NETGEAR®

ReadyNAS OS 6.8

Software Manual

August 2017
202-11207-15

350 E. Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for purchasing this NETGEAR product. You can visit *www.netgear.com/support* to register your product, get help, access the latest downloads and user manuals, and join our community. We recommend that you use only official NETGEAR support resources.

Trademarks

Compliance

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

See the regulatory compliance document before connecting the power supply.

Contents

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:

Note For more information about the topics covered in this manual, visit the support website at *www.netgear.com/support*.

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. We recommend 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 11. You use ReadyCLOUD to discover your storage system on your network.
2. *Create a Shared Folder* on page 52. Shared folders are the way you organize the data you store on your ReadyNAS system.
3. *Create a LUN* on page 86. LUNs are SAN data sets that allow data transfer and storage over iSCSI.
4. *Basic Snapshot Concepts* on page 112. Protect the data that is stored in folders and LUNs by creating snapshots.
5. *Create User Accounts* on page 128. 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 180. File-sharing protocols enable you to transfer files across a network.
7. *Backup Concepts* on page 228. 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. Click the ReadyNAS Coummunity button on the upper right side of the local admin page, or visit *https://community.netgear.com/t5/ReadyNAS-Network-Storage/ct-p/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://www.netgear.com/support/product/ReadyNAS_OS_6*.

Supported ReadyNAS Systems

This release of ReadyNAS OS supports the following ReadyNAS systems:

- RN102
- RN104
- RN202
- RN204
- RN212
- RN214
- RN312
- RN314

- RN316
- RN422
- RN424
- RN426
- RN428
- RN516
- RN524X
- RN526X
- RN528X
- RN626X
- RN628X
- RN716X
- RN2120
- RN2120 v2
- RN3130
- RN3138
- RN3220
- RN4220
- RR2304
- RR2312
- RR3312
- RR4312
- RR4360S
- RR4360X
- EDA 500

Supported Operating Systems

The ReadyNAS supports the following operating systems:

- Microsoft Windows 10 (32 and 64 bit)
- Microsoft Windows 8.1 (32 and 64 bit)
- Microsoft Windows 8 (32 and 64 bit)
- Microsoft Windows 7 (32 and 64 bit)
- Microsoft Windows Server 2012 (64 bit)
- Microsoft Windows Server 2008 R2 (64 bit)
- Apple Mac OS X 10.7 or later

- Linux, Unix, Solaris
- Apple iOS
- Google Android

Supported Browsers

The ReadyNAS local admin page supports the following browsers:

- Microsoft Edge
- Microsoft Internet Explorer 9.0 and later
- Apple Safari 5.0 and later
- Google Chrome 20 and later
- Mozilla Firefox 14 and later

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

Diskless Systems

If you own 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. We recommend you 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://www.netgear.com/support/product/ReadyNAS_OS_6.aspx*.

For basic configuration information, see *Basic Installation* on page 11.

For information about disk formats, see *RAID* on page 24.

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 14.

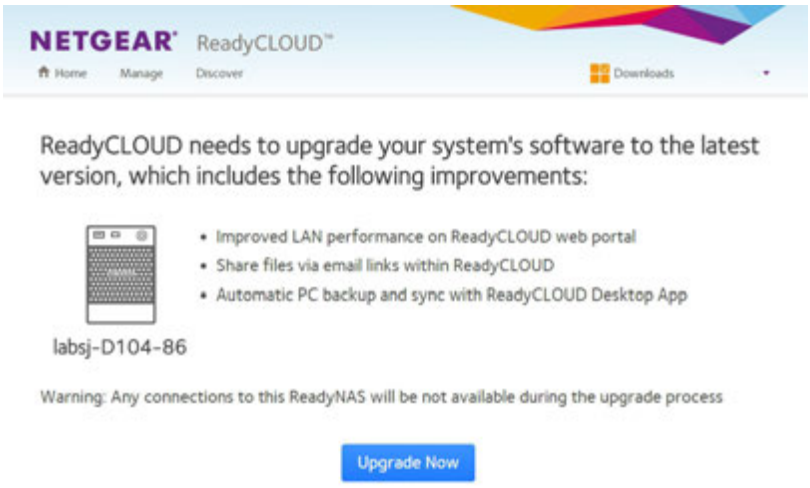
Upgrade Pre-6.2 ReadyNAS Firmware for Use With ReadyCLOUD

On some models of ReadyNAS running releases prior to ReadyNAS OS 6.2, you need to upgrade to RN OS 6.2 before upgrading to later releases. If you log in to ReadyCLOUD, you see a message about needing to upgrade the ReadyNAS system firmware.

The models are:

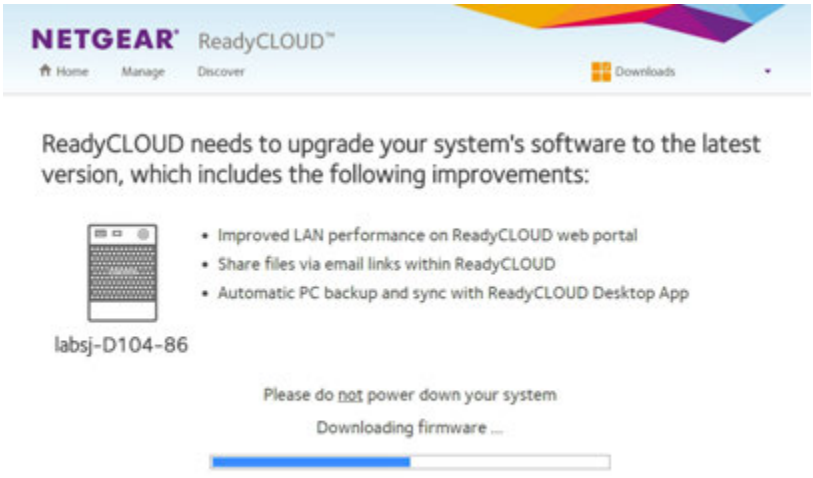
- ReadyNAS 102
- ReadyNAS 104
- ReadyNAS 202
- ReadyNAS 204
- ReadyNAS 212
- ReadyNAS 214
- ReadyNAS 2120
- ReadyNAS 2120 v2

If your ReadyNAS is one of these models, and is connected to ReadyCLOUD, when you log in to ReadyCLOUD, you see the following page:

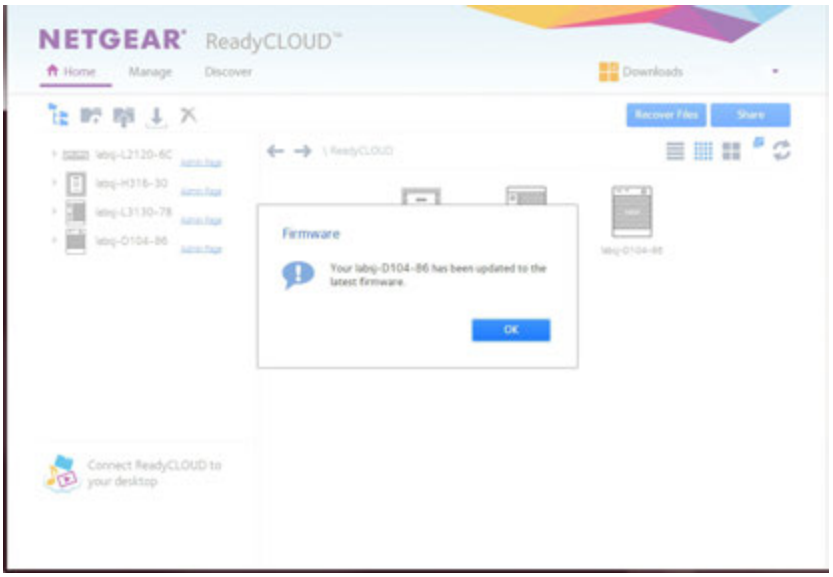


ReadyCLOUD now includes major new features, but these features require new firmware on the ReadyNAS system. When you log in to ReadyCLOUD from a ReadyNAS system, ReadyCLOUD checks to see if the ReadyNAS system firmware is recent enough to work with the new ReadyCLOUD. If it is not, you see the message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

During the download you see the following page:



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



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

Your system is now upgraded to ReadyNAS OS 6.2, and you can use the normal procedure to upgrade to more recent releases.

Discover and Set Up Your ReadyNAS Using ReadyCLOUD

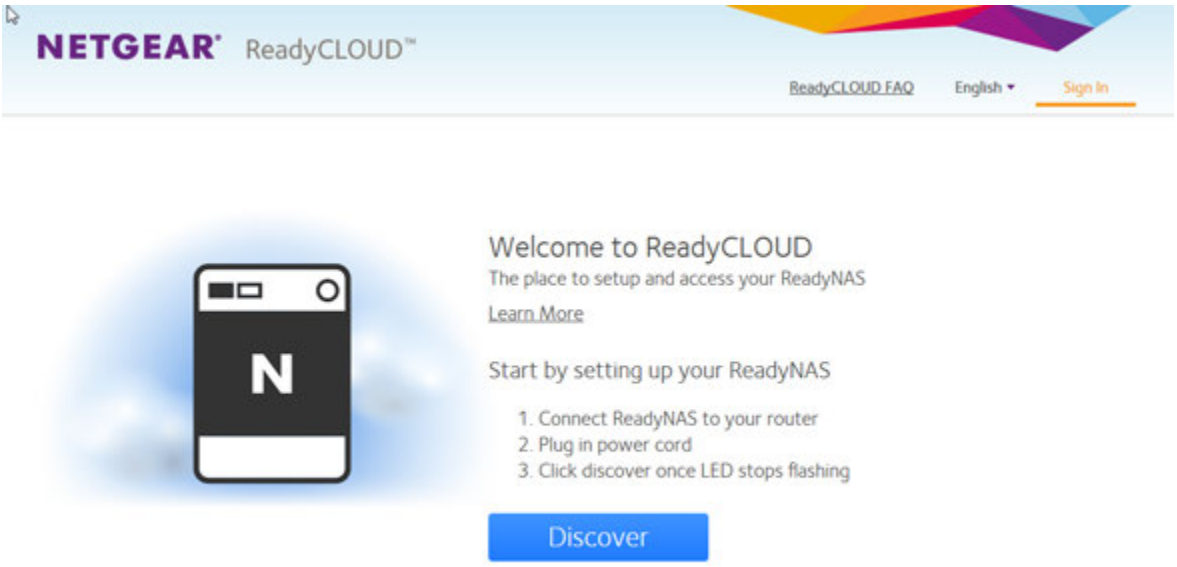
ReadyCLOUD is the online service that you use to discover and set up desktop ReadyNAS storage systems on your network. (Use the local admin page to set up rackmount ReadyNAS storage systems.) You can also use ReadyCLOUD to access and manage data on your ReadyNAS systems. For you to use ReadyCLOUD, your computer and storage system must be able to access the Internet.

Note If your computer and storage system cannot access the Internet, install and run the RAIDar utility instead. It includes versions for Windows, Mac, and Linux operating systems. It is available at *http://www.netgear.com/raidar*.

When you discover your device using ReadyCLOUD, you can choose whether to use ReadyCLOUD to set up and manage your device or use advanced offline installation.

To use ReadyCLOUD 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 Set up a new ReadyNAS **Start** button.



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

4. Click the **Setup** button.
5. To use ReadyCLOUD to set up your system, leave the **Setup with ReadyCLOUD (Default)** radio button selected and click the **Next** button.
6. Follow the onscreen instructions to set up your system.
   For more information about ReadyCLOUD, see *Use ReadyCLOUD* on page 139.
   For information about advanced offline installation, see *Local Setup Wizard* on page 15.

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.

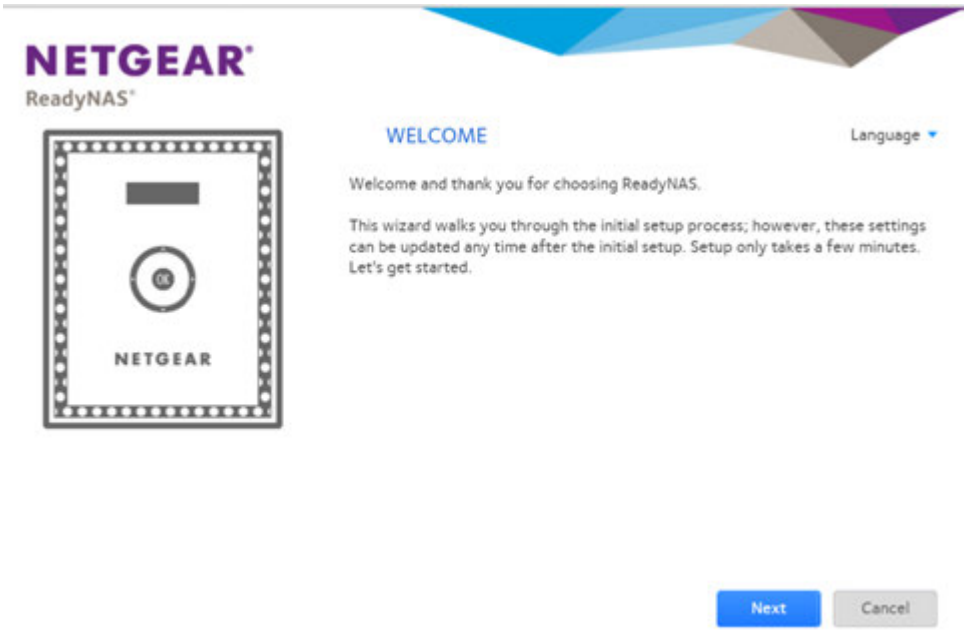


Figure 1. Setup wizard (Welcome page)

You can change the language setting for the setup wizard by selecting a language from the **Language** menu at the top right corner of the page.

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 160.
- **Alert contact**. For more information, see *Configure System Alerts* on page 164.
- **Host name**. For more information, see *Configure the Host Name* on page 164.
- **Administrator password and password recovery**. For more information, see *Set the Administrator Password* on page 162.

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 page displays, as shown in the following figure.

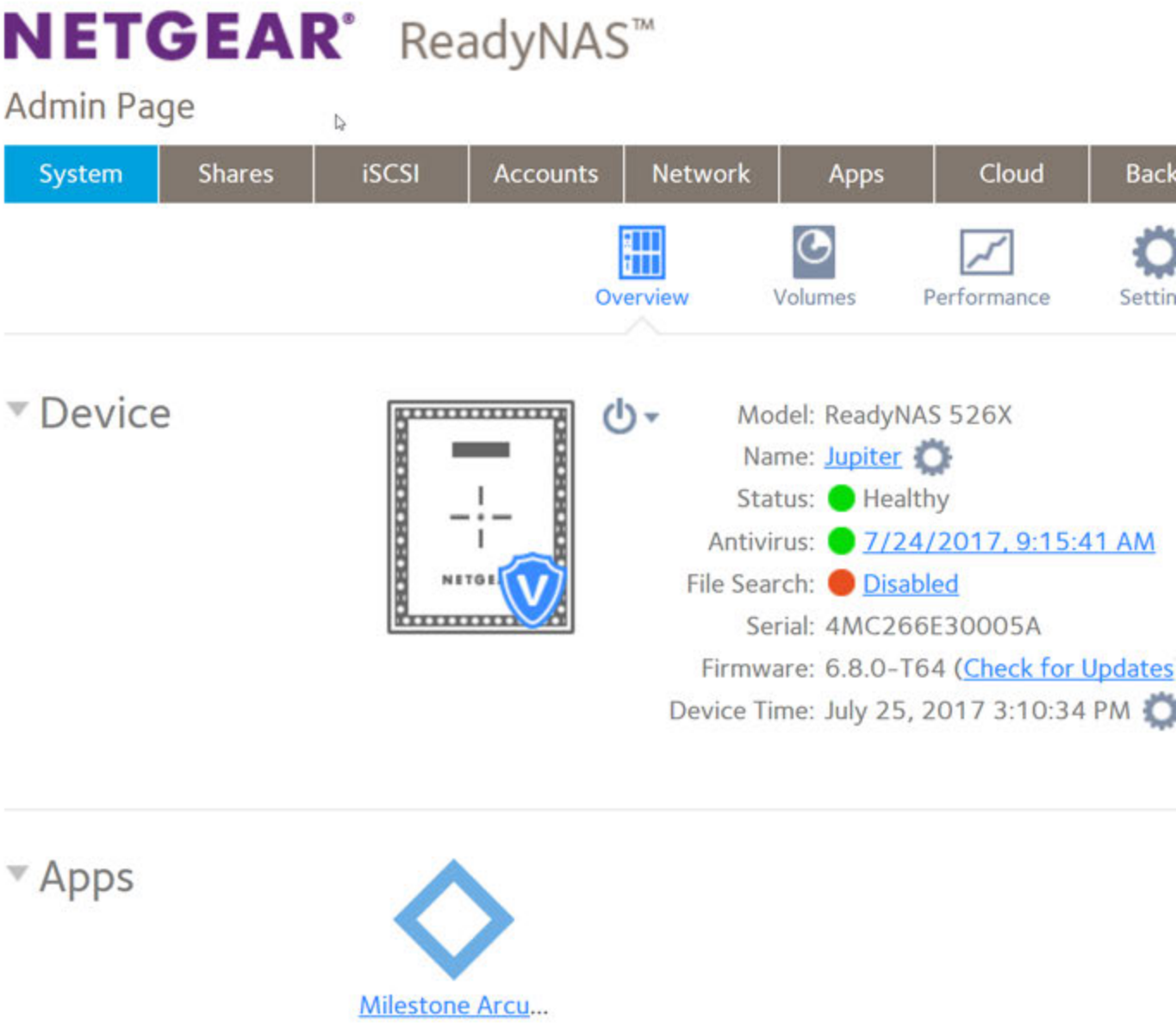


Figure 2. Local admin page (Overview page)

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 page and the navigation icons below it.
- Some pages are divided into multiple sections. You can collapse or expand sections of the page by clicking the triangle icon ( ) next to each section heading.
- To refresh the page, click the **Refresh** icon ( ) in the top right corner of the page.
- For help, click the **Help** icon ( ) in the top right corner of the page. A window opens on the admin page. You can move the help window around within the admin page. The content changes depending

on the navigation bar icon and the navigation icon you select. Close the help window by clicking the **X** icon in the upper left of the help window.

Figure 3. Example help page

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 page.

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.

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.

   Note The warning is because the certificate is a self-signed certificate, which browsers typically warn you about.

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 139).

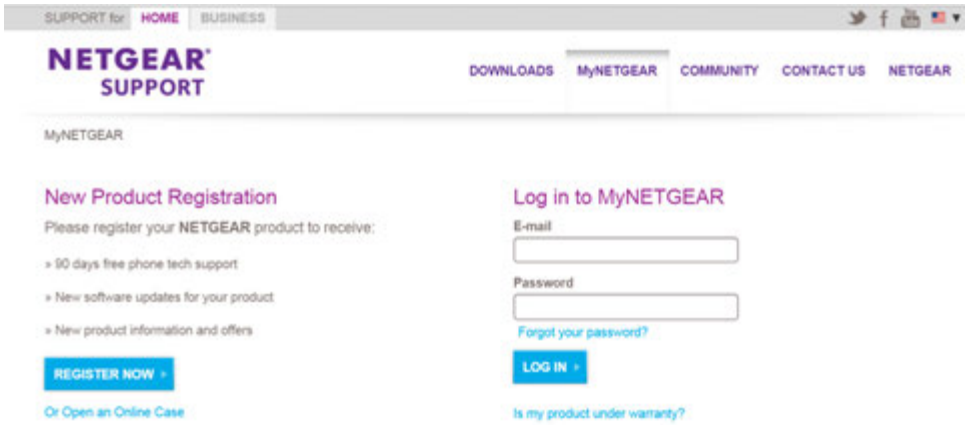
Register Your System

You must register your product before you can use NETGEAR support. When you first setup your ReadyNAS, the ReadyNAS creates a link unique to your ReadyNAS that you can use to register your system. The link displays in a notification bar at the top of the local admin page.

To register your ReadyNAS system, if the link is no longer available:

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

2. Open a web browser and visit *http://www.NETGEAR.com/register*.



3. Take one of the following actions:

   - If you never registered a NETGEAR product, click the **REGISTER NOW** 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 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**. Protects against site loss.

The ReadyNAS Community

The ReadyNAS community is part of the NETGEAR community. The NETGEAR community is a place where users and experts can come together to share tips and ideas, solve problems, and talk about everything NETGEAR products can do. The local admin page includes a link to the ReadyNAS part of the community.

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 be made up of up to two physical volumes (hard disk drives). A four-bay storage system can be made up of up to four physical volumes. A six-bay storage system can be made up of 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 are 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 28).

RAID Group

In ReadyNAS OS, a large RAID volume can be organized into RAID groups. RAID groups can improve performance by distributing I/O across more of the disks. During the process of creating a volume large enough to support RAID groups, ReadyNAS OS selects an appropriate RAID group structure for you. You can override this automatic structure before the volume is actually created.

X-RAID

X-RAID is an autoexpandable 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 includes only one volume that is made up of all installed hard disk drives. X-RAID's single-volume architecture provides two major advantages:

- Easy system management
- Auto expansion

Adding disks to a Flex-RAID formatted system is more complex. Disks must be added in ways compatible with the RAID level, or 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 use a ReadyNAS storage system with only one disk 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.

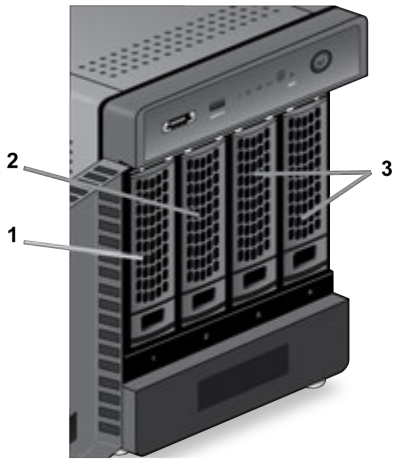


Figure 4. X-RAID disk usage

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 For systems with six or fewer bays, X-RAID reserves the capacity of one disk for data protection. For systems with more than six bays, with at least two disks and up to five disks, X-RAID reserves the capacity of one disk for data protection. For systems with six or more disks, the default format is RAID 6, which reserves two disks. 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 provides recovery 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.
- **RAID 50 (or 5+0)**. This RAID level uses both RAID 5 and RAID 0 technology. First, a disk is used to provide redundancy. Then your data is distributed across multiple disks to improve disk performance. A minimum of six disks are required. The total capacity of your storage system equals the capacity of all your disks minus the capacity of two disks.
- **RAID 60 (or 6+0)**. This RAID level uses both RAID 6 and RAID 0 technology. First, two disks are used to provide redundancy. Then your data is distributed across multiple disks to improve disk performance. A minimum of eight disks are required. The total capacity of your storage system equals the capacity of all of your disks minus the capacity of four disks.

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

Minimum 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	Yes. (Additional disk provides single redundancy and converts the volume to RAID 5.)
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.)
6 or more	RAID 50	No, but you can add two disks. (The additional disks provide dual redundancy and converts the volume to RAID 60.)
8 or more	RAID 60	No. (Volume is already protected with dual redundancy.)

Manage Volumes

You can manage volumes on your ReadyNAS system. You can add or delete volumes from the system. Additionally, you can change the volume's RAID mode and level, check volume status, perform volume maintenance, and configure volume protection. You can also extend the storage capacity on you ReadyNAS system.

Change RAID Mode

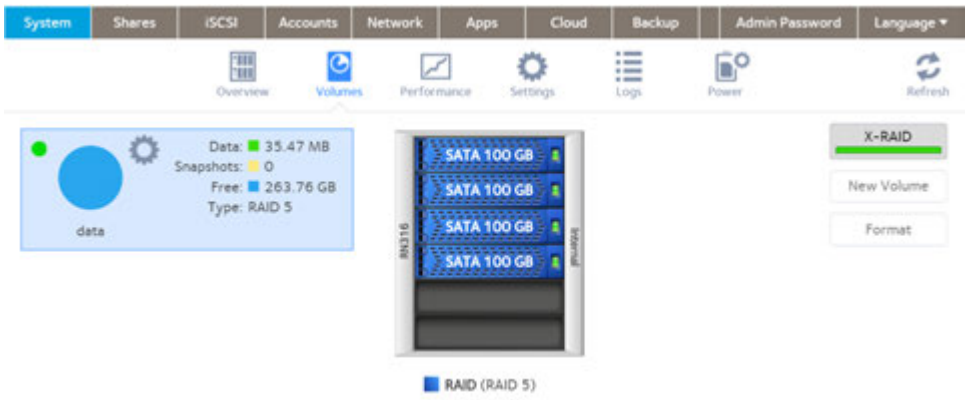
You can change the RAID mode that your ReadyNAS storage system uses. By default, your system's hard disks are configured into a single X-RAID volume (except RR4360, which only supports Flex-RAID).

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. Log in to the ReadyNAS.
2. Select **System > Volumes**.



3. Click the **X-RAID** button at the right side of the page.
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

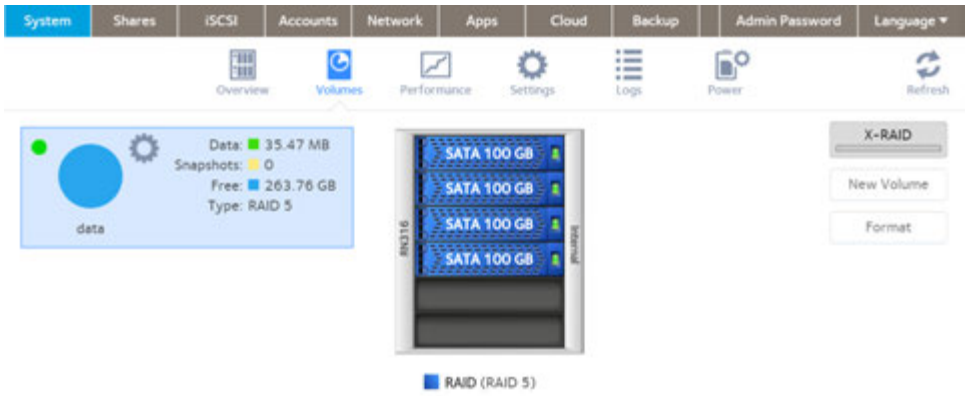
If your system contains only one volume, you can easily switch from Flex-RAID to X-RAID. Data on the Flex-RAID volume is preserved when you switch to X-RAID.

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 clean (meaning not part of another volume or from another system) 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. Log in to your ReadyNAS.
2. Select **System > Volumes**.



3. Click the **X-RAID** button at the right side of the page.
4. Confirm that you want to switch from Flex-RAID to X-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 26. 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.

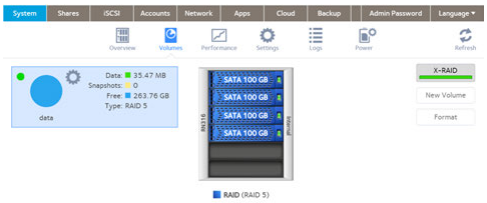
To change to RAID levels:

1. Log in to your ReadyNAS.
2. If any data is stored on the volumes that you want to reconfigure, back up your data.
3. Delete the volumes that you want to reconfigure (see *Delete a Volume* on page 35).
   The disks that were part of the volumes become available again for other purposes (the color of the disks turns black).
4. Create a new volume from the available disks and select the RAID level (see *Create and Encrypt a Volume* on page 33).
   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:

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



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

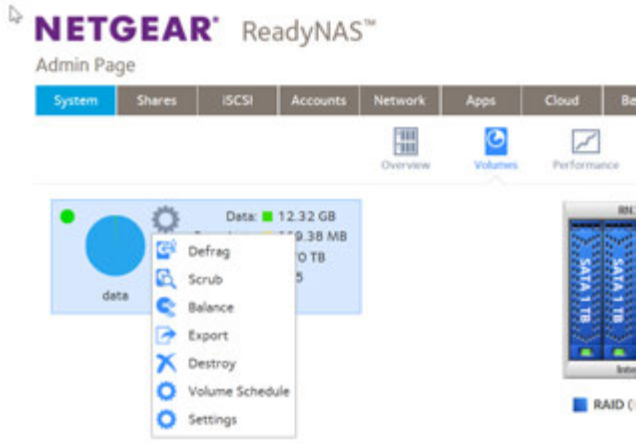
The following summary information is displayed next to each volume.

Item	Description
Data	The storage space that is consumed by data in MB, GB, or TB.
Snapshots	The storage space that is consumed by snapshots 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.

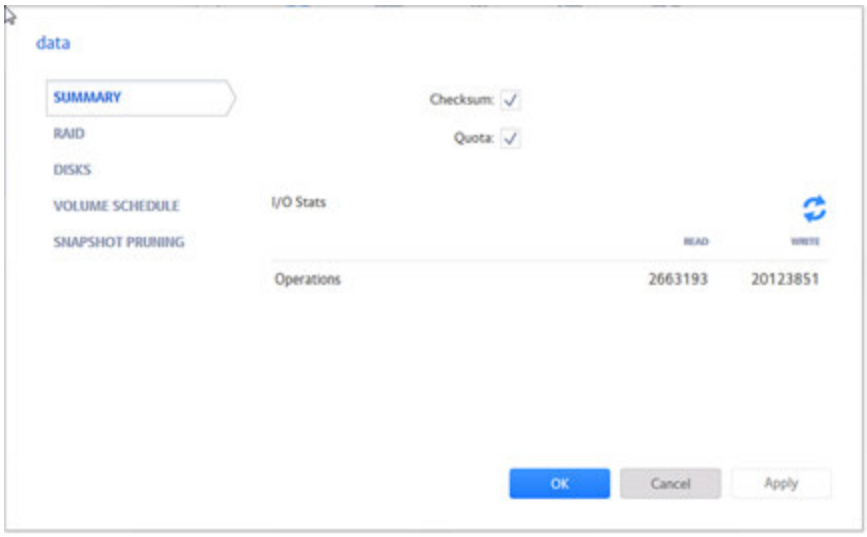
To view the I/O stats and disk status:

1. Log in to your ReadyNAS.
2. Select **System > Volumes**.
3. Select the volume from the list on the left.

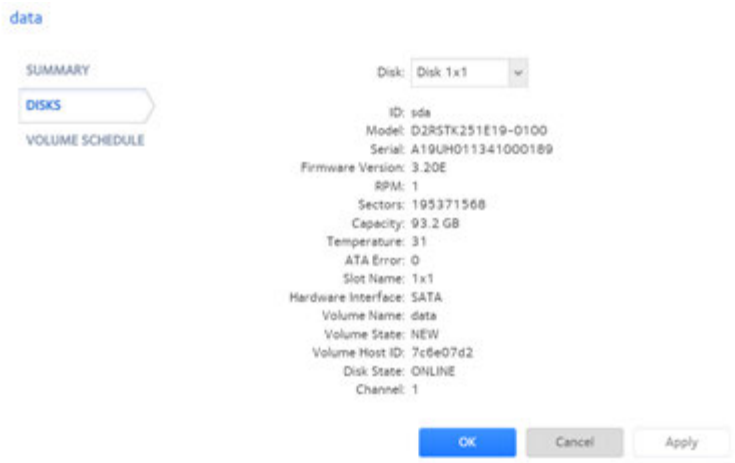
4. Click the **gear** icon.



5. Click the **Settings** button in the pop-up menu.



6. Click the **Disks** tab.



7. From the **Disk** menu, select a disk 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.

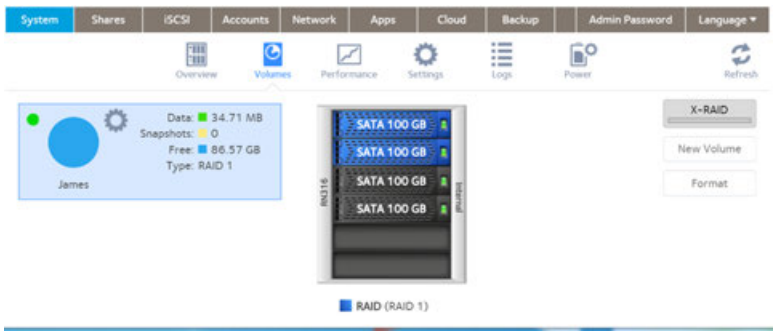
Configure the Checksum Function

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.

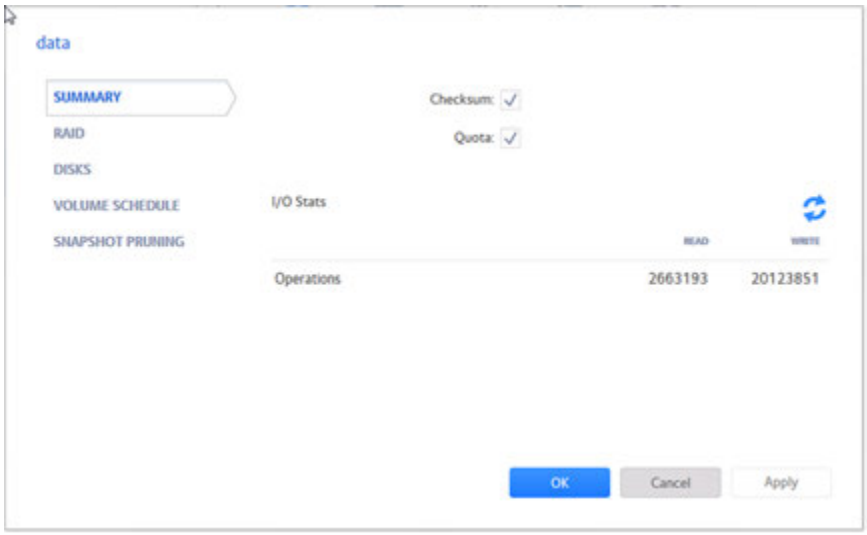
Bit rot protection uses the checksum functions to detect a read error. For information and bit rot protection, see *Bit Rot Protection* on page 51.

Enable or disable the checksum function:

1. Log in to your ReadyNAS.
2. Select **System > Volumes**.
3. Select one of the volumes listed on the left side of the page.
4. Click the **gear** icon.



5. Click the **Settings** button on the pop-up menu.



6. Select or clear the **Checksum** check box.
7. Click the **Apply** button.
8. Click the **OK** button.
   Your settings 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 specify that the encryption key be 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.

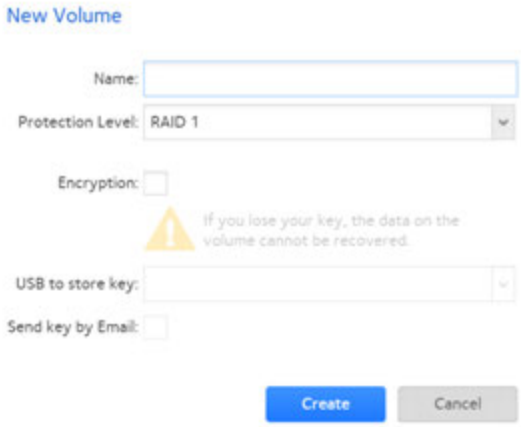
You must insert the USB drive with the encryption key into a USB port on the ReadyNAS for the volume to be unlocked and accessible. You must insert the USB drive to unlock an encrypted volume during reboot. If you do not insert the USB key on reboot, there is a 10-minute time-out during which you can 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. We recommend 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. Log in to your ReadyNAS.
2. Select **System > Volumes**.

3. From the enclosure graphic, select one or more disks to include in the new volume. Available disks are colored black.
4. Click the **New Volume** button at the right of the page.



5. Configure the following settings:

   - **Name**. Enter a name for the volume. The volume must not use the same name as a folder in the root folder system. The volume names home , apps , and job_ are reserved and cannot be used.
   - **Protection Level**. Use the drop down menu to select the protection level (RAID level).
   - **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 menu to store the generated key.
- **Send key by Email**. If you enabled encryption, select this check box to specify that the generated key be sent to a email address associated with the admin account. Make sure that you set the email account before creating the volume.

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

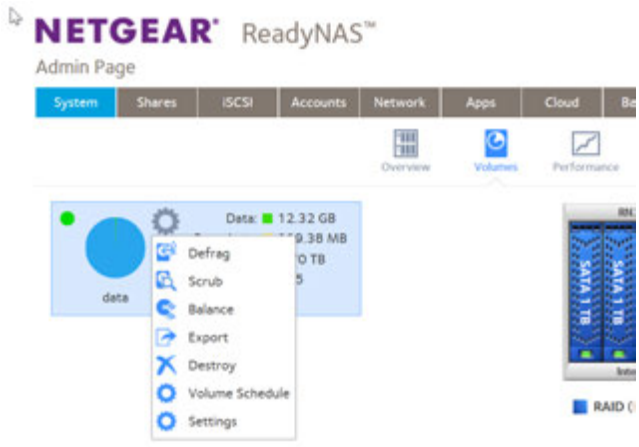
Delete a Volume

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.

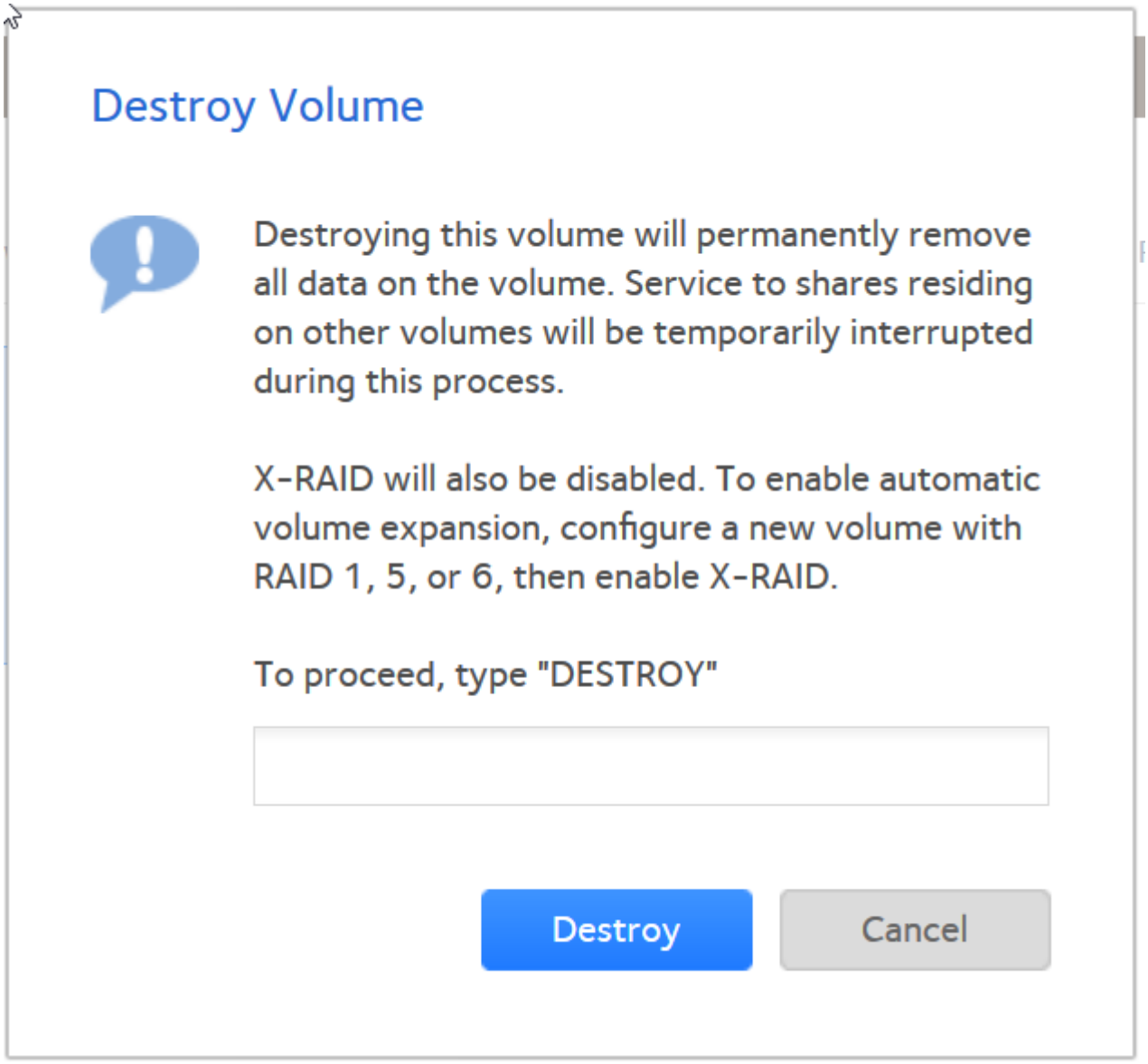
> **Note** The **Destroy** option is not available when the ReadyNAS uses a single volume X-RAID configuration. The **Destroy** option is available if you use at least two volumes, or the volume is a Flex-RAID volume.

To delete a volume:

1. Log in to the ReadyNAS.
2. Select **System > Volumes**.
3. Select the volume.



4. In the pop-up menu, click the **Destroy** button.



5. Type **DESTROY** to confirm your decision.
6. 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.

Both horizontal and vertical expansion is available for X-RAID and Flex-RAID volumes.

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.

When you expand a Flex-RAID volume you need to add disks in increments compatible with the RAID level of the volume.

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 164.

Horizontally Expand an X-RAID Volume

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 *https://www.netgear.com/support/product/ReadyNAS_OS_6.aspx*.

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 25. New disks are incorporated in the background while you continue to use your storage system.

Horizontally Expand a Flex-RAID Volume

Horizontal expansion of a Flex-RAID volume is possible, but more complex and less space efficient than expanding an X-RAID volume. In effect, you create a new Flex-RAID volume and ReadyNAS OS uses both the existing and new volumes as parts of the same larger volume. Other configurations are possible, but We recommend expanding the volume by the same number of disks as the original volume; for example, expand a 3-disk RAID 5 Flex-RAID volume by adding three disks.

To horizontally expand a Flex-RAID volume:

1. Add disks to the ReadyNAS, if necessary.
   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://www.netgear.com/support/product/ReadyNAS_OS_6*.
2. Log in to the local admin page.
3. Select **System > Volumes**.
4. Select the volume to expand.
5. Select the unallocated disks to add to the volume.
   When you select disks additional buttons appear on the volume.
6. Select the **Expand** button.
   A Window opens asking you to verify you want to expand the volume.
7. Select the **Yes** button.
   The volume expands immediately, but requires a resync, which starts immediately. The volume display includes a resync progress bar.

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 2. 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.

IMPORTANT:
To reduce the risk of data loss, we recommend 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://www.netgear.com/support/product/ReadyNAS_OS_6*.

   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 are recorded in the system log (see *System Logs* on page 215).
   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 164.
3. Repeat *Step 1* on page 38 – *Step 2* on page 38 until you replace the required number of disks with larger-capacity disks.
   For more information about X-RAID vertical expansion requirements, see *Table 2*.

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://www.netgear.com/support/product/ReadyNAS_OS_6*.

   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 are recorded in the system log (see *System Logs* on page 215).
   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 164.
3. Repeat *Step 1* on page 39 and *Step 2* on page 39 until you replace each disk in the volume with a larger-capacity disk.

Add Protection to a Volume

You can set up protection against disk failure. The types of protection available depend on the number of hard disks installed in the ReadyNAS system.

Adding 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 *https://www.netgear.com/support/product/ReadyNAS_OS_6.aspx*.

An X-RAID volume that includes two or more disks is automatically formatted to protect against the failure of one disk. Except for very large ReadyNAS systems (for example 12-bay systems), if you want to protect your data against the failure of two disks, you must switch to Flex-RAID and select RAID 6. (Very large ReadyNAS systems use RAID 6 by default.) 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 28.

Adding 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 3. Flex-RAID levels and data protection

Number of Disks per Volume	RAID Level	Can I add a disk to for data protection?
1	JBOD	Yes. Converts to RAID 1. (Additional disk provides redundancy.)
2	RAID 1	No. (Volume protection is already redundant.)
2 or more	RAID 0	Yes. Converts to RAID 5.
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.)

Add Protection to a Flex-RAID Volume

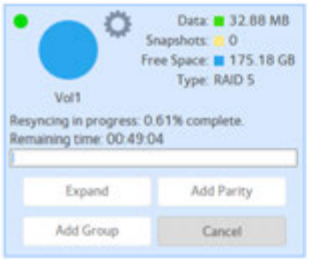
To add protection to a Flex-RAID volume:

1. Add disks to the ReadyNAS, if necessary.

   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://www.netgear.com/support/product/ReadyNAS_OS_6*.

2. Log in to the local admin page.
3. Select **System > Volumes**.
4. Select the volume.
5. Select the unallocated disks to add to the volume.

   When you select disks additional buttons appear on the volume. The active buttons change as you add disks.



6. Select the **Add Parity** button.

Note Which buttons are active depends on the volume and the number of disks selected.

The Add Parity window opens.

7. Select the **Yes** button.

   The volume expands immediately, but requires a resync, which starts immediately. The volume display includes a resync progress bar.

Add a Group to a Flex-RAID Volume

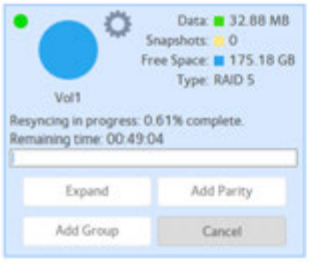
To add a group to a Flex-RAID volume:

1. Add disks to the ReadyNAS, if necessary.

   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://www.netgear.com/support/product/ReadyNAS_OS_6*.

2. Log in to the local admin page.
3. Select **System > Volumes**.
4. Select the volume.
5. Select the unallocated disks to add to the volume.

   When you select disks additional buttons appear on the volume. The active buttons change as you add disks.



6. Select the **Add Group** button.

Note Which buttons are active depends on the volume and the number of disks selected.

The Add Group window opens. Depending on the existing number of disks, the RAID type, and the number of disks added, new groups can be RAID 0/stripped to the existing disks, or concatenated to the existing disks.

7. (Optional) Select the **RAID0/Stripe** button or the **Concatenated** button.
8. Select the **Apply** button.

   The volume expands immediately, but requires a resync, which starts immediately. The volume display includes a resync progress bar.

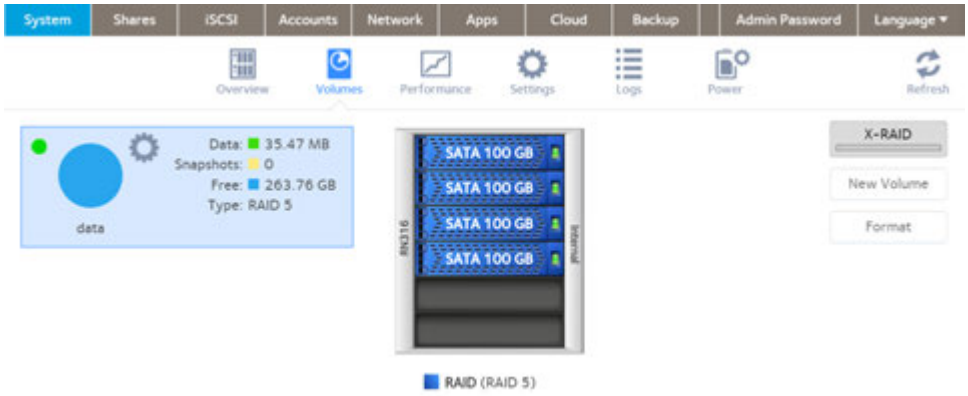
Use the Volume Management Wizard to Create a Volume

Normally ReadyNAS OS automatically formats all of the disks in a ReadyNAS storage system (for all models except an RR4360), in to a single X-RAID volume, but if you add disks or destroy existing volumes, you can use the volume management wizard to create volumes.

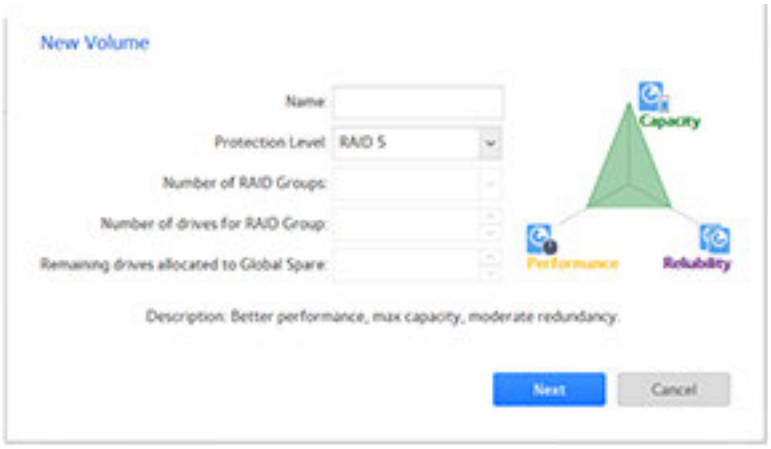
As is not the case with other ReadyNAS storage systems, when you first configure an RR4360, the volume management wizard starts automatically.

To create a volume with the volume management wizard:

1. Log in to the ReadyNAS.
2. Select **System** > **Volumes**.



3. Select the disks to include in the new volume.
4. Click the **New Volume** button.



5. Enter a name.
6. Leave the protection level as selected by ReadyNAS OS, or change it.

   The graphic shows the balance of capacity, performance, and reliabilty for the selected protection level and number of disks. As you change the RAID level, the graphic updates to show the changed balance.

   If more drives than the minimum necessary for the selected RAID level are available, the **Number of RAID Groups**, **Number of drives for RAID Group**, and **Remaining drives allocated to Global Spare** fields are active. You can chose to organize the volume with RAID groups, or assign disks to the global spares pool, or a combination of the two.
7. Click the **Next** button.
8. (Optional) Select the **Encryption** check box, and select one of the following options:

- **USB to store key**
- **Send key by Email**

9. Click the **Create** button.
   The New Volume window closes and the ReadyNAS starts to build the new volume (resync the drives).

Maintain Volumes

This section covers volume maintenance. Volumes can be scrubbed to check for errors, defragmented to improve disk performance, and balanced to use space more efficently and speed allocation of new chunks.

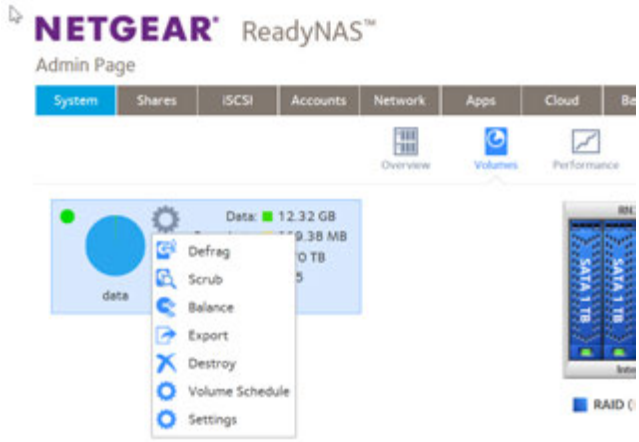
Scrub a Volume

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. Scrubbing every six to eight weeks is common.

> **Note** Scrubbing is not an erase function.

To scrub a volume:

1. Log in to your ReadyNAS.
2. Select **System > Volumes**.
3. Select a volume.
4. Click the **gear** icon.



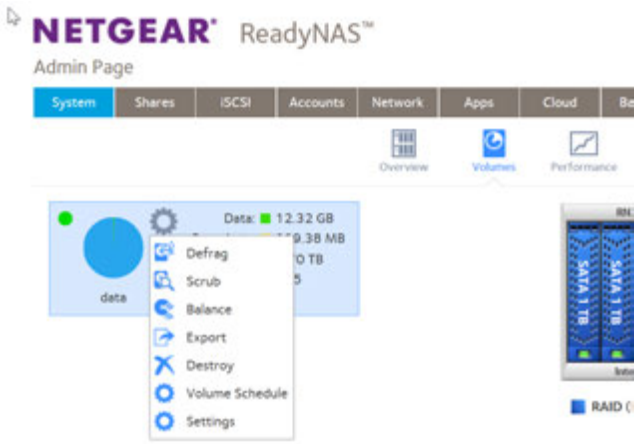
5. Click the **Scrub** button in the pop-up menu.
   A confirmation window opens.
6. Choose the **Yes** button to confirm.
   The scrubbing process starts.
   The start and completion of the volume scrub are recorded in the system log (see *System Logs* on page 215).
   If you set up email notifications for your system, you receive an email message when the process finishes. For more information about alert notifications, see *Configure System Alerts* on page 164.

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. Log in to your ReadyNAS.
2. Select **System > Volumes**.
3. Select a volume.
4. Click the **gear** icon.



5. Click the **Defrag** button in the pop-up menu.
   A confirmation window opens.
   Choose the **Yes** button to confirm.
   The defragmentation process starts.
   The start and completion of the volume defragmentation are recorded in the system log (see *System Logs* on page 215).
   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 164.

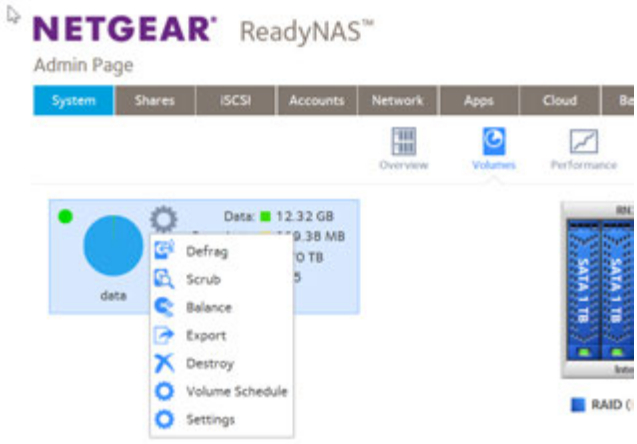
Balance a Volume

You can consolidate partially filled chunks of volumes and assign previously used chunks for reuse by balancing a volume. A balanced volume uses space more efficiently and speeds the allocation of new chunks during writes.

To balance a volume:

1. Log in to the ReadyNAS.
2. Select **System > Volumes**.
3. Select the volume.

4. Click the volume **gear** icon.



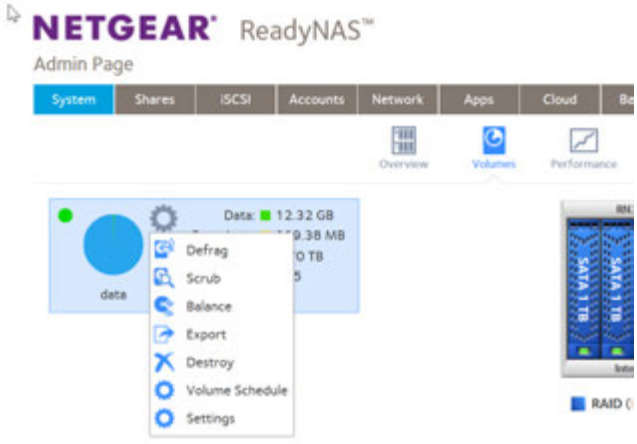
5. Click the **Balance** button.
   A window opens.
6. Click the **Yes** button in the pop-up window.
   The volume information updates to show the status of the balance operation, and the ReadyNAS system issues an alert and a log entry when the balance operation starts and when the operation completes.

Export a Volume

You can move a volume with its disks to another ReadyNAS device while the devices are running, but you must first export the volume. Other volumes on the ReadyNAS continue operating normally.

To export a volume:

1. Log in to the ReadyNAS.
2. Select **System > Volumes**.
3. Select the volume.
4. Click the volume **gear** icon.



5. Click the **Export** button.

The Export Volume window opens.

6. Type the word **EXPORT** in the text box in the Export Volume window.
7. Click the **Export** button.
   The volume is unmounted from the ReadyNAS and prepared to be added to another ReadyNAS system. Service to all shares is temporarily interrupted.

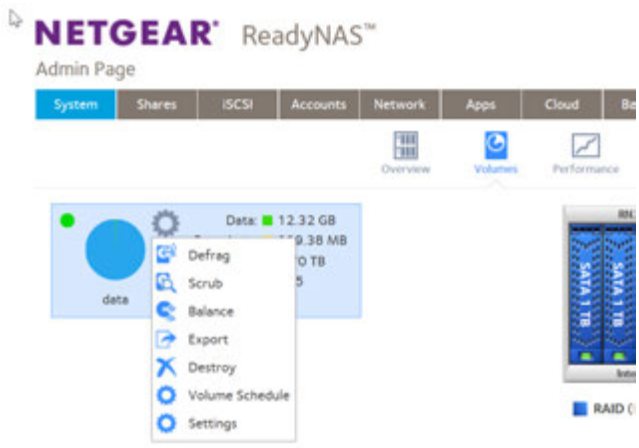
Note The ReadyNAS to which you move the volume must not include an existing volume with the same name as the volume that you plan to move.

Schedule Volume Maintenance

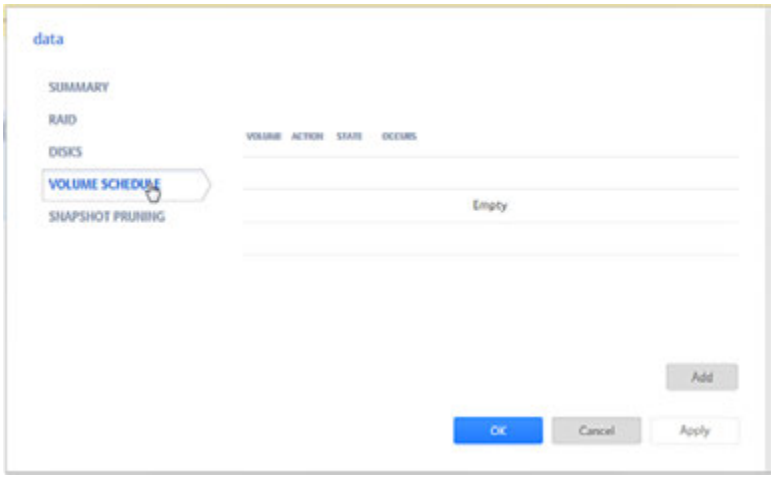
You can schedule routine maintenance operations (scrub, defrag, balance, and disk test) on a volume.

To create a schedule of routine volume maintenance:

1. Log in to the ReadyNAS.
2. Select **System > Volumes**.
3. Select the volume.
4. Click the volume **gear** icon.



5. Click the **Volume Schedule** button.



6. Click the **Add** button.
   The Add Schedule window opens.
7. Select the maintenance operation from the **Action** menu (**Scrub**, **Defrag**, **Balance**, **Disk Test**).
8. Select from the **Pattern** menu (**Daily**, **Weekly**, **Monthly**, **Yearly**).
   The Add Schedule window adjusts to show hours of the day, days of the week, dates of the month, or months of the year.
9. Select the hours, days, dates, or months.
10. Select the start time.
11. Click the **Add** button.
    The Add Schedule window closes. The Volume Schedule window updates to show the new schedule.

Shared Folders

3

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

- *Basic Shared Folder Concepts*
- *Manage Shared Folders*
- *Shared Folder Access Rights*
- *Access Shared Folders From a Network-Attached Device*

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 33.

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 5. Shared folder with file-sharing protocols enabled

Figure 6. 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

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 desktop ReadyNAS storage system, the following shared folders are created for you:

- Documents
- Music
- Pictures
- Videos

These folders are not automatically created on rack-mount ReadyNAS storage systems.

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. Some file-sharing protocols, UPnP, SNMP, SSH and antivirus, apply to the ReadyNAS system as a whole, not to indvidual folders.

For information about how to configure and enable file-sharing protocols for shared folders, see *Set Network Access Rights to Shared Folders* on page 61. For information about how to configure UPnP, SNMP, SSH, and antivirus, see *Configure Global Settings for System Services* on page 180.

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

Table 4. 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 referred to as the CIFS (Common Internet File Service) file-sharing protocol. SMB uses TCP/IP.	If Windows users access your storage system, enable this protocol.
AFP (Apple File Protocol)	Mac OS X computers can use AFP, but Apple now recommends SMB. Your ReadyNAS system supports AFP 3.3.	This protocol is enabled by default. However, Apple fully supports SMB for Mac OS X, and in a mixed Windows and Mac environment, We recommend using SMB only.
NFS (Network File Service)	Linux, Windows, 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.

Table 4. Supported file-sharing protocols (Continued)

Protocol	Description	Recommendation
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. Note: UPnP is used with ReadyCLOUD. If you use ReadyCLOUD, leave UPnP enabled.
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.
Antivirus	Adds antivirus scanning to new files written using the SMB protocol.	If users access files using the SMB protocol, and you want automatic antivirus scanning of those files, enable this protocol.

Quotas on Shared Folders

You can set and change quotas on shared folders. Without a quota, a shared folder can use all of the space on the volume it resides on. You cannot set quotas on home folders. Quotas are a property of the folder and can be set when the folder is created, or added or changed like any folder property.

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 checksum functions to check for bit rot and the redundancy in RAID-protected disks to 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 system. On higher-end models it is on by default. Bit rot protection can slow the performance of a system and increase fragmentation, and so is not on by default on lower-end models.

Home Folders

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

You use it like any other folder on the ReadyNAS system. 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. Your home folder is created the first time you log into the ReadyNAS system.

If a user account is deleted, the home folder for that account, and all of the content within it, is deleted.

You can view your folder by clicking **Shares > Shares > Home Folders** or **Shares > Browse > home**.

Manage Shared Folders

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

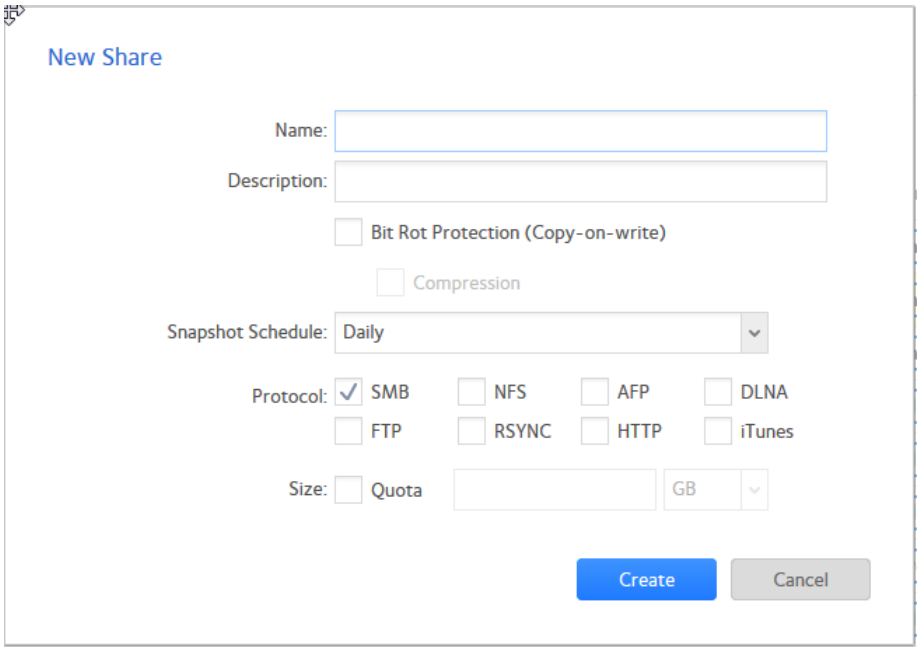
Create a Shared Folder

After you create a volume (see *Create and Encrypt a Volume* on page 33), you can create shared folders on that volume.

To create a shared folder:

1. Log in to the local admin page.
2. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.

3. Click the **New Shares** 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.
Bit Rot Protection	Select the **Bit Rot Protection (Copy-on-write)** check box to enable bit rot protection. For information, see *Bit Rot Protection* on page 51.
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. Note that compression is only available when bit rot protection is enabled.
Snapshot Schedule	The interval specifies how often a snapshot is taken. Make a selection from the menu: • **Never**. No shapshot is taken. • **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. For information about snapshots, see *Chapter 5, Snapshots* on page 111.
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 50.
Size	Select the **Size** check box to enable quotas. Enter the quota and make a selection from the menu (**MB** for megabytes, **GB** gigabytes, or **TB** for terrabytes). For information about quotas, see *Quotas on Shared Folders* on page 51.

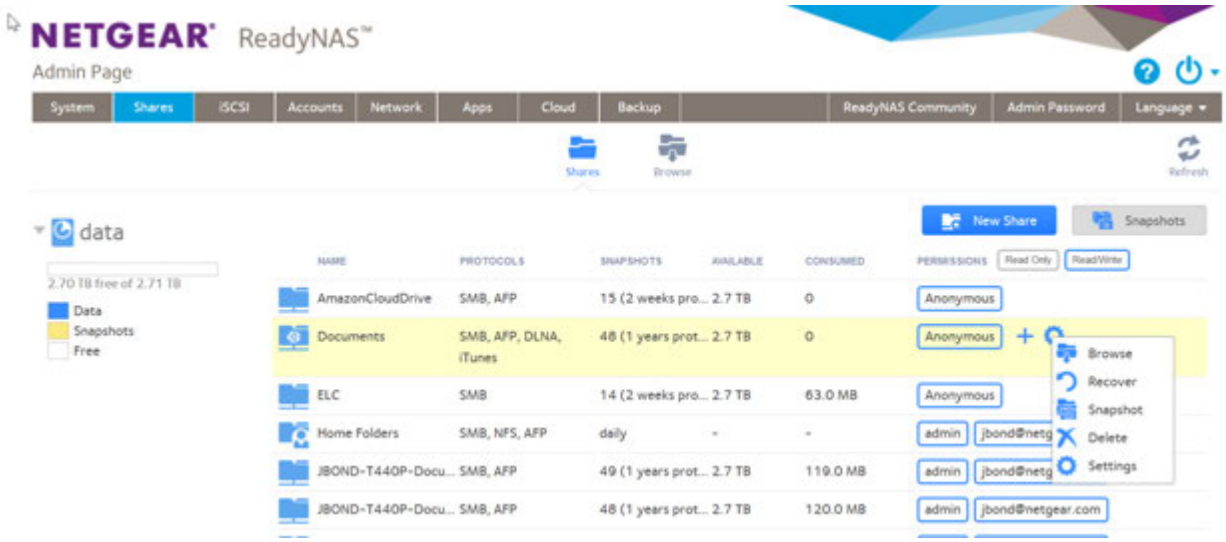
5. Click the **Create** button.

The ReadyNAS confirms the creation of a shared folder with the message “Folder or LUN successfully created.”

View and Change the Properties of a Shared Folder

To view and change the properties of a shared folder:

1. Log in to the local admin page.
2. 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. Click the **gear** icon for the folder.



5. Click the **gear** icon in the pop-up menu.
6. 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.
Bit Rot Protection	Select the **Bit Rot Protection (Copy-on-write)** check box to enable bit rot protection. For information, see *Bit Rot Protection* on page 51.
Compression	Select the **Compression** check box to enable data compression. Compression is only available if bit rot protection is enabled. Compression saves storage space and increases the speed of data transfers, but the compression and decompression processes require additional resources.
Network Access	
For information about how to provide folder access to users and groups, see *Set Network Access Rights to Shared Folders* on page 61.	
Snapshots	

(Continued)

Item	Description
For information about how to configure snapshots, see *View and Change Share Snapshot Properties* on page 113.	
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 74.	

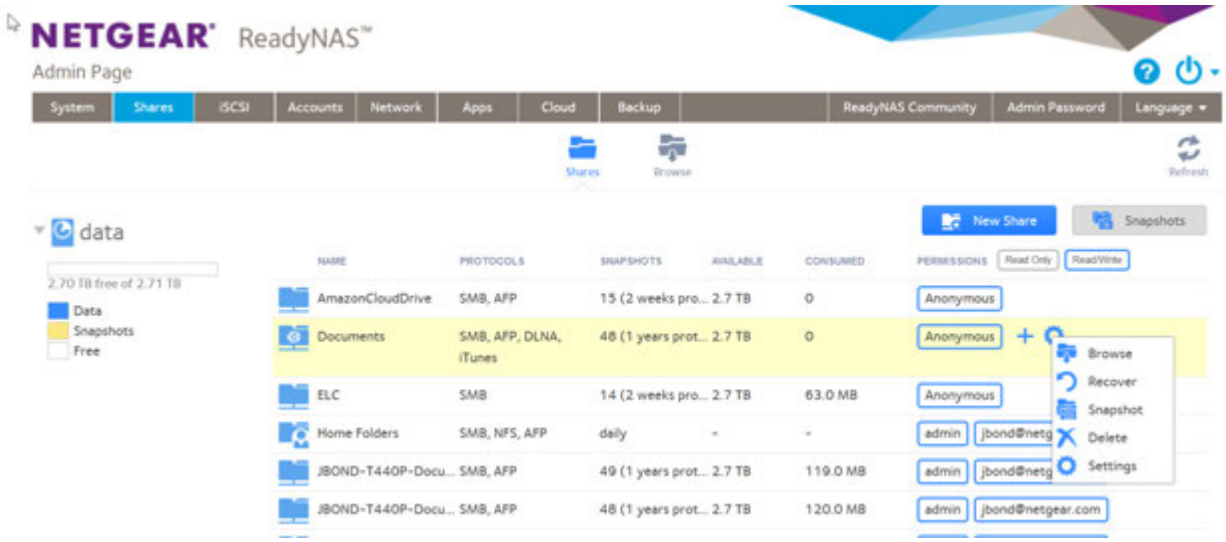
7. Click the **Apply** button.
8. Click the **OK** button.
   Your settings are saved and the pop-up menu closes.

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. Log in to your ReadyNAS.
2. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder.
4. Click the **gear** icon for the folder.



5. Click the **Delete** button in the pop-up menu.

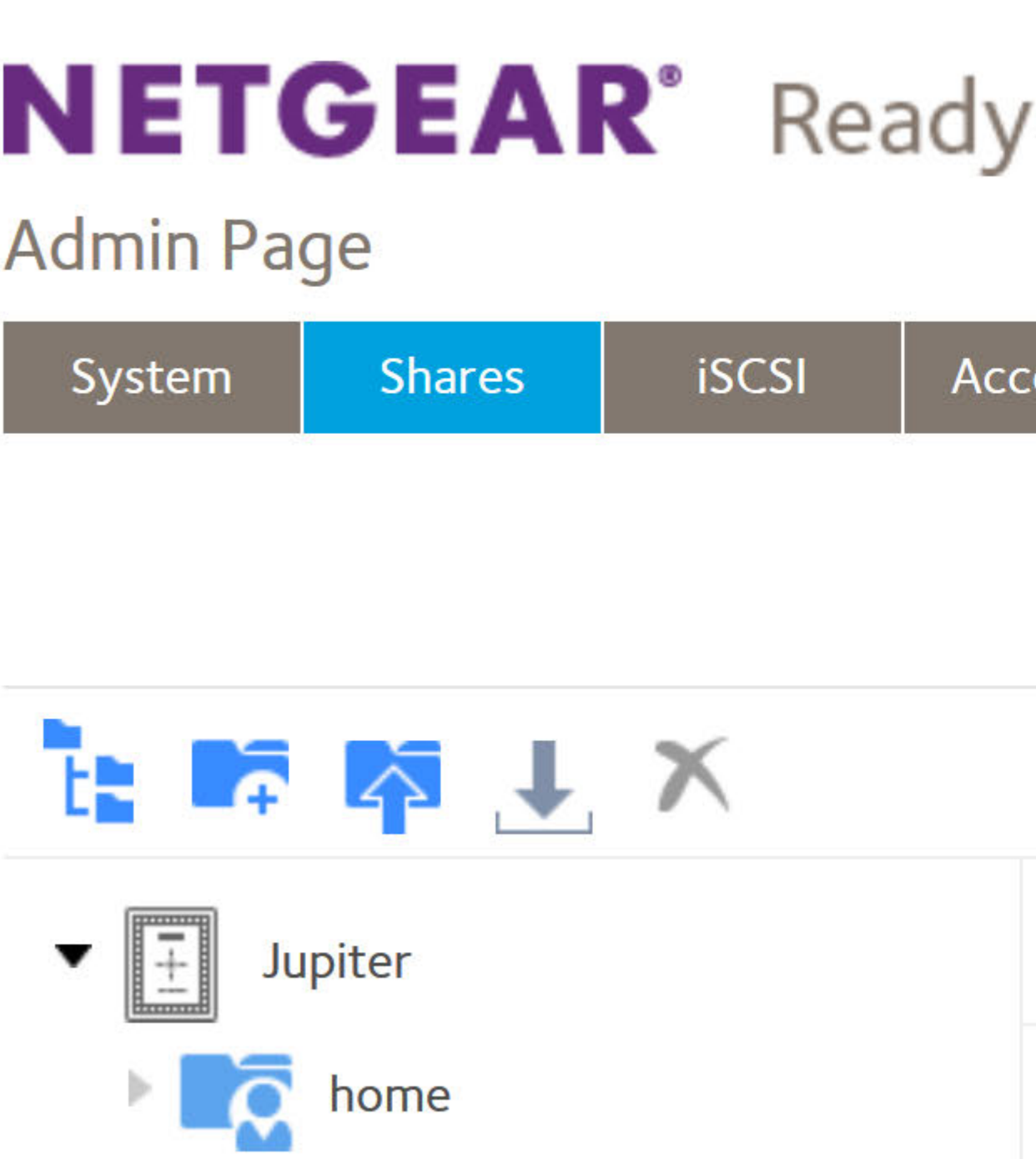
6. In the pop-up window, confirm the deletion by typing **DESTROY**.
7. Click the **Destroy** button.
   The shared folder is deleted.

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. Log in to the ReadyNAS.
2. Select **Shares > Browse**.



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

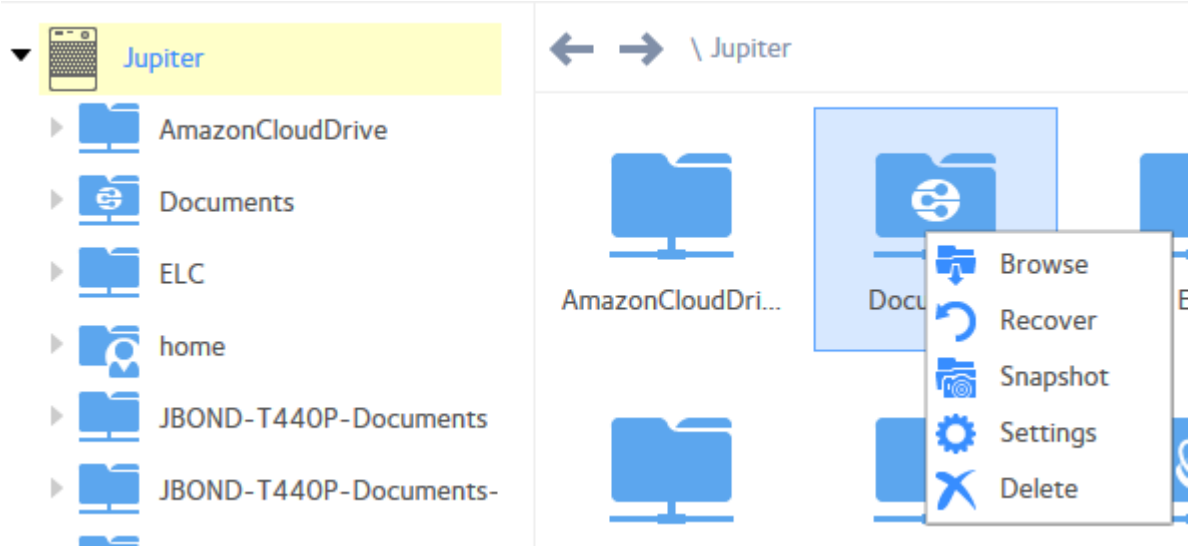
Tip Use the forward and back (←→) arrows to browse through folders. You can view files and folders as a list with details, as small icons, or as large icons. To change views, click one of the view icons (≡ ⊞ ⊞) at the right side of the page.

Set or Change Bit Rot Protection

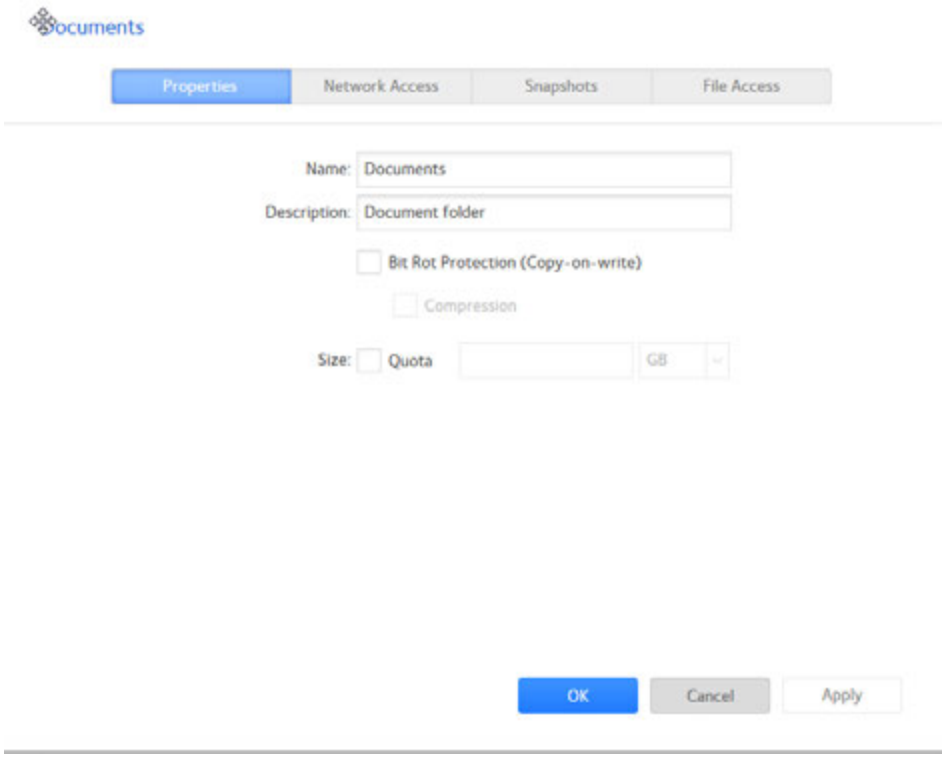
Bit rot protection can protect your data from the gradual loss of reliability of disks as they age. It can impact performance, so you can turn it on and off for individual folders. Bit rot protection is also called copy-on-write.

To set or change bit rot settings:

1. Log in to your ReadyNAS system.
2. Select **Shares > Browse**.
3. Right-click the folder.



4. In the pop-up menu, 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.

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 5. 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.

Table 5. Access right options (Continued)

Access Right	Description
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 125):

- **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 123.
- **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 window.

Set Network Access Rights to Shared Folders for Common Protocols

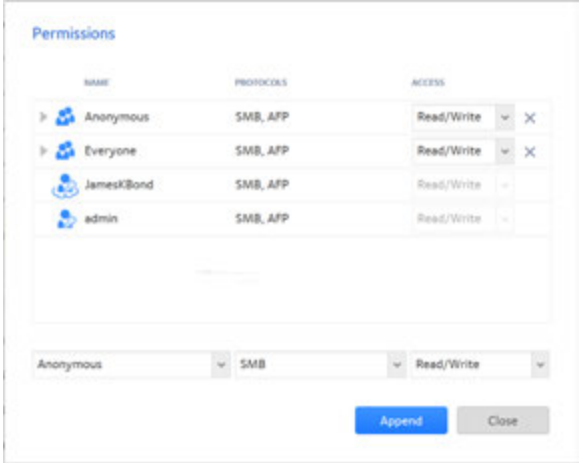
In addition to a way to set access rights for all protocols including advanced settings, the admin page provides a simplified way to set rights for the most commonly used networking protocols and settings.

The mostly commonly used networking protocols are SMB, AFP, FTP, and HTTP. Use this procedure as a simplified way to setting access rights for these protocols.

To set the network access rights for a shared folder:

1. Log in to the admin page.
2. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Hover over the shared folder that you want to configure.

4. Click the plus icon for the folder.



5. Adjust the settings as needed.

   - To adjust existing permissions for a user or group, use the **Access** menu for that user and select the new access level. You can click on the **arrow** icon by a user or group name to expand the list, if there are multiple protocols set for the user or group.
   - To remove permissions for a user or group, click the **X** icon for that user or group.
   - To add additional permissions, use the menus at the bottom of the window to specify the user, the protocol, and the access level, and click the **Append** button.

6. Click the **Close** button.
   Your changes are saved and the window closes.

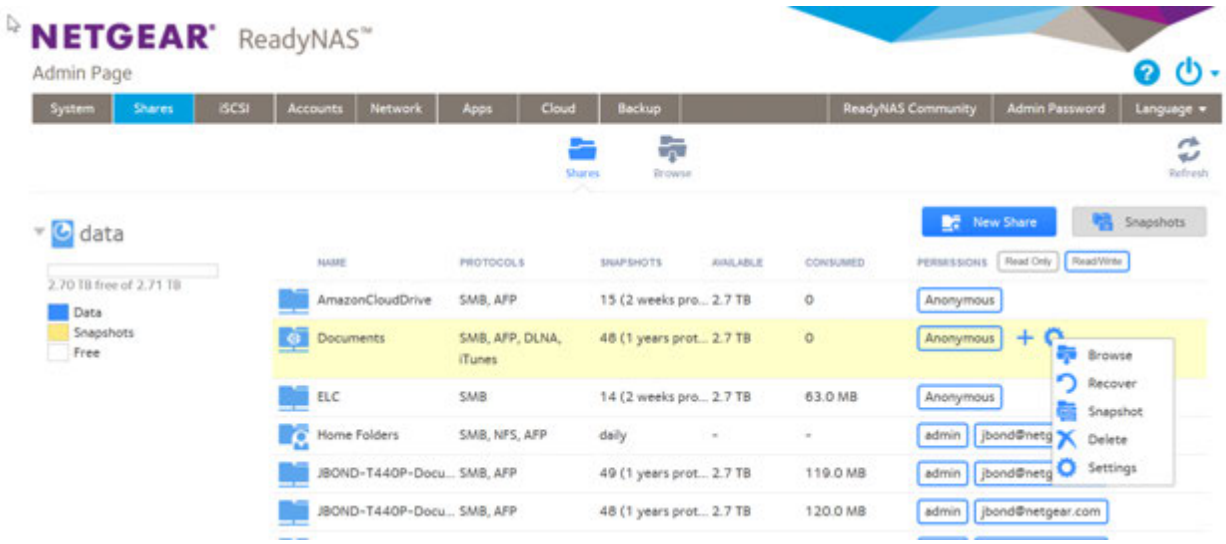
Set Network Access Rights to Shared Folders

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.

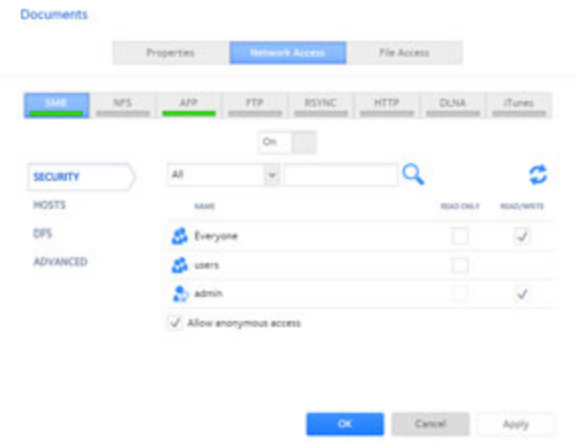
To set the network access rights for a shared folder:

1. Log in to your ReadyNAS.
2. 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. Click the **gear** icon for the folder.



5. Click the **Settings** button in the pop-up menu.
The shared folder settings display in a pop-up window.
6. Click the **Network Access** tab.



7. Click one of the file-sharing protocol buttons.
The page adjusts to display the access properties for the selected protocol.
8. 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 63.
   - *Configure Host Settings* on page 65.
   - *Configure Rsync Credentials* on page 67.
   - *Manage Access to Remote Shared Folders* on page 68.
   - *Hide a Shared Folder* on page 70.

9. 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 180.

- 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 180.

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

Configure User and Group Settings

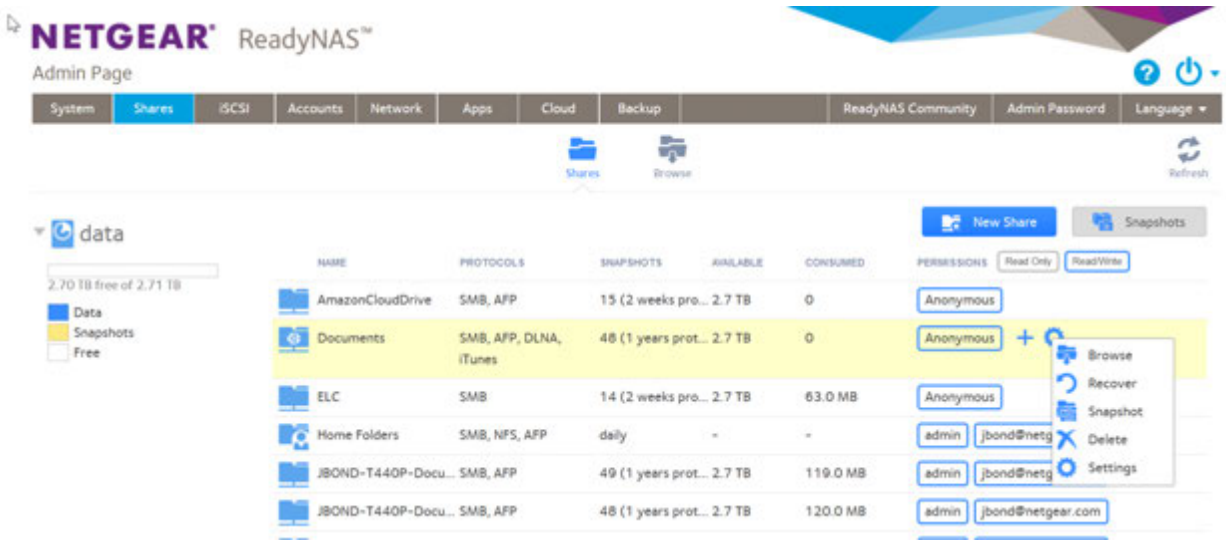
For SMB, AFP, FTP, and HTTP, you can configure access rights to an individual shared folder for users and groups. User and group settings do not apply to NFS and Rsync.

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 138.

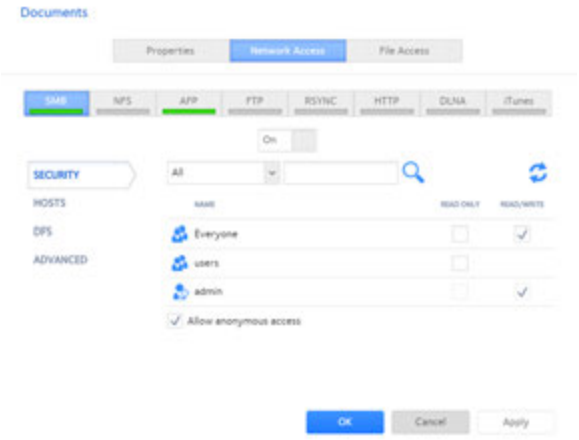
To configure user and group network access settings:

1. Log in to your ReadyNAS.
2. 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. Click the **gear** icon for the folder.



5. Click the **Settings** button in the pop-up menu.
   The shared folder settings display in a pop-up window.
6. Click the **Network Access** tab.



7. Select one of the file-sharing protocol buttons.
   The page adjusts to display the access properties for the selected protocol.
8. Click the **Security** tab on the left side of the pop-up window.
9. From the menu, 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 125.

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 ( ).

10. For each individual user ( ) and group ( ) that you want to allow 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.

11. (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.
12. (Optional for AFP) Configure the ReadyNAS system to override the Mac OS X settings.

    a. Click the **Advanced** tab.
    The page adjusts to show the AFP advanced settings.

    b. Select the **Automatic Permissions** check box and set the permissions for folder and file creation rights for

13. Click the **Apply** button.
14. Click **OK** button.
    Your settings are saved and the pop-up window closes.

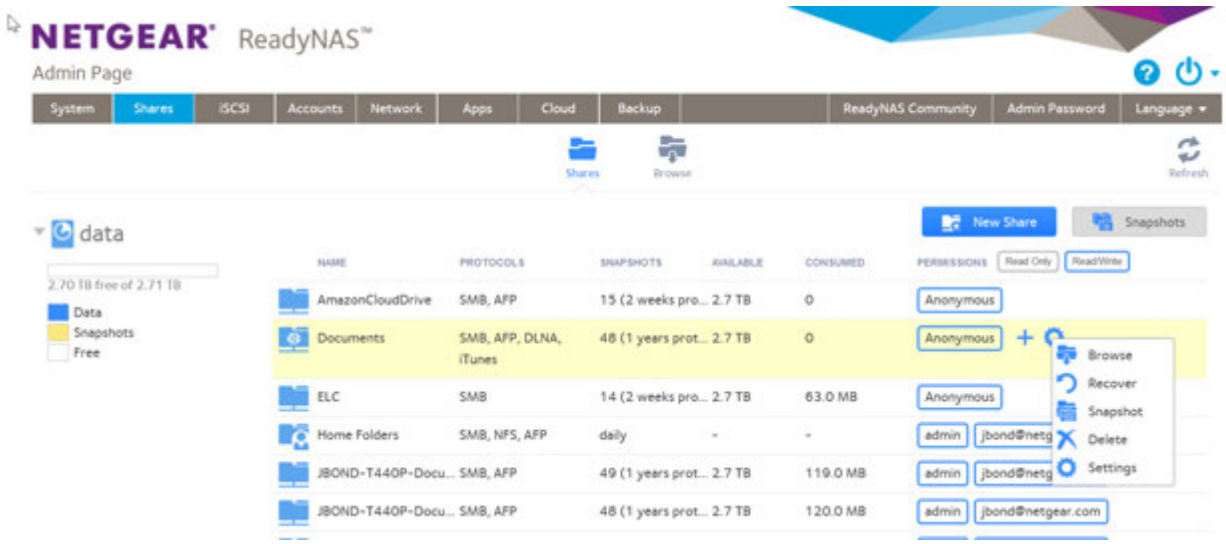
Configure Host Settings

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.

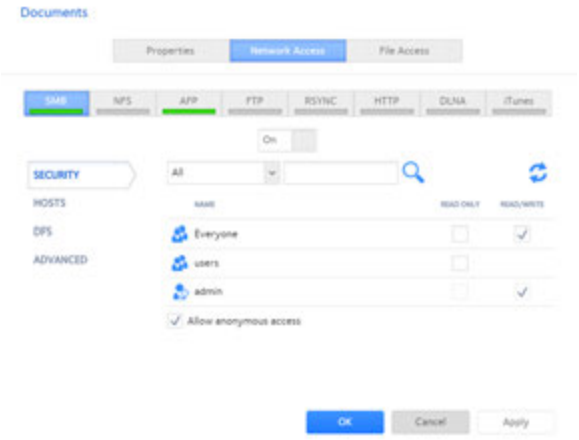
To add a host and configure host access settings:

1. Log in to your ReadyNAS.
2. 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. Click the **gear** icon for the folder.



5. Click the **Settings** button in the pop-up menu.
   The shared folder settings display in a pop-up window.
6. Click the **Network Access** tab.



7. Click one of the file-sharing protocol buttons.
   The page adjusts to display the access properties for the selected protocol.
8. Click the **Hosts** tab on the left side of the pop-up window.

> **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.

9. Click the **+** button.
   The Add Host pop-up window opens.
10. Enter the host IP address in the **IP address** field.
11. 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.

12. (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.

13. (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.

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

Configure Rsync Credentials

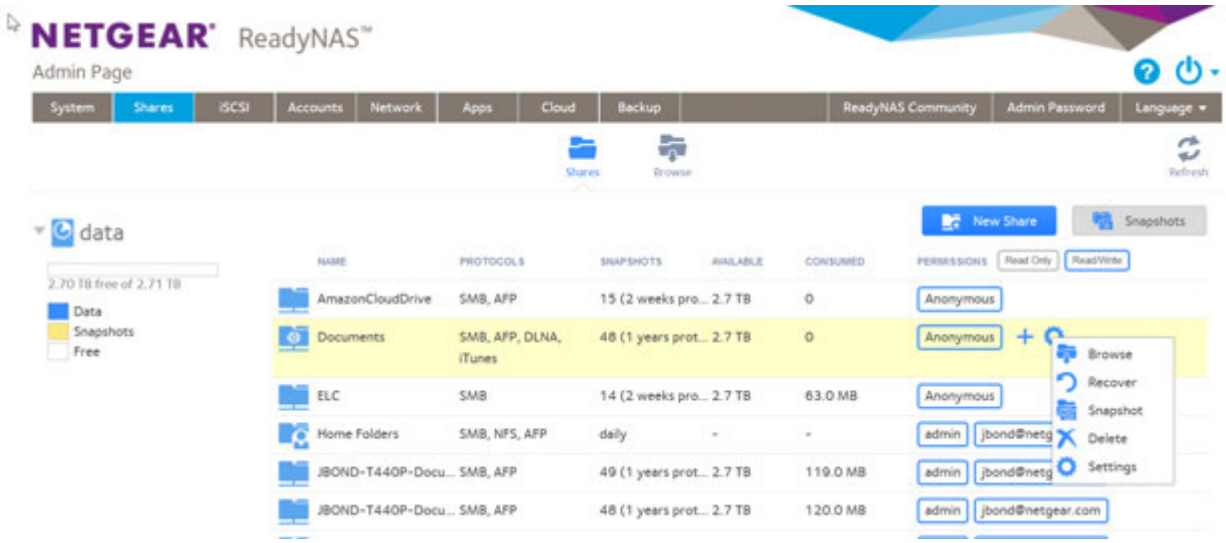
You can grant Rsync access to a ReadyNAS system in two ways: Rsync over SSH, or through the use of user credentials, an account and password. You can require users to enter Rsync credentials when accessing your storage system using Rsync.

Note Although the use of Rsync over SSH can be useful, particularly for remote backups, enabling SSH on your ReadyNAS system increases your security concerns. If you enable SSH root access, NETGEAR might deny you technical support. For information about using Rsync and SSH for remote backups, see *Create a Backup Job* on page 232 and *Configure Advanced Rsync Job Settings* on page 243.

To require credentials for Rsync sessions:

1. Log in to the ReadyNAS.
2. 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. Click the **gear** icon for the folder.



5. Click the **Settings** button in the pop-up menu.
   The shared folder settings display in a pop-up window.
6. In the folder settings pop-up window, click the **Network Access** tab.
7. Click the **RSYNC** file-sharing protocol button.
   The page adjusts.
8. Click the **Security** tab on the left side of the pop-up window.
9. Select the **Enable Password Protection** check box.
10. 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.

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

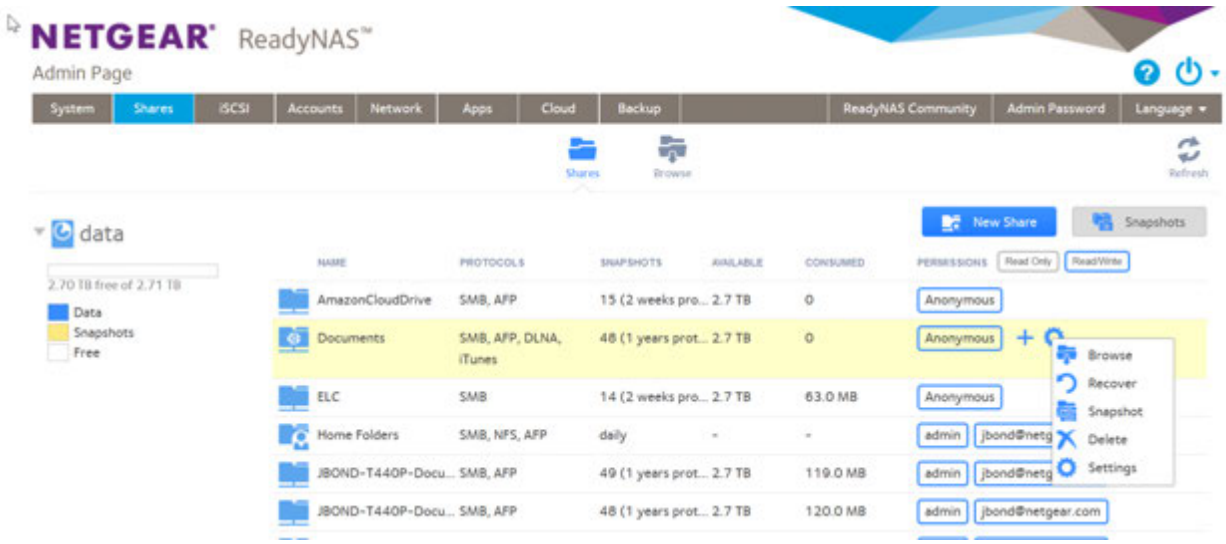
Manage Access to Remote Shared Folders

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.

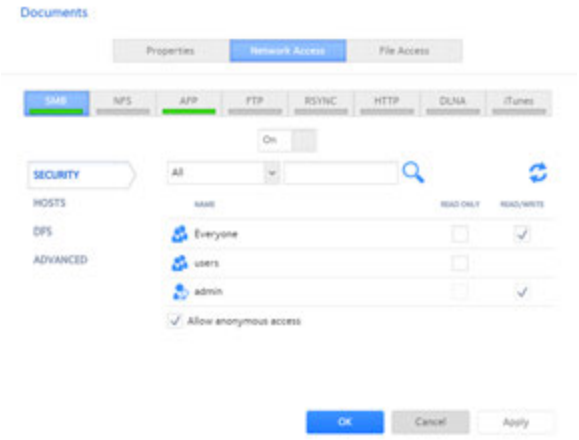
To enable access to a remote shared folder:

1. Log in to the ReadyNAS.
2. 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. Click the **gear** icon for the folder.



5. Click the **Settings** button in the pop-up menu.
   The shared folder settings display in a pop-up window.
6. Click the **Network Access** tab.



7. Click the **SMB** file-sharing protocol button.
   The window adjusts.
8. Select the **DFS** tab button on the left side of the pop-up window.
9. Select the **Enable DFS Root** check box.
10. Click the **+** button above the list of remote shared folders.
    The New External Folder page opens.
11. 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 Folder**. The name of the remote shared folder, as it appears on the network-attached device.

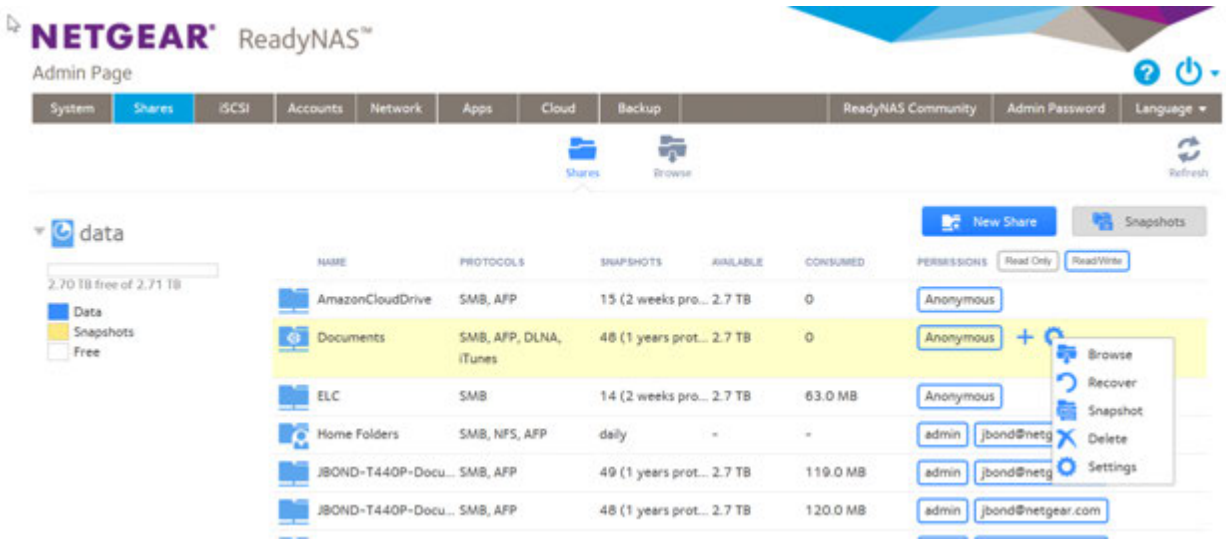
12. Click the **Add** button.
    The new remote shared folder appears on the list.
13. Click the **Apply** button.
14. Click the **OK** button.
    Your settings are saved and the pop-up window closes.
15. Make sure that the remote shared folder on the network-attached device is configured for file 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 78 or *Use a Mac OS X Device* on page 79.

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.

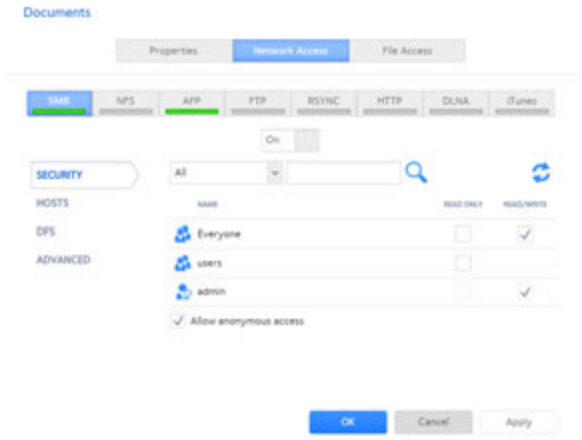
To configure advanced settings for SMB:

1. Log in to your ReadyNAS.
2. 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. Click the **gear** icon for the folder.



5. Click the **Settings** button in the pop-up menu.
   The shared folder settings display in a pop-up window.

6. Click the **Network Access** tab.



7. Click the **SMB** file-sharing protocol button.
   The page adjusts.
8. Click the **Advanced** tab on the left side of the pop-up window.
9. Select the **Hide this folder** check box.
10. Click the **Apply** button.
11. Click the **OK** button.
    Your settings are saved and the pop-up window closes.

Enable WebDAV

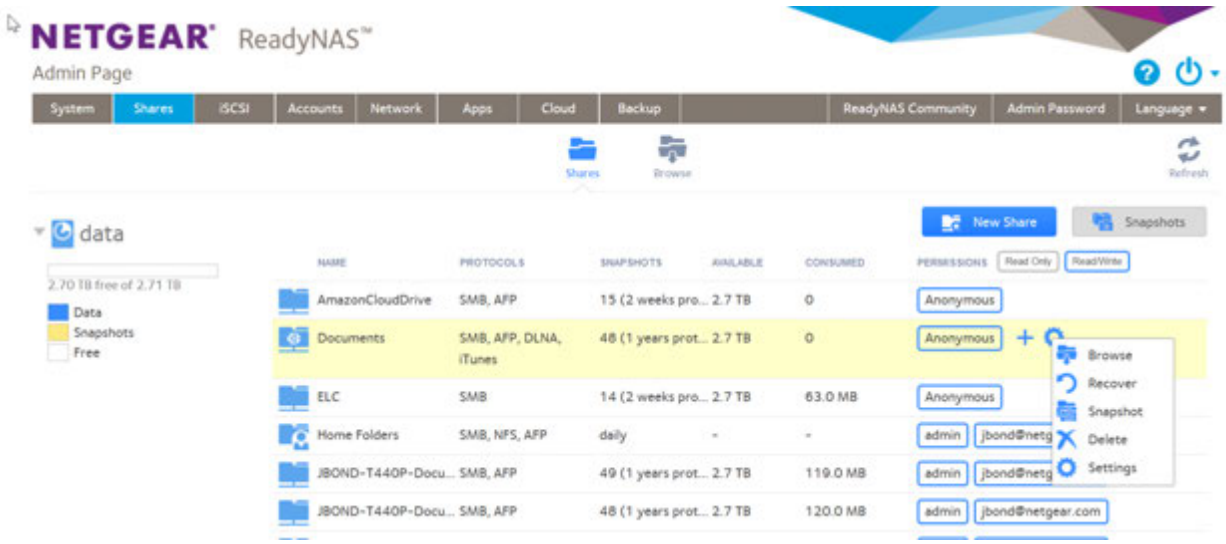
This feature is available only for HTTP and HTTPS. WebDAV is an extension of the HTTP and HTTPS protocols that facilitates document management and editing. Features of WebDAV include maintenance of document properties such as author, creation date, and modification date, and it provides overwrite protection. 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.

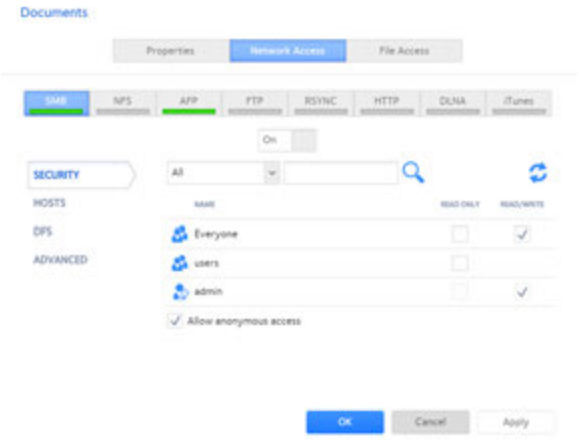
To enable WebDAV on an individual shared folder:

1. Log in to your ReadyNAS.
2. 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. Click the **gear** icon for the folder.



5. Click the **Settings** button in the pop-up menu.
   The shared folder settings display in a pop-up window.
6. Click the **Network Access** tab.



7. Click the **HTTP** file-sharing protocol button.

Note Enabling HTTP at the share level also enables HTTPS access.

   The page adjusts.
8. Click the **Off** button, if HTTP is off.
   The button changes to **On**.
9. Click the **WEBDAV** tab on the left side of the pop-up window.
   The window adjusts.
10. Select the **Enable WebDAV** check box.
11. Click the **Apply** button.

Your change is saved and the window returns to the **Security** window.

12. Click the **OK** button.
    Your settings are saved and the pop-up window closes.

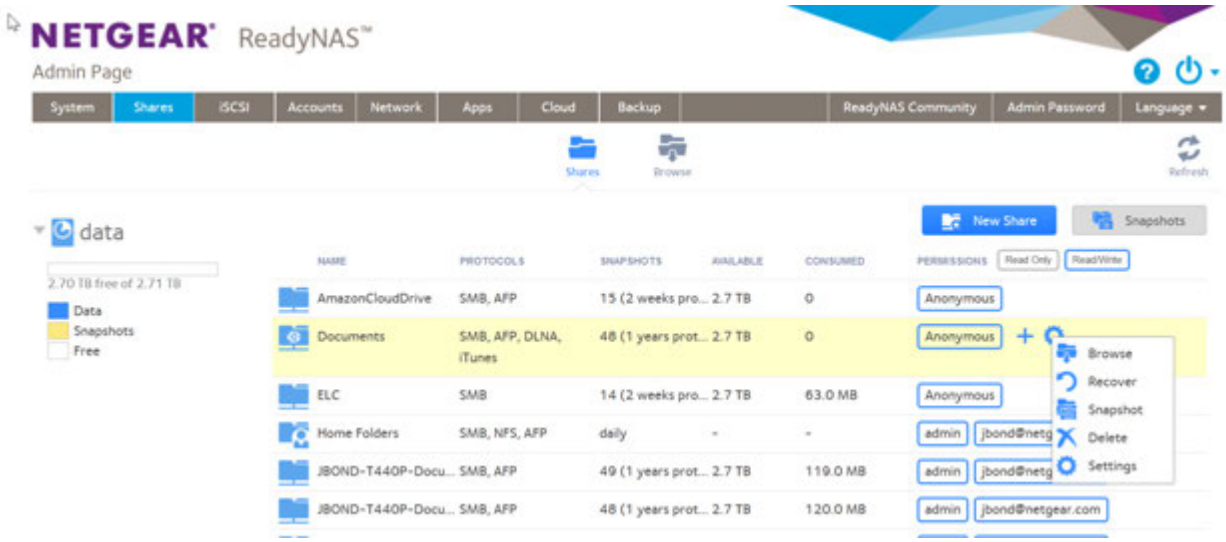
Squash, Map, Host IDs to ReadyNAS IDs

Sometimes it is useful to map user IDs or group IDs on a host connected over NFS to your ReadyNAS system to specific ReadyNAS OS user IDs and group IDs. For example, if the ReadyNAS is used to store VMs for a host, you might want to map (squash) all of the host UIDs and GIDs to a specific ReadyNAS UID and GID.

When a host system is running virtualization software, it is common to configure host UIDs and GIDs to the UID and GID for the anonymous user. Because there is no default anonymous user on a ReadyNAS, when you map UIDs and GIDs, you must also define the UID and GID for anonymous.

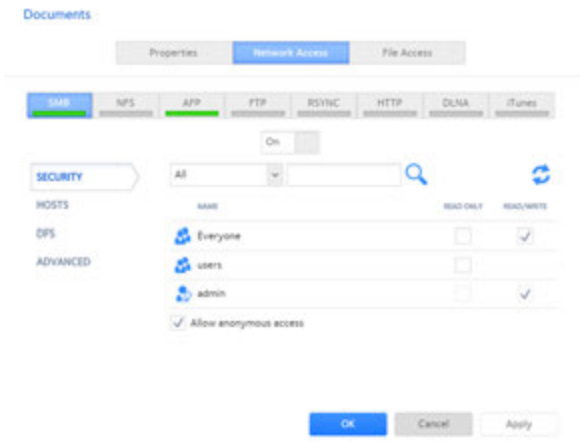
To map IDs to the anonymous IDs and define the anonymous IDs:

1. Log in to your ReadyNAS.
   A list of shared folders and LUNs on each volume displays.
2. Select the shared folder that you want to configure.
3. Click the **gear** icon for the folder.

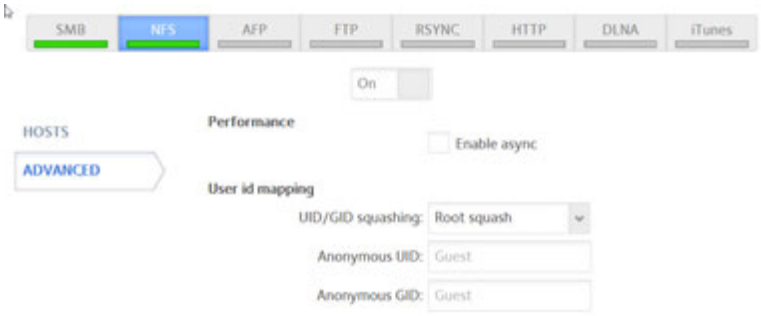


4. Click the **Settings** button in the pop-up menu.
   The shared folder settings display in a pop-up window.

5. Click the **Network Access** tab.



6. Click the NFS file sharing button.
   The page adjust to display the NFS access properties.
7. Click the **Advanced** button.



8. From the **UID/GID squashing** menu, one of the following: **No root squash**, **Root squash**, **All squash**.
   No root squash sets the ReadyNAS to not remap UIDs or GIDs. Root squash sets the host root UID and GID to anonymous, but otherwise does not remap. All squash maps all host UIDs and GIDs to the anonymous UID and GUID.
9. Enter the UID value you choose for the anonymous UID and the GID you choose for the anonymous GID.
10. Click the **OK** button.
    The window closes and squashing starts immediately.

Set Up Access Rights to Files and Folders

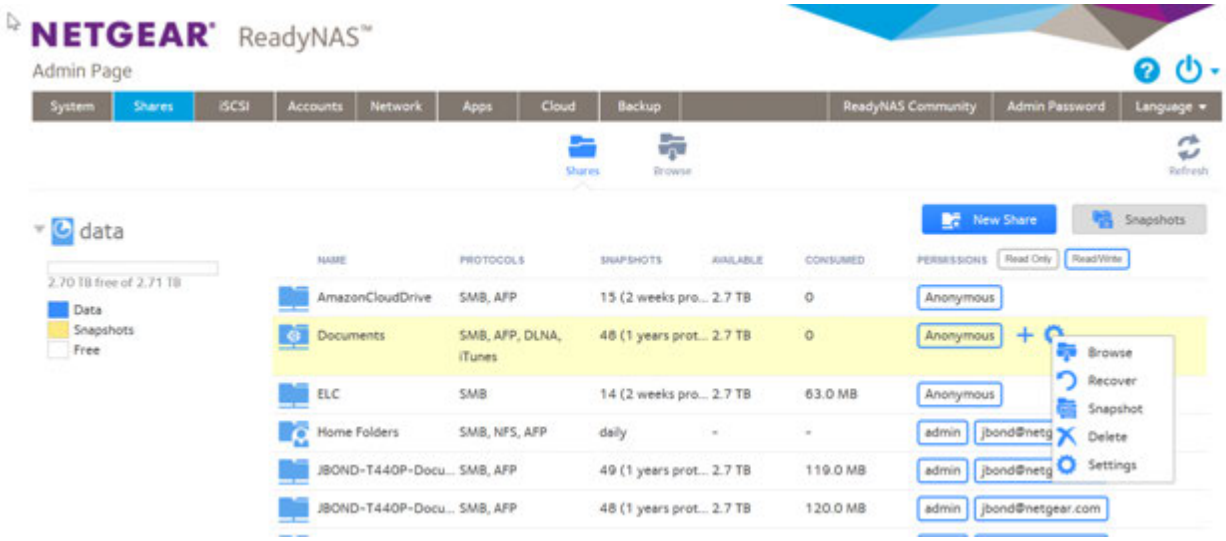
For each individual shared folder, you can configure the default access rights to files and folders.

Change Default Access Rights to Files and Folders

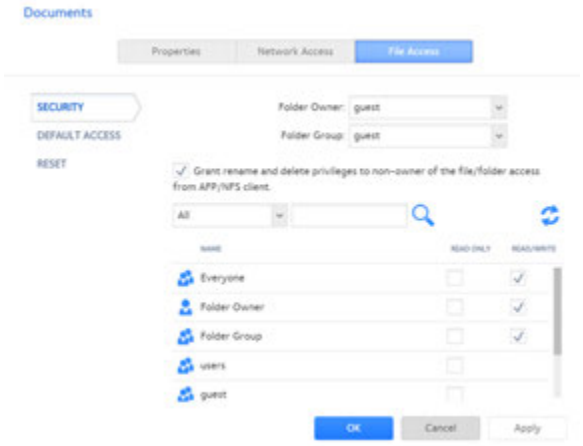
By default, owners, groups, and anyone else with access to the shared folder is granted read/write access to all files and folders on the shared folder.

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.
3. Click the **gear** icon for the folder.



4. In the pop-up menu, click the **Settings** button.
   The shared folder settings pop-up window opens.
5. Click the **File Access** tab in the window.



6. 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.

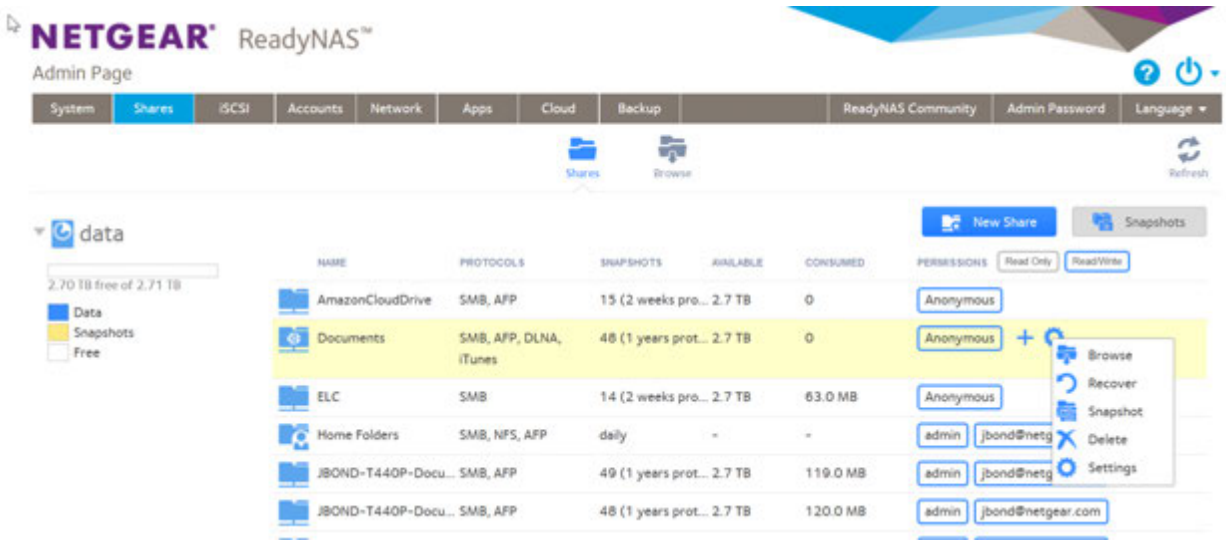
(Continued)

Item	Setting
Folder Owner Rights	Permissions granted to the folder owner. Select one of the check boxes: • **No box selected**. The folder owner is not granted access rights to the folder. • **Read Only**. The folder owner ia granted read-only access to the folder. • **Read/Write**. The folder owner is granted 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 are not granted access to folders that are owned by a member of the group. • **Read Only**. Members of the group are granted read-only access to folders that are owned by a member of the group. • **Read/Write**. Members of the group are granted 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 is granted access rights to the folder. • **Read Only**. Anyone outside folder group is granted read-only access to the folder. • **Read/Write**. Anyone outside the folder group is granted read/write access to the folder. This is the default setting.

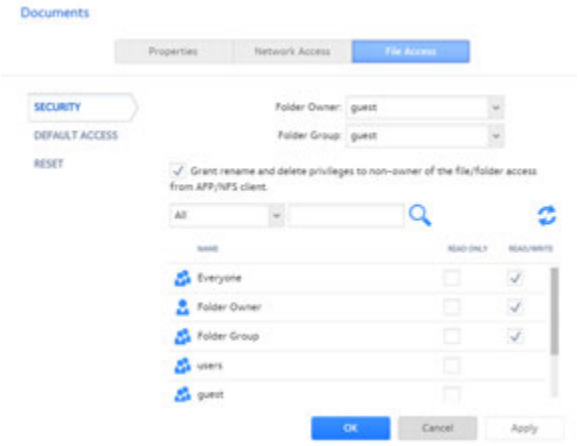
To restore the default file and folder access rights on an individual shared folder:

1. Log in to the ReadyNAS.
2. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder.

4. Click the **gear** icon for the folder.



5. In the pop-up menu, click the **Settings** button.
   The shared folder settings pop-up window opens.
6. Click the **File Access** tab in the window.



7. Click the **Reset** tab.
8. 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 59).

Note For snapshots to be accessible to users from their network-attached devices, you must select the **Allow snapshot access** check box on the shared folder settings window. For more information, see *View and Change the Properties of a Shared Folder* on page 54.

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 61.
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 Explorer 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 on 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 61.
2. Enter \\<hostname> in the File 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 File Explorer 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.

   Note SMB is recommended for mixed-platform environments.

   For more information, see *Set Network Access Rights to Shared Folders* on page 61.
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 61.
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 system.
   - <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 61.
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 61.
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 61.
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 61. 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.

Search Files

4

From the local admin page, you can search the files on your ReadyNAS system for file name, content, file type, file extension, size, and dates. If your ReadyNAS system is attached to a Mac, you can also use the Finder to search the files on the ReadyNAS.

- *Use the Mac Finder to Search Files*

Use the Mac Finder to Search Files

If your ReadyNAS system is connected to a Mac, you can use the Mac Finder to search the files on the ReadyNAS. If the ReadyNAS uses the SMB protocol with the Mac (the most common way), you must first set an SMB option.

To configure SMB to work with the Mac Finder:

1. Log in to the ReadyNAS system.
2. Select **System > Settings**.
   The page updates showing the system settings.
3. Click the **SMB** button.
   The SMB Settings window opens.
4. Select the **Enhance MacOS** check box.
5. Click the **Apply** button.
   The SMB Settings window closes.

You can now search the files on your ReadyNAS using the Mac Finder.

LUNs

5

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 33.

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 7. Thin LUN

Figure 8. 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 We recommend 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. The defaults depending on whether the LUN is thick provisioned (the default), or you select thin provisioned.

Table 6. LUN default settings

Item	Default (Thick Provision)	Default (Thin Provision)
Bit Rot Protection (Copy-on-write)	Disabled	Disabled
Compression	Disabled	Disabled
Snapshot Schedule	Never	Never
Sync Writes	Allowed	Allowed

Manage LUNs

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

Create a LUN

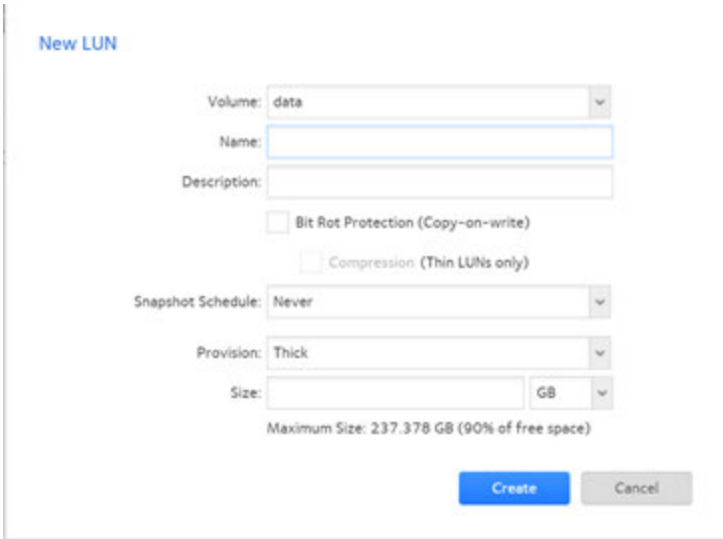
After you create a volume (see *Create and Encrypt a Volume* on page 33), you can create LUNs on that volume.

Note On ReadyNAS 102, 104, 202, 204, 212, 214, and 2120 systems, individual LUNs cannot exceed 8 TB.

To create a LUN:

1. Log in to your ReadyNAS.
2. Select **iSCSI**.
   A list of shared folders and LUNs on each volume displays.

3. Click the **New LUN** button.



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

Item	Description
Volume	The name of the volume on which the LUN resides.
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.
Bit Rot Protection (Copy-on-write)	Select the Bit Rot Protection (Copy-on-write) check box to enable bit-rot protection. For information, see *Bit Rot Protection* on page 51. Enabling bit rot protection also enables copy-on-write. Over time, copy-on-write increases disk fragmentation.
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.
Snapshot Schedule	Select from the **Snapshot Schedule** menu to enable data protection through snapshots and configure how often snapshots are taken. • **Never.** Snapshots are not taken. • **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. For more information about snapshots, see *Chapter 5, Snapshots* on page 111.

(Continued)

Item	Description	
Provision	Select how storage space is provisioned. Make a selection from the menu: • **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** We recommend that you do not use an overallocated thin LUN for storage of critical data. Instead, use a thick LUN.	
Size	Specify the size of the LUN. The maximum size that you can allocate to the LUN is stated at the bottom of the window.	
	Unit	Select the unit of measurement from the menu: • **MB**. • **GB**. This is the default unit of measurement. • **TB**.

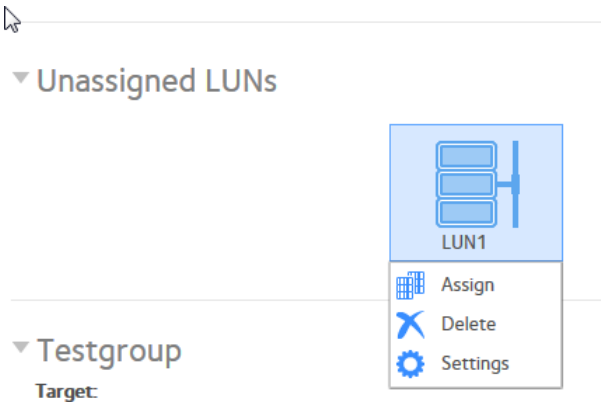
5. Click the **Create** button.
   The ReadyNAS confirms the creation of a LUN with the message “Folder or LUN successfully created.”
6. Click the **OK** button.
   The new LUN is added to the Shares page. Basic information is displayed to the right of the LUN.

View and Change the Properties of a LUN

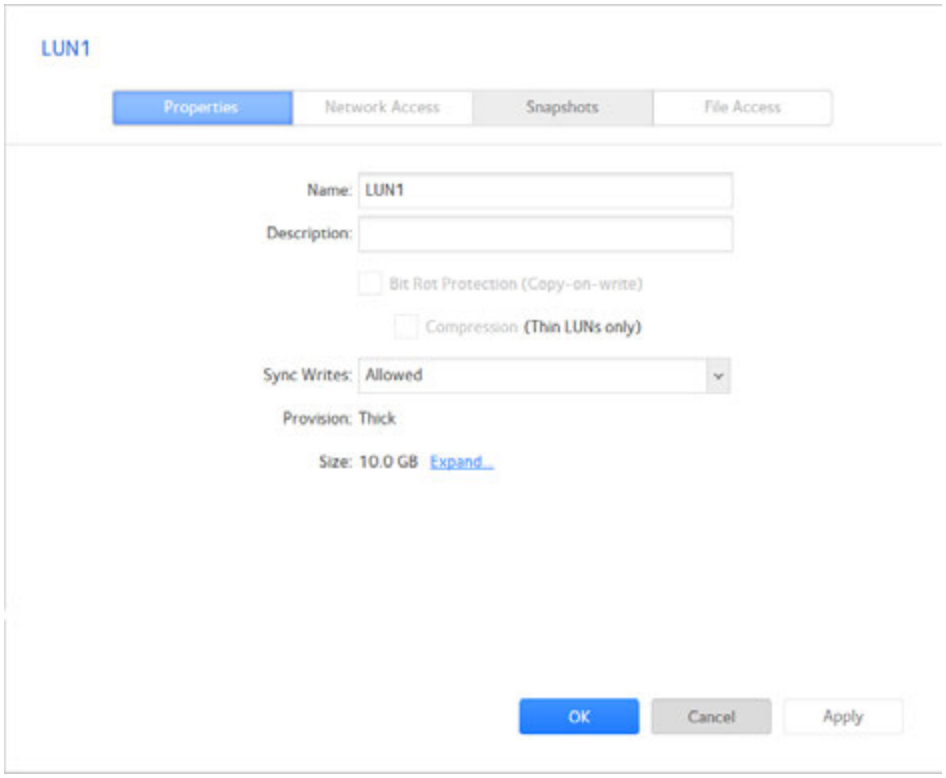
To view and change the properties of a LUN:

1. Log in to your ReadyNAS.
2. Select **iSCSI** .
   The screen updates showing the iSCSI LUNs and groups.

3. Select the LUN.



4. In the pop-up menu, click the **Settings** button.



5. View or 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.
Bit Rot Protection	Select the **Bit Rot Protection (Copy-on-write)** check box to enable bit rot protection. For information, see *Bit Rot Protection* on page 51. Bit rot protection can be set only when the LUN is created.

(Continued)

Item	Description
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. Compression can be set or turned off only when the LUN is created.
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 90.

6. Click the **Apply** button.
7. Click the **OK** button.
   Your settings are saved and the window closes.

For information about how to set access right for a LUN, see *LUN Groups and Access Rights* on page 93.

For more information about snapshots, see *Chapter 5, Snapshots* on page 111 .

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 93).

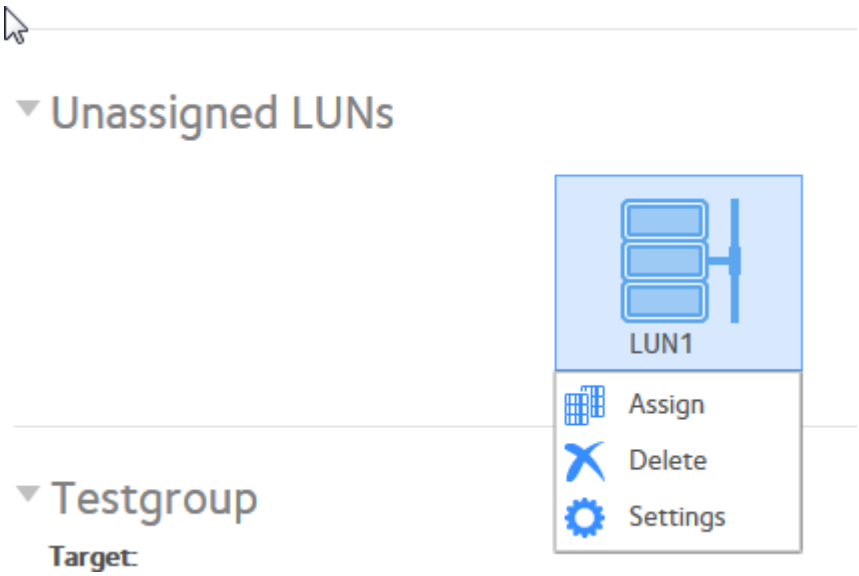
Note On ReadyNAS 102, 104, 202, 204, 212, 214, and 2120 systems, individual LUNs cannot exceed 8 TB.

Note File systems inside the LUN are not expanded by this procedure. After expanding the LUN, you can expand the file systems from the iSCSI initiator.

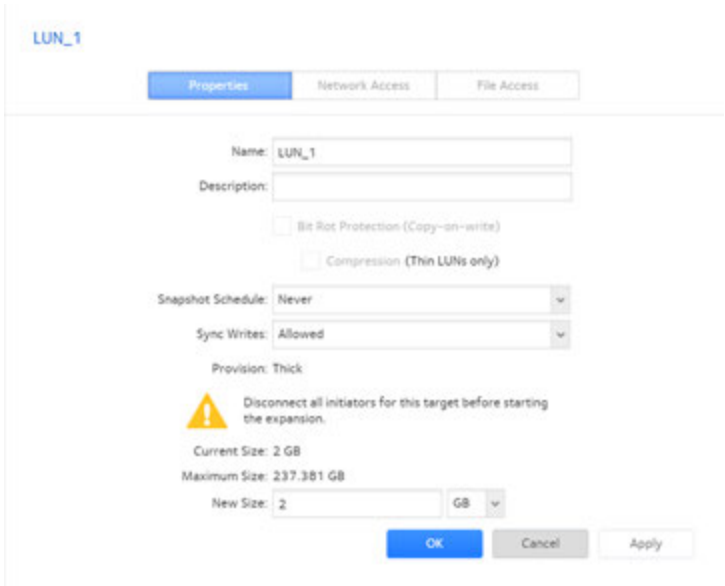
To expand the size of a LUN:

1. Log in to your ReadyNAS.
2. Select **iSCSI**.
   The screen updates showing the iSCSI LUNs and groups.

3. Select the LUN.



4. In the pop-up menu, click the **Settings** button.
   The LUN settings display in a pop-up window.
5. Click the **Expand** link.



6. 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**).

7. Click the **Apply** button.
   The new LUN size takes effect.

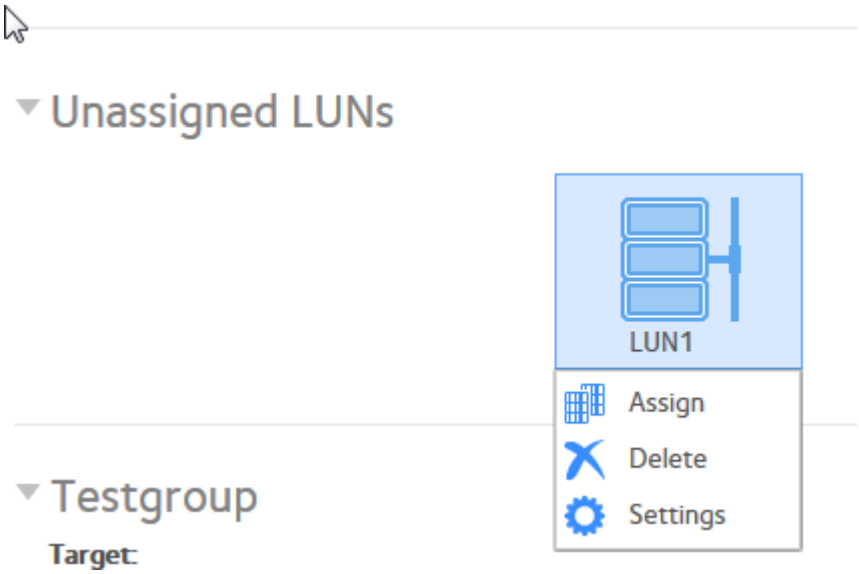
8. Click the **OK** button.
   Your settings are saved and the pop-up window closes.
9. (Optional) Add the LUN to the LUN group to which it belonged before the expansion.
   See *Create a LUN Group* on page 93.
   User access to the LUN is restored.

Delete a LUN

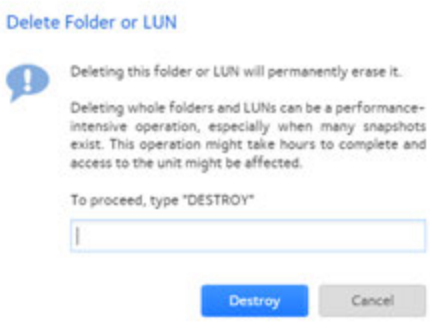
WARNING:
Deleting a LUN permanently removes the data within that LUN.

To delete a LUN from a volume:

1. Log in to your ReadyNAS.
2. Select **iSCSI**.
   The screen updates showing the iSCSI LUNs and groups.
3. Select the LUN.



4. In the pop-up menu, click the **Delete** button.



5. Confirm the deletion by typing **DESTROY**.
6. 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.

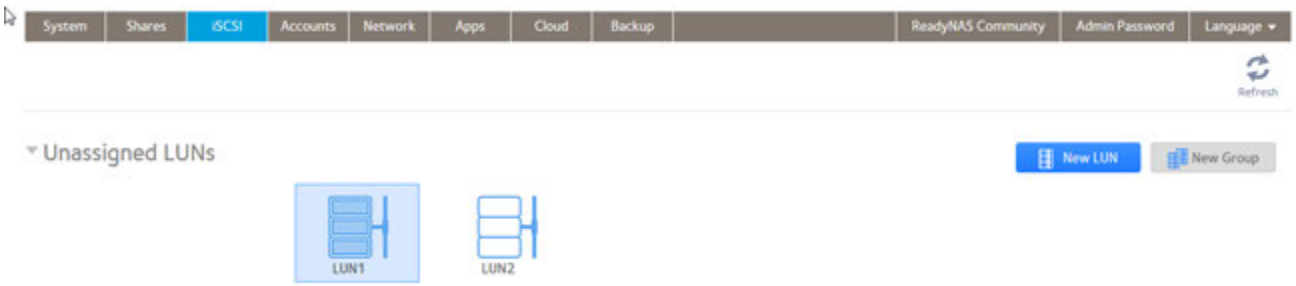
LUN groups allow you to organize LUNs and manage access rights to LUN groups. Access rights are either open or granted through internal CHAP authentication. Access rights apply to LUN groups, not to individual LUNs. You can easily assign a LUN to a LUN group or move a LUN from one LUN group to another LUN group.

Each LUN group is assigned 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 96. Each ReadyNAS supports a maximum of 256 iSCSI targets.

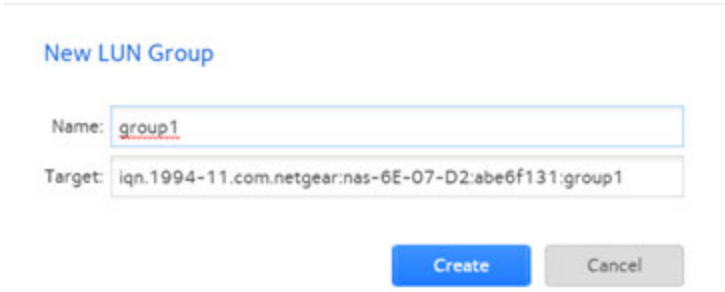
Create a LUN Group

To create a LUN group:

1. Log in to the ReadyNAS.
2. Select **iSCSI**.



3. Click the **New Group** button in the upper right of the window.



4. In the **Name** field, enter a name.
   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.

5. Click the **Create** button.
   The New LUN group is added to the iSCSI page.

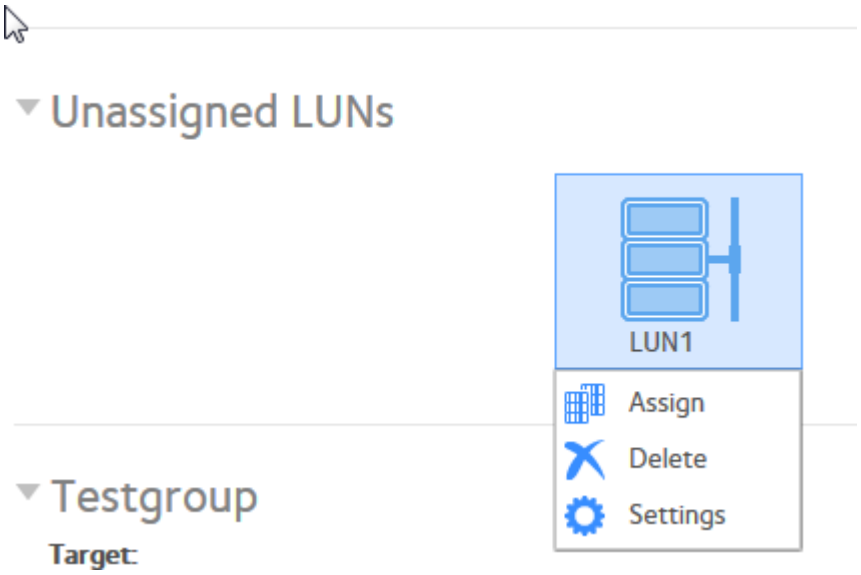
By default, CHAP is disabled and no client is allowed to access the LUN group (see *Manage Access Rights for LUN Groups* on page 96).

Assign a LUN to a LUN Group

To assign a LUN to a LUN group:

1. Log in to the ReadyNAS.
2. Select **iSCSI**.
   The iSCSI page displays the LUNs and LUN groups that you created.
   See *Create a LUN* on page 86.
3. 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.

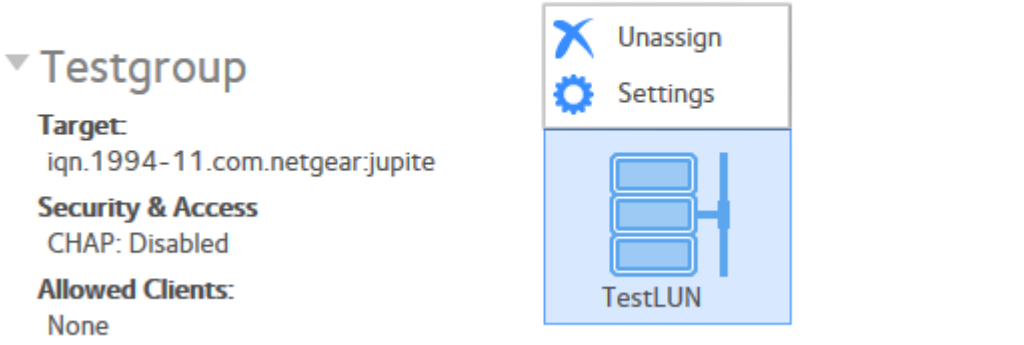


4. Click the **Assign** button.
   A pop-up window opens.
5. Select the LUN group to which you want to assign the LUN.
6. Click the **Apply** button.
   The LUN is assigned to the selected LUN group.

Remove a LUN From a LUN Group

To remove a LUN from a LUN group:

1. Log in to your ReadyNAS.
2. Select **iSCSI**.
   The iSCSI page displays the LUNs and LUN groups that you created.
3. Select the assigned LUN to remove from the group.

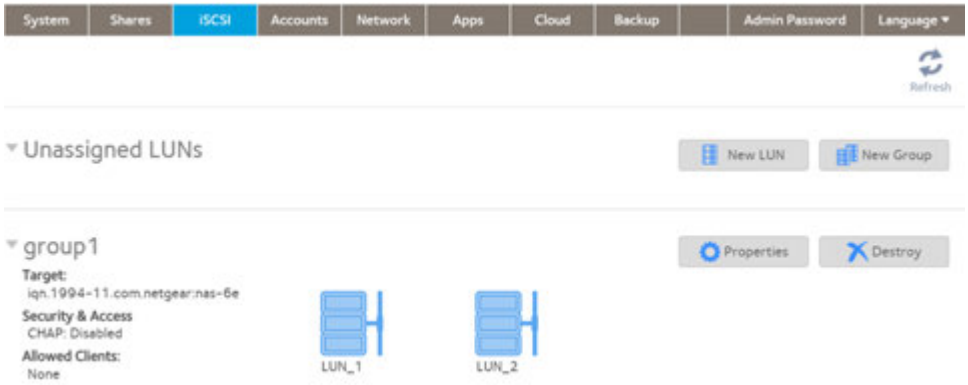


4. In the pop-up menu, click the **Unassign** button.
5. Confirm that you want to remove the LUN from the group.
   The LUN is returned to the unassigned state.

Delete a LUN Group

To delete a LUN group:

1. Log in to your ReadyNAS.
2. Select **iSCSI**.



3. Click the **Destroy** button to the right of the LUN group.
4. Confirm that you want to delete the LUN group.
   If any LUNs were assigned to the group, they are returned to the unassigned state.

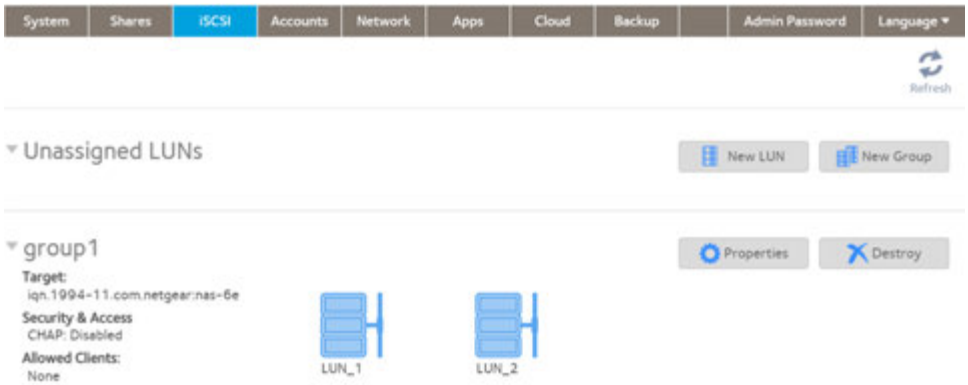
Manage Access Rights for LUN Groups

You can configure LUN group access, add and remove iSCSI initiators, and change the CHAP password for an iSCSI initiator.

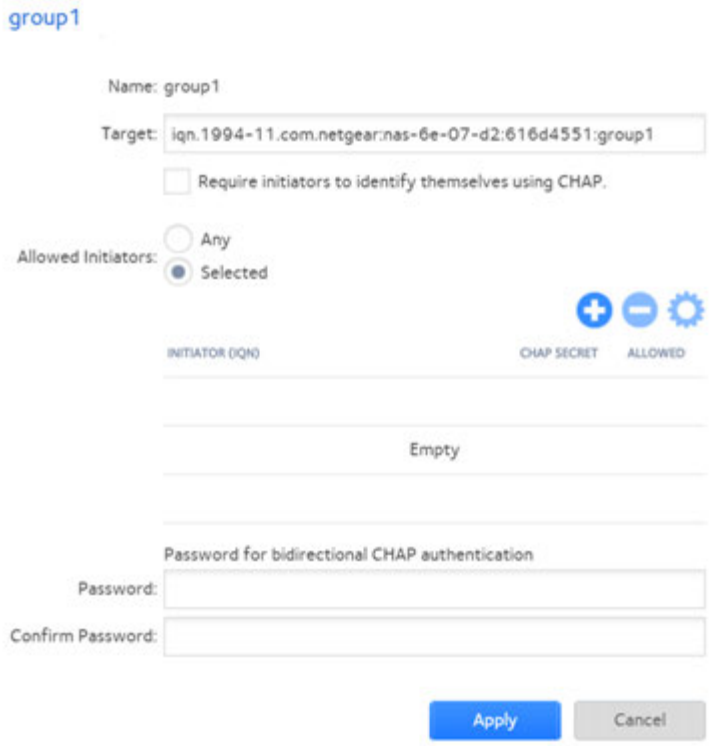
Configure Access to a LUN Group

To configure client access to a LUN group:

1. Log in to your ReadyNAS.
2. Select **iSCSI**.



3. Click the **Properties** button to the right of the LUN group.



4. 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 98).
Allowed Initiators	Select one of the following radio buttons: • **Any**. Access to the LUN group is granted to all initiators with information about the target address. (If CHAP authentication is enabled, access depends on CHAP authentication.) • **Selected**. Access to the LUN group is granted to iSCSI qualified names (IQNs) only. (If CHAP authentication is enabled, access depends on CHAP authentication.) For more information about configuring iSCSI initiators, see the following sections: • *Add an iSCSI Initiator* on page 98 • *Remove an iSCSI Initiator* on page 100 • *Edit the CHAP Password* on page 101

(Continued)

Item	Description	
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.

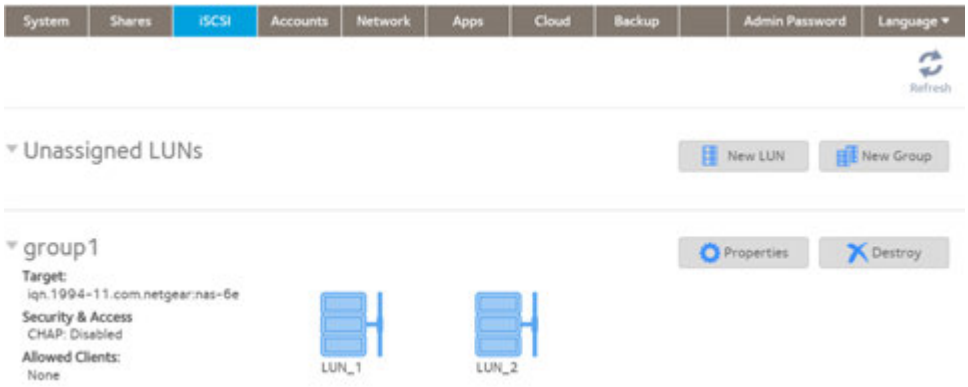
5. Click the **Apply** button.
   The new LUN group properties take effect immediately.

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 102.

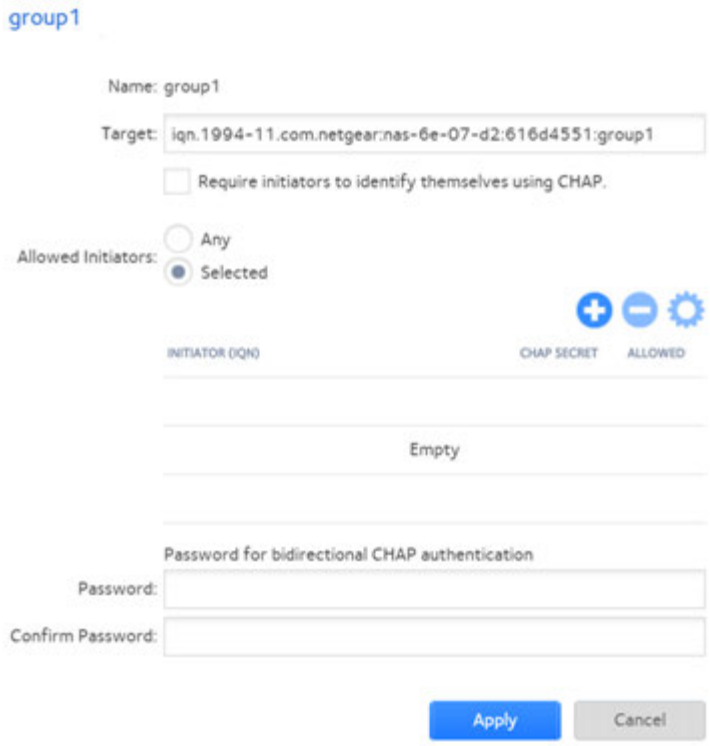
Add an iSCSI Initiator

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

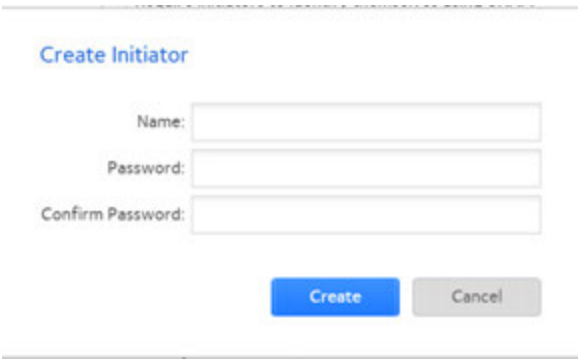
1. Log in to your ReadyNAS.
2. Select **iSCSI**.



3. Click the **Properties** button to the right of the LUN group.



4. Select the **Selected** radio button next to Allowed Initiators.
5. Click the **+** button ( ) to the right of the list of initiators.



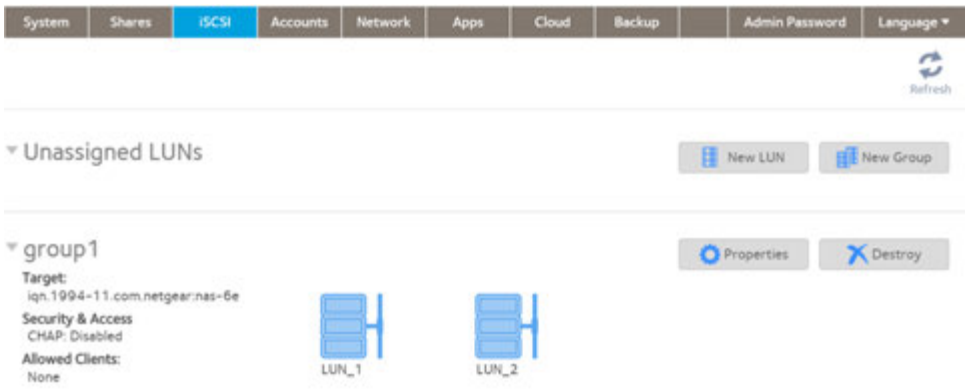
6. In the **Name** field, enter an IQN in the format as defined by *RFC 3720*, for example, iqn.2012-04.com.netgear:sj-tst-5200:a123b456 is a valid IQN.
7. (Optional) Enter a CHAP password that is between 12 and 16 characters long and confirm the CHAP password.
8. Click the **Create** button.

9. Select the **Allowed** check box to allow the initiator access to the LUN group.
10. 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. Log in to your ReadyNAS.
2. Select **iSCSI**.



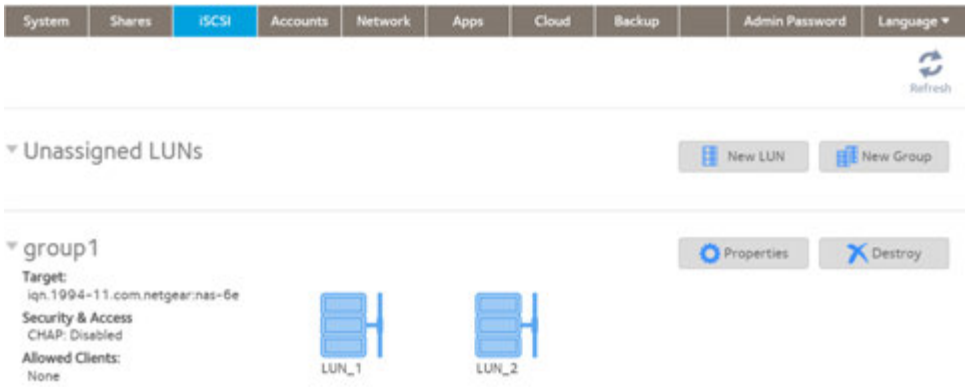
3. Click the **Properties** button to the right of the LUN group to manage.

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

Edit the CHAP Password

To edit the CHAP password for an iSCSI initiator:

1. Log in to your ReadyNAS.
2. Select **iSCSI**.



3. Click the **Properties** button to the right of the LUN group to manage.

4. Select the **Selected** radio button next to Allowed Initiators.
5. Select the initiator that you want to edit.
6. Click the **gear** button (⚙) to the right of the list of initiators.
   The Initiator Settings pop-up window opens.
7. Enter a new password in the fields.
8. Click the **Apply** button in the Initiator Settings pop-up window.
9. Click the **Apply** button in the LUN group properties window.
   Your settings 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 can access 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 122.

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 103.
2. Initialize and format LUNs in the LUN group.
   See *Initialize and Format LUNs* on page 108.

Set Up Initiator Access

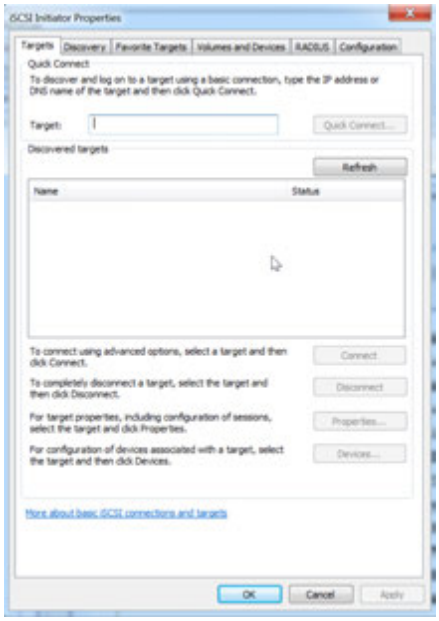
The following procedure uses the Microsoft iSCSI Software Initiator, which is freely available online and is integrated in Windows 7 and later.

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

Note Some of the steps in this procedure require that the Windows iSCSI service is running. If it is not, when you open the iSCSI initiator, Windows asks if you want it started.

To set up initiator access:

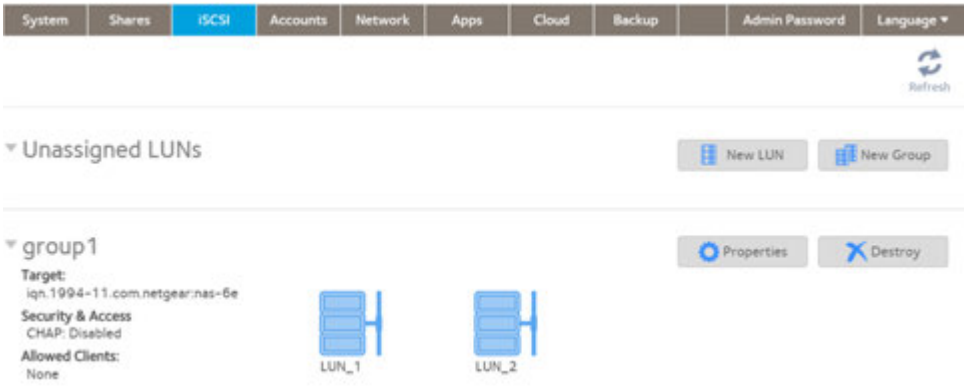
1. Open the iSCSI initiator and click the **Configuration** tab.
2. Copy the default name from the **Initiator Name** field.



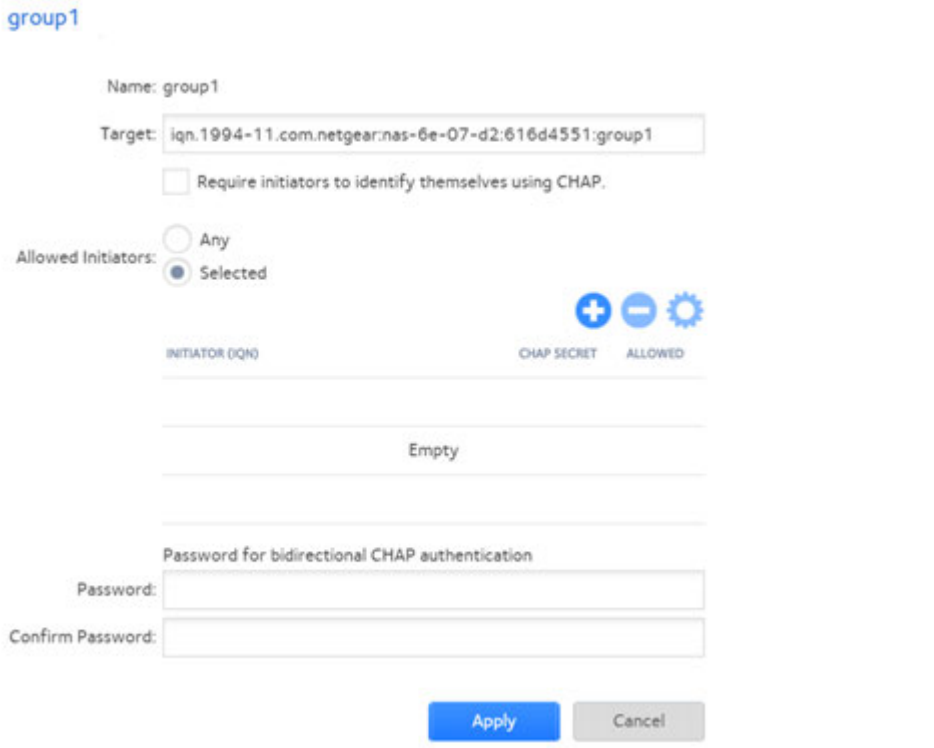
3. Create an iSCSi initiator on the ReadyNAS:

a. Log in to your ReadyNAS.

b. Select **iSCSI**.

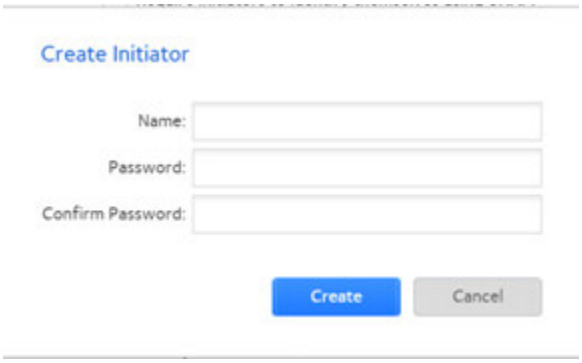


c. Click the **Properties** button to the right of the LUN group.



d. Select the **Selected** radio button.

e. Click the **+** button to the right of the list of initiators.



f. 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 103.

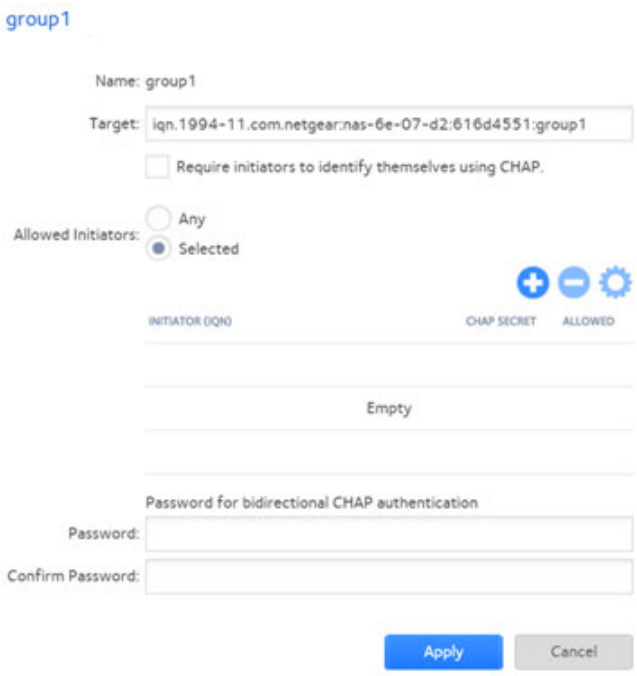
g. (Optional) Enter a CHAP password that is between 12 and 16 characters long and confirm the CHAP password.

h. Click the **Create** button.
The IQN is added to the table on the LUN group properties window.

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 103.
The initiator is allowed to access the LUN group.

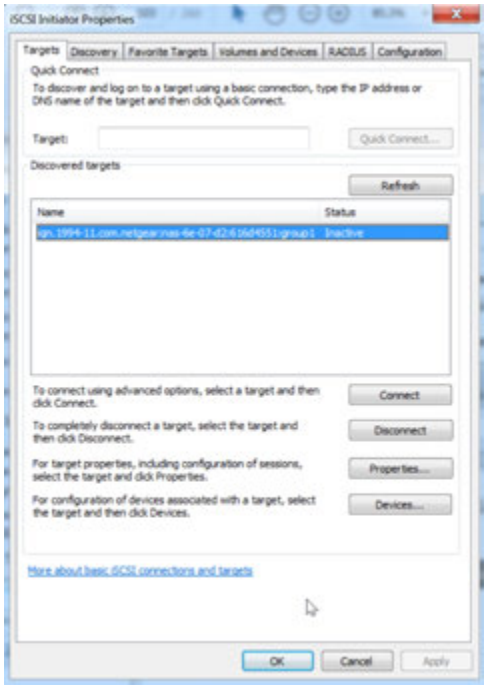


b. (Optional) Select the **Require initiators to identify themselves using CHAP** check box.
Selecting this check box allows only authenticated initiators to access LUNs in the LUN group. To gain access, initiators must provide the CHAP password that you created in *Step 3* on page 105.

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

5. On the iSCSI Initiator Properties page, click the **Targets** tab.

6. In the **Target** field, enter the IP address of the ReadyNAS.
7. Click the **Quick Connect** button.



8. If you selected the **Require initiators to identify themselves using CHAP** check box in *Step 4* on page 106, authenticate the connection.
   The initiator connects to the LUN group on the ReadyNAS.

The initiator can access 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 108.

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 103.

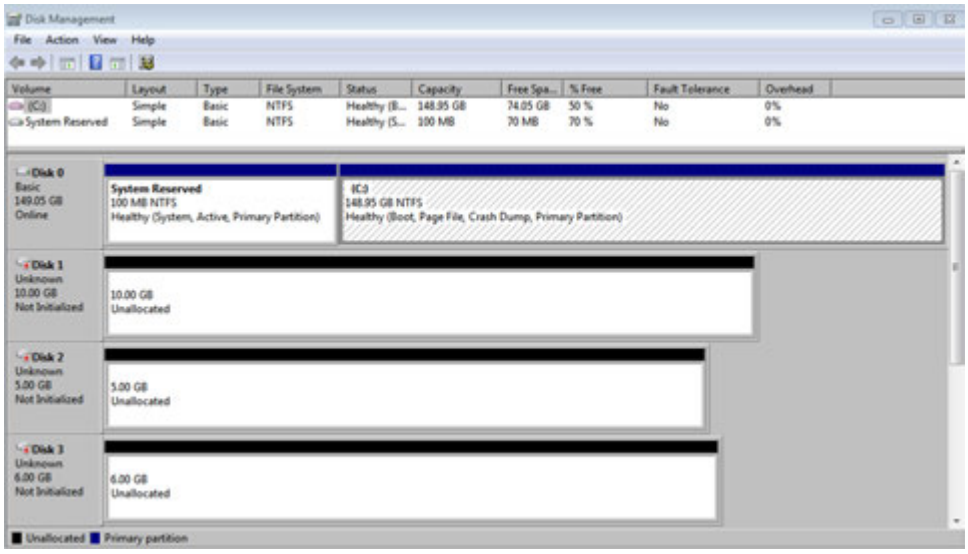
The following procedure uses the Microsoft iSCSI Software Initiator, which is freely available online and is integrated in Windows 7.

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 must be initialized and formatted.

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



2. Initialize unallocated disks:

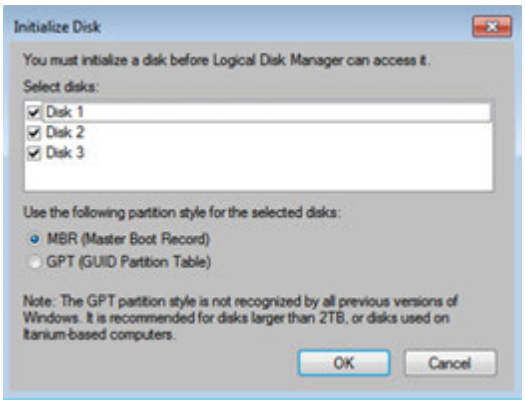
   a. Select an unallocated disk by clicking it.

   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.

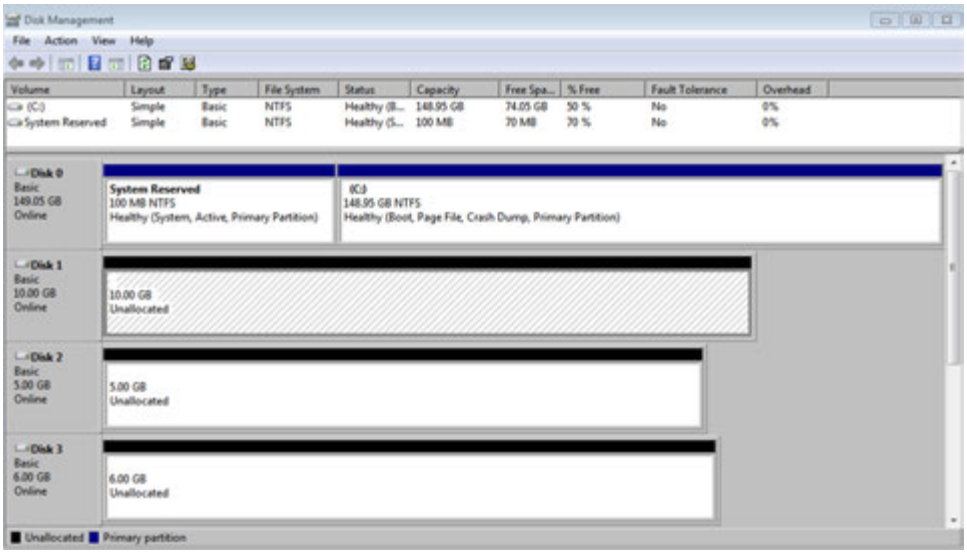
e. Click the **OK** button.



The selected disks are initialized.

3. Format an initialized disk:

a. Select the disk that you want to format.



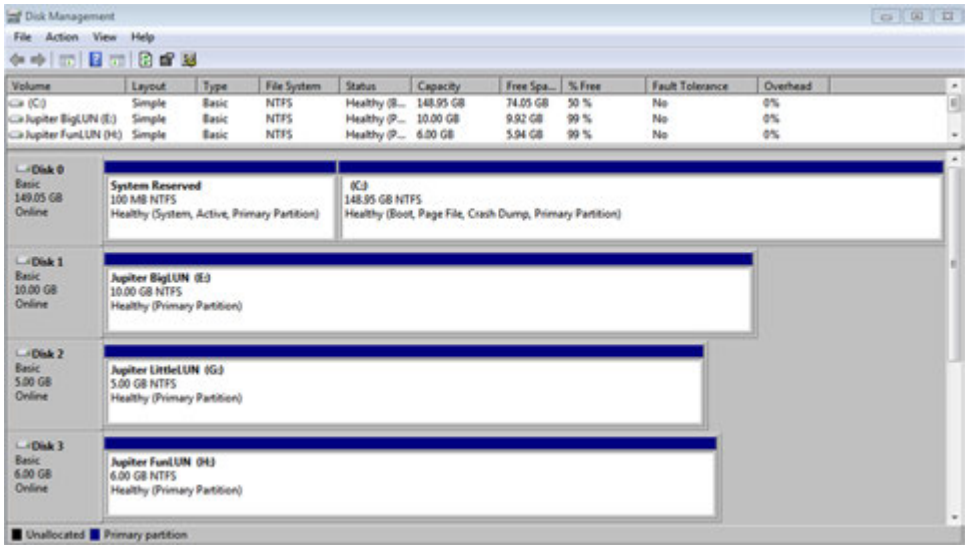
Selected disks are shaded.

b. In the Disk Management window, select **Action > All Tasks > New Simple Volume**.

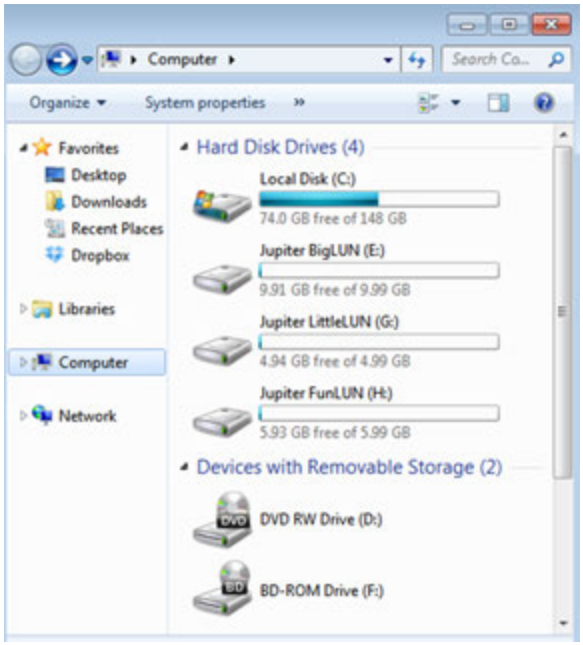
The New Simple Volume Wizard window displays.

c. Follow the default wizard formatting steps.

4. Repeat *Step 3* on page 109 for each initialized disk (LUN) that you want to access.



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



Snapshots

6

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 33. For information about how to create shared folders, see *Create a Shared Folder* on page 52. For information about how to create LUNs, see *Create a LUN* on page 86.

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. They take no space until the data they reference is changed or deleted. 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.

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 a threshold (set to a default of 5 percent) of the volume's total storage space, the oldest automatic snapshots are automatically deleted to bring the available storage space back to the threshold or higher. Manual snapshots are never automatically deleted. The threshold is part of the snapshot settings for a volume.

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

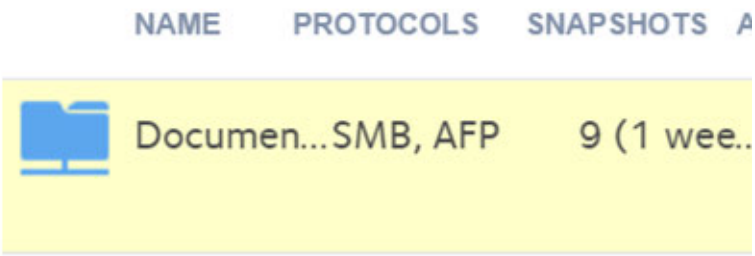


Figure 9. Shared folder with daily snapshots

Note For snapshots to be accessible to users from their network-attached device you must select the **Allow snapshot access** check box in the shared folder or LUN settings window. For more information, see *View and Change the Properties of a Shared Folder* on page 54.

Note Hourly snapshots are not taken for spun-down disks, but daily snapshots are taken.

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.
- Monthly snapshots are kept for as long as there is sufficient capacity. (The last weekly snapshot in a month becomes the monthly snapshot for that month.)

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 Using Recovery Mode* on page 116.

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 and changes made to the parent do not affect the clone. For information about how to clone snapshots, see *Clone Snapshots* on page 118.

View and Change Share Snapshot Properties

You can control the type of snapshot management, the schedule, and access for individual shares.

To view and change the snapshot properties of a share:

1. Log in to the ReadyNAS.
2. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder or LUN that you want to configure.
4. Click the **gear** icon.
   The shared folder or LUN settings pop-up menu opens.
5. Click the **gear** icon in the pop-up menu.
6. Select the **Snapshots** button.
7. Change the settings as explained in the following table.

Item	Description
Snapshot Management	Choose Smart or Custom.
Snapshot Schedule	The available options depend on whether you choose Smart or Custom Snapshot Management. Smart: Menu of Never, Hourly, Daily, or Weekly. Custom: View and control of when snapshots are taken (click the gear icon to change) and the snapshot retention policy.
Allow Snapshot Access	Select the Allow Snapshot Access check box to allow snapshot access to anyone with permission to access the shared folder.

8. Click the **OK** button.
   Your settings are saved and the pop-up menu closes.

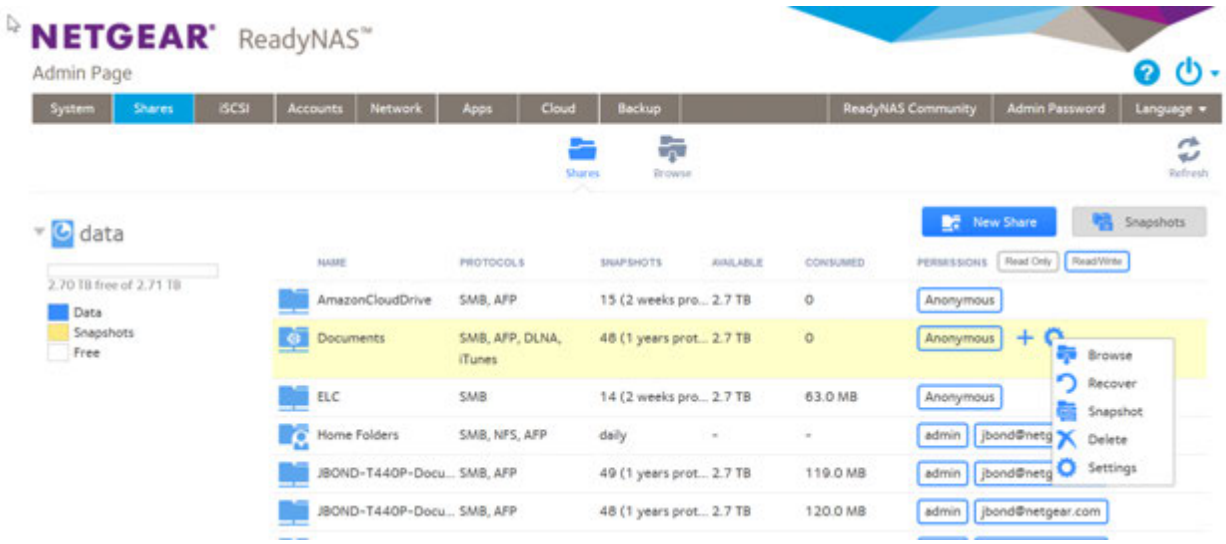
Manually Take a Snapshot

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

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

1. Log in to your ReadyNAS.
2. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the shared folder or LUN.

4. Click the **gear** icon.



5. In the pop-up menu, click the **Snapshot** button.
   The New Snapshot pop-up window displays.
6. Enter a name for the snapshot.
7. Click the **Create** button.
   The snapshot is created.

Browse Snapshots Using Recovery Mode

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

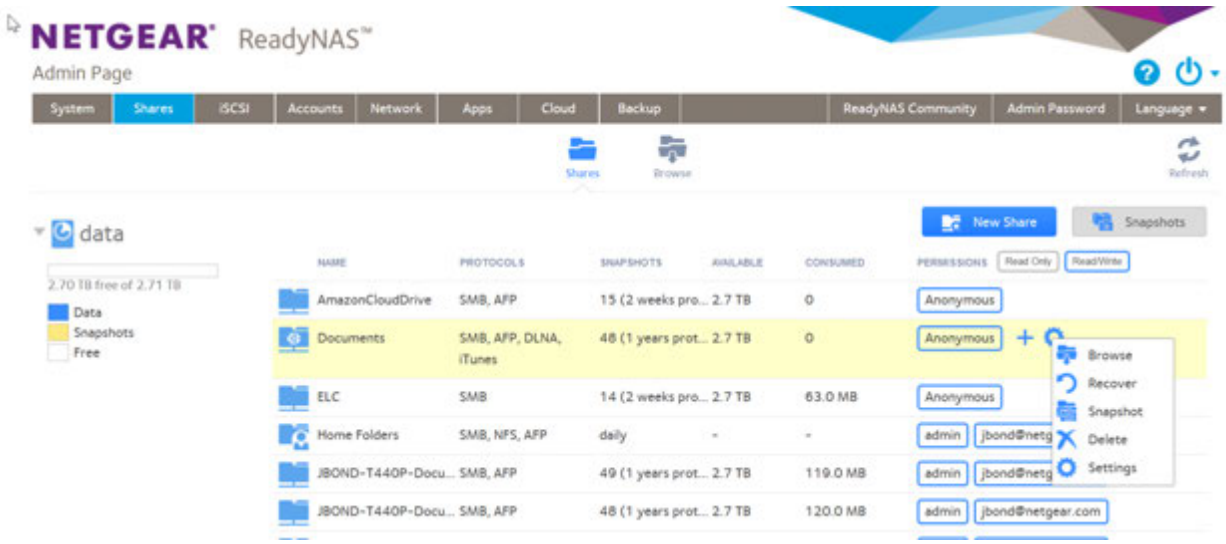
Sometimes you might want to recover individual files or subfolders within a shared folder without rolling back the entire shared folder. Recovery mode allows you to browse snapshots of shared folders and recover individual files or subfolders to your ReadyNAS.

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

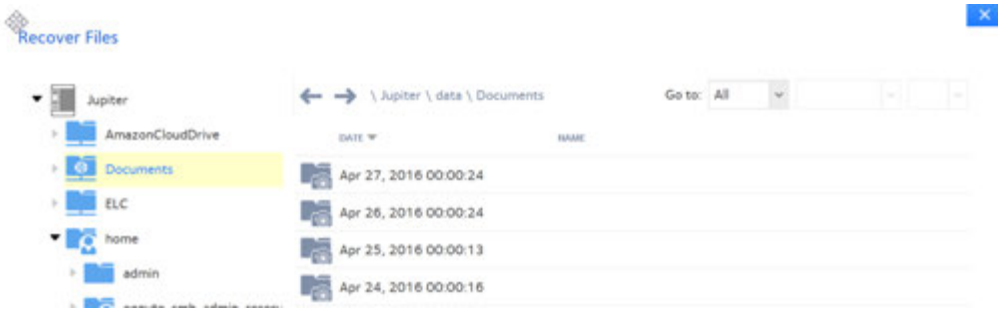
To browse and recover snapshot data using recovery mode:

1. Log in to your ReadyNAS.
2. Select **Shares > Shares**.
   A list of shared folders and LUNs on each volume displays.
3. Select the folder icon.

4. Click the gear icon.



5. In the pop-up menu, click the **Recover** button.
.



6. Right-click the snapshot.
The snapshot options menu opens.
7. Click the **Browse** button.
The contents of the selected snapshot display.
8. Continue browsing in recovery mode until you find the file or folder that you want to recover.
9. Right-click the file or folder.
10. In the pop-up menu, click the **Restore** button.
11. In the pop-up window, 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.

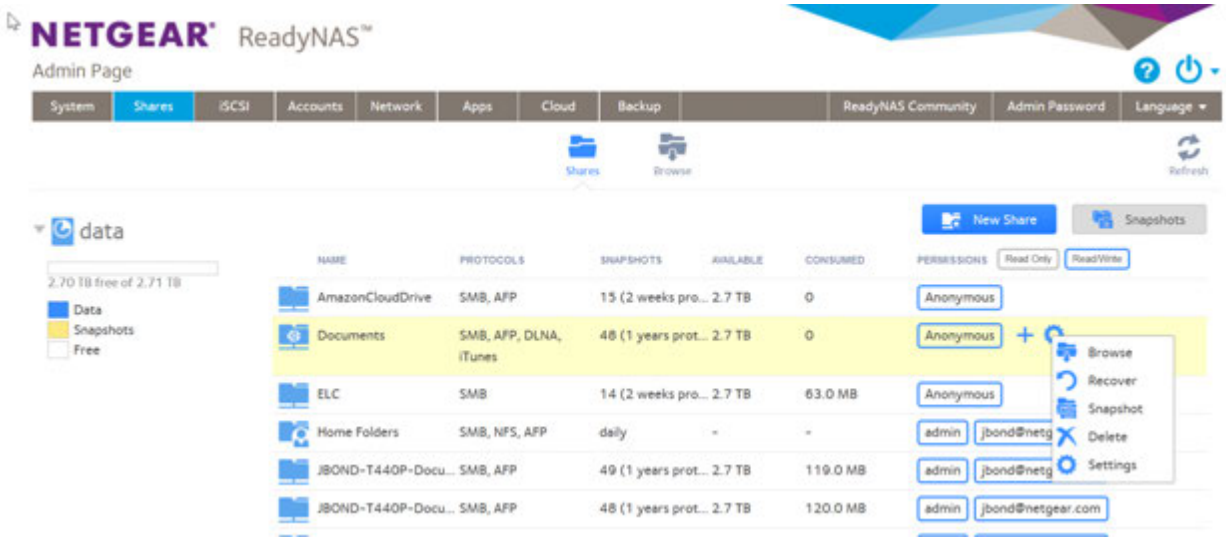
Roll Back to a Snapshot Using Recovery Mode

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

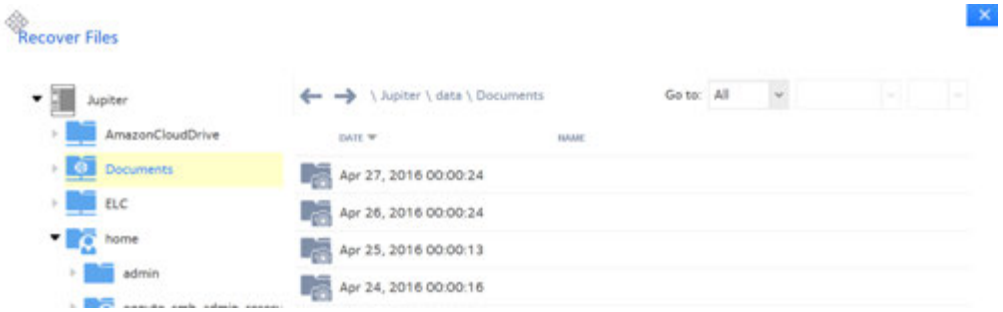
Recovery mode is available only for shared folders.

To roll back to a snapshot using recovery mode:

1. Log in to your ReadyNAS.
2. Select **Shares > Shares**.
   A list of shared folders on each volume displays.
3. Select the folder that contains the file or subfolder you want to browse.
4. Click the **gear** icon.

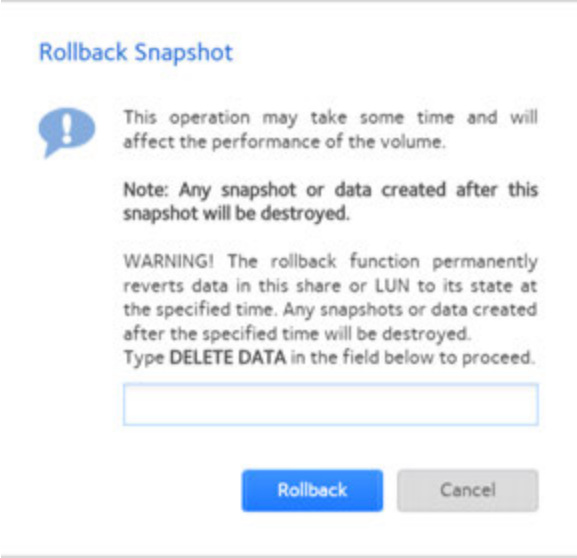


5. In the pop-up menu, click the **Recover** button.



6. Right-click the snapshot that contains the version of the folder to roll back to.
   The rollback options menu opens.

7. Click the **Rollback** button.



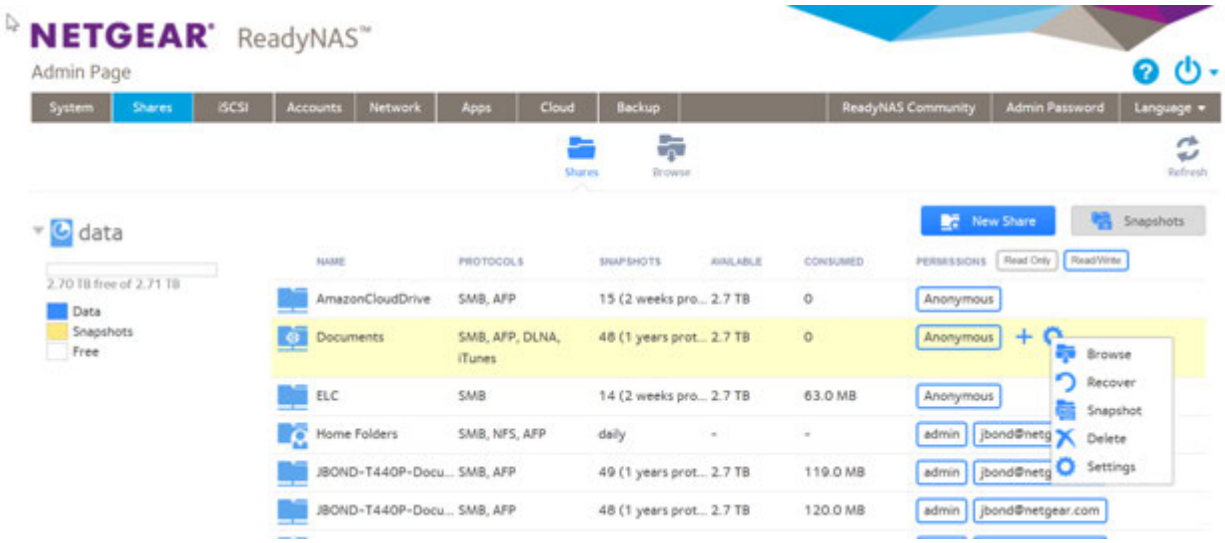
8. Confirm that you want to roll back to the selected snapshot by typing **DELETE DATA**.
9. Click the **Rollback** button.
   The shared folder is rolled back to the snapshot that you selected.

Clone Snapshots

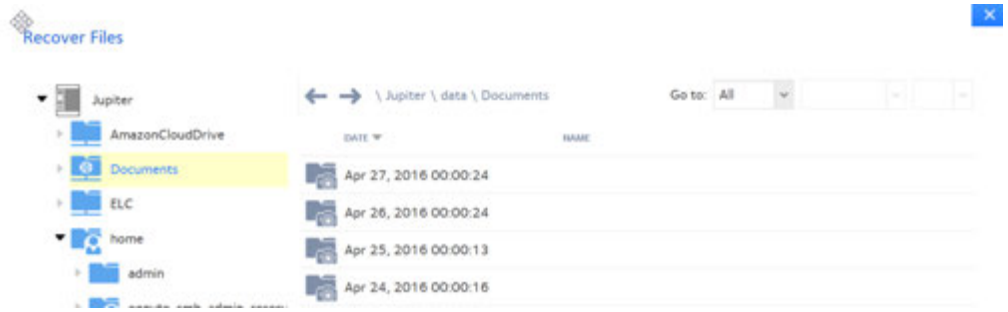
Cloning a snapshot copies the snapshot to create a new independent shared folder or LUN.

To clone a snapshot:

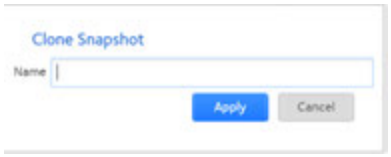
1. Log in to your ReadyNAS.
2. Select **Shares > Shares**.
   A list of shared folders and LUNs volume displays.
3. Select the folder that contains the file or subfolder you want to browse.
4. Click the **gear** icon.



5. In the pop-up menu, click the **Recover** button.



6. Right-click the snapshot that contains the version of the folder to roll back to.
The rollback options menu opens.
7. In the pop-up menu, click the **Clone** button.



8. Enter a name for the new folder or LUN.
9. Click the **Apply** button.
The cloned snapshot is added to the Shares page as a new shared folder or LUN.

Note A new shared folder is immediately accessible to users. A new LUN must first 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 112.

Delete Snapshots Using Recovery Mode

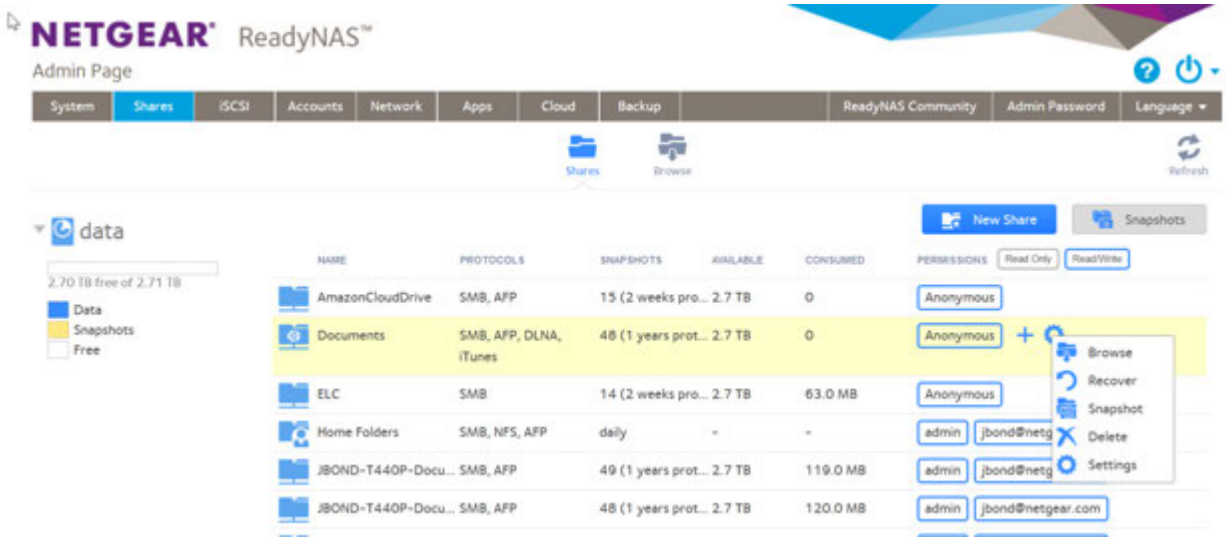
You can manually delete snapshots using recovery mode.

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

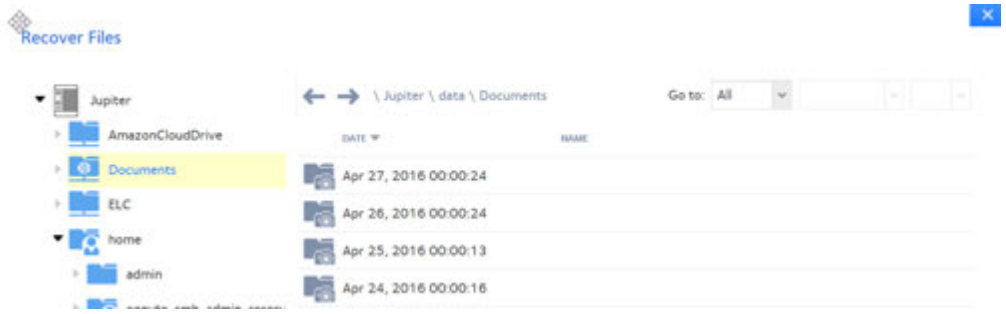
Recovery mode is available only for shared folders.

To delete a snapshot using recovery mode:

1. Log in to your ReadyNAS.
2. Select **Shares > Shares**.
   A list of shared folders on each volume displays.
3. Select the folder that contains the file or subfolder you want to browse.
4. Click the **gear** icon.



5. In the pop-up menu, click the **Recover** button.



6. Right-click the snapshot.
   The rollback options menu opens.
7. Click the **Delete** button.
8. 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.

Note You can add additional protection by backing up the snapshots using ReadyDR.

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 54.
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 with access to a shared folder can access its snapshots. Users without 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 77.
3. Locate the snapshot data on the ReadyNAS.

Snapshot data is stored in a snapshot subfolder within the shared folder. Users with 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 118. 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 94.
   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 with 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

7

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

User and Group Accounts

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 requires 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.

The ReadyNAS system administrator account allows special priviledges. The ReadyNAS system administrator can grant most, but not all, of these special priviledges to any user by assigning that user to the user group admin. Secondary admin accounts cannot do the following:

- Disable themselves
- Perform password recovery
- Perform password reset

Only one admin user (including the master admin account) can be logged in to the ReadyNAS at a time.

Home Folders

Home folders allow each user a private folder matching his or her account name. Home folders are automatically created when a user account is created. By default, home folders are available over SMB, AFP, and NFS protocols and are available optionally over FTP and DLNA protocols. All can be disabled.

You can control whether or not snapshots are enabled for home folders. You enable or disable snapshot protection for home folders through a switch for the default user (**Accounts > Default User**). If snapshot protection is enabled here, you can enable or disable it for individual home folders when viewing it in the **Shares** tab.

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 we recommend that you create and maintain only those accounts that you need.

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.

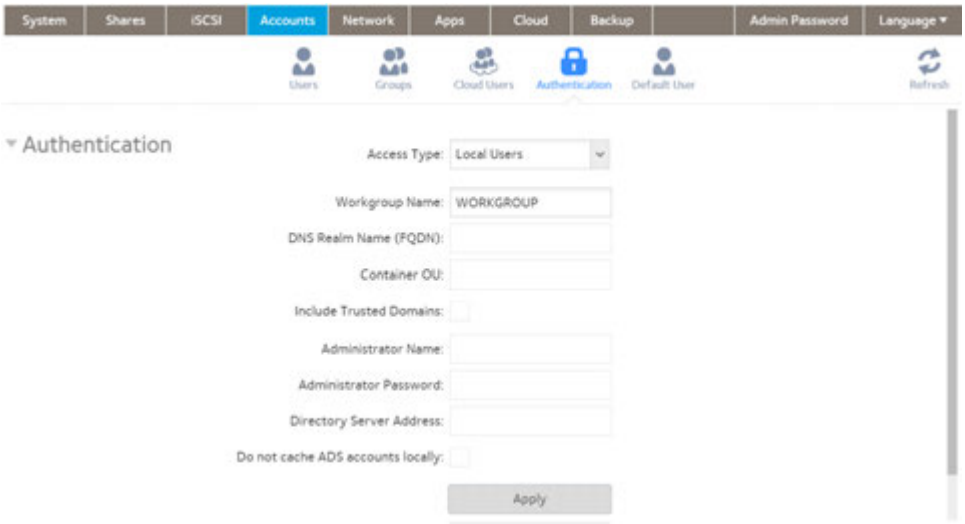
User and Group Management Modes

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. Log in to the ReadyNAS.
2. Select **Accounts > Authentication**.



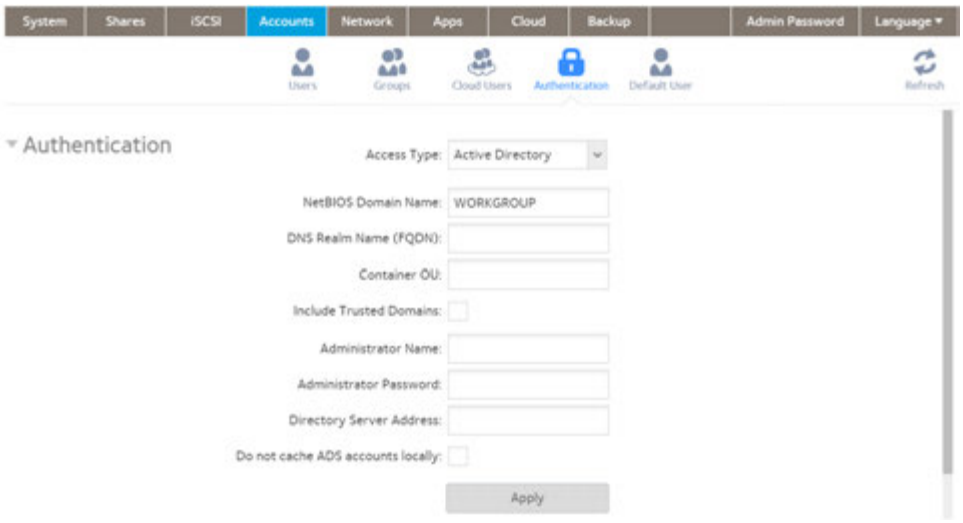
3. In the **Access Type** menu, select **Local users**.
4. (Optional) Enter a name for the workgroup.
   You can keep the default name of VOLUME.
5. Click the **Apply** button.
   Your settings are saved.

For more information about managing users and groups in Local Users mode, see *User Accounts* on page 127 and *Group Accounts* on page 132.

To configure Active Directory mode:

1. Log in to the ReadyNAS.
2. Select **Accounts > Authentication**.
   The page adjusts.
3. In the **Access Type** menu, select **Active Directory**.

The **Workgroup Name** field changes to **NetBIOS Domain Name**.



4. 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 does not match the prefix naming rules, the name differs 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, where company is the prefix, and community is the suffix of the name.
Container OU	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 Computers organizational unit (OU), but you can use the **Container OU** field to specify another OU. You can specify OUs by separating OU entries with slashes. 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 164).
Included Trusted Domains	Select the **Include Trusted Domains** check box to include active directory domains, and their accounts, recognized as trusted by the Active Directory used by the ReadyNAS system.
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.
Do not cache ADS accounts locally	Select this check box to prevent caching of ADS accounts. Caching can speed access, but downloading and updating the accounts of a large domain can also slow the ReadyNAS system. If this check box is clear, then the ReadyNAS system imports a list of users and groups from the Active Directory server. If the option is checked, then the ReadyNAS does not import a list of users and groups from AD.

(Continued)

Item	Description
ADS ID Map	Select the **Import** option to import an ADS map to this ReadyNAS system. Select the **Export** option to export this ReadyNAS system ADS map to a file for later uploading to other ReadyNAS systems.

Note For use with Windows systems, the ReadyNAS maps Windows IDs (Windows SIDs) to ReadyNAS IDs. In versions of ReadyNAS OS previous to ReadyNAS OS 6.5 and in systems upgraded from those earlier versions, the mapping is done when an account is first authenticated. You can import and export this map so that all ReadyNAS systems on a network use the same map.
Starting with ReadyNAS OS 6.5, the mapping is done by an algorithm using the SID. Because the algorithm is the same on all ReadyNAS systems, you do not need to transfer the mapping between systems on the network.

You cannot convert the maps on a ReadyNAS system from one method to the other.

5. Click the **Apply** button.
   Your settings are saved.
6. (Optional) Click the **Refresh ADS Accounts** button.
   User and group information about 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:

- The same time must be set on your Active Directory server and your ReadyNAS system clocks. We recommend 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. We recommend that you point your ReadyNAS to the Active Directory DNS to ensure that host names can be resolved.
- If you do not set the NTP server, the ReadyNAS device will set an NTP server.

User Accounts

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

The user account procedures assume 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 125.

You enable or disable home folder snapshot protection, enable or disable the use and capacity of private time machines, and specify the default primary group for a user through settings for the default user (**Accounts > Default User**).

Configure Default User Settings

When you create a user account, whether home folder snapshot protection is used, whether the user can have a private Time Machine, and the default group membership are all controlled by settings for the default user. You can change these defaults.

This procedure 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 125.

1. Log in to your ReadyNAS admin page.
2. Select **Accounts > Default User**.

   The default user settings display.

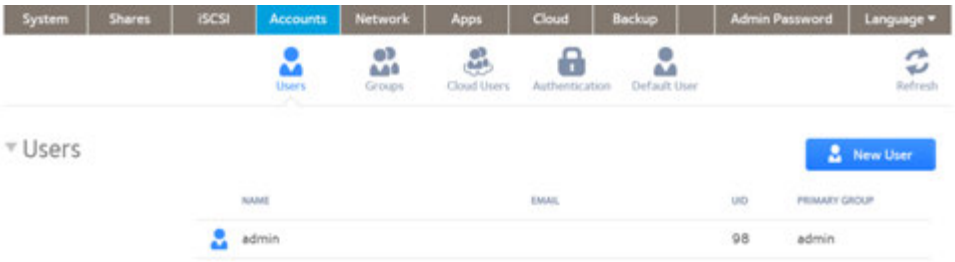
   You can turn home snapshot protection on or off, permit or disallow the use of private Time Machines, and set their capacity, and set the default primary group for new users. These settings apply to new users. They do not change the settings for existing users.
3. Click the **Apply** button.
   Your settings are saved.

Create User Accounts

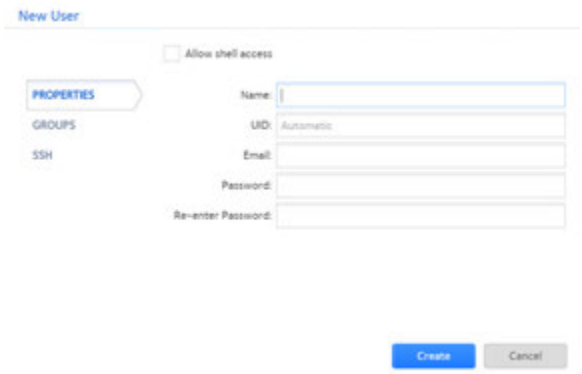
This procedure assumes that your ReadyNAS system is currently in Local Users mode. For more information about changing user and group management modes, see *User and Group Management Modes* on page 125.

To create a user account:

1. Log in to your ReadyNAS.
2. Select **Accounts > Users**.



3. Click the **New User** button.



4. Enter the following information for the new user:

   - **Name**. User names can be 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. User names cannot consist of numbers only. You cannot use @ in user names.
   - **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 menu, select the primary group to which the user is assigned. The default group is called users. A group called admin is also predefined.
     You can assign the primary group admin as a user's primary group to give that user most of the priviledges of the admin user. For the list of restrictions, see *User and Group Accounts* on page 124.
     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 133.

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

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

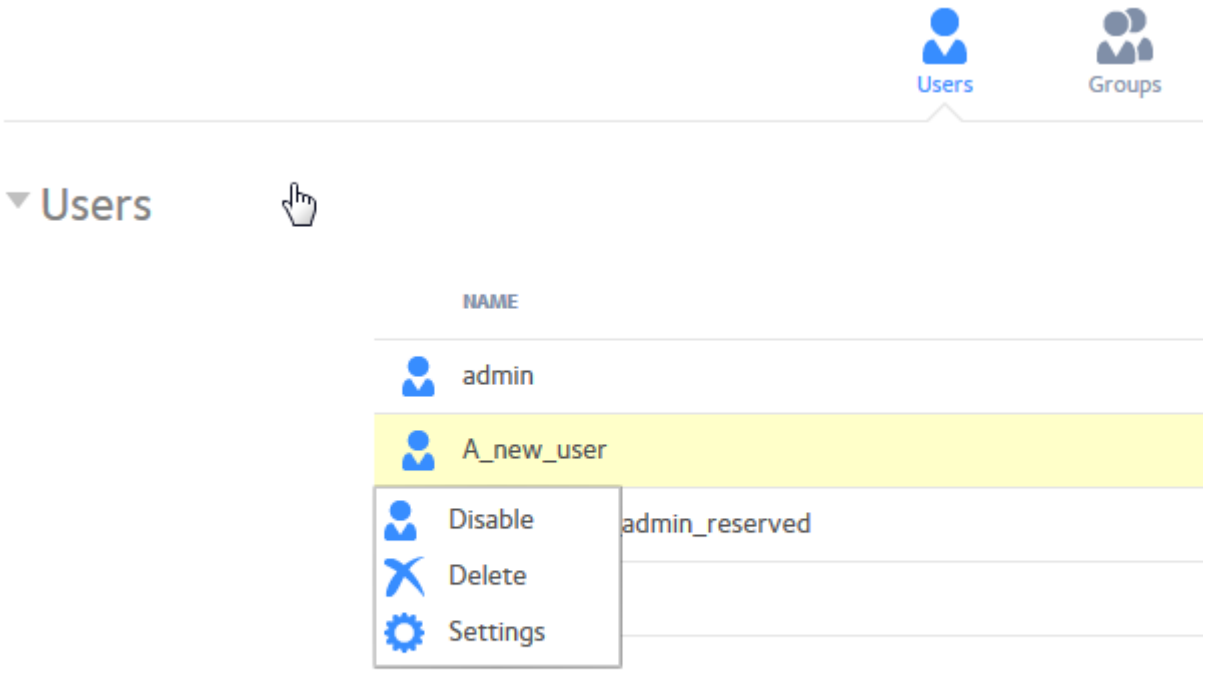
Edit User Accounts

This procedure 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 125.

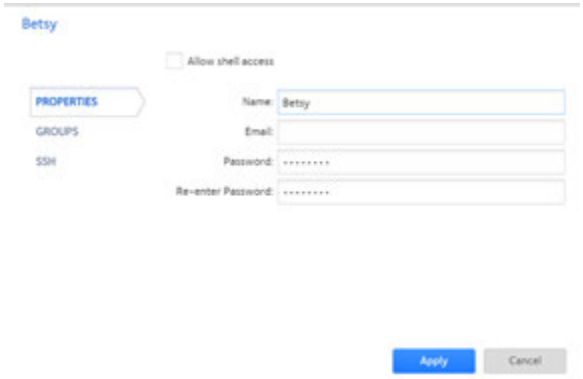
You can edit a user's name, email address, or password.

To edit a user account:

1. Log in to your ReadyNAS.
2. Select **Accounts > Users**.
   The list of current users displays.
3. From the list of users, select a user account.



4. Click the **Settings** button in the pop-up menu.



5. 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.

6. Click the **Apply** button.
   Your settings are saved.

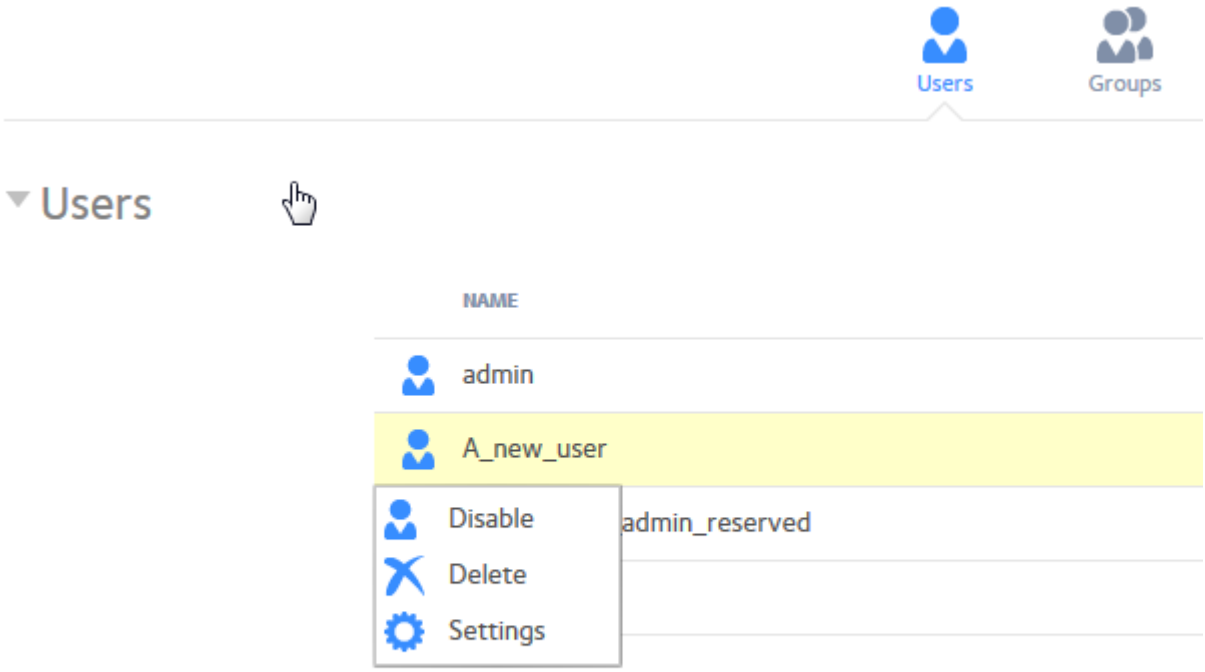
Delete User Accounts

This procedure 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 125.

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. Log in to your ReadyNAS.
2. Select **Accounts > Users**.
   The list of current users displays.
3. From the list of users, select the user account.



4. Click the **Delete** button in the pop-up menu.
5. Confirm the deletion.

The user is deleted.

Change User Passwords

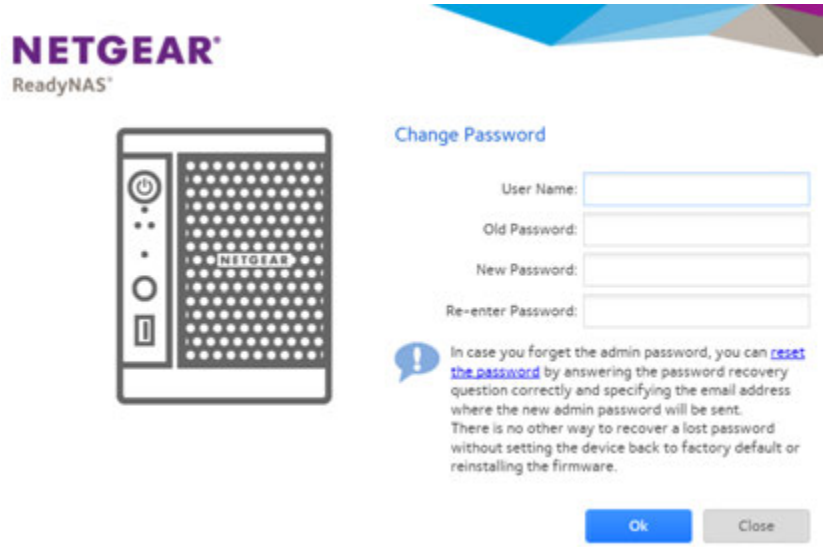
This procedure assumes that your ReadyNAS system is currently in Local Users mode. For more information about changing user and group management modes, see *User and Group Management Modes* on page 125.

The ReadyNAS administrator can change user passwords from the local admin page (see *Edit User Accounts* on page 129).

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 settings are saved.

Group Accounts

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

The group account procedures assume 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 125.

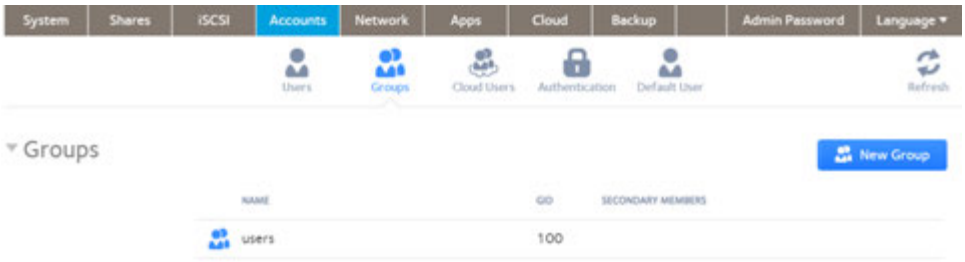
Create Groups

This procedure 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 125.

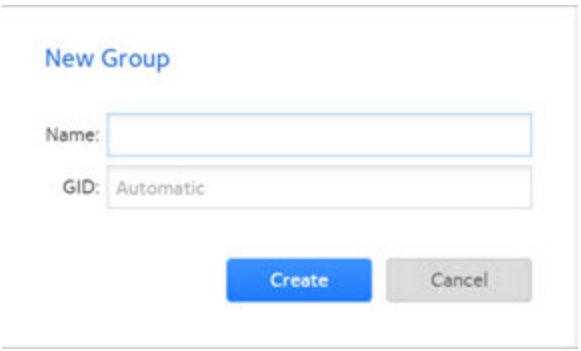
Use the local admin page to create groups.

To create a group:

1. Log in to your ReadyNAS.
2. Select **Accounts > Groups**.



3. Click the **New Group** button.



4. Enter the following information for the new group:

   - **Name**. Group names can be 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.

5. Click the **Create** button.
   The group is added to your system.

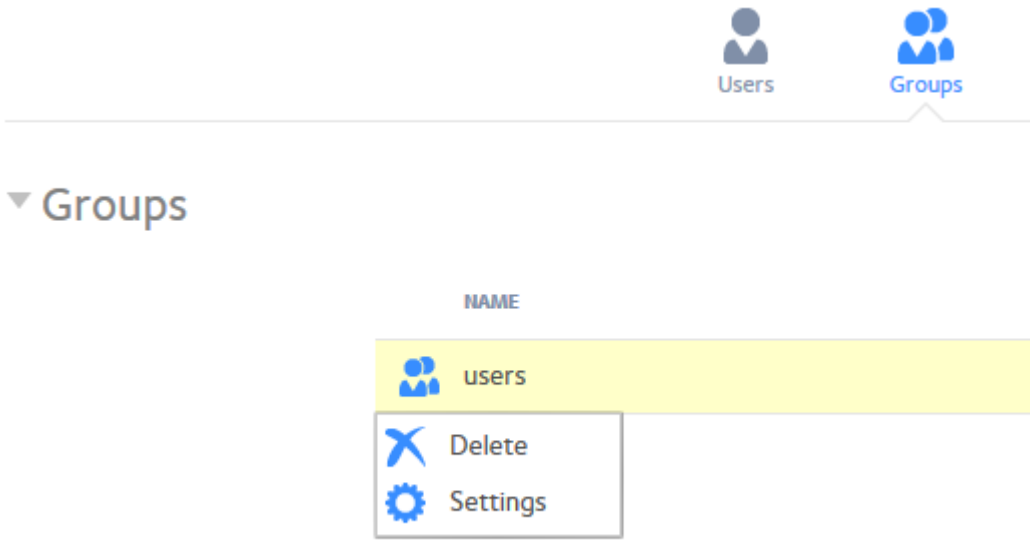
Edit Groups

This procedure 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 125.

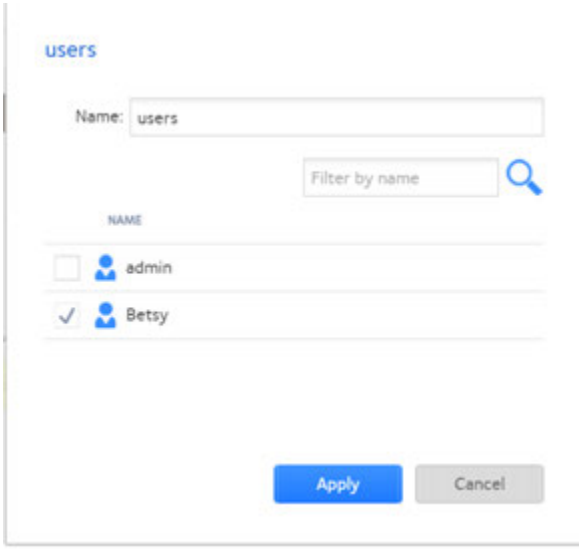
Use the local admin page to edit a group.

To edit a group:

1. Log in to your ReadyNAS.
2. Select **Accounts > Groups**.
   The list of groups displays.
3. Select the group.



4. Click the **Settings** button in the menu.



5. 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.

6. To change the group name, enter a new name in the **Name** field.
7. To add a user to this group as secondary member, select the check box next to the user's name.
8. 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 window. For information about how to edit primary group membership, see *Edit User Accounts* on page 129.

9. Click the **Apply** button.
   Your settings are saved.

Delete Groups

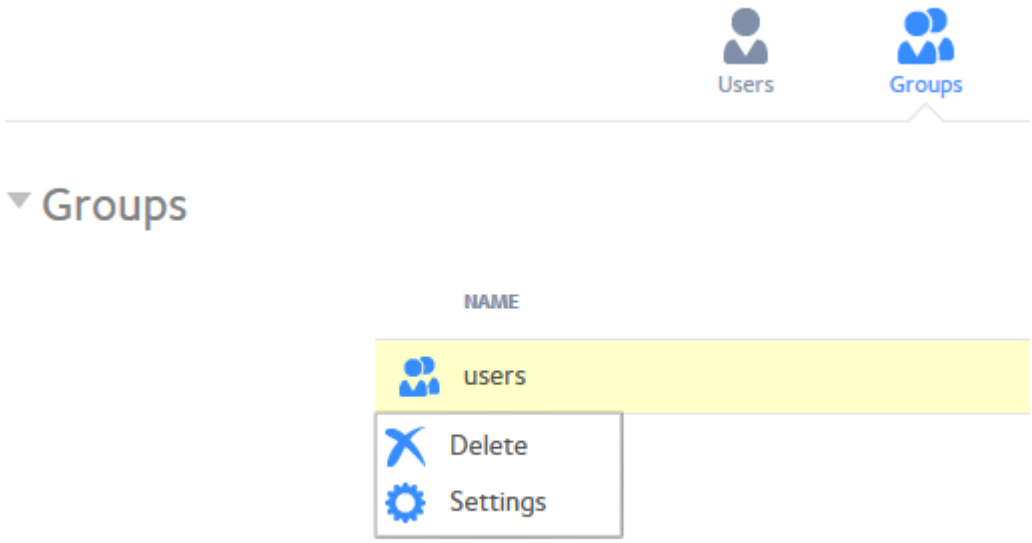
This procedure assumes that your ReadyNAS system is currently in Local Users mode. For more information about changing user and group management modes, see *User and Group Management Modes* on page 125.

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 129. For more information about deleting users, see *Delete User Accounts* on page 131.

To delete a group:

1. Log in to your ReadyNAS.
2. Select **Accounts > Groups**.
   The list of groups displays.

3. Select the group.



4. Click the **Delete** button in the menu.
5. Confirm the deletion.
   The group is deleted.

Cloud Users

Cloud users are users who can access your system using ReadyCLOUD.

ReadyCLOUD is a free cloud-based service that allows users to securely access your system from anywhere with 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.

Note You cannot delete a user from the local admin page. You must use the ReadyCLOUD portal to ReadyCLOUD users.

Grant Access to Cloud Users

If you want users to access your system using ReadyCLOUD, see *Use ReadyCLOUD to Share Folders Through Email* on page 140.

For more information about ReadyCLOUD, see *Access Shared Folders Using Cloud Services* on page 138.

Cloud User Access Rights

When you grant access to ReadyCLOUD users, those users can access your ReadyNAS system using ReadyCLOUD. 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 146.

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 61.

Use Cloud Services

8

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

> **Note** Starting with ReadyNAS OS 6.5, ReadyNAS Remote is no longer available. ReadyCLOUD replaces ReadyNAS Remote.

This chapter includes the following sections:

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 with 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 14.

Using ReadyCLOUD involves these high-level steps:

1. Add your ReadyNAS system to your MyNETGEAR account.
   See *Join ReadyCLOUD* on page 139.

   Note Starting with ReadyNAS OS 6.5, changes in the integration of ReadyNAS OS and ReadyCLOUD require MyNETGEAR single-sign-on accounts. If you own an earlier ReadyCLOUD account, when you first log back in to ReadyCLOUD, you will be assisted in upgrading your account.

2. (Optional) Grant access to ReadyCLOUD users.
   See *Use ReadyCLOUD to Share Folders Through Email* on page 140.
3. Access your data and manage your ReadyNAS system using ReadyCLOUD.
   See *Access Your System Using ReadyCLOUD* on page 147.

   Note ReadyCLOUD is not supported when the ReadyNAS is in Active Directory (Domain) mode.

Join ReadyCLOUD

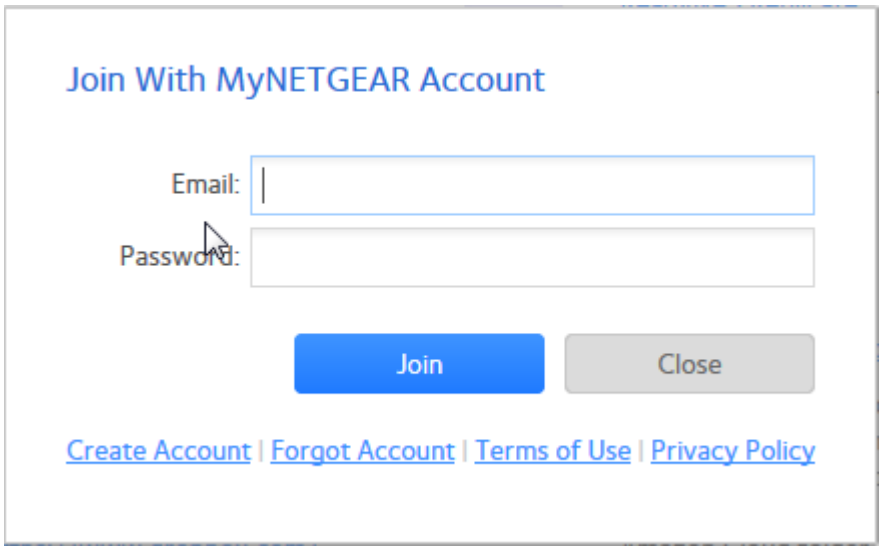
Before you can access your system using ReadyCLOUD, you must add your system to your ReadyCLOUD account. The ReadyCLOUD service is preinstalled on your ReadyNAS storage system.

Note Starting with ReadyNAS OS 6.5, changes in the integration of ReadyNAS OS and ReadyCLOUD require ReadyCLOUD single-sign-on accounts. If you have an earlier ReadyCLOUD account, when you first log back in to ReadyCLOUD, you will be assisted in upgrading your account.

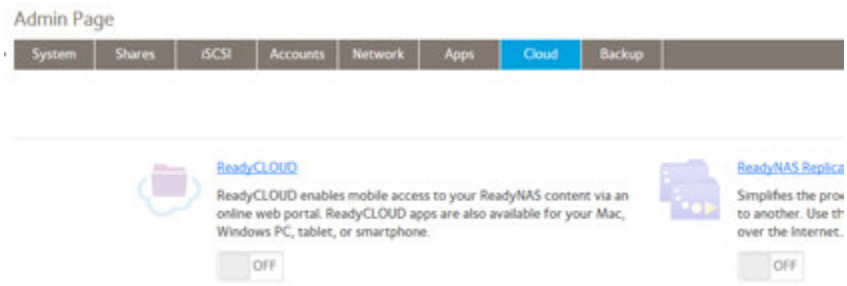
To add your ReadyNAS system to ReadyCLOUD:

1. Log in to your ReadyNAS.
2. Select **Cloud**.
   The page updates with the Cloud page.
3. Set the **On-Off** slider so the slider shows the **On** position to enable ReadyCLOUD.

4. When prompted, 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.

For information about granting access to ReadyCLOUD users, see *Use ReadyCLOUD to Share Folders Through Email* on page 140.

Note If you decide to remove your system from ReadyCLOUD, any ReadyCLOUD users and all data in their home folders, 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 147.

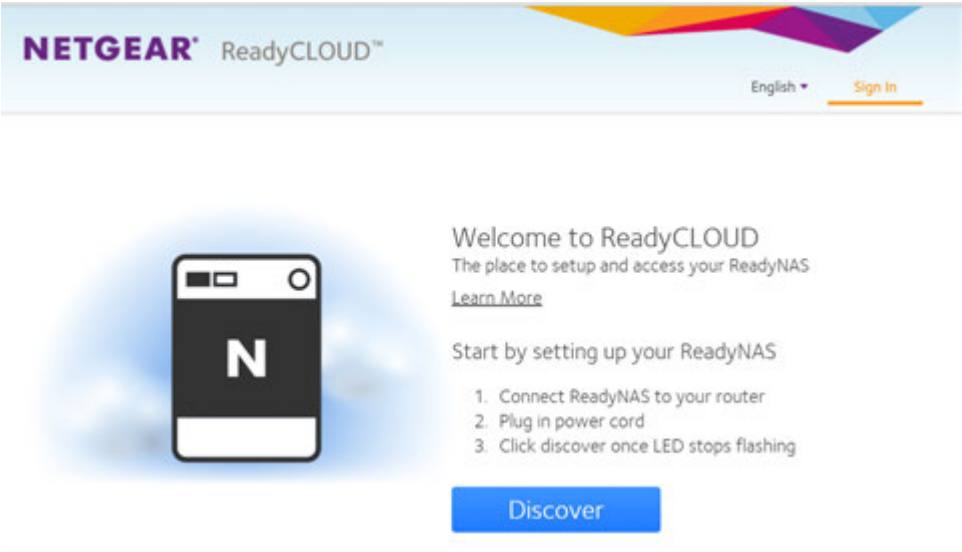
Use ReadyCLOUD to Share Folders Through Email

After you add your system to ReadyCLOUD, you can allow other users to access your folders. You can share in two ways: through an emailed link, or by granting permission to an existing ReadyCLOUD user. This procedure uses an emailed link.

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

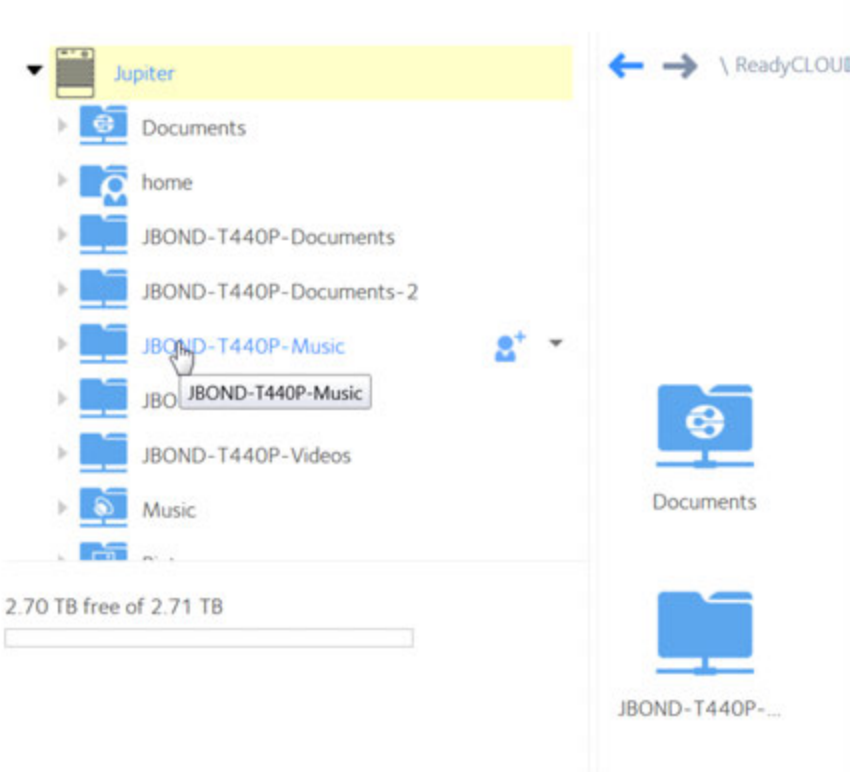
To grant access to a folder:

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

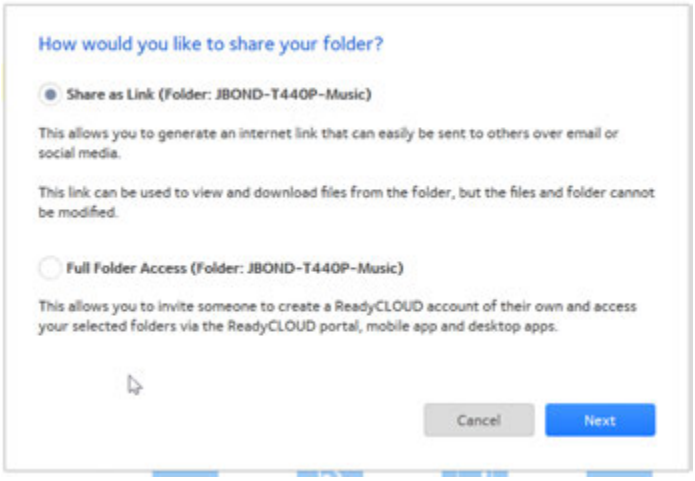


2. From the top menu bar, click the **Sign In** link near the top right corner of the page. A Sign in window opens.
3. Enter your ReadyCLOUD account credentials and click the **Sign In** button. You are signed in to ReadyCLOUD.
4. From the top menu bar, select **Home**.

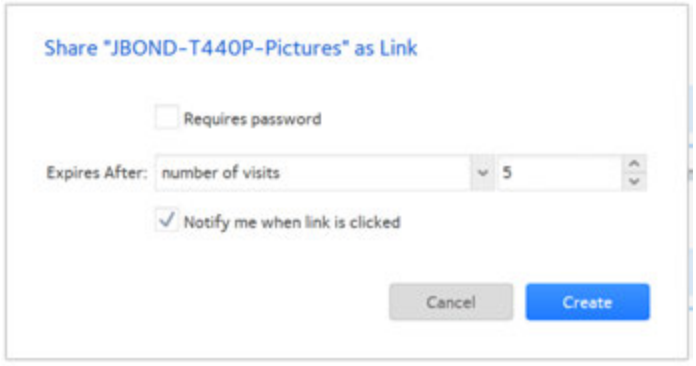
5. Select the folder you want to share.



6. Click the button on the upper right.

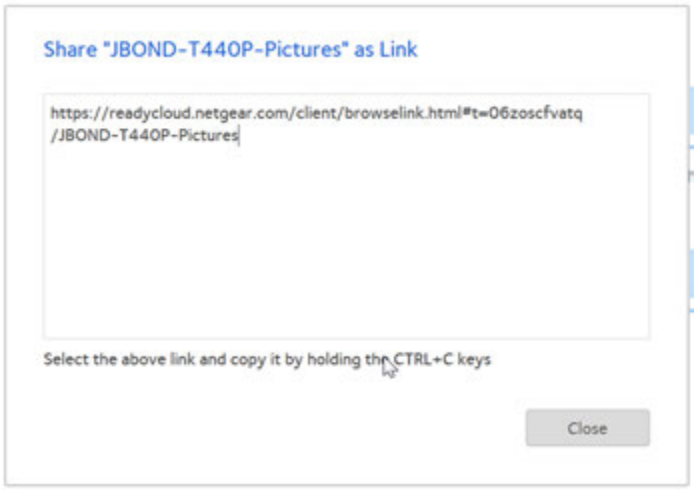


7. Click the **Next** button.



8. Review and adjust the options: **Requires password**, **Expires After number of visits** or **Expires After Date**, and **Notify me when link is clicked**.
9. Click the **Create** button.

Note If you select the **Expires After Date** option, a window opens with a calendar from which you can select the date.



10. Copy the link and paste it into an email message to the person you want to access the folder, and send the message.

    When the recipient clicks the link, ReadyCLOUD opens, showing the folder. The recipient can read the files in the folder, but cannot delete or change them.

For more information about using the ReadyCLOUD portal, see *Access Your System Using ReadyCLOUD* on page 147.

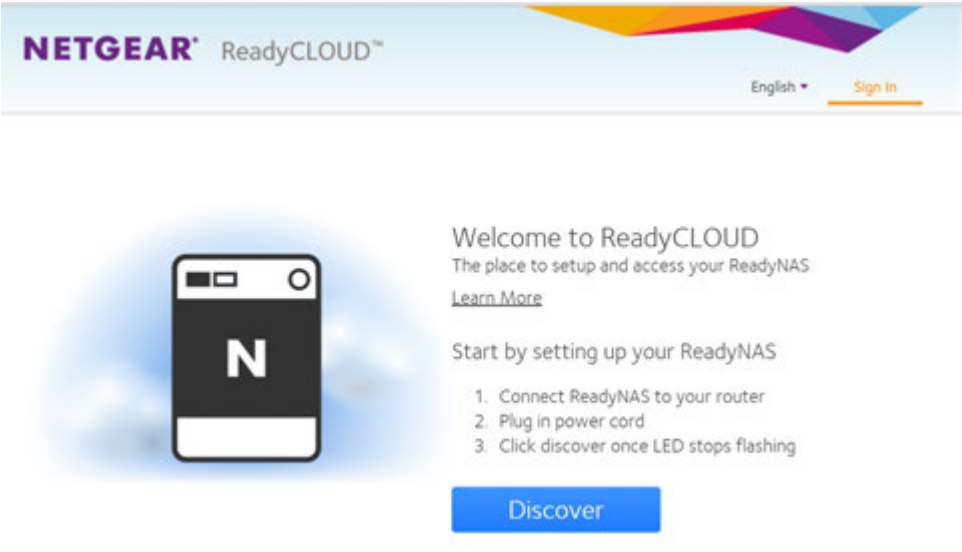
Use ReadyCLOUD to Share Folders With ReadyCLOUD Users

After you add your system to ReadyCLOUD, you can allow other users to access your folders. You can share in two ways: through an emailed link, or by granting permission to an existing ReadyCLOUD user. This procedure is for a ReadyCLOUD user.

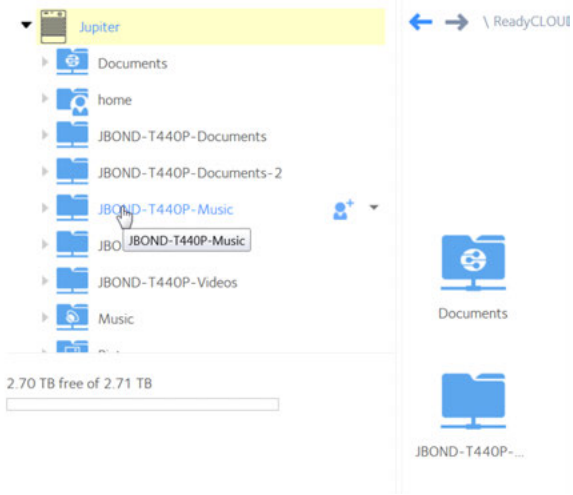
Note When you grant access to a ReadyCLOUD user, that user automatically gains access to your system from ReadyCLOUD.

To grant access to ReadyCLOUD users:

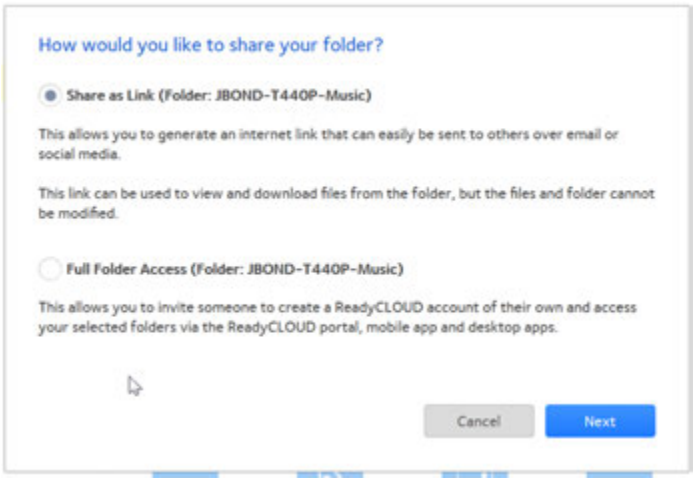
1. Open a web browser and visit *http://readycloud.netgear.com*.



2. From the top menu bar, click the **Sign In** link near the top right corner of the page. A Sign in window opens.
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 **Home**.
5. Select the folder you want to share.



6. Click the button on the upper right.



7. Click the **Full Folder Access** button.
   A window opens showing the list of current ReadyCLOUD users with access rights to the folder and a place to enter a new email address.
8. Enter the new user's email address.
   After you enter a correctly formatted email address, the address is compared to the list of known ReadyCLOUD users and the window adjusts to include a menu with **Read/Write** and **Read Only** options. If the user is not already registered with ReadyCLOUD, a message displays that an email inviting the user to join will be sent.
9. Click the **Invite** button.
   Users without an existing ReadyCLOUD account receive an email message 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 147.

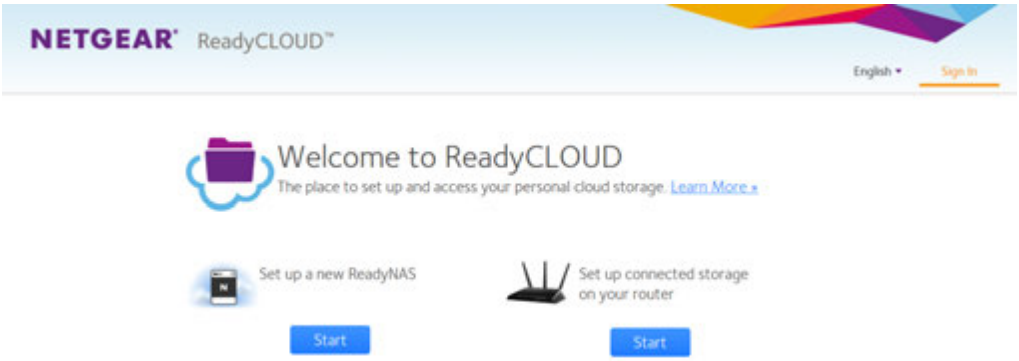
Delete ReadyCLOUD Users

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

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

To delete a ReadyCLOUD user:

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



2. From the top menu bar, click the **Sign In** link near the top right corner of the page.
   A sign in window opens.
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.
6. Select the **Delete** button.
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 can change the access rights.

You use the ReadyCLOUD web portal to configure the access rights to individual shared folders. For each user, you can specify the permissions for each shared folder. The following table lists the access right options.

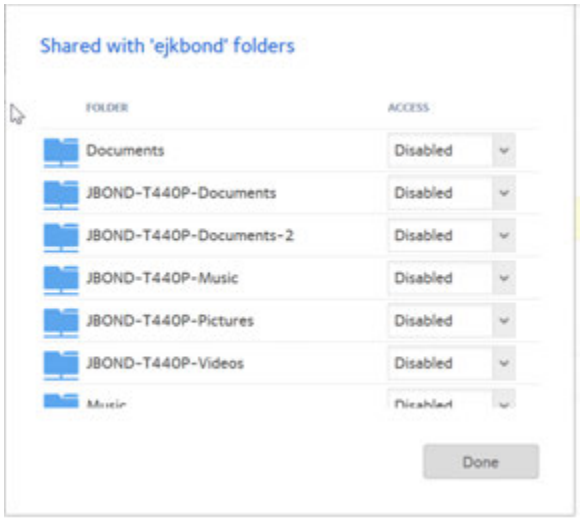
Table 7. Access right options

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.
Disabled	Access to this shared folder is disabled for the user.

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, click the **Sign In** link near the top right corner of the page.
   A sign in window opens.
3. Enter your ReadyCLOUD account credentials and click the **Sign In** button.
   You are signed in to ReadyCLOUD.
4. Select **Manage**.
   The ReadyNAS systems that you added to ReadyCLOUD using this account are displayed.
5. Select the user to configure.
6. Click the **gear** icon.



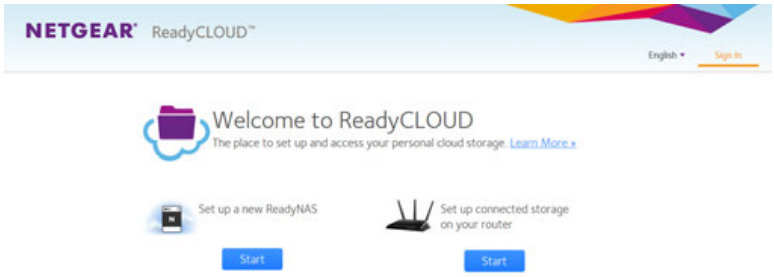
7. For each shared folder, select one of the following check boxes:
   - **Disabled**. The user is not granted access to the folder.
   - **Read Only**. The selected user or group is permitted only to read files on the shared folder.
   - **Read/Write**. The selected user or group is permitted to read, edit, create, and delete files on the shared folder.
8. Click the **Done** button.
   Your settings 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.

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, click the **Sign In** label near the top right corner of the page.
   A sign in window opens.
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.

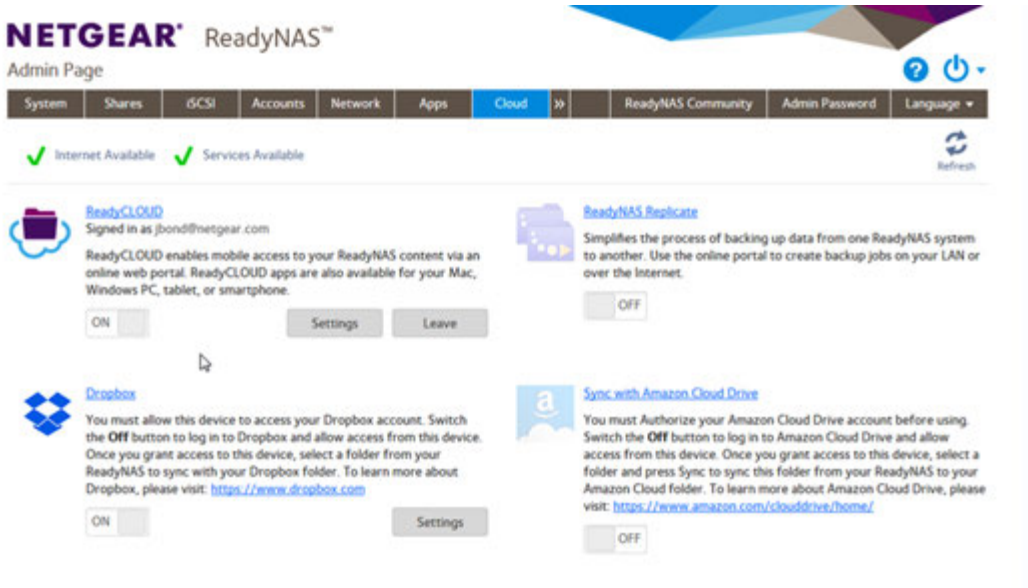
Sync With Amazon Cloud Drive

You can sync files between your ReadyNAS and your Amazon Cloud Drive.

For information on Amazon Cloud Drive, visit *amazon.com/clouddrive/home/*.

To set up syncing with your Amazon Cloud Drive:

1. Log in to your ReadyNAS.
2. Select **Cloud**.



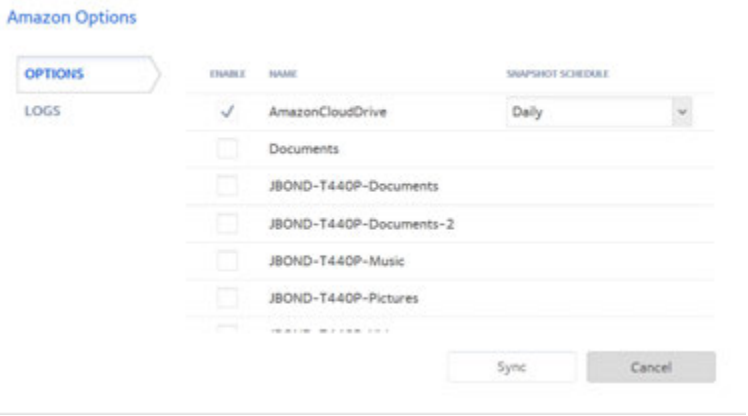
3. Set the Sync with Amazon Cloud Drive **On-Off** slider so that the slider shows the **On** position.
   Your default browser opens displaying the Amazon Cloud Drive page to authorize Amazon Cloud Drive to sync with the ReadyNAS.

4. Follow the directions on the page to authorize the ReadyNAS.

> **Note** If you do not already have an Amazon Cloud Drive, you will be guided through creating one. This requires logging in to, or creating, an Amazon account.

The Sync with Amazon Cloud Drive section adds a **Settings** button.

5. Click the **Settings** button.



6. Select shares to sync with your Amazon Cloud Drive.
7. You can accept or change the snapshot schedule for each selected share.

> **Note** If you delete a file on the Amazon Cloud Drive, any snapshots for that file are maintained on the ReadyNAS and managed according to the set snapshot policies.

8. Click the **Sync** button to immediately start a sync.
   The Amazon Options window closes and the files sync.

Sync With Amazon S3

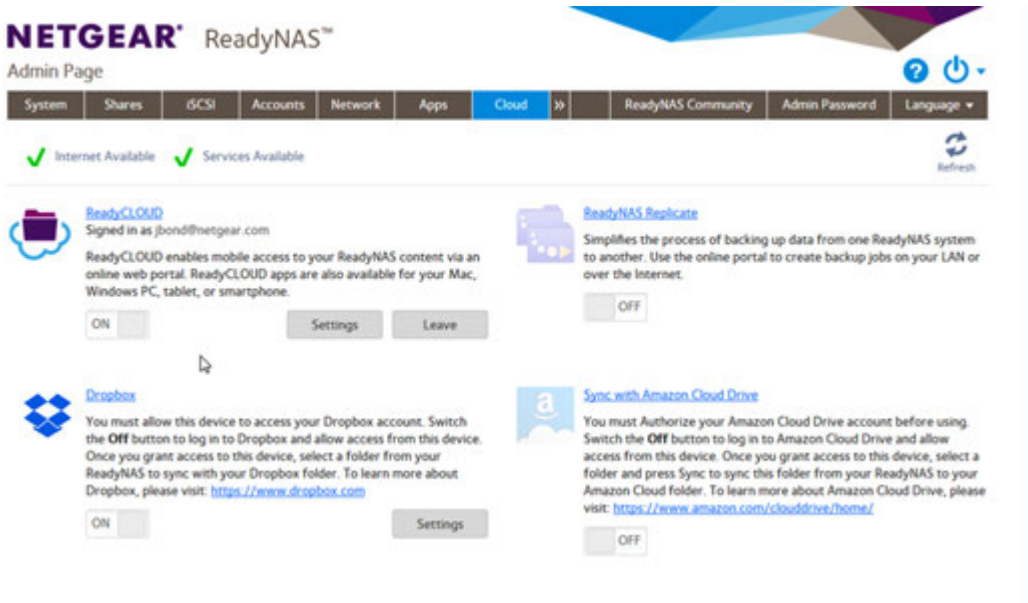
You can sync files between your ReadyNAS and your Amazon S3 space.

You must configure S3 before setting up syncing with your ReadyNAS. As part of the S3 setup process, you get both an S3 access key and an S3 secret key. You must enter both as part of the ReadyNAS synchronization setup. For information about Amazon S3, visit *aws.amazon.com/*.

To set up syncing:

1. Log in to your ReadyNAS.

2. Select **Cloud**.



3. Set the Amazon S3 **On-Off** slider so that the slider shows the **On** position.
   The Amazon S3 window opens.
4. Enter your Amazon S3 access key and secret key.
5. Select from the bucket name menu the desired bucket or select the **Create New Bucket** item, click the **Create** button, and create a new bucket.
6. (Optional) Adjust the upload chunk size, the storage class, the upload and download speed, and whether server-side encryption is used.
7. Click the **Next** button.
   The Amazon S3 - Session window updates.
8. Enter a value in the **Local Path** field by browsing the ReadyNAS to the location that you want to sync.
9. Enter a value in the **Cloud Storage Path** field by browsing the ReadyNAS to the location that you want to sync.
10. In the **Sync Direction** menu, select **Bidirection**, **Download cloud storage changes only**, or **Upload local storage changes only**.
11. Click the **Create** button.
    The Amazon S3 - Session window closes.

The ReadyNAS applies the settings to sync with your Amazon S3 drive.

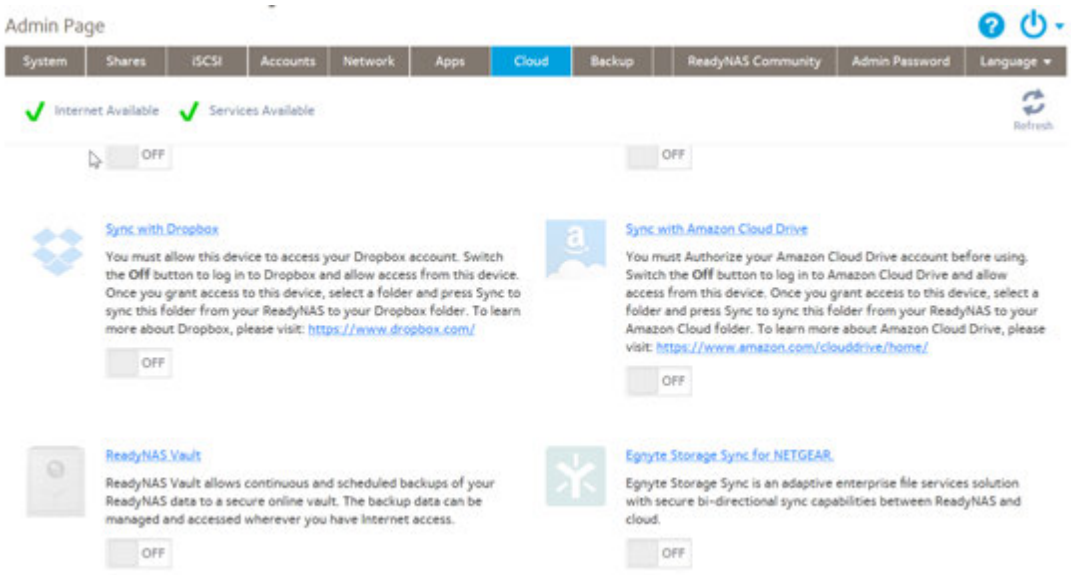
Note You can add and modify Amazon S3 drive session settings by clicking the Amazon S3 Drive **Settings** button.

Sync With 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 **Cloud**.



3. Set the Dropbox **On-Off** slider so that the slider shows the **On** position.
   A new browser window opens and takes you to *https://www.dropbox.com*.
4. Log in to your Dropbox account.
   A message displays asking if you want to allow the ReadyNAS to access your Dropbox account.
5. Click the **Allow** button.
   The Dropbox - Session window opens.
6. Use the Local Path **Browse** button to navigate to and select a location on the ReadyNAS to sync to Dropbox.
7. Use the Cloud Storage Path **Browse** button to navigate to and select a location in Dropbox.
8. Select a sync direction: **Bidirection**, **Download cloud storage changes only**, or **Upload local storage changes only**.
9. Click the **Create** button.
   The Dropbox - Session window closes. The Dropbox **On-Off** slider is now in **On** position. The combination of local path, Dropbox location path, and sync direction is called a session.

You can add, delete, or modify Dropbox sessions by clicking the Dropbox **Settings** button.

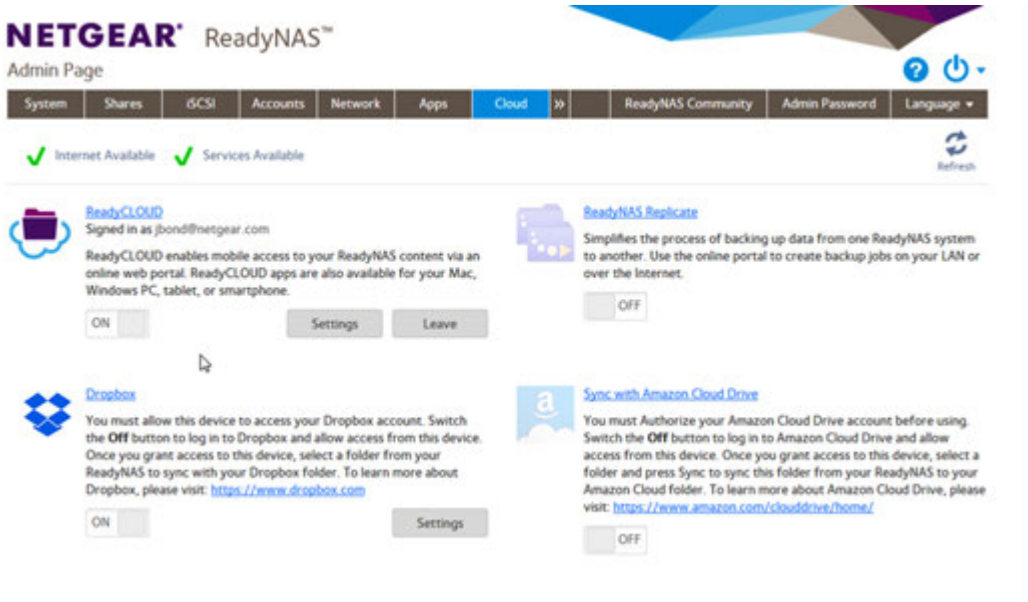
Sync With Egnyte

You can sync files between your ReadyNAS and Egnyte to enable Egnyte file sharing and collaboration.

For information on Egnyte services, visit *egnyte.com*.

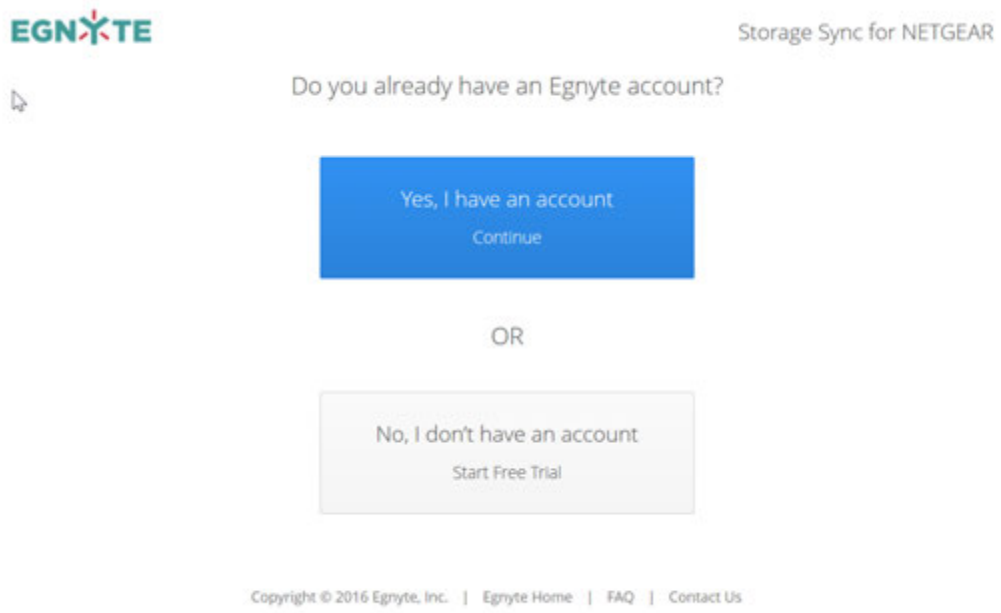
To set up syncing with Egnyte:

1. Log on to your ReadyNAS.
2. Select **Cloud**.



3. Set the Egnyte Storage Sync for NETGEAR **On-Off** slider so that the slider shows the **On** position. The ReadyNAS installs the Egnyte app.

4. Click the **Settings** button.



Note You might need to provide your administrator credentials before the page opens.

5. Select the **Yes, I have an account** button to go to the Egnyte configuration pages, or the **No, I don't have an account button** to first set up an account and then go to the Egnyte configuration pages.
6. Follow the prompts to configure the service.
   During configuration, you:
   a. Map your ReadyNAS users to Egnyte users.
   b. Select Egnyte folders to sync to the ReadyNAS.
   c. Start the sync service.

   The storage sync service is configured and started.
7. If desired, map Mac or Windows computer network drives to the ReadyNAS and the Egnyte sync service. Configured files and folders sync across computers, the ReadyNAS and the Egnyte sync service.

Sync With Google Drive

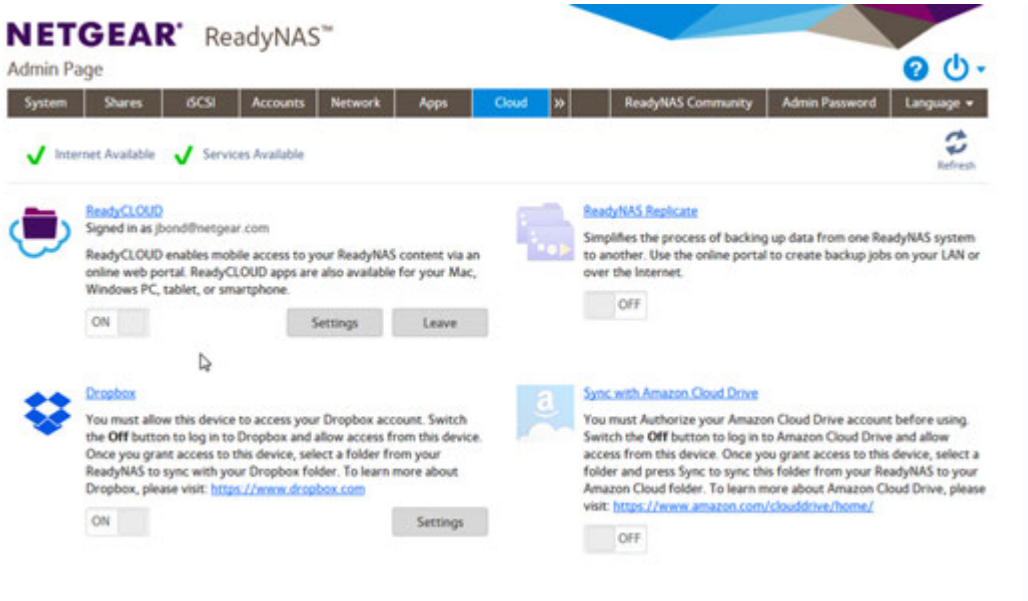
You can sync files between your ReadyNAS and your Google Drive.

For information about Google Drive, visit *drive.google.com/*.

To set up syncing:

1. Log in to your ReadyNAS.

2. Select **Cloud**.



3. Set the Google Drive **On-Off** slider so that the slider shows the **On** position.
   Your default browser opens displaying the Sign in with your Google Account page.
4. Log in to your Google account.

> **Note** If you did not already set up a Google Drive, you are guided through creating one. This requires logging in to, or creating, a Google account.

The page updates with the ReadyNAS would like to: page.

5. Click the **Allow** button.
   The Google Drive - Session window opens.
6. Enter a value in the **Local Path** field by browsing the ReadyNAS to the location that you want to sync.
7. Enter a value in the **Cloud Storage Path** field by browsing to the Google Drive location that you want to sync.
8. In the **Sync Direction** menu, select **Bidirection**, **Download cloud storage changes only**, or **Upload local storage changes only**.
9. Click the **Create** button.
   The Google Drive - Session window closes.

The ReadyNAS applies the settings to sync with your Google drive.

> **Note** You can add and modify Google Drive session settings by clicking the Google Drive **Settings** button. You can also change upload and download speeds.

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.

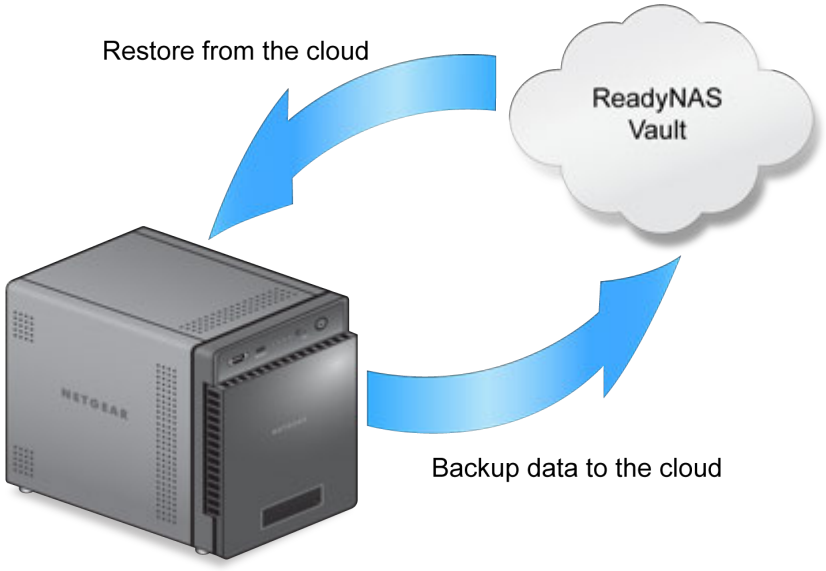
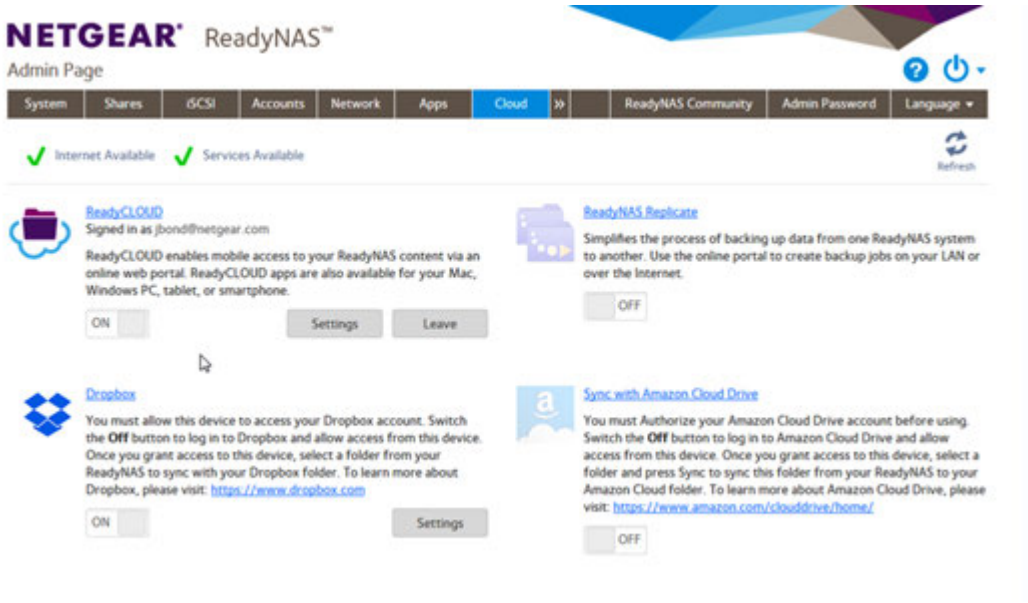


Figure 10. Using a ReadyNAS system to back up and recover data stored on a cloud

To set up ReadyNAS Vault on your system:

1. Log in to your ReadyNAS.
2. Select **Cloud**.



3. Set the ReadyNAS Vault **On-Off** slider so that the slider shows the **On** position.
   The ReadyNAS Vault Settings window opens.
4. From the Select Volume menu, select a volume where temporary data from ReadyNAS Vault can be stored.
5. Enter your ReadyNAS Vault account credentials and click the **Login** button.

   Note If you do not own 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 **Manage ReadyNAS Vault** button displays.
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 information about how to use ReadyNAS Vault, visit *readynasvault.com*.

ReadyNAS Replicate

ReadyNAS Replicate is a free service that allows you to replicate and restore data from one ReadyNAS system to another.

Using ReadyNAS Replicate involves these high-level steps:

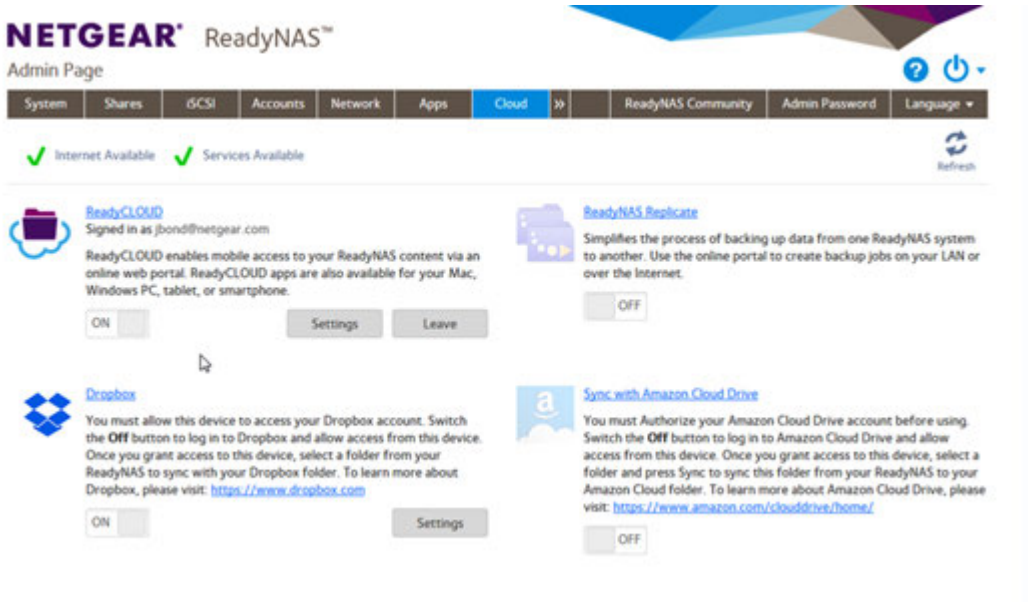
1. Enable ReadyNAS Replicate on your ReadyNAS systems.
   See *Enable ReadyNAS Replicate* on page 157.
2. Log in to the ReadyNAS Replicate web portal and begin replicating data between your ReadyNAS systems.
   For more information about using the ReadyNAS Replicate portal, see the *ReadyNAS Replicate Software Reference Manual* or visit *https://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. Log in to your ReadyNAS.
2. Select **Cloud**.



3. Set the ReadyNAS Replicate **On-Off** slider so that the slider shows the **On** position.
   The ReadyNAS Replicate window opens.
4. Enter your ReadyNAS Replicate login credentials and click the **Register** button, or if you do not have ReadyNAS Replicate credentials, go to *www.replicate.readynas.com*.
   Your system is registered with ReadyNAS Replicate and the ReadyNAS Replicate feature is enabled on your system.
5. 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 Software Reference Manual* or visit *www.replicate.readynas.com*.

System Settings

9

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

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 33.

Customize the Basic System Settings

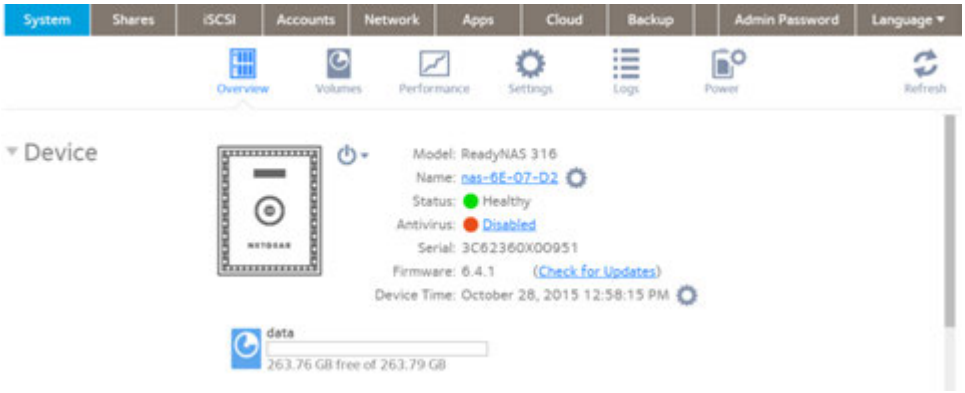
We recommend that you configure the basic system settings: clock, language, administrator password, system alerts, host name, and antivirus, before you use the ReadyNAS.

Set the Clock

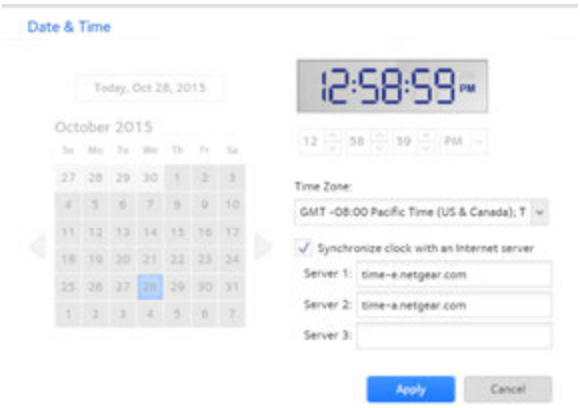
To enable the ReadyNAS to time-stamp files correctly, ensure that the time and date settings are accurate.

To set system time and date:

1. Log in to your ReadyNAS.
2. Select **System > Overview > Device**.



3. Click the **gear** icon to the right of the Device Time field.



4. In the **Time Zone** menu, select the correct time zone for your location.

> **Note** So that your files are correctly time-stamped, we recommend that you select the time zone in which the ReadyNAS is physically located.

5. 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 menus 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.

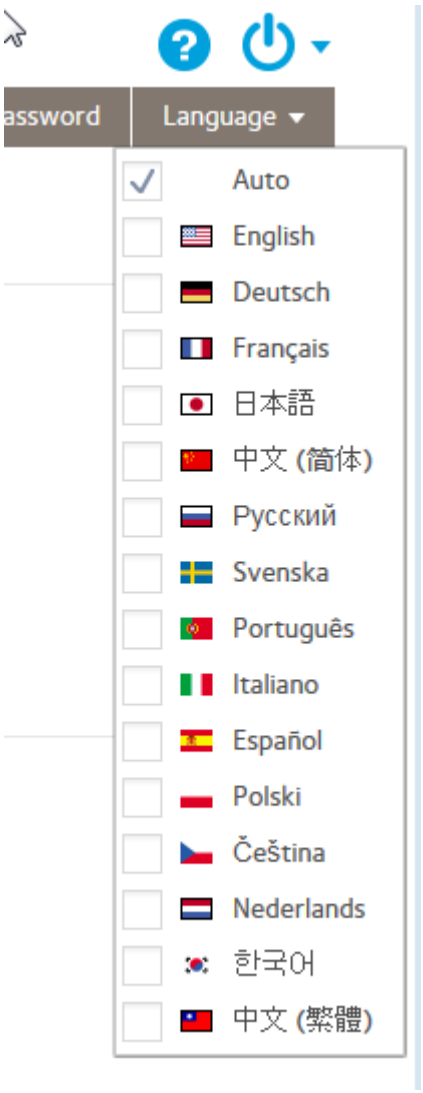
6. Click the **Apply** button.
   Your settings are saved.

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. Log in to the ReadyNAS.
2. Select **Language**.



3. From the **Language** menu, select a language 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 We recommend selecting a language based on the region in which you use the ReadyNAS.

Set the Administrator Password

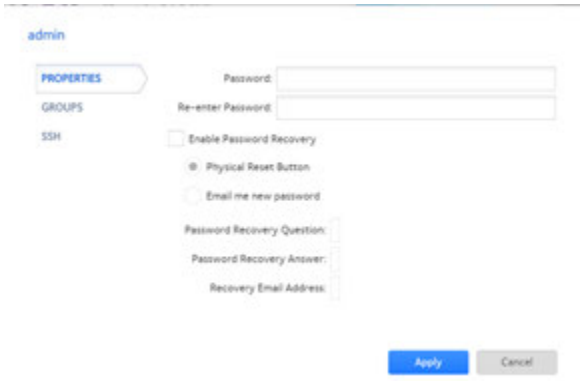
It is important to safeguard the administrator password and to change it regularly to protect your data.

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.

> **Note** Until you change the administrator password you cannot be authenticated as admin when accessing shares.

To change the administrator password:

1. Log in to the admin page.
2. Select **Admin Password**.



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

Item	Description	
Password	Enter a new administrator password.	
Re-enter Password	Confirm the new password.	
Enable Password Recovery	Select this check box to enable password recovery. Note that the **Physical Reset Button** method is available even if you do not enable password recovery, but you need physical access to the ReadyNAS system to use this method.	
Physical Reset Button	By default this button is selected, and you can use NETGEAR's password recovery tool to reset the administrator password to the default value, password. For information on using the password recovery tool with the **Physical Reset Button** method, see *Recover the Administrator Password* on page 224.	
Email me new password	Select this check box to enable password reset through email. Configure email alerts before selecting this option. The alert email connection (email provider, user, password, and so forth) is used to send you a new password.	
Password Recovery Question	Choose a question that few people can answer. For example, you might enter your first dog's name or your 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 224).
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.	

4. Click the **Apply** button.
   Your settings 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.

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

To configure the system alerts:

1. Log in to your ReadyNAS system.
2. Select **System > Settings > Alerts**.
3. 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.
4. 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.

5. Review the **Alert Contacts** list.
   Each address in the **Alert Contacts** list receives alerts.
6. Click the (**+**) icon to add a contact.

   a. Enter the new contact's email in the **Email** field.

   b. Click the **Add** button.

   If the ReadyNAS server recognizes the email provider, it automatically fills in the **Email Account Provider** value, **SMTP Server** address, and the **SMTP Port** number. Otherwise the **Email Account Provider** value is set to **Custom**, and you need to provide the other values.
7. Fill in the password.
8. Click the **Send Test Message and Apply** button.
   The ReadyNAS system attempts to send a test message. A window opens to report failure or success.

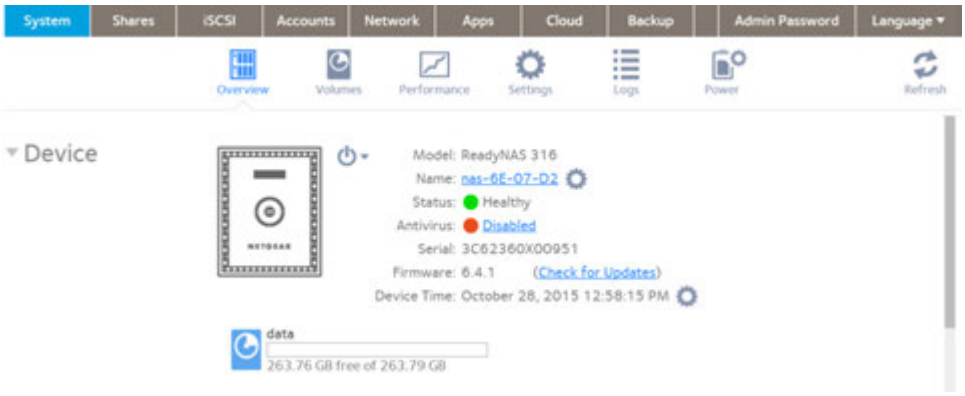
Configure the Host Name

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. Log in to your ReadyNAS.
2. Select **System > Overview > Device**.



3. Click the **gear** icon to the right of the **Name** field.
4. In the **Name** field in the Host Name pop-up window, enter a new host name.
   In most non-Asian character sets, the host name can be a maximum of 15 characters, can include only A–Z, a–z, 0–9, and _, and the first character must be alphabetic. If you use Asian language characters, the limit is lower.
5. Click the **OK** button.
   Your settings 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.

> **Note** The antivirus software requires a valid Internet gateway and DNS to update its antivirus signatures, and updates over networks with proxy servers are not currently supported. Communication is through port 443.

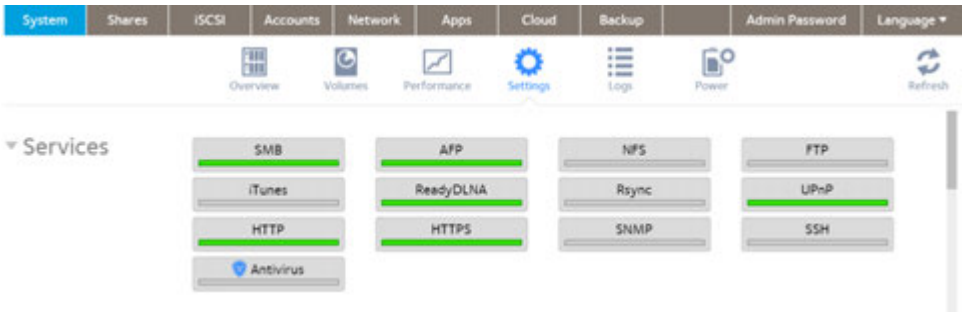
When enabled, the antivirus software scans new files as they are written over the SMB (CIFS) protocol. It does not scan existing files or files transferred over other protocols.

> **Note** To configure advanced settings, install the antivirus app, Anti-Virus Plus. For more information about installing apps, see *Install and Manage Apps* on page 208. With Anti-Virus Plus you can schedule scans, including scans of existing files.

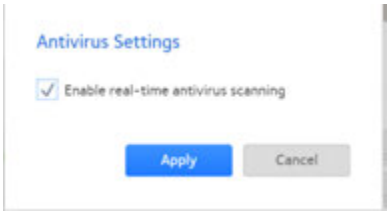
Enabling the antivirus software is optional.

To enable the free antivirus software:

1. Log in 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

The network settings include the Ethernet interface, bonded adapters, and static routes.

Basic Network 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.

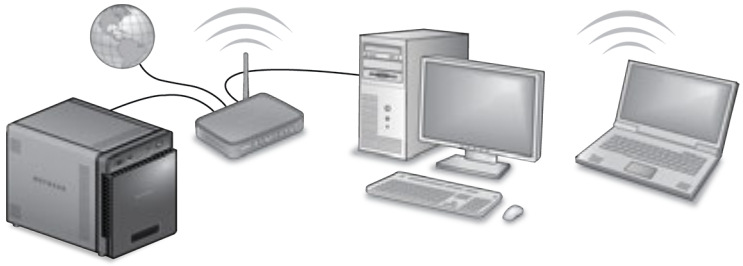


Figure 11. Example home network with ReadyNAS

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 is assigned 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 at least a maximum MTU size of 9214 bytes. (Some models support 9216 bytes.) Use this MTU size only if all components of your network, for example, network interface cards (NICs), hosts, and your switch, support packets of this size or larger. Also MTU sizes greater than the default can affect services such as ReadyCLOUD, ReadyNAS Replicate, and potentially Amazon Cloud.

DNS

DNS is short for Domain Name System. Because IP addresses are strings of numbers, they are hard to remember. It is easier to remember a name (for example, www.netgear.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.

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:

- MTU
- IPv4 settings including DNS servers
- IPv6 settings including DNS servers

The following table shows the default network configuration.

Table 8. Default network settings

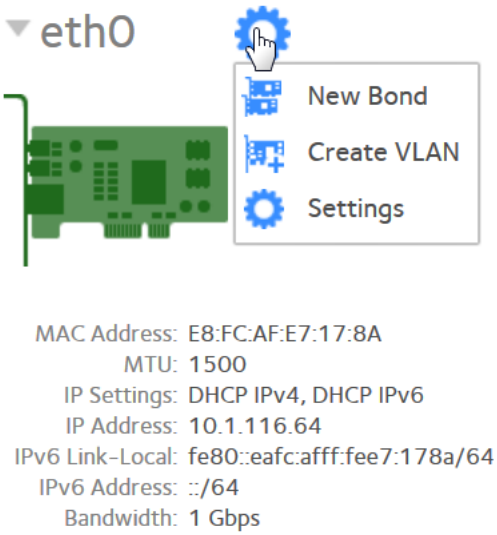
Item	Default Setting
Physical Ethernet interface	
MTU	1500
TCP/IP	IPv4 using DHCP IPv6 using DHCP
DNS	Retrieved using DHCP

Configure General and TCP/IP Settings

To configure an Ethernet interface:

1. Log in to your ReadyNAS.
2. Select **Network**.
   The Ethernet interfaces display.
3. Click the **gear** icon for an Ethernet interface:

   - Ethernet interfaces with active links are colored green.
   - Ethernet interfaces with inactive links are colored gray.



4. Click the **Settings** button in the pop-up menu.
   A window 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. The maximum depends on the ReadyNAS model, but is either 9214 or 9216.

6. Click the **IPv4** tab.
7. Configure the IPv4 settings as explained in the following table.

Note We recommend 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 page.

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 168. 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 14.

Item	Description	
IPv4 settings		
Configure	From the menu, 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. • **Static**. You must enter the IPv4 address and subnet mask for the ReadyNAS, and the router through which the ReadyNAS is connected to the network.	
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.	
+	Click to add a DNS server	
-	Select a DNS server and click to remove that server.	

8. Click the **IPv6** tab.

Item	Description	
IPv6 settings		
Configure	From the menu, select how IPv6 is configured: • **Automatically/DHCP**. 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. • **Static**. You must enter the IPv6 address and prefix length for the ReadyNAS and the router through which the ReadyNAS is connected to the network. • **Disable**. Disables IPv6 networking.	
Router	Enter the IPv6 address for the router through which the ReadyNAS connects to your network. The default setting is **undefined**.	Manual configuration only.
IPv6 Link-Local	Enter the link local address range.	
IPv6 Address	Enter the IPv6 address for the ReadyNAS.	
Prefix Length	Enter the prefix length for the ReadyNAS. The default prefix length is **64**.	
+	Add a DNS server.	
-	Select a DNS server and click to remove that server.	

9. Click the **Apply** button.
Your settings 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. NETGEAR does not recommend bonding interfaces with different speeds, for example bonding a 1 Gb interface with a 10 Gb interface.

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 9. 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 10. Hash type descriptions

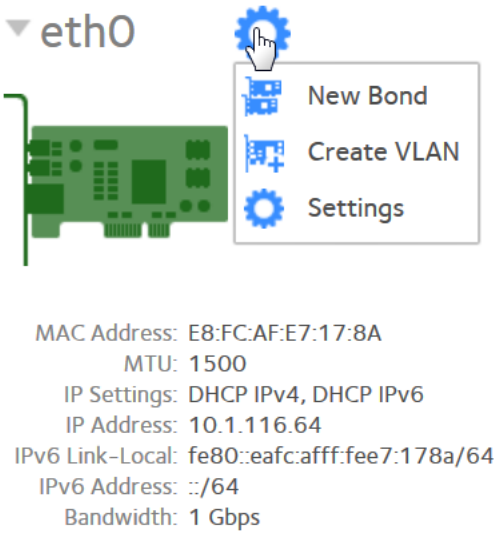
Hash Type	Description
Layer 2	Based on the source and destination MAC addresses. All traffic between the ReadyNAS and a particular device is transmitted on the same physical link.
Layer 3	Based on the source and destination IP addresses. Here too, all traffic between the ReadyNAS and a particular device 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. Log in to your ReadyNAS.
2. Select **Network > Links**.
   The page updates showing the Ethernet interfaces.
3. Click the **gear** icon next to the Ethernet interface you want to bond.



4. Click the **New Bond** button in the pop-up menu.
   A pop-up window opens.
   The options displayed depend on the teaming mode that is selected.
5. In the **Bond with** menu, select another available Ethernet interface to include in the bonded adapter.
6. In the **Teaming Mode** menu, select a teaming mode.
   For more information about teaming modes, see *Teaming Modes* on page 171.

7. (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 171.
8. (For Active Backup only) In the **Primary Device** menu, 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.
9. Click the **Create** button.
   The new bonded adapter displays on the Network page. 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. Log in to your ReadyNAS.
2. Select **Network > Bonds**.
   The page updates showing the bonded interfaces.
3. Click the **gear** icon for the bonded adapter.
4. Click the **Settings** button in the pop-up menu.
   The bond settings pop-up window opens.
5. 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.

6. Click the **IPv4** tab.
7. Configure the IPv4 settings as explained in the following table.

Note We recommend 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 page.

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. 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 Using ReadyCLOUD* on page 14.

Item	Description	
IPv4 settings		
Configure	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. • **Static**. You must enter the IPv4 address and subnet mask for the ReadyNAS, and the router through which the ReadyNAS is connected to the network.	
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.	
+	Click to add a DNS server	
-	Select a DNS server and click to remove that server.	

8. Click the **IPv6** tab.

Item	Description	
IPv6 settings		
Configure	From the menu, select how IPv6 is configured: • **Automatically/DHCP**. 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. • **Static**. You must enter the IPv6 address and prefix length for the ReadyNAS and the router through which the ReadyNAS is connected to the network. • **Disable**. Disables IPv6 networking.	
Router	Enter the IPv6 address for the router through which the ReadyNAS connects to your network. The default setting is **undefined**.	Manual configuration only.
IPv6 Link-Local	Enter the link local address range.	
IPv6 Address	Enter the IPv6 address for the ReadyNAS.	
Prefix Length	Enter the prefix length for the ReadyNAS. The default prefix length is **64**.	

(Continued)

Item	Description
+	Add a DNS server.
-	Select a DNS server and click to remove that server.

9. Click the **Apply** button.
   Your settings are saved.
10. 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:

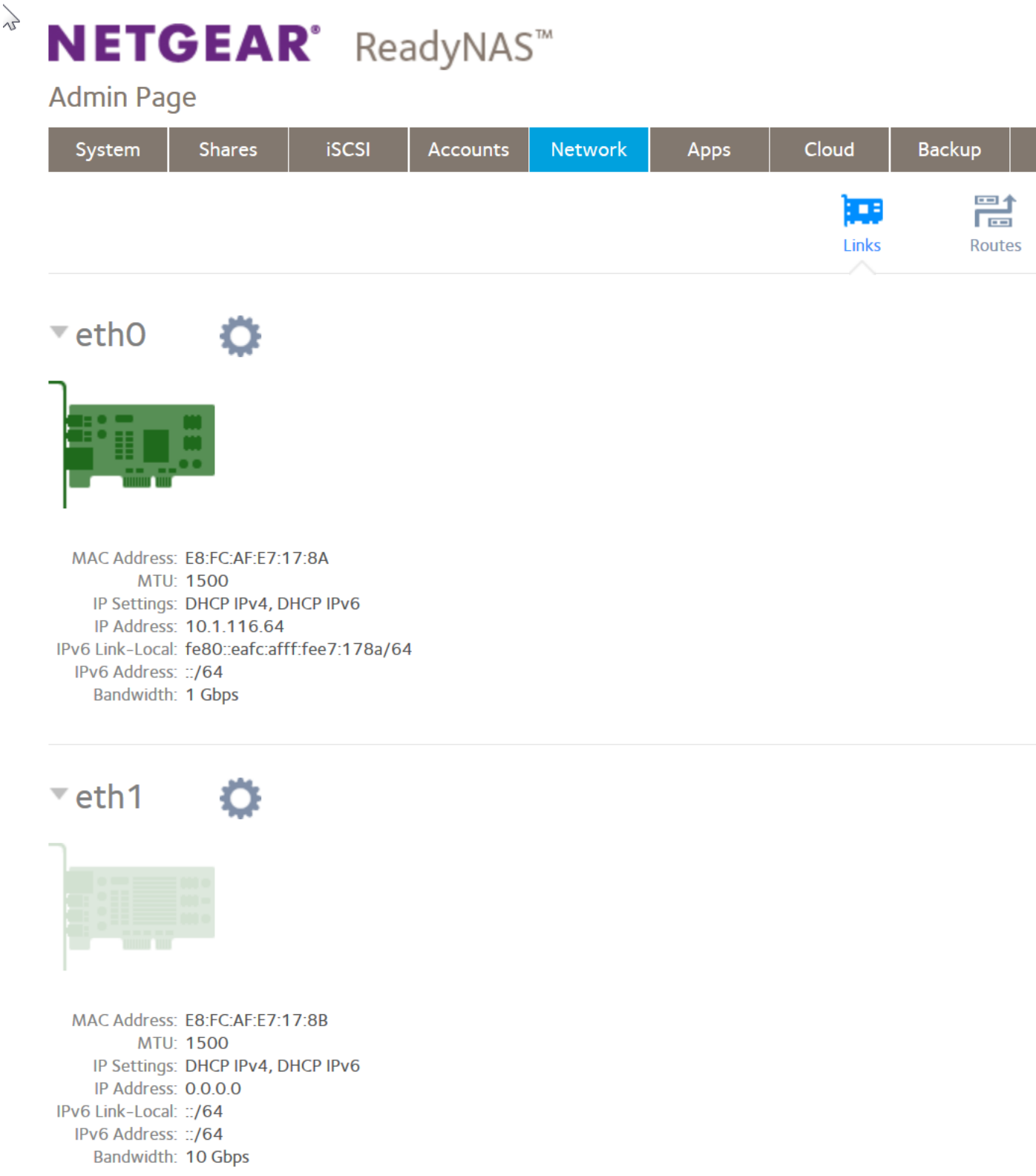
1. Log in to your ReadyNAS.
2. Select **Network > Bonds**.
   The page updates showing the bonded interfaces.
3. Click the **gear** icon for the bonded adapter.
4. Click the **Settings** button in the pop-up menu.
   The bond settings pop-up window opens.
5. Click the **Mode** tab.
6. In the **Teaming Mode** menu, select a teaming mode.
   For more information about teaming modes, see *Teaming Modes* on page 171.
7. (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 171.
8. (For Active Backup only) From the **Primary Device** menu, 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.
9. Click the **Apply** button.
   Your settings are saved.

Delete a Bonded Adapter

To delete a bonded adapter and reestablish separate Ethernet links:

1. Log in to your ReadyNAS.
2. Select **Network > Bonds**.
   The page updates showing the bonded interfaces.
3. Click the **gear** icon for the bonded adapter.
4. Click the **Delete** button in the pop-up menu.
5. Confirm the deletion.

The bonded Ethernet interfaces are separated into individual links.



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

Configure Static Routes

You can add and remove static routes. Static routes are not frequently used with ReadyNAS, but a few situations call for them. For example, if no automatically routed path to a device exists that the ReadyNAS must access, you can define a static path to it.

Before configuring a static route, you must configure the ReadyNAS adapter, its Ethernet address, and subnet mask.
To configure a static route, there must be a gateway between the network the ReadyNAS is on, and the network with the destination address. There is an address for the gateway on the network the ReadyNAS is on, and there is an address for the gateway on the network the destination address is on. Before configuring the static route, determine the gateway address on the network the ReadyNAS is on. You must also know the target IP address and the subnet mask for the target's network.

As a sample configuration, your ReadyNAS uses separate network connections to connect to the Internet and to a private network, and the default gateway is configured to connect to the Internet. The ReadyNAS can connect to anything on the private network and on the Internet, but if another private network is connected to the private network, the ReadyNAS cannot automatically find devices on the second private network. For example, one network interface on the ReadyNAS might use the address 10.1.0.1 to connect to a private network with addresses in the range 10.1.xxx.xxx. The 10.1 network connects to a private network with a server with the address 192.168.1.0 and with subnet mask 255.255.255.0. No automatic route exists from the ReadyNAS to the server, but you can specify a static route. For this example, the address 10.1.0.2 is the address of the gateway between the two private networks.

To configure a static route:

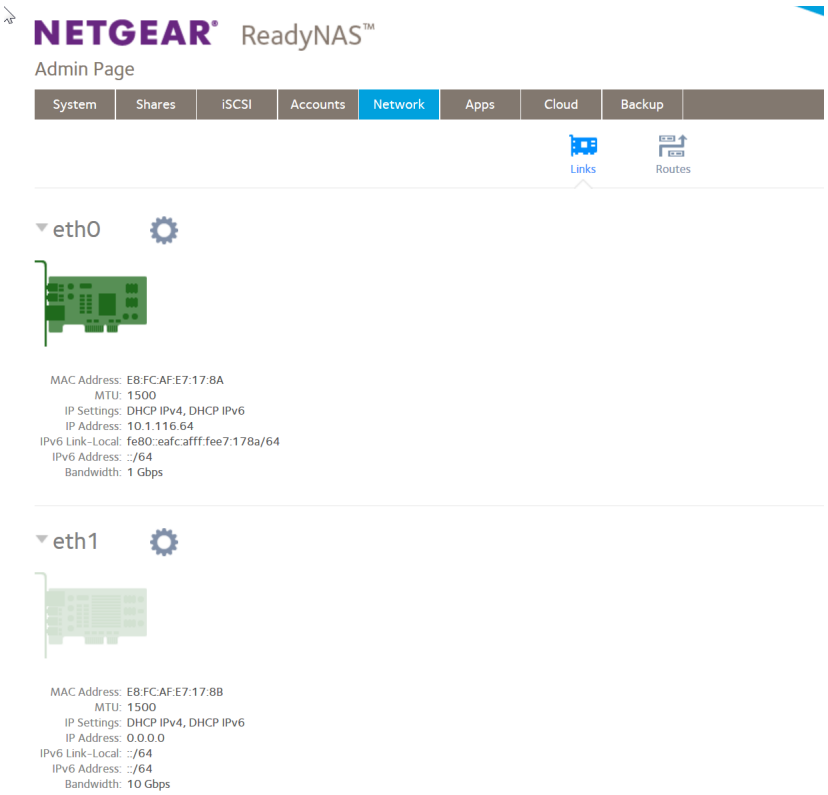
1. Log in to your ReadyNAS admin page.
2. Select **Network > Routes**.
   The window updates to show the configured routes.
3. Click the **+** button.
   The New Route page displays.
4. Enter the destination IP address in the **IP Address** field.
   In the sample configuration, the destination IP address is the address of the server, 192.168.1.0.
5. Enter the subnet mask for the destination network in the **Subnet Mask** field.
   In the sample configuration, the subnet mask is 255.255.255.0.
6. Enter the gateway address configured on the ReadyNAS in the **Gateway** field.
   In the sample configuration, the gateway address is 10.1.0.2.
7. Select the adapter on the ReadyNAS used for the private network from the **Adapter** menu.
   The IP address and subnet mask for that adapter fills automatically.
8. Click the **Add** button.
   The new static route shows in the list of routes.

Create a VLAN

You can create VLANs from any of the Ethernet interfaces on your ReadyNAS device.

To create a VLAN:

1. Log in to the ReadyNAS.
2. Select **Network**.



   Ethernet interfaces with active links are colored green. Ethernet interfaces with inactive links are colored gray.

3. Click the **gear** icon for an Ethernet interface.

   A pop-up window opens.

4. Click the **Create VLAN** button in the pop-up window.
   The Create VLAN window opens with **Name** and **VLAN ID** fields. The name field is grayed out.

   Note There can be no more than one VLAN ID on a network interface.

5. Type a number in the **VLAN ID** field.

   The ID value is a number from 1 to 4094.

   The name field is automatically populated with the VLAN name. The format is eth*n*.*VLAN ID* where *n* is the Ethernet interface number and *VLAN ID* is the number that you entered.

6. Click the **Add** button.
   The VLAN interface is created with Ethernet interface settings matching the Ethernet interface that you selected in *Step 3*.

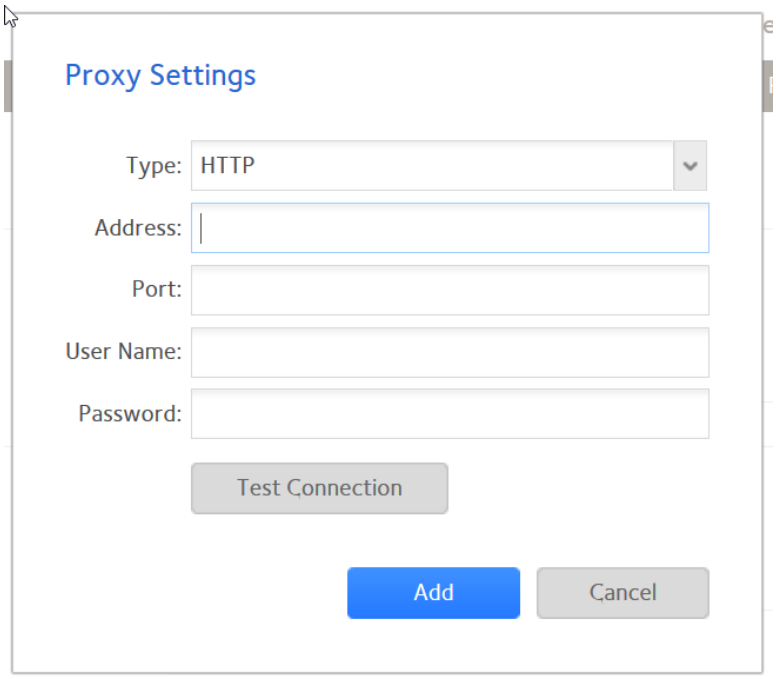
You can change the Ethernet settings. For information about changing the settings, see *Configure the Ethernet Interfaces* on page 168.

Add Global Proxy Settings

Your ReadyNAS system automatically configures some proxy settings. For example, ReadyCLOUD access provides a set of default proxy requirements. However, you can also manually configure proxy settings.

To add global proxy settings:

1. Log in to your ReadyNAS local admin page.
2. Select **Network**.
   The page updates to show network options.
3. Select **Advanced**.
   The page updates to show the advanced network options.
4. Click the add (plus) button in the Proxy section of the page.



5. Enter the proxy settings.

> **Note** User name and password are required only if user account authentication is required by the proxy server.

6. (Optional) Click the **Test** button
   The test attempts to connect to a NETGEAR server using the proxy settings. A window opens reporting success or failure of the connection. You can click the **Ignore** button to close the window.
7. Click the **Apply** button.
   The settings window closes and the new proxy settings display in the Proxy section of the page.

You can change existing settings by selecting the setting, clicking the **settings** icon, and editing entries. You can delete the setting by selecting the setting, clicking the **minus** icon, and confirming the deletion on the proxy window.

Configure Global Settings for System Services

File sharing protocols, for example, SMB or NFS, must be enabled for the ReadyNAS. When enabled, some of the protocols can be disabled for specific shares, or require additional configuration settings for individual accounts.

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.)

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 61.

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 System Services

The ReadyNAS supports the following system services:

Table 11. Supported System Services

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 referred to as the CIFS (Common Internet File Service) file-sharing protocol. SMB uses TCP/IP.	If Windows users access your storage system, enable this protocol.
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, We recommend using SMB only.

Table 11. Supported System Services (Continued)

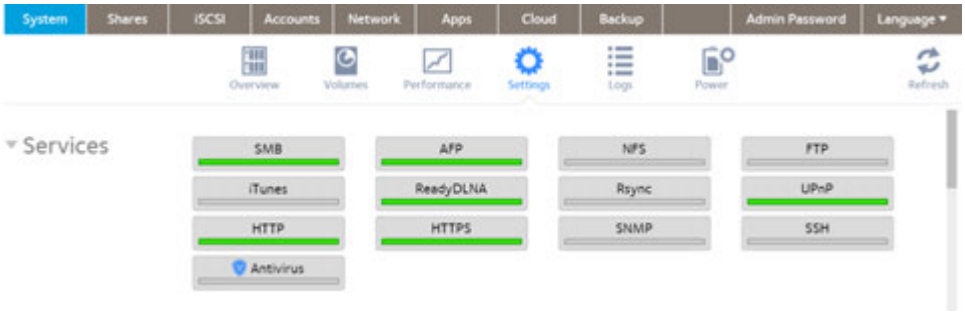
Protocol	Description	Recommendation
FTP (File Transfer Protocol) and FTPS (FTP with SSL encryption)	Many public file upload and download sites use FTP. The ReadyNAS supports anonymous or user access for FTP clients. You can elect to set up port forwarding to nonstandard ports for passive FTP, allowing 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, we recommend 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 and NFS are disabled.

Configure System Services

To configure global settings for system services:

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 window.

3. Configure one protocol at a time, as explained in the following sections.

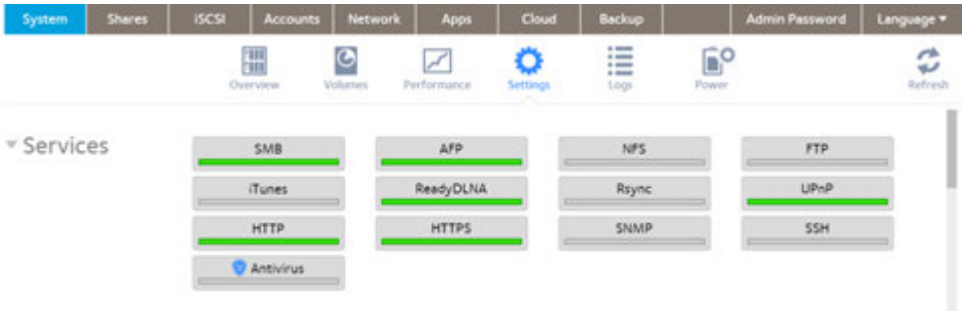
- *Configure SMB, AFP, Rsync, or SSH* on page 182.
- *Configure FTP* on page 183.
- *Configure NFS* on page 184.
- *Configure HTTP* on page 185.
- *Configure HTTPS* on page 186.

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. Log 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.

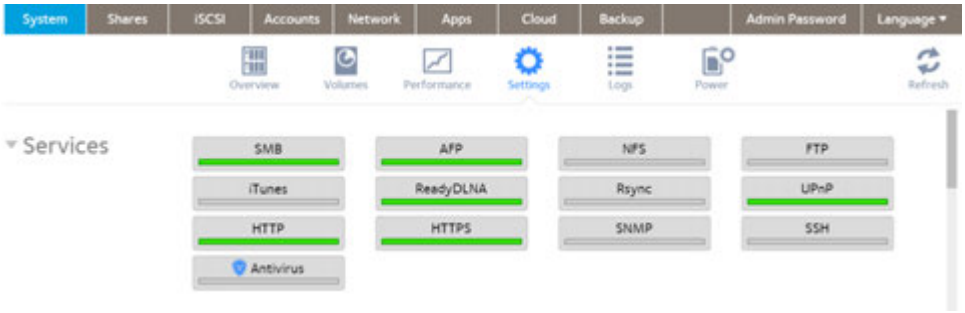
WARNING:
If you enable SSH root access, NETGEAR might deny you technical support. If you do enable SSH root access, the root password is identical to the administrator password that you configured.

Note After you enable SSH, you must configure individual user accounts to permit use of SSH. For information about how to enable the use of SSH by a user, see *Configure a User Account to Use SSH* on page 188.

Configure FTP

To configure FTP:

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



3. Click the **FTP** button.

4. 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 menu: • **Anonymous**. Users can connect anonymously. • **User**. Users are authenticated through the local database. This is the default setting.

(Continued)

Item	Description	
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.
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 215.	

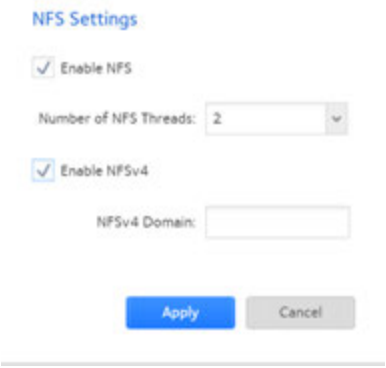
5. Click the **Apply** button.
   Your settings are saved.

Configure NFS

To configure NFS:

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

3. Click the **NFS** button.



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

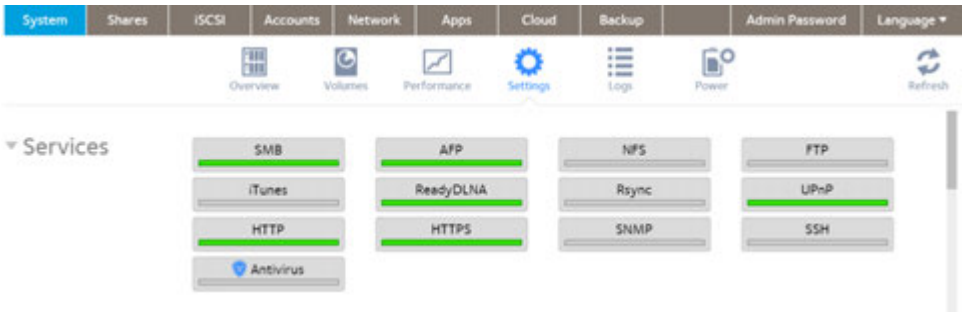
Item	Description
Enable NFS	Select the check box to enable NFS globally. Clear the check box to disable NFS globally.
Number of NFS Threads	If many clients connect to the ReadyNAS using the NFS protocol, increasing the number of NFS threads can improve performance.
Enable NFSv4	Select the check box to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

5. Click the **Apply** button.
Your settings are saved.

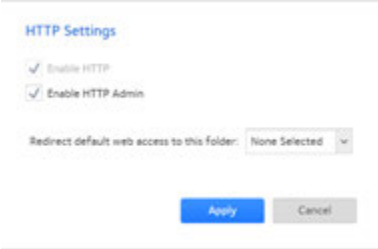
Configure HTTP

To configure HTTP:

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



3. Click the **HTTP** button.



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

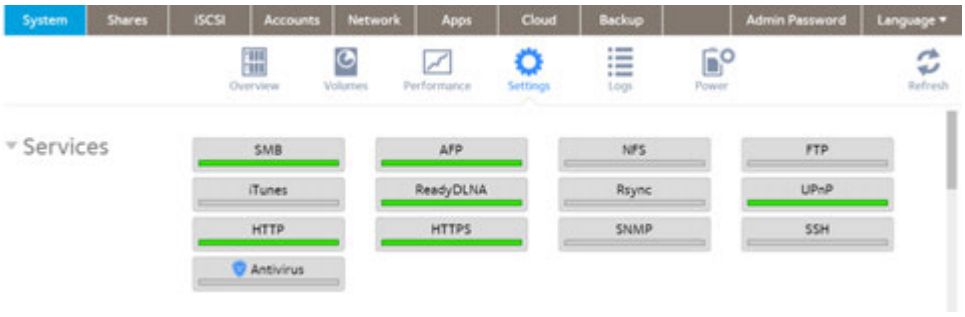
Item	Description
Enable HTTP	HTTP is always enabled.
Enable HTTP Admin	Select the check box to enable HTTP access to the local admin page. If this check box is cleared, attempts to access the local admin page using HTTP are automatically connected using HTTPS.
Redirect default web access to this folder	If you want to automatically redirect http://<ReadyNAS_IP_address> to a certain shared folder, select that folder from the menu. 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. Only folders with HTTP enabled for the folder, display in the menu.

5. Click the **Apply** button.
   Your settings are saved.

Configure HTTPS

To configure HTTPS:

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



3. Click the **HTTPS** button.

4. 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 must 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. We recommend 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, We recommend 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.

5. Click the **Apply** button.
Your settings are saved.

Download an SSH Public Key File

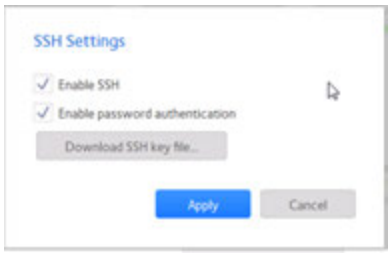
Every ReadyNAS system generates a public and a private SSH key. Before another system can connect to your ReadyNAS system through SSH, you must download and share the public key.

SSH must be enabled before you can download the key. You enable SSH in the same SSH Settings window from which you download the key, so you can do both at the same time.

To download the public key file:

1. Log in to your ReadyNAS system.

2. Select **System > Settings > Services > SSH**.



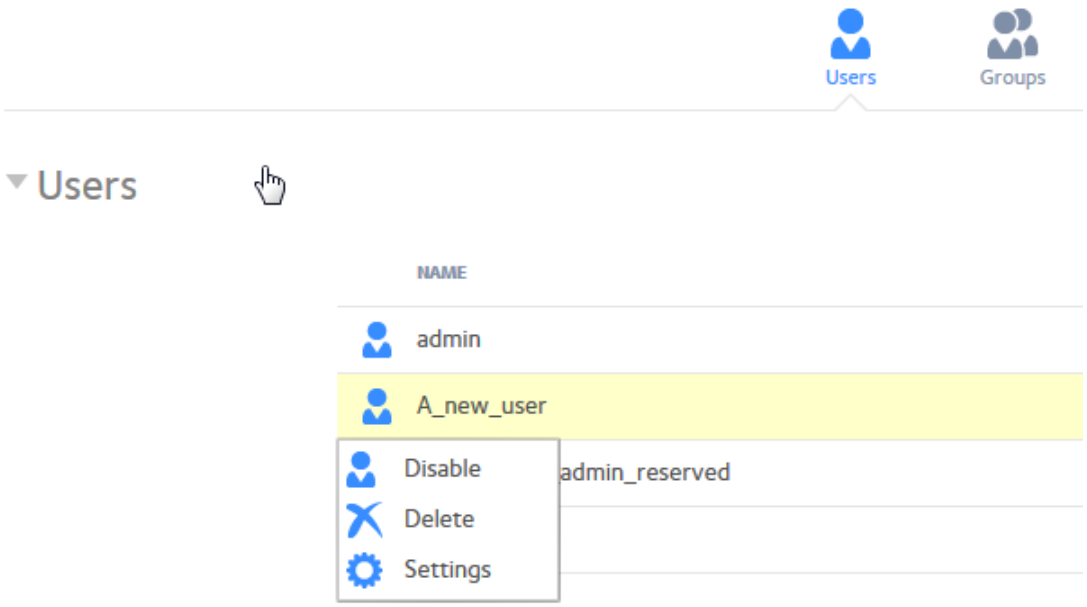
3. Click the **Download SSH key file** button.
   A window opens in your browser for selecting and downloading a file.
4. Follow your browser s procedure to save the file.
5. Click the **Apply** button or the **Cancel** button to close the SSH Settings window.

Configure a User Account to Use SSH

Before a user can use SSH, for example for remote backups, you must configure the user account for SSH.

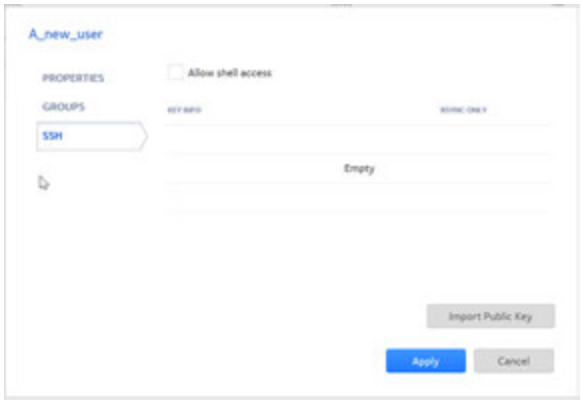
To add SSH usage to a user account:

1. Log in to your ReadyNAS.
2. Select **Accounts > Users**.
   The page updates and shows the list of users.
3. From the list of users, select the user account.



4. Click the **Settings** button in the pop-up menu.

5. Select the **SSH** label.



6. Click the **Import Public Key** button, if you want to add a public key.

> **Note** For each system you want to use SSH keys with, you must import the public key.

For each system, do the following:

a. Enter the location of the public key for the other system, or click the **Browse** button.

b. Click the **Upload** button.
The public key is imported, the Import Public Key window closes, and the public key is listed in the Key Info column.

7. To allow shell access, select the **Allow shell access** box.

8. To restrict the use of SSH for Rsync only, select the **RSYNC ONLY** check box for that system.

> **Note** Restricting SSH use to Rsync only reduces the security concerns introduced by enabling SSH.

9. Click the **Apply** button.
Your settings are saved.

Configure Media Services

You can configure the settings for ReadyDLNA, including creating a TiVo archive, 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.

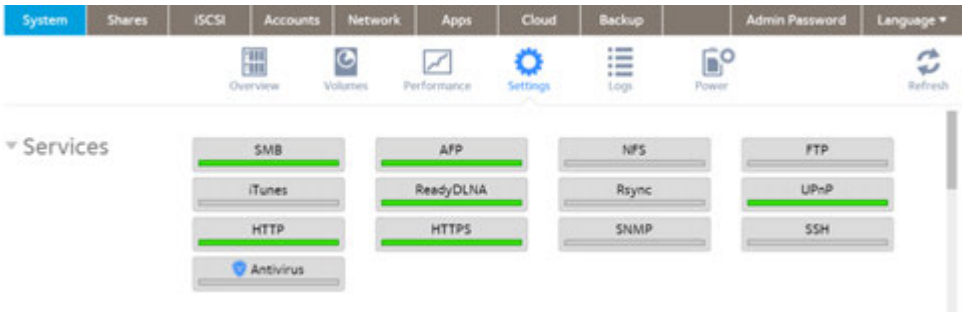
ReadyDLNA supports to following formats:

- **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`

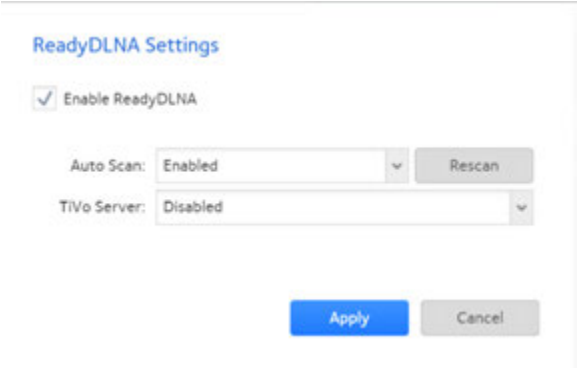
Enable ReadyDLNA

To enable the ReadyDLNA streaming service:

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



3. Click the **ReadyDLNA** button.



4. Select the **Enable ReadyDLNA** check box.
5. (Optional) In the **Auto Scan** menu, select **Enabled** or **Disabled**:

   - **Enabled**. The system automatically searches for DLNA-compliant devices.
   - **Disabled**. The system does not search for DLNA-compliant devices.

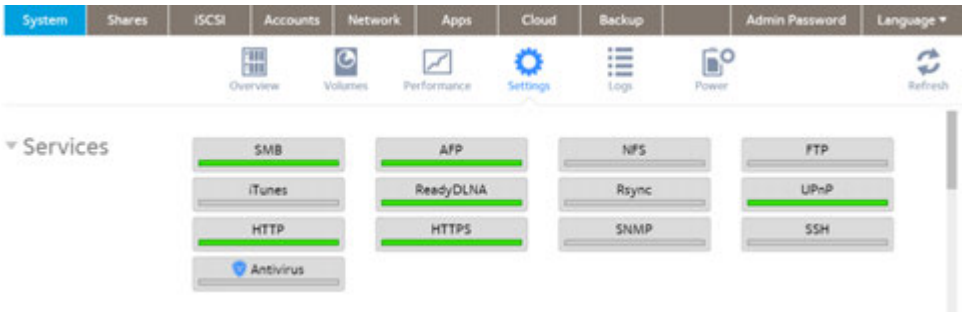
6. Click the **Apply** button.
   Your settings are saved.

Create a TiVo Archive

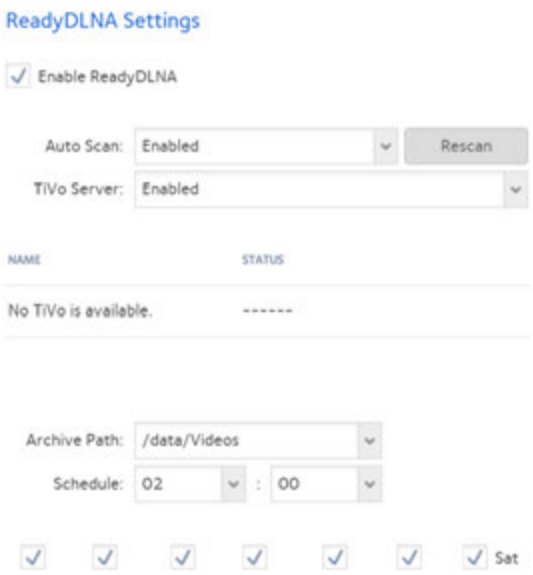
You can use your ReadyNAS system to store videos and media recorded on your TiVo box. The ReadyNAS downloads data from your TiVo box according to a schedule that you specify.

To create an archive of your TiVo data on your ReadyNAS:

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



3. Click the **ReadyDLNA** button.



4. Select the **Enable ReadyDLNA** check box.
5. In the **Auto Scan** menu, select **Enabled**.
6. Click the **Apply** button.
   Your settings are saved.
7. Again click the **ReadyDLNA** button.
   The ReadyDLNA Settings window opens.
8. In the **TiVo Server** menu, select **Enabled**.
   The system detects TiVo devices on your LAN and displays them in the list.
9. When prompted, enter the media access key provided by your TiVo box.
10. Select the **Activate** check box next to the name of your TiVo box.
11. In the **Archive Path** menu, select the path to the folder where you want to store data downloaded from your TiVo.
12. Use the check boxes and menus to schedule the time and days that the ReadyNAS downloads data from your TiVo box.
13. Click the **Apply** button.
    Your settings are saved.

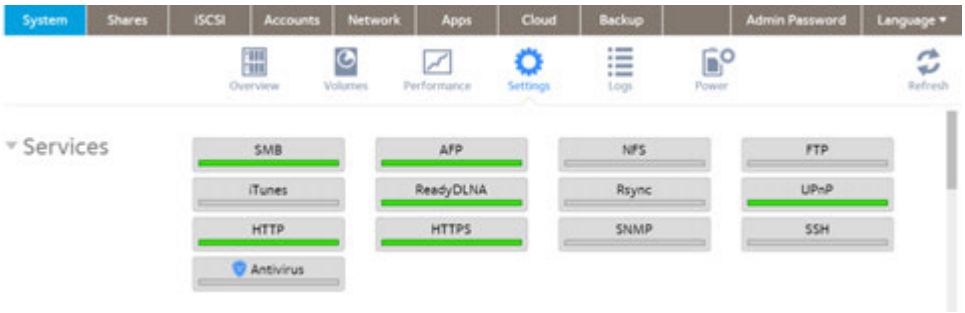
iTunes Streaming Server

iTunes Streaming Server enables iTunes clients to stream media files straight from your ReadyNAS system. The ReadyNAS supports the following iTunes formats:

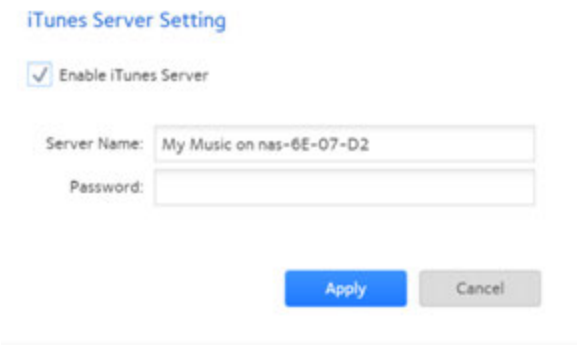
- **Audio**. mp3, m4a, m4p, wav, aif
- **Video**. m4v, mov, mp4
- **Playlist**. m3u, wpl

To set up iTunes Streaming Server:

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



3. Click the **iTunes** button.



4. 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.

5. Click the **Apply** button.
Your settings are saved.

Configure Discovery Services

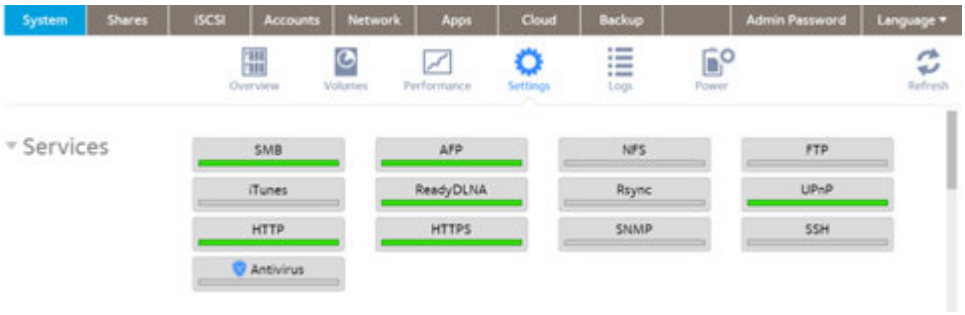
Discovery services are protocols that allow network-enabled devices like computers or your storage system to discover each other across networks. Your storage system supports the Bonjour and UPnP discovery service protocols:

- **Bonjour**. Enables discovery of various services on your ReadyNAS system and provides a way to connect to the local admin page for your ReadyNAS and AFP services. OS X includes 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:

Note UPnP is used with ReadyCLOUD. If you use ReadyCLOUD, leave UPnP enabled.

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



3. Click the **UPnP** button.
   - If the indicator is green, the protocol is enabled.
   - If the indicator is gray, the protocol is disabled.

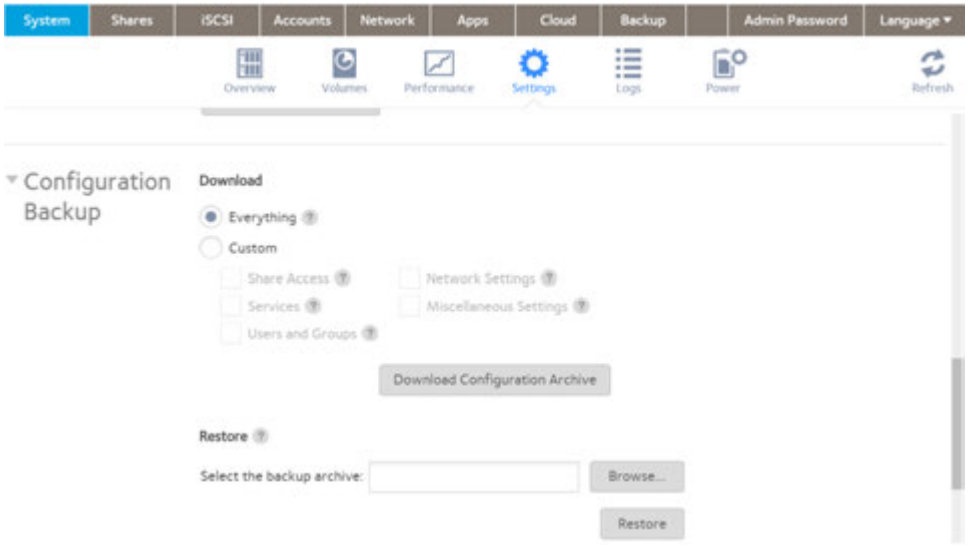
Back Up or Restore System Configuration

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.

Back Up Your System Configuration

To back up your system configurations:

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

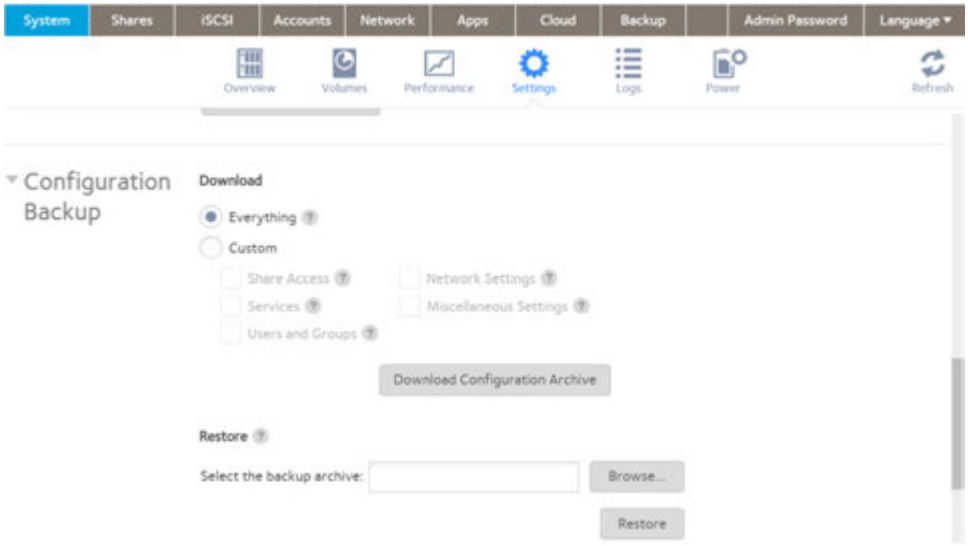


3. Select the **Everything** radio button or select the **Custom** radio button and select the check boxes for the settings to back up.
4. Click the **Download Configuration Archive** button.
   The selected system configuration settings are saved to a file that is downloaded to your computer.

Restore Your System Configuration

To restore system configuration from a file:

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



3. Click the **Browse** button to find the file containing your previously backed-up system configuration settings and select it.
4. Click the **Restore** button.
   The system configuration settings are restored according to the backup file that you selected.

System Power

10

You can manage some aspects of system power consumption. You can also use optional uninterruptible power supplies (UPS) to maintain operation during power outages.

This chapter includes the following topics:

Manage Power Usage

You can configure settings on your ReadyNAS system to reduce power consumption.

Enable the Power Timer

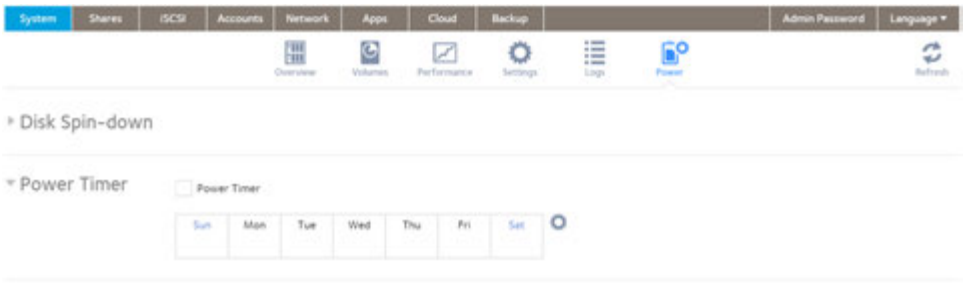
You can configure your ReadyNAS system to power itself on and off automatically according to a schedule.

CAUTION:

If you schedule this device to power off, data transfers are interrupted, pending backup jobs do not run, and snapshots are not taken.

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 window 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 settings are saved.

Enable Wake-on-LAN

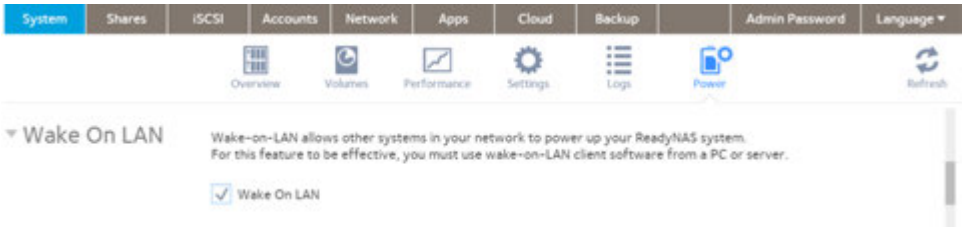
Wake-on-LAN is a way to remotely power up a network-attached device, like a computer or storage system. This feature allows you to conserve power by keeping a device turned off when it is not needed, but allows a remote system to turn it on when it is needed.

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.

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.

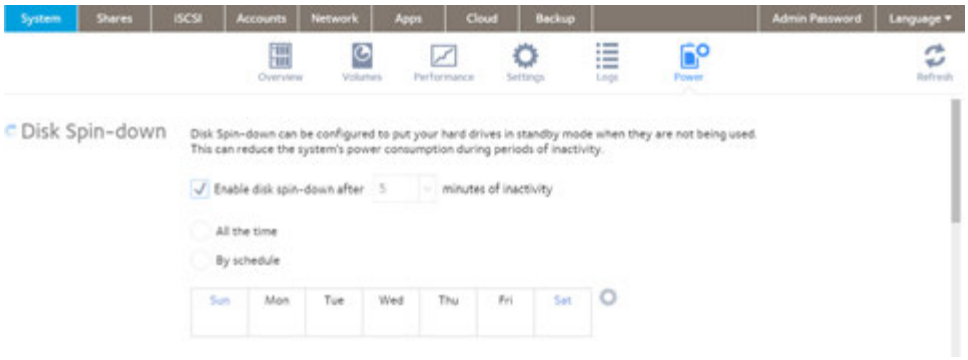
Note Hourly snapshots are not taken for spun-down disks, but daily snapshots are taken.

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**.
   The page updates showing the power settings.
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, use the **minutes of inactivity** menu to select a delay of between 5 minutes and 240 minutes of inactivity before the disks spin down.

6. Click the **Settings** icon to open a calendar.

7. Use the calendar to set the days and times in which spin-down is active. You can set, and the ReadyNAS system will remember, calendar settings whether spin-down is enabled or not.
8. Click the **Apply** button.
   Your settings are saved.

Optional Uninterruptible Power Supplies

Your ReadyNAS system supports the use of uninterruptible power supply (UPS) devices.

Uninterruptible Power Supplies

We recommend 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 the UPS internal battery voltage drops to the UPS low voltage setting, and the UPS sends a signal to the ReadyNAS, the ReadyNAS automatically shuts down gracefully.

UPS Configurations

The ReadyNAS supports UPS devices managed over SNMP, USB, and 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 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

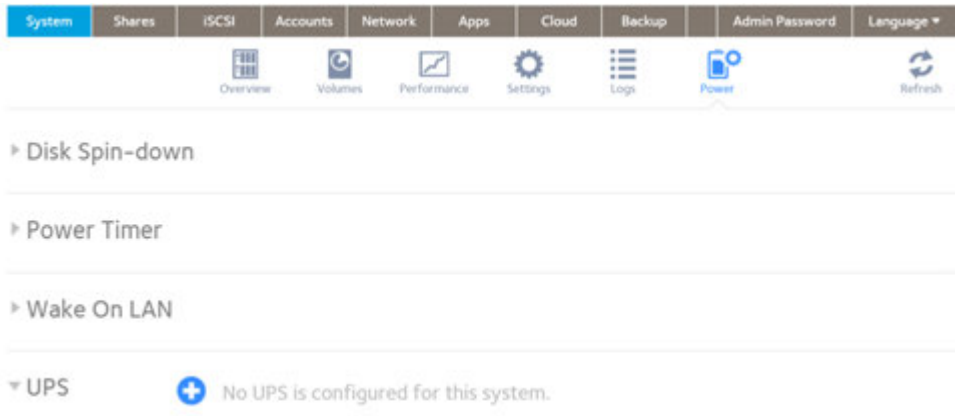
You can manually add, edit, and remove UPS devices as well as monitor the status of connected UPS devices.

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 pop-up Add UPS window opens. The available settings depend on whether you select **SNMP** or **Remote** in the **Type** pop-up menu.
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.

(Continued)

Item	Description	
Type	From the menu, 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 menu, 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 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 section.

Monitor a UPS

To monitor the status of a UPS:

1. Log in to your ReadyNAS.
2. Select **System > Power**.
   The window updates showing the power sections.
   When the ReadyNAS system detects the UPS device, it displays the following information about the device in the UPS list:

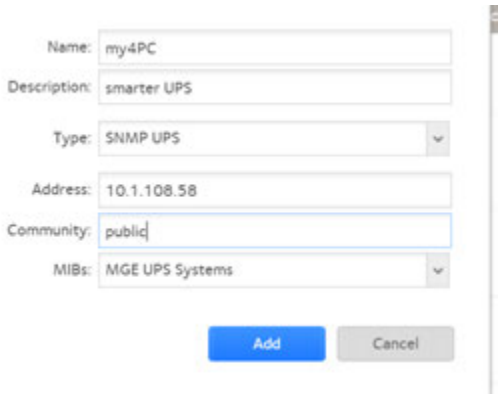
Item	Description
Status	The status of the UPS: • On line power • On battery • Low battery • On battery and Low battery • On line power and Low battery • Unknown
Name	The name of the UPS. For a remote UPS, the name is always UPS.
Description	The description that you gave the UPS.
Serial	The detected serial number of the UPS.
Model	The detected model of the UPS.
MFR	The detected manufacturer of the UPS.
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**.
   The window updates showing the power sections.
3. In the UPS section, select the UPS.
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 pop-up window depend on the type of UPS.

6. Modify the settings as required.
You cannot change the **Type** setting.
7. Click the **Apply** button.
Your settings 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**.
The window updates showing the power sections.
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.

ReadyNAS and Surveillance Video Management

11

You can install the ReadyNAS Milestone Arcus app on your server to view, store, and manage video streams.

Two 90-day free trial licenses are available for each business class ReadyNAS server:

- RN422
- RN424
- RN426
- RN428
- RN524X
- RN526X
- RN528X
- RN626X
- RN628X
- RR2304
- RN3138
- RR3312
- RR4312X
- RR4360X

You can buy additional full licenses directly from your ReadyNAS.

Before you can use the Milestone Arcus app, you must install and configure it. For information about installing the app, see the *ReadyNAS Milestone Arcus User Manual*, which is available at *https://www.netgear.com/support/product/ReadyNAS_OS_6.aspx*.

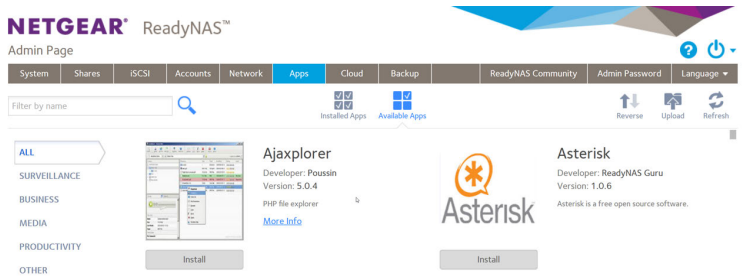
Installing the Milestone Arcus App 12

The Milestone Arcus app is available in the **SURVEILLANCE** section of the **Apps** page.

To install the app on your ReadyNAS:

1. Log in to your ReadyNAS.
2. Select **Apps > Available Apps**.

> **Note** The apps are listed in alphabetical order. Click the `Reverse` icon to change the order from A through Z to Z through A and back. You can also filter the apps listed by entering all or part of a name in the search field.



3. Click the **SURVEILLANCE** button.
   The window updates showing the surveillance specific apps.
4. Click the **Install** button below the app.
   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**.

Install and Manage Apps

13

From the local admin page, you can install and manage apps for your ReadyNAS, as follows:

- To install apps, select **Apps > Available Apps**.
  For information about installing apps, see *Install Free Apps* on page 209.
- To view your installed apps, select **Apps > Installed Apps**.
  For information about managing installed apps, see *Install and Manage Apps* on page 208.
  This chapter contains the following sections:
  - *Install Apps*
  - *Manage Installed Apps*

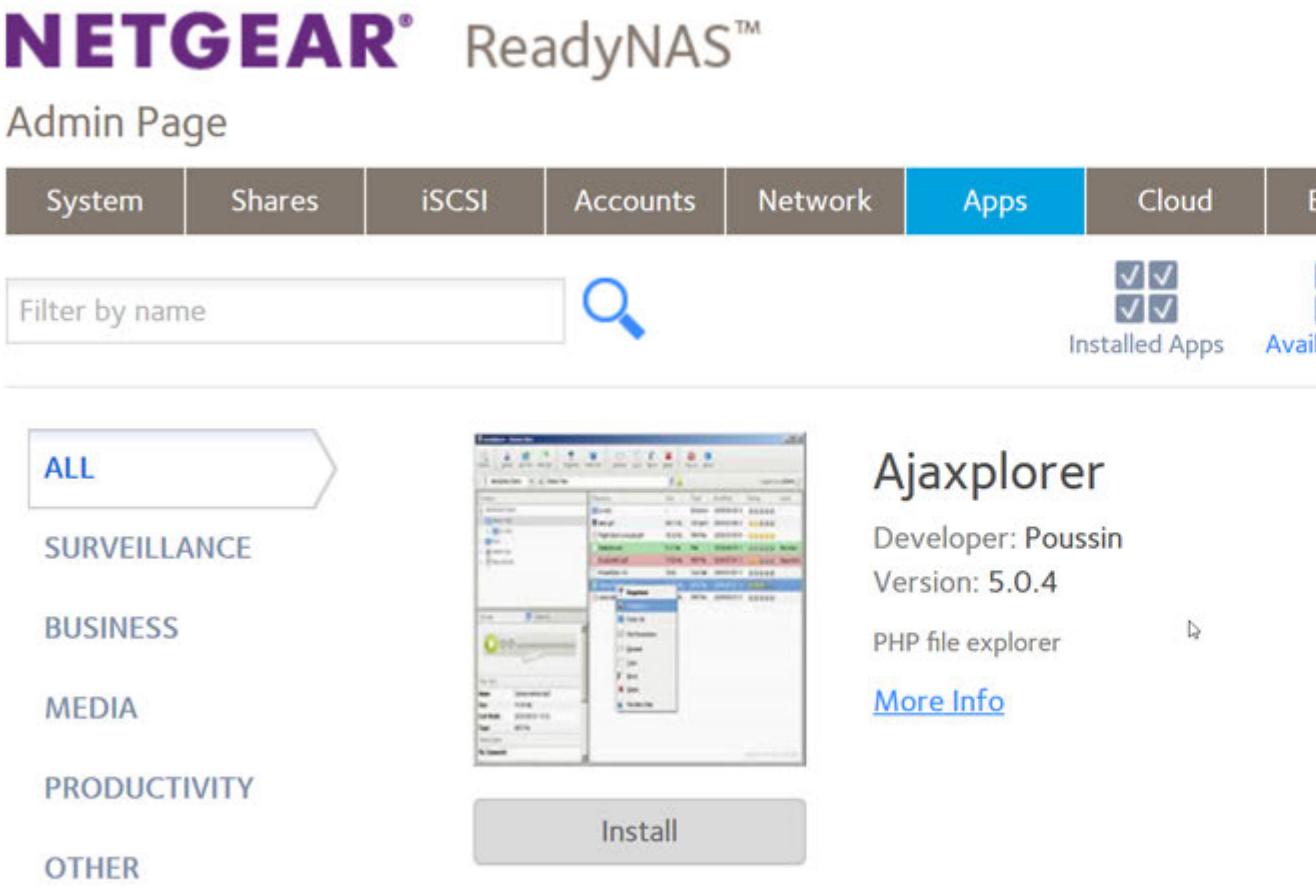
Install Apps

Many apps are available for your ReadyNAS.

To install an app on your ReadyNAS:

1. Log in to your ReadyNAS.
2. Select **Apps > Available Apps**.

> **Note** The apps are listed in alphabetical order. Click the `Reverse` icon to change the order from A through Z to Z through A and back. You can also filter the apps listed by entering all or part of a name in the search field.



3. Click the **Install** button below the app.
   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 210.

Manage Installed Apps

You can manage apps installed on your ReadyNAS from the local admin page.

To manage installed apps:

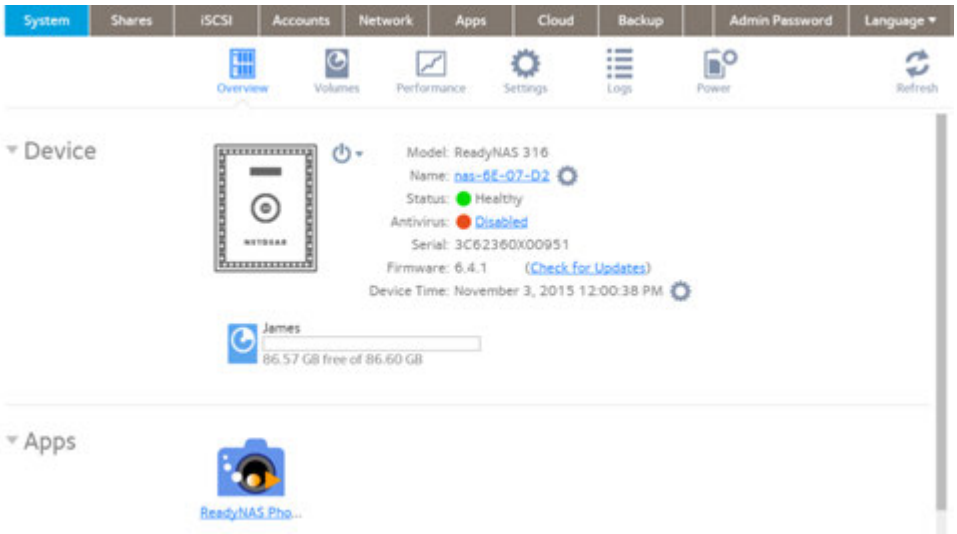
1. Log in to your ReadyNAS.
2. Select **Apps > Installed Apps**.

   A list of apps installed on your ReadyNAS system displays.

Note The apps are listed in alphabetical order. Click the **Reverse** icon to change the order from A through Z to Z through A and back. You can also filter the apps listed by entering all or part of a name in the search field.

From this page, you can launch, enable, disable, or remove installed apps.

Tip Installed apps that can be launched also appear on the Overview page. You can launch an app from this page by clicking it.



System Monitoring

14

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.

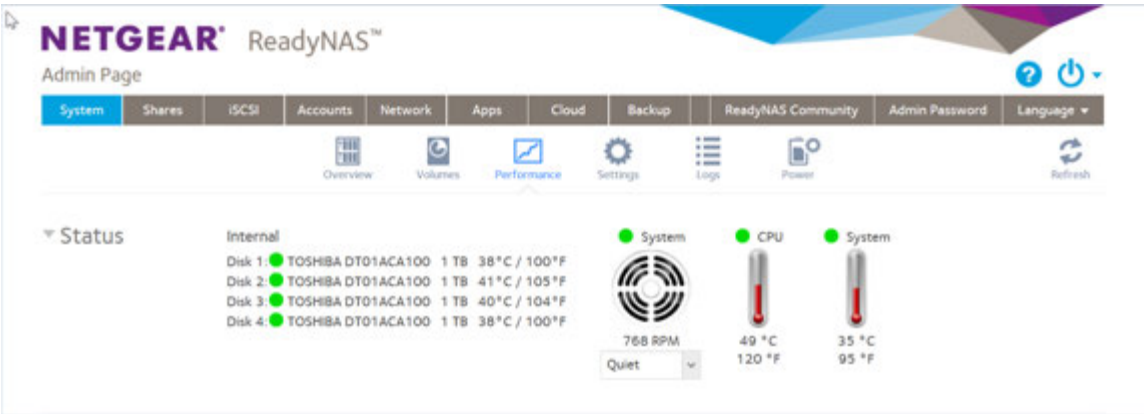
This chapter includes the following topics:

System and Disk Health Information

The ReadyNAS provides basic system health information about the fans, temperatures, optional uninterruptible power supplies, optional expansion disk arrays, and fan speed control.

To view system and disk health information:

1. Log in to your ReadyNAS.
2. Select **System > Performance > Status**.



3. To view disk status and health information, point to a disk status indicator.
4. To change the fan speed setting, select **Quiet**, a quieter, slower speed, **Balanced**, a medium speed, or **Cool**, higher and louder speed, from the drop-down menu below the **fan** icon. The actual speed of the fan depends on system temperature and the number and types of disks installed, and varies depending on activity. When the speed is set to **Quiet**, the average system temperature is higher than when the speed is set to **Balanced** or **Cool**.

System Real-Time and Historical Monitoring

The ReadyNAS provides status graphs for volume throughput, network throughput, volume utilization, and system temperatures.

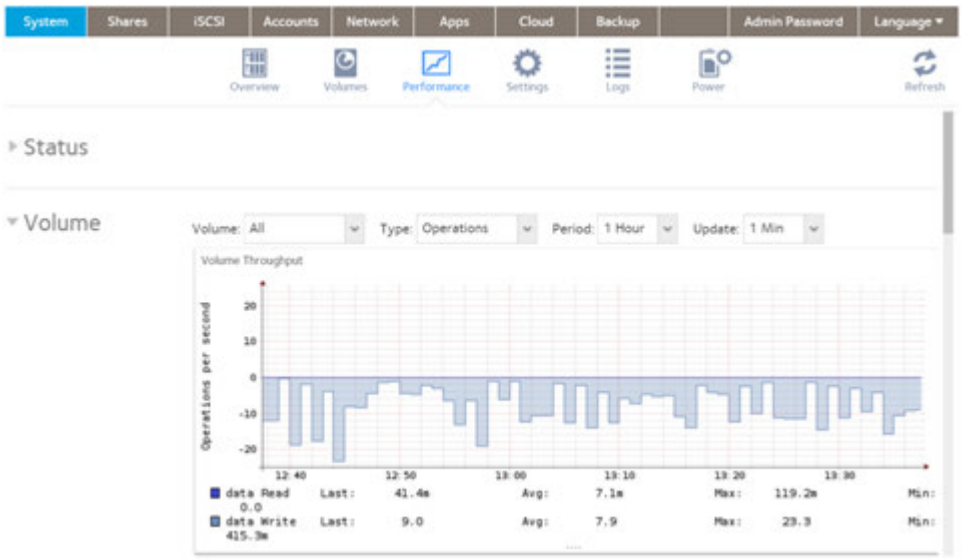
Note Status graphs are not supported for ReadyNAS 102, 104, 202, 204, 212, 214, or 2120 systems.

To display and configure the system status graphs:

1. Log in to your ReadyNAS.
2. Select **System > Performance**.
   The page updates showing the performance panes.
3. Scroll down to Volume, Network, Utilization, or Temperature to view the corresponding status graphics.

Volume

The Volume throughput graph shows the number of read and write operations per second.



The range is flexible and depends on your selections from the menus above the graphic. For example, the range can be from 0 to 200 operations. The upper part of the graph indicates the number of read operations (indicated by positive numbers). The lower part of the graph indicates the number of write operations (indicated by negative numbers).

From the menus above the graph, 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 graph is updated. You can select from 1 to 30 minutes.

Network

The Network throughput graph shows the network usage for Tx and Rx traffic in bytes per second.

The range is flexible and depends on your selections from the menus above the graph. For example, the range can be 0 to 60 bytes or from 0 to 40 KB. The upper part of the graph indicates the incoming (Rx) traffic; the lower part of the graph indicates the outgoing (Tx) traffic.

From the menus above the graph, 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

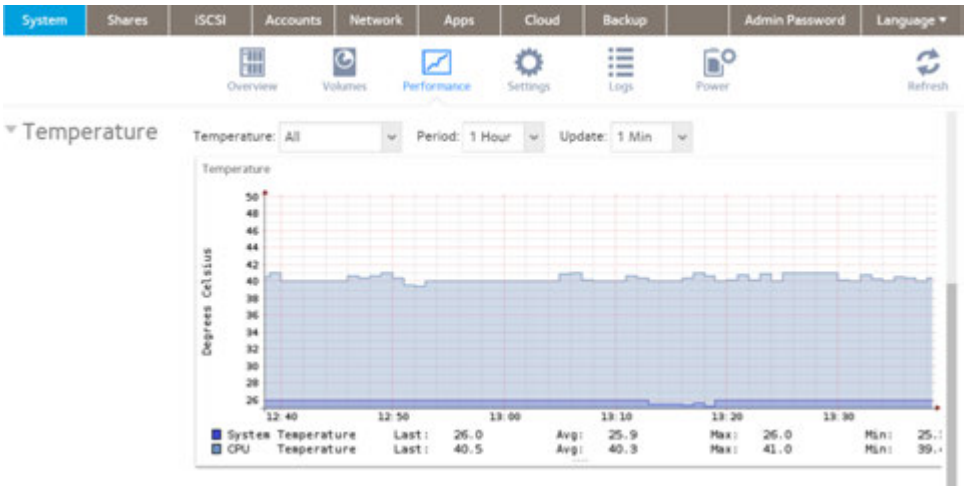
The Volume utilization graph shows the percentage of used storage space for an individual volume or for all volumes. The range is from 0 to 100 percent.

From the menus above the graph, 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 graph shows the system temperatures in degrees Celsius.



The range is flexible and depends on your selections from the menus above the graph and the temperatures that are measured. For example, the range can be from 0 to 50 degrees Celsius.

From the menus above the graph, you can adjust the following settings:

- **Temperature**. Select all temperatures, the system (SYS) temperature, or the CPU 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, 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

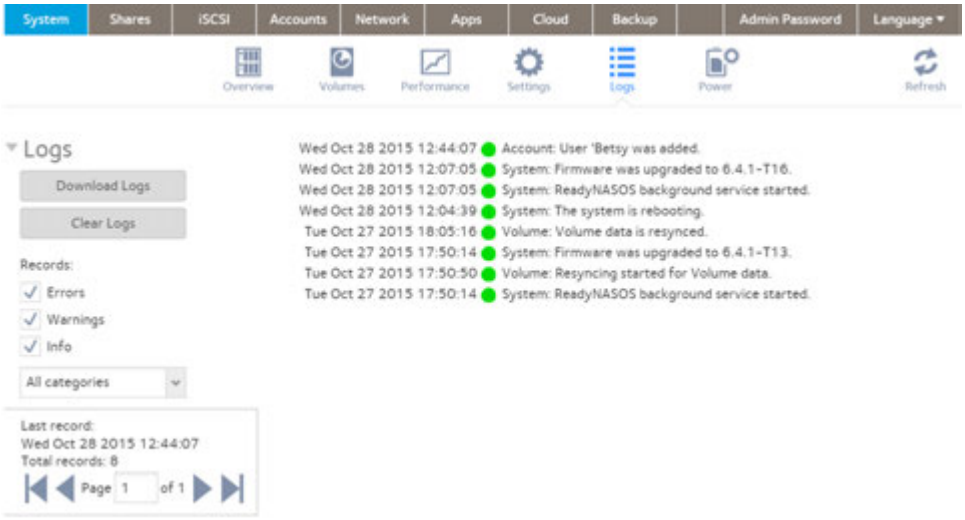
- Removal and addition of power supplies
- Removal and addition of a UPS
- Connection and disconnection of external USB devices

The following events are recorded in the system log and also generate alerts (see *Configure System Alerts* on page 164) and SNMP traps (see *SNMP Monitoring* on page 218). 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. Log in to your ReadyNAS.
2. Select **System > Logs and Alerts**.



3. To view additional messages, use the navigation box in the lower left corner of the page.
4. 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><YYYYMMDD><HHMMSS>.zip`, in which *<host name>* is the host name of the ReadyNAS,

<YYYYMMDD><HHMMSS> is the year, month, date, hour, minute, and second time stamp for the file (see *Configure the Host Name* on page 164).

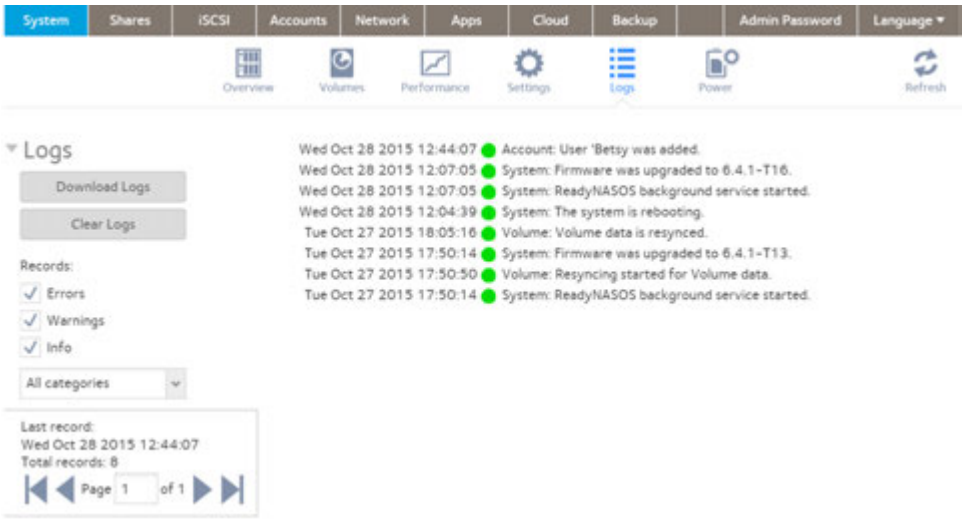
- **Clear the logs**. Click the **Clear Logs** button. The log entries onscreen are cleared but the log files remain intact.
- **Configure the logs**. Under Records, select which message levels and categories are logged. These selections affect the system logs, alerts, SNMP traps, and onscreen messages:
  - **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 system 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 system from which you want to download logs.
2. Select **System > Logs**.



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.

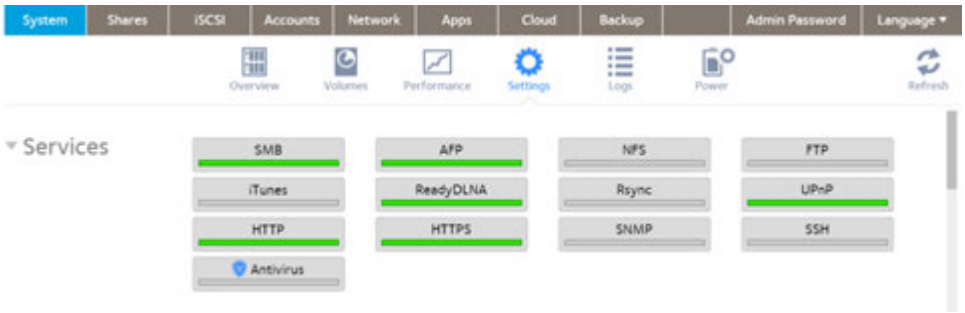
SNMP Monitoring

Use SNMP management systems such as HP OpenView or CA UniCenter for remote monitoring of the ReadyNAS. (Management over SNMP is not supported.)

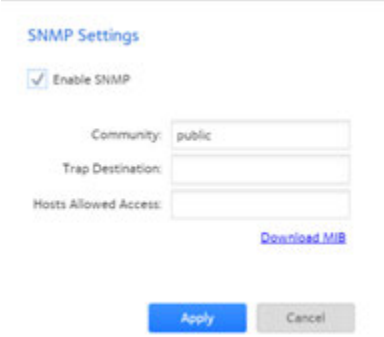
Configure SNMP

To configure SNMP:

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



3. Click the **SNMP** button.



4. 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 use a more segregated monitoring scheme.

(Continued)

Item	Description
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 215.
Hosts Allowed Access	Enter a network address that specifies the hosts that are allowed to access the ReadyNAS.

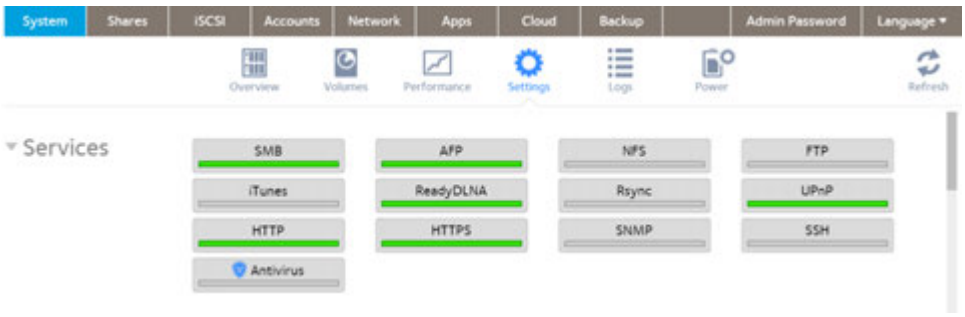
5. Click the **Apply** button.
   Your settings are saved.

Download the NETGEAR SNMP MIB

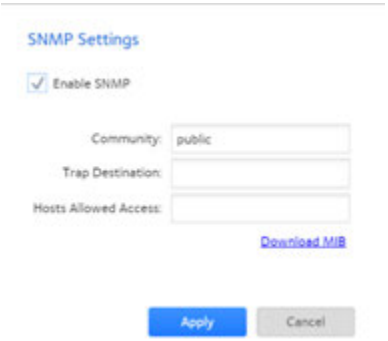
You can download the NETGEAR SNMP MIB from the local admin page and import it to your SNMP client applications. For information about the types of messages that the ReadyNAS can send to SNMP hosts, see *System Logs* on page 215.

To download the NETGEAR SNMP MIB:

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



3. Click the **SNMP** button.



4. Click the **Download MIB** link.
   The page updates showing the MIB.

System Maintenance 15

System maintenance includes upgrading and resetting firmware, recovering the administrator password, and shutting down or restarting the system.

This chapter describes how to maintain your ReadyNAS system. It includes the following sections:

Update Firmware

Firmware is the software that operates your ReadyNAS storage system. It is written directly to your system's onboard flash memory. NETGEAR periodically releases firmware updates to improve your storage system. Because firmware is stored in flash 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.

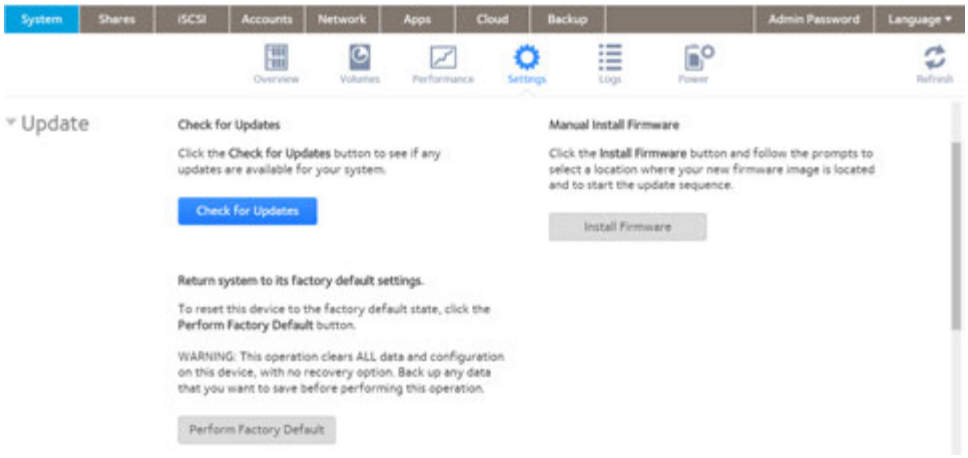
We recommend that you back up your data, especially data that cannot be replaced, before you perform a firmware update.

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



3. Click the **Check for Updates** button.
   The following occurs:

   - If no firmware update is available (or if your connection to the internet is interrupted), you are notified that your system is using the most current firmware.
   - If a firmware update is available, a pop-up window opens and you are prompted to update your system.

4. If a firmware update is available, click the **Update** button in the pop-up window.

The system downloads the new firmware. When the download is complete, you are prompted to reboot your system.

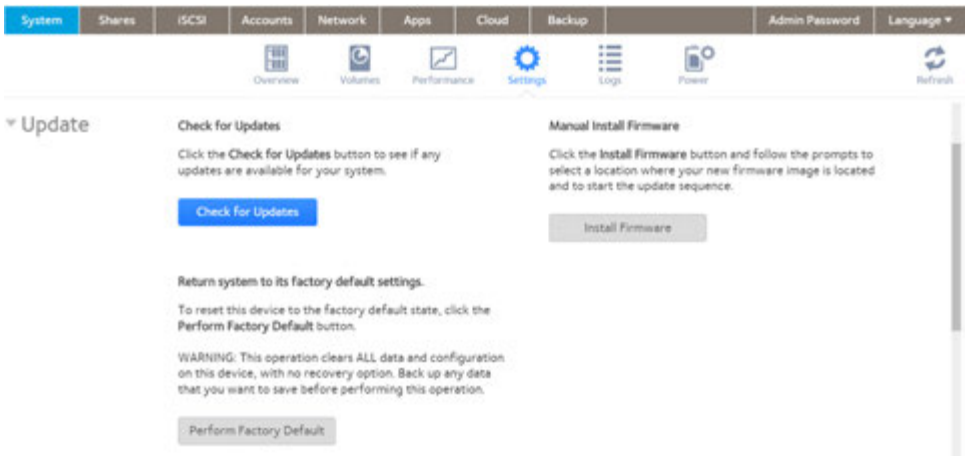
5. Click the **Reboot** button.
   Your system reboots and installs the new firmware. If you enabled email alerts, your ReadyNAS system sends a message when the firmware update finishes.

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 *www.netgear.com/support/product/ReadyNAS_OS_6*.
   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 your ReadyNAS.
4. Select **System > Settings > Update**.



5. Click the **Install Firmware** button.

6. Click the **Browse** button.
7. In the pop-up file browser, navigate to the file containing the updated firmware and select it.
   The Update Firmware pop-up window 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 window displays details about the new firmware.

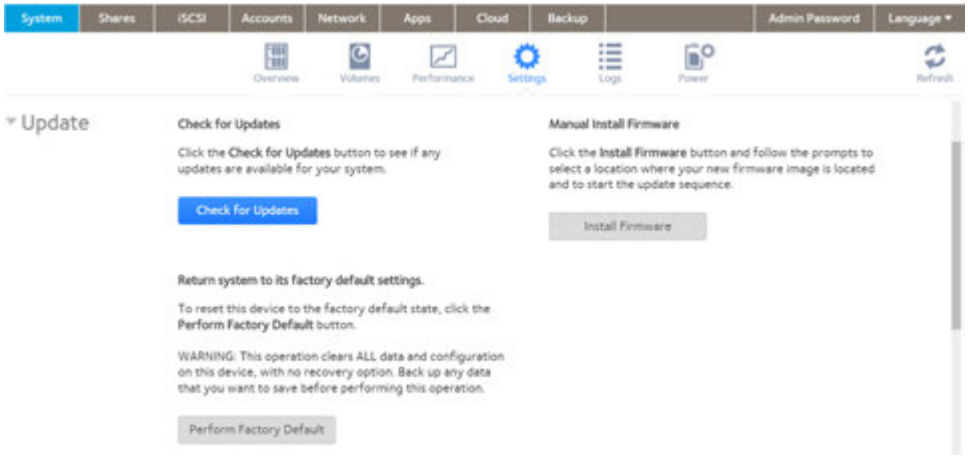
9. Click the **Install** button.
   You are prompted to reboot your ReadyNAS system to complete the firmware installation.
10. Reboot your ReadyNAS system.
    If you enabled email alerts, your ReadyNAS system sends a message when the firmware update finishes.

Reset the Firmware to Factory Defaults

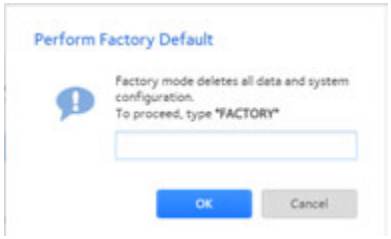
WARNING:
Resetting the ReadyNAS to factory defaults deletes not only the configuration but also all stored data. Back up the stored data if you intend to use it again.

To reset the ReadyNAS to factory defaults:

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



3. Click the **Perform Factory Default** button.



4. Type **FACTORY** (all capital letters) in the field.
5. 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 use NETGEAR s password recovery tool to recover a lost or forgotten administrator password in two ways:

- **Receive a new password through email**. You must enable and configure this method ahead of time. For more information, see *Set the Administrator Password* on page 162.
- **Use the physical reset button**. By default, this method is enabled, but it requires physical access to the ReadyNAS system. For more information, see *Set the Administrator Password* on page 162.

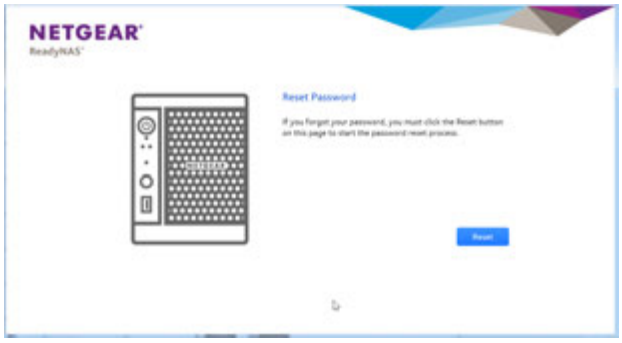
Note You can also perform an OS reinstall. This process reinstalls the firmware on the storage system and resets the administrator user name and password to factory defaults.

Receive a New Password Through Email

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 162. If you lost the password but did not enable administrator password recovery, see *Recover the Administrator Password Using the Physical Reset Button* on page 224.

To recover your administrator password using NETGEAR's password recovery tool through email:

1. Launch a web browser and visit < *ReadyNAS_IP_address*>/password_recovery.
   <*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 162.
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.

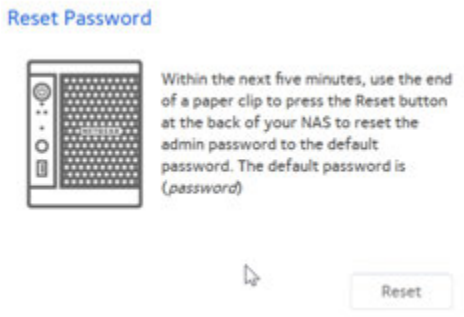
Recover the Administrator Password Using the Physical Reset Button

This process does not remove data from the system, but resets the administrator password to the factory default. The default password to log in to the local admin page is password.

Both user name and password are case-sensitive.

To recover your administrator password using NETGEAR's password recovery tool and the physical Reset button:

1. Launch a web browser and visit https://< *ReadyNAS_IP_address*>/password_recovery.
   The Password Recovery page displays.
   <*ReadyNAS_IP_address*> is the IP address of the storage system.



2. Follow the directions on the page.

For information about how to perform an OS reinstall on the storage system, see the hardware manual for your system, which is available at *www.netgear.com/support/product/ReadyNAS_OS_6.*

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. Log in to your ReadyNAS.

2. Click the **Power** icon near the upper right corner of the local admin page.
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.

Backup and Recovery 16

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.

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, 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:

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.

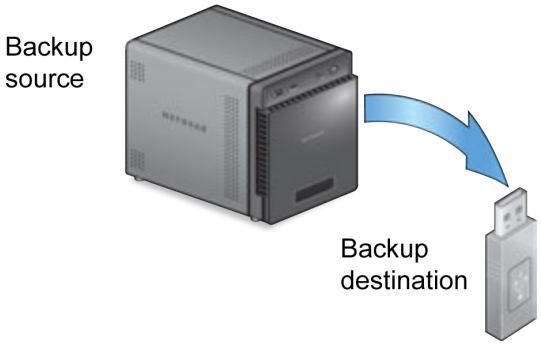


Figure 12. Backing up data from a ReadyNAS system to a secondary device (USB drive)

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.

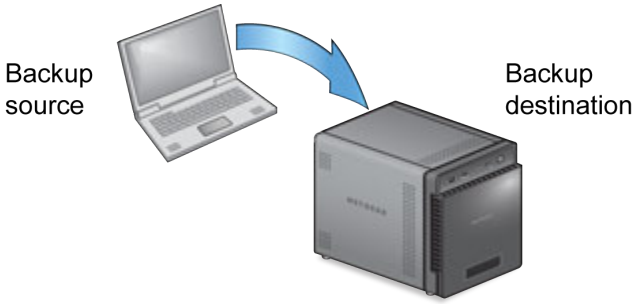


Figure 13. Backing up data from a computer to a ReadyNAS system

A full backup makes a copy of all 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 from data loss only if a disk fails. For more information about the protection that RAID configuration offers, see *RAID* on page 24.

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 230).

Local options for backup sources and destinations are described in the following table.

Table 12. 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 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.

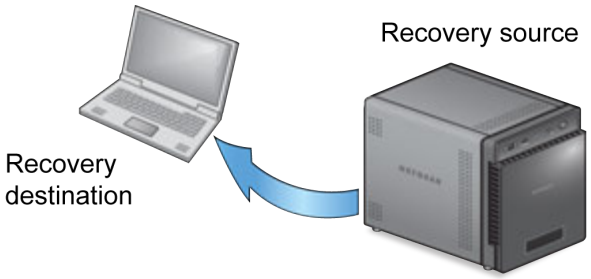


Figure 14. Recovering data from a ReadyNAS system to a laptop computer

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.

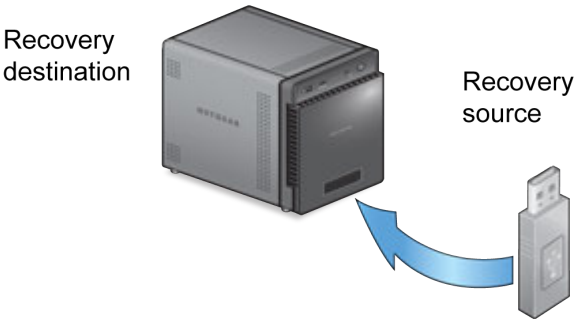


Figure 15. Restoring data from a USB drive to a ReadyNAS system

The ReadyNAS system treats recovery jobs like backup jobs. You use the Backup page 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 155.

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 13. 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 will 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 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.

Table 13. Backup protocols (Continued)

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 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. We recommend using remote SSH when backups are being transferred over the Internet.

Backups Compared to ReadyDR Backups

ReadyNAS OS provides both file backups, just called backups, and snapshot backups, called ReadyDR backups. Both operate similarly and both provide copies of your data, but because of the underlying differences, depending on what you are backing up and why, one might be better than the other for your specific case.

A file backup is a copy of the file that exists at the time of the back up. The backup contains no history of the file. (Although you can maintain file history by maintaining older backups.) A ReadyDR backup consists of all of the snapshots on a share or LUN. You have the same snapshot history in the ReadyDR backup as you do in the original. You can retrieve previous versions of a file in the same way you can retrieve previous versions through the original snapshots.

Back Up Files

You can create, configure and delete backup and recovery jobs. You can also manually start jobs and clear the job log.

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 245.

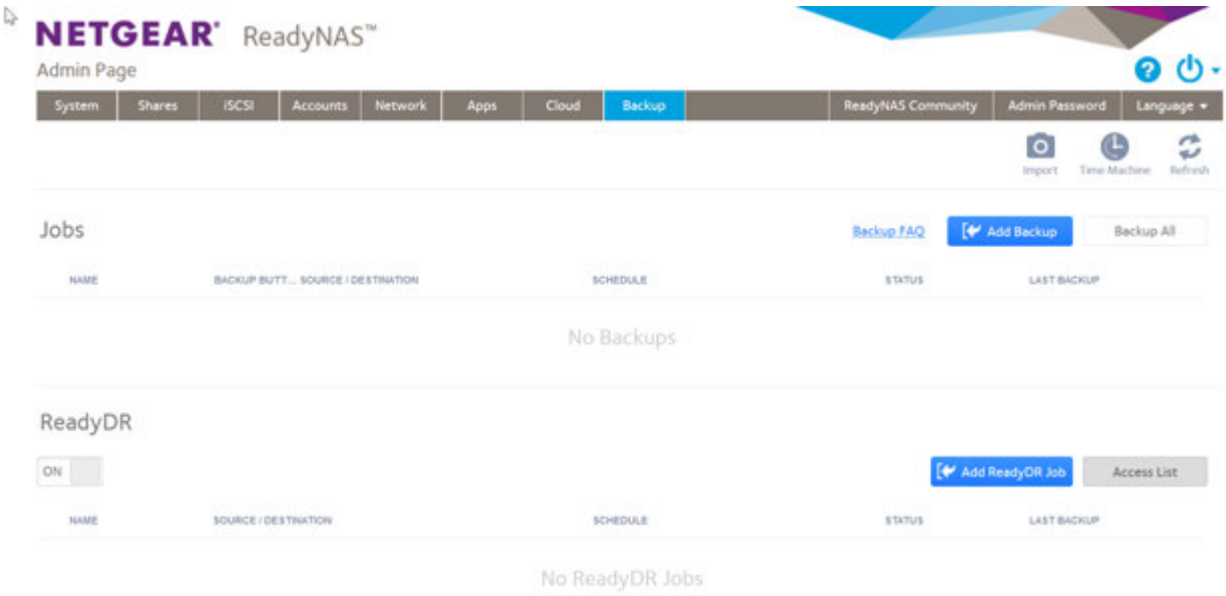
The first few times you back up data, it is a good practice to perform the backup manually. With a manual backup, you can make sure that access is granted to the remote backup source or destination and see how long the backup takes to run. You must know how long the backup job takes so that you can allow 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 249.

Note Backup and recovery jobs using Time Machine use different procedures. For more information, see *Time Machine* on page 260.

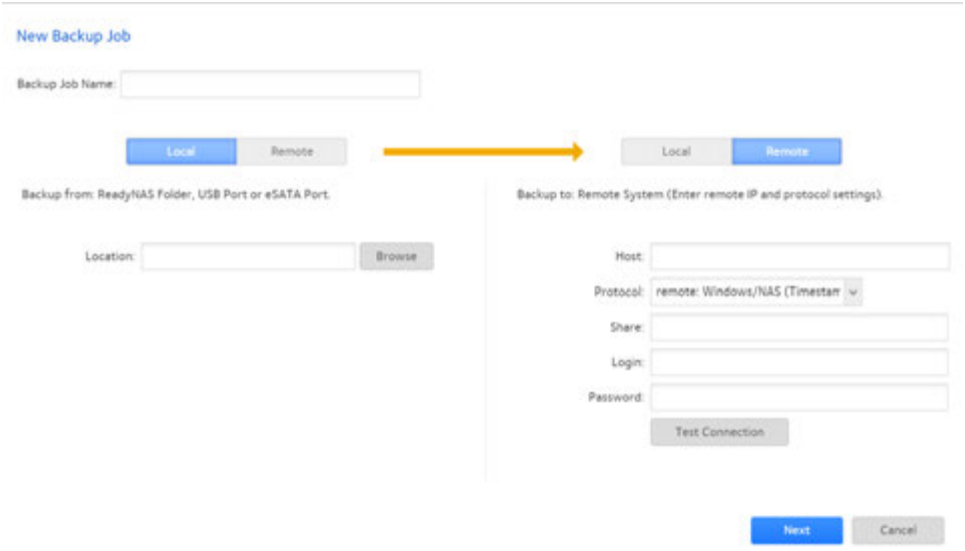
Create a Backup Job

To create a backup job:

1. Log in to your ReadyNAS.
2. Select **Backup**.



3. Click the **Add Backup** button.



4. In the **Backup Job Name** field, enter a name for the new backup job.
   The name can be a maximum of 255 characters.
5. From the pair of buttons on the left side of the window, to back up files that are local (on the ReadyNAS, or connected USB drive, or connected eSATA drive), click the **Local** button, 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 Rsync protocol is for expert users only.

     - If you select the Rsync 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 right side of the window, to store the backup locally (on the ReadyNAS, or connected USB drive, or connected eSATA drive), click the **Local** button, 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 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 Rsync protocol is for expert users only.

     - If you select the Rsync 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 opens.
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.
11. Click the **Finish** button.
    The New Backup Job: Schedule window closes and the new job is added to the Jobs list.

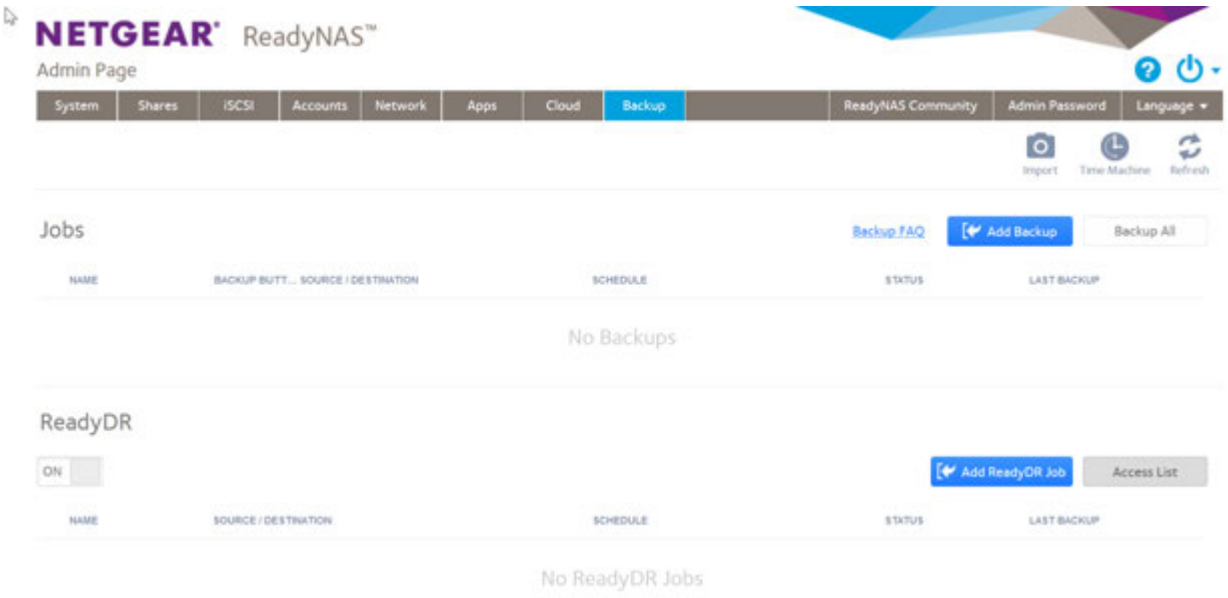
For more information about backup sources, destinations, and protocols, see *Backup and Recovery* on page 227.

Create a Recovery Job

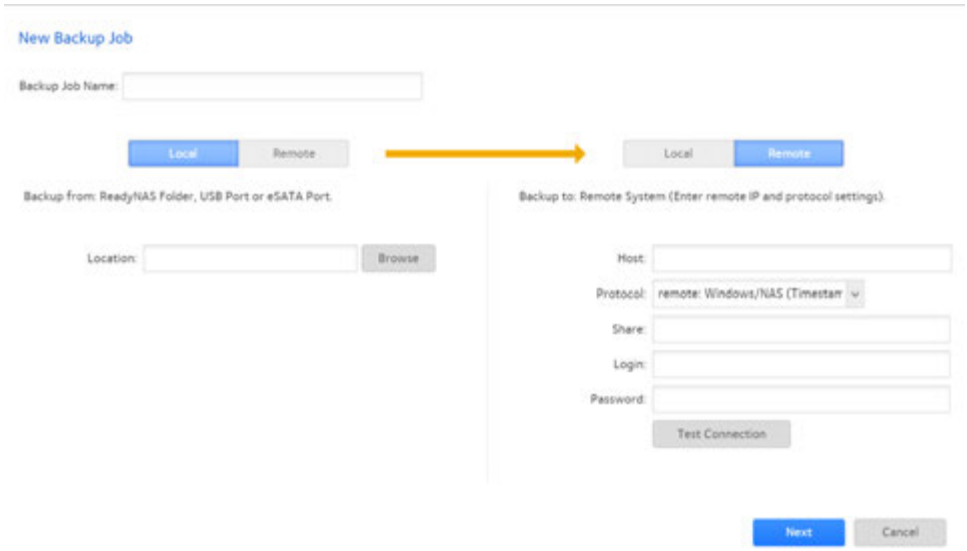
The ReadyNAS system treats recovery jobs like backup jobs. You use the Backup page to create a recovery job. In a recovery job, you reverse the source and destination that you used when you backed up the data. The recovery source is the backup destination and the recovery destination is the backup source.

To create a recovery job:

1. Log in to your ReadyNAS.
2. Select **Backup**.



3. Click the **Add Backup** button.



4. In the **Backup Job Name** field, enter a name for the new backup job.
   The name can be a maximum of 255 characters.
5. From the pair of buttons on the left side of the window, click the **Local** button to recover local files (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 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 Rsync protocol is for expert users only.

- If you select the Rsync 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 right side of the window, click the **Local** button to store the backup 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 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 Rsync protocol is for expert users only.

- If you select the Rsync 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 249.

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 *Recovery Concepts* on page 229.

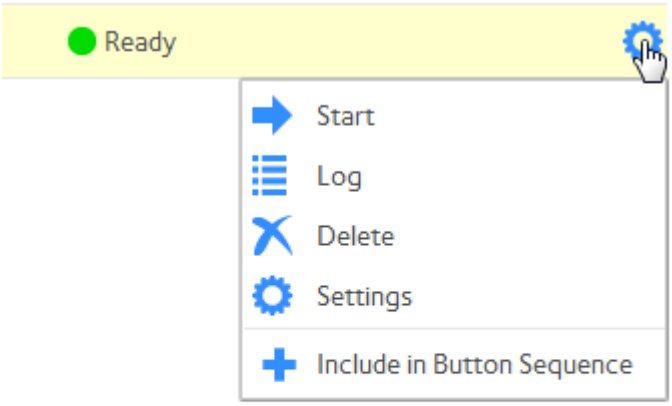
Modify a Backup or Recovery Job

After you create a backup or recovery job, you can change the job name, schedule, and other options.

Change the Name of a Job

To change the name of a backup or recovery job:

1. Log in to the ReadyNAS.
2. Select **Backup**.
   The page updates showing the backup jobs.
3. Mouse over the backup or recovery job from the Jobs list and click the displayed **gear** icon.



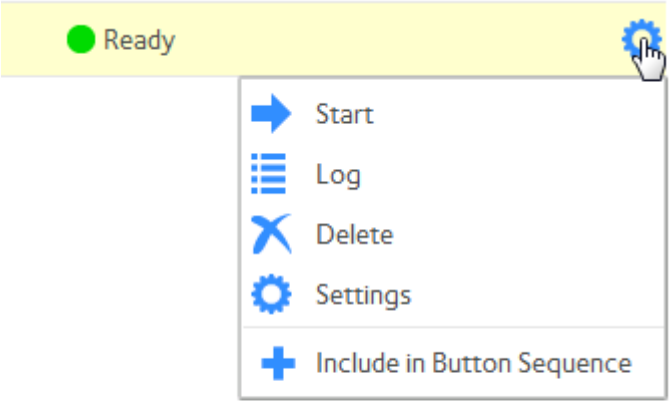
4. In the pop-up menu, click the **Settings** button.
   A pop-up window opens with the **General** tab selected.
5. In the **Name** field, enter a job name.
6. Click the **Apply** button.
   Your settings are saved.
7. Click the **OK** button.
   The pop-up window closes.

Configure a Local Job Source or Destination

To configure a local job source or destination:

1. Log in to the ReadyNAS.
2. Select **Backup**.
   The page updates showing the backup jobs.

3. Mouse over the backup or recovery job from the Jobs list and select the **gear** icon.



4. In the pop-up menu, click the **Settings** button.

5. Click the **Source** or **Destination** tab.
6. From the **Type** menu, 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 is the Time Machine data stored locally on the ReadyNAS.

7. In the **Name** menu, select the share, home share, volume, or external storage connection that you want to use.

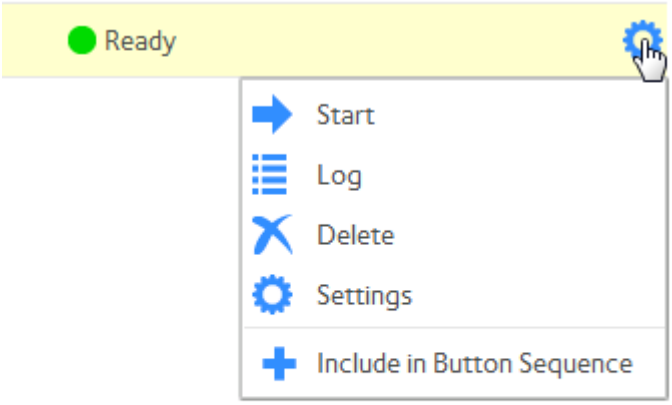
If you selected **timemachine**, the **Name** menu is automatically populated.

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 settings are saved.
11. Click the **OK** button.
    The pop-up window closes.

Configure a Remote Job Source or Destination

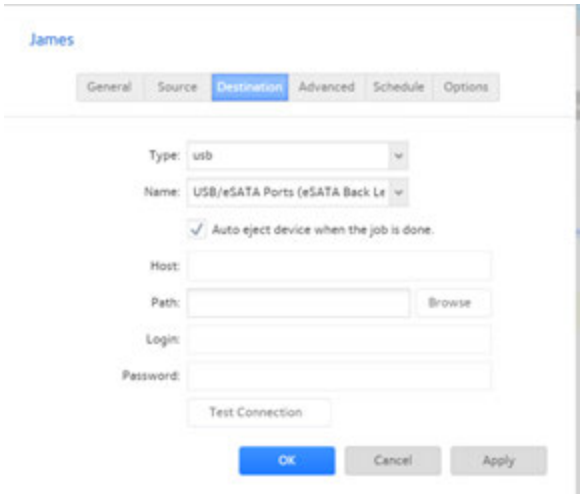
To configure a remote source or destination for a job:

1. Log in to the ReadyNAS.
2. Select **Backup**.
   The page updates showing the backup jobs.
3. Mouse over the backup or recovery job from the Jobs list and click the **gear** icon.



4. In the pop-up menu, click the **Settings** button.
   The settings window for that job opens.

5. Click the **Source** or **Destination** tab.



6. In the **Type** menu, select **remote**.
7. Select the protocol.

Item	Description
Windows/NAS (Timestamp)	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 is a share on a Windows computer. (Note that this protocol is not available for the remote destination.) 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.
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. We recommend 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 Rsync protocol is for expert users only.

- If you select the Rsync 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 settings are saved.
13. Click the **OK** button.
    The pop-up window closes.

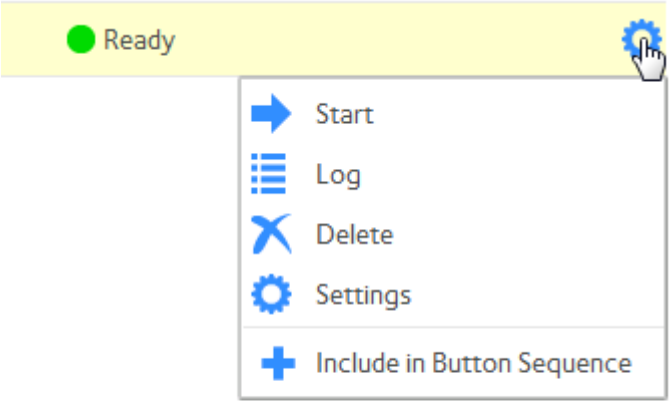
Configure Advanced Rsync Job Settings

You can configure advanced settings for jobs that use Rsync or Rsync over SSH.

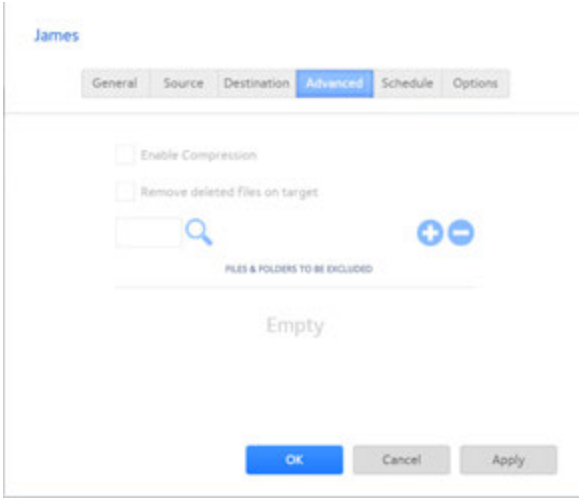
To configure Rsync job settings:

1. Log in to the ReadyNAS.
2. Select **Backup**.
   The page updates showing the list of backup and recovery jobs.

3. Mouse over the backup or recovery job and click the **gear** icon.



4. Click the **Settings** button.
   The job settings window opens.
5. Click the **Advanced** tab.



6. Configure the settings as described in the following table.

Item	Description
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 (Rsync backups only)	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 settings are saved.
9. Click the **OK** button.
   The pop-up window closes.

Schedule a Backup Job

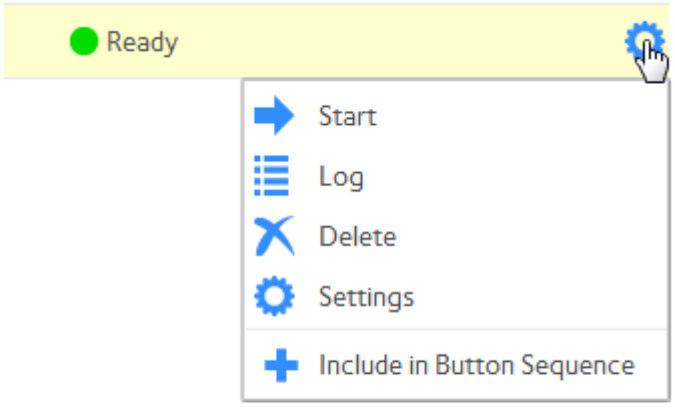
You can schedule a backup job to automatically run as frequently as once every hour, daily, or just once a week. The backup schedule is offset by five minutes from the hour to allow you to schedule snapshots on the hour (snapshots are almost instantaneous) and perform backups of those snapshots.

WARNING:
To ensure the integrity of the data stored on your primary device, never schedule a recovery job to run automatically.

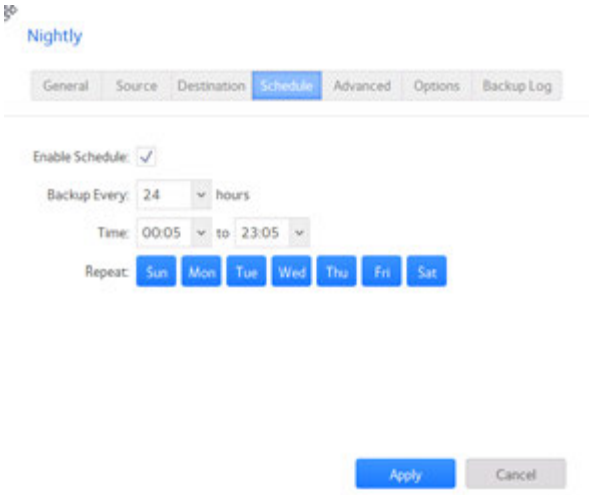
To schedule a backup job:

1. Log in to the ReadyNAS.
2. Select **Backup**.
   The page updates showing the list of backup and recovery jobs.

3. Mouse over the backup or recovery job and click the **gear** icon.



4. Click the **Settings** button.
   The job settings window opens.
5. Click the **Schedule** tab.



6. Select the **Enable Schedule** check box.
7. Specify a schedule for the job.
8. Click the **Apply** button.
   Your settings are saved and the pop-up window closes.

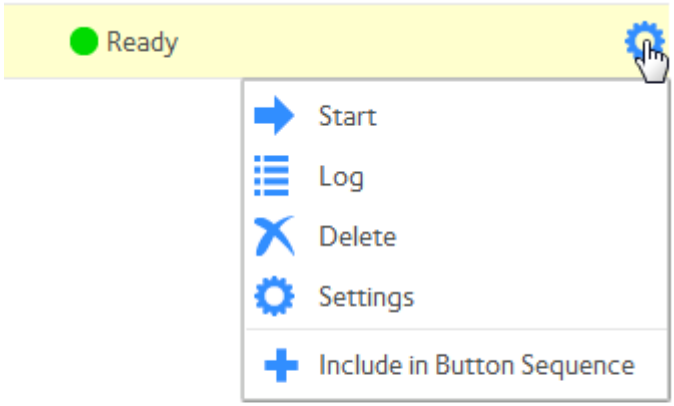
Configure the Job Options

To configure the options for a backup or recovery job:

1. Log in to the ReadyNAS.
2. Select **Backup**.

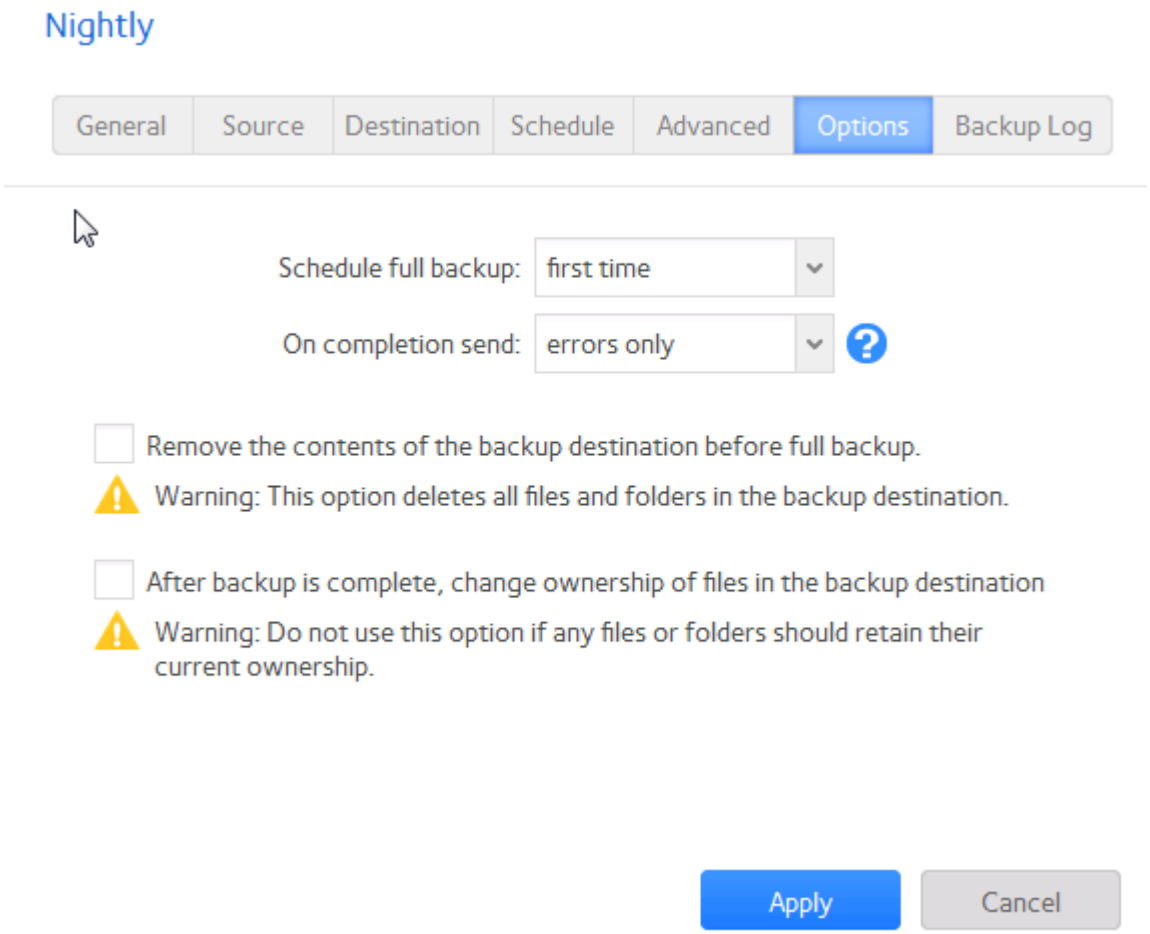
The jobs settings window opens.

3. Mouse over the backup or recovery job from the jobs list and click the **gear** icon.



4. In the pop-up menu, click the **Settings** button.
The job settings window opens.

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 215.

(Continued)

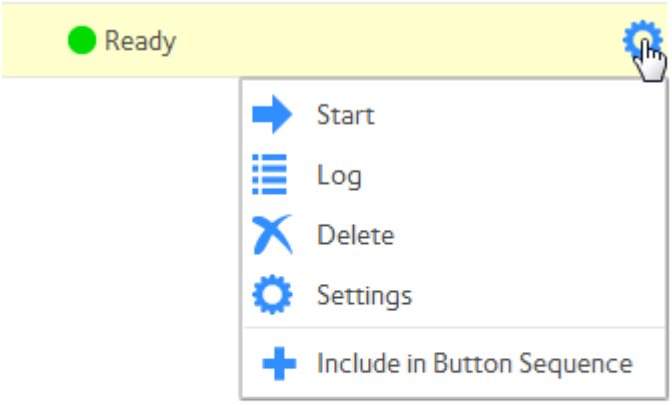
Item	Description
Remove the contents of the backup destination...	Selecting this check box erases the destination path contents before the backup is performed. We recommend that you do not select this check box for recovery jobs. **Note** When using this option, ensure that you correctly identify your backup source and backup destination. If you reverse them, you might permanently delete your files. We recommend that you do not enable this option unless your destination device is very low on storage space. We recommend that 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 settings are saved and the pop-up window 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**.
   The page updates showing the backup and recovery jobs.
3. Mouse over the backup or recovery job from the Jobs list and click the **gear** icon.



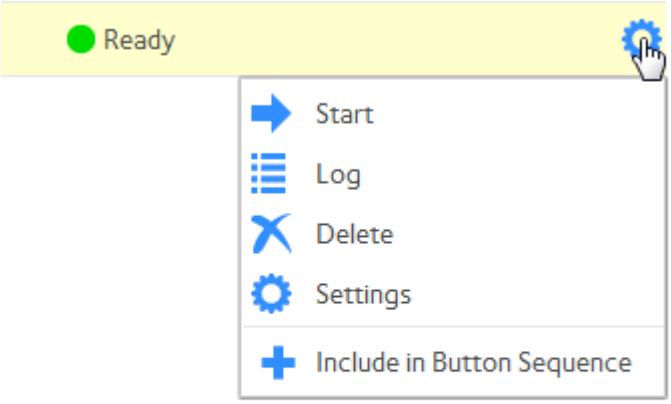
4. In the pop-up menu, click the **Start** button.

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**.
   The page updates showing the backup and recovery jobs.
3. Mouse over the backup or recovery job from the Jobs list and click the **gear** icon.



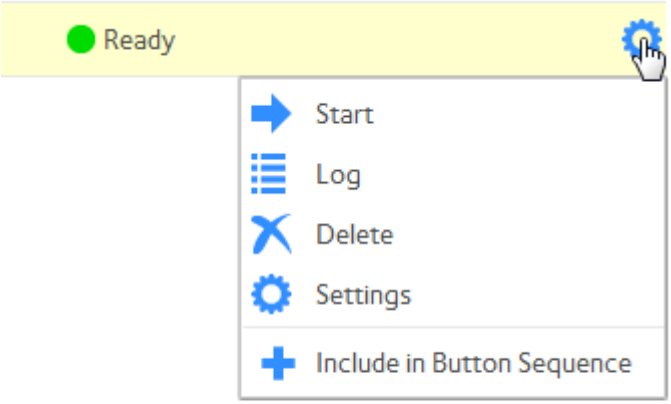
4. In the pop-up menu, click the **Delete** button.
5. Confirm the deletion.

View or Clear a Job Log

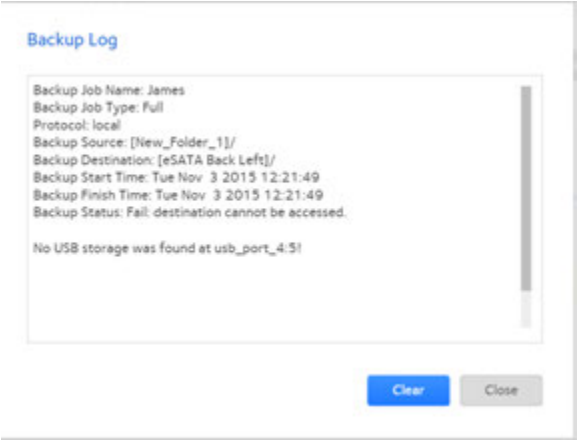
To view a backup or recovery job log:

1. Log in to your ReadyNAS.
2. Select **Backup**.
   The page updates showing the backup and recovery jobs.

3. Mouse over the backup or recovery job from the Jobs list and click the **gear** icon.



4. In the pop-up menu, click the **Log** button.



5. To clear the job log, click the **Clear** button.

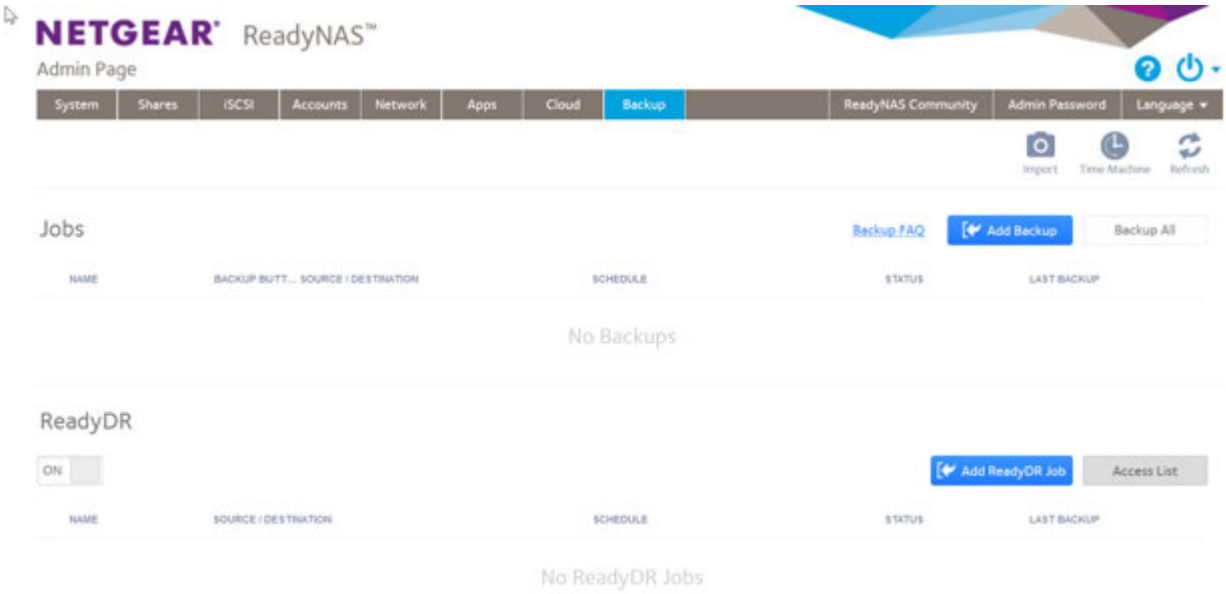
Configure the Backup Button

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.

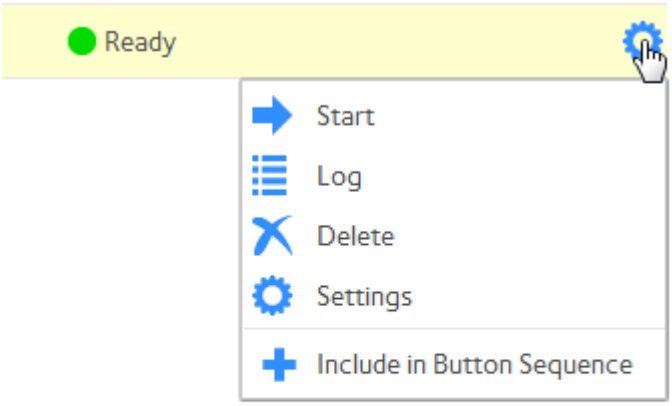
If no jobs are scheduled for the button, clicking the button does nothing.

To add a job to the Backup button sequence:

1. Log in to your ReadyNAS.
2. Select **Backup**.



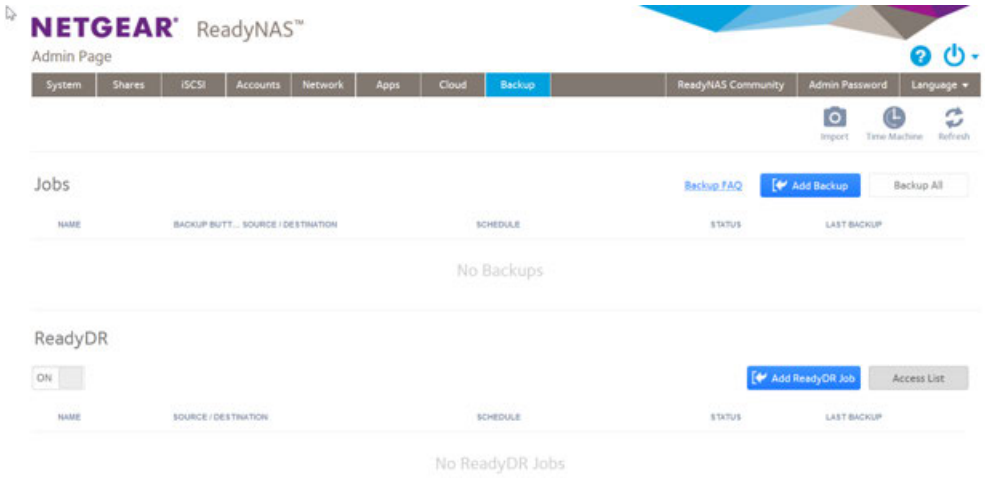
3. Mouse over the job and click the **gear** icon.



4. Click the **Include in Button Sequence** button.
   The pop-menu closes and the word **Yes** appears in the Backup Button column of the job listing.

To remove a job from the Backup button sequence:

1. Log in to your ReadyNAS.
2. Select **Backup**.



3. Mouse over the the job and click the **gear** icon.
   The **Options** window opens.
4. Click the **Exclude from Button Sequence** button.
   The window closes and the job listing updates without the word **Yes** in the Backup Button column and the job is removed from the Backup button sequence list.

Backup Snapshots With ReadyDR

ReadyDR is an alternative way to back up data on your ReadyNAS device. A ReadyNAS backup makes a copy of files, but a ReadyDR backup makes a copy of the snapshots on a share or LUN.

Because a ReadyDR backup consists of snapshots, you can retrieve not just the most recent version of a file, but the same previous versions that you could access on the ReadyNAS itself.

However, because the ReadyDR backup is share to ReadyDR share or LUN to ReadyDR share, both the source and destination must be on a ReadyNAS device, and if the source and destination are on different ReadyNAS devices, the communication method is specific to ReadyDR. The ReadyNAS device on which you create the ReadyDR job manages the communication for the job. This requires the other ReadyNAS device to validate the first device using the first device's public key. You must copy the public key from the first device and install it on the second device before creating the ReadyDR job. For information about transferring the key, see *Load System Access Key Before Using ReadyDR* on page 254.

A complete share or LUN including snapshots can be large, so the initial data transfer could take a substantial amount of time. To shorten this initial transfer period, you can seed the job with a complete copy of the share or LUN by exporting it to removable media and then importing it onto the destination ReadyNAS. For more information about seeding a ReadyDR job, see *Seed a ReadyDR Job* on page 255.

You can create, configure, and delete ReadyDR backup and recovery jobs. You can also manually start jobs and clear the job log.

You can use ReadyDR to backup data:

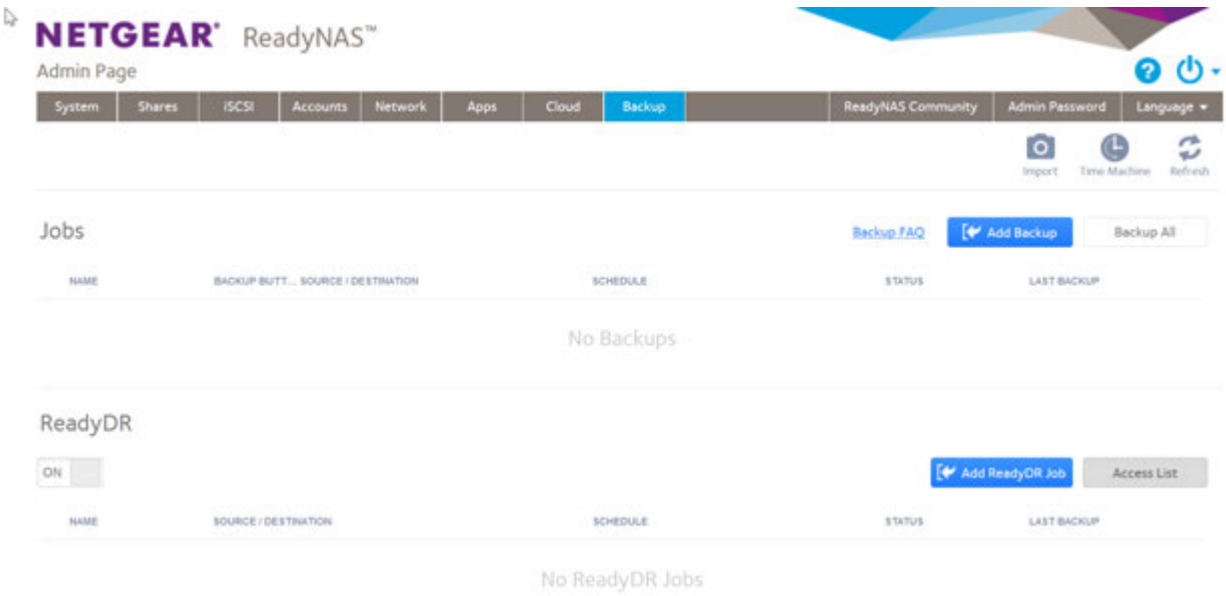
- From a the local ReadyNAS device to itself
- From the local ReadyNAS device to a remote ReadyNAS device
- From a remote ReadyNAS device to a local ReadyNAS device
- From one remote ReadyNAS device to a another ReadyNAS device

Load System Access Key Before Using ReadyDR

ReadyDR jobs are managed by the system on which the job was created. Before you can create a ReadyDR job transferring data between two systems, you must download and exchange the public key for the managing device so that the other device can validate the connection.

You do not need to exchange the key if the source and destination are the same device.

1. Log in to the ReadyNAS device on which you will create the ReadyDR job.
2. Select **Backup**.



3. If ReadyDR is not already on, move the **On-Off** slider to **ON**.
4. Click the **Access List** button.
   The Access List window opens.
5. Click the **Download key file** button.
   Your browser s open or save file window opens.
6. Save the file.
   The file name is `public_readydr_key-`*system_name*.
7. Log in to your other ReadyNAS device.
8. Select **Backup**.
9. If ReadyDR is not already on, move the **on-off** slider to **ON**.
10. Click the **Access List** button.

The Access List window opens.

11. Click the **Import Public Key** button.
    The Import Public Key window opens.
12. Browse to the previously saved public key file, and click the **Upload** button.
    The Import Public Key window closes and the Access List window shows the filename and fingerprint for the first ReadyNAS device.
13. Click the **Close** button.

Seed a ReadyDR Job

When a ReadyDR job first runs, all of the data on the share or LUN must be transferred to the destination. For large shares or LUNs, transfering this much data over the network can take a long time. You can eliminate this large initial network transfer by seeding the job by transferring the data using removable media.

If you seed a ReadyDR job, it must be seeded before the job runs the first time. When you create the job, you can select the **Export seed for this job** checkbox to stop the job before it runs. You can then create the seed archive. After importing the seed archive on the destination device, you restart the job.

You create a seed by exporting the share or LUN after you create the job. For more information about creating a seed file, see *Monitor and Change ReadyDR Jobs* on page 258.

Create a ReadyDR Job

A ReadyDR backup job backs up the snapshots on a share or LUN. The destination must be a ReadyDR share, which is created when you create the job.

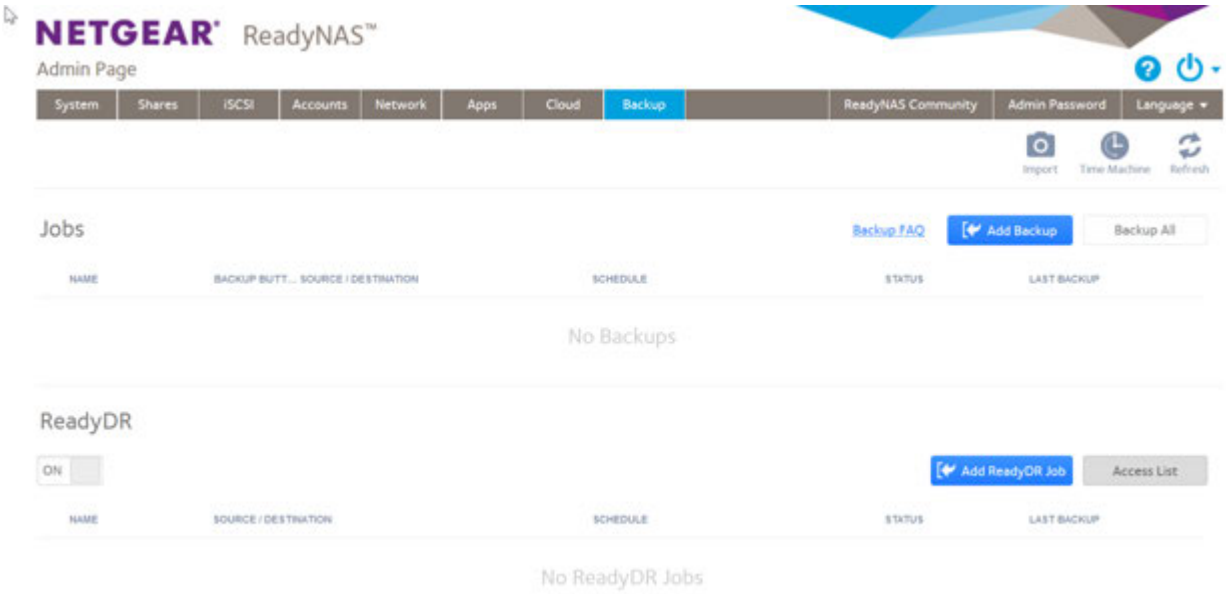
Before you create a ReadyDR job between a local and remote system, you must download the public key for the system on which you are creating the job, and import that key to the other device. For information about exchanging the key, see *Load System Access Key Before Using ReadyDR* on page 254.

The initial data transfer in a ReadyDR job transfers all of the data in the share or LUN. If this transfer occurs over a network, it might take a long time if the network is slow. During job creation you can create a seed archive file, copy it to removable media, and import it to the destination, and avoid the initial network transfer. For information about seeding, see *Seed a ReadyDR Job* on page 255.

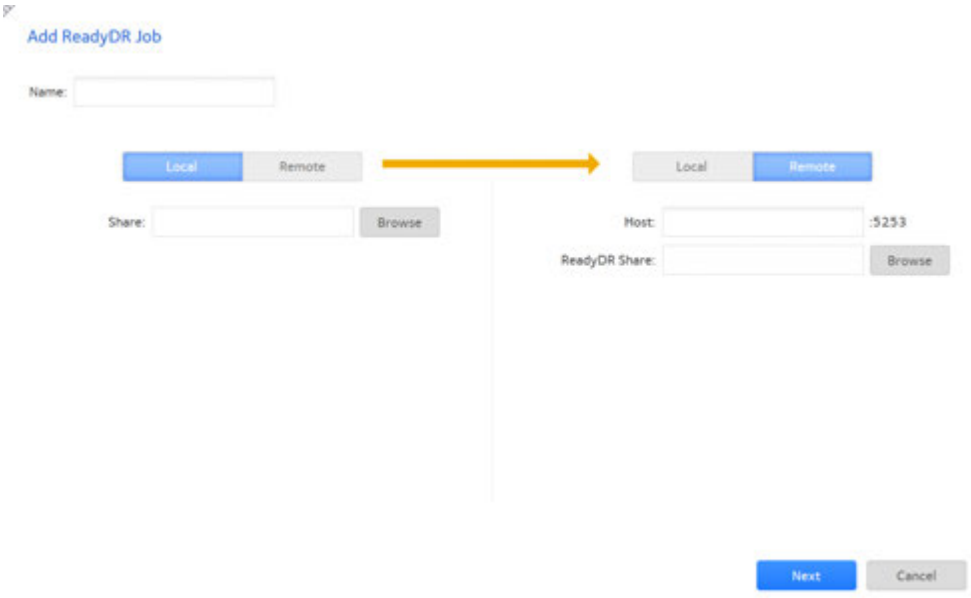
Note A destination LUN is always a thin LUN, even if the source LUN is a thick LUN. For information about thick and thin LUNs, see *Thin and Thick Provisioning* on page 85.

To create a ReadyDR backup job:

1. Log in to your ReadyNAS.
2. Select **Backup**.



3. Click the **Add ReadyDR Job** button.



4. In the **Name** field, enter a name for the new backup job.
   The name can be a maximum of 255 characters.
5. If the source for the job is local to the ReadyNAS device, on the left side of the window click the **Local** button. Otherwise, click the **Remote** button.
   The window adjusts to show the appropriate set of parameters.

Note If either the source or destination is on a remote device, you must install the local ReadyNAS's public key on the remote ReadyNAS. For information, see *Load System Access Key Before Using ReadyDR* on page 254.

6. Do one of the following:

   - If you clicked the **Local** button, click the **Browse** button and navigate to and select the share or LUN that you want to back up.
   - If you clicked the **Remote** button, do the following:

     a. Enter the host name.

     b. Click the **Browse** button and navigate to and select the share or LUN.

7. To store the backup locally, on the right side of the window click the **Local** button, or click the **Remote** button.
   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 and select the destination ReadyDR share.
   - If you clicked the **Remote** button, do the following:

     a. Enter the host name.

     b. Click the **Browse** button and navigate to and select the destination ReadyDR share.

9. Click the **Next** button.
   The Add ReadyDR Job window updates to show the options and schedule fields.
10. Adjust any of the schedule parameters as desired.
    You can schedule a job to automatically run as frequently as once every hour, daily, or just once a week.
11. Adjust the maximum bandwidth used for the transfer, if desired.
    If the network connection between the source and destination systems is fast, the transfer could slow either or both of the devices. This is very likely if the source and destination are both local. Zero, the default, sets no limit to the bandwidth.
12. To seed the job, click the **Export seed for this job** box.

Note Clicking the **Export seed for this job** box disables the job. After you transfer the seed archive file, start the job by selecting **Backup > ReadyDR**, selecting the job, clicking the **gear** icon, and selecting the **Enable** menu item. For information about transfering job seed archive files, see *Seed a ReadyDR Job* on page 255.

13. Click the **Finish** button.
    The window closes and the new job is added to the Jobs list.

Monitor and Change ReadyDR Jobs

You can manually start a job, view the job history, export a seed file, delete the job, enable a stopped job, and change the job settings.

To check the history or change job parameters:

1. Log in to your ReadyNAS.
2. Select **Backup**.
3. Select the ReadyDR job you want to monitor or change from the ReadyDR section.
4. Click the **gear** icon.
   The options menu opens.
5. Click the desired action.

Start	Immediately runs the job.
History	Displays the job history.
Export	Creates a file archive of the share or LUN and opens a file browse window where you select the destination. The file name follows the format `ReadyDR_Seed-`*.jobnamehostname* Use this file to seed a new ReadyDR job.
Delete	Deletes the job.
Enable	Enables a stopped job.
Disable	Disables the job.
Settings	Opens the settings window for the job. From this window you can change the schedule, and the **Bandwidth Limit**, **Compression**, and **Encrypted Transport** options.

Recovery Using ReadyDR Snapshots

When you need to recover shares and LUNs from a ReadyDR backup, you can recover them by cloning a backed up snapshot.

One application of ReadyDR is to maintain a disaster recovery site. Depending on specifics of your disaster recovery plan, you might want to restore the data to the original site, while in other cases you might want to use the disaster recovery site's ReadyNAS device as a replacement for the original ReadyNAS device. The process is different depending on the case.

Recovery to the Remote Site

If the ReadyDR share is on the server on which you want the recovered share or LUN, all you need to do is clone the snapshot. For information about cloning the snapshot, see *Clone Snapshots* on page 118.

Recovery to the Original Site

If you want the recovered share or LUN on the original ReadyNAS device, create a one time ReadyDR job to backup the ReadyDR share with the snapshots back to the original ReadyNAS device, and then clone the snapshots. For information on creating the ReadyDR job, see *Create a ReadyDR Job* on page 255. For information about cloning the snapshot, see *Clone Snapshots* on page 118.

Back Up a Camera or Other Media Device

Many cameras and other media devices support the Media Transfer Protocol (MTP) and the Picture Transfer Protocol (PTP). You can configure your ReadyNAS to backup such devices when you connect them to the ReadyNAS.

Your camera or other MTP supporting device must have MTP or PTP enabled before connecting it your ReadyNAS. Check your device documentation.

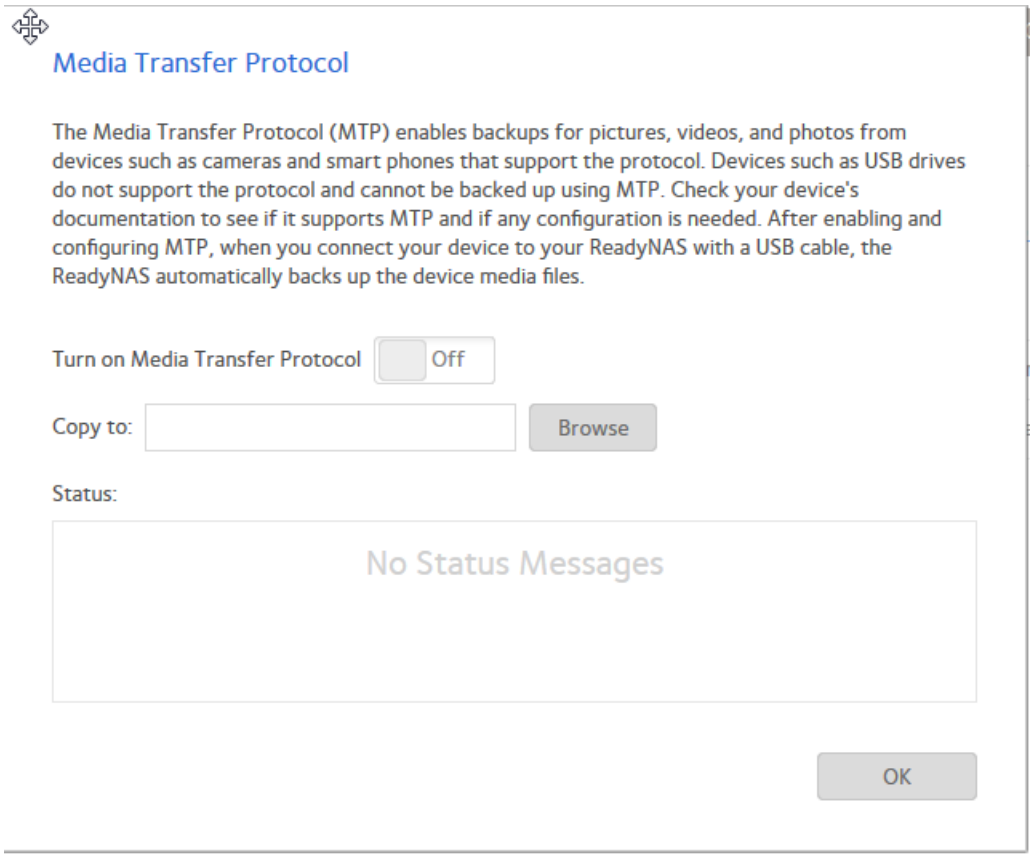
After enabling MTP backups, when you connect your device to the ReadyNAS with a USB cable, the ReadyNAS automatically backups up the device.

Note Recent versions of iOS and Android OS require you to authorize the ReadyNAS to access the device when you first connect them.

To enable automatic MTP or PTP backups:

1. Log in to the ReadyNAS.
2. Select **Backup**.

3. Click the **Import** icon.



4. Set the **On-Off** slider so the slider shows the On position.
5. Click the **Browse** button and browse to the folder in which you want to store the backups.
6. Click the **OK** button.
   Your settings are saved and the window closes.

Back Up Using 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 use 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 are allowed 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 page (**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.

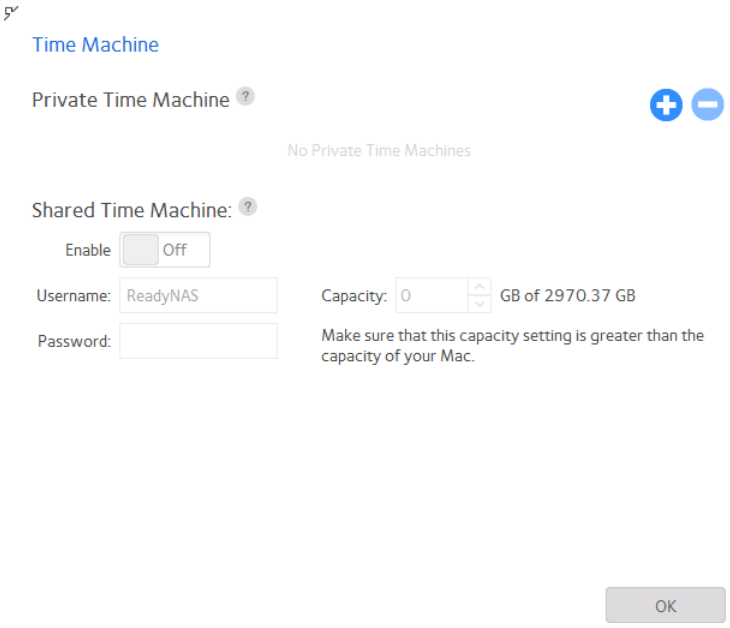
Back Up Your Mac Using a Shared Time Machine

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 private Time Machines used by individual users. 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. Select **Backup > Time Machine**.



3. If the Shared Time Machine **Enable** slide switch is not already set to On, set it to On.
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 264.) 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.
   The Time Machine window opens.
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**.
   The other disks are possible private Time Machine disks.
10. Click the **Use Disk** button.
11. When prompted, in the **Name** and **Password** fields, enter **ReadyNAS** or the shared Time Machine user name and password that you created in step *4* on page 261.
12. 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

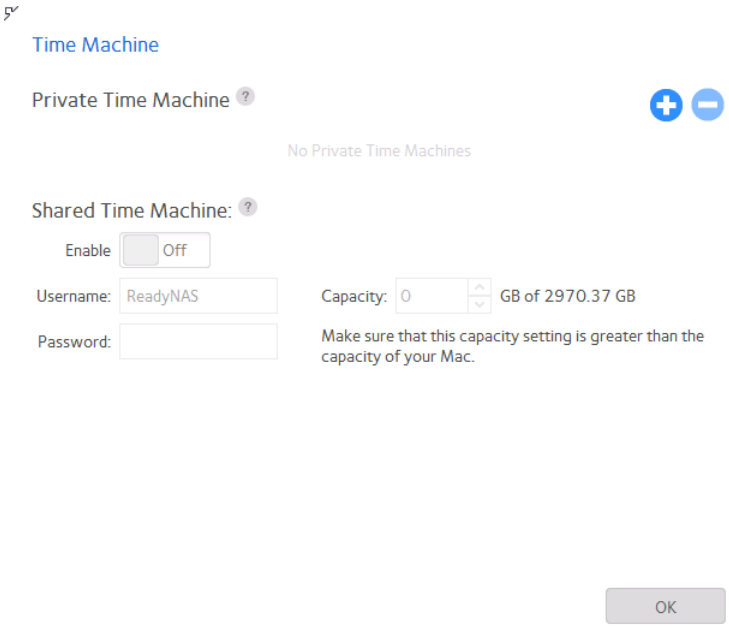
You can use your ReadyNAS as the disk for Time Machine backups. ReadyNAS OS supports two different types of Time Machine targets, a single Time Machine shared by several users, and private Time Machines used by individual users. Use this procedure for a private Time Machine.

Before performing these steps, verify that the AFP protocol is enabled on your ReadyNAS. Note that it is enabled by default.

To back up your Mac:

1. Log in to your ReadyNAS.

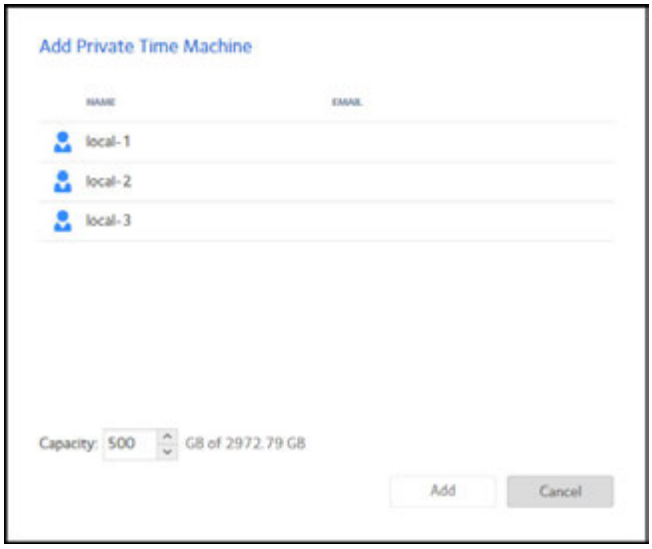
2. Select **Backup > Time Machine**.



User accounts already configured for a private Time Machine display here.

3. Click the add (**+**) button.

Note A maximum of 16 Time Machines can be specified. The 16 can be 16 private or 15 private and 1 shared Time Machine.



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 264.) 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**.
8. Click the **Use Disk** button.
   The connect window opens requesting the user name and password.
9. In the **Name** field, enter the user name.
10. In the **Password** field, enter the password for that account.
11. Click the **Connect** button.
    Time Machine begins the backup, which can take several minutes to start.

Increase Your Shared Time Machine Backup Capacity

The first time you run a Time Machine backup on your Mac, a sparse bundle (a Mac OS file system directory type) 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 261.)

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 180.
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 261.