NETGEAR

ReadyNAS for Business

Software Manual

Models:

1500
2100
3100
3200
4200

Pro 2
Pro 4
Pro 6

NVX
Pro Business

350 East Plumeria Drive
San Jose, CA 95134
USA

November 2010
202-10629-05
v1.0

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

Statement of Conditions

To improve 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.

Revision History

Publication Part Number	Version	Publish Date	Comment
202-10629-01	v1.0	May 2010	1st publication
202-10629-02	v1.1	June 2010	Compliance update
202-10629-03	v1.2	July 2010	Feature updates
202-10629-04	v1.3	July 2010	Compliance update; TM updates
202-10629-05	v1.0	November 2010	Feature and product updates

Table of Contents

Chapter 3 Manage User Accounts

Chapter 4 Manage & Access Shares

Chapter 5 Backing Up Your Data

Getting Acquainted

1

ReadyNAS for Business

This NETGEAR® ReadyNAS® for Business software manual describes how to configure and manage a ReadyNAS system.

This chapter contains the following sections:

Note: This manual documents common software features installed on most ReadyNAS business product models and is based on firmware v4.2.15. Variations per model are noted, as necessary.

What is the NETGEAR ReadyNAS?

NETGEAR® ReadyNAS® for Business network storage products provide businesses and home users with easy-to-use, high-performance gigabit network attached storage (NAS) solutions used to share and protect data.

ReadyNAS systems enable users across the LAN, or WAN, or over the Internet to back up and share data from Windows, Macintosh, and Linux systems.

Offering extensible, high-availability data protection, ReadyNAS systems come with robust, fail-safe features that can include:

- ECC memory that safeguards data from single-bit errors in memory (3100, 3200, 4200)
- Support for RAID 0, 1, 5, and 6, plus hot spare (RAID 6 on Pro, 3200, and 4200)
- Dual redundant Gigabit Ethernet ports
- NETGEAR's proprietary X-RAID2™ for automatic volume expansion
- Redundant power supplies (3100, 3200, and 4200)

In addition to providing NAS functionality, on selected ReadyNAS units you can set up iSCSI volumes so that the ReadyNAS can simultaneously act as a SAN (storage area network).

Your ReadyNAS continually monitors the entire system for abnormal situations or failures. Status indicators provide quick hardware and software status readings, and emails alerts inform you about critical events in the system.

Additionally, with the FrontView Management Console, the ReadyNAS can be customized with a wealth of add-on features developed by NETGEAR, NETGEAR's partners, and the ReadyNAS development community.

ReadyNAS Community Website

For more information about NETGEAR ReadyNAS products, visit the dedicated ReadyNAS Community Web site at ***http://readynas.com*** where you will find reviews, tutorials, a comparison chart, software updates, documentation, an active user forum, and much more.

ReadyNAS Business Product Lineup

NETGEAR offers a complete lineup of ReadyNAS home and business storage products, each with its own unique characteristics to fit your specific requirements. With all ReadyNAS products, the embedded operating system and easy-to-configure software makes installation, and upgrades a breeze.

ReadyNAS 1500

- iSCSI
- Redundant power supply
- ✔ ECC memory
- ✔ Ethernet teaming
- 10Gb Ethernet

The compact rack-mount chassis makes the ReadyNAS 1500 perfect for small businesses. With three USB 2.0 ports, and up to four SATA I or SATA II hard drives via lockable, hot-swappable disk trays, it provides up to 8 TB of network attached storage that can easily be expanded as larger capacity drives become available.

ReadyNAS 2100

Housed in a compact rack-mount chassis, the ReadyNAS 2100 is perfect for small to medium businesses. With three USB 2.0 ports, and up to four SATA I or SATA II hard drives via lockable, hot-swappable disk trays, it provides up to 8 TB of network attached storage that can easily be expanded as larger capacity drives become available.

- ✔ iSCSI
- Redundant power supply
- ✔ ECC memory (2100 v1)
  ECC memory (2100 v2)
- ✔ Ethernet teaming
- 10Gb Ethernet

ReadyNAS 3100

- ✔ iSCSI
- ✔ Redundant power supply
- ✔ ECC memory
- ✔ Ethernet teaming
- 10Gb Ethernet

With support for up to 500 users, the powerful but cost-effective ReadyNAS 3100 is ideal as a primary storage solution for mid-range enterprises and a high-performance secondary solutions for larger businesses. The ReadyNAS 3100 unified NAS and SAN architecture delivers a file sharing and virtualization platform that enables businesses to reduce costs and increase flexibility. Now you can solve first-time server virtualization, data replication, and disk-to-disk backup problems without sacrificing reliability or performance. You can also build remote access or optionally automate cloud-based archives all from a single investment.

ReadyNAS 3200

- iSCSI
- Redundant power supply
- ECC memory
- Ethernet teaming
- 10Gb Ethernet

The ReadyNAS 3200 is ideal for small to medium businesses that want high-end features at an SMB price. It features redundant power supplies and dual Gigabit Ethernet ports. It enables growing businesses to securely share, store, and protect business-critical data across the network in the most efficient manner. Housed in a compact rack-mount form, the RN3200 has two USB 2.0 ports, and supports up to 12 SATA I or SATA II hard drives using hot-swappable disk trays. With up to 24 TB of network attached storage, the RN3200 can be easily expanded as larger capacity drives become available. Also, the ability to allocate iSCSI target volumes makes it ideal for server virtualization, file sharing, disk-based backup, and online storage consolidation.

ReadyNAS 4200

- iSCSI
- Redundant power supply
- ECC memory
- Ethernet teaming
- 10Gb Ethernet

With support for up to 500 users, the powerful ReadyNAS 4200 is an ideal primary storage solution for mid-range enterprises, and a high-performance secondary solution for larger businesses. With a high density unified NAS and SAN architecture, the ReadyNAS 4200 delivers a cost effective file sharing and virtualization platform with high performance and reliability. Support for 10Gb Ethernet provides the maximum in throughput scalability for demanding applications. It's a powerful and affordable way to consolidate servers, build off-site disaster recovery solutions, or store, share, and protect business-critical data.

ReadyNAS Pro 6

- iSCSI
- Redundant power supply
- ECC memory
- Ethernet teaming
- 10Gb Ethernet

ReadyNAS Pro 6 is the most powerful desktop storage line of the award-winning ReadyNAS product family. Designed for small and medium businesses, workgroups and home offices, ReadyNAS Pro 6 delivers class-leading performance, ease-of-use, and a robust feature set in a small desktop chassis supporting 6 SATA channels and up to 12 TB of storage. This 6-bay, unified network storage simultaneously supports NAS and SAN and is packed with high-end server features, including RAID levels 0, 1, 5, 6, and Auto-Expandable X-RAID2® support for data protection against disk failure, system monitoring capabilities, snapshot and built-in secure replication. To ensure high availability to stored data, the ReadyNAS Pro 6 also features dual redundant Gigabit Ethernet ports for failover protection.

ReadyNAS Pro 4

- iSCSI
  Redundant power supply
  ECC memory
- Ethernet teaming
  10Gb Ethernet

ReadyNAS Pro 4 is NETGEAR's 4-bay desktop storage system with both NAS and iSCSI SAN support for business users in small offices, departments, and other small IT environments. It's a perfect solution for backup, serving files, and iSCSI SAN applications. Pro 4 provides X-RAID2™ automatic volume management, secure drag-and-drop remote access (ReadyNAS Remote), optional online backup solution (ReadyNAS Vault), replication (Rsync), and RAID 0/1/5 for data protection.

ReadyNAS Pro 2

- iSCSI
  Redundant power supply
  ECC memory
- Ethernet teaming
  10Gb Ethernet

ReadyNAS Pro 2 is NETGEAR's 2-bay desktop storage system with X-RAID2™ automatic volume management, secure drag-and-drop remote access (ReadyNAS Remote), optional online backup solution (ReadyNAS Vault), replication (Rsync), and RAID 0/1/5 for data protection. With the best-in-class performance, enterprise class drives and fully loaded features for small business users, the Pro 2 is a cost effective and versatile solution for small office network storage.

ReadyNAS PRO Business

- iSCSI
  Redundant power supply
  ECC memory
- Ethernet teaming
  10Gb Ethernet

The ReadyNAS Pro Business Edition, in a compact desktop chassis, supports up to six SATA I or SATA II hard drives using six lockable, hot-swappable disk trays. The ReadyNAS Pro Business edition supports iSCSI, snapshots with scheduling, selectable security modes, and other enterprise features. Three USB 2.0 ports enable USB drives or printer connections, and provide up to 12TB of network attached storage that can be easily expanded as larger capacity drives become available.

ReadyNAS NVX

- iSCSI
  Redundant power supply
  ECC memory
- Ethernet teaming
  10Gb Ethernet

Sporting a charcoal black exterior, the ReadyNAS NVX is the most capable four-bay desktop NAS system in the world, and comes with a 1GHz Intel CPU and 1GB of fast SO-DIMM, to give you a system capable of hitting 85MB/sec. The chrome curved handle in the back makes it easy to move between home and office, should the need arise. Because the NVX supports both NAS and SAN at the same time, you can use the NVX to combine file sharing and application storage in a single device. Additionally, for flexible and easy operation in file serving, backup to disk, and server virtualization environments, you can cut your network storage needs in half.

Initial Setup and Default Login

To set up and install your ReadyNAS system, follow the instructions on the *ReadyNAS Installation Guide* that came with your unit. An electronic copy of the installation guide is located on the product CD. You can also find it on the NETGEAR Web site, and on the ReadyNAS Community support page at ***http://readynas.com/documentation***. For a list of supported disks, go to ***http://readynas.com/hcl***.

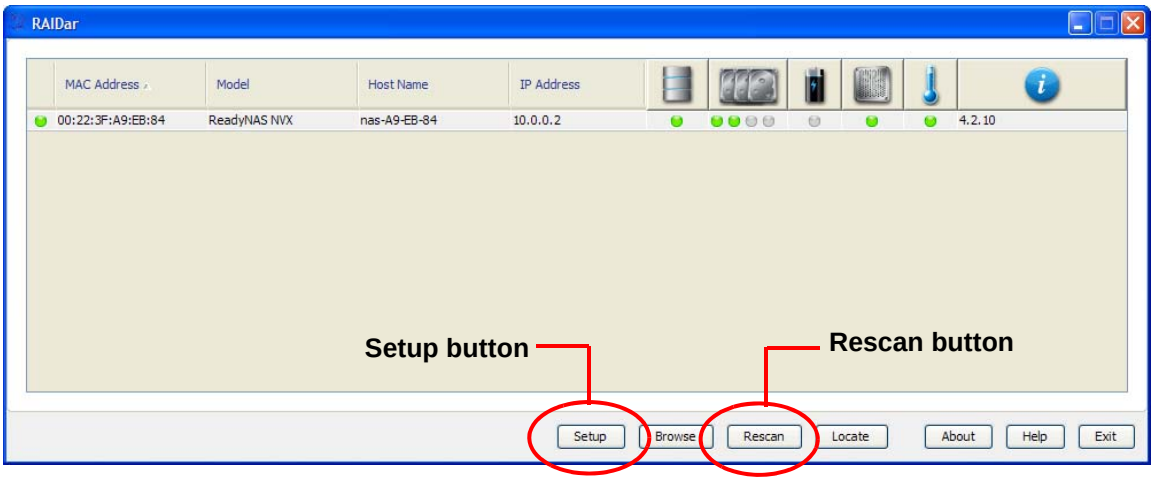
The RAIDar Utility

The RAIDar utility acts as a discovery tool that recognizes ReadyNAS devices on your network and enables easy setup and management of all your ReadyNAS units. If it is not already installed, you can find the RAIDar utility on your product *Resource CD*. The RAIDar utility versions provided are for Windows, Mac, and Linux.

Once installed, plug your ReadyNAS into the network and start the RAIDar utility. RAIDar automatically finds the unit(s) on the network without needing its IP address, and makes it easy to see the status of your units. All ReadyNAS device should be listed on the page. For more information about RAIDar, visit *http://www.readynas.com/raidar*.

The default IP configuration is set to DHCP; if the unit does not get an IP address, it defaults to 192.168.168.168.

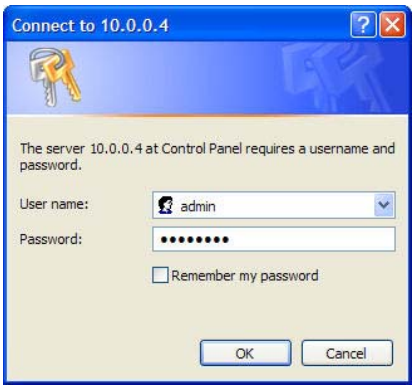
Note: If you are running RAIDar on Windows XP before SP2, disable the Internet connection firewall.



If no ReadyNAS device is detected, check the following and click **Rescan** to try again:

- Make sure the ReadyNAS device has power and is connected to your network.
- Make sure the PC running RAIDar is on the same subnet as the ReadyNAS device.

To view one of the ReadyNAS systems, select it from the list and click the **Setup** button. RAIDar opens your default browser and connects you to the selected ReadyNAS. You are prompted for your user name and password.



- Default administrator user name: **admin**
- Default password: **netgear1**

Both user name and password are case sensitive.

When you are logged in, the RAIDar utility connects to the FrontView Management Console, which you use to configure and manage your ReadyNAS systems. You can change the default password to a more secure password once you are in FrontView.

RAIDar Commands

Table 1. RAIDar Utility Commands

Command	Description
Setup	**Setup** launches the FrontView Management Console for the selected device. FrontView is a Web-based utility used to set up, configure and manage your devices. If this is a first-time installation, or the device has been reset to factory default, the setup wizard launches so you can configure the device.
Browse	Click **Browse** to see the shares available on the highlighted device. This only works with Windows 2000 and newer operating systems.
Rescan	**Rescan** updates the ReadyNAS device list and status.
Locate	**Locate** causes the LEDs on the ReadyNAS device to blink. This is useful if you have multiple ReadyNAS devices and you need to correlate the RAIDar entries to physical devices.
About	This menu option displays information about RAIDar.
Help	This menu option launches the help screen.
Exit	This menu option exits the RAIDar utility.

RAIDar LED Descriptions

The first LED column represents the global error status informing you if the ReadyNAS device is in normal operating mode, or if it is in a warning or failure condition.

The other column displays device-specific information, allowing you to view exactly what devices might need attention.

Note: Some LEDs are valid only for disk and volume.

Table 2. LED Descriptions for RAIDar

LED	Description
 Not present	**Off**: No disk or device is attached.
 Normal	**Green**: Device is in normal operating mode.
 Warning or Dead	**Amber:** The device has failed or is in a state where it needs attention.
 Inactive spare	This disk is a spare disk on standby. If a disk fails, this disk will automatically take over.
 Awaiting resync	**Green:** This disk is waiting to resync to the RAID volume. **Blinking Green**: The disk is in the process of resyncing. During the resync process, the volume is in degraded mode, which means performance is affected by the resync process, and another disk failure in the volume will render it dead.
 Life support mode	The volume has encountered multiple disk failures and is in the state of being marked dead. However, the ReadyNAS has blocked it from being marked dead in case someone accidentally pulled out the wrong disk during runtime. If the wrong disk was pulled out, shut down the ReadyNAS immediately, reconnect the disk, and power on the ReadyNAS. If you reconnect the disk during runtime, the ReadyNAS will mark it as a newly added disk and you will no longer be able to access the data on it.
 Background task active	**Blue**: The unit is running a lengthy background task, such as a system update.

FrontView Management Console

Once logged in using the RAIDar utility, the FrontView Management Console appears.

FrontView operates in two modes:

- *Setup Wizard Mode*
- *Advanced Control Mode*

Setup Wizard Mode

When the unit is installed for the first time, or is in its factory default state, FrontView opens in Setup Wizard mode. The Setup Wizard guides you step-by-step through the configuration process, assisting you in quickly integrating the ReadyNAS unit into your network.

> **Note:** For the initial setup, NETGEAR recommends using the Setup Wizard to ensure that all the necessary settings are configured. FrontView will automatically switch to the Advanced Control mode once the Setup Wizard has finished.

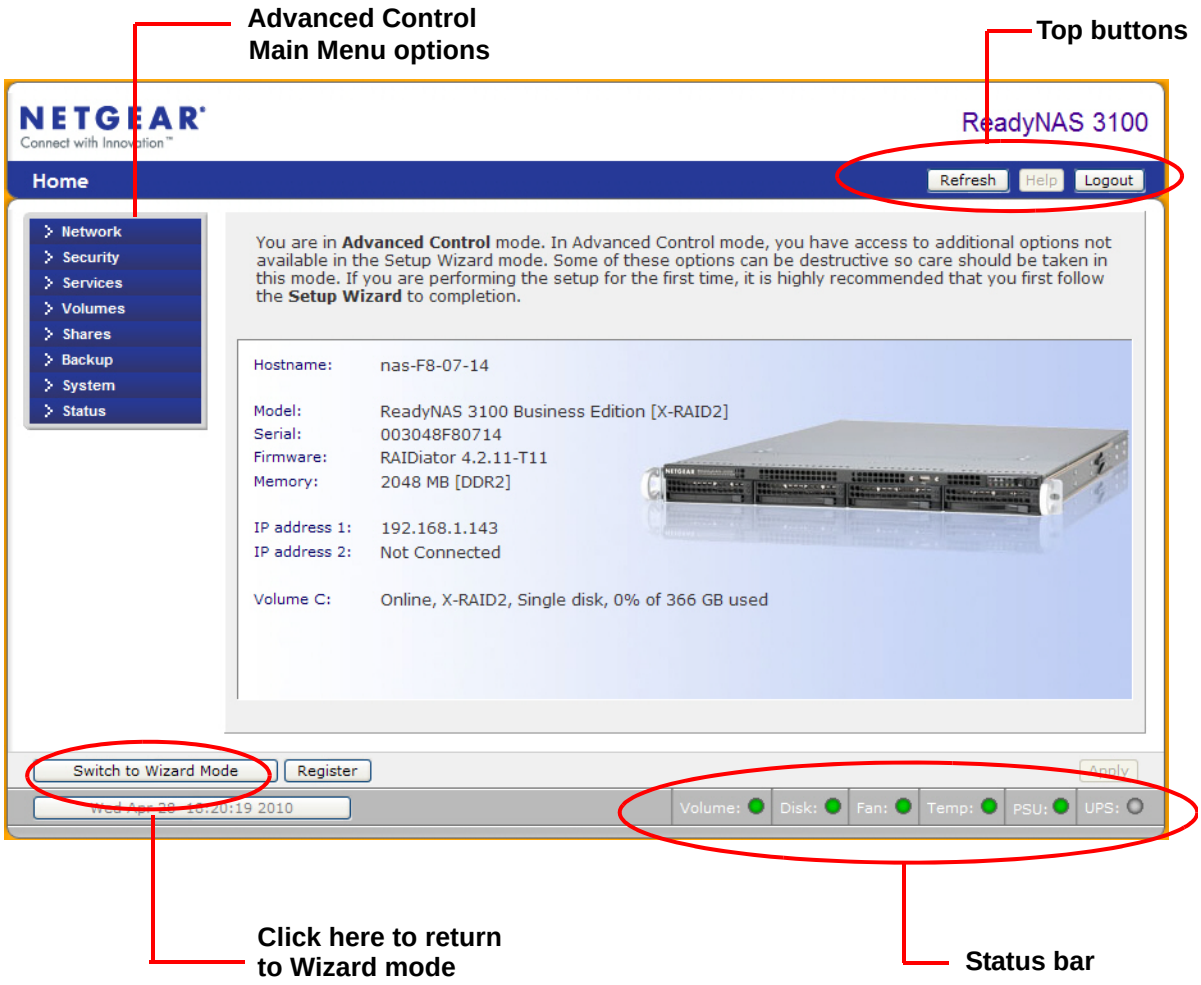
The **Home** screen provides detailed information about your unit.

Click here to switch between the Smart Wizard and the Advanced Control modes

Advanced Control Mode

The FrontView Advanced Control mode provides access to all available settings. In this mode, the menu on the left allows 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 with the **Refresh** button, display **help** where available, and use the **Logout** button to securely log out of a session.

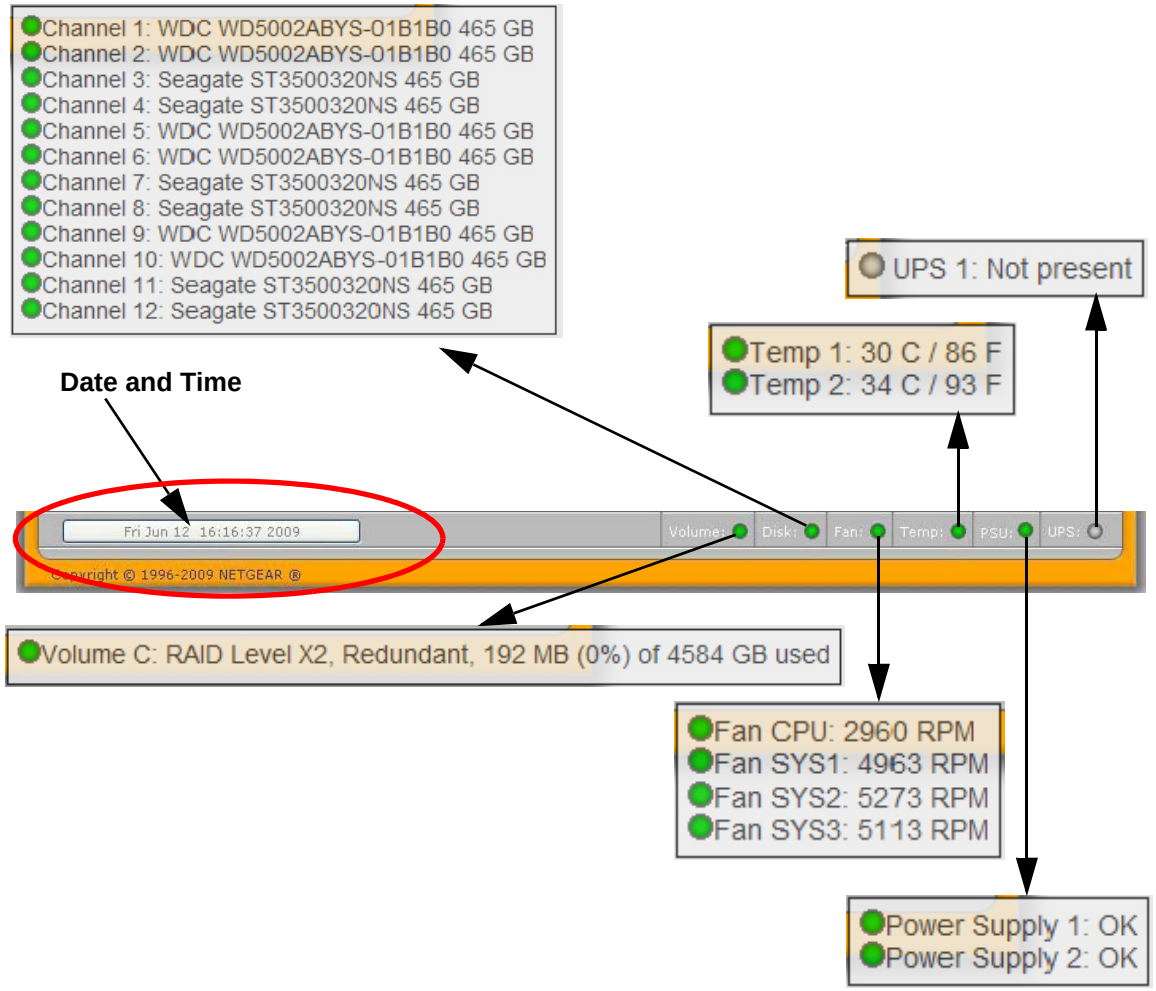


Status Bar

The status bar at the bottom of the screen gives a quick glimpse of the system status and provides access to the following information:

- **Date and Time**. When clicked, the date button opens the Clock screen.
- **Volume**. Indicates volume information.
- **Disks**. Indicates the channel, type and size of the installed disks.
- **Fan**. Indicates system and CPU RPMs.
- **Temperature**. Indicates the operating temperature.
- **PSU**. Indicates the status of one or more power supplies.
- **UPS**. Indicates the UPS status.

Move your mouse over the status light to display device information, or click a status light to open the related FrontView screen.



Managing Your ReadyNAS System

2

This chapter describes how to set up and manage the ReadyNAS Network Attached Storage system on your network, and contains the following sections:

- **Customizing Network Settings**
- **Setting Up Security**
- **Selecting Services for Share Access**
- **Adjusting System Settings**
- **Understanding Volume Management**

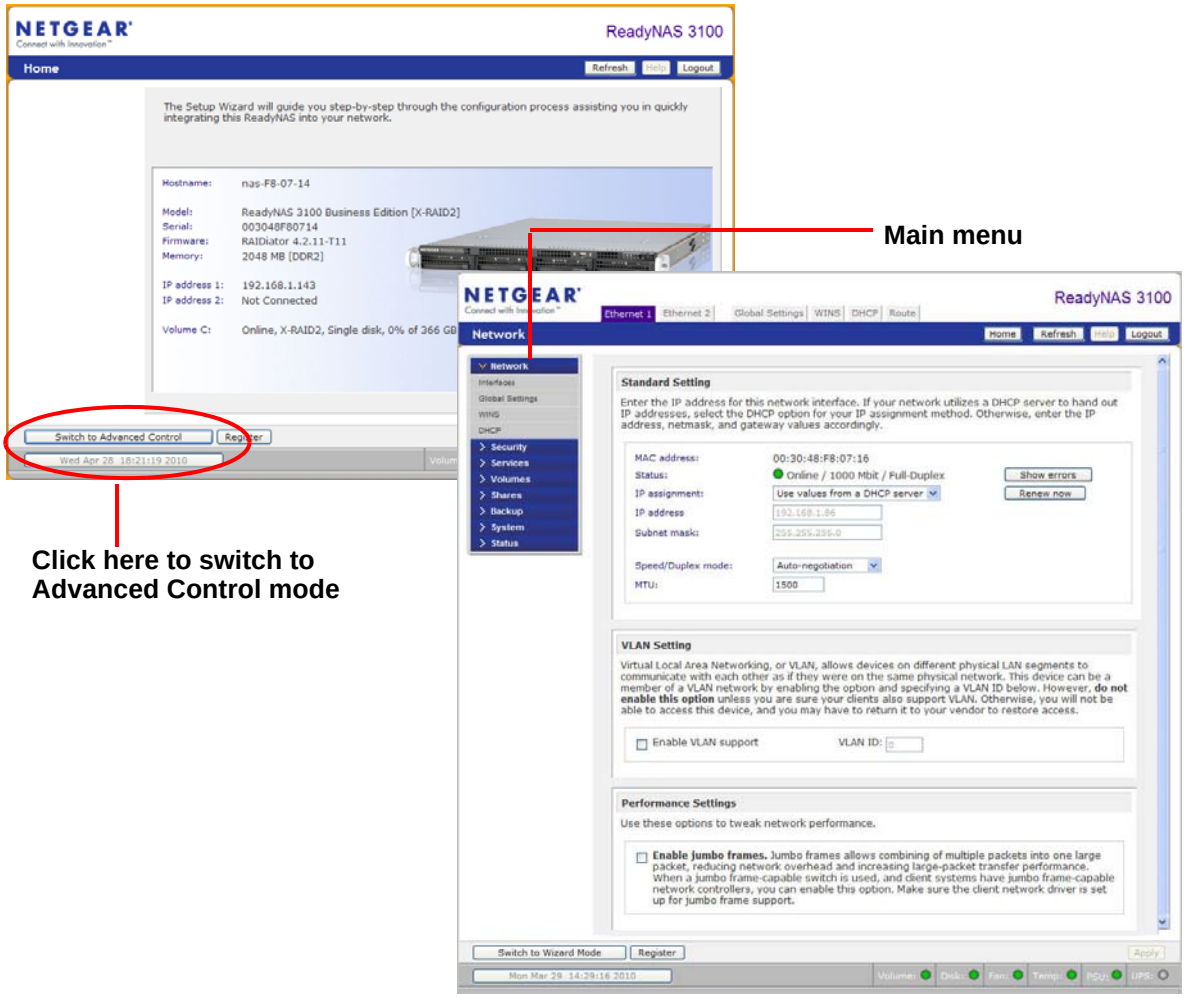
Customizing Network Settings

To access network settings, click the **Advanced Control** button on the bottom of the Smart Wizard Home screen to open advanced control features, and display the main menu. Then select **Network** to access the network settings configuration pages.

You can access ReadyNAS Network functionality from these tabs described in the following sections:

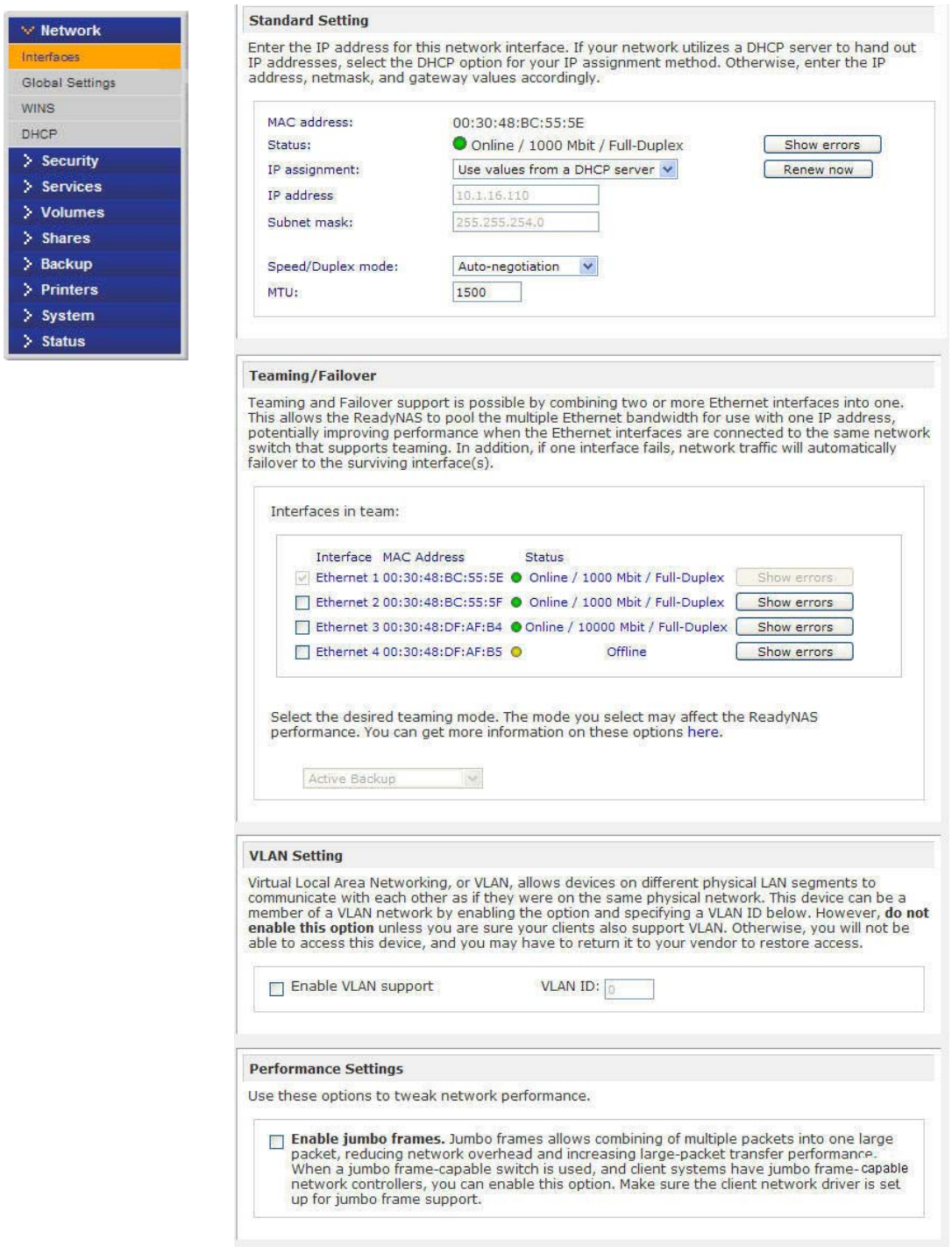
- *Ethernet Interfaces* on page 20.
- *Global Network Settings* on page 25.
- *WINS* on page 26.
- *DHCP* on page 26.
- *Route* on page 27.

Depending on your ReadyNAS model, the interface shows fewer or more Ethernet tabs.



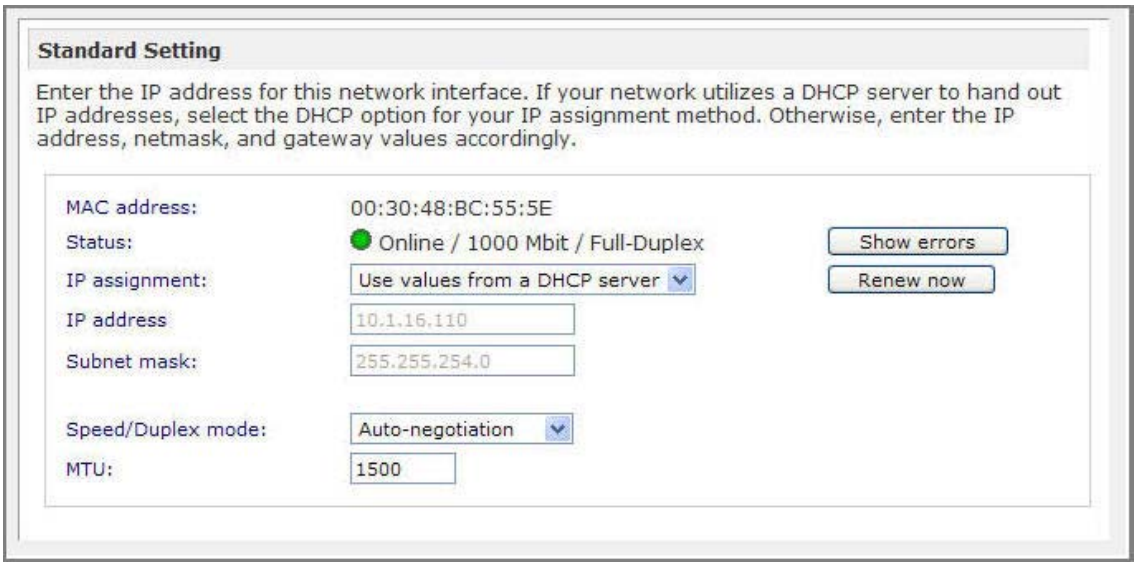
Ethernet Interfaces

To configure Ethernet interfaces, select **Network > Interfaces.** The default screen is the **Ethernet 1** screen. Use this screen to specify network interface-specific settings, including the *Standard Settings* , *Teaming/Failover* , *VLAN Settings* , and *Performance Settings* .



Standard Settings

Use this area to specify the IP address, network mask, speed/duplex mode, and MTU settings.



IP Assignment

From the pull-down menu, select **Use values from a DHCP** server or **Use values below**.

In most networks where a DHCP server is enabled, you can specify the **Use values from a DHCP server** option to automatically set the IP address and network mask.

- **Use values from a DHCP server**

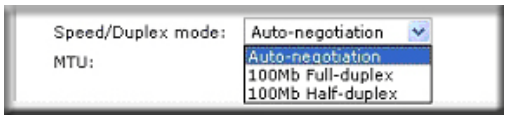
  If you elect to assign the IP address using **Use values from a DHCP server**, NETGEAR advises that you set the lease time on the DHCP server/router to a value of at least one day. Otherwise, you might notice that the IP address of the unit changes even when it has been turned off for only a few minutes. Most DHCP servers allow you to map a static IP address to a MAC address. If you have this option, this ensures your ReadyNAS maintains the same IP address, even in DHCP mode.

- **Use values below**

  If you assign a static IP address by selecting **Use values below**, be aware that the browser will lose connection to the ReadyNAS device after the IP address has been changed. To reconnect after assigning a static IP address, open the RAIDar utility and click **Rescan** to locate the device, and then reconnect.

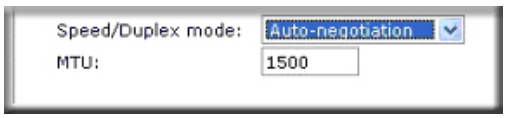
Speed/Duplex Mode

NETGEAR advises that you keep the setting in an Auto-negotiation mode; however, if you have a managed switch that works best when the devices are forced to a particular speed or mode, you can select either the full-duplex or half-duplex setting as needed.



MTU

NETGEAR advises that you leave the default setting; however, in some network environments, changing the default MTU value can fix throughput problems.



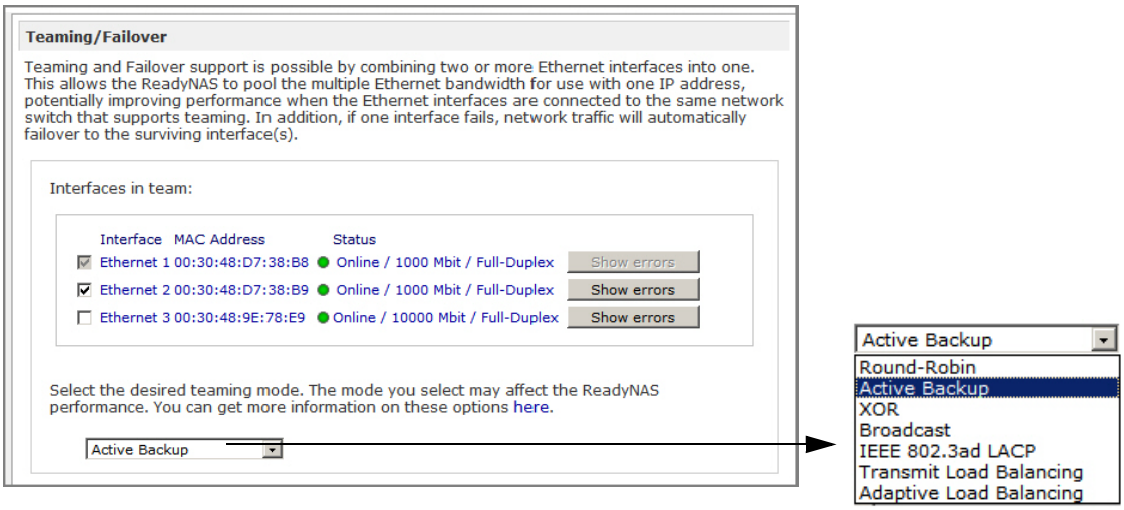
Teaming/Failover

Network teaming provides a way to aggregate the two network interfaces into a single logical teamed, or bonded, interface. A teamed interface can provide enhanced 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, make sure the interfaces are connected, select the interfaces to team from the **Teaming/Failover** section, and then select the teaming mode.
- 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.

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

The following Teaming/Failover options are available.



Select the bonding mode:

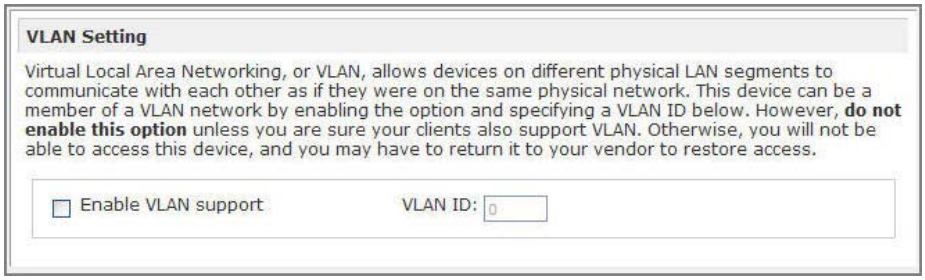
- **Round-Robin**. This mode provides load balancing and fault tolerance, and transmits packets in sequential order from the first available interface to the next.
- **Active Backup**. Only one interface in the bond is active. A different interface becomes active if, and only if, the active interface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

- **Transmit Load Balancing**. Set this mode for 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**. This mode 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

Use this section to specify whether or not to allow devices residing on different segments of a LAN (Virtual Local Area Network), 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.



If you want to use the ReadyNAS in a VLAN environment, select the **Enable VLAN support** check box, and enter a numeric **VLAN ID**. This requires a reboot of the ReadyNAS for the VLAN function to take effect.

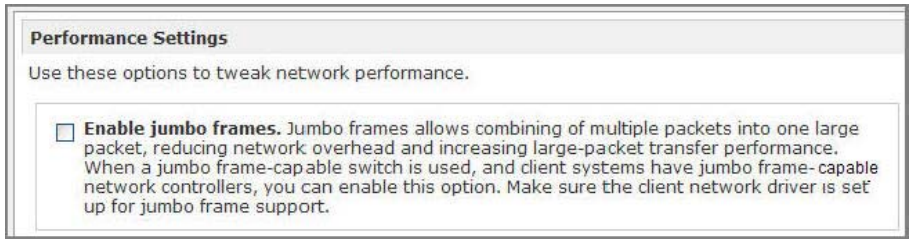
WARNING!

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

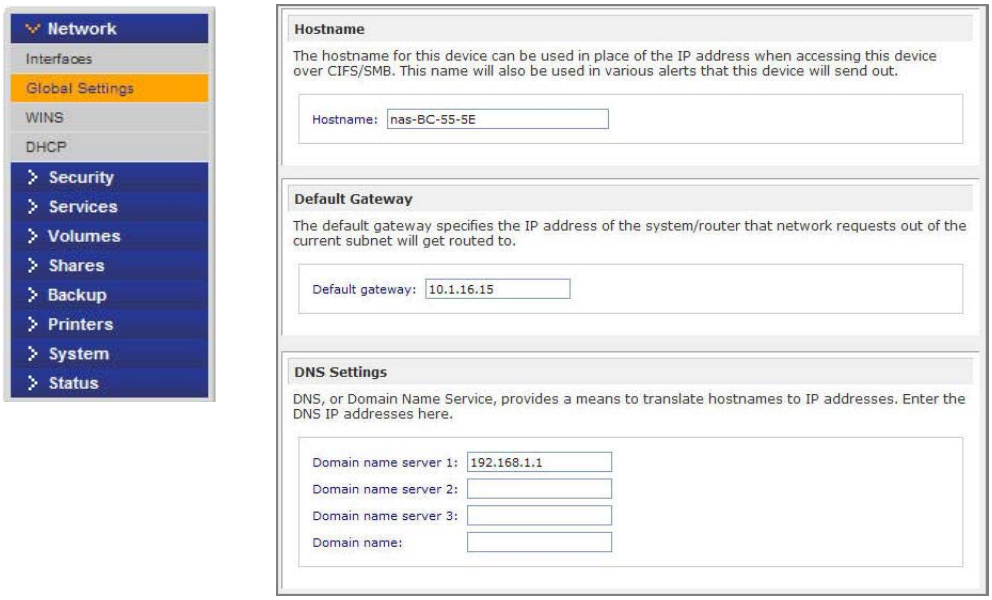
Performance Settings

The **Enable jumbo frames** option allows you to optimize the ReadyNAS for large data transfers.

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



Global Network Settings



Hostname

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

The default hostname is **nas**- followed by the last 3 bytes of its 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 screen, 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 address of the default gateway server here.

DNS Settings

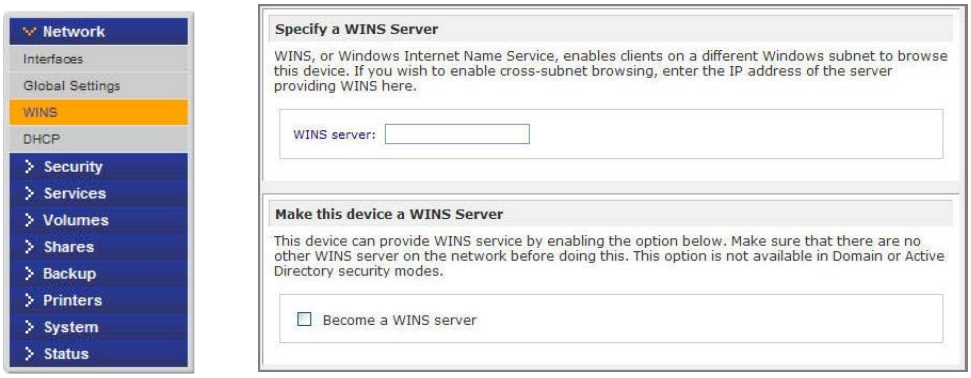
The DNS area allows you to specify up to three domain name service servers for hostname resolution. The DNS service translates host names into IP addresses.

If you selected the DHCP option in the Ethernet screen, 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 Windows Internet Naming Service (WINS) server allows the ReadyNAS or other devices on the network to be browsed from other subnets. This is useful if you want to browse by hostname across multiple subnets (for example, over VPN.

You can specify the WINS server IP address, or 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 screen allows you to specify your ReadyNAS as a DHCP server.

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

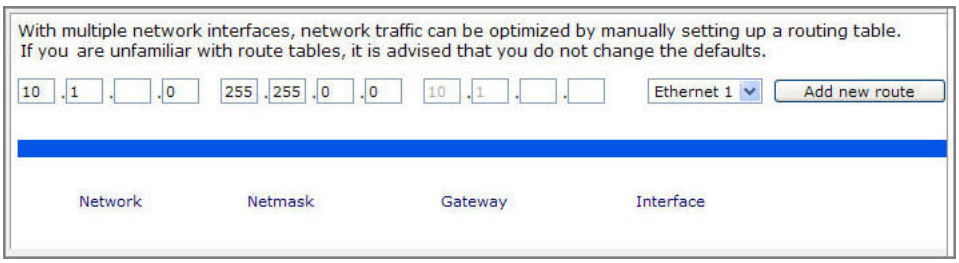
WARNING!

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

Route

Use the **Route** screen to specify a manual routing table for each Ethernet interface and to optimize performance.

For example, you could configure a manual routing table to assure that these Ethernet interfaces are directly routed over a fiber backbone and assure the unit does not experience the traffic congestion that can build up on a gigabit segment.



Setting Up Security

Use the **Security** screen to set the administrator password, administer security, and set up the password recovery feature on the ReadyNAS.

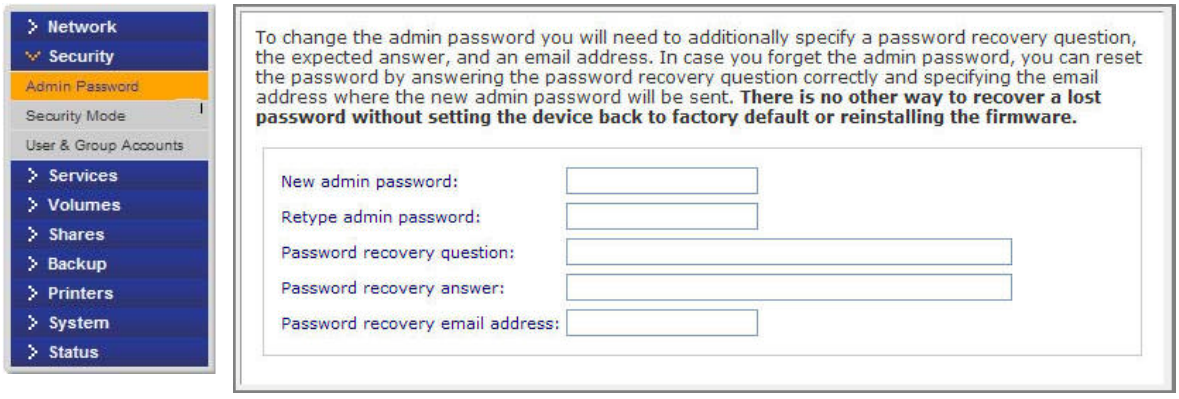
Access ReadyNAS Security functionality from these tabs:

- *Updating the Admin Password* on page 28.
- *Security Access Modes* on page 29.
- *Accounts* on page 29.

Updating the Admin Password

The **Admin Password** screen allows you to change the administrator user password. The administrator user is the only user who can access the FrontView Management Console, and has administrative privileges when accessing shares.

Note: Be sure to set a password different from the default password and keep it in a safe place. Anyone who obtains this password can change settings or erase data stored on the ReadyNAS.



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 email address. If, in the future, you forget the password, go to ***https://<readynas ip_address>/password_recovery***. Successfully answering the questions resets the admin password, which is then sent to the email address you enter on this screen.

Password Recovery

To recover a forgotten password:

There are two options for recovering or resetting a lost or compromised password:

1. In a Web browser, enter ***https://<readynas ip_address>/password_recovery***. You will be prompted for the email address and security question entered when you first set up the system. A new password will be sent to you at that email.
2. Optionally, you can reinstall the firmware, which does not remove data from the system, but resets the admin username and password to the factory defaults **admin** and **netgear1.**

   In a Web browser, enter:
   http://readynas.com/forum/faq.php#How_do_I_re-install_the_firmware%3F

Security Access Modes

See *Setting Security Access Modes* on page 52.

Accounts

See *Setting Up User and Group Accounts* on page 56.

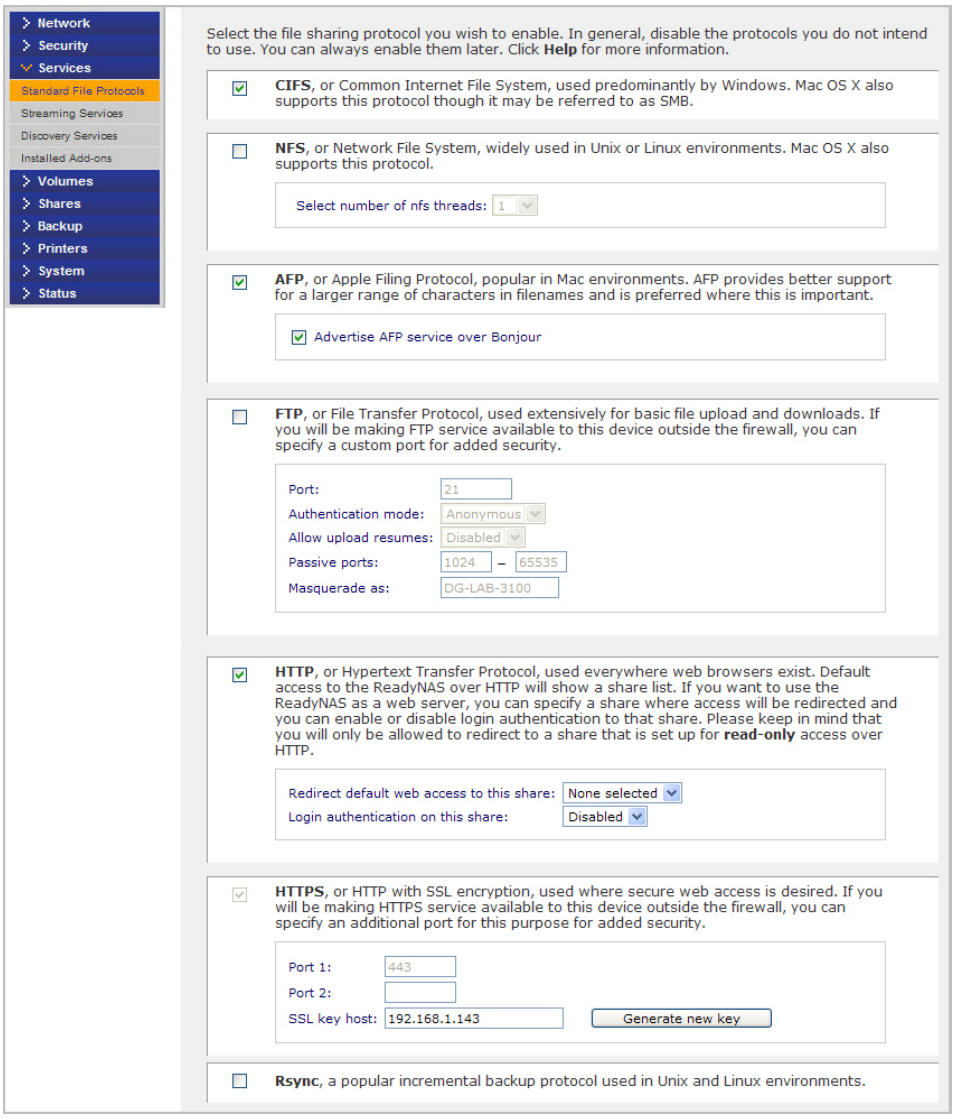
Selecting Services for Share Access

Access ReadyNAS Services functionality from these tabs:

- *Standard File Protocols* on page 30.
- *Discovery Services* on page 32.
- *Installed Add-Ons* on page 33.

Standard File Protocols

Standard file protocols are common file-sharing services that allow your workstation clients to transfer files to and from the ReadyNAS.



CIFS (Common Internet File Service)

Sometimes referred to as SMB, CIFS is used mainly by Microsoft Windows clients, and sometimes by Mac OS X clients. Under Windows, My Network Places and Network Neighborhood uses CIFS. This service is enabled by default.

NFS (Network File Service)

NFS is used by Linux and Unix clients. Mac OS 9/X users can access NFS shares through console shell access. ReadyNAS supports NFS v3 over UDP and TCP.

AFP (Apple File Protocol)

Mac OS 9 and OS X work best using this protocol because it handles an extensive character set. However, in a mixed PC and Mac environment, NETGEAR recommends CIFS/SMB over AFP, unless enhanced character set support is necessary for the Mac. ReadyNAS supports AFP 3.2.

FTP/FTPS (File Transfer Protocol and FTP with SSL encryption)

Widely used in public file upload and download sites. ReadyNAS supports anonymous or user access for FTP clients, regardless of the security mode selected. You can elect to set up port forwarding to nonstandard ports for better security when you access files over the Internet. Alternately, use an FTPS client for secure and encrypted login and data transfers.

HTTP (Hypertext Transfer Protocol)

ReadyNAS supports HTTP file manager, allowing read/write access to shares using the browser. This service can be disabled in lieu of HTTPS to allow for a more secure transmission of passwords and data. With the redirect option, access to **http://readynas_ip** can be automatically redirected to a share. This is useful if you do not want to expose your default share listing to outsiders. To redirect to a share, create an index file, such as index.htm or index.html, in your target share. You can also enable or disable login authentication to this share.

HTTPS (HTTP with SSL encryption)

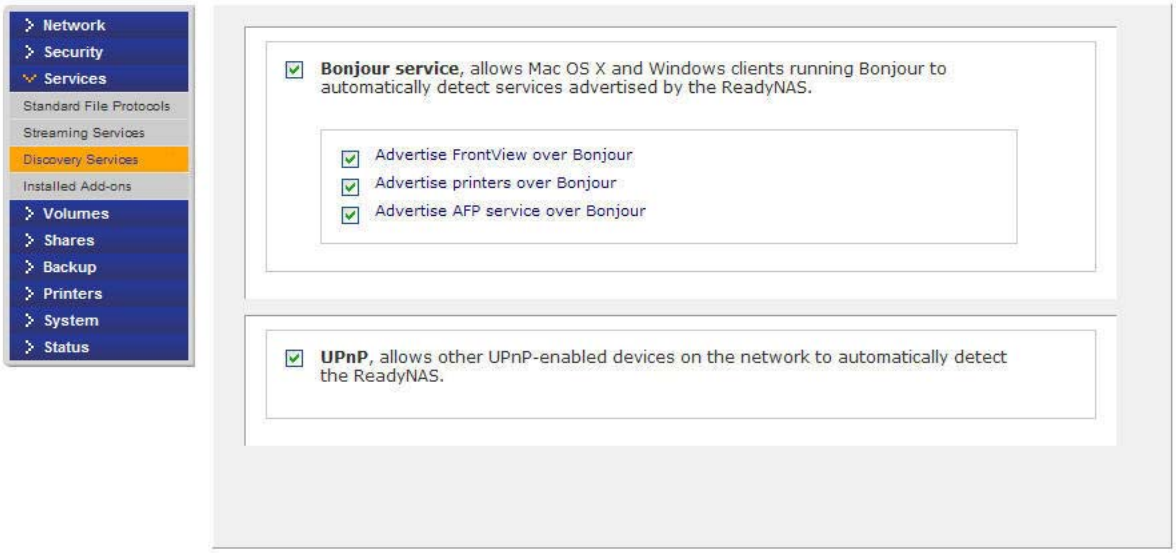
This service is enabled by default and cannot be disabled. Access to FrontView is strictly through HTTPS. If you want remote Web access to FrontView or your HTTPS shares, specify a nonstandard port (the default is 443) that you can forward on your router for better security. You can also regenerate the SSL key based on the hostname or IP address that users use to address ReadyNAS. This allows you to bypass the default dummy certificate warnings whenever users access the ReadyNAS over HTTPS.

Rsync

Rsync is an extremely popular and efficient form of incremental backup made popular on the Linux platform, but is now available for various other Unix systems, as well as Windows and Mac. Enabling Rsync service on the ReadyNAS allows clients to use Rsync to initiate backups to and from the ReadyNAS.

Discovery Services

Bonjour and **UPnP** discovery services are included with the ReadyNAS. You can download and install additional services from the **Add-ons** page at ***http://readynas.com***.



- **Bonjour**

  Bonjour service lets you discover various services on the ReadyNAS and provides a 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 Web site.

- **UPnP**

  UPnP (Universal Plug-n-Play) provides a means for UPnP-enabled clients to discover the ReadyNAS on your LAN.

Installed Add-Ons

You can access an array of new features and services by installing add-ons developed by NETGEAR, NETGEAR's partners, and community developers.

To view and download additional ReadyNAS add-ons that are not pre-installed on your system, visit ***http://readynas.com/addons*** and ***http://readynas.com/community_addons.***

ReadyNAS Remote

The ReadyNAS Remote add-on comes preinstalled and allows secure, remote access to shares on your ReadyNAS without complicated router or VPN setup. Once you access your shares from Windows using File Explorer or from a Mac using Finder, you can easily drag and drop files into your LAN environment.

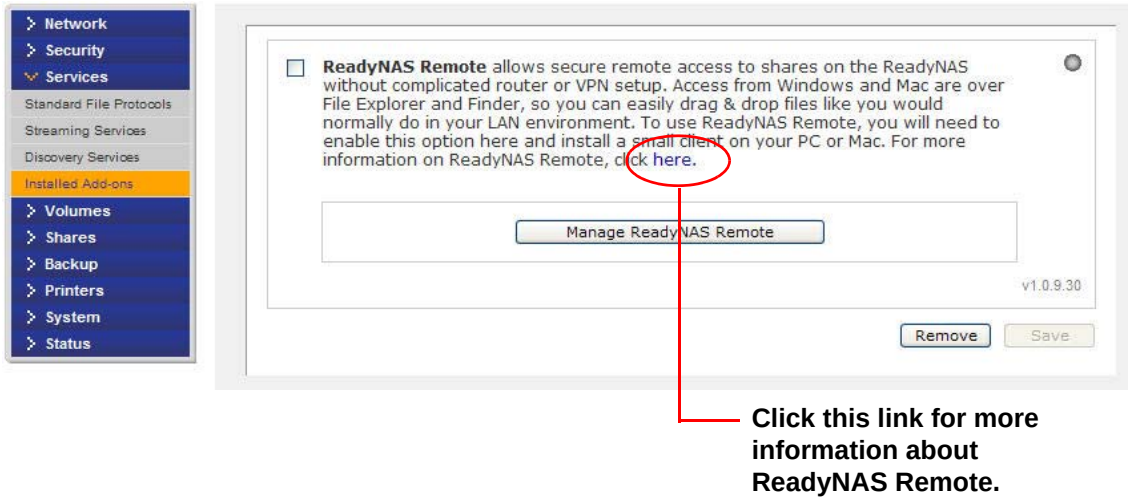
On Windows, you can map a ReadyNAS share to a drive letter, and access the share just as you would any typical local drive on your PC.

To use ReadyNAS Remote, you need to enable the functionality and install a small client on your Mac or PC. See *Remote Access* on page 81 for information about enabling remote access to your ReadyNAS.

To enable ReadyNAS Remote

1. Check the ReadyNAS **Remote** check box and click **Save**.
2. Click the **Manage ReadyNAS Remote** button to allow remote access to the ReadyNAS.

   For more information about how to set up remote access with **ReadyNAS** Remote, click the link on the FrontView Management Console interface, or go to ***http://readynas.com/remote***.



Adjusting System Settings

Use the **System** menu to adjust system settings and access ReadyNAS system functionality described in the following sections:

Clock

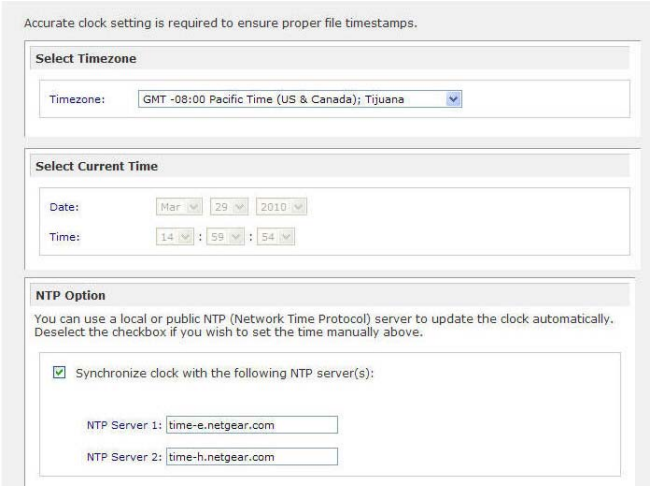
An accurate time setting are required to ensure proper file timestamps. To access the clock screen select **System > Clock** from the main menu.

Select Timezone & Current Time

Use these two sections to set your **Time zone** and the correct **Date and Time**.

NTP Option

You can synchronize the system time on the ReadyNAS 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 available public NTP servers by searching online. For an accurate clock sync, point the NTP server to the Domain IP.



Alerts

If you have specified email address in the contact list, you receive an email alert when a system event that requires attention occurs. For example, a device or enclosure failure, a quota violation, or low disk space warning will generate an email alert.

To access the **Alerts** screen select **System > Alerts** from the main menu. This contains three additional configuration areas, described in the following sections:

Contacts

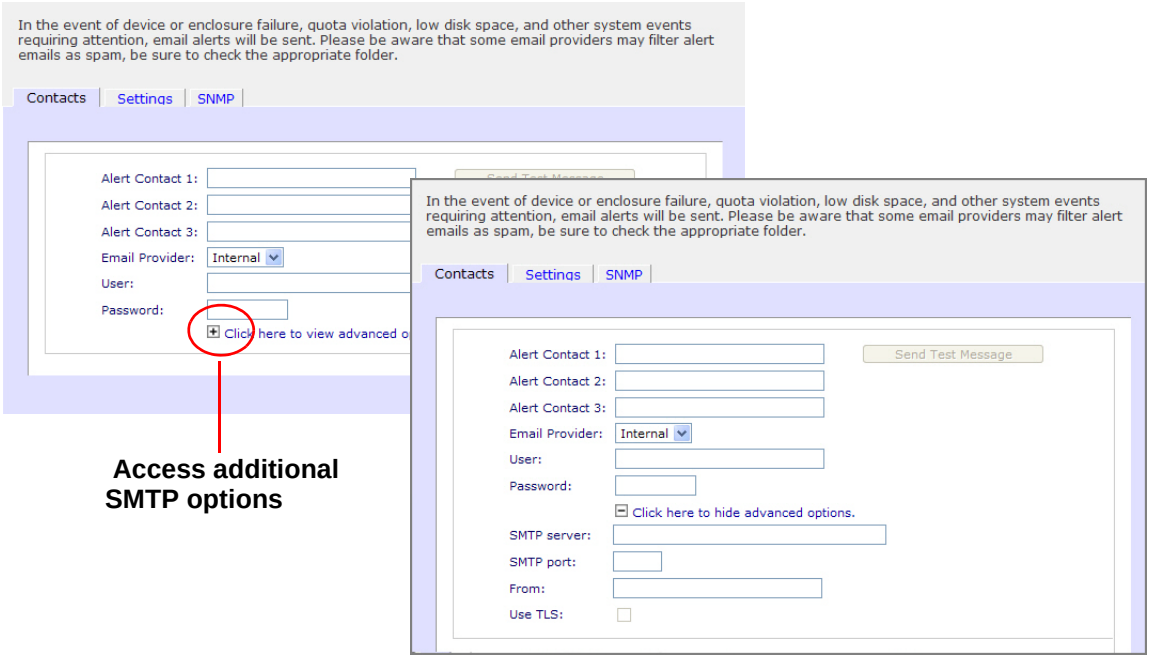
Use the **Contacts** screen to specify up to three email addresses where system alerts will be sent. The ReadyNAS device has a robust system monitoring feature and sends email alerts anytime something appears to be wrong, or when a device has failed. Make sure to enter a primary address and a backup address, if possible.

Use an email address tied to a mobile phone to monitor the device when you are away from your desk.

To set up an email contact:

1. Select an option from a list of popular email providers.
2. Add the user name and password needed to authenticate with the SMTP server.

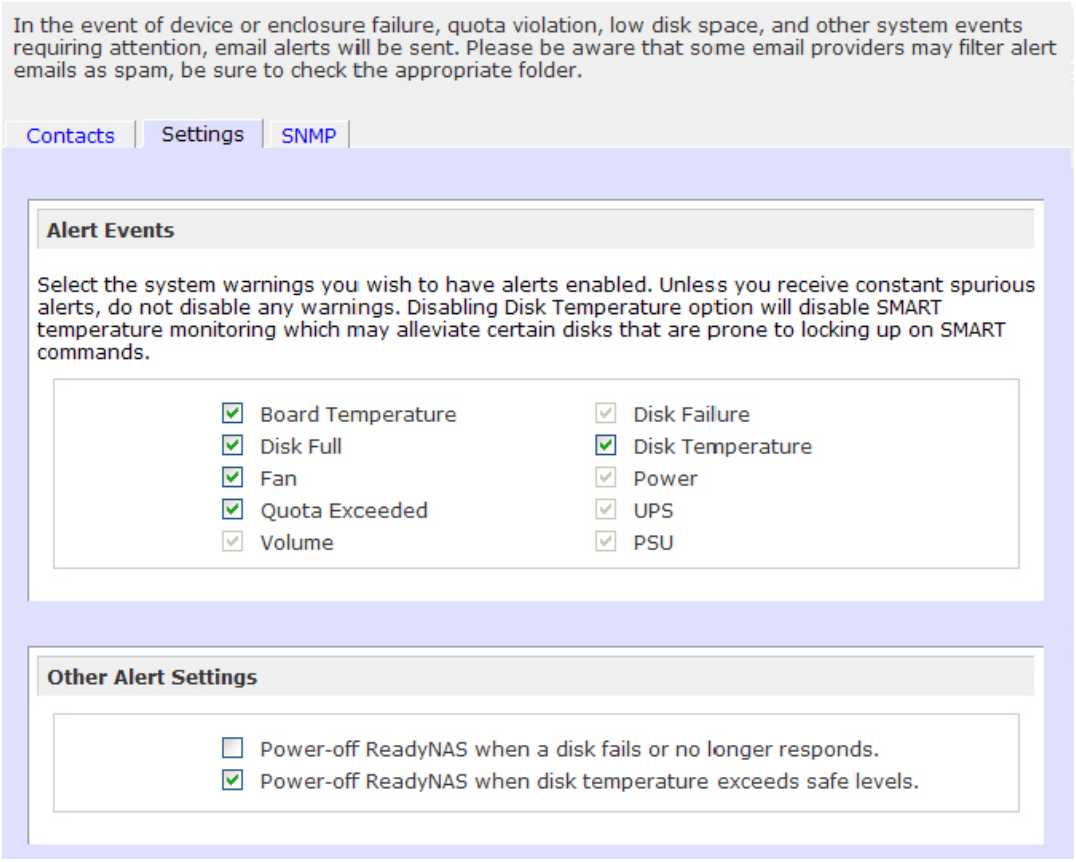
   In cases where the provider is not listed, click the ⊞ button to customize the SMTP setting for your provider.



Settings

ReadyNAS devices are preconfigured with mandatory and optional alerts for various system warnings and failures. Use the **Settings** screen to control the settings for optional alerts.

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

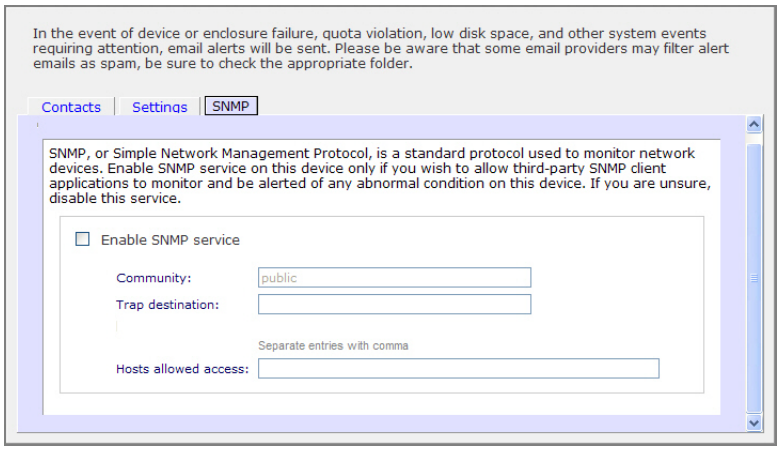


At the bottom of the screen in the **Other Alert Settings** section, there are additional options.

- Select the **Power-off NAS when a disk fails or no longer responds** option to gracefully power off the ReadyNAS if a disk failure or disk remove event is detected.
- Select the **Power-off NAS when disk temperature exceeds safe level** to gracefully power off the ReadyNAS when the disk temperature exceeds the nominal range.

SNMP

ReadyNAS devices can be set to work with SNMP management systems, such as HP OpenView or CA UniCenter, to monitor devices on your network.



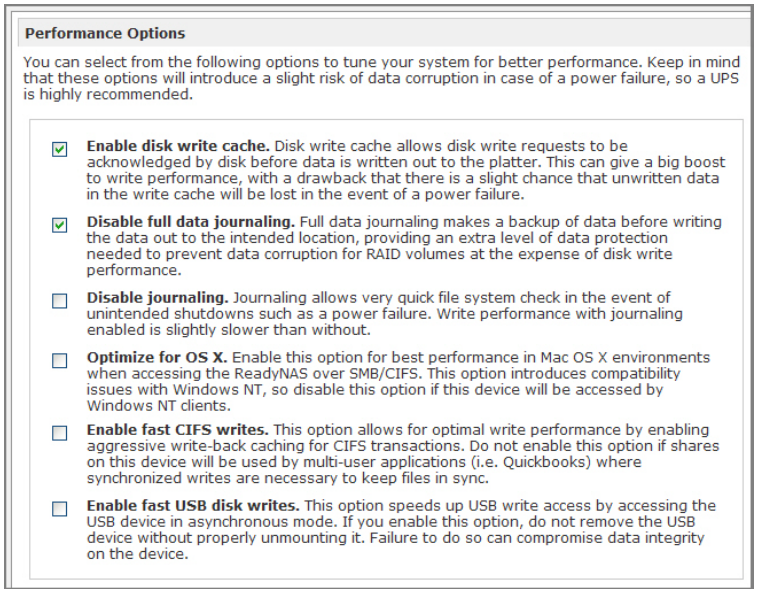
To set up SNMP service:

1. Select the **SNMP** screen 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 a more segregated monitoring scheme.
3. Enter a hostname 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 want to limit SNMP access to only a secure list of hosts, specify the hosts in the **Hosts allowed** access field.
5. Click **Apply** to save your settings.

   When you have saved the SNMP settings on the ReadyNAS, you can import the **NETGEAR SNMP MIB to your SNMP** client application. The NETGEAR MIB can be obtained from the *installation CD* included with your unit, or downloaded from ***http://readynas.com/download***.

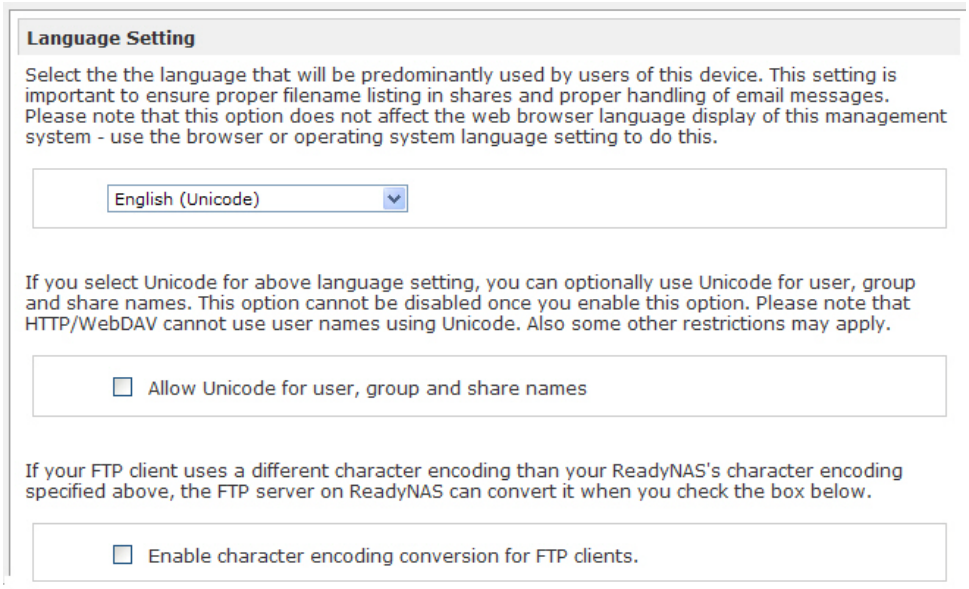
Performance Settings

You can select from several options to tune your system for better performance. Keep in mind that these options will introduce a slight risk of data corruption in case of a power failure, so using a USP is highly recommended. For information on **Performance** settings, see *Chapter 6, Optimization and Maintenance*, *Performance* on page 105.

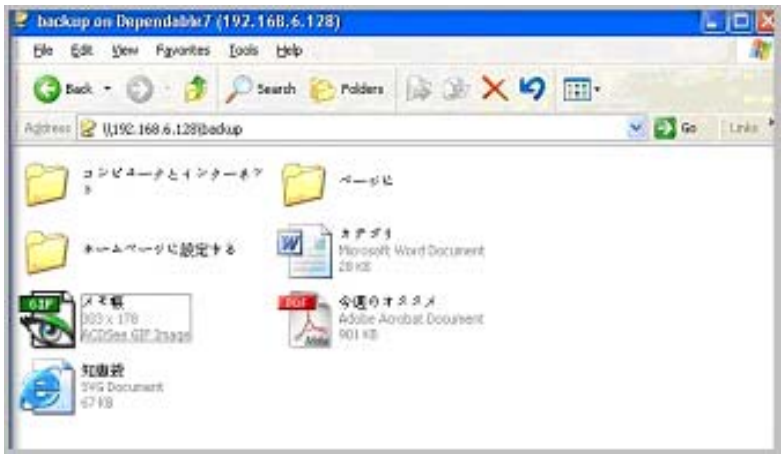


Language Settings

To ensure proper display of file names, use the **Language Setting** screen to set the ReadyNAS to the character set you want to use.



For example, selecting Japanese allows the ReadyNAS to support file names with Japanese names in Windows Explorer.



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

> **Note:** This option does not affect the FrontView display. To change the language in FrontView, adjust the browser language option.

If you want, select the **Allow Unicode for user, group and share names** check box 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.

To convert the ReadyNAS character encoding specified in Unicode to the character encoding used by your FTP client, select the **Enable character encoding conversion for FTP** clients check box.

Update

See *Updating ReadyNAS Firmware* on page 115.

Configure Backup

Use this to set up a system configuration backup for replication purposes. See ***http://readynas.com/configbackup*** for more detailed information.

See also, *Configuring Backup Jobs* on page 87.

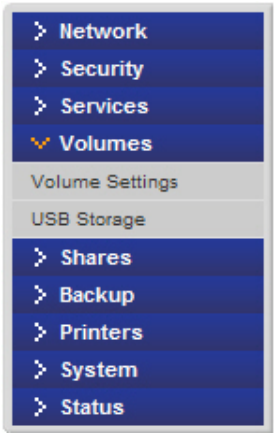
Power

See *Power Management* on page 107.

Shutdown

See *System Shutdown and File System Check* on page 113.

Understanding Volume Management



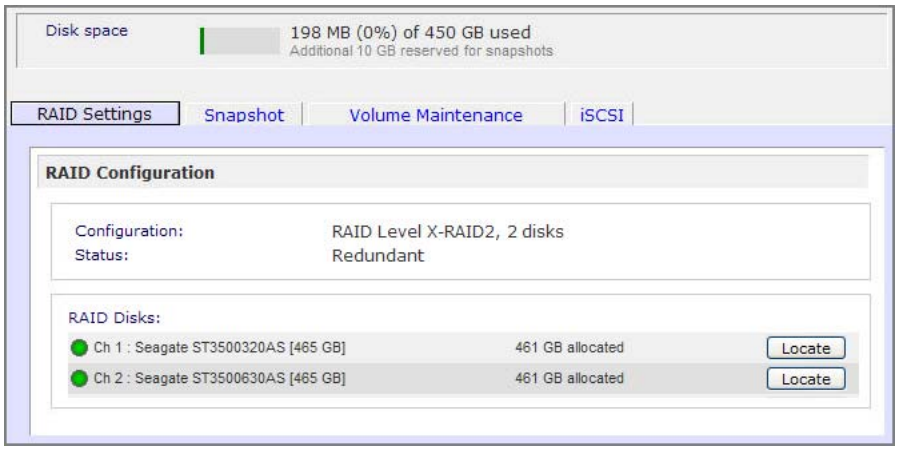
The ReadyNAS family offers the following volume technologies:

- *X-RAID2* on page 41.
- *Flex-RAID* on page 43.
- *USB Volumes* on page 48.
- *iSCSI Volumes* on page 50.

X-RAID2

X-RAID2™ is the NETGEAR auto-expandable RAID technology that allows you to expand your ReadyNAS capacity by adding additional disks, or replacing existing disks with higher capacity disks.

With X-RAID2, you do not need to know intricate details about RAID, except that as you need more space, your volume can grow without the need to reformat your drives or move your data to another location. Since the expansion happens online, you can continue to use the ReadyNAS while the underlying volume capacity increases.



Adding a Second Disk for Redundancy

With only one disk in your ReadyNAS, the X-RAID2 volume has no redundancy, and provides no protection from disk failure. However, if and when you feel the need for redundancy, add a new disk with at least the same the capacity as the first disk. You can elect to power off the ReadyNAS and add the disk, or you can hot-swap the disk while the ReadyNAS is online.

Depending on the size of the disk, within a few hours, your data volume will be fully redundant. Since the process occurs in the background, you can continue to use the ReadyNAS without interruption.

Adding More Disks

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

With X-RAID2, add the third disk using the ReadyNAS hot-swap disk tray. When adding multiple disks at the same time, power down the ReadyNAS, add the disk(s), and turn the unit back on. The X-RAID2 device initializes and scans the newly added disk(s) for bad sectors. This is done in the background, so you can continue using the ReadyNAS while the expansion proceeds. An email notice is sent when the volume has completed the expansion.

Replacing Disks for More Capacity

When more space is needed, but you are unable to install additional disks, you can still expand the volume capacity by replacing the existing disks with higher capacity disks.

The ReadyNAS supports hot-swapping, so you can swap disks without turning off the unit. Simply replace the first disk, and the ReadyNAS synchronizes the disk with data from the removed disk. This process can take 30 minutes or longer, depending on disk capacity, but you can continue to use the ReadyNAS while the new disk synchronizes. Upon completion, replace the second disk with another higher capacity disk, and allow that disk to synchronize. X-RAID2 expands the volume when a minimum of two disks are replaced. When you have replaced the number of disks you want to replace (minimum of two), reboot the ReadyNAS to initiate the background expansion. An email notice is sent when the volume has completed the expansion.

Changing RAID Modes

X-RAID2 is the default technology used by ReadyNAS. However, for a more flexible option, you can set ReadyNAS to Flex-RAID mode. This option allows you to assign a standard RAID level so you specify a hot spare, and create multiple volumes.

The process involves setting the ReadyNAS back to Factory Default and using RAIDar to configure the volume during a 10-minute delay during boot.

WARNING!

Setting the ReadyNAS to the factory default will erase all data.

For instruction on how to change RAID modes, see *Changing between X-RAID2 and Flex-RAID Modes* on page 46.

For more about RAID, X-RAID2 and Flex-RAID, see *Appendix A, Understanding RAID*.

Flex-RAID

Flex-RAID technology utilizes the industry-standard RAID levels 0, 1, 5 and 6.

Flex-RAID advantages include:

- 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, 5, or 6 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.

Reconfigure Volume C

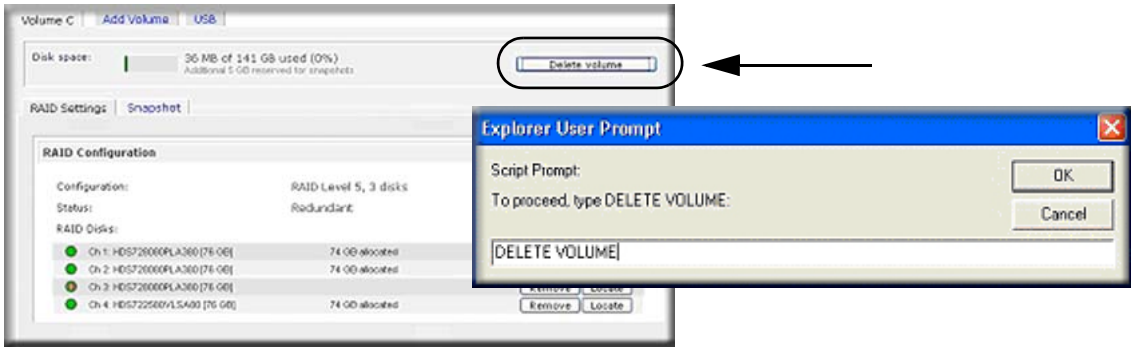
If you want to reconfigure the default Flex-RAID Volume C, split it into multiple volumes, specify a different RAID level, or specify a larger reserved space for snapshots, you need to reconfigure your volume. The first step is to delete the existing volume you want to replace.

To delete a volume:

1. Select the **Volume** screen of the volume you want to delete (if there are multiple volumes).
2. Click **Delete Volume** (in this case only Volume C is configured).
3. You are asked to confirm your intention by typing **DELETE VOLUME**.

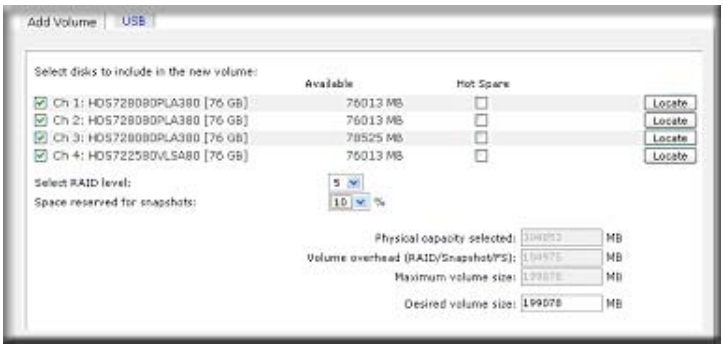
WARNING!

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



Adding a Volume

After deleting the volume, the **Add Volume** screen shows the available configurable space on the physical disks. All disks are selected by default, and you can specify a hot spare disk if you want. 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.



To add a volume:

1. **Select the disks**. The example shows that the first three disks are selected, and none of them are specified as a hot spare.
2. **Select the RAID level**. This will determine how the redundancy, capacity utilization, and performance are implemented for the volume. Typically in a configuration of three or more disks, NETGEAR recommends RAID level 5. In the example, RAID level 5 is selected for the disks.
3. **Specify the reserve space for a snapshot.** Next, select the percentage of the volume you want to allocate for snapshots. You can specify 0 if you want 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, 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 the example, 10 percent of the volume will be reserved for snapshots.

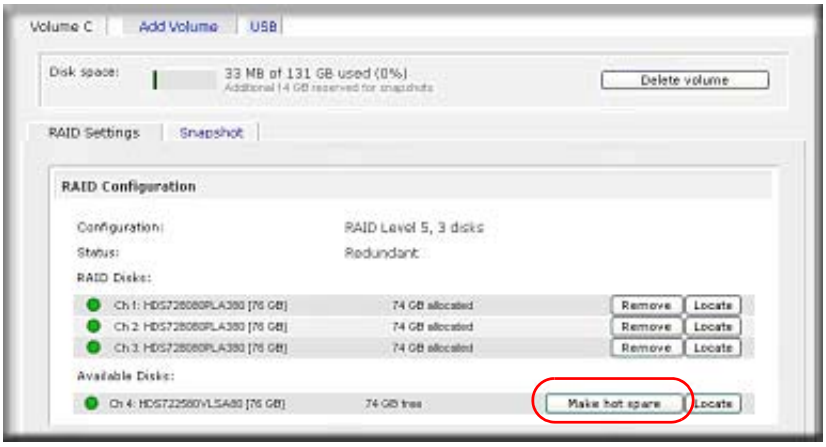
   If you do not reserve space for snapshots, the snapshot screen is not displayed in the Volume screen.
4. **Specify the volume size**. After you specify the volume parameters, enter the appropriate volume size if you want to configure a smaller volume size than the maximum displayed. The resulting volume 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 you reboot, an email notification is sent when the volume has been added. Use the RAIDar utility to reconnect to the ReadyNAS device.

RAID Settings

After a volume is added, return to the **Volume** screen and click the **RAID Settings** screen to display the current RAID information and configuration options for the volume.

Notice that the disk on Channel 4 that was not configured in the example is listed in the **Available Disks** section. To add this disk as a hot spare click **Make hot spare**.



To remove a disk from the volume, click **Remove**. The volume will still be available but in a non-redundant state. An additional disk failure would render this volume unusable.

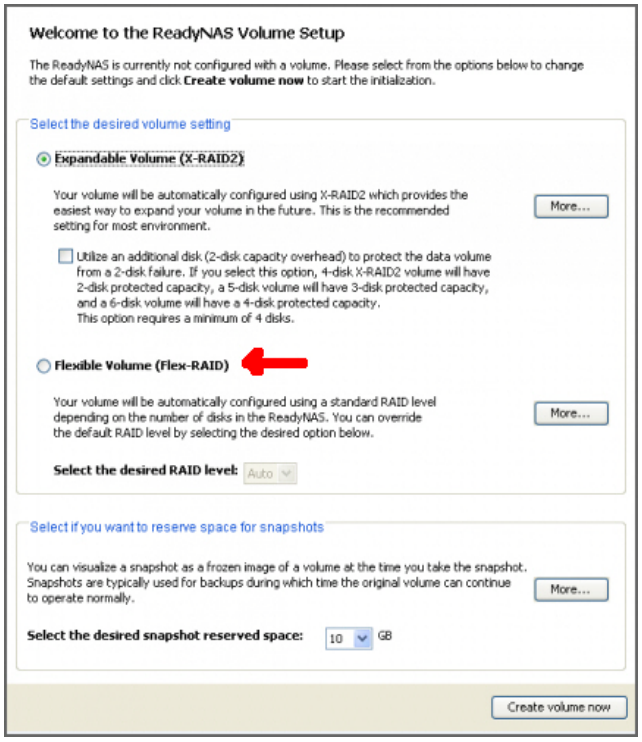
> **Note:** The **Remove** operation is a maintenance feature. Do not use it in a live environment. Its function is equivalent to hot-removing the disk or simulating a disk failure.

The **Locate** option is a way to verify that a disk is correctly situated in the expected disk slot. When clicked, it causes the disk LED to blink for 15 seconds. This is useful to identify a specific disk.

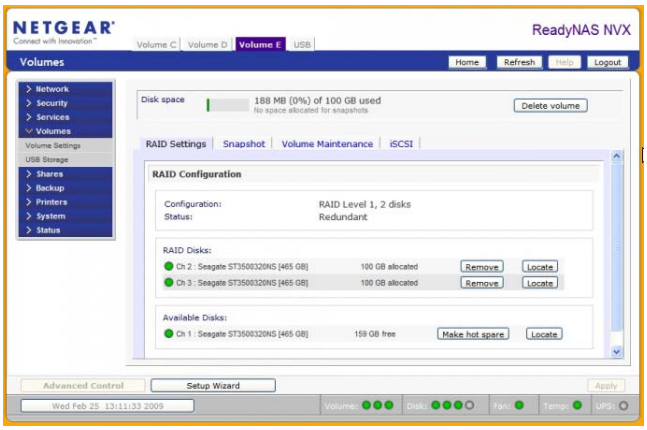
Changing between X-RAID2 and Flex-RAID Modes

RAID 0, 1, and 5 are part of the Flex-RAID RAID levels. To switch from Flex-RAID mode to X-RAID2 (expandable RAID), you need to backup your data first, and then reset your ReadyNAS back to factory default.

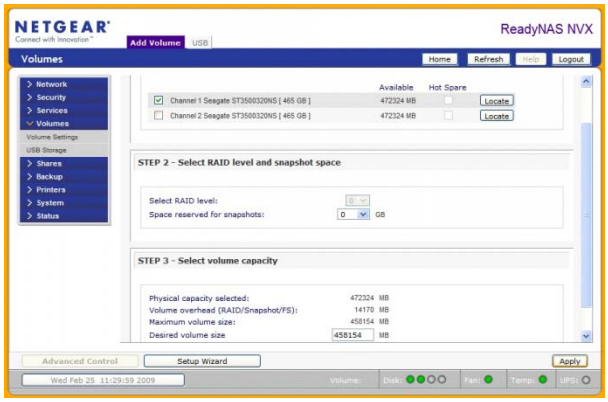
During the factory default process, you have a 10-minute window during the boot process to click the **Setup** button in RAIDar, and set the box to the desired RAID mode (Flex-RAID or X-RAID2). The RAIDar utility sends a prompt to **Click Setup** during this 10-minute time frame.



After selecting Flex-RAID, the system will create a RAID 1 volume automatically. You need to delete the existing volume first:



Once that's done, you should be able to select which type of RAID array you wish to create, as well as which drives it should be created on:

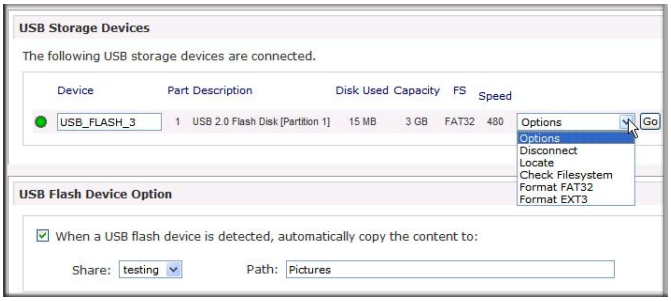


After creating the volume, you will be prompted to restart the device before the volume is added:

If you have already put data on it, and the RAID level is X-RAID2, you will need to backup your data and start again.

USB Volumes

The **USB** screen displays the USB disk and flash devices connected to the ReadyNAS, and offers various options for these devices. A flash device appears as USB_FLASH_1, and a disk device appears as USB_HDD_1.



When no USB is attached, the “No USB storage devices detected” message displays.

When multiple devices are attached, they are appended by an increasing device number, for example, USB_HDD_2.

When the device contains multiple partitions, the partitions are listed beneath the main device entry.

Partitions

Partitions on the storage devices must be one of the following file system formats: FAT32, NTFS, EXT2, EXT3. To the right of the access icons are command options.

The following commands are available:

Table 3. Partian Commands

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 to the disks and that the file system is correctly closed. The Disconnect option unmounts all partitions on the device. Once the device is disconnected, physically remove and re-connect to the network storage to regain access the USB device,.
Locate	In cases where you attach multiple storage devices and want to determine which device corresponds to the device listing, the Locate command causes the device LED to blink, if the device is 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 network storage 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 uses the new name rather than the default USB_FLASH_n or USB_HDD_n naming scheme.

The USB storage shares are listed on the **Share** screen, and access restrictions can be specified there. The share names reflect the USB device names. USB storage devices are shared using the name of the device appended with the partition number. To change the base device name select **Volumes > USB Storage**.

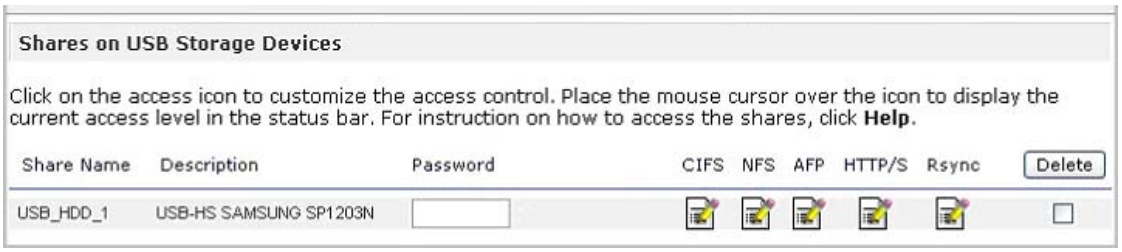
USB Flash Device Option

Toward the lower portion of the USB Storage screen is the **USB Flash Device Option** section, where you can elect to copy the content of a USB flash device to a specified share on connection. Files are copied to a unique timestamp folder to prevent existing data from being overwritten. This is useful for uploading pictures from digital cameras and music from MP3 players without 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

USB volume name and share access settings are persistent across mounts. The ReadyNAS attempts to remember the name as long as there is a unique ID associated with the USB device so that the next time the device is connected, the same share name or names will be available. Share access restrictions are saved across disconnects.



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 allows easy sharing of the USB device with other network storage and PC systems.

iSCSI Volumes

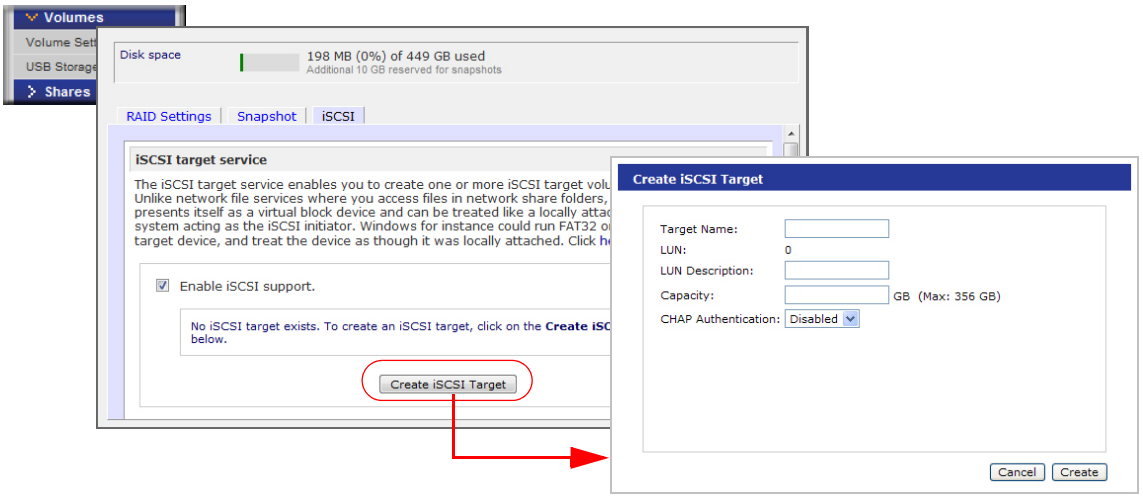
Use the **iSCSI** service to create one or more iSCSI volumes on the ReadyNAS.

> **Note:** iSCSI is not available on the ReadyNAS 1500.

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, select **Volumes > Volume Settings > iSCSI**.



To enable iSCSI support, click **Create iSCSI Target**, and enter the name of the target you want, and the capacity you want to reserve for this target device. Maximum capacity is slightly less than the full free space on the ReadyNAS. If you want 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.

For instructions on setting up iSCSI access from various operating systems, see the article, *Setting up the ReadyNAS to Be an iSCSI Target* at ***http://readynas.com/iSCSI*** on ReadyNAS.com.

Manage User Accounts

3

The topics in this chapter cover the setup and management of the ReadyNAS Network Attached Storage System in your network.

This chapter contains the following sections:

- **Setting Security Access Modes**
- **Setting Up User and Group Accounts**
- **Changing User Passwords**

Setting Security Access Modes

The ReadyNAS offers the **User** and **Domain** security access options.

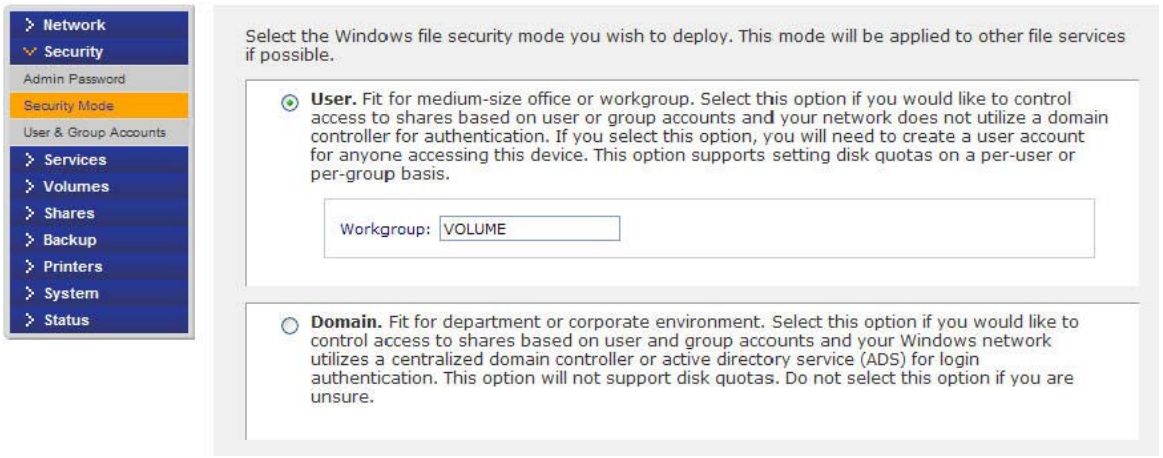
Select the appropriate option based on the required level of security and your current network authentication scheme.

User

NETGEAR recommends user security mode for the small and medium-size office or workgroup environments. User mode allows you to set share access restrictions based on user and group accounts. In this security mode, the administrator must set and maintain user and group accounts on the ReadyNAS device itself. See *User Security Mode* on page 53 for more information about using this option.

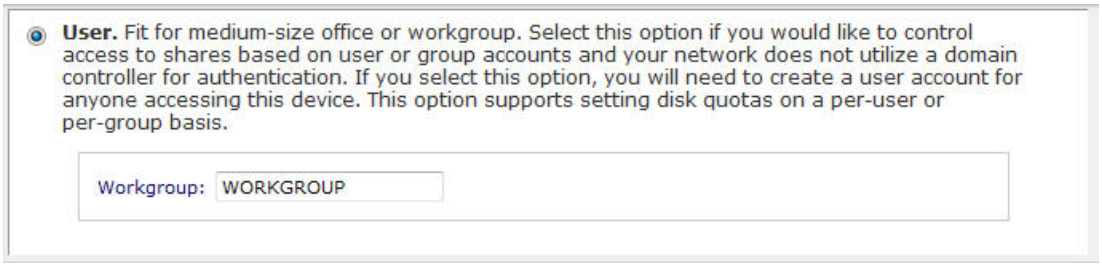
Domain

The Domain security mode is appropriate for department or corporate environments where a centralized Windows-based domain controller or active directory server is present. The ReadyNAS device integrates into this environment by creating a trusted relationship with the domain or ADS authentication server and allowing all user authentications to occur there. This eliminates the need for separate account administration on the device itself. See *Domain Security Mode* on page 54 for more information about using this option.



User Security Mode

This mode is ideal for small and medium-size offices or workgroups. Select the **User** security option to control access to shares based on user or group accounts and if your network does not utilize a domain controller for authentication.



In User security mode, the administrator specifies a workgroup name, and creates user and group accounts, and has control over how much disk space is allocated for each user or group. A user account needs to be created for anyone accessing this device. This option supports setting disk quotas on a per-user or per-group basis.

Each user is given a home share on the ReadyNAS device so personal data remains private. This home share is accessible only by that user, and by the administrator to perform backups. The option to automatically generate the private home share is controlled in the **Accounts/Preferences** screen, and can disabled as needed.

> **Note:** Private home shares are accessible only by users using CIFS (Windows), AFP (Mac), and FTP/S protocols.

You need the following information to set up the ReadyNAS for User security mode:

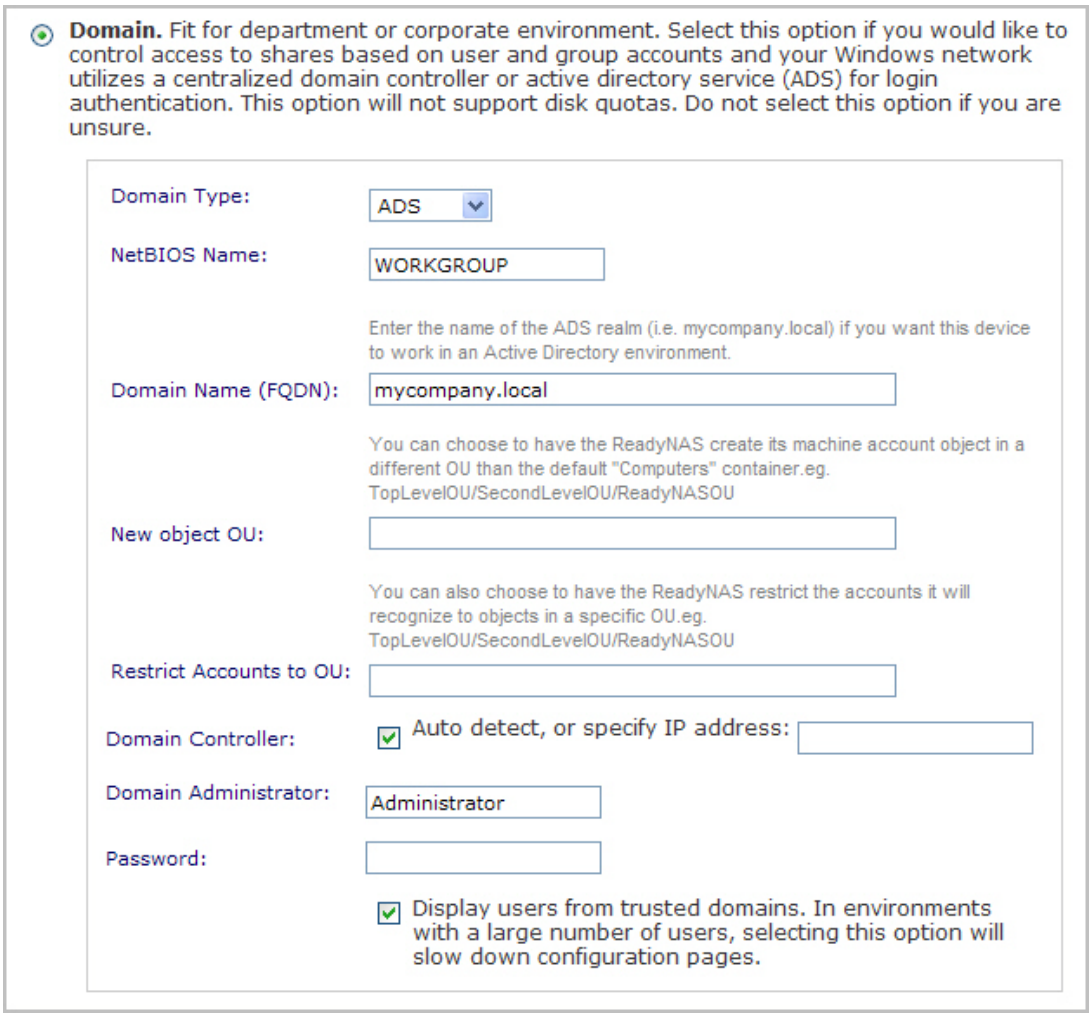
- Workgroup name
- Group names you want to create (for example, Marketing, Sales, Engineering)
- User names you want to create (plus email addresses if you will be setting disk quotas)
- Amount of disk space you want to allocate to users and groups (optional)

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

For the **Domain** security option, you need to create a trusted relationship with the domain controller or the active directory server (ADS) that will act as the authentication server for the ReadyNAS device. At this time ReadyNAS can be used in a domain environment that serves up to 32,000 users.



You need the following information to set up the ReadyNAS for Domain security mode:

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

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

Note: If there are a large number of users in your domain, the FrontView management system might slow to an unusable state. To help performance, you might want to clear the **Display users from trusted domains**... check box.

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.

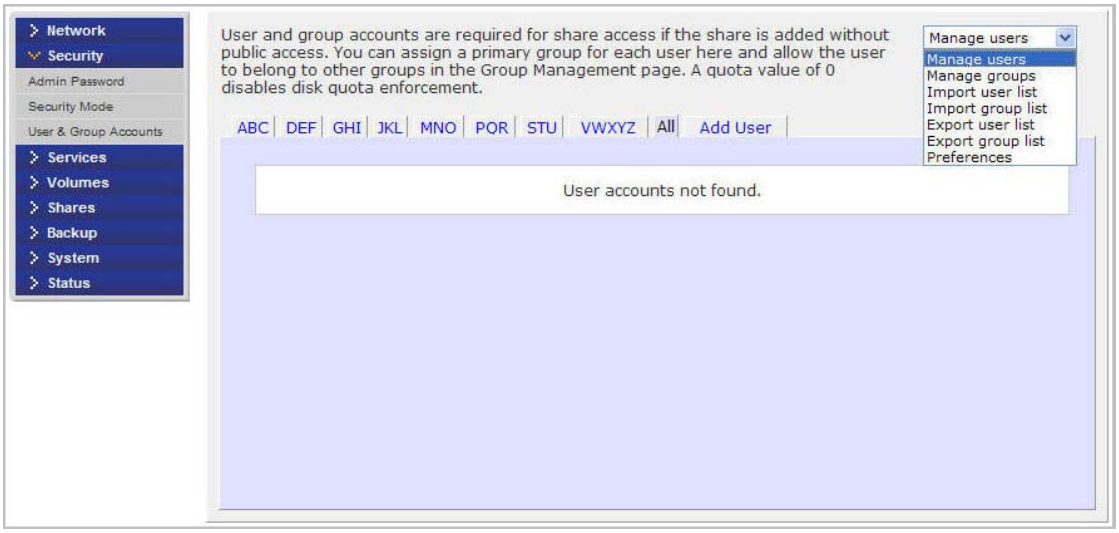
Accounts are managed on the domain controller. The ReadyNAS pulls the account information from the controller and displays it on the Accounts screen if you have the **Display users from trusted domains**… option enabled. If you want, you can assign a disk quota to the domain users and groups. If email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

Setting Up User and Group Accounts

Access to shares requires the correct login authentication. Each user and group can be set to the specific access required. For example, company financial data can be restricted to individual users, or users belonging to one particular group.

To manage user and group accounts, select **Security > User & Group Accounts**.

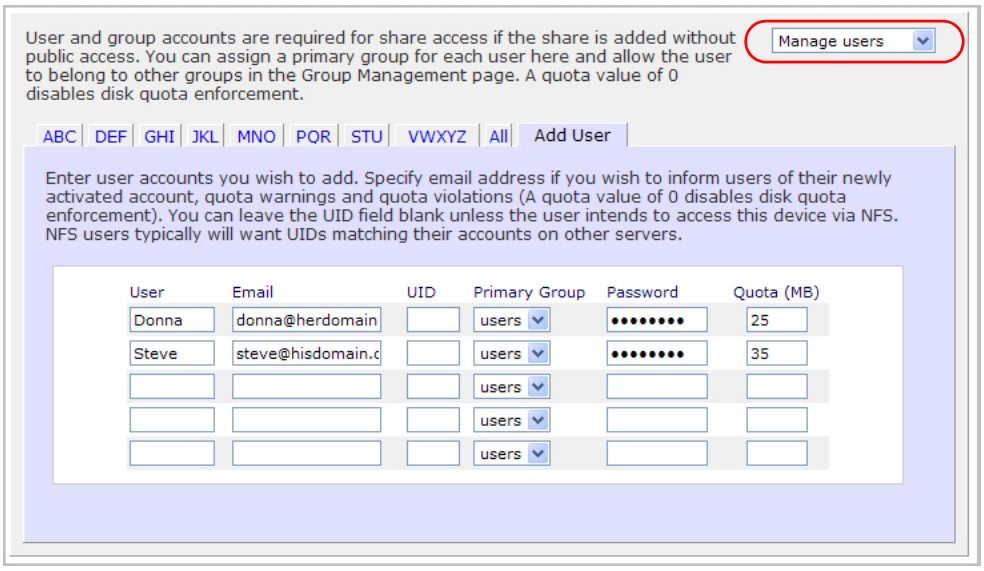
The pull-down menu provides access to several options, as described in the following sections.



Managing Users

To manage user accounts:

1. Select **Manage Users** from the pull-down menu.
2. Click the **Add User** screen to add a new user. You can add up to five users at a time.

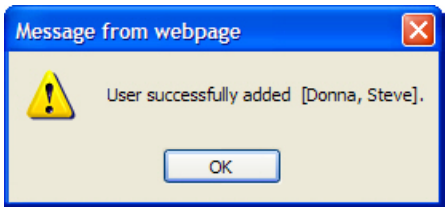


For each user, add the following information:

- User name
- Email address
- User ID
- Group association from the Primary Group pull-down menu
- Password
- Disk quota

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

Only the Username and Password fields are required; however, you should specify a user email address if you intend to set up disk quotas. Without an email address, the user will not be warned when disk usage approaches the specified disk quota limit.



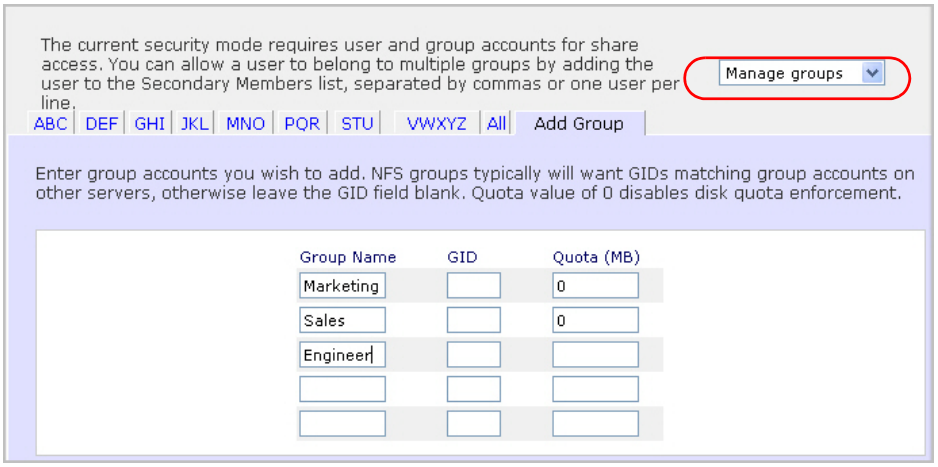
If you do not want to assign a disk quota, enter 0.

If you want 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.

Managing Groups

To add a new group:

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



2. Select the **Add Group** screen.

   You can add up to five groups at a time. If you expect to have just one large 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.

Importing User Lists

You can upload a CSV (comma separated value) formatted file containing the user account information. The file format is:

name1,password1,group1,email1,uid1,quota1

name2,password2,group2,email2,uid2,quota2

name3,password3,group3,email3,uid3,quota3

:

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. Set the default using the **Preferences** option. See *Preferences* on page 63.
- Email 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 want 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*. He belongs to the default group, receives no email notification, has a UID assigned automatically, and has a default quota.

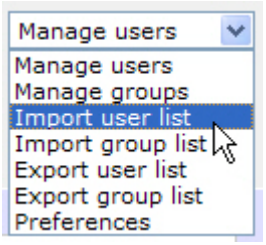
\barney,23stone,barney@bedrock.com

In this example, user *barney* has a password set to *23stone*. He belongs to the default group, receives email 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*. She belongs to the group *ourgroup*, receives email notification sent to *wilma@bedrock.com*, has a UID set to *225*, and a quota set to *50Mb*.

To import a user list:



1. Select **Security > User and Group Accounts.**
2. Select **Import User List** from the pull-down menu in the upper right corner.
3. Click **Browse** to select the file.
4. Click **Apply** to save your settings.

Importing Group Lists

A user can belong to multiple groups. Once user accounts are created, you can place users in secondary groups. 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 the Marketing and Sales groups.

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

You can view or change your groups by clicking the alphabetical index screen, or click **All** to list all groups.

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 values) formatted file containing the group account information.

The file format is:

name1,gid1,quota1,member11:member12:member13

name2,gid2,quota2,member21:member22:member23

name3,gid3,quota3,member31:member32:member33

:

Note the following:

- Spaces around commas are ignored.
- The name field is required.
- Quota is set to the 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 want 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.

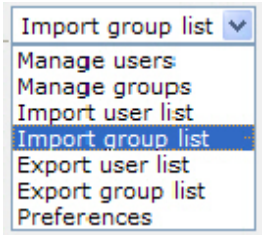
rubble,1007,5000,barney:betty

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

To import a group list:

Use this option to upload a CSV (comma-separated values) formatted file to simplify adding a list of users. Click **Help** for format specification and examples

1. Select **Security > User and Group Accounts.**
2. Select **Import group list** from the pull-down menu in the upper right corner.
3. **Click Browse** to locate the file containing the group list and upload a CSV (comma-separated values) formatted file containing the group account information.
4. Click **Apply** to save your settings.

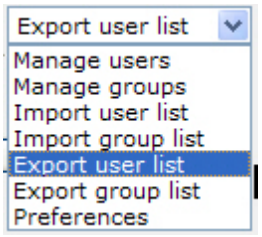


Exporting User Lists

You can export the user account list on the device into a CSV (comma-separated values) formatted file and have it sent by email. The file will also be backed up in the admin user home directory.

To export a user list:

1. Select **Security > User and Group Accounts.**
2. Select **Export user list** from the pull-down menu in the upper right corner.
3. Enter an email address and click the **Send user list** button.
4. Click **Apply** to save your settings.

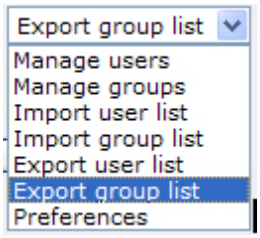


Exporting Group Lists

You can export the group list on this device into a CSV (comma-separated values) formatted file and have it sent by email. The file will also be backed up in the admin user home directory.

To export a group list:

1. Select **Security > User and Group Accounts.**
2. Select **Export group list** from the pull-down menu in the upper right corner.
3. Enter an email address and click the **Send user list** button.
4. Click **Apply** to save your settings.

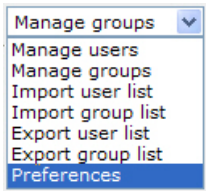


Preferences

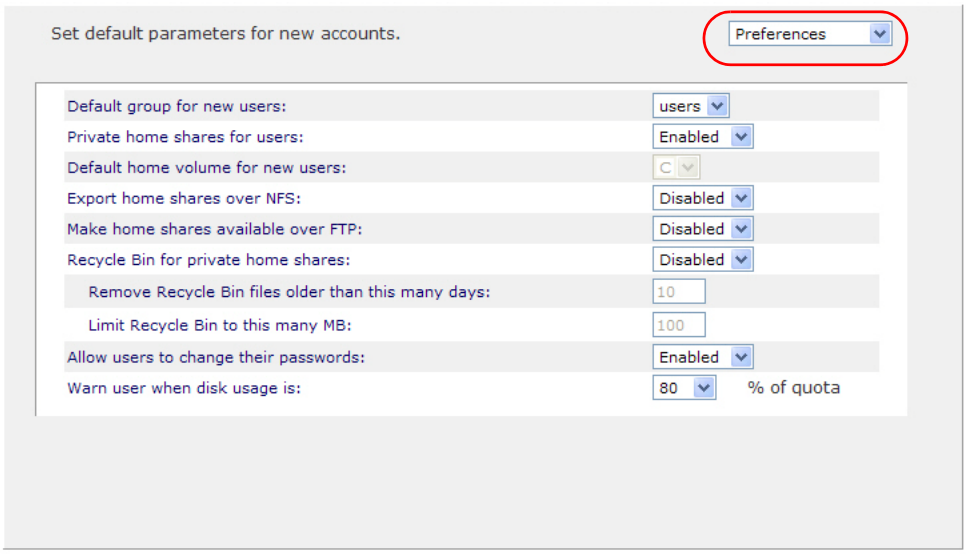
Use the **Preferences** option to set default parameters for new accounts.

To set account preferences:

1. Select **Preferences** from the pull-down menu in the upper right corner.



2. Set the parameters on the screen.



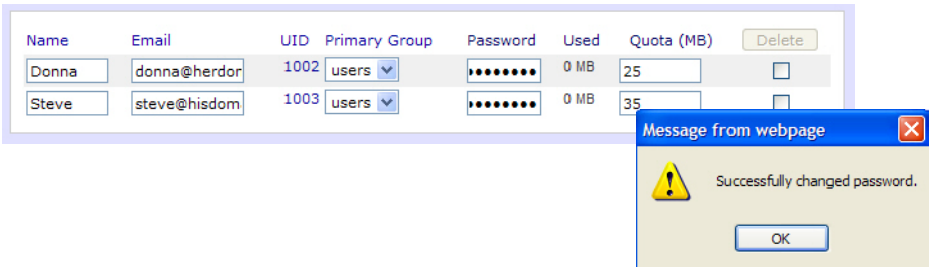
3. Click **Apply** to save your settings.

Changing User Passwords

In User security mode there are two ways user passwords can be changed.

1. The preferred method is to allow users to change their own passwords.
   a. Open a Web browser and use your existing password to log in to access the Web share listing screen at ***https://<ip_addr>/***.
   b. Select the **Password** screen, and follow the prompts to set a new password.

      This encourages users to change their passwords on a more regular basis for enhanced security, and relieves the administrator from this task.
2. Optionally, the administrator can change the passwords.
   a. Select **Security > User & Group Accounts.**
   b. Select **Manage Users** from the pull-down menu.
   c. Select the user whose password needs to be reset.
   d. Enter a new password in the **Password** field.
   e. Click **Apply to save changes.**



Note: In Domain security mode, the Password screen does not appear. User passwords in Domain mode must be set on the domain or ADS server.

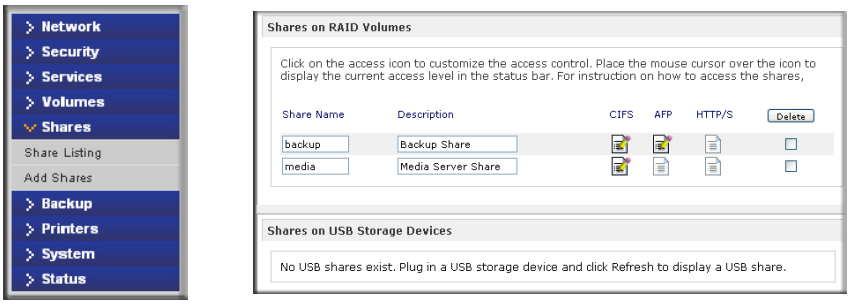
Manage & Access Shares

4

This chapter discusses managing and accessing data from the following operating systems and protocols, and contains the following sections:

Managing Shares

Shares enable you to organize the information stored on a volume. The administrator has access to that information and sets permissions for other users and groups. For example, for generic policies and forms, like blank expense reports, everyone should be able to access them. For sensitive data, like financial information, only the finance group and specified personnel should be granted access to it.



The Shares screen provides share service options for the ReadyNAS device, which includes share management (including data and print shares), volume management, and share service management.

Adding Shares

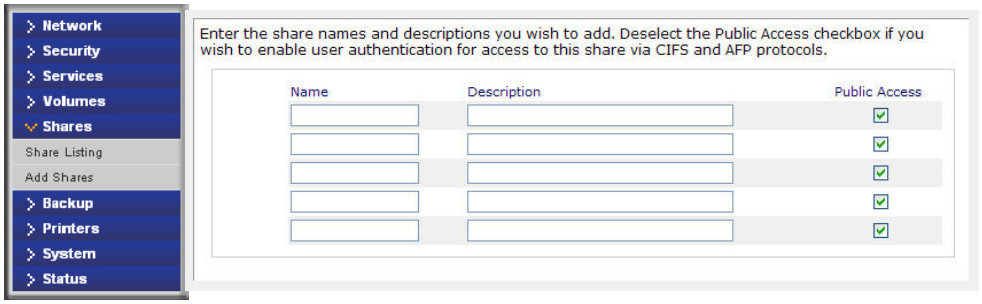
To add a share:

1. From the main menu, select **Shares > Add Shares**.

   If more than one volume is configured, click the volume where you want to add the share.

2. Enter the share name and description.

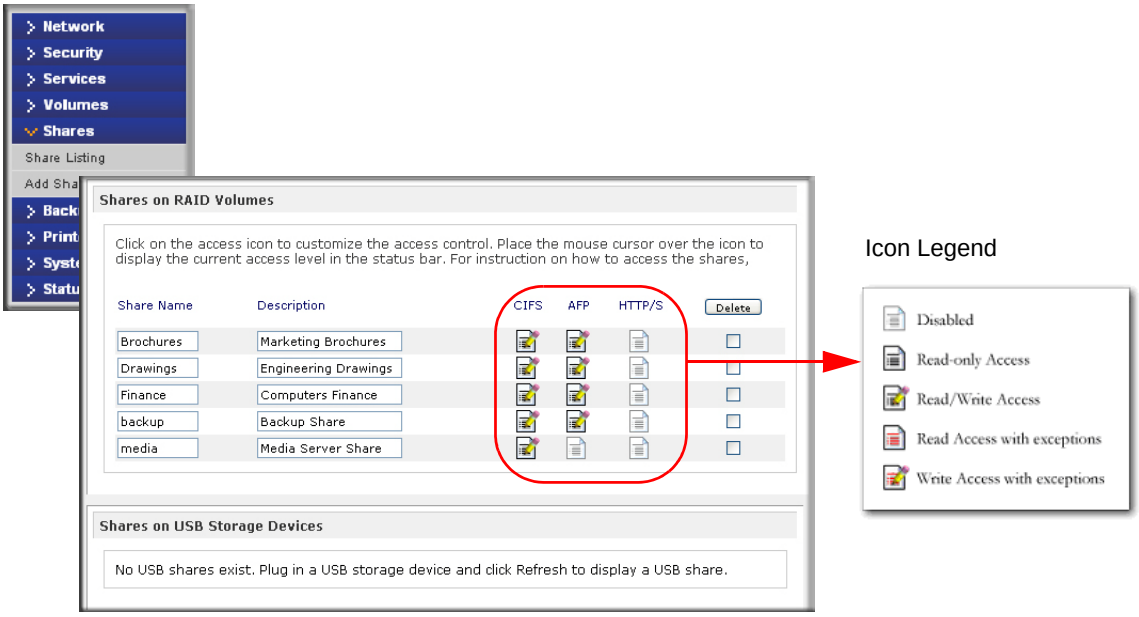
   Once you finish adding the shares, they will be accessible from different client operating systems, as described later in this chapter.



Note: Enabling public access means anyone on the network without a user account on the ReadyNAS can access the share.

Fine-Tuning Share Access

To manually fine-tune share access, select **Share Listing** once the shares are added.



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:

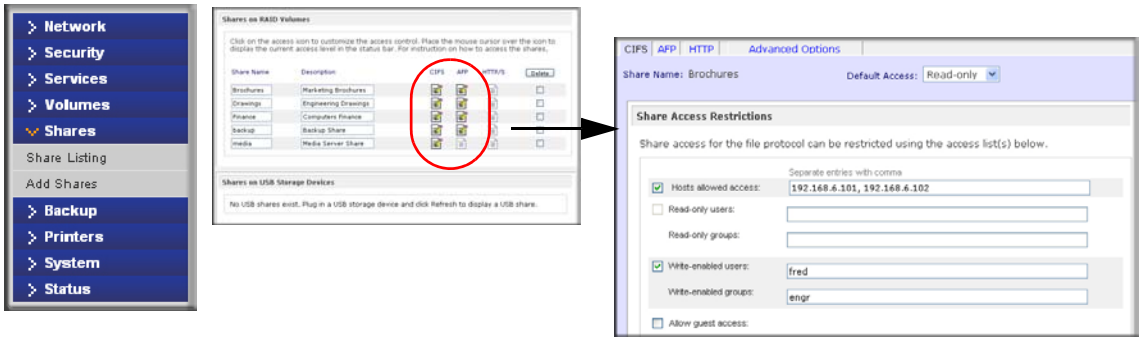
- **Disabled**. Access to this share is disabled.
- **Read-only Access**. Access to this share is read-only.
- **Read/Write Access**. Access to this share is read/write.
- **Read Access with exceptions**. Either (1) access to this share is read-only and allowed only for specified hosts, (2) access is 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.

To set the access rules for each file protocol, click the access icons to display the **Share Options** screen. 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 the **file system** icon.



Share Access Restriction

To limit share access to particular users or groups, 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, to allow read-only access to all, and read/write access only to user *fred* and group *engr*, set the following:

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

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

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:

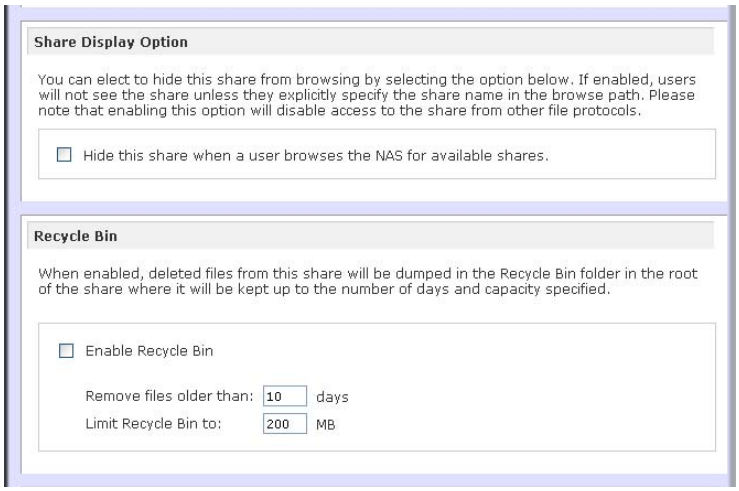
- Default: Disabled
- Hosts allowed access: 192.168.2.101, 192.168.2.102
- Read-only users: mary, joe
- Read-only groups: marketing, finance
- Write-enabled users: fred
- Write-enabled groups: engr

To grant guests access to this share, select the **Allow** guest access check box.

Share Display Option

Restricting access to a share does not prevent users from seeing the share in the browse list. In certain instances, such as backup shares, you might want to prevent users from seeing it.

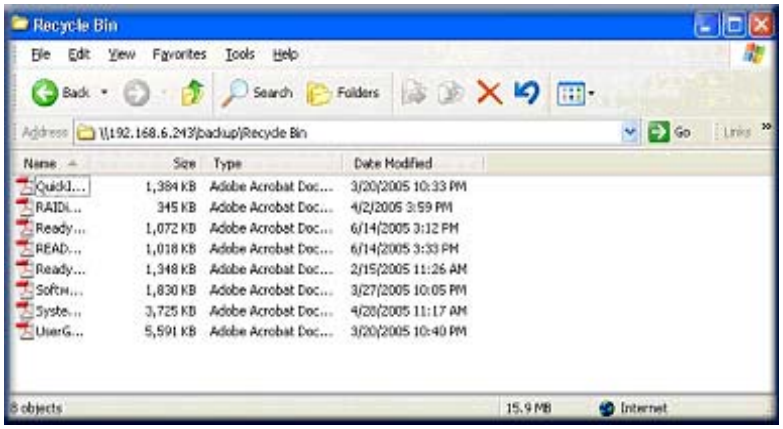
To hide a share, select the **Hide this share** check box. Users with access to this share must specify the path explicitly. For example, to access a hidden share, enter **\\host\share** in the Windows Explorer address bar.



Recycle Bin

A Recycle Bin can be enabled for each share for Windows users. Use the **Enable Recycle Bin** option is shown at the bottom of the CIFS screen.

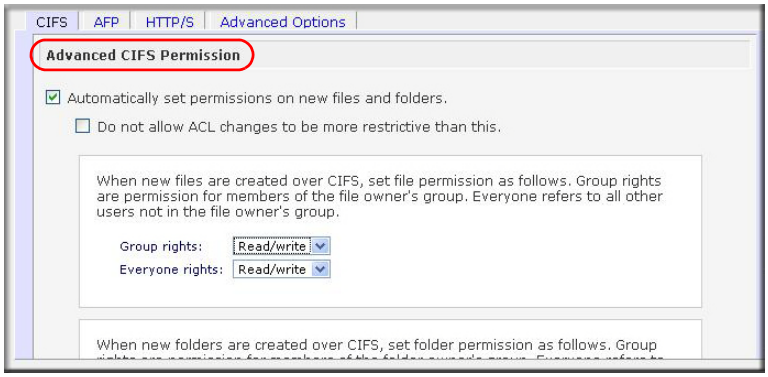
When this check box is selected, whenever a file is deleted, the file gets inserted into the **Recycle Bin** folder in the share rather than being permanently deleted. This allows for a grace period during which users can restore deleted files.



You can specify the grace period by setting how long to keep the files in the Recycle Bin and how large the Recycle Bin can get before the files are permanently erased.

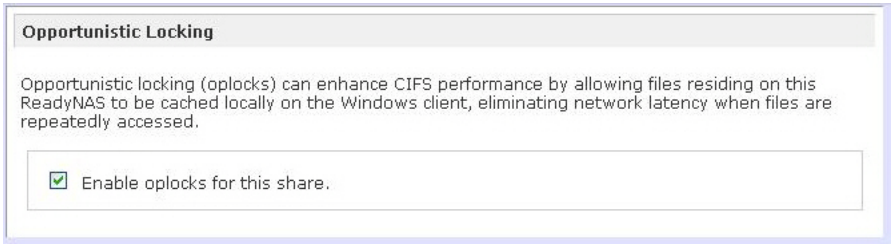
Advanced CIFS Permission

The **Advanced CIFS Permission** section offers options for setting the default permission of new files and folders created through CIFS. The default permission for 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. The default permission can be changed to meet additional security requirements.



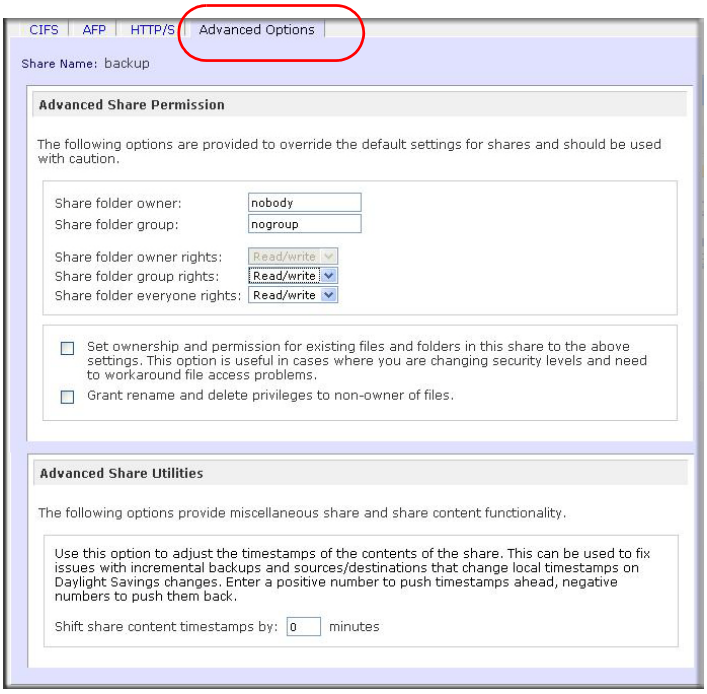
Opportunistic locking, often referred to as oplocks, enhances CIFS performance by allowing files residing on the ReadyNAS to be cached locally on the Windows client with the file or files opened, thus eliminating network latency when the files are constantly accessed.

When another client attempts to open the same file or files, the cached data is written to the ReadyNAS, and the oplock is released.



Advanced Options

Clicking the access icons on the Share LIst screen opens the **Advanced Options** screen, which offers advanced low-level file manipulation options that can affect file access through all file protocol interfaces. Care should be taken before these options are used, as anything that changes ownership and permissions might not be easily reversible.



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 select the **Grant rename and delete privilege to non-owners** option. In a collaborative environment, you might want to enable this option. In a more security-conscious environment, disable this option.

Advanced Share Utilities

Use this option to adjust the timestamps of the contents of the share. This can be used to fix issues with incremental backups, and sources or destinations that change local timestamps when daylight savings time changes. In the **Shift share content timestamps by field e**nter a positive number to push timestamps ahead, negative numbers to push them back.

Accessing Shares from a Web Browser

To see the share listings and access a share using a Web browser, click either **Browse** on the RAIDar utility, or enter **http://<ipaddr>** or **http://<hostname>** in the Microsoft Explorer browser address bar.

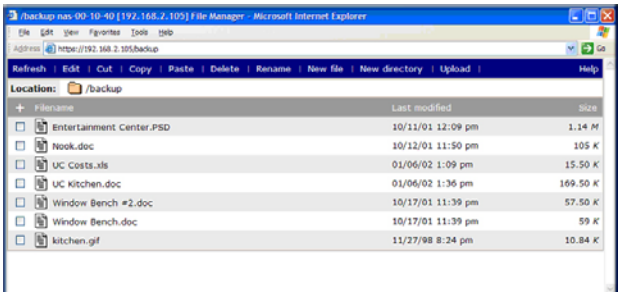
Hostname is the ReadyNAS hostname assigned in the **Network** screen. The default hostname starts with ***nas-*** followed by the last three hex bytes of the device MAC address.

To access a specific share, simply add the name of the share to the address.

For example, **http://<hostname>/backup**

For a secure encrypted connection use HTTPS. You are prompted to log in.

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, options for creating, modifying, and deleting files are displayed in the file manager.



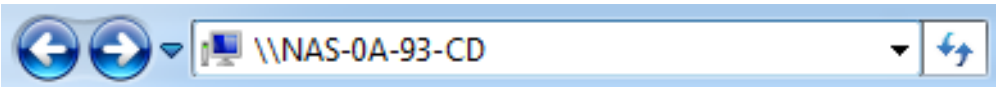
One useful application for a Web share is to set an internal company Web site. You can copy HTML files to the Web share using Windows, Mac, NFS, or HTTP. When you set HTTP access to read-only, HTML files (including index.htm and index.html) on the Web site can be viewed from any Web browser.

Note: Files created under the Web file manager can be deleted only under this file manager. The only exception is for the admin user. The admin user can change or delete any files created over the Web using any protocol. Files not created from the file manager can be modified within the file manager, but cannot be deleted here.

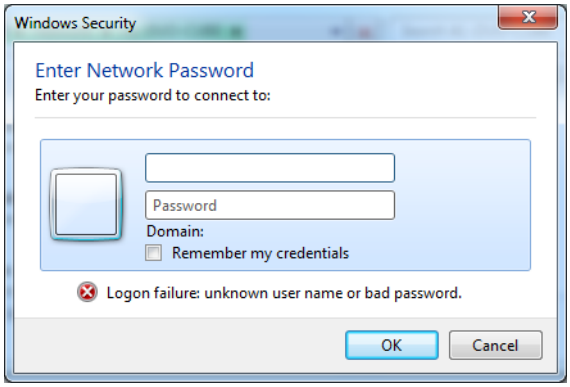
Accessing Shares from Windows

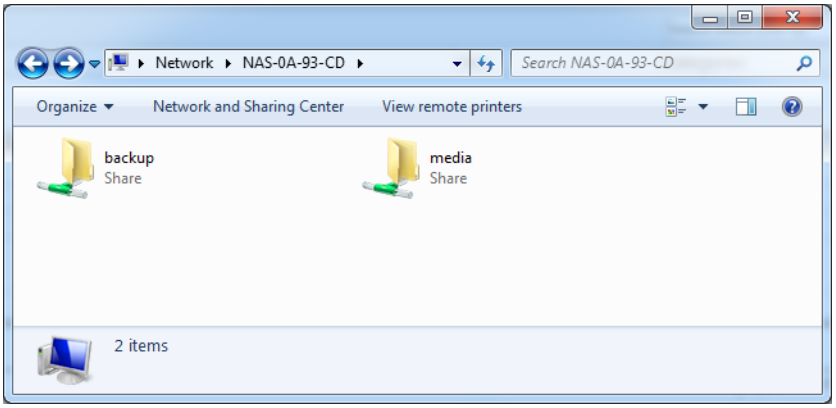
To access Shares from a PC

1. To see a list of shares in Windows, either click the Browse button in RAIDar or enter **\\<ip_address>** or **\\<hostname>** in the address bar.



2. When prompted, enter your user name and password to connect to the ReadyNAS. Windows Explorer will display the contents of the ReadyNAS share.

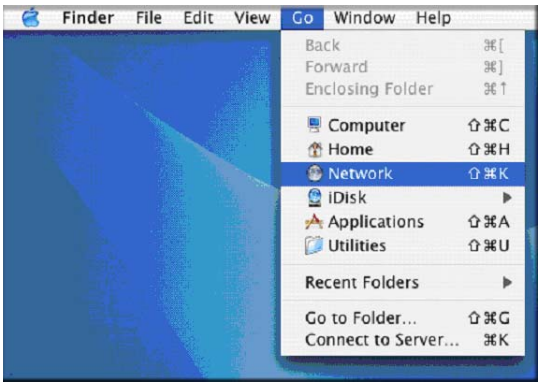




Accessing Shares from Mac OS X

To access the same share over AFP with OS X,

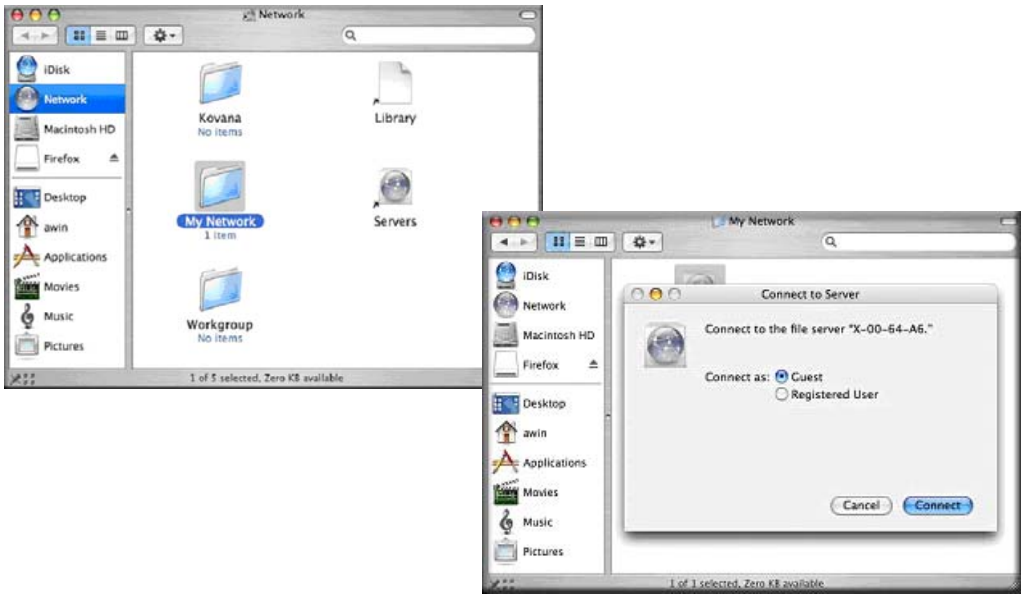
1. In **Finder, select the Go > Network** menu.
2. From here, access to the AFP share can be over Bonjour or over AppleTalk, depending on how you have chosen to advertise your AFP share.



AFP over Bonjour

To access the AFP share advertised over Bonjour on Mac OS X,

1. in **Finder** select **Go > Network** to see a listing of available networks.
2. Open the **My Network** folder to display the ReadyNAS hostname.



3. Enter the user name and password you want to use to connect to the ReadyNAS.
4. From the **Volumes** field, select the share you want to access and click **OK**.

AFP over AppleTalk

To advertise your AFP service over AppleTalk,

1. A list of available networks displays.

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

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

In Share security mode, if you have set up a password for your share, you need to specify only the user name and password. If you have not set up a user name, enter the share name in place of the user name.

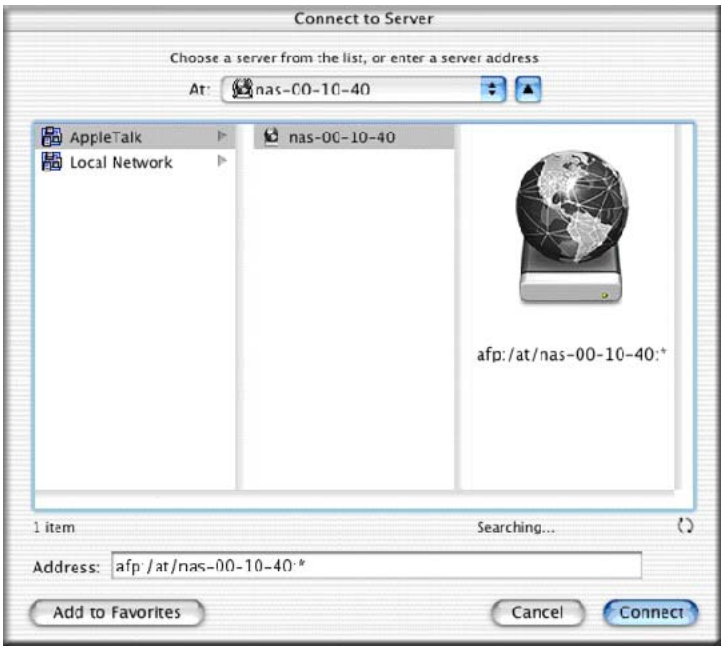
In User or Domain security mode, enter the user name and password you want to use to connect to the ReadyNAS.

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

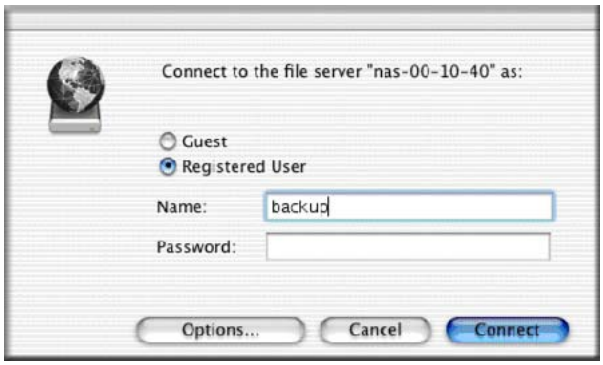
Accessing Shares from Mac OS 9

To access the same share under Mac OS 9:

1. select **Connect to Server** from the **Finder** menu, choose the ReadyNAS device entry from the AppleTalk section, and click **Connect**.

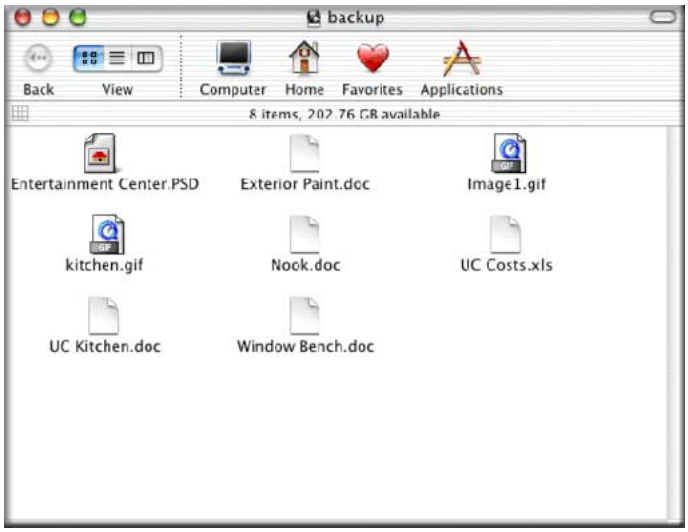


2. When prompted to log in, enter the share name and password if the ReadyNAS is configured for Share security mode; otherwise, enter a valid user account and password, and click **Connect**.



3. If no share password is set in Share mode, you can select the **Guest** radio button and leave the Password field blank. A successful login shows a list of one or more shares. Select the share that you want to connect to and click **OK**.

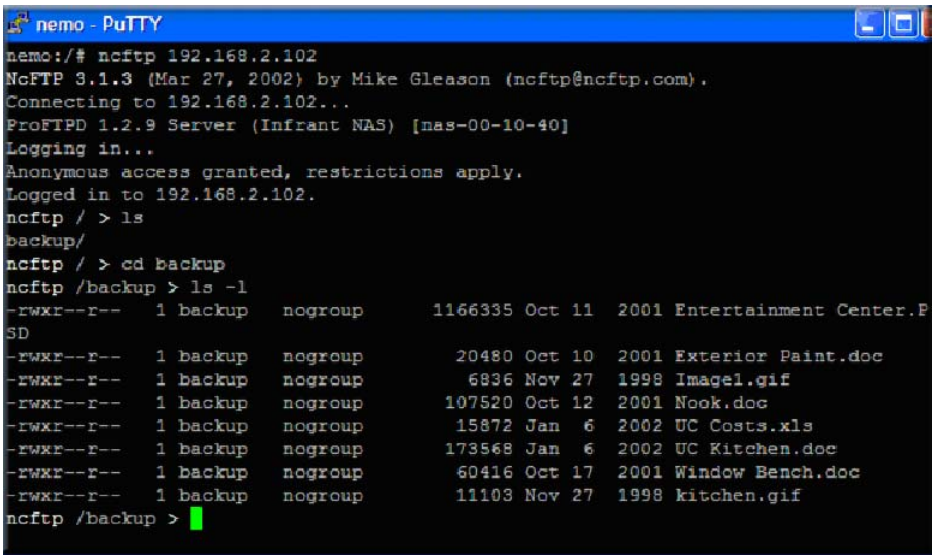
4. You should see the same files in the share that you do in Windows Explorer.



Accessing Shares through FTP/FTPS

To access the share using FTP in Share security mode:

1. Log in as ***anonymous*** and use your email address for the password.



2. To access the share, use the appropriate user login and password used to access the ReadyNAS.

Note: 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. Also, when using FTPS, only Explicit mode (also known as FTPES or AUTH TLS) is supported.

Accessing Shares from Linux/Unix

To access this share from a Linux or Unix client:

1. Mount the share over NFS by entering:

   mount <ipaddr>:/<backup /backup>

   where **backup** is the share name.

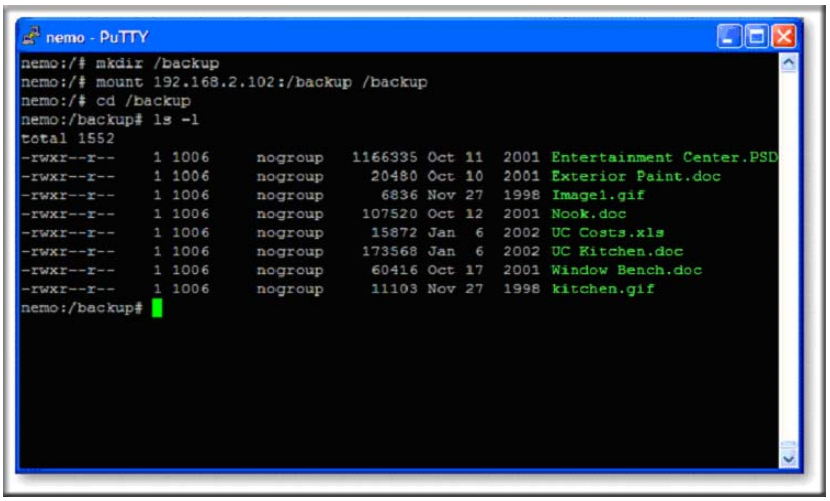
   Running the **ls** command in the mounted path displays the share content.

To access this share from a Linux or Unix client where backup is the share name

1. Mount the share over NFS by entering:

   mount <ipaddr>:/<backup /backup>

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



Note: The ReadyNAS does not support NIS as it is unable to correlate NIS information with CIFS user accounts. In mixed environments where you want CIFS and NFS integration, set the security to User mode and manually specify the UID and GID of the user and group accounts to match your NIS or other Linux/Unix server settings. The ReadyNAS can import a comma-delimited file containing the user and group information to coordinate Linux/Unix login settings. See *Managing Users* on page 57 for more information.

Remote Access

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

ReadyNAS Remote

ReadyNAS Remote is a Web-based add-on service that enables drag and drop file transfers from the Windows 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.

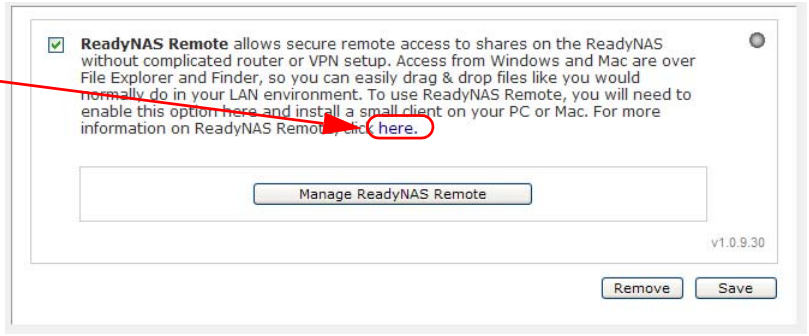
See *Installed Add-Ons* on page 33 for more information about add-on features.

To enable ReadyNAS Remote:

1. Install the **ReadyNAS Remote** client software for Mac or PC.

   The following screenshots are from a PC; however the Mac steps are nearly identical.

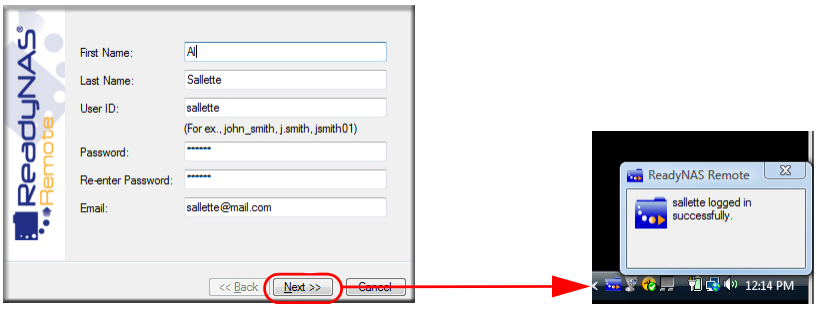
Link to ReadyNAS Remote desktop client and tutorial



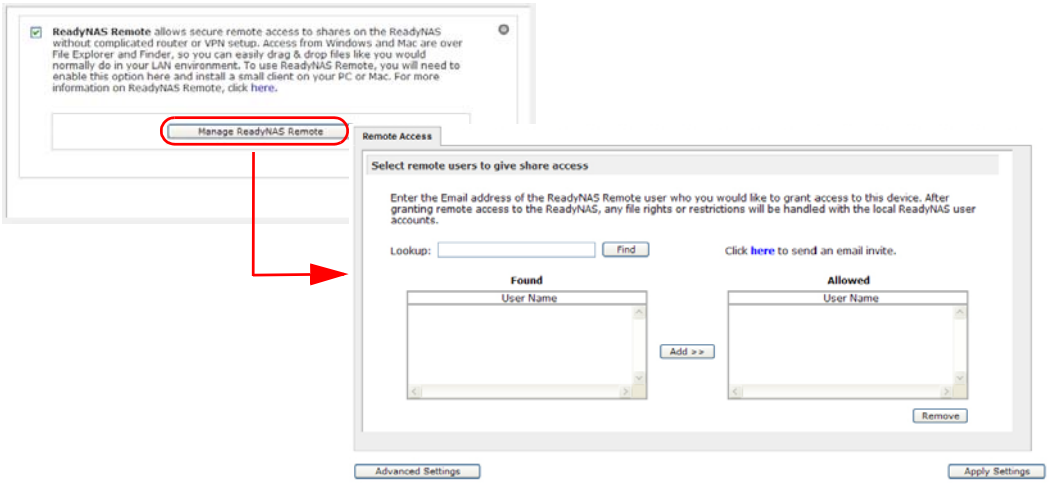
   a. Log in to **FrontView** and select **Services > Installed Add-ons > ReadyNAS Remote**.
   b. Click the "**here**" link on the screen, or go to ***http://readynas.com/download***, to download the client software from ReadyNAS.com, and view the setup tutorial.
   c. Install the **ReadyNAS Remote** client 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 need to configure your desktop firewall to give permission to the ReadyNAS Remote client software.

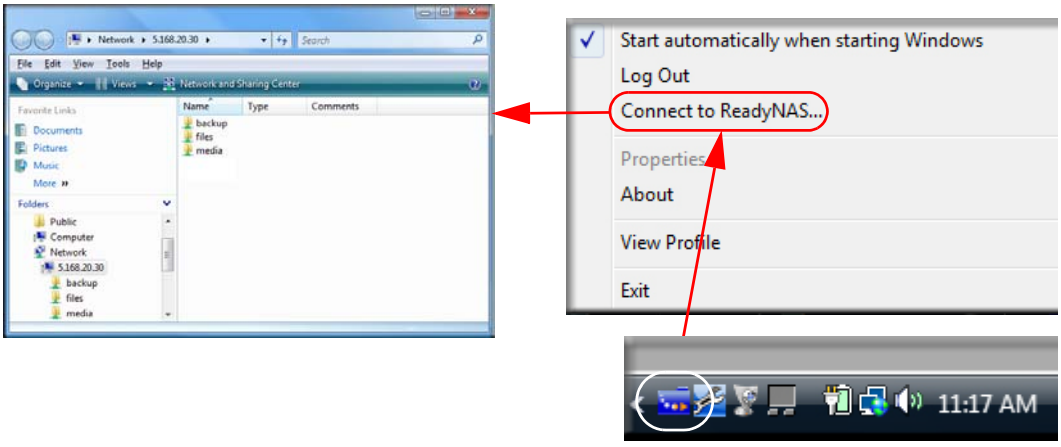
2. Click the link in the **ReadyNAS Remote** client software to create a ReadyNAS Remote account. A popup notice displays upon successful registration with the ReadyNAS Remote Web service.



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



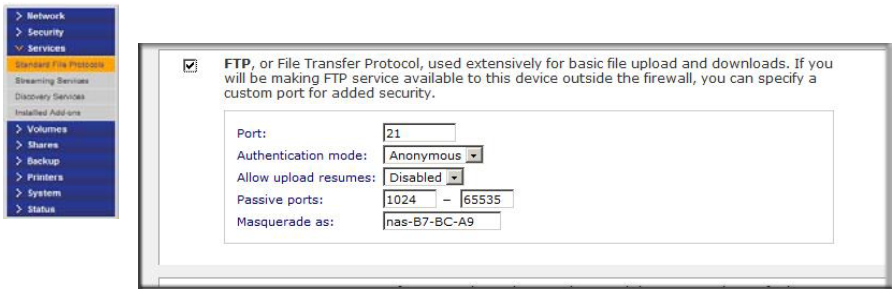
4. Use the ReadyNAS Remote client to log in to the ReadyNAS.



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. Select **Services > Standard File Protocols,** and select the FTP check box.



   a. **Port**. Defines the TCP/IP port that the FTP service will be using.

      The default port is 21. This port needs to be forwarded through the router. Refer to the port forwarding instructions provided with your router.

   b. **Authentication mode**.

      - **Anonymous**: No login information is required for FTP users.
      - **User**: Users need an account configured on the ReadyNAS from either User or Domain security mode.

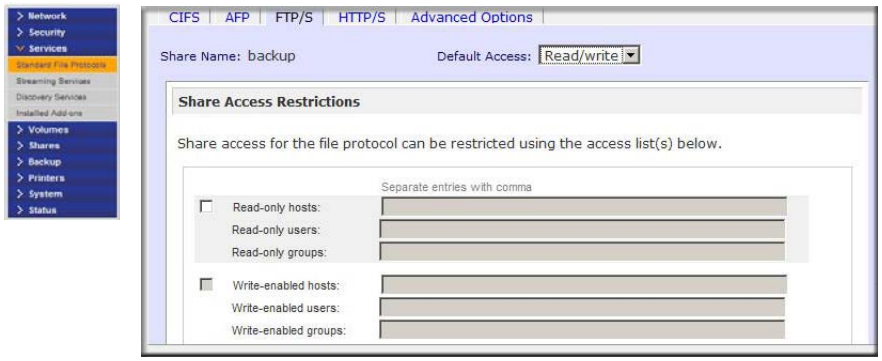
   c. **Allow upload resumes**. This option allows users to finish uploading a file to the FTP share if the connection had been previously interrupted. Without this option enabled, if the connection is dropped at 50 percent completion, the file upload must restart from the beginning.

   d. **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 you expect 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.

   e. **Masquerade as**. This field adjusts the hostname that the FTP server reports to an FTP client.

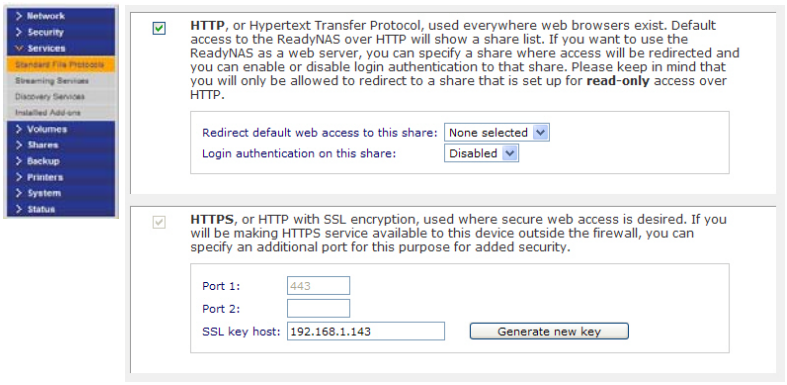
2. Configure the FTP share access options.

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



Remote HTTP/HTTPS Access

1. Select **Services > Standard File Protocols,** and select the HTTP check box.



HTTP

- **Redirect default Web access to this share**. Advanced configuration option allowing hosting of user-created HTTP Web pages on the ReadyNAS.
- **Login authentication on this share**. Configures the share for whether or not authentication is required if users are browsing to the user-created Web content.

HTTPS

HTTPS cannot be disabled; FrontView requires it.

- **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.

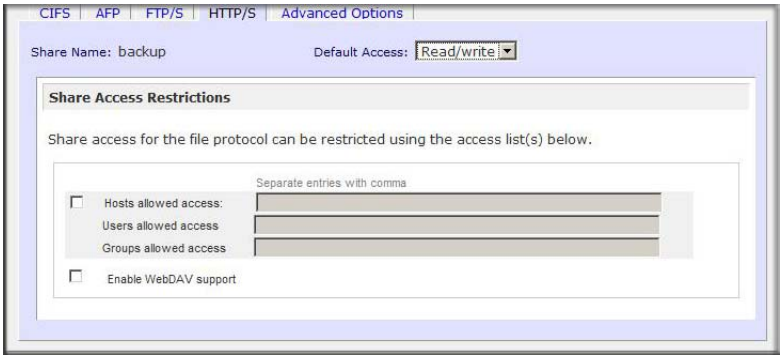
> **Note:** Changing the default HTTPS port requires enabling port forwarding of the port you choose on the router. Refer to the port forwarding instructions provided with your router.

- **SSL key host**. Use this field to configure the hostname used for the ReadyNAS to generate its SSL certificate, and then create a new SSL certificate. NETGEAR recommends that you 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 your Web browser.

  In this scenario, it is best to have a fixed IP configuration for the ReadyNAS so that the certificate remains valid. Also, if the WAN IP address configuration is DHCP, NETGEAR recommends that you use a Dynamic DNS service to access the ReadyNAS through a persistent fully qualified domain name provided by a DDNS service provider rather than through an IP address.

2. Configure the **HTTP/S** share access options.

   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 allows drag and drop file transfers similar to what you might experience with a standard Windows or Mac OSX computer. See the article *Accessing ReadyNAS remotely with WebDAV* at ***http://readynas.com/?p=126*** for instructions on how to set up WebDAV.

Backing Up Your Data

5

This chapter explains how to back up the data from your ReadyNAS, and contains the following sections:

- **Configuring Backup Jobs**
- **Time Machine Backup**
- **Snapshots**
- **ReadyNAS Vault Service**
- **Enabling Rsync and Specifying Rsync Rights**

Configuring Backup Jobs

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

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

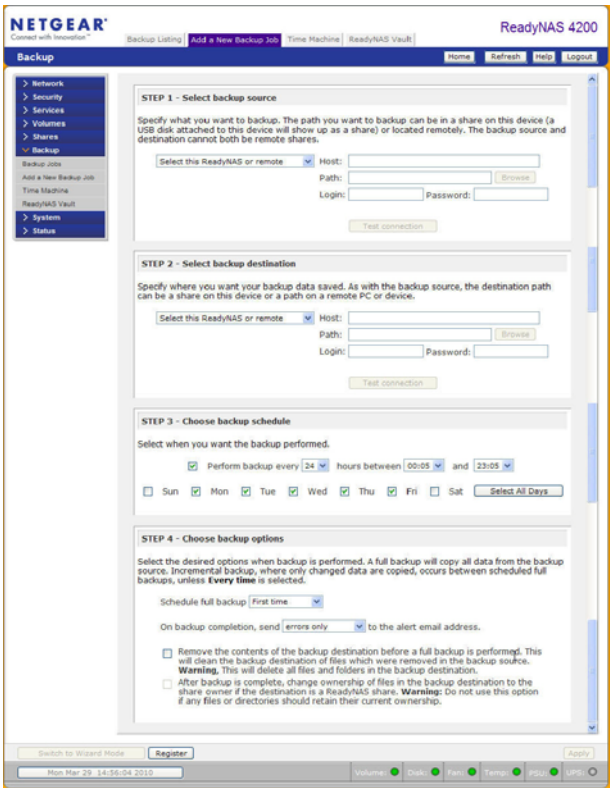
Adding a New Backup Job

The backup source can be

- Located remotely
- A public or a private home share
- An iSCSI individually addressable (logical) SCSI device (a logical unit number or LUN
- All home shares on the ReadyNAS

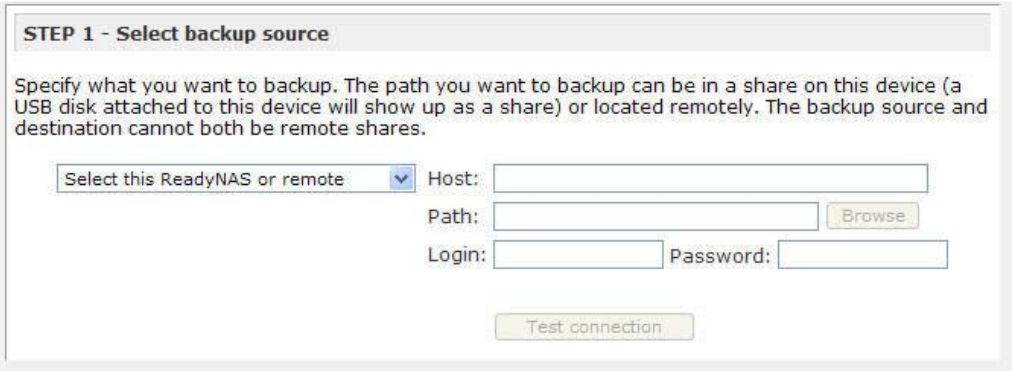
To create a new backup job:

From the main menu, select **Backup > Add a New Backup**. Follow the four steps.



1. Select backup source.

   The backup source can be a share or a path located locally on the ReadyNAS, or remotely on another ReadyNAS or a computer. If the source is local, you can select any share on the ReadyNAS, a USB device attached to the ReadyNAS, or you can elect to back up the entire data volume.



   If you selected a share or a USB device on the ReadyNAS, you can leave the path blank to back up the entire share or device, or enter a folder path to back up just the content of that folder.

   If you want to back up a remote source to the ReadyNAS, enter the remote host name, the folder path, and any login credential required to access that path.

   To ensure that you have the right access to the remote backup source, click **Test Connection** after entering the source parameters.

   Each file protocol uses a slightly different path notification, so refer to the following list for the correct form. Notice that a forward slash (/) is used instead of a backslash (\) in all instances.

   a. Remote Windows/NAS (Timestamp)

      Select this to back up a share from a Windows PC. Incremental backups use timestamps to determine whether files should be backed up.

      Examples of a Windows or remote ReadyNAS path:

         /myshare

         /myshare/myfolder

   b. Remote Windows/NAS (Archive Bit)

      Select this to back up a share from a Windows PC. Incremental backups use the archive bit of files, similar to Windows, to determine if they should be backed up.

      Examples of a Windows or remote ReadyNAS path:

         /myshare

         /myshare/myfolder

c. Remote Website

Select this to back up a Web site or a Web site 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.

Examples of a Web site path:

/myshare

/myshare/myfolder

d. Remote FTP Site

Select this to back up an FTP site or a path from that site.

Examples of an FTP path:

/myserver/mypath/mydir

/myserver/mypath/mydir/myfile

e. Remote NFS Server

Select this option to back up from a Linux or UNIX server across NFS. Mac OS X users can also use this option by setting up an NFS share from the console terminal.

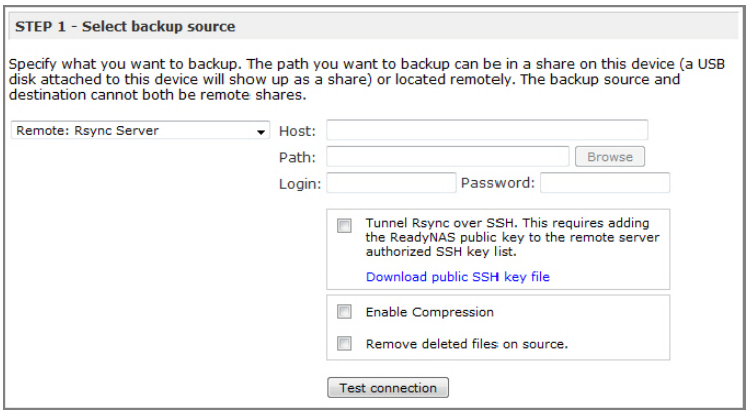
Examples of an NFS path:

/mypath

/mypath/myfolder

f. Remote Rsync Server

Select this to perform backups from a Rsync server. Rsync was originally available for Linux and other UNIX-based operating systems, but is also popular under Windows and Mac for its efficient use of incremental file transfers. This is the preferred backup method between two ReadyNAS devices. For more information, see *Enabling Rsync and Specifying Rsync Rights* on page 102.



When you elect to back up to a remote Rsync server, you are presented with additional options:

- **Tunnel Rsync over SSH**

  Enabling this option enables Rsync data transfers to go through a secure, encrypted SSH tunnel. This is recommended when backups are being transferred over the Internet. To use this option, you will need to download the public SSH file key from the ReadyNAS and add it to the remote Rsync server's authorized SSH key list. To download the key, click **Download public SSH key.**

  If the destination Rsync server is a ReadyNAS, select **Shares > Share Listing** on the Rsync screen, and click **Manage SSH Keys** to add the public key.

  More information about using Rsync with SSH see the article *Setting up Rsync over SSH* at: ***http:/readynas.com/rsync_ssh.***

- **Enable Compression**

  Compress data before transferring. This option is especially useful for slower network connections, such as when transferring data over a WAN.

- **Remove deleted files from target**

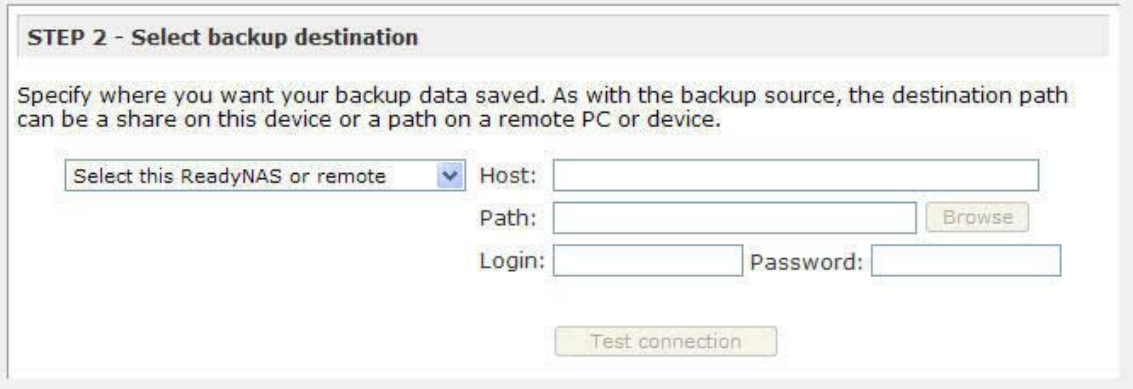
  This option ensures that the destination has exactly the same image as the ReadyNAS; however, it is important to understand that any accidental deletion of data on the ReadyNAS cannot be recovered.

- **File and directory exclusion list**

  Files and directories that you want to exclude from the backup can be specified here. Enter the files and directories as a comma-separated list.

2. **Select Backup Destination.**

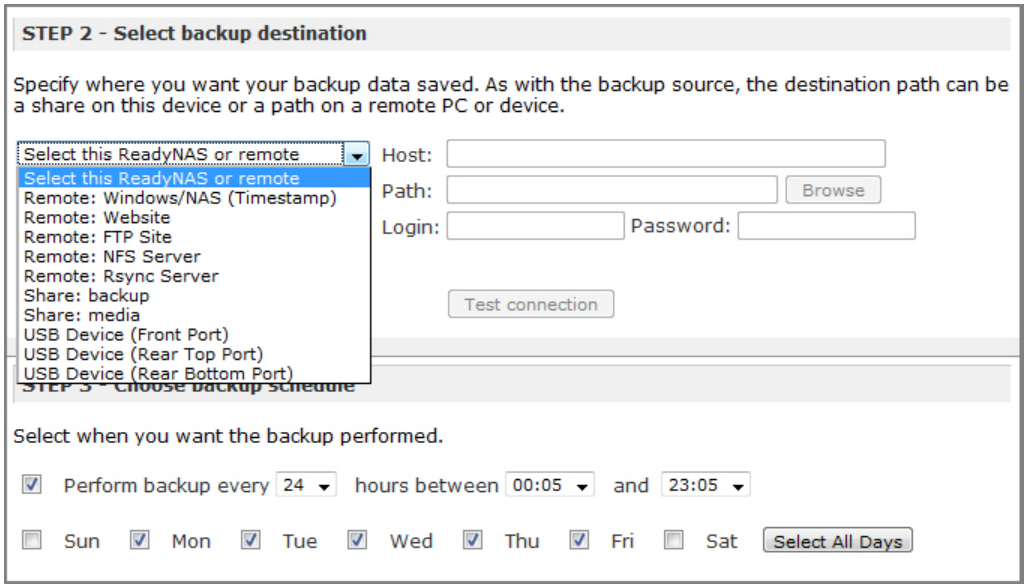
This step is similar to Step 1 except you are now specifying the backup destination. If you selected a remote backup source, you need to select a destination on the ReadyNAS. Note that either the source or destination must be the ReadyNAS.



If the source is the ReadyNAS, you can either enter a ReadyNAS destination, \or you can specify a remote backup destination.

The remote backup destination can be a remote Windows PC with a ReadyNAS system, a remote FTP site, a remote NFS server, a remote Rsync server, a ReadyNAS share, or a USB device.

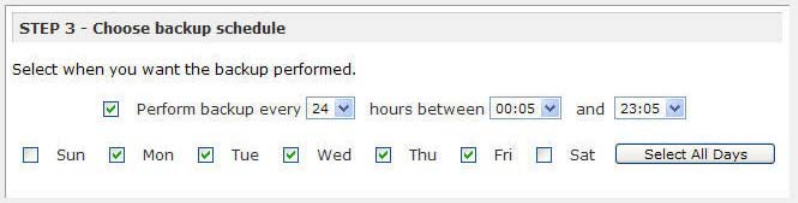
Note: You can select Rsync for a remote ReadyNAS if it is configured to serve data over Rsync.



3. Choose Backup Schedule.

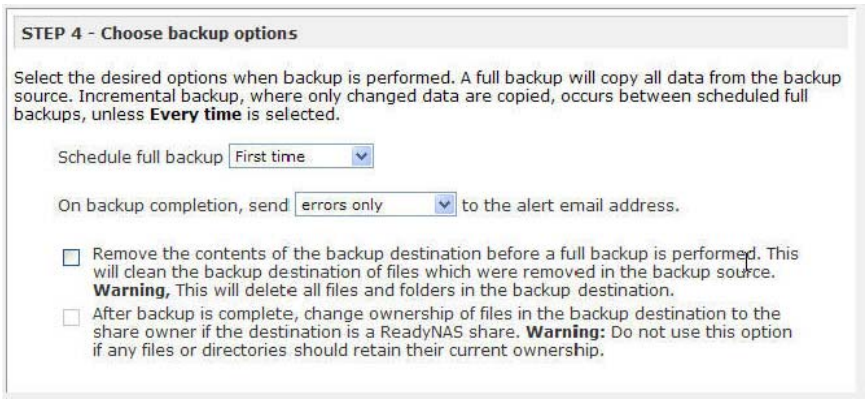
You can select a backup schedule as frequently as once every 4 hours, daily, or just once a week. The backup schedule is offset by 5 minutes from the hour to allow you to schedule snapshots on the hour (snapshots are almost instantaneous) and perform backups of those snapshots.

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



4. Choose Backup Options.

In this last step, set up how you want the backups to be performed.



a. Schedule a full backup

To select when you want full backups to be performed, select from these options:

- First time
- Every week
- Every 2 weeks
- Every 3 weeks
- Every 4 weeks
- 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. The next full backup is performed at the interval you choose calculated from this first backup. Incremental backups are performed between the full backup cycles.

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

b. 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 emails 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.

c. Remove files from backup destination

Select this option 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 an experiment with a test share to make sure you understand this option.

d. 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.

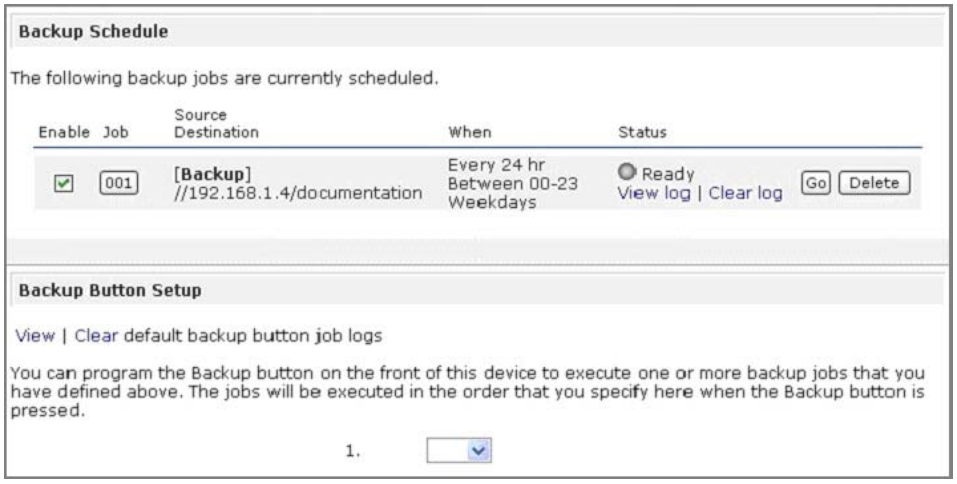
e. Click **Apply** to save your settings

Note: 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.

A summary of scheduled backup jobs displays; jobs are numbered beginning at 001.



To manage your backup jobs:

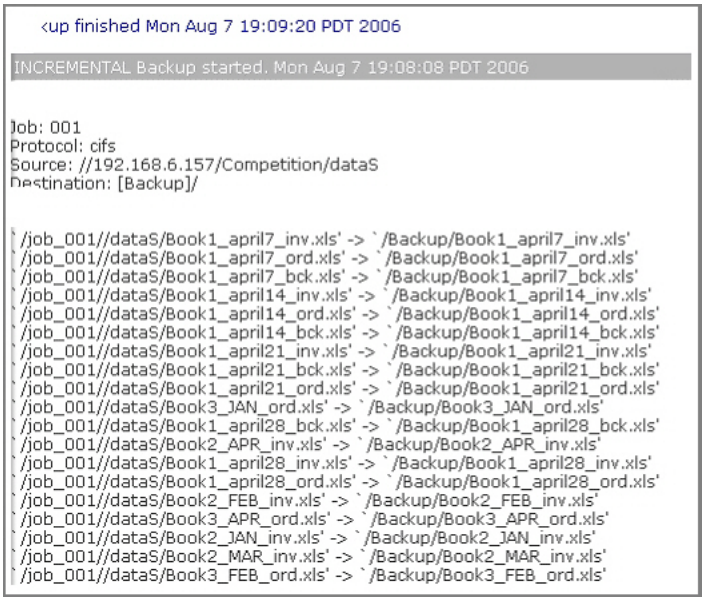
1. Click the **Job** number icon to modify the selected backup job.
2. Enable or disable job scheduling by selecting or clearing the **Enable** check box. Disabling the job does not delete the job, but removes it from the automatic scheduling queue.
3. Click **Delete** to permanently remove the job.
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 Log** to clear the current log detail.

Viewing the Backup Log

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

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



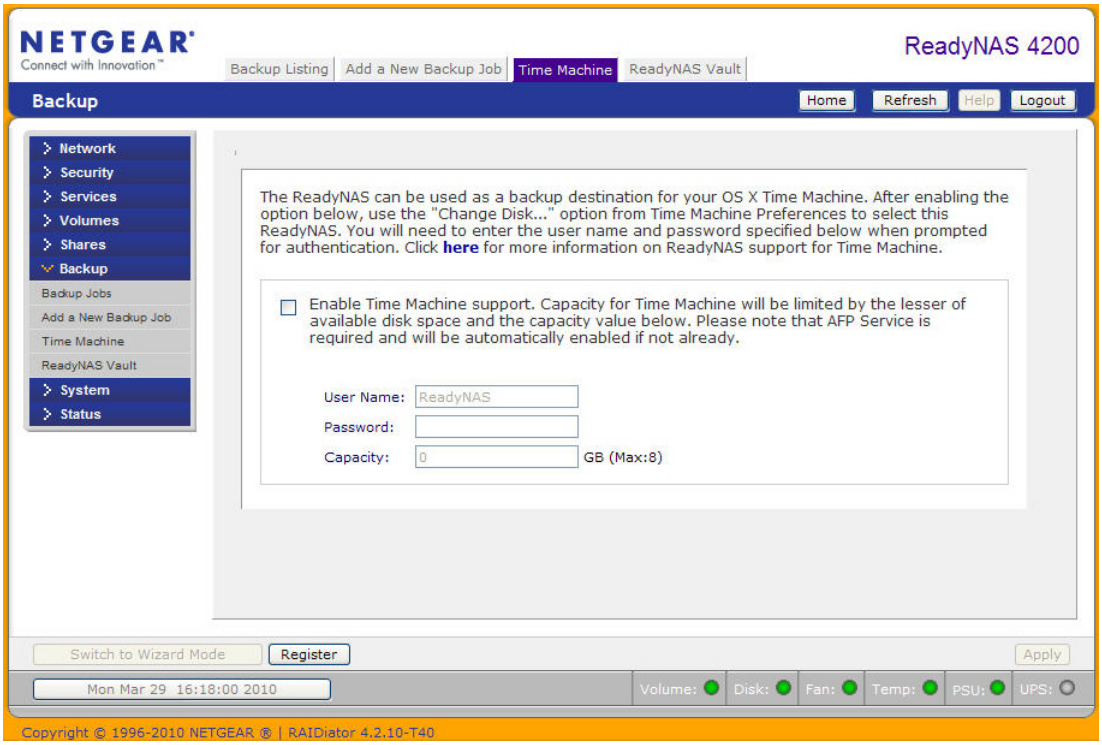
Editing a Backup Job

To edit a backup job, either click the three-digit job number button on the **Backup Jobs** screen, or click the **Edit Backup Job** link while viewing that job log. Make appropriate changes or adjustments to the job, as needed.

Time Machine Backup

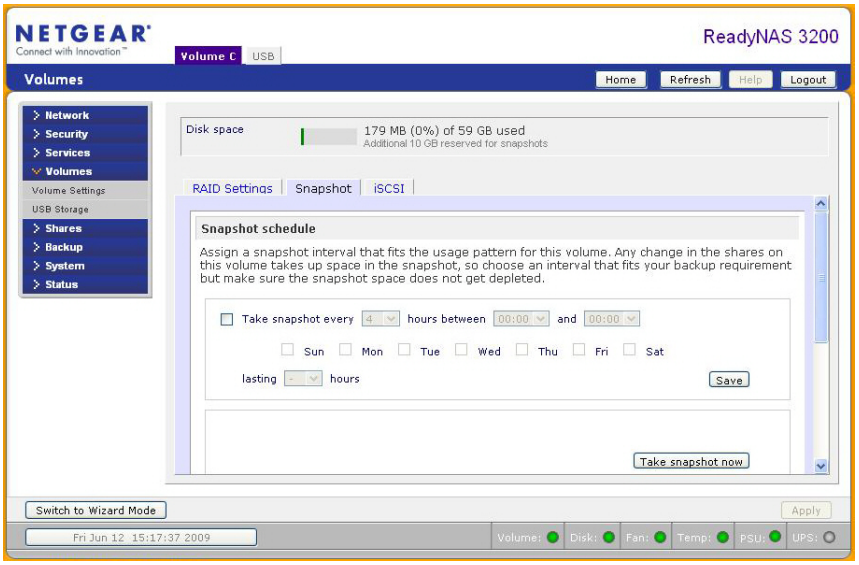
The ReadyNAS can be used as a backup destination for your Mac OS X Time Machine. After enabling the Time Machine option, use the **Change Disk** option from Time Machine Preferences to select this ReadyNAS. You need to enter the user name and password specified in the ReadyNAS when prompted by the MAC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

For information about ReadyNAS support for Time Machine, see the article *Easy Time Machine Setup with the ReadyNAS* at ***http://readynas.com/TimeMachine***.



Snapshots

The **Volume** screen allows you to schedule and take snapshots. Think of 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 continues to operate normally. As primary storage becomes larger, offline backups tend to become increasingly difficult because backup time increases beyond offline hours. Snapshots allow backups to occur without the need to take your systems offline.



Snapshots can also be used as temporary backups. For example, if a file on the ReadyNAS 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. From the **Volume** screen, click the **Snapshot** screen to display the Snapshot screen.

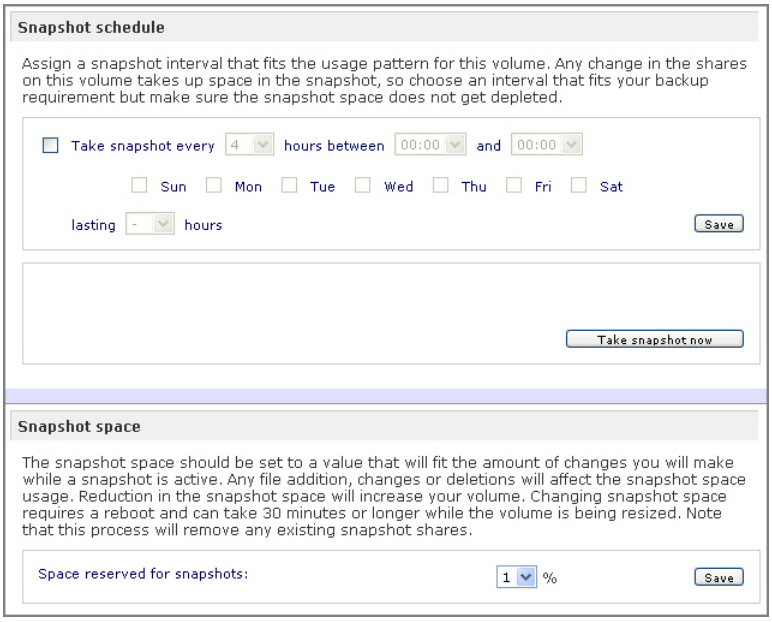
   Specify how often a snapshot should be taken. Snapshots can be scheduled in intervals from once every 4 hours to once a week.

> **Note:** If you do not see a Snapshot screen on the Volume screen, you did not reserve any space for snapshots when you added the volume. The ReadyNAS ships with a snapshot reserved space of 10GB. For information on how to reserve space for snapshots, see *Resizing Snapshot Space* on page 100.

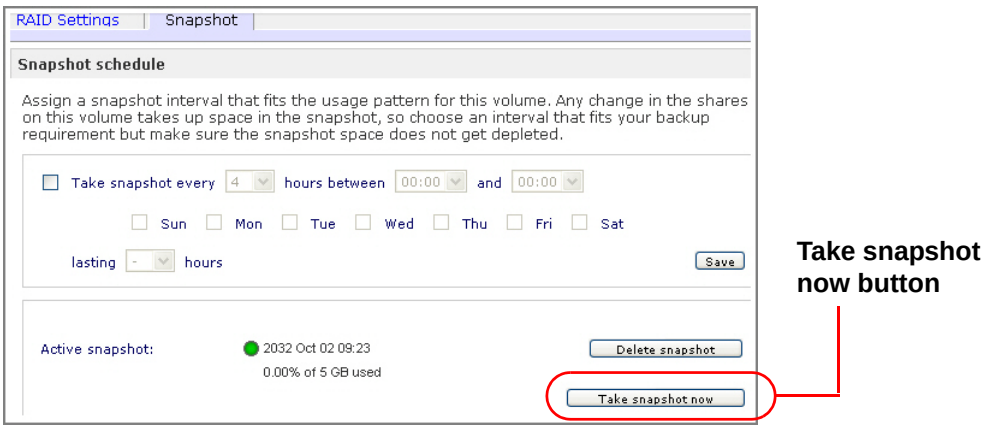
2. Specify the frequency and the days that you want to schedule a snapshot:

   When start and end times are set to 00:00, ReadyNAS takes one snapshot at midnight. A start time of 00:00 and an end time of 23:00 sets snapshots to be taken between midnight and 11 p.m. the next day at the interval you specify.

   Once you save the snapshot schedule, the time of the next snapshot displays. When the next snapshot is taken, it replaces the previous one.

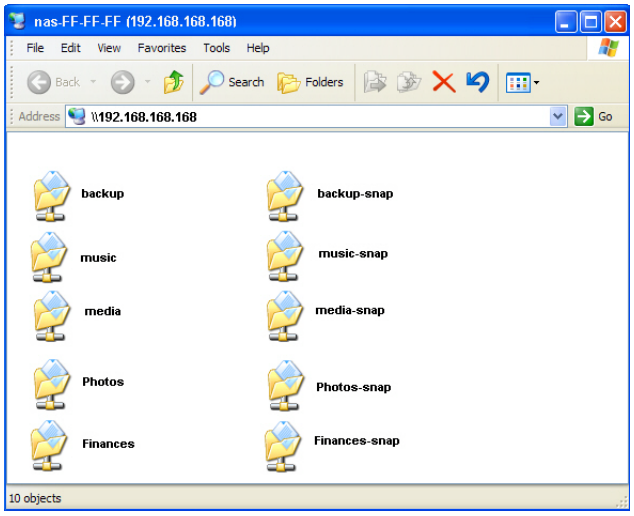


You can take manual snapshots at any time by clicking the **Take snapshot now** button.



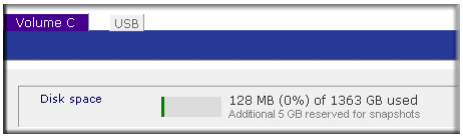
You can also specify how long a snapshot should last. If you use snapshots for backups, schedule the snapshot to last slightly longer than the expected duration of the backup. Having an active snapshot can affect the write performance to the ReadyNAS, so deactivating snapshots when not needed might be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

When a snapshot is taken, a duplicate snapshot appears in the browse list alongside the original share, except the duplicate share name has *-snap* appended to the original share name. For example, a snapshot taken of the share *music* is available as *music-snap*.



You can traverse a snapshot share just as you would a normal share except the snapshot share is read-only. 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.



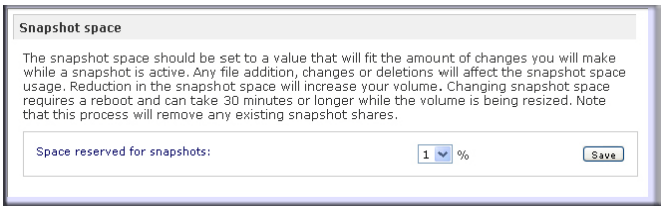
After the snapshot is taken, if changes on the volume exceed this reserved space, the snapshot is invalidated and can no longer be used.

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 becomes invalidated, an email 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 constantly get snapshot invalidation alerts, consider either increasing the frequency of the snapshot or 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 the specified percentage of your volume capacity.



Resizing the snapshot space occurs offline and can take a while depending on the data volume size, and the number of files in the volume. Expanding the snapshot space reduces the data volume size. Reducing the snapshot space expands the volume size.

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

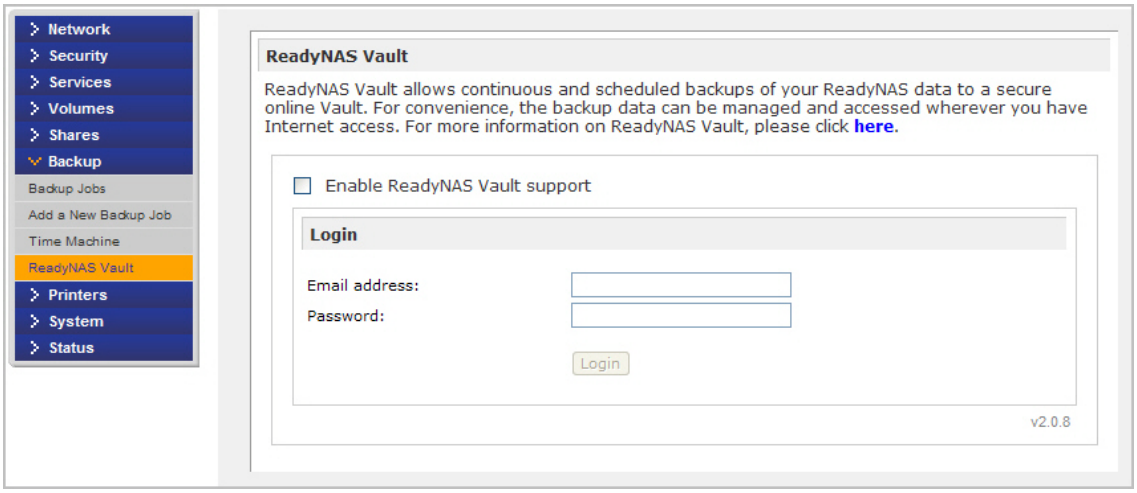
ReadyNAS Vault Service

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

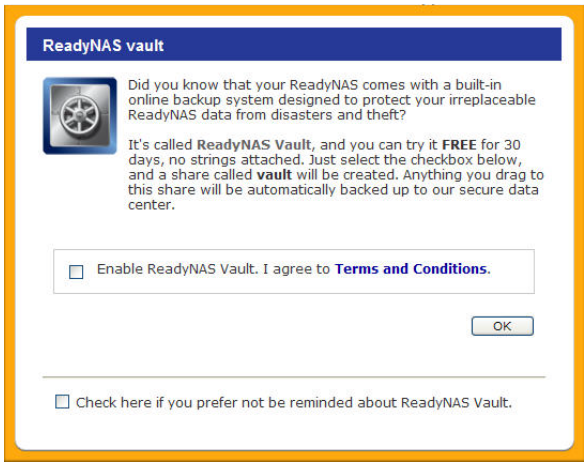
To enable the ReadyNAS Vault service:

1. Click the link on the ReadyNAS Vault screen in FrontView.

   For additional instructions, read the article "*Online Backups with* ReadyNAS *Vault*" at ***http://readynas.com/vault.***



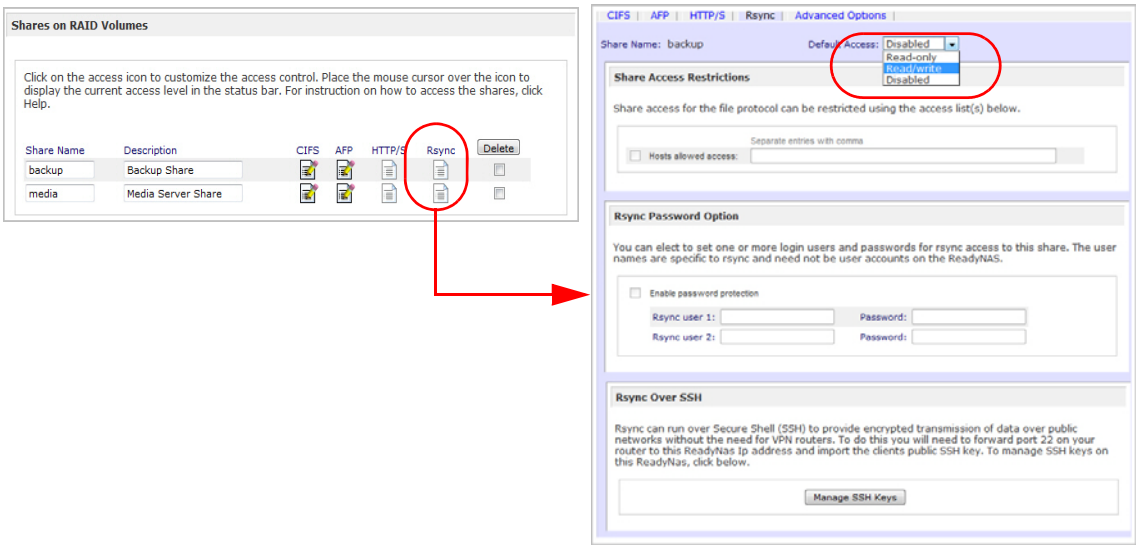
For convenience, if you have not already enrolled for the ReadyNAS Vault Service, a window appears in FrontView that gives you the option to sign up for a free trial of the ReadyNAS Vault service. Select the **Enable ReadyNAS Vault** check box, and a share called *vault* is automatically created. Anything dragged to this share is automatically backed up to the NETGEAR secure vault data center.



Enabling Rsync and Specifying Rsync Rights

Rsync is a fast and extraordinarily versatile file copying tool. It is famous for its delta-transfer algorithm. This tool reduces the amount of data sent over the network by sending only the differences between the source files and the existing files in the destination. Rsync is widely used for backups and mirroring.

Unlike other protocols, Rsync uses an arbitrary user name and password that are used only for Rsync access. To encrypt Rsync data transfers, run Rsync over SSH. Access to the share through Rsync is identical regardless of the security mode. The user account you specify does not need to exist on the ReadyNAS, or a domain controller.



You will see Rsync setting icons on the **Share Listing** screen if the Rsync service is enabled on the ReadyNAS.

To enable the Rsync service:

1. Select **Services > Standard File Protocols**.
2. Select the **default access rights**.
3. Assign a user name and password.

   You need to specify this when doing an Rsync backup.

   See *Remote Rsync Server* on page 89.

To enable Rsync access to a share or change access restrictions:

1. Click the **Rsync** icon on the **Share Listing** screen.

Examples

List ReadyNAS Rsync content for a Linux client:

To list the content of a ReadyNAS Rsync share with no user name and password defined for a Linux client:

 # 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: *****

For instructions on setting up an Rsync backup job, see *Configuring Backup Jobs* on page 87.

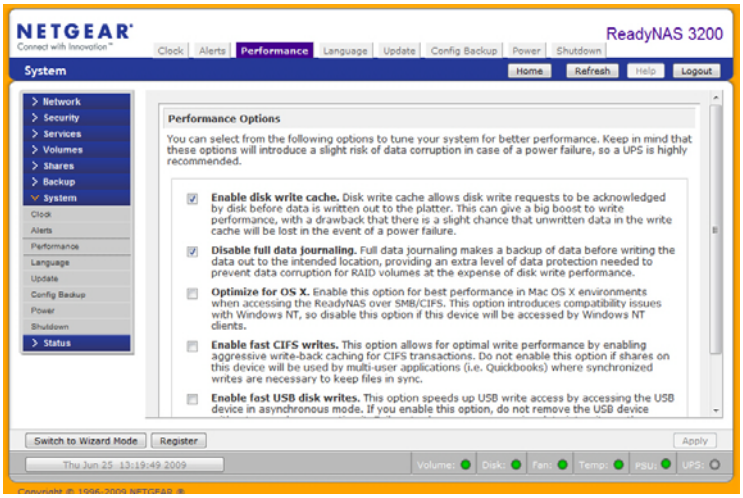
Optimization and Maintenance

6

This chapter discuses how to optimize performance and maintain your ReadyNAS system, and contains the following sections.

Performance

Select **System > Performance** from the main menu to configure system preferences.

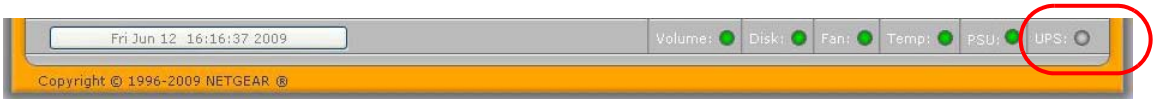


Note: Some settings suggest that you utilize an uninterruptible power supply (UPS) before enabling that option. See *Adding a UPS* on page 106.

- Select **Enable disk write cache** 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 the drawback that there is a slight chance that unwritten data in the write cache will be lost in the event of a power failure.
- The **Disable full data journaling** improves disk performance at the expense of data protection. Full data journaling makes a backup of data before writing the data out to the intended location, which provides the extra level of data protection needed to prevent data corruption for RAID volumes at the expense of disk write performance.
- The **Optimize for OS X option** provides the best performance in Mac OS X environments when connected to the ReadyNAS through the SMB/CIFS protocol. This option, however, introduces compatibility issues with Windows NT 4.0; do not enable this option if this device will be accessed by Windows NT 4.0 clients.
- The **Enable fast CIFS writes** option 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 correctly unmounting it. Failure to do so can compromise data integrity on the device.

Adding a UPS

Adding an uninterruptible power supply (UPS) to the ReadyNAS 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 back to the ReadyNAS. The UPS is detected automatically and shows up on the status bar. Hover over the status light to display more detail.



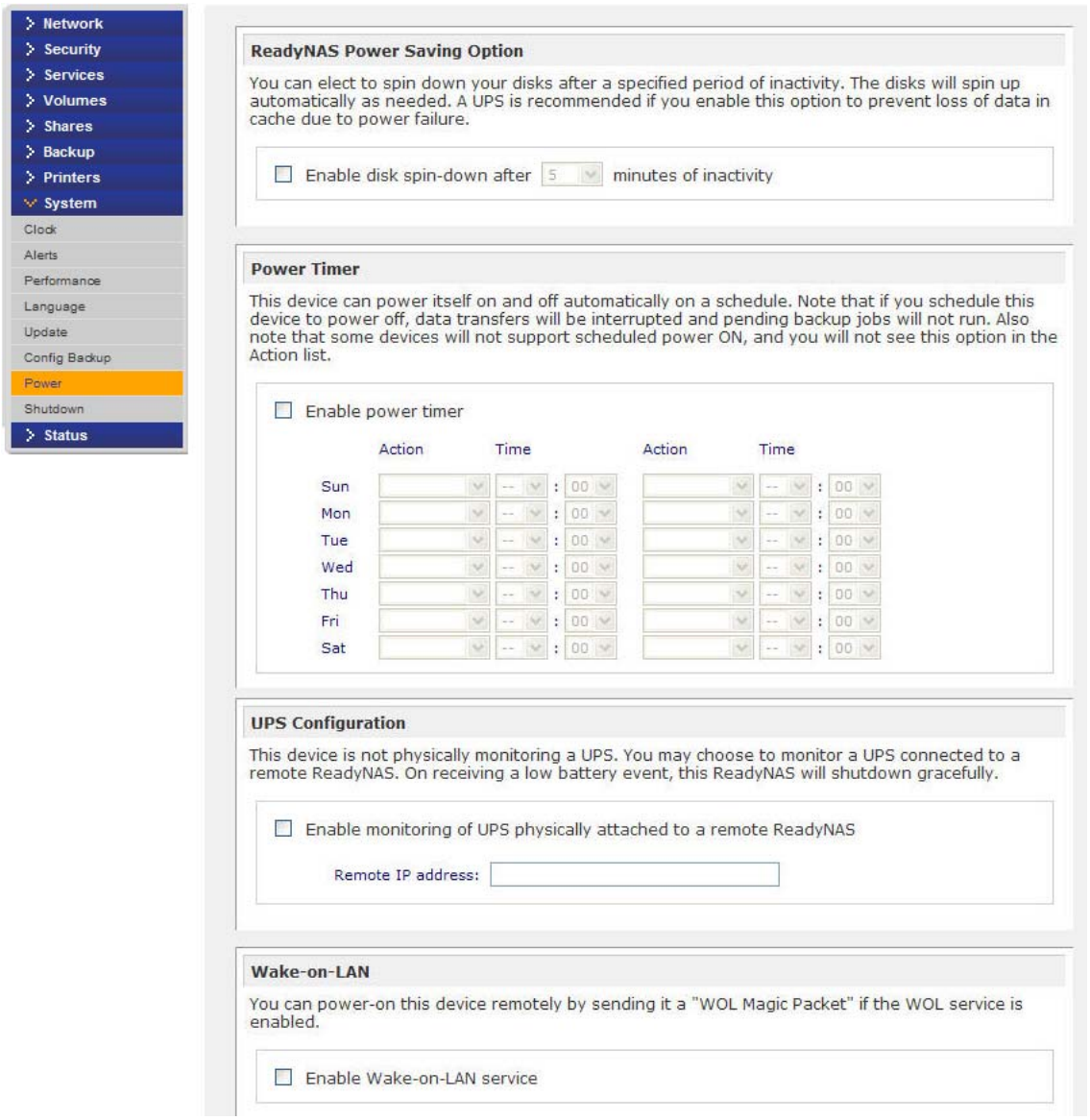
You are notified by email whenever the UPS status changes; for example, when a power failure forces the UPS into battery mode, or when the battery is low. When the battery is low, the ReadyNAS automatically shuts down safely.

See also, *Configuring UPS Battery Low Shutdown* on page 109.

Power Management

The ReadyNAS offers **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.

To display the power management options, select **System > Power.**



Power Saver - Disk Spin-Down Option

To reduce power consumption, set the ReadyNAS to spin down the disks after a specified time of inactivity. The disks will spin up as needed.

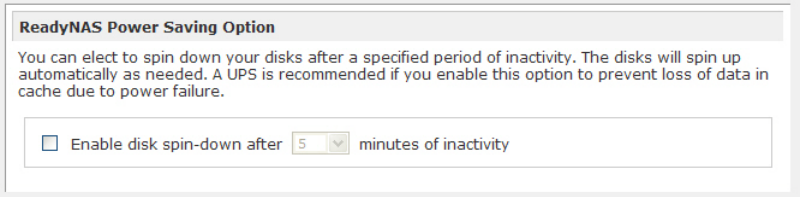
To enable spin-down mode:

1. In the ReadyNAS Power Saving Option section, select the **Enable disk spin-down after** check box.
2. Specify the minutes of inactivity before spin-down.

   The ReadyNAS can be scheduled to turn off and turn back on automatically. Select the **Enable power timer** check box and enter the action and time.

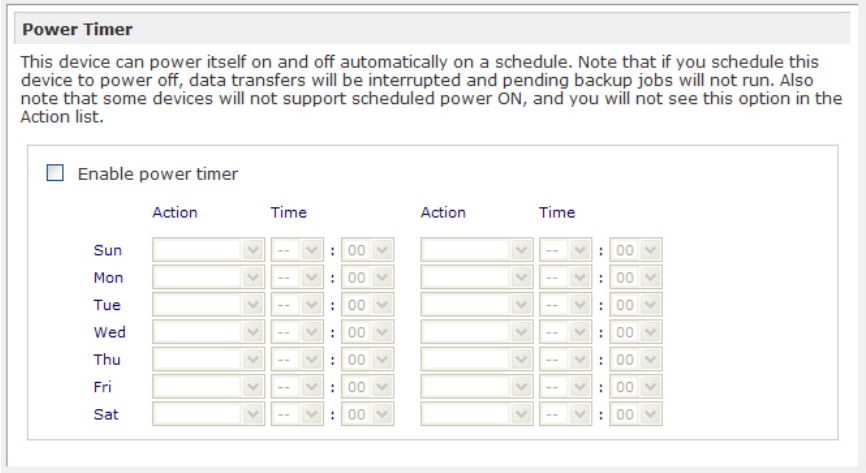
> **Note:** The Power ON option does not appear if the ReadyNAS hardware does not support this feature.

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



Power Timer

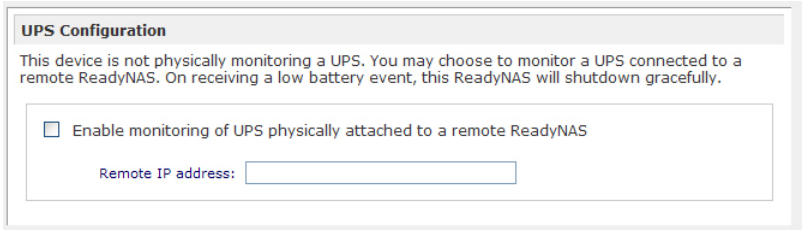
The ReadyNAS device can power itself on and off automatically on a schedule. Note that if you schedule this device to power off, data transfers will be interrupted and pending backup jobs will not run. Also note that some devices will not support scheduled power on, and you will not see this option in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



Configuring UPS Battery Low Shutdown

If this device is not connected to a UPS device, you can elect to enable a UPS connection to another ReadyNAS device. Select the **Enable monitoring of UPS physically attached to a remote ReadyNAS** check box and enter the IP address in the Remote IP address field.

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.

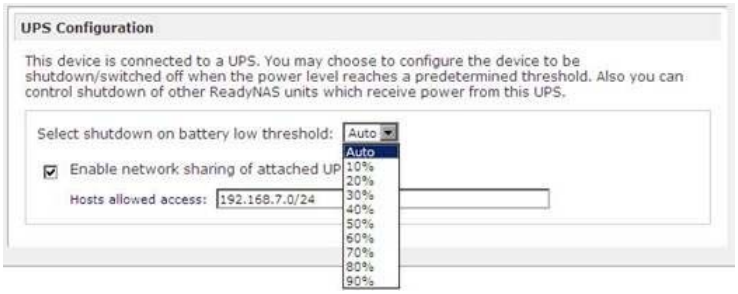


As an option, the ReadyNAS can remotely monitor the UPS when connected to a PC running Network UPS Tools (NUT).

For more information about NUT, visit ***http://networkupstools.org.***

APC

When an APC-brand UPS is connected, a shutdown on threshold drop-down option is available. See *Using the ReadyNAS to create a Network UPS for PCs* at ***http://readynas.com/forum/viewtopic.php?f=11&t=16744.***



Wake-on-LAN

You can power on this device remotely by sending it a WOL Magic Packet if the WOL service is enabled. The ReadyNAS supports Wake-on-LAN on the first Ethernet interface (LAN 1) only.

Viewing System Status

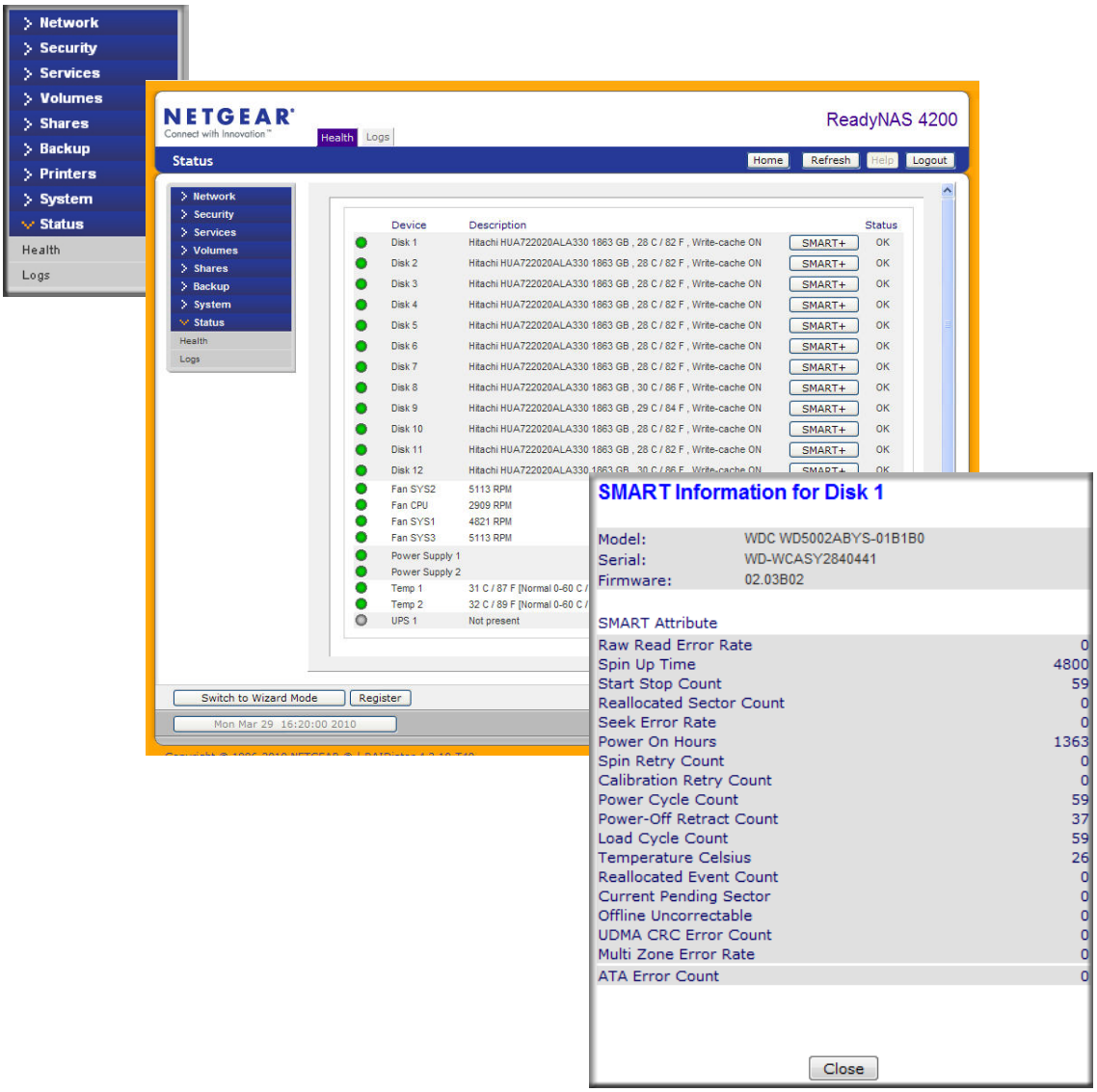
The Status menu contains links to the **Health** and **Logs** screens.

Health

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

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

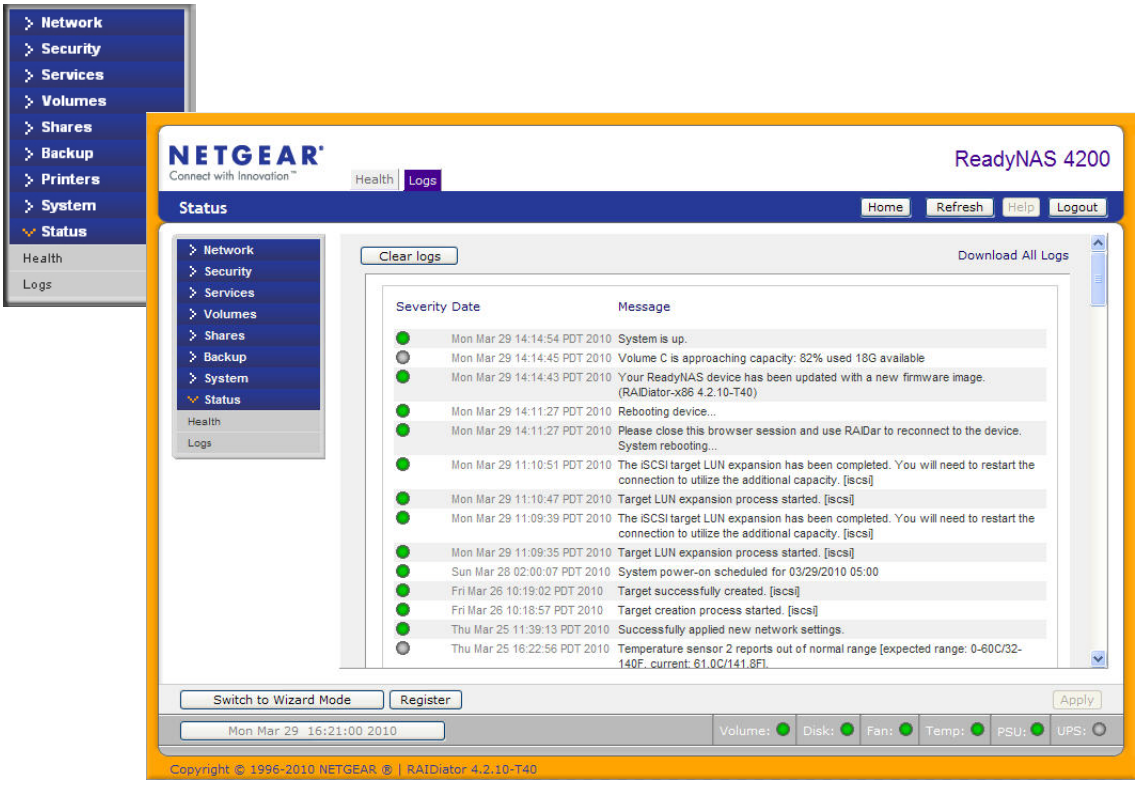
To recalibrate the fan, click **Recalibrate**.



Logs

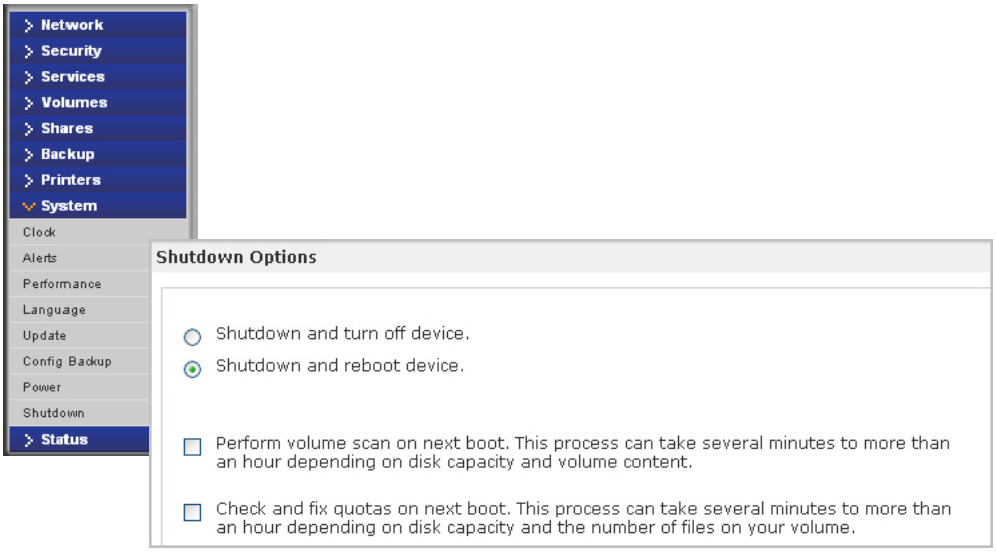
Select **Status > Logs** to access the **Logs** screen that provides information about the status of management tasks, including a timestamp.

The **Download All Logs** link is available so you can analyze low-level log information. When clicked, a .zip file of all logs in the file is created, which is used mainly by Technical Support..



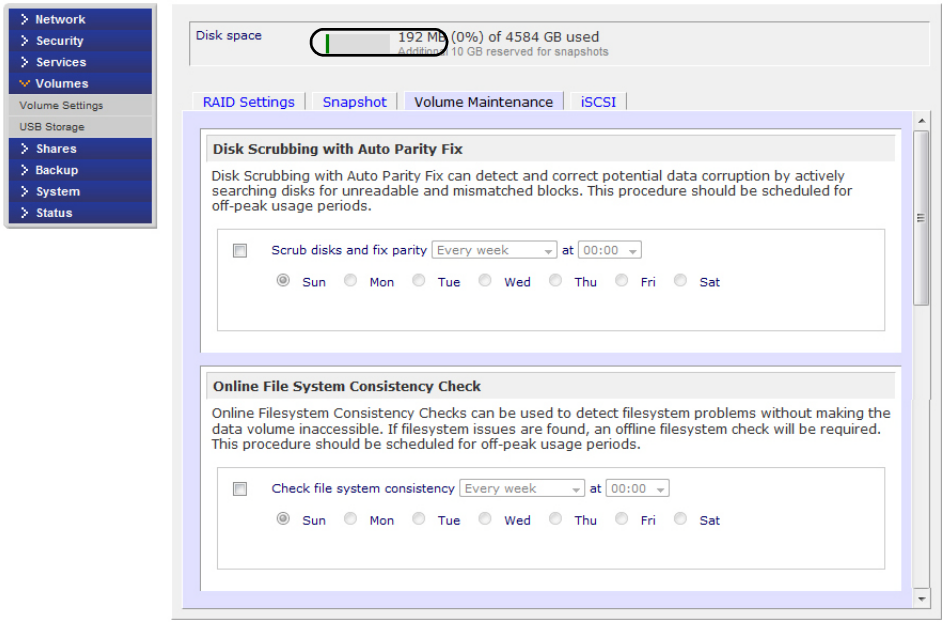
System Shutdown and File System Check

Use the **Shutdown Options** feature to turn off or reboot the ReadyNAS device. It performs 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. When you reboot you must close the browser window and use RAIDar to reconnect to FrontView.



Volume Maintenance

Use the **Volume Maintenance** options on the **Volume Settings** screen to set a rigorous high availability level of service, or if you suspect disk errors are impacting performance or just reflecting age of use.



These two options are available:

- **Disk Scrubbing with Auto Parity Fix.** Select this option to detect and correct potential data corruption by actively searching disks for unreadable and mismatched blocks. This procedure should be scheduled for off-peak usage periods.

  Note: *only if snapshots are enabled. See Snapshots on page 97.*

- **Online File System Consistency Check.** Select this option to detect file system problems without making the data volume inaccessible. If file system issues are found, an offline file system check will be required. This procedure should be scheduled for off-peak usage periods.

  Note: *only if journaling is not disabled. See Performance on page 105.*

For more information about Volumes, see *Understanding Volume Management* on page 41.

Updating ReadyNAS Firmware

The ReadyNAS device offers the option to upgrade the operating firmware either automatically using the **Remote Update** option, or by manually loading an update image that has been downloaded from the NETGEAR Web site.

Updating Direct from the NETGEAR Web Site

If the ReadyNAS 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.

Note: It is always a good practice to backup data - especially data that cannot be replaced - before you perform a firmware update.

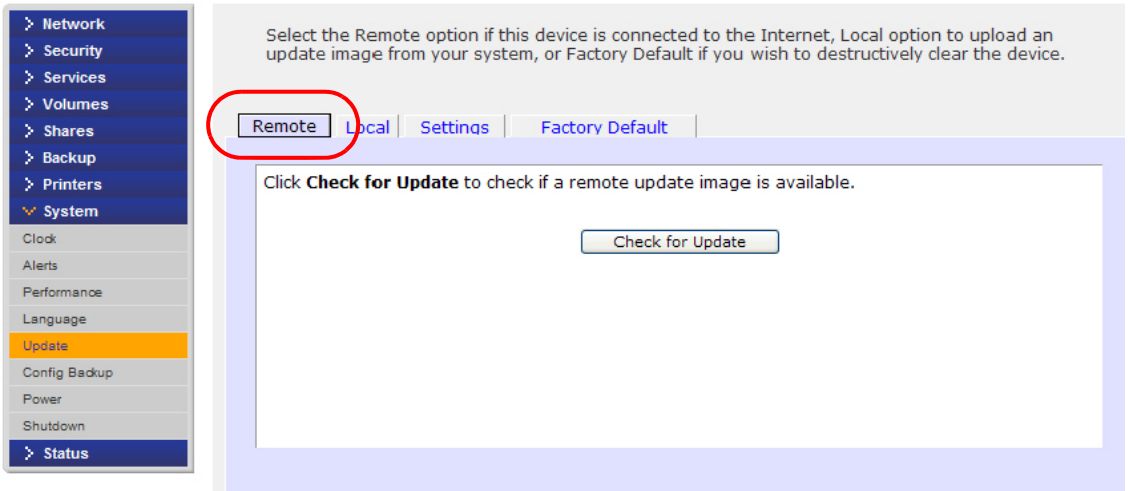
To use the Remote option:

1. Select **Update** from the main menu and then click the **Remote** screen.
2. Click **Check for Updates** to check for updates on the NETGEAR update server.
3. When prompted, click **Perform System Update**.

   After the download completes, you are prompted to reboot the system.

WARNING!

Do not click the browser Refresh button during the update process.

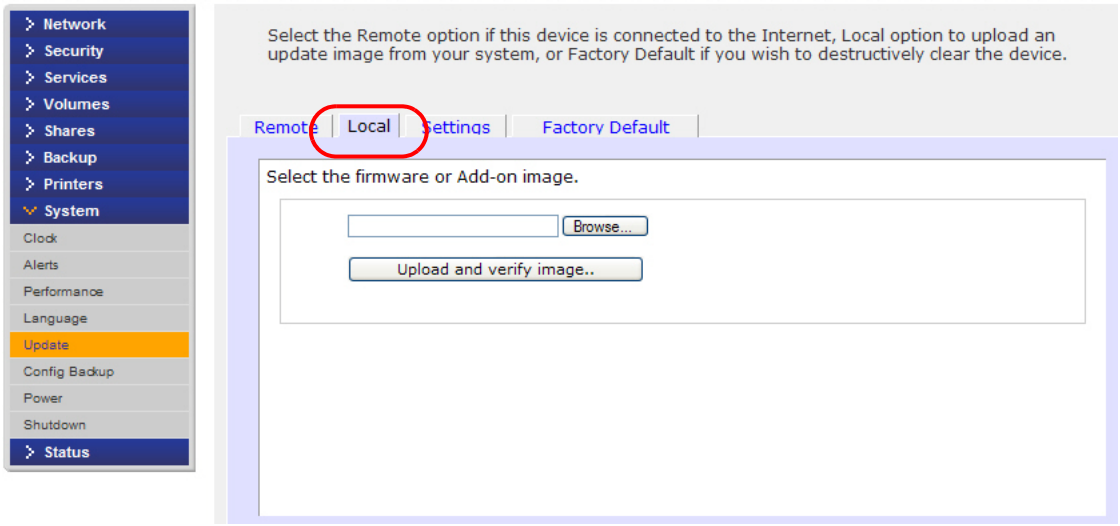


Updating from a Local Drive

When the ReadyNAS is not connected to the Internet, or Internet access is blocked, find a computer with internet access and download the RAIDiator firmware update image from ***http://readynas.com*** to a USB drive, or other transfer medium. Once downloaded, you can then upload that file to the ReadyNAS and perform the upgrade. The process takes several minutes, after which you need to reboot the system. You can then proceed with the upgrade.

To use the Local option:

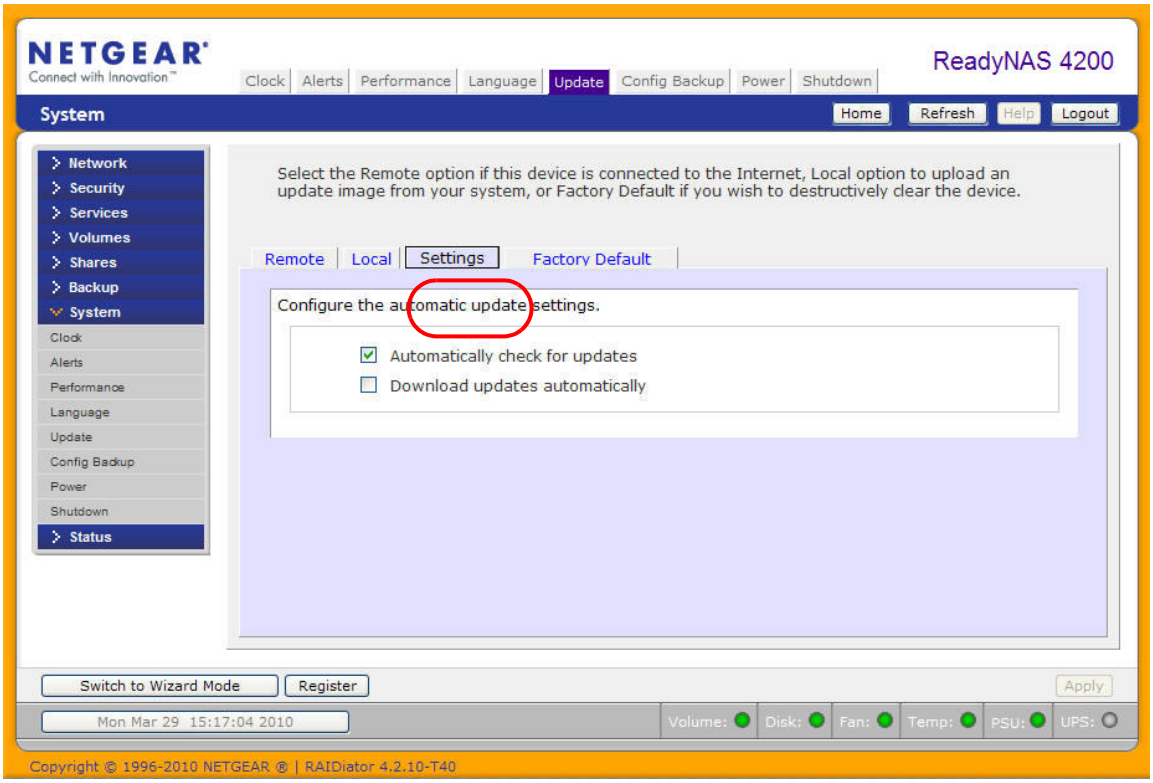
1. Select **Update** from the main menu, and then click the **Local** screen.
2. Click **Browse** to select the firmware image.
3. Click **Upload and verify image.**
4. When prompted, click **Perform System Update**.



Settings

Select **Update > Settings** to configure automatic update settings.

- Automatically check for updates
- Download updates automatically



Note: If an alert contact is configured, the administrator will get an email alert about available updates. See *Alerts* on page 35.

Restoring the Factory Default Settings

Use the **Factory Default** screen to reset the ReadyNAS device back to its factory default state.

Back up the data and configuration information that you want to keep prior to using this option. If you select this option, you must confirm the command by typing: **FACTORY**. You can also reset all settings to their factory defaults using the **Reset** button on the ReadyNAS chassis, according to the instructions in the *ReadyNAS Hardware Manual*.

WARNING!

Resetting to factory default erases everything, including data shares, volumes, configuration information, and user and group accounts. There is no way to recover after you confirm this command.

ReadyNAS Default Configuration Settings

Table 4.

Feature		Default
Login		
	User login URL when the ReadyNAS 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 RAIDiator firmware
	Discovery, multi-unit status monitoring, and RAID formatting utility	RAIDar for Windows, Mac, and Linux available from ***http://readynas.com***
LAN Connections		
	MAC address	Default address
	MTU size	1500
	Ports	**Note**: This setting is hardware-specific and will vary depending on the ReadyNAS system.
	LAN IP address	DHCP acquired

Understanding RAID

A

This appendix introduces the main benefits of X-RAID2, and provides an overview of RAID. It contains the following sections:

Understanding RAID

RAID is a well-established technology, and stands for Redundant Array of Independent Disks, which is a way of protecting your data in case of a disk failure. 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 following information.

RAID is used as an umbrella term for computer data storage schemes that can combine and replicate data among multiple hard disk drives. The different schemes and architectures are named by the word RAID followed by a number, as in RAID 0, RAID 1, and so on. RAID is designed to meet one of two key goals: increased data reliability or increased I/O performance. When multiple physical disks are set 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 operating system and computer user as one single disk.

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 more, depending on the type of RAID) disks in the array will not result in loss of data. A failed disk can be replaced by a new one, and the lost data can be 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.
- a RAID 5 array with several disks loses the capacity of one disk. Other types of RAID arrays are arranged so they are faster to write to, and read from, than a single disk.

RAID Levels

There are various RAID combinations that give various levels 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 those 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 might 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 you remove or add a drive; others support hot-swapping, allowing you to replace drives 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.

Note: RAID is not an meant to be an alternative or substitute for backing up data. Data might become damaged or destroyed without harm to the drive or drives on which they are stored. For example, part of the data might be overwritten by a system malfunction; a file might 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.

The Benefits of X-RAID2

X-RAID2 is a proven, NETGEAR technology for protecting your data, and is available only on NETGEAR ReadyNAS systems. Managing RAID volumes can be a complex chore, but X-RAID2 eliminates the complexity of volume management. X-RAID2 mode is an auto-expandable RAID technology and is the default configuration on most ReadyNAS units.

The ReadyNAS supports both X-RAID2 (the second generation X-RAID) and Flex-RAID (RAID 0/1/5/6) mode. Flex-RAID mode enables a more standard RAID configuration. See *Flex-RAID* on page 43 and *Flex-RAID* on page 124.

X-RAID2 Is Auto-expandable RAID

Over time, chances are that you will need to expand volume capacity to either add redundancy or add more file storage space. In typical RAID systems, the steps required to expand volumes can be so complex and error prone that it leads to data loss.

A major X-RAID2 advantage is its ability to automatically expand to include the full space of new disks. X-RAID2 enables volume expansion without reformatting your disks or shuffling data back and forth. X-RAID2 automates these complex tasks, and provides volume management features previously available only in enterprise-level storage solutions.

When as few as two of your disks have extra capacity, the data volume automatically expands its capacity. The data volume capacity increases every time a larger disk is added, regardless of the capacity of the other disks in the system.

The process occurs in the background, so access to the ReadyNAS is not interrupted. Furthermore, X-RAID2 supports multiple parity, which provides protection against two simultaneous disk failures.

Simplified Redundancy

X-RAID2 requires one data volume of 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, and so on.

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 need 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 and scan it 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 could take anywhere from 30 minutes to several hours. Synchronization occurs in the background so you can keep on working with the ReadyNAS during this time.

Once synchronization completes, the data volume is redundant. This means that if one disk fails, the other disk contains all the data, so your are protected from a disk failure. Furthermore, X-RAID2supports multiple parity, which provides protection against two simultaneous disk failures.

Note: X-RAID2 does not replace backups.

Easy Volume Expansion

X-RAID2 supports both vertical and horizontal expansion.

Horizontal expansion is the process of adding more disks to a ReadyNAS.

Vertical expansion increases the volume capacity when higher capacity disks are installed in the ReadyNAS. You can take advantage of higher capacity, or more affordable disks to grow the size of a ReadyNAS volume by replacing a disk with a larger one, adding more disks, or both, as they become available.

After the initialization process, the ReadyNAS synchronizes the new disk or disks, 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 also 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 completed, and there are a minimum of two disks with more capacity in the system, 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 new disk, less any additional overhead needed to assure the redundancy of the data on the volume.

You can expand the ReadyNAS volume repeatedly with additional disks and higher capacity disks, adding to the value of your investment in a ReadyNAS. For more information visit ***http://readynas.com/?cat=54.***

See *Changing between X-RAID2 and Flex-RAID Modes* on page 46 for more information.

Flex-RAID

Flex-RAID technology utilizes the industry-standard RAID levels 0, 1, 5, and 6. 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, and reconfigure your volume. See *Flex-RAID* on page 43 for more information about volumes.

Flex-RAID advantages include:

- 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, 5, or 6 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.

See *Changing between X-RAID2 and Flex-RAID Modes* on page 46 for more information.

Notification of Compliance

ReadyNAS for Business

B

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ReadyNAS for Business complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and

- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, ReadyNAS for Business, does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

European Union

The ReadyNAS for Business complies with essential requirements of EU EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC as supported by applying the following test methods and standards:

- EN55022: 2006 / A1: 2007
- EN55024: 1998 / A1: 2001 / A2 : 2003
- EN60950-1: 2005 2nd Edition
- EN 61000-3-2:2006
- EN 61000-3-3:1995 w/A1: 2001+A2: 2005

Index

T

U

V

W

X