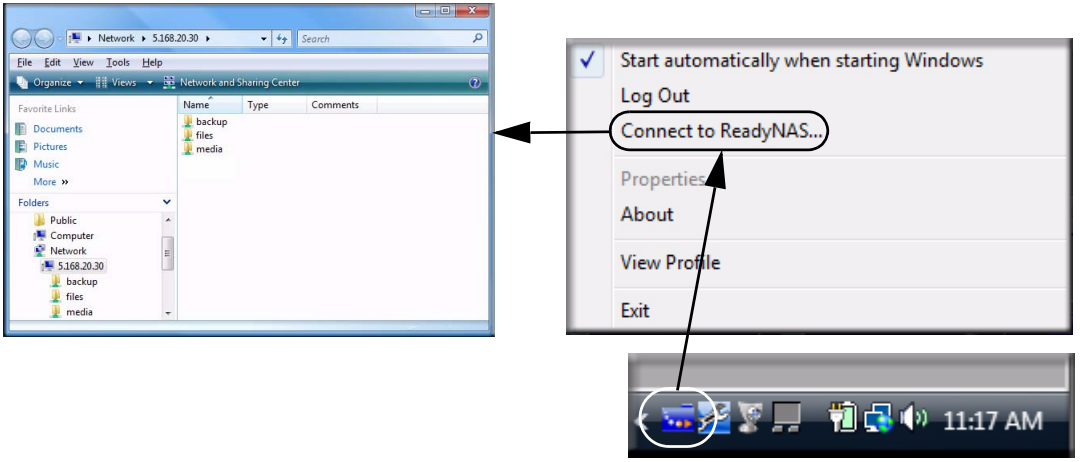


Figure 3-25

You can now drag and drop files between your desktop and the ReadyNAS as though you were on the ReadyNAS LAN.

Remote FTP Access

1. Go to **Services** > **Standard File Protocols** and enable FTP.

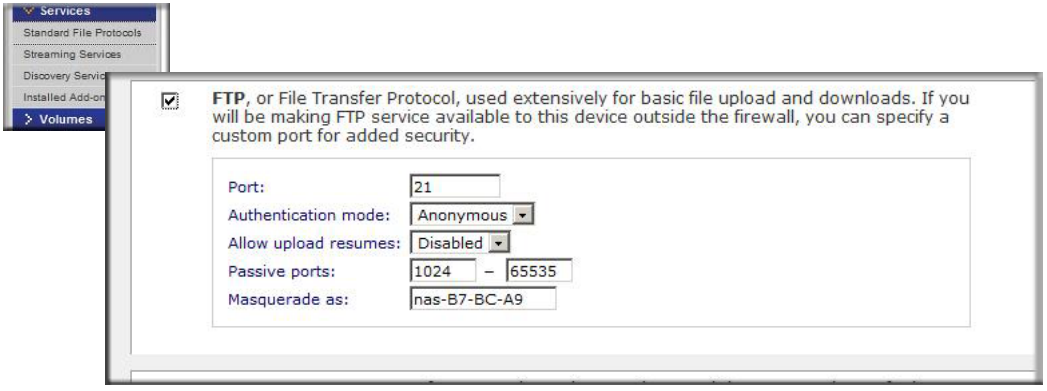


Figure 3-26

- **Port**: The TCP/IP port that the FTP service will be using.

> **Note:** The default is 21, this port will need to be forwarded through the router. Refer to the port forwarding instructions provided with your router.

- **Authentication mode**: There are two authentication modes:
  - **Anonymous**: No login information required for FTP users.
  - **User**: Users will need an account configured on the ReadyNAS from either user or domain security mode.
- **Allow upload resumes**: This option allows users to finish uploading a file to the FTP share if the connection had been previously interrupted. Without this option enabled, if the connection is dropped at 50% completion, the file upload must restart from the beginning.
- **Passive ports**: This port range is required to enable remote access to the ReadyNAS from over the Internet. This port range should be adjusted to the maximum number of concurrent sessions the user expects to run at one time. If you expect frequent concurrent access from many users, double this number, as each FTP user will consume a passive port.
- **Masquerade as**: This field is for adjusting the hostname that the FTP server reports to an FTP client.

2. Configure the FTP share access options.

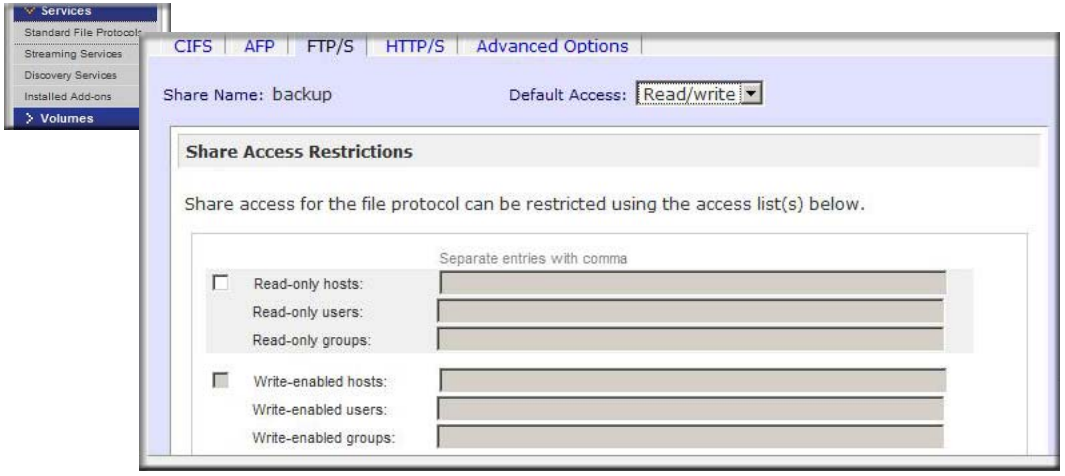


Figure 3-27

Change the Share Access Restrictions to allow FTP access to the share according to the user permissions you require.

Remote HTTP Access

1. Go to **Services** > **Standard File Protocols** and enable FTP.

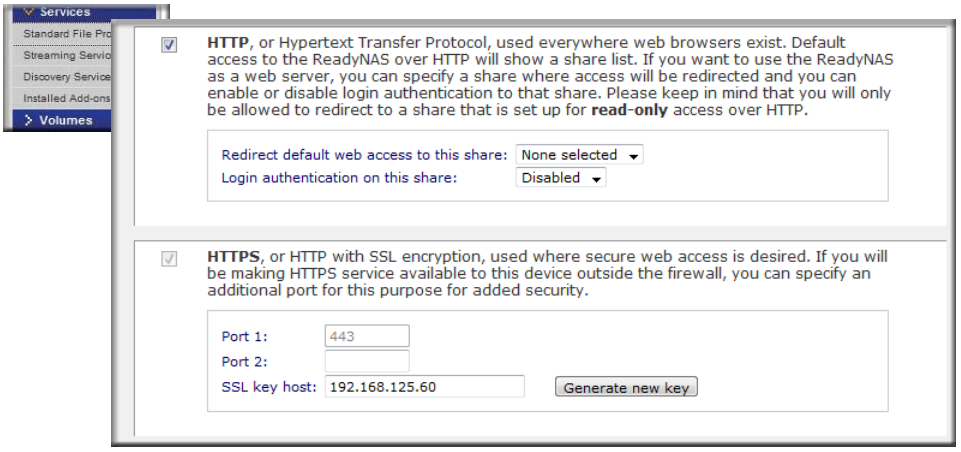


Figure 3-28

	Note: HTTPS cannot be disabled - Frontview requires it.

- **HTTP**
  - Redirect default web access to this share: Advanced configuration option allowing hosting of user created HTTP web page on the ReadyNAS.
  - Login authentication on this share: Configures the above mentioned share for whether or not authentication is required if users are browsing to the user created web content
- **HTTPS**
  - **Port 1**: This field cannot be modified; it is reserved for the ReadyNAS.
  - **Port 2**: This field can be used to allow https connections over a port other than the standard 443.

	Note: Changing the default https port will require enabling port forwarding of the port you choose on the router. Refer to the port forwarding instructions provided with your router.

– **SSL key host**: This field lets you configure the hostname used for the ReadyNAS to generate its SSL certificate, and then create a new SSL certificate. It is advised users update this field to match the current IP address of the ReadyNAS and then generate a new SSL certificate to avoid future certificate errors from their web browser.

	Note: In this scenario, it is best to have a fixed IP configuration for the ReadyNAS so that the certificate will remain valid. Also, if the WAN IP address configuration is DHCP, then it is advisable to use a Dynamic DNS service to access the ReadyNAS via a persistent fully qualified domain name a DDNS service provides rather than via an IP address.

2. Configure the HTTP/S share access options.

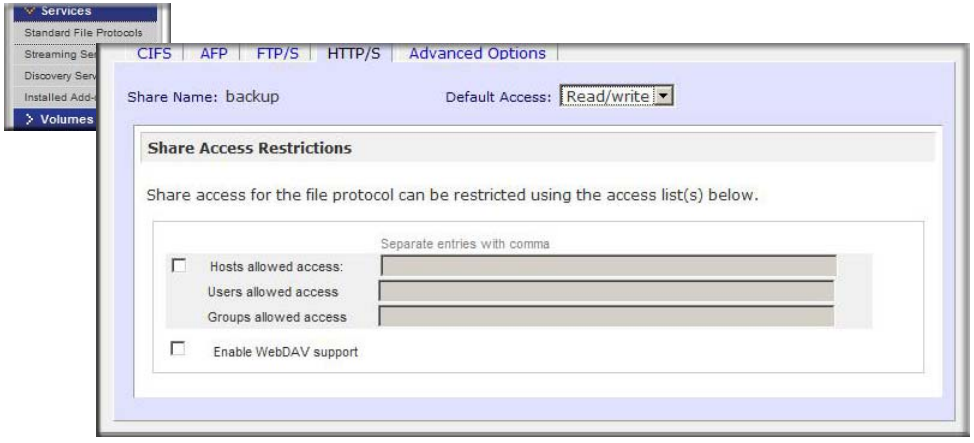


Figure 3-29

Change the Share Access Restrictions to allow HTTP access to the share according to the user permissions you require.

3. **Enable WebDAV support**: WebDAV is an HTTP connection method that can allow drag and drop file transfers similar to what users may experience with their standard Windows or Mac OSX computer. See ReadyNAS.com for a how-to explanation of how to set up WebDAV: *http://www.readynas.com/?p=126*

Chapter 4
Securing Your Data

This chapter explains how to back up the data from your ReadyNAS.

- "Configuring Backup Jobs"
- "MAC OS X Time Machine Backup"
- "Snapshots"
- "Backing Up the ReadyNAS to a USB Drive"
- "Back Up to the Web with the ReadyNAS Vault Service"

Configuring Backup Jobs

The Backup Manager integrated with the ReadyNAS 2100 allows the ReadyNAS 2100 to act as a powerful backup appliance. Backup tasks can be controlled directly from the ReadyNAS 2100 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 2100 can act as a simple central repository for both home and office environments. And with multiple ReadyNAS 2100 systems, you can set up one ReadyNAS 2100 to back up another directly.

Adding a New Backup Job

The backup source can be located remotely, it can be a public or a private home share, it can be an iSCSI individually addressable (logical) SCSI device (a logical unit number or LUN), or it can be all home shares on the ReadyNAS 2100.

To create a new backup job, select **Add a New Backup Job** and follow the 4-step procedure.

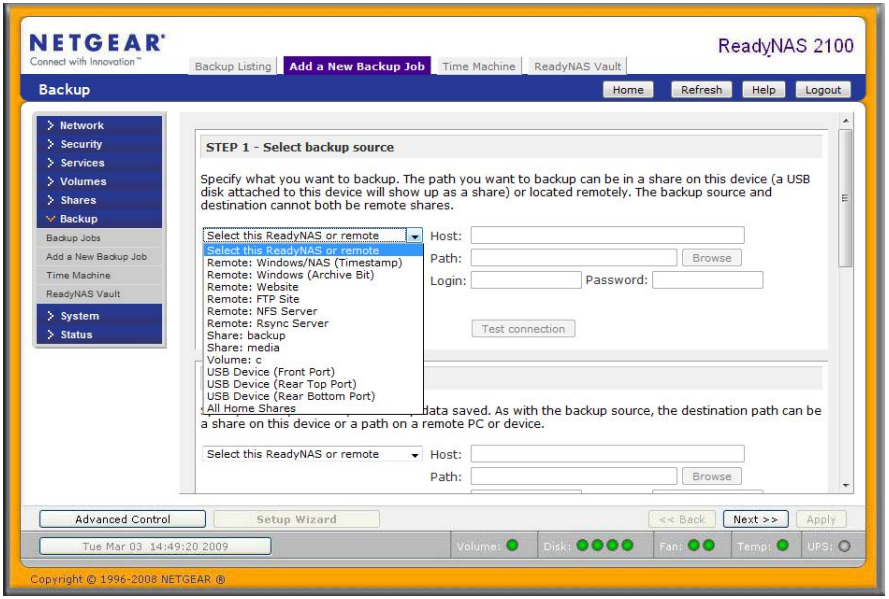


Figure 4-1

Step 1 – Select Backup Source

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:

- **iSCSI**. Select this if you wish to back up an iSCSI LUN.
- **Remote 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.
- **Remote 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.
- **Remote 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.
- **Remote FTP site**. Select this if you wish to back up an FTP site or a path from that site.
- **Remote 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.

- **Remote 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.
- **Share**. Select this if you wish to back up a ReadyNAS share.
- **Volume**. Select this if you wish to back up an entire volume which includes all shares on it.
- **USB Device.** Select this if you wish to back up a USB connected drive. Choose where the device is connected.
  - — Rear Top Port
  - — Rear Bottom Port
- **All Home Shares**. Select this if you wish to back up all private home shares on the ReadyNAS.

Once you have selected a backup source, you can enter the path from that source. If you selected a ReadyNAS 2100 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:

Note: Depending on the operating system you are working with, observe the correct backslash (forwarded or backward) accordingly.

- 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 Rsync path over an ssh link:

  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 2100 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 2100 (either the source or destination must be local to the ReadyNAS 2100). If you selected a ReadyNAS 2100 share for the source, you can either enter another local ReadyNAS 2100 share for the destination, or you can specify a remote backup destination.

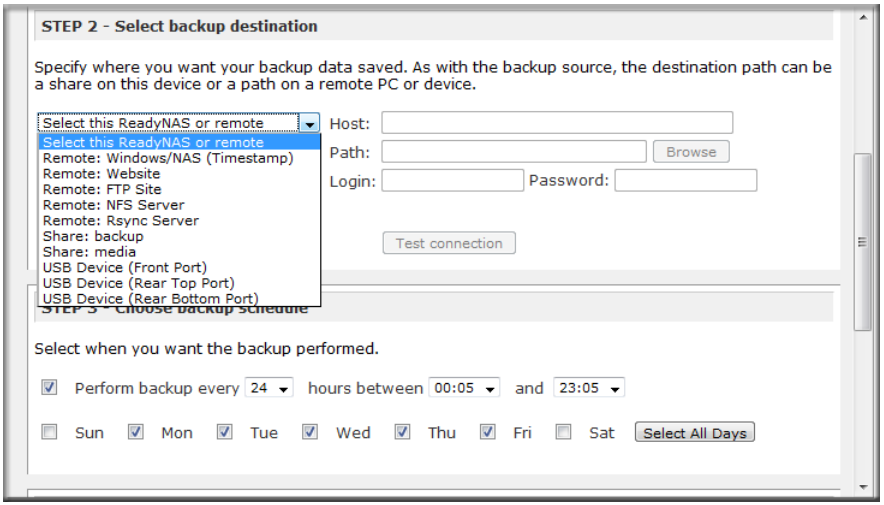


Figure 4-2

The remote backup destination can be any of the items on the list, including an iSCSI LUN, a Remote Windows PC/ReadyNAS 2100 system, Remote Website, a Remote FTP site, a Remote NFS Server, a Remote Rsync server, a ReadyNAS Share, or a USB Device (Front, Back Top or Bottom). Note that you can select **rsync** for a remote ReadyNAS 2100 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 4-9 to set up a snapshot schedule).

	Note: Backup jobs cannot go past midnight to the next day. Set a backup job start stop time that does not traverse midnight.

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.)

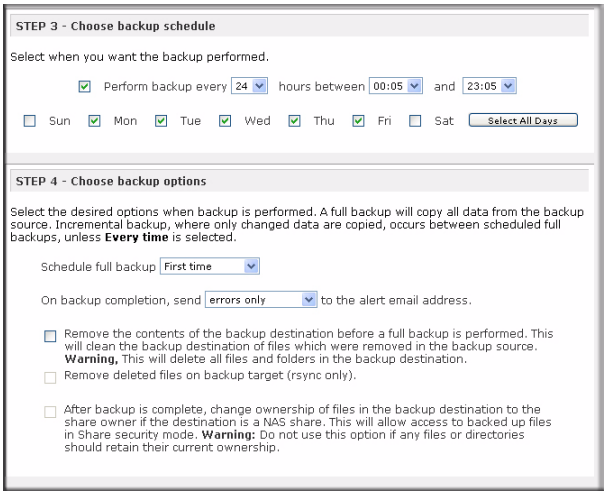


Figure 4-3

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.

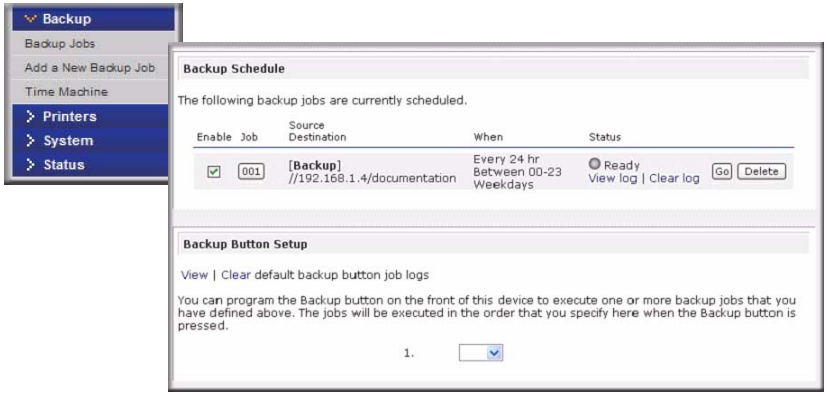


Figure 4-4

A summary of scheduled backup jobs displays; 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 clear the current log detail.

Programming the Backup Button

You can program the backup button (see the illustration at page 1-2) to execute one or more pre-defined backup jobs.

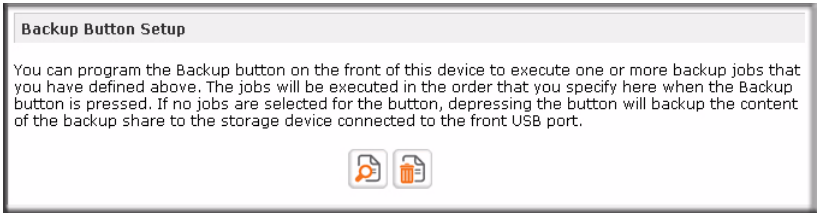


Figure 4-5

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.

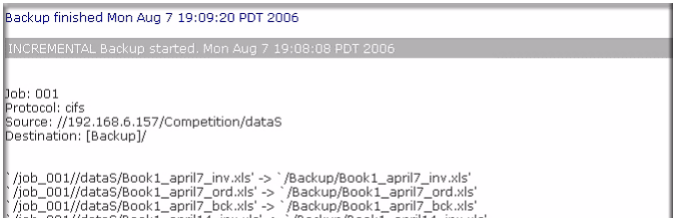


Figure 4-6

The log format might differ depending on the backup 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.

MAC OS X Time Machine Backup

The ReadyNAS can be used as a backup destination for your OS X Time Machine. After enabling the Time Machine option, use the “Change Disk...” option from Time Machine Preferences to select this ReadyNAS. You will need to enter the user name and password specified in the ReadyNAS when prompted by the MAC for authentication.

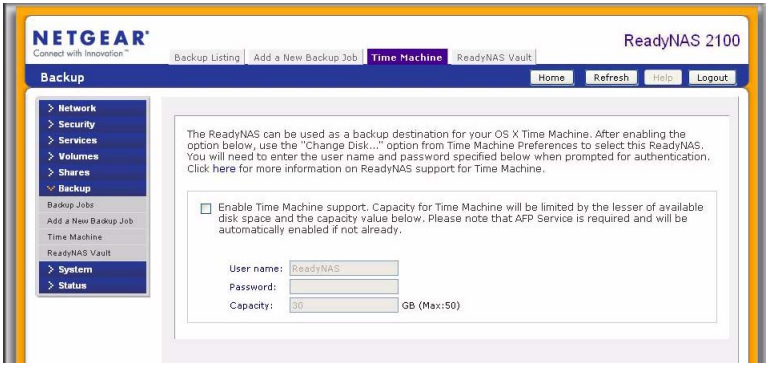


Figure 4-7

Go to *http://www.readynas.com/TimeMachine* for more information on ReadyNAS support for Time Machine.

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 panel on the Volume tab page. 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 2100 ships with a snapshot reserved space of 10 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, it replaces the previous one.

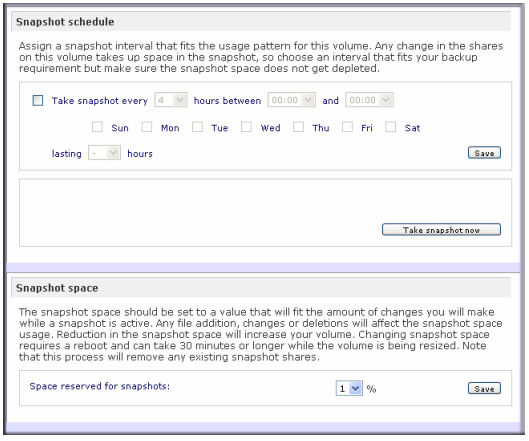


Figure 4-8

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

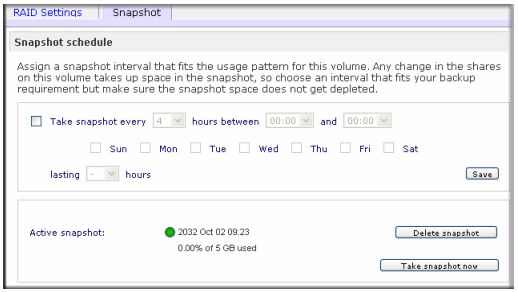


Figure 4-9

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 2100, 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**.

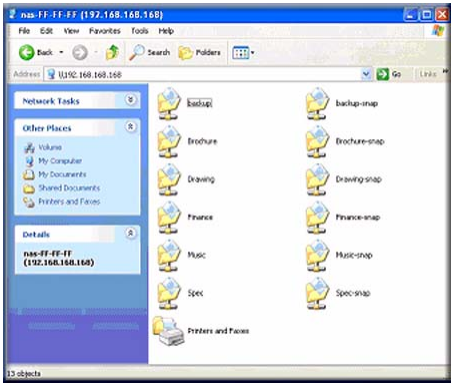


Figure 4-10

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.

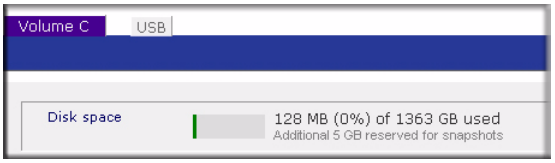


Figure 4-11

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 a percentage of your volume capacity.

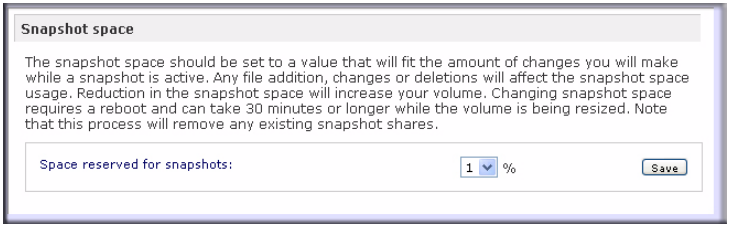


Figure 4-12

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.

Backing Up the ReadyNAS to a USB Drive

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

On the ReadyNAS 2100, 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. Be mindful of performance impact to users when backup jobs are run.

You can program backups for 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.

Back Up to the Web with the ReadyNAS Vault Service

ReadyNAS Vault allows continuous and scheduled backups of your ReadyNAS data to a secure online Vault. For convenience, the backup data can be managed and accessed wherever you have Internet access.

To enable the ReadyNAS Vault service, click the link on the ReadyNAS Vault tab page in FrontView or follow the instructions at *http://www.readynas.com/vault*.

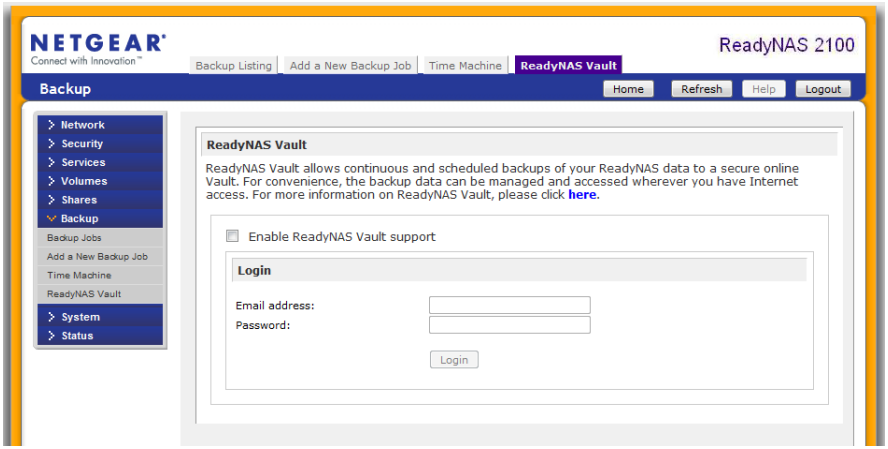


Figure 4-13

Chapter 5
Optimizing Performance and Maintaining the System

This chapter includes topics on system status, alerts, replacing failed disks, and scheduling.

- "Optimizing Performance"
- "Power Management"
- "Viewing System Status"
- "Control Panel Status and Diagnostic Information"
- "Using the System Diagnostic Boot Menu"

Optimizing Performance

If you wish to tweak the system performance, select System > Performance from the main menu.

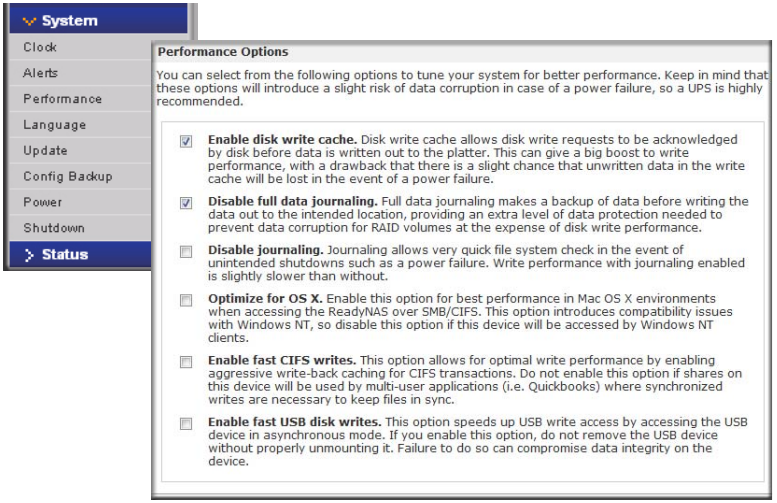


Figure 5-1

Note that some of the settings suggest that you utilize an Uninterruptible Power Supply (UPS) before enabling that option:

- Select the **Disable 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.
- Select **Enable disk write cache** if you want to allow disk write requests to be acknowledged by the disk before data is written out to the platter. This can give a big boost to write performance, with a drawback that there is a slight chance that unwritten data in the write cache will be lost in the event of a power failure.
- 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.
- The **Optimize for OS X** option provides the best performance in Mac OS X environments when connected to the ReadyNAS 2100 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 speeds 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 **Enable fast USB disk writes** 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 dismounting it. Failure to do so can compromise data integrity on the device.

Adding a UPS

Adding a UPS to the NAS is an easy way to protect against power failures. Simply connect the ReadyNAS power cable to the UPS, and connect the UPS USB monitoring cable between the UPS and the ReadyNAS. The UPS is detected automatically and shows up in the Status bar. Move the mouse pointer over the status light to display device information, or click a status light to display the status in more detail. You can move the mouse pointer over the UPS LED icon to display the current UPS information and battery life.

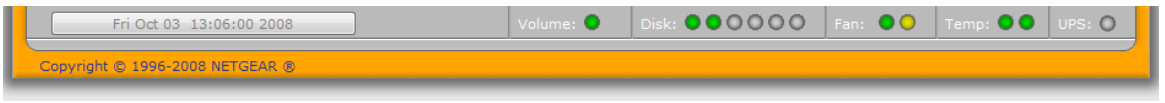


Figure 5-2

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.

Power Management

The ReadyNAS 2100 offers disk spin-down, power timer (time off/time on), UPS event, and wake-on-LAN 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.

	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 using a UPS if you use this option.

To enable spin-down mode, select the **Enable disk spin-down after...** check box, and specify the minutes of inactivity before spin up.

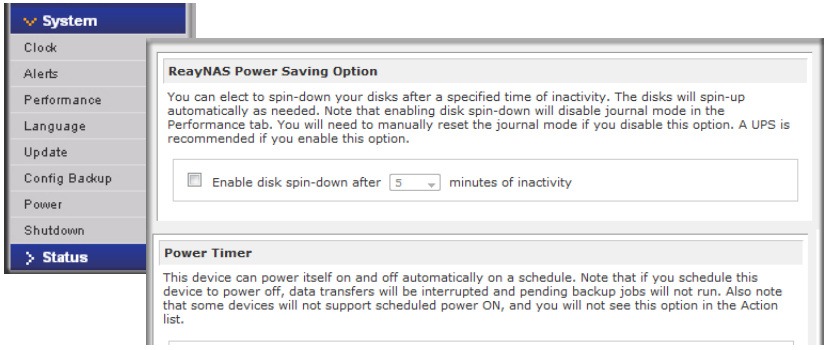


Figure 5-3

Power Timer

The ReadyNAS 2100 can be scheduled to power off and power back on (on certain models) automatically (see Figure 5-3). Select the **Enable power timer** check box and enter the action and time. (The **Power ON** option is available on the ReadyNAS 2100 NV through an add-on package.)[1] The **Power ON** option does not appear if the ReadyNAS 2100 hardware does not support this feature.

Note: When the ReadyNAS 2100 is powered off, any file transfers and backup jobs are interrupted, and backup jobs scheduled during the power off state do not run.

Configuring UPS Battery Low Shutdown

If this device is not connected to a UPS device, you may elect to enable a UPS connection to another NAS device. Select the **Enable monitoring of UPS physically attached to a remote ReadyNAS** 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.*

Wake-On-LAN

You can power-on this device remotely by sending it a “WOL Magic Packet” if the WOL service is enabled.

Note: The ReadyNAS 2100 supports Wake-On-LAN on the first Ethernet interface (LAN 1) only.

1. Please refer to the Release Notes for RAIDiator 4 on the NETGEAR Support site for more information.

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.

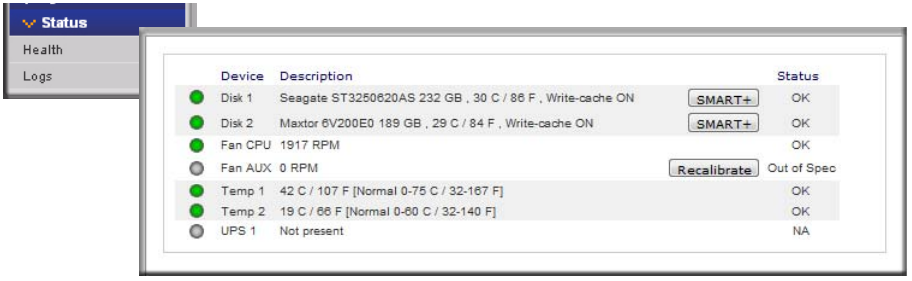


Figure 5-4

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

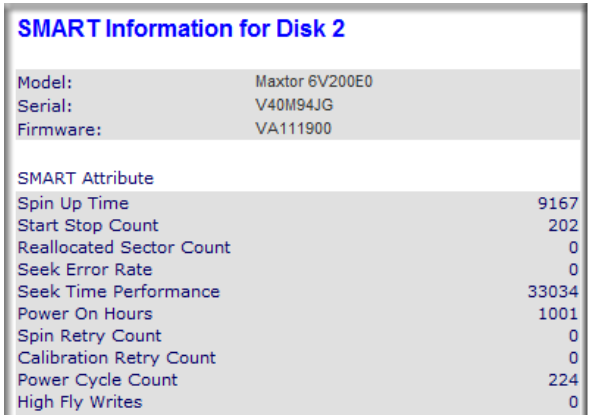


Figure 5-5

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.

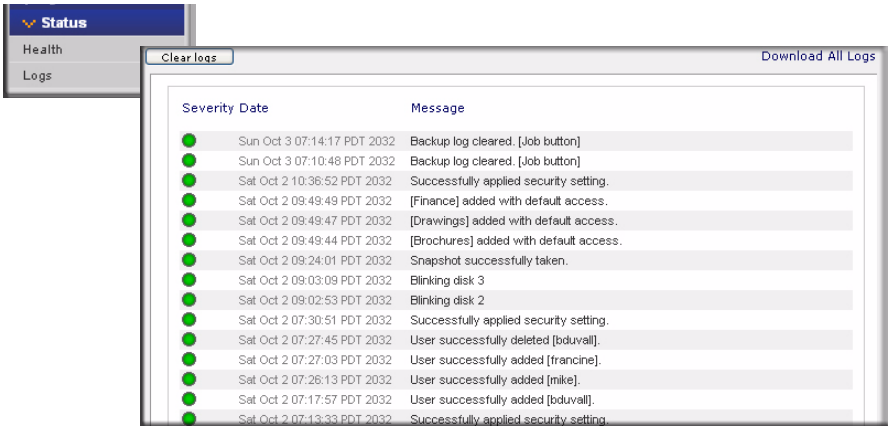


Figure 5-6

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.

Control Panel Status and Diagnostic Information

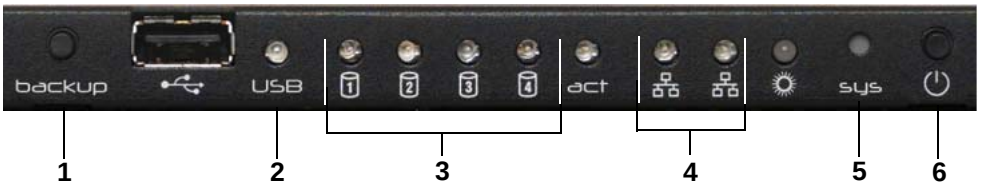


Figure 5-7

The function of each Control Panel item is described in the following table:

Table 5-1. LED Descriptions

Item	Activity	Description
1. Backup Button.	Push button	Backup: Push to initiate FrontView scheduled backup jobs. Diagnostics: Toggles between boot menu options (see SYS Reset below). Boot Sequence: Press to initiate boot from external USB.
2. USB Status LED.	On (Green) Blinking (Green) Off	On: A USB device is mounted. Blink: USB device dismounting *or* scheduled backup running. Off: USB device dismounted. See SYS Reset below for other boot codes.
3. Disk LEDs.	On (Green) Blink (Green) Off	LEDs • On green: Disk installed. • Blinking in unison: Power button pressed once; press the power button a second time to initiate a graceful shutdown. • Blink: Disk resynching *or* disk failure. • "Marching" LEDs: Volume expansion in progress. • Off: No disk installed Diagnostic LED indicators: • 1 & 2 stay on if boot memory test fails. • 1 & 3 stay on if device cannot boot. • Alternating between all Disk LEDs on and only Disk 2 LED on means no disk detected. • Alternating between all Disk LEDs on and only Disks 1 & 2 LEDs on means boot failure, possible corrupted root. • See SYS Button below for other boot codes.
4. LAN1 and LAN2 Ports.	On (Green) Off	On: The LAN port is linked. Off: The LAN port is disconnected.

Table 5-1. LED Descriptions (continued)

<table>
<tr><th>Item</th><th>Activity</th><th>Description</th></tr>
<tr><td>5. SYS Button. </td><td colspan="2">Diagnostics: To enter the diagnostic boot menu, press and hold the SYS button while powering the unit on. Keep pressing until all LEDs except the Disk ACT are on.
<table>
<tr><th rowspan="2">Boot Menu Options</th><th rowspan="2">USB LED</th><th colspan="4">Disk LED</th></tr>
<tr><th>1</th><th>2</th><th>3</th><th>4</th></tr>
<tr><td>Boot menu enabled</td><td>On</td><td>On</td><td>On</td><td>On</td><td>On</td></tr>
<tr><td>1. Normal boot</td><td>Off</td><td>On</td><td>Off</td><td>Off</td><td>Off</td></tr>
<tr><td>2. Factory default</td><td>Off</td><td>Off</td><td>On</td><td>Off</td><td>Off</td></tr>
<tr><td>3. OS Reinstall</td><td>Off</td><td>Off</td><td>Off</td><td>On</td><td>Off</td></tr>
<tr><td>4. Tech Support</td><td>Off</td><td>Off</td><td>Off</td><td>Off</td><td>On</td></tr>
<tr><td>5. Skip Volume Check</td><td>On</td><td>Off</td><td>Off</td><td>Off</td><td>Off</td></tr>
<tr><td>6. Memory Test</td><td>On</td><td>On</td><td>Off</td><td>Off</td><td>Off</td></tr>
<tr><td>7. Factory Test</td><td>On</td><td>Off</td><td>On</td><td>Off</td><td>Off</td></tr>
</table></td></tr>
<tr><td>8. Power Button. and LED </td><td>Push button

On (Blue)
Blinking
Off</td><td>Power button actions:
• Press once: Power the system on.
• Press twice - preferred shutdown: When the system is running, initiate preferred shutdown. After the first press, the system blinks all the LEDs in unison (including the power LED). After the second button press, the system initiates the shutdown. Doing nothing while all the LEDs are blinking in unison will let the system resume operating.
• Press and hold - forced shutdown: If the system is hung, press and hold the power button for 5 seconds to force shutdown.
LED
• On (blue): Power is supplied to the system.
• Blinking: The system is booting.
• Off: The system is powered off.</td></tr>
</table>

Shutdown

The Shutdown Options screen offers the option to either power off or reboot the ReadyNAS 2100 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.

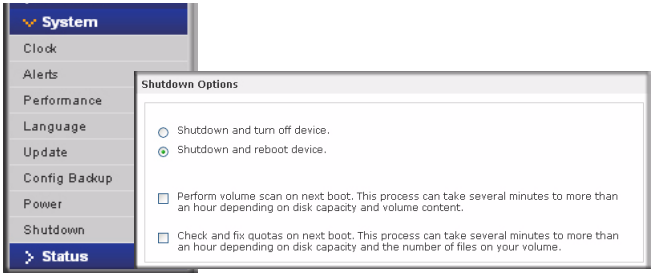


Figure 5-8

When you reboot or shut down the ReadyNAS 2100, you must close the browser window and use RAIDar to reconnect to FrontView.

Replacing a Failed Disk

	Note: Be sure to check the Hardware Compatibility list on the NETGEAR support site for a list of disks that have been qualified for the ReadyNAS 2100 to assure that you use a suitable 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.

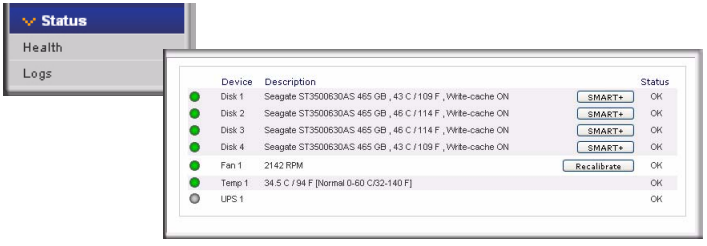


Figure 5-9

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.

Choosing a Replacement Disk

On the main menu, select Status > Health. Take note of the disk vendor and model used in your ReadyNAS. 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

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

To replace the disk:

1. View the disk status lights to identify which disk has failed.
2. If necessary, unlock the tray lock by moving it to the right, then press the release of the failed disk. The latch pops out.

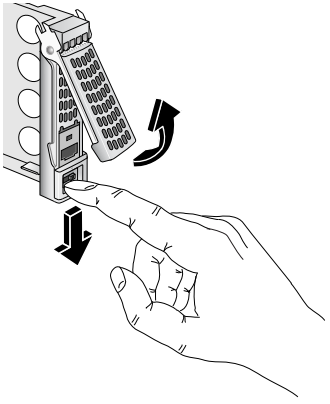


Figure 5-10

3. Pull out the disk tray, remove the screws, and replace the failed disk.

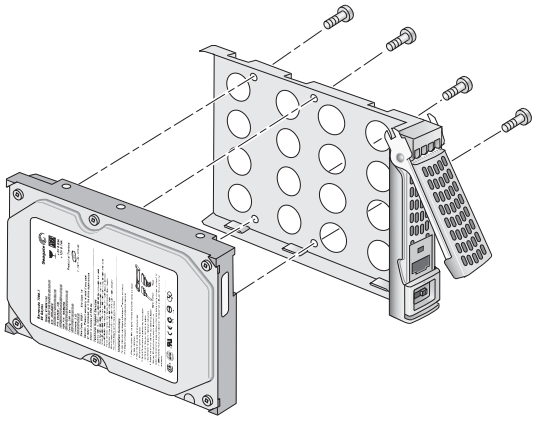


Figure 5-11

4. Reassemble the disk tray. Make sure that the hard disk connectors face the interior of the disk bay when you reassemble the disk.

5. If you want to prevent easy removal of the disk from the drive bay, set the tray lock.

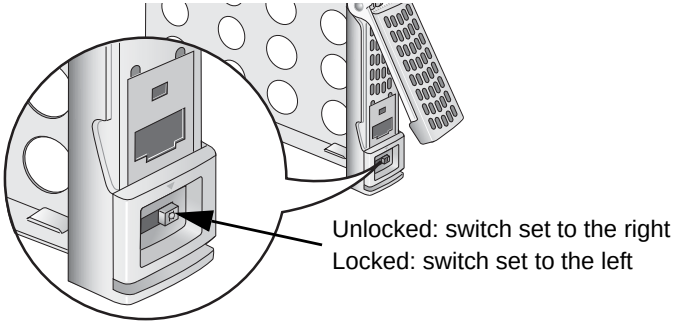


Figure 5-12

6. Slide the disk tray back in to the unit and secure the latch.

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.

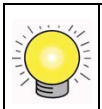
Using the System Diagnostic Boot Menu

The recessed reset switch allows you to perform six functions (see the table *"Control Panel Status and Diagnostic Information"* on page 5-7):

1. **Normal**: Bypass the diagnostic boot menu and perform a normal boot.
2. **Factory Default**: Reset the ReadyNAS back to factory default state, erasing all data on the disks. This option can be used to change between X-RAID2 and Flex-RAID mode.

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

3. **OS Reinstall**: While keeping the data volume in tact, re-install the RAIDiator firmware on the ReadyNAS, reset the admin password and change the DHCP assignment to DHCP client. This is helpful if you have lost your admin password and want to set it back to default, if errors in your network settings has made it impossible to connect to the ReadyNAS, or if you suspect that the operating system on your disk may somehow be corrupt. If you find that a configuration change makes the unit inaccessible, you can use option three to set the unit back to a factory default state.



Tip: If possible, use the configuration backup (see *"Configuration Backup"* on page 2-30) to save your configuration so that if you have to reset the unit to its factory default settings, you can simply restore all your settings from the configuration backup.

4. **Tech Support**: Enable the remote diagnostic function.
5. **Skip Volume Check**: Boot the system but bypass the volume check.
6. **Memory Test**: Perform a memory diagnostic.

Use the OS REINSTALL Option to Re-install the Firmware

To re-install the RAIDiator firmware on the ReadyNAS while leaving the data volume intact, follow these steps.

1. Power off the device.
2. While using a paper clip or push pin to press in the **SYS** switch, power on the unit. Wait for up to 30 seconds for the reset menu on the front to display, then release the reset switch.

Figure 5-13

The LEDs will indicate the boot menu is active.

3. Push the Backup button on the front panel three times to scroll through the menu to the **OS Reinstall** option (USB LED off, Disk 1 LED off, Disk 2 LED off, Disk 3 LED on, Disk 4 LED off).

Off Off Off **On** Off

Figure 5-14

4. Press the **SYS** button once to confirm the menu selection and proceed with that option.

Figure 5-15

The system will reboot reset to the factory default settings.

Using the Boot Menu to Format a RAID Volume

You can switch between the X-RAID2 (Expandable Volume) mode and the Flexible Volume (Flex-RAID 0/1/5 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: Using the Factory Default boot menu option will erase all the data on the hard disks. Do a full backup before using the Factory Default option.

To reconfigure your RAID setup, complete the following steps:

1. Power off the ReadyNAS.
2. While using a paper clip or push pin to press in the **SYS** switch, power on the unit. Wait for up to 30 seconds for the reset menu on the front to display, then release the reset switch.

Figure 5-16

The LEDs will indicate the reset menu is active.

3. Push the **BACKUP** button on the front panel two times to scroll through the menu to the Factory Default option (USB LED off, Disk 1 LED off, Disk 2 LED on, Disk 3 LED off, Disk 4 LED off).

Off Off **On** Off Off

Figure 5-17

4. Press the **SYS** button at the back to confirm the menu selection and proceed to that option.

   The system will reset to the factory default settings, and erase all the data on the disks.

5. Run the RAIDar utility. RAIDar will prompt you to click Setup**.**

Figure 5-18

6. Click **Setup** to display the ReadyNAS Volume Setup screen.

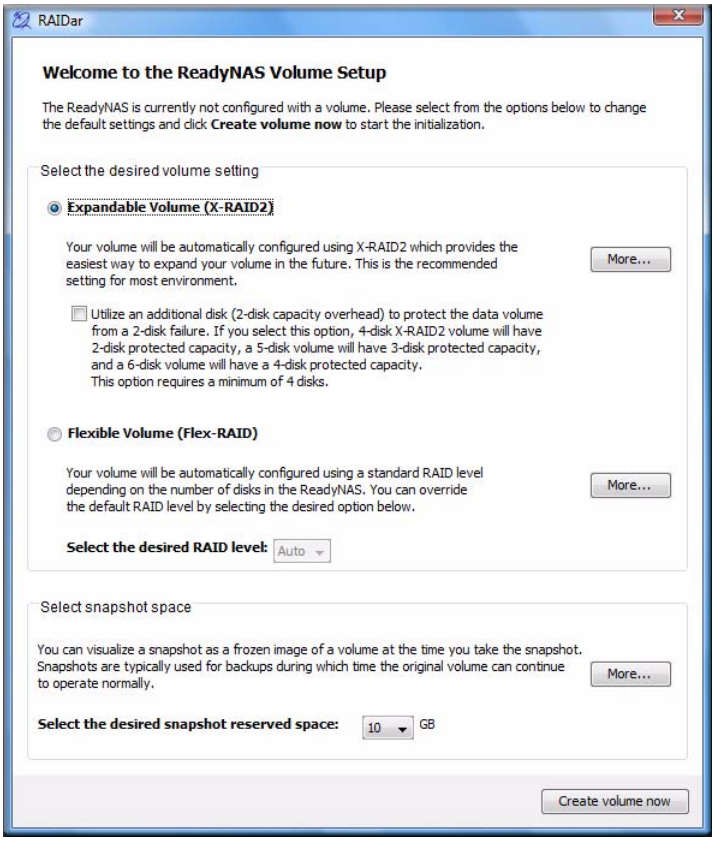


Figure 5-19

7. Select either the **Expandable Volume (X-RAID2)** or the **Flexible Volume (Flex-RAID)** radio button, configure the options accordingly, and click **Create Volume Now.** The volume and initialization process begins.

> **Note:** If no action is taken within 10 minutes, the system defaults to X-RAID2 with 10 GB reserved for snapshots.

RAIDar shows that the system is initializing the volume.

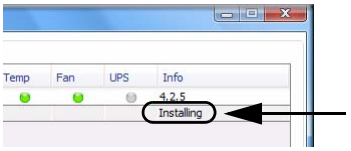


Figure 5-20

The system powers down when the volume initialization completes.

8. Power the system on. It will perform diagnostics while it boots.
9. Click **Rescan** in RAIDar to connect to the system.

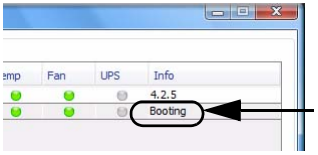


Figure 5-21

RAIDar will find the system and show that it is booting.

10. When RAIDar shows that the system is ready, click **Setup** to log in to FrontView and configure the system.

Appendix A
Default Settings

You can use the reset all settings to their factory defaults, according to the instructions in *"Use the OS REINSTALL Option to Re-install the Firmware"* on page 5-13.

Table A-1. ReadyNAS 2100 Default Configuration Settings

Feature		Default
Login		
	User Login URL when the ReadyNAS 2100 is not connected to a DHCP server	https://192.168.168.168
	Admin User Name (case sensitive)	admin
	Admin Login Password (case sensitive)	netgear1
Management		
	System configuration	FrontView web-based configuration and status monitoring built in to the ReadyNAS Radiator firmware
	Discovery, multi-unit status monitoring, and RAID formatting utility	RAIDar for Windows, Mac, and Linux available from *http:www.readynas.com*
LAN Connections		
	MAC Address	Default address
	MTU Size	1500
	Ports	2 Auto Sense 10/100/1000BASE-T, RJ-45
	LAN IP Address	DHCP acquired

Appendix B
Share Access from MAC and Linux Systems

This appendix presents examples of how shares on the ReadyNAS device can be accessed by the various MAC operating systems.

MAC OS X

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

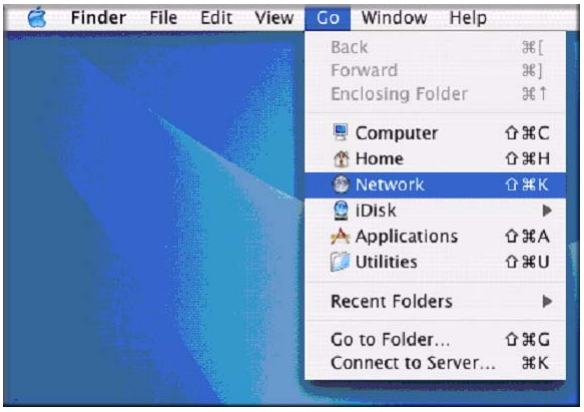


Figure B-1

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.

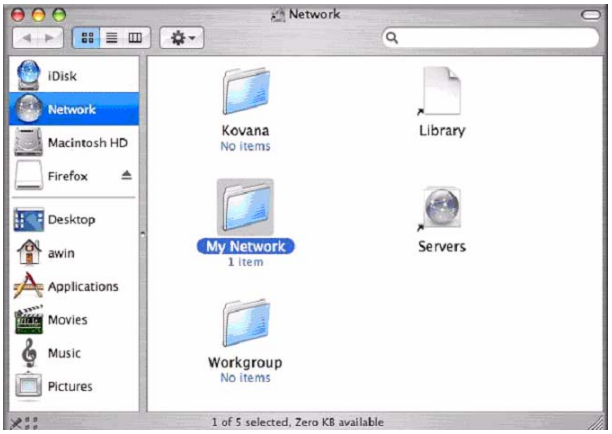


Figure B-2

Open the My Network folder to display the ReadyNAS hostname.

Figure B-3

Enter the user name and password you wish to use to connect to the ReadyNAS.

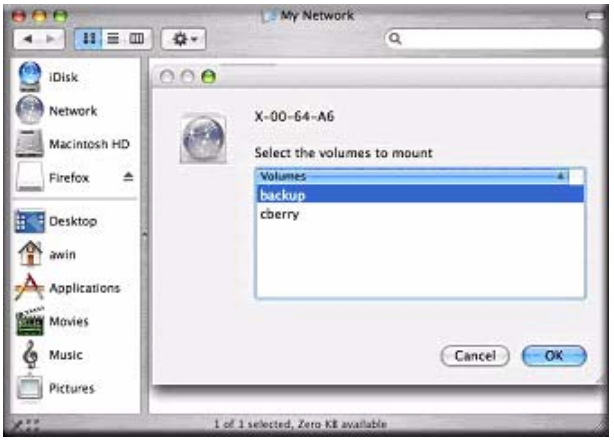


Figure B-4

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.

Figure B-5

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 B-6

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

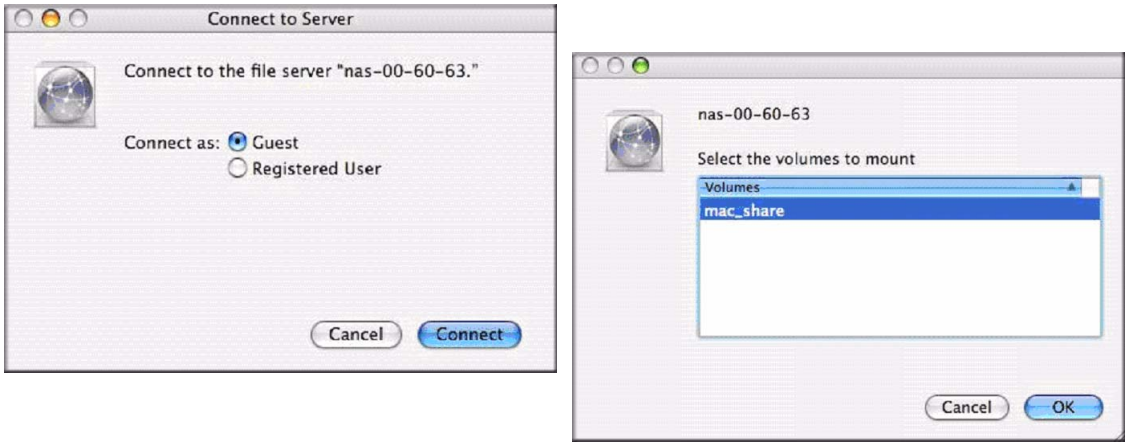


Figure B-7

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.

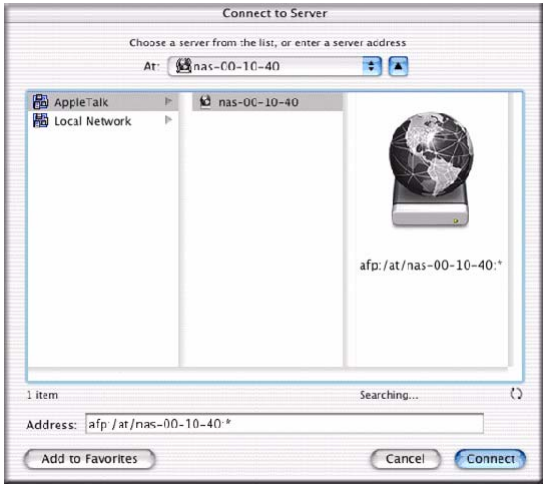


Figure B-8

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.**

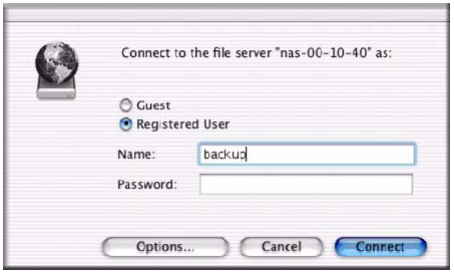


Figure B-9

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**.

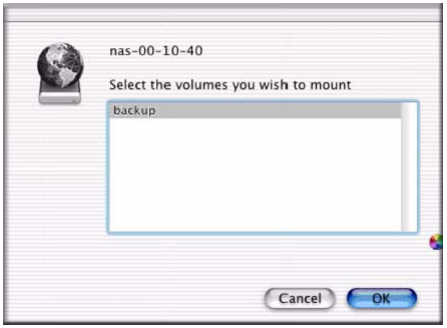


Figure B-10

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

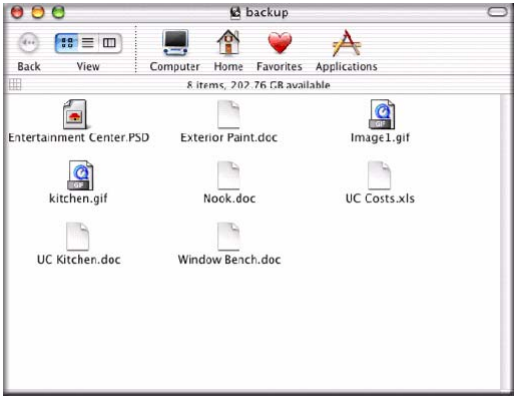


Figure B-11

Accessing Shares from Linux/Unix

To access this share from a Linux or Unix client where **backup** is the share name, you will need to mount the share over NFS by entering: mount ***<ipaddr>:/<backup /backup>***

Running the **ls** command in the mounted path displays the share content.

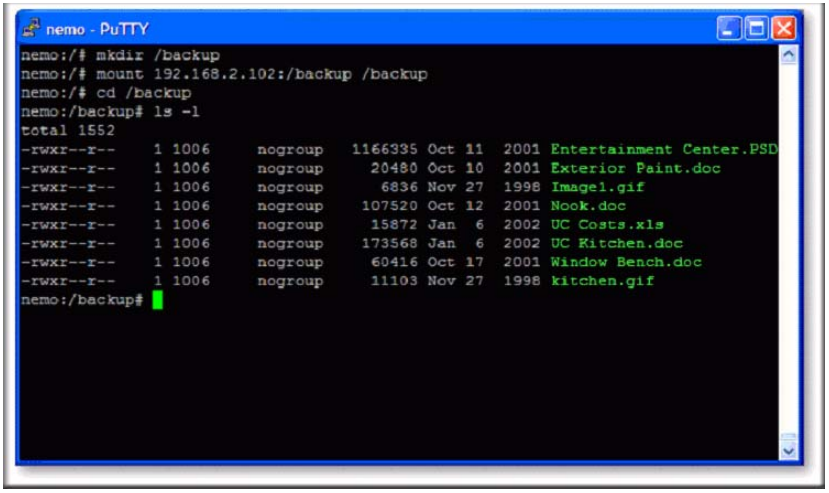


Figure B-12

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.

Appendix C
X-RAID2 and RAID

This appendix introduces the main benefits of X-RAID2, and provides an overview of RAID. The ReadyNAS 2100 supports both X-RAID2 and Flex-RAID mode. Flex-RAID mode enables a more standard RAID configuration, whereas the proven second generation X-RAID2 mode is an auto-expandable RAID technology that is available only on ReadyNAS and is the default configuration on the ReadyNAS 2100.

The Benefits of X-RAID2

RAID stands for Redundant Array of Independent Disks, which is a way of protecting your data in case of a disk failure. Managing RAID volumes can be a complex chore but X-RAID2 eliminates the complexity of volume management.

X-RAID2 Is Auto-Expandable RAID

Over time, people will expand volume capacity to either add redundancy or more file storage space. In typical RAID systems, the steps required for expanding volumes can be so complex and error prone that it leads to data loss. X-RAID2 enables volume expansion without reformatting the disks in the system or shuffling your data back and forth. X-RAID2 automates these complex tasks while providing volume management features previously available only in enterprise-level storage solutions.

Simplified Redundancy

X-RAID2 has one data volume that requires a minimum of one disk overhead to provide redundancy and protect against disk failure. In a two-disk X-RAID2 volume, the usable capacity is one disk, in a three-disk volume the usable capacity is two disks, in a four-disk volume, the usable capacity is three disks, etc.

Even with RAID, there is no data redundancy with one disk; if that disk fails, your data is lost. If you have a one-disk ReadyNAS and want protection from disk failure, you have to add a second disk that is at least as large as the first. It can be ‘hot-added’ while the ReadyNAS is running.

Whenever you add or replace a disk, the ReadyNAS will initialize it, scanning to make sure the disk is good. Once added, ReadyNAS will synchronize the new disk with the original disk. Depending on the disk size, the synchronization may take anywhere from 30 minutes to several hours. The synchronization occurs in the background so you can keep on working with the ReadyNAS during this time.

After the synchronization completes, the data volume is redundant: if one disk fails, the other disk contains all the data, so your are protected from a disk failure. Furthermore, X-RAID2 supports multiple parity which provides protection against two simultaneous disk failures.

Easy Volume Expansion

Horizontal expansion is the process of adding more disks to a ReadyNAS. X-RAID2 also supports vertical expansion which increases the volume capacity when you install larger disks in the ReadyNAS. You can take advantage of larger or more affordable disks as they become available to grow the size of a ReadyNAS volume by replacing a disk with a larger one, adding more disks, or both. After the initialization process, the ReadyNAS synchronizes the new disk(s) and assures data redundancy. This process can take 30 minutes to several hours, and occurs in the background, so you can continue using the ReadyNAS. Also, the synchronization process can traverse system shutdowns. If you need to shut the system down while it is performing a synchronization, you can do so freely; when you restart the ReadyNAS, it resumes the synchronization.

Once you have done this and you have a minimum of two disks with more capacity in the system, just reboot the ReadyNAS to start the volume expansion which occurs in the background. When the process completes, the data stored on the volume remains intact, but the volume capacity will have expanded to include the capacity of the disk less any additional overhead needed to assure the redundancy of the data on the volume.

You can expand the ReadyNAS volume repeatedly with more and larger capacity disks, adding to the value of your investment in a ReadyNAS.

Overview of RAID

RAID is well established technology, and high quality reference material about RAID is widely available on the Internet at sites like Wikipedia (*http://en.wikipedia.org/wiki/RAID*), which is the source of the information below.

RAID is used as an umbrella term for computer data storage schemes that can divide and replicate data among multiple hard disk drives. The different schemes/architectures are named by the word RAID followed by a number, as in RAID 0, RAID 1, etc. RAID's various designs all involve two key design goals: increased data reliability or increased input/output performance. When multiple

physical disks are set up to use RAID technology, they are said to be in a RAID array. This array distributes data across multiple disks, but the array is seen by the computer user and operating system as one single disk. RAID can be set up to serve several different purposes.

RAID Basics

RAID Redundancy is achieved by either writing the same data to multiple drives (known as mirroring), or writing extra data (known as parity data) across the array, calculated such that the failure of one (or possibly more, depending on the type of RAID) disks in the array will not result in loss of data. A failed disk may be replaced by a new one, and the lost data reconstructed from the remaining data and the parity data. Organizing disks into a redundant array decreases the usable storage capacity. For instance, a 2-disk RAID 1 array loses half of the total capacity that would have otherwise been available using both disks independently, and a RAID 5 array with several disks loses the capacity of one disk. Other types of RAID arrays are arranged so that they are faster to write to and read from than a single disk.

RAID Levels

There are various combinations of these approaches giving different trade-offs of protection against data loss, capacity, and speed. RAID levels 0, 1, and 5 are the most commonly found, and cover most requirements.

- **RAID 0** (striped disks) distributes data across several disks in a way that gives improved speed and no lost capacity, but all data on all disks will be lost if any one disk fails. Although such an array has no actual redundancy, it is customary to call it RAID 0.
- **RAID 1** (mirrored settings/disks) duplicates data across every disk in the array, providing full redundancy. Two (or more) disks each store exactly the same data, at the same time, and at all times. Data is not lost as long as one disk survives. Total capacity of the array equals the capacity of the smallest disk in the array. At any given instant, the contents of each disk in the array are identical to that of every other disk in the array.
- **RAID 5** (striped disks with parity) combines three or more disks in a way that protects data against loss of any one disk; the storage capacity of the array is reduced by one disk.
- **RAID 6** (striped disks with dual parity) (less common) can recover from the loss of two disks.
- **RAID 10** (or 1+0) uses both striping and mirroring. “01” or “0+1” is sometimes distinguished from “10” or “1+0”: a striped set of mirrored subsets and a mirrored set of striped subsets are both valid, but distinct, configurations.

RAID can involve significant computation when reading and writing information. With traditional “real” RAID hardware, a separate controller does this computation. In other cases the operating system or simpler and less expensive controllers require the host computer's processor to do the computing, which reduces the computer's performance on processor-intensive tasks. Simpler RAID controllers may provide only levels 0 and 1, which require less processing.

RAID systems with redundancy continue working without interruption when one (or possibly more, depending on the type of RAID) disks of the array fail, although they are then vulnerable to further failures. When the bad disk is replaced by a new one the array is rebuilt while the system continues to operate normally. Some systems have to be powered down when removing or adding a drive; others support hot swapping, allowing drives to be replaced without powering down. RAID with hot-swapping is often used in high availability systems, where it is important that the system remains running as much of the time as possible.

RAID is not a good alternative to backing up data. Data may become damaged or destroyed without harm to the drive(s) on which they are stored. For example, part of the data may be overwritten by a system malfunction; a file may be damaged or deleted by user error or malice and not noticed for days or weeks; and, of course, the entire array is at risk of physical damage.

Index

Numerics

1100 backup
  USB 4-13

A

accessing shares
  FTP/FTPS 3-19
  Linux/Unix B-7
  MAC OS X B-1
  over MAC OS 9 B-5
  Rsync 3-20
  Web browser 3-18
account preferences
  settings 3-10
active directory server. See ADS.
Adding a Volume
  Flex-RAID 2-15
admin user
  password, setting of 2-8
ADS 3-4
Advanced Options 3-17
AFP 2-11
  over AppleTalk B-3
  over Bonjour B-2
  share B-1
alerts
  general settings 2-24
  setting contacts 2-23
Apple File Protocol. See AFP.
AppleTalk
  AFP B-3

B

Backup Button
  programming 4-8
Backup Jobs
  adding new 4-1
  configuring 4-1
  editing 4-9
  options 4-6
  scheduling 4-5, 4-7
Backup Log 4-8
Backup Manager 4-1
Bonjour
  2-12
  AFP B-2

C

CA UniCenter 2-25
changing between X-RAID and Flex-RAID 5-12
changing modes 2-18
CIFS 2-10
CIFS permission 3-14
Clock
  NTP 2-23
Comma Separated Value. See CSV
Common Internet File Service. See CIFS.
CSV 3-9
  format of 3-7

D

Default Gateway 2-6
Deleting a Volume
  Flex-RAID 2-14
DHCP 2-7
  enabling/disabiling 2-8
  settings 2-2
Discovery Services 2-10

UPnP 2-12
discovery services
Bonjour 2-12
Disk Spin-Down 5-3
DNS Settings 2-7
domain
security mode 3-4
security options 3-2

E

Enable WebDAV support 3-26
EXT3 2-21

F

Factory Default Settings 2-30
failed disk
ordering replacement disks 5-10
replacing on NV+ 5-10
replacing, how to 5-9
FAT32 2-21
File Transfer Protocol. See FTP.
Flex-RAID 2-13, 2-14
adding a volume 2-15
deleting a volume 2-14
frame size 2-6
FrontView
accessing 1-7
FTP 2-11
backup jobs 4-2
FTP/FTPS
accessing shares 3-19

G

group
accounts, setting up 3-5
groups
accounts, creating 3-2
managing 3-6

H

health
status of ReadyNAS 5-5
home share
accounts/preference, creating 3-3
user 3-2
Hostname 2-6
default 2-6
setting 2-6
hot spare 2-17
HP OpenView 2-25
Hypertext Transfer Protocol. See HTTP.
HTTP 2-11
HTTPS
with SSL encryption 2-11

I

import users
user accounts 3-9
IP address
setting 2-2
static, setting 2-2

J

jumbo frames
performance settings 2-5

L

Language
settings 2-27
Unicode 2-28
LEDs
explanation of 1-3, 5-7
Linux/Unix
accessing shares B-7
Logs 5-6

M

MAC address

host name use 2-6

MAC OS 9
accessing shares B-5

MAC OS X
accessing shares B-1

MTU 2-3

N

netgear1 1-6

Network File Service. See NFS.

NFS 2-10

NFS server
backup jobs 4-2

NTP
clock 2-23

NV+
replacing disk 5-10

O

Organization Unit. See OU.

OU 3-4

P

password
changing 3-10
recovery of 2-9
setting admin user 2-8

performance
fine-tuning 5-1
settings, jumbo frames 2-5

ports
explanation of WAN and LAN 1-3, 5-7

Power Management 5-3

Power Timer 5-4

R

RAID
setup, reconfiguring 5-14

RAID Settings 2-16

ReadyNAS
health 5-5
updating 2-28
viewing Logs 5-6

replacement disks
ordering 5-10

resynchronizing volume 5-12

Rsync 2-11
accessing shares 3-20
server, backup jobs 4-3

S

security mode
domain 3-4
user 3-2

security options
domain 3-2
user 3-2

shares
access restriction, domain mode 3-14
adding 3-11
advanced CIFS permission 3-14
display option, domain mode 3-14
fine-tuning 3-12
managing 3-11
selecting services 2-10
setting access in Domain Mode 3-13

Shutdown 5-16

SMART+Self-Monitoring, Analysis and Reporting Technology. See SMART+.

SMB 2-10

SMTP 2-26

Snapshots 4-9
expiration 4-12
resizing space 4-12
scheduling 4-10
taking manually 4-11
temporary backups 4-10

SNMP 2-25
CA UniCenter 2-25
HP OpenView 2-25
setting up 2-25

Speed/Duplex Mode 2-3

Standard File Protocols 2-10
Support 1-ii

T

trusted domains 3-5

U

UBB
1100 backup 4-13
Unicode 2-28
HTTP 2-28
WebDAV 2-28
updating
remote method 2-29
updating ReadyNAS 2-28
UPnP 2-12
UPS
configuration of 5-4
performance, adding 5-2
USB 2-21
backing up to 4-13
flash device 2-21
formats, EXT3 2-21
formats, FAT32 2-21
shares 2-19, 2-20
storage 2-20
USB storage
partitions 2-20
user
accounts, creating 3-2
security mode 3-2
security options 3-2
user accounts
import users 3-9
managing 3-8
setting up 3-5

V

VLAN
settings 2-5
support enabling 2-5
Volume Management 2-13
X-RAID 2-14
Flex-RAID 2-13
X-RAID 2-17
VPN
setting WINS server 2-7

W

Web browser
accessing shares 3-18
WINS
2-7
workgroup
name 3-2
setup 3-3

X

X-RAID 2-14
adding a second disk 2-17
adding more disks 2-18
using hot-swap trays 2-18
volume management 2-17