Support

Thank you for purchasing this NETGEAR product.

After installing your device, locate the serial number on the label of your product and use it to register your product at https://my.netgear.com. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR web site. For product updates, additional documentation, and support, visit http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR.
Phone (Other Countries): Check the list of phone numbers at http://support.netgear.com/general/contact/default.aspx.

NETGEAR recommends that you use only the official NETGEAR support resources.

Compliance

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

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © NETGEAR, Inc. All rights reserved.

Revision History

<table>
<thead>
<tr>
<th>Publication Part Number</th>
<th>Version</th>
<th>Publish Month</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>202-11025-09</td>
<td>OS 1.4</td>
<td>October 2014</td>
<td>• Updated manual for ReadyRECOVER, and some corrections.</td>
</tr>
<tr>
<td>202-11025-08</td>
<td>OS 1.4</td>
<td>January 2014</td>
<td>• Updated manual to support OS 1.4 and OS 1.4.1.</td>
</tr>
<tr>
<td>202-11025-07</td>
<td>OS 1.3</td>
<td>May 2013</td>
<td>• Updated manual to support ReadyDATA 516.</td>
</tr>
</tbody>
</table>
| 202-11025-06            | OS 1.2  | March 2013    | • Updated information about File and Folder permissions. (See Configure the File and Folder Access Settings on page 104.)
|                         |         |               | • Added information about Smart Snapshot Management for shares and LUNs. (See Smart Snapshot Management on page 189.)
<p>|                         |         |               | • Changed name of lock period icon to zoom icon and updated description. For an example of how to use this icon, see Roll Back to a Snapshot on page 183. |
| 202-11025-05            | OS 1.1  | December 2012 | • Revised information about cloned shares and LUNs. (See Manage Snapshots for Shares and LUNs on page 177.) |
| 202-11025-04            | OS 1.1  | November 2012 | • Moved the chapter about managing disks and volumes ahead of the chapter about configuring the system, network, and global file-sharing protocol settings. |</p>
<table>
<thead>
<tr>
<th>Document ID</th>
<th>OS Version</th>
<th>Date</th>
<th>Updates</th>
</tr>
</thead>
</table>
| 202-11025-03 | OS 1.1     | September 2012 | • Revised Supported Browsers.  
• Added Optional Uninterruptible Power Supplies.  
• Revised multiple screens to remove the Language menu that is now included in the Profile menu.  
• Removed information about setting up share quotas for users and groups. This information might be added back for a later release.  
• Where applicable, added a note to explain that without at least one volume, changes are not saved after you reload the ReadyDATA. |
| 202-11025-02 | OS 1.1     | June 2012  | • Revised and added information to Manage Replication and Recovery Between Two or More Systems.  
• Added information about share quotas to View and Change the Properties of a Share.  
• Changed the Language selection (see Select the Language on page 48). |
| 202-11025-01 | OS 1.1     | June 2012  | First publication.                                                      |
# Table of Contents

## Chapter 1  Getting Started

- Quick-Start Guide ................................................. 9
- Additional Documentation .................................. 11
- Supported Operating Systems .............................. 11
- Supported Browsers .......................................... 11
- Install the ReadyDATA in Your Network ............. 12
- Use RAIDar to Discover the ReadyDATA ............ 13
- Register the ReadyDATA ..................................... 16

## Chapter 2  Manage Disks and Volumes

- Supported Disks and Initial Startup .................... 18
- About RAID Levels, Volumes, and Disk Representation .... 19
  - RAID Levels .................................................... 20
  - Volumes: Overview ........................................... 21
  - Optional Expansion Disk Arrays and Volumes ....... 22
  - Graphical Enclosure and Color Coding of the Disks Onscreen .... 23
  - RAID and Volume Implementation ...................... 24
- Manage Volumes .................................................. 26
  - Create a Volume and Select the RAID Level ......... 26
  - View the Properties of a Volume ....................... 31
  - Search for a Volume .......................................... 33
  - Expand a Volume .............................................. 33
  - Configure Write and Read Boost Disks to Improve Performance 36
  - Export and Import a Volume ............................. 39
  - Delete a Volume .............................................. 40
  - Scrub a Volume .............................................. 41
  - Configure Global Spare Disks ............................ 42

## Chapter 3  Configure the System Settings

- Customize the Basic System Components ............... 46
- Set the Clock .................................................... 46
- Select the Language .......................................... 48
- Set the Administrator Password ......................... 49
- Configure System Alerts .................................... 50
- Configure the Host Name ................................... 52
- Set the Theme .................................................... 52
- Configure the Network Settings ......................... 53
Configure the Physical Ethernet Interfaces .......................................................... 55
Configure the Virtual Network Interface Cards .................................................. 56
Automatic Private IP Addressing Without a DHCP Server .................................. 63
Configure Channel Bonding .................................................................................. 63
Configure Global File-Sharing Protocols ............................................................... 67
Supported File-Sharing Protocols ......................................................................... 68
Configure File-Sharing Protocols ......................................................................... 68

Chapter 4  Manage Shares and LUNs

Shares and LUNs .................................................................................................... 74
Manage Shares for Network Attached Storage ...................................................... 74
About Shares .......................................................................................................... 75
Create a Share ......................................................................................................... 77
View and Change the Properties of a Share ........................................................... 80
Migrate a Share to Another Volume ....................................................................... 83
Export a Share to a NAS ......................................................................................... 85
Import a ReadyDATA Share ................................................................................... 87
Delete a Share ......................................................................................................... 89
Set Up Access Rights to Shares ............................................................................. 90
Configure the Network Access Settings ................................................................. 94
Configure the File and Folder Access Settings ....................................................... 104
Reset Security Settings ......................................................................................... 105
Manage LUNs for Storage Area Networks ............................................................. 105
About LUNs ............................................................................................................ 105
Create a LUN .......................................................................................................... 107
View and Change the Properties of a LUN, Including Size Expansion ................. 109
Migrate a LUN to Another Volume ........................................................................ 115
Export a LUN to a NAS ........................................................................................ 116
Import a ReadyDATA LUN ..................................................................................... 118
Delete a LUN .......................................................................................................... 119
Assign LUNs to LUN Groups and Manage Access Rights ..................................... 121
Assign a LUN to a LUN Group ............................................................................... 121
Remove a LUN from a LUN Group ....................................................................... 123
Remove a LUN Group ............................................................................................ 124
Manage Access Rights for LUN Groups ............................................................... 124
Access a Share from Network-Attached Device ............................................... 127
Use a Windows Device ......................................................................................... 128
Use a Mac OS X Device ....................................................................................... 129
Use a Linux or Unix Device ................................................................................. 130
Access LUN Groups from an iSCSI-Attached Device .......................................... 131
Access LUN Groups Using Microsoft iSCSI Software Initiator .......................... 132

Chapter 5  Manage User Groups and User Accounts

About Security, User Groups, and Users ............................................................... 140
Configure the Global Security Access Mode ....................................................... 140
Manage User Groups for the Local Database ...................................................... 142
Create a User Group ............................................................................................ 143
Delete a User Group .................................................. 144
Edit a User Group .................................................... 144
Manage User Accounts for the Local Database ................. 146
Create a User Account .............................................. 146
Delete a User Account ............................................... 148
Edit a User Account .................................................. 149

Chapter 6  System Maintenance and Monitoring

System Maintenance .................................................. 152
Update the Firmware .................................................. 152
Reset the Firmware to Factory Defaults ........................... 156
Shut Down or Restart the System ................................... 158
Recover the Administrator Password ............................... 158

System Monitoring .................................................... 159
System Real-Time and Historical Monitoring ....................... 159
System Health Information ........................................... 163
Disk Status and Health Information ................................ 163
System Logs .............................................................. 165
SNMP Monitoring ....................................................... 166
Optional Uninterruptible Power Supplies .......................... 167
About Uninterruptible Power Supplies .............................. 167
UPS Configurations ..................................................... 167
Add and Monitor UPS Devices ....................................... 171

Chapter 7  Backup, Replication, and Recovery

Manage Snapshots for Shares and LUNs ......................... 177
Basic Snapshot Concepts ............................................. 177
Automatic and Manual Snapshots .................................. 178
Importing Snapshots ................................................... 182
Roll Back to a Snapshot ............................................... 183
Clone a Snapshot ....................................................... 186
Delete a Snapshot ....................................................... 189
Recover Data from a ReadyDATA to an Attached Device .... 193
Recover Data from a Snapshot to a Network-Attached Device 193
Recover Data from a Snapshot to an iSCSI-Attached Device 193
Recover Data from a Snapshot to a Windows Server .......... 194
Manage Replication and Recovery Between Two or More Systems .... 194
About Replication ....................................................... 195
Recover Replicated Data .............................................. 196
Seed or Reseed Replication ........................................... 196
Access ReadyDATA Replicate and Register Systems ........... 197
Schedule or Resume Periodic Replication Using ReadyDATA Replicate .... 199
Configure or Resume Continuous Replication Using ReadyDATA Replicate 209
View the Network Using ReadyDATA Replicate ................... 217
View the Jobs Using ReadyDATA Replicate ....................... 218
Monitor the Jobs Using ReadyDATA Replicate .................... 220
Run Job Reports Using ReadyDATA Replicate ......................... 222
Exchange Certificates for Local Replication ......................... 223
Schedule Replication for Local Replication ......................... 225
Resume Local Replication ............................................. 233
Monitor and Manage Local Replication .............................. 243

Appendix A  Factory Default Settings

Index
Getting Started

This software manual describes how to configure and manage a ReadyDATA system that runs ReadyDATA OS 1.4 for production storage, backup storage, and disaster recovery.

Because this product is intended for business use, this manual is written for network and data center administrators who are familiar with RAID networking concepts.

This chapter includes the following sections:

- Quick-Start Guide
- Additional Documentation
- Supported Operating Systems
- Supported Browsers
- Install the ReadyDATA in Your Network
- Use RAIDar to Discover the ReadyDATA
- Register the ReadyDATA

---

**Note:** For more information about the topics covered in this manual, visit the support website at [http://support.netgear.com](http://support.netgear.com).

---

**Note:** Firmware updates with new features and bug fixes are made available from time to time on [downloadcenter.netgear.com](http://downloadcenter.netgear.com). Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

---

**Note:** In this manual, the term *volume* refers to a logical volume with a RAID configuration, and the terms *hard disk drive* and *disk* refer to a physical storage device.
Quick-Start Guide

This manual provides detailed instructions about using your ReadyDATA system, and the NETGEAR recommendations about configuring and managing the system and backing up the data and system configuration.

Note: If you are using your ReadyDATA system with ReadyRECOVER, after installing the ReadyDATA system and connecting it to your network, see the ReadyRECOVER Software User Manual. You can use a ReadyDATA system using ReadyRECOVER for applications alongside ReadyRECOVER, but ReadyRECOVER requires a dedicated disk volume in the system.

ReadyRECOVER on your ReadyDATA system works with ShadowProtect agents on your (supported) Windows systems to provide:

- **Protection of physical and virtual servers, workstations and desktops.** These include the following:
  - Windows physical servers
  - VMware, Hyper-V, and Xen servers (Windows guest operating systems)
  - Windows workstations and desktops
- **Synthetic full backups.** Every backup is represented as a full image (.vhdx) and provides quick single-file restoration and hardware-independent full restoration of server operating systems and their applications to any supported platform (physical servers, virtualization platforms, workstations, desktops).
  - **Fifteen-minute recovery points.** Backups can be set to 15-minute intervals, regardless of the total capacity of the server (64 TB maximum per logical drive).
  - **Storage efficiency.** The storage consumption of this solution is highly efficient because all data is compressed when it is written and only unique blocks of ongoing backups must be stored on disk. The more backups that are stored, the larger the savings become.
- **WAN efficiency.** For customers replicating backup sets offsite, only incremental block changes are replicated with ReadyDATA replicate.

The ReadyDATA system relies on the following software applications:

- **RAIDar.** A set-up utility to locate the ReadyDATA on the LAN and launch Dashboard.
- **Dashboard.** A browser-based interface to configure and manage the ReadyDATA.

To start using the ReadyDATA system quickly, review the following sections and chapters in this order:

1. *Install the ReadyDATA in Your Network* on page 12. Follow the instructions in the installation guide that came with your system and the hardware manual for your system.
These documents are available at www.netgear.com/readydata. Connect the ReadyDATA to a DHCP server.

2. Use RAIDar to Discover the ReadyDATA on page 13. Use RAIDar to locate the ReadyDATA on the network.

3. Create a Volume and Select the RAID Level on page 26. Assign the disks to volumes and select the RAID level for each volume. Without at least one volume, changes are not saved after you reload the ReadyDATA. Make sure that you create a volume before you configure any other settings.

4. Chapter 3, Configure the System Settings. Configure the basic system components, network settings, and global file-sharing protocols.

5. Create a Share on page 77 and Create a LUN on page 107. Create shares (NAS data sets) for data transfer and storage over SMB, NFS, AFP, and FTP. Create LUNs (SAN data sets) for data transfer and storage over iSCSI.

6. Create a User Account on page 146. Create a user account for each person who should have access to the ReadyDATA, or connect to an external Active Directory.

7. Set Up Access Rights to Shares on page 90 and Assign LUNs to LUN Groups and Manage Access Rights on page 121. Set the access right for the shares and LUNs.

8. Manage Snapshots for Shares and LUNs on page 177. Back up the data that is stored in the shares and LUNs by creating snapshots.
Additional Documentation

NETGEAR maintains a website that supports ReadyDATA products. Visit www.netgear.com/readydata for reviews, tutorials, comparison charts, software updates, documentation, an active user forum, and much more.

The following documentation is available at www.netgear.com/readydata:

- Hardware manual
- Installation guide
- Data sheet
- White papers
- ReadyRECOVER Software User Manual

Supported Operating Systems

The ReadyDATA is supported on the following operating systems:

- Microsoft Windows Vista, 7, and 8
- Microsoft Windows Server 2003 R2, all editions, x86 and x64
- Microsoft Windows Server 2008/2008R2 and 2012, all editions, x86 and x64
- Apple Mac OS X 10.5 Leopard or later
- VMware ESX 3.5
- VMware vSphere ESX and ESXi Server 4/4.1
- VMware vSphere ESXi 5.x
- Citrix XenServer 6
- RedHat Enterprise Linux AS 4.7/5.2 or later
- SUSE Linux Server 10.1/10.2 or later, x86 and x64
- Fedora 8 or later
- HP-UX 11
- Solaris 10 or later

Supported Browsers

The ReadyDATA Dashboard supports the following browsers:

- Microsoft Internet Explorer 9.0+
- Apple Safari, 2.0+
- Google Chrome 18+
- Mozilla Firefox 14+
- Opera 9.5+
Note: If you have difficulty accessing the ReadyDATA Dashboard, or if you notice unexpected behavior, try using another browser.

Install the ReadyDATA in Your Network

Install the ReadyDATA as explained in the installation guide that came with your system. LED status information and the boot menu are explained in the hardware manual for your system.

Connect the ReadyDATA to your network, and make sure that a DHCP server can reach the ReadyDATA. By default, the ReadyDATA is configured to receive an IPv4 IP address from a DHCP server.

Note: If the ReadyDATA cannot locate a DHCP server, it is assigned an IP address through Automatic Private IP Addressing (APIPA). For more information, see Automatic Private IP Addressing Without a DHCP Server on page 63.

If you want to use the ReadyDATA with an IPv6 address, first access the ReadyDATA through the IPv4 address assigned by the DHCP server, and then configure the IPv6 setting as explained in Configure the Network Settings on page 53.

Note: For information about the default system settings, see Appendix A, Factory Default Settings.

Note: If an unexpected condition or failure prevents the ReadyDATA from booting after you complete an initial set-up procedure, see the LED status information in the hardware manual for your system.
Use RAIDar to Discover the ReadyDATA

RAIDar is a software application that you use to discover ReadyDATA systems on the network. RAIDar is included on the resource CD that came with your system. It includes versions for Windows, Mac, and Linux operating systems. RAIDar is also available at www.netgear.com/readydata.

RAIDar displays the discovered ReadyDATA units with their status LED icons. The volume, disk, UPS, and fan LED icons are not operational for the ReadyDATA.

You can use the following buttons to learn more about the ReadyDATA units on the network:

- **Setup.** Launches Dashboard for the highlighted ReadyDATA.
- **Browse.** Displays the shares available on the highlighted system (LUNs are not displayed). This feature works on a Windows platform only.
- **Rescan.** Updates the list of ReadyDATA systems on the network, and updates the status of each system that is discovered.
- **Locate.** Nonfunctional button.
- **About.** Displays RAIDar information.
- **Help.** Displays the help screen.
- **Exit.** Closes RAIDar.

➢ To discover the ReadyDATA system and launch the Dashboard:

1. Install the appropriate version of RAIDar on a computer that is connected to the same LAN as the ReadyDATA.

   **Note:** If you are using Windows XP before SP2, disable the Internet connection firewall.

2. Launch the RAIDar utility.
RAIDar displays a screen that lists the systems on the network and provides details about the status of each system it discovers.

By default, the virtual NICs (VNICs) of the ReadyDATA are DHCP enabled for IPv4, and the RAIDar utility should be able to discover the ReadyDATA.

**Note:** The ReadyDATA requires a DHCP server for initial discovery.

If the ReadyDATA is not detected, check the following and click the **Rescan** button to try again:

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

3. Highlight the ReadyDATA and click the **Setup** button.

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

4. Log in to the ReadyDATA using the default login credentials:
   - As the default user name, enter **admin** (case-sensitive).
   - As the default password, enter **password** (case-sensitive).
The Dashboard has two main bars:

- **Navigation bar.** Located across the top of the screen, the navigation bar helps you navigate through Dashboard. You can also configure the language for the system and the administration password, and access help. To return to the Dashboard home screen, select **System**, or if you are in a system configuration screen, select **Overview**.

- **System configuration bar.** Located below the navigation bar, the system configuration bar helps you to navigate through the four configuration screens that you access from the System menu. To return to the Dashboard home screen, select **Overview**.

Some screens show section headings on the left side. When you select a section heading, settings are displayed that let you configure the ReadyDATA.

The configuration procedures in this manual indicate the selection from the navigation bar, and, if applicable, the selection from the system configuration bar and the section heading on a screen. 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 system configuration bar, and **Services** is the section heading on the **Settings** screen.
Register the ReadyDATA

You must register your product before you can use NETGEAR telephone support. Register the ReadyDATA by accessing the NETGEAR Product Registration website.

➢ To register the ReadyDATA:

1. Locate the serial number on the Dashboard home screen or on the chassis label of your product.

   The product registration web page displays.

3. Take one of the following actions:
   • If you have never registered a NETGEAR product, click the Continue button.
   • If you have registered a NETGEAR product in the past, enter your email address and password and click the Log in button.

4. Follow the prompts.

   The ReadyDATA is registered.
This chapter describes how to configure the disks and volumes in the ReadyDATA. It contains the following sections:

- Supported Disks and Initial Startup
- About RAID Levels, Volumes, and Disk Representation
- Manage Volumes
Supported Disks and Initial Startup

The ReadyDATA 5200 supports up to 12 disks. With optional expansion disk arrays that can contain either 12 or 24 disks each, you can increase the total number of supported disks to 60. The following figure shows a ReadyDATA 5200 with an optional expansion disk array that supports 24 disks and another array that supports 12 disks.

The ReadyDATA 516 supports up to 6 disks and does not support expansion disk arrays.

---

**Note:** ReadyDATA systems do not recognize non-NETGEAR disks. When you insert a non-NETGEAR disk, Dashboard displays the error message *Disk is not signed by NETGEAR*. ReadyDATA systems recognize only disks that you obtain through NETGEAR or a NETGEAR authorized reseller.

---

For information about adding and removing disks, see the hardware manual for your system.

![Figure 1. ReadyDATA 5200 with optional disk expansion arrays as displayed on Dashboard](image)

The first time that you start your ReadyDATA storage system, you can do so with or without disks installed.

If you start with disks installed, several scenarios are possible, each of which affects the way that the disks are displayed in the graphical enclosure of Dashboard:

- **Disks do not contain data:**
  These disks are made available as unallocated disks.
• **Disks do not contain data that is recognized by the ReadyDATA:**
  These disks are made available as unallocated disks. If you attempt to use these disks for another volume, you are *not* warned of possible data loss.

• **Disks contain a portion of a ReadyDATA volume:**
  These disks are indicated as being part of a non-operational volume. If you attempt to use these disks for another volume, you are warned of possible data loss.

• **Disks contain a complete volume from a foreign ReadyDATA storage system:**
  - If the disks were imported successfully, the virtual disk LEDs in the graphical enclosure in the Dashboard provide a visual indication.
  - The volume is mounted on the ReadyDATA.
  - Any shares and LUNs on the volume are configurable through Dashboard.
  - Clients can access the shares through the configured file-sharing protocols, but you must reconfigure the LUN settings (see *Manage Access Rights for LUN Groups* on page 124).

### About RAID Levels, Volumes, and Disk Representation

This section includes the following topics:

• **RAID Levels**
• **Volumes: Overview**
• **Optional Expansion Disk Arrays and Volumes**
• **Graphical Enclosure and Color Coding of the Disks Onscreen**
• **RAID and Volume Implementation**
RAID Levels

Redundant array of independent disks (RAID) is a storage technology that balances data protection, system performance, and storage space by determining how the storage system distributes data. Many different ways of distributing data have been standardized into various RAID levels. Each RAID level offers a trade-off 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.

Various RAID combinations provide different levels of protection against data loss, capacity, and speed. The ReadyDATA supports the following RAID levels:

- **RAID 0** (striped disks) distributes data across several disks in a way that gives improved speed and no lost capacity, but all data on all disks is lost if any one disk fails. Although such an array has no actual redundancy, it is customary to call it RAID 0.

- **RAID 1** (mirrored disks) duplicates data across two disks in the array, providing full redundancy. Two disks each store exactly the same data, at the same time, and at all times. Data is not lost as long as one disk survives. Total capacity of the array equals the capacity of the smallest disk in the array. At any given instant, the contents of both disks in the array are identical.

- **RAID 5** (striped disks with single parity; in a ZFS system also referred to as RAIDz1) combines three or more disks in a way that protects data against loss of any one disk; the storage capacity of the array is reduced by one disk.

- **RAID 6** (striped disks with dual parity; in a ZFS system also referred to as RAIDz2) can recover from the loss of two disks.

- **RAID 10** (or 1+0) uses both striping and mirroring. “01” or “0+1” is sometimes distinguished from “10” or “1+0”; a striped set of mirrored subsets and a mirrored set of striped subsets are both valid, but distinct, configurations.

- **RAID 50** (or 5+0) combines multiple RAID 5 sets providing RAID 5 reliability with improved write performance for larger configurations. The striping of disks in RAID 5 improves write performance, but the incremental improvement decreases as the number of disks increases. In RAID 50, striping across the RAID 5 sets provides improved performance. RAID 50 is provided as an option through a pop-up screen during the creation of a RAID 5 volume with six or more disks.

- **RAID 60** (or 6+0) combines multiple RAID 6 sets providing RAID 6 reliability with improved write performance for larger configurations. The striping of disks in RAID 6 improves write performance, but the incremental improvement decreases as the number of disks increases. In RAID 60, striping across the RAID 6 sets provides improved performance. RAID 60 is provided as an option through a pop-up screen during the creation of a RAID 6 volume with eight or more disks.

A RAID set with redundancy continues to function without interruption when one (or possibly more, depending on the selected RAID level) disk of the array fails, although the array is then vulnerable to further failures. When you replace a bad disk with a new one, the array is rebuilt while the ReadyDATA continues to operate normally. The ReadyDATA supports high availability, allowing you to hot-swap disks without powering down.
Select the RAID level based on the number of disks and protection level that you want to use for the volume:

Table 1. RAID level and required number of disks

<table>
<thead>
<tr>
<th>RAID Level</th>
<th>Number of Required Disks</th>
<th>Redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 0</td>
<td>1 or more</td>
<td>None</td>
</tr>
<tr>
<td>RAID 1</td>
<td>2 only (more disks are not supported in RAID 1)</td>
<td>Supported</td>
</tr>
<tr>
<td>RAID 5</td>
<td>3 or more</td>
<td>Supported for one disk</td>
</tr>
<tr>
<td>RAID 6</td>
<td>4 or more</td>
<td>Supported for two disks</td>
</tr>
<tr>
<td>RAID 10</td>
<td>4 or more, but an even number</td>
<td>Supported for all disks</td>
</tr>
<tr>
<td>RAID 50</td>
<td>6 or more, but an even number</td>
<td>Supported for one disk per RAID 5 set</td>
</tr>
<tr>
<td>RAID 60</td>
<td>8 or more, but an even number</td>
<td>Supported for two disks per RAID 6 set</td>
</tr>
</tbody>
</table>

Note: Although a RAID system can be used to back up data from other disks or another array, RAID is not meant to be an alternative or substitute for backing up data. Data might become damaged or destroyed without harm to the disk or disks on which it is stored. For example, part of the data might be overwritten by a system malfunction; a file might be damaged or deleted by user error or malice, and not noticed for days or weeks; and the entire array is at risk of physical damage.

Volumes: Overview

In the most general sense, volumes are data storage devices. Volumes can be either physical or logical. In this manual, the term volume refers to a logical volume with a RAID set, and the terms hard disk drive, disk, and physical volume refer to a physical storage device.

The ReadyDATA treats disks and volumes in the following ways:

- Each logical volume can correspond to one disk.
- A logical volume can be made up of more than one disk.
- You cannot divide a single disk among two or more volumes.
- Although you can install different types of disks within the ReadyDATA, you can select only disks of the same physical performance characteristics to be members of one volume. For example, you cannot mix nearline SATA 7,200 rpm disks with SAS 15,000 rpm disks within one volume.

After you create a volume (see Create a Volume and Select the RAID Level on page 26), you can make the following changes to the volume:
• Expand the volume by adding more disks (see Expand a Volume on page 33)
• Attach write cache and read cache SSD disks to boost the performance of volumes that contain slower disks such as SATA 7,200 rpm or nearline SAS 7,200 rpm disks (see Configure Write and Read Boost Disks to Improve Performance on page 36)
• Export the volume (see Export and Import a Volume on page 39)
• Delete the volume (see Delete a Volume on page 40)

You can configure any disk that is not allocated to a volume as a hot spare for any volume in case of failure (see Configure Global Spare Disks on page 42). Because the hot spare provides only a temporary solution, it can be of any physical performance characteristics, that is, it does not need to match the physical performance characteristics of the disks in the volumes.

**Note:** ReadyRECOVER requires its own volume. If you use ReadyRECOVER, include this requirement in your space and volume planning. The ShadowProtect agent can create this volume for you. See the ReadyRECOVER Software User Manual for more information.

### Optional Expansion Disk Arrays and Volumes

You can create a volume that spans more than one enclosure by using one or more optional expansion disk arrays (EDA2000 and EDA4000).

The number of volumes that you can create within a ReadyDATA is limited only by the total number of disks in the ReadyDATA and expansion disk arrays. With several expansion disk arrays, the ReadyDATA supports up to 60 disks and volumes.

**Note:** When you span a volume across several enclosures, the volume is dependent on the availability of all enclosures. If one enclosure fails, the entire volume goes offline.
Graphical Enclosure and Color Coding of the Disks Onscreen

The physical disks that are installed in the ReadyDATA and optional expansion disk arrays are represented in a graphical enclosure onscreen:

![Figure 2. ReadyDATA with optional disk expansion arrays as displayed on Dashboard](image)

The disks in the graphical enclosure are color coded. The meaning of the colors is explained in the following table:

Table 2. Disk color codes

<table>
<thead>
<tr>
<th>Sample</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Black</td>
<td>Not assigned to a volume. Available for selection.</td>
</tr>
<tr>
<td></td>
<td>Gray</td>
<td>Assigned to a volume. Not available for selection.</td>
</tr>
<tr>
<td></td>
<td>Gray, no</td>
<td>The disk is not signed by NETGEAR. Not available for use with ReadyDATA.</td>
</tr>
<tr>
<td>label</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blue</td>
<td>Member of the displayed volume.</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>Write boost disk for the displayed volume.</td>
</tr>
<tr>
<td></td>
<td>Orange</td>
<td>Read boost disk for the displayed volume.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Assigned as a global spare disk.</td>
</tr>
</tbody>
</table>

The status LED icon on a disk icon (on the right side) can be off, green, or red:

- **Off.** Indicates that the status of the disk is unknown (for example, see the black and gray disks in the previous table).
• **Green.** Indicates that the disk is online (for example, see the blue, yellow, orange, and green disks in the previous table).

• **Red.** Indicates that the disk is bad or faulty.

For more information about disk status and disk health, see *Disk Status and Health Information* on page 163 and the hardware manual.

### RAID and Volume Implementation

The ReadyDATA supports a new, proprietary RAID architecture that is both flexible and easy to administer. This new architecture is based on the Zettabyte File System (ZFS), allowing you to configure different RAID levels for different volumes on the same platform.

Volume and RAID level are tied together on the ReadyDATA in the following ways:

• You can select the RAID level for a volume only when you create the volume. After you create a volume, you cannot change the RAID level.

• When you create a volume, you select the disks that participate in the RAID set. You can select from the following RAID levels: RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10. You can add more disks to a volume, but in the process of doing so, you cannot change the RAID level. A single exception exists: When you expand a RAID 1 volume, the RAID level is automatically upgraded to RAID 10.

RAID levels are indicated onscreen as follows:

• **New RAID sets.** A new RAID set is indicated with a plus sign: RAID 0+, RAID 1+, RAID 5+, and RAID 6+. The exception is RAID 10, which is indicated with a plus sign and a zero: RAID 1+0.

• **Expanded RAID sets:**
  - An expanded RAID 0 set is indicated in the same way as a new RAID set: RAID 0+.
  - An expanded RAID 1 set is indicated with a plus sign and a zero, and becomes in fact a RAID 10 set: RAID 1+0.
  - Expanded RAID 5 and RAID 6 set indicated with a plus sign, a zero, and an expansion sequence number that indicates the number of RAID groups that have been added:
    • RAID 5+0, nx
    • RAID 6+0, nx
  
  For example, a RAID 6 set expanded twice by the addition of two RAID groups goes from RAID 6+ to RAID 6+0, 2x, and then to RAID 6+0, 3x.

  - An expanded RAID 10 set is indicated in the same way as a new RAID 10 set: RAID 1+0.
The following table explains the RAID nomenclature. The sequential expansion number is indicated by n, and x indicates *times* (for example, 2x is two times).

**Table 3. RAID nomenclature on the ReadyDATA**

<table>
<thead>
<tr>
<th>RAID Level</th>
<th>New RAID</th>
<th>Expanded RAID</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 0</td>
<td>RAID 0+</td>
<td>RAID 0+</td>
</tr>
<tr>
<td>RAID 1</td>
<td>RAID 1+</td>
<td>RAID 1+0, nx</td>
</tr>
<tr>
<td>RAID 5</td>
<td>RAID 5+</td>
<td>RAID 5+0, nx</td>
</tr>
<tr>
<td>RAID 6</td>
<td>RAID 6+</td>
<td>RAID 6+0, nx</td>
</tr>
<tr>
<td>RAID 10</td>
<td>RAID 1+0</td>
<td>RAID 1+0</td>
</tr>
</tbody>
</table>
Manage Volumes

This section includes the following topics:

- Create a Volume and Select the RAID Level
- View the Properties of a Volume
- Search for a Volume
- Expand a Volume
- Configure Write and Read Boost Disks to Improve Performance
- Export and Import a Volume
- Delete a Volume
- Scrub a Volume
- Configure Global Spare Disks

---

**Note:** After you make a change on the Storage screen, you might need to click the *Refresh* button (⟳) to update the display.

---

Create a Volume and Select the RAID Level

➢ **To create a volume and select the RAID level:**

1. On the ReadyDATA screen, select **System > Storage**.
   The Storage screen displays.
   The following figure shows one optional expansion disk array and one volume. A new system does not have any volumes.
2. In the enclosure, click the disks that you want to select as members of the volume. You can select disks with a black color coding only. If you have an expansion disk array, you can select disks from both the ReadyDATA and the expansion disk array.

The selected disks are highlighted and all volume buttons become available, including the **New Volume button** under the enclosure:

3. Below the enclosure, click **New Volume** button.

The New Volume pop-up screen displays:
The RAID levels that are displayed depend on the number of disks that you selected.

4. Configure the following settings:
   - **Name.** Enter a name for the volume. The volume name must begin with a letter, and can contain only alphanumeric characters, underscores (_), hyphens (-), periods (.), and colons (:). The volume names mirror, logs, and spare are reserved and cannot be used, as are all names that begin with the c[0–9] pattern. However, you can use names that begin with the C[a–z0–9] or c[a–z] pattern.
   - **RAID.** From the drop-down list, select the RAID level. The RAID level that you can select depends on the number of disks that you selected in Step 2. For more information, see Table 1 on page 21.
     If you select RAID 5 and six or more disks (or RAID 6 and eight or more disks), a screen opens letting you select RAID 5+0 instead of RAID 5 (or RAID 6+0 instead of RAID 6).

5. Click the **Create** button.
   The volume is created.

6. To the left of the enclosure, click the new volume and note the following:
   - The color of the selected disks in the enclosure turns blue (1).
   - The name of the new volume displays above the enclosure (2).
   - The selected RAID level for the new volume displays below the enclosure (3).
   - Information about the new volume displays to the left of the enclosure (4).
   - The virtual LED indicates the health status of the volume (5).
Information about the volume displays to the left of the enclosure, and is explained in the following table. The color coding refers to the colors in the volume icon (that is, the circle) and the information that is displayed to the right of it. The volume icons are black in the previous figure but can display colored slices.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Color Coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>The volume storage space that filled by data in MB, GB, or TB.</td>
<td>Purple</td>
</tr>
<tr>
<td>Snapshots</td>
<td>The number of snapshots that have been taken.</td>
<td>Green</td>
</tr>
<tr>
<td>Reserved</td>
<td>The volume storage space that is reserved in MB, GB, or TB.</td>
<td>Orange</td>
</tr>
<tr>
<td>Free</td>
<td>The volume storage space that is available in MB, GB, or TB.</td>
<td>Black or gray</td>
</tr>
<tr>
<td>Type</td>
<td>The configured RAID level.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Dedupe</td>
<td>By default, dedupe is 1.00, indicating that deduplication is enabled and that the initial deduplication ratio is set. A number higher than 1.00 indicates that data has been deduplicated and that the deduplication ratio has increased. The deduplication ratio is the data capacity of the volume divided by its usable storage capacity. <strong>Note:</strong> You cannot disable deduplication on a volume, but you can do so on a share or LUN that resides on the volume.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Compression</td>
<td>By default, compression is 0.00, indicating that compression is enabled but that data has not yet been compressed. A number higher than 0.00 indicates the number of times that data has been compressed. For example, 5.00 indicates that data has been compressed five times.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Virtual health LED</td>
<td>The volume is healthy.</td>
<td>Green</td>
</tr>
</tbody>
</table>
### Item

<table>
<thead>
<tr>
<th>Description</th>
<th>Color Coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>The volume is degraded.</td>
<td>Yellow</td>
</tr>
<tr>
<td><strong>Note:</strong> Even though the health LED might be yellow and not red, the volume might actually be bad or faulty if the number in the Free field (to the right of the volume icon) is a strange or negative number and if the numbers in the Data, Snapshots, and Reserved fields (also to the right of the volume icon) are zero.</td>
<td></td>
</tr>
<tr>
<td>The volume is bad or faulty.</td>
<td>Red</td>
</tr>
</tbody>
</table>
View the Properties of a Volume

➢ To view the properties of a volume:

1. Select System > Storage.

   The Storage screen displays.

2. To the left of the graphical enclosure, click the volume that you want to explore.

3. Click the gear icon.

   A pop-up menu displays.

4. Select Properties.

   The properties of the volume display at the right side of the screen in the Summary section (see the following figure).

5. (Optional) Click the I/O Stats label.

   I/O statistics display.

6. (Optional) Click the Disks label.

7. Status and health information about the disks that are members of the volume displays.
Note: You can also use a shortcut to display the properties of a volume. Click the screen Expand button (.expand) on the top right of the screen to display the properties (see the red oval in the previous figure). Click the same button (which now shows a reversed arrow (shrink)) again to hide the properties (see the red oval in the previous figure).

The following table explains the properties:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td></td>
</tr>
<tr>
<td>RAID</td>
<td>The configured RAID level.</td>
</tr>
<tr>
<td>Data</td>
<td>The storage space filled with data in MB, GB, or TB.</td>
</tr>
<tr>
<td>Snapshots</td>
<td>The number of snapshots that have been taken.</td>
</tr>
<tr>
<td>Reserved</td>
<td>The storage space that is reserved in MB, GB, or TB.</td>
</tr>
<tr>
<td>Free</td>
<td>The storage space that is available in MB, GB, or TB and in a percentage.</td>
</tr>
<tr>
<td>Health</td>
<td>The health of the volume. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Online</strong>. The volume is healthy.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Degraded</strong>. The volume is degraded.</td>
</tr>
</tbody>
</table>
Search for a Volume

1. Select System > Storage.

   The Storage screen displays.

2. Below the navigation bar, select your search criteria in one of the following ways:
   • From the All Volumes drop-down list, select a volume.
   • In the Filter by name field, enter a volume name (you can enter the initial letters of the name). If needed, to the right of the field, click the magnifier glass button to search for the volume.

Expand a Volume

You can expand 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 all disks in the volume with higher-capacity disks.

Expansion is immediate, independent of the amount of stored data on the volume, and does not affect users. You cannot change the RAID level during the expansion. The only exception is a horizontal expansion of a volume with RAID 1, which becomes RAID 10.

**Horizontal Expansion**

Horizontal expansion requires that you add the correct number of disks for the selected RAID level, and that the disks are of the same physical performance level (disk type, speed, and size). For example, you can expand an existing volume that consists of four disks in a RAID 6 set by adding four more disks.

The following table explains the minimum number of disks required to expand a volume horizontally:

**Table 4. Disks required for horizontal volume expansion**

<table>
<thead>
<tr>
<th>RAID Level</th>
<th>Number of Disks Required for Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 0</td>
<td>Any.</td>
</tr>
<tr>
<td>RAID 1</td>
<td>Even number. RAID level automatically upgrades to RAID 10.</td>
</tr>
<tr>
<td>RAID 5</td>
<td>3 or a multiple of 3.</td>
</tr>
<tr>
<td>RAID 6</td>
<td>4 or a multiple of 4.</td>
</tr>
<tr>
<td>RAID 10</td>
<td>4 or more, but an even number.</td>
</tr>
</tbody>
</table>

An expanded RAID 5 volume is a RAID 50 (RAID 5+0) volume. An expanded RAID 6 volume is a RAID 60 (RAID 6+0) volume.

➢ **To expand an existing volume horizontally:**

1. Add the required number of disks to your storage system as indicated in *Table 4*.

   For more information about how to add a disk to your system, see the hardware manual for your system, which is available at [www.netgear.com/readydata](http://www.netgear.com/readydata).

2. Select System > Storage.

   The Storage screen displays.
3. To the left of the graphical enclosure, click the volume that you want to expand.

4. In the enclosure, click the disk or disks that you want to add to the volume.

   You can select disks with a black color coding only. The selected disk or disks are highlighted, and to the left of the enclosure, the **Expand** button displays:

   ![Expand button](image)

   **Note:** The **Expand** button becomes available only if you select enough disks for the configured RAID level of the volume.

5. Click the **Expand** button.

   A pop-up screen displays, asking you to confirm the expansion.

6. Click the **Yes** label.

   The volume is expanded, and updated information about the volume displays to the left of the enclosure.
Vertical Expansion

To vertically expand a volume, you must replace all disks in the volume with larger-capacity disks of the same physical performance level (disk type and speed). You can vertically expand volumes with RAID 1, RAID 5, RAID 6, or RAID 10.

For example, you can expand an existing volume in a RAID 6 set that consists of four 500 GB SATA 7,200 rpm disks by replacing all four disks with 750 GB SATA 7,200 rpm disks.

➢ To vertically expand a 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 www.netgear.com/readydata.

   Note: You must use supported disks in your ReadyDATA system. For more information, see Supported Disks and Initial Startup on page 18.

2. Wait for the volume to resync your data.

   You can continue to use your ReadyDATA system while the volume is resyncing. Resyncing can take several hours. The start and completion of the resyncing process is recorded in the system log (see System Logs on page 165).

   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 50.

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

Configure Write and Read Boost Disks to Improve Performance

To enhance the performance of an existing volume and improve I/O operations, you can add one or more high-performance disks such as SSDs to unload write (log) or read (cache) operations, or both. You can easily remove write and read disks from a volume. For write and read operations, you would not need to select disks with very large storage capacities.

You can attach both write and read disks to a volume:

• **Write boost.** Assign one or more separate write disks to improve the write performance of the array. NETGEAR recommends that you use SSDs that are optimized for writing.

• **Read boost.** Assign one or more separate cache disks to accelerate read operations in the array. NETGEAR recommends that you use SSDs that are optimized for reading.
To attach a write or read boost disk to an existing volume:

1. Select System > Storage.
   - The Storage screen displays (see the following figure).
2. To the left of the graphical enclosure, click the volume that you want to expand.
3. In the enclosure, click the disk or disks that you want to configure as write or read disks for the volume.

   You can select disks with a black color coding only. The selected disk or disks are highlighted.

Note: The previous figure shows SAS disks as write boost and read boost disks. However, you would normally use SSDs for such purposes.

4. Perform one of the following actions:
   - Click the Write boost button. The selected disk or disks are assigned to the volume for write operations. The color of the selected log disks in the enclosure turns yellow: 🟦
     (You would normally use an SSD as a write boost disk.)
   - Click the Read boost button. The selected disk or disks are assigned to the volume for read operations. The color of the selected cache disks in the enclosure turns orange:
(You would normally use an SSD as a read boost disk.)

Updated information about the volume displays to the left of the enclosure.

➢ **To detach a write or read boost disk from a volume:**

1. Select **System > Storage**.
   
The Storage screen displays (see the following figure).

2. To the left of the graphical enclosure, click the volume from which you want to remove write or read disks.

3. Perform one or both of the following actions in the enclosure:
   - Click the write boost disk or disks that you want to remove from the volume. You can select disks with a yellow color coding only.
   - Click the read boost disk or disks that you want to remove from the volume. You can select disks with an orange color coding only.

The selected disk or disks are highlighted, and to the left of the enclosure, the **Detach** button displays:

![Detaching disk](image)

**Note:** The previous figure shows SAS disks that are used as write boost and read boost disks. However, you would normally use SSDs for such purposes.

4. Click the **Detach** button.

Updated information about the volume displays to the left of the enclosure. A detached write or read disk becomes available again for other purposes (the color of the disk turns black).
Export and Import a Volume

The ReadyDATA lets you export an existing volume by exporting the disks on which the volume resides. You can physically insert the disks in other slots of the chassis, in an optional expansion disk array, or in another ReadyDATA that runs the same firmware version.

The share names and all share data, the LUN names and all LUN data, and all snapshots on the shares and LUNs are migrated to the new location, but you need to redefine the following settings:

• **For shares.** User permissions if an Active Directory is not integrated.
• **For LUNs.** iSCSI targets and initiator permissions.

Other than a minimal downtime during the export and import process, users are not affected, if you redefine these settings.

➢ **To export a volume:**

1. **Select System > Storage.**

   The Storage screen displays.

2. To the left of the graphical enclosure, click the volume that you want to export.

3. Click the Export button ( ).

   **Note:** The Export button is not displayed when the ReadyDATA has a single volume only. There must be at least two volumes.

4. Confirm your action.

   In the graphical enclosure, the slots with the disks that are marked for export are now shown with question mark icons.
5. Remove the disks from the physical enclosure.

➢ To import a volume:

1. Insert all disks on which the volume resides in the slots of a ReadyDATA or optional expansion disk array.

The following occurs:

- If the disks are imported successfully, the color of the imported disks in the enclosure turns blue.

- The volume is mounted on the ReadyDATA.

2. If an Active Directory is not integrated, reconfigure user permissions for shares.

   See Configure the Network Access Settings on page 94.

3. Reconfigure iSCSI targets and initiator permissions for LUNs.

   See Assign a LUN to a LUN Group on page 121 and Manage Access Rights for LUN Groups on page 124.

Delete a Volume

Before you delete a volume, migrate the data (shares and LUNs) to another volume or another storage device (see Migrate a Share to Another Volume on page 83 and Migrate a LUN to Another Volume on page 115).

➢ To delete a volume:

1. Select System > Storage.

   The Storage screen displays.
2. To the left of the graphical enclosure, click the volume that you want to delete.
3. Click the gear icon.
   A pop-up menu displays.
   
   ![Volume Information Screen]

4. Select **Destroy**.
   A pop-up screen displays.

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

5. Type **DESTROY** (all capital letters) in the field of the screen to confirm your decision.
6. Click the **Yes** 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).

**Scrub a Volume**

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

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

- **To scrub a volume:**
  1. Select **System > Storage**.
     The Storage screen displays.
2. To the left of the graphical enclosure, click the volume that you want to scrub.

3. Click the scrub icon ( ).

   Scrubbing starts, and the progress is shown in a progress bar. To stop scrubbing while in it is progress, click the X button to the right of the progress bar.

---

**Configure Global Spare Disks**

A global spare disk is a redundant disk that can automatically take the place of a failed disk in any volume. A failed disk and a spare disk taking over do not need to have the same physical performance characteristics because the replacement is temporary, similar to using a spare tire on a car with a flat tire that needs to be repaired.

**IMPORTANT:**

Having a spare disk take over after a failure is a temporary solution; replace the failed disk as soon as possible.
To create a global spare disk:

1. Select **System > Storage**.
   The Storage screen displays (see the following figure).

2. In the graphical enclosure, click the disk or disks that you want to assign as global spare disks.
   You can select disks with a black color coding only. The selected disks are highlighted and all volume buttons become available, including the **Global spare** button under the enclosure:

3. Click the **Global spare** button.
   The color of the selected disk or disks in the enclosure turns green:

   ![Global Spare Disk](image)

   The disk or disks are now available as global spare disks.

To remove a global spare disk:

1. Select **System > Storage**.
   The Storage screen displays (see the following figure).

2. In the graphical enclosure, click the global spare disk or disks that you want to remove.
   You can select disks with a green color coding only. The selected disks are highlighted and the **Remove spare** button under the enclosure becomes available:
3. Click the **Remove spare** button.

The removed spare disk or disks become available again for other purposes (the color of the disks turns black).
Configure the System Settings

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

- Customize the Basic System Components
- Configure the Network Settings
- Configure Global File-Sharing Protocols

**Note:** Without at least one volume, changes are not saved after you reload the ReadyDATA. 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. For information about how to configure volumes, see *Chapter 2, Manage Disks and Volumes.*
Customize the Basic System Components

NETGEAR recommends that you configure the basic system components that are described in the following sections before you use the ReadyDATA:

- Set the Clock
- Select the Language
- Set the Administrator Password
- Configure System Alerts
- Configure the Host Name
- Set the Theme

Set the Clock

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

➢ To set the system time and date:

1. Select System > Overview > Hardware.

   The Dashboard home screen displays the system information:

   ![Dashboard home screen](image)

2. To the right of the Device Time field with the date and time, click the clock icon.

   The Date and Time Settings screen displays:
3. From the **Time Zone** drop-down list, select the correct time zone for your location.
   So that your files are correctly time-stamped, NETGEAR recommends that you select the time zone in which the ReadyDATA is physically located.

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

5. Click the **Apply** button.
   If you change the time zone, you must restart the ReadyDATA, as follows:
   a. Click the power icon in the upper right corner of the navigation bar:

   ![Power Icon](image)

   ![Power Icon](image)

   b. From the drop-down list, select **Restart**.
   c. Confirm your selection.
      The ReadyDATA shuts down gracefully and then restarts.
      If you enabled email alerts, the ReadyDATA sends a message after it restarts.
Select the Language

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

➢ To configure language settings:

1. On the navigation bar, at the right, select Profile.

   The Profile menu displays:

   ![Profile menu]

2. In the Language section, specify a language by selecting a check box, or select the Auto check box, which enables the ReadyDATA to set the language automatically to the one used by the browser.

   After you change the language, Dashboard restarts.

   **Note:** NETGEAR recommends selecting a language based on the region in which you use the ReadyDATA.
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 this password can change settings or erase data that is stored on the ReadyDATA.

To change the administrator password:

1. On the navigation bar, at the right, select Profile.
   The Profile menu displays (see the following figure).

2. Select Change Admin Password.
   The Change Admin Password pop-up screen displays:

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter a new administrator password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Reenter the new password.</td>
</tr>
<tr>
<td>Password Recovery Question</td>
<td>Choose a question that few people can answer. For example, you might enter</td>
</tr>
<tr>
<td></td>
<td>First dog’s name? or Best friend in Kindergarten? as your password</td>
</tr>
<tr>
<td></td>
<td>recovery question.</td>
</tr>
<tr>
<td>Password Recovery Answer</td>
<td>Enter the answer to the question you provided in the Password Recovery</td>
</tr>
<tr>
<td></td>
<td>field.</td>
</tr>
<tr>
<td>Recovery Email Address</td>
<td>Enter the email address to which you want a reset password to be sent.</td>
</tr>
</tbody>
</table>

4. Click the Apply button.
Configure System Alerts

If you provide an email address for alert notices, system events such as disk errors and failures, changes in network connectivity, power supply failures, fan speed irregularities and fan failures, and CPU and enclosure temperature violations generate email alert messages. The ReadyDATA divides system events into two categories, mandatory and optional. Mandatory events always generate email alert messages. You can control which optional system events generate email alert messages.

Email Alert Contacts

To receive an email message alerting you if a system event that requires your attention occurs, provide one or more email addresses for alert messages. You can use an email address that is accessible from a smartphone to help you monitor the ReadyDATA when you are away from it.

➢ To manage alert email contacts:

1. Select System > Settings > Alerts.

   The Settings screen displays the alerts settings:

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Contacts</td>
<td>Click the plus button (+) to add a contact email addresses. Click the plus button (+) to add more contact email addresses. Select an address and then click the gear icon to edit an existing alert contact, or click the minus button (−) to delete it.</td>
</tr>
<tr>
<td>User</td>
<td>Enter the user name that is associated with the email address.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password that is associated with the email address.</td>
</tr>
</tbody>
</table>
Configure the System Settings

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

   The Settings screen displays the alert events settings:

   ![Alert Events Settings](image)

   2. In the Alert Events section, select or clear any event check boxes.

   You can clear any nondimmed event check boxes (**Disk Full**, **Fan**, and **Disk Temperature**).

   Events represented by dimmed check boxes (**Disk Failure**, **Volume**, **Power**, and **UPS**) always trigger email alerts.

### Item Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>Enter the address of the outgoing SMTP server.</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>Enter the port number for the outgoing SMTP server.</td>
</tr>
<tr>
<td>From</td>
<td>Enter a name that identifies the sender of the email alert.</td>
</tr>
<tr>
<td>Use TLS</td>
<td>Select this check box to use email encryption over TLS.</td>
</tr>
</tbody>
</table>

3. (Optional) To determine if you configured the contact information correctly, click the **Send Test Message** button.

**Alert Event Settings**

The ReadyDATA is preconfigured to generate email alert messages when system events occur. You can determine which optional system events generate alerts. NETGEAR recommends that you keep all alerts enabled; however, if you are aware of a problem, you could disable an alert temporarily.

- **To manage alert event settings:**

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

  The Settings screen displays the alert events settings:

  ![Alert Events Settings](image)

  2. In the Alert Events section, select or clear any event check boxes.

     You can clear any nondimmed event check boxes (**Disk Full**, **Fan**, and **Disk Temperature**).

     Events represented by dimmed check boxes (**Disk Failure**, **Volume**, **Power**, and **UPS**) always trigger email alerts.
3. Click Apply.

Configure the Host Name

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

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

➢ To change the host name:

1. Select **System > Overview > Hardware**.
   
The Dashboard home screen displays the system information:

   ![Dashboard Home Screen](image)

2. Click the gear icon to the right of the Name field.
   
The New Hostname pop-up screen displays:

   ![New Hostname Pop-up](image)

3. In the **Name** field, enter a new host name.
   
The host name can have a maximum of 14 characters. Only the following characters can be used: A-Z, a-z, 0-9, and minus (-).

4. Click the **Apply** button.

Set the Theme

Changing the Dashboard theme is optional.

➢ To change the Dashboard theme:

1. On the navigation bar, at the right, select **Profile**.
2. In the Theme section, select either the **Black** check box (which is the default selection) or the **Silver** check box.

![Theme selection screenshot]

The Dashboard display adjusts according to your selection.

**Configure the Network Settings**

This section includes the following topics:

- *Configure the Physical Ethernet Interfaces*
- *Configure the Virtual Network Interface Cards*
- *Automatic Private IP Addressing Without a DHCP Server*
- *Configure Channel Bonding*

The ReadyDATA provides two physical 1 Gb Ethernet interfaces and two physical 10 Gb Ethernet interfaces. The Ethernet interfaces can be used independently as individual interfaces or combined in a channel-bonded configuration using LACP and hash types 2 through 4. Channel bonding provides redundancy or increased throughput.

You can create and attach virtual NICs (VNICS) to individual and bonded interfaces. The primary benefit of virtual networking is that it allows the ReadyDATA to service many separate networks and to control how much bandwidth is used for each storage-related task.

For each VNIC, you can configure the following settings:

- VLAN membership
- Bandwidth limits
- IPv4 or IPv6 settings
- DNS servers

The following figure illustrates the use of VNICS in a ReadyDATA network configuration. (Throttle refers to the bandwidth limit.)
Figure 3. VNICS in a ReadyDATA Network Configuration

The following table lists the default network settings before any configuration has occurred:

Table 5. Default network settings

<table>
<thead>
<tr>
<th>Item</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Ethernet interface (eth1 and eth2)</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>1500</td>
</tr>
<tr>
<td>Speed (Mbps)</td>
<td>1000</td>
</tr>
<tr>
<td>Duplex</td>
<td>Full</td>
</tr>
<tr>
<td>Bonding</td>
<td>None</td>
</tr>
<tr>
<td>VNNIC</td>
<td>One attached to each interface (for example, vnic0 to eth0 and vnic1 to eth1)</td>
</tr>
<tr>
<td>Virtual NICs (vnic0 and vnic1)</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>1500</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>0</td>
</tr>
<tr>
<td>Bandwidth limit</td>
<td>None</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>IPv4 with DHCP enabled, and IPv6 disabled</td>
</tr>
<tr>
<td>DNS</td>
<td>No server</td>
</tr>
</tbody>
</table>
Configure the Physical Ethernet Interfaces

➢ To configure an Ethernet interface:

1. Select **Network**.

   The Network screen displays:

   ![Network Screen]

2. Click the gear icon to the right of an Ethernet interface.

   A pop-up menu displays (see the following figure).

3. Select **Properties**.

   The Ethernet Properties screen displays for the selected interface:

   ![Ethernet Properties Screen]
Configure the System Settings

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>Enter the MTU in bytes. The default setting is 1500 bytes.</td>
</tr>
<tr>
<td>Speed (Mbps)</td>
<td>Specify the interface speed. Because this setting does not determine the link speed, you can specify any setting between 1 Mbps and the maximum speed supported by the interface (either 1,000 Mbps or 10,000 Mbps).</td>
</tr>
<tr>
<td>Duplex</td>
<td>Select the duplex method from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• Auto. The ReadyDATA autosenses the type of duplex connection.</td>
</tr>
<tr>
<td></td>
<td>• Full. Full duplex, the default setting.</td>
</tr>
<tr>
<td></td>
<td>• Half. Half duplex.</td>
</tr>
</tbody>
</table>

5. Click the **Apply** button.

Configure the Virtual Network Interface Cards

By default, each physical Ethernet interface has one virtual NIC (VNIC) that has the following configuration:

- A name that is based on the number of the associated Ethernet interface. For example, vnic0 is associated with eth0.
- DHCP-enabled for IPv4
- No VLAN membership

The default VNIC has the same numbering as the Ethernet interface that it is associated with (eth0 has vnic0; eth1 has vnic1).

You can add multiple VNICs to each single physical Ethernet interface and channel interface.
To create and configure a VNIC:

1. Select **Network**.

   The Network screen displays:

   ![Network Screen](image)

   - **eth0**
     - MAC Address: 00:36:62:36:12:1B
     - Duplex: Full
     - Speed: 10Gbps
   - **vnic0**
     - MAC Address: 00:36:62:36:12:1B
     - MTU: 1500
     - VLAN: 0
     - IP Settings: DHCP IPv4
     - IP Address: 192.168.1.41
     - Bandwidth: 10Gbps
   - **eth1**
     - MAC Address: 00:36:62:36:12:1B
     - Duplex: Full
     - Speed: 10Gbps
   - **vnic1**
     - MAC Address: 00:36:62:36:12:1B
     - MTU: 1500
     - VLAN: 0
     - IP Settings: DHCP IPv4
     - IP Address: 192.168.1.158
     - Bandwidth: 10Gbps

2. Click the gear icon to the right of an Ethernet interface.
   
   A pop-up menu displays (see the following figure).

3. Select **Create VNIC**.

   ![Create VNIC Pop-up](image)

   The new VNIC displays next to the Ethernet interface. New VNICs are numbered in sequential and ascending order irrespective of the interface they are attached to. For example, in a system with two Ethernet interfaces, eth0 (with default vnic0) and eth1 (with default vnic1), a new VNIC is numbered vnic2, irrespective of whether you attach it to eth0 or eth1.
4. Click the gear icon to the right of the VNIC that you just created. A pop-up menu displays:

5. Select Properties.
   The VNIC Settings pop-up screen displays with the General pane in view. (You can switch back and forth between the VNIC panes by clicking the General, TCP/IP, and DNS tabs.)

6. Configure the general settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lists the VNIC name. The name is vnicX, in which X is a number in sequential and ascending order irrespective of the interface the VNIC is attached to. The VNICs in a system with two interfaces are vnic0 and vnic1.</td>
</tr>
<tr>
<td>MTU</td>
<td>Enter the MTU in bytes. The default setting is 1500 bytes.</td>
</tr>
</tbody>
</table>
7. Click the TCP/IP tab.

The IP settings display. The IPv4 and IPv6 settings are mutually exclusive.

8. Select whether to use IPv4 or IPv6.

When you select a configuration method from the **Configure IPv4** drop-down list, the IPv6 settings are dimmed; when you select a configuration method from the **Configure IPv6** drop-down list, the IPv4 settings are dimmed.

The following figure shows the IPv4 settings; the next figure shows the IPv6 settings.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Enter a VLAN ID. The default setting ID is 0.</td>
</tr>
<tr>
<td>Note: If you use VLAN IDs, the switch to which you connect the ReadyDATA must support VLAN tagging.</td>
<td></td>
</tr>
<tr>
<td>Bandwidth Limit (Mbps)</td>
<td>Enter the bandwidth limit in Mbps. Depending on the Ethernet interfaces that are installed in the ReadyDATA, the maximum limit is either 1,000 Mbps or 10,000 Mbps.</td>
</tr>
</tbody>
</table>
9. Configure the IP settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPv4 settings</strong></td>
<td></td>
</tr>
<tr>
<td>Configure IPv4</td>
<td>From the drop-down list, select how IPv4 is configured:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Using DHCP.</strong> The ReadyDATA functions as a DHCP client, and the IPv4 settings are automatically configured by a DHCP server on your network.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manually.</strong> You must enter the IPv4 address and subnet mask for the ReadyDATA, and the router through which the ReadyDATA is connected to the network.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>Enter the IPv4 address for the ReadyDATA.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet mask for the ReadyDATA.</td>
</tr>
<tr>
<td>Router</td>
<td>Enter the IPv4 address for the router through which the ReadyDATA connects to your network. The default setting is 192.168.1.1.</td>
</tr>
<tr>
<td><strong>IPv6 settings</strong></td>
<td></td>
</tr>
<tr>
<td>Configure IPv6</td>
<td>From the drop-down list, select how IPv6 is configured:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatically.</strong> The ReadyDATA is configured with an IPv6 address through stateless autoconfiguration without the requirement of a DHCPv6 server on your network. The ReadyDATA does need to be connected to the Internet for stateless autoconfiguration to function.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Using DHCP.</strong> The ReadyDATA functions as a DHCPv6 client, and the IPv6 settings are automatically configured by a DHCPv6 server on your network. The default prefix length for DHCP is /64, to support some common DHCPv6 servers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manually.</strong> You must enter the IPv6 address and prefix length for the ReadyDATA and the router through which the ReadyDATA is connected to the network.</td>
</tr>
</tbody>
</table>
Configure the System Settings

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>Enter the IPv6 address for the ReadyDATA.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Enter the prefix length for the ReadyDATA. The default address is ::1 (that is, 0::1).</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Enter the IPv6 address for the router through which the ReadyDATA connects to your network. The default prefix length is 128. You can specify a prefix length by appending /prefix length, for example, /64, when you specify the IP address.</td>
</tr>
</tbody>
</table>

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

10. For IPv4 settings, you can select (or clear) the Primary Router check box to make this VNIC the primary route for data to and from the ReadyDATA.

11. Click the DNS tab. The DNS settings display:

12. To add a DNS server, click the + button.

13. Enter an IP address.

14. Click the Add button.
15. If you want to add more DNS servers, repeat Step 12 through Step 14. You can configure multiple DNS servers.

16. If you want to remove a DNS server, select the server, and click the – button.

17. To save the settings on all three VNIC panes, click the Apply button.

**Note:** If you change the IP address of the ReadyDATA, your browser loses its connection to Dashboard. To reconnect to the ReadyDATA, launch the RAIDar utility, click the Rescan button to locate the device, and click the Setup button to reconnect.

➢ **To remove a VNIC:**

1. **Select Network.**

   The Network screen displays:

   ![Network Screen](image)

2. Click the gear icon to the right of the VNIC that you want to remove. A pop-up menu displays:
3. Select the **Remove** icon.
4. Confirm the removal.

**Automatic Private IP Addressing Without a DHCP Server**

The ReadyDATA requires an IPv4 DHCP server for initial configuration of the VNICs, which, by default, are configured as DHCP clients.

If the ReadyDATA cannot locate a DHCP server, it is assigned an IP address through Automatic Private IP Addressing (APIPA). The IP address is in the 169.254.x.x/16 subnet. The last two octets of the address are based on the MAC address of the physical interface, which is printed on a label next to the physical interface. You need to convert the hexadecimal MAC address to decimal numbers to determine the last two octets of the IP address. In the unlikely situation that another device with the same IP address is on the subnet, the ReadyDATA attempts to use the next IP address (169.254.x.x+1).

For example, if the MAC address is 00:25:90:63:91:be, the IP address is 169.254.145.190/16. The fifth octet of the MAC address is 91, which translates to 145 in decimal notation. The sixth octet of the MAC address is be, which translates to 190 in decimal notation.

**Configure Channel Bonding**

Channel bonding is optional.

A bonded channel combines two Ethernet interfaces into a single logical link or link aggregation group (LAG). Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing.

The ReadyDATA supports a static LAG and a dynamic LAG with active or passive LACP for automatic configuration of a channel link with another device. Both the ReadyDATA and the device with which the channel link is established must support the same mode (static LAG or dynamic LAG).

On the ReadyDATA, LAGs are implemented with three hash types:

- **Layer 2.** Based on the source and destination MAC addresses. All traffic between the ReadyDATA 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 ReadyDATA and a particular device is transmitted on the same physical link.
- **Layer 4.** Based on the source and destination port numbers. Traffic between the ReadyDATA and a particular device can be spread across multiple links.

You can select to use combinations of hash types, in which case the hash types are used simultaneously and the connection might be more secure but slightly slower.

After you create an aggregation link, you can expand the link with yet another interface (three Ethernet interfaces), or even another aggregation link (four Ethernet interfaces). Alternately, with four Ethernet interfaces, you can create two aggregation links and then aggregate these two links into one double aggregation link that consists of all four Ethernet interfaces.
To configure a bonded channel:

1. Select **Network**.

   The Network screen displays:

   ![Network Screen](image)

   2. Click the gear icon to the right of an Ethernet interface.

      A pop-up menu displays (see the following figure).

   3. Select **Bond with**.

      A second pop-up screen displays the Ethernet interfaces and, if already configured, the aggregated interfaces (bonded channels):

   ![Bonded Adaptor Pop-up](image)

   4. Select the name of the interface that you want to be member of the bonded channel.

      The New Bonded Adaptor pop-up screen displays:
5. Configure the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| LACP Mode     | Select the LACP mode from the drop-down list:  
|               | • **Off**. The aggregation interface does not transmit LACPDUs to other LACP devices or respond to LACPDUs from other LACP devices. Select this mode for a static LAG. This is the default setting.  
|               | • **Active**. The aggregation interface actively transmits LACPDUs to other LACP devices to set up a link channel. Select this mode for a dynamic LAG with active LACP.  
|               | • **Passive**. The aggregation interface responds only to LACPDUs from other LACP devices. Select this mode for a dynamic LAG with passive LACP.  
|               | **Note**: Both the ReadyDATA and the device with which the channel link is established must support the same mode. |
| LACP Timer    | If the LACP mode is set to **Active**, select a value for the LACP timer from the drop-down list:  
|               | • **Short**. LACPDUs are sent frequently, with a short interval between LACPDU transmissions. This is the default setting.  
|               | • **Long**. LACPDUs are sent infrequently, with a long interval between LACPDU transmissions. |
| Hash Type     | Select one or more check boxes to specify the hash types to be used:  
|               | • **Layer 2**. The channel link that is established is based on the source and destination MAC addresses.  
|               | • **Layer 3**. The channel link that is established is based on the source and destination IP addresses.  
|               | • **Layer 4**. The channel link that is established is based on the source and destination port numbers. |

6. Select the **Create** button.

The new bonded channel displays as an aggregation interface (aggrX, in which X is a number in sequential and ascending order) on the Network screen.

7. To configure the new aggregation interface further, click the gear icon to the right of the aggregation interface.

A pop-up menu displays:
8. Select **Properties**.

The aggregation settings pop-up screen displays:

```
86

9. Configure the general settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Use the default name or enter a custom name. The default name is aggrX, in which X is a number in sequential and ascending order.</td>
</tr>
<tr>
<td>MTU</td>
<td>Enter the MTU in bytes. The default setting is 1500 bytes.</td>
</tr>
<tr>
<td>LACP Mode</td>
<td>You configured these settings when you set up the aggregation interface. For information about these settings, see the table in Step 5. (Make changes on the aggregation settings pop-up screen.)</td>
</tr>
<tr>
<td>LACP Timer</td>
<td></td>
</tr>
<tr>
<td>Hash Type</td>
<td></td>
</tr>
</tbody>
</table>

10. Click the **Apply** button.

11. Configure the switch or router to which the ReadyDATA is attached for channel bonding.
To remove an aggregation link and reestablish separate Ethernet interfaces:

1. Select **Network**.

   The Network screen displays:

   ![Network screen](image)

2. Click the gear icon to the right of the aggregation interface that you want to remove.

   A pop-up menu displays:

   ![Pop-up menu](image)

3. Select **Remove**.

4. Confirm the removal.

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

**Configure Global File-Sharing Protocols**

Network access to data stored on the ReadyDATA is through file-sharing protocols, which handle the type of access and transfer of data, or for Bonjour and SNMP, discovery and management of the ReadyDATA in a network. For shares, you can select several protocols; for LUNs, the protocol is always iSCSI. (iSCSI is enabled by default.)
The global file-sharing protocol settings affect the file-sharing protocols that allow access to shares. If a protocol is globally disabled, you can configure it for a share, but it does not take effect until you enable the protocol globally. For information about how to configure and enable file-sharing protocols for shares, see File-Sharing Protocols to Access Shares on page 76.

**Supported File-Sharing Protocols**

The ReadyDATA supports the following file-sharing protocols:

- **SMB (Server Message Block)**. Used mainly by Microsoft Windows computers and sometimes by Mac OS X computers for share access. SMB uses TCP/IP. SMB is enabled by default.
- **AFP (Apple File Protocol)**. Used by Mac OS X computers for share access. AFP is enabled by default.
- **NFS (Network File Service)**. Used by Linux and Unix clients for share access. Mac OS X users can access NFS shares through console shell access. The ReadyDATA supports NFS over UDP and TCP. NFS is disabled by default.
- **FTP (File Transfer Protocol)**. The ReadyDATA supports anonymous and controlled user access for FTP clients. You can elect to set up port forwarding to nonstandard ports for better security when you access files over the Internet. FTP is disabled by default.
- **SNMP**. Lets you monitor but not manage the ReadyDATA over a network management system. SNMP is disabled by default.
- **SSH**. Lets you remotely manage the ReadyDATA over an SSH connection. SSH is disabled by default.

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

**Configure File-Sharing Protocols**

> To view and globally configure file-sharing protocols:

1. Select **System > Settings > Services**.

The Services section of the Setting screen displays (the following figure shows the top of the screen only):

![Protocol Settings Screen](image)

The protocol buttons with a green LED are globally enabled; those with a black LED are globally disabled. Click a protocol button to display the protocol settings screen.
2. Configure the protocol settings one protocol at a time.

Setting the protocols is explained in the following:

- Configure SMB, AFP, NFS, or SSH
- Configure FTP
- Configure SNMP

**Note:** For information about the Replicate button (see the previous figure), see *Chapter 7, Backup, Replication, and Recovery."

**Configure SMB, AFP, NFS, or SSH**

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

➢ **To enable or disable any of these protocols:**

1. Select *System > Settings > Services.*

   The Services section of the Setting screen displays (the following figure shows the top of the screen only):

2. Click the protocol button (*SMB*, *AFP*, *NFS*, or *SSH*).
3. Select the **Enable** check box to enable the protocol; clear the **Enable** check box to disable the protocol.
4. Click the **Apply** button.

**WARNING:**

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

**Configure FTP**

➢ **To configure FTP:**

1. Select *System > Settings > Services.*

   The Services section of the Setting screen displays (the following figure shows the top of the screen only):
2. Click the **FTP** button.

The FTP Settings screen displays:

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable FTP</td>
<td>Select the check box to enable FTP globally; clear the check box to disable FTP globally.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the number of the port that is used for FTP control traffic on the ReadyDATA. The default port number is 21.</td>
</tr>
<tr>
<td>Authentication mode</td>
<td>Select the authentication mode from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Anonymous</strong>. Users can connect anonymously. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>User</strong>. Users are authenticated through the local database.</td>
</tr>
<tr>
<td>Allow upload resumes</td>
<td>Select whether users are allowed to resume a paused or stalled upload by making a selection from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>. Resuming an upload is disabled. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>. Resuming an upload is enabled.</td>
</tr>
<tr>
<td>Passive ports</td>
<td>Enter the beginning port and ending port of the passive port range. This is the port range on the ReadyDATA that is available to clients who initiate a connection to the ReadyDATA. The default range is 32768–65535.</td>
</tr>
<tr>
<td>Use Masquerade Address</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Configure the System Settings

Configure SNMP

1. Select **System > Settings > Services**.

   The Services section of the Setting screen displays (the following figure shows the top of the screen only):

   ![Services Screen](image1)

   1. Click the **SNMP** button.

   The SNMP Settings screen displays:

   ![SNMP Settings](image2)

4. Click the **Apply** button.
2. Configure the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SNMP</td>
<td>Select the check box to enable SNMP globally; clear the check box to disable SNMP globally.</td>
</tr>
<tr>
<td>Community</td>
<td>Enter the community. Normally, you would enter <strong>public</strong> for a read-only community and <strong>private</strong> for a read-write community. You can leave the <strong>Community</strong> field set to <strong>public</strong> (which is the default setting), or specify a private name if you have a more segregated monitoring scheme.</td>
</tr>
<tr>
<td>Trap destination</td>
<td>Enter the IP address to which the ReadyDATA sends the traps that it generates. For information about the types of messages that can be sent, see <strong>System Logs</strong> on page 165.</td>
</tr>
<tr>
<td>Hosts allowed access</td>
<td>Enter a network address that specifies the hosts that are allowed to access the ReadyDATA.</td>
</tr>
</tbody>
</table>

3. Click the **Apply** button.

**Note:** For information about the NETGEAR SNMP MIB, see **SNMP Monitoring** on page 166.
This chapter describes how to create, manage, and access shares and LUNs on the ReadyDATA. This chapter includes the following sections:

- Shares and LUNs
- Manage Shares for Network Attached Storage
- Set Up Access Rights to Shares
- Manage LUNs for Storage Area Networks
- Assign LUNs to LUN Groups and Manage Access Rights
- Access a Share from Network-Attached Device
- Access LUN Groups from an iSCSI-Attached Device

Note: Without a volume, you cannot configure any shares or LUNs. For information about how to configure volumes, see Chapter 2, Manage Disks and Volumes.
Shares and LUNs

The volumes on your ReadyDATA can be divided into shares and logical unit numbers (LUNs), both of which are logical entities on one or more disks.

- **Shares.** Shares are NAS data sets that allow data transfer and storage over SMB, NFS, AFP, and FTP. (For general information about these protocols, see *Configure Global File-Sharing Protocols* on page 67.) Dashboard displays shares in the following way:

Figure 4. Share icon

- **LUNs.** LUNs are SAN data sets that allow data transfer and storage over iSCSI and Fiber Channel devices. The ReadyDATA supports iSCSI devices only. Dashboard displays LUNs in the following way:

Figure 5. LUN icon

Shares and LUNs enable you to organize data in a volume by type, group, user, department, and so on. Within one volume, you can create multiple shares and LUNs, each one with its own specific configuration.

This chapter explains the configuration and use of shares and LUNs in detail.

**Manage Shares for Network Attached Storage**

This section describes the following topics:

- **About Shares**
- **Create a Share**
- **View and Change the Properties of a Share**
- **Migrate a Share to Another Volume**
- **Export a Share to a NAS**
- **Import a ReadyDATA Share**
- **Delete a Share**
About Shares

Each share has a configuration that is independent of other shares that reside on the same volume. A share configuration includes settings such as logbias, compression, deduplication (referred to as dedupe), protection, file-sharing protocols, and access rights.

The configuration settings of a share are stored in the volume (that is, in the pool) in which the share resides. This design allows a share to be portable when a disk is moved from one array to another array. You can specify whether a snapshot is created, and with what frequency it is created.

Note: ReadyRECOVER creates and manages its own shares within the volume dedicated to ReadyRECOVER. Do not make changes to these shares. Do not create non-ReadyRECOVER shares within a ReadyRECOVER volume. For more information, see the ReadyRECOVER Software User Manual.

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

- **Undefined.** The entire nonreserved storage space on the volume is available to the share. Storage space is assigned on demand instead of up front. This method greatly improves the utilization rate of the share because storage space is assigned only as data is written to the share. The size of the share is reported as the entire nonreserved storage space on the volume. As data is written to the share, the used storage space is displayed on the volume icon in purple.

- **Quota.** You set a quota for the share. All storage space that you specify when you create the share is also allocated up front. The share size cannot grow beyond the quota, but you can increase the quota. The size of the share is reported as the quota that you specify. As data is written to the share, the used storage space is displayed on the volume icon in purple.

Although the quota of an individual share cannot exceed the size of the volume, a volume allows oversubscription: The aggregate quota of the shares on a volume can exceed the size of the volume. Taking reserved storage space into account, storage space is assigned on demand.

In addition, whether you set a quota or not, you can reserve share storage space to guarantee that storage space is available on the volume. Snapshots, other shares, and LUNs on the volume cannot consume storage space that is reserved. The reserved storage space is displayed on the volume icon in orange.
The following table explains the default settings of a share. You can change these settings when you create or change the share.

**Table 6. Share default settings**

<table>
<thead>
<tr>
<th>Item</th>
<th>Default State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logbias(^a)</td>
<td>Latency</td>
</tr>
<tr>
<td>Compression</td>
<td>Disabled</td>
</tr>
<tr>
<td>Dedupe</td>
<td>Disabled</td>
</tr>
<tr>
<td>Protection</td>
<td>Continuous</td>
</tr>
<tr>
<td>Sync Writes</td>
<td>Allowed</td>
</tr>
<tr>
<td>Interval</td>
<td>Daily</td>
</tr>
<tr>
<td>Size</td>
<td>No limitation</td>
</tr>
<tr>
<td>Access</td>
<td>Denied until you set permissions</td>
</tr>
</tbody>
</table>

\(^a\) You can change the logbias only when you change the properties of a share.

**File-Sharing Protocols to Access Shares**

The availability of a file-sharing protocol for shares depends on the global file-sharing protocol setting. If a protocol is globally disabled, you can configure it for a share, but it does not take effect until you enable the protocol globally. For information about global file-sharing protocols, see *Configure Global File-Sharing Protocols* on page 67.

Shares are accessed over a LAN or WAN network connection. Network access to data stored on the ReadyDATA is managed by file-sharing protocols, which also handle the transfer of data. You can enable multiple protocols for an individual share, allowing users to access the share through various methods. The ReadyDATA supports the following file-sharing protocols for share access:

- **SMB (Server Message Block).** Used mainly by Microsoft Windows computers and sometimes by Mac OS X computers. SMB uses TCP/IP.
- **AFP (Apple File Protocol).** Used by Mac OS X computers.
- **NFS (Network File Service).** Used by Linux and Unix clients. Mac OS X users can access NFS shares through console shell access. The ReadyDATA supports NFS over UDP and TCP.
- **FTP.** The ReadyDATA 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 ReadyDATA.
Create a Share

After you create a volume (see Create a Volume and Select the RAID Level on page 26), you can create shares on that volume.

➢ To create a share:

1. Select Shares.

2. Click the Data Set button (with four cubes).

   The Shares screen displays, showing the configured volumes on the left:

   3. Click the + button ( ) to the right of the volume to which you want to add a share.

      The New Share pop-up screen displays:
4. Configure the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the share. Do not include spaces in the name.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description to help identify the share.</td>
</tr>
<tr>
<td>Compression</td>
<td>Select the <strong>Compression</strong> check box to enable data compression. Compression saves storage space and increases the speed of data transfers, but the compression and decompression processes require more resources. By default, the <strong>Compression</strong> check box is cleared.</td>
</tr>
<tr>
<td>Dedupe</td>
<td>Select the <strong>Dedupe</strong> check box to enable deduplication, which prevents storage of redundant data on the share. Unique data is stored only once on the share, and other instances of the identical data are removed and replaced by a pointer to the unique data. This storage method saves storage space and increases the speed of data transfers. By default, the <strong>Dedupe</strong> check box is cleared. <strong>Note:</strong> In order to find duplicated data, the ReadyDATA creates and manages a table of data to compare to. If this table gets too large, deduplication is disabled. If this happens, the ReadyDATA issues an alert and makes a log entry. If you look at the property settings, the dedupe check box will no longer be set.</td>
</tr>
</tbody>
</table>
### Manage Shares and LUNs

#### Protection
Select the **Continuous Protection** check box to enable data protection through snapshots and configure the frequency at which snapshots are made. By default, the **Continuous Protection** check box is selected. For more information about snapshots, see *Manage Snapshots for Shares and LUNs* on page 177.

#### Smart Snapshot Management
Select the **Smart Snapshot Management** check box to enable automatic snapshot pruning. When enabled, the ReadyDATA deletes snapshots as necessary so that hourly snapshots are kept for 48 hours, daily snapshots are kept for four weeks, weekly snapshots are kept for eight weeks, and monthly snapshots are kept indefinitely.

#### Interval
The interval specifies how often a snapshot is made. Make a selection from the drop-down list:
- **Hourly.** A snapshot is taken every hour on the hour.
- **Daily.** A snapshot is taken every day at midnight. This is the default setting.
- **Weekly.** A snapshot is taken every week on Friday at midnight.

#### Share (NAS)
Click the **Share (NAS)** button, which is the default setting. (Clicking the **LUN (SAN)** button creates a LUN; see *Create a LUN* on page 107.)

#### Type
Select the check boxes for the file-sharing protocols that you want to enable on the share:
- **SMB**
- **NFS**
- **AFP**
- **FTP**

For information about these protocols, see *File-Sharing Protocols to Access Shares* on page 76.

**Note:** If the New Share pop-up screen displays a red triangle with an exclamation mark for a protocol (for example, ), the protocol is globally disabled. For information about how to enable the protocol globally, see *Configure Global File-Sharing Protocols* on page 67.

#### Size
If you do not set a size, the share has unlimited access to the storage space on the volume, and the utilization rate of the share is greatly improved (over predefining the size) because storage space is assigned only as data is written to the share. By default, when you create a share, no quota or reserve is set.

**Quota**
Select the **Size** check box and enter the size of the storage space that is available to the share.

**Reserve**
Select the **Reserve** check box to reserve guaranteed storage space for the share on the volume.

---

5. Click the **Create** button.

The ReadyDATA confirms the creation of a share with the message “Data Set successfully created.” The new share is added to the Shares screen. Basic information is displayed to the right of the share.
View and Change the Properties of a Share

➢ To view and change the properties of a share:

1. Select Shares.

2. Click the Data Set button (with four cubes). The Shares screen displays (see the following figure).

3. Select the share that you want to explore by clicking it. The color of the share turns purple.

4. Right-click the share. A pop-up menu displays:

5. Select Properties. The Properties pane for the selected share displays at the right of the screen (see the next figure). The properties that are displayed in the Access section depend on the selected file-sharing protocol or protocols.

---

**Note:** You can also use a shortcut to display the Properties pane of a share. Click the screen Expand button on the top right of the screen to display the Properties pane (see the red oval on the top right of the previous figure). Click the same button (which now displays as a reversed arrow) again to hide the Properties pane.
6. Change the settings as explained in the following table. Click the Flag button (FLAG) to save any changes in a field or drop-down list.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>The size is provided for information only. To change the size, see the Size fields in the Properties section of the Properties pane.</td>
</tr>
<tr>
<td>Path</td>
<td>The path is provided for information only.</td>
</tr>
</tbody>
</table>

Manage Shares and LUNs
## Properties

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>You can enter a new name to identify the share. Names must be unique. Do not include spaces in the name.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter an optional description to help identify the share.</td>
</tr>
</tbody>
</table>
| **Logbias** | Change the logbias setting by making a selection from the Logbias drop-down list:  
  - **Latency.** Data requests are handled at high priority with a minimum of delay, but data throughput might not be optimum. This is the default setting that is automatically assigned when you create a share.  
  - **Throughput.** Data requests are handled with high data throughput, but delays in response to requests might occur. |
| **Sync Writes** | Change the setting by making a selection from the drop-down list:  
  - **Allowed.** An application can use synchronous writes, but they are not required.  
  - **Forced.** Synchronous writes are required.  
  - **Disabled.** Synchronous writes are not used.  
  The setting applies to both application writes and snapshot writes between ReadyDATAs. |
| **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 more resources. |
| **Dedupe** | Select the **Dedupe** check box to enable deduplication, which prevents storage of redundant data on the share. Unique data is stored only once on the share, and other instances of the identical data are removed and replaced by a pointer to the unique data. This storage method saves storage space and increases the speed of data transfers. |
| **Size** | You can increase the quota or reservation of an existing share without affecting or disconnecting any users. Expansion is instant, regardless of the data size. |
| **Quota** | Select the **Size** check box and enter the size of the storage space that is available to the share. |
| **Reserve** | Select the **Reserve** check box to reserve guaranteed storage space for the share on the volume. |
|             | Select the unit of measurement from the drop-down list:  
  - **MB**  
  - **GB**  
  - **TB** |
### Migrate a Share to Another Volume

Migrating a share to another volume allows you to reorganize a volume or remove the shares from a volume before deleting the volume.

**WARNING:**

Migrating a share to another volume causes all users to be disconnected from the share.
To migrate a share to another volume:

1. Select Shares.
2. Click the Data Set button (with four cubes, ![Image]).
   The Shares screen displays (see the following figure).
3. Select a share by clicking it.
   The color of the share turns purple:

4. Right-click the share.
   A pop-up menu displays.
5. Select Migrate To.
   A second pop-up menu displays the volumes:
By default, the volume on which the share resides is flagged.

6. Select the name of the destination volume.

7. Confirm the migration.
   
   A progress circle (○) displays the progress of the migration.

Export a Share to a NAS

Exporting a share to a network-attached server and then importing it allows you to easily and more quickly transfer a share by transporting the server or associated media to another location. You can use the exported share to seed replication between distant sites, to more quickly and simply resume operation in a disaster recovery scenario.

The export bundles all of the data from the share, including all snapshots, into a single file on the NFS server.

➢ To export a share to another volume:

1. Select Shares.

2. Click the Data Set button (with four cubes, 🎨 🎨 🎨 🎨).
   
The Shares screen displays (see the following figure).

3. Select a share by clicking it.
   
The color of the share turns purple:

4. Right-click the share.
A pop-up menu displays.

![Pop-up menu](image)

5. **Select Export to NAS.**

A pop-up screen displays:

![Export Share/LUN over NFS](image)

6. **Enter the appropriate values for the destination.**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Server Address</td>
<td>Enter the address of the NFS server.</td>
</tr>
<tr>
<td>Force UDP transfer</td>
<td>When this check box is selected, the default, only UDP transfers are used.</td>
</tr>
<tr>
<td>NFS Path</td>
<td>Enter the path to the directory for the file containing the exported share.</td>
</tr>
<tr>
<td>File Name</td>
<td>Enter a file name for the exported share. The export saves all of the data from the share including the snapshots and related information in a single file.</td>
</tr>
</tbody>
</table>
7. Confirm the export.
   The ReadyDATA sends an alert email when the export finishes.

**Import a ReadyDATA Share**

If you have exported a share to a network-attached server, you can import it to the ReadyDATA. For large data sets, exporting a share, moving the NAS (or media with the exported file) to the same LAN as the destination ReadyDATA, and then importing is much quicker than replicating the share over a WAN. Use this process for seeding replication from a share to a remote share, and for speeding disaster recovery.

➢ **To import a share from another volume:**

1. Select Shares.
2. Click the **Data Set** button (with four cubes).
   The Shares screen displays (see the following figure).
3. Click the **Import Share/LUN from NFS** icon next to the destination volume.

![Import Share/LUN from NFS](image)

The Import Share/LUN from NFS Server screen opens.
4. Enter the appropriate values for the source.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Server Address</td>
<td>Enter the address of the NFS server.</td>
</tr>
<tr>
<td>Force UDP transfer</td>
<td>When this check box is selected, the default, only UDP transfers are used.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Path</td>
<td>Enter the path to the directory for the file containing the exported share.</td>
</tr>
<tr>
<td>File Name</td>
<td>Enter the file name for the exported share.</td>
</tr>
</tbody>
</table>

5. Confirm the import.

The ReadyDATA sends an alert email when the import finishes.
Delete a Share

**WARNING:** Deleting a share permanently removes the data within that share.

**Note:** You cannot delete a share that is the parent of a clone. To delete the parent share, you must first delete all of its clones. For more information about clones, see *Clone a Snapshot* on page 186.

➢ To delete a share from a volume:

1. Select **Shares**.
2. Click the **Data Set** button (with four cubes, 📀 📀 📀 📀). The Shares screen displays (see the following figure).
3. Select a share by clicking it. The color of the share turns purple:

![Share Screen](image)

4. Click the **–** button (−) to the right of the share.
A pop-up screen displays.

5. Confirm the deletion by typing **DESTROY** into the field.
6. Click the **Destroy** button.

The share is deleted.

**Set Up Access Rights to Shares**

This section discusses the following topics:

- **Configure the Network Access Settings**
- **Configure the File and Folder Access Settings**
- **Reset Security Settings**

A file-sharing protocol determines how you set up access rights to an individual share and grant or restrict access rights to users, groups, hosts, or all of these. For example, you might want to grant a user read/write permission on one share, read-only permission on another share, and no access rights at all on a third share.

The following access rights options are available:

- **Read Only**. This permission allows a user or group (or users or groups on a host) to read files on the share but prevents the editing, creation, and deletion of files and folders on the share.

- **Read/Write**. This permission allows a user or group (or users or groups on a host) to read, edit, create, and delete files and folders on the share. By default, all users and groups have read/write access.

The global security access mode determines whether users are authenticated through the local database of the ReadyDATA or through an external Active Directory (see **Configure the Global Security Access Mode** on page 140):

- **Local user database**. If you use the local database, first create user groups and user accounts before you set up share access rights. The groups and users are displayed in the Access section on the Properties pane of a share. For more information about creating and managing groups and user accounts, see **Chapter 5, Manage User Groups and User Accounts**.
• **Active Directory.** If you use an external Active Directory, the user and group information is downloaded into the ReadyDATA and displayed in the Access section on the Properties pane of a share.

A button with a red triangle and an exclamation mark (for example, ![FTP](https://example.com/ftp)) indicates that the file-sharing protocol is globally disabled. For information about how to enable the protocol, see *Configure Global File-Sharing Protocols* on page 67. Even though a file-sharing protocol can be globally enabled, you can disable it for an individual share.

The access settings that you can configure for an individual share depend on the file-sharing protocol that is assigned to the share:

**Table 7. Access settings and file-sharing protocols**

<table>
<thead>
<tr>
<th>Access Settings</th>
<th>Protocols</th>
<th>SMB</th>
<th>NFS</th>
<th>AFP</th>
<th>FTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Users and group access</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Host access</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td>Permissions for newly created files and folders</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous advanced settings</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File and folder</td>
<td>File and folder access</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>

➢ **To set up the access rights for a share:**

1. Select Shares.

2. Click the Data Set button (with four cubes, ![Data Set](https://example.com/data-set)).

   The Shares screen displays (see the following figure).

3. Select the share that you want to explore by clicking it.
The color of the share turns purple:

4. Click the screen Expand button (☐) on the top right of the screen.
The Properties pane displays:

5. Locate the Network Access section and select one of the following buttons, each of which corresponds to a file-sharing protocol:
   - SMB
   - NFS
   - AFP
   - FTP

   The pane adjusts to display the access properties for the selected protocol.

6. Configure the access settings for the selected protocol as explained in the following sections (not all sections apply to all protocols):
   - Configure the Network Access Settings on page 94
7. Set the **On-Off** switch for the selected protocol:
   - To apply the access settings, click the **On-Off** switch so that the switch shows the **On** position.
   - To save the configured access settings but prevent them from taking effect, click the **On-Off** switch so that the switch shows the **Off** position.

**Note:** The settings take effect immediately (that is, no **Apply** button exists to confirm the changes).

### Configure the Network Access Settings

The user and group access settings let you set access rights to an individual share for groups and users. The host access settings let you set access rights to an individual share for users on a host.

The table in the Network section displays either the groups and users that you defined in the local database or the ones that are downloaded from the Active Directory server. For information about the local database and an Active Directory connection, see *Chapter 5, Manage User Groups and User Accounts*.

The following figure shows the Network section on the Properties pane of a share (in this example, the SMB protocol is shown):

![Figure 6. Network section of the share properties pane (SMB)](image-url)
User and Group Settings
For SMB, AFP, and FTP, you can configure access rights for groups and individual users. User and group settings do not apply to NFS.

➢ To configure user and group access settings:

1. Select Shares.
2. Click the Data Set button (with four cubes).
   The Shares screen displays (see the following figure).
3. Select the share that you want to explore by clicking it.
   The color of the share turns purple:

   ![Share Configuration Screen](image)

4. Click the screen Expand button () on the top right of the screen.
5. Locate the Network Access section and select one of the following buttons, each of which corresponds to a file-sharing protocol:
   - SMB
   - NFS
   - AFP
   - FTP

   The pane adjusts to display the access properties for the selected protocol.

6. From the All drop-down list, make one of the following selections to specify the information that you want to display onscreen:
• **All.** The default group Everyone and all groups that you configured on the Security screen or that were downloaded from the AD server are displayed, the default setting.

• **Users.** Only the individual users that you configured on the Security screen or that were downloaded from the AD server are displayed.

• **Groups.** Only the groups that you configured on the Security screen or that were downloaded from the AD server are displayed.

To search for a particular user or group, use the search field on the right.

To update the user and group information, click the **Refresh** button (⟳).

7. For each group and individual user to which you want to grant access to the share, select one of the following check boxes:

   • **Read Only.** The selected user or group is permitted to only read files on the share.

   • **Read/Write.** The selected user or group is permitted to read, edit, create, and delete files on the share.

   **Note:** If the ReadyDATA uses the local database, you can select the default group **Everyone** and set read-only or read/write access for everyone.

8. (Optional for SMB and AFP). Allow anonymous access to the share.

   If the ReadyDATA uses the local database and you have granted the default group Everyone access, you can select the **Anonymous** check box to allow anonymous access to the share. In this situation, users are not required to provide access credentials.

---

**Host Settings**

For SMB, NFS, and FTP, you can configure access rights for users on hosts. 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. Host settings do not apply to AFP.

If the table contains many hosts, use the search field on the right to search for a particular host.

➢ **To add a host and configure host access settings:**

1. Select **Shares**.

2. Click the **Data Set** button (with four cubes, ⏹️). The Shares screen displays (see the following figure).

3. Select the share that you want to explore by clicking it.
The color of the share turns purple:

4. Click the screen **Expand** button (확장) on the top right of the screen.
The Properties pane displays:

5. Locate the Network Access section and select one of the following buttons, each of which corresponds to a file-sharing protocol:
   - SMB
   - NFS
   - FTP

The pane adjusts to display the access properties for the selected protocol.

6. To add the IP address of a host from which access can be granted, click the + button (➕).

The Add Host pop-up screen displays.
7. Enter the host IP address in the **IP address** field. You can specify a range of IP addresses using CIDR notation, for example, 126.254.1.0/24, which includes every host on the 126.254.1 subnet.

8. Click the **Add** button.

   The host is added to the table.

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

9. For each host to which you want to grant access to the share, select one of the following check boxes:
   - **Read Only.** The users on the selected host are permitted to only read files on the share.
   - **Read/Write.** The users on the selected host are permitted to read, edit, create, and delete files on the share.

10. (Optional for NFS) For each host for which you want to grant the users root access, select the **Root Access** check box.

To remove a host:

1. Select **Shares**.

2. Click the **Data Set** button (with four cubes).

   The Shares screen displays (see the following figure).

3. Select the share that you want to explore by clicking it.

   The color of the share turns purple:

![Shares screen](image)

4. Click the screen **Expand** button ( ) on the top right of the screen.
The Properties pane displays:

5. Locate the Network Access section and select one of the following buttons, each of which corresponds to a file-sharing protocol:
   - SMB
   - NFS
   - AFP
   - FTP

   The pane adjusts to display the access properties for the selected protocol.

6. Select the host from the table by clicking it.

7. Click the – button (−).
8. Confirm the removal.

**Configure Advanced Access Settings**

By default, a share is visible to all users on all of the configured hosts. You can change by selecting the *Hide this share* check box to prevent users from discovering the share unless they explicitly specify the share name in the browse path. By default, this check box is cleared.

➢ To hide a share:

1. Select Shares.

2. Click the Data Set button (with four cubes).

   The Shares screen displays (see the following figure).

3. Select the share that you want to explore by clicking it.

   The color of the share turns purple:

4. Click the screen Expand button on the top right of the screen.
The Properties pane displays:

5. Locate the Network Access section and select one of the following buttons, each of which corresponds to a file-sharing protocol:
   - SMB
   - NFS
   - FTP

   The pane adjusts to display the access properties for the selected protocol.

6. Under the Advanced section, select the Hide this share check box.

7. Click the Apply button.
Configure the File and Folder Access Settings

The file and folder access settings let you change the default rights for access to folders and their files on an individual SMB, AFP, NFS, or FTP share.

The following figure shows the File and Folder Permissions section on the Properties pane of a share:

![File and Folder Permissions Section](image)

Figure 7. File and Folder Permissions Section

The following table explains the file and folder access settings:

### Table 8. File and folder access settings

<table>
<thead>
<tr>
<th>Item</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder Owner</td>
<td>You can assign a single user or the administrator as the folder owner. By default, the folder owner is set to guest.</td>
</tr>
<tr>
<td>Folder Group</td>
<td>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.</td>
</tr>
<tr>
<td>Folder Owner Rights</td>
<td>Make a selection from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled.</strong> The folder owner does not have access rights to a folder.</td>
</tr>
<tr>
<td></td>
<td><strong>Read-Only.</strong> The folder owner has read-only access to a folder.</td>
</tr>
<tr>
<td></td>
<td><strong>Read/Write.</strong> The folder owner has read/write access to a folder, the default setting.</td>
</tr>
</tbody>
</table>
Table 8. File and folder access settings

<table>
<thead>
<tr>
<th>Item</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder Groups Rights</td>
<td>Make a selection from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>. Members of a group have no access to a folder owned by a member of the group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Read-Only</strong>. Members of a group have read-only access to a folder owned by a member of the group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Read/Write</strong>. Members of a group have read/write access to a folder owned by a member of the group, the default setting.</td>
</tr>
<tr>
<td>Folder EveryOne Rights</td>
<td>Make a selection from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>. No one outside the group in which a group member owns a folder has access rights to the folder.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Read-Only</strong>. Anyone outside the group in which a group member owns a folder has read-only access to the folder.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Read/Write</strong>. Anyone outside the group in which a group member owns a folder has read/write access to the folder, the default setting.</td>
</tr>
</tbody>
</table>

**Reset Security Settings**

To set all access rights to the files and folders in an individual share to default settings, click **Reset permissions**. After you have reset the access rights, owners, groups, and anyone else with access to the share has read/write access to all files and folders on the share.

**Manage LUNs for Storage Area Networks**

This section describes the following topics:

- **About LUNs**
- **Create a LUN**
- **View and Change the Properties of a LUN, Including Size Expansion**
- **Migrate a LUN to Another Volume**
- **Export a LUN to a NAS**
- **Import a ReadyDATA Share**
- **Delete a LUN**

**About LUNs**

Each LUN has a configuration that is independent of other LUNs that reside on the same volume. A LUN configuration includes settings such as logbias, compression, deduplication (referred to as dedupe), protection, file-sharing protocols, provisioning, LUN size, and access rights.

The configuration settings of a LUN are stored in the volume (that is, in the pool) in which the LUN resides. This design allows a LUN to be portable when a disk is moved from one array...
to another array. However, iSCSI settings are not moved when you migrate a LUN from one volume to another volume or when you move the disk or disks on which the volume with the LUN resides to another array. (For information about how to configure the iSCSI settings, see Manage Access Rights for LUN Groups on page 124.)

You can specify whether a snapshot is created, and with what frequency it is created.

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

- **Thin.** 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. As data is written to the LUN, the used storage space is displayed on the volume icon in purple.

  A thin LUN lets you over-allocate its size, that is, you can assign a LUN size that is larger than the size of the volume. You can then expand the 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 over-allocated LUN resides so that you do not run out of storage space unexpectedly.

  **Note:** NETGEAR recommends that you do not use an over allocated 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 also allocated up front, and the storage space is reserved on the volume. Snapshots, other LUNs, and shares on the volume cannot consume storage space that is reserved. The reserved storage space is displayed on the volume icon in orange. 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. As data is written to the share, the used storage space is displayed on the volume icon in purple.

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

**Table 9.  LUN default settings**

<table>
<thead>
<tr>
<th>Item</th>
<th>Default State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logbias¹</td>
<td>Latency</td>
</tr>
<tr>
<td>Compression</td>
<td>Disabled</td>
</tr>
<tr>
<td>Dedupe</td>
<td>Disabled</td>
</tr>
<tr>
<td>Protection</td>
<td>Continuous</td>
</tr>
<tr>
<td>Interval</td>
<td>Daily</td>
</tr>
<tr>
<td>Provision</td>
<td>Thick</td>
</tr>
</tbody>
</table>
Create a LUN

After you create a volume (see Create a Volume and Select the RAID Level on page 26), you can create LUNs on that volume.

➢ To create a LUN:

1. Select Shares.

2. Click the Data Set button (with four cubes, 

The Shares screen displays, showing the configured volumes on the left:

3. Click the + button ( ) to the right of the volume to which you want to add a LUN.

The New LUN pop-up screen displays:
4. Configure the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the LUN. Do not include spaces in the name.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description to help identify the LUN.</td>
</tr>
<tr>
<td>Compression</td>
<td>Select the <strong>Compression</strong> check box to enable data compression. Compression saves storage space and increases the speed of data transfers, but the compression and decompression processes require more resources. By default, the <strong>Compression</strong> check box is cleared.</td>
</tr>
<tr>
<td>Protection</td>
<td>Select the <strong>Continuous Protection</strong> check box to enable data protection through snapshots and configure the frequency at which snapshots are made. By default, the <strong>Continuous Protection</strong> check box is selected. For more information about snapshots, see Manage Snapshots for Shares and LUNs on page 177.</td>
</tr>
<tr>
<td>Smart Snapshot Management</td>
<td>Select the <strong>Smart Snapshot Management</strong> check box to enable automatic snapshot pruning. When enabled, the ReadyDATA deletes older snapshots so that hourly snapshots are kept for 48 hours, daily snapshots are kept for four weeks, weekly snapshots are kept for eight weeks, and monthly snapshots are kept indefinitely.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval specifies how often a snapshot is made. Make a selection from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hourly</strong>. A snapshot is taken every hour on the hour.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Daily</strong>. A snapshot is taken every day at midnight. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Weekly</strong>. A snapshot is taken every week on Friday at midnight.</td>
</tr>
<tr>
<td>LUN (SAN)</td>
<td>Click the <strong>LUN (SAN)</strong> button. (Clicking the <strong>Share (NAS)</strong> button creates a share; see Create a Share on page 77.)</td>
</tr>
</tbody>
</table>
5. Click the **Create** button.

The ReadyDATA confirms the creation of a LUN with the message “Data Set successfully created.” The new LUN is added to the Shares screen. Basic information is displayed to the right of the LUN.

## View and Change the Properties of a LUN, Including Size Expansion

- **To view and change the properties of a LUN:**
  1. Select **Shares**.
  2. Click the **Data Set** button (with four cubes).
      
      The Shares screen displays (see the following figure).
  3. Select the LUN that you want to explore by clicking it.
      
      The color of the LUN turns purple.
  4. Right-click the LUN.
      
      A pop-up menu displays:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Provision** | Select how storage space is provisioned. Make a selection from the drop-down list:  
  • **Thin**. Even though you specify the size of the LUN when you create it, storage space is assigned on demand instead of up front. The size of the LUN is reported as the total storage space that you specify when you create the LUN.  
  • **Thick**. All storage space that you specify when you create the LUN is also allocated up front. The size of the LUN is reported as the total storage space that you specify when you create the LUN, the default method.  
  
  **Note:** Make sure that you watch the volume capacity of the volume on which the over allocated LUN resides so you do not run out of storage space unexpectedly.  
  **Note:** NETGEAR recommends that you do not use an over allocated 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 screen.                                     |
| **Unit**   | Select the unit of measurement from the drop-down list:  
  • **MB**.  
  • **GB**, the default unit of measurement.  
  • **TB**.  |
| **Block size** | Select the block size from the drop-down list. 4 KB block size is the default when you create an NTFS on a server, but 64 KB is recommended. The block size for the NTFS must be equal or larger than the block size selected here. |
5. Select **Properties**.

The Properties pane for the selected LUN displays at the right of the screen (see the next figure).

---

**Note:** You can also use a shortcut to display the Properties pane of a LUN. Click the screen **Expand** button (.expand) on the top right of the screen to display the Properties pane (see the red oval on the top right of the previous figure). Click the same button (which now displays as a reversed arrow (contract)) again to hide the Properties pane.
6. Change the settings as explained in the following table. Click the flag button (✓) to save any changes in a field or drop-down list.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>The size is provided for information only. For information about how to expand the size of an existing LUN, see <em>Expand the Size of a LUN</em> on page 113.</td>
</tr>
<tr>
<td>Path</td>
<td>The path is provided for information only.</td>
</tr>
<tr>
<td>Properties</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name to identify the LUN. Do not include spaces in the name.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description to help identify the LUN.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Logbias         | Change the logbias setting by making a selection from the Logbias drop-down list:  
  - **Latency**. Data requests are handled at high priority with a minimum of delay, but data throughput might not be optimum, the default setting that is automatically assigned when you create a share.  
  - **Throughput**. Data requests are handled with high data throughput, but there might be delay in response to requests. |
| Sync Writes     | Change the setting by making a selection from the drop-down list:  
  - **Allowed**.  
  - **Forced**. Synchronous writes are required.  
  - **Disabled**. Synchronous writes are not used. |
| 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 more resources. |
| Dedupe          | Select the Dedupe check box to enable deduplication, which prevents storage of redundant data on the share. Unique data is stored only once on the share, and other instances of the identical data are removed and replaced by a pointer to the unique data. This storage method saves storage space and increases the speed of data transfers. By default, the Dedupe check box is cleared.  
  
  **Note:** You can enable deduplication for a thin LUN but not for a thick LUN.  
  
  **Note:** NETGEAR does not recommend enabling deduplication for performance-sensitive data on applications such as virtual machines and databases. |
| Provision       | Select **Convert** to change the provisioning, thick to thin, or thin to thick. When you select **Convert**, a confirmation screen opens. Click the **Yes** button, to confirm. |
| Size            | For information about how to expand the size of an existing LUN, see *Expand the Size of a LUN* on page 113. |
| Protection      | Select the Continuous Protection check box to enable data protection through snapshots and configure the frequency at which snapshots are made. By default, the Continuous Protection check box is selected. For more information about snapshots, see *Manage Snapshots for Shares and LUNs* on page 177.  
  
  **Note:** For shares or LUNs that were created before the release of this feature, Smart Snapshot Management is disabled by default. |
| Smart Snapshot Management | Select the Smart Snapshot Management check box to enable automatic snapshot pruning. When enabled, the ReadyDATA deletes older snapshots so that hourly snapshots are kept for 48 hours, daily snapshots are kept for four weeks, weekly snapshots are kept for eight weeks, and monthly snapshots are kept indefinitely.  
  
  **Note:** For shares or LUNs that were created before the release of this feature, Smart Snapshot Management is disabled by default. |
| Interval        | The interval specifies how often a snapshot is made. Make a selection from the drop-down list:  
  - **Hourly**. A snapshot is taken every hour on the hour.  
  - **Daily**. A snapshot is taken every day at midnight, the default setting.  
  - **Weekly**. A snapshot is taken every week on Friday at midnight. |
Note: The changes that you make on the Properties pane take effect immediately (that is, no Apply button exists to confirm the changes).

For information about how to set access right for a LUN, see Assign LUNs to LUN Groups and Manage Access Rights on page 121.

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 the users by removing the LUN from the LUN group to which the users have access (see Assign a LUN to a LUN Group on page 121).

➢ To expand the size of a LUN:

1. Select Shares.
2. Click the Data Set button (with four cubes, 
3. The Shares screen displays (see the following figure).
4. Select the LUN for which you want to expand the size.
5. The color of the LUN turns purple:

4. Right-click a share or LUN.
A pop-up menu displays:

5. Select **Expand**.

The Expand LUN pop-up screen displays:

6. Enter the following settings:
   - **New Size**. Specify the new size of the LUN. The maximum size that you can allocate to the 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 **Expand** button.

The new LUN size takes effect.

8. Add the LUN to the LUN group to which it belonged before the expansion.

   See **Assign a LUN to a LUN Group** on page 121.

User access to the LUN is restored.

---

**Note:** You can also expand a LUN from the Properties pane by clicking the **Expand size** link on the Properties pane.
Migrate a LUN to Another Volume

Migrating a LUN to another volume allows you to reorganize a volume or remove the LUNs from a volume before deleting the volume.

**WARNING:**

Migrating a LUN to another volume causes all users to be disconnected from the LUN.

**Note:** You cannot migrate a cloned LUN to a volume that does not contain its parent. For more information about clones, see *Clone a Snapshot* on page 186.

- To migrate a LUN to another volume:
  1. Select Shares.
  2. Click the Data Set button (with four cubes, 🎯). The Shares screen displays (see the following figure).
  3. Select a LUN by clicking it. The color of the LUN turns purple:
4. Right-click the share.
   A pop-up menu displays (see the following figure).

5. Select **Migrate To**.
   A second pop-up screen displays the volumes:

   ![Migrate To pop-up menu](image)

   By default, the volume on which the share resides is flagged.

6. Select the name of the destination volume.
7. Confirm the migration.
   A progress circle (○) displays the progress of the migration.

### Export a LUN to a NAS

Exporting a LUN to a network-attached server and then importing it allows you to easily and more quickly transfer a share by transporting the server or associated media to another location. You can use the exported LUN to seed replication between distant sites, and to more quickly and simply resume in a disaster recovery scenario.

The export bundles all of the data from the LUN, including all snap shots, into a single file on the NFS server.

- **To export a LUN to another volume:**
  1. Select **Shares**.
  2. Click the **Data Set** button (with four cubes, ![Data Set button](image)).
     The Shares screen displays.
  3. Select a LUN by clicking it.
     The color of the LUN turns purple:
4. Right-click the share.  
   A pop-up menu displays.

![Pop-up menu displaying export options](image)

5. Select Export to NAS.  
   A pop-up screen displays:

![Export Share/LUN over NFS](image)

6. Enter the appropriate values for the destination.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Server Address</td>
<td>Enter the address of the NFS server.</td>
</tr>
<tr>
<td>Force UDP transfer</td>
<td>Check to require that only UDP transfers are used. This is the default.</td>
</tr>
</tbody>
</table>
7. Confirm the export.
   The ReadyDATA sends an alert email when the export finishes.

**Import a ReadyDATA LUN**

If you have exported a LUN to a network attached server, you can import the LUN to the ReadyDATA. For large data sets, exporting a LUN, moving the NAS (or media with the exported file) to the same LAN as the destination ReadyDATA, and then importing is much quicker than replicating the LUN over a WAN. Use this process for seeding replication from a share to a remote LUN, and for speeding disaster recovery.

➢ **To import a LUN from another volume:**

1. Select **Shares**.
2. Click the **Data Set** button (with four cubes, ![cubes]).
   The LUN screen displays (see the following figure).
3. Click the **Import Share/LUN from NFS** icon next to the destination volume.

![Import Share/LUN from NFS Screen](image)

The Import Share/LUN from NFS Server screen opens.
4. Enter the appropriate values for the source.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Server Address</td>
<td>Enter the address of the NFS server.</td>
</tr>
<tr>
<td>Force UDP transfer</td>
<td>Check to require only UDP transfers are used. This is the default</td>
</tr>
<tr>
<td>NFS Path</td>
<td>Enter the path to the directory for the file containing the exported share.</td>
</tr>
<tr>
<td>File Name</td>
<td>Enter the file name for the exported share.</td>
</tr>
</tbody>
</table>

5. Confirm the import. The ReadyDATA sends an alert email when the import finishes.

Delete a LUN

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

*Note:* You cannot delete a LUN that is the parent of a clone. To delete the parent LUN, you must first delete all of its clones. For more information about clones, see *Clone a Snapshot* on page 186.

- **To delete a LUN from a volume:**
  1. Select **Shares**.
  2. Click the **Data Set** button (with four cubes). The Shares screen displays (see the following figure).
3. Select a LUN by clicking it.
   The color of the LUN turns purple:

![LUN Selection Diagram]

4. Click the – button (red) to the right of the LUN.
   A pop-up screen displays.

![Destroy Data Set Dialog]

5. Confirm the deletion by typing **DESTROY** in the field.
6. Click the **Destroy** button.
   The LUN is deleted.
Assign LUNs to LUN Groups and Manage Access Rights

This section discusses the following topics:

- Assign a LUN to a LUN Group
- Remove a LUN from a LUN Group
- Remove a LUN Group
- Manage Access Rights for LUN Groups

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 and apply to LUN groups, not to individual LUNs. However, you can easily assign a LUN to a LUN group, or move a LUN from one LUN group to another LUN group.

Each LUN group has an iSCSI target address (for example, iqn.1994-11.com.netgear:f2f2fdd4) that allows iSCSI clients to access the LUN group. For more information, see Access a Share from Network-Attached Device on page 127.

Assign a LUN to a LUN Group

➢ To create a LUN group and assign a LUN to it:

1. Select SAN.

   The SAN screen displays the LUNs that you have created (see Create a LUN on page 107):

   ![Unassigned LUNs]

   When you create a LUN, the LUN is unassigned. You need to create a LUN group and assign one or more LUNs to the LUN group.

2. To create a LUN group, click the + button in the upper right of the screen.
The New LUN Group pop-up screen displays:

3. In the **Name** field, enter a name for the LUN group.
   The default name is groupX, in which X is a number in sequential and ascending order.
   The **Target** field is automatically populated. The target is the string that an iSCSI client needs to be able to connect to the LUN.

4. Click the **Create** button.
   The New LUN group is added to the SAN screen (see the following figure). By default, CHAP is disabled and no client is allowed to access the LUN group (for more information, see *Manage Access Rights for LUN Groups* on page 124).

5. To assign a LUN to the newly created LUN group, click the + button (➕) to the right of an unassigned LUN.
   The Assign to pop-up menu displays.

6. Select **Assign to** (or point to **Assign to**), and select a LUN group from the submenu:

The LUN is now assigned to the selected LUN group:
Remove a LUN from a LUN Group

To remove a LUN from a LUN group:

1. Select SAN.

   The SAN screen displays:

   ![SAN screen with Unassigned LUNs]

2. Click the – button ( ) to the right of the LUN.

3. Confirm the LUN exclusion from the group.

   The LUN is returned to the unassigned state.
Remove a LUN Group

**Note:** You cannot remove a LUN group that has a LUN assigned to it. You must first remove the LUN from the LUN group.

➢ To remove a LUN group:

1. Select SAN.
   
The SAN screen displays:

2. Click the gear icon to the right of the LUN group.
   
   A pop-up menu displays:

3. Select Remove.

4. Confirm the removal.

Manage Access Rights for LUN Groups

➢ To configure client access to a LUN group:

1. Select SAN.
2. Click the gear icon to the right of the LUN group.
A pop-up menu displays:

3. Select **Properties**.
The LUN Group Properties pop-up screen displays (the following figure shows examples):
4. Configure the properties as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name is provided for information only and cannot be changed.</td>
</tr>
<tr>
<td>Target</td>
<td>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 by clicking the cross at the right of the field and then replace the content with a custom target address.</td>
</tr>
<tr>
<td>Require initiators to identify themselves using CHAP</td>
<td>By default, access to the LUN group is open to the initiators that you add to the table onscreen. Select this check box to enable CHAP authentication, and to allow only authenticated initiators access to the LUN group.</td>
</tr>
<tr>
<td>Allowed Initiators</td>
<td>Select one of the following radio buttons:</td>
</tr>
<tr>
<td></td>
<td>• Any. Access to the LUN group is granted to all initiators that have information about the target address. (If CHAP authentication is enabled, access is dependent on CHAP authentication.)</td>
</tr>
<tr>
<td></td>
<td>• Selected. Access to the LUN group is granted to iSCSI qualified names (IQNs) only. (If CHAP authentication is enabled, access is dependent on CHAP authentication.)</td>
</tr>
</tbody>
</table>

To add an IQN to the table and allow access to the LUN group:

1. Click the + button above and on the right of the empty table of initiators. The Create initiator pop-up screen displays:
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 131.

### Access a Share from Network-Attached Device

This section discusses the following topics:

- *Use a Windows Device*
- *Use a Mac OS X Device*
- *Use a Linux or Unix Device*

Users access shares and snapshots on the ReadyDATA from their network-attached devices, using the SMB, AFP, NFS, or FTP file-sharing protocol, depending on their device, the file-sharing protocols that you enabled for share access (see *Create a Share* on page 77), and the access rights that you granted (see *Set Up Access Rights to Shares* on page 90).
Users can employ any backup application to back up local data from their network-attached device to a share on the ReadyDATA.

**Note:** For snapshots to be accessible to users from their network-attached devices, you need to select the **Allow snapshot access** check box in the Protection section of the Properties pane of a share. For more information, see *View and Change the Properties of a Share* on page 80.

## Use a Windows Device

Users can access shares on the ReadyDATA using a network-attached Windows-based device.

- **To access an SMB share using a network-attached Windows device:**
  1. In the Windows Explorer address bar, enter the IP address or host name of the ReadyDATA:

     ![Network Address Bar](image)

     You are prompted to log in to the ReadyDATA:

     ![Windows Security Prompt](image)

     2. Enter a user name and password.

        Windows Explorer displays the contents of all available shares on the ReadyDATA:
Use a Mac OS X Device

Users can access shares on the ReadyDATA using a network-attached OS X device.

➢ To access an AFP or SMB share using a network-attached OS X device:

1. In Finder, select Go > Connect to Server.

   The Connect to Server screen displays.

2. Connect to the ReadyDATA using either AFP or SMB:
   - **AFP.** Enter either one of the following commands in the *Server Address* field:
     
     ```
     afp://<ip address>
     
     or
     
     afp://<host name>
     ```
   - **SMB.** Enter either one of the following commands in the *Server Address* field:
     
     ```
     smb://<ip address>
     
     or
     
     smb://<host name>
     ```

   *<ip address>* is the IP address of the ReadyDATA.

   *<host_name>* is the host name of the ReadyDATA.

3. Click the Connect button.

   You are prompted to log in to your ReadyDATA.

4. Enter a user name and password.

   You are prompted to select a volume.

   **Note:** Mac OS X calls ReadyDATA shares volumes.
5. Select a volume or volumes (that is, share or shares on the ReadyDATA).
6. Click the **OK** button.

Finder displays the contents of the share or shares in a window.

**Use a Linux or Unix Device**

You can access shares on the ReadyDATA using a network-attached Linux or Unix device that supports the SMB or NFS file-sharing protocol.

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

Using a terminal program, enter the following command:

```
mount [-t smb -o username=<user name>,password=<password>] //<ReadyDATA IP address>/<share name> <mount point>
```

Where:
- `<user name>` and `<password>` match the user name and password on the ReadyDATA.
- `<ReadyDATA IP address>` is the IP address of the ReadyDATA.
- `<share name>` is the name of the share that you want to access.
- `<mount point>` is the name of an empty folder on the Linux or Unix device.

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

Using a terminal program, enter the following command:

```
mount [-t nfs -o username=<user name>,password=<password>] //<ReadyDATA IP address>/<volume name>/<share name> <mount point>
```

Where:
- `<user name>` and `<password>` match the user name and password on the ReadyDATA.
- `<ReadyDATA IP address>` is the IP address of the ReadyDATA.
Managing Shares and LUNs

ReadyDATA OS 1.4

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

**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 ReadyDATA) present themselves on the client system as virtual block devices and can be treated as locally attached disks. Windows, for example, can run FAT32 or NTFS on the iSCSI target device and treat the devices as though they are locally attached.

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

---

**Note:** Unlike snapshots that reside on a share, snapshots that reside on a LUN are not visible to users. For information about how to recover data using a snapshot on a LUN, see *Recover Data from a Snapshot to an iSCSI-Attached Device* on page 193.
Access LUN Groups Using Microsoft iSCSI Software Initiator

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

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

➢ To configure LUN access through an iSCSI initiator:
   1. Open the iSCSI initiator and click the **Configuration** tab.
   2. Copy the default name from the **Initiator Name** field. You need the name in a later step.
   3. On the ReadyDATA Dashboard, select **SAN**.
The SAN screen displays:

4. Click the gear icon to the right of the LUN group to which you want to connect the server. A pop-up menu displays.
5. Select **Properties**.

   The LUN Group Properties pop-up screen displays:

6. Next to Allowed Initiators, select the **Selected** radio button.
7. Click the + button on the right above the empty table of initiators.
The Create initiator pop-up screen displays:

8. Paste the default iSCSI initiator name in the **Name** field.

9. Click the **Create** button.

The LUN Group Properties pop-up screen displays again and the initiator is added to the table on the LUN Group Properties pop-up screen.

10. On the LUN Group Properties screen, next to the iSCSI initiator name, select the **Allowed** check box:

11. Click the **Apply** button.
12. On the iSCSI Initiator Properties screen, click the **Targets** tab:

![iSCSI Initiator Properties](image)

13. In the **Target** field, enter the IP address of the ReadyDATA.

14. Click the **Quick Connect** button.

The server connects to the LUN group on the ReadyDATA, but the LUNs in the LUN group cannot yet be displayed in Windows Explorer.

15. Open the Windows Disk Management application.

Each LUN in the LUN group displays as an unallocated disk that needs to be initialized and formatted.

**Tip:** If the disks do not display from the Disk Management menu, select *Action > Refresh.*
16. Initialize each new disk by selecting **Action > All Tasks > Initialize Disk** from the Disk Management menu.

17. Format each new disk.
   a. Select the disk that you want to format:
   b. From the Disk Management menu, select **Action > All Tasks > New Simple Volume**.
The New Simple Volume Wizard pop-up screen displays.

c. Follow the default wizard formatting steps.

Alternately, you can give the volume label for the new disk that represents the LUN the same name as the LUN.

The LUNs are now accessible as hard disk drives (referred to as new volumes if you kept the default volume label) through Windows Explorer.
The following figure shows three LUNs: New Volume (F:), New Volume (H:), and Marketing (I):
Manage User Groups and User Accounts

This chapter describes how to configure the global security access mode and how to create and manage user accounts. It contains the following sections:

- About Security, User Groups, and Users
- Configure the Global Security Access Mode
- Manage User Groups for the Local Database
- Manage User Accounts for the Local Database

Note: Without at least one volume, changes are not saved after you reload the ReadyDATA. Make sure that you create a volume before you configure users groups and users accounts. For information about how to configure volumes, see Chapter 2, Manage Disks and Volumes.
About Security, User Groups, and Users

The security settings determine which users can access a share, and if they have read-only or read/write access to the share. However, before you can set security settings at the share level, you must first configure the global security settings that determine whether the ReadyDATA uses its local user database or an Active Directory.

**Note:** Access to LUNs is not regulated by the local user database or an Active Directory. For information about LUN access options, see Assign LUNs to LUN Groups and Manage Access Rights on page 121.

The local database lets you manage up to 60,000 users and up to 60,000 user groups. You must create and maintain the user groups and accounts on the ReadyDATA. A ReadyDATA in an Active Directory environment can serve up to 65,535 users. Accounts for these users are created and maintained in the Active Directory, and are pulled into the ReadyDATA.

Configure the Global Security Access Mode

The ReadyDATA lets you use its local user database or an Active Directory for authentication of user and group access to shares. You configure either one or the other:

- **Local user database.**
  The local user database lets you create user groups and accounts on the ReadyDATA. You set access rights to shares at the share level (see Set Up Access Rights to Shares on page 90). NETGEAR recommends that you first create user groups, and then create user accounts, so you can assign users to groups.

- **Active Directory.**
  If your network includes a centralized Windows-based Active Directory server, this option is available to you. The ReadyDATA forms a trusted relationship with the Active Directory server and allows all user authentications to occur there. Users and groups are displayed in the Access section of the Properties pane on the Shares screen. You set access rights to shares at the share level (see Set Up Access Rights to Shares on page 90).

➢ To configure the local user database settings:

2. From the Access type drop-down list, select Local users.

   Except for the Workgroup Name field, all fields are dimmed. The following figure shows only the upper part of the Settings screen with the local database settings:
3. (Optional) Enter a name for the workgroup.
   You can keep the default name of VOLUME.

4. Click the Apply button.

To configure the Active Directory settings:

2. From the Access type drop-down list, select Active Directory.

The name of the Workgroup Name field changes to NetBIOS Domain Name, and all fields become available. The following figure shows only the upper part of the Settings screen with the Active Directory settings:
3. Configure the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBIOS Domain Name</td>
<td>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. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>DNS Realm Name</td>
<td>Enter the DNS realm name, which is normally the DNS domain name or the Active Directory domain name, for example, company.community.com. In this example, company is the prefix, and community is the suffix of the name.</td>
</tr>
<tr>
<td>Include trusted domains</td>
<td>Select this check box to enable the ReadyDATA to automatically include the users of domains that have a trust relationship with the primary domain. <strong>Note:</strong> If the total number of users does not exceed 65,535, including trusted domains does not affect the responsiveness of the Dashboard.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>Specify the location of the computer account of the ReadyDATA in the Active Directory. By default, the computer account for the ReadyDATA is placed in the \users organizational unit (OU), but you can use the Organizational Unit field to specify another OU. <strong>Note:</strong> The name of the computer account (also referred to as machine account) is the same as the host name of the ReadyDATA (see Configure the Host Name on page 52).</td>
</tr>
<tr>
<td>Administrator Name</td>
<td>Enter the name of the administrator of the Active Directory.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Enter the password of the administrator of the Active Directory.</td>
</tr>
<tr>
<td>Server address</td>
<td>Enter the IP address of the Active Directory server.</td>
</tr>
</tbody>
</table>

4. Click the **Apply** button.

To refresh the user accounts from the Active Directory server, click **Refresh ADS accounts** label.

**Manage User Groups for the Local Database**

This section discusses the following topics:

- Create a User Group
- Delete a User Group
- Edit a User Group

Management of user groups applies to the local user database only. If you select an Active Directory, groups are pulled into the ReadyDATA from the Active Directory server.
Create a User Group

➢ To create a user group:


   The Security screen displays (see the following figure).

2. Click the Groups button.

   The following figure shows some examples. If you have not yet created any groups, only
   the default group with the name users and group ID (GID) 100 displays.

   ![Security Screen](image)

3. At the top right of the screen, click the New Group button ( ).

   The New Group pop-up screen displays:

   ![New Group Screen](image)

4. Configure the following settings:
   • GID. Either leave the assignment of the group ID (GID) as Automatic, or enter a
     custom GID. If you leave automatic assignment, GIDs are assigned in increments
     of 2, starting with 102. That is, GIDs are assigned as 102, 104, 106, and so on.
   • Name. Enter a name to identify the group.

5. Click the Create button.

   The group is added to the table on the Security screen.
Delete a User Group

When you delete a user group that is the primary group for a user, the user is no longer assigned to any group. You need to edit the user account and assign the user to another primary group.

➢ To delete a user group:

   
The Security screen displays (see the following figure).

2. Click the Groups button.
   
The groups display:

3. Highlight the row of the group that you want to delete, or select the group’s check box.
   
If your system has many groups, you can use the search field on the left above the table.

4. At the top right of the screen, click the Remove Group button ( ).

5. Confirm the deletion.

Edit a User Group

➢ To edit a user group:

   
The Security screen displays (see the following figure).

2. Click the Groups button.
   
The groups display:
3. Highlight the row of the group that you want to edit, or select the group’s check box. If your system has many groups, you can use the search field on the left above the table.

4. At the top right of the screen, click the screen Expand button ( ). The Group details pane displays. (The following figure contains examples of groups and users.)

5. Make changes as required, using the following guidelines:
   • You can change the name that identifies the group in the Name field.
   • You cannot change the GID.
   • You can add one or more members to the group by selecting the check box that is associated with each member. The check boxes for members for which the group is the primary group are dimmed (for more information, see Create a User Account on page 146).
6. Click the **Apply** button.

7. Click the screen **Expand** button (which now shows as a reversed arrow) again.

   The **Group** details pane is hidden.

---

**Note:** The members column in the previous screen shows only the users that you manually added to the group as explained in Step 5. Members for which the group is the primary group are not shown in the members column.

---

**Manage User Accounts for the Local Database**

This section discusses the following topics:

- *Create a User Account*
- *Delete a User Account*
- *Edit a User Account*

Except for administrative accounts, management of user accounts applies to the local user database only. If you select an Active Directory, user accounts are pulled into the ReadyDATA from the Active Directory server.

**Tip:** NETGEAR recommends that you first create groups, then set new user account preferences, and then create user accounts, so you can assign users to groups.

**Create a User Account**

You can create up to 65,535 user accounts on the ReadyDATA.

➢ **To create a user account:**

1. Select **Security**.

   Make sure that the **Users** button is highlighted (it is by default; if it is not, click the **Users** button). The Security screen displays. If you have not yet created any user accounts, none are shown, that is, no default user accounts exist.
2. Click the **New User** button (tıp). The New User pop-up screen displays:

3. Configure the settings as explained in the following table. With exception of the **Email Address** field, all fields are required.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the user. User names can have a maximum of 31 characters in most non-Asian languages. If you use Asian language characters, the limit is lower. You can use most alphanumeric and punctuation characters for a user name.</td>
</tr>
<tr>
<td>UID</td>
<td>Either leave the assignment of the user ID (UID) as <strong>Automatic</strong>, or enter a custom UID. If you leave automatic assignment, UIDs are assigned in increments of 1, starting with 100. That is, UIDs are assigned as 100, 101, 102, and so on.</td>
</tr>
</tbody>
</table>
4. Click the **Create** button.

The user is added to the table on the Security screen.

---

**Note:** On the Security screen, users are sorted by user name. You cannot change the sort order.

### Delete a User Account

**WARNING:**

Files on the ReadyDATA that are owned by a user for which you delete the user account might become inaccessible. When you delete a user account, the ReadyDATA deletes the associated home share and its contents.

➢ To delete a user account:

1. Select **Security**.

The Security screen displays. Make sure that the **Users** button is highlighted (it is by default; if it is not, click the **Users** button).
2. Highlight the row of the user account that you want to delete, or select the user account’s check box.

   If your system has many user accounts, you can use the search field on the left above the table.

3. At the top right of the screen, click the **Remove User Account** button (.erase).

4. Confirm the deletion.

**Edit a User Account**

➢ **To edit a user account:**

1. Select **Security**.

   The Security screen displays. Make sure that the **Users** button is highlighted (it is by default; if it is not, click the **Users** button).

2. Highlight the row of the user account that you want to edit, or select the user account’s check box.
If your system has many user accounts, you can use the search field on the left above the table.

3. At the top right of the screen, click the screen Expand button ( ).

The User account details pane displays. (The following figure contains an example.)

![User account details pane](image)

4. In the User account details pane, change the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the user. User names can have a maximum of 31 characters in most non-Asian languages. If you use Asian language characters, the limit is lower. You can use most alphanumeric and punctuation characters for a user name.</td>
</tr>
<tr>
<td>Primary Group</td>
<td>From the drop-down list, select the primary group to which the user is assigned. For information about creating groups, see Create a User Group on page 143. (Note: In addition to belonging to a single primary group, a user can belong to many other groups. You can assign more groups on the group detail pane (see Edit a User Group on page 144).)</td>
</tr>
<tr>
<td>Email Address</td>
<td>(Optional) Enter the email address of the user.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password. Each user password can have a maximum of 255 characters.</td>
</tr>
<tr>
<td>Re-enter Password</td>
<td>Reenter the user password.</td>
</tr>
</tbody>
</table>

Note: You cannot change the UID.

5. Click the Apply button.

6. Click the screen Expand button (which now shows as a reversed arrow ) again.

The User account details pane is hidden.
This chapter describes how to manage your ReadyDATA storage system’s configuration, network settings, add-ons, and USB storage devices. It contains the following sections:

- System Maintenance
- System Monitoring
- Optional Uninterruptible Power Supplies

**Note:** Without at least one volume, changes are not saved after you reload the ReadyDATA. Make sure that you create a volume before you update the firmware or configure system logs, SNMP monitoring, and optional uninterruptible power supplies. For information about how to configure volumes, see Chapter 2, Manage Disks and Volumes.

**Note:** For information about how to set up system alerts, see Configure System Alerts on page 50.
System Maintenance

This section discusses the following topics:

- Update the Firmware
- Reset the Firmware to Factory Defaults
- Shut Down or Restart the System
- Recover the Administrator Password

Update the Firmware

NETGEAR might periodically release firmware updates to improve the ReadyDATA. The firmware on the ReadyDATA is referred to as ReadyDATA OS. You can update the firmware on the ReadyDATA remotely from the NETGEAR website or manually from a local drive.

When you update the firmware, the stored data on the ReadyDATA is not affected. However, as a security measure, NETGEAR recommends that you back up the stored data, especially data that cannot be replaced, before you perform a firmware update.

WARNING:

You cannot update the firmware if there are no volumes on the ReadyDATA. To update the firmware, create at least one volume.

Update Firmware Remotely

If the ReadyDATA has an Internet connection, updating firmware remotely is the easiest method.

➢ To update firmware remotely:

1. Select System > Settings > Update.

The following figure shows the Settings screen with the firmware options:
2. Click the **Check for Updates** button.

The ReadyDATA contacts the NETGEAR update server:

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

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

3. If a firmware update is available, click the **Install Firmware** button.

A status bar on the left of the screen shows the progress of the firmware download. After the firmware download completes, you are prompted to reboot the system.

4. Click the **Reboot** button under the Update heading.

If you enabled email alerts, the ReadyDATA sends a message when the firmware update finishes.
5. You can verify that the ReadyDATA runs the new firmware by selecting **System > Overview > Hardware**.

The Dashboard home screen displays. The firmware version is listed in the **Firmware** field.

---

**Update Firmware Locally**

If the ReadyDATA is installed at a location that does not have Internet access, you need to update your firmware locally.

- **To update firmware locally:**
  1. Using a computer that has Internet access, download the latest firmware for the ReadyDATA from [http://downloadcenter.netgear.com/](http://downloadcenter.netgear.com/) to a USB drive or connected computer.
  2. Connect the USB drive with the updated firmware file to your ReadyDATA.
     
     For more information about the USB ports on the ReadyDATA, see the *ReadyDATA Hardware Manual*.
  3. Select **System > Settings > Update**.

    The following figure shows the Settings screen with the firmware options:
4. Click the **Install Firmware** button. The Update Firmware pop-up screen displays:

5. Click the **Browse** button, navigate to the file containing the updated firmware, and select it.
6. Click the **Upload** button.

A progress circle shows the progress of the firmware upload. After the firmware upload is complete, you are prompted to reboot the system.
7. Click the Reboot button under the Update heading.
   If you enabled email alerts, the ReadyDATA sends a message when the firmware update finishes.

8. You can verify that the ReadyDATA runs the new firmware by selecting System > Overview > Hardware.
   The Dashboard home screen displays. The firmware version is listed in the Firmware field.

Reset the Firmware to Factory Defaults

**WARNING:**
Resetting the ReadyDATA 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 ReadyDATA to factory defaults:

   1. Select System > Settings > Update.
      The following figure shows the Settings screen with the firmware options:
2. Click the **Perform Factory Default** button.

The Perform Factory Default pop-up screen displays:

3. Type **FACTORY** (all capital letters) in the field.
4. Click the **OK** button.

If you enabled email alerts, the ReadyDATA sends a message when the factory defaults are restored.
Shut Down or Restart the System

Use the **Power** icon that is accessible from any Dashboard screen to gracefully shut down or restart the ReadyDATA.

➢ **To gracefully shut down or restart the system:**

1. Click the **Power** icon in the upper right corner of the navigation bar:

2. Select one of the following options from the drop-down list:
   - **Shut down.** Gracefully power down the system.
   - **Restart.** Gracefully power down the system and restart it.

3. Confirm your selection.
   - If you enabled email alerts, the ReadyDATA sends a message after it restarts.

Recover the Administrator Password

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

- **Use NETGEAR’s password recovery tool.** This web-based tool requires that you enable administrator password recovery on your ReadyDATA before you can use it. For more information, see *Set the Administrator Password* on page 49.

- **Perform an OS reinstall reboot.** This process reinstalls the firmware on the ReadyDATA and resets the administrator user name and password to factory defaults.

Recover the Administrator Password Using NETGEAR’s Password Recovery Tool

This procedure is an option *only* if you enabled password recovery by providing a password recovery question, answer, and email address as described in *Set the Administrator Password* on page 49. If you lost the password but did not enable administrator password recovery, see *Recover the Administrator Password Using an OS Reinstall Reboot* on page 159.

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

1. Go to https://<ReadyDATA_IP_address>/password_recovery.
   - `<ReadyDATA_IP_address>` is the IP address of the ReadyDATA.
   - The ReadyDATA Password Recovery screen displays:
2. Enter the email address and password recovery answer that you enabled on the ReadyDATA.

   See Set the Administrator Password on page 49.

3. Click the Recover button.

   NETGEAR resets the administrator password and sends an email message with the new password to the password recovery email address.

**Recover the Administrator Password Using an OS Reinstall Reboot**

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

For information about how to perform an OS reinstall reboot on the ReadyDATA, see the ReadyDATA Hardware Manual.

**System Monitoring**

This section discusses the following topics:

- **System Real-Time and Historical Monitoring**
- **System Health Information**
- **Disk Status and Health Information**
- **System Logs**
- **SNMP Monitoring**
- **Add and Monitor UPS Devices**

**System Real-Time and Historical Monitoring**

The ReadyDATA provides status graphics for volume throughput, network throughput, cache usage and effectiveness (ZFS ARC), volume utilization, and system temperatures.
To display and configure the system status graphics, select System > Overview:
The Dashboard home screen displays. The status monitoring graphics are located below the Hardware section (if a graphic does not display, click the associated heading on the left of the screen).

- **Volume.**

![Dashboard home screen](image)

The Volume throughput graphic shows either the number of read and write operations per second or the bandwidth consumed per second:

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

- **Bandwidth.** The range is flexible and depends on your selections from the drop-down lists above the graphic. For example, the range can be from 0 to 4 Mbps. The upper part of the graphic indicates the bandwidth consumed for read operations (indicated by positive numbers); the lower part of the graphic indicates the bandwidth consumed for write operations (indicated by negative numbers).

From the drop-down lists above the graphic, you can adjust the following settings:

- **Volume.** Select all volumes or individual volumes.
- **Operations.** 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 five minutes to one year.
- **Update.** Select how often the information in the graphic is updated. You can select from 5 to 50 seconds.

- **Network.**

![Network Throughput Graph](image)

The Network throughput table shows the network usage for Tx and Rx traffic in bytes per second. The range is flexible and depends on your selections from the drop-down lists above the graphic. For example, the range can be from 0 to 60 bytes or from 0 to 40 KB. The upper part of the graphic indicates the Rx traffic; the lower part of the graphic indicates the Tx traffic.

From the drop-down lists above the graphic, you can adjust the following settings:

- **Network.** Select all network interfaces, individual interfaces, individual VNICs, or individual aggregation links.

- **Protocol.** Select all protocols or individual protocols (SMB, NFS, AFP, HTTP, SSH, iSCSI, or SNMP).

- **Period.** Select the period over which the network usage is measured. You can select from five minutes to one year.

- **Update.** Select how often the information in the table is updated. You can select from 5 to 50 seconds.

- **ZFS ARC (Cache)**

![ZFS ARC Graph](image)

The ZFS ARC table and graph shows various metrics for the cache such as hits, misses, l2 hits, and l2 misses. The **ZFS ARC** drop-down list (at the top of the graph) selects from
several cache effectiveness measures. You can also adjust the time range displayed (Period), and the frequency of updates.

• **Utilization.**

![Utilization Graph]

The Volume utilization graphic shows the percentage that an individual volume or all volumes are used. The range is from 0 to 100 percent.

From the drop-down lists above the graphic, you can adjust the following settings:

- **Volume.** Select all volumes or individual volumes.
- **Period.** Select the period over which the utilization is measured. You can select from five minutes to one year.
- **Update.** Select how often the information in the table is updated. You can select from 5 to 50 seconds.

• **Temperature.**

![Temperature Graph]

The Temperature graphic shows the system temperatures in degrees Celsius. The range is flexible and depends on your selections from the drop-down lists above the graphic and the temperatures that are measured. For example, the range can be from 0 to 50 degrees Celsius.

From the drop-down lists above the graphic, you can adjust the following settings:

- **Temperature.** Select all temperatures, the system (SYS) temperature, the CPU temperature, or the auxiliary (AUX) temperature.
- **Period.** Select the period over which the temperatures are measured. You can select from five minutes to one year.
- **Update.** Select how often the information in the table is updated. You can select from 5 to 50 seconds.

**System Health Information**

The ReadyDATA provides basic system health information about the fans, temperatures, power supplies, and optional UPS on the internal enclosure and optional expansion disk arrays.

➢ **To view system health information:**

Select **System > Info > Health.**

The following figure shows only the Health section on the Info screen. The messages are self-explanatory.

---

**Disk Status and Health Information**

The ReadyDATA provides disk status and health information for each disk that is installed in its enclosure and expansion units.

➢ **To view disk status and health information for an individual disk:**

1. Select **System > Storage.**

The Storage screen displays:
2. Point to a disk in the graphical enclosure.

Disk status and health information displays in a pop-up screen:

Most fields are self-explanatory. The following fields, however, require some explanation:

- **Volume State.** NEW, ACTIVE, EXPORTED, or DESTROYED.
- **Disk State.** AVAIL (available), ONLINE, OFFLINE, UNKNOWN, or FAULTED.
- **Channel.** The slot in which the disk is installed. (On the ReadyDATA, slots are numbered in sequential and ascending order from the bottom to the top of the enclosure, starting with 1 at the bottom left and ending with 12 at the top right.)
Note: If a disk fails, it is shown with a cross icon in the graphical enclosure (see Figure 2 on page 23, which does not include a failed disk).

System Logs

You can view system log messages onscreen, download the complete system logs to a local computer or USB drive, and receive system alerts. System logs provide information about the status of various system management tasks, including a time stamp. 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, or snapshot, or quota violations, or low disk space
- Addition and removal of hot-swappable disks
- Detection of disk types and hardware statistics
- Removal and addition of SAS-attached expansion enclosures
- Removal and addition of SSDs
- Removal and addition of power supplies
- Removal and addition of a UPS
- Connection and disconnection of external USB devices

In addition to a record in the system logs, the following events also generate alerts (see Configure System Alerts on page 50) and SNMP traps (see SNMP Monitoring on page 166) and are displayed onscreen:

- Disk errors and failures
- Changes in network connectivity
- Power supply failures
- UPS failures
- Fan speed irregularities and fan failures
- CPU and enclosure temperature violations

➢ To display and manage the system logs:

1. Select System > Info > Logs.
   The following figure shows only the Logs section on the Info screen:
2. Do any of the following:
   - **Download the logs.** Click the Download Logs button to download a zipped file with all log files to your browser's default download location. The default name of the zipped file is `System_log_<host name>.zip`, in which `<host name>` is the host name of the ReadyDATA (see *Configure the Host Name* on page 52).
   - **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 drop-down list, you can select to log individual categories only: System, Disk, Volume, Share, Account, or Miscellaneous.

3. To view more messages onscreen use the navigation box in the lower left of the screen.

**SNMP Monitoring**

Use SNMP management systems such as HP OpenView or CA UniCenter for remote monitoring of the ReadyDATA. (Management over SNMP is not supported.) For information about the types of messages that the ReadyDATA can send to SNMP hosts, see *System Logs* on page 165.

For information about how to configure SNMP and SNMP hosts, see *Configure SNMP* on page 71.
You can import the NETGEAR SNMP MIB to your SNMP client applications. This MIB is on the installation CD included with your unit. You can also download the MIB from http://support.netgear.com.

Optional Uninterruptible Power Supplies

This section discusses the following topics:

• About Uninterruptible Power Supplies
• UPS Configurations
• Add and Monitor UPS Devices

About Uninterruptible Power Supplies

NETGEAR recommends that you connect the ReadyDATA physically to one or more uninterruptible power supply (UPS) devices to protect against data loss due to power failures. Once connected, you can add up to three UPS devices to the Dashboard to enable the ReadyDATA to monitor and manage them. The ReadyDATA supports SNMP UPS devices and remote UPS devices.

If you enable email alerts, the ReadyDATA sends a message if a UPS status changes. For example, if a power failure forces a UPS into battery mode, or when a battery is low, you receive an email message.

When any UPS battery is low, or when a power failure occurs, the ReadyDATA automatically shuts down gracefully. In a configuration with an optional expansion disk array that is also connected to a UPS, before the ReadyDATA shuts down, it saves data to disks in the expansion disk array. However, the expansion disk array does not automatically shut down. If the batteries in the UPS to which the expansion disk array is connected become low, the expansion disk array shuts down ungracefully, but data has already been saved and is therefore safe.

Both the ReadyDATA and expansion disk arrays have dual power supplies. For full power protection, all power supplies should be connected to UPS devices.

UPS Configurations

The ReadyDATA supports UPS devices managed over SNMP and UPS devices managed over a remote connection.

UPS Devices Managed over SNMP

An SNMP UPS lets the ReadyDATA query the manufacturer-specific MIB. The ReadyDATA monitors and manages the UPS through SNMP. The Ethernet connection between the UPS and the ReadyDATA passes through a switch.
The following figures show scenarios that include a UPS that is managed over SNMP. Although dual power supplies and dual UPS devices are not shown in all figures, for full power protection, each power supply should be connected to a UPS.

Figure 8. ReadyDATA with a UPS managed over SNMP

Figure 9. ReadyDATA with dual UPS devices managed over SNMP
**Figure 10.** ReadyDATA and expansion disk array with a UPS managed over SNMP

**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 ReadyDATA monitors and manages the UPS over the remote connection. The Ethernet connection between the UPS and the ReadyDATA passes through a switch.

The following figures show scenarios that include a UPS that is managed over a remote connection. Although dual power supplies and dual UPS devices are not shown in these figures, for full power protection, each power supply should be connected to a UPS.
Figure 11. ReadyDATA with a UPS managed remotely over a Linux NUT server

Figure 12. ReadyDATA with a UPS managed remotely over a remote ReadyNAS
Add and Monitor UPS Devices

You can add up to three UPS devices to Dashboard.

➢ To add a UPS device to Dashboard and monitor the UPS device:

1. Select System > Settings > UPS.

   The following figure shows the UPS screen with one UPS device already added:

   ![UPS Screen with One Device Added]

   2. Click the + button (+) on the left above the UPS table.

   The Add UPS screen displays. The first figure shows the settings for adding an SNMP UPS; the second figure shows the settings for adding a remote UPS.

   ![Add UPS Screen]

   ```
   ![Add UPS Screen with SNMP UPS Settings]
   ```

   ```
   ![Add UPS Screen with Remote UPS Settings]
   ```
3. Configure the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name       | Enter a name to identify the UPS:  
- For an SNMP UPS, enter any name.  
- For a remote, UPS you do not have any options: You must enter UPS. |
| Description| An optional description to help identify the UPS. |
| Type       | From the drop-down list, select one of the following options:  
- **SNMP UPS**. An SNMP UPS lets the ReadyDATA query the manufacturer-specific MIB. The ReadyDATA 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 ReadyDATA monitors and manages the UPS over the remote connection. |
| Address    | Enter the IP address of the SNMP UPS. |
| Community  | Enter public or private, depending on the manufacturer’s requirement or the UPS’s configuration. |
| MIB        | From the drop-down list, select the MIB for one of the following manufacturers:  
- MGE UPS Systems  
- American Power Conversion (APC)  
- SOCOMEC  
- Powerware  
- Eaton Powerware (Monitored)  
- Eaton Powerware (Managed)  
- Raritan  
- BayTech  
- HP/Compaq AF401A  
- Cyberpower RMCARD201/RMCARD100/RMCARD202 |
4. Click the Add button.

The UPS device is added to the UPS table.

The following table explains the columns of the UPS table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Status** | The status of the UPS. The options are as follows:  
  • 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 to the UPS. |
| **Serial** | The detected serial number of the UPS. |
| **Model** | The detected model of the UPS. |
To edit a UPS device in the UPS table:

1. Select **System > Settings > UPS**.

   The following figure shows the UPS screen with one UPS device:

   ![UPS Screen](image)

2. In the UPS table, highlight the UPS device that you want to modify.

3. Click the gear icon to the right of the UPS table.

   The UPS Settings screen displays. The fields on this screen are identical to those on the Add UPS screen (see the figures in Step 2 of *To add a UPS device to Dashboard and monitor the UPS device*: on page 171).

4. Modify the settings as required.

   You cannot change the type settings.

5. Click **Apply**.

   The modified UPS settings are displayed in the UPS table.

To remove a UPS device from the UPS table:

1. Select **System > Settings > UPS**.

   The following figure shows the UPS screen with one UPS device:

   ![UPS Screen](image)
2. In the UPS table, highlight the UPS device that you want to remove.
3. Click the – button on the right above the table.
4. Confirm the removal.
   The UPS device is removed from the UPS table.
This chapter describes how to configure snapshots for backup and recovery and how to configure replication between two ReadyDATA storage systems. It contains the following sections:

- **Manage Snapshots for Shares and LUNs**
- **Recover Data from a ReadyDATA to an Attached Device**
- **Manage Replication and Recovery Between Two or More Systems**

**Note:** Without a volume, you cannot configure any shares or LUNs. Without shares or LUNs, you cannot configure any snapshots. For information about how to configure volumes, see *Chapter 2, Manage Disks and Volumes*. For information about how to configure shares and LUNs, see *Chapter 4, Manage Shares and LUNs*. 
Manage Snapshots for Shares and LUNs

This section discusses the following topics:

- Basic Snapshot Concepts
- Automatic and Manual Snapshots
- Importing Snapshots
- Roll Back to a Snapshot
- Clone a Snapshot
- Delete a Snapshot

Basic Snapshot Concepts

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

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

The ReadyDATA can automatically take snapshots of a 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.

If you configure both snapshots and continuous replication (see Manage Replication and Recovery Between Two or More Systems on page 194), you have continuous protection.

WARNING:

When the available storage space on a volume decreases below 200 GB, or the consumed space is greater than 75 percent of total capacity, the oldest automatic snapshots are automatically deleted to bring the available storage space back to 200 GB or higher and 25 percent available space or higher. Manual snapshots are never automatically deleted.

Once protection is available, the shares and LUNs on the Shares screen indicate the number of snapshots and the number of days with protection (a share with daily protection is shown on the left; a LUN with hourly protection is shown on the right):
Rolling Back

You can replace a folder or LUN with an earlier version by rolling back to a snapshot. When you roll back to a snapshot, the entire folder or LUN is replaced with the version captured by the snapshot. All snapshots that were taken after the snapshot that was used for rolling back are deleted. For information about how to roll back to a snapshot, see Roll Back to a Snapshot on page 183.

Clones

You can copy a snapshot to become a new independent data set (that is, a new share or LUN). Changes made to the clone do not affect the parent (“origin”) and changes made to the parent do not affect the clone. To handle storage in an efficient way, common blocks of data between the parent and the clone are shared. Because the clone is linked to the parent in this way, the parent cannot be deleted when a clone exists. Additionally, the clone cannot be migrated to a volume that does not contain the parent. For information about how to clone snapshots, see Clone a Snapshot on page 186.

Automatic and Manual Snapshots

You can configure the system to take snapshots according to a schedule that you specify or you can manually take snapshots.

Automatic Snapshots

When you create a share or LUN (or when you change the properties of a share or LUN), you can select continuous and automatic protection with hourly, daily, or weekly 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 Protection section of the Properties pane of a share. For more information, see View and Change the Properties of a Share on page 80.
• For information about configuring automatic snapshots of a share, see Create a Share on page 77.
• For information about configuring automatic snapshots of a LUN, see Create a LUN on page 107.

**Manually Take a Snapshot**

You can take a manual snapshot either from the Shares screen or from the Snapshot screen.

➢ **To take a snapshot of a share or LUN manually from the Shares screen:**

1. Select Shares.
2. Click the Data Set button (with four cubes).
   The Shares screen displays:

   3. Select the share or LUN for which you want to take a manual snapshot by clicking it.
   The color of the share or LUN turns purple.

4. Right-click a share or LUN.
   A pop-up menu displays. In the following figure, the share pop-up menu is shown on the left; the LUN pop-up menu is shown on the right.
5. Select **Take Snapshot**.
   
The New Snapshot pop-up screen displays:

6. Enter a name for the snapshot.
7. Click the **Create** button.
   
The snapshot is created.

➢ **To take a snapshot of a share or LUN manually from the Snapshot screen:**

1. Select **Shares**.
2. Click the **Snapshot** button (with a clock, ![clock icon]).
   
The Snapshot screen displays:
3. On the left side of the screen, select the share or LUN for which you want to take a manual snapshot by clicking it.

The color of the share or LUN turns purple.

4. Right-click a share or LUN.

5. Select **Take Snapshot**.

The New Snapshot pop-up screen displays:

6. Enter a name for the snapshot.

7. Click the **Create** button.

The snapshot is created.
Importing Snapshots

A volume can contain snapshots that are not listed in the snapshot timeline, for example after you import a share or LUN from a NAS. You can import these snapshots into the timeline using the Import Snapshots command.

➢ To import snapshots:

1. Select Shares.

2. Click the Data Set button (with four cubes, 🕰️ 🕰️ 🕰️ 🕰️).

   The Shares screen displays:

3. Select the share or LUN into which you want to import snapshots.

   The color of the share or LUN turns purple.

4. Right-click a share or LUN.

   A pop-up menu displays. In the following figure, the share pop-up menu is shown on the left; the LUN pop-up menu is shown on the right.
The message “Snapshots successfully imported,” shows in a new screen, when the import succeeds.

5. Click the **OK** button to close the message screen.

**Roll Back to a Snapshot**

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

**WARNING:**

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

➢ **To rollback a snapshot using the snapshot timeline:**

1. Select **Shares**.
2. Click the **Snapshot** button (with a clock, ![Clock Icon]).
   The Snapshot screen displays.
The shares and LUNs are displayed on the left of the screen.

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

Snapshots are displayed as marker icons along the timeline.

- The timeline centers on the zoom icon (🔍) as you zoom in and out. You can move the zoom icon by clicking anywhere along the timeline. Moving the zoom icon establishes a new center of focus when you zoom in and out.
• Adjust the vertical slider on the right of the timeline as needed. The + button zooms in, the – button zooms out.

[Diagram of a timeline with slider and arrow buttons]

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

[Diagram of a timeline with arrow buttons]

Note: The snapshot is not shown in the previous screen because it was not taken in the 2:00 AM–2:50 AM timespan.
**Tip:** Click the clock icon that is located in the middle of the Snapshot screen under the name of the selected share or LUN. A calendar pop-up screen displays, allowing you to jump to a desired month and date.

5. Right-click the snapshot that you want to roll back to.
6. From the pop-up menu that displays, select **Rollback**.

7. Confirm your decision by clicking the **Yes** button.

The share or LUN is rolled back to the snapshot that you selected.

---

**Clone a Snapshot**

You can copy a snapshot to become a new independent data set (that is, a new share or LUN). Changes made to the clone do not affect the parent (“origin”) and changes made to the parent do not affect the clone. To handle storage in an efficient way, common blocks of data between the parent and the clone are shared. Because the clone is linked to the parent in this way, the parent cannot be deleted when a clone exists. Additionally, the clone cannot be migrated to a volume that does not contain the parent.

➢ **To select and clone a snapshot using the snapshot timeline:**

1. Select **Shares**.

2. Click the **Snapshot** button (with a clock, ![Clock Icon](clock.png)).

   The Snapshot screen displays.
The shares and LUNs are displayed on the left of the screen.

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

Snapshots are displayed as purple marker icons along the timeline.

- The timeline centers on the zoom icon ( ) as you zoom in and out. You can move the zoom icon by clicking anywhere along the timeline. Moving the zoom icon establishes a new center of focus when you zoom in and out.
• Adjust the vertical slider on the right of the timeline as needed. The + button zooms in, the – button zooms out.

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

Note: The snapshot is not shown in the previous screen because it was not taken in the 2:00 AM–2:50 AM timespan.
Backup, Replication, and Recovery

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

5. Right-click the snapshot that you want to clone.
6. From the pop-up menu that displays, select **Clone**.

A pop-up screen displays:

7. In the **Name** field, enter a new name for the share or LUN.
8. Click the **Apply** button.

A cloned snapshot is added to the Shares screen as a new share or LUN. A new share is immediately accessible to users. A new LUN first must be added to a LUN group before users can gain access to it.

Delete a Snapshot

You can enable Smart Snapshot Management to automatically prune older snapshots and you can manually delete snapshots.

Smart Snapshot Management

When you create a share or LUN (or when you change the properties of a share or LUN), you can enable Smart Snapshot Management. Smart Snapshot Management provides an easy
way to reduce the total number of historical snapshots per share or LUN. When this feature is enabled, ReadyDATA automatically deletes older hourly and daily snapshots so that hourly snapshots are kept for 48 hours, daily snapshots are kept for four weeks, weekly snapshots are kept for eight weeks, and monthly snapshots are kept indefinitely.

For information about enabling Smart Snapshot Management for a share, see Create a Share on page 77.

For information about enabling Smart Snapshot Management for a LUN, see Create a LUN on page 107.

**Manually Delete a Snapshot**

You can manually delete snapshots from the Snapshots screen.

➢ **To manually delete a snapshot:**

1. Select Shares.

2. Click the Snapshot button (with a clock, ![clock icon]).

   The Snapshot screen displays.

   The shares and LUNs are displayed on the left of the screen.

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

Snapshots are displayed as purple marker icons along the timeline.

- The timeline centers on the zoom icon ( ), as you zoom in and out. You can move the zoom icon by clicking anywhere along the timeline. Moving the zoom icon establishes a new center of focus when you zoom in and out.
- Adjust the vertical slider on the right of the timeline as needed. The button zooms in, the button zooms out.

Note: The snapshot is not shown in the previous screen because it was not taken in the 2:00 AM–2:50 AM timespan.
**Tip:** Click the clock icon that is located in the middle of the Snapshot screen under the name of the selected share or LUN. A calendar pop-up screen displays, allowing you to jump to a desired month and date.

5. Right-click the snapshot that you want to delete.
6. From the pop-up menu that displays, select **Remove**.

A pop-up screen displays:

7. Confirm your decision by clicking the **Yes** button.
   The selected snapshot is deleted.
Recover Data from a ReadyDATA to an Attached Device

This section discusses the following topics:

- Recover Data from a Snapshot to a Network-Attached Device
- Recover Data from a Snapshot to an iSCSI-Attached Device
- Recover Data from a Snapshot to a Windows Server

Users can employ any back-up application to back up data from their network-attached device to a share or from their iSCSI-attached device to a LUN on the ReadyDATA, and simplify access the backed-up data on the share or LUN.

Users who do not back up their data can still be protected from data loss if you provide them access to data that is available in a snapshot on the ReadyDATA. Access to snapshots differs according to the type of attached device that a user employs.

Recover Data from a Snapshot to a Network-Attached Device

For snapshots to be accessible to users from their network-attached device, you must select the Allow snapshot access check box in the Protection section of the Properties pane of a share. For more information, see View and Change the Properties of a Share on page 80.

After you make snapshots available, users with a network-attached device have access to the snapshots that reside on a share on the ReadyDATA according to their access rights.

For those users with read/write access to the share, recovering data is a simple process: They click the snapshot subfolder in a share, and then have access to all snapshots that are available on that share. Users can explore the data that is available in a snapshot and recover any desired file or folder.

For information about how to access a share, see Access a Share from Network-Attached Device on page 127.

Recover Data from a Snapshot to an iSCSI-Attached Device

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

Cloning a snapshot to become a LUN is an instantaneous process that does not consume additional storage space, unless more data is written to the clone. Because no additional storage space is consumed, cloning snapshots is very efficient.

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 a Snapshot* on page 186. 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 121.

   The LUN clone appears on the iSCSI-attached device as a virtual block device. The iSCSI-attached device treats LUNs in the LUN group as locally attached disks. Now users can access the LUN clone from the iSCSI-attached device.

3. **Locate the snapshot data on the LUN clone from the iSCSI-attached device.**
   Users can access data on the LUN clone according to their access rights. Users who have read/write access to the LUNs in the LUN group can explore the snapshot data in the LUN clone and recover any desired data.

**Recover Data from a Snapshot to a Windows Server**

ReadyDATA snapshots for shares are accessible directly from Windows Server 2008 and Windows Server 2012 when SMB is used to connect the server to the ReadyDATA. You can view and select snapshots from the *Previous Versions* tab of a file’s Properties dialog. Note that there are some differences between using the ReadyDATA snapshots and a local Windows Server snapshot, such as: a Windows Restore does not delete the later snapshots on the ReadyDATA, access is over the network so performance might be slower than expected, a user with write permission can modify the actual snapshot.

**Manage Replication and Recovery Between Two or More Systems**

This section discusses the following topics:

- *About Replication*
- *Recover Replicated Data*
- *Seed or Reseed Replication*
- *Access ReadyDATA Replicate and Register Systems*
- *Schedule or Resume Periodic Replication Using ReadyDATA Replicate*
- *Configure or Resume Continuous Replication Using ReadyDATA Replicate*
- *View the Network Using ReadyDATA Replicate*
- *View the Jobs Using ReadyDATA Replicate*
- *Monitor the Jobs Using ReadyDATA Replicate*
- *Run Job Reports Using ReadyDATA Replicate*
- *Exchange Certificates for Local Replication*
- *Schedule Replication for Local Replication*
The ReadyDATA supports backup and recovery operations through its advanced snapshot functionality. For information about snapshots, see Manage Snapshots for Shares and LUNs on page 177. Replication is specifically between two ReadyDATA storage systems on which shares and LUN can be mirrored.

About Replication

Replication capabilities are integrated into the ReadyDATA, and you do not need to install a replication add-on. You can enable replication with the simple click of a button. You have the choice of managing replication locally or accessing the NETGEAR ReadyDATA Replicate™ software application so that you can use its centralized management console to configure the replication settings (see Access ReadyDATA Replicate and Register Systems on page 197).

ReadyDATA replication supports two types of replication:

- Periodic replication
  This type of replication is driven by the clock. Data is replicated periodically, from once per hour to once per month, based on how you schedule replication. This configuration collects changes that occur over the selected time period and replicates them in line with the replication schedule.

- Continuous replication
  This type of replication is driven by activity at the source system. Data is replicated to the destination device constantly. Whenever new blocks are written on the source system, they are immediately sent to the destination system. If a disaster occurs, the most current data possible is in a secondary location. For optimum protection, use continuous replication rather than periodic replication.

You can configure replication only per individual share or LUN, that is, you cannot configure replication at the system level. You select a share or LUN as the source of the replication, and a volume on the remote system as the destination for the replication.

The replication process leverages the information that is contained in special hidden snapshots to minimize the time it takes to determine what block-based data needs to be moved between the systems. These hidden snapshots are not the same as the regular snapshots that you create manually or set up to be created automatically.

Replication of an incomplete hidden snapshot resumes from the point where it failed, that is, if a 200 MB snapshot fails to replicate at 90 percent completion, replication resumes at 90 percent completion to replicate the remaining 20 MB.

If you use the ReadyDATA Replicate™ software application, you do not use an explicit destination IP address. Data that is replicated over the Internet is automatically encrypted for increased safety.

If you manage replication locally, you must establish the destination by using an IP address or domain name, and you must exchange access keys between both systems.
The replication status is reported at both the source and the destination systems in a replication relationship, and includes the age of the snapshot that is transferred and the size of the data that is transferred. For example, if a 50 MB snapshot was created 20 seconds before being transferred to a remote system as part of replication, the status that is reported is Target is 50 MB / 20 seconds behind source, or a similar status message.

For more information, see the white paper Building Backup-to-Disk and Disaster Recovery Solutions with the ReadyDATA 5200 that is available from the ReadyDATA website at www.netgear.com/readydata.

Recover Replicated Data

In a replication configuration, after data has been lost at the source system, or after the source system has been compromised, no special steps are required to recover data. If the configuration is one of continuous replication, the data on the destination is fully current. If the configuration is one of periodic replication, the data on the destination is current as of the last snapshot.

Once you have configured replication for each individual share and LUN on the source system, all data is available at the secondary location on the destination system. You only must provide users access to their share or LUN on the destination system.

After the source system has been repaired and brought back online, you have the option to configure reverse replication to replicate data from the destination system back to the source system. If a significant amount of data is on the original destination site, the first job after starting reverse replication can take a long time. You can substantially shorten this time by seeding the reverse replication. For information about seeding replication, see Seed or Reseed Replication on page 196.

Seed or Reseed Replication

When a share or LUN has a large amount of data and you want to replicate that data to another ReadyDATA, the initial replication job can take a significant amount of time because all of the data must be moved to the destination system. If the amount of data is large enough, and the connection between systems is slow, for example over a WAN, you can start up much more quickly by seeding the destination system with the complete, initial state of the source.

This speed-up can be especially valuable when you are reestablishing the original source during disaster recovery following the loss of the original source system.

➢ To seed replication:

1. Create the seed by exporting the source share or LUN.

   Use the appropriate procedure. See Export a Share to a NAS on page 85, or Export a LUN to a NAS on page 116.

2. Move the NAS with exported share or LUN to the same LAN as the destination system.

3. Import the share or LUN, using the appropriate procedure. See Import a ReadyDATA Share on page 87, or Import a ReadyDATA LUN on page 118.
Follow the appropriate procedure: Schedule or Resume Periodic Replication Using ReadyDATA Replicate on page 199, Configure or Resume Continuous Replication Using ReadyDATA Replicate on page 209, or Resume Local Replication on page 233.

Access ReadyDATA Replicate and Register Systems

NETGEAR ReadyDATA Replicate is an online application that provides a simplified, reliable replication solution to protect business data against downtime and disasters.

ReadyDATA Replicate allows data from one ReadyDATA to be replicated to and restored from another ReadyDATA. Using a centralized web portal, you create, manage, and monitor replication and restore tasks that operate across ReadyDATA systems from multiple locations.

The ReadyDATA provides replication functionality, that is, you do not need to install anything on the ReadyDATA for replication to function. However, you do need to create a ReadyDATA remote ID before you can access ReadyDATA Replicate.

---

**Note:** You do not need a license to access ReadyDATA Replicate.

---

➢ **To access ReadyDATA Replicate and register systems:**

   The access screen displays:

   ![Sign in with your NETGEAR ReadyDATA Replicate ID](image)

   2. (Optional) Click the **Join Now** link to create a remote ID and password, if you do not yet have them.

2. Sign in using your remote ID and password.

   The ReadyDATA Replicate Network screen displays:
On a ReadyDATA that you want to register for replication, open the Dashboard.

Select **System > Settings > Services**

The Services section with the file-sharing protocols on the Settings screen displays.

The following figure shows the top of the Settings screen only:

6. Click the **Replicate** button.

The Replicate settings pop-up screen displays:
7. Click the **Service** button.

8. Enter the following settings:
   - In the **Username** field, enter the remote ID that you used to access the ReadyDATA Replicate application in **Step 3**.
   - In the **Password** field, enter the password that you used to access the ReadyDATA Replicate application in **Step 3**.

9. Click the **Apply** button.

10. To register another ReadyDATA for replication, repeat **Step 4 to Step 9**.
    
    After you have registered one or more ReadyDATA systems, the systems display on the ReadyDATA Replicate Network screen.
    
    To display the Replicate Network screen, from the Views menu on the left, select **Network**.
    
    **Note:** For the ReadyDATA systems to be displayed, you might need to click the **Refresh** button in the upper right corner of the Replicate Network screen.

---

### Schedule or Resume Periodic Replication Using ReadyDATA Replicate

After you have registered at least two ReadyDATA systems for ReadyDATA Replicate, you can schedule the replication of a share or LUN from one ReadyDATA to another.
If a job is no longer running, for example because you stopped it, or because of a system loss, you can resume the job.

If the source share or LUN is large, the initial replication transfer takes a substantial amount of time, particularly if the source and destination ReadyDATAs are connected by a WAN. You can shorten this time by seeding the destination site. For information about seeding replication, see *Seed or Reseed Replication* on page 196.

➢ To schedule or resume periodic replication of a share or LUN:

   The access screen displays:

   ![Sign in with your NETGEAR ReadyDATA Replicate ID](image)

2. Sign in using your remote ID and password.
   The ReadyDATA Replicate Network screen displays:
3. From the Tools menu on the left, select **Scheduled Replicate**.

The first Scheduled Replicate screen displays:

4. Configure the settings on the first screen as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Keep the default name for the replication configuration, or overwrite the default name with another name.</td>
</tr>
</tbody>
</table>
5. At the bottom right of the screen, click the **Next** button.

The next Scheduled Replicate screen displays:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Source | From the Source drop-down list, select the ReadyDATA from which you want to replicate a share or LUN, that is, select the source system. Then do the following:  
1. Select the volume on which the share or LUN resides.  
2. Double-click the volume.  
3. Select the share or LUN. |
| Destination | Do one of the following:  
• To configure a new job, from the **Destination** drop-down list, select the ReadyDATA to which you want to replicate a share or LUN, that is, select the destination system. Then select the volume to which you want to replicate the share or LUN.  
• To resume an existing job, from the **Destination** drop-down list, select the ReadyDATA to which you want to replicate a share or LUN, that is, select the destination system. Double-click the volume containing the share or LUN assigned when the job was first configured, and then select the share or LUN.  
• To configure a new job, but use a seed, from the **Destination** drop-down list, select the ReadyDATA to which you want to replicate a share or LUN, that is, select the destination system. Double-click the volume containing the share or LUN containing the replication seed, and then select the share or LUN. |

**Note:** In the previous figure, the name of the volume to which the share or LUN is replicated is identical to the name of the volume from which the share or LUN is replicated. This is not a typical situation.
If you did not select a share or LUN (you are configuring a new job without a seed), the screen is similar to the following:
• If you selected a share or LUN (you are resuming a job, or seeding a new job), the next screen displays the snapshots on the share or LUN.

6. If you are configuring a new job without a seed, skip this step, otherwise select the snapshot to use as a base for replication and click the Next button.
The next Scheduled Replicate screen displays.

![Scheduled Replicate Screen](image)

7. (Optional) Configure the settings on the screen as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Share/LUN Name</td>
<td>Lists the name of the share or LUN selected earlier.</td>
</tr>
<tr>
<td>Advanced Settings for Data Transmission</td>
<td></td>
</tr>
<tr>
<td>Show Progress</td>
<td>Select the check box to view the progress of the data transfer.</td>
</tr>
<tr>
<td>Compression</td>
<td>Select the check box to enable data compression during the data transfer. Then configure the compression rate. By default, compression is disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After the data has been transferred, the data is not stored compressed unless it was already compressed on the source share or LUN.</td>
</tr>
<tr>
<td>Compression Level</td>
<td>Set the compression level by clicking the up or down arrows to increase or decrease the level. You can select from 1 through 9. For example, 5 indicates that data is compressed five times.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Select the check box to enable encryption. By default, encryption is disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> NETGEAR recommends that you encrypt sensitive data.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you do not use an explicit destination IP address, data that is replicated over the Internet is automatically encrypted for increased safety. When you select the <strong>Encryption</strong> check box, data that is replicated over the Internet is encrypted twice.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Deduplication         | Select the check box to enable deduplication during the data transfer. Deduplication prevents transfer of redundant data and increases the speed of the data transfer.  
  **Note:** After the data has been transferred, the data is not stored in a deduplicated format unless it was already deduplicated on the source share or LUN. |
| Use P2P Service       | Select the check box to enable point-to-point data transmission. This check box is selected by default. If P2P is not selected, data is transmitted to the ReadyDATA Replicate site from the source and then transmitted to the destination site. If the check box is selected, transmission is from the source to the destination without going through the ReadyDATA replicate site. |
| Explicit IP Address   | ReadyDATA Replicate automatically selects the physical Ethernet interfaces and VNICs for communication between the source and destination systems. If you want to use a specific interface on the destination system, you can specify its IP address.  
  To specify a specific interface, enter the IP address of the interface on the destination system. The address is automatically appended with port number 6819.  
  **Note:** You must set up port forwarding if the source and destination are behind a firewall.  
  **Note:** If you use an explicit destination IP address, data that is replicated over the Internet is not automatically encrypted. You must select the Encryption check box to enable encryption. |
| Explicit Domain Name  | ReadyDATA Replicate automatically selects the physical Ethernet interfaces and VNICs for communication between the source and destination systems. If, instead, you want to use a specific domain name for the destination system, you can specify it here. The name is automatically appended with port number 6819.  
  **Note:** You must set up port forwarding if the source and destination are behind a firewall.  
  **Note:** If you use an explicit destination domain name, data that is replicated over the Internet is not automatically encrypted. You must select the Encryption check box to enable encryption. |
| P2P FallBack          | Select the check box to enable use of transmission through the ReadyDATA Replicate site if communication problems with P2P transmission occur. |
8. At the bottom right of the screen, click the **Next** button.

The next Scheduled Replicate screen displays:

9. Configure the settings on the third screen as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective from</td>
<td>This field is for information only. It states the date as of which the replication schedule is effective.</td>
</tr>
<tr>
<td>Repeat</td>
<td>From the <strong>Repeat</strong> drop-down list, select how replication is repeated:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hourly</strong>. From the <strong>Starting at</strong> list, select the time within the hour.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Daily</strong>. From the <strong>Starting at</strong> list, select the hour and the time within the hour.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Every weekday</strong>. This option excludes Saturdays and Sundays. From the <strong>Starting at</strong> list, select the hour and the time within the hour.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Monthly</strong>. From the <strong>Starting at</strong> menu, select the hour and the time within the hour, and select the day of the month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Custom</strong>. Customize the replication pattern with hourly, daily, weekly, and monthly options. The screen adjusts according to the option that you select.</td>
</tr>
<tr>
<td>Starting at</td>
<td>From the <strong>Starting at</strong> list, select the time at which replication starts. The options depend on your selection from the <strong>Repeat</strong> drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• For the <strong>Hourly</strong> option, select on the quarter hour, on the half hour, or on the three quarters of an hour.</td>
</tr>
<tr>
<td></td>
<td>• For the <strong>Daily</strong>, <strong>Every weekday</strong>, and <strong>Monthly</strong> options, select on the quarter hour, on the half hour, or on the three quarters of an hour, from 1 through 23.</td>
</tr>
</tbody>
</table>

10. At the bottom right of the screen, click the **Next** button.
The final Scheduled Replicate screen displays:

This screen provides an overview of the configured replication schedule. If you want to change the schedule, click the **Back** button.

11. Click the **Apply** button.

The Jobs screen displays, showing the replication configuration:
Configure or Resume Continuous Replication Using ReadyDATA Replicate

**Note:** For full disaster recovery, configure continuous replication for each individual share and LUN.

After you have registered at least two ReadyDATA systems for ReadyDATA Replicate, you can schedule the replication of a share or LUN from one ReadyDATA to another. If a job is no longer running, for example because you stopped it, or because of a system loss, you can resume the job. If the source share or LUN is large, the initial replication transfer takes a substantial amount of time, particularly if the source and destination ReadyDATAs are connected by a WAN. You can shorten this time by seeding the destination site. For information about seeding replication, see *Seed or Reseed Replication* on page 236.

➢ To schedule or resume continuous replication of a share or LUN:

   
   The access screen displays:

   ![Sign in with your NETGEAR ReadyDATA Replicate ID](image)

2. Sign in using your remote ID and password.
   
   The ReadyDATA Replicate Network screen displays:
3. From the Tools menu on the left, select **Continuous Replicate**.

   The first Continuous Replicate screen displays:
4. Configure the settings on the first screen as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Keep the default name for the replication schedule, or overwrite the default name with another name.</td>
</tr>
<tr>
<td>Source</td>
<td>From the <strong>Source</strong> drop-down list, select the ReadyDATA from which you want to replicate a share or LUN, that is, select the source system. Then do one of the following: 1. Select the volume on which the share or LUN resides. 2. Double-click the volume. 3. Select the share or LUN.</td>
</tr>
</tbody>
</table>
| Destination | Do one of the following:  
|           | • To configure a new job, from the **Destination** drop-down list, select the ReadyDATA to which you want to replicate a share or LUN, that is, select the destination system. Then select the volume to which you want to replicate the share or LUN.  
|           | • To resume an existing job, from the **Destination** drop-down list, select the ReadyDATA to which you want to replicate a share or LUN, that is, select the destination system. Double-click the volume containing the share or LUN assigned when the job was first configured, and then select the share or LUN.  
|           | • To configure a new job, but use a seed, from the **Destination** drop-down list, select the ReadyDATA to which you want to replicate a share or LUN, that is, select the destination system. Double-click the volume containing the share or LUN containing the replication seed, and then select the share or LUN. |

**Note:** In the previous figure, the name of the volume to which the share or LUN is replicated is identical to the name of the volume from which the share or LUN is replicated. This is not a typical situation.

5. At the bottom right of the screen, click the **Next** button.

The next Continuous Replicate screen displays:
• If you did not select a share or LUN (you are configuring a new job without a seed), the screen is similar to the following:
• If you selected a share or LUN (you are resuming a job, or seeding a new job), the next screen displays the snapshots on the share or LUN
6. If you are configuring a new job without a seed, skip this step, otherwise select the snapshot to use as a base for replication and click **Next**.

The next Continuous Replicate screen displays:

![Scheduled Replicate]

7. Configure the settings on the screen as explained in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New data set name</td>
<td>Enter a name for the share or LUN on the destination system.</td>
</tr>
</tbody>
</table>
| Advanced Settings for Data Transmission | Select the check box to enable data compression during the data transfer. Then configure the compression rate. By default, compression is disabled.  
**Note:** After the data has been transferred, the data is not stored compressed unless it was already compressed on the source share or LUN.  
Compression Ratio | Select the compression rate by making a selection from the drop-down list. You can select from 1 through 10, and unlimited. For example, 5 indicates that data is compressed five times. |
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Select the check box to enable encryption. By default, encryption is disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> NETGEAR recommends that you encrypt sensitive data.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you do not use an explicit destination IP address, data that is replicated over the Internet is automatically encrypted for increased safety. When you select the Encryption check box, data that is replicated over the Internet is encrypted twice.</td>
</tr>
<tr>
<td>Deduplication</td>
<td>Select the check box to enable deduplication during the data transfer.</td>
</tr>
<tr>
<td></td>
<td>Deduplication prevents transfer of redundant data and increases the speed of the data transfer.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After the data has been transferred, the data is not stored in a deduplicated format unless it was already deduplicated on the source share or LUN.</td>
</tr>
<tr>
<td>Explicit Destination IP Address</td>
<td>ReadyDATA Replicate automatically selects the physical Ethernet interfaces and VNICs for communication between the source and destination systems. If you want to use a specific interface on the destination system, you must specify its IP address.</td>
</tr>
<tr>
<td></td>
<td>To specify a specific interface, select the check box to enable an explicit destination IP address. Then configure the IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must set up port forwarding if the source and destination are behind a firewall.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you use an explicit destination IP address, data that is replicated over the Internet is not automatically encrypted. You must select the Encryption check box to enable encryption.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the interface on the destination system. The address is automatically appended with port number 6819.</td>
</tr>
</tbody>
</table>
8. At the bottom right of the screen, click the **Next** button.

The final Continuous Replicate screen displays:

![Continuous Replicate Screen](image)

This screen provides an overview of the replication configuration. If you must change the schedule, click the **Back** button.

9. Click the **Apply** button.

The Jobs screen displays, showing the replication configurations:
View the Network Using ReadyDATA Replicate

The Network screen graphically displays all the systems that are registered for replication and their status.

➢ To view the Network screen:
   
   Click the Network label.
   
   The Network screen displays.
Double-click a system to display the host name and the volumes on the system. Double-click a volume to display the shares and LUNs on the volume.

The bottom panel of the Network screen displays the following information:

- Host name.
- ReadyDATA firmware version if the system is online. If the system is offline, *Offline* is stated.
- Device model.
- Free space on the device.
- Total size of all volumes on the device.
- Total space used on all volumes on the device.

To update the information onscreen click the **Refresh** icon.

**View the Jobs Using ReadyDATA Replicate**

The Jobs screen displays the configured replication jobs, and lets you disable, edit, and delete jobs.

➢ **To view the Jobs screen:**

Click the **Jobs** label.
The **Jobs** screen displays.

- **To disable a job:**
  1. Click the **Jobs** label.
  2. Click the red icon (the stop sign) to the left of the job.

- **To reenable a disabled job:**
  1. Click the **Jobs** label.
  2. Click the red icon.

- **To edit a job:**
  1. Click the **Jobs** label.
  2. Click the edit icon to the left of the job.
3. Each time you click **Next**, you see the next window in the job creation wizard. Most job parameters cannot be edited and are shown in gray.

4. To finish, click **Apply**.

- **To delete a job:**
  Click the blue icon (the X) to the left of the job.

- **To reorganize the table with jobs and group the jobs:**
  To the right of a column heading in the table, click the drop-down list.

  You can do the following:

  - Sort the jobs in ascending order.
  - Sort the jobs in descending order.
  - Add or remove columns from the table.

  **Note:** To update the information in the table Click the **Refresh** icon.

**Monitor the Jobs Using ReadyDATA Replicate**

The Monitor screen displays the status of pending and active jobs. Active jobs are currently running; pending jobs are the next occurrence of a scheduled replication job. You can also
run a scheduled replication job immediately, and cancel an active job. Continuous replication jobs are always active jobs.

➢ **To run a job immediately:**
   1. In the Views pane, click the Monitor icon.
   2. Click the blue icon (the arrow) to the left of the job.

➢ **To display details about a job that is running:**
   1. In the Views pane, click the Monitor icon.
   2. On the status bar to the right of the job, click the Expand icon.
      
      The status bar expands to displays details about the job:
To cancel a job that is running:
1. In the Views pane, click the Monitor icon.
2. To the right of the status bar, click the Cancel button.

To reorganize the table with jobs and group the jobs:
1. In the Views pane, click the Monitor icon.
2. To the right of a column heading in the table, click the drop-down list.
3. Select in the list to do one of the following:
   • Sort the jobs in ascending order.
   • Sort the jobs in descending order.
   • Add or remove columns from the table.
4. To update the information in the table click the Refresh button.

Run Job Reports Using ReadyDATA Replicate
You can generate a report that shows the outcome of a scheduled replication job.

To run a report:
1. In the Views pane, click the Reports icon.
2. Select a job from the Report drop-down list.
   The report runs automatically, and generates a detailed progress report (see the following figure).
3. Click the + button to the left of a job to display the details of the job. If a job fails, the report indicates where the problem occurred.

To reorganize the table with reports and group the reports:

1. In the Views pane, click the Reports icon.
2. To the right of a column heading in a table, click the drop-down list.
   You can select from the following:
   - Sort the reports in ascending order.
   - Sort the report in descending order.
   - Add or remove columns from the table.
   - Group the reports by a field.
   - Show the reports in a group (you can also click the Grouping button above the table).
3. To update the information in the table click the Refresh button.

Exchange Certificates for Local Replication

Before creating a local replication job between two ReadyDATA systems, you must copy each system's local certificate to the other. This is not necessary if the replication job is managed by ReadyDATA Replicate.

To access and exchange certificates between ReadyDATA systems:

1. Log in to both ReadyDATA systems.
2. On the first ReadyDATA, select Replicate.
3. Click Certificates.
4. In the Local Certificate section, click the **Copy To Clipboard** button.
   The Copy Certificate screen opens, displaying the certificate.

   ![Copy Certificate](image)

5. Press Ctrl + C.
6. Click the **Close** button.
7. On the second ReadyDATA, select Replicate.
8. Click the **Certificates** button.
   The Certificates screen displays.

   ![Certificates](image)

9. Click the add icon (➕).
The New Certificate screen displays.

10. Type the first ReadyDATA’s name into the **Name** field.
11. In the **Key** field type **Ctrl + V**.
12. Click the **Add** button.
13. Repeat the process exchanging the roles of the ReadyDATAs.

**Schedule Replication for Local Replication**

You create replication jobs on the source ReadyDATA.

If the source share or LUN is large, the initial replication transfer takes a substantial amount of time, particularly if the source and destination ReadyDATAs are connected by a WAN. You can shorten this time by seeding the destination site. For information about seeding replication, see *Seed or Reseed Replication* on page 196. If you seed a destination use the resume job procedure, *Resume Local Replication* on page 233.

➢ **To create a replication job:**

1. On the source ReadyDATA, select Replicate.
2. Click the **Jobs** button.
The Jobs screen displays.

3. Click the **New Job** button.

The New Job wizard opens.
4. Click the icon for the ReadyDATA.
   The volumes display.

5. Double-click the volume containing the share or LUN you want to replicate.
6. Select the share or LUN you want to replicate.
7. In the **IP address or domain** field, enter the IP address or domain name of the destination ReadyDATA.
8. In the **Access key** field, select the previously added access key for the destination ReadyDATA.
9. Click the **Connect** button.
If the ReadyDATA can be reached, and the access key is valid, an icon for the system displays.

10. Click the icon for the ReadyDATA.
    The volumes on the destination display.

11. Select the destination volume.
12. Click the **Next** button.

The window updates showing various job parameters. Only the name for the new share or LUN and the IP address are required.

(Optional) Configure the following advanced settings:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Progress</td>
<td>Select the check box to view the progress of the data transfer.</td>
</tr>
<tr>
<td>Compression</td>
<td>Select the check box to enable data compression during the data transfer.</td>
</tr>
<tr>
<td></td>
<td>Then configure the compression rate. By default, compression is disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After the data has been transferred, the data is not stored</td>
</tr>
<tr>
<td></td>
<td>compressed unless it was already compressed on the source share or LUN.</td>
</tr>
<tr>
<td>Compression Level</td>
<td>Set the compression level by clicking the up or down arrows to increase or</td>
</tr>
<tr>
<td></td>
<td>decrease the level. You can select from 1 through 9. For example, 5 indicates</td>
</tr>
<tr>
<td></td>
<td>that data is compressed five times.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encryption</td>
<td>Select the check box to enable encryption. By default, encryption is disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> NETGEAR recommends that you encrypt sensitive data.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you do not use an explicit destination IP address, data that is replicated over the Internet is automatically encrypted for increased safety. When you select the Encryption check box, data that is replicated over the Internet is encrypted twice.</td>
</tr>
<tr>
<td>Deduplication</td>
<td>Select the check box to enable deduplication during the data transfer. Deduplication prevents transfer of redundant data and increases the speed of the data transfer.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After the data has been transferred, the data is not stored in a deduplicated format unless it was already deduplicated on the source share or LUN.</td>
</tr>
<tr>
<td>Explicit IP Address</td>
<td>ReadyDATA Replicate automatically selects the physical Ethernet interfaces and VNICs for communication between the source and destination systems. If you want to use a specific interface on the destination system, you can specify its IP address.</td>
</tr>
<tr>
<td></td>
<td>To specify a specific interface, enter the IP address of the interface on the destination system. The address is automatically appended with port number 6819.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must set up port forwarding if the source and destination are behind a firewall.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you use an explicit destination IP address, data that is replicated over the Internet is not automatically encrypted. You must select the Encryption check box to enable encryption.</td>
</tr>
<tr>
<td>Explicit Domain Name</td>
<td>ReadyDATA Replicate automatically selects the physical Ethernet interfaces and VNICs for communication between the source and destination systems. If instead, you want to use a specific domain name for the destination system, you can specify it here. The name is automatically appended with port number 6819.</td>
</tr>
</tbody>
</table>
13. Click the **Next** button.
The first screen in the scheduling procedure displays.

14. Select *Continuously* or *Periodically* from the drop-down list and click the **Next** button.
If you select **Continuously**, the screen displays with a message about continuous replication.

**Continuous replication jobs transfer data in real-time between two systems for the best possible protection.**
If you select **Periodically**, a plot of the hours in a week displays.

15. If you selected **Periodically**, select the times you would like the replication to occur.
   
   Any combination of hours is allowed. Selected times are green. Select a row by clicking the day, or a column by clicking the hour. You can also adjust when after the start of the hour, replication starts.

16. Click the **Next** button.
   
   The screen updates to show a summary of the job.

17. Click **Finish**
   
   The New Job wizard closes and the replication job starts.

**Resume Local Replication**

If a replication job is blocked, for example because of a network or system failure, or if you manually stop or remove a replication job, you can resume it. If you seed a new replication job to speed the initial transfer, or reseed an existing job as part of disaster recovery, you use this procedure to resume the replication instead of creating a new job (see *Seed or Reseed Replication* on page 196 for more information).

➢ **To resume a replication job:**

1. On the source ReadyDATA, select **Replicate**.
2. Click the **Jobs** button.
   The Jobs screen displays.

3. Click the **New Job** button.
   The New Job wizard opens.
4. Click the icon for the ReadyDATA.
   The volumes display.

5. Double-click the volume containing the share or LUN you want to replicate.
6. Select the share or LUN you want to replicate.
7. In the **IP address or domain** field, enter the IP address or domain name of the destination ReadyDATA.
8. In the **Access key** field, select the previously added access key for the destination ReadyDATA.
9. Click the **Connect** button.
If the ReadyDATA can be reached, and the access key is valid, an icon for the system displays.

10. Click the icon for the ReadyDATA.
    The volumes on the destination display.

11. Click the Resume button.
12. Double-click the destination volume.
    The shares and LUNs on the volume display.
13. Click the share or LUN that contains a replica of the source.
14. Click **Next**.

The screen displays the available snapshots.
15. Select the appropriate snapshot (usually the most recent).
16. Click the **Next** button.

The screen updates showing various job parameters.
17. Click the **Next** button.

The first screen in the scheduling procedure displays.
18. Select **Continuously** or **Periodically** from the drop-down list and click the **Next** button. If you select **Continuously**, the screen displays with a message about continuous replication.
If you select **Periodically**, a plot of the hours in a week displays.

![New Job window with scheduling options](image)

19. If you selected **Periodically**, select the times you would like the replication to occur.

   Any combination of hours is allowed. Selected times are green. Select a row by clicking the day, or a column by clicking the hour. You can also adjust when after the start of the hour, replication starts.

20. Click the **Next** button.

   The screen updates to show a summary of the job.

21. Click **Finish**

   The New Job wizard closes and the replication job starts.
Monitor and Manage Local Replication

From the Jobs section of the Replicate screen, you can view the status, logs, and properties of all jobs with data sources on that system. You can manually trigger a job, stop a running job, and disable, reenable, and delete a job.

Also from the Replicate screen you can determine any jobs using the system as a target and disconnect the destination from the job (leaving the job configured on the source system, but with broken status).
This appendix provides the factory default settings of the ReadyDATA.

To reset all settings to their factory defaults, use the procedure that is explained in *Reset the Firmware to Factory Defaults* on page 156, or press the Reset button on the front panel of the ReadyDATA as explained in the *ReadyDATA Hardware Manual*. The ReadyDATA returns to the factory configuration settings that are shown in the following table:

**Table 10. ReadyDATA factory default settings**

<table>
<thead>
<tr>
<th>Item</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System settings</strong></td>
<td></td>
</tr>
<tr>
<td>Device Time</td>
<td>GMT -08:00 Pacific Time (US &amp; Canada); Tijuana</td>
</tr>
<tr>
<td>Services</td>
<td></td>
</tr>
<tr>
<td>SMB</td>
<td>Globally enabled</td>
</tr>
<tr>
<td>AFP</td>
<td>Globally enabled</td>
</tr>
<tr>
<td>NFS</td>
<td>Globally disabled</td>
</tr>
<tr>
<td>FTP</td>
<td>Globally disabled</td>
</tr>
<tr>
<td>Port number</td>
<td>21</td>
</tr>
<tr>
<td>Authentication mode</td>
<td>Anonymous</td>
</tr>
<tr>
<td>Allow upload resumes</td>
<td>Disabled</td>
</tr>
<tr>
<td>Passive ports</td>
<td>32768–65535</td>
</tr>
<tr>
<td>Masquerade address</td>
<td>Disabled</td>
</tr>
<tr>
<td>SNMP</td>
<td>Globally disabled</td>
</tr>
<tr>
<td>Community</td>
<td>Public</td>
</tr>
<tr>
<td>Trap destination</td>
<td>Blank</td>
</tr>
<tr>
<td>Hosts allowed access</td>
<td>Blank</td>
</tr>
<tr>
<td>SSH</td>
<td>Globally disabled</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Globally enabled (nonconfigurable)</td>
</tr>
<tr>
<td>Replicate</td>
<td>Globally disabled</td>
</tr>
<tr>
<td>User name</td>
<td>Blank</td>
</tr>
<tr>
<td>Password</td>
<td>Blank</td>
</tr>
<tr>
<td>Language</td>
<td>English</td>
</tr>
</tbody>
</table>
Table 10. ReadyDATA factory default settings (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>RES- followed by the last 6 bytes of the system’s primary MAC address</td>
</tr>
<tr>
<td><strong>Network settings</strong></td>
<td></td>
</tr>
<tr>
<td>Ethernet interface settings</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>1500</td>
</tr>
<tr>
<td>Speed (Mbps)</td>
<td>1000</td>
</tr>
<tr>
<td>Duplex</td>
<td>Full</td>
</tr>
<tr>
<td>Bonding</td>
<td>None</td>
</tr>
<tr>
<td>VNIC</td>
<td>One attached to each interface (for example, vnic0 to eth0 and vnic1 to eth1)</td>
</tr>
<tr>
<td>VNIC settings</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>1500</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>0</td>
</tr>
<tr>
<td>Bandwidth limit</td>
<td>None</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>IPv4 with DHCP enabled, and IPv6 disabled</td>
</tr>
<tr>
<td>DNS</td>
<td>No server</td>
</tr>
<tr>
<td><strong>Storage settings</strong></td>
<td></td>
</tr>
<tr>
<td>Volumes</td>
<td>No default volumes</td>
</tr>
<tr>
<td>Compression</td>
<td>Enabled (nonconfigurable)</td>
</tr>
<tr>
<td>Deduplication</td>
<td>Enabled (nonconfigurable)</td>
</tr>
<tr>
<td>Shares</td>
<td>No default shares</td>
</tr>
<tr>
<td>Logbias</td>
<td>Latency</td>
</tr>
<tr>
<td>Compression</td>
<td>Disabled (configurable)</td>
</tr>
<tr>
<td>Deduplication</td>
<td>Disabled (configurable)</td>
</tr>
<tr>
<td>Protection</td>
<td>Continuous</td>
</tr>
<tr>
<td>Protection interval</td>
<td>Daily</td>
</tr>
<tr>
<td>Size</td>
<td>Unlimited access to the storage space on the volume, assigned on demand</td>
</tr>
<tr>
<td>Access</td>
<td>Denied until you set permissions</td>
</tr>
</tbody>
</table>
### Table 10. ReadyDATA factory default settings (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LUNs</strong></td>
<td>No default LUNs</td>
</tr>
<tr>
<td></td>
<td>Logbias Latency</td>
</tr>
<tr>
<td></td>
<td>Compression Disabled (configurable)</td>
</tr>
<tr>
<td></td>
<td>Deduplication Disabled (configurable)</td>
</tr>
<tr>
<td></td>
<td>Protection Continuous</td>
</tr>
<tr>
<td></td>
<td>Protection interval Daily</td>
</tr>
<tr>
<td></td>
<td>Provisioning Thick</td>
</tr>
<tr>
<td></td>
<td>Access Denied until you set permissions</td>
</tr>
<tr>
<td><strong>Snapshots</strong></td>
<td>Hourly On the hour</td>
</tr>
<tr>
<td></td>
<td>Daily At midnight</td>
</tr>
<tr>
<td></td>
<td>Weekly At midnight on Friday</td>
</tr>
<tr>
<td><strong>Security settings</strong></td>
<td></td>
</tr>
<tr>
<td>Administrative settings</td>
<td>User name admin</td>
</tr>
<tr>
<td></td>
<td>Password password</td>
</tr>
<tr>
<td></td>
<td>Password recovery Question Blank</td>
</tr>
<tr>
<td></td>
<td>Answer Blank</td>
</tr>
<tr>
<td></td>
<td>Email address Blank</td>
</tr>
<tr>
<td>Authentication</td>
<td>Access type Local users</td>
</tr>
<tr>
<td></td>
<td>Workgroup name VOLUME</td>
</tr>
<tr>
<td>Default groups</td>
<td>users with GUID 100</td>
</tr>
<tr>
<td>Default users</td>
<td>None</td>
</tr>
<tr>
<td><strong>SAN settings</strong></td>
<td>No default group</td>
</tr>
<tr>
<td></td>
<td>Target Automatically issued</td>
</tr>
<tr>
<td></td>
<td>CHAP authentication Disabled</td>
</tr>
<tr>
<td></td>
<td>Initiators None</td>
</tr>
<tr>
<td></td>
<td>Bidirectional CHAP authentication Disabled</td>
</tr>
<tr>
<td><strong>System monitoring</strong></td>
<td></td>
</tr>
<tr>
<td>Alerts</td>
<td>Disabled (email, user, and server information is blank)</td>
</tr>
<tr>
<td>Event types</td>
<td>All event types are enabled</td>
</tr>
</tbody>
</table>
## Table 10. ReadyDATA factory default settings (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logs</td>
<td>Records: Errors enabled, Warnings enabled, Info enabled</td>
</tr>
<tr>
<td></td>
<td>Categories: All (System, Disk, Volume, Share, Account, and Miscellaneous)</td>
</tr>
<tr>
<td>Status graphics</td>
<td>Volume: All volumes</td>
</tr>
<tr>
<td></td>
<td>Type: Operations</td>
</tr>
<tr>
<td></td>
<td>Period: 5 minutes</td>
</tr>
<tr>
<td></td>
<td>Update: 5 seconds</td>
</tr>
<tr>
<td></td>
<td>Network: All Ethernet interfaces and VNICs</td>
</tr>
<tr>
<td></td>
<td>Protocol: All (SMB, NFS, AFP, HTTP, SSH, iSCSI, and SNMP)</td>
</tr>
<tr>
<td></td>
<td>Period: 5 minutes</td>
</tr>
<tr>
<td></td>
<td>Update: 5 seconds</td>
</tr>
<tr>
<td></td>
<td>Utilization: All volumes</td>
</tr>
<tr>
<td></td>
<td>Period: 5 minutes</td>
</tr>
<tr>
<td></td>
<td>Update: 5 seconds</td>
</tr>
<tr>
<td></td>
<td>Temperature: All (SYS, CPU, and AUX)</td>
</tr>
<tr>
<td></td>
<td>Period: 5 minutes</td>
</tr>
<tr>
<td></td>
<td>Update: 5 seconds</td>
</tr>
</tbody>
</table>
Index

A
access modes 140
access rights
  LUNs 124
  shares 90–105
Active Directory (AD)
  enabling 141
  setting permissions 90–97
address mask, FTP 71
administrator password
  recovering 158
  setting 49
AFP (Apple File Protocol) settings 68–69, 93, 96
aggregation links 63
alerts, configuring 50
allocating storage space
  LUNs 109
  shares 79, 82
anonymous share access 97
Apple File Protocol (AFP) settings 68–69, 93, 96
authentication mode, FTP 70
automatic snapshots
  LUNs 112
  shares 79, 83, 108, 112
auxiliary temperature 163

B
bandwidth limit, configuring 59
bandwidth monitoring, volumes 160
bidirectional CHAP authentication, LUNs 127
bonded channel 63
boosting I/O operations 36
browsers supported 11

cache operations 36
channel bonding, configuring 63
CHAP authentication, LUNs 126
clearing system logs 166
clock settings 46
cloning snapshots 186
community, SNMP 72
compression, configuring
  LUNs 108, 112
  replication 205, 214, 229
  shares 78, 82
continuous protection, configuring
  LUNs 112
  shares 79, 83, 108, 112
continuous replication 195
CPU status 163

dashboard, described 15
data recovery 196
date settings 46
deduplication, configuring
  LUNs 112
  replication 206, 215, 230
  shares 78, 82
default settings 244
defaults
  resetting 156
DHCPv6 client and server 60
disks
  color codes 23
  global spares 42
  mirroring 20
  mixing types 21, 42
  status and health 33, 163
  supported numbers and types 18
DNS realm name, Active Directory 142
DNS servers, configuring 61
documentation 11
downloading
  firmware 154
  system logs 166
duplex setting, configuring 56

e-mail contact, alerts 50
encryption, configuring replication 215
Ethernet interfaces 53
events, monitoring 165
expanding
  LUNs 113
  shares 82
  volumes 33
expansion disk arrays 22
exporting volumes 39

F
factory defaults
  resetting 156
  settings 244
failures, monitoring 165
fans, status 163
files and folders, share access rights 104
file-sharing protocols, configuring
  for shares 76–79
  globally 67–72
firmware, updating 152–156
FTP settings 68–71, 93, 96, 99, 101, 103

G
global spare disks, configuring 42
  group ID (GID) 143
  group settings, share access rights 95
  groups, LUNs 121
GUI 15

H
hash types, configuring LACP 63–66
health information, system 163
host name, configuring 52
host settings, share access rights 97
hosts, SNMP 72

I
I/O operations, improving 36
I/O statistics 33
importing volumes 39
importing. See also migrating initiators, configuring for LUNs 126
interface speed, configuring 56
IP addresses
  AD server 142
  DNS servers 61
  explicit destination, replication 206, 215, 230
  IPv4 and IPv6 60
  masking for FTP 71
  network router 60
IQNs (iSCSI qualified names) 126
iSCSI initiator 131

J
jobs, replication 218–222

L
LACP and LAG, configuring 63–66
language settings 48
layer 2, 3, and 4 hash types 63–66
LED, virtual 23
levels, RAID 20
links, aggregation 63
Linux devices, accessing shares 130
local database
  enabling 140
  managing 142–150
  setting permissions 90–97
local firmware update 154
log operations, boosting 36
logical volume 21
logs, system, configuring 165–166
lost administrator password, recovering 158
LUNs
  accessing remotely 131
  managing 105–127

M
Mac OS X devices, accessing shares 129
manual snapshots, shares and LUNs 178–181
mask address, FTP 71
message levels and categories, logging 166
MIBs
  NETGEAR SNMP 167
  UPS manufacturer SNMP 172
migrating
  LUNs 115
  shares 83, 85, 87, 116, 118
mirrored disks 20
MTU configuring
  aggregation channel 66
Ethernet interface 56
VNIC 58
N
navigation bar, Dashboard 15
NetBIOS domain name, Active Directory 142
NETGEAR SNMP MIB 167
Network File Service (NFS) settings 68–69, 93, 96, 99, 101, 103
network settings
   DHCP server 60
   host name 52
Network UPS Tools (NUT) 169
NFS (Network File Service) settings 68–69, 93, 96, 99, 101, 103
NTP server 47
NUT (Network UPS Tools) 169

O
operating systems supported 11
operations, monitoring for volumes 160
OS X devices, accessing shares 129
OU (organization unit), Active Directory 142

P
passive ports, FTP 70
passwords
   administrator 49
   recovering administrator’s 158
   users accounts 148, 150
performance, improving 36–38
periodic continuous 209
periodic replication 195, 199
permissions
   LUNs 124
   shares 90–105
port number, FTP 70
power failures, UPS 167
power supplies, status 163
prefix length, IPv6 61
primary group, user accounts 148, 150
product registration 16
protection, configuring
   LUNs 112
   shares 79, 83, 108, 112
protocols, configuring
   for shares 76–79
   globally 67–72
provision storage space, LUNS 109

Q
quick-start guide 9
quota, configuring for shares 79, 82

R
RAID levels 20
RAIDar utility 13
read operations 36
read-only and read/write shares 90–97
ReadyDATA Replicate, registering systems 197
ReadyDATA website 11
ReadyNAS, remote server 169
recovering data 196
recovery, password 49
registration procedure 16
remote firmware update 152
remote servers, UPS 169
remote share access 127
remote UPS 167, 172
replication
   continuous 209
   described 195
   periodic 199
reports, replication jobs 222
reserve storage space
   LUNs 109
   shares 79, 82
resetting
   factory defaults 156
   share permissions 105
restarting system 158
reverse replication 196
rolling back snapshots 183

S
security access modes 140
Server Message Block (SMB) settings 68–69, 93, 96, 99, 101, 103
shares
   accessing remotely 127
   configuring 74–105
shutting down system 158
size, configuring
   LUNs 109
   shares 79, 82
Smart Snapshot Management 189
SMB (Server Message Block) settings 68–69, 93, 96, 99, 101, 103
snapshots, configuring
  LUNs 112
  shares 79, 83, 108, 112
snapshots, managing 177–192
SNMP
  monitoring 166
  settings 68–72
SNMP UPS 167, 172
spare disks 42
speed, configuring for interfaces 56
SSH settings 68–69
storage space, reserved
  LUNs 109
  shares 79, 82
striped disks 20
support technical 2
system
  monitoring 159–167
  shutting down 158
system alerts, configuring 50
system configuration
  alert event settings 51
  clock 46
  time and date 46
system configuration bar, Dashboard 15

T
targets
  iSCSI initiator 132
  LUN groups 122, 126
technical support 2
temperatures, system monitoring 162
thin and thick provisioning, LUNs 109
time settings 46
timeline, snapshots 177–192
trademarks 2
trap destination address, SNMP 72
troubleshooting
  lost administrator password 158
  RAIDar does not detect ReadyDATA system 14
  reconnecting after losing IP address 62
trusted domains, Active Directory 142

U
Unix devices, accessing shares 130
UPS
  configuring and monitoring 167–174
  health status 163
user accounts
  creating 146
  managing 146–150
user groups, managing 142–146
user ID (UID) 147
user interface 15
user settings, share access rights 95
utilization, monitoring for volumes 162

V
virtual disk LED 23
VNICS, configuring 56–62
volumes
  managing 26–44
  monitoring 160–162

W
Windows devices, accessing shares 128
write operations, boosting 36