NETGEAR

ReadyNAS for Home RAIDiator 4.2

Software Manual

x86 Models:

Ultra Series (2, 4, 6)
Ultra Plus Series (2, 4, 6)
Pro Pioneer
NVX Pioneer

350 East Plumeria Drive
San Jose, CA 95134
USA

September 2011
202-10654-06

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.

Table of Contents

Chapter 4 Users and Groups

Chapter 5 System Settings

Chapter 6 Monitor, Maintain, and Optimize

Chapter 7 Backup and Recovery

Appendix A Notification of Compliance

Index

Getting Started

1

This *NETGEAR® ReadyNAS for Home RAIDiator 4.2 Software Manual* describes how to configure and manage your ReadyNAS storage system.

Your ReadyNAS® storage system relies on the following software applications:

- **RAIDar**. Use this setup utility to find your ReadyNAS system on your local area network and launch FrontView.
- **FrontView**. Use this browser-based interface to configure and manage your ReadyNAS system.

This chapter includes the following topics:

Quick-Start Guide

This manual provides conceptual information about storage systems, detailed instructions about using your system, and NETGEAR's recommendations about configuring, managing, and backing up your system. NETGEAR recommends that you read this manual to make the best use of your storage system.

To quickly start using your system, review the following sections in this order:

1. *RAIDar* on page 10. You use RAIDar to discover your storage system on your network.
2. *Setup Wizard* on page 14. This wizard guides you through initial setup of your system in a few simple screens.
3. *Manage File-Sharing Protocols* on page 35. File-sharing protocols enable you to transfer files across a network.
4. *Create Shares* on page 37. Shares are similar to folders or directories and are the way you organize the data you store on your ReadyNAS system.
5. *Create User Accounts* on page 63. You create a user account for each person that you want to allow to access your ReadyNAS system.
6. *Basic Backup Concepts* on page 127. You can back up the data you store on your ReadyNAS system and you can use your ReadyNAS system to back up data you store on other devices.

Additional Documentation

NETGEAR maintains a community website that supports ReadyNAS products. Visit *http://www.readynas.com* for reviews, tutorials, comparison charts, software updates, documentation, an active user forum, and much more.

For information about your system's hardware, see the *ReadyNAS Ultra, Ultra Plus, NVX, and Pro Series Hardware Manual*, which is available at *http://www.readynas.com/documentation*.

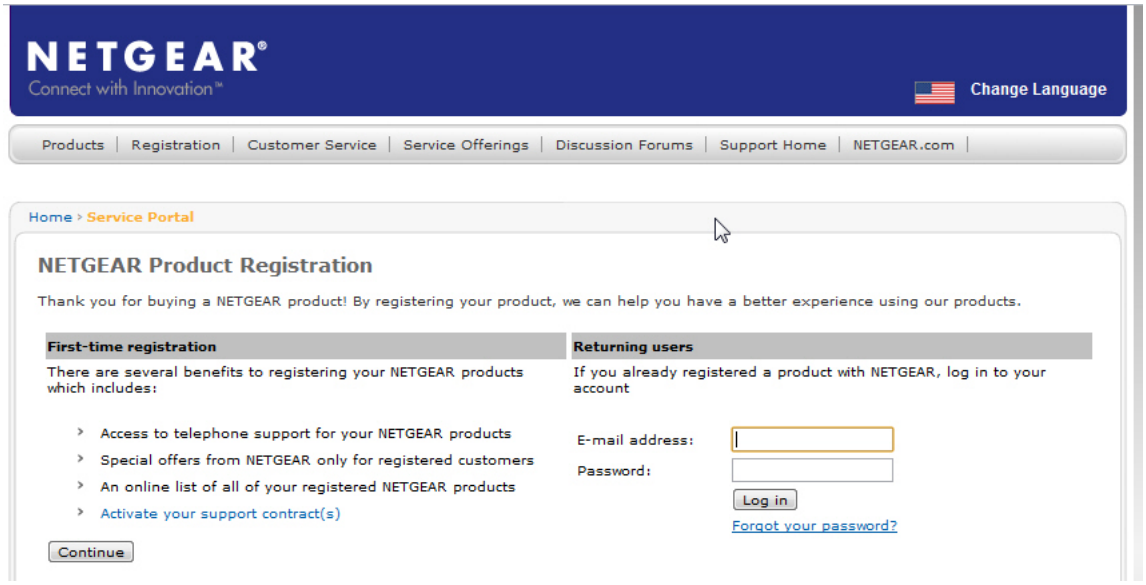
Register Your System

Registration is required before you can use the NETGEAR telephone support service. You can register your system by clicking the **Register** button in FrontView or the Setup Wizard, or by accessing the NETGEAR Product Registration website directly.

➢ **To register your system using the NETGEAR Product Registration website:**

1. Locate the serial number on the label of your product.
2. Using a browser, visit *http://www.NETGEAR.com/register*.

   The product registration web page displays.



   If you have never registered a NETGEAR product, click the **Continue** button.

   If you have registered a NETGEAR product in the past, enter your email address and password and click the **Log in** button.

3. Follow the prompts to register your ReadyNAS system.

Diskless Units

If you have a diskless ReadyNAS storage system, you must first install and format at least one disk before you can use RAIDar or FrontView. For more information, see the *ReadyNAS Ultra, Ultra Plus, NVX, and Pro Series Hardware Manual.*

You must use supported disks in your ReadyNAS system. For a list of supported disks, see *http://www.readynas.com/hard_disk_hcl*.

RAIDar

RAIDar is a software application that you use to discover ReadyNAS storage systems on your network. RAIDar is included on the *Resource CD* that came with your unit. It includes versions for Windows, Mac, and Linux operating systems. It is also available at *http://readynas.com/start*.

RAIDar displays several LED icons to help you determine the status of your system, as shown in *Figure 1*.

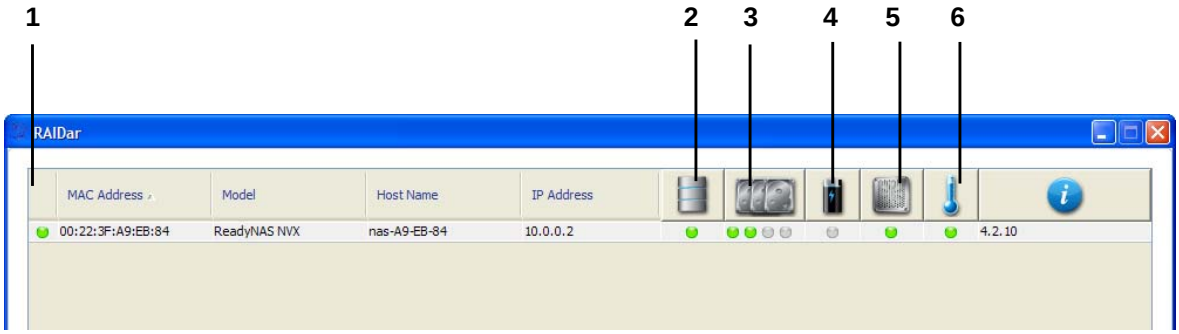


Figure 1. RAIDar LED icons

1. Overall status
2. Volume status
3. Disk status
4. UPS status
5. Fan status
6. Temperature

Table 1 provides a description of each LED icon.

Table 1. RAIDar LED icon descriptions

LED Icon	Description
	No disk or device is attached.
	The device is operating normally.
	The device failed or needs attention.
	This disk is a spare disk on standby. If a disk fails, this disk takes over automatically.
(Blinking)	This disk is currently resyncing.

Table 1. RAIDar LED icon descriptions (Continued)

LED Icon	Description
	The volume is in life-support mode. Life-support mode happens when the volume encounters multiple disk failures and might be dead. However, the ReadyNAS storage system has blocked it from being marked dead in case someone accidentally removed the wrong disk while the system was running. If the wrong disk was pulled out, shut down the system immediately, reconnect the disk, and power-on the system. **Note:** If you reconnect the disk while the system is running, the disk will be marked as a newly added disk and all the data on that disk will be lost during the initialization process.
	A lengthy background task such as a system update is in progress.

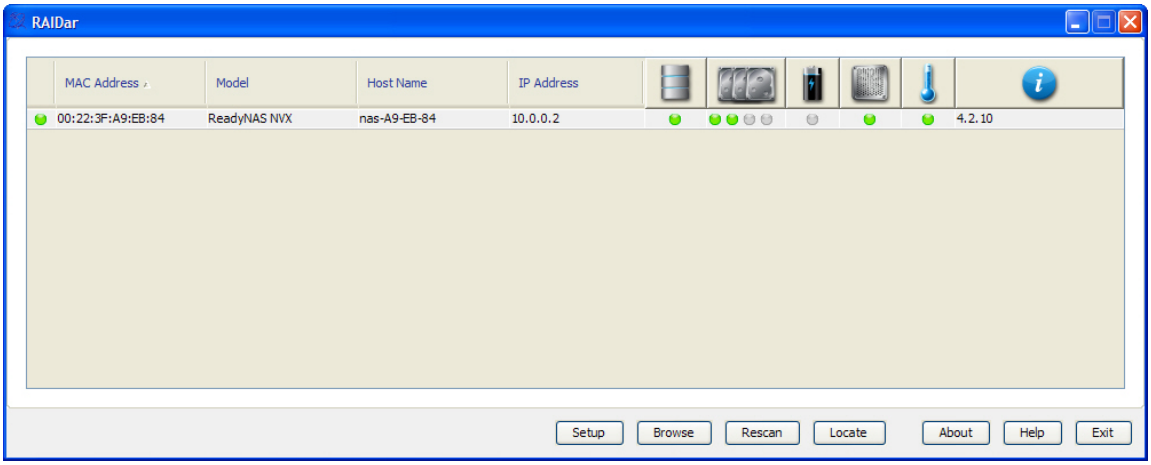
You can use the following buttons to learn more about the ReadyNAS system or systems on your network:

- **Setup**. Launches FrontView for the highlighted system.
- **Browse**. Displays the shares available on the highlighted system. This feature works on the Windows platform only.
- **Rescan**. Updates the list of ReadyNAS systems on the network and updates the status of each system it discovers.
- **Locate**. Causes the LEDs on the highlighted system to blink. This is useful if you have multiple ReadyNAS storage systems and you need to determine which RAIDar entry corresponds to which physical system.
- **About**. Displays RAIDar information.
- **Help**. Displays the help screen.
- **Exit**. Closes RAIDar.

➢ **To discover your ReadyNAS system and launch FrontView:**

1. Install the appropriate version of RAIDar on a computer that is connected to the same local area network (LAN) as your ReadyNAS storage system.
2. If you are using Windows XP before SP2, disable the Internet connection firewall.
3. Launch the RAIDar utility.

   RAIDar displays a window that lists the ReadyNAS system or systems on your network and provides details about the status of each system it discovers.



The default IP configuration is set to DHCP, which is how home routers assign IP addresses by default.

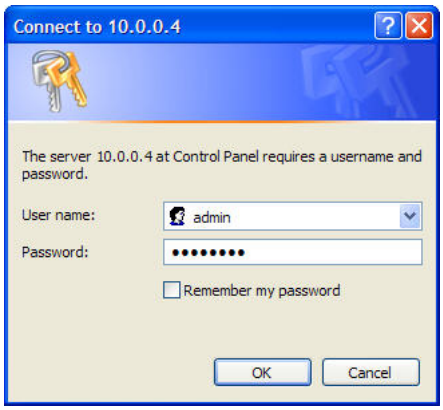
If you are not using DHCP on your router, or if it is not working properly, your storage system cannot get an IP address. In that case, your system uses 192.168.168.168. If this happens, you must make a direct connection between your storage system and your computer. To establish this connection, follow your operating system's instructions for assigning a static IP address to your computer in the 192.168.168 subnet.

If your ReadyNAS system is not detected, check the following and click **Rescan** to try again:

- Make sure the ReadyNAS device is turned on and is connected to your network.
- Make sure your client PC running RAIDar is on the same subnet as the ReadyNAS device.
- If you are running RAIDar on Windows XP before SP2, disable the Internet connection firewall.

4. Highlight your ReadyNAS system and click the **Setup** button.

   RAIDar opens your default browser and prompts you to log in to the storage system.



5. Log in to the unit using the default login credentials:
   - **Default user name**. admin
   - **Default password**. netgear1

   Both user name and password are case-sensitive.

   The first time you connect to your ReadyNAS system, a Setup Wizard displays to guide you through initial configuration. This wizard also displays the first time you log in to your system after you perform a factory default reboot. For more information about factory default reboots, see the appropriate hardware manual for your storage system.

   Any other time you log in to your unit, FrontView displays.

Setup Wizard

When you launch FrontView for the first time, FrontView launches in Wizard mode. FrontView also launches in Wizard mode the first time you use your storage system after a factory default reboot.

NETGEAR recommends using the Setup Wizard the first time you use your storage system. The Setup Wizard guides you step-by-step through the configuration process, assisting you in quickly integrating your ReadyNAS storage system into your network. Follow the Setup Wizard's prompts to configure the following settings:

- **Disk configuration**. The Setup Wizard configures your system in X-RAID2 mode. For more information, see *X-RAID2* on page 18. If you want to configure your system in Flex-RAID mode, you can change the configuration after you complete the Setup Wizard. For more information, see *Change from X-RAID2 to Flex-RAID* on page 29.
- **Time and date**. For more information, see *Clock* on page 79.
- **Contact email addresses**. For more information, see *Email Alert Contacts* on page 80.
- **IP addresses**. For more information, see *Ethernet* on page 88.
- **Hostname**. For more information, see *Hostname* on page 91.
- **DNS settings**. For more information, see *DNS* on page 92.
- **Administrator password and password recovery question and answer**. For more information, see *Administrator Password* on page 84.
- **User and group accounts**. For more information, see *Basic User and Group Concepts* on page 61.
- **File-sharing protocols**. For more information, see *File-Sharing Protocols* on page 33.
- **Streaming services**. For more information, see *Streaming Services* on page 95.
- **Shares**. For more information, see *Basic Share Concepts* on page 32.
- **Printers**. For more information, see *Printer Queue Service* on page 87.
- **Product registration**. For more information, see *Register Your System* on page 9.

To switch to Advanced Control mode, click the **Switch to Advanced Control** button.

When you complete the wizard, FrontView automatically switches to Advanced Control mode. *Figure 2* shows the FrontView home screen in Advanced Control mode.

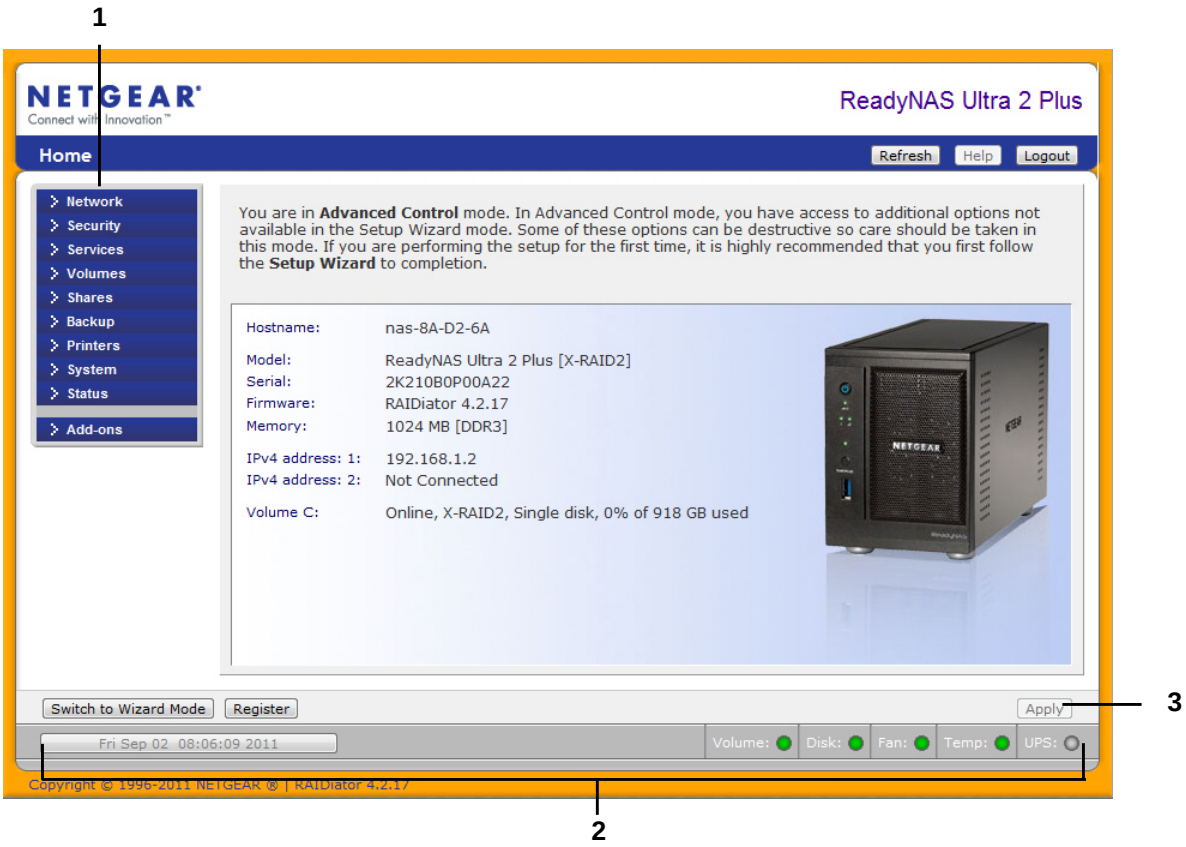


Figure 2. FrontView home screen in Advanced Control mode

1. Main menu
2. Status bar
3. Apply button

To return to Wizard mode, click the **Switch to Wizard Mode** button.

FrontView includes a main menu on the left side of the window that helps you navigate through it. The status bar at the bottom of the FrontView screen provides you with a quick overview of your system's status and provides access to the following information:

- Date and time
- Volume
- Disks
- Fan
- Temperature
- UPS

Hover your cursor over a status LED to display device information, or click a LED light or the date and time data to open the related FrontView screen.

2. Disk Configuration

This chapter describes how to configure the disks in your ReadyNAS storage system. It contains the following sections:

- *Basic Disk Configuration Concepts*
- *Manage Disk Configuration*

Basic Disk Configuration Concepts

To get the most out of your ReadyNAS storage system, it is helpful to understand some disk configuration concepts. Understanding these concepts is the first step to making good decisions about how to configure, manage, and use your ReadyNAS storage system.

You can configure your storage system's hard disks in a variety of ways. The most common way to configure disks is using one of the many RAID technologies.

RAID

RAID is short for redundant array of independent disks. RAID is a storage technology that balances data protection, system performance, and storage space by determining how the storage system distributes data. Many different ways of distributing data have been standardized into various RAID levels. Each RAID level offers a tradeoff of data protection, system performance, and storage space. For example, one RAID level might improve data protection but reduce storage space. Another RAID level might increase storage space but also reduce system performance.

Your ReadyNAS storage system supports X-RAID2™, a proprietary single-volume RAID architecture that is easy to administer, and Flex-RAID, which allows you to format your disks in a variety of industry-standard RAID levels.

Volumes

In the most general sense, volumes are data storage devices. Your computer treats an internal hard drive as a volume. It also treats a portable USB thumb drive as a volume.

Volumes can be either physical or logical. Usually, the term *physical volume* refers to a hard disk drive. When this term is used in this way, a two-bay storage system can have up to two physical volumes (hard disk drives), a four-bay storage system can have up to four physical volumes (hard disk drives), and a six-bay storage system can have up to six physical volumes.

The term *logical volume* refers to the way that you divide, or partition, your storage space, for example:

- Each logical volume can correspond to a hard disk drive
- A logical volume can be made up of more than one hard disk drive
- A hard disk drive can be divided into multiple logical volumes

In this manual, the term *volume* refers to a *logical volume*. In this manual, the terms *hard disk drive* and *disk* refer to a *physical volume*.

X-RAID2

X-RAID2 is an autoexpandable RAID technology that is available only on ReadyNAS systems.

Because X-RAID2 is a single-volume architecture, if you configure your hard disk drives to use X-RAID2, your storage system has only one volume that is made up of all installed hard disk drives. X-RAID2's single volume architecture has two major advantages:

- Easy system management
- Auto expansion

With typical RAID formatting, if you want to add disks or replace disks with larger capacity disks, you must back up the data to another system, add a new disk, reformat the RAID volume, and restore the data to the new RAID volume. With X-RAID2, none of those administrative tasks are required. Instead, with X-RAID2, your volume automatically expands to accommodate additional disks or larger capacity disks when you replace smaller capacity disks.

With X-RAID2, you can start out with one hard disk, add a second disk for data protection, then add more disks for additional capacity, and X-RAID2 accommodates the new disks automatically. You can replace existing disks with larger capacity disks and X-RAID 2 automatically accommodates the new disks.

X-RAID2 requires a minimum of two hard disks to provide protection against disk failure. If you have a one-disk ReadyNAS storage system 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 added while the system is running.

X-RAID2 uses the first disk to store data, and the second disk to store parity information that allows it to re-create data if a disk fails. This means that In a two-disk system, the usable storage space is one disk. In a three-disk system, the usable storage space is two disks, and in a four-disk volume, the usable storage space is three disks.

Figure 3 illustrates how X-RAID2 uses new disks.

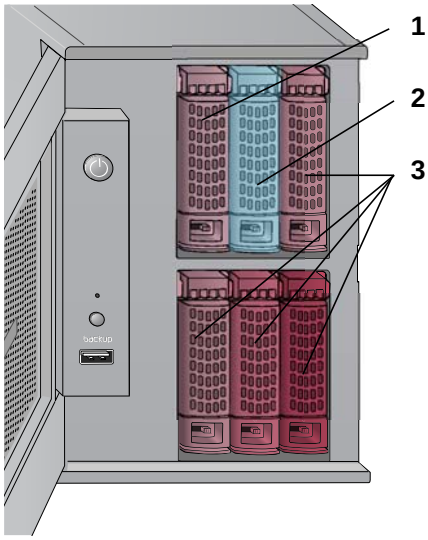


Figure 3. X-RAID2 disk usage

1. Initial storage space
2. Data protection
3. Additional storage space

With X-RAID2, you do not need to know intricate details about RAID to administer your system. X-RAID2 allows you to add storage space without reformatting your drives or moving your data to another location. Because the expansion happens online, you can continue to use the ReadyNAS while the underlying volume capacity increases.

Flex-RAID

NETGEAR's Flex-RAID technology allows you to choose from among several industry-standard RAID levels:

- **RAID 0**. This is the simplest RAID level, and is misnamed, because it does not offer redundancy to protect your data from loss in the event that one of your drives fails. RAID 0 distributes data across multiple disks, which allows it to offer better performance than disks that do not use RAID formatting. The total capacity of your storage system equals the capacity of all of your disk drives.
- **RAID 1**. This RAID level provides full redundancy of your data, because it duplicates data across multiple disks, providing full redundancy. In RAID 1, exactly the same data is stored on two or more disks at all times. RAID 1 protects your data from loss if one disk fails. The total capacity of your storage system equals the capacity of your smallest disk.
- **RAID 5**. Supported on systems with at least four drive bays, this RAID level also provides data redundancy, but it requires at least three disks. RAID 5 uses one disk to protect you from data loss if one disk fails. The total capacity of your storage system equals the capacity of all your disks minus the capacity of one disk.

- **RAID 6**. Supported on ReadyNAS systems with at least six drive bays, this RAID level requires a minimum of four installed disks. While very similar to RAID 5, RAID 6 uses two sets of parity data, meaning that you are protected against data loss if one or two disks fail. The total capacity of your storage system equals the capacity of all your disks minus the capacity of two disks.
- **RAID 10**. Supported on systems with at least four drive bays, this RAID level duplicates data the way that RAID 1 does, but also uses mirroring. RAID 10 provides excellent data protection but at the cost of storage capacity. RAID 10 requires that an even number of drives are installed in your system, and it requires that a minimum of four drives are installed. The total capacity of your storage system equals the capacity of your smallest drive multiplied by the number of drives, divided by two.

Manage Disk Configuration

You can use FrontView to manage the configuration of the hard disks installed in your system.

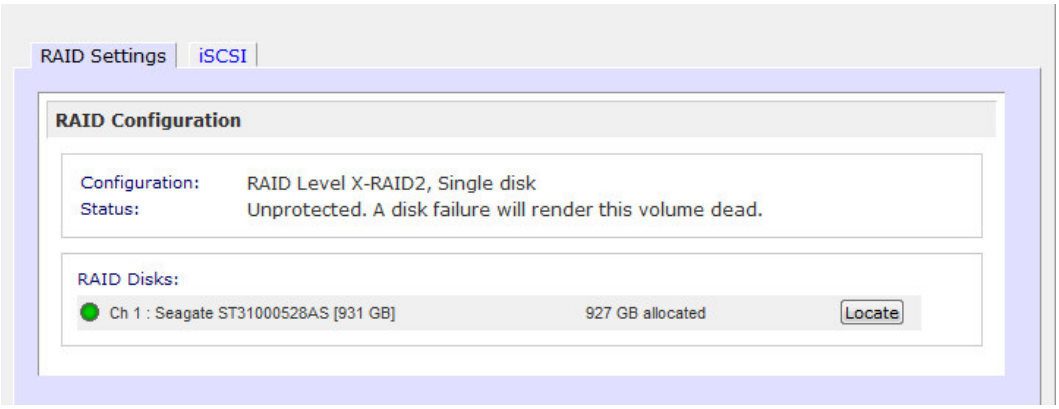
Locate a Disk

If you have multiple disks installed in your ReadyNAS system, you might want to use the Disk LEDs to identify which disk maps to which information in FrontView.

➢ **To locate a disk:**

1. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings screen displays.



2. Click the **Locate** button in the row for the disk you want to identify.

   That disk's LED blinks for 15 seconds.

   For more information about the disk LEDs on your system, see the *ReadyNAS Ultra, Ultra Plus, NVX, and Pro Series Hardware Manual*.

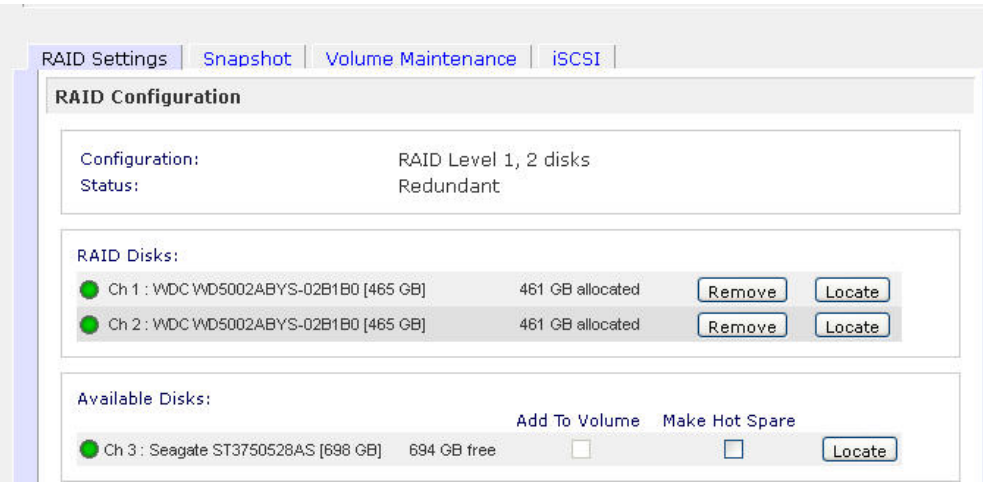
Make a Disk a Hot Spare

A hot spare disk remains in standby mode and automatically replaces data from a failed disk from the volume. If your volume is configured as RAID 1 or RAID 5, and your system at least one disk more than the minimum for that RAID level installed, you can specify one disk to function as a hot spare.

➢ **To make a disk a hot spare:**

1. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings screen displays.



2. In the row for the disk you want to make a hot spare, select the **Make Hot Spare** check box.
3. Click the **Apply** button.

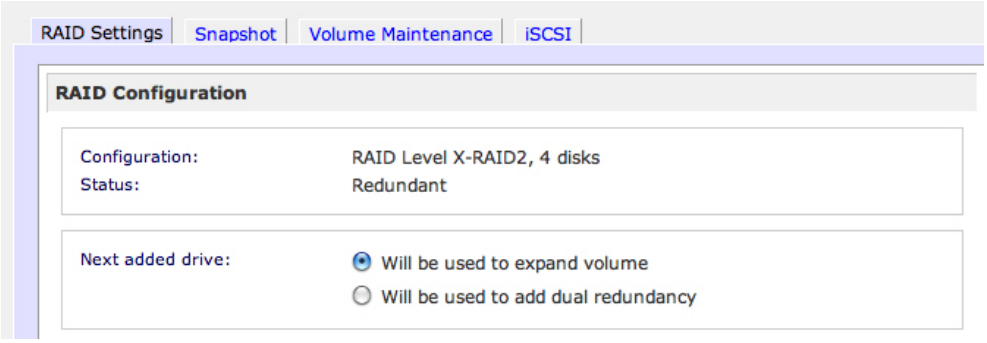
Implement Dual Redundancy

If your 6-bay ReadyNAS system is uses X-RAID2 mode, you can configure it to use added disks to expand storage space or to increase data protection by implementing dual redundancy. Dual redundancy protects you against data loss if two disks fail. The tradeoff is that the disk that is used for dual redundancy protection cannot be used for storage space.

➢ **To implement dual redundancy:**

1. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings screen displays.



2. Select the **Will be used to add dual redundancy** radio button.
3. Click the **Apply** button.

   The next disk you add will be used to implement dual redundancy.

Remove a Disk from a Volume

If you remove a disk from a volume, the volume is still available but in a nonredundant state. If a disk failure occurs after you remove a disk from a volume, this volume becomes unusable. This is useful to test performance in a degraded volume. This procedure is only appropriate for controlled test environments.

WARNING!

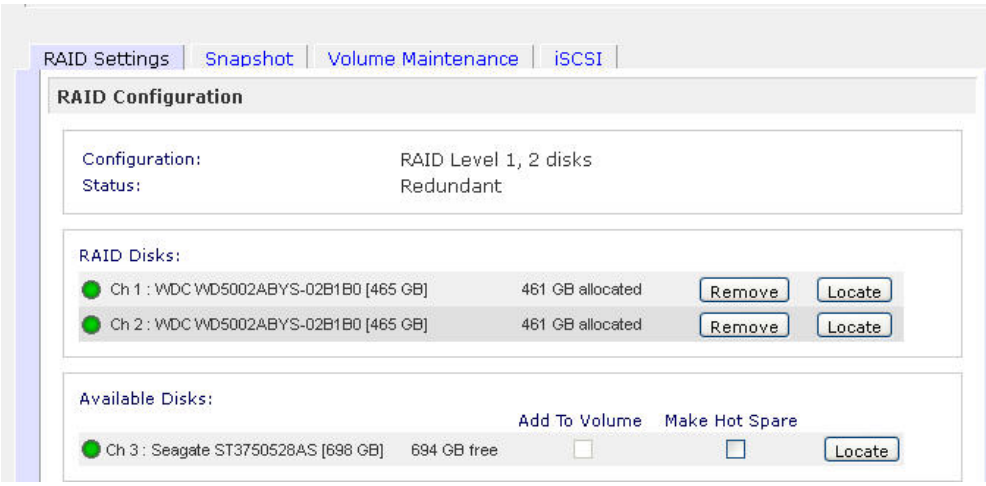
Do not remove a disk from a volume in a live production environment. Depending on how your ReadyNAS system is configured, you risk losing data when removing a disk from a volume.

This procedure applies only to ReadyNAS systems that are configured in Flex-RAID mode.

➢ **To remove a disk from a volume:**

1. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings screen displays.



2. In the row for the disk you want to remove, click the **Remove** button.

   You are prompted to confirm the remove command.

3. Click the **OK** button.

   The disk is removed from the volume.

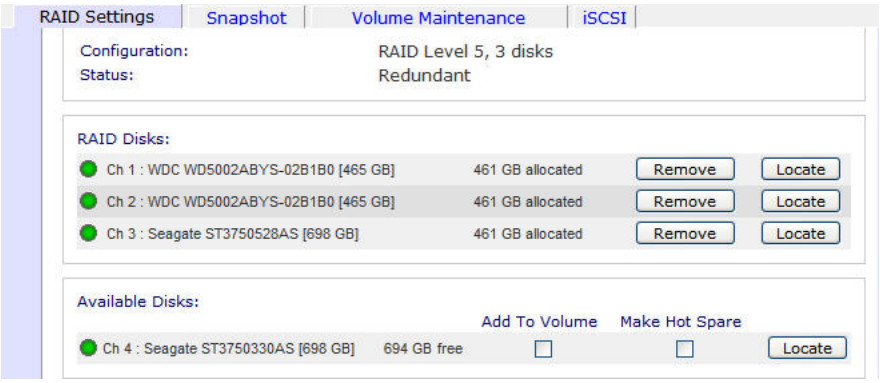
Expand a Flex-RAID Volume

You can expand volumes that are formatted in Flex-RAID mode without losing data.

➢ **To expand Flex-RAID volumes:**

1. Select **Volume > Volume Settings**.

   The Volume Settings screen displays.



2. In the Available Disks pane, select the **Add To Volume** check box for the disk where you want to expand the volume.

   A pop-up window displays advising you that the disk will be used for volume expansion after you reboot your system.

3. Click the **OK** button.

   The pop-up window closes.

4. Click the **Apply** button.

   A pop-up window displays advising you to reboot your system.

5. Click the **OK** button.

   The pop-up window closes.

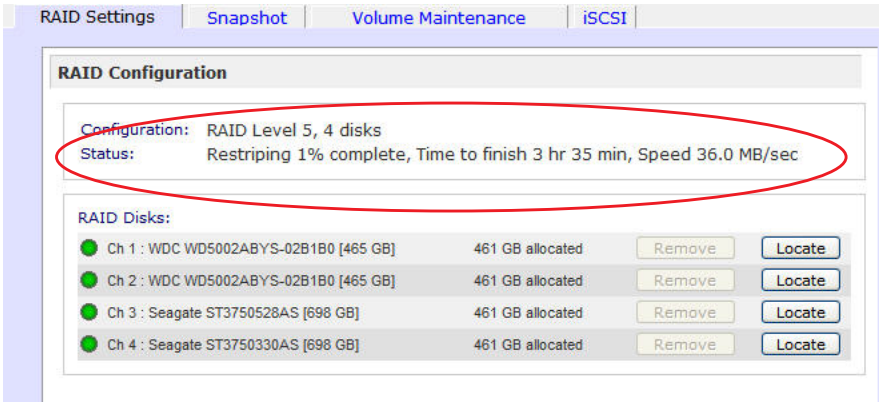
6. Select **System > Shutdown**.
7. The Shutdown Options screen displays.
8. Select the **Shutdown and reboot device** radio button and click **Apply**.

   After your system restarts, a pop-up window displays advising you that the volume expansion process is under way. Ensure that your system is not interrupted during this process.

9. Click the **OK** button.

   The pop-up window closes.

   The RAID Configuration pane advises you of the progress of the volume expansion process.



   The volume expansion process can take several hours. If you set up email notifications for your system, you receive an email message when the expansion process completes.

Reconfigure a Volume in Flex-RAID Mode

You can reconfigure a Flex-RAID volume, split it into multiple volumes, specify a different RAID level, or specify a larger reserved space for snapshots. The process involves these high-level steps:

1. Delete the volume that you want to reconfigure.

WARNING!

The process of deleting a volume erases all data stored on that volume. That data cannot be recovered.

2. Create the replacement volume.
3. Specify RAID settings.

These steps are explained in more detail in the following section.

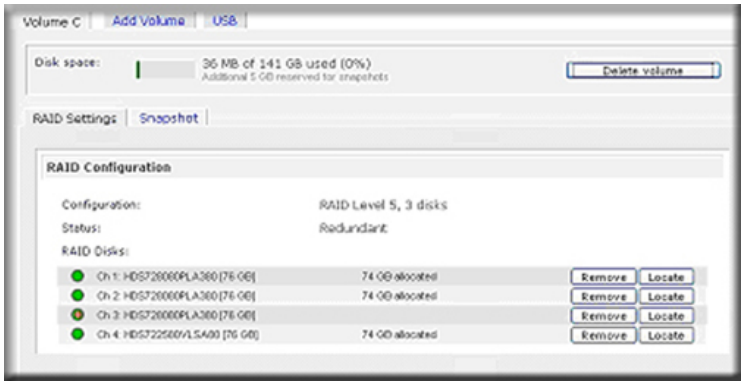
➢ **To reconfigure a Flex-RAID volume:**

1. If the volume that you intend to delete contains any data that you want to keep, back up that data.

   For more information, see *Back Up Data Stored On Your ReadyNAS System* on page 130.

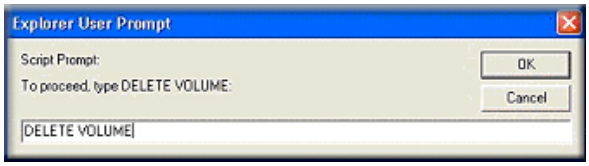
2. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings screen displays. If your system is configured with multiple volumes, click the tab for the volume that you want to delete.



   In this example, the ReadyNAS system has just one volume, Volume C.

3. Click the **Delete Volume** button.
4. A dialog box displays asking you to confirm the delete volume command.

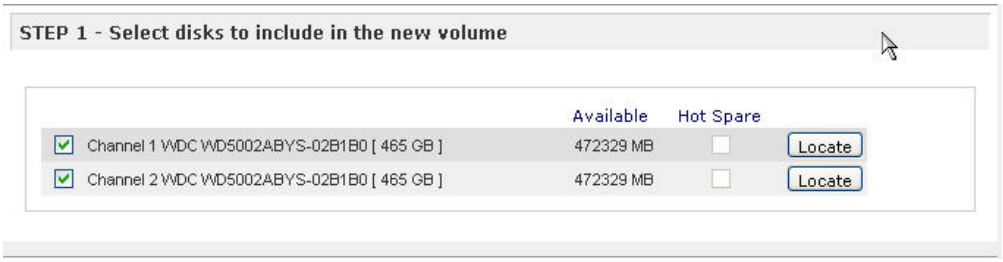


5. Enter **DELETE VOLUME** in the field and click the **OK** button.

   The volume is deleted.

6. Click the **Add Volume** tab.

   The Add Volume screen displays.



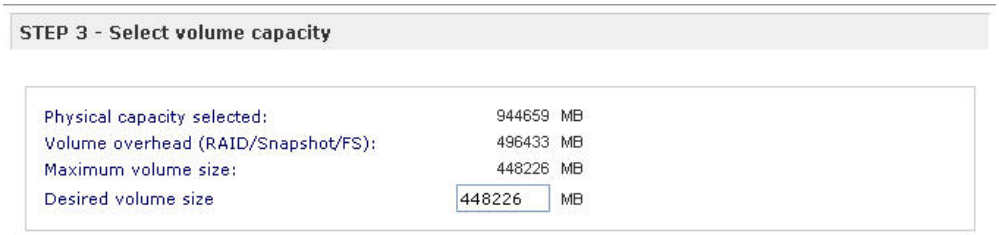
7. In the STEP 1 pane, select the check boxes for the disks you want to include in the new volume.
8. (Optional) Select the **Hot Spare** check box for any disk that you want to specify as a hot spare.

   For more information, see *Make a Disk a Hot Spare* on page 21.

9. In the STEP 2 pane, using the **Select RAID level** drop-down list, assign a RAID level to this volume.

   For more information about RAID levels, see *Flex-RAID* on page 19.

10. In the STEP 3 pane, enter the maximum size for this volume in the **Desired volume size** field.



11. Click the **Apply** button.

    You are prompted to reboot your system.

12. Reboot your system.
13. Use RAIDar to reconnect to your ReadyNAS system.

    For more information, see *RAIDar* on page 10.

14. Restore any backed-up data to the reconfigured volume.

    For more information, see *Recover Data to Your ReadyNAS System* on page 134.

Change RAID Modes

You can change the RAID mode that your ReadyNAS storage system uses. Because this process erases all data, if data is stored on your system, you must first back it up to another storage device before changing the RAID format.

The process involves resetting your ReadyNAS storage system to factory default settings and using RAIDar to configure the volume during a 10-minute delay during boot.

Change from Flex-RAID to X-RAID2

You can reconfigure your ReadyNAS system from Flex-RAID mode to X-RAID2 mode.

➢ **To change from Flex-RAID to X-RAID2:**

1. If any data is stored on your system, back up your data.

   For more information, see the *Back Up Data Stored On Your ReadyNAS System* on page 130.

2. Perform a factory reset reboot.

WARNING!

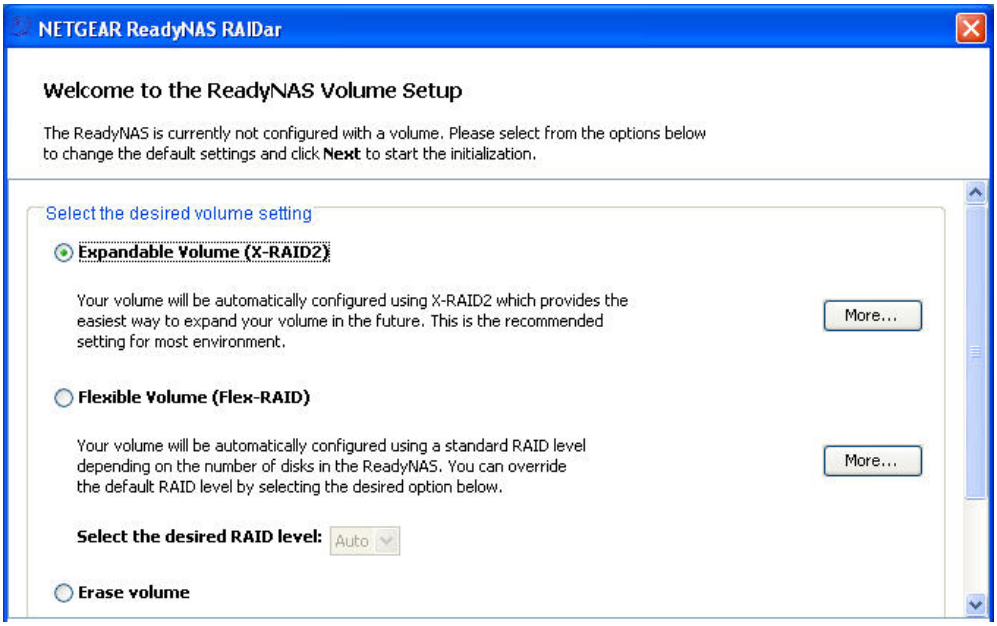
Setting your ReadyNAS system to its factory defaults erases all data and configuration settings.

The process for performing a factory reset reboot varies by storage system. For more information about how to perform a factory reset reboot, see the *ReadyNAS Ultra, Ultra Plus, NVX, and Pro Series Hardware Manual*.

During the factory reboot process, you have a 10-minute window to choose a RAID configuration. RAIDar sends a prompt to click the Setup button during this 10-minute time frame.

3. Launch RAIDar, highlight your storage system, and click the **Setup** button.

   The ReadyNAS Volume Setup screen displays.



   If you do not select a format within 10 minutes, your system reboots in the same mode that it was previously using.

4. Select the **Expandable Volume (X-RAID2)** radio button.
5. (Optional) Select the check box below the Expandable Volume (X-RAID2) radio button.

   This option implements dual redundancy. It is available only on 4-bay or 6-bay ReadyNAS systems. For more information, see *Implement Dual Redundancy* on page 22.

6. Click the **Next** button.

   You are prompted to confirm the volume creation command.

7. Click the **OK** button.

   The volume is formatted.

   This can take quite a while, depending on the size of your hard disk drives.

8. (Optional) Restore any backed-up data to the reformatted disks.

   For more information, see *Recover Data to Your ReadyNAS System* on page 134.

Change from X-RAID2 to Flex-RAID

You can reconfigure your system from X-RAID2 mode (the factory default mode) to Flex-RAID mode.

➢ **To change from X-RAID2 to Flex-RAID:**

1. If any data is stored on your system, back up your data.

   For more information, see the *Back Up Data Stored On Your ReadyNAS System* on page 130.

2. Perform a factory reset reboot.

WARNING!

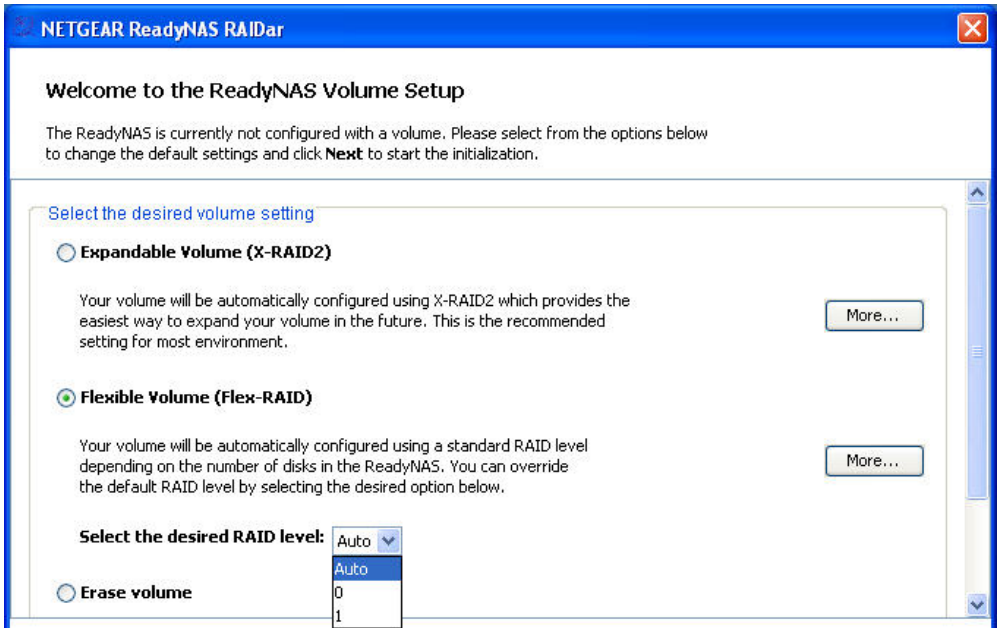
Setting your ReadyNAS system to its factory defaults erases all data and configuration settings.

The process for performing a factory reset reboot varies by storage system. For more information about how to perform a factory reset reboot, see the *ReadyNAS Ultra, Ultra Plus, NVX, and Pro Series Hardware Manual*.

During the factory reboot process, you have a 10-minute window to choose a RAID configuration. RAIDar sends a prompt to click the Setup button during this 10-minute time frame.

3. Launch RAIDar, highlight your storage system, and click the **Setup** button.

   The ReadyNAS Volume Setup screen displays.



If you do not select a format within 10 minutes, your system reboots in the same mode that it was previously using.

4. Select the **Flexible Volume (Flex-RAID)** radio button.
5. Select a RAID level from the **Select the desired RAID level** drop-down menu.

   If you select Auto, your ReadyNAS system automatically chooses a RAID level based on the number of disks that are installed in your system, as follows:

Number of installed disks	RAID level automatically chosen
1	RAID 1
2	
3	RAID 5
4	
5	RAID 6
6	

6. Click the **Next** button.

   You are prompted to confirm the volume creation command.

7. Click the **OK** button.

   The volume is formatted. This can take quite a while, depending on the size of your hard disk drives.

8. (Optional) Restore your any backed-up data to the reformatted disks.

   For more information, see *Recover Data to Your ReadyNAS System* on page 134.

3 Shares

This chapter describes how to create, manage, and access shares on your storage system. This chapter includes the following topics:

- *Basic Share Concepts*
- *Manage File-Sharing Protocols*
- *Create Shares*
- *Manage Shares*
- *Access Shares Remotely*

Basic Share Concepts

The volume or volumes on your ReadyNAS storage system are divided into shares, which are similar to folders or directories.

Data Organization

Shares are the way that you group your data. You might want to group your data by type, for example:

- Photos
- Music
- Videos
- Documents

Another option is to group your data by user:

- Tom
- Rick
- Mary

Organizations might choose to group data by department:

- Accounting
- Sales
- Personnel

You can combine these schemes or come up with your own scheme.

Your ReadyNAS storage system comes with two shares already created:

- backup
- media

If you want, you can delete or rename these shares. You can create other shares to organize your data.

File-Sharing Protocols

Shares can be accessed over a network. Network access to data stored on your ReadyNAS system is managed by file-sharing protocols, which handle the transfer of data. You can access a share on your ReadyNAS from other network-attached devices (for example, a laptop or a tablet) if the share is enabled for a file-sharing protocol that the network-attached device supports. You can enable a share to support more than one fire-sharing protocol.

Table 2 lists the file-sharing protocols that your ReadyNAS storage system supports.

Table 2. Supported file-sharing protocols

Protocol	Description	Recommendation
CIFS (Common Internet File Service)	Used mainly by Microsoft Windows computers and sometimes by Mac OS X computers, this protocol is enabled by default. It is sometimes referred to as the SMB (Server Message Block) file-sharing protocol.	If Windows users will access your storage system, enable this protocol.
NFS (Network File Service)	Used by Linux and Unix computers. Your ReadyNAS system supports NFS v3 over UDP and TCP.	If Linux or Unix users will access your storage system, enable this protocol.
AFP (Apple File Protocol)	Used by Mac OS 9 and Mac OS X computers. Your ReadyNAS system supports AFP 3.2.	If only Mac OS 9 and OS X users will access this your storage system, enable this protocol. However, in a mixed Windows and Mac environment, NETGEAR recommends using CIFS only.
FTP (File Transfer Protocol) and FTPS (FTP with SSL encryption)	Used by many public file upload and download sites.	If users will access your storage system using FTP, enable this protocol.
HTTP (Hypertext Transfer Protocol and HTTPS (HTTP with SSL encryption)	Used on the world wide web.	If users will access your storage system from a device with a web browser, including a smart phone or tablet computer, enable this protocol.
Rsync	Fast file-transfer protocol that uses a delta-transfer algorithm that sends only the differences between the source file and the existing file.	If users will access your storage system from a device that supports Rsync, enable this protocol.

When users access a share, it appears in their computer like a hard disk, and users can interact with it like they interact with a hard disk, depending on the access rights that are granted to the share and protocol combination.

Access Rights

For each share you create, you can determine the access rights for each file-sharing protocol that you enable for that share. *Table 3* lists access rights and shows the icon FrontView uses for each access right.

Table 3. Access rights options

Access right	FrontView icon	Description
Disabled		No one can access this share using this protocol.
Read-only		Users can read files on this share using this protocol, but cannot edit or create files on this share using this protocol.
Read/write		Users can read, edit, and create files on this share using this protocol.
Read-only with exceptions		Unless otherwise specified, users can only read files on this share using this protocol. At least one of the following exceptions exists: • Access to this share using this protocol is read-only and allowed only for specified hosts. • Access to this share using this protocol is read-only except for one or more users or groups that are granted read/write permission. • Access to this share using this protocol is disabled except for one or more users or groups that are granted read-only privilege.
Read/write with exceptions		Unless otherwise specified, users can read, edit, and create files on this share using this protocol. At least one of the following exceptions exists: • Access to this share using this protocol is read-only and allowed only for specified hosts. • Access to this share using this protocol is read-only except for one or more users or groups that are granted read/write permission. • Access to this share using this protocol is disabled except for one or more users or groups that are granted read-only privilege.

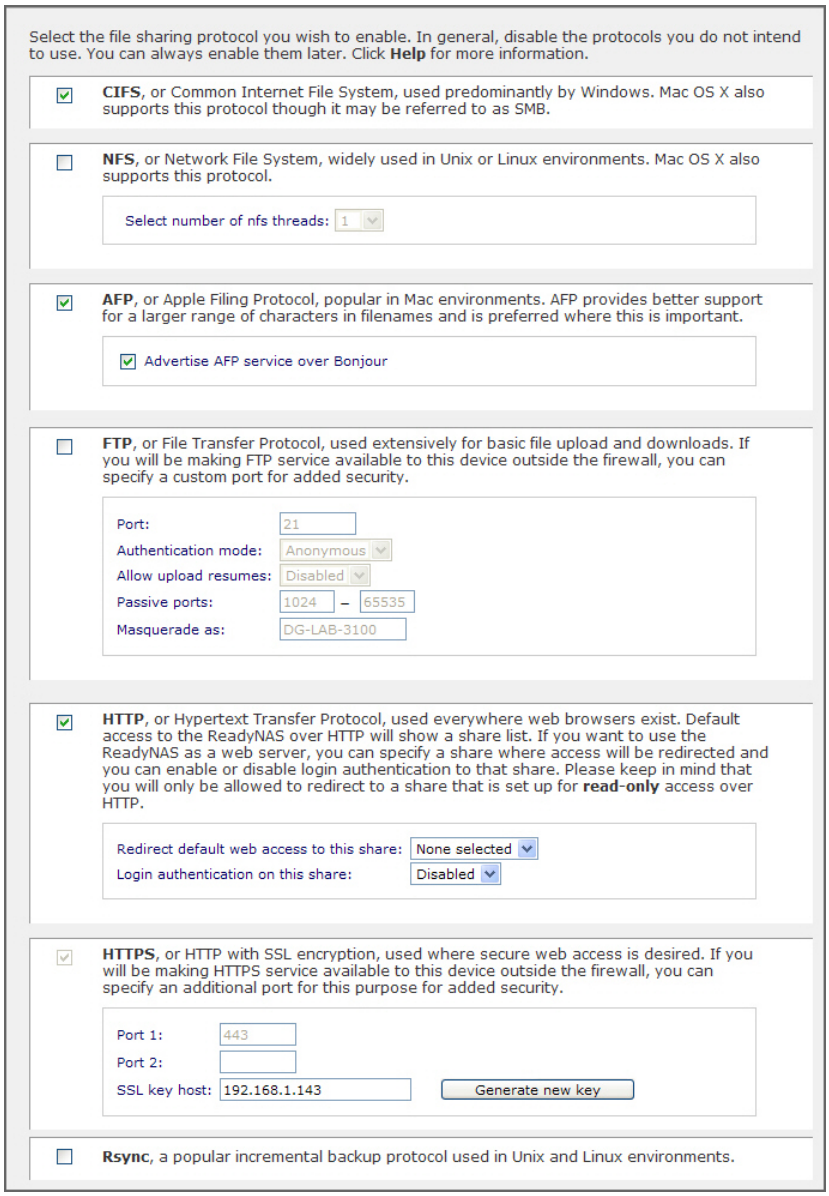
Manage File-Sharing Protocols

You can use FrontView to enable file-sharing protocols for your entire ReadyNAS system. For best performance, enable only those file-sharing protocols that you use. For example, if you do not use Linux or Unix computers to transfer files to and from your ReadyNAS system, disable the NFS file-sharing protocol. Disabling file-sharing protocols that you do not use maximizes system memory and improves system performance.

➢ **To manage file-sharing protocols:**

1. Select **Services > Standard File Protocols** from the FrontView main menu.

   The Standard File Protocols screen displays.



2. Select check boxes for any file-sharing protocols that you want to enable.

   If you are enabling the FTP file-sharing protocol, note the following:

   - **Port**. Defines the TCP/IP port that the FTP service uses.The default port is 21. This port must be forwarded through the router. See the port forwarding instructions provided with your router.
   - **Authentication mode**. Select **User** to require anyone trying to access your system using FTP to have a user account. Select **Anonymous** to waive this requirement.
   - **Allow upload resumes**. Allows users to finish uploading a file to the FTP share if the connection is interrupted. If this option is disabled, if the connection is dropped before the file is completely transferred, the file upload must start over from the beginning.
   - **Passive port range**. Required to enable remote access to your ReadyNAS system over the Internet. Adjust the port range 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 consumes a passive port.
   - **Masquerade as**. Adjusts the hostname that the FTP server reports to an FTP client.

   If you are enabling access HTTP file-sharing protocol, note the following:

   - **Redirect default Web access to this share**. Select a share from this drop-down list if you want to automatically redirect http://<ReadyNAS_IP_address> to that 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 and enable the HTTP protocol for read-only access to that share.
   - **Login authentication on this share**. Specifies whether or not authentication is required if users are browsing to the user-created web content on this share.

   If you are enabling the HTTPS file-sharing protocol, note the following:

   - HTTPS cannot be disabled; FrontView requires it.
   - Field details:
     - **Port 1**. Cannot be modified; it is reserved for your ReadyNAS system.
     - **Port 2**. Modify to allow HTTPS connections over a port other than the standard 443. Changing the default HTTPS port requires enabling port forwarding of the port you choose on the router. See the port forwarding instructions provided with your router.
     - **SSL key host.** Configures the hostname used for your ReadyNAS system 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 your ReadyNAS system 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 your ReadyNAS system 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.

- If you are enabling the Rsync file-sharing protocol, you can require a user name and password from anyone trying to access a share using the Rsync file-sharing protocol. These requirements are established at the share level. For more information, see *step 4* in the *Fine-Tuning Share Access* procedure.

3. Clear check boxes for any file-sharing protocols that you want to disable.
4. Click the **Apply** button.

   Your changes are saved.

Create Shares

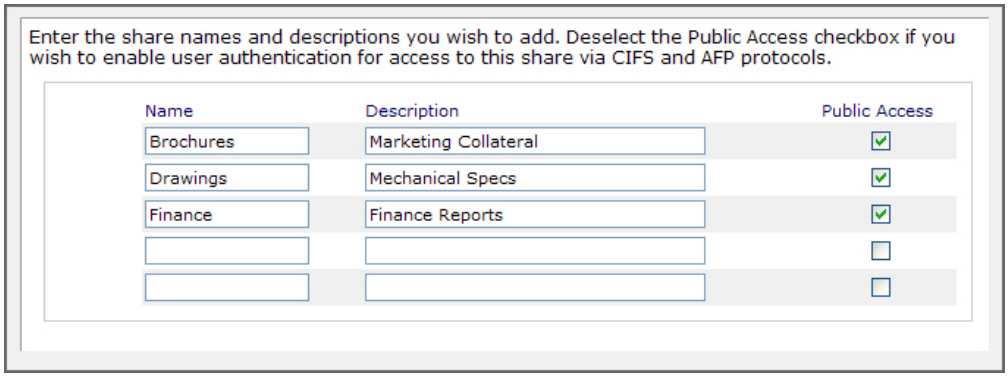
By default, new shares have the CIFS protocol enabled with read/write permissions.

➢ **To create a share:**

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

   If you have more than one volume configured on your ReadyNAS system, FrontView prompts you to select the volume where you want to create the share.

   The Add Shares screen displays.



2. Enter a share name and an optional description for each share you want to create.
3. Select or clear the **Public Access** check box for each share.

   Enabling public access means that anyone on your local area network with or without a user account on the ReadyNAS can access the share.

4. Click the **Apply** button.

   The share or shares are created.

Manage Shares

You can adjust file-sharing protocols and settings on shares. The options that are available vary by file-sharing protocol.

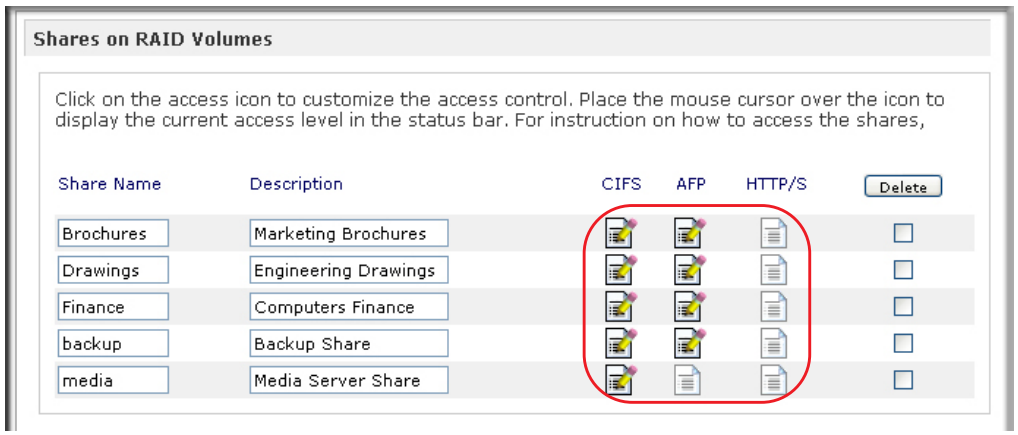
View Shares

Use FrontView to view shares that exist on your ReadyNAS system.

➢ **To view shares:**

Select **Share > Share Listing** from the FrontView main menu.

The Shares on RAID Volumes screen displays.



Note the icons in the protocol columns to the right of each share description. These icons indicate the access rights for each protocol for that share. For more information about these icons, see *Access Rights* on page 34.

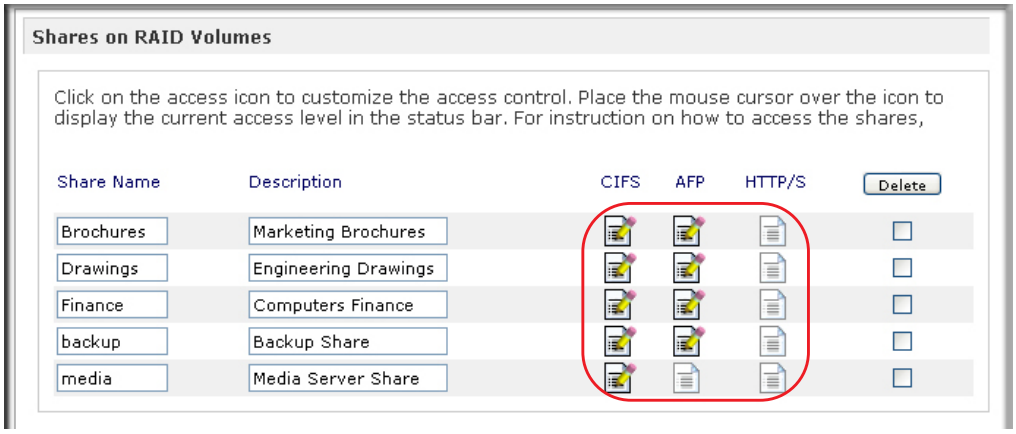
Fine-Tuning Share Access

Use FrontView to fine-tune how shares can be accessed. You can set protocols and privileges for each share. For example, you might want to enable the FTP file-sharing protocol for one share but disable it for another.

➢ **To fine-tune share access:**

1. Select **Share > Share Listing** from the FrontView main menu.

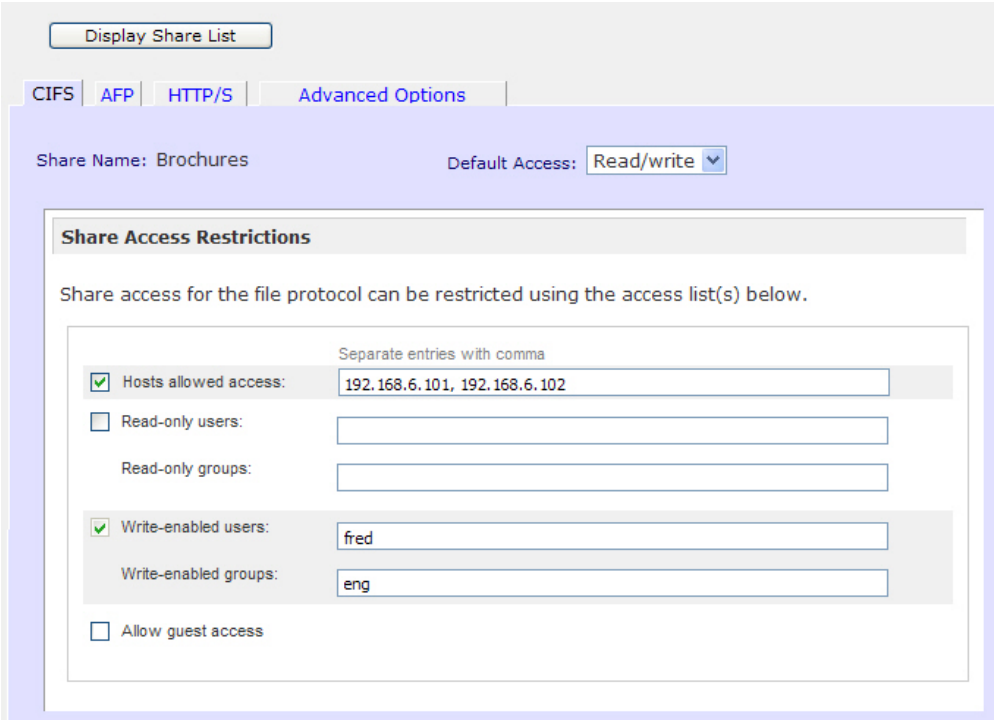
   The Shares on RAID Volumes screen displays.



   Note the icons in the protocol columns to the right of each share description. These icons indicate the access rights for each protocol for that share. For more information about these icons, see *Access Rights* on page 34.

2. Click an access rights icon in the row for the share whose access you want to adjust.

   The Share Access Restrictions screen for that share displays.



3. Click the tab for the protocol for which you want to adjust settings on this share.

4. (Optional) Enter any access restrictions that you want to enforce.

   This example shows share access restrictions for the CIFS and Rsync file-sharing protocols. Share access restriction options vary by protocol.

   - CIFS options:
     - **Hosts Allowed Access**. Select this check box and enter the IP addresses of any hosts allowed to access this share using this protocol.

       If you do not select this check box and enter at least one IP address, no hosts are barred from accessing this share using this protocol.

     - **Read-only users**. Select this check box and enter the names of any users that are allowed read-only access this share using this protocol.

       If you do not select this check box and enter at least one user name, no users are barred from read-only access to this share using this protocol.

     - **Read-only groups**. Select this check box and enter the names of any groups that are allowed read-only access this share using this protocol.

       If you do not select this check box and enter at least one group name, no groups are barred from read-only access to this share using this protocol.

     - **Write-enabled users**. Select this check box and enter the names of any users who are allowed write-enabled access to this share using this protocol.

       If you do not select this check box and enter at least group name, no groups are barred from write-enabled access to this share using this protocol.

     - **Write-enabled group**. Select this check box and enter the names of any groups who are allowed write-enabled access to this share using this protocol.

       If you do not select this check box and enter at least group name, no groups are barred from write-enabled access to this share using this protocol.

     - **Allow guest access**. Select this check box to allow people who do not have user accounts to access your system.
   - Rsync options:
     - **Hosts Allowed Access**. Select this check box and enter the IP addresses of any hosts allowed to access this share using this protocol.

       If you do not select this check box and enter at least one IP address, no hosts are barred from accessing this share using this protocol.

     - **Enable Password Protect**. Select this check box and create at least one Rsync user account and password. You can create a maximum of two Rsync user accounts and passwords for each share. These credentials are completely separate from your ReadyNAS storage system’s user accounts.

If you do not select this check box and enter at least one Rsync user account and password, no credentials are required to access this share using Rsync.

If you enable both host and password restrictions, only users accessing from listed hosts and using listed credentials can access this share using Rsync.

5. Click the **Apply** button.

   Your changes are saved.

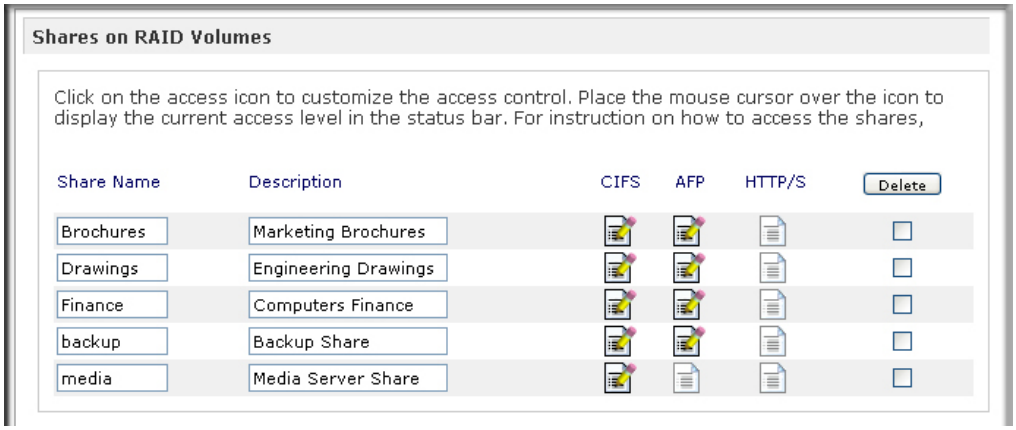
Enable WebDAV Support

WebDAV is short for web-based distributed authoring and versioning. It is an HTTP extension that allows drag-and-drop file transfers similar to what you experience with a standard Windows or Mac OS X computer.

➢ **To enable WebDAV support:**

1. Select **Share > Share Listing** from the FrontView main menu.

   The Shares on RAID Volumes screen displays.



2. Click an access rights icon for the share on which you want to enable WebDAV support.
3. The Share Access Restrictions screen displays.
4. Click the **HTTP/S** tab.

5. Choose **Read-only** or **Read/write** from the **Default Access** drop-down list.
6. Click the **Enable WebDAV support** check box.
7. Click the **Apply** button.

   WebDAV support is enabled.

Delete a Share

Use FrontView to delete a share.

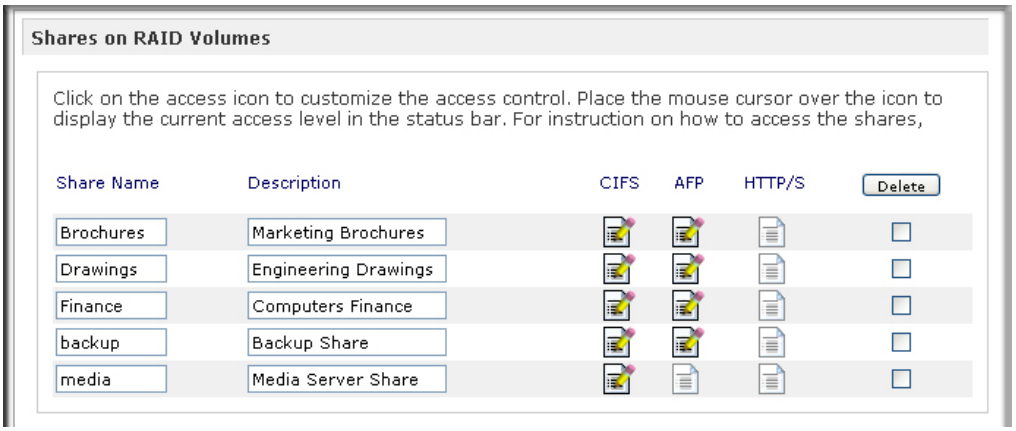
WARNING!

Deleting a share also deletes all of the data within that share.

➢ **To delete a share:**

1. Choose **Share > Share Listing** from the FrontView main menu.

   The Shares on RAID Volumes screen displays.



2. In the row of the share that you want to delete, select the **Delete** column check box.
3. Click the **Delete** button.

   You are prompted to confirm the delete command.
4. Click the **OK** button.

   The share and all of its contents are deleted.

Hide a Share

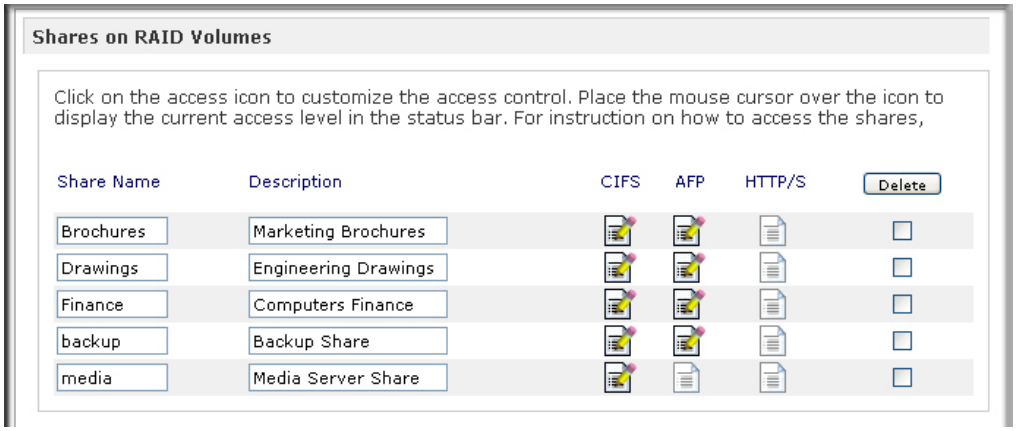
The CIFS protocol allows you to hide a share from users. This means that anyone using CIFS to browse the volume hosting the hidden share cannot see it in listings. Instead, users must enter the hidden share's full path name to see it.

The system administrator can see hidden shares no matter how he or she accesses the ReadyNAS system. If you hide a share, all other protocols for that share are disabled.

➢ **To hide a share:**

1. Select **Share > Share Listing** from the FrontView main menu.

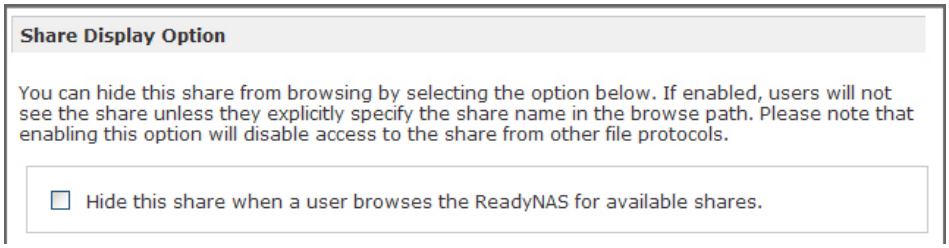
   The Shares on RAID Volumes screen displays.



2. In the row for the share that you want to hide, click the CIFS access rights icon.

   The Share Access Restrictions screen for that share and protocol combination displays.

3. Scroll down to the Share Display Option pane.



4. Select the **Hide this share when a user browses the ReadyNAS for available shares** check box.
5. Click the **Apply** button.

   The share is hidden and all protocols except CIFS are disabled for this share.

Enable the Recycle Bin

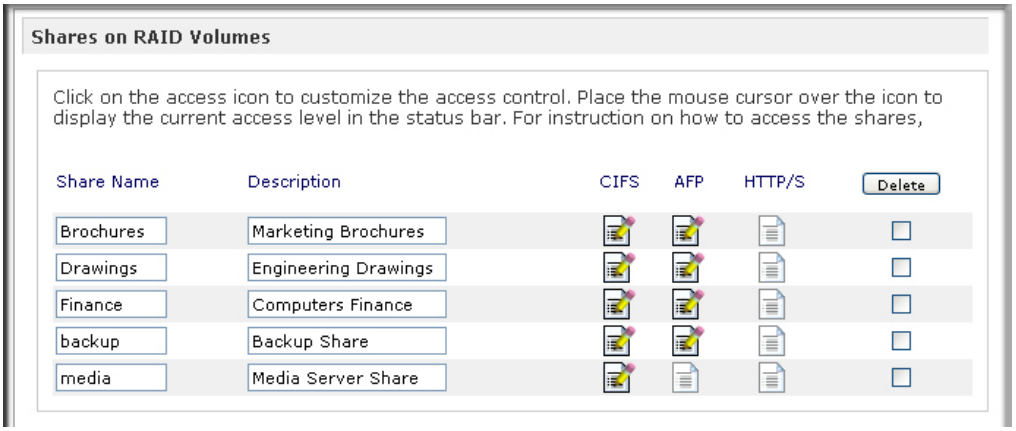
The CIFS protocol offers a Recycle Bin. This allows for a grace period during which users can retrieve deleted files from the Recycle Bin.

When the Recycling Bin is enabled, deleted files are placed in the Recycle Bin for a period of time before being permanently deleted when the share is accessed using CIFS. Files deleted when accessed using other protocols are deleted immediately.

➢ **To enable the Recycle Bin:**

1. Choose **Share > Share Listing** from the FrontView main menu.

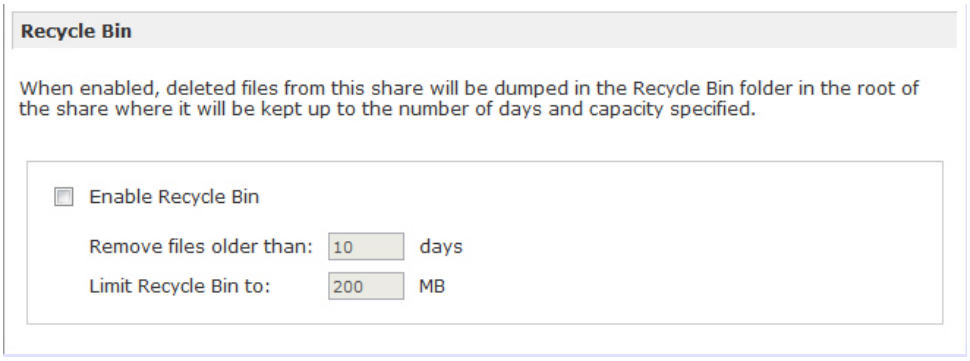
   The Shares on RAID Volumes screen displays.



2. In the row for the share for which you want to enable the Recycle Bin, click the CIFS access rights icon.

   The Share Access Restrictions screen for that share and protocol combination displays.

3. Scroll down to the Recycle Bin pane.



4. Select the **Enable Recycle Bin** check box.
5. Enter the maximum number of days to keep files in the **Remove files older than** field.

   Files that are older than the value you specify here are permanently deleted.

6. Enter a size limit (in megabytes) for the Recycle Bin in the **Limit Recycle Bin to** field.

   When the Recycle Bin exceeds this limit, files are deleted, beginning with the oldest first, until the Recycle Bin no longer exceeds this limit.

7. Click the **Apply** button.

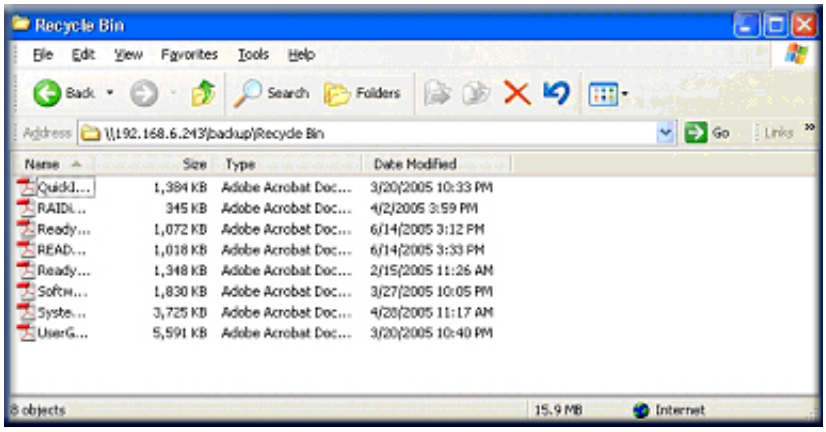
   FrontView creates a Recycle Bin folder in this share.

Retrieve Files from the Recycle Bin

When you enable the Recycle Bin on a share, FrontView creates a Recycle Bin folder in that share.

➢ **To retrieve files from recycle bin:**

1. On a computer that is attached to the same LAN as your ReadyNAS system, browse to the share containing the Recycle Bin.



2. Drag the file out of the Recycle Bin folder and drop it into a different folder.

Manage Advanced Permissions

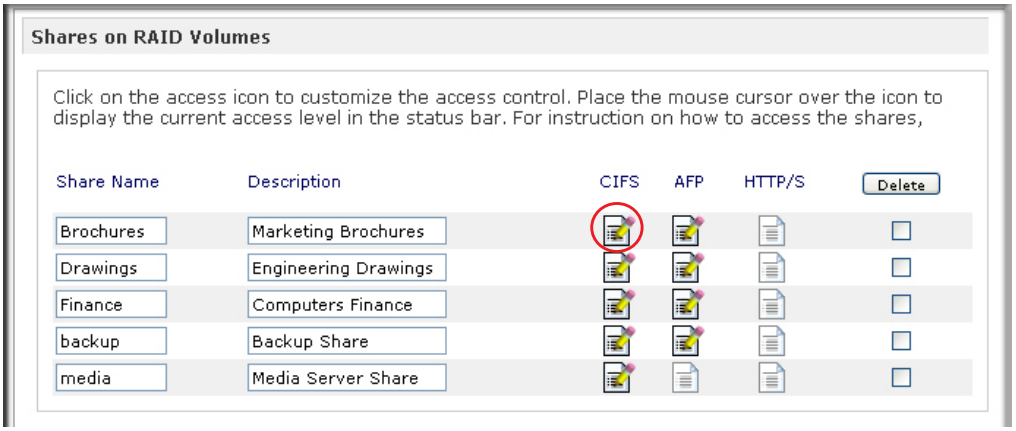
Advanced Permission settings vary by file-sharing protocol. When a new file or folder is created, these settings determine which groups and users can access that file or folder.

You can change these settings to match your security requirements.

➢ **To manage default share permissions:**

1. Select **Share > Share Listing** from the FrontView main menu.

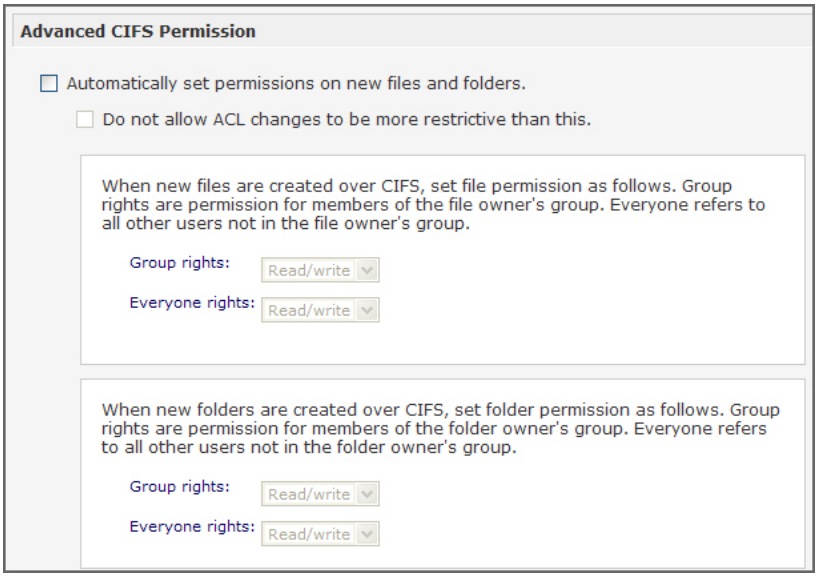
   The Shares on RAID Volumes screen displays.



2. Click the access rights icon in protocol column for the share and protocol combination whose default share permissions you want to adjust.

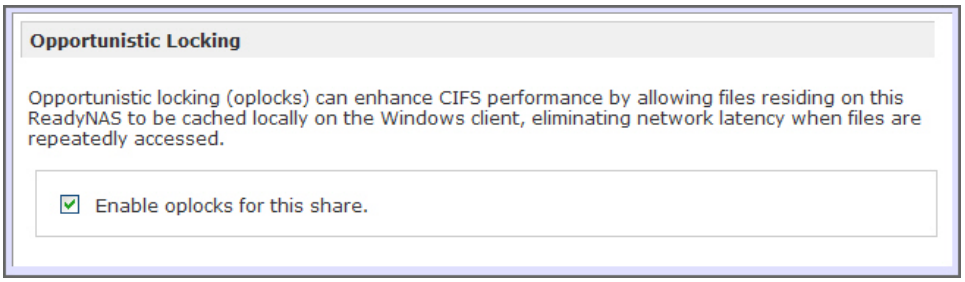
   The Share Access Restrictions screen for that share and protocol combination displays.

3. Scroll down to the Advanced Permission pane.



   These settings vary by protocol. This example describes the Advanced Permission options for the CIFS file-sharing protocols.

4. Adjust the settings as needed.
   - **Automatically set permissions on new files and folders**. Select this check box to activate the settings in the next panes. Clear this check box to dim the settings in those panes.
   - **Do not allow ACL changes to be more restrictive than this**. ACL is short for access control lists, which are a feature of the CIFS file-sharing protocol. Select this check box to override any ACL settings. Clear this check box to allow users to set more restrictive permissions.
   - **Groups rights** and **Everyone rights** for new files. These drop-down lists are dimmed unless you select the Automatically set permissions on new files and folders check box. You can choose to set permissions as read/write, read-only, or disabled.
   - **Groups rights** and **Everyone rights** for new folders. These drop-down lists are dimmed unless you select the Automatically set permissions on new files and folders check box. You can choose to set permissions as read/write, read-only, or disabled.
   - **Enable oplocks for this share.** Select this check box to enable opportunistic locking.



   Opportunistic locking, often referred to as oplock, is available only on the CIFS protocol. Opportunistic locking improves CIFS performance by allowing files on your ReadyNAS system to be temporarily stored (cached) locally on the Windows-based computer with the file or files opened, thus eliminating network latency when the files are constantly accessed.

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

5. Click the **Apply** button.

   Your changes are saved.

Manage File-Level Access

You can use FrontView to manage file-level access. NETGEAR recommends that only advanced users with detailed knowledge about how these options work change these settings.

WARNING!

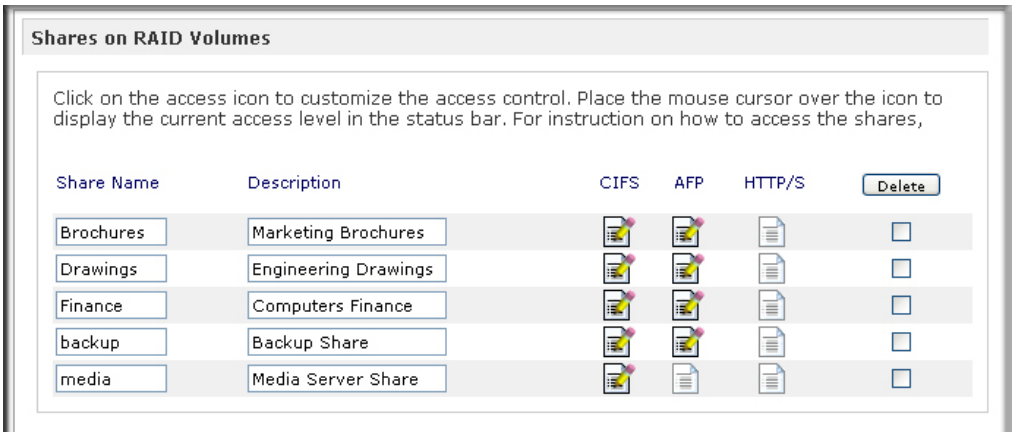
Changes that you make to file-level access can affect ownership and permissions and can be difficult to reverse.

If you configure file-level access settings that conflict with share-level settings, your ReadyNAS system uses the file-level settings.

➢ **To manage file-level access:**

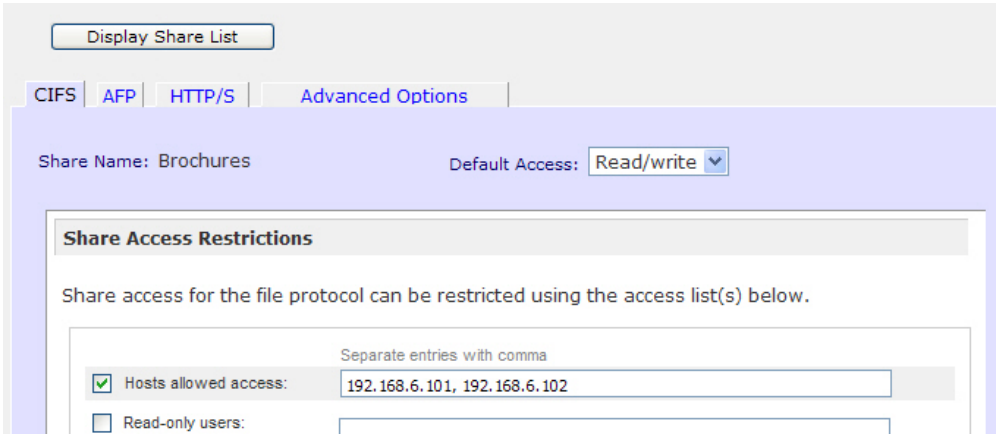
1. Select **Share > Share Listing** from the FrontView main menu.

   The Shares on RAID Volumes screen displays.

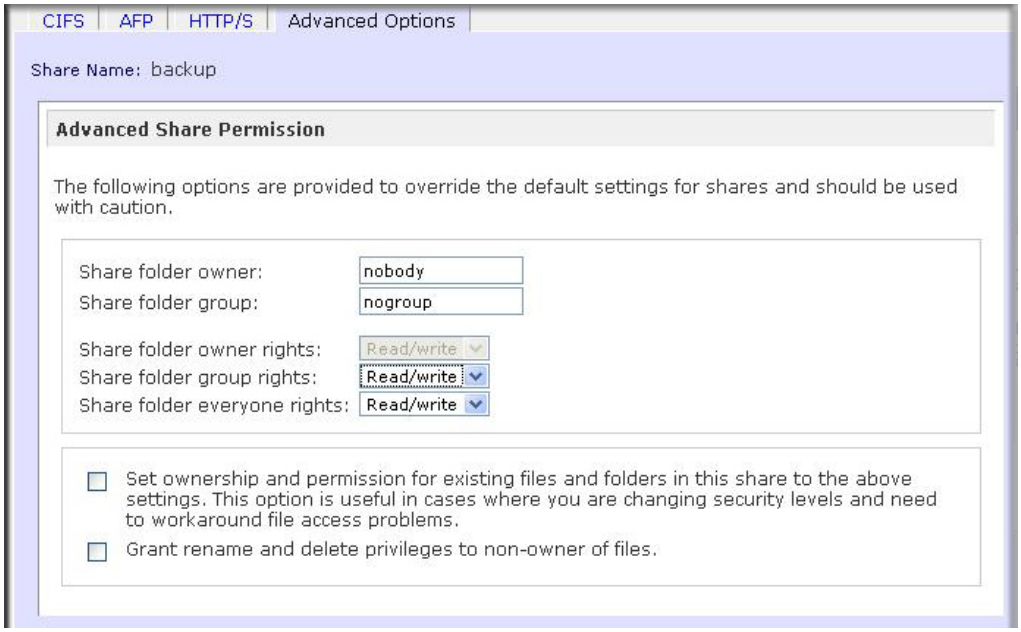


2. Click an access rights icon.

   The Share Access Restrictions screen for that share and protocol combination displays.



3. Click the **Advanced Options** tab.
4. (Optional) Adjust the Advance Share Permission settings.

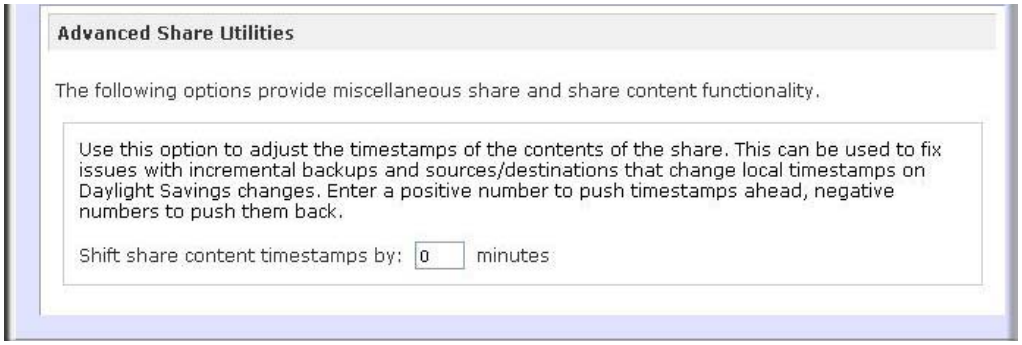


NETGEAR recommends not changing the Share folder owner, Share folder group, Share folder owner rights, Share folder group rights, or Share folder everyone rights settings. Changes that you make to these settings can affect ownership and permissions and can be difficult to reverse.

The **Set ownership and permission for existing files and folders** option performs a one-time change to your existing files and folders to reflect the settings in the pane above. Depending on the size of the share, this can take a while to finish.

The **Grant rename and delete privilege to non-owners** check box allows others to modify shares that they do not own. In a collaborative environment, you might want to enable this option. In a more security-conscious environment, disable this option.

5. (Optional) Scroll down to the **Advanced Share Utilities** pane and adjust the setting as needed.



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

6. Click the **Apply** button.

   Your changes are saved.

Access Shares Remotely

You can remotely access shares on your ReadyNAS system using other network-connected devices like a laptop or tablet.

To access a share, both the share and the network-connected device must support the same protocol. For example, Linux computers support the NFS file-sharing protocol, so users with those devices can access the shares on which you enable the NFS protocol.

Access Shares Using a Web Browser

You can use a web browser to access files that are stored on your ReadyNAS system.

Note: If you are accessing your files from a network that is outside of your LAN, you must configure port forwarding on your router. For more information, see your router user manual.

➢ **To access a share using a web browser:**

1. Ensure that the HTTP file-sharing protocol is enabled on your ReadyNAS system.

   For more information, see *Manage File-Sharing Protocols* on page 35.

2. Launch a web browser.
3. Navigate to the ReadyNAS system and share you want to access using the following syntax:

   http://<hostname>/shares

   <hostname> is the name that you assigned to your ReadyNAS system or the default hostname if you did not change it.

   For a secure, encrypted connection replace **http** with **https**.

   You are prompted to log in to your ReadyNAS system.

4. Enter a user ID and password.

   You can log in with administrator or user credentials. If you log in as a user, your access is limited by the settings configured by the ReadyNAS system administrator.

   Your shares are displayed in a web page.

Access Shares Using a Windows Device

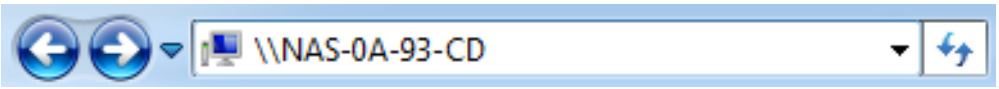
You can access shares on your ReadyNAS system using a network-attached Windows-based device.

➢ **To access a share using a network-attached Windows device:**

1. Ensure that the CIFS file-sharing protocol is enabled on your ReadyNAS system.

   For more information, see *Manage File-Sharing Protocols* on page 35.

2. Enter **\\<hostname>** in the Windows Explore My Computer address bar.



   <hostname> is the name that you assigned to your ReadyNAS system or the default hostname if you did not change it.

   You are prompted to log in to your ReadyNAS system.

3. Enter a user ID and password.

   You can log in with administrator or user credentials. If you log in as a user, your access is limited by the settings configured by the ReadyNAS system administrator.

   Windows Explorer displays the contents of all available shares on your ReadyNAS system.

Access Shares Using a Mac OS X Device

You can access shares on your ReadyNAS system using a network-attached OS X device.

➢ **To access a share using a network-attached OS X device:**

1. Ensure that the AFP or CIFS file-sharing protocol is enabled on your ReadyNAS system.

   For more information, see *Manage File-Sharing Protocols* on page 35.

2. In Finder, select **Go > Connect to Server**.

   The Connect to Server dialog box displays.

3. Connect to your ReadyNAS system as follows:
   - If you are using the AFP file-sharing protocol, enter the following command in the **Server Address** field:

     afp://<hostname>

   - If you are using the CIFS file-sharing protocol, enter the following command in the **Server Address** field**:**

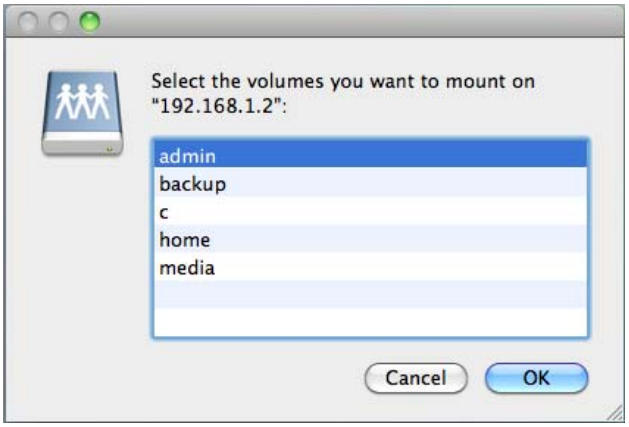
     smb://<hostname>

     In both cases, <hostname> is the name that you assigned to your ReadyNAS system or the default hostname if you did not change it.
4. Click the **Connect** button.

   You are prompted to log in to your ReadyNAS system.
5. Enter a user ID and password.

   You can log in with administrator or user credentials. If you log in as a user, your access is limited by the settings configured by the ReadyNAS system administrator.

   You are prompted to select a volume. Mac OS X calls your ReadyNAS shares *volumes*.



6. Select the volume or volumes (share or shares) you want to access and click the **OK** button.

   Finder displays the volume contents in a window.

Access Shares Using a Mac OS 9 Device

You can access shares on your ReadyNAS system using a network-attached OS 9 device.

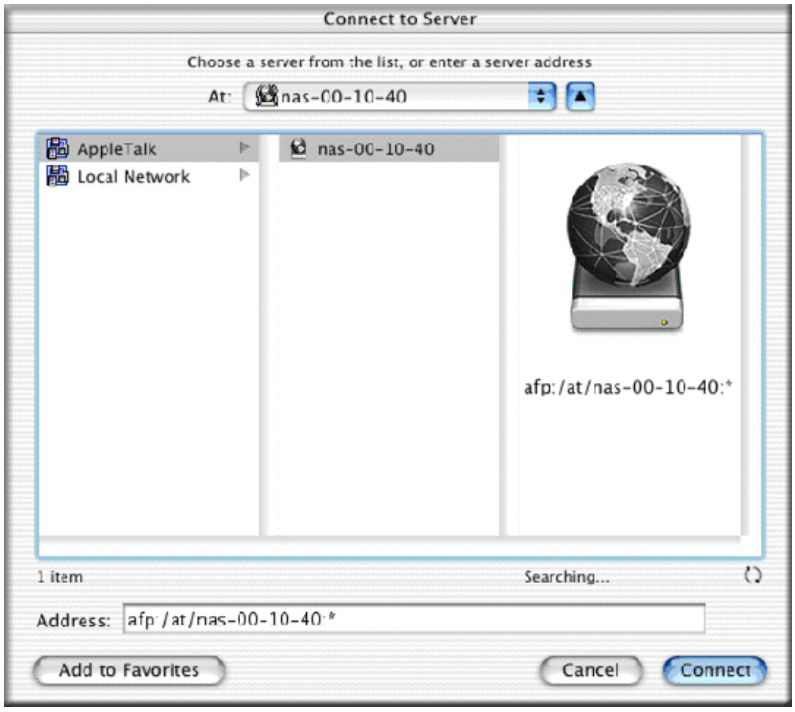
➢ **To access a share using a network-attached Mac OS 9 device:**

1. Ensure that the AFP file-sharing protocol is enabled on your ReadyNAS system.

   For more information, see *Manage File-Sharing Protocols* on page 35.

2. In Finder, choose **Go > Connect to Server**.

   The Connect to Server dialog box displays.



3. Select your ReadyNAS system and click the **Connect** button.

   You are prompted to log in to your ReadyNAS system.

4. Enter a user ID and password and click the **Connect** button.

   You can log in with administrator or user credentials. If you log in as a user, your access is limited by the settings configured by the ReadyNAS system administrator.

   You are prompted to select a volume. Mac OS 9 calls your ReadyNAS shares *volumes*.

5. Select a volume (share) and click the **OK** button.

   Finder displays the volume contents in a window.

Access Shares Using a Linux or Unix Device

You can access shares on your ReadyNAS system using a network-attached Linux or Unix device.

Note: Your ReadyNAS system does not support NIS because it is unable to correlate NIS information with CIFS user accounts. In mixed environments where you want CIFS and NFS integration, manually specify the user ID and group ID of the user and group accounts to match your NIS or other Linux or Unix server settings. Your ReadyNAS system can import a comma-delimited file containing the user and group information to coordinate Linux or Unix login settings. See *Create User Accounts in Batches* on page 65 for more information.

➢ **To access a share using a network-attached Linux or Unix device:**

1. Ensure that the NFS file-sharing protocol is enabled on your ReadyNAS system.

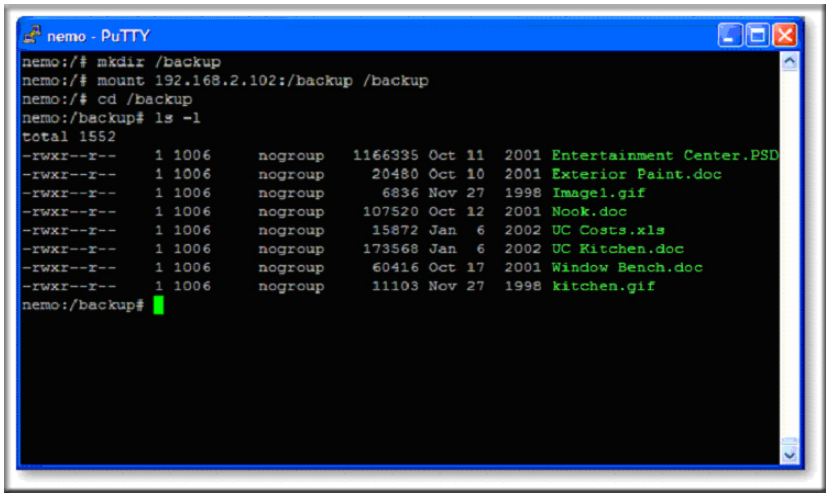
   For more information, see *Manage File-Sharing Protocols* on page 35.

2. Using a terminal program, enter the following command:

   `mount <ReadyNAS_IP_address>:/<share_name> <share_name>`

   Note the following:

   - <ReadyNAS_IP_address> is the IP address of your ReadyNAS system.
   - <share_name> is the name of the share you want to access.



   For example, if your ReadyNAS system's IP address is 192.168.2.102 and you want to mount the backup share, enter **`mount 192.168.2.102:/backup backup`** in your terminal program.

Access Shares Using FTP and FTPS

You can use FTP and FTPS to access any shares that are enabled for the FTP and FTPS file-sharing protocols.

For better security, use an FTPS client to connect to your ReadyNAS using the FTP file-sharing protocol. With FTPS, your password and data are encrypted.

If you are using FTPS, you must use explicit mode (also known as FTPES or AUTH TLS) in your FTP client.

➢ **To access a share using FTP:**

1. Ensure that the FTP file-sharing protocol is enabled on your ReadyNAS system.

   For more information, see *Manage File-Sharing Protocols* on page 35.

2. Launch an FTP client or a terminal program.
3. Log in to your ReadyNAS system, as follows:
   - If you required user FTP access when you enabled the FTP-file sharing protocol, log in using user or administrator credentials for your ReadyNAS system. If you log in as a user, your access is limited by the settings configured by the ReadyNAS system administrator.
   - If you allowed anonymous access when you enabled the FTP-file sharing protocol, log in as **anonymous** and use your email address for the password.

Access Shares Using Rsync

You can use Rsync to access any shares that are enabled for the Rsync file-sharing protocol. Instead of browsing shares as you do with some other file-sharing protocols, with Rsync, you copy files from your ReadyNAS system to another computer that supports the Rsync file-sharing protocol. If you previously copied these files, Rsync only copies the differences between the source files and the destination files, making the transfer much quicker than using other file-sharing protocols. The first time you copy files using the Rsync file-sharing protocol, you see no performance difference.

➢ **To access shares using Rsync:**

1. Ensure that the Rsync file-sharing protocol is enabled on your ReadyNAS storage system.

   For more information, see *Manage File-Sharing Protocols* on page 35.

2. On a network-attached device that supports the Rsync file-sharing protocol, launch a terminal program or an Rsync client.
3. Enter any required credentials for the share.

   For more information about Rsync share access credentials, see *Fine-Tuning Share Access* on page 38.

   For more information about Rsync terminal program commands, see *http://rsync.samba.org*.

   For more information about using an Rsync client application, see the documentation that accompanies the application.

Access Shares Using ReadyNAS Remote

ReadyNAS Remote is a web-based add-on service that allows you to drag and drop files between your ReadyNAS system and your PC or Mac using the CIFS file-sharing protocol. All file permissions and share security settings are retained as if you were on your LAN. All data is encrypted so that it is transmitted securely.

ReadyNAS Remote uses an add-on on your ReadyNAS system and a small software program for your Mac or PC.

For more information about installing and managing add-ons on your ReadyNAS system, see *Add-Ons* on page 97.

Enable ReadyNAS Remote

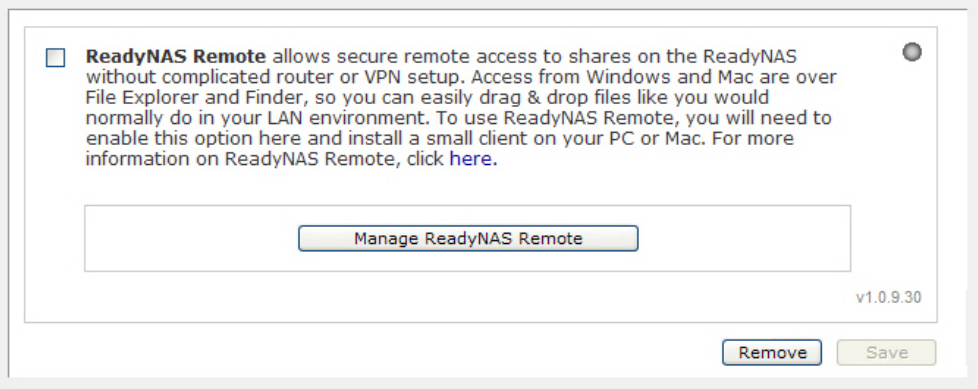
The ReadyNAS Remote add-on is preinstalled on your ReadyNAS storage system. Before you can access shares using ReadyNAS Remote add-on, you must enable the add-on your ReadyNAS system.

➢ **To enable ReadyNAS Remote:**

1. Select **Add-ons > Installed** from the FrontView main menu.

   A screen displays listing all add-ons currently installed on your ReadyNAS system.

2. Scroll down to the ReadyNAS Remote pane.



3. Select the **ReadyNAS Remote** check box and click the **Save** button.
4. Click the **Manage ReadyNAS Remote** button.

   The Remote Access window displays.

5. Use the interface to grant users permission to access your ReadyNAS system with ReadyNAS Remote add-on.
6. Click the **Apply Settings** button.
7. Click the **here** link in the ReadyNAS Remote description.

   An online tutorial about ReadyNAS Remote displays.

8. Scroll down to the links for the ReadyNAS Remote client software versions.
9. Click the link for the appropriate version for your Mac or PC.
10. Follow the prompts to download the ReadyNAS Remote client software to your computer.

Install ReadyNAS Remote Client Software

Before you can access shares using ReadyNAS Remote, you must install the ReadyNAS Remote client software on your Mac or PC.

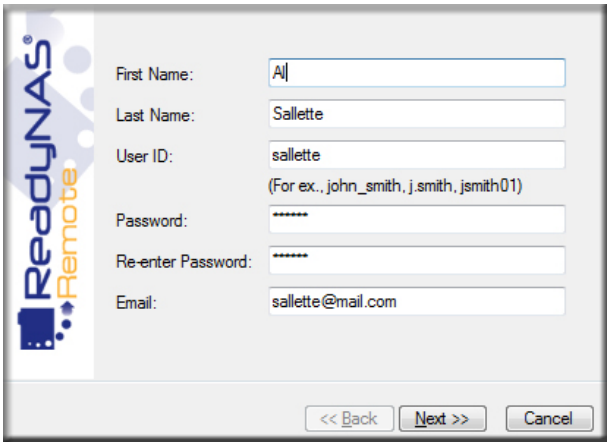
➢ **To install the ReadyNAS Remote client software on your computer:**

1. Install the ReadyNAS Remote client software.

   A wizard guides you through the installation process.

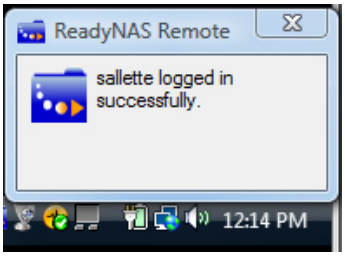
   When you complete the installation, you are prompted to create a ReadyNAS Remote account.

2. Follow the wizard's prompts to create a free ReadyNAS Remote account.



Remember your the user ID and password you create; you need these credentials to access shares.

A pop-up window displays when you successfully register with the ReadyNAS Remote web service.



Access Shares

You can use ReadyNAS Remote to drag and drop files between your computer and your ReadyNAS system, even when your computer is not on the same LAN as your ReadyNAS system.

➢ **To access shares using ReadyNAS Remote:**

1. Ensure that the CIFS file-sharing protocol is enabled on your ReadyNAS system.

   For more information, see *Manage File-Sharing Protocols* on page 35.

2. Launch the ReadyNAS Remote client software on your PC or Mac.
3. Log in to your ReadyNAS Remote account.
4. Connect to your ReadyNAS system.
5. Your shares open in a File Explorer (PC) or Finder (Mac) window.

   You can now drag and drop files between your PC or Mac and your ReadyNAS system as though you were on the ReadyNAS LAN.

Users and Groups

4

This chapter describes how to create and manage user and group accounts. It contains the following sections:

- *Basic User and Group Concepts*
- *User Accounts*
- *Groups*

Basic User and Group Concepts

Users are the people to whom you grant access to your storage system. When you want to allow someone to access your ReadyNAS system, you create a user account for that person. The ReadyNAS storage system administrator sets up user accounts and decides which shares each user is permitted to access.

If your ReadyNAS storage system is being used at home, you might decide that each member of the family should have a user account, but that only the parents can access financial data stored on your system. You might decide that all accounts can access photos and music stored on the system. You can set the appropriate permissions for each user.

The ReadyNAS system administrator can set up groups to make it easier to manage large numbers of users. For example, if your ReadyNAS storage system is being used in a business, you might decide that every employee should have a user account. However, you might decide that only users in the accounting department can access information in the accounting share, but that all users can access data stored in the company benefits share. You can create a group for each department and place all users in the appropriate group or groups.

User Accounts

Use FrontView to create, manage, and delete user accounts on your ReadyNAS storage system.

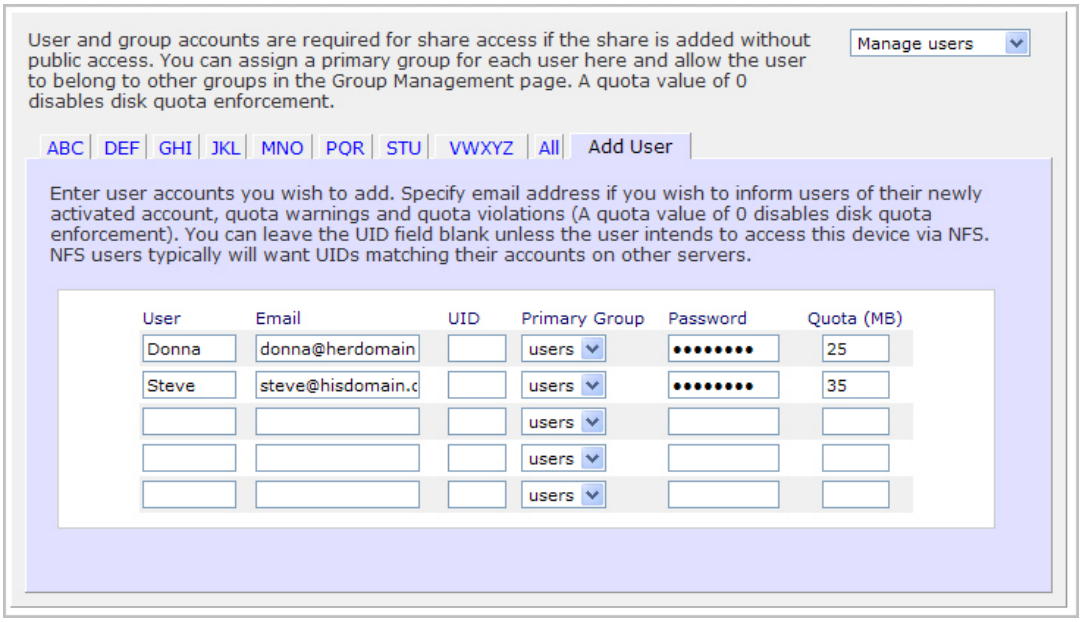
Set Default User Account Parameters

Use FrontView to set default parameters for new user accounts.

➢ **To set default account preferences:**

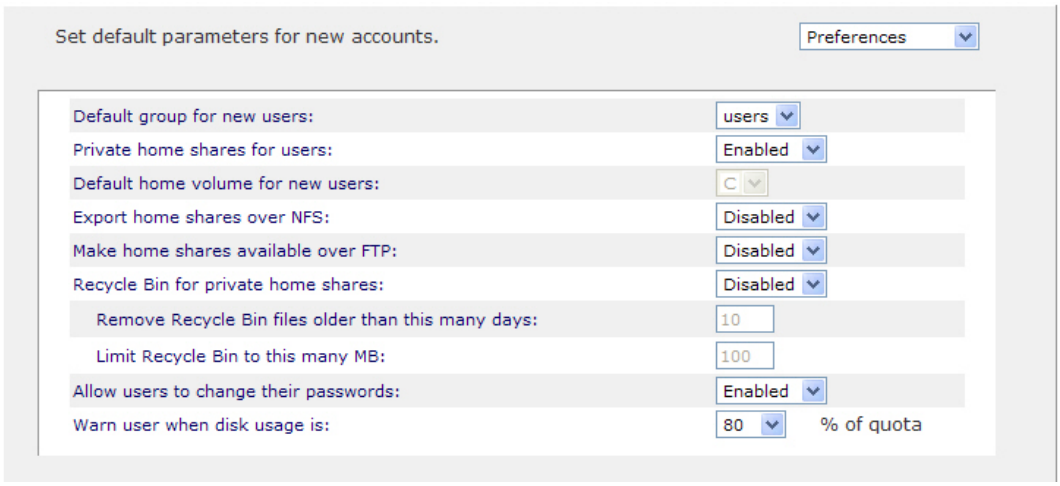
1. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



2. From the drop-down list in the upper-right corner, select **Preferences**.

   The Default User Account Parameters screen displays.



3. Use the drop-down lists and fields to set default parameters for new users.

   Note the following:

   - **Default group for new users**. Determines into which group new user accounts are placed when created. If you have not created any groups, all users are placed in the users group.
   - **Private home shares for users**. Enabling private home shares creates a share for each new user account. This share is visible only to that user and the system administrator. The share is created the first time a user logs in to the ReadyNAS system. Disable private home shares to prevent home shares from being created for each user account.
   - **Default home volume for new users**. This setting determines to which volume new users are assigned. If you are using X-RAID2 mode, this option is disabled, because X-RAID2 has only one volume. If you are using Flex-RAID and you have only one volume, this option is disabled.
   - **Make home shares available over FTP**. Enable this option to allow home shares to be accessed using the FTP file-sharing protocol. Disable this option to prevent home shares from being access using the FTP file-sharing protocol.
   - **Recycle Bin for private home shares**. This applies only to shares that are accessed using the CIFS file-sharing protocol. If you enable this, you can also determine how long files are held in the Recycle Bin before they are permanently deleted and how large the Recycle Bin can grow.
   - **Allow users to change their passwords**. If you enable this feature, users can change their own passwords. If you disable it, the ReadyNAS system administrator must change user passwords. For more information, see *Change User Passwords* on page 69.
   - **Warn user when disk usage is**. Select a percentage from the drop-down list. When a user's files reach this percentage of quota, an email alert is sent to the user, if you provided an email address for that user and established a quota for that user.

4. Click the **Apply** button.

   Your settings are saved.

Create User Accounts

You can create user accounts manually or in large batches.

Manually Create User Accounts

You can manually create up to five user accounts at one time.

To create more than five user accounts at one time, you can import a comma-separated-value (CSV) file. For more information, see *Create User Accounts in Batches* on page 65.

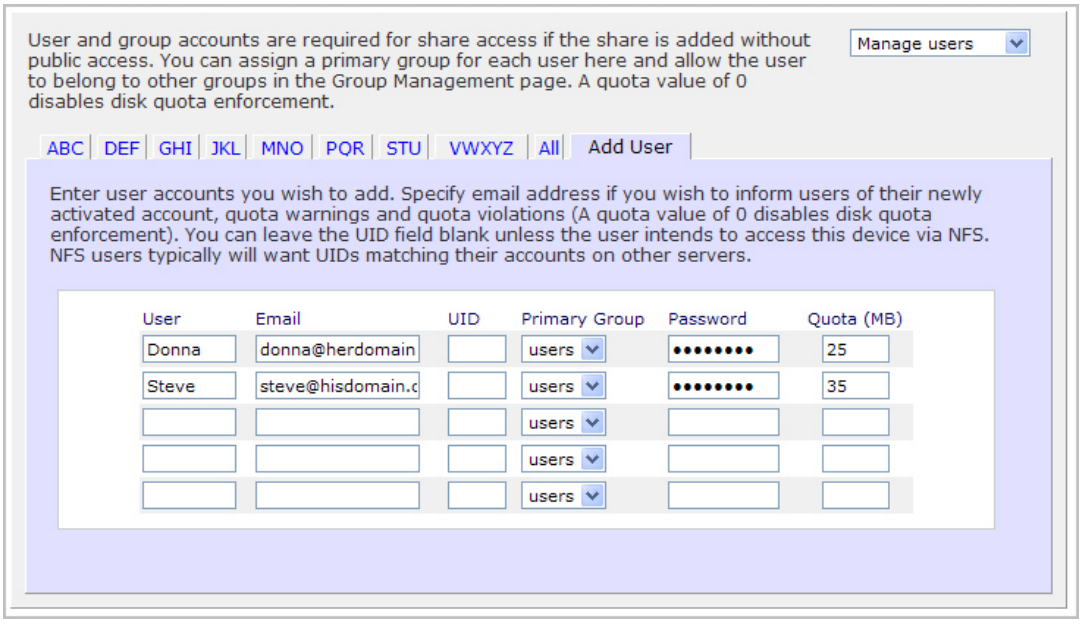
➢ **To manually create a user account:**

1. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.

2. Click the **Add User** tab.

   The User screen displays.



3. For each user you want to create, enter the following information:
   - **User name**. Required. The name you choose must be unique among all users and shares. For example, if you have a share named Eunice, you cannot have a user named Eunice.
   - **Email address**. Optional. NETGEAR recommends providing an email address if you enforce quotas for this user. Without an email address, the user is not warned when disk usage approaches the quota.
   - **User ID**. Optional. If you do not create a user ID, your ReadyNAS system assigns one.
   - **Group association**. Optional.
   - **Password**. Required.
   - **Disk quota**. Optional. If you do not enter a quota, your ReadyNAS system places no limits on the amount of space this user can consume.
4. Click the **Apply** button.

   The user or users are added to your ReadyNAS system.

Create User Accounts in Batches

You can create many user accounts at one time by uploading a comma-separated-value (CSV) file to your ReadyNAS system. The file must use the following format:

```
name1,password1,group1,email1,uid1,quota1

name2,password2,group2,email2,uid2,quota2

name3,password3,group3,email3,uid3,quota3
```

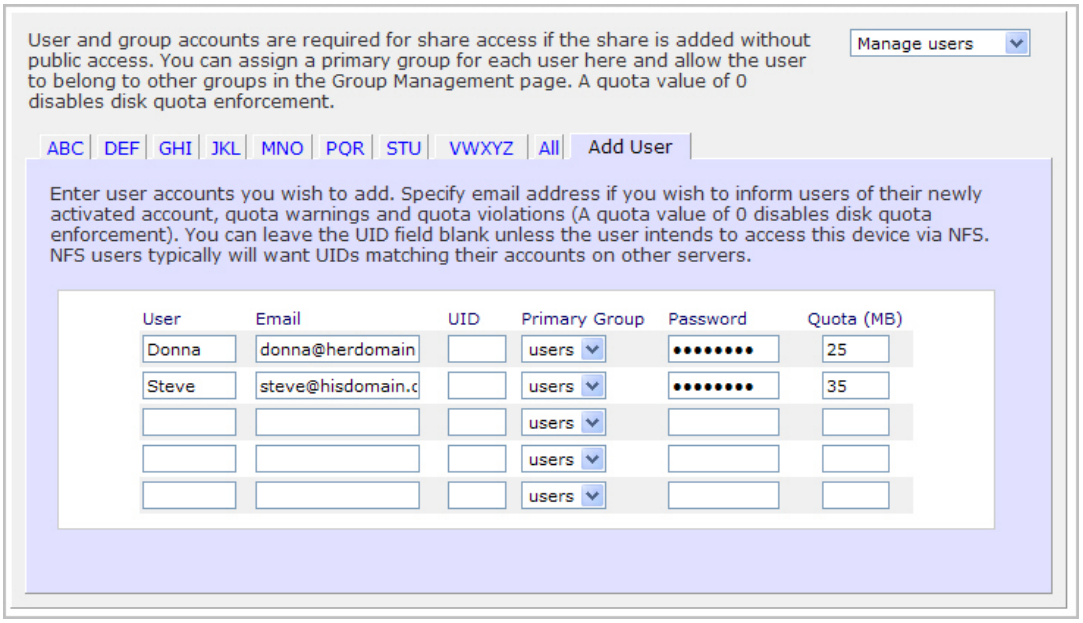
Note the following:

- Spaces around commas are ignored.
- The name and password fields are required.
- If a listed group account does not exist, it is automatically created.
- 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.

➢ **To create many user accounts at one time:**

1. On your computer, create a CSV file listing users you want to create.
2. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



3. From the drop-down list in the upper-right corner, select **Import User List**.

   You are prompted to browse for your user file.
4. Click the **Browse** button.

   A dialog box opens.
5. Navigate to the file and click the **Open** button.

   The users are added to your ReadyNAS system.

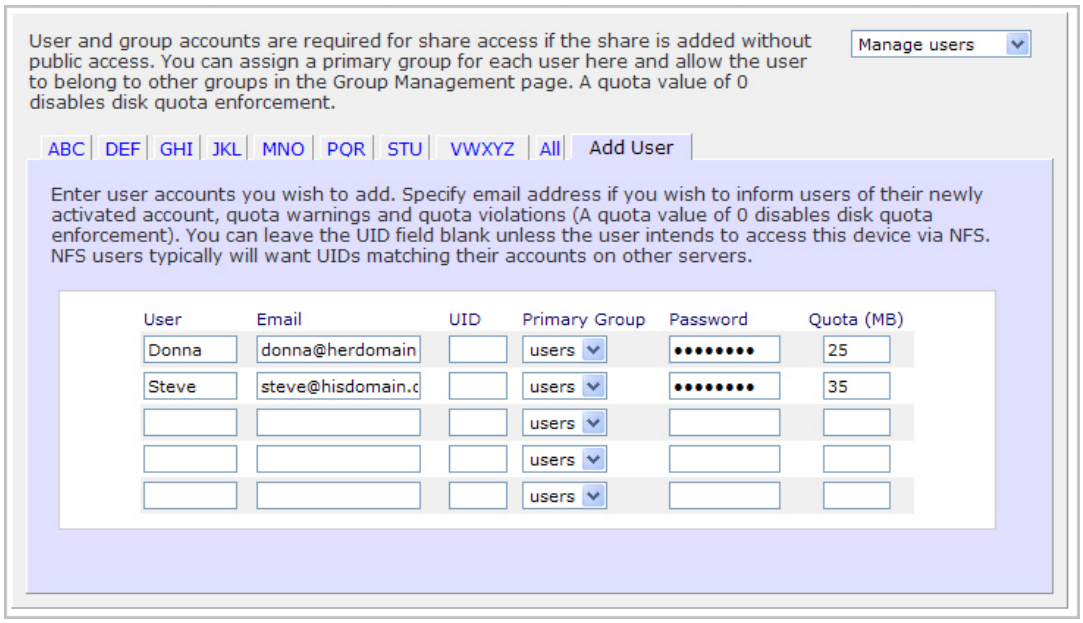
Edit User Accounts

Use FrontView to edit a user's name, email address, primary group assignment, password, or quota.

➢ **To edit a user's settings:**

1. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



   If your system has only a few users, they all display on the screen.

   If your system has many users, click the appropriate tab to find the user whose settings you want to edit.

2. Edit the settings for the user as needed.
3. Click the **Apply** button.

   Your changes are saved.

Delete User Accounts

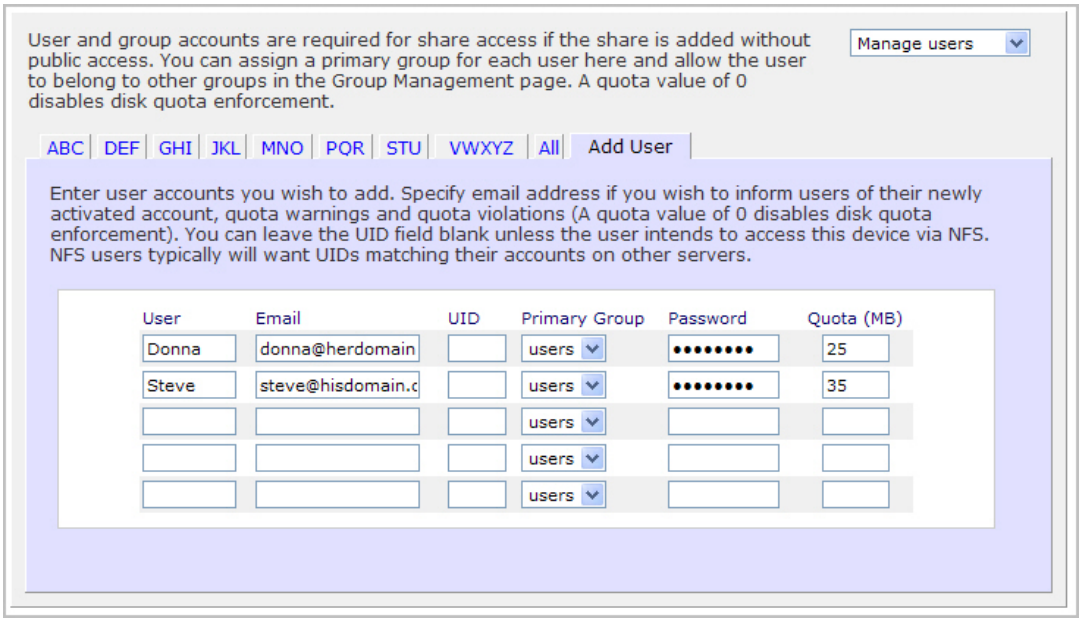
When you delete a user, the home share assigned to that user is deleted. Any files that user owns that are in other shares remain but do not have an owner assigned, which can be fixed in one of two ways:

- Edit the advanced share permissions in FrontView. For more information, see *Manage File-Level Access* on page 48.
- Manually configure file permissions from their computer. For more information, see the documentation that accompanied your operating system.

➢ **To delete a user:**

1. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



   If your system has only a few users, they all appear on the screen.

   If your system has many users, click the appropriate tab to find the user that you want to delete.

2. Select the **Delete** check box in the row for the user that you want to delete.

   The Delete button becomes active.

3. Click the **Delete** button.

   The user is deleted.

Change User Passwords

A user password can be changed by the user to whom the account is assigned, if you enabled that feature, or it can be changed by the ReadyNAS system administrator. For security reasons, NETGEAR recommends that users change their passwords on a regular basis.

User Password Change by User

This procedure assumes that you enabled users to change their own passwords. For more information, see *Set Default User Account Parameters* on page 61.

➢ **To change a user password (user action):**

1. Open a web browser and navigate to https://<ReadyNAS_IP_address>/.

   <ReadyNAS_IP_address> is the IP address of the ReadyNAS system on which the user has an account.

2. Log in to the ReadyNAS system using your user name and existing password.
3. Click the **Password** tab.

   The Change Password screen displays.

4. Enter your current password in the **Current Password** field.
5. Enter a new password in the **New Password** field.
6. Enter your new password in the **Re-type new password** field.
7. Click the **Change Password** button.

   Your new password is saved.

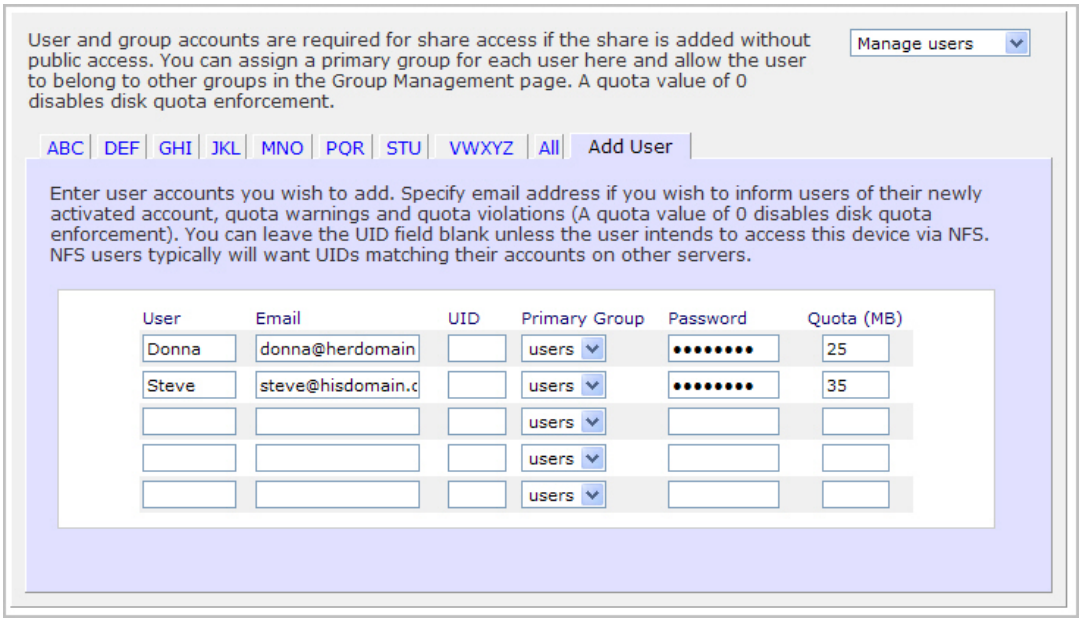
User Password Change by Administrator

If you do not enable users to change their own passwords, the ReadyNAS system administrator is the only person who can change user passwords. For more information about enabling users to change their own passwords, see *Set Default User Account Parameters* on page 61.

➢ **To change a user password (administrator action):**

1. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



   If your system has only a few users, they all appear on the screen.

   If your system has many users, click the appropriate tab to find the user that you want to delete.

2. Select the user whose password needs to be changed.
3. Enter a new password in the **Password** field.
4. Click the **Apply** button.

   The new password is saved.

Export User Lists

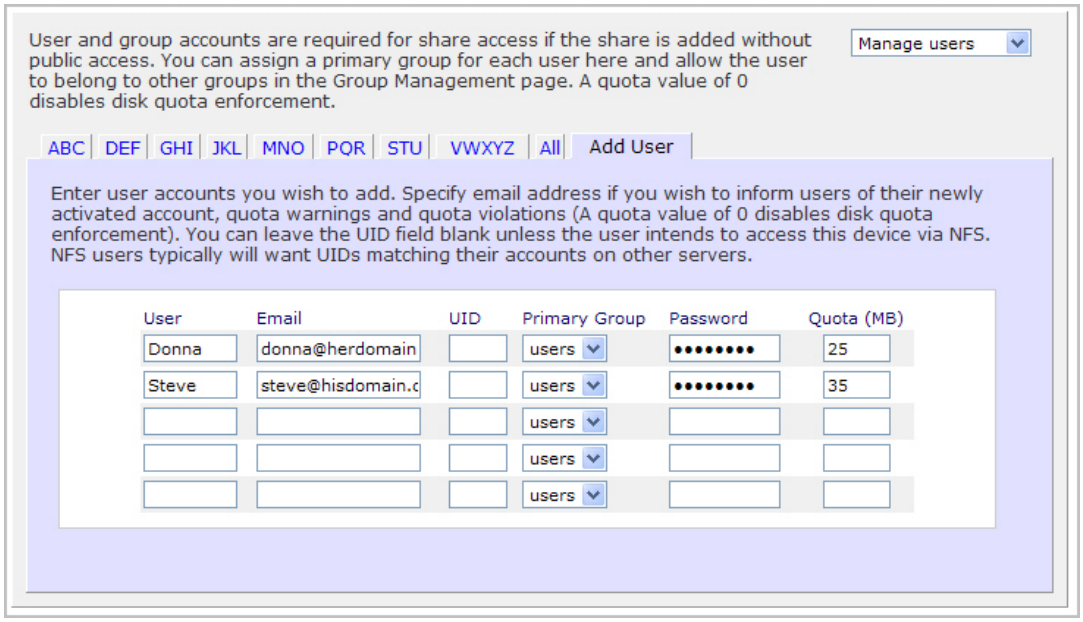
You can download a list of your ReadyNAS system's user accounts in a comma-separated value (CSV) file. The file is also backed up in the administrator's home directory.

You might want to export a group list to make it easy to transfer groups from one ReadyNAS system to another.

➢ **To export a user list:**

1. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



1. From the drop-down list in the upper-right corner, select **Export user list**.

   The Export User List screen displays.

2. Click the **Download User List** link.

   You are prompted to save the file on your computer.

3. Follow the prompts.

Groups

Use FrontView to create, manage, and delete groups of users on your ReadyNAS storage system. Creating groups is optional. If you do not create groups of users, all users are placed into the group called users.

Create Groups

You can create groups manually or in large batches.

Manually Create Groups

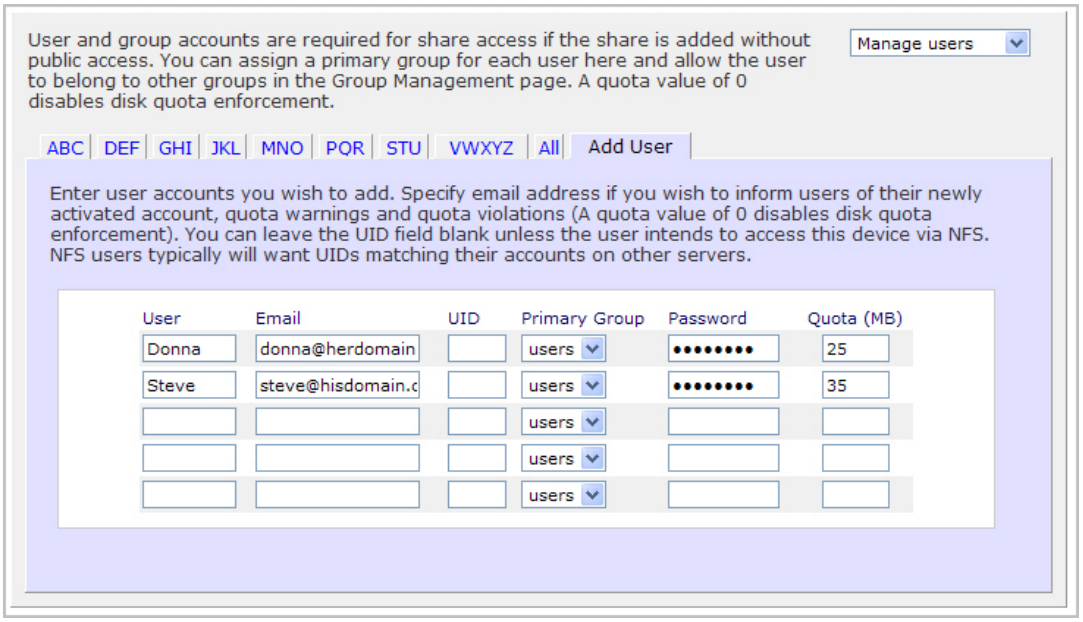
Use FrontView to manually create up to five group accounts at one time.

To create more than five group accounts at one time, you can import a CSV file. For more information, see *Create Groups in Batches* on page 73.

➢ **To manually create a group:**

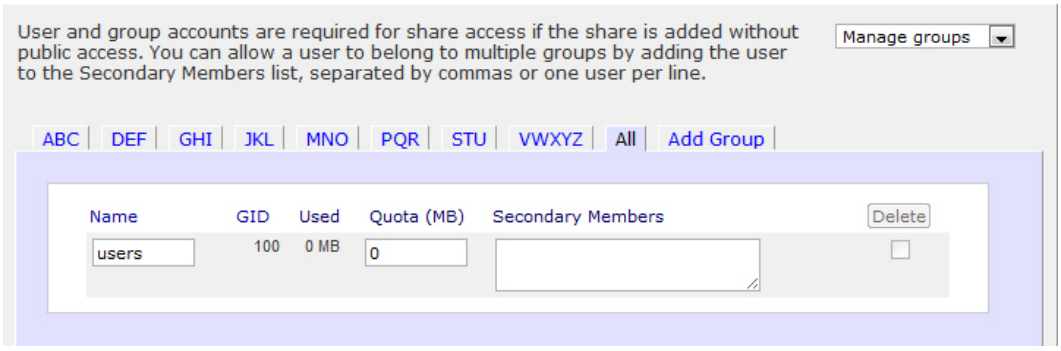
1. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



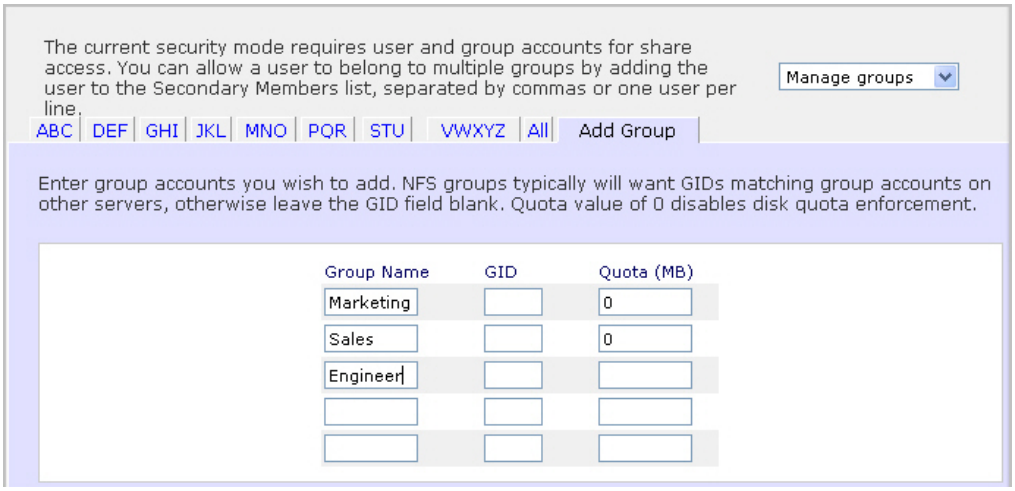
2. From the drop-down list in the upper-right corner, select **Manage Groups**.

   The Group screen displays.



3. Click the **Add Group** tab.

   The Add Group screen displays.



   You can add up to five groups at a time.

   For each group that you want to create, provide the following information:

   - **Group Name**. Required. The group name you provide must be unique among all group names on your ReadyNAS system. For example, if you have a group named Accounting on your ReadyNAS system, you cannot create another group named Accounting.
   - **Group ID**. Optional. If you do not create a group ID, your ReadyNAS system assigns one.
   - **Disk quota**. Optional. If you do not enter a quota, your ReadyNAS system places no limits on the amount of space this group can consume.

4. Click the **Apply** button.

   The group or groups are created.

Create Groups in Batches

You can create many groups at one time by uploading a CSV file to your ReadyNAS system. The file must use the following format:

name1,gid1,quota1,member1:member2:member3

name2,gid2,quota2,member1:member2:member3

name3,gid3,quota3,member1:member2:member3

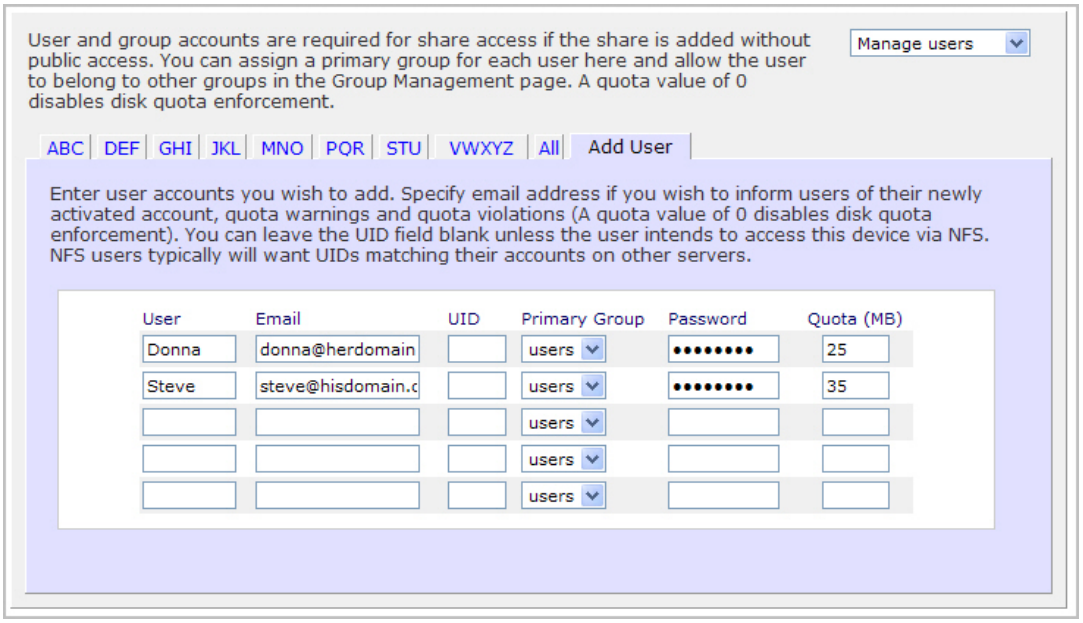
Note the following:

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

➢ **To create many user accounts at one time:**

1. On your computer, create a CSV file listing groups you want to create.
2. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



3. Select **Import Group List** from the drop-down list in the upper right corner.

   You are prompted to browse for your user file.

4. Click the **Browse** button.

   A dialog box opens.

5. Navigate to the file and click the **Open** button.

   The groups are added to your ReadyNAS system.

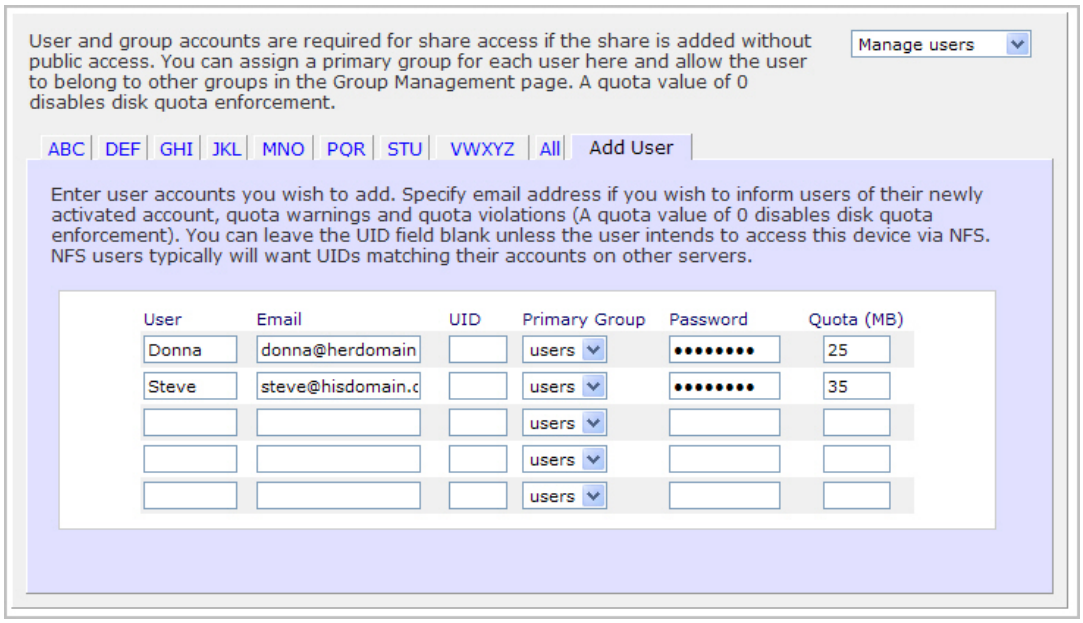
Edit Groups

Use FrontView to edit a group's name or quota or to add users to a group as secondary group members.

➢ **To edit a group's settings:**

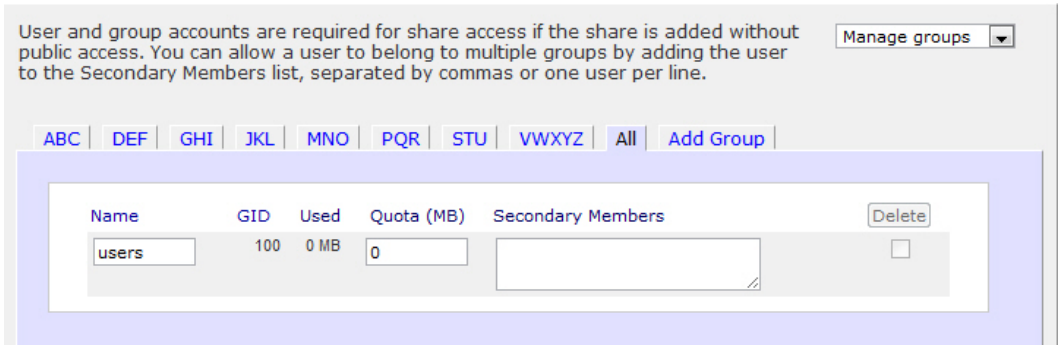
1. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



2. From the drop-down list in the upper-right corner, select **Manage groups**.

   The Groups screen displays.



   If your system has only a few groups, they all display on the screen.

   If your system has many groups, click the appropriate tab to find the group that you want to delete.

3. Edit the settings for the group as needed.
4. Click the **Apply** button.

   Your changes are saved.

Delete a Group

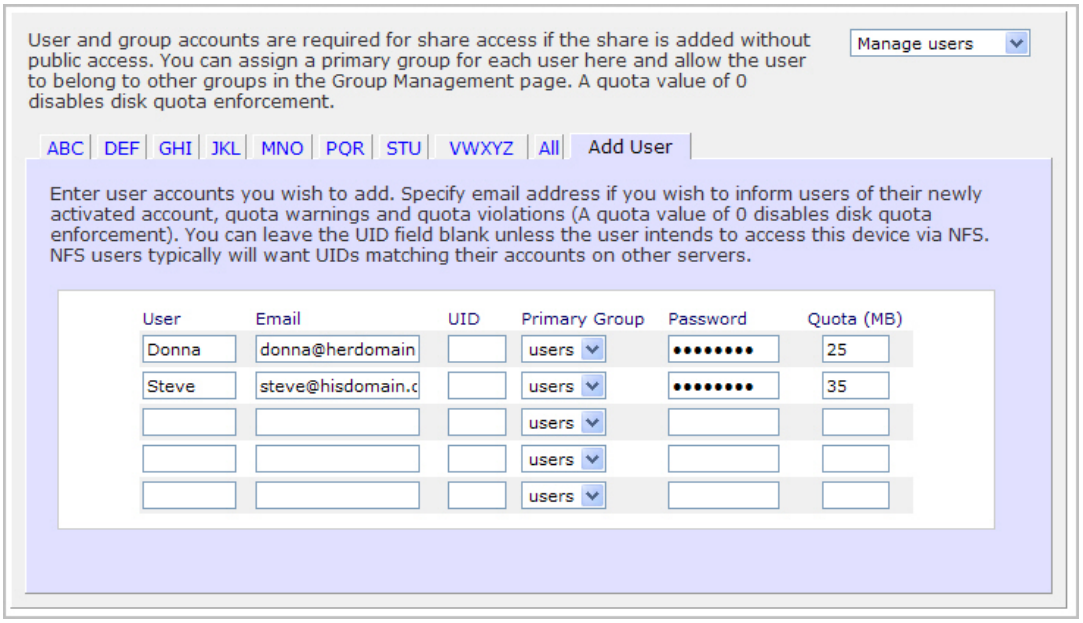
Use FrontView to delete a group. Before you can delete a group, you must first ensure that the group has no users assigned to it, as follows:

- **Reassign users in that group to a different group**. For more information, see *Edit User Accounts* on page 67.
- **Delete users in that group**. For more information, see *Delete User Accounts* on page 68.

➢ **To delete a group:**

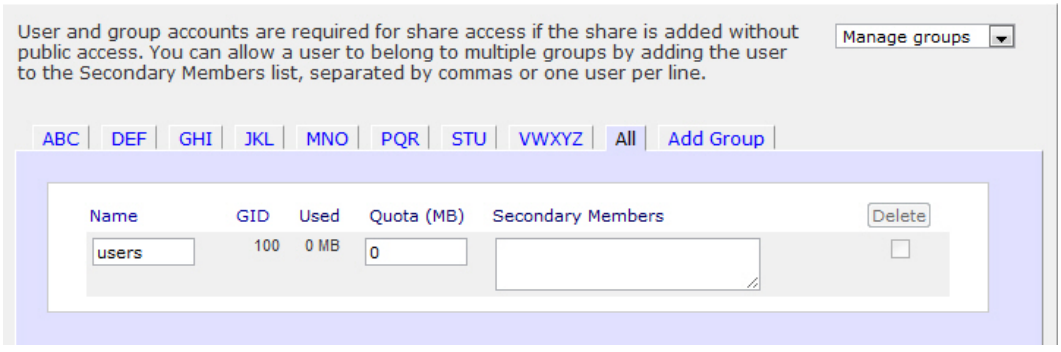
1. Ensure that all users in the group that you want to delete are reassigned to another group or deleted.
2. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



3. From the drop-down list in the upper-right corner, select **Manage Groups**.

   The Groups screen displays.



If your system has only a few groups, they all display on the screen.

If your system has many groups, click the appropriate tab to find the group that you want to delete.

4. Select the **Delete** check box in the row for the group that you want to delete.

   The Delete button becomes active.

5. Click the **Delete** button.

   The group is deleted.

Export Group Lists

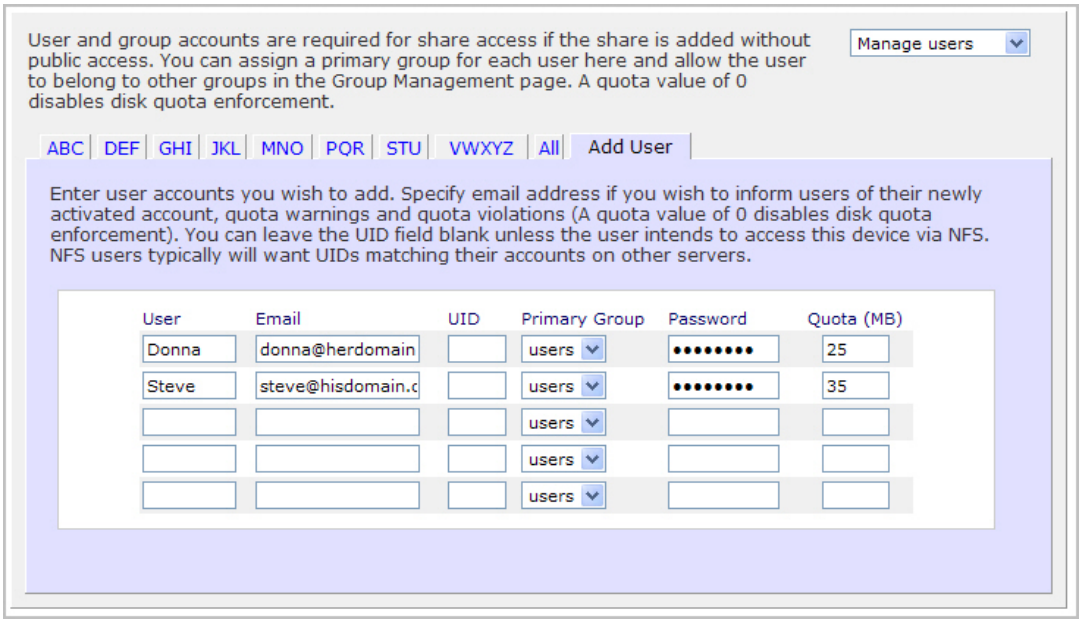
You can download the group list on this device into a comma-separated values (CSV) file. The file is backed up in the admin user home directory.

You might want to export a group list to make it easy to transfer groups from one ReadyNAS system to another.

➢ **To export a group list:**

1. Select **Security > User & Group Accounts** from the FrontView main menu.

   The User screen displays.



1. From the drop-down list in the upper-right corner, select **Export group list**.

   The Export Group List screen displays.

2. Click the **Download Group List** link.

   You are prompted to save the file on your computer.

3. Follow the prompts.

System Settings

5

This chapter describes how to manage your ReadyNAS storage system's configuration, network settings, streaming and discovery services, add-ons, USB devices, and iSCSI targets. It contains the following sections:

System Configuration

Use FrontView to manage the configuration of your ReadyNAS storage system.

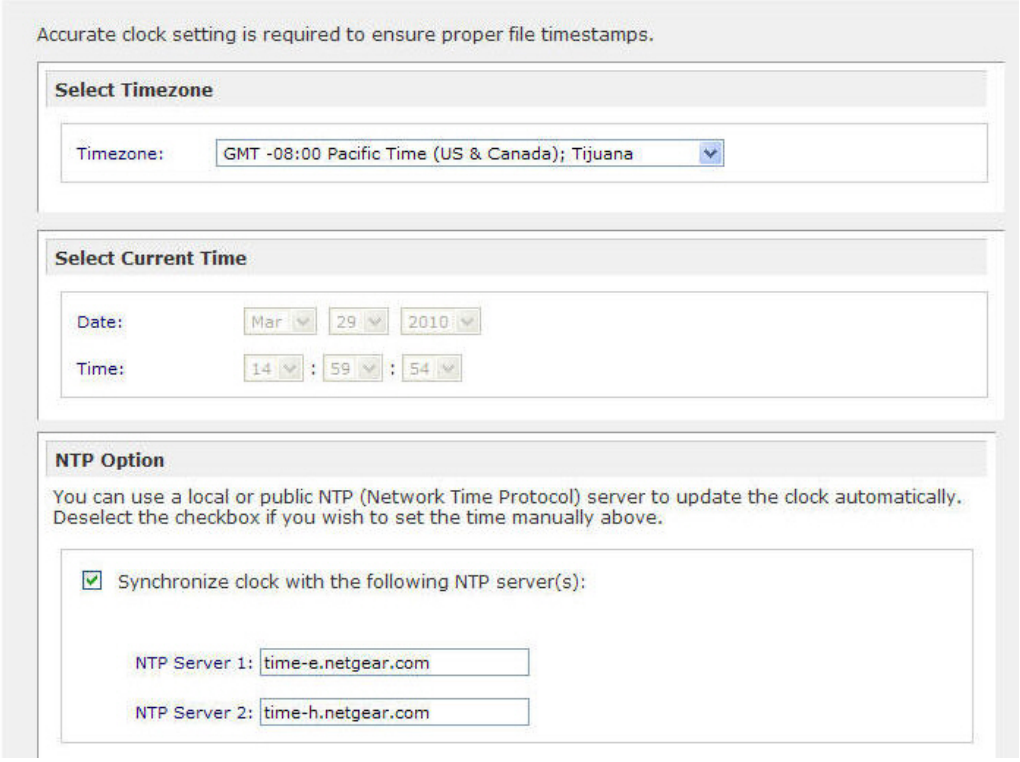
Clock

To enable your ReadyNAS system to correctly time stamp your files, you must ensure that your ReadyNAS system's time and date settings are accurate.

➢ **To set system time and date:**

1. Select **System > Clock** from the main menu.

   A screen displaying clock settings displays.



2. From the **Timezone** drop-down list, select the correct time zone for your location.

3. Select the correct time by doing one of the following:
   - Select the **Synchronize clock with the following NTP servers** check box and ensure that details about at least one NTP server are present. When you select this check box, the fields in the Select Current Time pane dim.

     You can choose to keep the default servers or enter up to two NTP servers closer to your location. You can find available public NTP servers by searching online.
   - Clear the **Synchronize clock with the following NTP servers** check box and use the **Date** and **Time** drop-down lists to manually set the time.

     When you clear this check box, the fields in the NTP Option pane dim.
4. Click the **Apply** button.

Alerts

To receive an email message alerting you if a system event that requires your attention occurs, provide at least one email address in the ReadyNAS system's contact list. For example, system events such as a fan failure, a hard disk failure, a quota violation, or low disk space generate email alert messages. Your storage system divides system events into two categories, mandatory and optional. Mandatory events always generate email alert messages. You can control which optional system events generate email alert messages.

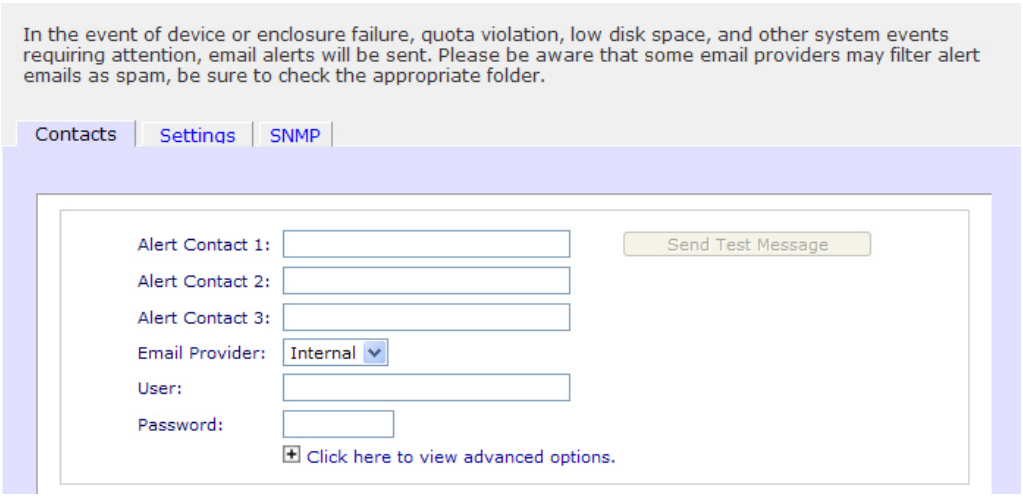
Email Alert Contacts

You can enter up to three email addresses to receive system alerts. It is a good idea to enter a primary email address and a backup email address. You can use an email address that is accessible from a smart phone to help you monitor your ReadyNAS system when you are away from it.

➢ **To manage email contacts:**

1. Select **System > Alerts** from the main menu.

   The Contacts screen displays.



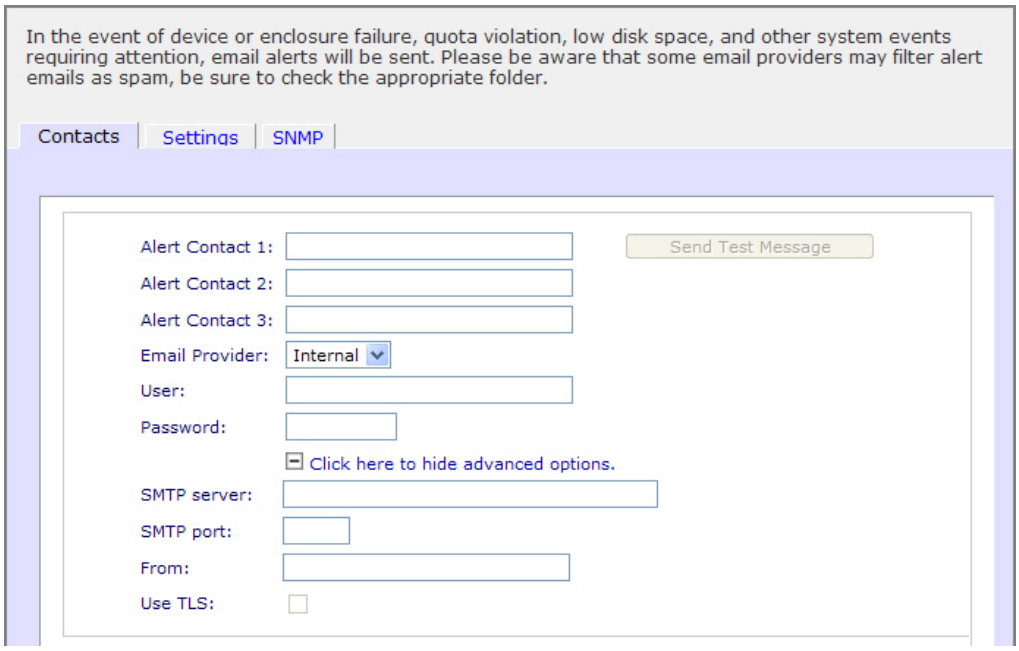
2. Enter an email address in one of the **Alert Contact** fields.

   You can also edit an existing alert contact or delete it by clearing the field.

3. Select your email service provider from the **Email Provider** drop-down list.

   If your email service provider is not listed, click the ⊞ button to customize the outgoing mail server (STMP) settings for your provider.

   The screen expands to display advanced options.



   Enter the details for your email service provider. These are often available on the Internet, or you can contact your email service provider for the information.

4. Enter your email address in the **User** field and password in the **Password** field.

   Your storage system uses these credentials to authenticate with your email service provider's outgoing mail server so that it can send email alerts.

5. (Optional) Click the **Send Test Message** button to determine if you configured the contact information correctly.
6. Click the **Apply** button.

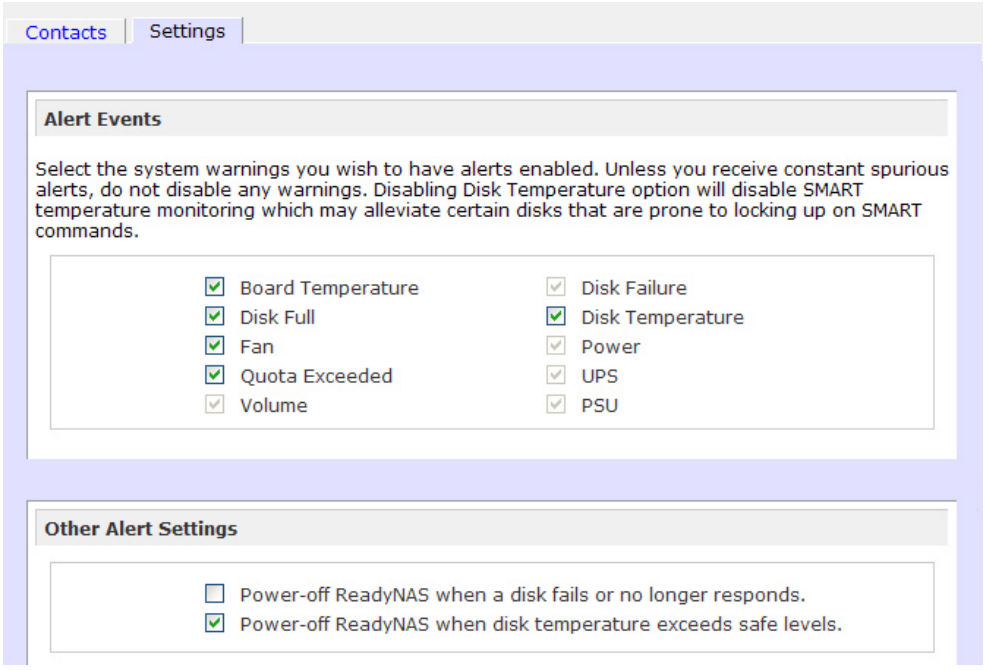
Alert Event Settings

Your ReadyNAS storage system is preconfigured to generate email alert messages when mandatory and optional system events occur. You can determine which optional system events generate alerts. NETGEAR recommends that you keep all alerts enabled; however, you might choose to temporarily disable an alert if you are aware of a problem.

➢ **To manage alert event settings:**

1. Select **System > Alerts** from the main menu and click the **Settings** tab.

   The Settings screen displays.



2. Select or clear any event check boxes.

   You can choose to clear any non-dimmed events in the Alert Events pane. Dimmed events always send email alerts.

3. Select or clear any check boxes in the **Other Alert Settings** pane, as follows:
   - Select the **Power-off NAS when a disk fails or no longer responds** check box 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** check box to gracefully power off the ReadyNAS when the disk temperature exceeds the nominal range.
4. Click the **Apply** button.

Language

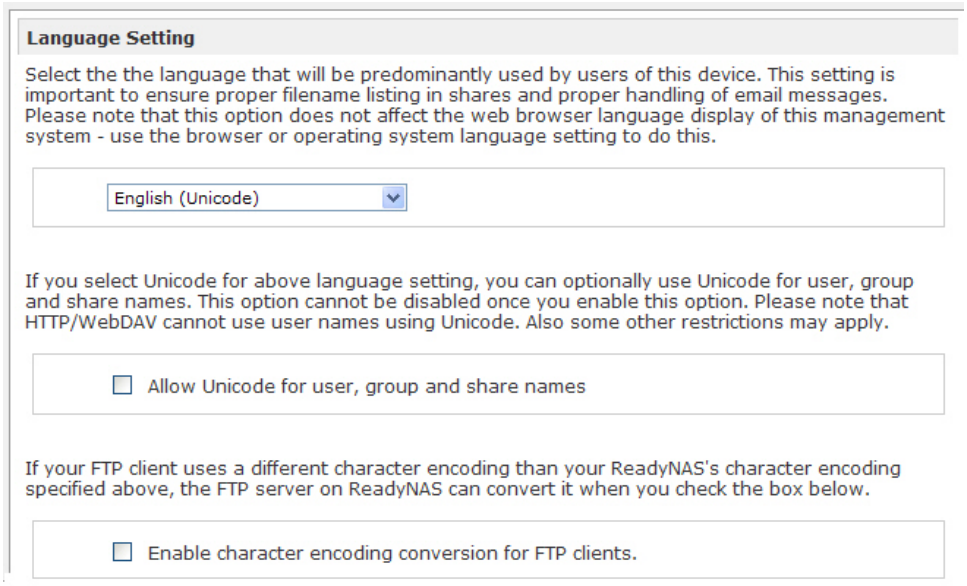
To ensure that your ReadyNAS storage system correctly displays file names, configure your system to use the appropriate character set. For example, selecting Japanese allows the ReadyNAS to support files with Japanese names in Windows Explorer.

Note: This setting does not control the language used in the FrontView interface. To change the language in FrontView, adjust your browser's language option.

➢ **To configure language settings:**

1. Select **System > Language** from the main menu.

   The Language Setting screen displays.



2. Select a language from the drop-down list.

   NETGEAR recommends choosing a language based on the region where the device is being used.

3. (Optional) For greater flexibility in regions where English is not spoken, select the **Allow Unicode for user, group and share names** check box.

WARNING!

You cannot undo this option.

HTTP and WebDAV access do not work with Unicode user names.

4. (Optional) 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.
5. Click the **Apply** button.

   Your settings are saved.

Administrator Password

The ReadyNAS storage system's administrator is the only user who can access FrontView. The administrator can access any file on the ReadyNAS system, including private home shares. For those reasons, it is important to safeguard the administrator password and to change it regularly to protect your data.

Change the Administrator Password

Be sure to choose an administrator password that is 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 your ReadyNAS system.

➢ **To change the administrator password:**

1. Select **Security > Admin Password** from the main menu.

   An administrator password screen displays.

2. Enter a new password in the **New Admin Password** field and re-enter the new password in the **Retype Admin Password** field.
3. Click the **Apply** button.

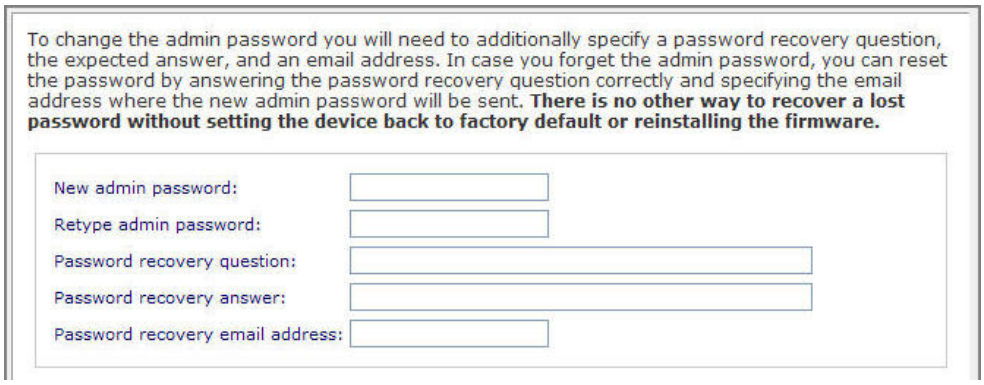
Enable Administrator Password Recovery

If you lose or forget your administrator password, NETGEAR can reset it for you if you previously enabled administrator password recovery. If you do not enable administrator password recovery, you must perform an OS reinstall reboot on your ReadyNAS system to reset the administrator password to the factory default password.

➢ **To enable administrator password recovery:**

1. Select **Security > Admin Password** from the main menu.

   An administrator password screen displays.



2. Enter a question in the **Password Recovery Question** field.

   Choose a question that very few people can answer. For example, you might enter *First dog's name?* or *Best friend in Kindergarten?* as your password recovery question.

3. Enter the answer to your question in the **Password Recovery Answer** field.
4. Enter an email address in the **Password Recovery Email Address** field.
5. Click the **Apply** button.

   Administrator password recovery is enabled.

Recover Your Administrator Password

You can recover a lost or forgotten administrator password in two ways:

- **Using NETGEAR's password recovery tool**. This web-based tool requires that you enable administrator password recovery on your ReadyNAS storage system before you can use it. For more information, see *Enable Administrator Password Recovery* on page 85.
- **Performing an OS reinstall reboot**. This process reinstalls the firmware on your system and resets the administrator user name and password to factory defaults.

Recover Your Administrator Password Using NETGEAR's Password Recovery Tool

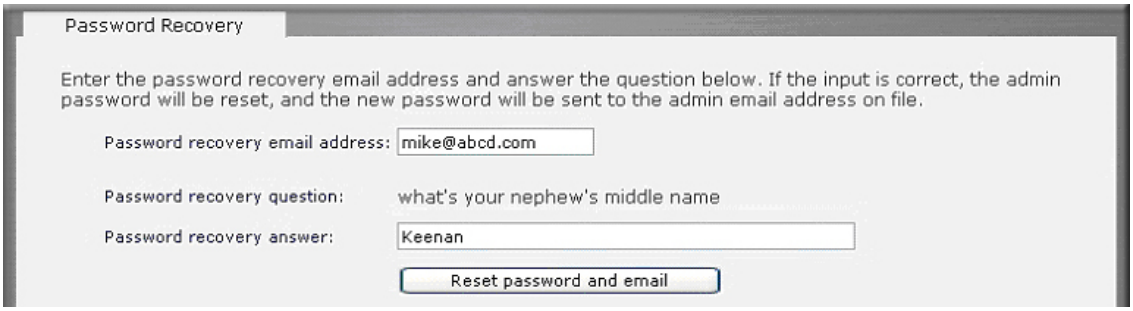
This procedure is an option only if you enabled password recovery by providing a password recovery question, answer, and email address as described in *Enable Administrator Password Recovery* on page 85. If you lost your password but did not enable administrator password recovery, see *Recover Your Administrator Password Using an OS Reinstall Reboot* on page 86

➢ **To recover your administrator password using NETGEAR's password recovery tool:**

1. Using a web browser, visit https://<ReadyNAS_IP_address>/password_recovery.

   <ReadyNAS_IP_address> is the IP address of your ReadyNAS system.

   The ReadyNAS password recovery screen displays.



2. Enter the email address and password recovery answer you enabled on your ReadyNAS storage system and click the **Reset password and email** button.

   NETGEAR resets your administrator password and sends an email message with the new password to you.

Recover Your Administrator Password Using an OS Reinstall Reboot

This process does not remove data from the system, but resets the administrator user name and password to the factory defaults:

- **Factory default user name**. admin
- **Factor default password**. netgear1

➢ **To recover your administrator password using an OS reinstall reboot:**

Perform an OS reinstall reboot on your storage system.

The process for performing an OS reinstall reset reboot varies by storage system. For more information about how to perform a factory reset reboot, see the *ReadyNAS Ultra, Ultra Plus, NVX, and Pro Series Hardware Manual*.

Printer Queue Service

You can connect a printer to your ReadyNAS system and share it across your local area network. Your ReadyNAS system supports single-function USB printers.

➢ **To connect a printer:**

1. Connect a USB cable from a single-function USB printer to a USB port on your ReadyNAS system.

   For more information about the USB ports on your ReadyNAS system, see the *ReadyNAS Ultra, Ultra Plus, NVX, and Pro Series Hardware Manual.*

2. Power on the printer.
3. Select **Printer > Printer Queue Service** from the FrontView main menu.

   The Printer screen displays showing the printer you connected.

System Shutdown

Use FrontView to gracefully shut down your ReadyNAS storage system. When you reboot your system, you must close the browser window and use RAIDar to reconnect to FrontView.

➢ **To gracefully shut down your system:**

1. Select **System > Shutdown** from the FrontView main menu.

   The Shutdown Options screen displays.

2. Choose a shutdown option:
   - Select the **Shutdown and turn off device** radio button to shut down your system.
   - Select the **Shutdown and reboot device** radio button to shut down your system and automatically reboot it.
3. (Optional) Select the **Perform volume scan on next boot** check box.

   You do not need to select this option unless you suspect data integrity problems. This can take more than an hour depending on your disk capacity and content.

4. (Optional) Select the **Check and fix quotas on next boot** check box.

   You do not need to select this option unless you suspect quota problems. This can take more than an hour depending on your disk capacity and content.

5. Click the **Apply** button.

   Your system shuts down, and if you selected the reboot option, reboots.

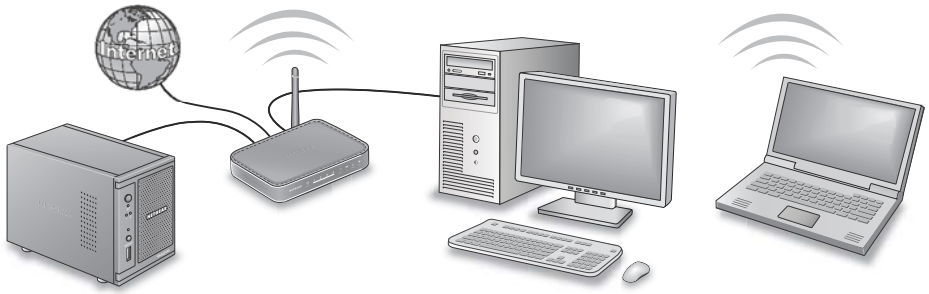
6. Close the FrontView browser window.
7. When you reboot, use RAIDar to reconnect to your ReadyNAS system.

   For more information, see *RAIDar* on page 10.

Network Settings

The acronym *NAS* in ReadyNAS is short for *network-attached storage*. Your local area network (LAN) is an integral part of managing and using your ReadyNAS storage system. Connecting your ReadyNAS storage system to the Internet expands your ability to access data stored on your ReadyNAS system when you are away from it. It also allows you to share data with people located around the world.

A typical network setup that includes a ReadyNAS system resembles this illustration.



You can use FrontView to adjust your ReadyNAS system's network settings.

Ethernet

Your ReadyNAS storage system uses Ethernet technology to transfer information on your local area network. Ethernet technology divides data into smaller pieces, called packets or frames, before transmitting it on your network. Ethernet technology includes methods to check for data transmission errors.

Every device that uses Ethernet technology has a unique MAC (media access control) address that is used to identify the source device and the destination device. MAC addresses are assigned when a device is manufactured. Your ReadyNAS storage system's MAC address is listed on a sticker on the bottom of the system. It is also listed in the FrontView interface on the Network Standard Setting screen. Access it by selecting **Network > Interfaces** from the FrontView main menu.

IP (Internet Protocol) addresses are another key component for sharing data over a network. A unique IP address is assigned to every network-connected device. IP addresses come in

two varieties: static and dynamic. Static IP addresses do not change, but dynamic IP addresses do change.

Unlike MAC addresses, IP addresses are not assigned by the device's manufacturer. Static IP addresses are assigned by your ISP (Internet service provider) or network administrator. Dynamic IP addresses are assigned by a DHCP (Dynamic Host Control Protocol) server. In most cases, the DHCP server belongs to an ISP, but a router or other device, like your ReadyNAS storage system, can also act as a DHCP server.

You can configure how your ReadyNAS storage system negotiates speed and duplex settings. Speed refers to the rate at which data is transferred across the network. Duplex mode refers to how communications between two devices on a network are handled. Full-duplex means that communications from one device to another can happen in both directions at the same time. Half-duplex mode means that communication can go in only one direction at a time. For example, in full-duplex mode, Device A can receive information from Device B at the same time that Device B is receiving information from Device A. In half-duplex mode, Device B cannot send information to Device A while Device A is sending information to Device B.

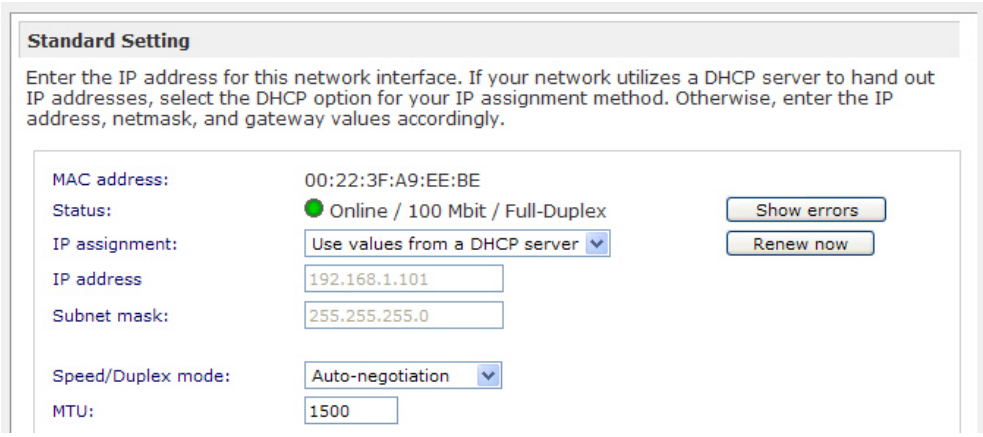
You can also configure the maximum size of packets that are sent across a network. This setting is called MTU (maximum transmission unit). A large MTU can help speed data transmission in some circumstances. However, using a large packet size becomes inefficient if an error occurs during transmission. That is because if any part of a large packet is corrupt, the entire large packet must be resent. If you use a smaller MTU, smaller packets are resent if a communication error occurs.

In most environments, your ReadyNAS storage system's default network settings allow you to connect and communicate with your ReadyNAS storage system over your local area network and the Internet. However, you can adjust these settings to accommodate your needs.

➢ **To configure Ethernet settings:**

1. Select **Network > Interfaces** from the FrontView main menu.

   The Network Standard Setting screen displays.



2. Select a method for assigning an IP address.

   You can select from two options in the **IP assignment** drop-down list:

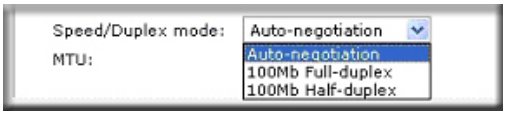
   - **Use values from a DHCP server**. In most networks, a DHCP server is enabled, so you can select this option to automatically set the IP address and network mask.

     If you select this option, NETGEAR recommends that you set the lease time on the DHCP server or router to a value of at least one day. Otherwise, you might notice that the IP address of the unit changes even after it being 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, enabling it ensures that your ReadyNAS maintains the same IP address, even in DHCP mode.

   - **Use values below**. If you select this option to assign a static IP address, note that your browser loses its connection to your ReadyNAS storage system if the IP address changes. To reconnect to your ReadyNAS system after assigning a static IP address that has changed, open the RAIDar utility and click **Rescan** to locate the device, and then reconnect.

     Also note that you must take care to correctly enter the IP address. If you enter an incorrect IP address, you cannot connect to your ReadyNAS system. To recover from an incorrectly entered IP address, you must perform an OS reinstall reboot. For more information, see the *ReadyNAS Ultra, Ultra Plus, NVX, and Pro Series Hardware Manual.*

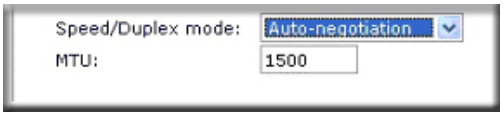
3. Set a speed/duplex mode.



   Select an option from the **Speed/Duplex mode** drop-down list.

   NETGEAR recommends that you use the Auto-negotiation option. 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.

4. Set an MTU (maximum transmission unit) size.



   Choose an option from the **MTU** drop-down list.

   NETGEAR recommends that you use the default setting of 1500; however, in some network environments, changing the default MTU value can fix throughput problems.

5. Click the **Apply** button.

   Your settings are saved.

Hostname

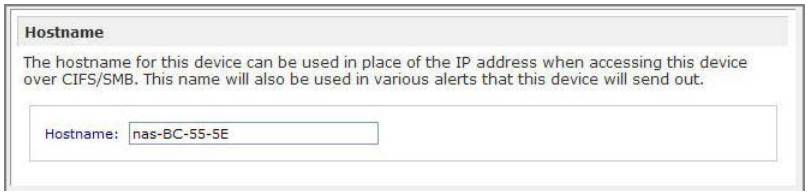
Your ReadyNAS storage system uses the hostname to advertise itself on your network. When you review your network using RAIDar, your PC, your Mac, or any other interface, you can recognize your storage system by its hostname.

The default hostname is *nas-* followed by the last 3 bytes of the system's primary MAC address. You can change the hostname to one that is easier to remember and recognize.

➢ **To change the hostname:**

1. Select **Network > Global Settings** from the main list.

   The Global Settings screen displays.



2. Enter a new hostname in the **Hostname** field.

   The host name must be unique on your LAN. For example, if your router's hostname is Fido, you cannot use Fido as your ReadyNAS system's hostname. Use only alphanumeric characters and hyphens in your hostname.

3. Click the **Apply** button.

   Your settings are saved.

Gateway

A gateway is a device that connects your local area network to other networks, including the Internet. In FrontView, you specify the IP address of the device that does this job in your local area network. In most homes and smaller offices, this is the IP address of a router connected to a cable modem or DSL service.

If you selected the DHCP option when you configured your Ethernet settings, the default gateway field is automatically populated with the setting from your DHCP server.

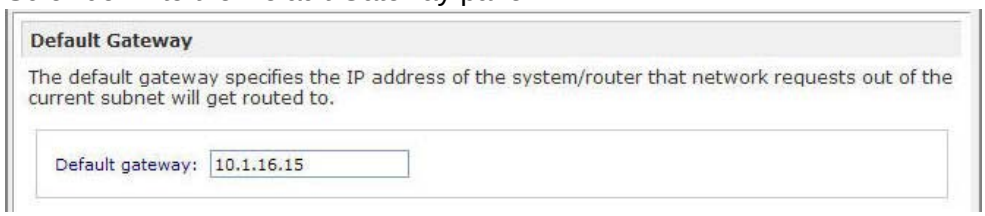
If you selected the static option when you configured your Ethernet settings, you must manually specify the IP address of the default gateway server if you want to access your ReadyNAS system over the Internet. Your network administrator can help you determine your gateway IP address.

➢ **To manually configure the default gateway:**

1. Select **Network > Global Settings** from the FrontView main menu.

   The Global Settings screen displays.

2. Scroll down to the Default Gateway pane.



3. In the **Default gateway** field, enter the IP address of your gateway device.
4. Click the **Apply** button.

DNS

DNS is short for Domain Name System. Because IP addresses are a string of numbers, they are hard to remember. It is much easier to remember a name (for example, www.readynas.com) than it is to remember a string of numbers when you want to visit a website. A DNS server translates IP addresses into website names and website names into IP addresses.

You can specify up to three DNS servers in your ReadyNAS storage system.

If you selected the DHCP option when you configured your Ethernet settings, the Domain Name Server fields are automatically populated with the DNS settings from your DHCP server.

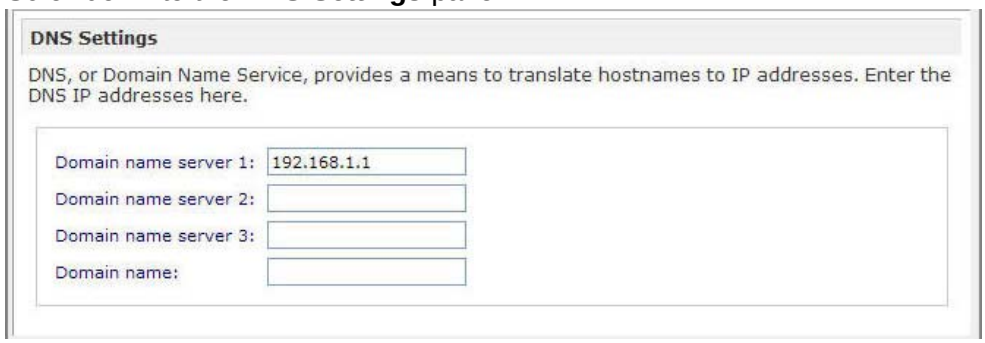
If you selected the static option when you configured your Ethernet settings, you must manually specify the IP addresses of the DNS servers and the domain name if you want to access your ReadyNAS system over the Internet. Your network administrator can help you determine your domain name server IP address.

➢ **To manually configure DNS settings:**

1. Select **Network > Global Settings** from the FrontView main menu.

   The Global Settings screen displays.

2. Scroll down to the **DNS Settings** pane.



3. In at least one **Domain name server** field, enter at a DNS server IP address.
4. (Optional) In the **Domain name** field, enter a domain name in the **Domain name** field.
5. Click the **Apply** button.

   Your settings are saved.

WINS

A WINS (Windows Internet Name Service) server allows network-attached devices like computers and storage systems to be browsed from computers that are not on your LAN. Most Macs also support WINS technology. This is useful if you use a VPN (virtual private network).

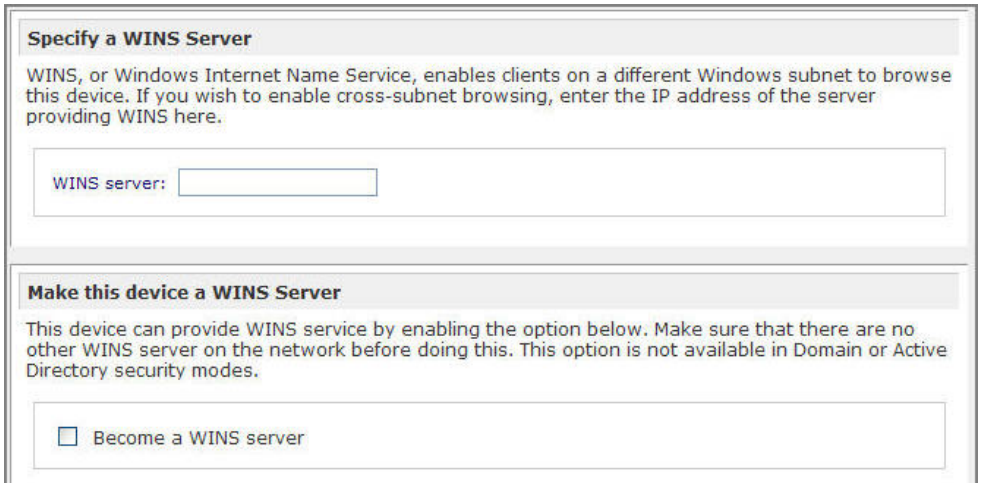
Enable WINS

You can enable WINS so that your ReadyNAS system can be browsed by computers and devices on other subnets.

➢ **To enable WINS:**

1. Select **Network > WINS** from the FrontView main menu.

   The WINS screen displays.



2. In the **WINS server** field, enter the IP address of a WINS server.
3. Click the **Apply** button.

   Your settings are saved.

Enable your ReadyNAS System as a WINS Server

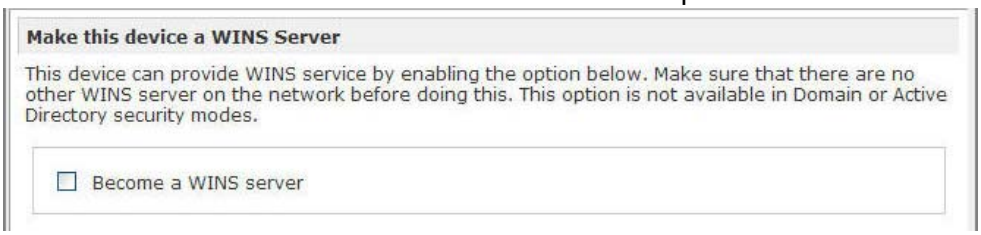
If no other WINS servers exist on your network, you can enable your ReadyNAS system as a WINS server.

➢ **To enable your ReadyNAS system as a WINS server:**

1. Select **Network > WINS** from the FrontView main menu.

   The WINS screen displays.

2. Scroll down to the **Make this device a WINS Server** pane.



3. Select the **Become a WINS server** check box.
4. Click the **Apply** button.

   Your settings are saved.

DHCP

DHCP (Dynamic Host Configuration Protocol) service simplifies management of a network by dynamically assigning IP addresses to new clients on a network.

WARNING!

Enabling DHCP service on a network that is already using another DHCP server creates conflicts that can interfere with your ability to access the Internet.

You can enable your ReadyNAS storage system to work as a DHCP server. This feature is available only on ReadyNAS storage systems that are installed in networks where DHCP service is not already available.

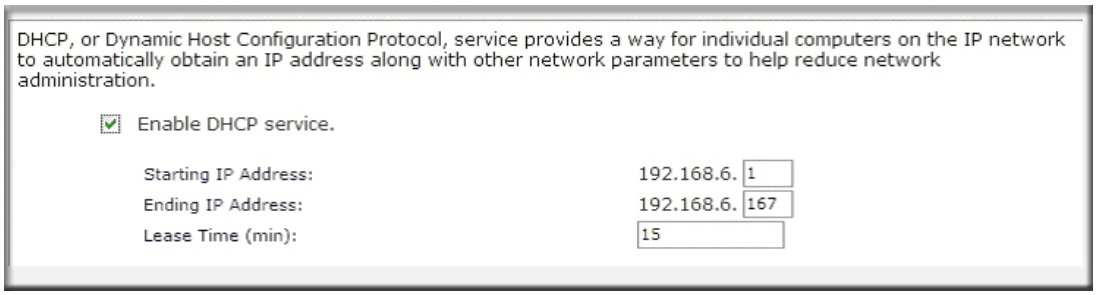
If you want to use this device as a DHCP server, you must first specify static addresses in your network configuration settings. For more information, see *Network Settings* on page 88.

➢ **To make your ReadyNAS system a DHCP server:**

1. Select **Network > WINS** from the FrontView main menu.

   If you already have DHCP service, a message displays telling you that this feature is not available your ReadyNAS system.

   If you do not currently have a DHCP service on your network, a DHCP details screen displays.



2. Select the **Enable DHCP service** check box.
3. Click the **Apply** button.

   Your settings are saved.

Streaming Services

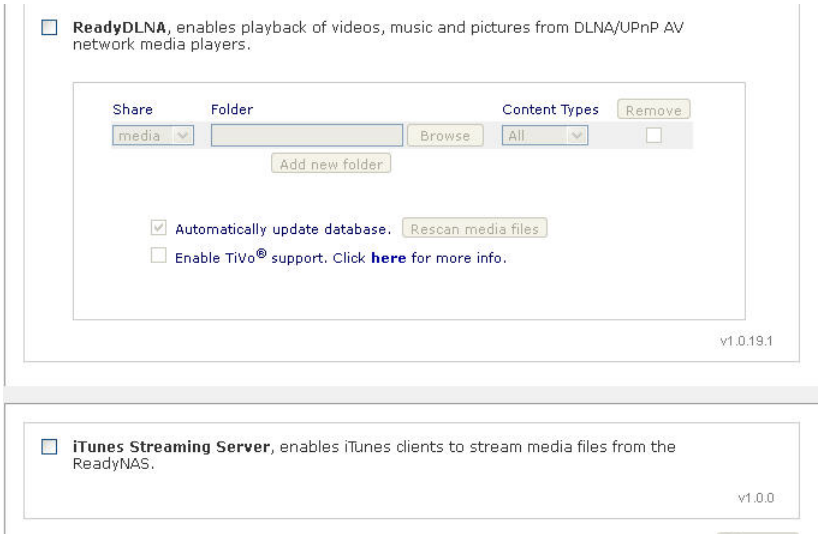
Streaming services allow you to send multimedia content directly from the ReadyNAS to a device that plays the multimedia content, without the need to have your PC or Mac powered on. Your ReadyNAS system supports the following streaming services:

- **ReadyDLNA**. ReadyDLNA provides media streaming service to standalone networked home media adapters and networked DVD players that are Digital Living Network Alliance (DLNA) standard compliant. The ReadyNAS comes with a reserved media share that is advertised and recognized by the players. Copy your media files to the Videos, Music, and Pictures folders in that share to display them on your player. If you wish, you can specify a different media path where your files reside.
- **iTunes Streaming Server**. iTunes Streaming Server enables iTunes clients to stream media files straight from your ReadyNAS system. Click the setup link for more detailed configuration options.

➢ **To manage streaming services:**

1. Select **Services > Streaming Services** from the FrontView main menu.

   The Streaming Services screen displays.



2. Select check boxes for any streaming services that you want to enable.
3. Clear check boxes for any streaming services that you want to disable.
4. Click the **Apply** button.

   Your settings are saved.

Discovery Services

Discovery services are protocols that allow network-enabled devices like computers or your ReadyNAS storage system discover each other across networks. Your ReadyNAS storage system supports these discovery service protocols:

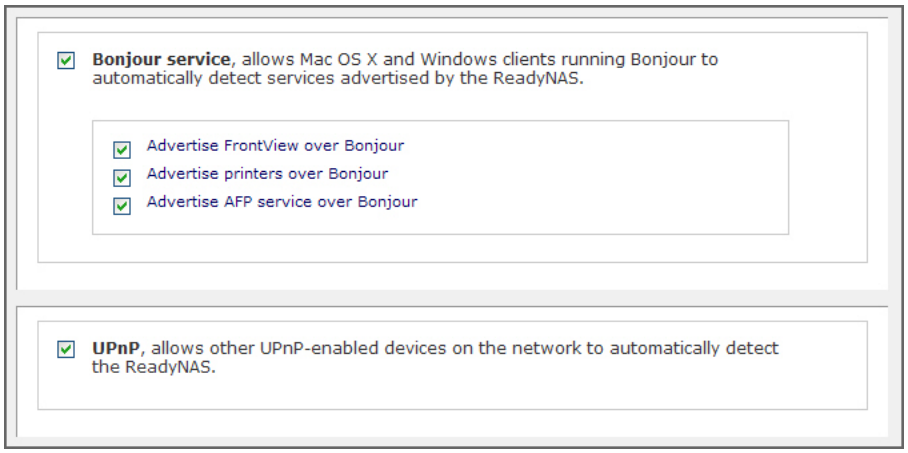
- **Bonjour**. Enables discovery of various services on your ReadyNAS system and provides a way to connect to FrontView, IPP printing, and AFP services. OS X has built-in Bonjour support, and you can download Bonjour for Windows from Apple's website.
- **UPnP (Universal Plug-n-Play)**. Allows UPnP-enabled clients to discover your ReadyNAS system on your LAN.

Other discovery services are available as add-ons. For more information about finding, installing, and managing add-ons for your ReadyNAS storage system, see *Add-Ons* on page 97.

➢ **To manage discovery services:**

1. Select **Services > Discovery Services** from the FrontView main menu.

   The Discovery Services screen displays.



2. Select check boxes for any discovery services that you want to enable.
3. Clear check boxes for any discovery services that you want to disable.
4. Click the **Apply** button.

   Your settings are saved.

Add-Ons

Add-ons are applications for your ReadyNAS storage system. You can add a wide variety of features and services for your ReadyNAS system by installing add-ons developed by NETGEAR, NETGEAR's partners, and community developers.

To view and download additional ReadyNAS add-ons, visit *http://readynas.com/addons* and *http://readynas.com/community_addons.*

Manage Add-Ons

You can use FrontView to view and manage add-ons that are currently installed on your ReadyNAS storage system.

Your ReadyNAS storage systems has the ReadyNAS Remote add-on preinstalled. This add-on allows secure, remote access to shares on your ReadyNAS without complicated router or VPN setup. After you access your shares from a PC using Windows File Explorer or from a Mac using Finder, you can easily drag and drop files within your LAN. For more information, see *Access Shares Using ReadyNAS Remote* on page 57.

➢ **To manage installed add-ons:**

1. Select **Add-ons > Installed** from the FrontView main menu.

   A screen displays listing all add-ons currently installed on your unit.

2. (Optional) To learn more about an installed add-on, click the link in the add-on description.

   A detailed description of the add-on displays.

3. (Optional) To remove an add-on, select the check box for the add-on you want to remove, click the **Remove** button, and follow the prompts.

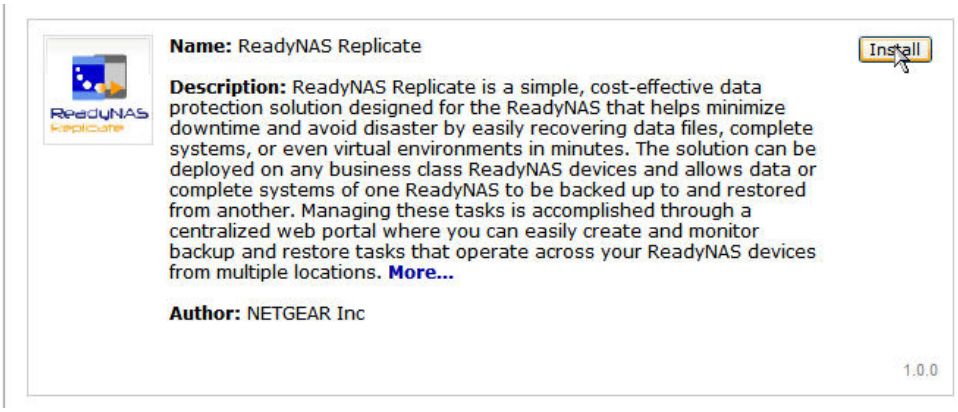
Browse and Install Add-ons

You can use FrontView to browse for and install add-ons that are available through NETGEAR, and to install add-ons that you downloaded from other sources.

➢ **To browse for and install available add-ons:**

1. Select **Add-ons > Available** from the FrontView main menu.

   A screen displays showing all add-ons available through NETGEAR.



2. (Optional) To install an add-on, click the **Install** button.

   A download progress bar displays and you are notified when the installation process completes. Some add-ons require you to reboot your ReadyNAS system to complete the installation. The new add-on is listed on the Installed screen.

Install Previously Downloaded Add-Ons

If you download add-ons directly to your ReadyNAS system without using the FrontView interface, you must use FrontView to install them.

➢ **To install previously downloaded add-ons:**

1. Select **Add-ons > Add New** from the FrontView main menu.
2. Browse to the add-on you want to upload.
3. Click the **Upload and verify image** button.

   In a moment, you are prompted to confirm the upload command.
4. Confirm the upload command.

   The add-on is installed. Some add-ons require you to reboot your ReadyNAS system to complete the installation.

USB Storage Devices

You can connect USB disk and flash drives to your ReadyNAS system and use FrontView to manage them.

USB storage devices can be divided into partitions. Partitions on the storage devices must be formatted in one of the following file system formats:

- FAT32
- NTFS
- EXT2
- EXT3

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

Even when access authorization is based on user login, files on a USB device are saved with User ID 0, regardless of the user account. This allows easy sharing of the USB device with other network storage and PC systems.

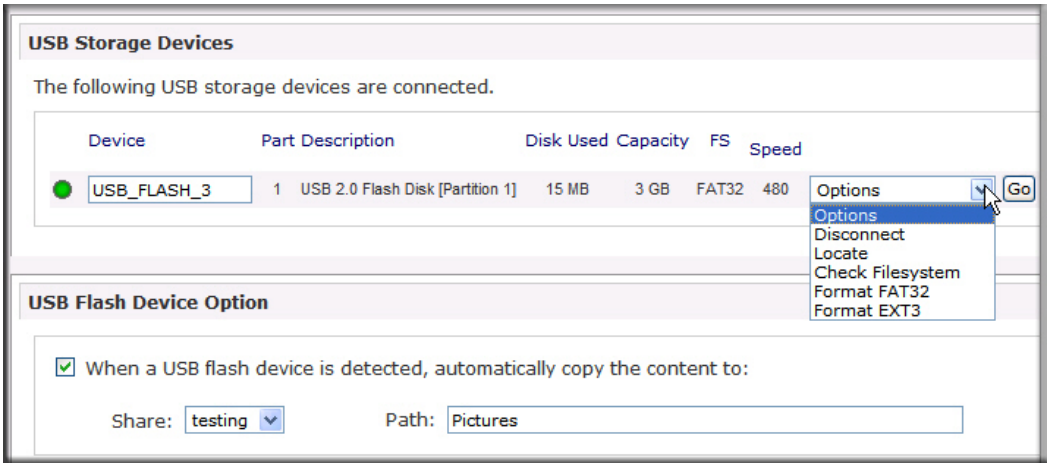
Manage USB Storage Devices

Use FrontView to manage USB storage devices that are attached to your ReadyNAS system.

➢ **To manage USB storage devices:**

1. Choose **Volumes > USB Storage** from the FrontView main menu.

   The USB Storage screen displays, showing information about any USB storage devices that are currently connected to your ReadyNAS system.



   If you currently do not have a USB storage device connected, a “No USB storage devices detected” message displays.

   A flash device displays as USB_FLASH_1, and a disk device displays as USB_HDD_1. When you attach multiple devices, the device names use a higher device number, for example, USB_HDD_2.

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

2. (Optional) To rename the USB storage device, enter a new name for the device in the field in the **Device** column to rename the USB storage device.

   The next time the same device is connected, FrontView uses the new name rather than the default USB_FLASH_<number> or USB_HDD_<number> naming scheme.

3. (Optional) Select an option from the drop-down list, as follows.

   - **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 option 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.
   - **Locate**. If you attach multiple storage devices and want to determine which device corresponds to the device listing, the Locate option 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. FAT32 imposes a 4-GB limitation per file.
- **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, which FAT32 does not support. You can add support for EXT3 to the Windows and OS X operating systems. EXT3 does not impose a file size limitation.

4. Click the **Go** button.

Copy USB Content Upon Connection

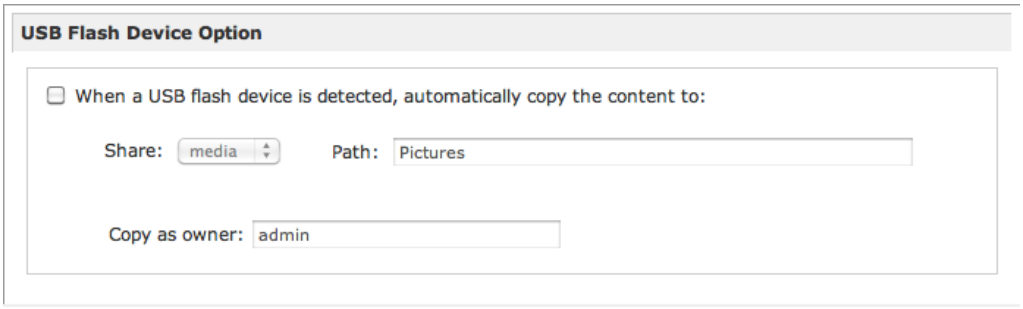
You can configure your ReadyNAS system to copy the content of a USB flash device to a specified share whenever a USB flash device is connected to it. Files are copied to a unique timestamp folder to prevent existing data from being overwritten. This is useful for uploading pictures from digital cameras and music from MP3 players without a PC.

➢ **To configure USB flash drive auto-copy upon connection:**

1. Select **Volumes > USB Storage** from the FrontView main menu.

   The USB Storage screen displays, showing information about any USB storage devices that are currently connected to your ReadyNAS system.

   Scroll down to the USB Flash Device Option pane.



2. Select the **When a USB flash device is detected, automatically copy the content to** check box.
3. Select a share from the **Share** drop-down menu.
4. Enter a path in the **Path** field.
5. Enter a user name or **admin** in the Copy **as owner** field.
6. Click the **Apply** button.

   Your settings are saved.

iSCSI Targets

iSCSI is a storage networking standard that uses the Small Computer System Interface (SCSI) to transfer data across a LAN. It is typically used in environments that use applications that require block-level access to a storage system. For example, database programs and virtualization programs often require block-level storage access. Most other file-sharing protocols (for example, CIFS, NFS, and AFP) access storage systems at the file level.

To use iSCSI, you must dedicate space on your ReadyNAS storage system by creating an iSCSI target that has one or more logical unit numbers (LUNs) assigned to it. A LUN is a division of space within an iSCSI target. You use an iSCSI initiator on your server, PC, or Mac to connect to the LUN and make use of the connection just as you would a local hard disk device.

Create an iSCSI Target

Each iSCSI target you create automatically creates a LUN 0 within the new iSCSI target. LUN 0 is required on each iSCSI target.

You can create additional LUNs, numbered from 1 to 254, for each target. You can allocate space to each LUN individually. You can access each LUN as a different connection. For more information, see *Add a LUN to an iSCSI Target* on page 104.

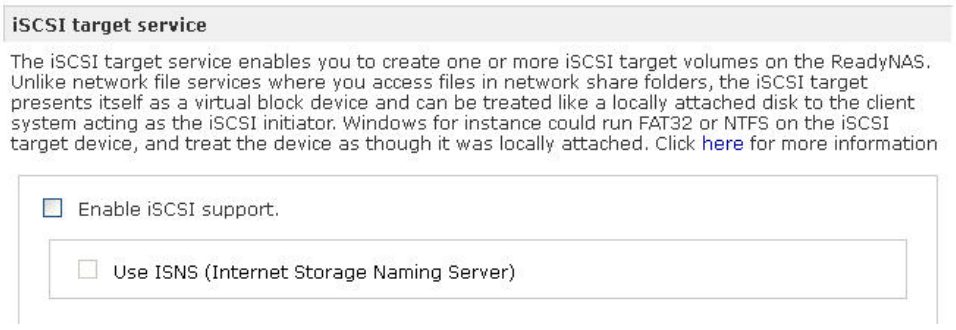
You can configure each iSCSI target to require CHAP authentication. CHAP authentication requires anyone accessing LUNs on iSCSI targets on which it is enabled to provide login credentials

➢ **To create an iSCSI target:**

1. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings Screen displays.

2. Click the **iSCSI** tab.
3. The iSCSI target service screen displays.



4. Click the **Enable iSCSI support** check box and click the **Apply** button.

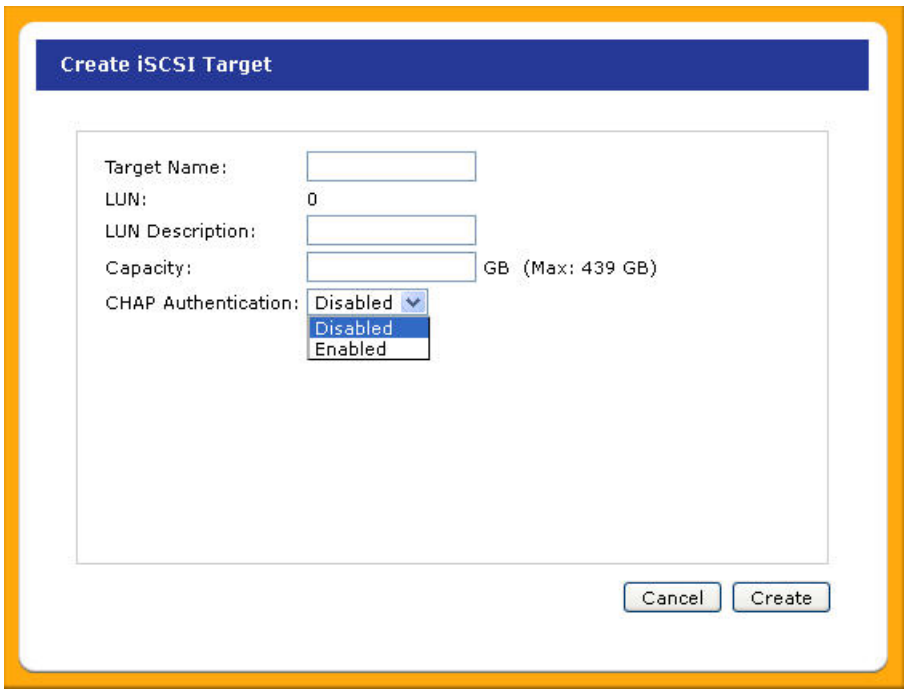
   The screen refreshes.

5. (Optional) Click the **Use ISNS** check box.

   Most home users do not have an Internet Storage Naming Server, which is required to use ISNS.

6. Click the **Create iSCSI Target** button.

   The Create iSCSI Target dialog box displays.



7. Complete the fields as follows:
   - **Target Name**. Required.
   - **LUN Description**. Optional.
   - **Capacity**. Required.
   - **CHAP Authorization**. Default is to disable to CHAP authorization. Select **Enabled** to require CHAP authorization to access this iSCSI target.
8. Click the **Create** button.

   The iSCSI target service screen refreshes showing the newly created iSCSI target.

Manage iSCSI Targets

You can use FrontView to manage the iSCSI targets you create on your ReadyNAS system. You can add a LUN to a target, modify a target, or modify a LUN within a target.

Add a LUN to an iSCSI Target

LUNs can help you fine-tune access to your iSCSI targets. They can also help you more precisely control which part of an iSCSI target is used in backup and recovery jobs.

➢ **To add a LUN to an iSCSI targets:**

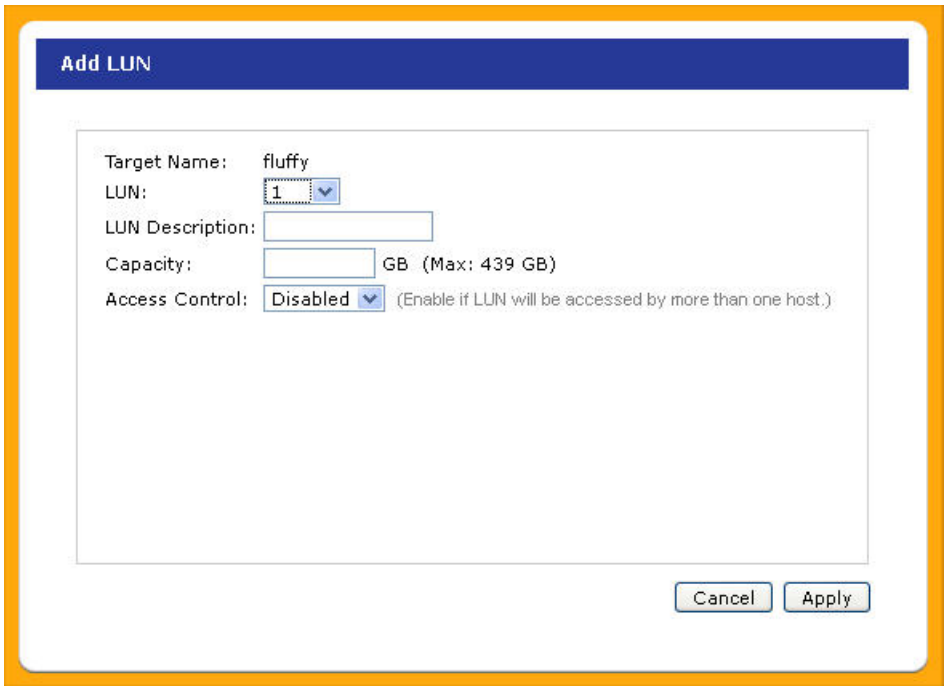
1. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings Screen displays.
2. Click the **iSCSI** tab.

   The iSCSI target service screen displays.
3. Scroll down to the section of the screen that shows your iSCSI targets.

4. In the row for the target that you want to manage, click the **+LUN** button to assign another LUN to this target.

   The Add LUN dialog box displays.



5. Complete the fields as follows:
   - **Target Name**. Required.
   - **LUN Description**. Optional.
   - **Capacity**. Required.
   - **Access Control**. Optional.
6. Click the **Apply** button.

   The LUN is created and the iSCSI target service screen refreshes showing the newly created LUN in the iSCSI target.

   The first LUN that you create is always LUN 0, and it cannot be assigned a different number.

Modify an iSCSI Target

You can use FrontView to modify an iSCSI target on your ReadyNAS system, or to modify a LUN within an iSCSI Target.

You cannot change the number assigned to LUN 0.

➢ **To modify an iSCSI target:**

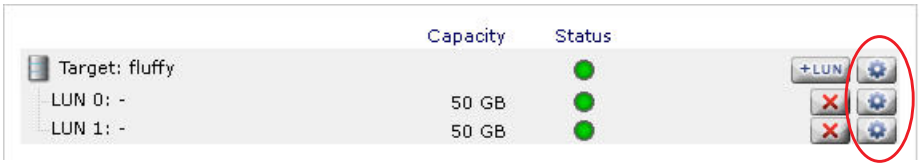
1. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings Screen displays.

2. Click the **iSCSI** tab.

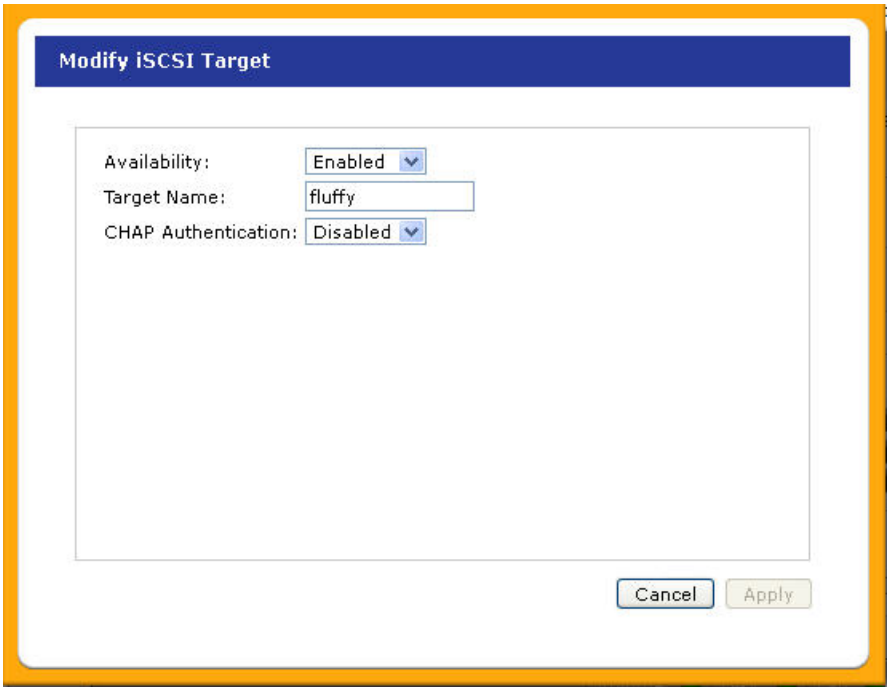
   The iSCSI target service screen displays.

3. Scroll down to the section of the screen that shows your iSCSI targets.



4. (Optional) In the row for the target that you want to manage, click a modify icon.

   The Modify iSCSI Target dialog box displays.

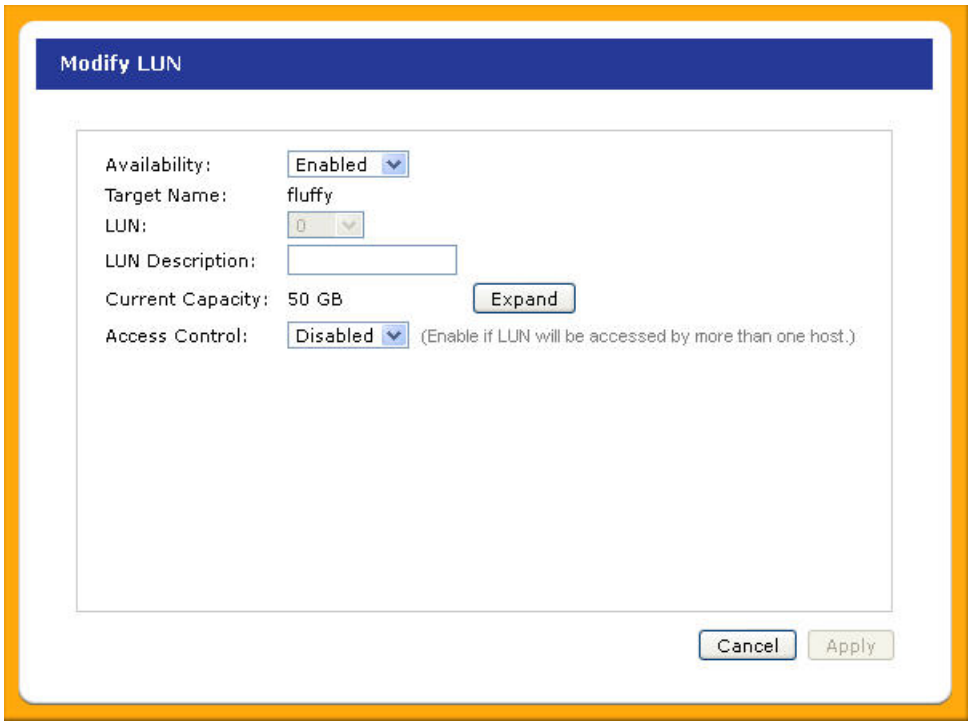


5. (Optional) Edit the options as needed and click the **Apply** button.

   Your settings are saved and the iSCSI target service screen refreshes.

6. (Optional) In the row for the target and LUN combination that you want to manage, click the modify icon.

   The Modify LUN dialog box displays.



   If you are modifying LUN 0, you cannot change the LUN number.

7. (Optional) Edit the options and click the **Apply** button.

   Your settings are saved and the iSCSI target service screen refreshes.

Delete a LUN

You can delete any LUN other than LUN 0 individually. If you delete LUN 0, the entire target and all LUNS within it are deleted. This is because LUN 0 is required for any iSCSI target.

WARNING!

When you delete a LUN, you permanently erase all data stored on that LUN.

This procedure describes how to delete LUNs other than LUN 0.

➢ **To delete a LUN:**

1. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings Screen displays.

2. Click the **iSCSI** tab.

   The iSCSI target service screen displays.

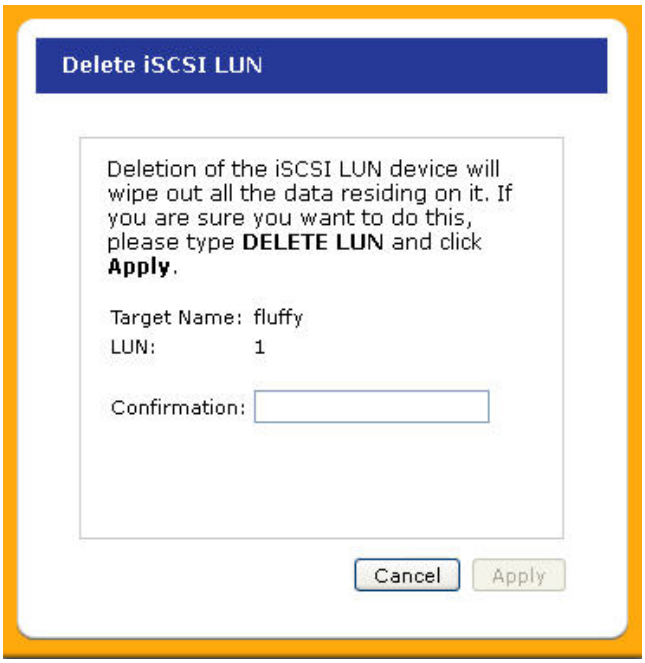
3. Scroll down to the section of the screen that shows your iSCSI targets.

4. In the row for the LUN that you want to delete, click a delete icon.

WARNING!

Do not click the delete icon for LUN 0. If you do, you start the process of deleting the entire iSCSI target.

The Delete iSCSI LUN dialog box displays.



5. Enter **DELETE LUN** in the **Confirmation** field and click the **Apply** button.

   The LUN is deleted and all data stored on the LUN is erased.

Delete an iSCSI Target

To delete an entire iSCSI target, delete the target's LUN 0.

WARNING!

When you delete an iSCSI target, you permanently erase all data stored on that iSCSI target.

➢ **To delete an iSCSI target:**

1. Select **Volume > Volume Settings** from the FrontView main menu.

   The Volume Settings Screen displays.

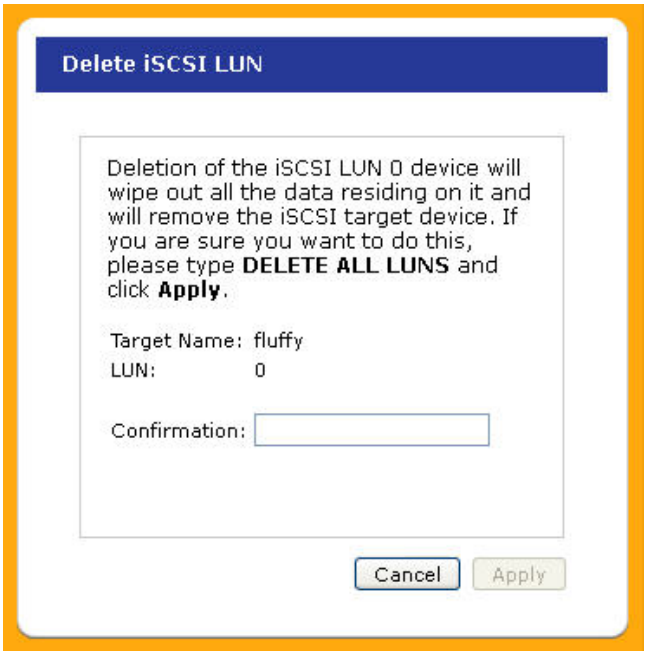
2. Click the **iSCSI** tab.

   The iSCSI target service screen displays.

3. Scroll down to the section of the screen that shows your iSCSI targets.

4. In the row for the LUN 0, click the delete icon.

   The Delete iSCSI LUN dialog box displays.



5. Enter **DELETE ALL LUNS** in the **Confirmation** field and click the **Apply** button.

   The iSCSI target is deleted and all data stored in the LUN is erased.

Connect to an iSCSI Target

You can use an iSCSI initiator on your server, PC, or Mac to connect to a LUN within an iSCSI target and make use of the connection just as you would a local hard disk drive.

➢ **To connect to an iSCSI target:**

1. Determine if your server, PC, or Mac has an iSCSI initiator, and if it does not, download and install one.

   If your computer uses OS X or Windows XP, your operating system does not come with an iSCSI initiator and you need to download and install one if you have not previously done so. If your computer uses Windows Vista or Windows 7, your operating system has an iSCSI initiator already installed.

   For more information, see the documentation that came with your operating system.

2. Configure the iSCSI initiator so that it can find your ReadyNAS system by providing your ReadyNAS system's IP address or hostname.

   For more information, see the documentation that came with your iSCSI initiator.

3. If required by the iSCSI target you want to access, provide the CHAP credentials you configured for that target.

   The iSCSI initiator displays a list of available iSCSI targets. If your ReadyNAS system has multiple iSCSI targets, the iSCSI initiator shows only the targets supported by the CHAPS credentials you entered.

   You can interact with the iSCSI targets just like you would a local hard disk drive.

   For more information, see the following articles on ReadyNAS.com:

   - *Access iSCSI target with Windows Vista and 2008 Server*
   - *Access iSCSI target with Mac OS X*

Monitor, Maintain, and Optimize

6

This chapter describes how to maintain your ReadyNAS system and optimize its performance. It contains the following sections:

- *Monitor*
- *Maintain*
- *Optimize*

Monitor

Use FrontView to monitor the status of your ReadyNAS storage system.

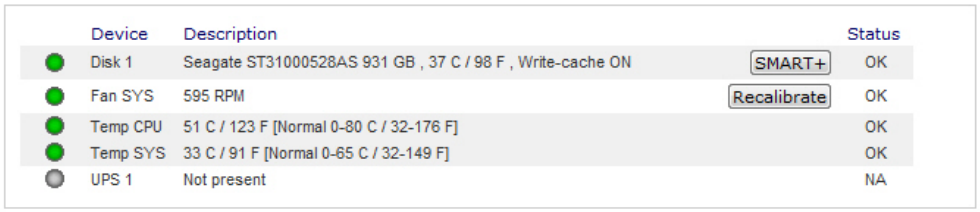
System Health

You can view status details for your ReadyNAS system's disks, fan, temperature, and uninterruptible power supply (UPS) device, if your system is connected to a UPS. When available, normal expected values are provided.

➢ **To view system status:**

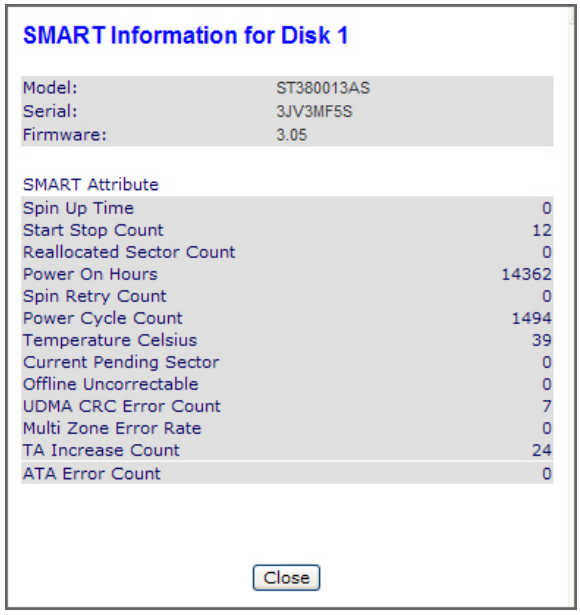
1. Select **Status > Health** from the FrontView main menu.

   The Health screen displays.



2. (Optional) In the row for the disk you want to monitor, click the **SMART+** button.

   That disk's internal disk log displays.



3. (Optional) If your fan seems to be running too much or not enough, click the **Recalibrate** button.

Note: Note this option is not available on all ReadyNAS systems.

The fan is recalibrated. This process takes a few minutes, during which the fan spins up and down. You can continue to use your ReadyNAS system while the fan is recalibrated.

System Logs

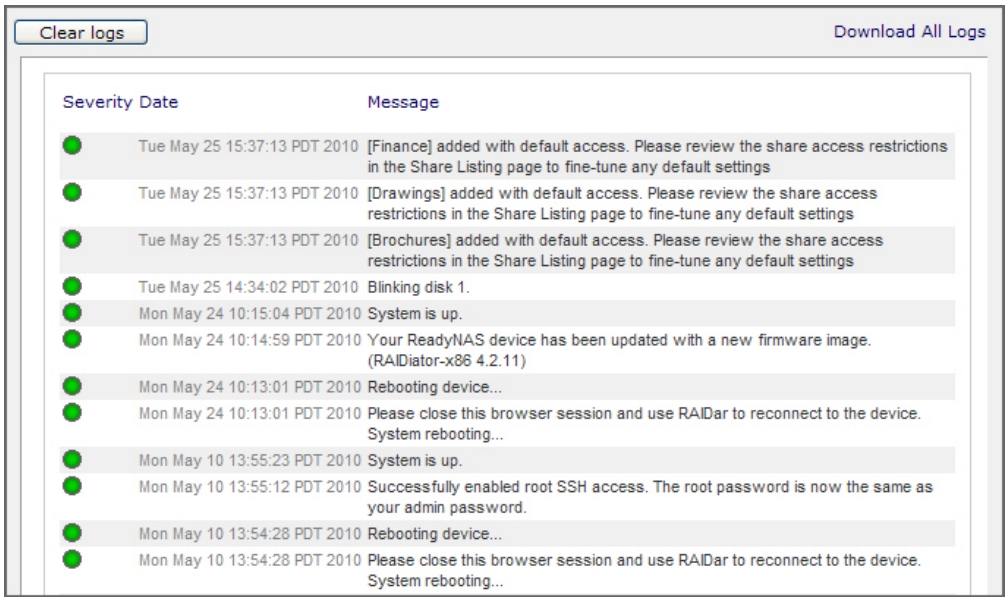
System logs provide information about the status of various system management tasks, including a timestamp. These logs are used primarily to troubleshoot problems. If you call NETGEAR technical support, the representative might ask you to send your system logs.

In addition to system logs, your ReadyNAS storage system also maintains backup logs. For more information, see *View a Backup Log* on page 150.

➢ **To manage system logs:**

1. Select **Status > Logs** from the FrontView main menu.

   The Logs screen displays.



2. (Optional) Click the **Download All Logs** link.

   A .zip file of all logs files is downloaded to your browser's default download location.

3. (Optional) Click the **Clear logs** button.

   The log entries shown on the screen are cleared. Your log files remain intact.

Maintain

Use FrontView to update the firmware on your system, manage power usage, and manage UPS devices.

Firmware

Firmware is the software that operates your ReadyNAS storage system. It is written directly to your system's read-only memory. NETGEAR periodically releases firmware updates to improve your storage system. Because firmware is stored in read-only memory, updating the firmware requires a special process.

The firmware on your ReadyNAS system is called RAIDiator, and your system uses the 4.2 version of RAIDiator. Updates are numbered chronologically, for example:

- RAIDiator 4.2.16
- RAIDiator 4.2.17

You can update the firmware on your ReadyNAS system remotely from the NETGEAR website, or manually from a local drive. The update process changes only the firmware; it does not modify your data.

NETGEAR recommends that you back up your data, especially data that cannot be replaced, before you perform a firmware update.

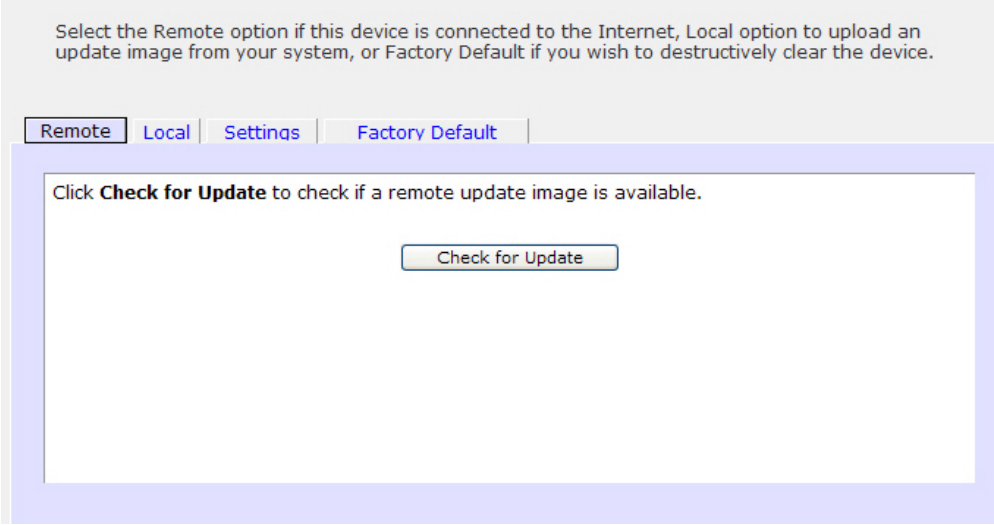
Update Firmware Remotely

If your ReadyNAS system has Internet access, this remote method is easiest.

➢ **To update firmware remotely:**

1. Select **System > Update** from the FrontView main menu.

   The Update screen displays.



Note: If you have not registered your ReadyNAS system, you are prompted to register it. For more information, see *Register Your System* on page 9. If you want to update your system now, click the **Register** button. To continue with the firmware update process, click the **Later** button. The Update screen displays.

2. Click the **Check for Update** button.

   If no firmware update is available, you are notified that your system has the most current firmware.

   If a firmware update is available, you are prompted to update your system.

3. If a firmware update is available, click the **Perform System Update** button.

   WARNING!

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

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

4. Reboot your system.

   If you enabled email alerts, your ReadyNAS system sends a message when the firmware update is complete.

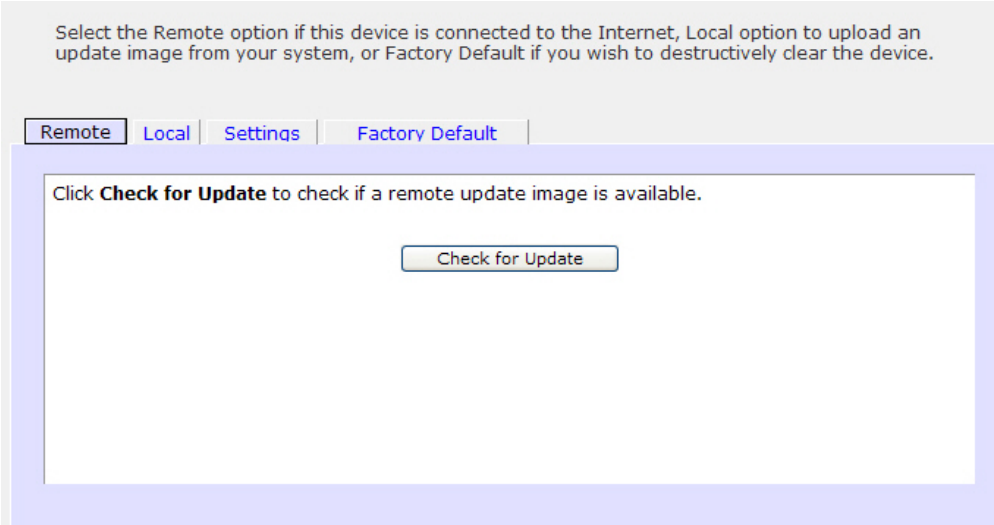
Update Firmware Locally

If you keep your ReadyNAS system in a place that does not have Internet access, for example, at a remote vacation cabin, you must update your firmware locally.

➢ **To update firmware locally:**

1. Using a computer that has Internet access, download the latest firmware for your system from *http://readynas.com/downloads* to a USB drive or other transfer medium.
2. Select **System > Update** from the FrontView main menu.

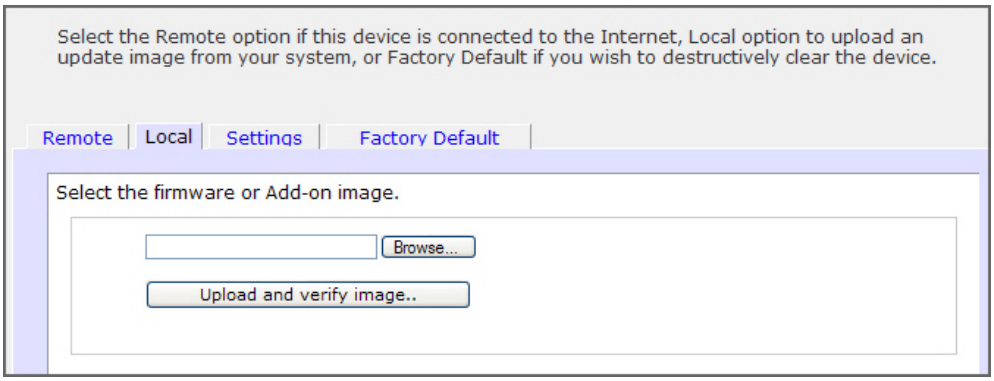
   The Update screen displays.



> **Note:** If you have not registered your ReadyNAS system, you are prompted to register it. For more information, see *Register Your System* on page 9. If you want to update your system now, click the **Register** button. To continue with the firmware update process, click the **Later** button. The Update screen displays.

3. Click the **Local** tab.

   The Local screen displays.



4. Click the **Browse** button.

   A pop-up window displays prompting you to find the firmware file.

5. Navigate to the file containing the firmware update and click the **Open** button.
6. Click the **Upload and verify image** button.

   The firmware file uploads to your ReadyNAS system.
7. When prompted, click the **Perform System Update** button.

   You are prompted to reboot your ReadyNAS system to complete the firmware installation.
8. Reboot your ReadyNAS system.

   If you enabled email alerts, your ReadyNAS system sends a message when the firmware update completes.

Firmware Update Settings

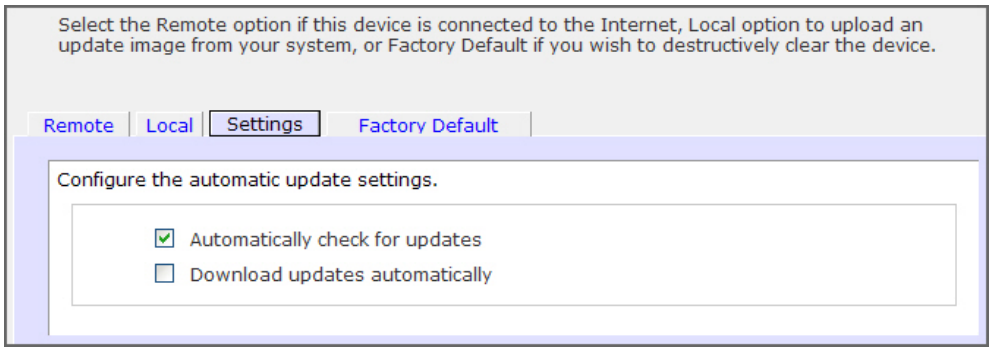
You can configure FrontView to automatically check for and download firmware updates.

➢ **To manage firmware update settings:**

1. Select **System > Update** from the FrontView main menu.

   The Update screen displays.
2. Click the **Settings** tab.

   The Settings screen displays.



3. Check or clear the **Automatically check for updates** check box.

   If you enable this option, your ReadyNAS system checks weekly for firmware updates, and if it finds one, sends an email message to the system administrator if email alerts are enabled.
4. Check or clear the **Download updates automatically** check box.

   If you enable this option, your ReadyNAS system automatically downloads any firmware update and installs it the next time you reboot your ReadyNAS storage system.
5. Click the **Apply** button.

   Your settings are saved.

Power Usage

You can configure settings on your ReadyNAS system to reduce power usage and manage a UPS.

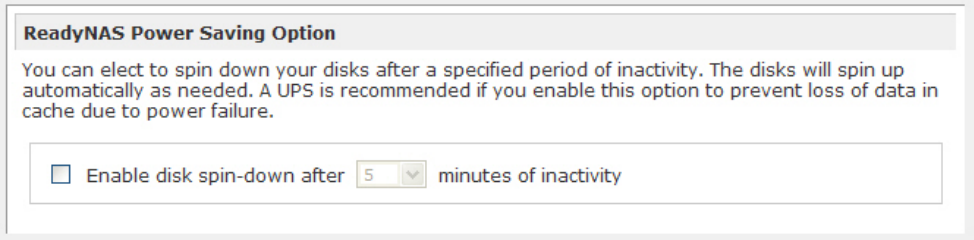
Enable Spin-Down Mode

To reduce power consumption, configure your ReadyNAS system to spin down the disks after a specified time of inactivity. The disks will spin when needed.

➢ **To enable spin-down mode:**

1. Select **System > Power** from the FrontView main menu.

   The Power screen displays.



2. In the ReadyNAS Power Saving Option pane, select the **Enable disk spin-down after** check box.
3. Using the drop-down list, specify the number of minutes of inactivity that triggers disk spin-down.
4. Click the **Apply** button.

   Your settings are saved.

Enable the Power Timer

You can configure your ReadyNAS system to power itself on and off automatically according to a schedule. Note that if you schedule this device to power off, data transfers will be interrupted and pending backup jobs will not run.

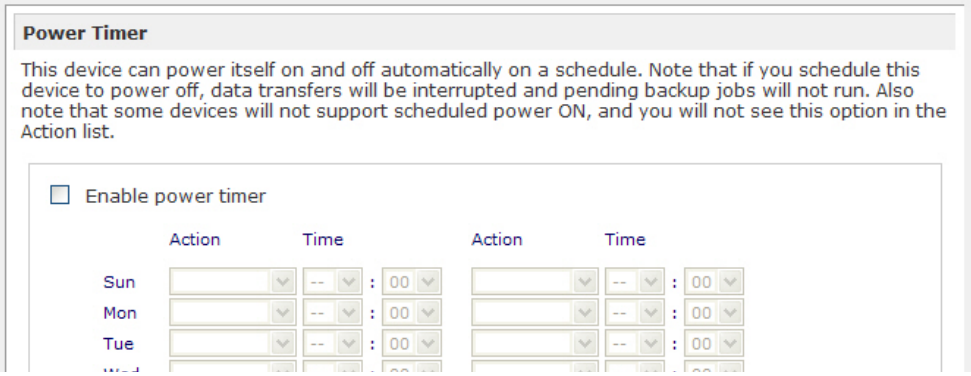
Not all ReadyNAS systems support this feature. If your system does not, the Power On option does not display in the Action list.

➢ **To enable the power timer:**

1. Select **System > Power** from the FrontView main menu.

   The Power screen displays.

   Scroll down to the Power Timer pane.



2. Select the **Enable power timer** check box.

   The drop-down lists become active.

3. Use the drop-down lists to configure when your ReadyNAS system powers itself off and powers itself back on.
4. Click the **Apply** button.

   Your settings are saved.

Connect to a UPS

Connecting your ReadyNAS storage system to an uninterruptible power supply (UPS) device is an easy way to protect against data loss due to power failures.

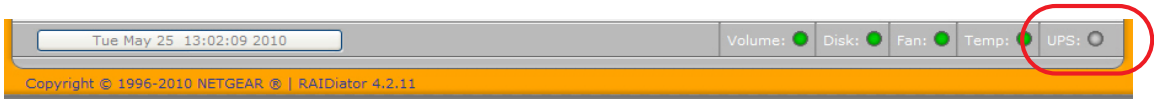
If you set up email notifications, your ReadyNAS system sends you an email alert message whenever the UPS status changes. For example, if a power failure forces the UPS into battery mode, or when the battery is low, you receive an email message. When the battery is low, your ReadyNAS system automatically shuts down safely.

➢ **To connect your ReadyNAS system to a UPS:**

1. Connect the ReadyNAS power cable to the UPS.
2. Connect the UPS USB monitoring cable to a USB port on your ReadyNAS system.

   FrontView detects compatible UPS units automatically and displays information about the UPS on the status bar.

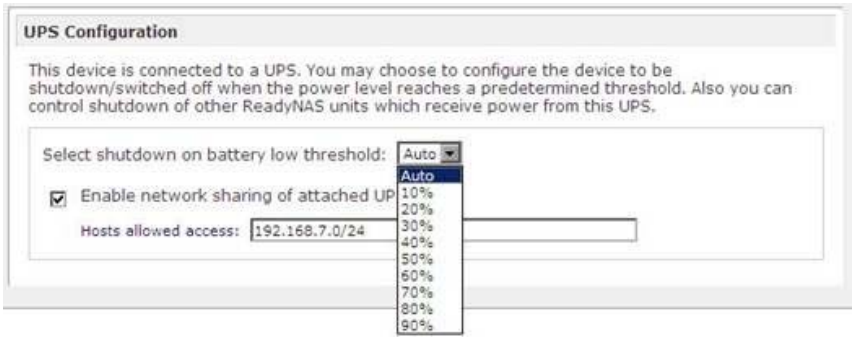
   For a list of compatible UPS units, see the hardware compatibility list at *http://www.readynas.com/?page_id=92*.



3. (Optional) Hover your cursor over the status light to display more details.
4. (Optional) If you have an APC brand UPS unit, you can configure the low battery threshold at which automatic shut down occurs:
   a. Select **System > Power** from the FrontView main menu.

      The Power screen displays.

   b. Scroll down to the UPS Configuration pane.



   c. From the **Select shutdown on battery low threshold** drop-down menu, select a battery low threshold.

      This option does not display if you connect a UPS device that is not made by APC.

   d. Click the **Apply** button.

      Your settings are saved.

Configure Remote UPS Low Battery Shutdown

You can monitor a UPS that is not directly connected to your ReadyNAS system in two ways:

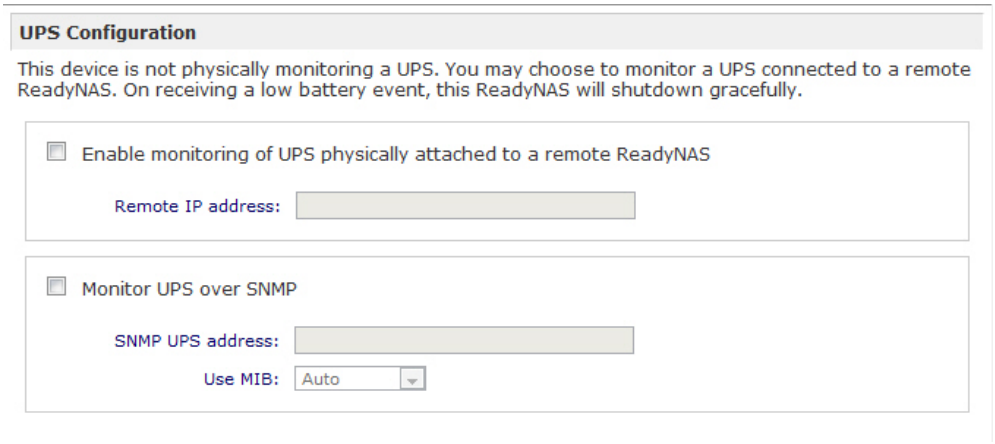
- **Monitor a UPS connected to another ReadyNAS system on your LAN**. If this ReadyNAS system is not connected to a UPS device and you have more than one ReadyNAS system, you can enable a UPS connection to another ReadyNAS device. If you use this option, the ReadyNAS system gracefully shuts down automatically when a low battery condition is detected on a UPS connected to another ReadyNAS. This is useful when a UPS is shared by multiple ReadyNAS systems, even though only one ReadyNAS system is monitoring the battery status.
- **Monitor a SNMP UPS on your LAN**. If your ReadyNAS unit is connected to a LAN that has an SNMP UPS, you can configure your ReadyNAS system to shut down automatically when a low battery condition is detected.

In the following procedure, the remote ReadyNAS system is the system that has the UPS directly connected to it. The local ReadyNAS system is the system that does not have a UPS directly connected to it.

➢ **To configure remote UPS low battery shutdown:**

1. Ensure that the remote ReadyNAS system is configured to allow remote UPS monitoring:
   a. On the remote ReadyNAS system, select **System > Power** from the FrontView main menu.
   b. Scroll down to the UPS Configuration pane.
   c. Click the **Enable network sharing of attached UPS** check box.
   d. Choose an access restriction option, as follows:
      - Leave the **Hosts allowed access field** blank to allow any system on you LAN to share this UPS.
      - Enter the IP address of the local ReadyNAS system in the **Hosts allowed access field** to restrict sharing of this UPS to only that ReadyNAS system.
   e. Click the **Apply** button.
2. On your local ReadyNAS system, select **System > Power** from the FrontView main menu.

   The Power screen displays.
3. Scroll down to the UPS Configuration pane.



4. (Optional) Select the **Enable monitoring of UPS physically attached to a remote ReadyNAS** check box and enter the IP address of the remote ReadyNAS system in the Remote IP address field.
5. (Optional) Select the **Monitor UPS over SNMP** check box, enter the SNMP UPS address, and choose an option from the **Use MIB** drop-down list.

   For more information about MIB settings, see the documentation that accompanied your SNMP UPS.
6. Click the **Apply** button.

   Your settings are saved.

Enable Wake-on-LAN

Wake-on-LAN is a way to remotely power up a network-attached device, like a computer or storage system. This allows you to conserve power by keeping a device turned off when it is not needed, but allows a remote system to turn it on when it is needed.

Wake-on-LAN works when one network-attached device sends a signal, called a magic packet, to another network-attached device. If wake-on-LAN is enabled in the target device, the packet signals the device to power up.

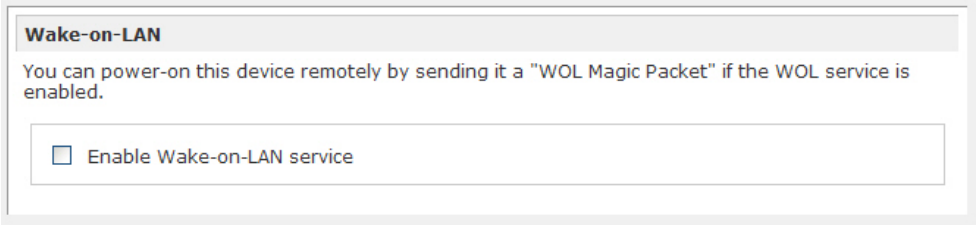
Your ReadyNAS system supports wake-on-LAN on the first Ethernet port (LAN 1) only.

➢ **To enable wake-on-LAN:**

1. Select **System > Power** from the FrontView main menu.

   The Power screen displays.

2. Scroll down to the Wake-on-LAN pane.



3. Select the **Enable Wake-on-LAN service** check box.
4. Click the **Apply** button.

   Your settings are saved.

Volume Maintenance

Volume maintenance helps you enforce high availability. It also helps you detect disk errors.

➢ **To perform volume maintenance:**

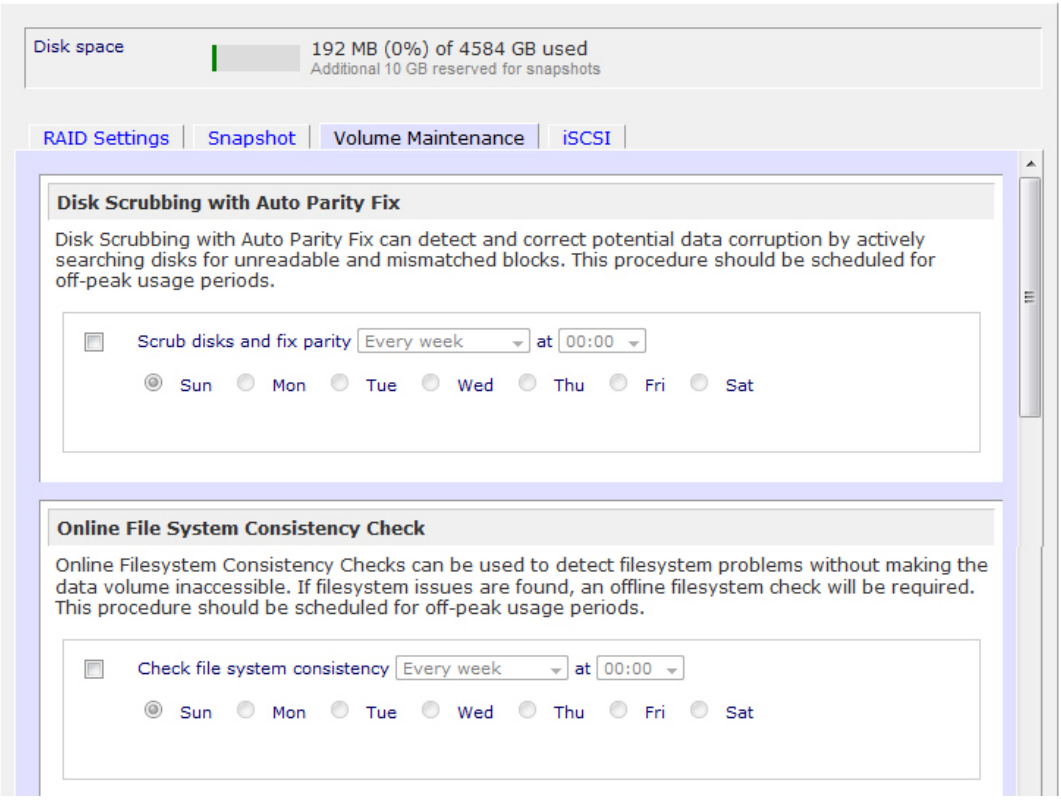
1. Select **Volumes > Volume Settings** from the FrontView main menu.

   The RAID Configuration screen displays.

2. Click the **Volume Maintenance** tab.

   You must have at least two disks installed in your ReadyNAS system for this tab to display.

   The Volume Maintenance screen displays.



3. (Optional) Select the **Disk Scrubbing with Auto Parity Fix** check box and use the drop-down lists and radio buttons to establish a schedule.

   This operation detects and corrects potential data corruption by actively searching disks for unreadable and mismatched blocks. Schedule this operation for off-peak usage periods.

4. (Optional) Select the **Online File System Consistency Check** check box and use the drop-down lists and radio buttons to establish a schedule.

   This operation detects file system problems without making the data volume inaccessible. If file system issues are found, an offline file system check will be required. Schedule this operation for off-peak usage periods.

5. Click the **Apply** button.

   Your settings are saved.

Optimize

Use FrontView to tune your ReadyNAS storage system for better performance.

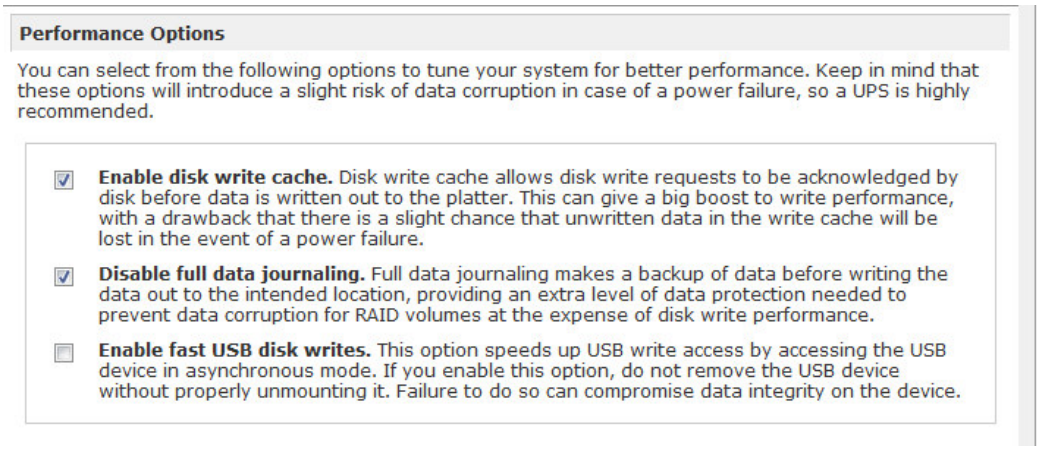
System Performance

Enabling system performance optimization options can introduce a slight risk of data corruption if you experience a power failure. NETGEAR recommends connecting your ReadyNAS storage system to a UPS if you enable these settings.

➢ **To optimize system performance:**

1. Select **System > Performance** from the FrontView main menu.

   The Performance Options screen displays.



2. (Optional) Select the **Enable disk write cache** check box.

   Enabling this option allows disk write requests to be acknowledged by the disk before data is written to the disk. This can give a big boost to write performance; however, this option introduces the slight risk that unwritten data in the write cache will be lost if power fails.

3. (Optional) Select the **Disable full data journaling** check box.

   Disabling 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.

4. (Optional) Select the **Enable fast USB disk writes** check box.

   Enabling this option speeds USB write access by accessing the USB device in asynchronous mode. If you enable this option, never remove the USB device without correctly unmounting it. Incorrectly removing your USB device when this option is enabled can cause data on the USB device to become corrupted.

5. Click the **Apply** button.

   Your settings are saved.

Jumbo Frames

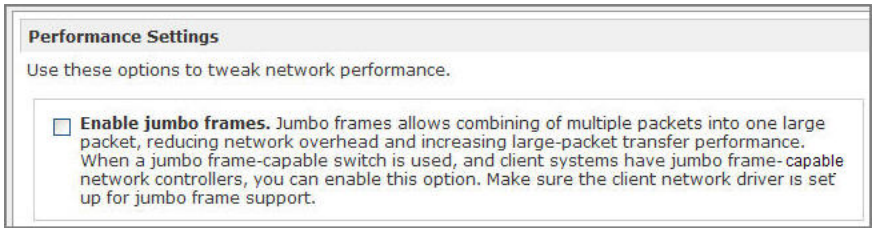
You can enable the use of jumbo frames on your ReadyNAS storage system to optimize it for large data transfers. Use this option only if your network interface card (NIC) and your switch support jumbo frames. Your ReadyNAS system supports a maximum frame size of 9000 bytes. You must use a switch capable of this frame size or larger.

➢ **To enable jumbo frames:**

1. Select **Network > Interfaces** from the FrontView main menu.

   The Network Standard Setting screen displays.

2. Scroll down to the Performance Settings pane.



3. Select the **Enable jumbo frames** check box.
4. Click the **Apply** button.

   Your settings are saved.

7. Backup and Recovery

If your data is important enough to store, it is important enough to back up. Data can be lost due to a number of events, including natural disaster (for example, fire or flood), theft, improper data deletion, and hard drive failure. By regularly backing up your data, you can recover your data if any of these happen to you.

Businesses sometimes use backup data to comply with data retention regulations and to archive information before making major changes to their IT environments, such as batch updates to databases. Both home and business users should back up important data that might be lost due to a natural disaster or the loss of a device that stores data.

This chapter includes the following sections:

Basic Backup Concepts

A *backup* is a copy of data that you use if your primary copy is deleted or damaged. The process of storing primary data on a second device is called *backing up*.

The process of restoring backed-up data to the device where the primary copy is kept is called *recovery*.

A *full backup* makes a copy of all of the data stored on the primary system. Your first backup of a primary system is always a full backup job. The length of time a full backup takes depends on the amount of stored data.

An *incremental backup* copies only the data that has changed since your last backup process. An incremental backup job takes much less time than a full backup job.

Note: RAID configuration of disks is not a substitute for backing up data. RAID configuration protects you only from data loss in the event that a disk fails. For more information about the protection that RAID configuration offers, see *RAID* on page 17.

Backup and Recovery Roles

A *backup source* is the place that data that is being backed up is primarily stored. A *backup destination* is the place where the backed-up data is stored. If you need to recover your data, the backup target becomes the recovery job source.

Your ReadyNAS system can manage backup and recovery processes for many devices on your network. For example, you can back up data that is stored on your ReadyNAS storage system to other devices, for example, a USB drive.

Figure 4 shows the roles that devices play when you back up data that is stored on your ReadyNAS system to another device, and when you return that data to the ReadyNAS system with a recovery process.

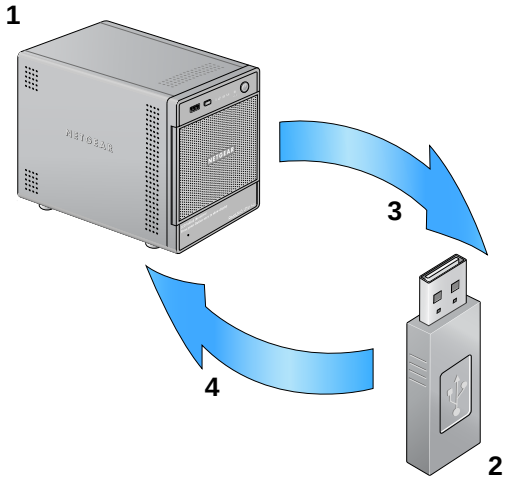


Figure 4. Using a device to back up and recover data stored on a ReadyNAS system

1. ReadyNAS storage system serving as backup source and recovery destination
2. USB drive serving as backup destination and recovery source
3. Backup process
4. Recovery process

The backup process illustrated in *Figure 4* is described in *Back Up Data Stored On Your ReadyNAS System* on page 130.

The recovery process illustrated in *Figure 4* is described in *Recover Data to Your ReadyNAS System* on page 134.

You can also use your ReadyNAS storage system to store backed-up data from other devices, like your laptop.

Figure 5 shows the roles that devices play when you back up data that is stored on a device, for example, a laptop computer, to your ReadyNAS system, and the roles that devices play when you return that data to that device with a restore process.

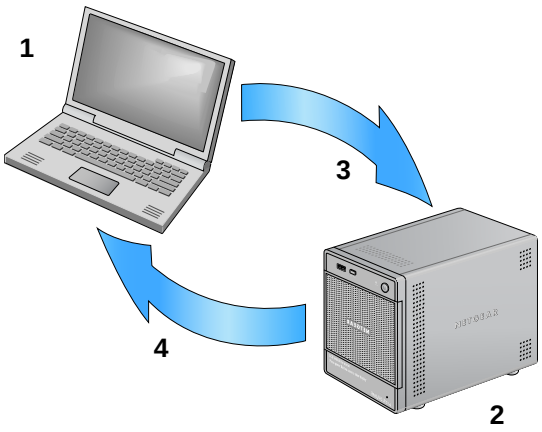


Figure 5. Using a ReadyNAS system to back up and recover data stored on a laptop computer

1. Laptop computer serving as backup source and recovery destination
2. ReadyNAS storage system serving as backup destination and recovery source
3. Backup process
4. Recovery process

The backup process illustrated in *Figure 5* is described in *Back Up Data Stored on a Network-Attached Device* on page 139.

The recovery process illustrated in *Figure 5* is described in *Recover Data to a Network-Attached Device* on page 143.

Backup Protocols

Because backup and recovery jobs are transfers of data over a network, file-sharing protocols are used for backup and recovery jobs. For more information about file-sharing protocols used by your ReadyNAS storage system, see *Streaming Services* on page 95.

Your ReadyNAS system supports full backups using the FTP and HTTP protocols, and full and incremental backups using the CIFS (SMB), NFS, and Rsync protocols.

Back Up Data Stored On Your ReadyNAS System

You can use FrontView to back up data that is stored on your ReadyNAS to another network-attached device.

Figure 6 illustrates the backup process described in this section.

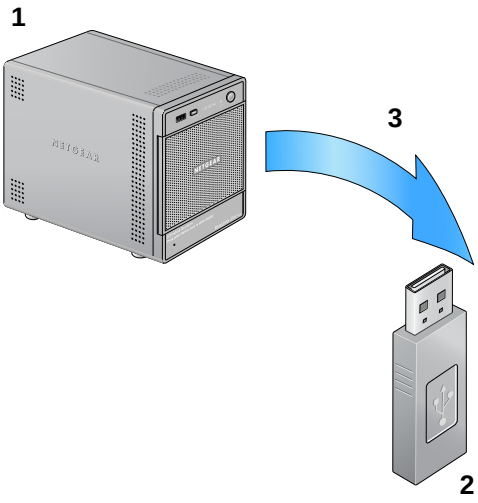


Figure 6. Backing up data from a ReadyNAS system to a USB drive

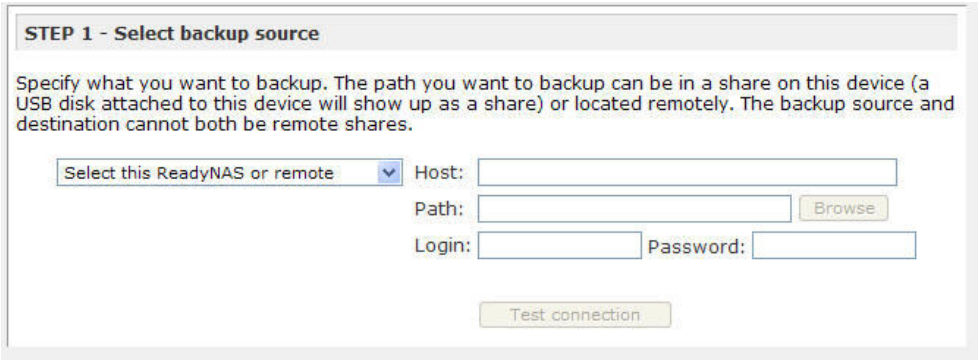
1. ReadyNAS system serving as backup source
2. USB drive serving as backup destination
3. Backup process

Backup and recovery jobs ReadyNAS Vault and Time Machine require different procedures. For more information, *ReadyNAS Vault* on page 153 or *Time Machine* on page 154.

➢ **To back up data stored on your ReadyNAS system:**

1. Select **Backup > Add a New Backup** from the FrontView Main menu.

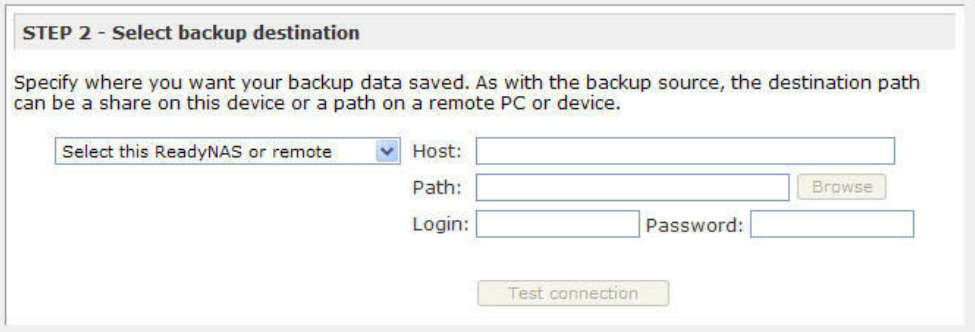
   The Add a New Backup Job screen displays.



2. From the drop-down list in the STEP 1 - Select backup source pane, select a backup source from your ReadyNAS system.

   Depending on how your ReadyNAS system is configured, these options vary. If you have previously created one or more iSCSI targets on your ReadyNAS system, you can choose an iSCSI target as your backup source. For more information about creating and managing iSCSI targets, see *iSCSI Targets* on page 102.

3. From the drop-down menu in the STEP 2 - Select a backup destination pane, select a backup destination that is not part of your ReadyNAS system.



   Depending on how your network is configured, these options vary. Select USB device that is attached to your ReadyNAS system or a remote location.

4. If necessary, enter the remote host name, the folder path, and any login credentials required to access that path.

   If you select a backup destination that requires a path, use a forward slash (/) to separate directories, for example:

   /<share name>/<folder name>

   Do not use a backslash (\) in paths.

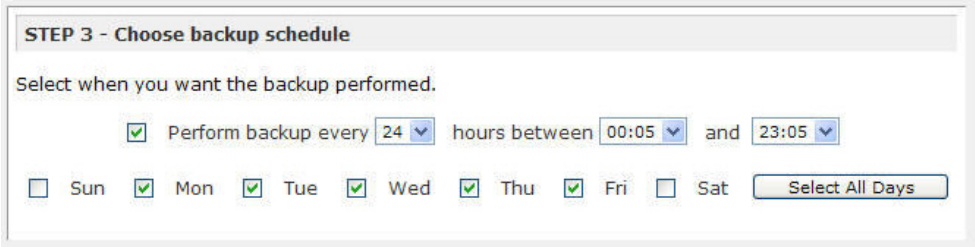
   If you select a a USB device that is connected to your ReadyNAS system, you can leave the path blank to put the data at the top level of the USB device's directory, or enter a folder path to place the backed-up data in a specific folder.

   If you select a remote Rsync server, you must enter the Rsync server's host name and a path. Depending on how the Rsync server is configured, you might need to enter a user name and password. Whether or not you need to enter login credentials depends on how the Rsync server is configured. For more information, contact the Rsync server's system administrator.

5. (Optional) To ensure that you are able to access the remote backup destination, click the **Test connection** button.

   A pop-up window displays indicating whether you can access the destination.

6. From the STEP 3 - Choose backup schedule pane, determine whether this backup job will run automatically or whether it must be started manually, as follows:



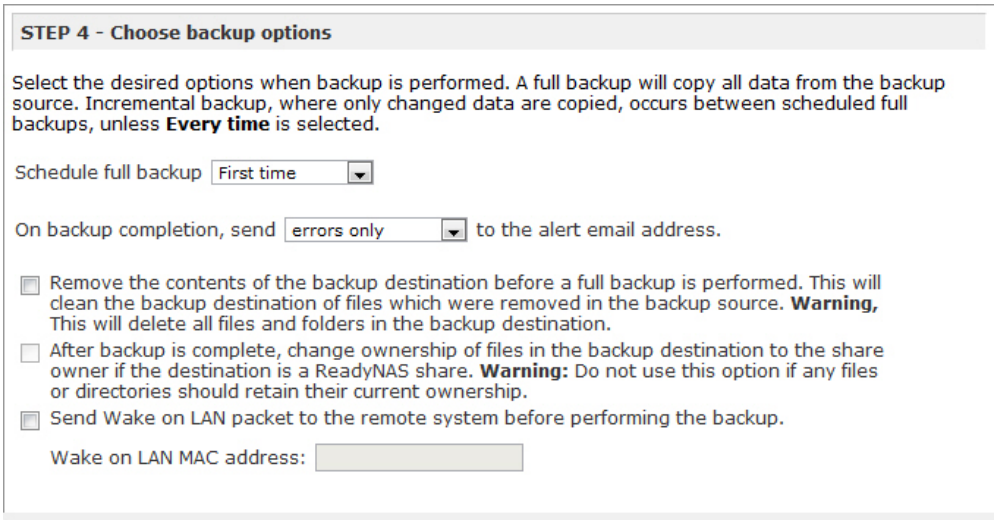
- **Run backup job automatically**. Select the **Perform backup every** check box and use the day check boxes and time drop-down lists to create a backup schedule.

  Backups can occur as frequently as every 4 hours. You can also set them to run daily or one time each week. The time settings determine when the backup job starts. Depending on the size of the backup job, it might not finish by the later time setting.

  The backup schedule is offset by 5 minutes from the hour.

- **Require backup job to be started manually**. Clear the **Perform backup every** check box.

7. Using the drop-down lists and check boxes in the Step 4 - Choose backup options pane, configure backup options:



a. Choose an option from the **Schedule a full backup** drop-down list.

   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.

   When you backup your ReadyNAS system to a website or FTP site, you can only do a full backup every time.

b. Using the **On backup completion, send** drop-down list, choose what type of logs to send when the backup job completes.

You can send a log that lists only errors encountered during backup, full backup logs consisting of file listings (can be large), or status and errors (status refers to completion status).

Backup log emails are restricted to approximately 10,000 lines. For more information about viewing full backup logs, see *Manage Backup Jobs* on page 147.

c. (Optional) Select the **Remove files from backup destination** check box.

Select this check box if you want to erase the destination path contents before the backup is performed.

WARNING!

When using this option, ensure that you have correctly identified your backup source and backup destination. If you reverse them, you might permanently delete your source files. NETGEAR recommends not enabling this option unless your destination device is very low on storage space.

Best practice is to experiment with this option using a test share to make sure that you understand how it works.

d. (Optional) Select the **Change ownership of backup files** check box.

Your ReadyNAS system attempts to maintain original file ownership whenever possible. However, you can automatically change 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. (Optional) Select the **Wake-on-LAN** check box and enter the MAC address of destination device.

Use this option whenever the destination device is set to power down automatically. If you do not set this option and the device is powered down when the backup job is scheduled to begin, the backup job might not happen.

If your destination device is set to power down automatically, you must also configure the destination device to accept wake-on-LAN notifications. If you do not configure the destination to accept wake-on-LAN notifications, and it is powered down when the backup job is scheduled to begin, the backup job might fail.

8. Click the **Apply** button.

Your backup job settings are saved and this backup job displays in the backup schedule. For more information about viewing scheduled backup jobs, see *Manage Backup Jobs* on page 147.

If you set a backup schedule for this job in *step 6*, your backup job starts at the date and time you specified.

If you did not set a schedule for this job in *step 6*, you must manually start the backup job by pushing the Backup button on your ReadyNAS unit or by manually starting the backup job using FrontView. For more information about the location of the Backup button on your system, see the appropriate hardware manual. For more information about using FrontView to manually start a backup job, see *Manually Start a Backup Job* on page 150.

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. You can do this after you save the backup job.

Recover Data to Your ReadyNAS System

You can use FrontView to restore data that you previously backed up to another network-attached device to your ReadyNAS storage system.

Before you can recover data, you must first back it up. For more information about backing up data that you store on your ReadyNAS system, see *Back Up Data Stored On Your ReadyNAS System* on page 130.

Figure 7 illustrates the recovery process described in this section.

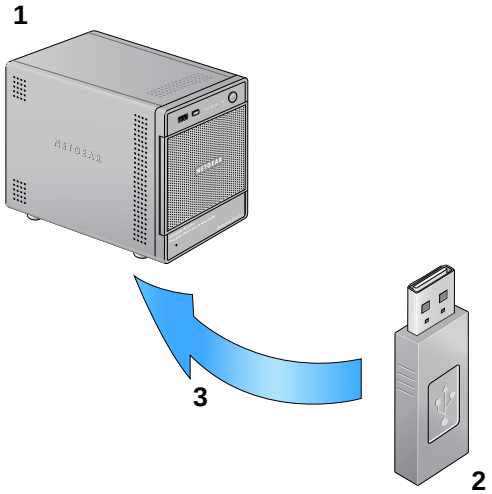


Figure 7. Restoring data from a USB drive to a ReadyNAS system

1. ReadyNAS system serving as recovery destination
2. USB drive serving as recovery source
3. Recovery process

WARNING!

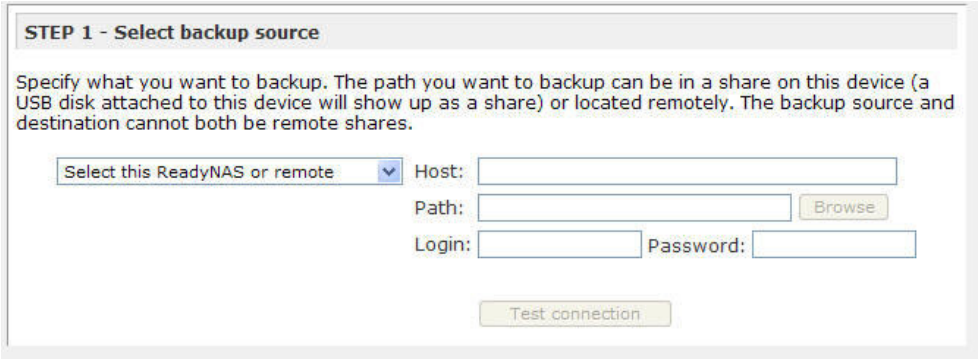
Although this is a recovery procedure, your ReadyNAS system treats it like a backup job. This means that you use FrontView screens labeled *backup* and you reverse the source and destination systems you used when you backed up the data that you are recovering.

Backup and recovery jobs ReadyNAS Vault and Time Machine require different procedures. For more information, *ReadyNAS Vault* on page 153 or *Time Machine* on page 154.

➢ **To recover backup data to your ReadyNAS system:**

1. Select **Backup > Add a New Backup** from the FrontView Main menu.

   The Add a New Backup Job screen displays.



2. From the drop-down list in the STEP 1 - Select backup source pane, select the device where you backed up your ReadyNAS data.

   Depending on how your network is configured, these options vary. Select a USB device that is attached to your ReadyNAS system, or remote location that stores your backed-up ReadyNAS data.

   If you select a recovery source that requires a path, use a forward slash (/) to separate directories, for example:

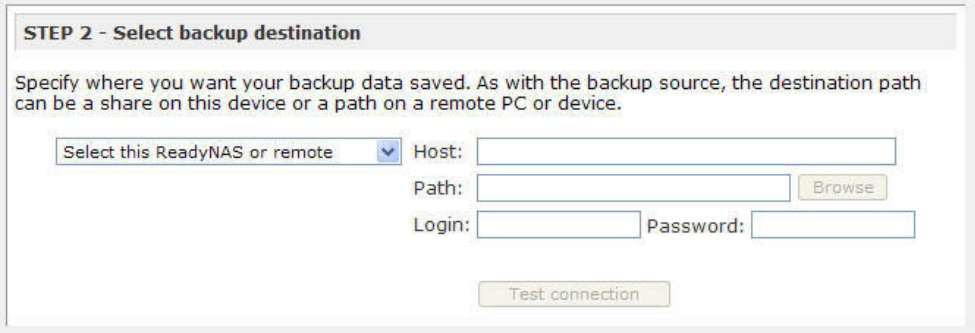
   /<share name>/<folder name>

   Do not use a backslash (\) in paths.

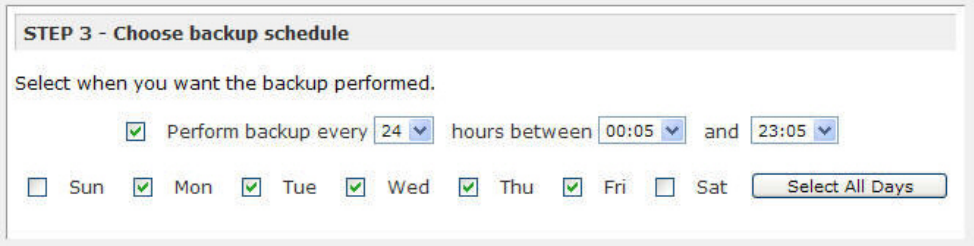
   If you select a remote Rsync server, you must enter the Rsync server's host name and a path. Depending on how the Rsync server is configured, you might need to enter a user name and password. Whether or not you need to enter login credentials depends on how the Rsync server is configured. For more information, contact the Rsync server's system administrator.

3. If necessary, enter the remote host name, the folder path, and any login credential required to access that path.
4. (Optional) To ensure that you are able to access the remote backup destination, click the **Test Connection** button.

   A pop-up window displays indicating whether you can access the destination.
5. From the drop-down menu in the STEP 2 - Select a backup destination pane, select a backup destination that is part of your ReadyNAS system.



   Depending on how your ReadyNAS system is configured, these options vary. You can restore just a share, an entire volume, or multiple volumes. If you have previously created one or more iSCSI targets on your ReadyNAS system, you can restore data to an iSCSI target. For more information about creating and managing iSCSI targets, see *iSCSI Targets* on page 102.
6. From the STEP 3 - Choose backup schedule pane, clear the **Perform backup every** check box.

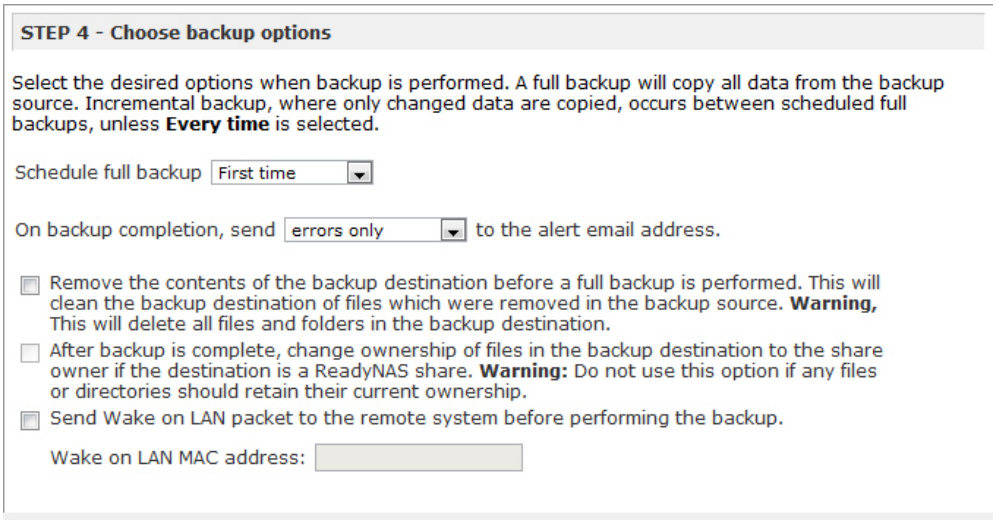


   Clearing this check box forces the recovery procedure to be started manually, which ensures that the recovery job does not happen automatically.

WARNING!

To ensure the integrity of the data stored on your primary device, never automatically schedule a recovery job.

7. Using the drop-down lists and check boxes in the Step 4 - Choose backup options pane, configure backup options:



   a. From the **Schedule a full backup** drop-down list, select **Every Time**.

   b. From the **On backup completion, send** drop-down list, select what type of logs to send when the recovery job completes.

      You can send a log that lists only errors encountered during recovery, full logs consisting of file listings (can be large), or status and errors (status refers to completion status).

      Log email messages are restricted to approximately 10,000 lines. For more information about viewing full logs, see *View a Backup Log* on page 150.

   c. Ensure that the **Remove files from backup destination** check box is clear.

      Selecting this check box erases the destination path contents before the backup is performed, which NETGEAR does not recommend for recovery jobs.

WARNING!

When using this option, ensure that you have correctly identified your backup source and backup destination. If you reverse them, you might permanently delete your source files. NETGEAR recommends not enabling this option unless your destination device is very low on storage space.

Best practice is to experiment with this option using a test share to make sure that you understand how it works.

d. (Optional) Select the **Change ownership of backup files** check box.

Your ReadyNAS system attempts to maintain original file ownership whenever possible. However, you can automatically change 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.

8. Click the **Apply** button.

Your backup job settings are saved and this recovery job displays in the backup schedule as a backup job. Because you did not assign a schedule to it, you must manually start the job.

9. Select **Backup > Backup Jobs** from the FrontView main menu.

The Backup Schedule screen displays.

Each job is assigned a number beginning at 001.

10. Click the **Go** button for this recovery job.

The recovery process begins.

Back Up Data Stored on a Network-Attached Device

You can use your ReadyNAS storage system to back up data that is stored primarily on another network-attached device.

Figure 8 illustrates the backup process described in this section.

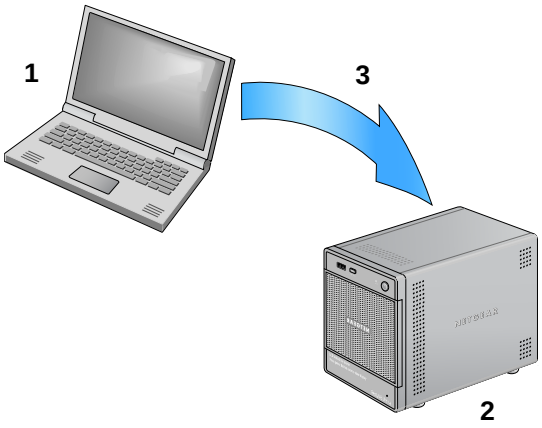


Figure 8. Backing up data from a laptop computer to a ReadyNAS system

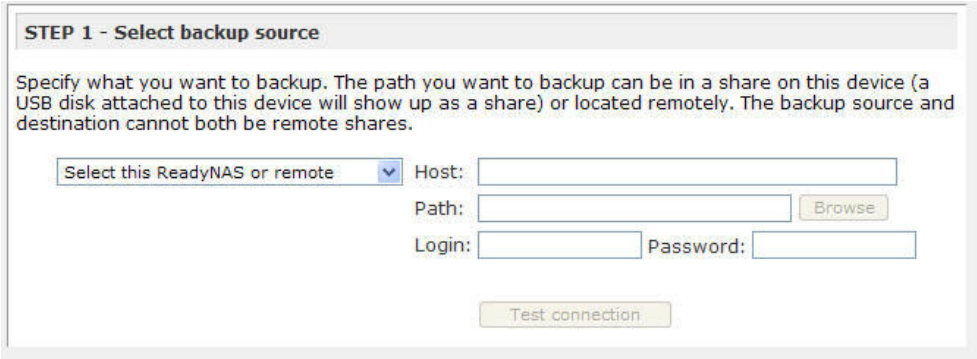
1. Laptop computer serving as backup source
2. ReadyNAS system serving as backup destination
3. Backup process

Backup and recovery jobs ReadyNAS Vault and Time Machine require different procedures. For more information, *ReadyNAS Vault* on page 153 or *Time Machine* on page 154.

➢ **To back up data stored on another network-attached device:**

1. Select **Backup > Add a New Backup** from the FrontView Main menu.

   The Add a New Backup Job screen displays.



2. From the drop-down list in the STEP 1 - Select backup source pane, select a backup source that is not part of your ReadyNAS system.

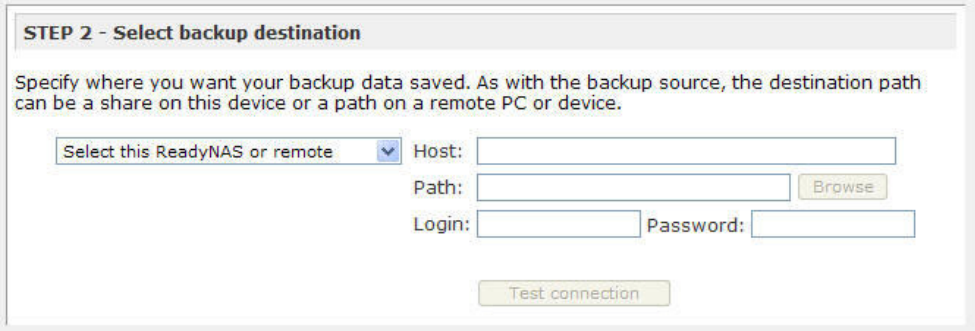
   Depending on how your network is configured, these options vary. Select a USB device that is attached to your ReadyNAS system or a remote location.

   If you select a remote Rsync server, you must enter the Rsync server's host name and a path. Depending on how the Rsync server is configured, you might need to enter a user name and password. Whether or not you need to enter login credentials depends on how the Rsync server is configured. For more information, contact the Rsync server's system administrator.

3. If necessary, enter the remote host name, the folder path, and any login credential required to access that path.
4. (Optional) To ensure that you are able to access the remote backup destination, click the **Test connection** button.

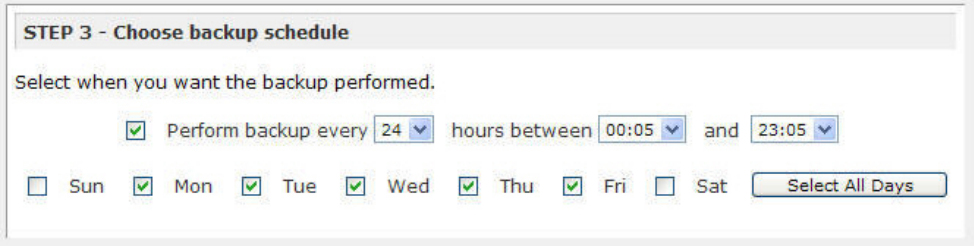
   A pop-up window displays indicating whether you can access the destination.

5. From the drop-down list in the STEP 2 - Select a backup destination pane, select a backup destination that is part of your ReadyNAS system.



   Depending on how your ReadyNAS system is configured, these options vary. Select a share, a volume, or multiple volumes. If you have previously created one or more iSCSI targets on your ReadyNAS system, you can choose an iSCSI target as your backup destination. For more information about creating and managing iSCSI targets, see *iSCSI Targets* on page 102.

6. From the STEP 3 - Choose backup schedule pane, determine whether this backup job will run automatically or whether it must be started manually, as follows:



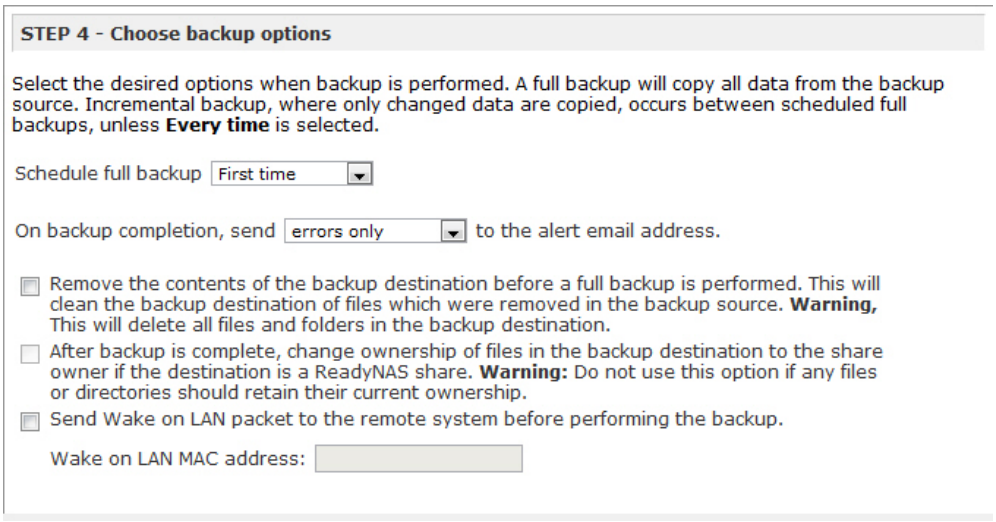
- **Run backup job automatically**. Select the **Perform backup every** check box and use the day check boxes and time drop-down menus to create a backup schedule.

  Backups can occur as frequently as every 4 hours. You can also set them to run daily or one time each week. The time settings determine when the backup job starts. Depending on the size of the backup job, it might not finish by the later time setting.

  The backup schedule is offset by 5 minutes from the hour.

- **Require backup job to be started manually**. Clear the **Perform backup every** check box.

7. Using the drop-down lists and check boxes in the Step 4 - Choose backup options pane, configure backup options:



   a. From the **Schedule a full backup** drop-down list, select an option.

      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 website or FTP site only have the option to do a full backup every time.

   b. Using the **On backup completion, send** drop-down list, select what type of logs to send when the backup job completes.

      You can send a log that lists only errors encountered during backup, full backup logs consisting of file listings (can be large), or status and errors (status refers to completion status).

      Backup log email messages are restricted to approximately 10,000 lines. For more information about viewing full backup logs, see *Manage Backup Jobs* on page 147.

c. (Optional) Select the **Remove files from backup destination** check box.

Select this check box if you want to erase the destination path contents before the backup is performed.

WARNING!

When using this option, ensure that you have correctly identified your backup source and backup destination. If you reverse them, you might permanently delete your source files. NETGEAR recommends not enabling this option unless your destination device is very low on storage space.

Best practice is to experiment with this option using a test share to make sure that you understand how it works.

d. (Optional) Select the **Change ownership of backup files** check box.

Your ReadyNAS system attempts to maintain original file ownership whenever possible. However, you can automatically change 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. (Optional) Select the **Wake-on-LAN** check box and enter the MAC address of your ReadyNAS system.

Use this option whenever your destination device is set to power down automatically. If you do not set this option and the destination device is powered down when the backup job is scheduled to begin, the backup job might not happen.

If your destination device is set to power down automatically, you must also configure the destination device to accept wake-on-LAN notifications. If you do not configure the destination to accept wake-on-LAN notifications, and it is powered down when the backup job is scheduled to begin, the backup job might fail.

8. Click the **Apply** button.

Your backup job settings are saved and this backup job displays in the backup schedule. For more information about viewing scheduled backup jobs, see *Manage Backup Jobs* on page 147.

If you set a backup schedule for this job in *step 6*, your backup job starts at the date and time you specified.

If you did not set a schedule for this job in *step 6*, you must manually start the backup job by pushing the Backup button on your ReadyNAS unit or by manually starting the backup job using FrontView. For more information about the location of the Backup button on your system, see the appropriate hardware manual. For more information about using FrontView to manually start a backup job, see *Manually Start a Backup Job* on page 150.

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. You can do this after you save the backup job.

Recover Data to a Network-Attached Device

You can use FrontView to restore data that you previously backed up to your ReadyNAS device to another network-attached device. Before you can recover data, you must first back it up.

Figure 9 illustrates this process.

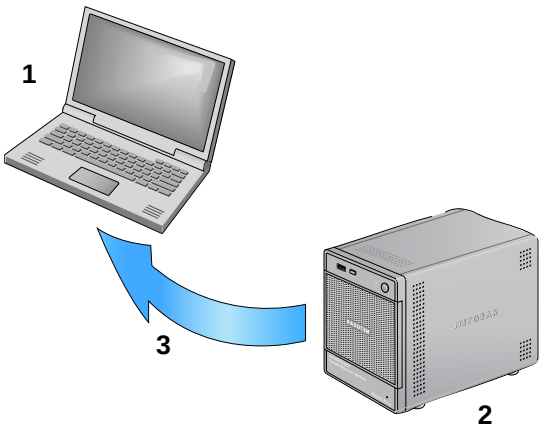


Figure 9. Recovering data from a ReadyNAS system to a laptop computer

1. Laptop computer serving as recovery destination
2. ReadyNAS system serving as recovery source
3. Recovery process

WARNING!

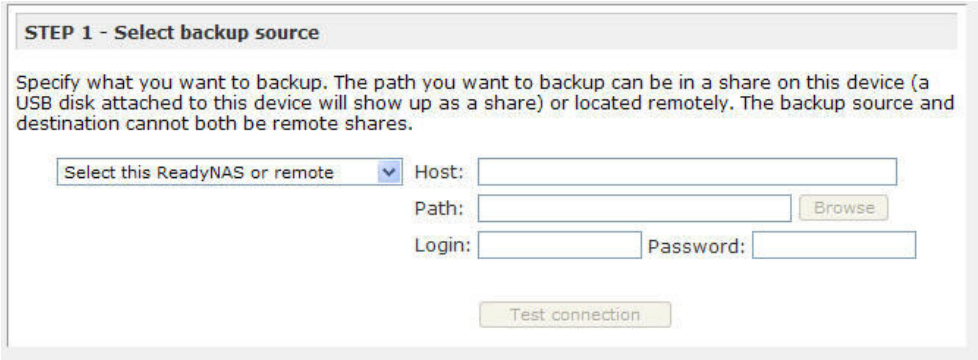
Although this is a recovery procedure, your ReadyNAS system treats it like a backup job. This means that you use FrontView screens labeled *backup* and you reverse the source and destination systems you used when you backed up the data that you are recovering.

Backup and recovery jobs ReadyNAS Vault and Time Machine require different procedures. For more information, *ReadyNAS Vault* on page 153 or *Time Machine* on page 154.

➢ **To recover backup data to your ReadyNAS system:**

1. Select **Backup > Add a New Backup** from the FrontView Main menu.

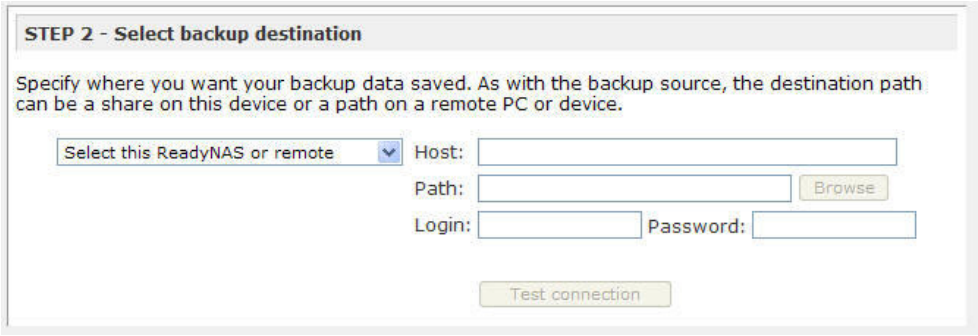
   The Add a New Backup Job screen displays.



2. From the drop-down list in the STEP 1 - Select backup source pane, select the share on your ReadyNAS system where you backed up your network-attached device's data.

   If you have previously created one or more iSCSI targets on your ReadyNAS system, you can recover data that you backed up to an iSCSI target. For more information about creating and managing iSCSI targets, see *iSCSI Targets* on page 102.

3. From the drop-down list in the STEP 2 - Select a backup destination pane, select the network-attached device, website, or FTP site where you want to restore data.



   Depending on how your network is configured, these options vary.

   If you select a recovery destination that requires a path, use a forward slash (/) to separate directories, for example:

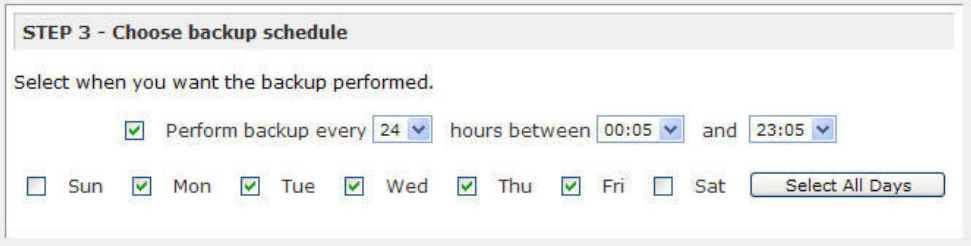
   /<share name>/<folder name>

   Do not use a backslash (\) in paths.

   If you select a remote Rsync server, you must enter the Rsync server's host name and a path. Depending on how the Rsync server is configured, you might need to enter a user name and password. Whether or not you need to enter login credentials depends on how the Rsync server is configured. For more information, contact the Rsync server's system administrator.

4. If necessary, enter the remote host name, the folder path, and any login credential required to access that path.
5. (Optional) To ensure that you are able to access the remote backup destination, click the **Test Connection** button.

   A pop-up window displays indicating whether you can access the destination.
6. From the STEP 3 - Choose backup schedule pane, clear the **Perform backup every** check box.:

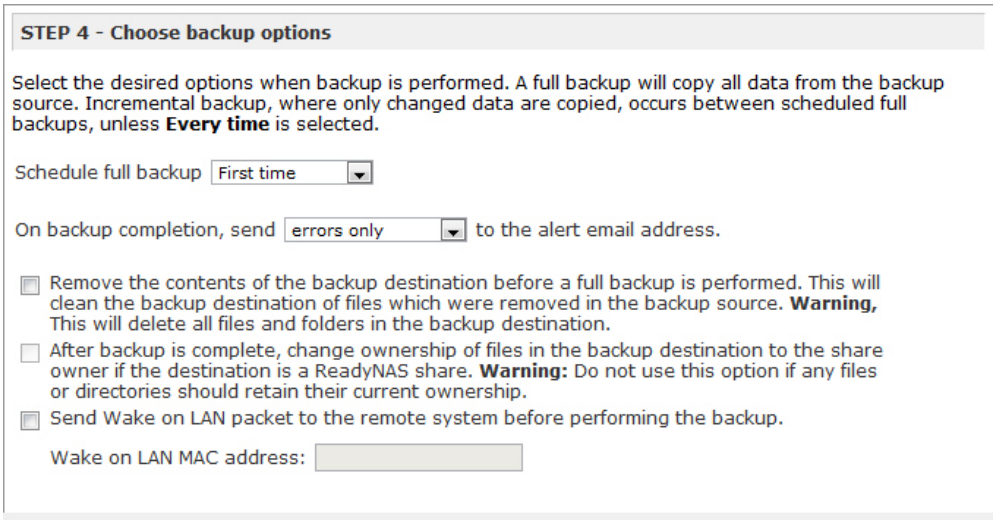


   Clearing this check box forces the recovery procedure to be started manually, which ensures that the recovery job does not happen automatically.

WARNING!

To ensure the integrity of the data stored on your primary device, never automatically schedule a recovery job.

7. Using the drop-down lists and check boxes in the Step 4 - Choose backup options pane, configure backup options:



a. From the **Schedule a full backup** drop-down list, select **Every Time**.

b. From the **On backup completion, send** drop-down list, select what type of logs to send when the recovery job completes,

   You can send a log that lists only errors encountered during recovery, full logs consisting of file listings (can be large), or status and errors (status refers to completion status).

   Log email messages are restricted to approximately 10,000 lines. For more information about viewing full logs, see *View a Backup Log* on page 150.

c. Ensure that the **Remove files from backup destination** check box is clear.

   Selecting this check box erases the destination path contents before the backup is performed, which NETGEAR does not recommend for recovery jobs.

WARNING!

If using this option, ensure that you have correctly identified your backup source and backup destination. If you reverse them, you might permanently delete your source files. NETGEAR recommends not enabling this option unless your destination device is very low on storage space.

   Best practice is to experiment with this option using a test share to make sure that you understand how it works.

d. (Optional) Select the **Change ownership of backup files** check box.

   Your ReadyNAS system attempts to maintain original file ownership whenever possible. However, you can automatically change 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.

8. Click the **Apply** button.

   Your backup job settings are saved and this recovery job displays in the backup schedule as a backup job. Because you did not assign a schedule to it, you must manually start the job.

9. Select **Backup > Backup Jobs** from the FrontView main menu.

   The Backup Schedule screen displays.

   Each job is assigned a number beginning at 001.

10. Click the **Go** button for this recovery job.

    The recovery process begins.

Manage Backup Jobs

Use FrontView to manage backup jobs and backup logs and to configure how the Backup button on your system operates.

Edit a Backup Job

Use FrontView to edit backup jobs that you created earlier.

➢ **To edit a backup job:**

1. Select **Backup > Backup Jobs** from the FrontView main menu.

   The Backup Schedule screen displays.

   If you have created at least one backup job, the Backup Schedule screen lists all backup jobs. Each job is assigned a number beginning at 001.

   If you have not created any backup jobs, a message displays in this screen telling you that your ReadyNAS system has no backup jobs.

2. Click the job number button for the backup job you want to edit.

   A screen displays listing the details of the backup job. These are the same options that are available when you create a backup job.

3. Edit the backup job as desired.
4. Click the **Apply** button.

   Your changes are saved.

Remove a Backup Job from the Automatic Scheduling Queue

You can use FrontView to change a job from automatically running to instead require a manual start.

➢ **To remove a backup job from the automatic scheduling queue:**

1. Select **Backup > Backup Jobs** from the FrontView main menu.

   The Backup Schedule screen displays.

   If you have created at least one backup job, the Backup Schedule screen lists all backup jobs. Each job is assigned a number beginning at 001.

   If you have not created any backup jobs, a message displays in this screen telling you that your ReadyNAS system has no backup jobs.

2. Clear the **Enable** check box next to the job that you want to remove from the automatic scheduling queue.

   Disabling the job does not delete the job, but removes it from the automatic scheduling queue. Click the **Apply** button.

   The job is no longer in the automatic scheduling queue. The backup job must now be manually started.

Delete a Backup Job

Deleting a backup job permanently removes it from your ReadyNAS system.

➢ **To delete a backup job:**

1. Select **Backup > Backup Jobs** from the FrontView main menu.

   The Backup Schedule screen displays.

   If you have created at least one backup job, the Backup Schedule screen lists all backup jobs. Each job is assigned a number beginning at 001.

   If you have not created any backup jobs, a message displays in this screen telling you that your ReadyNAS system has no backup jobs.

2. Click the **Delete** button in the row for the job that you want to permanently remove.

   You are prompted to confirm the delete command.

3. Confirm the deletion.

   The backup job is deleted.

Manually Start a Backup Job

You can manually start a backup job that you did not put in the automatic scheduling queue when you created it, or you can manually start a job that you put in the automatic scheduling queue but that you want to force to run immediately.

➢ **To manually start a backup job:**

1. Select **Backup > Backup Jobs** from the FrontView main menu.

   The Backup Schedule screen displays.

   If you have created at least one backup job, the Backup Schedule screen lists all backup jobs. Each job is assigned a number beginning at 001.

   If you have not created any backup jobs, a message displays in this screen telling you that your ReadyNAS system has no backup jobs.

2. Click the **Go** button in the row for the backup job that you want to manually start.

   The backup job starts.

View a Backup Log

You can use FrontView to view the full logs of completed backup jobs or the partial backup logs of jobs that are in progress.

In addition to backup logs, your ReadyNAS system also maintains system logs. For more information, see *System Logs* on page 113.

➢ **To view backup logs:**

1. Select **Backup > Backup Jobs** from the FrontView main menu.

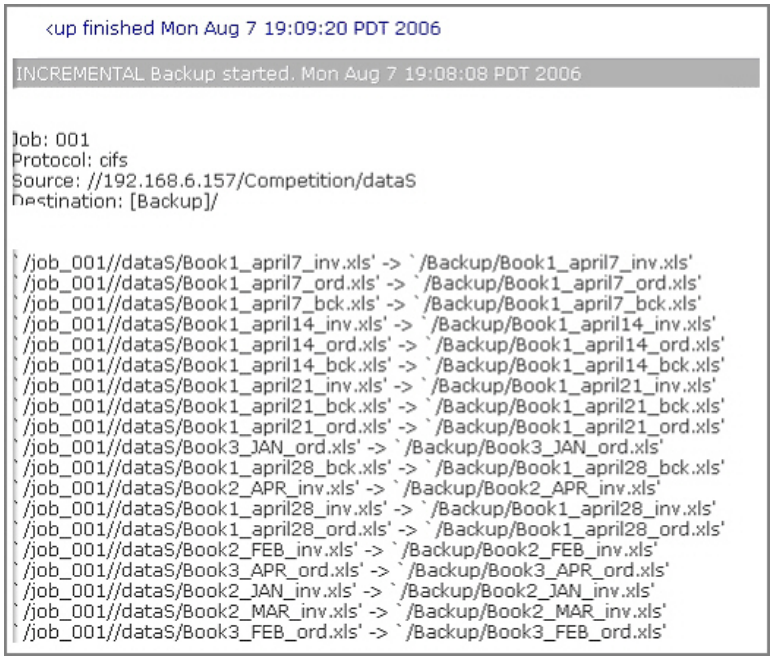
   The Backup Schedule screen displays.

   If you have created at least one backup job, the Backup Schedule screen lists all backup jobs. Each job is assigned a number beginning at 001.

   If you have not created any backup jobs, a message displays in this screen telling you that your ReadyNAS system has no backup jobs.

2. Click the **View log** link in the row for the backup job whose log you want to view.

   The backup log displays.



   You can view the backup log while a backup job is running or after it completes.

   The log format varies based on the backup source and backup destination types. All backup logs list the time the job started, the time the job completed, and whether it completed successfully or with errors.

Clear a Backup Log

You can use FrontView to clear a backup log that is stored on your ReadyNAS system.

➢ **To clear a backup log:**

1. Select **Backup > Backup Jobs** from the FrontView main menu.

   The Backup Schedule screen displays.

   If you have created at least one backup job, the Backup Schedule screen lists all backup jobs. Each job is assigned a number beginning at 001.

   If you have not created any backup jobs, a message displays in this screen telling you that your ReadyNAS system has no backup jobs.

2. Click the **Clear log** link in the row for the backup job whose log you want to clear.

   The backup log is erased.

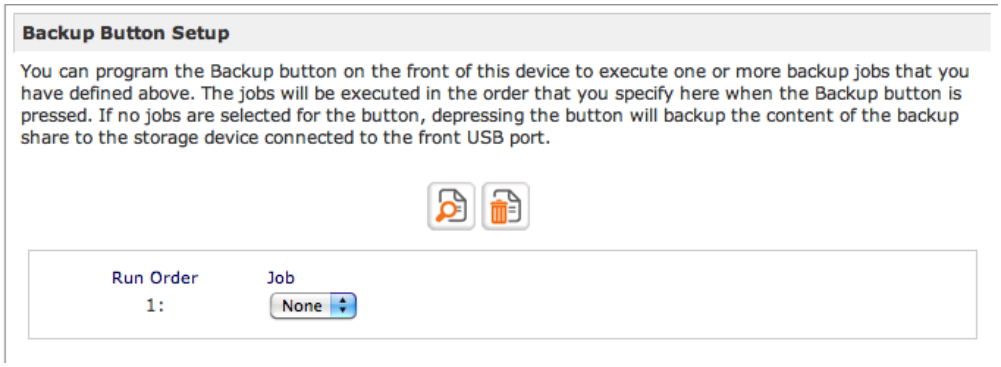
Configure the Backup Button

You can use FrontView to configure the Backup button on your ReadyNAS storage system to execute one or more backup jobs that you previously created. When you press the Backup button, the jobs are executed in the order that you specified in the backup schedule.

If no jobs are scheduled for the button, pressing the Backup button backs up the content of the backup share to the storage device connected to the front USB port.

➢ **To configure the Backup button:**

1. Select **Backup > Backup Jobs** from the FrontView main menu.
2. Scroll down to the Backup Button Setup pane.



3. Use the drop-down lists to set the order of the backup jobs tied to the Backup button.
4. Click the **Apply** button.

   Your settings are saved.

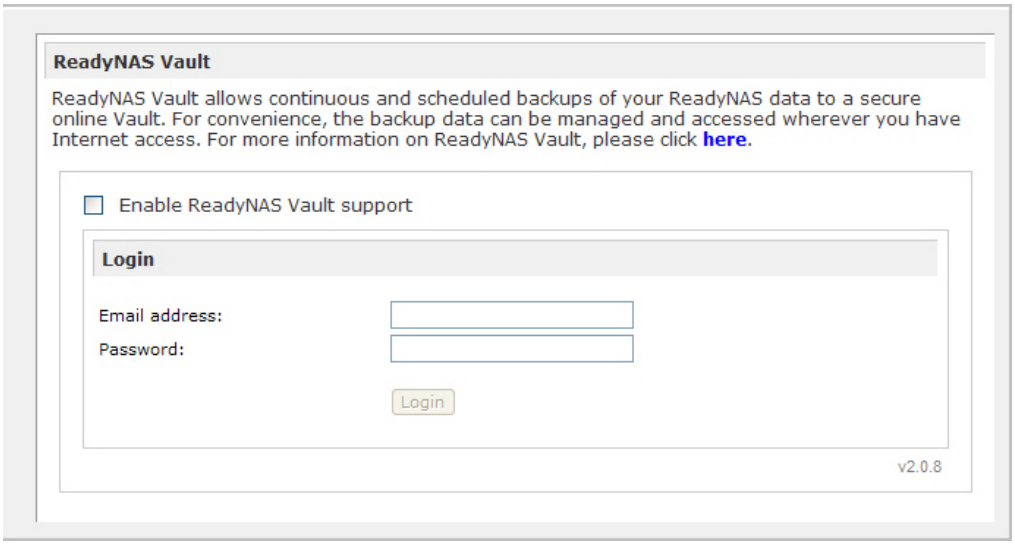
ReadyNAS Vault

You can back up data to the web using ReadyNAS Vault, which enables you to create continuous and scheduled backup jobs of your ReadyNAS data to a secure online data center. You pay a fee for this service based on the amount of space you use. You can access the data that you backup to ReadyNAS Vault data wherever you have Internet access.

➢ **To use the ReadyNAS Vault service:**

1. Choose **Backup > ReadyNAS Vault** from the FrontView main menu.

   The ReadyNAS Vault screen displays.



2. Select the **Enable ReadyNAS Vault support** check box and click the **Apply** button.

   You are prompted to create a ReadyNAS Vault account.

3. Click the **Click here to Register** link.

   The Register screen displays.

4. Enter your email address, create a password, confirm your password, and click the **Register** button.

   A pop-up window displays informing you that you successfully registered.

5. Click the **OK** button.
6. Click the **Manage ReadyNAS Vault** button.

   A new screen displays. You are prompted to log in to ReadyNAS Vault again.

7. Enter your password and click the **Submit** button.

   A ReadyNAS Vault configuration wizard launches.

8. Follow the prompts to choose shares to back up to ReadyNAS Vault.

   You can now use the ReadyNAS Vault interface to backup and restore files using ReadyNAS Vault.

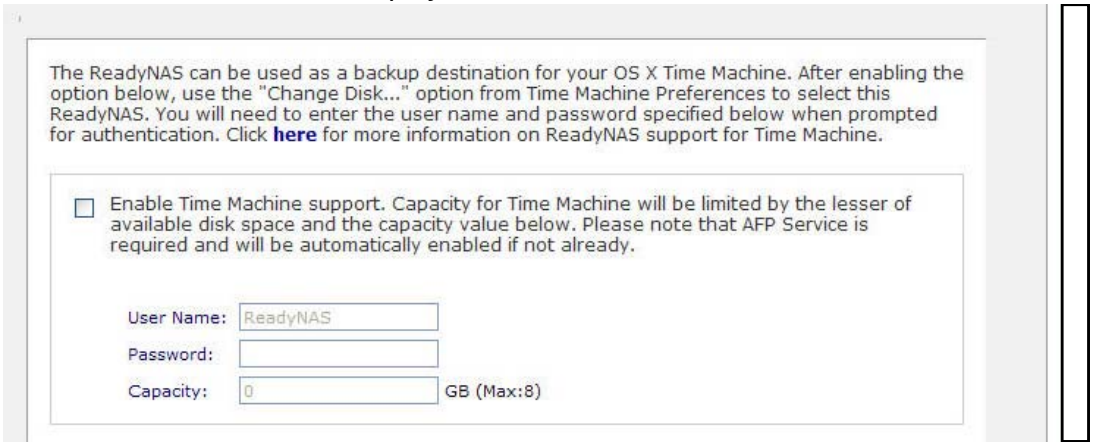
Time Machine

You can use your ReadyNAS storage system to back up data stored on your Mac OS X Time Machine.

➢ **To back up data stored on your Time Machine to your ReadyNAS system:**

1. Select **Backup > Time Machine** from the FrontView main menu.

   The Time Machine screen displays.



2. Click the **Enable Time Machine support** check box.
3. Enter **ReadyNAS** in the **User Name** field.
4. Create a password and enter it in the **Password** field.

5. Enter the maximum amount of space on your ReadyNAS storage system that you want to devote to Time Machine backups in the **Capacity** field.

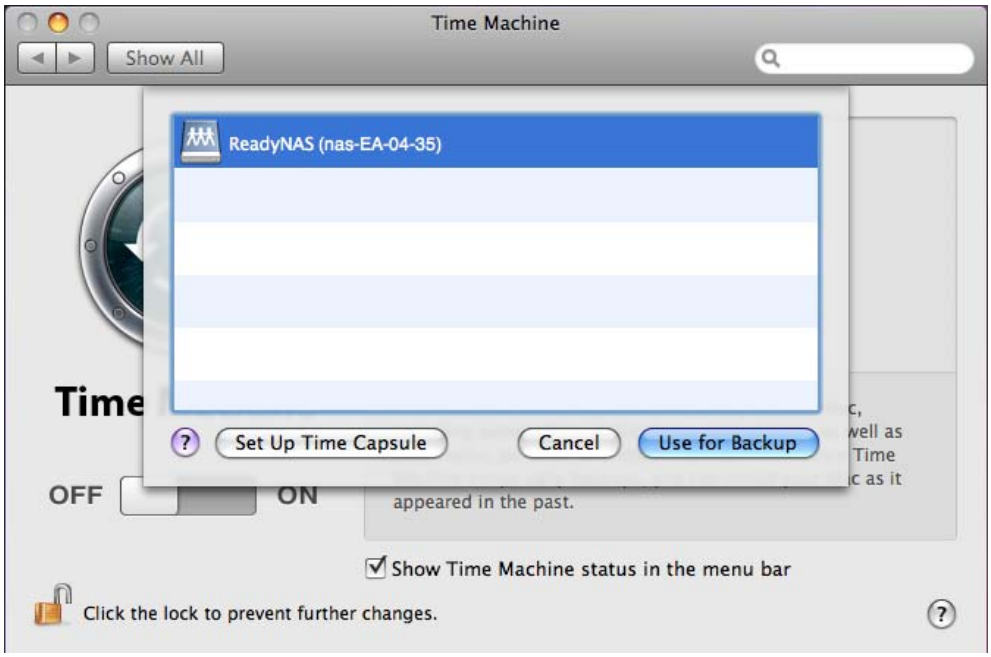
   If Time Machine backups exceed this quota, the ReadyNAS system deletes older versions of Time Machine backups to bring Time Machine backups within this quota.

6. Click the **Apply** button.

   Your settings are saved.

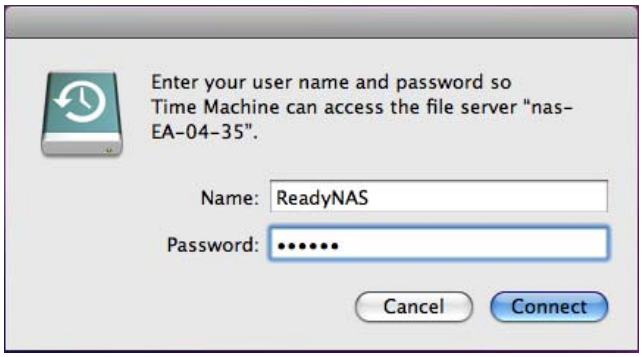
7. Launch Time Machine and click the **Choose Backup Disk** button.

   A pop-window displays that lists available disks, including your ReadyNAS system.



8. Select your ReadyNAS system and click the **Use for Backup** button.

   A dialog box displays, prompting you to provide login credentials.



9. Enter the user name you created in *step 3* in the **Name** field.
10. Enter the password you created in *step 4* in the **Password** field and click the **Connect** button.

    Time Machine begins the backup. This can take several minutes.

Notification of Compliance

8

Regulatory Compliance Information

This section includes user requirements for operating these products 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.

These products' 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

These products do 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 these products comply 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

These digital apparatus, ReadyNAS Ultra 2, Ultra 4, Ultra 6, Ultra 2 Plus, Ultra 4 Plus, Ultra 6 Plus, Pro Pioneer, and NVX Pioneer, do 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

These products comply 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

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X