NETGEAR®

ReadyNAS OS 6.2

Software Manual

Models:

ReadyNAS 102
ReadyNAS 104
ReadyNAS 312
ReadyNAS 314
ReadyNAS 316
ReadyNAS 516
ReadyNAS 716X
ReadyNAS 2120
ReadyNAS 2120 v2
ReadyNAS 3220
ReadyNAS 4220
EDA 500

March 2014
202-11207-08

350 E. Plumeria Drive
San Jose, CA 95134

Support

Thank you for purchasing this NETGEAR product.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website.

For product updates, additional documentation, and support, visit *http://support.netgear.com*.

Trademarks

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.

See the regulatory compliance document before connecting the power supply.

Contents

Chapter 8 System Maintenance

Chapter 9 Backup and Recovery

Getting Started

1

This manual describes how to configure and manage your ReadyNAS® storage system.

Your ReadyNAS storage system relies on the following applications:

- **ReadyCLOUD**. Use this online service to discover your ReadyNAS system on your local area network and access the local admin page.
- **Local admin page**. Use this browser-based interface to configure and manage your ReadyNAS system.

This chapter includes the following sections:

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. *Basic Installation* on page 10. You use ReadyCLOUD to discover your storage system on your network.
2. *Create a Shared Folder* on page 42. Shared folders are the way you organize the data you store on your ReadyNAS system.
3. *Create a LUN* on page 83. LUNs are SAN data sets that allow data transfer and storage over iSCSI.
4. *Basic Snapshot Concepts* on page 106. Protect the data that is stored in folders and LUNs by creating snapshots.
5. *Create User Accounts* on page 130. You create a user account for each person that you want to allow to access your ReadyNAS system.
6. *Configure Global Settings for File-Sharing Protocols* on page 159. File-sharing protocols enable you to transfer files across a network.
7. *Basic Data Backup and Recovery Concepts* on page 196. You can back up the data that you store on your ReadyNAS system and you can use your ReadyNAS system to back up data that you store on other devices.

Additional Documentation

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

For information about your system's hardware, see the hardware manual for your system, which is available at *http://support.netgear.com/product/ReadyNAS-OS6*

Supported Operating Systems

The ReadyNAS supports the following operating systems:

- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Apple Mac OS X10.5 Leopard or later
- Linux, Unix, Solaris
- Apple iOS
- Google Android

Supported Browsers

The ReadyNAS local admin page supports the following browsers:

- Microsoft Internet Explorer 9.0+
- Apple Safari 6.0+
- Google Chrome 20+
- Mozilla Firefox 14+

If you have difficulty accessing the local admin page or if you notice unexpected behavior, try using another browser.

Diskless Systems

If you have a diskless ReadyNAS, you must first install and format at least one disk before you can discover your system with ReadyCLOUD or visit the local admin page. You must use supported disks. For a list of supported disks, visit *http://www.netgear.com/readynas-hcl*. Make sure that the ReadyNAS is powered off before inserting any disks.

If you want to use disks that were previously formatted for an operating system other than ReadyNAS OS 6 (for example, Windows, Linux, or previous-generation ReadyNAS), you must reformat the disks. You can reformat the disks by installing them, powering on the system, and performing a factory reset before continuing the configuration.

The details of installation for both new and previously formatted disks depend on the model. For detailed instructions, see the hardware manual for your system, which is available at *http://support.netgear.com/product/ReadyNAS-OS6*.

For basic configuration information, see *Basic Installation* on page 10.

For information about disk formats, see *RAID* on page 20.

Basic Installation

After you follow these instructions, your ReadyNAS system is ready to use in a production environment. Setup takes approximately 15 minutes.

To install your storage system:

1. Install all available disks that you want to use in your storage system.

   Note: If you are using previously formatted disks that contain data, you must reformat these disks before continuing. For information about formatting disks, see the hardware manual for your system.

   For a list of supported disks, see the Hardware Compatibility List at *http://www.netgear.com/readynas-hcl*

   For information about installing disks, see the hardware manual for your system.

2. Place your system in a location that provides adequate ventilation.
   High-capacity disks can produce considerable heat. It is important to ensure that the fan exhausts are unobstructed.

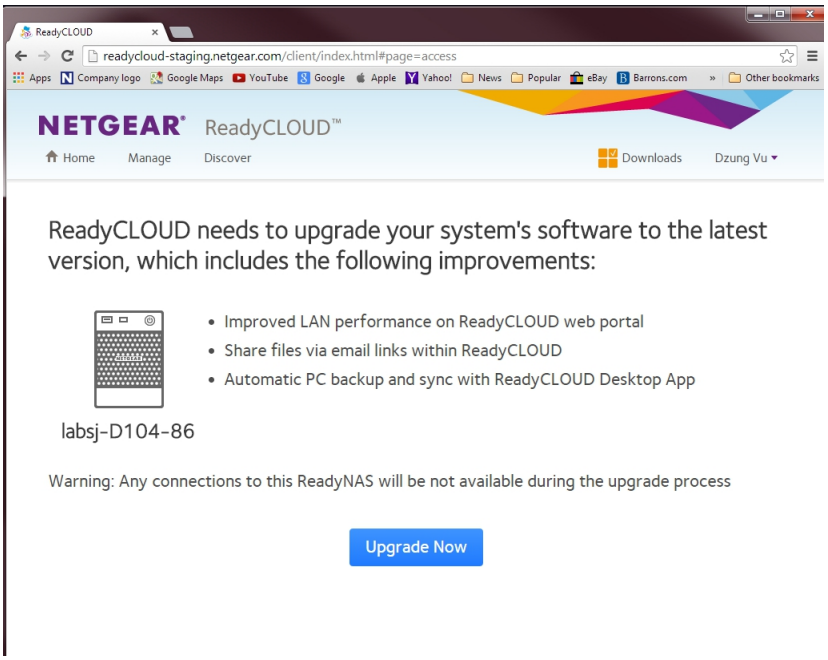
For a complete list of placement considerations, see the hardware manual for your system.

3. Connect the power adapter to the power cord.
4. Connect the power adapter to the back of the system and plug the power cord into a wall outlet or power strip.
5. Use an Ethernet cable to connect an Ethernet port on the storage system to your network.
6. If necessary, press the Power button to turn on the system.
7. Wait for the Power LED to turn solid blue or for the status display screen to display the system's IP address.
8. Use ReadyCLOUD to discover and set up your system on the network.
   See *Discover and Set Up Your ReadyNAS* on page 13.

Upgrade ReadyNAS Firmware for Use with ReadyCLOUD

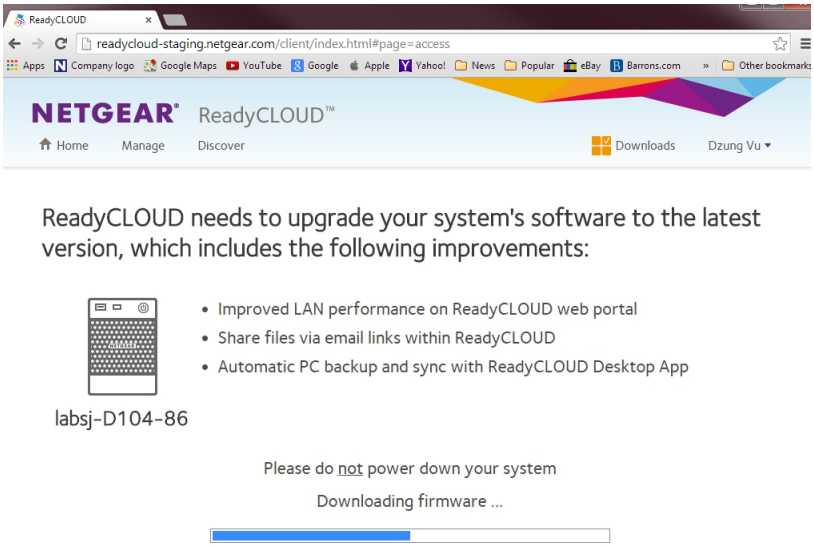
The first time you log into ReadyCLOUD after upgrading your ReadyNAS, you see a message about needing to upgrade the ReadyNAS system firmware.

When you log into ReadyCLOUD you see the following window:

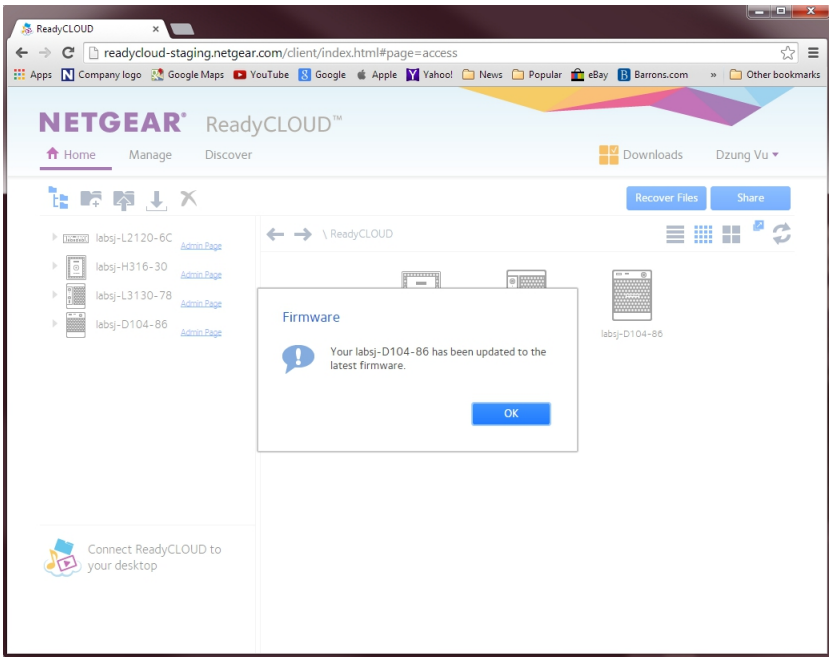


ReadyCLOUD now includes major new features, but these features require new firmware on the ReadyNAS system. When you log in to ReadyCLOUD from a ReadyNAS system, ReadyCLOUD checks to see if the ReadyNAS system firmware is recent enough to work with the new ReadyCLOUD. If it is not, you see the message and the **Upgrade Now** button. Click the button to start the download and automatic restart.

During the download you see the following window:



When the download and restart complete, you see the following window:



Click the **OK** button to dismiss the message and continue to ReadyCLOUD.

Discover and Set Up Your ReadyNAS

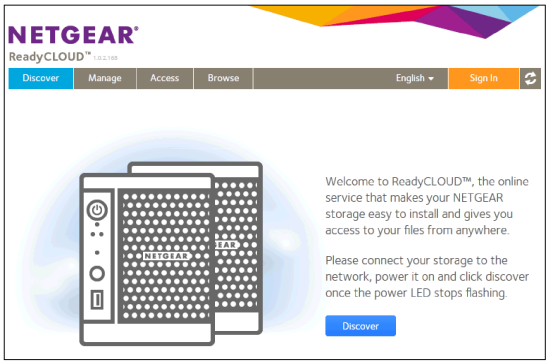
ReadyCLOUD is the online service that you use to discover and set up ReadyNAS storage systems on your network. You can also use ReadyCLOUD to access and manage data on your ReadyNAS systems. For you to use ReadyCLOUD, your computer and storage system must have Internet access.

> **Note:** If your computer and storage system do not have Internet access, install and run the RAIDar utility instead. RAIDar is on the resource CD that came with your system. It includes versions for Windows, Mac, and Linux operating systems. It is also available at *http://www.netgear.com/raidar*

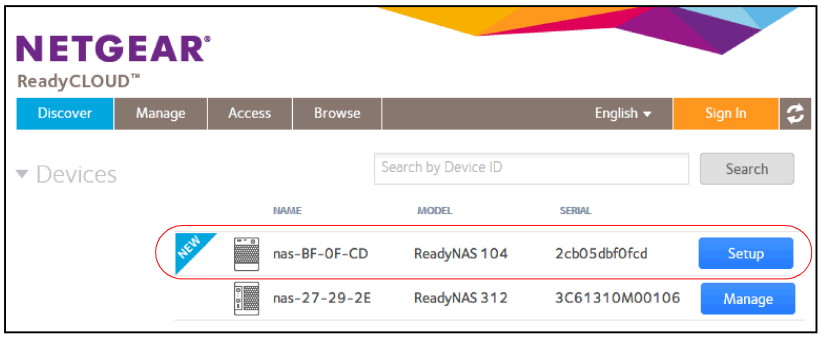
When you discover your device using ReadyCLOUD, you can choose whether to immediately use ReadyCLOUD to setup and manage your device, or whether to use the device's local admin page. If you choose to use local administration now, you can still use ReadyCLOUD later.

To discover and set up your storage system:

1. Visit *http://readycloud.netgear.com* on a computer that uses the same local area network (LAN) and Internet connection as your storage system.



2. Click the **Discover** button.
   ReadyCLOUD automatically detects your ReadyNAS system on the network.
   Your new ReadyNAS system is marked with a NEW label.



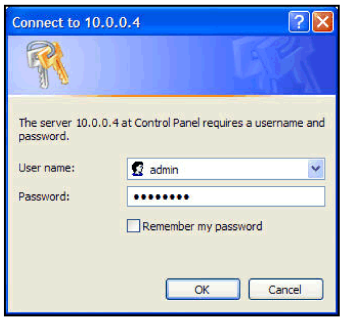
3. Click the **Setup** button.
4. Select whether to use ReadyCLOUD or the local admin page to use to set up your system:
   - **Option 1**. Select **Join Now**.
     a. Sign in to ReadyCLOUD or create a user account.

     Tip: If you already set up a ReadyNAS Remote account, you can sign in to ReadyCLOUD using your ReadyNAS Remote credentials.

     b. Follow the prompts to set up your ReadyNAS system.

     For more information about ReadyCLOUD, see *Use ReadyCLOUD* on page 65.
   - **Option 2**. Select **Join Later**.
     An SSL certificate security warning displays. This warning ensures an encrypted authentication and secure access to the ReadyNAS local admin page for your storage system.

     a. Accept the certificate.

     b. Enter **admin** for the user name, enter **password** for the password, and click the **OK** button. Both user name and password are case-sensitive.

     You can change these credentials when you configure your system. NETGEAR recommends that you change your password as soon as possible.

The ReadyNAS local admin page displays in your browser and launches a setup wizard.

c. Follow the prompts of the setup wizard that launches in your browser.

Local Setup Wizard

The first time you access the local admin page, a setup wizard prompts you to configure the basic settings of your ReadyNAS storage system.

Note: The local setup wizard is for users who choose to set up their ReadyNAS system using Offline mode. If you set up your system using ReadyCLOUD mode and the ReadyCLOUD setup wizard, the local setup wizard does not display.

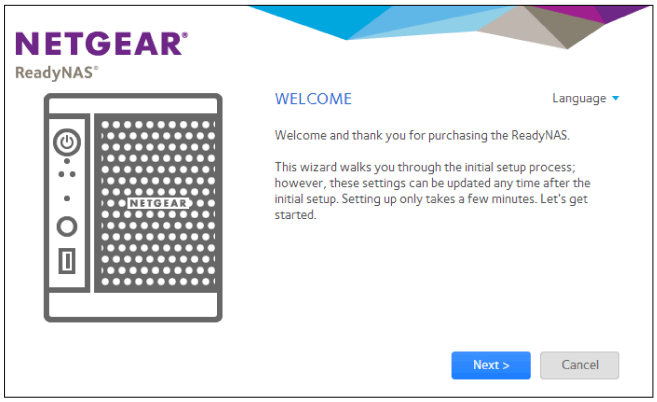


Figure 1. Setup wizard (Welcome screen)

You can change the language setting for the setup wizard by clicking the Language list title at the top right corner of the screen and selecting a language from the drop-down list.

The setup wizard guides you through the initial configuration process to help you quickly integrate your ReadyNAS storage system into your network. Follow the setup wizard's prompts to configure the following settings:

- **Time and date**. For more information, see *Set the Clock* on page 139.
- **Alert contact**. For more information, see *Configure System Alerts* on page 142.
- **Host name**. For more information, see *Configure the Host Name* on page 145.
- **Administrator password and password recovery**. For more information, see *Set the Administrator Password* on page 140.

Local Admin Page

The local admin page is a browser-based interface that you use to configure and manage your ReadyNAS system. When you visit the local admin page, the Overview screen displays, as shown in the following figure.

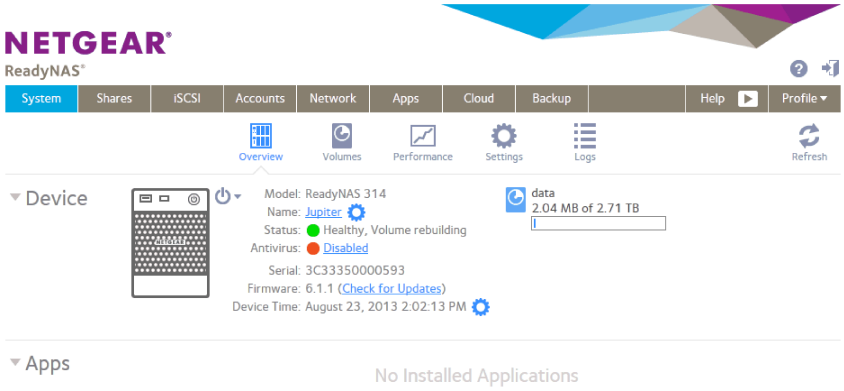


Figure 2. Local admin page (Overview screen)

The following list describes the features of the local admin page:

- To navigate through the local admin page, use the navigation bar across the top of the screen and the navigation icons below it.
- Some screens are divided into multiple sections. You can collapse or expand sections of the screen by clicking the triangle icons (▾) next to each section heading.
- To refresh the screen, click the **Refresh** icon (↻) in the top right corner of the screen.
- For more information about your product, visit an official NETGEAR support page by clicking the **Support** icon (?) in the top right corner of the screen.
- To log out of the local admin page, click the **Logout** icon ( ) in the top right corner of the screen.

Other features of the local admin page are described in other chapters.

In this manual, instructions for navigating through the local admin page begin by specifying the selection from the navigation bar and then, if necessary, specifying the selections from the row of navigation icons and section headings. For example, to configure the global file-sharing protocols, select **System > Settings > Services**. System is the selection from the navigation bar. Settings is the selection from the row of navigation icons. Services is the selection from the section headings on the Settings screen.

Access the Local Admin Page

If your computer is connected to the same LAN as your storage system, follow these instructions to access the local admin page.

For information about remote access to the local admin page, see the *ReadyNAS Remote User Manual*.

To access the local admin page:

1. Open a web browser and visit **https://*<hostname>***.

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

Note: You can also enter ***https://<ReadyNAS IP address>***, where *<ReadyNAS IP address>* is the IP address of the ReadyNAS.

An SSL certificate security warning displays.

2. Accept the certificate.
   A login prompt displays.
3. Enter the login credentials for your system and click the **OK** button.
   If you did not change the credentials, the default credentials are as follows:
   - **user name**. admin
   - **password**. password

   Both user name and password are case-sensitive.

   The local admin page displays.

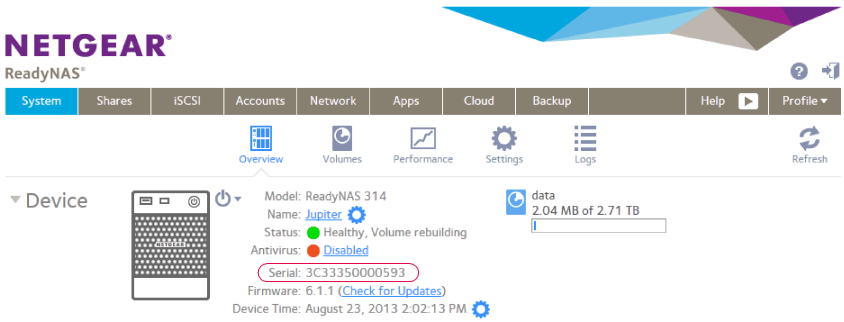
You can also access the local admin page from ReadyCLOUD (see *Use ReadyCLOUD* on page 65).

Register Your System

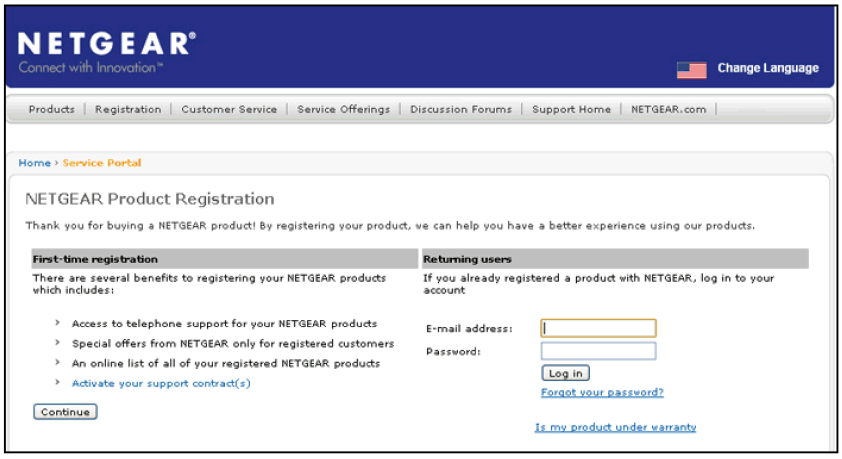
You must register your product before you can use NETGEAR telephone support. Register your ReadyNAS system at the NETGEAR Product Registration web page.

To register your ReadyNAS system:

1. Locate the serial number of the system.
   You can find the serial number on the Overview screen of local admin page or on the chassis label of your product.



2. Open a web browser and visit *http://www.NETGEAR.com/register*.
   The Product Registration web page displays.



3. Take one of the following actions:
   - If you never registered a NETGEAR product, click the **Continue** button.
   - If you registered a NETGEAR product in the past, enter your email address and password and click the **Log in** button.
4. Follow the prompts.
   The ReadyNAS is registered.

Five Levels of File Protection

File and data protection strategies such as various RAID levels or snapshots can go only so far in protecting data from loss, but ReadyNAS OS provides five separate strategies that work together to provide substantially better protection than any one strategy.

The different levels of disk redundancy provided by RAID types provide degrees of file protection from the loss of one or more disks, but cannot do anything about accidental deletion or corruption; can mask, but not prevent, gradual corruption caused by the slow degradation of the disks; and cannot provide protection from a site disaster. Snapshot technologies provide protection against accidental deletion or corruption but by themselves cannot protect against disk loss or site loss.

ReadyNAS OS allows you to use five different types of protection simultaneously:

- RAID. Protects against disk failure.
- Snapshot technology. Protects against accidental data deletion or corruption by providing point-in-time recovery.
- Real-time antivirus. Protects against loss or corruption from viruses.
- Bit rot protection. Protects against the degradation of data from disk aging.
- Offsite backup using ReadyNAS Vault or a second ReadyNAS. Protects against site loss.

Volume Configuration

2

This chapter describes how to configure and manage the volumes in your ReadyNAS storage system. It includes the following sections:

- *Basic Volume and RAID Concepts*
- *Manage Volumes*

Basic Volume and RAID Concepts

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

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. 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.

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

RAID

Your ReadyNAS storage system allows you to configure your hard disks using one of the many RAID technologies.

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-RAID™ mode, a proprietary single-volume RAID architecture that is easy to administer, and Flex-RAID mode, which allows you to format your disks in a variety of industry-standard RAID levels.

When you power on your system for the first time or if you reset your system to its factory default settings, the optimal RAID mode and level are automatically selected for you based on the number of disks that are installed. You can also configure the RAID settings manually (see *Change RAID Mode* on page 23).

X-RAID

X-RAID is an auto-expandable RAID technology that is available only on ReadyNAS systems. With X-RAID, you do not need to know intricate details about RAID to administer your system. X-RAID 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 your ReadyNAS system while the volume capacity increases.

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

- Easy system management
- Auto-expansion

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

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

X-RAID 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 must add a second disk that is at least as large as the first. It can be added while the system is running.

X-RAID uses the capacity of one disk for data storage and reserves the capacity of a second disk for data protection, which allows the volume to recreate data if a disk fails. In a two-disk system, the usable storage space is one disk. In a three-disk system, the usable storage space is two disks. In general, the total capacity of your storage system equals the capacity of all your disks minus the capacity of one disk.

The following figure illustrates how X-RAID uses new disks.

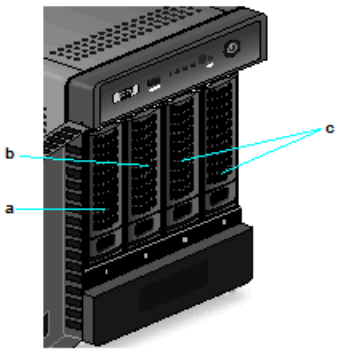


Figure 3. X-RAID disk usage

1. The first disk that you install is used for initial (unprotected) storage space.
2. The second disk that you install is reserved for data protection (parity information).
3. Installing additional disks increases your storage space.

> **Note:** X-RAID reserves the capacity of one disk for data protection. The actual space reserved for data protection is distributed across all disks.

Flex-RAID

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

- **JBOD**. This most basic RAID level does not protect your data from loss if one of your drives fails. JBOD is available only on volumes consisting of a single hard disk.
- **RAID 0**. RAID 0 distributes data across multiple disks, resulting in improved disk performance compared to systems that do not use RAID formatting. The total capacity of your storage system equals the capacity of the smallest of your disk drives times the number of disks. RAID 0 is available on volumes consisting of two or more hard disks.
- **RAID 1**. This RAID level provides full redundancy of your data, because it duplicates data across multiple disks. 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**. This RAID level also provides data redundancy, but it requires at least three disks. RAID 5 uses the capacity of one disk to protect you from data loss if one disk fails. Your data is distributed across multiple disks to improve disk performance. The total capacity of your storage system equals the capacity of all your disks minus the capacity of one disk. It is supported on systems with at least four drive bays.
- **RAID 6**. This RAID level can recover from the loss of two disks. Your data is distributed across multiple disks to improve disk performance. The total capacity of your storage system equals the capacity of all your disks minus the capacity of two disks. It is supported on systems with at least four drive bays.
- **RAID 10 (or 1+0)**. This RAID level uses both RAID 1 and RAID 0 technology. First, your data is duplicated so that exactly the same data is stored on two or more disks. Then, the data is distributed across additional disks to improve disk performance. It is supported on systems with at least four drive bays.

The Flex-RAID levels that you can select depend on the number of disks included in the volume. The following table describes the Flex-RAID levels that are available for a given number of disks. It also indicates whether adding a disk for data protection is possible for each configuration.

Table 1. Flex-RAID levels and data protection

Number of Disks per Volume	RAID Level	Can I add a disk for data protection?
1	JBOD	No. (JBOD is available only for volumes consisting of one disk)
2	RAID 1	No. (Volume protection is already redundant.)
2 or more	RAID 0	No. (RAID 0 does not offer protection.)
3 or more	RAID 5	Yes. (Additional disk provides dual redundancy and converts the volume to RAID 6.)
4 or more(even number)	RAID 10	No. (Volume protection is already redundant.)
4 or more	RAID 6	No. (Volume is already protected with dual redundancy.)

Manage Volumes

This section discusses volume management on your ReadyNAS system. You can add or delete volumes from the system. Additionally, you can change the volume's RAID mode and level. This section also covers volume status, volume maintenance and volume protection. In addition to volume topics, this section also covers extending the storage capacity on you ReadyNAS system.

Change RAID Mode

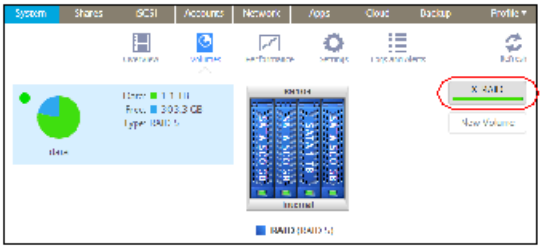
You can change the RAID mode that your ReadyNAS storage system uses. By default, your system's hard disks are configured into a single X-RAID volume.

Change from X-RAID to Flex-RAID

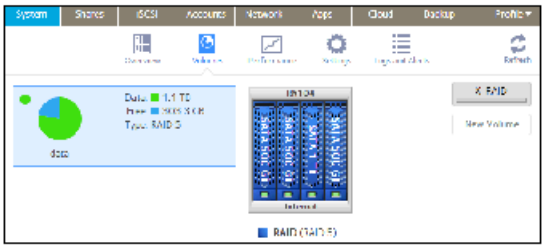
Your ReadyNAS system can easily change a volume from X-RAID to Flex-RAID mode. Data on the X-RAID volume is preserved when you switch to Flex-RAID. The RAID level of the resulting Flex-RAID volume is automatically assigned based on the number of disks that are installed.

To change from X-RAID to Flex-RAID:

1. Login to your ReadyNAS
2. Select **System > Volumes**.
3. Click the **X-RAID** button at the right side of the screen.



4. Confirm that you want to switch from X-RAID to Flex-RAID.
   The volume switches from X-RAID mode to Flex-RAID mode and the indicator on the X-RAID button turns gray.



The RAID level is automatically assigned based on the number of disks that are installed.

Change from Flex-RAID to X-RAID

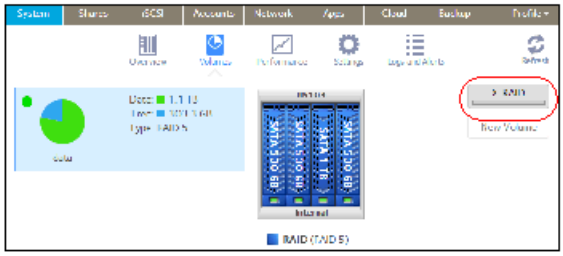
If your system contains only one volume, you can easily switch from Flex-RAID to X-RAID. Data on the Flex-RAID volume is preserved when you switch to X-RAID.

If your system contains multiple volumes, you must first reconfigure your disks into a single volume.

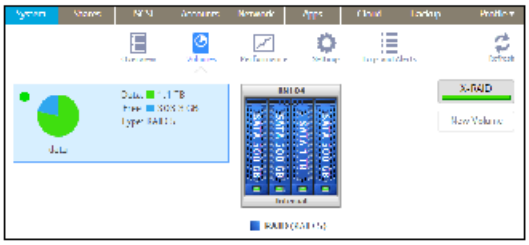
> **Note:** When you switch to X-RAID mode, any extra disks installed in your system are automatically reformatted and used for storage expansion.You cannot change the RAID mode of a RAID 0 or RAID 10 volume.

To change from Flex-RAID to X-RAID on a single-volume system:

1. Select **System > Volumes**.
2. Click the **X-RAID** button at the right side of the screen.



3. Confirm that you want to switch from X-RAID to Flex-RAID.
   The volume switches from Flex-RAID mode to X-RAID mode and the indicator on the X-RAID button turns green.



Any available drives are automatically used for storage expansion.

Change to a Different Flex-RAID Level

In Flex-RAID mode, you assign one of several RAID levels to your volume. Available RAID levels depend on the number of disks that you want the volume to include. For more information, see *Flex-RAID* on page 22. You can reconfigure your volumes to use a different RAID level.

> **Note:** Changing the RAID level of a volume erases all data. If data is stored on your system, you must back up the data to another storage device before changing the RAID level.You cannot change the RAID level of a RAID 0 volume.

To change to RAID levels:

1. If any data is stored on the volumes that you want to reconfigure, back up your data.
2. Delete the volumes that you want to reconfigure (see *Delete a Volume* on page 30).
   The disks that were part of the volumes become available again for other purposes (the color of the disks turns black).
3. Create a new volume from the available disks and select the RAID level (see *Create and Encrypt a Volume* on page 28).

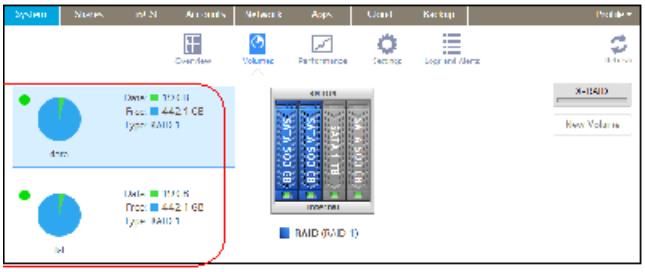
The volume is formatted according to your specifications. Formatting can take quite a while, depending on the size of your hard disk drives.

View the Status of a Volume

To view a summary of the volume status:

Select **System > Volumes**.

The volumes are listed at the left side of the screen.

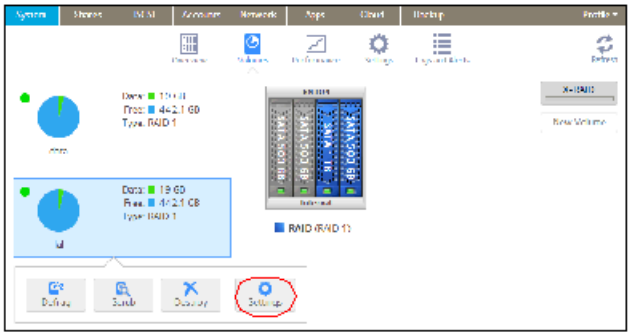


The following summary information is displayed next to each volume.

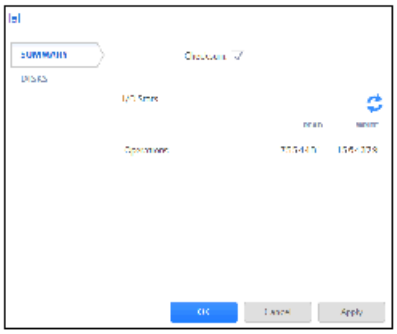
Item	Description
Data	The storage space that is consumed by data in MB, GB, or TB.
Free	The storage space that is available in MB, GB, or TB.
Type	The configured RAID level.
Health indicator	The color of the indicator to the right of the volume icon indicates the health of the volume: • **Green**. The volume is healthy. • **Yellow**. The volume is degraded. • **Red**. The volume is bad or faulty.

To view the I/O stats and disk status:

1. Select **System > Volumes**.
2. Select the volume from the list on the left.
3. From the pop-up menu that displays, select **Settings**.



A pop-up screen displays the I/O stats in the Summary tab.



4. Click the **Disks** tab.
5. From the **Disk** drop-down list, select one of the disks in the volume to view its status.

Note: The disks are listed by their position in the enclosure: <column>x<row>. For example, Disk 3X1 is the third disk from the left in the top row of the enclosure.

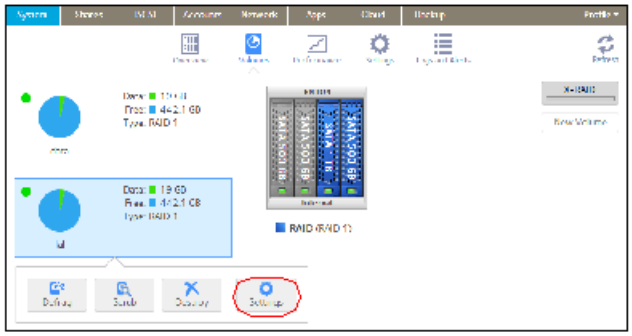
Configure the Checksum Function

Checksum functions help detect data transmission errors. The ReadyNAS uses a checksum function to improve accuracy and consistency when writing data to a volume. You can enable or disable the checksum

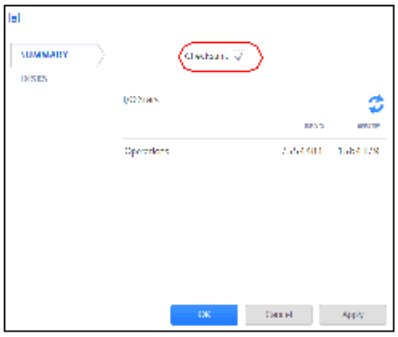
function on each volume. Enabling the checksum function improves the integrity of your data but reduces performance speeds.

Enable or disable the checksum function:

1. Select **System > Volumes**.
2. Select one of the volumes listed on the left side of the screen.
3. From the pop-up menu that displays, select **Settings**.



A pop-up screen displays.



4. In the Summary tab, select or clear the **Checksum** check box.
5. Click the **Apply** button.
6. Click the **OK** button.
   Your changes are saved.

Create and Encrypt a Volume

During volume creation you can also enable volume encryption. Encryption is optional. When encryption is enabled, data is encrypted in real time as it is written to the volume. You cannot encrypt existing volumes. Encryption is possible only when you are creating new volumes. When created, the volume will be a Flex-RAID volume, but after you create it, you can change it to an X-RAID volume.

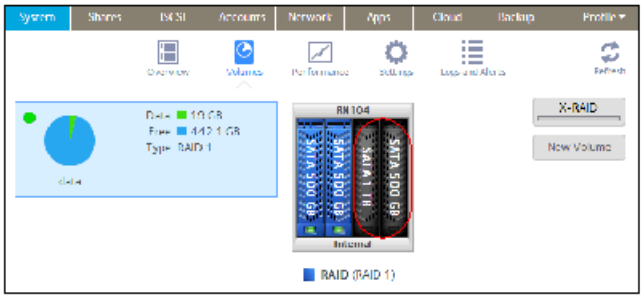
You need a USB drive to store the encryption key that is generated during volume creation. You can also have the encryption key emailed to you for safe keeping. If you lose the USB drive with the encryption key, you can load the emailed encryption key onto another USB drive.

You must insert the USB drive with the encryption key into a USB port on the ReadyNAS for the volume to be unlocked and accessible. You must insert the USB drive to unlock an encrypted volume during reboot. If you do not insert the USB key on reboot, there is a 10-minute timeout during which you can insert the key, otherwise you wll not be able to access the encrypted volume until the ReadyNAS is again rebooted. You can remove the USB drive after unlocking the volume. NETGEAR recommends storing the USB drive with the encryption key in a safe and secure location when not in use.

WARNING:
If you lose the encryption key, the encrypted drive is irrecoverable.

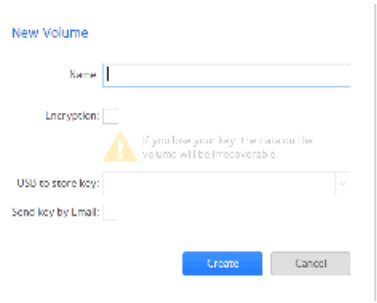
To create a volume, select the RAID level and enable encryption:

1. Select **System > Volumes**.
2. From the enclosure graphic, select the disks that you want to include in the new volume.



Available disks are colored black.

3. Click the **New Volume** button at the right of the screen.
The New Volume pop-up screen displays.



4. Configure the following settings:

- **Name**. Enter a name for the volume. The volume must not have the same name as a folder in the root folder system. The volume names home, apps, and job_ are reserved and cannot be used.
- **Encryption**. Select this check box to enable encryption on the volume. A key will be generated. If you lose your key, the data on the volume will be irrecoverable.
- **USB to store key**. If you enabled encryption, select a USB storage device from the drop-down list to store the generated key.
- **Send key by Email**. If you enabled encryption, select this check box to have the generated key sent to a email address associated with the admin account. Make sure that you have set the email account before creating the volume.

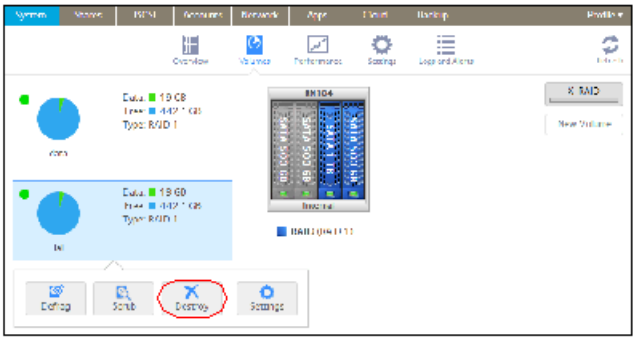
5. Click the **Create** button.
   The new volume is created and appears in the list of volumes at the left of the screen.

Delete a Volume

Before you delete a volume, make sure that you back up any data (folders and LUNs) that you want to save to another volume or another storage device.

To delete a volume:

1. Select **System > Volumes**.
2. Select the volume that you want to delete.
3. From the pop-up menu that displays, select **Destroy**.



Note: The **Destroy** option is not available when the ReadyNAS uses a single volume only. The **Destroy** option is available if you have at least two volumes.

A pop-up screen displays.

4. Type **DESTROY** to confirm your decision.
5. Click the **Destroy** button.
   The volume is deleted. The disks that were part of the volume become available again for other purposes (the color of the disks turns black).

Expand Storage Capacity

You can expand the storage capacity of an existing volume in two ways:

- **Horizontal expansion**. Expand the volume by adding more disks to the volume.
- **Vertical expansion**. Expand the volume by replacing disks in the volume with larger-capacity disks.

X-RAID makes horizontal volume expansion easy. If your X-RAID volume includes two or more disks, the volume expands automatically when you add disks.

You can expand a Flex-RAID volume by adding an additional JBOD disk or two additional RAID 0 disks.

Vertical expansion is available for X-RAID and Flex-RAID volumes.

You can continue to use your ReadyNAS system while the new disks are incorporated in the background. The process of volume expansion can take several hours. If you set up email notifications for your system, you receive an email message when the process finishes. For more information about alert notifications, see *Configure System Alerts* on page 142.

Horizontally Expand an X-RAID Volume

Horizontal expansion is available for X-RAID volumes only.

To horizontally expand an X-RAID volume:

Add a disk to an X-RAID volume that includes two or more disks.

For more information about how to add a disk to your ReadyNAS system, see the hardware manual for your system, which is available at *http://support.netgear.com/product/ReadyNAS-OS6*.

The system automatically determines whether the new disk is used for protection or storage. When you add a second disk, the new disk is used for data protection. When you add a third or fourth disk, the new disk is used to increase your storage capacity. For more information, see *X-RAID* on page 20. New disks are incorporated in the background while you continue to use your storage system.

Vertically Expand a Volume

Both X-RAID and Flex-RAID volumes support vertical expansion.

When you vertically expand a Flex-RAID volume, you must replace all disks in the volume with larger-capacity disks.

Note: Vertical expansion is not available for RAID 0 volumes.

When you vertically expand an X-RAID volume, you must replace disks in the volume according to the following table.

Table 3. X-RAID vertical expansion requirements

RAID Level	Disk Replacements Required for Vertical Expansion
RAID 1	Replace 2 or more disks with larger-capacity disks.
RAID 5	Replace 2 or more disks with larger-capacity disks.
RAID 6	Replace 4 or more disks with larger-capacity disks.

If you replace fewer disks than required for vertical expansion, the disks are reserved for data protection. Your available storage capacity does not increase to accommodate the reserved disks until you replace the required number of disks.

Note: To reduce the risk of data loss, NETGEAR recommends that you back up your data before vertically expanding a volume.

To vertically expand an X-RAID volume:

1. Replace one disk in the volume with a larger-capacity disk.
   For more information about how to add a disk to your system, see the hardware manual for your system, which is available at *http://support.netgear.com/product/ReadyNAS-OS6*.

   Note: You must use supported disks in your ReadyNAS system. For a list of supported disks, visit *http://www.netgear.com/readynas-hcl*.

2. Wait for the volume to resync your data.
   You can continue to use your ReadyNAS system while the volume is resyncing. Resyncing can take several hours. The start and completion of the resyncing process is recorded in the system log (see *System Logs* on page 176).

If you set up email notifications for your system, you receive an email message when the process finishes. For more information about alert notifications, see *Configure System Alerts* on page 142.

3. Repeat *Step 1* on page 32 – *Step 2* on page 32 until you have replaced the required number of disks with larger-capacity disks.
   For more information about X-RAID vertical expansion requirements, see *Table 2* on page 32.

To vertically expand a Flex-RAID volume:

1. Replace one disk in the volume with a larger-capacity disk.
   For more information about how to add a disk to your system, see the hardware manual for your system, which is available at *http://support.netgear.com/product/ReadyNAS-OS6*.

   Note: You must use supported disks in your ReadyNAS system. For a list of supported disks, visit *http://www.netgear.com/readynas-hcl*.

2. Wait for the volume to resync your data.
   You can continue to use your ReadyNAS system while the volume is resyncing. Resyncing can take several hours. The start and completion of the resyncing process is recorded in the system log (see *System Logs* on page 176).

   If you set up email notifications for your system, you receive an email message when the process finishes. For more information about alert notifications, see *Configure System Alerts* on page 142.

3. Repeat *Step 1* on page 33 and *Step 2* on page 33 until you have replaced each disk in the volume with a larger-capacity disk.

Add Protection to a Volume

This section discusses protection against disk failure. The types of protection available depend on the number of hard disks installed in the ReadyNAS system.

Add Protection to an X-RAID Volume

X-RAID requires a minimum of two hard disks to provide protection against disk failure. To add protection from disk failure to a one-disk ReadyNAS storage system, you must add a second disk that is at least as large as the first. You can add it while the system is running. For more information about how to add a disk to your system, see the hardware manual for your system, which is available at *http://support.netgear.com/product/ReadyNAS-OS6*.

An X-RAID volume that includes two or more disks is automatically formatted to protect against the failure of one disk. If you want to protect your data against the failure of two disks, you must switch to Flex-RAID and select RAID 6. To use RAID 6, you must install four or more disks. For more information about how to switch to Flex-RAID, see *Change from X-RAID to Flex-RAID* on page 23.

Add Protection to a Flex-RAID Volume

In certain cases, you can add a disk to a Flex-RAID volume to increase data protection. The following table indicates whether adding a disk for data protection is possible for each Flex-RAID configuration.

Table 4. Flex-RAID levels and data protection

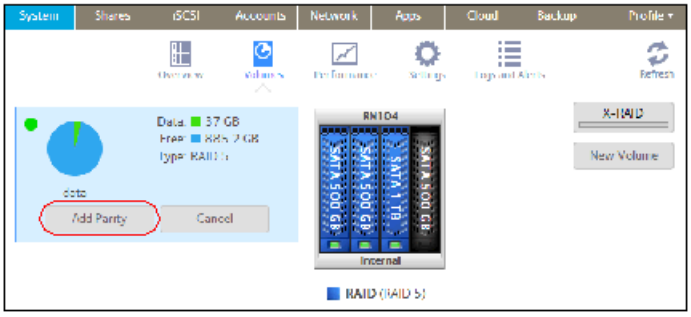
Number of Disks per Volume	RAID Level	Can I add a disk to for data protection?
1	RAID 1	Yes. (Additional disk provides redundancy.)
2	RAID 1	No. (Volume protection is already redundant.)
2 or more	RAID 0	No. (RAID 0 does not offer protection.)
3 or more	RAID 5	Yes. (Additional disk provides dual redundancy and converts the volume to RAID 6.)
4 or more (even number)	RAID 10	No. (Volume protection is already redundant.)
4 or more	RAID 6	No. (Volume is already protected with dual redundancy.)

Disks added to a Flex-RAID volume can be used only for protection. They cannot be used for storage (horizontal expansion). If you want to add a disk for increased storage capacity, you must do one of the following:

- Create a volume using the added disks (see *Create and Encrypt a Volume* on page 28).
- Change the RAID level (see *Change to a Different Flex-RAID Level* on page 25).
- Switch to X-RAID (see *Change from Flex-RAID to X-RAID* on page 24).

To add a protection to a Flex-RAID volume:

1. Add a disk to your ReadyNAS storage system.
   For more information about how to add a disk to your system, see the hardware manual for your system, which is available at *http://support.netgear.com/product/ReadyNAS-OS6.*
2. Select **System > Volumes**.
   The new disk is displayed in the enclosure graphic and is colored black.
3. Select the new disk from the enclosure graphic.
4. Click the **Add Parity** button next to a volume that allows or requires additional protection.



A pop-up screen appears and asks you to confirm your decision.

5. Click the **Yes** button.
   Your data protection is increased in the background while you continue to use your storage system.

You can continue to use your ReadyNAS system while the extra disks are incorporated in the background. The process of increasing data protection can take several hours. If you set up email notifications for your system, you receive an email message when the process finishes. For more information about alert notifications, see *Configure System Alerts* on page 142.

Maintain Volumes

This section covers volume maintenance. Volumes can be srcubbed to check for errors and defragmented to improve disk performance.

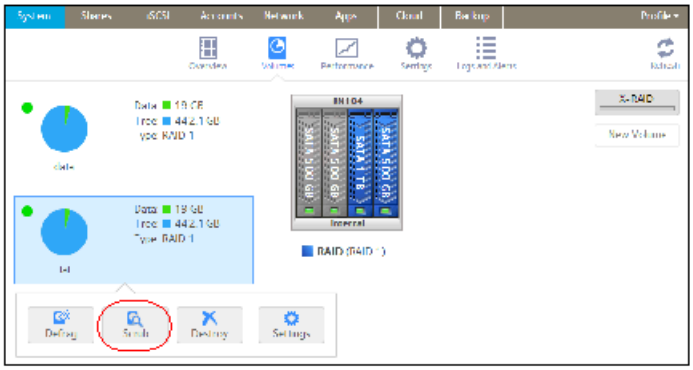
Scrub a Volume

Scrubbing cleans and validates all data on a volume and checks the volume for errors. No data is deleted. Folders, LUNs, and snapshots on the volume remain intact.

Note: Scrubbing is not an erase function.

To scrub a volume:

1. Select **System > Volumes**.
2. Select the volume that you want to scrub.
3. From the pop-up menu that displays, select **Scrub**.



The scrubbing process starts.

The start and completion of the volume scrub are recorded in the system log (see *System Logs* on page 176).

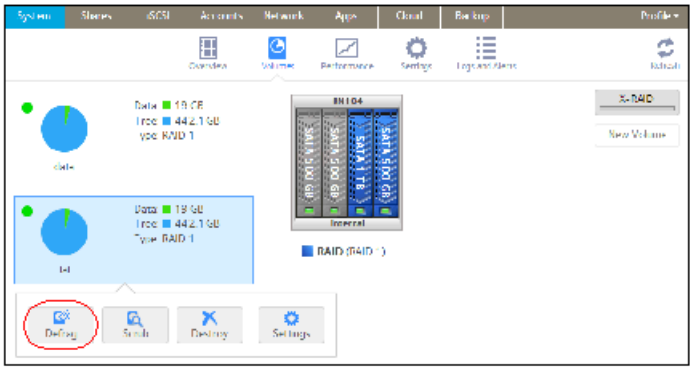
If you set up email notifications for your system, you receive an email message when the process finishes. For more information about alert notifications, see *Configure System Alerts* on page 142.

Defragment a Volume

Over time, deletion, creation, and modification of files can fragment your data. Defragmenting a volume improves disk performance and reduces data fragmentation.

To defragment a volume:

1. Select **System > Volumes**.
2. Select the volume that you want to defragment.
3. From the pop-up menu that displays, select **Defrag**.



The defragmentation process starts.

The start and completion of the volume defragmentation are recorded in the system log (see *System Logs* on page 176).

If you set up email notifications for your system, you receive an email message when the process finishes. For more information about alert notifications, see *Configure System Alerts* on page 142.

Shared Folders

3

This chapter describes how to create, manage, and access shared folders on the ReadyNAS. It includes the following sections:

Note: Without a volume, you cannot configure any shared folders. For information about how to create volumes, see *Create and Encrypt a Volume* on page 28.

Basic Shared Folder Concepts

The volumes on your ReadyNAS can be divided into shared folders and logical unit numbers (LUNs), both of which are logical entities on one or more disks. Shared folders and LUNs enable you to organize data in a volume by type, group, user, department, and so on. A single volume can contain multiple shared folders and LUNs.

Shared folders are NAS data sets that allow data transfer and storage over a network. You can create a maximum of 1,024 shared folders on the ReadyNAS. The local admin page displays shared folders in the following way:

Figure 4. Shared folder with file-sharing protocols enabled

Figure 5. Shared folder with file-sharing protocols disabled

Shared folders are configured independently of one another, even though multiple shared folders can reside on the same volume. You can configure properties of a shared folder, including compression, protection, file-sharing protocols, and access rights. You can also specify whether and how often a snapshot is created. These properties are explained in this chapter.

Data Organization

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

- Documents
- Music
- Pictures
- Videos

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.

Shared Folder Defaults

If you used ReadyCLOUD or the local setup wizard to configure your ReadyNAS storage system, the following shared folders are created for you:

- Backup
- Documents
- Music
- Pictures
- Videos

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

File and Folder Names

A shared folder can contain subfolders to help you organize your data files. If all characters in the file or folder name are alphanumeric, the maximum length of the name is 255 characters. If you use other kinds of characters, the maximum length might be reduced. For example, if a file or folder name uses Kanji or Hanzi characters, the maximum length of the name might be 83 characters.

File-Sharing Protocols

You can access shared folders over a LAN or WAN 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 shared folder on your ReadyNAS from other network-attached devices (for example, a laptop or a tablet) if you enable the file-sharing protocol that the network-attached device uses to access the ReadyNAS. You can enable multiple protocols for an individual shared folder, allowing users to access the shared folder through various methods.

For information about how to configure and enable file-sharing protocols for shared folders, see *Set Network Access Rights to Shared Folders* on page 48.

The following table lists the file-sharing protocols that your ReadyNAS storage system supports.

Table 5. Supported file-sharing protocols

Protocol	Description	Recommendation
SMB(Server Message Block)	Used mainly by Microsoft Windows computers and sometimes by Mac OS X computers, this protocol is enabled by default. It is sometimes	If Windows users access your storage system, enable this protocol.

Protocol	Description	Recommendation
	referred to as the CIFS (Common Internet File Service) file-sharing protocol. SMB uses TCP/IP.	
AFP(Apple File Protocol)	Mac OS X computers use AFP. Your ReadyNAS system supports AFP 3.3.	If only Mac OS X users access your storage system, you can enable this protocol. However, Apple fully supports SMB for Mac OS X, and in a mixed Windows and Mac environment, NETGEAR recommends using SMB only.
NFS(Network File Service)	Linux and Unix computers use NFS. Mac OS X users can access NFS shared folders through console shell access. Your ReadyNAS system supports NFS v3 over UDP and TCP and NFS v4 over TCP.	If Linux or Unix users access your storage system, enable this protocol.
FTP(File Transfer Protocol) and FTPS(FTP with SSL encryption)	Many public file upload and download sites use FTP. The ReadyNAS supports anonymous or user access for FTP clients. You can elect to set up port forwarding to nonstandard ports for passive FTP, allowing clients to initiate a connection to the ReadyNAS.	If users access your storage system using FTP, enable this protocol.
iTunes	Used by iTunes servers.	If users store iTunes media on your storage system, enable this protocol.
ReadyDLNA	Used by DLNA (Digital Living Network Alliance) servers	If users store media served by the ReadyDLNA server, enable this protocol.
Rsync	Fast file transfer protocol that uses a delta-transfer algorithm to send only the differences between the source file and the existing file.	If users access your storage system from a device that supports Rsync, enable this protocol.
UPnP (Universal Plug and Play)	Protocol for automatically controlling router ports to enable network devices to discover other devices.	If users attach UPnP devices to your network, enable this protocol.
HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP with SSL encryption)	Used on the World Wide Web.	If users access your storage system from a device with a web browser, including a smartphone or tablet computer, enable this protocol.
SNMP	An Internet-standard protocol for device management.	If you use SNMP to manage the network, enable this protocol.
SSH (Secure Shell)	Protocol for secure data communication.	If users connect to systems using SSH,enable this protocol.

Protocol	Description	Recommendation
Antivirus	Adds antivirus scanning to new files written using the SMB protocol.	If users access files using the SMP protocol, and you want automatic antivirus scanning of those files, enable this protocol.

Bit Rot Protection

Bit rot is a term sometimes used to describe the gradual changes in disks causing a slow loss of reliability. ReadyNAS OS can use the redundancy in RAID-protected disks to check for bit rot and rewrite corrected data.

RAID levels other than RAID 0 provide data redundancy used to detect, and in some cases correct, disk read errors. Sometimes a read error is a one-time error, but other times, the data on the disk is no longer reliable because of changes to the disk with age (disk bit rot). With bit rot protection turned on, when an error is detected, the data is rewritten, which restores the reliability of the data, in effect restarting the clock on the bit rot.

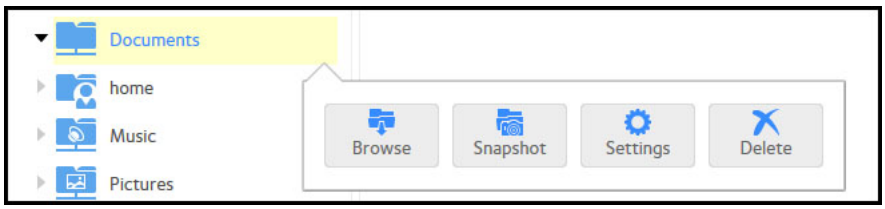
Bit rot protection is available for any folder stored on your ReadyNAS server and is on by default.

Managing Bit Rot Protection

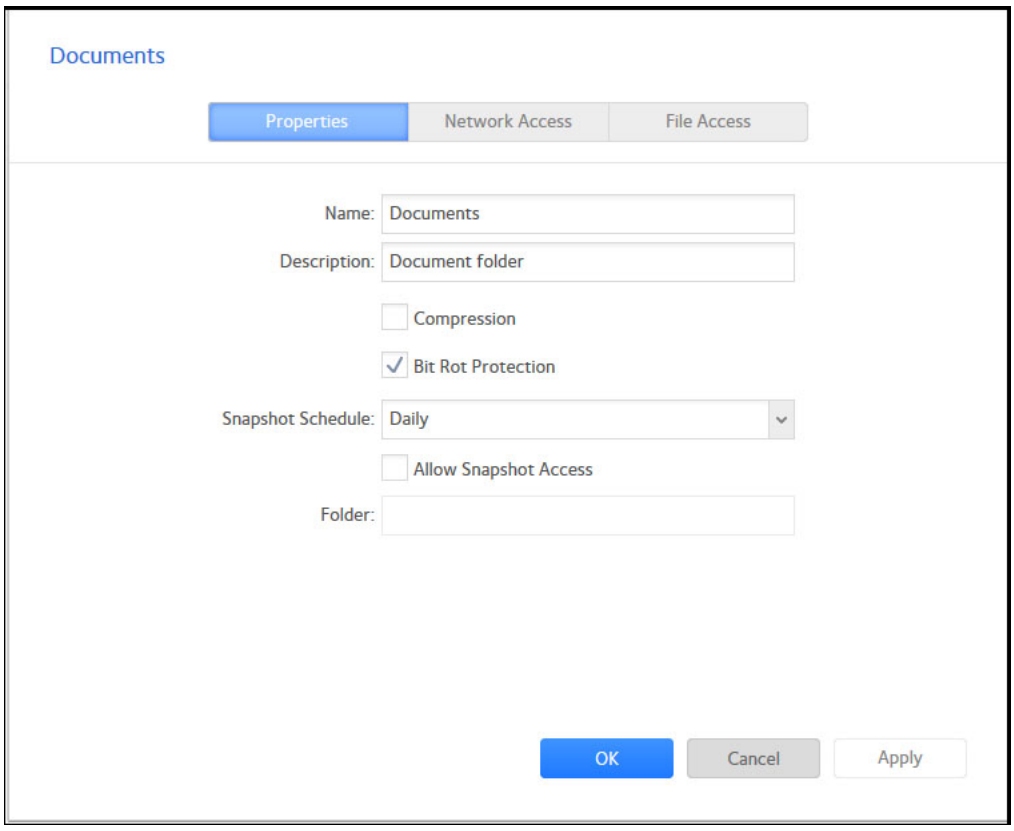
Bit rot protection protects your data from the gradual loss of reliablity of disks as they age. You can verify if bit rot protection is turned on for a folder, turn it on, if it is not, or turn it off. Bit rot protection is on by default for all folders on your ReadyNAS.

To set or change bit rot settings:

1. Log in to your ReadyNAS server.
2. Navigate to the folder (select **Shares > Browse**).
3. Right-click the folder.



4. Double-click the **Settings** button.



5. Examine the **Bit Rot Protection** check box.
   A check indicates that bit rot protection is on.
6. If you want to change the setting, select or clear the check box.

Home Directories

Starting in OS version 6.2, every account on a ReadyNAS owns a private folder under the home folder. The content of your home folder is not visible to the other accounts on the ReadyNAS. You can share the ReadyNAS with other people while keeping content private.

You use it like any other folder on the ReadyNAS. If you use a private Time Machine to back up a Mac, that Time Machine is stored in your home directory. Snapshots, if used, of content within the home folder are also within the home folder, with the same protection.

Manage Shared Folders

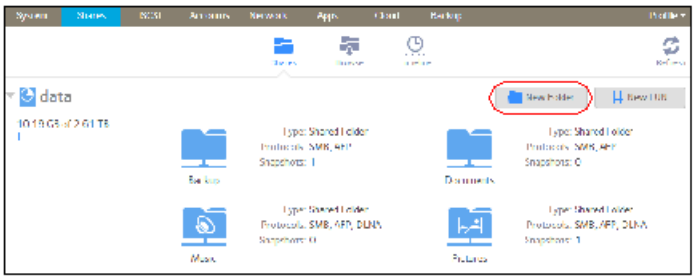
From the local admin page, you can create, modify, delete, and browse shared folders on your ReadyNAS.

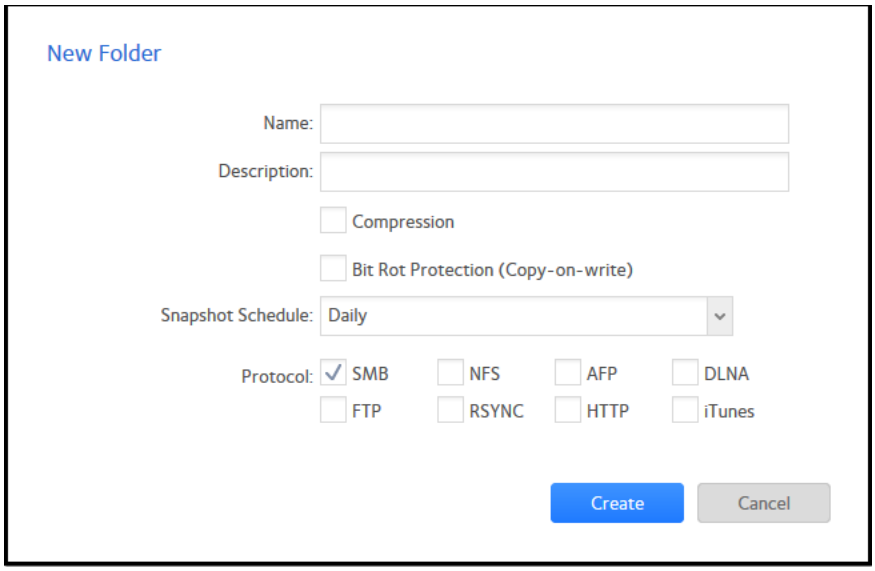
Create a Shared Folder

After you create a volume (see *Create and Encrypt a Volume* on page 28), you can create shared folders on that volume.

To create a shared folder:

1. Login to the Admin page.
2. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Click the **New Folder** button to the right of the volume to which you want to add a shared folder.





4. Configure the settings as explained in the following table:

Item	Description
Name	A unique name to identify the shared folder. Do not include spaces in the name.
Description	An optional description to help identify the shared folder.
Compression	Select the **Compression** check box to enable data compression. Compression saves storage space and increases the speed of data transfers, but the compression and decompression processes require additional resources. By default, the **Compression** check box is cleared.
Continuous Protection	Select the **Continuous Protection** check box to enable data protection through snapshots and configure how often snapshots are taken. By default, the **Continuous Protection** check box is selected. For more information about snapshots, see *Chapter 5, Snapshots* on page 105.

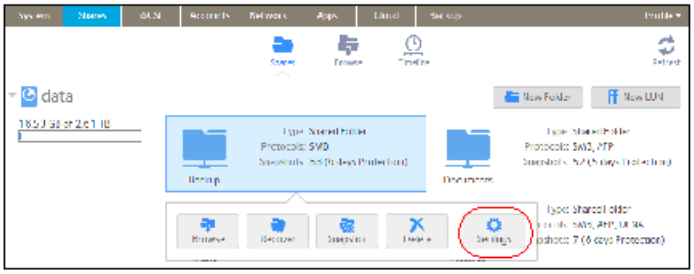
Item	Description	
	Interval	The interval specifies how often a snapshot is taken. Make a selection from the drop-down list: • **Hourly**. A snapshot is taken every hour on the hour. • **Daily**. A snapshot is taken every day at midnight. • **Weekly**. A snapshot is taken every week on Friday at midnight.
Protocol	Select the check box next to each file-sharing protocol that you want to enable on the shared folder. For information about these protocols, see *File-Sharing Protocols* on page 39.	

5. Click the **Create** button.
   The ReadyNAS confirms the creation of a shared folder with the message “Folder or LUN successfully created.”
6. Click the **OK** button.
   The new shared folder is added to the Shares screen. Basic information is displayed to the right of the shared folder.

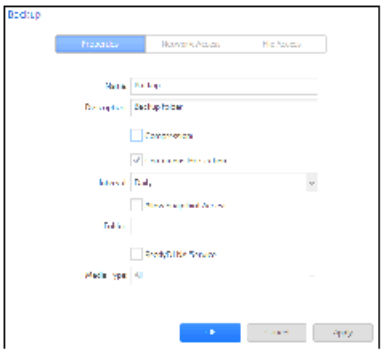
View and Change the Properties of a Shared Folder

To view and change the properties of a shared folder:

1. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
2. Select the shared folder that you want to configure.
3. From the pop-up menu that displays, select Settings.



The folder settings display in a pop-up screen.



4. Change the settings as explained in the following table.

Item	Description	
Properties		
Name	A unique name to identify the shared folder. Do not include spaces in the name. All characters must be alphanumeric.	
Description	An optional description to help identify the shared folder.	
Compression	Select the **Compression** check box to enable data compression. Compression saves storage space and increases the speed of data transfers, but the compression and decompression processes require additional resources.	
Continuous Protection	Select the **Continuous Protection** check box to enable data protection through snapshots and configure how often snapshots are taken. By default, the Continuous Protection check box is selected. For more information about snapshots, see *Chapter 5, Snapshots* on page 105.	
	Interval	The interval specifies how often a snapshot is taken. Make a selection from the drop-down list: • **Hourly**. A snapshot is taken every hour on the hour. • **Daily**. A snapshot is taken every day at midnight. • **Weekly**. A snapshot is taken every week on Friday at midnight.
Allow Snapshot Access	Select the **Allow Snapshot Access** check box to allow snapshot access to anyone who has permission to access the shared folder. The default snapshot access folder displays in the Snapshot folder field. When you allow snapshot access, a subfolder with the name snapshot is created on the shared folder to allow users access to data from past snapshots. Users can then access older versions of their files or recover files that were deleted.	
ReadyDLNA	Select the **ReadyDLNA Service** check box to enable ReadyDLNA for the folder. For more information about ReadyDLNA, see *ReadyDLNA* on page 165.	
	Media Type	Specify the type of media that you want to stream from the folder. Make a selection from the drop-down list: • All • Video • Audio • Images
Network Access		

Item	Description
For information about how to provide folder access to users and groups, see *Set Network Access Rights to Shared Folders* on page 48.	
File Access	
For information about how to configure access rights for files and folders, see *Set Up Access Rights to Files and Folders* on page 57.	

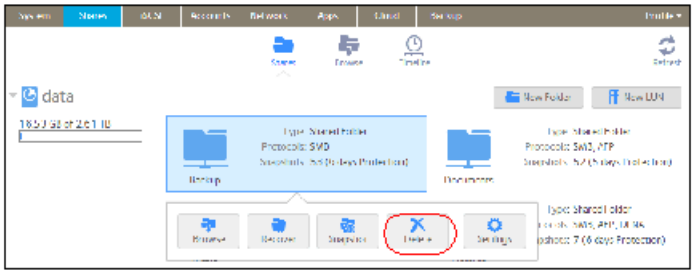
5. Click the **Apply** button.
6. Click the **OK** button.
   Your changes are saved and the pop-up screen closes.

Delete a Shared Folder

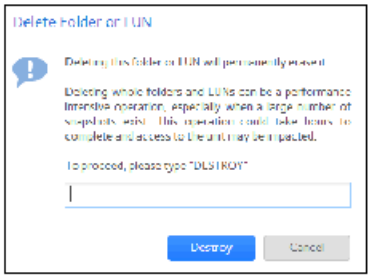
WARNING:
Deleting a shared folder permanently removes the data within that shared folder, including its snapshots.

To delete a shared folder from a volume:

1. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
2. Select the shared folder that you want to delete.
3. From the pop-up menu that displays, select **Delete**.



4. In the pop-up screen that displays, confirm the deletion by typing **DESTROY**.



5. Click the **Destroy** button.

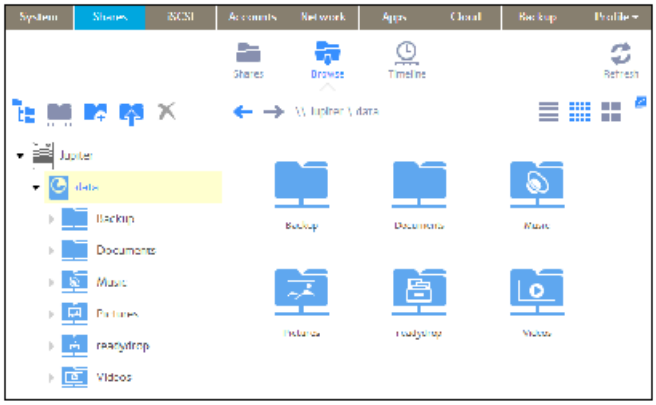
The shared folder is deleted.

Browse a Shared Folder

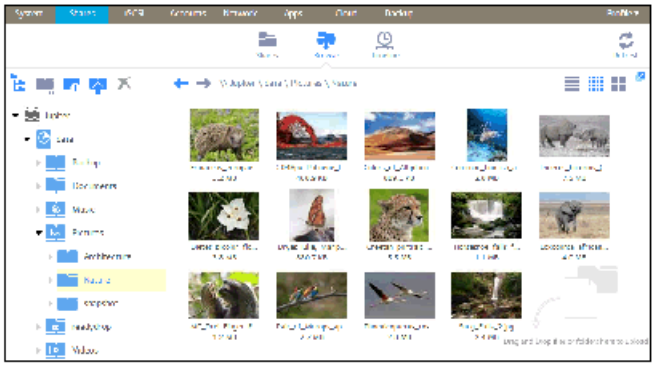
You can browse the contents of a shared folder or external storage device from the local admin page.

To browse data on your ReadyNAS:

1. Select **Shares > Browse**.
   A list of shared folders on each volume displays.



2. Select the shared folder or subfolder that you want to browse.
   The contents of the folder display.



Tip: Use the forward and back (←→) arrows to browse through folders. You can view files and folders as a list with details, as small icons, or as large icons. To change views, select one of the view icons (▪▪▪) at the right side of the screen.

Shared Folder Access Rights

Access rights apply to individual shared folders. For each shared folder, you control the file-sharing protocols that can be used to access the shared folder and the access rights granted to each user, group,

and host. For example, you might want to grant a user read/write permission on one shared folder, read-only permission on another shared folder, and no access rights at all on a third shared folder. By default, all users and groups have read/write access.

The following table lists access right options.

Table 8. Access right options

Access Right	Description
Read-only	The user with this permission can read files on this shared folder, but cannot edit or create files on this shared folder.
Read/write	A user with this permission can read, edit, and create files on this shared folder.
Read-only for everyone with exceptions	Access to this shared folder is read-only for all users except for one or more users who are granted read/write permission.
Read/write for everyone with exceptions	Access to this shared folder is read/write for all users except for one or more users who are granted read-only permission.
Disabled with exceptions	Access to this shared folder is disabled for all users except for one or more users who are granted either read-only or read/write permission.

User and Group Authentication

The way that users and groups are authenticated depends on the user and group management mode that you selected (see *User and Group Management Modes* on page 127):

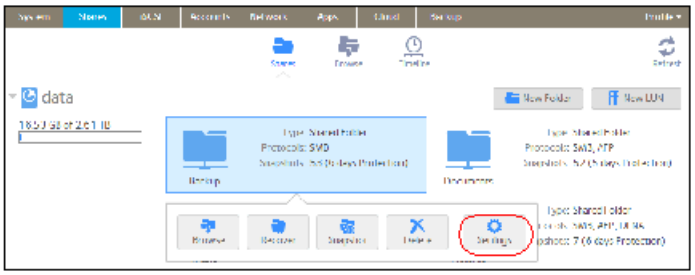
- **Local user database**. If you use the local database, create group and user accounts before you set up shared folder access rights. For more information about creating and managing groups and user accounts, see *Chapter 6, Users and Groups* on page 125.
- **Active Directory**. If you use an external Active Directory, the user and group information is downloaded to the ReadyNAS. User and group access rights are listed when you click the Access tab in the shared folder settings pop-up screen.

Set Network Access Rights to Shared Folders

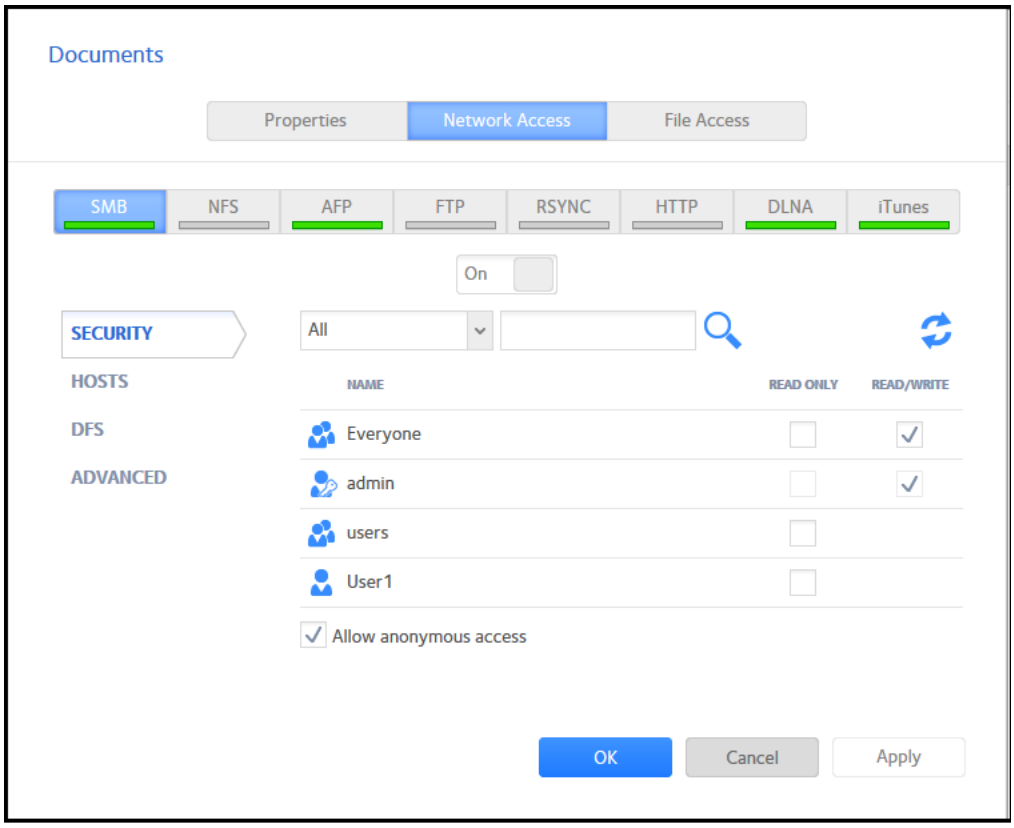
To set the network access rights to an individual shared folder, you configure the network access settings for each file-sharing protocol used to access the shared folder on your storage system.

To set the network access rights for a shared folder:

1. Login to your ReadyNAS.
2. From the ReadyNAS Admin Page select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder that you want to configure.



4. Select **Settings**.
   The shared folder settings display in a pop-up screen.
5. Click the **Network Access** tab.



6. Click one of the file-sharing protocol buttons
   The screen adjusts to display the access properties for the selected protocol.
7. Configure the network access settings for the selected protocol.
   For more information, see the following sections (not all sections apply to all protocols):

- *Configure User and Group Settings* on page 50.
- *Configure Host Settings* on page 52.
- *Configure Rsync Credentials* on page 53.
- *Manage Access to Remote Shared Folders* on page 54.
- *Hide a Shared Folder* on page 56.

8. Set the **On-Off** slider for the selected protocol:
   - To enable the protocol for the selected folder, set the **On-Off** slider so that the slider shows the **On** position.
     The indicator on the protocol button turns green.

     Note: When you enable a file-sharing protocol for an individual shared folder, the protocol is also enabled globally. For more information about global settings, see *Configure Global Settings for File-Sharing Protocols* on page 159.

   - To save the configured access settings but prevent them from taking effect, set the **On-Off** slider so that the slider shows the **Off** position.
     The indicator on the protocol button turns gray.

     Note: When you disable a file-sharing protocol for an individual shared folder, the protocol remains enabled globally so that you can still access other folders that might be using the protocol. For more information about global settings, see *Configure Global Settings for File-Sharing Protocols* on page 159.

9. Click the **Apply** button.
10. Click the **OK** button.
    Your changes are saved and the pop-up screen closes.

Configure User and Group Settings

For SMB, AFP, FTP, and HTTP, you can configure access rights to an individual shared folder for users and groups. User and group settings do not apply to NFS and rsync.

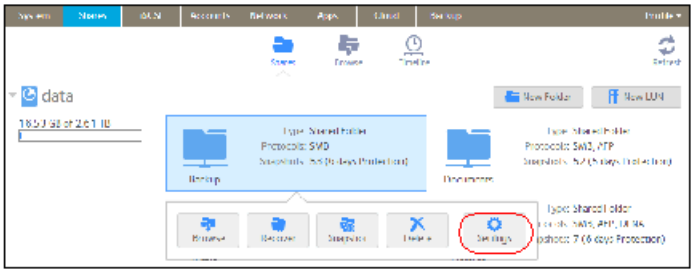
Note: You cannot configure access rights for the ReadyNAS admin ( ) or for Cloud users ( ). For more information about Cloud users, see *Access Shared Folders Using Cloud Services* on page 65.

To configure user and group network access settings:

1. Login to your ReadyNAS.
2. From the ReadyNAS Admin Page select **Shares > Shares**.

A list of shared folders and LUNs on each volume displays.

3. Select the shared folder that you want to configure.



4. Select **Settings**.
   The shared folder settings display in a pop-up screen.
5. On the folder settings pop-up screen, click the **Network Access** tab.
6. Select one of the file-sharing protocol buttons
   The screen adjusts to display the access properties for the selected protocol.
7. Click the **Security** tab on the left side of the pop-up screen.
8. From the drop-down list, select the information that you want to view:
   - **All**. The default group Everyone and all groups that you configured on the local database or that were downloaded from the Active Directory server are displayed. This is the default setting.
   - **Users**. Only the individual users that you configured on the local database or that were downloaded from the Active Directory server are displayed.
   - **Groups**. Only the groups that you configured on the local database or that were downloaded from the Active Directory server are displayed.

   For information about using the local database or an Active Directory, see *User and Group Management Modes* on page 127.

   Tip: To search for a particular user or group, use the search field next to the **Search** icon ( ).To update the user and group information, click the **Refresh** icon ( ).

9. For each individual user ( ) and group ( ) that you want to access the shared folder, select one of the following check boxes:
   - **Read Only**. The selected user or group is permitted only to read files on the shared folder.
   - **Read/Write**. The selected user or group is permitted to read, edit, create, and delete files on the shared folder.

   Note: If the ReadyNAS uses the local database, you can select the default group Everyone to grant all users and groups read-only or read/write access.

10. (Optional for SMB and AFP) Allow anonymous access to the shared folder.

If the ReadyNAS uses the local database and you grant the default group Everyone access, you can select the **Allow anonymous access** check box to allow anonymous access to the shared folder. In this situation, users are not required to provide their account credentials when accessing the shared folder.

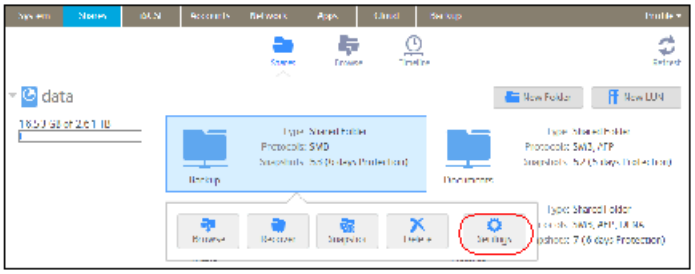
11. Click the **Apply** button.
12. Click **OK** button.
    Your changes are saved and the pop-up screen closes.

Configure Host Settings

For SMB, NFS, FTP, rsync, and HTTP, you can configure access rights for users on hosts. Host settings do not apply to AFP. The access rights that you configure for one host apply to all users on the host. For NFS, you can also configure the access rights that apply to any host, and, for individual hosts, you can configure whether root access is granted.

To add a host and configure host access settings:

1. Login to your ReadyNAS.
2. From the ReadyNAS Admin Page select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder that you want to configure.



4. Select **Settings**.
   The shared folder settings display in a pop-up screen.
5. On the folder settings pop-up screen, click the **Network Access** tab.
6. Click one of the file-sharing protocol buttons
   The screen adjusts to display the access properties for the selected protocol.
7. Click the **Hosts** tab on the left side of the pop-up screen.

Note: If the host access list is empty, any host is allowed to access the shared folder. If you add at least one host to the list, access to the shared folder is restricted to hosts on the list only.

8. Click the + button ( ).

9. Enter the host IP address in the **IP address** field.
10. Click the **Add** button.
    The host is added to the host access list.

> **Note:** For SMB, the access rights for each host depend on the access rights of the user.

11. (Optional for rsync) Select the default access rights for users on the listed hosts:
    - **Read Only**. The users on the listed hosts are permitted only to read files on the shared folder.
    - **Read/Write**. The users on the listed hosts are permitted to read, edit, create, and delete files on the shared folder.
12. (Optional for NFS and FTP) For each host on the host access list, select one of the following check boxes:
    - **Read Only**. The users on the selected host are permitted only to read files on the shared folder.
    - **Read/Write**. The users on the selected host are permitted to read, edit, create, and delete files on the shared folder.

> **Note:** For NFS only, you can set access rights for AnyHost, which is a default entry in the host access list. You cannot grant root access to AnyHost.

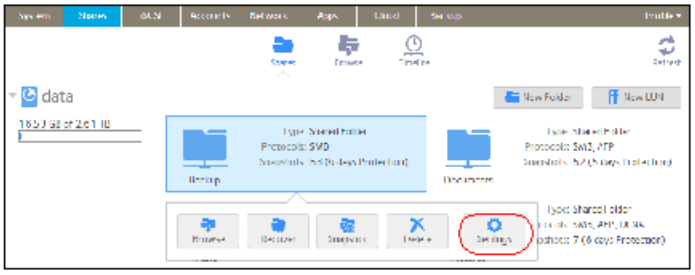
13. (Optional for HTTP) For each host on the host access list, you can grant or deny access rights.
14. (Optional for NFS) For each host for which you want to grant the users root access, select the **Root Access** check box.
15. Click the **Apply** button.
    Your changes are saved.
16. Click the **OK** button.
    Your changes are saved and the pop-up screen closes.

Configure Rsync Credentials

You can require users to enter rsync credentials when accessing your storage system using rsync.

To require credentials for rsync sessions:

1. Login to your ReadyNAS.
2. From the ReadyNAS Admin Page select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder that you want to configure.



4. Select **Settings**.
   The shared folder settings display in a pop-up screen.
5. On the folder settings pop-up screen, click the **Network Access** tab.
6. Click the **RSYNC** file-sharing protocol button.
   The screen adjusts.
7. Click the **Security** tab on the left side of the pop-up screen.
8. Select the **Enable Password Protection** check box.
9. Click the + button ( ) and create at least one rsync user account and password.

   Note: Rsync credentials are completely separate from your ReadyNAS storage system's user accounts.

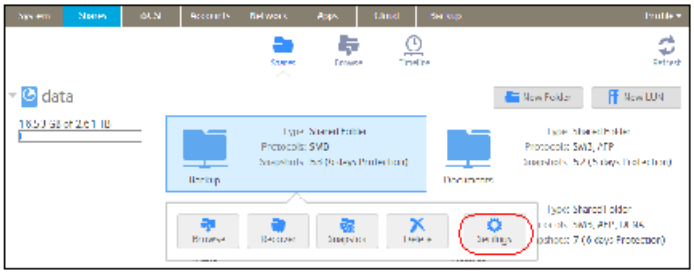
10. Click the **Apply** button.
11. Click the **OK** button.
    Your changes are saved and the pop-up screen closes.

Manage Access to Remote Shared Folders

The SMB protocol allows you to access remote shared folders on other network-attached devices and treat them as if they resided locally on your ReadyNAS system.

To enable access to a remote shared folder:

1. Login to your ReadyNAS.
2. From the ReadyNAS Admin Page select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder that you want to configure.



4. Select **Settings**.
   The shared folder settings display in a pop-up screen.
5. On the folder settings pop-up screen, click the **Network Access** tab.
6. Click the **SMB** file-sharing protocol button.
   The window adjusts.
7. Click the **DFS** tab on the left side of the pop-up screen.
8. Select the **Enable DFS Root** check box.
9. Click the + button ( ) above the list of remote shared folders.

10. Enter the following information:
    - **Name**. The name of the remote shared folder, as you want it to appear on your ReadyNAS.
    - **Address**. The IP address of the network-attached device where the remote shared folder resides.
    - **Remote share**. The name of the remote shared folder, as it appears on the network-attached device.
11. Click the **Add** button.
    The new remote shared folder appears on the list.
12. Click the **Apply** button.
13. Click the **OK** button.
    Your changes are saved and the pop-up screen closes.
14. Make sure that the remote shared folder on the network-attached device is configured for file sharing.

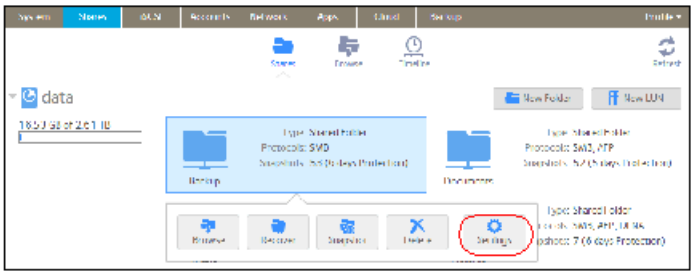
You can now access the remote shared folder from your ReadyNAS system using the SMB protocol. For information about how to access your system using the SMB protocol, see *Use a Windows Device* on page 61 or *Use a Mac OS X Device* on page 62.

Hide a Shared Folder

This feature is available for SMB only. Hiding a folder prevents users from discovering the folder unless they explicitly specify the folder name in the browse path.

To configure advanced settings for SMB:

1. Login to your ReadyNAS.
2. From the ReadyNAS Admin Page select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder that you want to configure.



4. Select **Settings**.
   The shared folder settings display in a pop-up screen.
5. On the folder settings pop-up screen, click the **Network Access** tab.
6. Click the **SMB** file-sharing protocol button.
   The screen adjusts.
7. Click the **Advanced** tab on the left side of the pop-up screen.
8. Select the **Hide this folder** check box.
9. Click the **Apply** button.
10. Click the **OK** button.
    Your changes are saved and the pop-up screen closes.

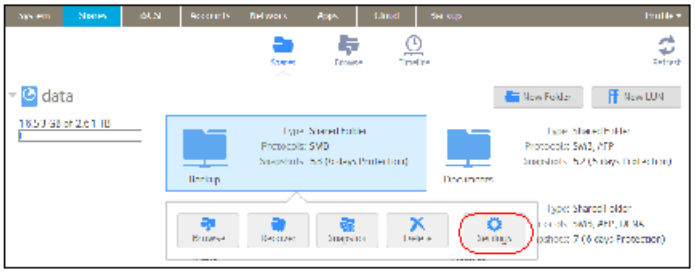
Enable WebDAV

This feature is available only for HTTP (which includes HTTPS, which is required in some cases). WebDAV is an extension of the HTTP protocol that facilitates document management and editing. Features of WebDAV include maintenance of document properties such as author, creation date, and modification date, and it provides overwrite protection. Access is to a shared folder and the contained files.

After you enable WebDAV access, you can access the files in the shared folder over the Internet from a computer or mobile device in a manner similar to accessing the files over a LAN or through a VPN. The specifics depend on the device and application using WebDAV.

To enable WebDAV on an individual shared folder:

1. Login to your ReadyNAS.
2. From the ReadyNAS Admin Page select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder that you want to configure.



4. Select **Settings**.
   The shared folder settings display in a pop-up screen.
5. On the folder settings pop-up screen, click the **Network Access** tab.
6. Click the **HTTP** file-sharing protocol button.
   The screen adjusts.
7. Click the **WEBDAV** tab on the left side of the pop-up screen.
8. Select the **Enable WebDAV** check box.
9. Click the **Apply** button.
10. Click the **OK** button.
    Your changes are saved and the pop-up screen closes.

Set Up Access Rights to Files and Folders

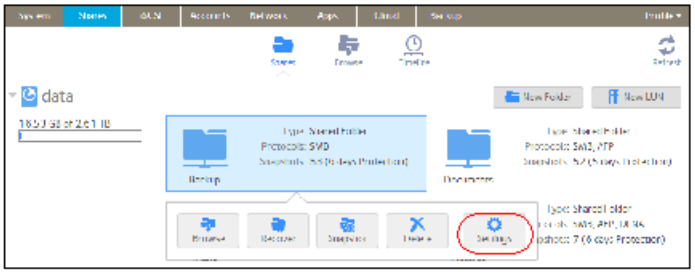
For each individual shared folder, you can configure the default access rights to files and folders.

Change Default Access Rights to Files and Folders

By default, owners, groups, and anyone else with access to the shared folder has read/write access to all files and folders on the shared folder.

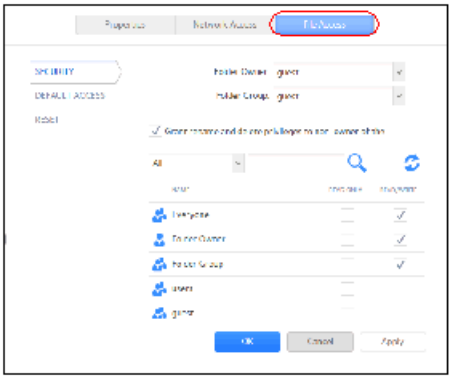
To change the default access rights to files and folders on an individual shared folder:

1. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
2. Select the shared folder that you want to configure.
3. From the pop-up menu that displays, select **Settings**.



The shared folder settings display in a pop-up screen.

4. Click the **File Access** tab on the pop-up screen.



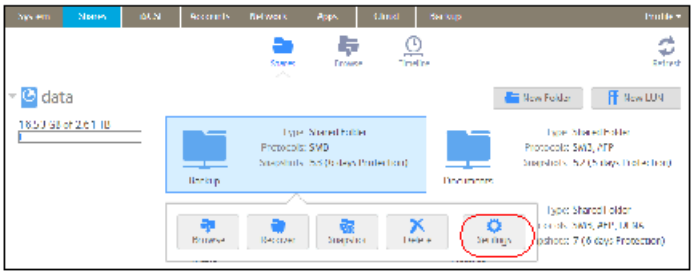
5. Configure the file and folder access rights as explained in the following table:

Item	Setting
Folder Owner	You can assign a single user or the administrator as the folder owner. By default, the folder owner is set to guest.
Folder Group	You can assign a single group, a single user, or the administrator as the folder group. By default, the folder group is set to guest.

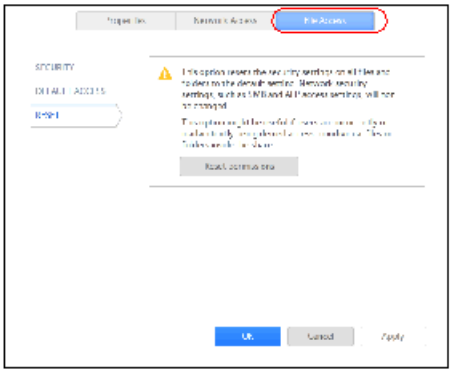
Item	Setting
Folder Owner Rights	Permissions granted to the folder owner. Select one of the check boxes: • **No box selected**. The folder owner does not have access rights to the folder. • **Read Only**. The folder owner has read-only access to the folder. • **Read/Write**. The folder owner has read/write access to the folder. This is the default setting.
Folder Group Rights	Permissions granted to members of the same group as the owner's primary group. Select one of the check boxes: • **No box selected**. Members of the group have no access to folders that are owned by a member of the group. • **Read Only**. Members of the group have read-only access to folders that are owned by a member of the group. • **Read/Write**. Members of the group have read/write access to folders that are owned by a member of the group. This is the default setting.
Folder Everyone Rights	Permissions granted to users who are not the folder owner and not members of the folder group. Select one of the check boxes: • **No box selected**. No one outside the folder group has access rights to the folder. • **Read Only**. Anyone outside folder group has read-only access to the folder. • **Read/Write**. Anyone outside the folder group has read/write access to the folder. This is the default setting.

To restore the default file and folder access rights on an individual shared folder:

1. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
2. Select the shared folder that you want to configure
3. From the pop-up menu that displays, select **Settings**.



   The shared folder settings display in a pop-up screen.
4. Click the **File Access** tab on the pop-up screen.



5. Click the **Reset** tab.
6. Click the **Reset permissions** button.
   The default access rights are restored. Owners, groups, and anyone else with access to the shared folder gains read/write access to all files and folders on the shared folder.

Access Shared Folders from a Network-Attached Device

You can remotely access shared folders and snapshots on your storage system using other network-attached devices, such as a laptop or tablet. The network-attached device must support one of the enabled file-sharing protocols. How a shared folder is accessed depends on the OS of the network-attached device, the file-sharing protocols that you enabled for shared folder access, and the access rights that you granted (see *Shared Folder Access Rights* on page 47).

Note: For snapshots to be accessible to users from their network-attached devices, you need to select the **Allow snapshot access** check box on the shared folder settings pop-up screen. For more information, see *View and Change the Properties of a Shared Folder* on page 44.

Use 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 your LAN, you must configure port forwarding on your router. For more information, see your router user manual.

To access a shared folder using a web browser:

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

For more information, see *Set Network Access Rights to Shared Folders* on page 48.

2. Launch a web browser.
3. Navigate to the ReadyNAS system and shared folder you want to access using the following syntax:
   http://<hostname>/<shared folder>
   where:
   - <hostname> is the name that you assigned to your ReadyNAS system or the default host name if you did not change it.
   - <shared folder> is the name of the shared folder that you want to access.

   Note: If you cannot access the ReadyNAS using its host name, try entering http://<ReadyNAS IP address> in the Windows Explore address bar instead. <ReadyNAS IP address> is the IP address of the ReadyNAS.

   - (Optional) 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.

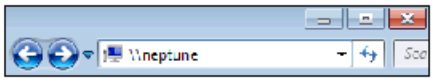
   Your shared folders are displayed in a web page.

Use a Windows Device

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

To access a shared folder using a network-attached Windows device:

1. Ensure that the SMB file-sharing protocol is enabled on your ReadyNAS system.
   For more information, see *Set Network Access Rights to Shared Folders* on page 48.
2. Enter \\<hostname> in the Windows Explorer address bar.

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

   Note: If you cannot access the ReadyNAS using its host name, try entering \\<ReadyNAS IP address> in the Windows Explore address bar instead. <ReadyNAS IP address> is the IP address of the ReadyNAS.

   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.

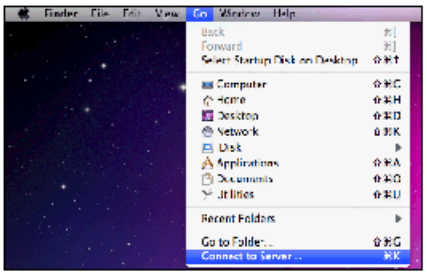
Windows Explorer displays the contents of all available shared folders on your ReadyNAS system.

Use a Mac OS X Device

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

To access a shared folder using a network-attached OS X device:

1. Ensure that the AFP or SMB file-sharing protocol is enabled on your ReadyNAS system.
   For more information, see *Set Network Access Rights to Shared Folders* on page 48.
2. In Finder, select **Go > Connect to Server**.

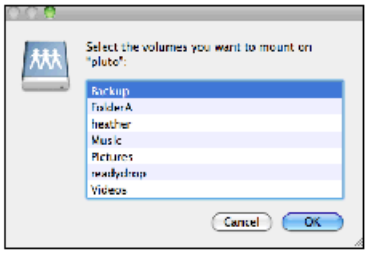


   The Connect to Server dialog box displays.
3. Connect to your ReadyNAS system as follows:
   - If you are using the AFP file-sharing protocol, enter the following command in the **Server Address** field:
     afp://<hostname>
   - If you are using the SMB file-sharing protocol, enter the following command in the **Server Address** field:
     smb://<hostname>

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

   Note: If you cannot access the ReadyNAS using its host name, try entering **afp://**<ReadyNAS IP address> or **smb://**<ReadyNAS IP address> instead. <ReadyNAS IP address> is the IP address of the ReadyNAS.
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 shared folders volumes.



6. Select the volume or volumes (shared folder or folders) you want to access and click the **OK** button. Finder displays the volume contents.

Use a Linux or Unix Device

You can access shared folders 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 SMB user accounts. In mixed environments where you want SMB 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 setting.

To access an SMB shared folder using a network-attached Linux or Unix device:

1. Ensure that the SMB file-sharing protocol is enabled on your ReadyNAS system.
   For more information, see *Set Network Access Rights to Shared Folders* on page 48.
2. Using a terminal program, enter the following command:
   mount [-t smb -o username= <user name> ,**password=** <password> **] //** <ReadyNAS IP address> **/** <shared folder name> <mount point>
   - <user name> **and** <password> match the user name and password on the **ReadyNAS**.
   - <ReadyNAS IP address> is the IP address of the ReadyNAS.
   - <shared folder name> is the name of the shared folder that you want to access.
   - <mount point> is the name of an empty folder on the Linux or Unix device.

To access an NFS shared folder 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 *Set Network Access Rights to Shared Folders* on page 48.
2. Using a terminal program, enter the following command:
   mount [-t nfs] <ReadyNAS IP address> **:/** <volume name> **/** <shared folder name> <mount point>

- <ReadyNAS IP address> is the IP address of the ReadyNAS.
- <volume name> is the name of the volume on which the shared folder resides.
- <shared folder name> is the name of the shared folder that you want to access.
- <mount point> is the name of an empty folder on the Linux or Unix device.

Use FTP and FTPS

You can use FTP and FTPS to access any shared folders 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 shared folder using FTP:

1. Ensure that the FTP file-sharing protocol is enabled on your ReadyNAS system.
   For more information, see *Set Network Access Rights to Shared Folders* on page 48.
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.

Use Rsync

You can use Rsync to access any shared folders that are enabled for the Rsync file-sharing protocol. Instead of browsing shared folders 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 copies only 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 shared folders using Rsync:

1. Ensure that the Rsync file-sharing protocol is enabled on your ReadyNAS storage system.
   For more information, see *Set Network Access Rights to Shared Folders* on page 48.
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 shared folder.

For more information about Rsync shared folder access credentials, see *Configure Rsync Credentials* on page 48. For more information about Rsync terminal program commands, visit *http://rsync.samba.org*.

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

Access Shared Folders Using Cloud Services

Several cloud-based services are preinstalled on your ReadyNAS system, including ReadyCLOUD and ReadyNAS Remote. You can use these services to remotely access your storage system.

Use ReadyCLOUD

ReadyCLOUD is an online service that you use to discover and set up ReadyNAS storage systems on your network. After you discover your ReadyNAS system using ReadyCLOUD, you can use ReadyCLOUD to securely access and manage your system from anywhere that has an Internet connection.

For more information about discovering your device using ReadyCLOUD or creating a ReadyCLOUD account, see *Discover and Set Up Your ReadyNAS* on page 13.

Using ReadyCLOUD involves these high-level steps:

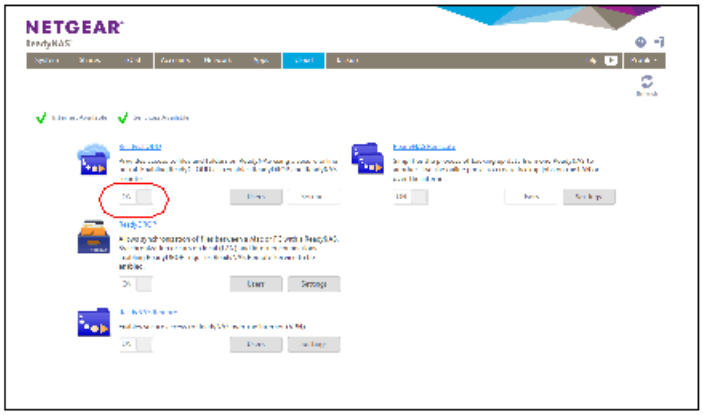
1. Add your ReadyNAS system to your ReadyCLOUD account.
   See *Join ReadyCLOUD* on page 65.
2. (Optional) Grant access to ReadyCLOUD users.
   See *Add ReadyCLOUD Users* on page 66.
3. Access your data and manage your ReadyNAS system using ReadyCLOUD.
   See *Access Your System Using ReadyCLOUD* on page 72.

Join ReadyCLOUD

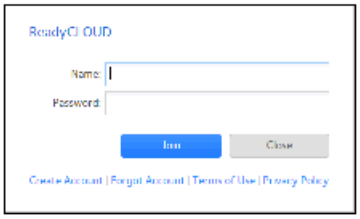
The ReadyCLOUD service is preinstalled on your ReadyNAS storage system. Before you can access your system using ReadyCLOUD, you must add your system to your ReadyCLOUD account.

To add your ReadyNAS system to ReadyCLOUD:

1. Login to your ReadyNAS.
2. On the local admin page, select the **Cloud** tab.
3. Set the **On-Off** slider so the slider shows the **On** position to enable ReadyCLOUD.



4. On the pop-up screen that displays, enter your ReadyCLOUD account credentials.



5. Click the **Join** button.
   Your system is added to ReadyCLOUD.

   The ReadyCLOUD account that you used to add your system to ReadyCLOUD is automatically granted access to your system as the ReadyCLOUD admin.

You can now use the ReadyCLOUD web interface to access your system from anywhere with an Internet connection.

For information about granting access to ReadyCLOUD users, see *Add ReadyCLOUD Users* on page 66.

Note: If you decide to remove your system from ReadyCLOUD, any ReadyCLOUD users that you added will lose access to the system.

For more information about using the ReadyCLOUD web portal, see *Access Your System Using ReadyCLOUD* on page 72.

Add ReadyCLOUD Users

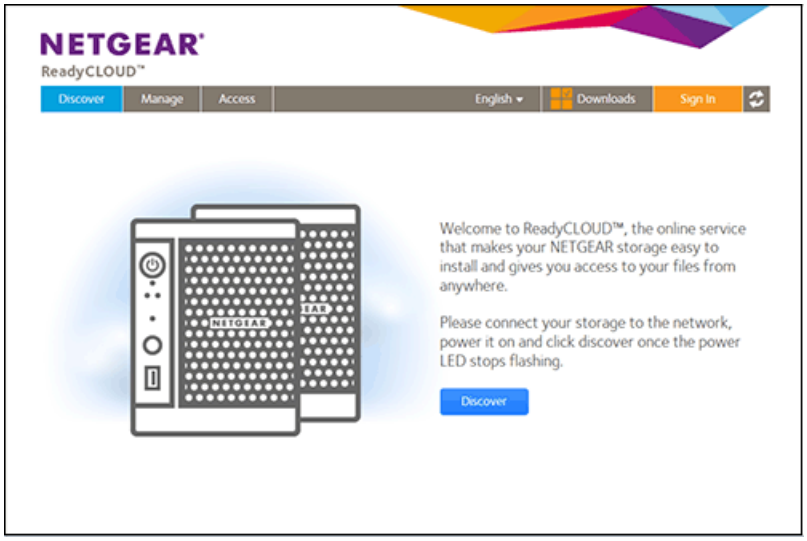
After you add your system to ReadyCLOUD, you can allow other ReadyCLOUD users to access your system using their ReadyCLOUD accounts.

For more information about joining ReadyCLOUD, see *Join ReadyCLOUD* on page 65.

Note: When you grant access to a ReadyCLOUD user, that user automatically gains access to your system from ReadyCLOUD and ReadyNAS Remote.

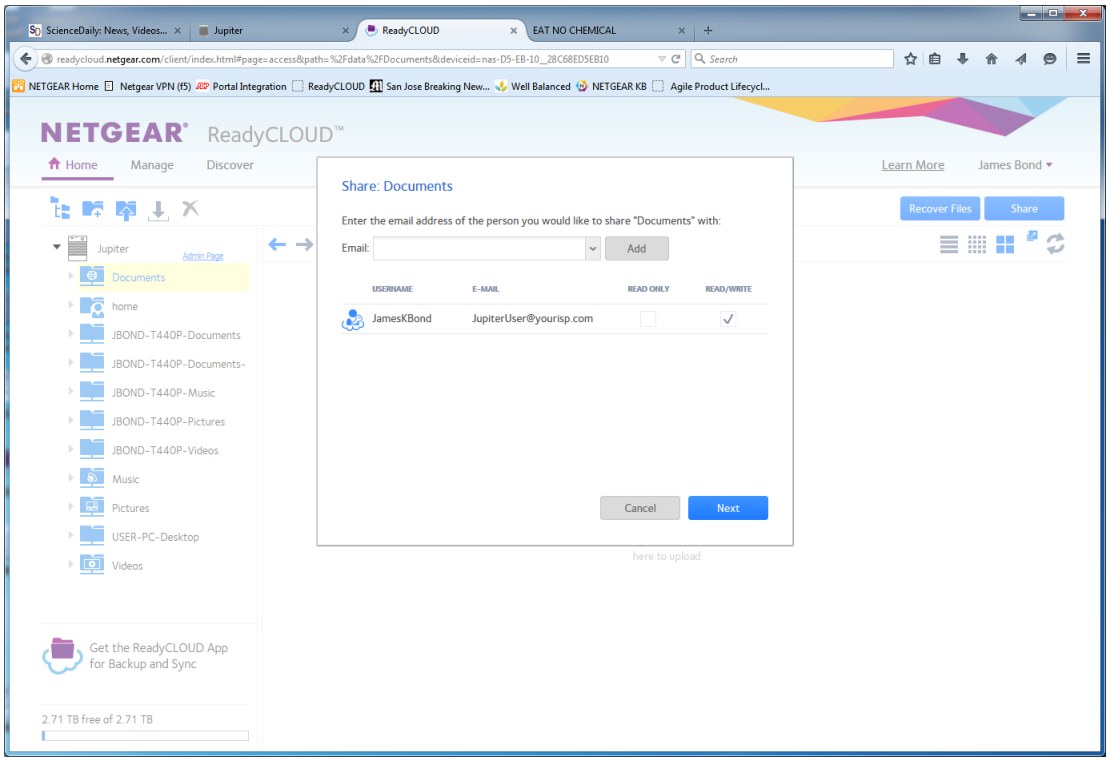
To grant access to ReadyCLOUD users:

1. Open a web browser and visit *http://readycloud.netgear.com*.



2. From the top menu bar, select **Sign In** near the top right corner of the screen.

3. Enter your ReadyCLOUD account credentials and click the **Sign In** button.
   You are signed in to ReadyCLOUD and a page for your previously added ReadyNAS displays.
4. From the top menu bar, select **Home**.
5. Select the folder you want to share.
6. Click the **Share** button on the upper right.
   The Share: Documents window opens.



7. Enter the user email address and click the **Add** button.
8. If the email address matches someone with a ReadyCLOUD account, the user name is displayed next to the email address. Click the **Add** button to confirm.
   Otherwise, the email address is added to the list with **Pending** in the **User name** field.
9. Click the **Next** button.
   If any of your folders permit anonymous access, a window listing the those documents opens. You can remove access before continuing.
10. Click the **Finish** button.
    Users without an existing ReadyCLOUD account receive an email with a link to create a ReadyCLOUD accout. They must create a ReadyCLOUD account before accessing your files.

Note: When you grant access to a ReadyCLOUD user, that user is also added to the Cloud Users list on the local admin page for your system.

For more information about using the ReadyCLOUD portal, see *Access Your System Using ReadyCLOUD* on page 72.

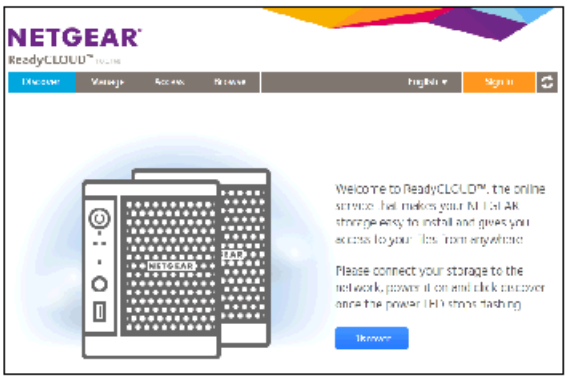
Delete ReadyCLOUD Users

You must use the ReadyCLOUD web portal to delete a ReadyCLOUD user. When you delete a ReadyCLOUD user, that user can no longer use his or her ReadyCLOUD account to access your ReadyNAS system.

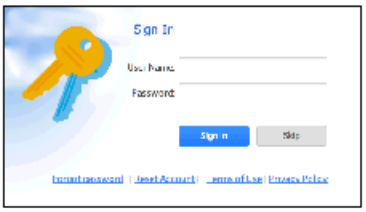
Note: When you delete a ReadyCLOUD user, that user automatically loses access to your system from ReadyCLOUD and ReadyNAS Remote.

To delete a ReadyCLOUD user:

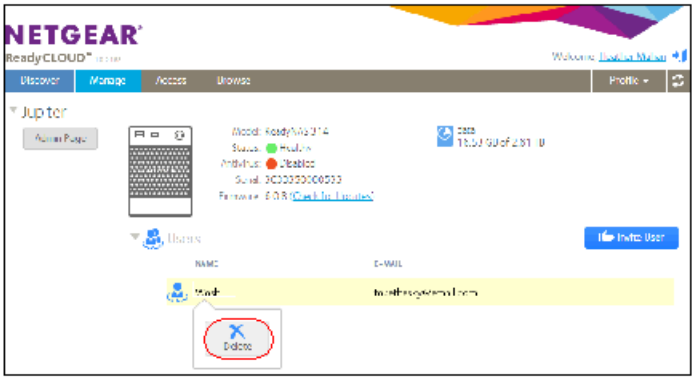
1. Open a web browser and visit *http://readycloud.netgear.com*.



2. From the top menu bar, select **Sign In** near the top right corner of the screen.



3. Enter your ReadyCLOUD account credentials and click the **Sign In** button.
   You are signed in to ReadyCLOUD.
4. From the top menu bar, select **Manage**.
   The ReadyNAS systems that you added to ReadyCLOUD using this account display.
5. From the system's **User** list, select the ReadyCLOUD user that you want to delete.



6. Select **Delete**.
7. Confirm the deletion.
   The selected ReadyCLOUD user can no longer use his or her ReadyCLOUD account to access your ReadyNAS system.

Manage Permissions for ReadyCLOUD Users

By default, when you grant access to ReadyCLOUD users, those users can view and edit shared folders on your ReadyNAS system.

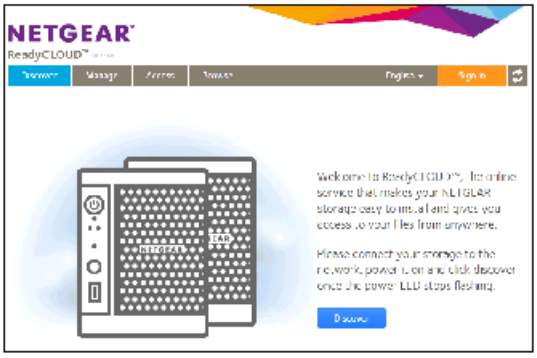
You use the ReadyCLOUD web portal to configure the access rights to individual shared folders. For each shared folder, you can specify which ReadyCLOUD users have permission to view or edit the folder. The following table lists the access right options.

Table 10. Access right options

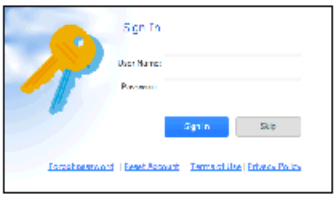
Access Right	Description
Read-only	The user with this permission can read files on this shared folder, but cannot edit or create files on this shared folder.
Read/write	A user with this permission can read, edit, and create files on this shared folder.
Read-only for everyone with exceptions	Access to this shared folder is read-only for all users except for one or more users who are granted read/write permission.
Read/write for everyone with exceptions	Access to this shared folder is read/write for all users except for one or more users who are granted read-only permission.
Disabled with exceptions	Access to this shared folder is disabled for all users except for one or more users who are granted either read-only or read/write permission.

To set the ReadyCLOUD access rights for a shared folder:

1. Open a web browser and visit *http://readycloud.netgear.com*.



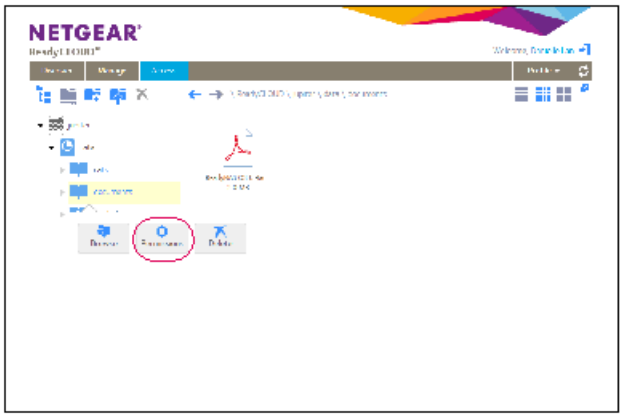
2. From the top menu bar, select **Sign In** near the top right corner of the screen.



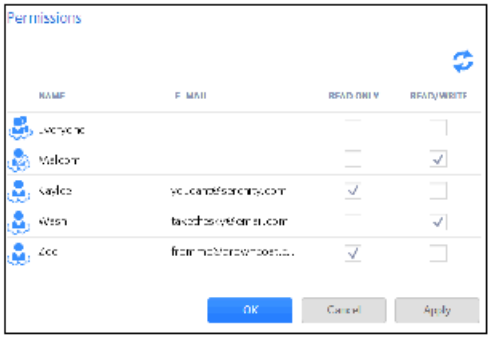
3. Enter your ReadyCLOUD account credentials and click the **Sign In** button.
4. From the top menu bar, select **Access**.
   The ReadyNAS systems that you added to ReadyCLOUD using this account are displayed.

Note: You can also set ReadyCLOUD permissions from the Browse screen.

5. Select the shared folder that you want to configure.



6. Select **Permissions**.



7. For each ReadyCLOUD user that you want to access the shared folder, select one of the following check boxes:
   - **Read Only**. The selected user or group is permitted only to read files on the shared folder.
   - **Read/Write**. The selected user or group is permitted to read, edit, create, and delete files on the shared folder.

   Note: You can select the default group Everyone and set read-only or read/write access for all ReadyCLOUD users.

8. Click the **Apply** button.
9. Click the **OK** button.
   Your changes are saved.

Access Your System Using ReadyCLOUD

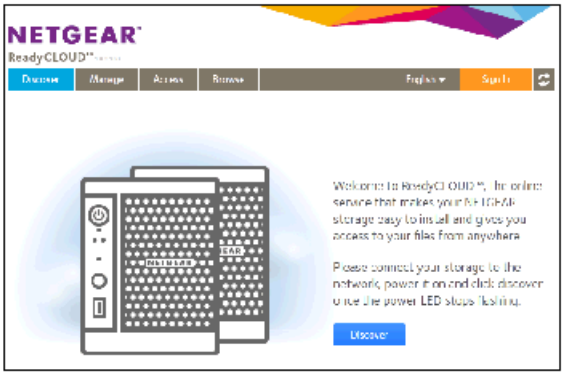
If you added your system to ReadyCLOUD, you and your ReadyCLOUD users can use the ReadyCLOUD portal to access your ReadyNAS from anywhere with an Internet connection.

For information about joining ReadyCLOUD, see *Join ReadyCLOUD* on page 65.

For information about adding ReadyCLOUD users, see *Add ReadyCLOUD Users* on page 66.

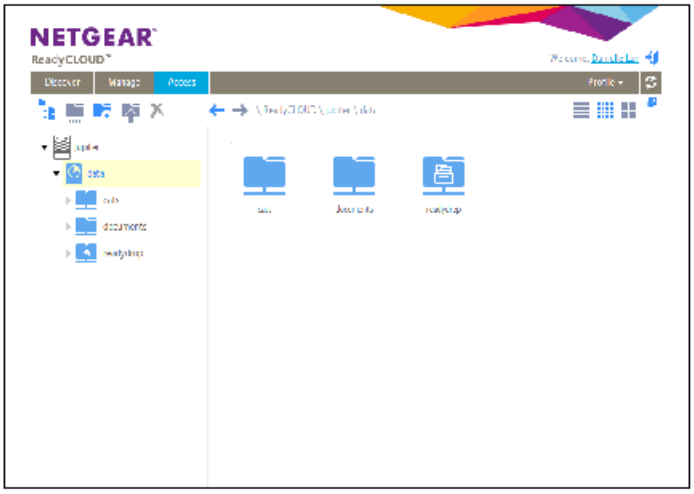
To access your data and manage your ReadyNAS using ReadyCLOUD:

1. Open a web browser and visit *http://readycloud.netgear.com*.



2. From the top menu bar, select **Sign In** near the top right corner of the screen.

3. Enter your ReadyCLOUD account credentials and click the **Sign In** button.
   You are signed in to ReadyCLOUD. You can now use the ReadyCLOUD web interface to access your data and manage any systems that you added to your ReadyCLOUD account.



Use ReadyNAS Remote

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

ReadyNAS Remote uses preinstalled software on your ReadyNAS system and a small software program for your Windows or Mac computer.

Using ReadyNAS Remote involves these high-level steps:

1. Enable ReadyNAS Remote on your ReadyNAS storage system.
   See *Enable ReadyNAS Remote* on page 74.
2. Grant access to ReadyNAS Remote users.
   See *Add ReadyNAS Remote Users* on page 75.
3. Install ReadyNAS Remote client software on your computer.
   See *Install the ReadyNAS Remote Client on Remote Devices* on page 77.
4. Access your shared folders.
   See *Access Shared Folders Using ReadyNAS Remote* on page 77.

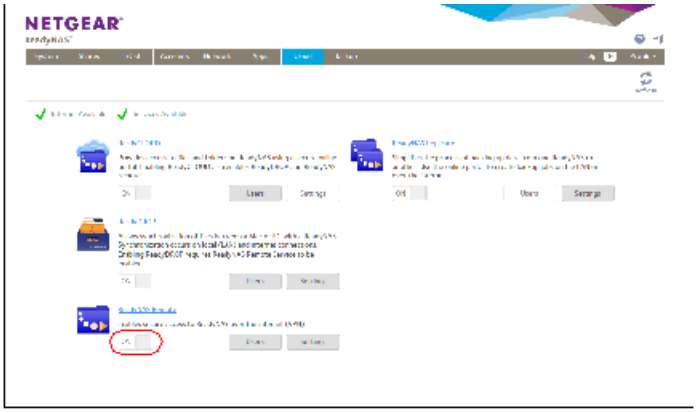
For more information about ReadyNAS Remote, see the *ReadyNAS Remote User Manual*.

Enable ReadyNAS Remote

The ReadyNAS Remote service is preinstalled on your ReadyNAS storage system. Before you can access shared folders using ReadyNAS Remote, you must enable it on your ReadyNAS system.

To enable ReadyNAS Remote:

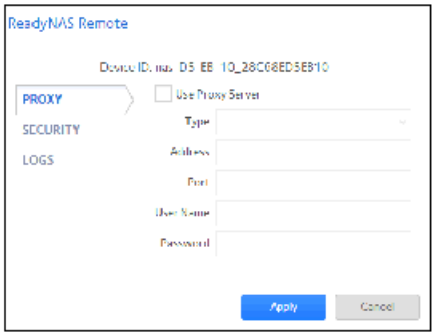
1. Login to your ReadyNAS.
2. On the local admin page, click the **Cloud** tab.
3. Set the **On-Off** slider so that the slider shows the **On** position next to ReadyNAS Remote.



The ReadyNAS Remote service verifies that your Internet connection is working and that your device is online.

ReadyNAS Remote is enabled.

4. (Optional) Configure advanced settings for the ReadyNAS Remote service:
   1. Select **Settings** next to ReadyNAS Remote.



2. Configure the options.
3. Click the **Apply** button.
   Your changes are saved and the pop-up screen closes.

Add ReadyNAS Remote Users

After you enable ReadyNAS Remote on your system, you can allow other ReadyNAS Remote users to access your system using their ReadyNAS Remote accounts.

For information about enabling ReadyNAS Remote on your system, see *Enable ReadyNAS Remote* on page 74.

ReadyNAS Remote users can access your system using enabled file-sharing protocols. Access to individual shared folders is granted or restricted according to the access rights that you specify when you configure access to the shared folder.

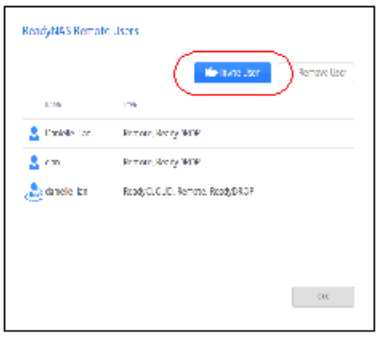
If you did not enable anonymous access to a shared folder, anyone who tries to access the system must provide valid ReadyNAS user account credentials.

For more information about managing access to shared folders on your system, see *Set Network Access Rights to Shared Folders* on page 48.

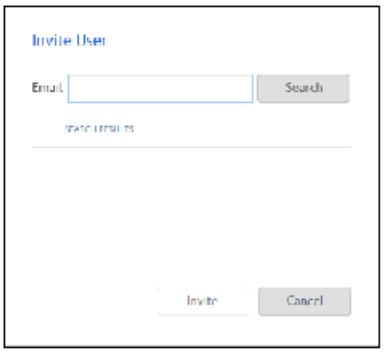
Note: ReadyNAS Remote users can access your system using only ReadyNAS Remote. If you also want users to access your system using ReadyCLOUD, add the users from ReadyCLOUD instead. See *Add ReadyCLOUD Users* on page 66.

To grant access to ReadyNAS Remote users:

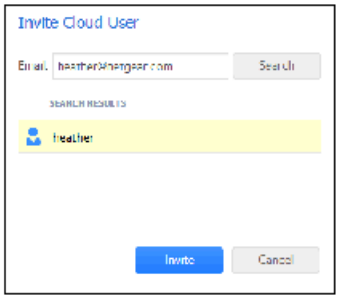
1. Login to your ReadyNAS.
2. On the local admin page, click the **Cloud** button.
3. Click the Users button.



4. Click the **Invite Users** button.



5. Enter the email address of the ReadyNAS Remote user to whom you want to grant access.
6. Click the **Search** button.
   One of the following screens displays:
   - If the email address is linked to a ReadyNAS Remote account, the account's user name displays in the search results list. Select the user name and click the **Invite** button. The selected ReadyNAS Remote user can now access your ReadyNAS system using his or her ReadyNAS Remote account. The user name is added to the Cloud Users list with a user icon.



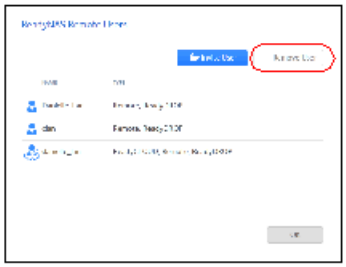
   - If the email address is not linked to a ReadyNAS Remote account, you are prompted to send an email inviting the person to create a ReadyNAS Remote account. The person's email address is added to the Cloud Users list with an envelope icon. When the person creates a ReadyNAS Remote account using that email address, the envelope icon changes to a user icon.

Remove ReadyNAS Remote Users

When you remove a ReadyNAS Remote user, that user can no longer use his or her ReadyNAS Remote account to access your ReadyNAS system.

To remove a ReadyNAS Remote user:

1. Login to your ReadyNAS.
2. On the local admin page, click the **Cloud** tab.
3. Click the **Users** button next to ReadyNAS Remote.



Note: The Cloud Users list includes both ReadyNAS Remote and ReadyCLOUD users. Do not remove ReadyCLOUD users from the Cloud Users list on the local admin page. If you want to delete a ReadyCLOUD user, use the ReadyCLOUD portal. See *Delete ReadyCLOUD Users* on page 69.

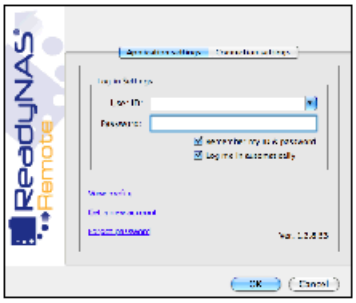
4. Select the user you want to remove.
5. Click the **Remove User** button.
6. Confirm the removal.
   The ReadyNAS Remote user can no longer access your ReadyNAS system and is removed from the Cloud Users list.

Install the ReadyNAS Remote Client on Remote Devices

Before you can access shared folders using ReadyNAS Remote, you must install the ReadyNAS Remote client software on your Windows or Mac computer.

To install the ReadyNAS Remote client on remote devices:

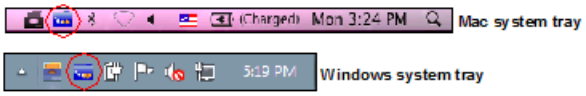
1. Using the device from which you want to remotely access a ReadyNAS system, visit *http://www.netgear.com/ReadyNAS-remote*.
2. Download the appropriate client software for your operating system and install it according to your operating system's instructions.
3. Launch the ReadyNAS Remote client.
4. Log in to your ReadyNAS Remote account or create a free ReadyNAS Remote account.



Tip: If you created a ReadyCLOUD account, you can use your ReadyCLOUD credentials to log in to ReadyNAS Remote. For more information about ReadyCLOUD, see *Discover and Set Up Your ReadyNAS* on page 13.

The ReadyNAS Remote client is installed on your device.

The **ReadyNAS Remote** icon displays in your system tray.



Access Shared Folders Using ReadyNAS Remote

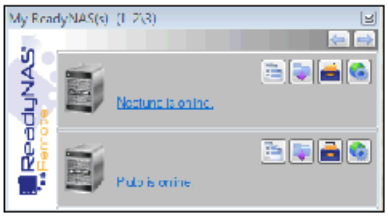
You can use ReadyNAS Remote to drag and drop files between your computer and your ReadyNAS system, even when your computer is not on the same LAN as your ReadyNAS system.

To access shared folders using ReadyNAS Remote on a Windows computer:

1. Launch the ReadyNAS Remote client software on your computer.
2. Right-click the **ReadyNAS Remote** icon in the system tray.

3. From the pop-up menu that displays, select **Log In**.
   The **ReadyNAS Remote** icon blinks while the device is connecting and displays as blue when it is connected.
4. Click the **ReadyNAS Remote** icon in the system tray.

A list of your ReadyNAS Remote devices displays.



5. Click the system that you want to access.
6. Enter valid ReadyNAS user or admin credentials.

> **Note:** The credentials that you enter to access shared folders on the system are different from your ReadyNAS Remote credentials. Accessing shared folders requires you to enter credentials for a user account on the system.

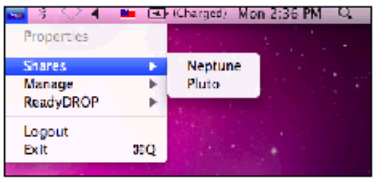
Your shared folders open in Windows Explorer.

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

To access shared folders using ReadyNAS Remote on a Mac computer:

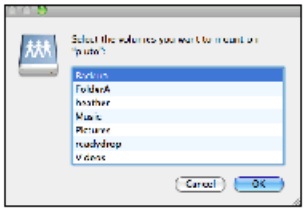
1. Launch the ReadyNAS Remote client software on your computer.
2. Click the **ReadyNAS Remote** icon in the system tray.

3. From the drop-down menu that displays, select **Shares**.



4. Select the ReadyNAS Remote device that you want to access.
5. Enter valid ReadyNAS user or admin credentials.

> **Note:** The credentials that you enter to access shared folders on the system are different from your ReadyNAS Remote credentials. Accessing shared folders requires you to enter credentials for a user account on the system.



6. Select the shared folders that you want to access and click the **OK** button.
   Your shared folders open in Finder.

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

LUNs

4

This chapter describes how to create, manage, and access LUNs on the ReadyNAS. It includes the following sections:

- *Basic LUN Concepts*
- *Manage LUNs*
- *LUN Groups and Access Rights*
- *Access LUN Groups from an iSCSI-Attached Device*

Note: Without a volume, you cannot configure any LUNs. For information about how to create volumes, see *Create and Encrypt a Volume* on page 28.

Basic LUN Concepts

The volumes on your ReadyNAS can be divided into shares and logical unit numbers (LUNs), both of which are logical entities on one or more disks. Shares and LUNs enable you to organize data in a volume by type, group, user, department, and so on. A single volume can contain multiple shares and LUNs.

LUNs are SAN (storage area network) data sets that allow data transfer and storage over iSCSI and Fibre Channel devices. The ReadyNAS supports iSCSI devices only. Each ReadyNAS system supports up to 256 LUNs. The local admin page displays LUNs in the following way:

Figure 6. Thin LUN

Figure 7. Thick LUN

Each LUN is configured independently of other LUNs that reside on the same volume. You can configure settings such as compression, protection, provisioning, LUN size, and access rights. You can also specify whether and how often a snapshot is created. These settings are explained in the following sections.

Thin and Thick Provisioning

You can specify the size of a LUN in two ways:

- **Thin**. A thin LUN lets you overallocate its size. That is, you can assign a LUN size that is larger than the size of the volume. Even though you specify the size of a thin LUN when you create it, storage space is assigned on demand instead of up front. This method greatly improves the utilization rate of the LUN because storage space is assigned only as data is written to the LUN. However, the size of the LUN is reported as the total storage space that you specify when you create the LUN.
  You can expand a volume as needed (if necessary, adding disks in the process) without expanding the size of the LUN and therefore, without disconnecting users. Make sure that you watch the volume capacity of the volume on which the overallocated LUN resides so you do not run out of storage space unexpectedly.

  Note: NETGEAR recommends that you do not use an overallocated LUN for storage of critical data. Instead, use a thick LUN.

- **Thick**. All storage space that you specify when you create a thick LUN is allocated up front and the storage space is reserved on the volume. Snapshots, other LUNs, and shared folders on the volume cannot consume storage space that is reserved. The size of the LUN is reported as the total storage

space that you specify when you create the LUN. You cannot assign more storage space than the available nonreserved storage space on the volume.

Default LUN Settings

The following table explains the default settings of a LUN. You can change these settings when you create or change the LUN.

Table 11. LUN default settings

Item	Default State
Compression	Disabled
Continuous Protection	Enabled
Interval	Daily
Provision	Thick
Access	Denied until you set permissions

Manage LUNs

From the local admin page, you can create, modify, or delete a LUN.

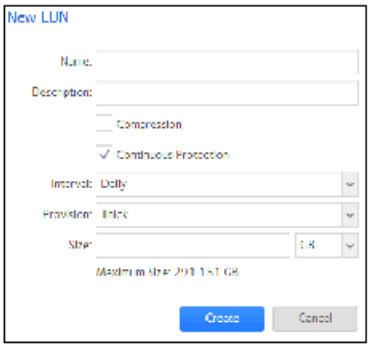
Create a LUN

After you create a volume (see *Create and Encrypt a Volume* on page 28), you can create LUNs on that volume. The following procedure describes how to create a LUN from the Shares screen. You can also create a LUN from the iSCSI screen.

Note: On ReadyNAS 102, 104, and 2120 systems, individual LUNs cannot exceed 8 TB.

To create a LUN:

1. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
2. Click the **New LUN** button to the right of the volume to which you want to add a LUN.



3. Configure the settings as explained in the following table:

Item	Description
Name	A unique name to identify the LUN. Do not include spaces in the name. All characters must be alphanumeric.
Description	An optional description to help identify the LUN.
Compression	Select the **Compression** check box to enable data compression. Compression saves storage space and increases the speed of data transfers, but the compression and decompression processes require additional resources. By default, the **Compression** check box is cleared.
Continuous Protection	Select the **Continuous Protection** check box to enable data protection through snapshots and configure how often snapshots are taken. By default, the **Continuous Protection** check box is selected. For more information about snapshots, see *Chapter 5, Snapshots* on page 105.

<table>
<tr><th>Item</th><th colspan="2">Description</th></tr>
<tr><td></td><td>Interval</td><td>The interval specifies how often a snapshot is made. Make a selection from the drop-down list:
• Hourly. A snapshot is taken every hour on the hour.
• Daily. A snapshot is taken every day at midnight. This is the default setting.
• Weekly. A snapshot is taken every week on Friday at midnight.</td></tr>
<tr><td>Provision</td><td colspan="2">Select how storage space is provisioned. Make a selection from the drop-down list:
• Thin. Even though you specify the size of the LUN when you create it, storage space is assigned on demand instead of up front. The size of the LUN is reported as the total storage space that you specify when you create the LUN.
• Thick. All storage space that you specify when you create the LUN is also allocated up front. The size of the LUN is reported as the total storage space that you specify when you create the LUN. This is the default method.

Note: Make sure that you watch the volume capacity of the volume on which the overallocated LUN resides so you do not run out of storage space unexpectedly.

Note: NETGEAR recommends that you do not use an overallocated thin LUN for storage of critical data. Instead, use a thick LUN.</td></tr>
<tr><td rowspan="2">Size</td><td colspan="2">Specify the size of the LUN. The maximum size that you can allocate to the LUN is stated at the bottom of the screen.</td></tr>
<tr><td>Unit</td><td>Select the unit of measurement from the drop-down list:
• MB.
• GB. This is the default unit of measurement.
• TB.</td></tr>
</table>

4. Click the **Create** button.
   The ReadyNAS confirms the creation of a LUN with the message “Folder or LUN successfully created.”
5. Click the **OK** button.
   The new LUN is added to the Shares screen. Basic information is displayed to the right of the LUN.

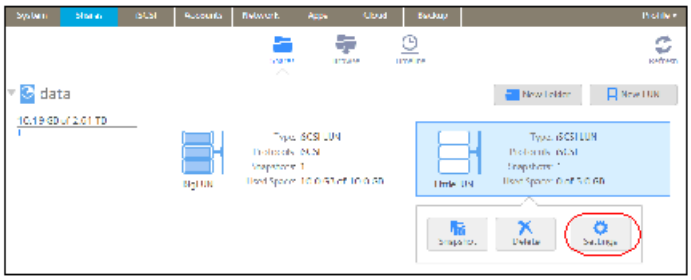
View and Change the Properties of a LUN

To view and change the properties of a LUN:

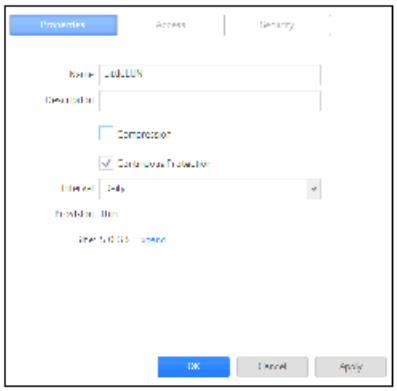
1. Select **Shares > Shares**.

A list of shared folders and LUNs on each volume displays.

2. Select the LUN that you want to configure.
3. From the pop-up menu that displays, select **Settings**.



The LUN settings display in a pop-up screen.



4. Change the settings as explained in the following table.

Item	Description
Name	A unique name to identify the LUN. Do not include spaces in the name.
Description	An optional description to help identify the LUN.
Compression	Select the **Compression** check box to enable data compression. Compression saves storage space and increases the speed of data transfers, but the compression and decompression processes require additional resources. By default, the **Compression** check box is cleared.
Continuous Protection	Select the **Continuous Protection** check box to enable data protection through snapshots and configure how often snapshots are taken. By default, the **Continuous Protection** check box is selected. For more information about snapshots, see *Chapter 5, Snapshots* on page 105 .

Item	Description	
	Interval	The interval specifies how often a snapshot is made. Make a selection from the drop-down list: • **Hourly**. A snapshot is taken every hour on the hour. • **Daily**. A snapshot is taken every day at midnight. This is the default setting. • **Weekly**. A snapshot is taken every week on Friday at midnight.
Provision	The provision setting is provided for information only. You cannot change the provision setting of an existing LUN.	
Size	For information about how to expand the size of an existing LUN, see *Expand the Size of a LUN* on page 87.	

5. Click the **Apply** button.
6. Click the **OK** button.
   Your changes are saved and the pop-up screen closes.

For information about how to set access right for a LUN, see *LUN Groups and Access Rights* on page 89.

Expand the Size of a LUN

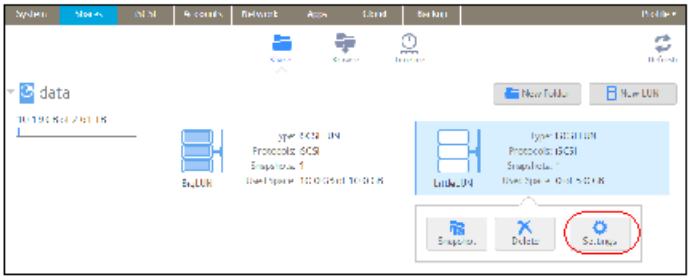
After you create a LUN, you cannot change the provision setting (thin or thick), but you can expand the size of the LUN.

Expansion is instant, regardless of the data size, but you must first disconnect all users that are connected to the LUN. Disconnect access to the LUN by removing the LUN from the LUN group to which the users have access (see *Create a LUN Group* on page 90).

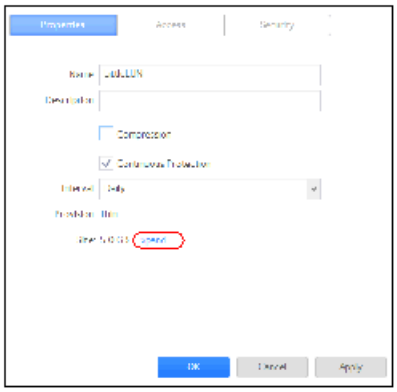
Note: On ReadyNAS 102, 104, and 2120 systems, individual LUNs cannot exceed 8 TB.

To expand the size of a LUN:

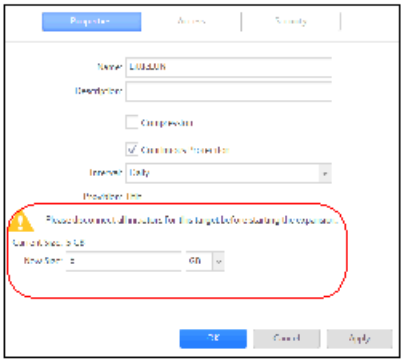
1. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
2. Select the LUN that you want to expand.
3. From the pop-up menu that displays, select **Settings**.



The LUN settings display in a pop-up screen.



4. Click the **Expand** link.
   The size expansion options display.



5. Enter the following settings:
   - **New Size**. Specify the new size of the LUN. The maximum size that you can allocate to a thick LUN is stated above the New Size field.
   - **Unit**. Select the unit of measurement from the drop-down list (MB, GB, or TB).
6. Click the **Apply** button.
   The new LUN size takes effect.
7. Click the **OK** button.
   Your changes are saved and the pop-up screen closes.
8. (Optional) Add the LUN to the LUN group to which it belonged before the expansion.

See *Create a LUN Group* on page 90.

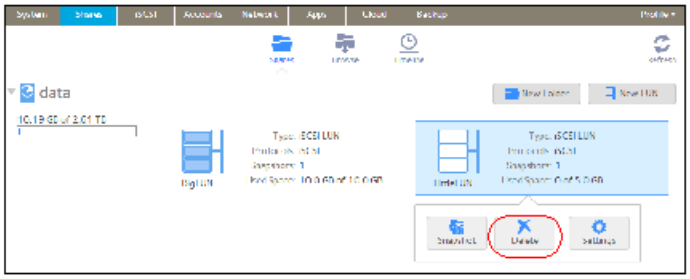
User access to the LUN is restored.

Delete a LUN

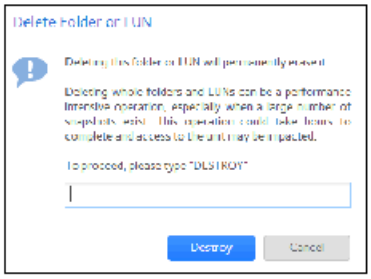
WARNING:
Deleting a LUN permanently removes the data within that LUN.

To delete a LUN from a volume:

1. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
2. Select the LUN that you want to delete.
3. From the pop-up menu that displays, select **Delete**.



4. In the pop-up screen that displays, confirm the deletion by typing **DESTROY**.



5. Click the **Destroy** button.
   The LUN is deleted.

LUN Groups and Access Rights

When you create a LUN, the LUN is unassigned. To access your storage system from an iSCSI-attached device, you must create a LUN group and assign one or more LUNs to the LUN group.

LUN groups allow you to organize LUNs and manage access rights to LUN groups. Access rights are either open or granted through internal CHAP authentication. Access rights apply to LUN groups, not to

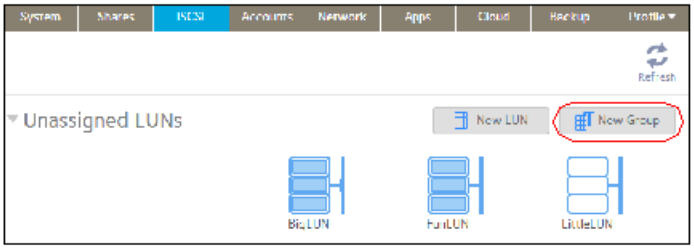
individual LUNs. You can easily assign a LUN to a LUN group or move a LUN from one LUN group to another LUN group.

Each LUN group has an iSCSI target address (for example, iqn.1994-11.com.netgear:f2f2fdd4) that allows iSCSI clients to access the LUN group. For more information, see *Manage Access Rights for LUN Groups* on page 92. Each ReadyNAS supports a maximum of 256 iSCSI targets.

Create a LUN Group

To create a LUN group:

1. Select **iSCSI**.
   The iSCSI screen displays the LUNs and LUN groups that you created.
2. To create a LUN group, click the **New Group** button in the upper right of the screen.



   The New LUN Group pop-up screen displays.

3. In the **Name** field, enter a name for the LUN group.
   The default name is groupX, where X is a number in sequential and ascending order.

   The Target field is automatically populated. The target is the string that an iSCSI client needs to be able to connect to the LUN.
4. Click the **Create** button.
   The New LUN group is added to the iSCSI screen.

By default, CHAP is disabled and no client is allowed to access the LUN group (see *Manage Access Rights for LUN Groups* on page 92).

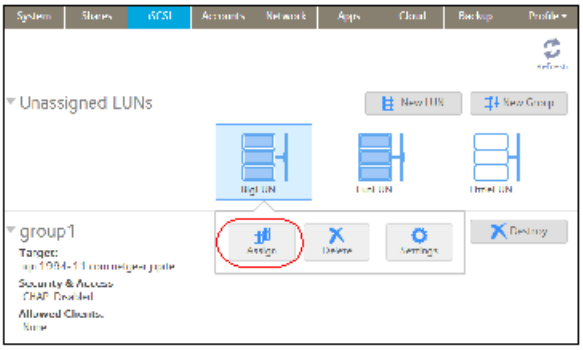
Assign a LUN to a LUN Group

To assign a LUN to a LUN group:

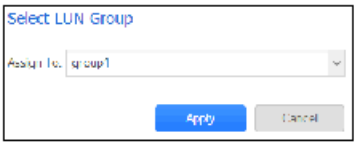
1. Select **iSCSI**.
   The iSCSI screen displays the LUNs and LUN groups that you created (see *Create a LUN* on page 83).
2. Select the unassigned LUN that you want to assign to a group.

Tip: You can also create a LUN by clicking the **New LUN** button to the right of the unassigned LUNs. By default, news LUNs are unassigned.

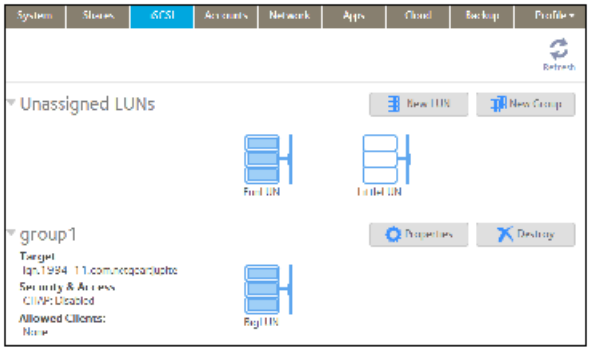
3. From the pop-up menu that displays, select **Assign**.



A pop-up screen displays.



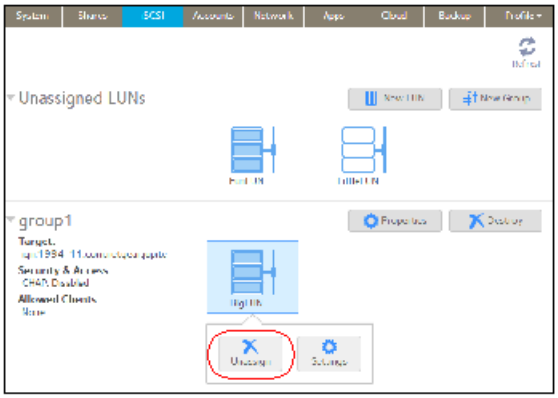
4. From the drop-down list, select the LUN group to which you want to assign the LUN.
5. Click the **Apply** button.
   The LUN is assigned to the selected LUN group.



Remove a LUN from a LUN Group

To remove a LUN from a LUN group:

1. Select **iSCSI**.
   The iSCSI screen displays the LUNs and LUN groups that you created.
2. Select the assigned LUN that you want to remove from the group.
3. From the pop-up menu that displays, select **Unassign**.

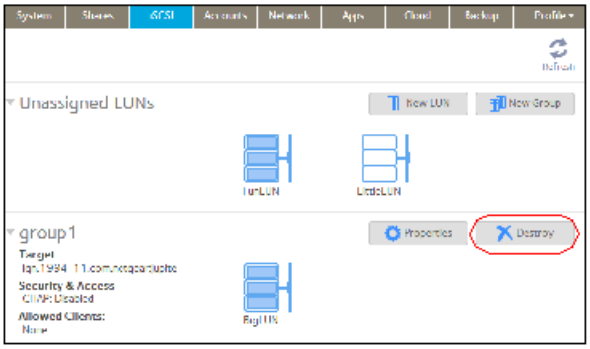


4. Confirm that you want to remove the LUN from the group.
   The LUN is returned to the unassigned state.

Delete a LUN Group

To delete a LUN group:

1. Select **iSCSI**.
   The iSCSI screen displays the LUNs and LUN groups that you created.
2. Click the **Destroy** button to the right of the LUN group that you want to delete.



3. Confirm that you want to delete the LUN group.
   If any LUNs were assigned to the group, they are returned to the unassigned state.

Manage Access Rights for LUN Groups

This section covers configuring LUN group access, adding and removing iSCSI initiators, and changing the CHAP password for an iSCSI initiator.

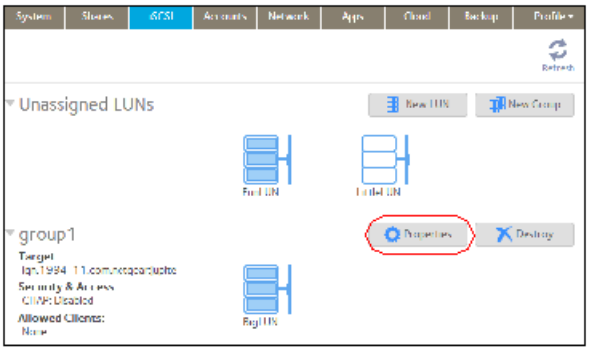
Configure Access to a LUN Group

To configure client access to a LUN group:

1. Select **iSCSI**.

The iSCSI screen displays the LUNs and LUN groups that you created.

2. Click the **Properties** button to the right of the LUN group that you want to manage.



A pop-up screen displays.

3. Configure the settings as explained in the following table:

Item	Description
Name	The name is provided for information only and cannot be changed.
Target	The target is the address that an iSCSI client (that is, an initiator) needs to access the LUN group. The Target field is automatically populated, but you can delete the content and then replace the content with a custom target address.
Require initiators to identify themselves using CHAP	Select this check box to enable CHAP authentication and to allow only authenticated initiators access to the LUN group. By default, access to the LUN group is open to the initiators that you add to list of initiators (see *Add an iSCSI Initiator* on page 94).
Allowed Initiators	Select one of the following radio buttons: • **Any**. Access to the LUN group is granted to all initiators that have information about the target address. (If CHAP authentication is enabled, access is dependent on CHAP authentication.) • **Selected**. Access to the LUN group is granted to iSCSI qualified names (IQNs) only. (If CHAP authentication is enabled, access is dependent on CHAP authentication.) For more information about configuring iSCSI initiators, see the following sections:

Item	Description	
	• *Add an iSCSI Initiator* on page 94 • *Remove an iSCSI Initiator* on page 96 • *Edit the CHAP Password* on page 96	
Password for bidirectional CHAP authentication	By default, access to an initiator by a LUN in the LUN group is open. To require a LUN in the LUN group to be authenticated before accessing an initiator, set a password for bidirectional CHAP authentication.	
	Password	Enter a CHAP password with a length of at least 12 characters. Maximum length is 16 characters.
	Confirm Password	Confirm the CHAP password.

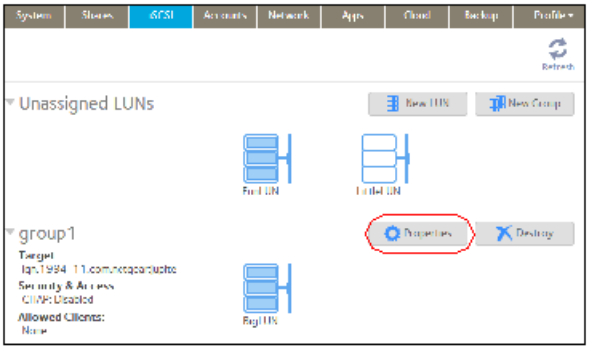
4. Click the **Apply** button.
   The new LUN group properties take effect immediately.

For information about how to set up and access a LUN from a client device, see *Access LUN Groups from an iSCSI-Attached Device* on page 98.

Add an iSCSI Initiator

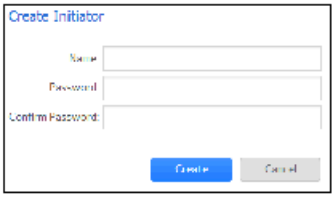
To add an iSCSI initiator and allow access to the LUN group:

1. Select **iSCSI**.
   The iSCSI screen displays the LUNs and LUN groups that you created.
2. Click the **Properties** button to the right of the LUN group that you want to manage.



A pop-up screen displays.

3. Select the **Selected** radio button next to Allowed Initiators.
4. Click the **+** button ( ) to the right of the list of initiators.
   The Create Initiator pop-up screen displays.



5. In the **Name** field, enter an IQN in the format as defined by *RFC3720*.
   For example, iqn.2012-04.com.netgear:sj-tst-5200:a123b456 is a valid IQN.
6. (Optional) Enter a CHAP password that is between 12 and 16 characters long and confirm the CHAP password.
7. Click the **Create** button.
   The IQN is added to the list of initiators on the LUN Group Properties pop-up screen.
8. In the Allowed column, select the check box to allow the initiator access to the LUN group.

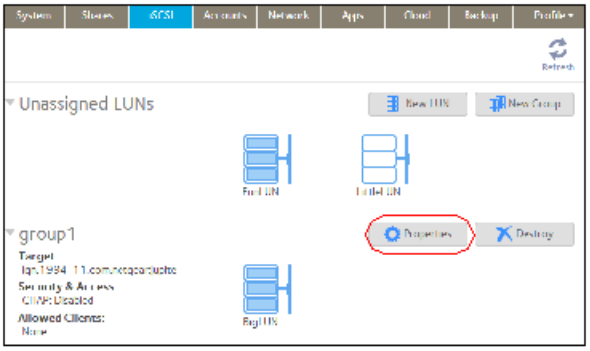
9. Click the **Apply** button.

The new LUN group properties take effect immediately.

Remove an iSCSI Initiator

To remove an iSCSI initiator from the LUN group:

1. Select **iSCSI**.
   The iSCSI screen displays the LUNs and LUN groups that you created.
2. Click the **Properties** button to the right of the LUN group that you want to manage.



A pop-up screen displays.

3. Select the **Selected** radio button next to Allowed Initiators.
4. Select the initiator that you want to remove from the list.
5. Click the – button (.) to the right of the list of initiators.
6. Confirm that you want to remote the selected initiator.
   The selected initiator is removed from the list of initiators.
7. Click the **Apply** button.
   Your changes are saved.

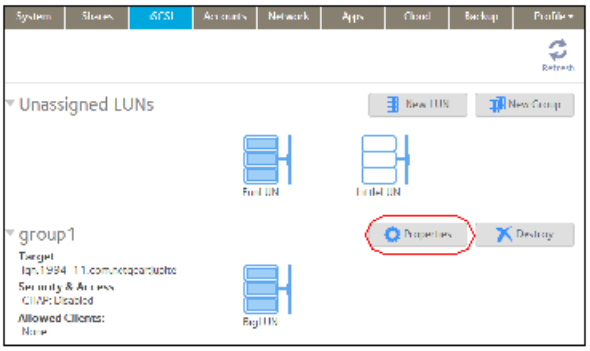
Edit the CHAP Password

To edit the CHAP password for an iSCSI initiator:

1. Select **iSCSI**.

The iSCSI screen displays the LUNs and LUN groups that you created.

2. Click the **Properties** button to the right of the LUN group that you want to manage.



A pop-up screen displays.

3. Select the **Selected** radio button next to Allowed Initiators.
4. Select the initiator that you want to edit from the list.
5. Click the **gear** button (⚙) to the right of the list of initiators.
   The Initiator Settings pop-up screen displays.

6. Enter a new password in the fields.
7. Click the **Apply** button on the Initiator Settings pop-up screen.
8. Click the **Apply** button on the LUN group properties screen.

Your changes are saved.

Access LUN Groups from an iSCSI-Attached Device

An iSCSI initiator application lets you set up a connection from a server to a LUN group (and therefore to individual LUNs). Normally, users would not initiate such a LUN connection. The network administrator would provide access to a LUN group through a server.

The iSCSI targets (that is, the LUNs in the LUN group on the ReadyNAS) present themselves on the client system as virtual block devices and can be treated as a locally attached disks. Windows, for instance, can run FAT32 or NTFS on the iSCSI target device and treat the devices as though they were locally attached.

When they have access to a LUN group, users can employ any backup application to back up local data from their iSCSI-attached device to a LUN.

Note: Unlike snapshots that reside on a share, snapshots that reside on a LUN are not visible to users. For information about how to recover data using a snapshot on a LUN, see *Recover Data from a Snapshot to an iSCSI-Attached Device* on page 124.

Accessing LUN groups from iSCSI-attached devices requires these high-level steps:

1. Set up iSCSI initiator access to the LUN group.
   See *Set Up Initiator Access* on page 98.
2. Initialize and format LUNs in the LUN group.
   See *Initialize and Format LUNs* on page 102.

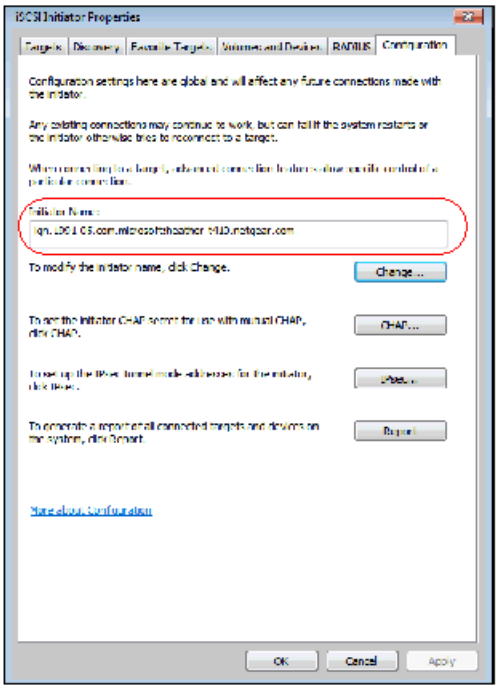
Set Up Initiator Access

The following procedure uses the Microsoft iSCSI Software Initiator, which is freely available online and is integrated in Windows 7.

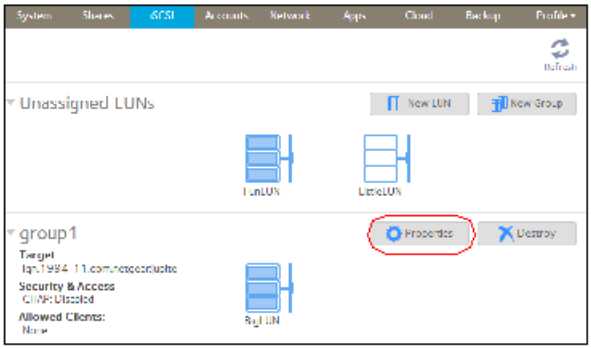
Note: If you use an operating system other than Windows, the steps are different, but the basic tasks remain the same.

To set up initiator access :

1. Open the iSCSI initiator and click the **Configuration** tab.
2. Copy the default name from the **Initiator Name** field.



3. Create an iSCSi initiator on the ReadyNAS:
   a. On the ReadyNAS local admin page, select **iSCSI**.
      The iSCSI screen displays.
   b. Click the **Properties** button to the right of the LUN group.



   A pop-up screen displays.

c. Select the **Selected** radio button next to Allowed Initiators.

d. Click the + button (⊕) to the right of the list of initiators.
The Create Initiator pop-up screen displays.

e. Paste the default iSCSI initiator name in the **Name** field.
The default iSCSI initiator name is the name that you copied in *Step 2* on page 98.

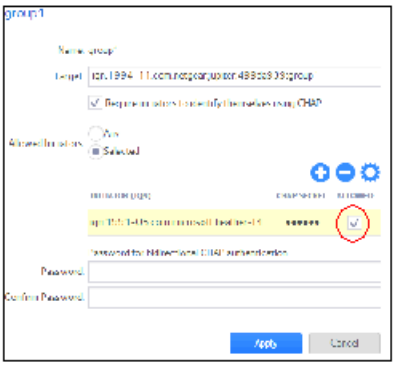
f. (Optional) Enter a CHAP password that is between 12 and 16 characters long and confirm the CHAP password.

g. Click the **Create** button.
The IQN is added to the table on the LUN group properties pop-up screen.

4. Configure the LUN group settings.

Note: If you are connecting to a LUN group using a Windows device, make sure that you leave the **Password** for bidirectional CHAP authentication fields blank.

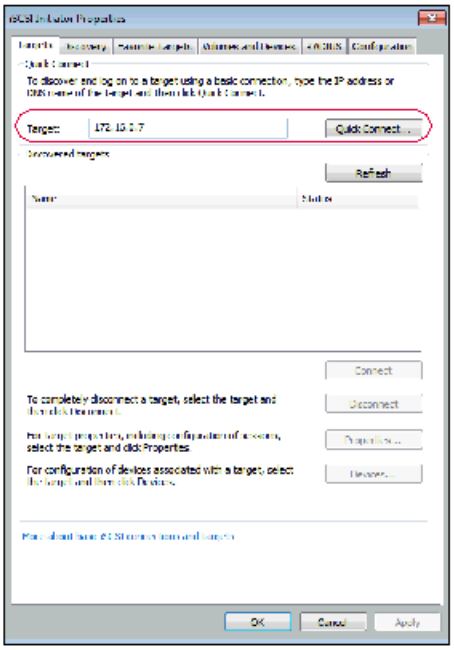
a. In the Allowed column of the initiator table, select the check box next to the initiator that you created in *Step 3* on page 99.
The initiator is allowed to access the LUN group.



b. (Optional) Select the **Require initiators to identify themselves using CHAP** check box.
Selecting this check box allows only authenticated initiators to access LUNs in the LUN group. To gain access, initiators must provide the CHAP password that you created in *Step 3* on page 100.

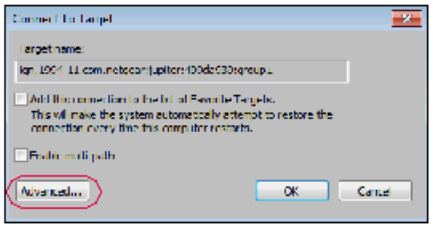
c. Click the **Apply** button.
The new LUN group properties take effect immediately.

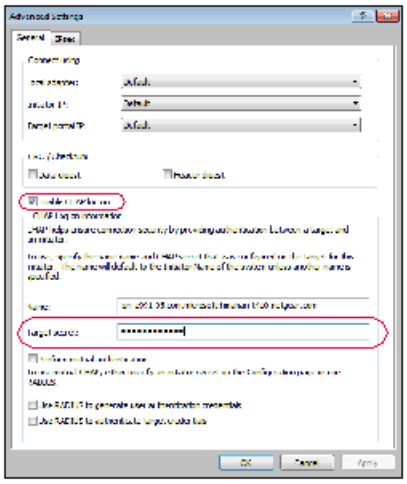
5. On the iSCSI Initiator Properties screen, click the **Targets** tab.
6. In the **Target** field, enter the IP address of the ReadyNAS.



7. Click the **Quick Connect** button.
8. Authenticate the connection.
If you selected the **Require initiators to identify themselves using CHAP** check box in *Step 4* on page 101, you must provide the CHAP password.

a. In the pop-up screen that displays, click the **Advanced** button.





b. Select the **Enable CHAP log on** check box.
c. In the **Target secret** field, enter the CHAP password that you created in *Step 3* on page 100.
d. Click the **OK** button on the Advanced Settings screen.
e. Click the **OK** button on the Connect To Target screen.
The initiator connects to the LUN group on the ReadyNAS.

The initiator has access to the LUN group, but you cannot view the LUNs in the LUN group using Windows Explorer until you initialize and format the LUNs.

For information about initializing and formatting LUNs, see *Initialize and Format LUNs* on page 102.

Initialize and Format LUNs

After you set up initiator access to the LUN group, you must initialize and format each LUN in the LUN group.

For more information about setting up initiator access, see *Set Up Initiator Access* on page 98.

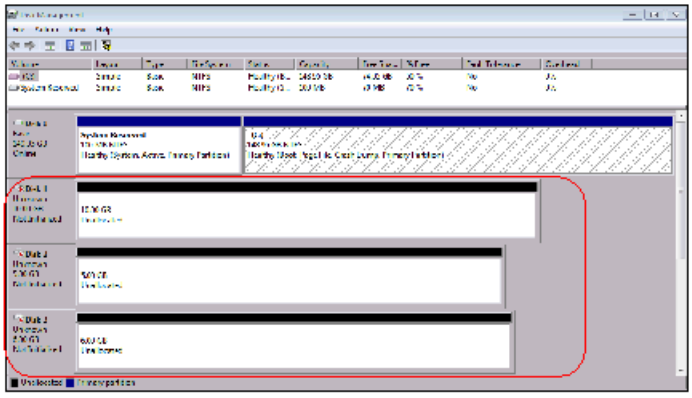
The following procedure uses the Microsoft iSCSI Software Initiator, which is freely available online and is integrated in Windows 7.

Note: If you use an operating system other than Windows, the steps are different, but the basic tasks remain the same.

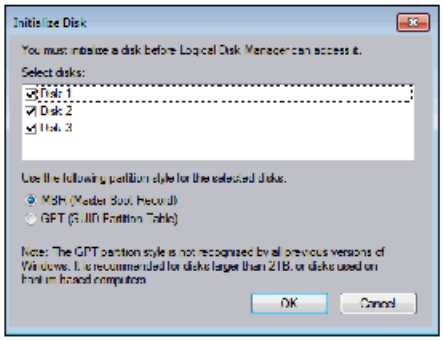
To initialize and format LUNs in the LUN group:

1. Open the Windows Disk Management application.
   Each LUN in the LUN group displays as an unallocated disk that needs to be initialized and formatted.

   Tip: If the disks do not display, select **Action > Refresh** in the Disk Management window.

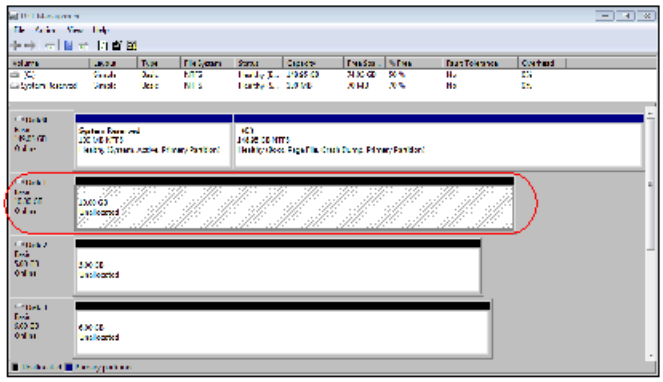


2. Initialize unallocated disks:
   a. Select an unallocated disk by clicking it.
   b. In the Disk Management window, select **Action > All Tasks > Initialize Disk**.
   c. Select the check box next to each unallocated disk that you want to initialize.
   d. Select the partition style that you want to use for the selected disks.
   e. Click the **OK** button.



   The selected disks are initialized.

3. Format an initialized disk:
   a. Select the disk that you want to format.

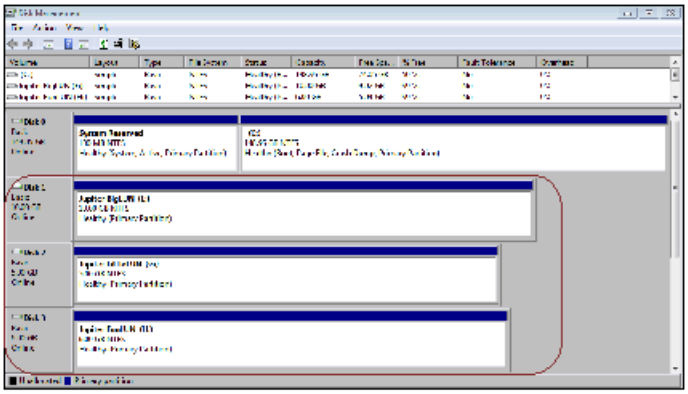


Selected disks are shaded.

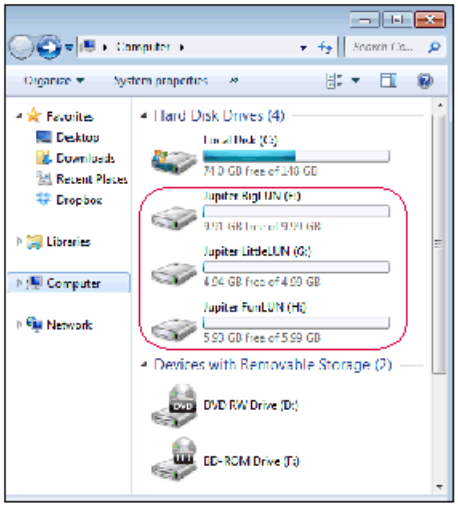
b. In the Disk Management window, select **Action > All Tasks > New Simple Volume**. The New Simple Volume Wizard pop-up screen displays.

c. Follow the default wizard formatting steps.

4. Repeat *Step 3* on page 103 for each initialized disk (LUN) that you want to access.



The LUNs are formatted as hard disk drives and are accessible through Windows Explorer.


Computer
Organize
System properties
Favorites
Desktop
Downloads
Recent Places
Dropbox
Libraries
Computer
Network
Hard Disk Drives (4)
Jupiter BigLUN (F:)
Jupiter LittleLUN (G:)
4.04 GB free of 4.00 GB
Jupiter FunLUN (H:)
5.93 GB free of 5.99 GB
Devices with Removable Storage (2)
DVD RW Drive (D:)
CD-ROM Drive (E:)

Snapshots

5

This chapter describes how to manage snapshots of shared folders and LUNs. It includes the following sections:

Note: Without a volume, you cannot configure any shared folders or LUNs. Without shared folders or LUNs, you cannot configure any snapshots. For information about how to create volumes, see *Create and Encrypt a Volume* on page 28. For information about how to create shared folders, see *Create a Shared Folder* on page 42. For information about how to create LUNs, see *Create a LUN* on page 83.

Basic Snapshot Concepts

The ReadyNAS can provide protection of shared folders and LUNs through snapshots. Snapshots contain references to data on a shared folder or LUN. Strictly speaking, snapshots are not backups, but they function as backups because you can recover data from snapshots.

You can take snapshots only of shared folders or LUNs. You cannot take a snapshot of a volume. Snapshots reside on the same volume as the shared folder or LUN from which they were created.

Note: Snapshots are not supported for the home folders that the ReadyNAS automatically creates for each user. For more information about home folders, see *User and Group Account Limitations* on page 127.

The ReadyNAS can automatically take snapshots of a shared folder or LUN according to a schedule that you specify. You can also manually take or delete individual snapshots at any time. Depending on available storage space, you can keep an unlimited number of snapshots.

WARNING:
When the available storage space on a volume decreases below 5 percent of the volume's total storage space, the oldest automatic snapshots are automatically deleted to bring the available storage space back to 5 percent or higher. Manual snapshots are never automatically deleted.

Once protection is available, the shared folders and LUNs on the Shares screen indicate the number of snapshots and the number of days with protection.

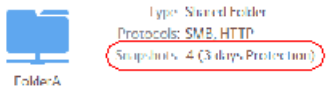


Figure 8. Shared folder with daily snapshots

Note: For snapshots to be accessible to users from their network-attached device, you must to select the **Allow snapshot access** check box in the shared folder or LUN settings pop-up screen. For more information, see *View and Change the Properties of a Shared Folder* on page 44.

Smart Snapshot Management

ReadyNAS OS 6.1 and later uses Smart Snapshot Management to reduce the number of automatic (continuous) snapshots per shared folder or LUN. Every hour, this feature automatically prunes older hourly, daily, and weekly snapshots, according to the following rules:

- Hourly snapshots are kept for 48 hours.
- Daily snapshots are kept for four weeks.
- Weekly snapshots are kept for eight weeks.

Note: The Smart Snapshot Management feature does not prune manual snapshots.

Rolling Back

You can replace a shared folder or LUN with an earlier version by rolling back to a snapshot. When you roll back to a snapshot, the entire shared folder or LUN is replaced with the version captured by the snapshot. All snapshots that were taken after the snapshot that was used for rolling back are deleted. For information about how to roll back to a snapshot, see *Roll Back to a Snapshot* on page 112.

Clones

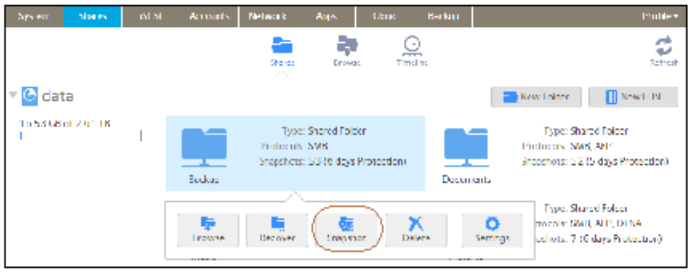
You can copy a snapshot to become a new independent shared folder or LUN. Changes made to the clone do not affect the parent shared folder or LUN (“origin”) and changes made to the parent do not affect the clone. For information about how to clone snapshots, see *Clone Snapshots* on page 117.

Manually Take a Snapshot

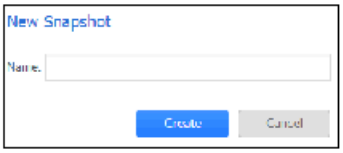
You can manually take snapshots from the Shares screen and the Timeline screen. The following procedure describes how to take snapshots from the Shares screen.

To manually take a snapshot of a shared folder or LUN:

1. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
2. Select the shared folder or LUN that you want to take a snapshot of.
3. From the pop-up menu that displays, select **Snapshot**.



The New Snapshot pop-up screen displays.



4. Enter a name for the snapshot.
5. Click the **Create** button.
   The snapshot is created.

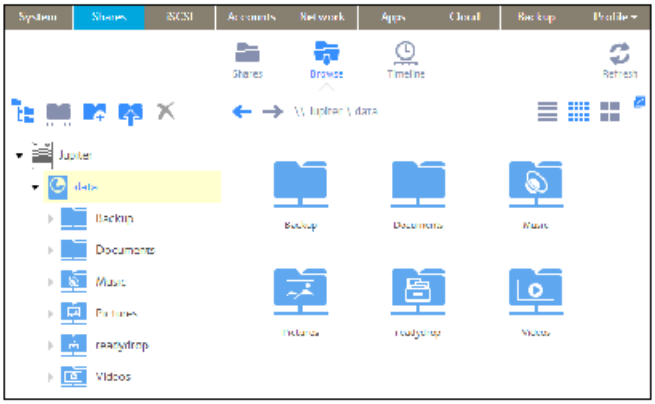
Browse Snapshots Using Recovery Mode

Sometimes you might want to recover individual files or subfolders within a shared folder without rolling back the entire shared folder. Recovery mode allows you to browse snapshots of shared folders and recover individual files or subfolders to your ReadyNAS.

Recovery mode is available only for shared folders. For information about now to recover data from a LUN snapshot, see *Roll Back to a Snapshot Using the Timeline* on page 114.

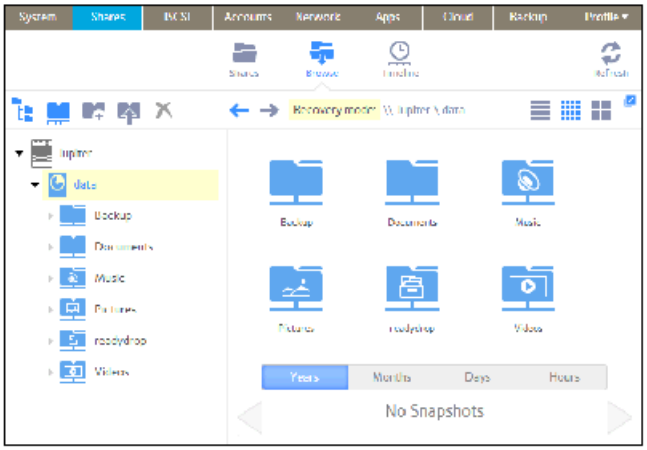
To browse and recover snapshot data using recovery mode:

1. Select **Shares > Browse**.
   A list of shared folders on each volume displays.

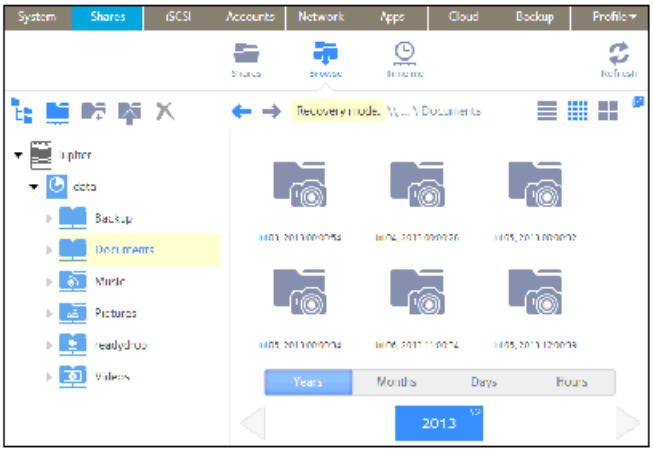


2. Click the **Recovery** icon (.).

The **Recovery** icon turns blue to indicate that you are browsing in recovery mode. Recovery mode allows you to browse snapshots of your shared folders.

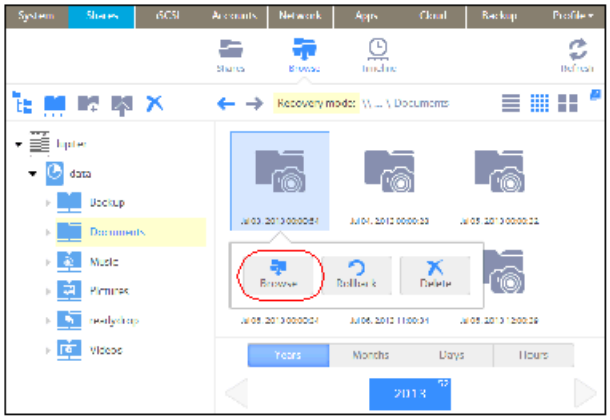


3. Select the shared folder whose snapshots you want to browse.
   Snapshots of the selected shared folder display.

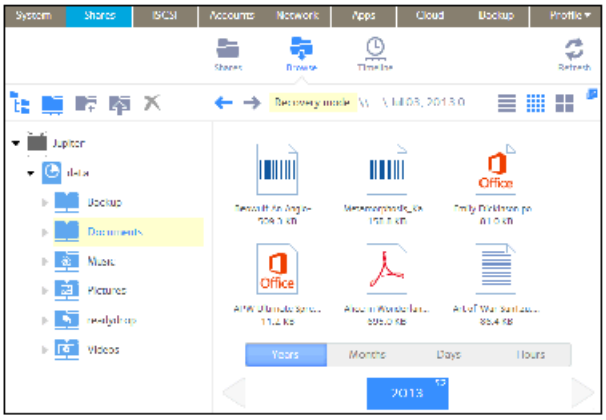


Tip: You can use the tabs and arrows at the bottom of the screen to browse snapshots by year, month, day, or hour.

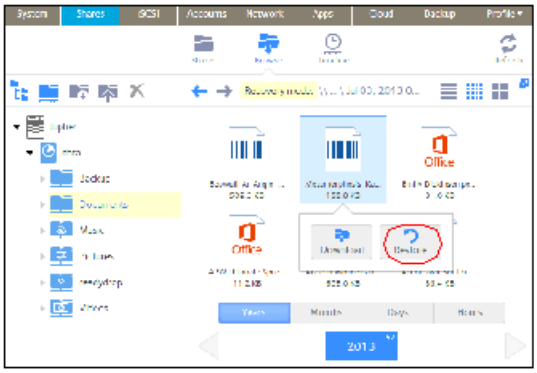
4. Select the snapshot that you want to browse.
5. From the drop-down menu that displays, select **Browse**.



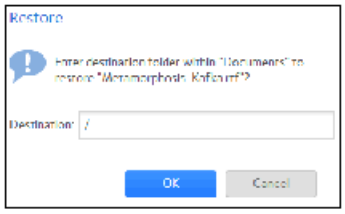
6. The contents of the selected snapshot display.



7. Continue browsing in recovery mode until you find the file or folder that you want to recover.
8. Select the file or folder that you want to recover.
9. From the drop-down menu that displays, select **Restore**.



10. In the pop-up screen that displays, enter the path to a recovery destination for the selected snapshot data.



The recovery destination must be within the folder whose snapshots you are browsing.

The recovered file or folder is recovered from the snapshot data and restored to the recovery destination that you specified.

Roll Back to a Snapshot

You can replace a shared folder or LUN with an earlier version by rolling back to a snapshot of that folder or LUN.

WARNING:
Rolling back is a destructive process. All snapshots that were taken after the selected snapshot are deleted.

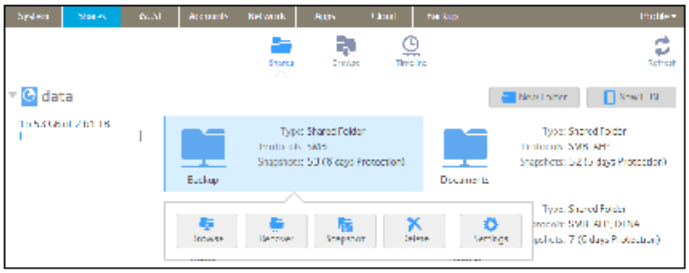
Roll Back to a Snapshot Using Recovery Mode

Recovery mode provides an easy way to browse your snapshots and roll back to earlier versions of your shared folders.

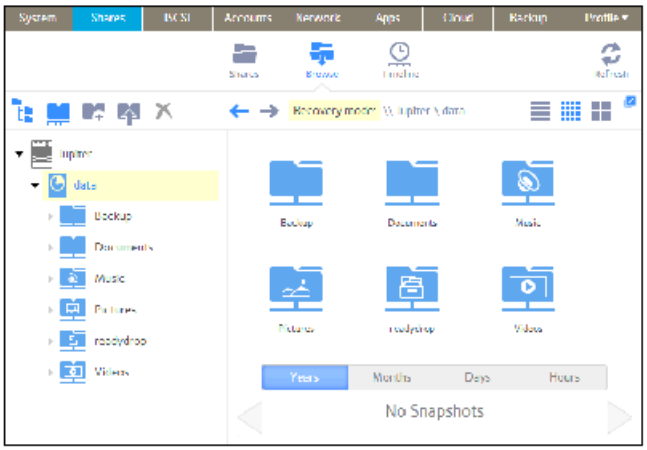
Recovery mode is available only for shared folders. For information about how to recover data from a LUN snapshot, see *Roll Back to a Snapshot Using the Timeline* on page 114.

To roll back to a snapshot using recovery mode:

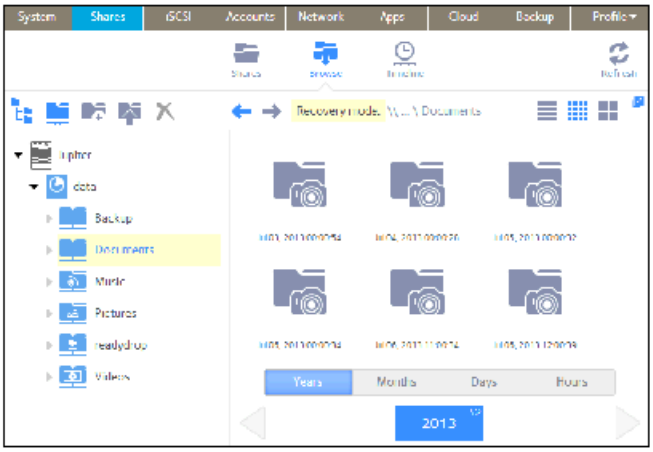
1. Select **Shares > Browse**.



2. Click the **Recovery** icon ( ).
The Recovery icon turns blue to indicate that you are browsing in recovery mode. Recovery mode allows you to browse snapshots of your shared folders.

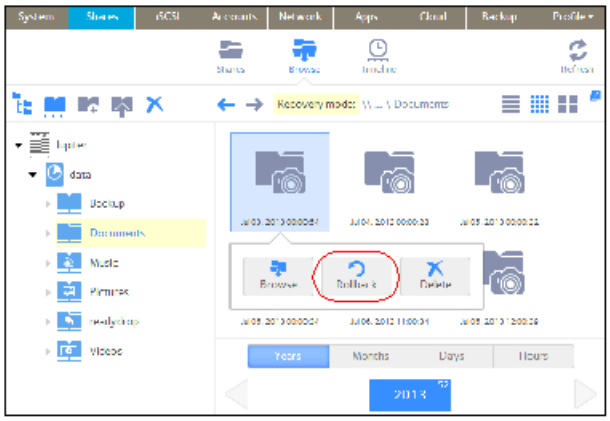


3. Select the shared folder whose snapshots you want to browse.
   Snapshots of the selected shared folder are displayed.

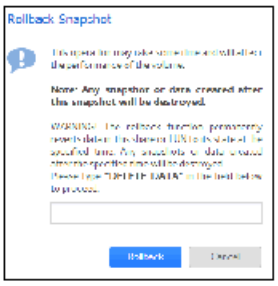


Tip: You can use the tabs and arrows at the bottom of the screen to browse snapshots by year, month, day, or hour.

4. Select the snapshot that contains the version of the folder that you want to roll back to.
5. From the drop-down menu that displays, select **Rollback**.



6. Confirm that you want to roll back to the selected snapshot by typing **DELETE DATA** in the pop-up screen that displays.



7. Click the **Rollback** button.
   The shared folder is rolled back to the snapshot that you selected.

Roll Back to a Snapshot Using the Timeline

You can use the snapshot timeline to locate and roll back to snapshots of shared folders and LUNs.

To roll back to a snapshot using the snapshot timeline:

1. Select **Shares > Timeline**.
   The snapshot timeline displays.

   Shared folders and LUNs that have snapshots display on the left of the screen.

2. Select the shared folder or LUN whose snapshots you want to view.
3. Locate the snapshot using the controls on the timeline.

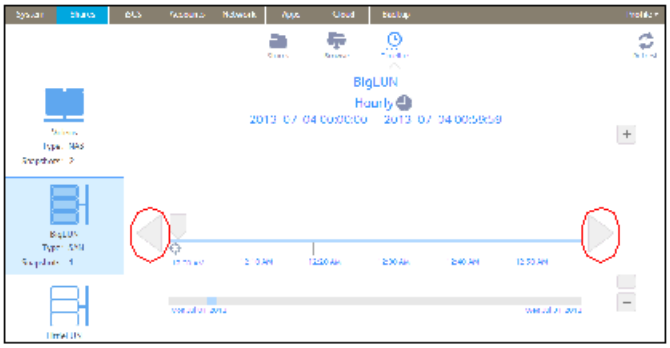
   Automatic snapshots are displayed as gray marker icons ( ) along the timeline.

   Manual snapshots are displayed as blue marker icons ( ) along the timeline.

   You can use the following icons to navigate the timeline:

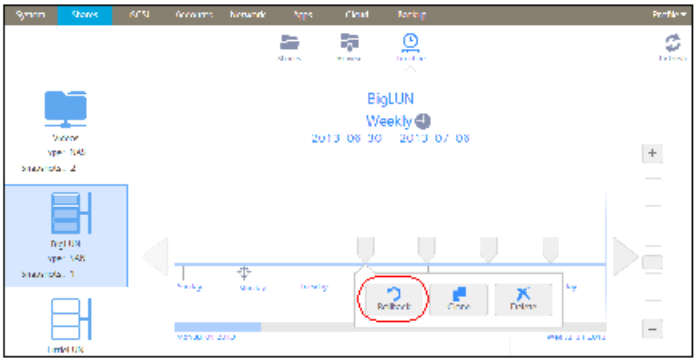
   - The timeline centers on the **zoom** icon ( ) as you zoom in and out. You can move the **zoom** icon by clicking anywhere along the timeline. Moving the **zoom** icon establishes a new center of focus when you zoom in and out.
   - Adjust the vertical slider on the right of the timeline as needed. To expand the timeline to years, click the **+** icon. To limit the timeline to hours, click the **–** icon.

   - Use the arrow buttons to the left and right of the timeline as needed to move forward in time (right arrow button) or back in time (left arrow button) in time.

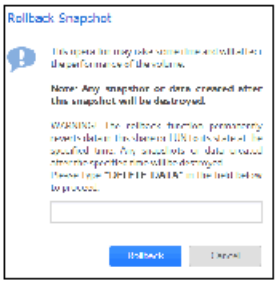


Tip: Click the **clock** icon ( ) that is located in the middle of the Snapshot screen under the name of the selected folder or LUN. A calendar pop-up screen displays, allowing you to jump to a desired month and date.

4. On the snapshot timeline, select the snapshot that you want to roll back to.
5. From the pop-up menu that displays, select **Rollback**.



6. Confirm that you want to roll back to the selected snapshot by typing **DELETE DATA** in the pop-up screen that displays.



7. Click the **Rollback** button.
   The shared folder or LUN is rolled back to the snapshot that you selected.

Clone Snapshots

Cloning a snapshot copies the snapshot to create a new independent shared folder or LUN.

To clone a snapshot:

1. Select **Shares > Timeline**.
   The snapshot timeline displays.

   Shared folders and LUNs that have snapshots are displayed on the left of the screen.

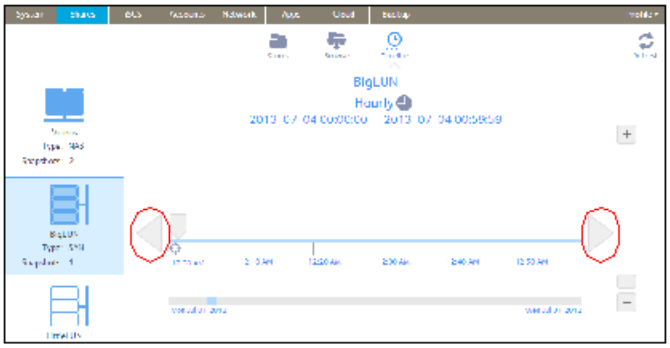
2. Select the shared folder or LUN whose snapshots you want to view.
3. Locate the snapshot using the controls on the timeline.
   Automatic snapshots are displayed as gray marker icons ( ) along the timeline.

   Manual snapshots are displayed as blue marker icons ( ) along the timeline.

   You can use the following icons to navigate the timeline:

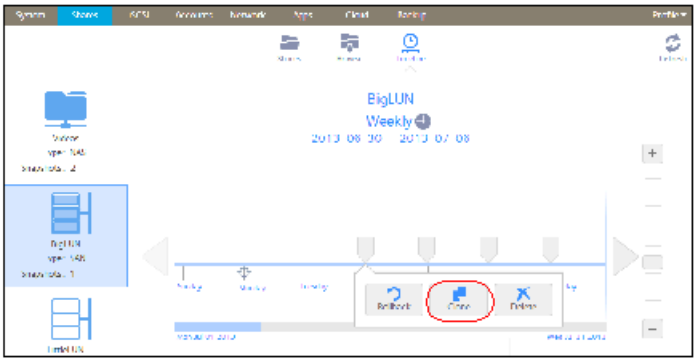
   - The timeline centers on the **zoom** icon ( ) as you zoom in and out. You can move the **zoom** icon by clicking anywhere along the timeline. Moving the **zoom** icon establishes a new center of focus when you zoom in and out.
   - Adjust the vertical slider on the right of the timeline as needed. To expand the timeline to years, click the **+** icon. To limit the timeline to hours, click the **–** icon.

- Use the arrow buttons to the left and right of the timeline as needed to move forward in time (right arrow button) or back in time (left arrow button) in time.

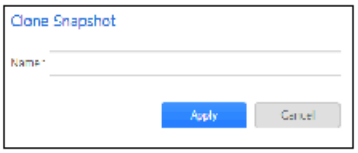


Tip: Click the **clock** icon ( ) that is located in the middle of the Snapshot screen under the name of the selected folder or LUN. A calendar pop-up screen displays, allowing you to jump to a desired month and date.

4. On the snapshot timeline, select the snapshot that you want to clone.
5. From the pop-up menu that displays, select **Clone**.



6. In the pop-up screen that displays, enter a name for the new folder or LUN.



7. Click the **Apply** button.
   The cloned snapshot is added to the Shares screen as a new shared folder or LUN.

Note: A new shared folder is immediately accessible to users. A new LUN first needs to be added to a LUN group before users can gain access to it.

Delete Snapshots

You can manually delete snapshots using recovery mode or the snapshot timeline.

ReadyNAS OS 6.1 and later uses Smart Snapshot Management to automatically prune your snapshots. For information, see *Smart Snapshot Management* on page 108.

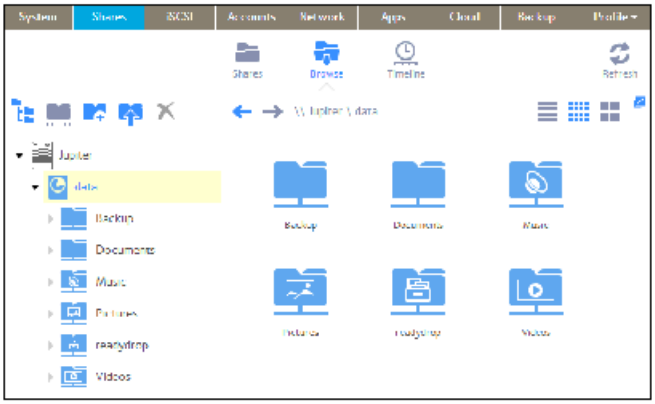
Delete Snapshots Using Recovery Mode

Recovery mode provides an easy way to manage and delete snapshots of your shared folders.

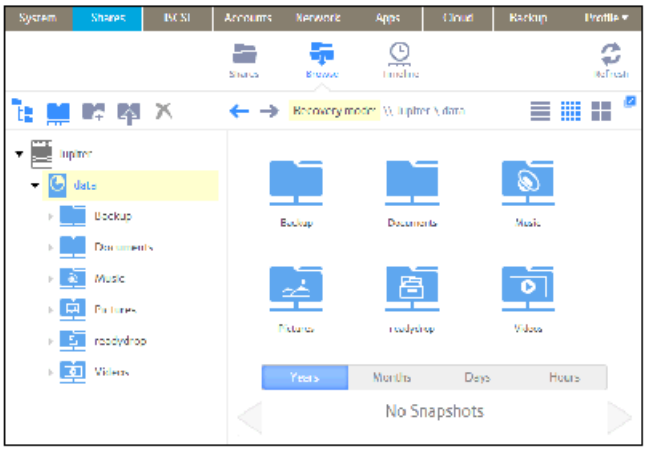
Recovery mode is available only for shared folders. For information about how to delete snapshots of LUNs, see *Delete Snapshots Using the Timeline* on page 121.

To delete a snapshot using recovery mode:

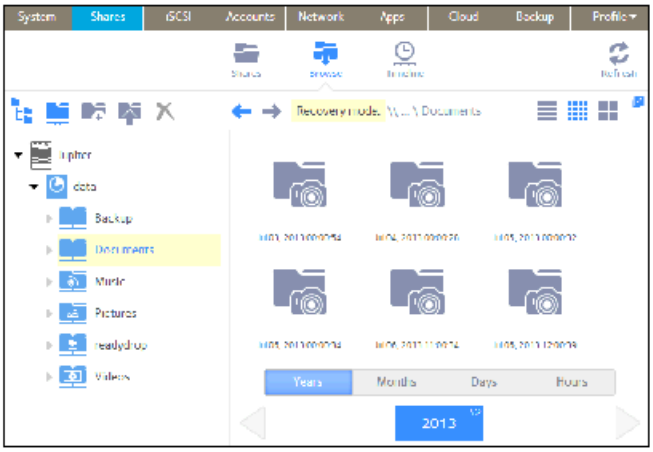
1. Login to your ReadyNAS.
2. Select **Shares > Browse**.



3. Click the **Recovery** icon ( ).
   The **Recovery** icon turns blue to indicate that you are browsing in recovery mode. Recovery mode allows you to browse snapshots of your shared folders.

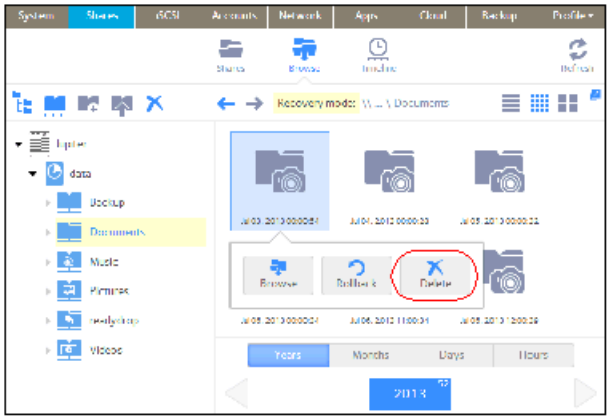


4. Select the shared folder whose snapshots you want to browse.



Tip: You can use the tabs and arrows at the bottom of the screen to browse snapshots by year, month, day, or hour.

5. Select the snapshot that you want to delete.



6. Select **Delete**.
7. Confirm the deletion.
   The snapshot is deleted.

Delete Snapshots Using the Timeline

You can use the snapshot timeline to locate and delete snapshots of shared folders and LUNs.

To delete a snapshot using the snapshot timeline:

1. Login to your ReadyNAS.
2. Select **Shares > Timeline**.
   The snapshot timeline displays.

   Shared folders and LUNs that contain snapshots are displayed on the left of the screen.

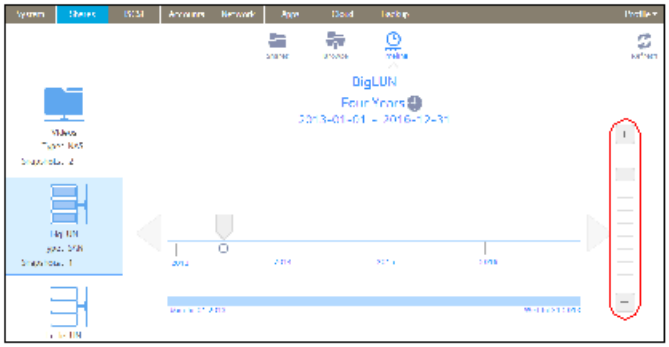
3. Select the shared folder or LUN whose snapshots you want to view.
4. Locate the snapshot using the controls on the timeline.

   Automatic snapshots are displayed as gray marker icons ( ) along the timeline.

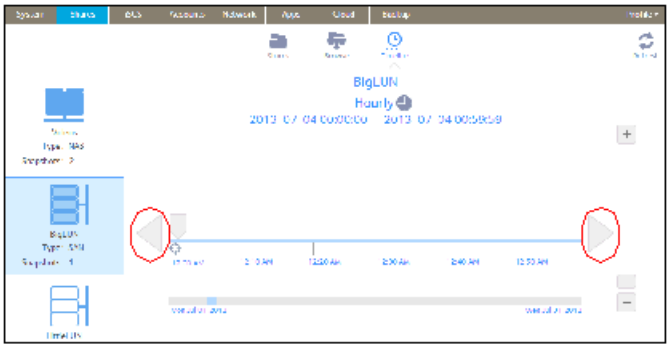
   Manual snapshots are displayed as blue marker icons ( ) along the timeline.

   You can use the following icons to navigate the timeline:

   - The timeline centers on the **zoom** icon ( ) as you zoom in and out. You can move the **zoom** icon by clicking anywhere along the timeline. Moving the **zoom** icon establishes a new center of focus when you zoom in and out.
   - Adjust the vertical slider on the right of the timeline as needed. To expand the timeline to years, click the **+** icon. To limit the timeline to hours, click the **–** icon.

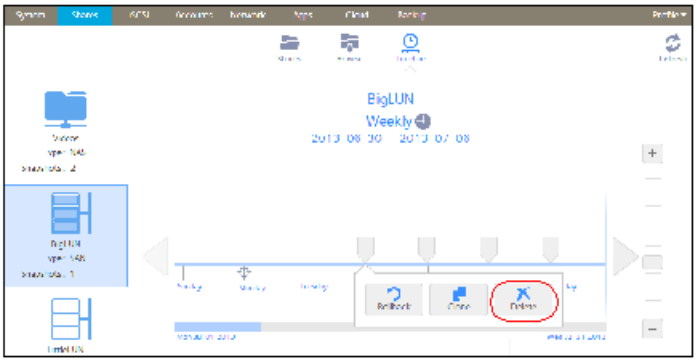


   - Use the arrow buttons to the left and right of the timeline as needed to move forward in time (right arrow button) or back in time (left arrow button) in time.



Tip: Click the **clock** icon ( ) that is located in the middle of the Snapshot screen under the name of the selected folder or LUN. A calendar pop-up screen displays, allowing you to jump to a desired month and date.

5. On the snapshot timeline, select the snapshot that you want to delete.



6. Select **Delete**.
7. Confirm the deletion.

The snapshot is deleted.

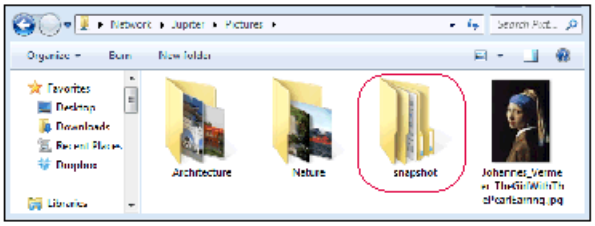
Recover Data from a Snapshot

The best way to protect against data loss is to back up your data. Regularly taking snapshots of your data can also help prevent loss, because you can recover data from snapshots.

Recover Data from a Snapshot to a Network-Attached Device

Recovering data from a snapshot to a network-attached device, such as a laptop or tablet, involves the following high-level steps:

1. Enable access to snapshots.
   You must allow users to access snapshots from network-attached devices. You can grant access to snapshots by selecting the **Allow snapshot access** check box when you configure the properties of a shared folder. For more information, see *View and Change the Properties of a Shared Folder* on page 44.
2. Access a shared folder from a network-attached device.
   Snapshots reside on the same volume as the shared folder (or LUN) from which they were created. After you enable access to snapshots, users can access snapshots of shared folders according to their access rights. Users who have access to a shared folder can access its snapshots. Users who do not have access to a shared folder cannot access its snapshots. For more information about accessing a shared folder from a network-attached device, see *Access Shared Folders from a Network-Attached Device* on page 60.
3. Locate the snapshot data on the ReadyNAS.
   Snapshot data is stored in a snapshot subfolder within the shared folder. Users who have read/write access to the shared folder can explore the snapshot data and recover earlier versions of files or folders.



Recover Data from a Snapshot to an iSCSI-Attached Device

Strictly speaking, users who access the ReadyNAS through an iSCSI-attached device cannot access snapshots. However, you can clone a snapshot of a LUN to become a new independent LUN, and then assign the LUN clone to a LUN group that the users can access.

To recover data from the LUN clone, users must access the LUN clone from the same type of iSCSI-attached device that was used to format the parent of the clone. For example, if the parent LUN was formatted using a Windows device, users must access the LUN clone using a Windows device.

Recovering data from a snapshot to an iSCSI-attached device involves the following high-level steps:

1. Clone a snapshot of a LUN.
   See *Clone Snapshots* on page 117. Cloning a snapshot of a LUN creates a new independent LUN.
2. Assign the LUN clone to a LUN group that the users can access.
   See *Assign a LUN to a LUN Group* on page 90.

   The LUN clone appears on the iSCSI-attached device as a virtual block device. The iSCSI-attached device treats LUNs in the LUN group as locally attached disks. Now users can access the LUN clone from the iSCSI-attached device.
3. Locate the snapshot data on the LUN clone from the iSCSI-attached device.
   Users can access data on the LUN clone according to their access rights. Users who have read/write access to the LUNs in the LUN group can explore the snapshot data in the LUN clone and recover any desired data.

Users and Groups

6

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

Basic User and Group Concepts

Users are the people to whom you grant access to your storage system. If your company uses Windows Active Directory, you can use that to manage ReadyNAS users. Otherwise, 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 folders and LUNs each user is permitted to access.

If your ReadyNAS storage system is used at home, you might create a user account for each member of the family, but allow only the parents to access financial data stored on your system. You might decide that all user 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 shared folder, but that all users can access data stored in the company benefits shared folder. You can create a group for each department and place all users in the appropriate group or groups.

Home Folders

Home folders allow each user to have a private folder matching his or her account name. Home folders are always available over SMB and AFP protocols and are available optionally over NFS and FTP protocols.

To enable home folders:

1. Login to your ReadyNAS.
2. Select **System > Settings > Home Folders**.
3. Set the **On-Off** slider so that the slider shows the **On** position to enable Home Folders.
4. Select the check boxes of the optional protocols to enable home folders over those protocols.

User and Group Account Limitations

You can create up to 8,192 user accounts and up to 8,192 group accounts on your ReadyNAS storage system. However, creating many accounts on your system can degrade its performance, so NETGEAR recommends that you create and maintain only those accounts you need, preferably fewer than 250.

When you add a user, a private home folder is created for that user. This private home folder is visible only to the user and the system administrator.

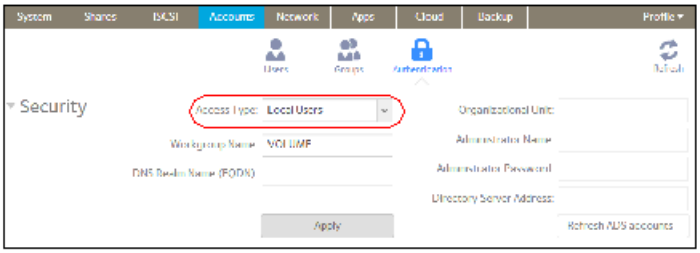
User and Group Management Modes

You can choose between two modes to manage user and group accounts on your ReadyNAS: Local Users mode and Active Directory mode. You configure either one or the other:

- **Local Users mode**. This mode lets you manually manage user and group accounts on your ReadyNAS storage system using its local database.
- **Active Directory mode**. This mode requires an Active Directory database. If you use Active Directory mode, you do not use your ReadyNAS system to manage your users and groups. Instead, you manage them with your Active Directory database and the changes are transferred to your ReadyNAS system every 12 hours.

To configure Local Users mode:

1. Select **Accounts > Authentication**.
2. From the **Access Type** drop-down list, select **Local users**.
   Except for the **Workgroup Name** field, all fields are dimmed.

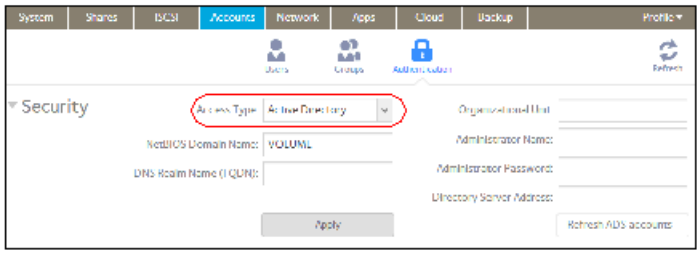


3. (Optional) Enter a name for the workgroup.
   You can keep the default name of VOLUME.
4. Click the **Apply** button.

For more information about managing users and groups in Local Users mode, see *User Accounts* on page 129 and *Group Accounts* on page 133.

To configure Active Directory mode:

1. Select **Accounts > Authentication**.
2. From the **Access Type** drop-down list, select **Active Directory**.
   The **Workgroup Name** field changes to NetBIOS Domain Name and all fields become available.



3. Configure the settings as explained in the following table:

Item	Description
NetBIOS Domain Name	Enter the name of the NetBIOS domain, for example, company. Normally, the NetBIOS domain name is identical to the prefix of the DNS realm name. If the NetBIOS domain name does not properly represent the organizational structure or

Item	Description
	does not match the prefix naming rules, the name will differ from the prefix of the DNS realm name.
DNS Realm Name (FQDN)	Enter the DNS realm name, which is normally the DNS domain name or the Active Directory domain name, for example, company.community.com. In this example, company is the prefix, and community is the suffix of the name.
Organizational Unit	This setting is optional. Specify the location of the computer account of the ReadyNAS in the Active Directory. By default, the computer account for the ReadyNAS is placed in the \users organizational unit (OU), but you can use the Organizational Unit field to specify another OU. You can specify OUs by separating OU entries with commas. Specify the lowest-level OU first. **Note:** The name of the computer account (also referred to as the machine account) is the same as the host name of the ReadyNAS (see *Configure the Host Name* on page 145).
Administrator Name	Enter the name of the administrator of the Active Directory.
Administrator Password	Enter the password of the administrator of the Active Directory.
Directory Server address	This setting is optional. Enter the IP address of the Active Directory server.

4. Click the **Apply** button.
   Your changes are saved.
5. (Optional) Click the **Refresh ADS Accounts** button.
   User and group information on your ReadyNAS system is updated immediately.

For more information about managing users and groups with Active Directory, see your Active Directory documentation.

Keep the following precautions in mind when using Active Directory mode:

- Your Active Directory server and your ReadyNAS system must have the same time set on their system clocks. NETGEAR recommends that you choose your domain controller as your NTP server to ensure that time settings are the same.
- The DNS server that you use must be able to resolve the host name of the domain controller. NETGEAR recommends that you point your ReadyNAS to the Active Directory DNS to ensure that host names can be resolved.

User Accounts

Use Local Users mode to manually create, manage, and delete user accounts on your ReadyNAS storage system.

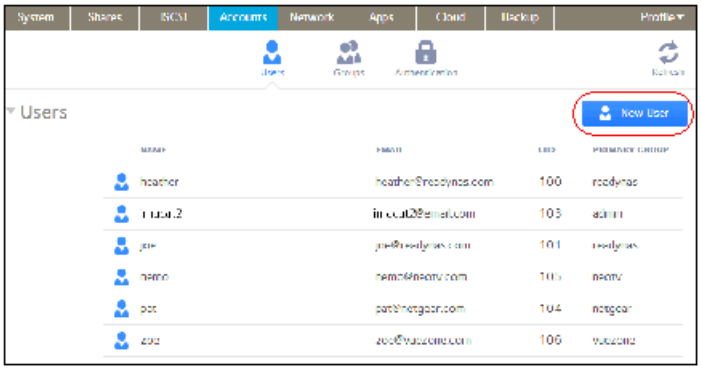
This section assumes that your ReadyNAS system is currently in Local Users mode. For more information about changing user and group management modes, see *User and Group Management Modes* on page 127.

Create User Accounts

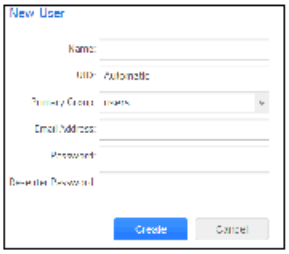
Use the local admin page to create user accounts.

To create a user account:

1. Select **Accounts > Users**.
2. Click the **New User** button.



The New User pop-up screen displays.



3. Enter the following information for the new user:
   - **Name**. User names can have a maximum of 31 characters in most non-Asian languages. If you use Asian language characters, the limit is lower. You can use most alphanumeric and punctuation characters for a user name.
   - **UID**. The UID is a unique user ID number assigned to each user. By default, the ID number is automatically set, but you can manually enter a number if you prefer.
   - **Primary Group**. From the drop-down list, select the primary group to which the user is assigned. The default group is called users.
     For information about creating groups, see *Create Groups* on page 133.

Note: In addition to belonging to a single primary group, a user can belong to multiple secondary groups. For information about assigning a user to a secondary group, see *Edit Groups* on page 134.

- **Email Address**. (Optional) Enter the user's email address.
- **Password**. Enter a password. Each user password can have a maximum of 255 characters.
- **Re-enter Password**. Reenter the user password.

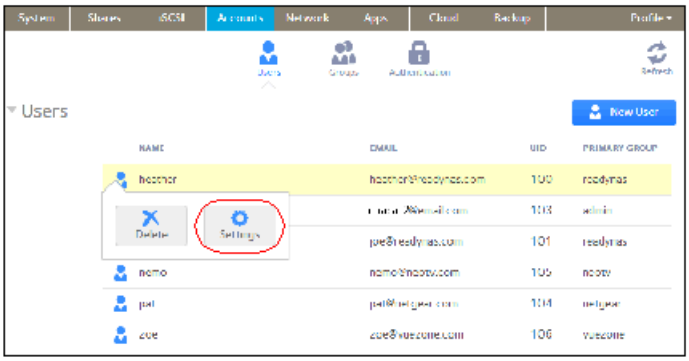
4. Click the **Create** button.
   A new user account is created.

Edit User Accounts

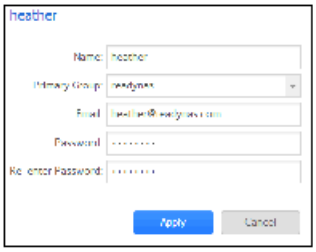
Use the local admin page to edit a user's name, email address, or password.

To edit a user account:

1. Select **Accounts > Users**.
2. From the list of users, select the user account that you want to edit.
3. Select **Settings** from the pop-up menu that displays.



4. In the pop-up screen that displays, edit the settings for the user as needed.



You can edit the user's name, primary group assignment, email address, and password.

Note: If you edit the user's name, you must also recreate the user's password.

5. Click the **Apply** button.

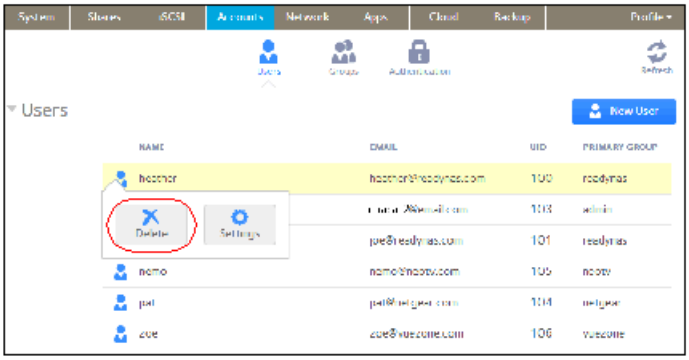
Your changes are saved.

Delete User Accounts

Use the local admin page to delete user accounts. Files on your ReadyNAS system that are owned by the deleted user might become inaccessible. When you delete a user, your ReadyNAS system deletes that user's private home folder and its contents.

To delete a user:

1. Select **Accounts > Users**.
2. From the list of users, select the user account that you want to delete.
3. From the pop-up menu that displays, select **Delete**.



4. Confirm the deletion.
   The user is deleted.

Change User Passwords

The ReadyNAS administrator can change user passwords from the local admin page (see *Edit User Accounts* on page 131).

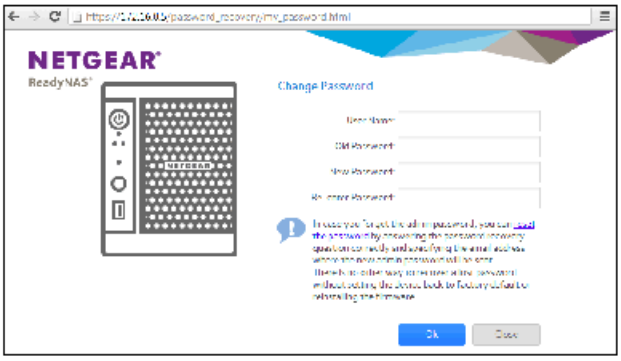
Users can also change their passwords using the ReadyNAS change password tool.

To change the password of your ReadyNAS user account:

1. On a computer that uses the same LAN as your ReadyNAS system, open a web browser and type: **https://<ReadyNAS IP address>/password_recovery/my_password.html**

   Where <ReadyNAS IP address> is the IP address of the ReadyNAS.

   The ReadyNAS change password tool displays in the browser window.



2. In the **User Name** and **Old Password** fields, enter your ReadyNAS user account credentials.
3. In the **New Password** and **Re-enter Password** fields, enter your new password.
4. Click the **OK** button.
   Your changes are saved.

Group Accounts

Use Local Users mode to manually create, manage, and delete group accounts on your ReadyNAS storage system.

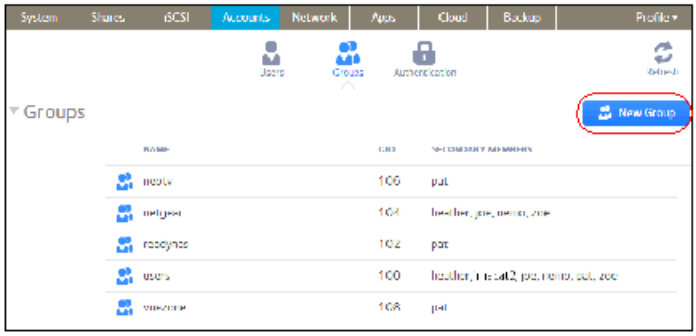
This section assumes that your ReadyNAS system is currently in Local Users mode. For more information about changing user and group management modes, see *User and Group Management Modes* on page 127.

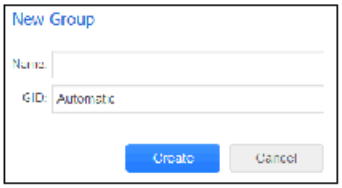
Create Groups

Use the local admin page to create groups.

To create a group:

1. Select **Accounts > Groups**.
2. Click the **New Group** button.





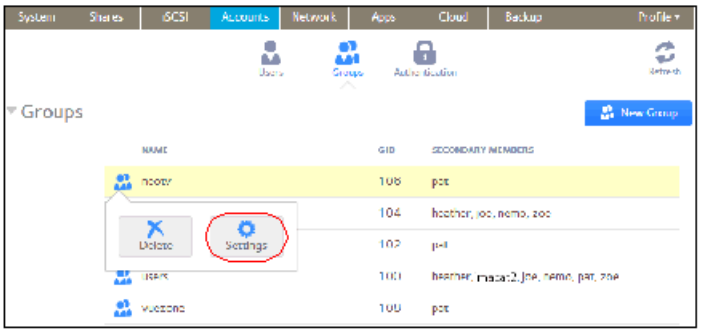
3. Enter the following information for the new group:
   - **Name**. Group names can have a maximum of 31 characters in most non-Asian languages. If you use Asian language characters, the limit is lower. You can use most alphanumeric and punctuation characters for a group name.
   - **GID**. The GID is a unique group ID number assigned to each group. By default, the ID number is automatically set, but you can manually enter a number if you prefer.
4. Click the **Create** button.
   The group is added to your system.

Edit Groups

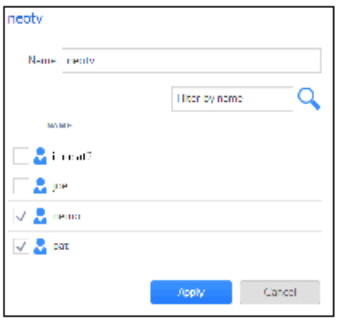
Use the local admin page to edit a group.

To edit a group:

1. Select **Accounts > Groups**.
2. From the list of groups, select the group that you want to edit.
3. From the pop-up menu that displays, select **Settings**.



4. In the pop-up screen that displays, edit the settings for the group as needed.



Use these guidelines to determine a user's group membership status:

- If the check box next to a user is selected and can be cleared, that user is a secondary member of the group.
- If the check box next to a user is selected and cannot be cleared, that user is a primary member of the group.
- If the check box next to a user is clear, that user is not a primary or secondary member of the group.

5. To change the group name, enter a new name in the **Name** field.
6. To add a user to this group as secondary member, select the check box next to the user's name.
7. To remove a user as a secondary member of this group, clear the check box next to the user's name.

Note: You cannot edit primary group membership from this screen. For information about how to edit primary group membership, see *Edit User Accounts* on page 131.

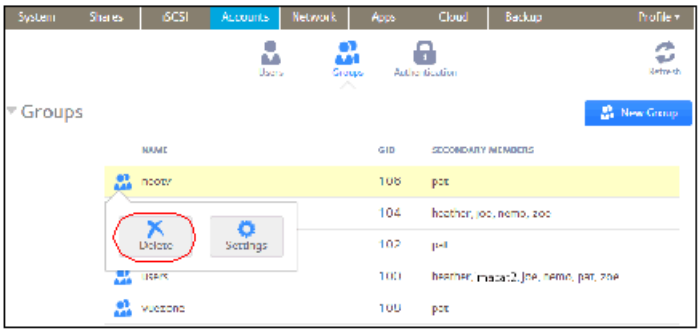
8. Click the **Apply** button.
Your changes are saved.

Delete Groups

Use the local admin page to delete a group. To be eligible for deletion, a group cannot contain any primary members. For more information about moving users to a different group, see *Edit User Accounts* on page 131. For more information about deleting users, see *Delete User Accounts* on page 132.

To delete a group:

1. Select **Accounts > Groups**.
2. From the list of groups, select the group you want to delete.
3. From the pop-up menu that displays, select **Delete**.



4. Confirm the deletion.
   The group is deleted.

Cloud Users

Cloud users are users who can access your system using ReadyCLOUD or ReadyNAS Remote.

ReadyCLOUD and ReadyNAS Remote are free cloud-based services that allow users to securely access your system from anywhere that has an Internet connection.

You can view a complete list of your system's Cloud users by selecting **Accounts > Cloud Users** on the local admin page.

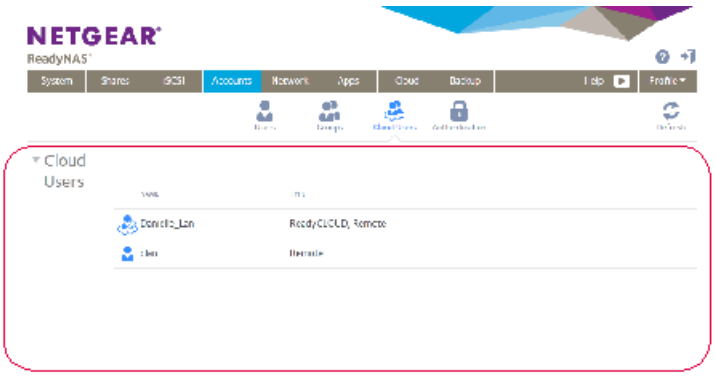


Figure 9. Cloud Users list

Grant Access to Cloud Users

If you want users to access your system using both ReadyCLOUD and ReadyNAS Remote, see *Add ReadyCLOUD Users* on page 66.

If you want users to access your system using ReadyNAS Remote only, see *Add ReadyNAS Remote Users* on page 75.

For more information about ReadyCLOUD and ReadyNAS Remote, see *Access Shared Folders Using Cloud Services* on page 65.

Cloud User Access Rights

When you grant access to ReadyCLOUD users, those users can access your ReadyNAS system using ReadyCLOUD and ReadyNAS Remote. You use the ReadyCLOUD web portal to configure access rights for users accessing your system from ReadyCLOUD. See *Manage Permissions for ReadyCLOUD Users* on page 70.

When you grant access to ReadyNAS Remote users, those users can access your ReadyNAS system using ReadyNAS Remote.

ReadyNAS Remote users access your system using enabled file-sharing protocols. Access to individual shared folders is granted or restricted according to the access rights that you specify when you configure access to the shared folder.

If you did not enable anonymous access to a shared folder, anyone who tries to access system must provide valid ReadyNAS user account credentials.

For more information about managing access to shared folders on your system, see *Set Network Access Rights to Shared Folders* on page 48.

For more information about using ReadyNAS Remote, see *Access Shared Folders Using ReadyNAS Remote* on page 78.

System Settings

7

This chapter describes how to configure the basic settings of the ReadyNAS. It contains the following sections:

- *Customize the Basic System Settings*
- *Configure the Network Settings*
- *Configure Global Settings for File-Sharing Protocols*
- *Configure Media Services*
- *Configure Discovery Services*
- *Install and Manage Apps*

Note: Without at least one volume, changes are not saved after you reload the ReadyNAS. Make sure that you create a volume before you configure the system, network, and global file-sharing protocol settings, and before you update the firmware. Without a volume, you cannot configure any shared folders. For information about how to create volumes, see *Create and Encrypt a Volume* on page 28.

Customize the Basic System Settings

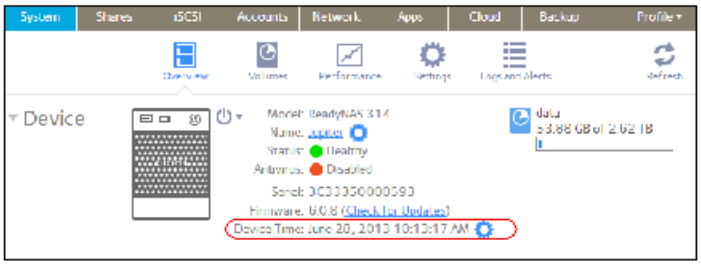
NETGEAR recommends that you configure the basic system settings that are described in this section before you use the ReadyNAS.

Set the Clock

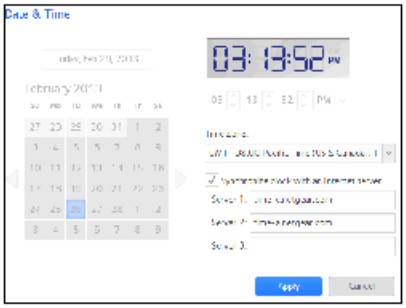
To enable the ReadyNAS to time-stamp files correctly, ensure that the time and date settings are accurate.

To set system time and date:

1. Select **System > Overview > Device**.
2. Click the **gear** icon ( ) to the right of the **Device Time** field.



The Date and Time screen displays.



3. From the **Time Zone** drop-down list, select the correct time zone for your location.

Note: So that your files are correctly time-stamped, NETGEAR recommends that you select the time zone in which the ReadyNAS is physically located.

4. Select the correct date and time by doing one of the following:
   - Select the **Synchronize clock with an Internet server** check box. When you select this check box, the calendar and time drop-down lists dim, and the system's date and time are synchronized with a NETGEAR NTP server.
   - Clear the **Synchronize clock with an Internet server** check box and use the calendar and time controls to set the date and time manually.
5. Click the **Apply** button.

Your changes are saved.

Select the Language

To make sure that the ReadyNAS correctly displays file names, configure the system to use the appropriate character set. For example, selecting Japanese allows the ReadyNAS to support files with Japanese names in Windows Explorer. ReadyNAS OS 6 supports unicode.

To configure language settings:

1. Login to your ReadyNAS.
2. On the navigation bar of the local admin page, select **Profile**.

3. From the drop-down menu that displays, select the language that you prefer or select **Auto**.
   When **Auto** is selected, the local admin page automatically detects and uses the language that your web browser uses.

   After you change the language, the local admin page reloads.

Note: NETGEAR recommends selecting a language based on the region in which you use the ReadyNAS.

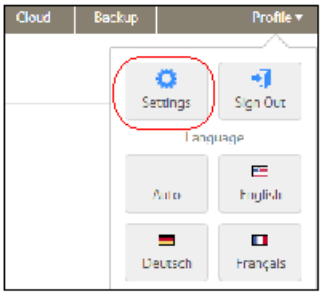
Set the Administrator Password

It is important to safeguard the administrator password and to change it regularly to protect your data.

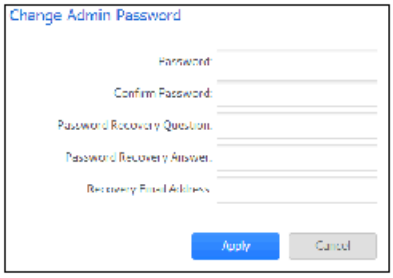
Choose an administrator password that is different from the default password and keep it in a safe place. Anyone who obtains the administrator password can change settings or erase data that is stored on the ReadyNAS.

To change the administrator password:

1. Login to your ReadyNAS.
2. On the navigation bar of the local admin page, select **Profile**.



3. Select **Settings**.
   The Change Admin Password pop-up screen displays.



4. Configure the settings as explained in the following table:

Item	Description	
Password	Enter a new administrator password.	
Confirm Password	Reenter the new password.	
Password Recovery Question	Choose a question that few people can answer. For example, you might enter First dog's name ? or Best friend in Kindergarten ? as your password recovery question.	Complete these fields to be able to recover a lost or forgotten administrator password with NETGEAR's password recovery tool (see *Recover the Administrator Password* on page 183).
Password Recovery Answer	Enter the answer to the question you provided in the Password Recovery Question field.	
Recovery Email Address	Enter the email address to which you want a reset password to be sent.	

5. Click the **Apply** button.

Your changes are saved.

Configure System Alerts

You can configure the ReadyNAS to send email alerts when certain system events occur, such as disk errors, changes in network connectivity, power supply failures, fan speed irregularities, and temperature violations.

The ReadyNAS divides system events into two categories, mandatory and optional. Mandatory events always generate email alerts. You can control which optional system events generate email alerts.

Email Alert Contacts

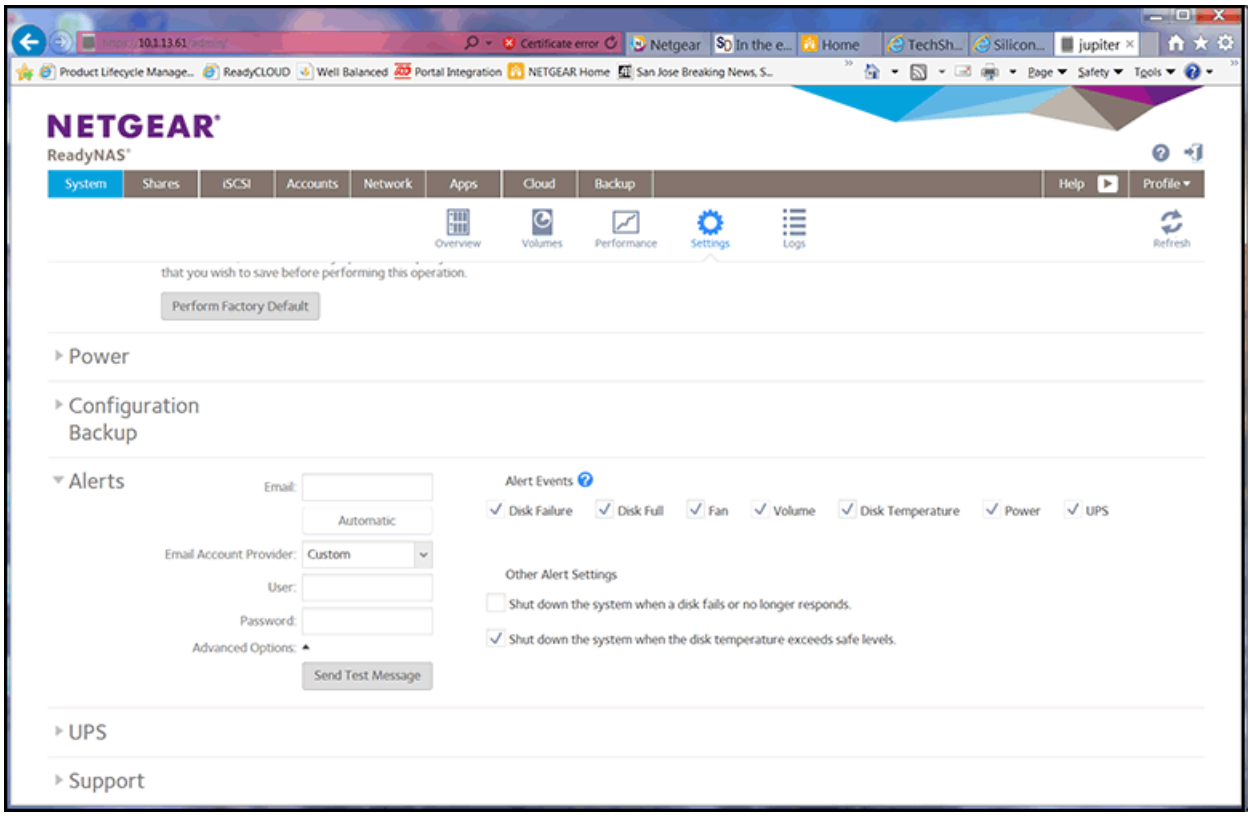
When certain system events occur, the ReadyNAS sends alerts to email addresses that you specify using an authorized email account.

By entering your email account information, you authorize the ReadyNAS to send email alerts from that account.

You can control which system events generate email alerts. For more information about alert events, see *Alert Event Settings* on page 145.

To configure the email alert recipients and sender:

1. Select **System > Settings > Alerts**.

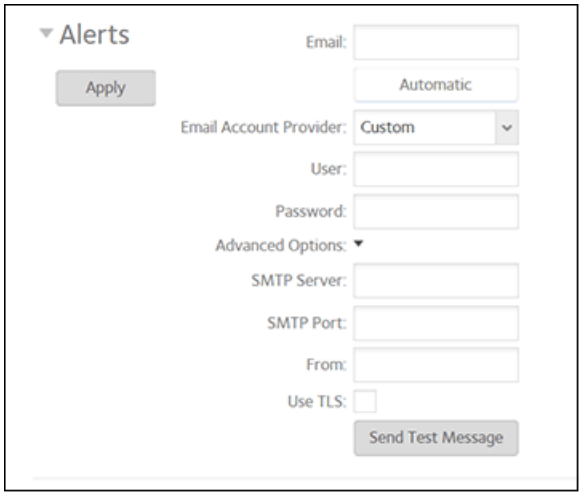


2. In the **Email** field, enter the email address that you want to receive alerts.

   Tip: If you want multiple email addresses to receive alerts, separate each email address with a space (not a comma).

   The **Automatic** button is highlighted.

3. Click the **Automatic** button.
   If the ReadyNAS recognizes the email provider, it automatically fills in the advanced options and the **User** field.
4. If the **User** field is filled in, enter the password as descriped in the following table and skip the next step; if the **User** field is not filled in, click the **Advanced Options** button.



5. Configure the email sender settings as explained in the following table.

Note: When the storage system sends email alerts, it sends them from the account that you enter here.

Item	Description	
Email Account Provider	Select your email account provider from the drop-down list: • **Gmail** • **AOL** • **Yahoo** • **Custom** (requires you to manually complete fields under **Advanced Options**)	
User	Enter the user name that is associated with the selected account provider. This information is required only if the SMTP server requires authentication.	
Password	Enter the password that is associated with your email account. This information is required only if the SMTP server requires authentication.	
Advanced Options	If you selected a recognized provider such as Gmail, AOL, or Yahoo as your email account provider, the Advanced Options fields are automatically populated. If you selected Custom, you must enter the Advanced Options fields manually.	
	SMTP Server	Enter the address of the outgoing SMTP server.
	SMTP Port	Enter the port number for the outgoing SMTP server. If no port number is entered, the default port number is 25.
	From	Enter a valid email address that identifies the sender of the email alert.

Item	Description	
	Use TLS	Select this check box to use email encryption over TLS.

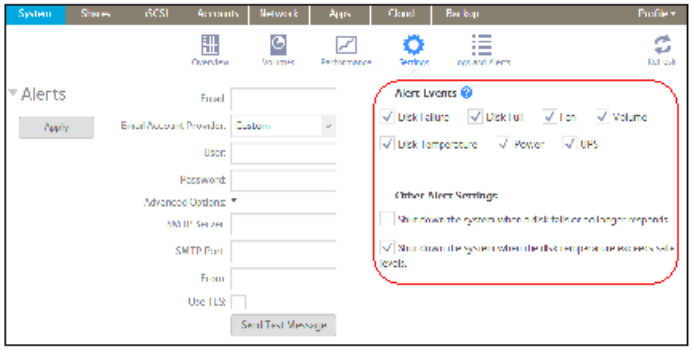
6. To determine if you configured the email settings correctly, click the **Send Test Message** button.
7. Click the **Apply** button under the Alerts heading.
   Your changes are saved.

Alert Event Settings

The ReadyNAS automatically generates email alert messages when certain system events occur. You can determine which optional system events generate alerts. NETGEAR recommends that you keep all alerts enabled. However, if you are aware of a problem, you can disable an alert temporarily.

To manage alert event settings:

1. Select **System > Settings > Alerts**.
2. In the Alert Events section, select the check box next to each event that you want to generate an alert.



   If you do not want an event to generate an alert, clear its check box.

   Dimmed events (Disk Failure, Volume, Power, and UPS) always generate email alerts.

3. In the Other Alert Settings section, select the check box next to each response that you want ReadyNAS system to execute in case of emergency:
   - **Shut down the system when a disk fails or no longer responds**. When this check box is selected, if a disk fails, your ReadyNAS system powers off.
   - **Shut down the system when disk temperature exceeds safe levels**. When this check box is selected, if disk temperature exceeds safe levels, your ReadyNAS system powers off.
4. Click the **Apply** button under the Alerts heading.
   Your changes are saved.

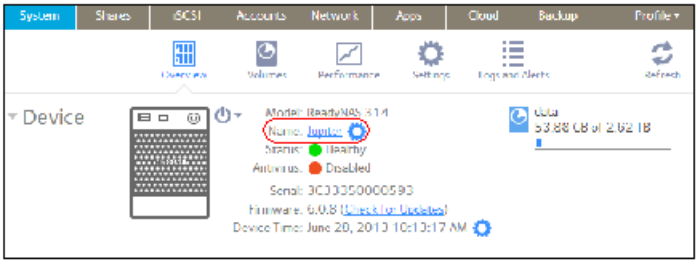
Configure the Host Name

The ReadyNAS uses a host name to advertise itself on the network. When you review the network using ReadyCLOUD, a computer, or any other interface, you can recognize the ReadyNAS by its host name.

The default host name is nas-xx-xx-xx, where xx-xx-xx is the last 6 bytes of the system's primary MAC address. You can change the host name to one that is easier to remember and recognize.

To change the host name:

1. **Select System > Overview > Device**.



2. Click the **gear** icon ( ) to the right of the **Name** field.

3. In the **Name** field, enter a new host name.
   In most non-Asian character sets, the host name can have a maximum of 15 characters, can only include A-Z, a-z, 0-9, and _, and the first character must be alphabetic. If you use Asian language characters, the limit is lower.
4. Click the OK button.
   Your changes are saved.

Enable Antivirus

Your ReadyNAS system comes with free antivirus software that provides real-time virus scans using signature and heuristic algorithms. The antivirus software helps protect your system from viruses, malware, worms, and Trojans.

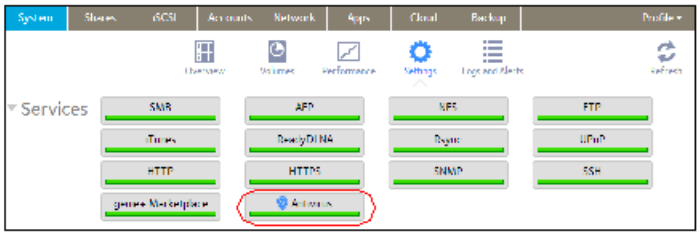
The antivirus software scans new files as they are written over the SMB (CIFS) protocol. It does not scan existing files or files transferred over other protocols.

To configure advanced settings, install the Antivirus app. For more information about installing apps, see *Install and Manage Apps* on page 169.

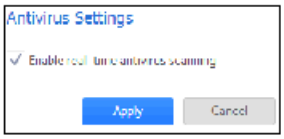
Enabling the antivirus software is optional.

To enable the free antivirus software:

1. Login to your ReadyNAS.
2. Select **System > Settings > Services**.



3. Click the **Antivirus** button.



4. Select the **Enable real-time antivirus scanning** check box.
5. Click the **Apply** button.
   The indicator on the Antivirus button turns green and the antivirus software is enabled.

Configure the Network Settings

This section covers basic networking concepts and the configurable network settings on your ReadyNAS storage system.

Network Basic Concepts

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.

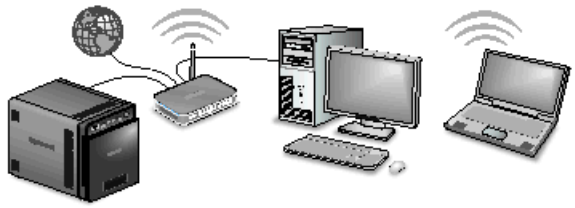


Figure 10. Example home network with ReadyNAS

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.

MAC Addresses

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 the system's label. You can also view it by selecting **Network** on the local admin page.

IP Addresses

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 can also act as a DHCP server.

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.

MTU

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.

Your ReadyNAS system supports a maximum MTU size of 9000 bytes. Use this MTU size only if all components of your network, for example network interface cards (NIC), hosts, and your switch support packets of this size or larger.

DNS

DNS is short for Domain Name System. Because IP addresses are a string of numbers, they are hard to remember. It is easier to remember a name (for example, www.readynas.com) than 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 option to assign an IP address automatically when you configured your Ethernet settings, the DNS fields are populated with the DNS settings from your DHCP server and cannot be edited.

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

Configure the Ethernet Interfaces

All ReadyNAS systems provide at least one physical Ethernet interface.

On ReadyNAS systems with two or more Ethernet interfaces, the interfaces can be used independently as individual links or combined into a bonded adapter. Bonding can provide redundancy or increased throughput.

For each Ethernet interface, you can configure the following settings:

- IPv4 and IPv6 settings
- DNS servers

The following table shows the default network configuration.

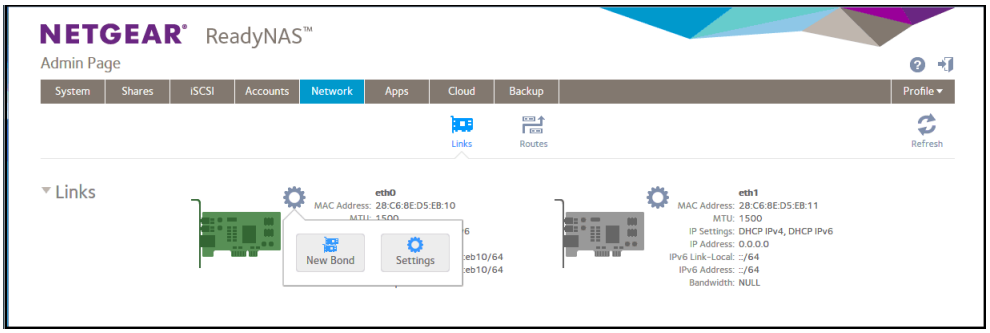
Table 18. Default network settings

Item	Default Setting
Physical Ethernet interface	
MTU	1500
TCP/IP	IPv4 using DHCP IPv6 using DHCP
DNS	No server

Configure General and TCP/IP Settings

To configure an Ethernet interface:

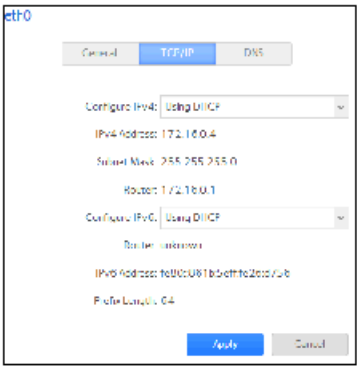
1. Login to the ReadyNAS.
2. Select **Network > Links**.
3. Click the settings **gear** icon for the Ethernet interface that you want to configure:
   - Ethernet interfaces with active links are colored green.
   - Ethernet interfaces with inactive links are colored gray.



4. From the pop-up menu that displays, select **Settings**.
   A pop-up screen displays the settings for the selected Ethernet interface.
5. Click the **General** tab and configure the settings as explained in the following table:

Item	Description
Name	Cannot be edited. Displays the name of the Ethernet interface.
Bandwidth (Mbps)	Cannot be edited. Displays the bandwidth of the Ethernet interface.
MTU	Enter the MTU in bytes. The default setting is 1500 bytes.

6. Click the **TCP/IP** tab.



7. Configure the TCP/IP settings as explained in the following table.

Note: NETGEAR recommends that you use DHCP address reservation to make sure that the DHCP server always assigns the same IP address to the interfaces of the ReadyNAS. The MAC addresses of the physical interfaces are shown on the Network screen.

Note: If you enter an IP address manually, you must provide DNS server information if you want to access your ReadyNAS system over the Internet. For more information, see

DNS on page 148. If the IP address changes, your browser loses its connection to your storage system. To reconnect to your ReadyNAS system, use ReadyCLOUD to rediscover your device. See *Discover and Set Up Your ReadyNAS* on page 13.

Item	Description	
IPv4 settings		
Configure IPv4	From the drop-down list, select how IPv4 is configured: • **Using DHCP**. The ReadyNAS functions as a DHCP client, and the IPv4 settings are automatically configured by a DHCP server on your network. • **Manually**. You must enter the IPv4 address and subnet mask for the ReadyNAS, and the router through which the ReadyNAS is connected to the network.	
IPv4 Address	Enter the IPv4 address for the ReadyNAS.	Manual configuration only.
Subnet Mask	Enter the subnet mask for the ReadyNAS.	
Router	Enter the IPv4 address for the router through which the ReadyNAS connects to your network.	
IPv6 settings		
Configure IPv6	From the drop-down list, select how IPv6 is configured: • **Automatically**. The ReadyNAS is configured with an IPv6 address through stateless autoconfiguration without the requirement of a DHCPv6 server on your network. The ReadyNAS must be connected to the Internet for stateless auto configuration to function. • **Using DHCP**. The ReadyNAS functions as a DHCPv6 client. The IPv6 settings are automatically configured by a DHCPv6 server on your network. • **Manually**. You must enter the IPv6 address and prefix length for the ReadyNAS and the router through which the ReadyNAS is connected to the network.	
Router	Enter the IPv6 address for the router through which the ReadyNAS connects to your network. The default setting is unknown.	Manual configuration only.
IPv6 Address	Enter the IPv6 address for the ReadyNAS.	
Prefix Length	Enter the prefix length for the ReadyNAS. The default prefix length is 64.	

8. Click the **Apply** button.
   Your changes are saved.

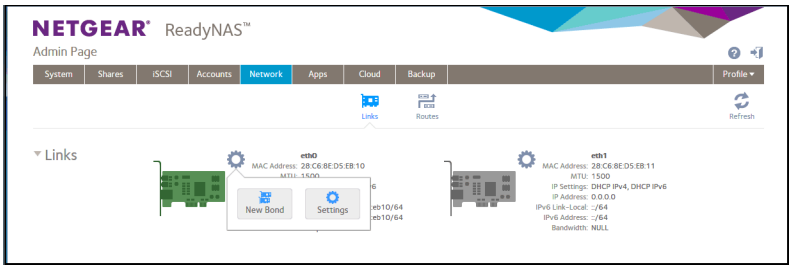
Configure DNS Settings

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

If you selected the option to assign an IP address manually when you configured your Ethernet settings, you must manually specify the IP addresses of the DNS servers and the domain name to access your storage system over the Internet. Your network administrator can help you determine your Domain Name Server IP address.

To add DNS information for an Ethernet interface:

1. Select **Network > Links**.
2. Select the settings gear icon for the Ethernet interface that you want to configure:
   - Ethernet interfaces with active links are colored green.
   - Ethernet interfaces with inactive links are colored gray.



3. From the pop-up menu that displays, select **Settings**.
   A pop-up screen displays the settings for the selected Ethernet interface.
4. Click the **DNS** tab.

5. Click the **+** icon to the right of the list of DNS servers.
6. In the pop-up screen that displays, enter the server IP address.

7. Click the **Add** button.
   The DNS server is added to the list.
8. Click the **Apply** button.

Your changes are saved.

Configure Bonded Adapters

Creating a bonded adapter is optional. A bonded adapter combines two Ethernet interfaces into a single logical link. Network devices treat the bonded adapter as a single link, which increases fault tolerance and provides load sharing.

Note: Bonding is available only on ReadyNAS systems with two or more Ethernet interfaces.

Teaming Modes

The ReadyNAS supports several teaming modes. Both the ReadyNAS and the device with which the bonded adapter is linked must support the same teaming mode. The available teaming modes are described in the following table.

Table 21. Teaming mode descriptions

Teaming Mode	Description
IEEE 802.3ad LACP	Creates aggregation groups that use the same speed and duplex settings. Utilizes all interfaces in the active aggregator according to the 802.3ad specification. You need a switch that supports IEEE 802.3ad dynamic link aggregation.
Active Backup	Only one interface in the bond is active. A different interface becomes active if, and only if, the active interface fails. The bond's MAC address is externally visible on only one port to avoid confusing the switch. You can decide which interface is active by default.
Transmit Load Balancing	Adapter bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each interface. Incoming traffic is received by the current interface. If the receiving interface fails, another interface takes over the MAC address of the failed receiving interface.
Adaptive Load Balancing	Includes transmit load balancing plus receive load balancing for IPV4 traffic and does not require any special switch support. The receive load balancing is achieved by ARP negotiation.
Round-Robin	Transmit packets in sequential order from the first available interface to the next. This mode provides load balancing and fault tolerance.
XOR	Transmit based on the default simple transmit hash policy. This mode provides load balancing and fault tolerance.
Broadcast	Transmit everything on all slave interfaces. This mode provides fault tolerance.

Hash Types

If you select the IEEE 802.3ad LACP or the XOR teaming mode, you must select which hash type option you want to use:

- Layer 2
- Layer 2+3 (uses Layer 2 and Layer 3 hash types simultaneously)
- Layer 3+4 (uses Layer 3 and Layer 4 hash types simultaneously)

Each hash type is described in the following table.

Table 22. Hash type descriptions

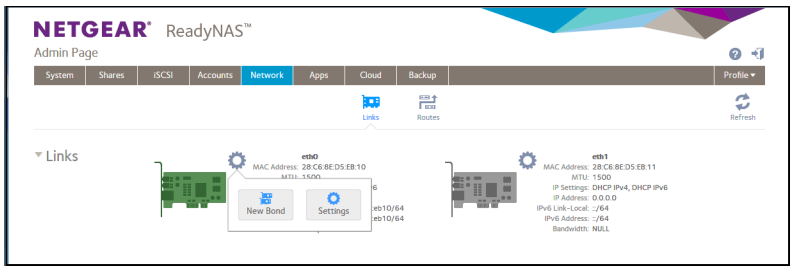
Hash Type	Description
Layer 2	Based on the source and destination MAC addresses. All traffic between the ReadyNAS and a particular device is transmitted on the same physical link.
Layer 3	Based on the source and destination IP addresses. Here too, all traffic between the ReadyNAS and a particular device is transmitted on the same physical link.
Layer 4	Based on the source and destination port numbers. Traffic between the ReadyNAS and a particular device can be spread across multiple links.

Create a Bonded Adapter

You can create a bonded adapter on ReadyNAS systems with two or more Ethernet interfaces.

To create a bonded adapter:

1. Select **Network > Links**.
2. Click the settings **gear** icon next to the Ethernet interface you want to bond.

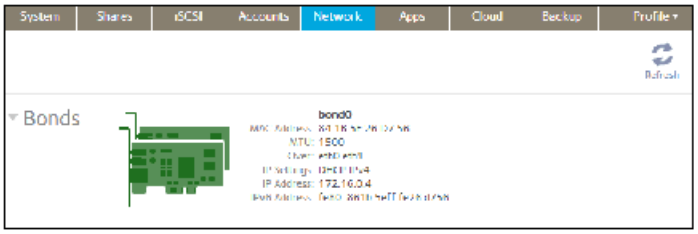


3. From the pop-up menu that displays, select **New Bond**.
   A pop-up screen displays.

   The options displayed depend on the teaming mode that is selected.
4. From the **Bond with** list, select another available Ethernet interface to include in the bonded adapter.
5. From the **Teaming Mode** list, select a teaming mode.
   For more information about teaming modes, see *Teaming Modes* on page 153.
6. (For IEEE 802.3ad LACP and XOR only) Select the radio button next to the hash type option that you want to use.
   For more information about hash types, see *Hash Types* on page 153.
7. (For Active Backup only) From the **Primary Device** list, select the Ethernet interface that is active by default.

Other Ethernet interfaces in the bond become active if and only if the active interface fails.

8. Click the **Create** button.
   The new bonded adapter displays on the Network screen. The bonded adapter is named bondX, where X is a number in sequential and ascending order.



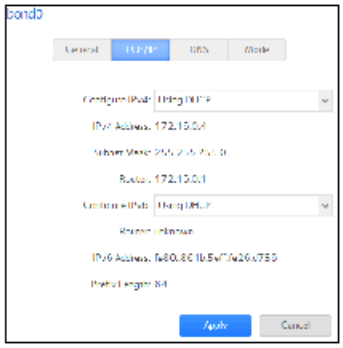
Configure General and TCP/IP Settings

To configure a bonded adapter:

1. Select **Network > Bonds**.
2. Select settings **gear** icon for the bonded adapter that you want to configure.
3. From the pop-up menu that displays, select **Settings**.
   The bond settings pop-up screen displays.
4. Configure the settings in the **General** tab as explained in the following table:

Item	Description
Name	Cannot be edited. Displays the name of the bonded adapter.
MTU	Enter the MTU in bytes. The default setting is 1500 bytes.

5. Click the **TCP/IP** tab.



6. Configure the TCP/IP settings as explained in the following table.

Note: NETGEAR recommends that you use DHCP address reservation to make sure that the DHCP server always assigns the same IP address to the interfaces of the

ReadyNAS. The MAC addresses of the physical interfaces are shown on the Network screen.

Note: If you enter an IP address manually, you must provide DNS server information if you want to access your ReadyNAS system over the Internet. For more information, see *DNS* on page 148. If the IP address changes, your browser loses its connection to your ReadyNAS storage system. To reconnect to your ReadyNAS system, use ReadyCLOUD to rediscover your device. See *Discover and Set Up Your ReadyNAS* on page 13.

Item	Description	
IPv4 settings		
Configure IPv4	From the list, select how IPv4 is configured: • **Using DHCP**. The ReadyNAS functions as a DHCP client, and the IPv4 settings are automatically configured by a DHCP server on your network. • **Manually**. You must enter the IPv4 address and subnet mask for the ReadyNAS and the router through which the ReadyNAS is connected to the network.	
IPv4 Address	Enter the IPv4 address for the ReadyNAS.	Manual configuration only.
Subnet Mask	Enter the subnet mask for the ReadyNAS.	
Router	Enter the IPv4 address for the router through which the ReadyNAS connects to your network.	
IPv6 settings		
Configure IPv6	From the list, select how IPv6 is configured: • **Automatically**. The ReadyNAS is configured with an IPv6 address through stateless auto configuration without the requirement of a DHCPv6 server on your network. The ReadyNAS must be connected to the Internet for stateless autoconfiguration to function. • **Using DHCP**. The ReadyNAS functions as a DHCPv6 client. The IPv6 settings are automatically configured by a DHCPv6 server on your network. • **Manually**. You must enter the IPv6 address and prefix length for the ReadyNAS and the router through which the ReadyNAS is connected to the network.	
Router	Enter the IPv6 address for the router through which the ReadyNAS connects to your network. The default setting is unknown.	Manual configuration only.
IPv6 Address	Enter the IPv6 address for the ReadyNAS.	
Prefix Length	Enter the prefix length for the ReadyNAS. The default prefix length is 64.	

7. Click the **Apply** button.

Your changes are saved.

8. Configure the switch or router to which the ReadyNAS is attached to support the bonded adapter.

Configure DNS Settings

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

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

To add DNS information for a bonded adapter:

1. Select **Network > Bonds**.
2. Select the settings **gear** icon for the bonded adapter that you want to configure.
3. From the pop-up menu that displays, select **Settings**.
   The bond settings pop-up screen displays.
4. Click the **DNS** tab.

5. Click the **+** icon (.) to the right of the list of DNS servers.
6. In the pop-up screen that displays, enter the server IP address.

7. Click the **Add** button.
   The DNS server is added to the list.
8. Click the **Apply** button.

Your changes are saved.

9. Configure the switch or router to which the ReadyNAS is attached to support the bonded adapter.

Change the Teaming Mode

To change the teaming mode of a bonded adapter:

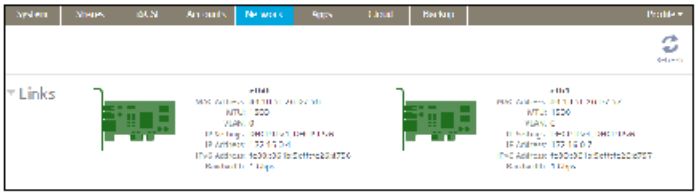
1. Select **Network > Bonds**.
2. Select the settings **gear** icon for the bonded adapter that you want to configure.
3. From the pop-up menu that displays, select **Settings**.
   The bond settings pop-up screen displays.
4. Click the **Mode** tab.

5. From the **Teaming Mode** list, select a teaming mode.
   For more information about teaming modes, see *Teaming Modes* on page 153.
6. (For IEEE 802.3ad LACP and XOR only) Select the radio button next to the hash type option that you want to use.
   For more information about hash types, see *Hash Types* on page 153.
7. (For Active Backup only) From the **Primary Device** list, select the Ethernet interface that is active by default.
   Other Ethernet interfaces in the bond become active if and only if the active interface fails.
8. Click the **Apply** button.
   Your changes are saved.

Delete a Bonded Adapter

To delete a bonded adapter and reestablish separate Ethernet links:

1. Select **Network > Bonds**.
2. Select the settings **gear** icon for the bonded adapter that you want to delete.
3. From the pop-up menu that displays, select **Delete**.
4. Confirm the deletion.
   The bonded Ethernet interfaces are separated into individual links.



5. Reconfigure the switch or router to which the ReadyNAS is attached for single interfaces.

Configure Global Settings for File-Sharing Protocols

This section covers file-sharing concepts and configuring the different types of file-sharing protocols on your ReadyNAS storage system.

Basic File-Sharing Concepts

Network access to data stored on your ReadyNAS system is managed by file-sharing protocols, which handle the transfer of data. For shares, you can enable several protocols. For LUNs, the protocol is always iSCSI. (iSCSI is enabled by default.) The ReadyNAS can handle a maximum of 1,024 concurrent connections.

Global settings for file-sharing protocols apply to your entire ReadyNAS system. Share settings for file-sharing protocols apply to individual shares.

When you enable a file-sharing protocol for an individual shared folder, the protocol is also enabled globally. When you disable a file-sharing protocol for an individual shared folder, the protocol remains enabled globally so that you can still access other folders that might be using the protocol.

If a protocol is disabled globally, you can configure its settings for individual shares, but the settings are not effective until you enable the protocol. For information about how to configure and enable file-sharing protocols for individual shares, see *Set Network Access Rights to Shared Folders* on page 48.

For best performance, enable only those file-sharing protocols that you use. Disable the file-sharing protocols that you do not use to maximize system memory and improve system performance. 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.

Supported File-Sharing Protocols

The ReadyNAS supports the following file-sharing protocols:

Table 25. Supported file-sharing protocols

Protocol	Description	Recommendation
SMB (Server Message Block)	Used mainly by Microsoft Windows computers and sometimes by Mac OS X computers, this protocol is enabled by default. It is sometimes	If Windows users access your storage system, enable this protocol.

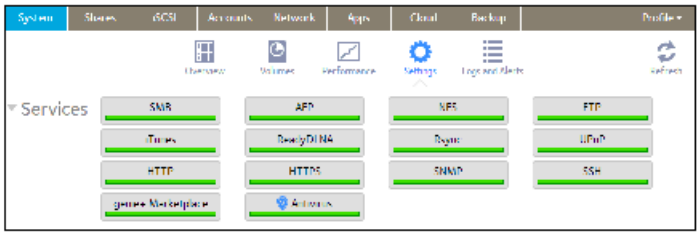
Protocol	Description	Recommendation
	referred to as the CIFS (Common Internet File Service) file-sharing protocol. SMB uses TCP/IP.	
NFS (Network File Service)	Linux and Unix computers use NFS. Mac OS X users can access NFS shared folders through console shell access. Your ReadyNAS system supports NFS v3 over UDP and TCP and NFS v4 over TCP.	If Linux or Unix users access your storage system, enable this protocol.
AFP (Apple File Protocol)	Mac OS X computers use AFP. Your ReadyNAS system supports AFP 3.3.	If only Mac OS X users access your storage system, enable this protocol. However, in a mixed Windows and Mac environment, NETGEAR recommends using SMB only.
FTP (File Transfer Protocol) and FTPS (FTP with SSL encryption)	Many public file upload and download sites use FTP. The ReadyNAS supports anonymous or user access for FTP clients. You can elect to set up port forwarding to nonstandard ports for passive FTP, allowing clients to initiate a connection to the ReadyNAS.	If users access your storage system using FTP, 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 access your storage system from a device that supports Rsync, enable this protocol.
HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP with SSL encryption)	Used on the World Wide Web.	If users access your storage system from a device with a web browser, including a smartphone or tablet computer, enable this protocol.
SSH	Lets you remotely manage the ReadyNAS over an SSH connection.	For security reasons, NETGEAR recommends that you do not enable SSH. If you enable SSH root access, NETGEAR reserves the right to deny you technical support.

By default, SMB and AFP are enabled and FTP, NFS, and SSH are disabled.

Configure File-Sharing Protocols

To configure global settings for file-sharing protocols:

1. Log in to your ReadyNAS.
2. Select **System > Settings > Services**.



Protocol buttons with a green indicator are globally enabled. Those with a gray indicator are globally disabled. Click a protocol button to display the protocol settings screen.

3. Configure one protocol at a time, as explained in the following sections.
   - *Configure SMB, AFP, Rsync, or SSH* on page 161.
   - *Configure FTP* on page 161.
   - *Configure NFS* on page 163.
   - *Configure HTTP* on page 164.
   - *Configure HTTPS* on page 164.

Configure SMB , AFP , Rsync, or SSH

The only option for these protocols is to enable or disable the protocol globally.

To configure SMB, AFP, Rsync, or SSH:

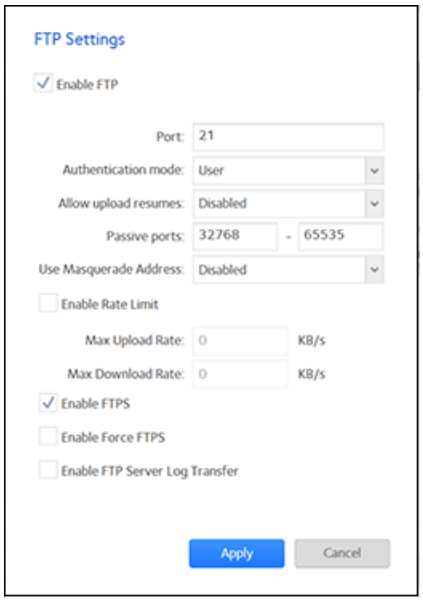
1. Logi in to your ReadyNAS.
2. Select **System > Settings > Services**.
3. Click the protocol button (**SMB**, **AFP**, **Rsync**, or **SSH**).
   - If the indicator is green, the protocol is enabled.
   - If the indicator is gray, the protocol is disabled.

WARNING:
For SSH, if you enable SSH root access, NETGEAR might deny you technical support. If you do enable SSH root access, the SSH root password is identical to the administrator password that you configured.

Configure FTP

To configure FTP:

1. Select **System > Settings > Services**.
2. Click the **FTP** button.



3. Configure the settings as explained in the following table:

Item	Description	
Enable FTP	Select the check box to enable FTP globally. Clear the check box to disable FTP globally.	
Port	Enter the number of the port that is used for FTP control traffic on the ReadyNAS. The default port number is 21.	
Authentication mode	Select the authentication mode from the drop-down list: • **Anonymous**. Users can connect anonymously. • **User**. Users are authenticated through the local database. This is the default setting.	
Allow upload resumes	Select whether users are allowed to resume a paused or stalled upload: • **Disabled**. Resuming an upload is disabled. This is the default setting. • **Enabled**. Resuming an upload is enabled.	
Passive ports	Enter the beginning port and ending port of the passive port range. This is the port range on the ReadyNAS that is available to clients who initiate a connection to the ReadyNAS. The default range is 32768–65535.	
Use Masquerade Address	Select whether the ReadyNAS displays its real IP address or masks this with another IP address or DNS name: • **Disabled**. The real IP address is displayed. • **Enabled**. The real IP address is masked. Use the **Masquerade as** field to specify an IP address or DNS name.	
	Masquerade as	Enter a public IP address or DNS name.
Enable Rate Limit	Max Upload Rate	Enter the maximum upload rate per session in KB/s.
	Max Download Rate	Enter the maximum download rate per session in KB/s.

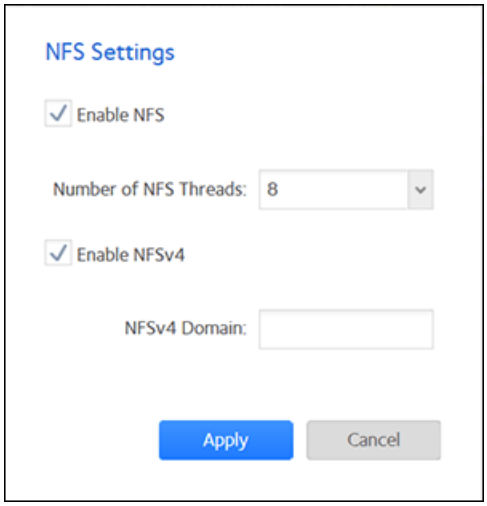
Item	Description
Enable FTPS	Select the check box to allow FTP connections with TLS encryption. Enabling this option does not require FTP connections to use TLS encryption.
Enable Force FTPS	Select the check box to require the use of FTPS.
Enable FTP Server Log Transfer	Select this check box to include FTP file transfers in the system log. For more information about the system log, see *System Logs* on page 176.

4. Click the **Apply** button.
   Your changes are saved.

Configure NFS

To configure NFS:

1. Select **System > Settings > Services**.
2. Click the **NFS** button.



3. Configure the NFS settings as explained in the following table:

Item	Description
Enable NFS	Select the check box to enable NFS globally. Clear the check box to disable NFS globally.
Number of NFS Threads	You can select from 8 to 32 threads. If many clients connect to the ReadyNAS using the NFS protocol, increasing the number of NFS threads can improve performance.
Enable NFSv4	Select the check box to enable NFSv4 globally. Clear the check box to disable NFS globally.
NFSv4 Domain	If you enable NFSv4, you can specify the NFSv4 domain.

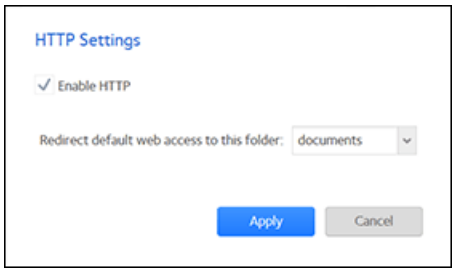
4. Click the **Apply** button.

Your changes are saved.

Configure HTTP

To configure HTTP:

1. Select **System > Settings > Services**.
2. Click the **HTTP** button.



3. Configure the HTTP settings as explained in the following table:

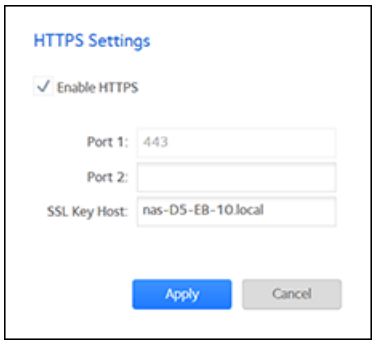
Item	Description
Enable HTTP	Select the check box to enable HTTP globally. Clear the check box to disable HTTP globally.
Redirect default web access to this folder	If you want to automatically redirect http://<*ReadyNAS_IP_address*> to a certain shared folder, select that folder from the drop-down list. This is useful if you do not want to expose your default folder listing to outsiders. To redirect to a shared folder, create an index file (such as index.htm or index.html) in your target shared folder and enable the HTTP protocol for read-only access to that folder.

4. Click the **Apply** button.
   Your changes are saved.

Configure HTTPS

To configure HTTPS:

1. Select **System > Settings > Services**.
2. Click the **HTTPS** button.
   The HTTPS Settings screen displays.



3. Configure the HTTPS settings as explained in the following table:

Item	Description
Enable HTTPS	HTTPS cannot be disabled. The local admin page requires HTTPS to be enabled.
Port 1	Cannot be modified. Port 1, the value 443, is reserved for your ReadyNAS system.
Port 2	Set to a value in the range 1024–65535. Check to see if you need to enable port forwarding of the port you choose on the router. See the port forwarding instructions provided with your router.
SSL Key Host	Configures the host name used for your ReadyNAS system to generate its SSL certificate and then creates 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 use 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.

4. Click the **Apply** button.
Your changes are saved.

Configure Media Services

This section covers configuring the settings for ReadyDLNA and iTunes streaming server on your ReadyNAS storage system.

ReadyDLNA

The ReadyDLNA service lets you stream media on your ReadyNAS to DLNA players such as the Sony PlayStation 3, Xbox 360, TiVo, and DLNA-enabled TVs. You can stream your media to any device that complies with the Digital Living Network Alliance (DLNA) standard, including mobile clients, such as iPads, iPhones, and Android devices.

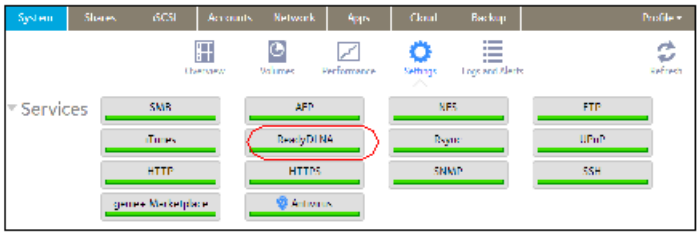
ReadyDLNA supports to following formats:

- **Music**. wav, wma, pcm, ogg, mp3, m4a, flac, aac
- **Video**. 3gp, mp4, wmv, xvid, vob, ts, tivo, mts, mpeg, mpg, mov, mkv, m4v, m4p, m2t, m2ts, flv, flc, fla, divx, avi, asf
- **Photo**. jpg, jpeg
- **Playlist**. m3u, pls

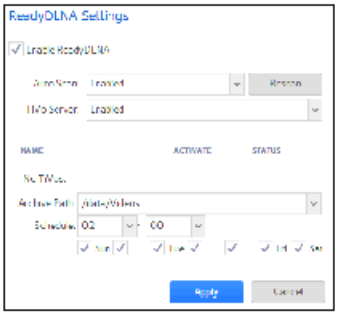
Enable ReadyDLNA

To enable the ReadyDLNA streaming service:

1. Select **System > Settings > Services**.
2. Click the **ReadyDLNA** button.



A pop-up screen displays.



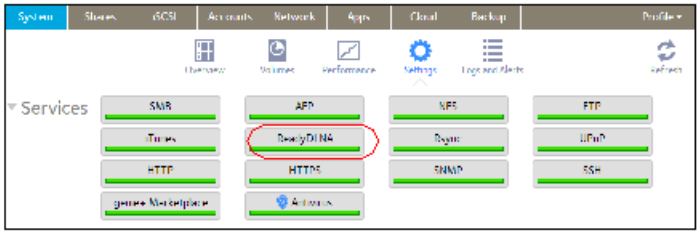
3. Select the Enable ReadyDLNA check box.
4. (Optional) From the **Auto Scan** drop-down list, select **Enabled** or **Disabled**:
   - **Enabled**. The system automatically searches for DLNA-compliant devices.
   - **Disabled**. The system does not search for DLNA-compliant devices.
5. Click the **Apply** button.
   Your changes are saved.

Create a TiVo Archive

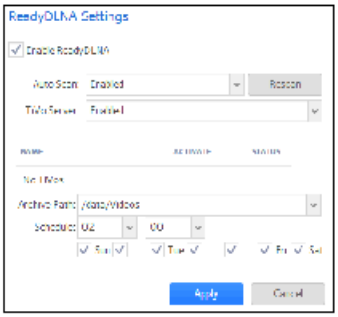
You can use your ReadyNAS system to store videos and media recorded on your TiVo box. The ReadyNAS downloads data from your TiVo box according to a schedule that you specify.

To create an archive of your TiVo data on your ReadyNAS:

1. Select **System > Settings > Services**.
2. Click the **ReadyDLNA** button.



A pop-up screen displays.



3. Select the **Enable ReadyDLNA** check box.
4. From the **Auto Scan** drop-down list, select **Enabled**.
5. Click the **Apply** button.
6. Again click the **ReadyDLNA** button.
7. From the **TiVo Server** drop-down list, select **Enabled**.
   The system detects TiVo devices on your LAN and displays them in the list.
8. When prompted, enter the media access key provided by your TiVo box.
9. Select the **Activate** check box next to the name of your TiVo box.
10. From the **Archive Path** drop-down list, select the path to the folder where you want to store data downloaded from your TiVo.
11. Use the check boxes and drop-down lists to schedule the time and days that the ReadyNAS downloads data from your TiVo box.
12. Click the **Apply** button.
    Your changes are saved.

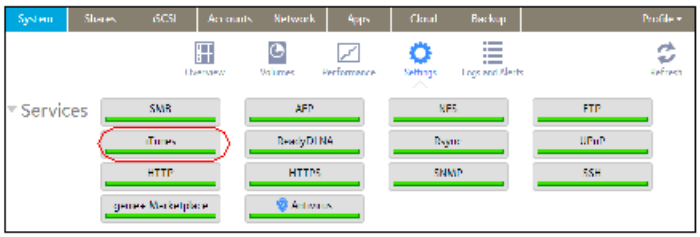
iTunes Streaming Server

iTunes Streaming Server enables iTunes clients to stream media files straight from your ReadyNAS system. The ReadyNAS supports the following iTunes formats:

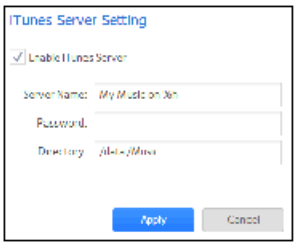
- Audio. mp3, m4a, m4p, wav, aif
- Video. m4v, mov, mp4
- Playlist. m3u, wpl

To set up iTunes Streaming Server:

1. Select **System > Settings > Services**.
2. Click the **iTunes** button.



A pop-up screen displays.



3. Configure the iTunes server settings as explained in the following table:

Item	Description
Enable iTunes Server	Select the check box to enable the iTunes server. Clear the check box to disable the iTunes server.
Server Name	Enter a name that your ReadyNAS will use to advertise itself to your iTunes clients. By default, the server name is set to My Music on %h where %h is the host name of your ReadyNAS system.
Password	Enter a password to limit access to your ReadyNAS iTunes server.
Directory	Enter the path to the folder on the ReadyNAS system where you store your music files. Your iTunes clients will stream music from this folder. By default, the path is set to /data/Music.

4. Click the **Apply** button.
Your changes are saved.

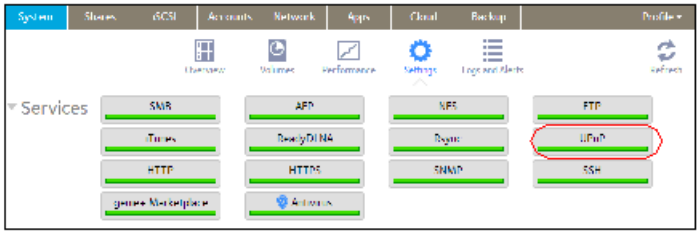
Configure Discovery Services

Discovery services are protocols that allow network-enabled devices like computers or your storage system to discover each other across networks. Your storage system supports the Bonjour and UPnP discovery service protocols:

- **Bonjour**. Enables discovery of various services on your ReadyNAS system and provides a way to connect to the local admin page for your ReadyNAS, IPP printing, and AFP services. OS X has built-in Bonjour support. You can download Bonjour for Windows from Apple's website. Bonjour is not configurable on your ReadyNAS.
- **UPnP (Universal Plug-n-Play)**. Allows UPnP-enabled clients to discover your ReadyNAS system on your LAN. You can enable or disable UPnP on your ReadyNAS.

To enable the UPnP:

1. Select **System > Settings > Services**.
2. Click the **UPnP** button.



- If the indicator is green, the protocol is enabled.
- If the indicator is gray, the protocol is disabled.

Install and Manage Apps

From the local admin page, you can install and manage apps for your ReadyNAS.

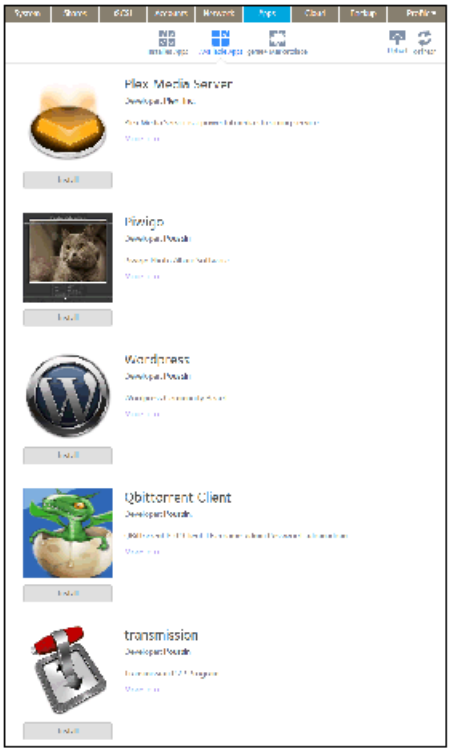
- To install apps, select **Apps > Available Apps**.
  For information about installing apps, see *Install Free Apps* on page 169.
- To view your installed apps, select **Apps > Installed Apps**.
  For information about managing installed apps, see *Manage Installed Apps* on page 170.

Install Apps

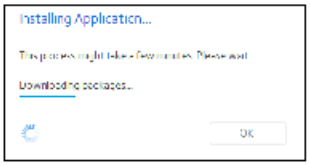
Many apps are available for your ReadyNAS.

To install an app on your ReadyNAS:

1. Log in to your ReadyNAS.
2. On the local admin page, select **Apps > Available Apps**.



3. Click the **Install** button below the app that you want to install.
   A pop-up window informs you that the download and installation process is in progress.



   A notification appears when the installation process is complete.

   You can view the installed app by selecting **Apps > Installed Apps**.

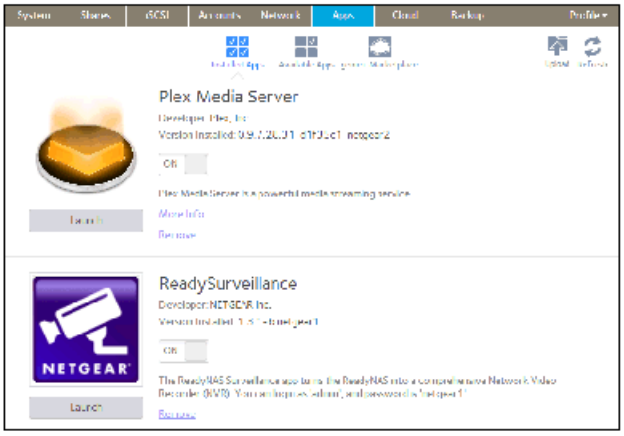
   For information about managing installed apps, see *Manage Installed Apps* on page 170.

Manage Installed Apps

You can manage apps installed on your ReadyNAS from the local admin page.

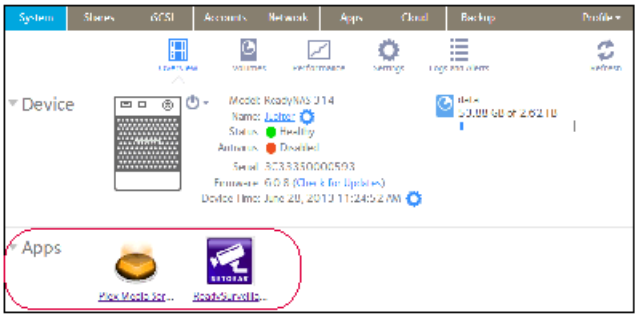
To manage installed apps:

1. **Log in to your ReadyNAS.**
2. **Select Apps > Installed Apps on the local admin page.**
   A list of apps installed on your ReadyNAS system displays.



From this window, you can launch, enable, disable, or remove installed apps.

Tip: Installed apps that can be launched also appear on the Overview window. You can launch an app from this window by clicking it.



System Maintenance

8

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

- *System Monitoring*
- *System Maintenance*
- *Optional Uninterruptible Power Supplies*

System Monitoring

The local admin page for your ReadyNAS system provides system and disk health information as well as system logs. Real-time historical monitoring is available for most models. You can also enable the SNMP protocol to remotely monitor your ReadyNAS system using an SNMP client.

System and Disk Health Information

The ReadyNAS provides basic system health information about the fans, temperatures, optional uninterruptible power supplies, and optional expansion disk arrays.

To view system and disk health information :

1. Select **System > Performance > Status**.

2. (Optional) To view disk status and health information, point to a disk status indicator.

System Real-Time and Historical Monitoring

The ReadyNAS provides status graphics for volume throughput, network throughput, volume utilization, and system temperatures.

> **Note:** Status graphics are not supported for ReadyNAS 102 and 104 systems.

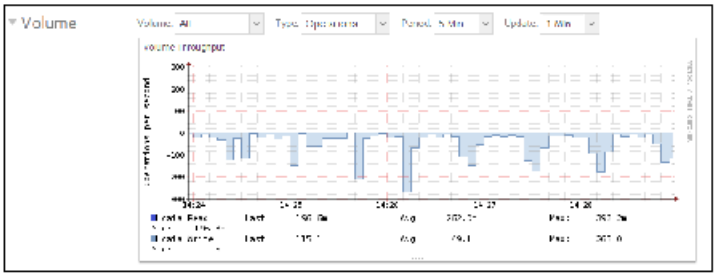
To display and configure the system status graphics:

1. Select **System > Performance**.
2. Scroll down to Volume, Network, Utilization, or Temperature to view the corresponding status graphics.

The following sections describe the information displayed on these status graphics.

Volume

The Volume throughput graphic shows the number of read and write operations per second.



The range is flexible and depends on your selections from the drop-down lists above the graphic. For example, the range can be from 0 to 200 operations. The upper part of the graphic indicates the number of read operations (indicated by positive numbers). The lower part of the graphic indicates the number of write operations (indicated by negative numbers).

From the drop-down lists above the graphic, you can adjust the following settings:

- **Volume**. Select all volumes or individual volumes.
- **Type**. Select the number of operations per second or the bandwidth consumed per second.
- **Period**. Select the period over which the operations or bandwidth is measured. You can select from 5 minutes to 1 year.
- **Update**. Select how often the information in the graphic is updated. You can select from 1 to 30 minutes.

Network

The Network throughput graphic shows the network usage for Tx and Rx traffic in bytes per second.

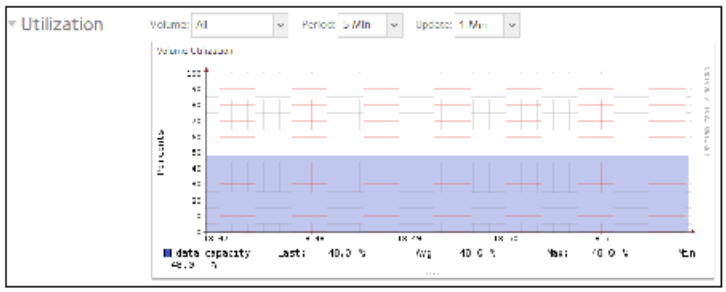
The range is flexible and depends on your selections from the drop-down lists above the graphic. For example, the range can be 0 to 60 bytes or from 0 to 40 KB. The upper part of the graphic indicates the incoming (Rx) traffic; the lower part of the graphic indicates the outgoing (Tx) traffic.

From the drop-down lists above the graphic, you can adjust the following settings:

- **Network**. Select all network interfaces, individual interfaces, or individual bonds.
- **Protocol**. Select all protocols or individual protocols (SMB, NFS, AFP, HTTP, HTTPS, SSH, iSCSI, or SMTP).
- **Period**. Select the period over which the network usage is measured. You can select from 5 minutes to 1 year.
- **Update**. Select how often the information in the table is updated. You can select from 1 to 30 minutes.

Utilization

The Volume utilization graphic shows the percentage of used storage space for an individual volume or for all volumes. The range is from 0 to 100 percent.

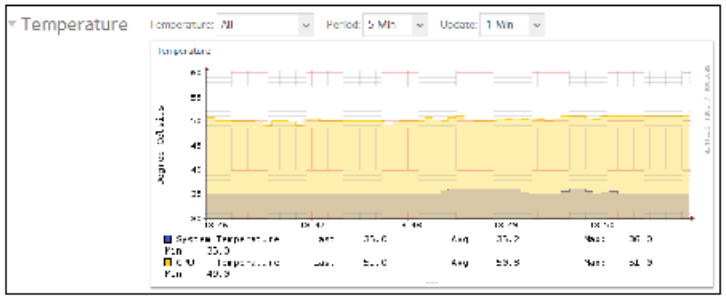


From the drop-down lists above the graphic, you can adjust the following settings:

- **Volume**. Select all volumes or individual volumes.
- **Period**. Select the period over which the utilization is measured. You can select from 5 minutes to 1 year.
- **Update**. Select how often the information in the table is updated. You can select from 1 to 30 minutes.

Temperature

The Temperature graphic shows the system temperatures in degrees Celsius.



The range is flexible and depends on your selections from the drop-down lists above the graphic and the temperatures that are measured. For example, the range can be from 0 to 50 degrees Celsius.

From the drop-down lists above the graphic, you can adjust the following settings:

- **Temperature**. Select all temperatures, the system (SYS) temperature, the CPU temperature, or the auxiliary (AUX) temperature.
- **Period**. Select the period over which the temperatures are measured. You can select from 5 minutes to 1 year.
- **Update**. Select how often the information in the table is updated. You can select from 1 to 30 minutes.

System Logs

System logs provide information about the status of various system management tasks, including a time stamp. You can view system log messages from the local admin page, download the complete system logs to a local computer or USB drive, and receive system alerts. These logs are used primarily to troubleshoot problems. If you call NETGEAR technical support, the representative might ask you to send your system logs.

Depending on the settings, the system logs record events such as the following:

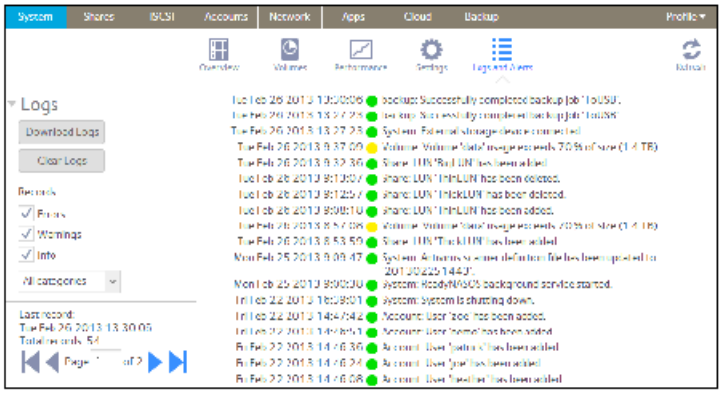
- System events such as the creation or deletion of a share, LUN, snapshot, or low disk space
- Addition and removal of hot-swappable disks
- Detection of disk types and hardware statistics
- Removal and addition of eSATA expansion chassis
- Removal and addition of SSDs
- Removal and addition of power supplies
- Removal and addition of a UPS
- Connection and disconnection of external USB devices

The following events are recorded in the system log and also generate alerts (see *Configure System Alerts* on page 142) and SNMP traps (see *SNMP Monitoring* on page 178). Warnings also display on the local admin page when these events occur:

- Disk errors and failures
- Changes in network connectivity
- Power supply failures
- UPS failures
- Fan speed irregularities and fan failures
- CPU and enclosure temperature violations

To display and manage the system logs:

1. Select **System > Logs and Alerts**.



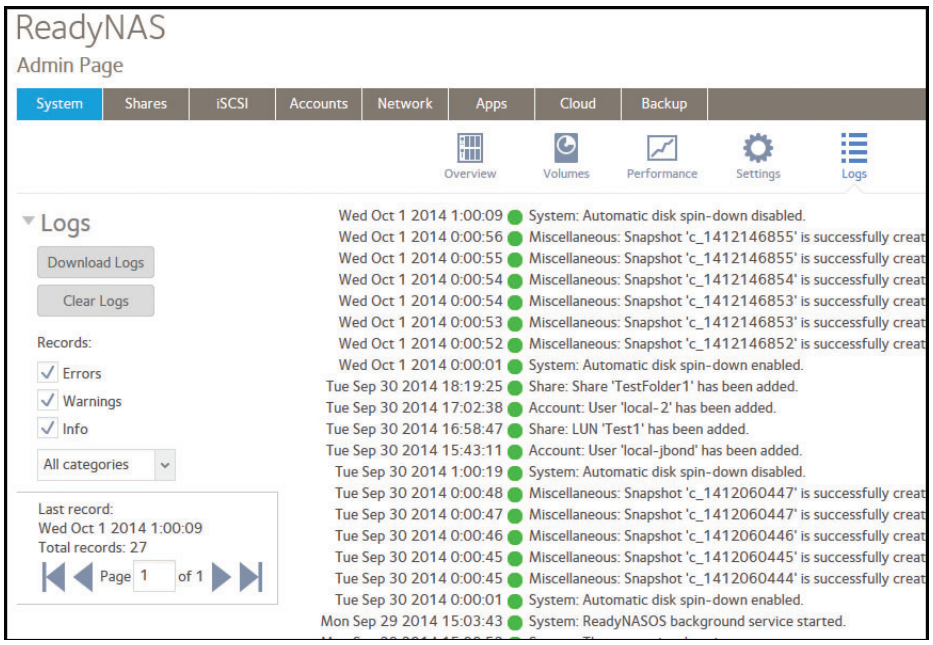
2. To view additional messages, use the navigation box in the lower left corner of the screen.
3. Do any of the following:
   - **Download the logs**. Click the **Download Logs** button to download a zipped file with all log files to your browser's default download location. The default name of the zipped file is `System_log-<host name >.zip`, in which <*host name*> is the host name of the ReadyNAS (see *Configure the Host Name* on page 145).
   - **Clear the logs**. Click the **Clear Logs** button. The log entries onscreen are cleared but the log files remain intact.
   - **Configure the logs**. Under Records, select which message levels and categories are logged. These selections affect the system logs, alerts, SNMP traps, and onscreen messages:
     - **Message levels**. By default, the **Errors**, **Warnings**, and **Info** check boxes are selected, causing errors, warnings, and informational messages to be logged. You can clear any check boxes.
     - **Message categories**. By default, messages for all categories are logged. From the list, you can select to log individual categories only: **System**, **Disk**, **Volume**, **Share**, **Backup**, **Account**, or **Miscellaneous**.

Downloading Logs

Your ReadyNAS server creates logs for both routine and exceptional actions. These logs can help support diagnose the cause of a problem. For support to read the logs, you must download them and send them to support.

To download logs:

1. Log in to the ReadyNAS server from which you want to download logs.
2. Select **System > Logs**.
   The available logs and actions displays.



3. Click the **Download Logs** button.
   Your browser opens the Save File window.
4. Save the file on your computer, remembering the location.
5. If you downloaded the log at support's request, follow their directions on transferring the file to them.

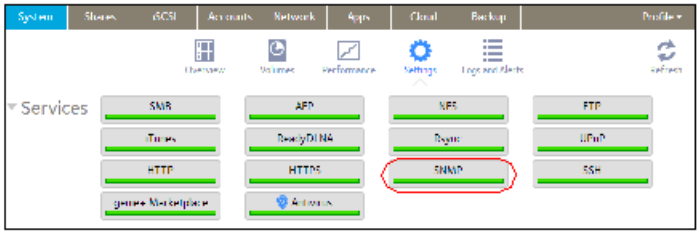
SNMP Monitoring

Use SNMP management systems such as HP OpenView or CA UniCenter for remote monitoring of the ReadyNAS. (Management over SNMP is not supported.)

Configure SNMP

To configure SNMP:

1. Select **System > Settings > Services**.
2. Click the **SNMP** button.



3. Configure the settings as explained in the following table:

Item	Description
Enable SNMP	Select the check box to enable SNMP globally. Clear the check box to disable SNMP globally.
Community	Enter the community. Normally, you would enter public for a read-only community and private for a read/write community. You can leave the Community field set to public (which is the default setting) or you can specify a private name if you have a more segregated monitoring scheme.
Trap Destination	Enter the IP address to which the ReadyNAS sends the traps that it generates. For information about the types of messages that the ReadyNAS sends, see *System Logs* on page 176.
Hosts Allowed Access	Enter a network address that specifies the hosts that are allowed to access the ReadyNAS.

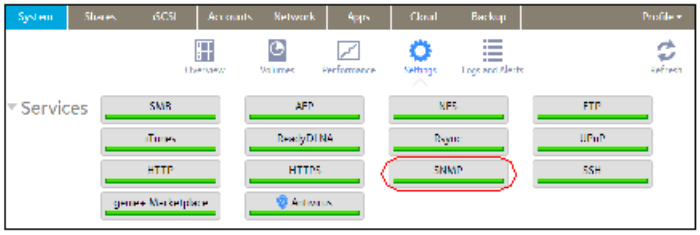
4. Click the **Apply** button.
   Your changes are saved.

Download the NETGEAR SNMP MIB

You can download the NETGEAR SNMP MIB from the local admin page and import it to your SNMP client applications. For information about the types of messages that the ReadyNAS can send to SNMP hosts, see *System Logs* on page 176.

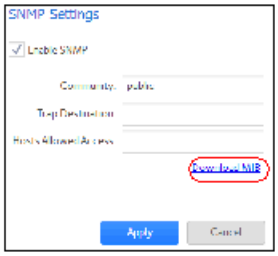
To download the NETGEAR SNMP MIB:

1. Select **System > Settings > Services**.
2. Click the **SNMP** button.



The SNMP Settings screen displays.

3. Click the **Download MIB** link.



System Maintenance

This sections covers upgrading and resetting firmware, recovering the administrator password, shutting down or restarting the system, and managing system power.

Update 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.

Updates are numbered chronologically, for example:

- ReadyNAS OS 6.0.1
- ReadyNAS OS 6.0.2

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.

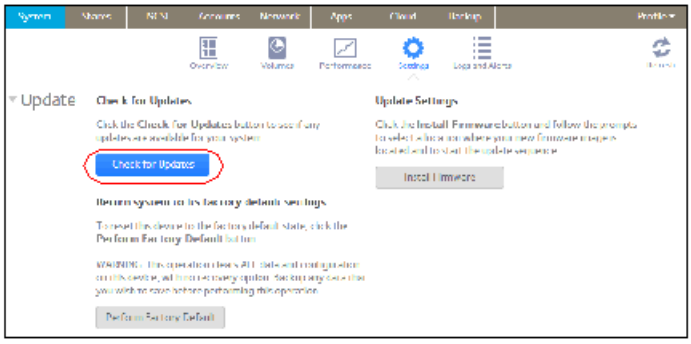
NETGEAR recommends that you back up your data, especially data that cannot be replaced, before you perform a firmware update.

Update Firmware Directly from the NETGEAR Website

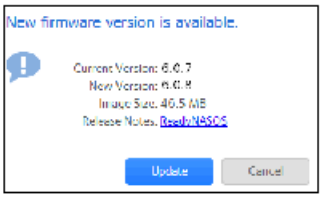
If your ReadyNAS system can access the Internet, the remote method is easiest way to update your firmware.

To update firmware remotely:

1. Select **System > Settings > Update**.
2. Click the **Check for Updates** button.



   - If no firmware update is available, you are notified that your system is using 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 **Update** button on the pop-up screen that displays.



   The system downloads the new firmware. When the download is complete, you are prompted to reboot your system.

4. Click the **Reboot** button.
   Your system reboots and installs the new firmware. If you enabled email alerts, your ReadyNAS system sends a message when the firmware update finishes.

Update Firmware Without Direct Internet Access

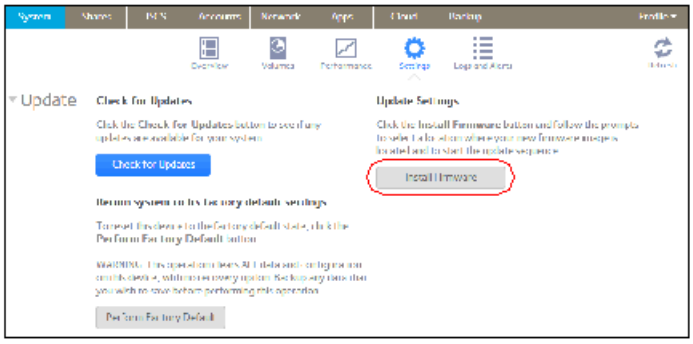
If you keep your ReadyNAS system in a location without Internet access, for example, at a remote vacation cabin, you must update your firmware locally.

To update firmware locally:

1. Using a computer that can access the Internet, download the latest firmware for your system from *http://support.netgear.com/product/ReadyNAS-OS6*.

If you can later connect this computer to the local area network with the ReadyNAS, download directly to the computer; otherwise, download the file to a USB drive or other portable media.

2. Connect the computer on which you downloaded the latest firmware to the network with the ReadyNAS, or if you downloaded to a USB drive, connect the USB drive to a computer on the local network.
3. Log in to the ReadyNAS.
4. On the local admin page, select **System > Settings > Update**.



5. Click the **Install Firmware** button.

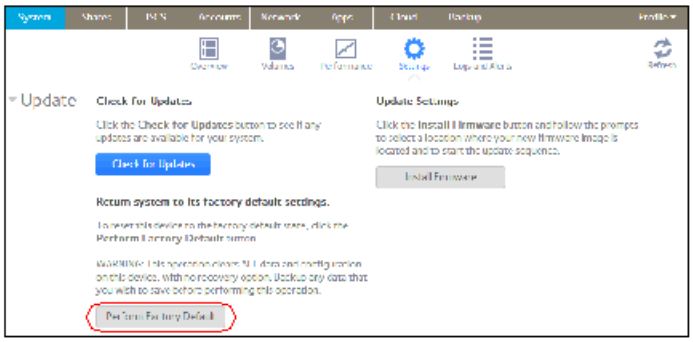
6. Click the **Browse** button.
7. In the pop-up file browser that displays, navigate to the file containing the updated firmware and select it.
   The Update Firmware pop-up screen displays the name of the selected file in the **File Name** field.
8. Click the **Upload** button.
   The firmware file uploads to your ReadyNAS system. After a few moments, the Update Firmware pop-up screen displays details about the new firmware.
9. Click the **Install** button.
   You are prompted to reboot your ReadyNAS system to complete the firmware installation.
10. Reboot your ReadyNAS system.
    If you enabled email alerts, your ReadyNAS system sends a message when the firmware update finishes.

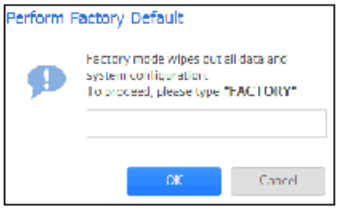
Reset the Firmware to Factory Defaults

WARNING:
Resetting the ReadyNAS to factory defaults deletes not only the configuration but also all stored data. Back up the stored data if you intend to use it again.

To reset the ReadyNAS to factory defaults:

1. Select **System > Settings > Update**.
2. Click the **Perform Factory Default** button.





3. Type **FACTORY** (all capital letters) in the field.
4. Click the **OK** button.
   The process of resetting your system to its factory default settings begins. If you enabled email alerts, the ReadyNAS sends a message when the factory defaults are restored.

Recover the Administrator Password

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

- **Use NETGEAR's password recovery tool**. This web-based tool requires that you enable administrator password recovery on your storage system before you can use it. For more information, see *Set the Administrator Password* on page 140.
- **Perform an OS reinstall reboot**. This process reinstalls the firmware on the storage system and resets the administrator user name and password to factory defaults.

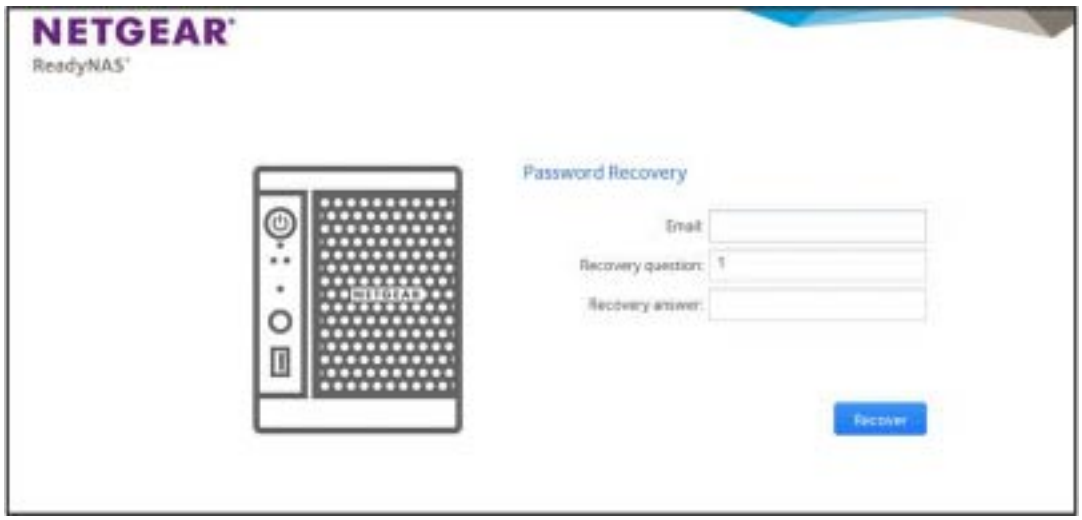
Recover the Administrator Password Using NETGEAR's Password Recovery Tool

This procedure is an option only if you enabled password recovery. For more information about setting up password recovery, see *Set the Administrator Password* on page 140. If you lost the password but did not enable administrator password recovery, see *Recover the Administrator Password Using an OS Reinstall Reboot* on page 184.

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

1. Launch a web browser and visit https://< *ReadyNAS_IP_address*>/password_recovery.
   The Password Recovery screen displays.

<ReadyNAS_IP_address> is the IP address of the storage system.



2. Enter the email address, the number of the recovery question (1 for the first question, and so on), and password recovery answer that you specified on the storage system.
   See *Set the Administrator Password* on page 140.
3. Click the **Recover** button.
   NETGEAR resets the administrator password and sends an email message with the new password to the password recovery email address.

Recover the 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. The default credentials to log in to the local admin page are as follows:

- **User name**: admin
- **Password**: password

Both user name and password are case-sensitive.

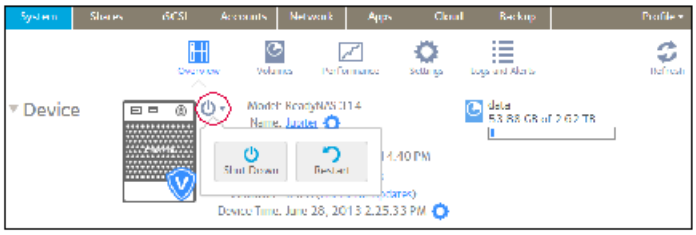
For information about how to perform an OS reinstall reboot on the storage system, see the hardware manual for your system, which is available at *http://support.netgear.com/product/ReadyNAS-OS6.*

Shut Down or Restart the System

Use the **Power** icon at the top right corner of the local admin page to gracefully shut down or restart the ReadyNAS.

To gracefully shut down or restart the system:

1. Select **System > Overview**.
2. Click the **Power** icon next to the image of your system.



3. From the pop-up menu that displays, select one of the following options:
   - **Shut down**. Gracefully power down the system.
   - **Restart**. Gracefully power down the system and restart it.
4. Confirm your selection.

If you enabled email alerts, the ReadyNAS sends a message after it restarts.

Manage Power Usage

You can configure settings on your ReadyNAS system to reduce power consumption.

Enable the Power Timer

You can configure your ReadyNAS system to power itself on and off automatically according to a schedule.

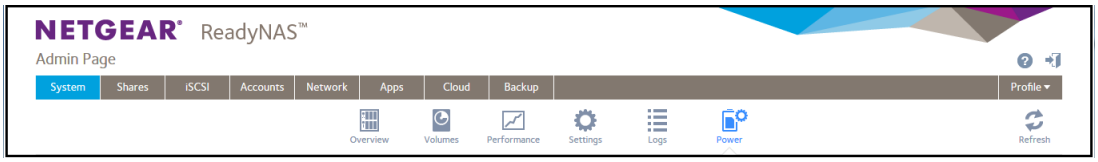
Not all ReadyNAS systems support this feature. If your system does not, the **Power On** option does not display in the **Action** list.

When the power timer is enabled, if the unit is disconnected from AC power, it powers on when AC power is reconnected.

> **Note:** If you schedule this device to power off, data transfers are interrupted and pending backup jobs do not run.

To enable the power timer:

1. Log in to your ReadyNAS system.



2. Select **System > Power**.
3. If not already expanded, expand **Power Timer**.
4. Select the **Power Timer** check box.
5. Click the **gear** icon ( ) next to the weekly calendar.

6. Set the power schedule for the system by clicking squares on the grid.
   The colors indicate the following:
   - Blue squares indicate time when the system is scheduled to be powered on.
   - Light and dark gray squares indicate time when the system is scheduled to be powered off.

   Tip: You can click the sun and moon icons at the top of the Power Timer pop-up screen to select entire day and night sections of the schedule. You can click the name of a day or the hour to select an entire row or column of the schedule.

   By default, the system is scheduled to remain powered off.
7. Click the **Apply** button.
   Your changes are saved.

Enable Wake-on-LAN

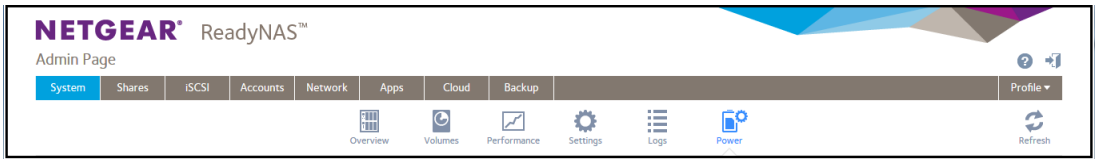
Wake-on-LAN is a way to remotely power up a network-attached device, like a computer or storage system. This feature allows you to conserve power by keeping a device turned off when it is not needed, but allows a remote system to turn it on when it is needed.

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. By default, wake-on-LAN is not enabled. When wake-on-LAN is enabled, if the unit is disconnected from AC power, it powers on when AC power is reconnected.

To enable wake-on-LAN:

1. Log in to your ReadyNAS.



2. Select **System > Power**.
3. If not already expanded, expand **Wake On LAN**.
4. Select the **Wake On LAN** check box.

What Is Disk Spin-Down

Disk spin-down reduces the rotation speed of your ReadyNAS disks. When the disks are spun down, power consumption is reduced, the disks are quieter, and disk life is extended; however, the disks must spin back up before the ReadyNAS can read or write data to them. This can cause an apparent slow down in disk performance and, depending on the application, can cause time outs.

You can control whether spin-down is used, how long a period of inactivity is needed before disk spin-down, and if used, what days and times it is enabled. If you use spin-down and also use applications that automatically read or write to the disks, either disable spin-down when the applications start writing to the disks, or verify that the disks spin back up fast enough not to cause a time out. It can take up to 10 seconds for disks to spin up. In some file server applications, a 10-second delay might be acceptable. For databases, virtualization, and many applications, the delay might cause the application or host operating system to time out and return an error.

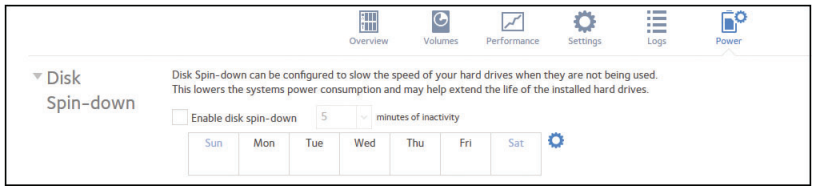
The energy saved depends on model, but a common figure is that a drive uses 5.3W during read/write operations, 3.4W while idle, and only 0.4W while in standby or sleep mode.

Set or Change Disk Spin-Down

Allowing disks to slow or spin down when not being actively used can potentially save power and extend the life of the disks, but this can also slow effective read/write speeds and can make the disks appear to be off-line or cause time outs.

To set or change the disk spin-down settings:

1. Log in to your ReadyNAS system.
2. Select **System > Power**.
3. If not already expanded, expand **Disk Spin-down**.



4. Select the **Enable disk spin-down** check box to enable spin-down, or, if it is enabled, clear the check box to disable it.
5. If spin-down is enabled, you can use the **minutes of inactivity** menu to select a delay of between 5 minutes and 45 minutes of inactivity before the disks spin down.
6. Click the **Settings** icon to open a calendar.

Use the calendar to set the days and times in which spin-down is active. You can set, and the ReadyNAS server will remember, calendar settings whether spin-down is enabled or not.

Optional Uninterruptible Power Supplies

Your ReadyNAS system supports the use of optional uninterruptible power supply (UPS) devices. This section discusses UPS basics, configuration and management.

Uninterruptible Power Supplies

NETGEAR recommends that you physically connect the ReadyNAS to one or more uninterruptible power supply (UPS) devices to protect against data loss due to power failures. Once a UPS is connected, you can use the ReadyNAS local admin page to monitor and manage it.

If you enable email alerts, the ReadyNAS sends a message when the status of a UPS changes. For example, if a power failure forces a UPS into battery mode or if a battery is low, you receive an email message.

When any UPS battery is low or when a power failure occurs, the ReadyNAS automatically shuts down gracefully.

UPS Configurations

The ReadyNAS supports UPS devices managed over SNMP and UPS devices managed over a remote connection.

UPS Devices Managed over SNMP

An SNMP UPS lets the ReadyNAS query the manufacturer-specific Management Information Base (MIB). The ReadyNAS monitors and manages the UPS using the SNMP protocol. The Ethernet connection between the UPS and the ReadyNAS passes through a switch.

UPS Devices Managed over a Remote Connection

A remote UPS is attached to a remote server, such as a ReadyNAS or a Linux server that is running Network UPS Tools (NUT). The ReadyNAS monitors and manages the UPS over the remote connection. The Ethernet connection between the UPS and the ReadyNAS passes through a switch.

Manage UPS Devices

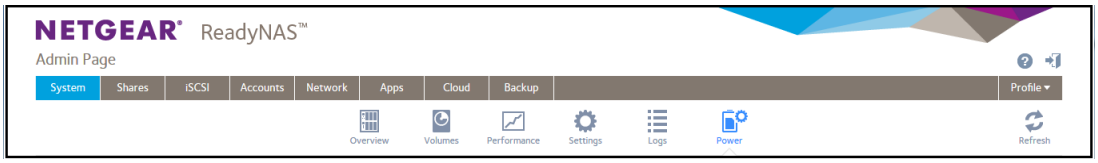
You can manually add, edit, and remove UPS devices as well as monitor the status of connected UPS devices.

Add a UPS

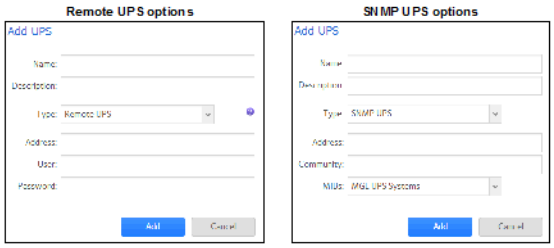
If your UPS is not automatically detected when you connect it to your ReadyNAS system, you must manually add the UPS.

To add a UPS:

1. Log in to your ReadyNAS.



2. Select **System > Power** .
3. If not already expanded, expand **UPS**.
4. Click the **+** icon next to the UPS heading.



The options displayed depend on the type of UPS that you want to add.

5. Configure the settings as explained in the following table:

Item		Description
Name	Enter a name to identify the UPS: • For an SNMP UPS, enter any name. • For a remote UPS, you must enter **UPS**.	
Description	An optional description to help identify the UPS.	
Type	From the drop-down list, select one of the following options: • **SNMP UPS**. An SNMP UPS lets the ReadyNAS query the manufacturer-specific MIB. The ReadyNAS monitors and manages the UPS through SNMP. • **Remote UPS**. A remote UPS is attached to a remote server, such as a ReadyNAS or a Linux server that is running Network UPS Tools (NUT). The ReadyNAS monitors and manages the UPS over the remote connection.	
SNMP UPS only	Address	Enter the IP address of the SNMP UPS.
	Community	Enter **public** or **private**, depending on the manufacturer's requirement or the UPS's configuration.
	MIB	From the drop-down list, select the MIB for one of the following manufacturers: • **MGE UPS Systems** • **American Power Conversion (APC)** • **SOCOMEC** • **Powerware** • **Eaton Powerware (Monitored)** • **Eaton Powerware (Managed)** • **Raritan** • **BayTech** • **HP/Compac AF401A** • **Cyberpower RMCARD201/RMCARD100/RMCARD202**
Remote UPS only	Address	Enter the IP address of the remote UPS.
	User	For a remote UPS that is attached to a Linux server that is running NUT, enter the user name used to access the remote UPS. For a remote UPS that is attached to a ReadyNAS, enter **monuser**. This

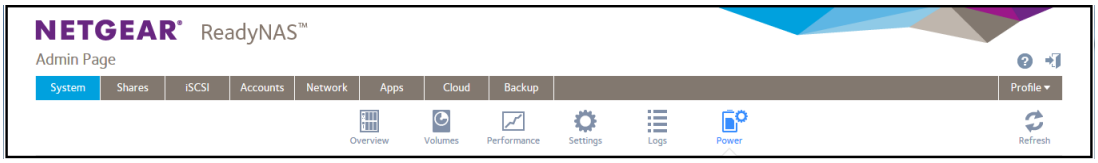
Item		Description
		user name is required for the ReadyNAS to access the remote UPS; do not enter another user name.
	Password	For a remote UPS that is attached to a Linux server that is running NUT, enter the password used to access the remote UPS. For a remote UPS that is attached to a ReadyNAS, enter **pass**. This password is required for the ReadyNAS to access the remote UPS; do not enter another password.

6. Click the **Add** button.
   The UPS is added to the UPS list.

Monitor a UPS

To monitor the status of a UPS:

1. Log in to your ReadyNAS.



2. Select **System > Power**.
   When the ReadyNAS system detects the UPS device, it displays the following information about the device in the UPS list:

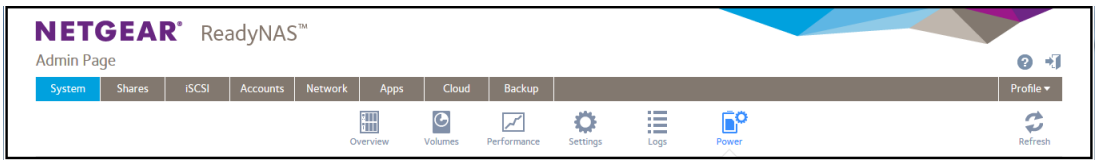
Item	Description
Status	The status of the UPS: • On line power • On battery • Low battery • On battery and Low battery • On line power and Low battery • Unknown
Name	The name of the UPS. For a remote UPS, the name is always UPS.
Description	The description that you gave the UPS.
Serial	The detected serial number of the UPS.
Model	The detected model of the UPS.
MFR	The detected manufacturer of the UPS.

Item	Description
Address	The IP address of the UPS.

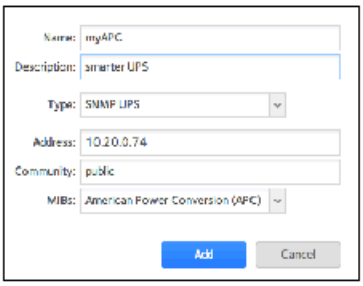
Edit a UPS

To edit a UPS in the UPS list:

1. Log in to your ReadyNAS.



2. Select **System > Power**.
3. From **UPS**, select the UPS that you want to edit.
4. Click the **gear** icon ( ) to the right of the UPS list.
5. In the UPS list, highlight the UPS that you want to modify.



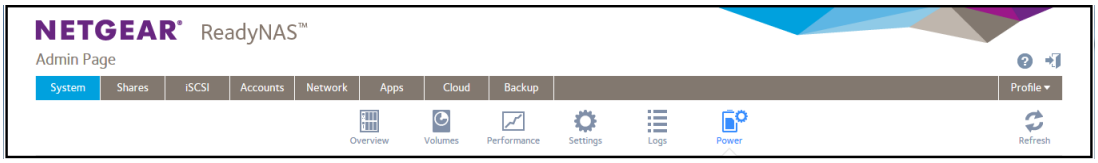
The fields on this screen depend on the type of UPS.

6. Modify the settings as required.
   You cannot change the **Type** setting.
7. Click the **Apply** button.
   Your changes are saved. The modified UPS settings are displayed in the UPS list.

Remove a UPS

To remove a UPS from the UPS list:

1. Log in to your ReadyNAS.



2. Select **System > Power**.
3. Select the UPS that you want to remove from the **UPS** list.
4. Click the **–** icon to the right of the list.
5. Confirm the removal.
   The UPS is removed from the UPS list. Your ReadyNAS system stops monitoring and managing the UPS.

Backup and Recovery

9

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. If you regularly back up your data, you can recover your data if any of these situations occur.

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. At home and in business settings, you should back up important data that might be lost due to a natural disaster or the loss of a device that stores data.

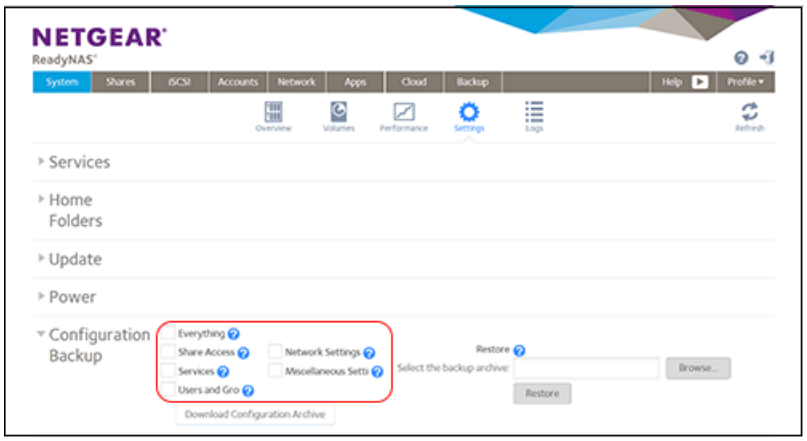
This chapter includes the following sections:

Back Up or Restore System Configuration

In addition to backing up data, you can back up and restore your system configuration settings. The backup configuration file can also save your shared folder access settings, service settings, local users and groups, network settings, and more. You cannot save iSCSI settings. You can also save up to 50 MB of data from your volumes, including the contents of your files and folders.

To back up your system configurations:

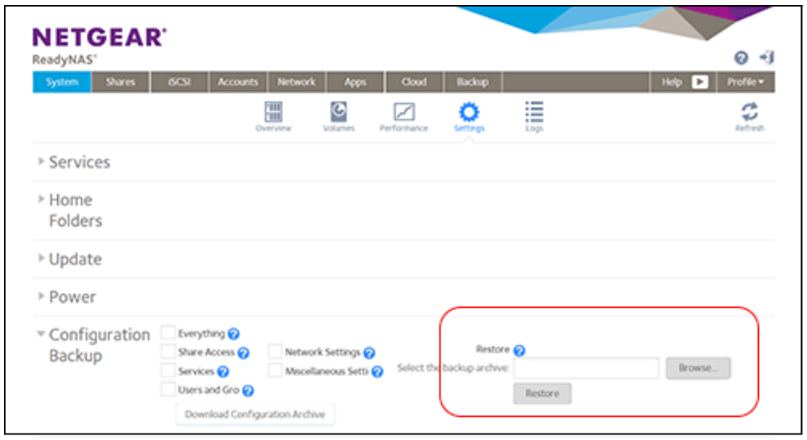
1. Select **System > Settings > Configuration Backup**.



2. Select the **Everything** check box or select the check boxes for the settings that you want to back up.
3. Click the **Download Configuration Archive** button.
   The selected system configuration settings are saved to a file that is downloaded to your computer.

To restore system configuration from a file:

1. Select **System > Settings > Configuration Backup**.



2. Click the **Browse** button to find the file containing your previously backed-up system configuration settings and select it.
3. Click the **Restore** button.

The system configuration settings are restored according to the backup file that you selected.

Basic Data Backup and Recovery Concepts

Your ReadyNAS system can manage backup and recovery for many devices on your network. For example, you can back up data that is stored on your ReadyNAS storage system to secondary devices, such as a USB drive. You can also use your ReadyNAS storage system to store backed-up data from other devices, like your laptop.

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.

A *backup source* is the place where you store the primary copy of the data that you want to back up. A backup destination is the place where you store the backed-up data.

If you store primary copies of your data on your ReadyNAS system, you can create a backup job to back up your data to a secondary device on the same network.

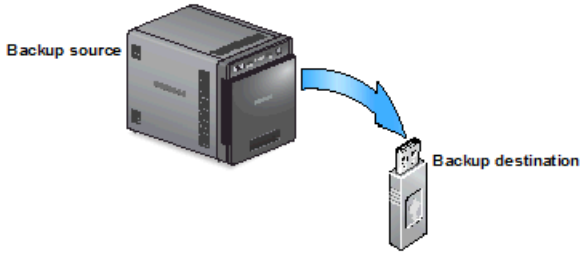


Figure 11. Backing up data from a ReadyNAS system to a secondary device (USB drive)

If you store primary copies of your data on your computer or other device, you can create a backup job to back up your data to a ReadyNAS system that is on the same network.

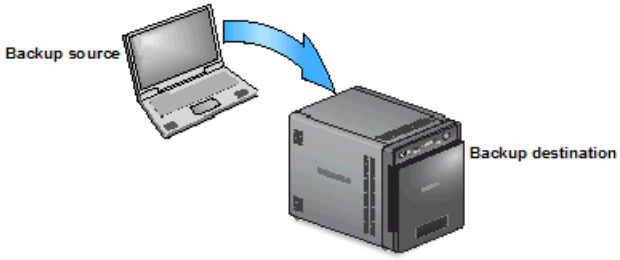


Figure 12. Backing up data from a computer to a ReadyNAS system

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 amount of time a full backup takes depends on the amount of stored data.

An incremental backup copies only the data that 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 if a disk fails. For more information about the protection that RAID configuration offers, see *RAID* on page 20.

A backup source or destination can be local (stored on the ReadyNAS) or remote (stored somewhere else). If the backup source or destination is remote, you must select the backup protocol that you want to use (see *Backup Protocols* on page 198).

Local options for backup sources and destinations are described in the following table.

Table 34. Local backup sources and destinations

Item	Description
volume: <volume name>	Source or destination is a volume on the ReadyNAS.
share: <share name>	Source or destination is a shared folder on the ReadyNAS.
All Home Shares	Source or destination is every user's home share on the ReadyNAS.
home: <home share name>	Source or destination is a user's home share on the ReadyNAS.
External Storage (<location of connection>)	Source or destination is connected a USB or eSATA port on the ReadyNAS.
Time Machine	Source or destination is the Time Machine data stored locally on the ReadyNAS.

Recovery Concepts

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

A recovery source is the place where you store the backed-up data. A recovery destination is the place to which you want to restore the backed-up data. The recovered data replaces a deleted or damaged primary copy.

If you store backed-up data on the ReadyNAS system, you can create a recovery job to restore backed-up data to your computer or other primary device.

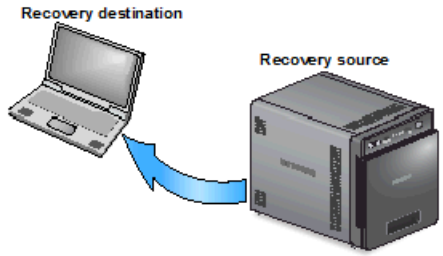


Figure 13. Recovering data from a ReadyNAS system to a laptop computer

If you store backed-up data on another device on the network, such as a USB drive, you can create a recovery job to restore backed-up data to your ReadyNAS system.

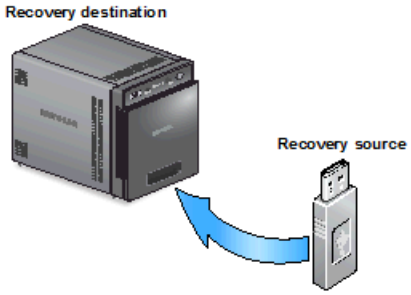


Figure 14. Restoring data from a USB drive to a ReadyNAS system

The ReadyNAS system treats recovery jobs like backup jobs. You use the Backup screen to create a recovery job. In a recovery job, you reverse the source and destination that you used when you backed up the data. The recovery source is the backup destination and the recovery destination is the backup source.

Secure Cloud Backups

A secure cloud backup lets you use online backup and recovery tools, such as ReadyNAS Vault, to save data over the Internet to a remote location and restore the data, if needed. For more information about backing up your data using ReadyNAS Vault, see *ReadyNAS Vault* on page 229.

Backup Protocols

When you back up data to a remote destination or recover it from a remote source, data is transferred over a network using file-sharing protocols.

You can select which protocol you want to use for the job. The options that are available to you depend on how your ReadyNAS system is configured. Backup protocols are described in the following table.

Table 35. Backup protocols

Item	Description
Windows/NAS (Timestamp)	Source or destination is a share on a Windows computer, or a share on another NAS. Incremental backups with this protocol use time stamps to determine whether files should be backed up.
Windows (Archive Bit)	Source is a share on a Windows computer. Incremental backups with this protocol use the archive bit of files, similar to Windows, to determine whether they should be backed up.
FTP	Source or destination is an FTP site or a path from that site.
NFS	Source or destination is on a Linux or UNIX device accessed using NFS. Mac OS X users can also use this option by setting up an NFS share from the console terminal.
Rsync server	Source or destination is accessed using an Rsync server. Rsync was originally available for Linux and other UNIX-based operating systems, but is also popular under Windows and Mac for its efficient use of incremental file transfers. Using Rsync is the preferred backup method when backing up from one ReadyNAS device to another.
Rsync over Remote SSH	Source or destination is accessed using an Rsync server. Rsync data transfers to go through a secure, encrypted SSH tunnel. NETGEAR recommends using remote SSH when backups are being transferred over the Internet.

Backup Job Recommendations

By default, all backup jobs are scheduled to run every day. You can edit these settings after you create each backup job. For more information, see *Schedule a Backup Job* on page 212.

The first few times you back up data, it is a good practice to perform the backup manually. With a manual backup, you can make sure that access is granted to the remote backup source or destination and see how long the backup takes to run. You must know how long the backup job takes so that you can allow enough time in the schedule for it to complete before you schedule the next backup. You can run a manual backup after you create each backup job. For more information, see *Manually Start a Backup or Recovery Job* on page 215.

Note: Backup and recovery jobs using Time Machine use different procedures. For more information, see *Time Machine* on page 222.

Manage Backup and Recovery Jobs

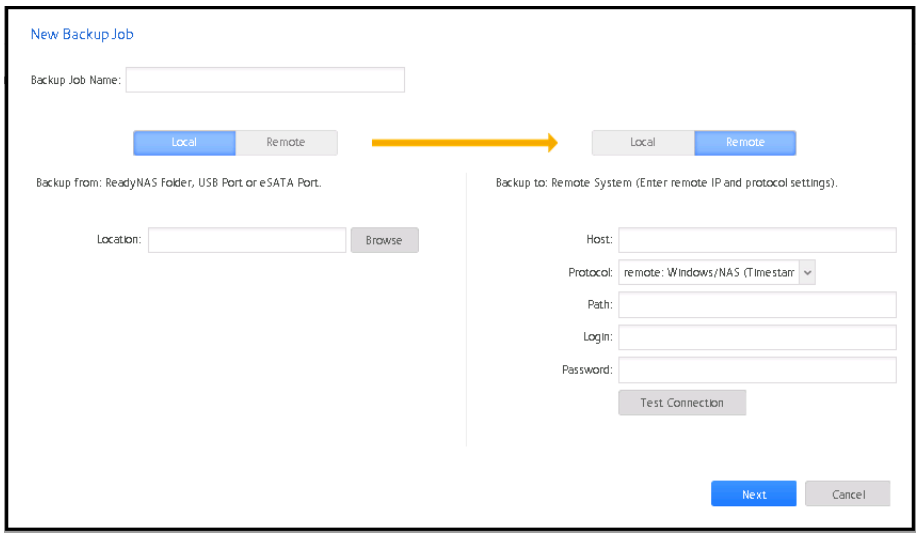
This section covers creating, configuring and deleting backup and recovery jobs. This section also covers manually starting jobs and clearing the job log.

Create a Backup Job

To create a backup job:

1. Log in to your ReadyNAS.

2. From the Admin Page, select **Backup > Backups**.
3. Click the **Add Backup** button.



4. In the **Backup Job Name** field, enter a name for the new backup job.
   The name can have a maximum of 255 characters.
5. From the pair of buttons on the right side of the window, click the **Local** button if the files you want to back up are local (on the ReadyNAS, or connected USB drive, or connected eSATA drive) or click the **Remote** button.
   The window adjusts to show the appropriate set of parameters.
6. Do one of the following:
   - If you clicked the **Local** button, click the **Browse** button and navigate to the file or folder you want to back up.
   - If you clicked the **Remote** button, enter the host name, select the backup protocol, and enter the path and, if required, the login ID and password.
     Enter the folder path according to the following:

- If you select a Windows protocol, use a forward slash (/) to separate directories, for example, enter one of the following:
  /<share name>/<folder name>
- If you select the FTP protocol and you want to specify an absolute path, start with a forward slash (/). Relative paths cannot start with a forward slash. For example:
  - *<relative path>*
  - */<absolute path>*
- If you select the NFS protocol, specify the export point followed by the path, for example:
  /<export point>/path
- If you select the Rsync server protocol, specify the module name followed by the path, for example:
  <module name>/path

WARNING:
Backing up using the Rysnc protocol is for expert users only.

- If you select the Rysnc over Remote SSH protocol, specify the relative or absolute path, for example:
  - *<relative path>*
  - */<absolute path>*

WARNING:
During backup using the Rsync over Remote SSH protocol, specifying an absolute path might overwrite existing files at that destination. Backing up using the Rsync over Remote SSH protocol is for expert users only.

- Do not use a backslash (\) in paths.

Note: If you configured a remote source, you can immediately test the connection by clicking the **Test Connection** button.

7. From the pair of buttons on the left side of the window, click the **Local** button if you want the backup stored locally (on the ReadyNAS, or connected USB drive, or connected eSATA drive) or click the **Remote** button.

Note: The source and destination of the job cannot both be remote.

The window updates to show the appropriate set of parameters.

8. Do one of the following:
   - If you clicked the **Local** button, click the **Browse** button and navigate to the destination folder.
   - If you clicked the **Remote** button, enter the host name, select the backup protocol, the path, and if required, the login ID and password. Enter the folder path according to the following:
     - If you select a Windows protocol, use a forward slash (/) to separate directories, for example, enter one of the following:
       /<share name>/<folder name>
     - If you select the FTP protocol and you want to specify an absolute path, start with a forward slash (/). A relative path cannot start with a forward slash. For example:
       - *<relative path>*
       - */<absolute path>*
     - If you select the NFS protocol, specify the export point followed by the path, for example:
       /<export point>/path
     - If you select the Rsync server protocol, specify the module name followed by the path, for example:
       <module name>/path

       WARNING:
       Backing up using the Rysnc protocol is for expert users only.

     - If you select the Rysnc over Remote SSH protocol, specify the relative or absolute path, for example:
       - *<relative path>*
       - */<absolute path>*

       WARNING:
       During backup using the Rsync over Remote SSH protocol, specifying an absolute path might overwrite existing files at that destination. Backing up using the Rsync over Remote SSH protocol is for expert users only.

     - Do not use a backslash (\) in paths.

Note: If you configured a remote destination, you can immediately test the connection by clicking the **Test Connection** button.

9. Click the **Next** button.
   The New Backup Job: Schedule window displays.
10. Adjust any of the schedule parameters as desired.

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

11. Click the **Finish** button.
    The New Backup Job: Schedule window closes and the new job is added to the **Jobs** list.

For more information about backup sources, destinations, and protocols, see *Basic Data Backup and Recovery Concepts* on page 196.

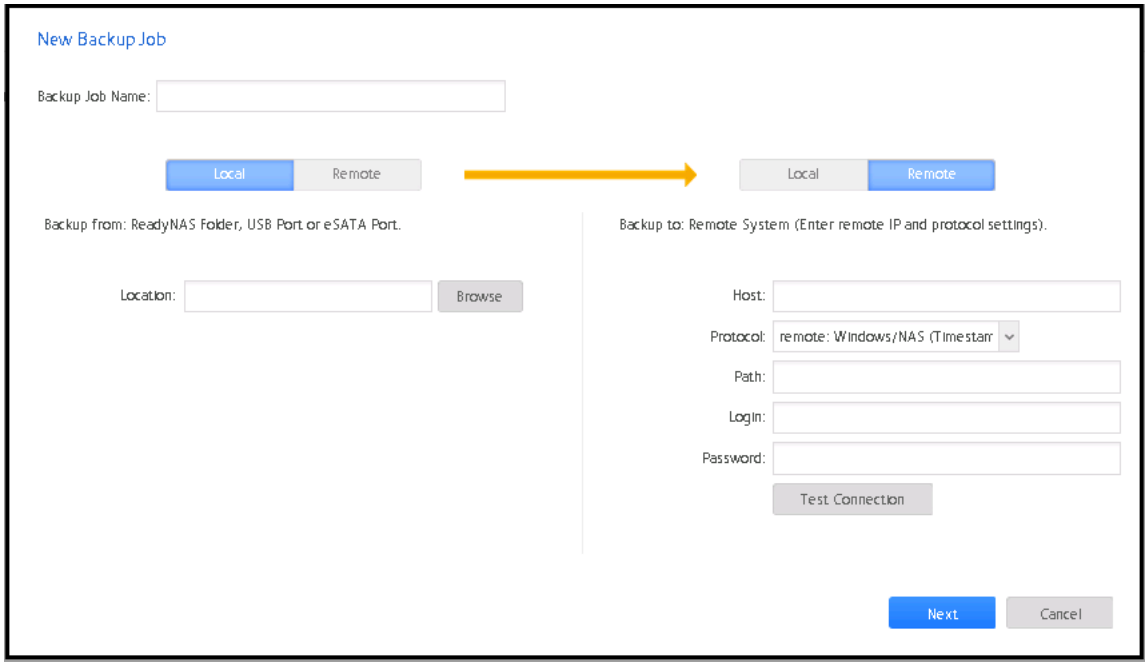
Create a Recovery Job

The ReadyNAS system treats recovery jobs like backup jobs. You use the Backup screen to create a recovery job. In a recovery job, you reverse the source and destination that you used when you backed up the data. The recovery source is the backup destination and the recovery destination is the backup source.

To create a recovery job:

1. **Log in to your ReadyNAS.**

2. **From the Admin Page, select Backup > Backups.**
3. **Click the Add Backup button.**



4. **In the Backup Job Name field, enter a name for the new backup job.**

The name can have a maximum of 255 characters.

5. From the pair of buttons on the right side of the window, click the Local button if the files you want to recover are local (on the ReadyNAS, or connected USB drive, or connected eSATA drive) or click the Remote button.
   The window adjusts to show the appropriate set of parameters.
6. Do one of the following:
   - If you clicked the Local button, click the Browse button and navigate to the file or folder you want to recover from the backup.
   - If you clicked the Remote button, enter the host name, select the backup protocol, the path, and if required the login ID and password.
     Enter the folder path according to the following:
     - If you select a Windows protocol, use a forward slash (/) to separate directories, for example, enter one of the following:
       /<share name>/<folder name>
     - If you select the FTP protocol and you want to specify an absolute path, start with a forward slash (/). A relative path cannot start with a forward slash. For example:
       - *<relative path>*
       - */<absolute path>*
     - If you select the NFS protocol, specify the export point followed by the path, for example:
       /<export point>/path
     - If you select the Rsync server protocol, specify the module name followed by the path, for example:
       <module name>/path

       WARNING:
       Backing up using the Rysnc protocol is for expert users only.

     - If you select the Rysnc over Remote SSH protocol, specify the relative or absolute path, for example:
       - *<relative path>*
       - */<absolute path>*

       WARNING:

During backup using the Rsync over Remote SSH protocol, specifying an absolute path might overwrite existing files at that destination. Backing up using the Rsync over Remote SSH protocol is for expert users only.

- Do not use a backslash (\) in paths.

Note: If you configured a remote source, you can immediately test the connection by selecting the Test Connection button.

7. From the pair of buttons on the left side of the window, click the Local button if you want the backup stored locally (on the ReadyNAS, or connected USB drive, or connected eSATA drive) or click the Remote button.

Note: The source and destination of the job cannot both be remote.

The window adjusts to show the appropriate set of parameters.

8. Do one of the following:
   - If you clicked the Local button, click the Browse button and navigate to the destination folder.
   - If you clicked the Remote button, enter the host name, select the backup protocol, the path, and if required the login ID and password.
     Enter the folder path according to the following:
     - If you select a Windows protocol, use a forward slash (/) to separate directories, for example, enter one of the following:
       /<share name>/<folder name>
     - If you select the FTP protocol and you want to specify an absolute path, start with a forward slash (/). A relative path cannot start with a forward slash. For example:
       - *<relative path>*
       - */<absolute path>*
     - If you select the NFS protocol, specify the export point followed by the path, for example:
       /<export point>/path
     - If you select the Rsync server protocol, specify the module name followed by the path, for example:
       <module name>/path

WARNING:

Backing up using the Rysnc protocol is for expert users only.

- **If you select the Rysnc over Remote SSH protocol, specify the relative or absolute path, for example:**
  - ***<relative path>***
  - ***/<absolute path>***

WARNING:
During backup using the Rsync over Remote SSH protocol, specifying an absolute path might overwrite existing files at that destination. Backing up using the Rsync over Remote SSH protocol is for expert users only.

- **Do not use a backslash (\) in paths.**

Note: **If you configured a remote destination, you can immediately test the connection by clicking the Test Connection button.**

9. **Click the Next button.**
   The New Backup Job: Schedule window displays.
10. **Clear the Enabled 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 schedule a recovery job to run automatically.

Note: **Because you cleared the Enable check box, you must manually start the recovery job. For information about manually starting a job, see *Manually Start a Backup or Recovery Job* on page 215.**

Select the Finish button.
The New Backup Job: Schedule window closes and the recovery job is added to the Jobs list.

For information about recovery sources, destinations, and protocols, see *Basic Data Backup and Recovery Concepts* on page 196.

Modify a Backup or Recovery Job

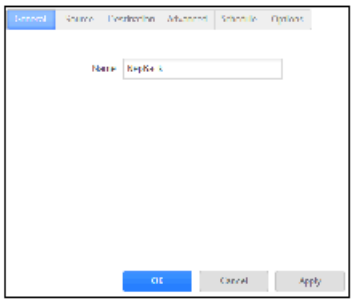
After you create a backup or recovery job, you can change the job name, source and destination, schedule, and other options.

Change the Name of a Job

To change the name of a backup or recovery job:

1. Log in to your ReadyNAS.
2. Select **Backup > Backups > Jobs**.

3. Select the backup or recovery job from the jobs list.
4. Select **Settings**.

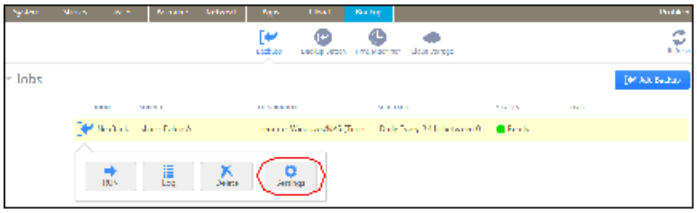


5. In the **General** tab, enter a new job name.
6. Click the **Apply** button.
   Your changes are saved.
7. Click the **OK** button.
   The pop-up screen closes.

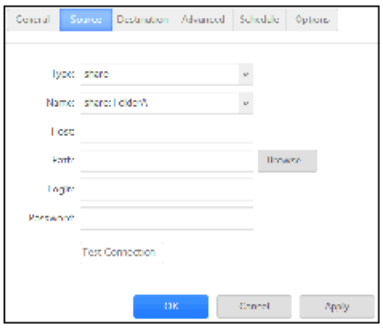
Configure a Local Job Source or Destination

To configure a local job source or destination:

1. Log in to your ReadyNAS.
2. Select **Backup > Backups > Jobs**.



3. Select the backup or recovery job from the jobs list.
4. Select **Settings**.



5. Click the **Source** or **Destination** tab.
6. From the **Type** drop-down list, select one of the options described in the following table.

Item	Description
share	The source or destination is a shared folder on the ReadyNAS.
home	The source or destination is a home share on the ReadyNAS.
volume	The source or destination is a volume on the ReadyNAS.
usb	The source or destination is an external storage device that is connected locally to the ReadyNAS.
timemachine	The source or destination is the Time Machine data stored locally on the Ready-NAS.

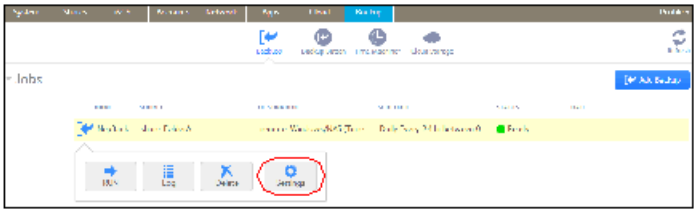
7. From the **Name** drop-down list, select the share, home share, volume, or external storage connection that you want to use.
   If you selected **timemachine**, the **Name** field is automatically populated.
8. (Optional) Enter the path to the folder that you want the job to target or click the **Browse** button to locate it.
   If you select an external storage device that is connected to your ReadyNAS system, you can leave the path blank to back up or recover the data at the top level of the USB device's directory.
9. If necessary, enter the login credentials required to access the source or destination.
10. Click the **Apply** button.
    Your changes are saved.
11. Click the **OK** button.

The pop-up screen closes.

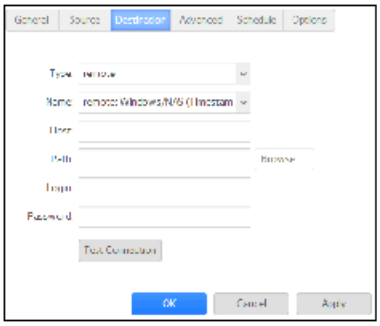
Configure a Remote Job Source or Destination

To configure a remote source or destination for a job:

1. Log in to your ReadyNAS.
2. Select **Backup > Backups > Jobs**.
3. Select the backup or recovery job from the jobs list.



4. Select **Settings**.



5. Click the **Source** or **Destination** tab.
6. From the **Type** drop-down list, select **remote**.
7. Select the protocol that you want to use.

Item	Description
Windows/NAS (Times-tamp)	Source or destination is a share on a Windows computer. Incremental backups with this protocol use time stamps to determine whether files will be backed up.
Windows (Archive Bit)	Source or destination is a share on a Windows computer. Incremental backups with this protocol use the archive bit of files, similar to Windows, to determine whether they will be backed up.
FTP	Source or destination is an FTP site or a path from that site.
NFS	Source or destination is on a Linux or UNIX device accessed using NFS. Mac OS X users can also use this option by setting up an NFS share from the console terminal.

Item	Description
Rsync server	Source or destination is accessed using an Rsync server. Rsync was originally available for Linux and other UNIX-based operating systems, but is also popular under Windows and Mac for its efficient use of incremental file transfers. Using Rsync is the preferred backup method when you are backing up from one ReadyNAS device to another.
Rsync over Remote SSH	Source or destination is accessed using an Rsync server. Rsync data transfers to go through a secure, encrypted SSH tunnel. NETGEAR recommends using remote SSH when backups are being transferred over the Internet.

8. In the **Host** field, enter the remote host name.
9. In the **Path** field, enter the folder path according to the following:
   - If you select a Windows protocol, use a forward slash (/) to separate directories, for example: */<share name>/<folder name>*
   - If you select the FTP protocol and you want to specify an absolute path, start with a forward slash (/). A relative path cannot start with a forward slash. For example:
     - *<relative path>*
     - */<absolute path>*
   - If you select the NFS protocol, specify the export point followed by the path, for example: */<export point>/path*
   - If you select the Rsync server protocol, specify the module name followed by the path, for example: *<module name>/path*

     WARNING:
     Backing up using the Rysnc protocol is for expert users only.

   - If you select the Rysnc over Remote SSH protocol, specify the relative or absolute path, for example:
     - *<relative path>*
     - */<absolute path>*

     WARNING:

During backup using the Rsync over Remote SSH protocol, specifying an absolute path might overwrite existing files at that destination. Backing up using the Rsync over Remote SSH protocol is for expert users only.

- Do not use a backslash (\) in paths.

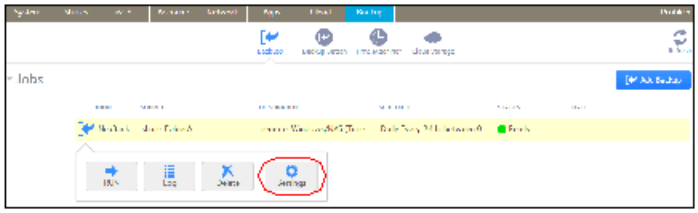
10. If necessary, enter the login credentials required to access the source or destination.
11. To determine if your ReadyNAS system can access the remote destination, click the **Test Connection** button.
12. Click the **Apply** button.
    Your changes are saved.
13. Click the **OK** button.
    The pop-up screen closes.

Configure Advanced Rsync Job Settings

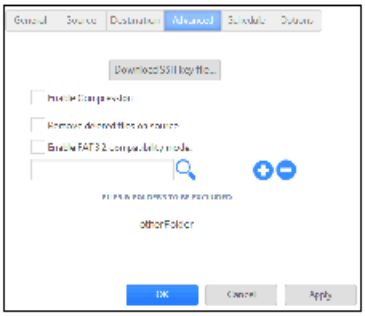
You can configure advanced settings for jobs that use Rsync or Rsync over SSH.

To configure Rsync job settings:

1. Log in to your ReadyNAS.
2. Select **Backup > Backups > Jobs**.
3. Select the backup or recovery job from the jobs list.



4. Select **Settings**.



5. Click the **Advanced** tab.
6. Configure the settings as described in the following table.

Item	Description
Download SSH Key file	If you are using Rsync over SSH, click this button to download the public SSH file key. Add the key to the authorized SSH key list of the remote Rsync server.
Enable Compression	Compresses data before transferring. This option is especially useful for slower network connections, such as when you are transferring data over a WAN.
Remove deleted files on source	If this check box is selected, the job is differential: New and modified files are copied to the destination. If a file is deleted from the source, the corresponding file on the destination is deleted. If this check box is cleared, the job is incremental: New and modified files are copied to the destination. If a file is deleted from the source, the corresponding file remains on the destination and is not deleted.
Enable FAT32 compatibility mode	If this check box is selected, Rsync does not copy file permissions, allowing you to back up your data to a FAT32 file system.

7. (Optional) Specify files and folders that you do not want to copy to the destination:
   - To add a new file or folder to the list, click the **+** button ( ).
   - To remove a file or folder from the list, select it and click the **–** button ( ).
   - To search for a file or folder in the list, type the name of the file or folder in the search field next to the search icon ( ).
8. Click the **Apply** button.
   Your changes are saved.
9. Click the **OK** button.
   The pop-up screen closes.

Schedule a Backup Job

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

WARNING:
To ensure the integrity of the data stored on your primary device, never schedule a recovery job to run automatically.

To schedule a backup job:

1. Log in to your ReadyNAS.
2. Select **Backup > Backups > Jobs**.
3. Select the backup or recovery job from the jobs list.

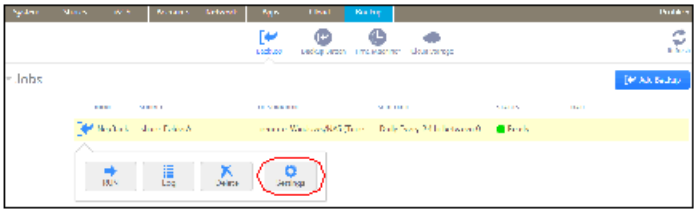
4. Select **Settings**.
5. Click the **Schedule** tab.

6. Select the **Enabled** check box.
7. Specify a schedule for the job using the drop-down lists and check boxes.
8. Click the **Apply** button.
   Your changes are saved.
9. Click the **OK** button.
   The pop-up screen closes.

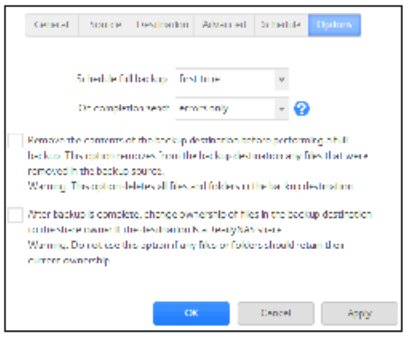
Configure the Job Options

To configure the options for a backup or recovery job:

1. Log in to your ReadyNAS.
2. Select **Backup > Backups > Jobs**.
3. Select the backup or recovery job from the jobs list.



4. Select **Settings**.



5. Click the **Options** tab.
6. Configure the options as described in the following table.

Item	Description
Schedule full backup	From the drop-down list, specify how often to run a full backup. The first full backup is performed at the next scheduled occurrence of the backup depending on the schedule that you specify. The next full backup is performed after the interval that you specify, calculated from this first backup. Incremental backups are performed between the full backup cycles.
On completion send	Select what type of logs to send when the backup job finishes. You can send a log that lists only errors during backup, 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 *System Logs* on page 176.
Remove the contents of the backup destination...	Selecting this check box erases the destination path contents before the backup is performed. NETGEAR recommends that you do not select this check box for recovery jobs. **Note:** When using this option, ensure that you correctly identify your backup source and backup destination. If you reverse them, you might permanently delete your files. NETGEAR recom-

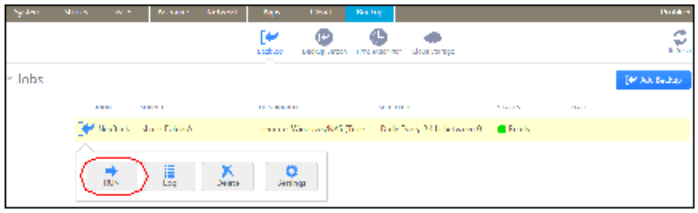
Item	Description
	mends that you do not enable this option unless your destination device is very low on storage space. NETGEAR recommends you experiment with this option using a test share to make sure that you understand how it works.
After backup is complete, change ownership of the files...	Your ReadyNAS system attempts to maintain original file ownership whenever possible. Selecting this check box automatically changes the ownership of the backed-up files to match the ownership of a shared folder destination.

7. Click the **Apply** button.
   Your changes are saved.
8. Click the **OK** button.
   The pop-up screen closes.

Manually Start a Backup or Recovery Job

To manually start a backup or recovery job:

1. Log in to your ReadyNAS.
2. Select **Backup > Backups > Jobs**.
3. Select the backup or recovery job from the jobs list.

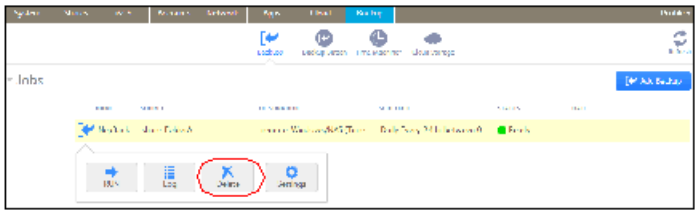


4. Select **Start**.
   The job starts. You can view its progress in the Status column of the jobs list.

Delete a Backup or Recovery Job

To delete a backup or recovery job:

1. Log in to your ReadyNAS.
2. Select **Backup > Backups > Jobs**.
3. Select the backup or recovery job from the jobs list.

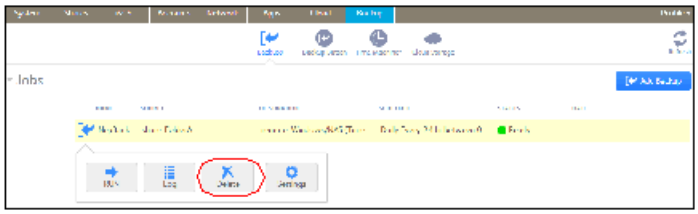


4. Select **Delete**.
5. Confirm the deletion.

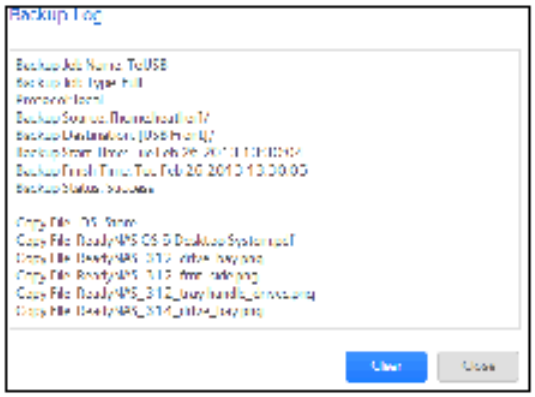
View or Clear a Job Log

To view a backup or recovery job log:

1. Log in to your ReadyNAS.
2. Select **Backup > Backups > Jobs**.
3. Select the backup or recovery job from the jobs list.



4. Select **Log**.



5. To clear the job log, click the **Clear** button.

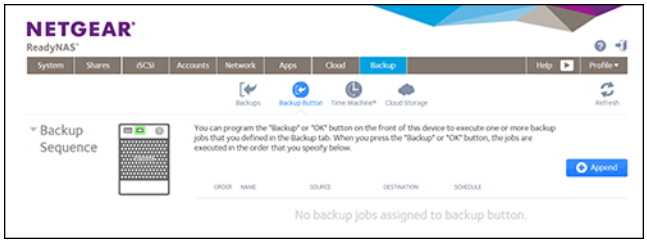
Configure the Backup Button

You can configure the **Backup** button (or the **OK** button on models with **OK** buttons) on your ReadyNAS storage system to execute one or more backup jobs that you previously created. When you click the button, the jobs are executed in the order that you specified in the backup schedule.

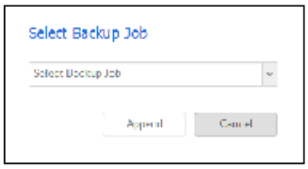
If no jobs are scheduled for the button, pressing the button does nothing.

To add a job to the Backup button sequence:

1. Log in to your ReadyNAS.
2. Select **Backup > Backup Button > Backup Sequence**.



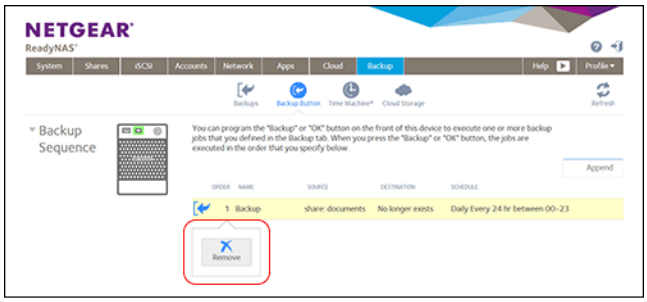
3. Click the **Append** button.



4. Select a backup job from the drop-down list.
5. Click the **Append** button.
   The job appears in the backup button list.

To remove a job from the Backup button sequence:

1. Log in to your ReadyNAS.
2. Select **Backup > Backup Button > Backup Sequence**.
3. Select the job that you want to remove from the **Backup** button sequence.



4. From the pop-up menu that displays, select the **Remove** button.
5. Confirm the removal.

The job is removed from the backup button list.

Back Up Windows Computers and Mac Computers to ReadyNAS

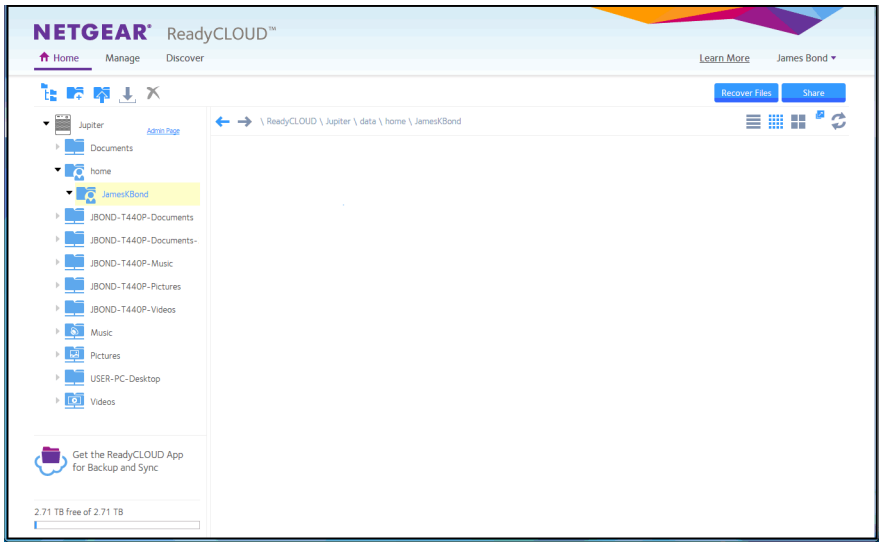
You can automatically back up files from Windows computers and Mac computers over a network to your ReadyNAS by using the ReadyCLOUD desktop app on your computer. The ReadyCLOUD app connects your computer to the ReadyNAS. No data is stored in the cloud. All data is stored on the ReadyNAS.

This procedure requires that you created a ReadyCLOUD account and linked your ReadyNAS to it.

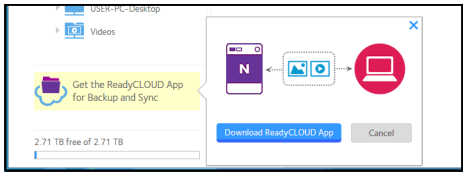
After you install the ReadyCLOUD app on your computer and choose which directories are backed up, the ReadyCLOUD app backs up the files in those directories to the ReadyNAS. The backup copies are kept synched to the copies on the computer.

To create a synched backup of your computer on your ReadyNAS:

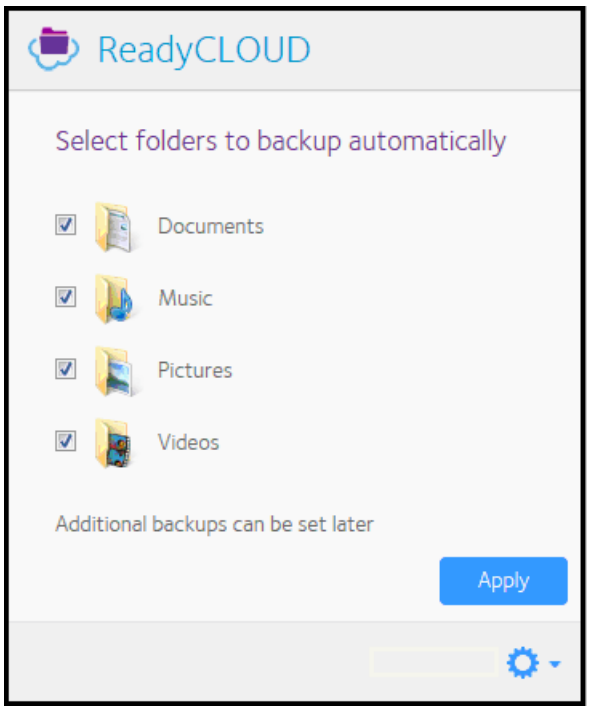
1. Sign in to your ReadyCLOUD account.



2. Double-click the **Get the ReadyCLOUD App for Backup and Sync** icon.



3. Select the **Download ReadyCLOUD App** button.
   Your browser download wizard opens.
4. Download and run the ReadyCLOUD installation app.
   The ReadyCLOUD app window opens. The app opens a virtual private network (VPN) connection directly between your computer and your ReadyNAS. After what might be a few minutes, the app window lists directories commonly chosen to be backed up.



5. If desired, unselect any or all of the default folders.
   After this initial configuration, you can add other folders to the backup.
6. Select the **Apply** button to confirm your selections.
   The selected files and folders are backed up to your ReadyNAS. When files change on the computer, the ReadyCLOUD app synchs the changes to your ReadyNAS.

Note: From ReadyCLOUD, you can invite additional users to read and change these files.

File Synchronization Across Computers

You can keep files synchronized across multiple Windows computers and Mac computers over a network using the ReadyCLOUD desktop app on the computers and your ReadyNAS.

As with services such as Dropbox, synchronized copies of files can reside on multiple Windows computers and Mac computers and on your ReadyNAS. As is not the case with such services, your data is not stored in the cloud. Because the data is stored on your ReadyNAS, you can store as much data as will fit in the space on your computers and ReadyNAS.

You can extend and revoke access permission to other users with ReadyCLOUD accounts. On your ReadyNAS, select **Cloud > ReadyCLOUD > Users** to invite and manage user access, or visit the Manage window of the ReadyCLOUD website.

Work on Files Across Windows Computers and Mac Computers Using ReadyNAS

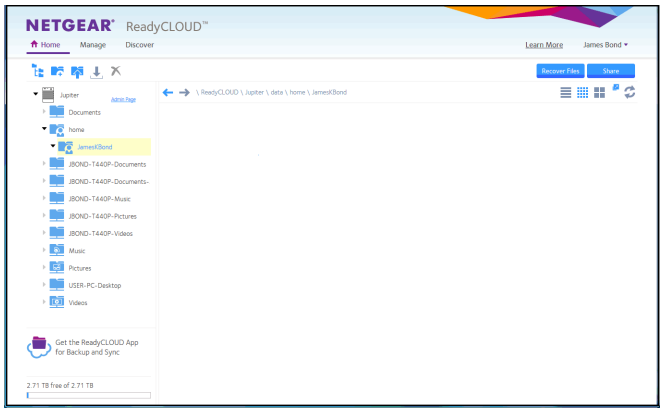
You can share files with Windows computers and Mac computers over a network using your ReadyNAS and the ReadyCLOUD app on the computers. The ReadyNAS and the ReadyCLOUD app keep the local copies in synch. No information is stored in the cloud.

This procedure requires that you created a ReadyCLOUD account and linked your ReadyNAS to it.

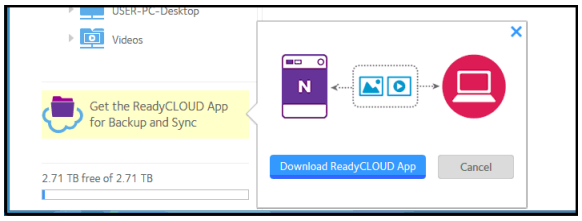
You first install the ReadyCLOUD app on your computer and choose which directories are backed up to the ReadyNAS, and then on the ReadyNAS you invite other ReadyCLOUD users to share files you select.

To create a synched backup of your computer on your ReadyNAS:

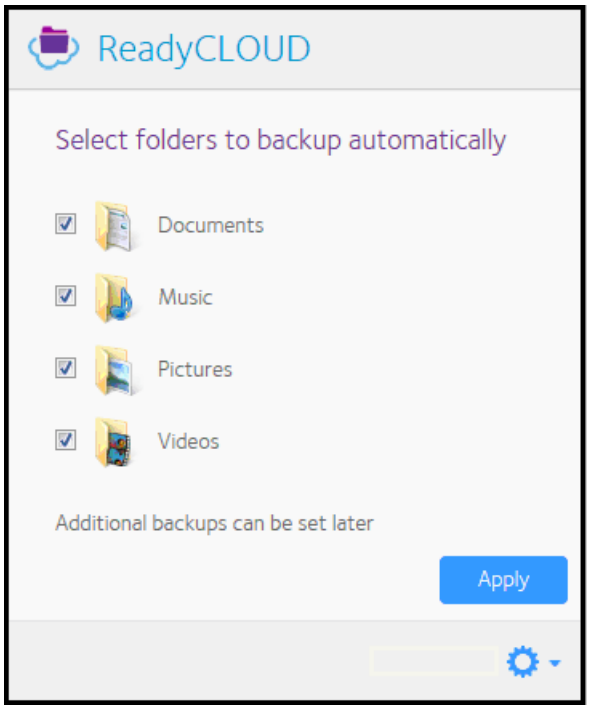
1. Sign in to your ReadyCLOUD account.



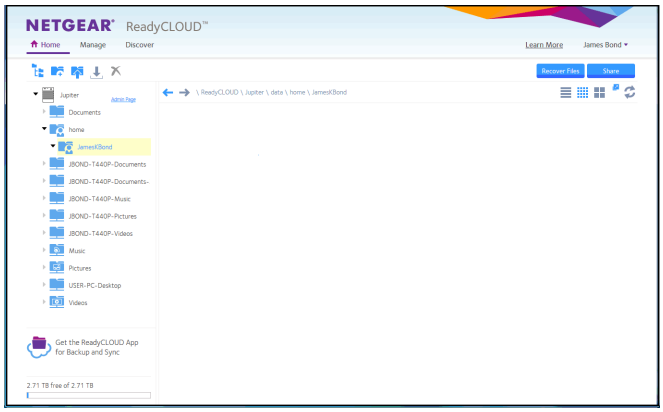
2. Double-click the **Get the ReadyCLOUD App for Backup and Sync** icon.



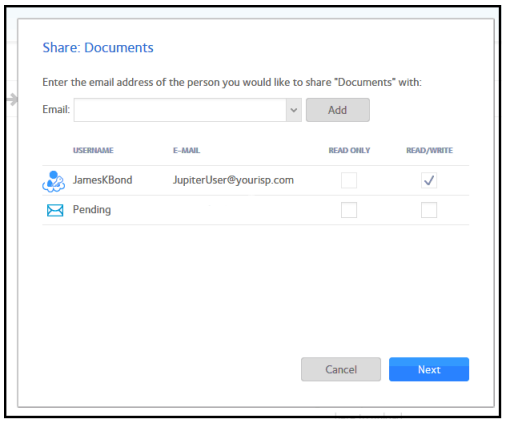
3. Select the **Download ReadyCLOUD App** button.
   Your browser download wizard opens.
4. Down-load and run the ReadyCLOUD installation app.
   The ReadyCLOUD app window opens. The app opens a virtual private network (VPN) connection directly between your computer and your ReadyNAS. After what might be a few minutes, the app window lists directories commonly chosen to be backed up.



5. If desired, unselect any or all of the default folders.
   After this initial configuration, you can add other folders to the backup.
6. Select the **Apply** button to confirm your selections.
   The selected files and folders are backed up to your ReadyNAS. When files change on the computer, the ReadyCLOUD app synchs the changes to your ReadyNAS.
7. Log in to the ReadyCLOUD website.

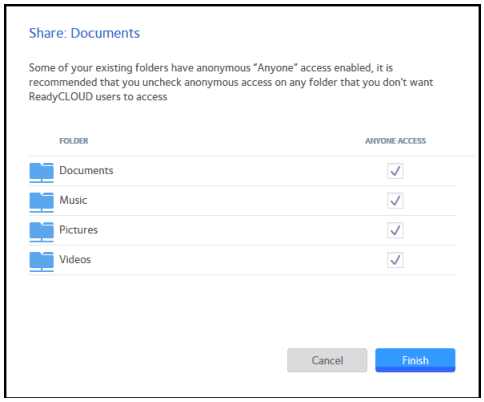


8. Select the folder to share.
9. Click the **Share** button.



10. Enter the email address of the person with whom you want to share the files and select the **Add** button.
    The email address is added to the list of users with the label Pending.
11. Select the **READ ONLY** check box or the **READ/WRITE** check box, and select the **Next** button.

    If access is set to anonymous for any of the folders on the ReadyNAS, you can change that before proceeding.



12. Select the **Finish** button.
    ReadyNAS Remote (email address remoteadmin@netgear.com) sends email to the pending users with a subject line similar to "Invitation to ReadyCLOUD **Please do not reply**."

The invited users click the link in the email to visit ReadyCLOUD and create ReadyCLOUD accounts. After creating accounts, the users download and configure the ReadyCLOUD app.

Time Machine

You can use Mac OS X Time Machine and your ReadyNAS storage system to back up and retrieve data for your Mac computer. This combines the ease of a native Mac backup with the space and reliability of your ReadyNAS.

Starting in ReadyNAS OS 6.2, in addition to a shared Time Machine that can be used by any Mac account, you can also configure individual accounts to have their own private Time Machines. An account can use the shared Time Machine or its private Time Machine, but not both. A shared Time Machine and private Time Machines can exist on the same ReadyNAS.

When configuring a shared Time Machine, you set up a specific user name and password. All users of the shared Time Machine use this user name and password when connecting from Time Machine on the Mac. All users of the shared Time Machine have equal access to all data in the shared Time Machine.

An account using a private Time Machine must exist on the ReadyNAS. You can configure an existing ReadyNAS account to use a private Time Machine, or add the account directly in the Private Time Machine section of the Time Machine window (**Backup > Time Machine**). The space for a private Time Machine is part of the account's home folder and is invisible to other users of the ReadyNAS.

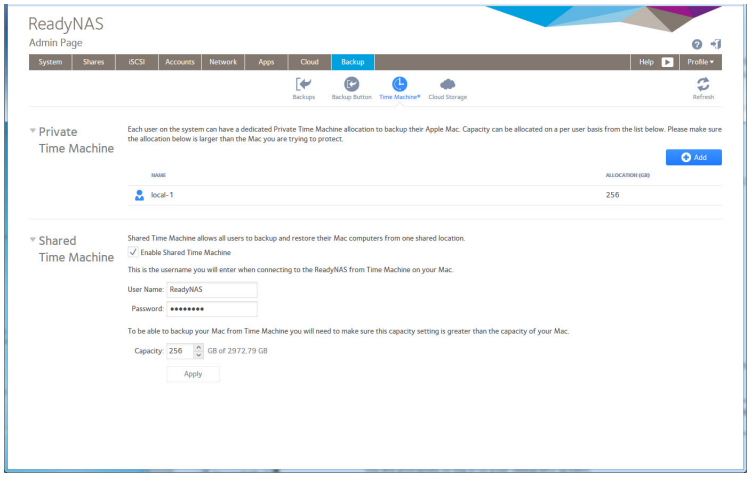
Back Up Your Mac Using a Shared Time Machine

You can use your ReadyNAS as the disk for Time Machine backups. ReadyNAS OS supports two different types of Time Machine targets, a single Time Machine shared by several users, and Time Machines private to an individual user. Use this procedure for a shared Time Machine.

Before performing these steps, verify that the AFP protocol is enabled on your ReadyNAS. Note that it is enabled by default.

To back up data on your Mac to your ReadyNAS system using Time Machine:

1. Log in to your ReadyNAS.
2. On the local admin page for your ReadyNAS, select **Backup > Time Machine**.



3. If the **Enable Shared Time Machine** checkbox is not already selected, select it.
4. Change the default user name and password.
   The default user name is ReadyNAS and the default password is the login password for the ReadyNAS. You use these credentials later when connecting to the ReadyNAS from the Mac.
5. In the **Capacity** field, enter the maximum amount of space on your ReadyNAS storage system that you want to devote to Time Machine backups.

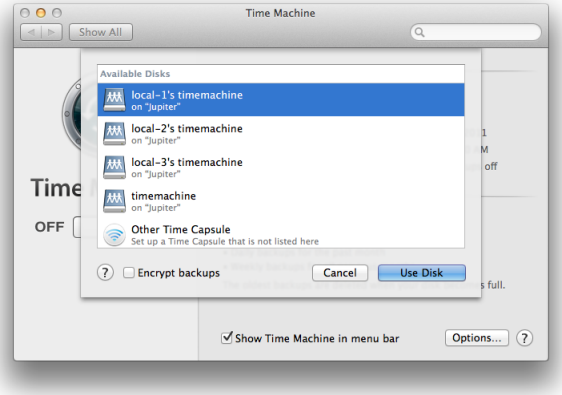
Note: The first time you run Time Machine on your Mac, a sparse bundle is created on your ReadyNAS to store the backup data. The maximum size of the sparse bundle

is the size that you specify in the **Capacity** field. Make sure that you allocate more space than is needed so that the sparse bundle can accommodate additional data later.

If you want to increase the size of the sparse bundle, you must delete the sparse bundle and create a new Time Machine backup. (See *Increase Your Time Machine Backup Capacity* on page 227.) After you run Time Machine for the first time, simply changing the number in the **Capacity** field does not increase the size of the sparse bundle.

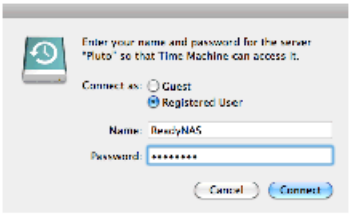
6. Click the **Apply** button.
   Your settings are saved.
7. On your Mac OS X computer, launch Time Machine.

8. Click the **Add or Remove Backup Disk** button.
   A pop-up window lists available disks, including your ReadyNAS system.



9. Select the disk named **timemachine** and click the **Use Disk** button.

(The other disks are possible private Time Machine disks.)



10. In the **Name** and **Password** fields, enter **ReadyNAS** or the shared Time Machine user and password you created in step *4* on page 223.
11. Click the **Connect** button.
    Time Machine begins the backup, which can take several minutes to start.

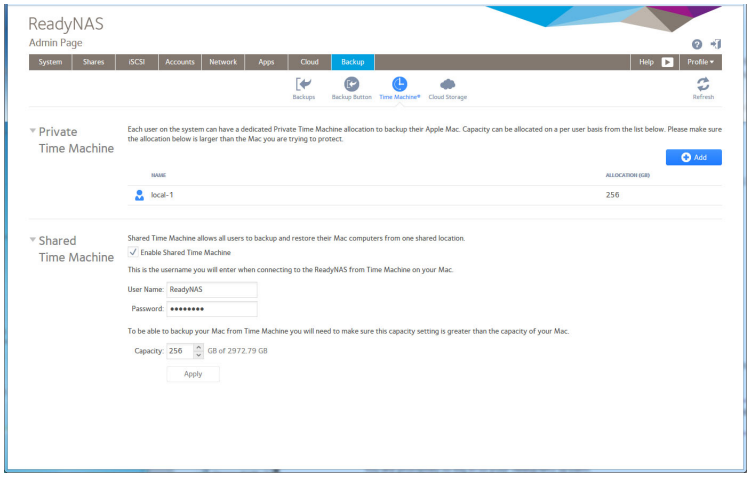
Back Up Your Mac Using a Private Time Machine

You can use your ReadyNAS as the disk for Time Machine backups. ReadyNAS OS supports two different types of Time Machine targets, a single Time Machine shared by several users, and Time Machines private to individual users. Use this procedure for a Private Time Machine.

Before performing these steps, verify the AFP protocol is enabled on your ReadyNAS. Note that it is enabled by default.

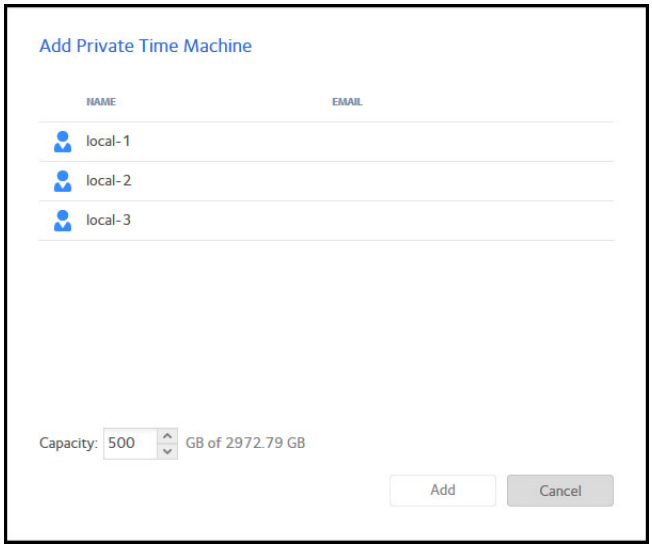
To back up your Mac:

1. Log in to your ReadyNAS.
2. On the local admin page for your ReadyNAS, select **Backup > Time Machine**.



User accounts already configured for a private Time Machine display here.

3. Click the add (**+**) button.



4. Select the user name, adjust the capacity as necessary, and click the **Add** button.

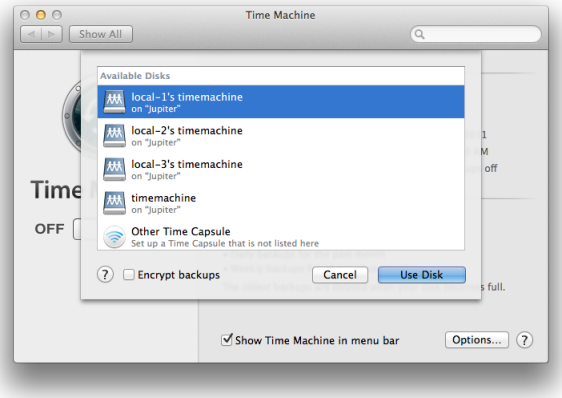
   The necessary reserved capacity depends on how the Time Machine is used, but typically it is greater than the capacity of the Mac to allow for a complete backup plus changes.

   Note: The first time you run Time Machine on your Mac, a sparse bundle is created on your ReadyNAS to store the backup data. The maximum size of the sparse bundle is the size that you specify in the **Capacity** field. Make sure that you allocate more space than is needed so that the sparse bundle can accommodate additional data later.

   If you want to increase the size of the sparse bundle, you must delete the sparse bundle and create a new Time Machine backup. (See *Increase Your Time Machine Backup Capacity* on page 227.) After you run Time Machine for the first time, simply changing the number in the **Capacity** field does not increase the size of the sparse bundle.

5. On your Mac OS X computer, open the Time Machine preferences.

6. Click the **Add or Remove Backup Disk** button.
   A pop-up window lists available disks.



7. Select the disk named *user name* **timemachine** and click the **Use Disk** button.

   The connect window opens requesting the user name and password.
8. In the **Name** field, enter the user name.
9. In the **Password** field, enter the password for that account.
10. Click the **Connect** button.

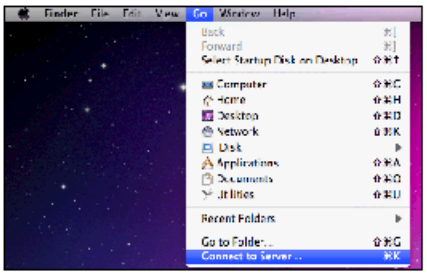
Increase Your Time Machine Backup Capacity

The first time you run a Time Machine backup on your Mac, a sparse bundle is created on your ReadyNAS to store the backup data. The maximum size of the sparse bundle is the size that you specify when you enable Time Machine on your ReadyNAS. (See *Back Up Your Mac Using Time Machine* on page 223.)

After you run Time Machine for the first time, the size of the sparse bundle that stores your Mac backup data is fixed. If you want to increase the size of the sparse bundle, you must delete the sparse bundle and create a new Time Machine backup.

To increase the capacity of the Time Machine backup on your ReadyNAS:

1. Ensure that the AFP file-sharing protocol is enabled on your ReadyNAS system.
   For more information, see *Configure Global Settings for File-Sharing Protocols* on page 159.
2. In Finder, select **Go > Connect to Server**.

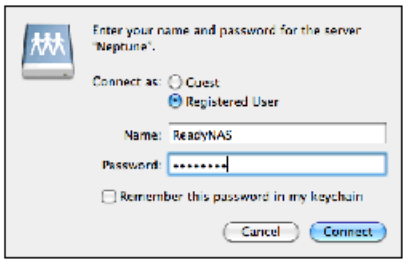


   The Connect to Server dialog box displays.
3. Enter the following command in the **Server Address** field:
   afp://<hostname>

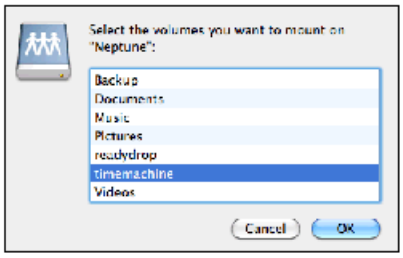
   <hostname> is the name that you assigned to your ReadyNAS system or the default host name if you did not change it.

> **Note:** If you cannot access the ReadyNAS using its host name, try entering **afp://***<ReadyNAS IP address>* instead. *<ReadyNAS IP address>* is the IP address of the ReadyNAS.

4. Click the **Connect** button.
   You are prompted to log in to your ReadyNAS system.
5. In the **Name** field, enter **ReadyNAS**.
6. In the **Password** field, enter the password that you created when you enabled Time Machine on your ReadyNAS.
7. Click the **Connect** button.



   You are prompted to select a volume. Mac OS X calls your ReadyNAS shared folders volumes.



8. Select **timemachine** and click the **OK** button.
   Finder displays the volume contents.

WARNING:
Deleting the sparse bundle deletes all Time Machine backup data stored on your ReadyNAS.

9. Delete the sparse bundle file ending in .sparsebundle.
10. Create a new Time Machine backup and specify a larger capacity.
    See *Back Up Your Mac Using Time Machine* on page 223.

ReadyNAS Vault

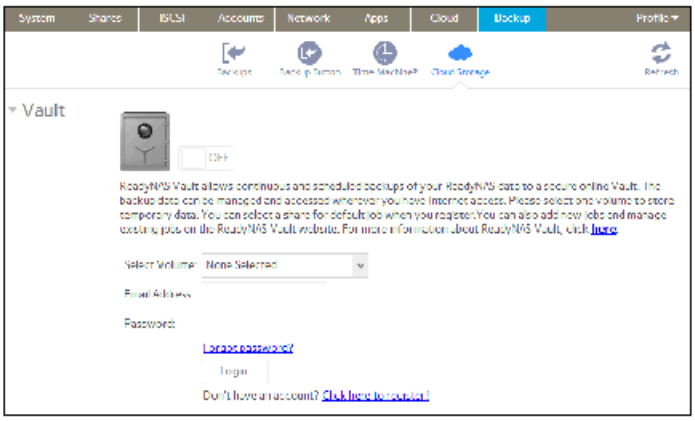
With ReadyNAS Vault, your ReadyNAS data can be backed up securely to a remote secure data center. Your data is encrypted before it is sent over the Internet. Backup administration is over a 128-bit SSL connection, the same method that banks and financial institutions use.

The following figure illustrates two concepts: backing up data from a ReadyNAS system to the cloud and restoring backed-up data to a ReadyNAS system from the cloud.

Figure 15. Using a ReadyNAS system to back up and recover data stored on a cloud

To set up ReadyNAS Vault on your system:

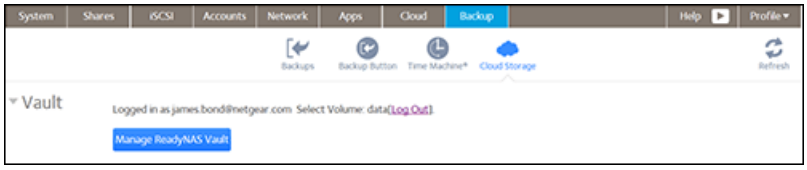
1. Log in to your ReadyNAS.
2. Select **Backup > Cloud Storage > Vault**.



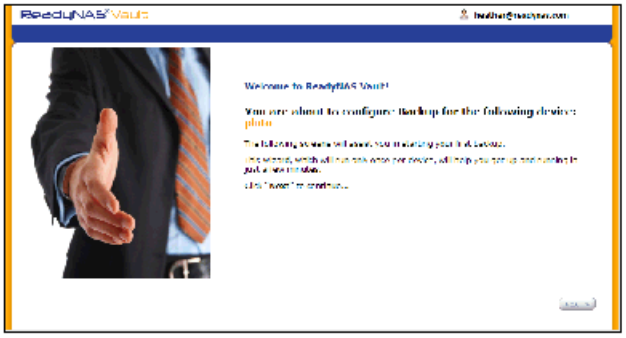
3. From the **Select Volume** drop-down list, select a volume where temporary data from ReadyNAS Vault can be stored.
4. Set the **On-Off** slider so that the slider shows the **On** position.
5. Enter your ReadyNAS Vault account credentials and click the **Login** button.

Note: If you do not have an account yet, click the **Click here to register** link to set one up. You can use the same ReadyNAS Vault account for all of your ReadyNAS systems.

The screen adjusts to display new options.



6. Click the **Manage ReadyNAS Vault** button.
A setup wizard launches in a new browser window to help you configure ReadyNAS Vault backups for your ReadyNAS system.



Note: After initial setup, you can change your ReadyNAS Vault backup settings at any time by clicking the **Manage ReadyNAS Vault** button.

7. Follow the instructions of the ReadyNAS Vault setup wizard.

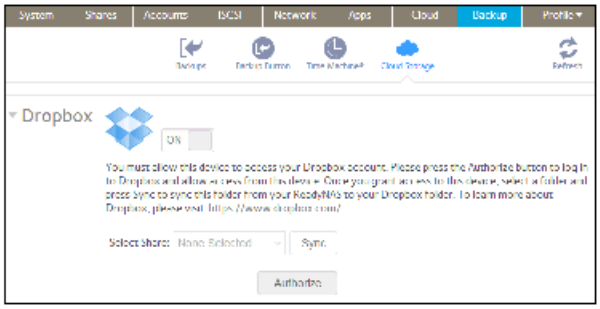
For more instructions about how to use ReadyNAS Vault, visit *http://www.netgear.com/ReadyNAS-vault*.

Dropbox

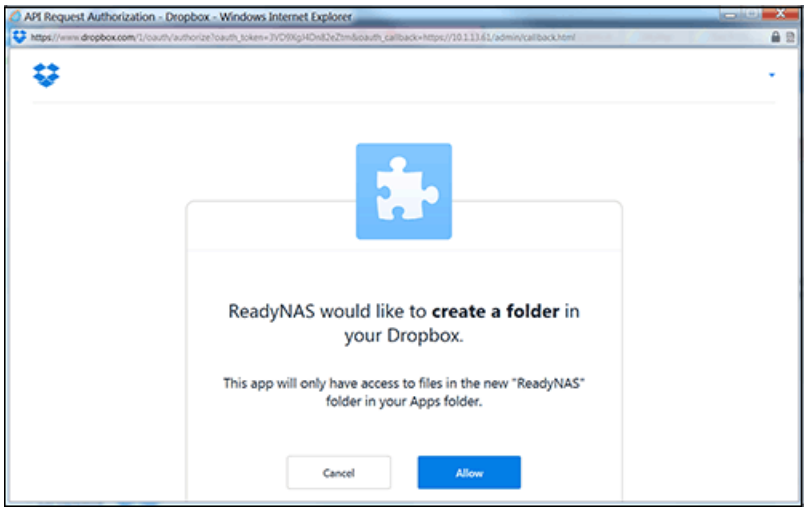
The ReadyNAS allows you to easily back up data from your system to your Dropbox account. From the local admin page, you can select a share on the ReadyNAS and sync it to a folder on your Dropbox account. For more information about Dropbox, visit *https://www.dropbox.com*.

To set up Dropbox backup on your system:

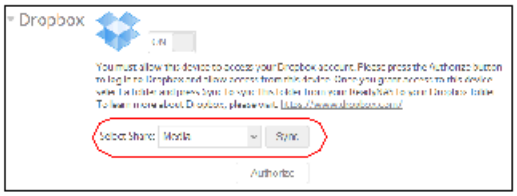
1. Log in to your ReadyNAS.
2. Select **Backup > Cloud Storage > Dropbox**.



3. Set the **On-Off** slider so that the slider shows the **On** position.
4. Click the **Authorize** button to allow the ReadyNAS to access your Dropbox account.
   A new browser window launches and takes you to *https://www.dropbox.com*.
5. Log in to your Dropbox account.
   A message displays asking if you want to allow the ReadyNAS to access your Dropbox account.



6. Click the **Allow** button.
   The ReadyNAS system creates a folder called ReadyNAS inside the Apps folder of your Dropbox.
7. From the drop-down list on the local admin page, select a share to sync with your Dropbox.



8. Click the **Sync** button.
   The contents of the share on your ReadyNAS system are copied to the ReadyNAS folder on your Dropbox account.

ReadyNAS Replicate

ReadyNAS Replicate is a free service that allows you to replicate and restore data from one ReadyNAS system to another. It uses ReadyNAS Remote as its underlying communication technology.

Using ReadyNAS Replicate involves these high-level steps:

1. Enable ReadyNAS Remote on your ReadyNAS systems.
   See *Enable ReadyNAS Remote* on page 74.
2. Enable ReadyNAS Replicate on your ReadyNAS systems.
   See *Enable ReadyNAS Replicate* on page 233.
3. Log in to the ReadyNAS Replicate web portal and begin replicating data between your ReadyNAS systems.

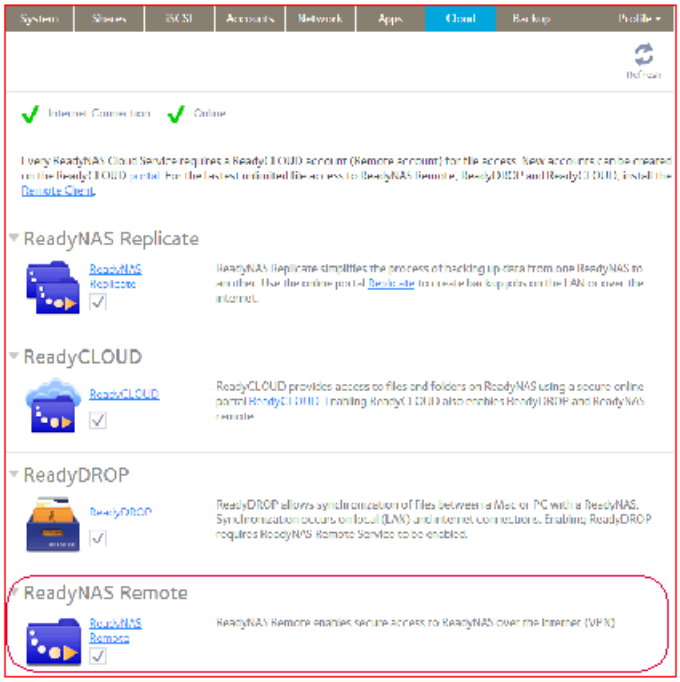
For more information about using the ReadyNAS Replicate portal, see the ReadyNAS Replicate User Manual or visit *https://www.replicate.readynas.com*.

Enable ReadyNAS Replicate

To use ReadyNAS Replicate, you must enable the ReadyNAS Replicate feature on your system and register your system with ReadyNAS Replicate.

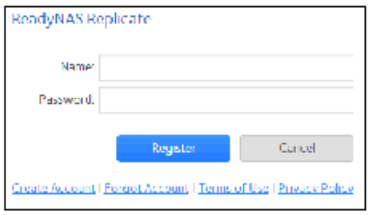
To enable ReadyNAS Replicate:

1. On the local admin page for your ReadyNAS OS 6 system, select **Cloud**.
   A list of Cloud services and Cloud users displays.
2. Make sure that ReadyNAS Remote is enabled.
   When ReadyNAS Remote is enabled, the check box below the link is selected.



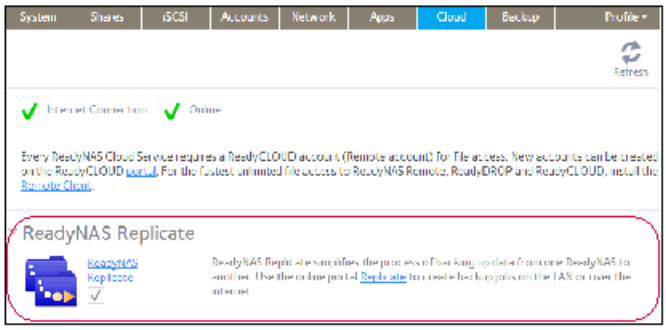
For more information about ReadyNAS Remote, see *Use ReadyNAS Remote* on page 73.

3. Enable ReadyNAS Replicate and register your system.
   1. Select the check box below ReadyNAS Replicate.
      A pop-up screen displays and prompts you to register your system with ReadyNAS Replicate.



   2. Enter your ReadyNAS Remote login credentials and click the **Register** button.

Your system is registered with ReadyNAS Replicate and the ReadyNAS Replicate feature is enabled on your system.



4. Repeat this process on each ReadyNAS OS 6 system that you want to use with ReadyNAS Replicate. You can now use the ReadyNAS Replicate web portal to replicate and restore data between your ReadyNAS systems.

   For more information about using the ReadyNAS Replicate portal, see the ReadyNAS Replicate User Manual or visit *https://www.replicate.readynas.com*.