ioSafe®
disaster proof hardware

ioSafe® R4 : Disaster-proof NAS/RAID

User's Guide, ioSafe R4

/N: 900-10004-00 REV 02

CONGRATULATIONS!

This product represents the latest in disaster proof computer equipment. This system has the following disaster proof specifications:

1. Fire proof data storage to 1700 F, 1 hr duration per UL72
2. Waterproof data storage to 30' depth, 30 days in fresh water or salt water.

IMPORTANT NOTE: DISASTER RECOVERY

Please refer to the website for the latest disaster recovery procedures and product warranties. While no device can protect against every disaster, this ioSafe R4 system has been tested to protect data against fires, floods and building collapse. More information is available and updated online at our website www.iosafe.com. Please see the website or details in this manual for the terms and conditions of our Disaster Recovery Service.

If you have a disaster please contact the ioSafe Disaster Response Team at 1.888.984.6723 x430 for assistance in recovery of your ioSafe unit. Due to the unique nature of individual disasters, different recovery strategies may have to be employed depending on your particular circumstances. Let the experts at ioSafe assist with recovery.

Some general rules regarding recovery are as follows:

1. Don't attempt to recover the ioSafe R4 unit by yourself. The lack of our expert support might lead to irretrievable data loss. Let our disaster support engineers help recover your critical data.
2. Turn off the power.
3. Do not restart the ioSafe R4 after a disaster without first consulting with an ioSafe disaster support person first.
4. Do not try to reconfigure or re-initialize the RAID array.

http://www.iosafe.com

Appendix A
Limited Warranty Statement
Warranty Services

End User Limited Product Warranty

ioSafe Incorporated, ("ioSafe") values your business and always attempts to provide you the very best data protection and recovery services.

No limited warranty is provided by ioSafe unless you are the original customer of the product. ioSafe's warranty is non-transferable. No limited warrant is provided unless your ioSafe product ("Product") was purchased from an authorized distributor or authorized reseller. Distributors may sell Products to resellers who then sell Products to end users. Please see below for warranty information or obtaining service. No warranty service is provided unless the Product is returned ioSafe.

Warranty Policy

ioSafe warrants to the end user customer, subject to limitations list below, that the warranted hardware components, listed below, shall be free from defects in material or workmanship and will conform to ioSafe's specification for the particular Product for the applicable warranty period. ioSafe further warrants that for the applicable warrant period shown below and starting from the date of purchase, the media on which any software included in the hardware components is furnished will be free from defects in materials and workmanship under normal use. Except for the foregoing, such software is provided AS IS. During the applicable warranty period ioSafe will repair or replace (at ioSafe's option) any warranted hardware part which does not comply with this warranty with a new or functionally equivalent replacement part, provided the defective part is returned to ioSafe as described in the "Returned Materials Authorization (RMA)" section detailed below.

Warranted Product	Warranty Period
ioSafe S2	3 Years – Optional 5 Years
ioSafe R4	3 Years – Optional 5 Years

Note:
The limited warranty extends only for the period of time set forth above. The period commences from the date of purchase of the original Product. To verify the warranty of your Product, please maintain the receipt of the original Purchase. In the United States, some states do not allow limitations on how long implied warranties last, so the above limitation may not apply to you.

THERE ARE NO WARRANTIES WHICH EXTEND BEYOND THE FACE OF THE IOSAFE LIMITED WARRANTY. IOSAFE DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE PRODUCTS, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE EXCLUSION OF THE IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

Return Material Authorization (RMA)

No Product may be returned directly to ioSafe without first contacting ioSafe for a Return Material Authorization ("RMA") number. If it is determined that the Product may be defective, you will be given an RMA number and instructions for Product return. An unauthorized return, i.e. one for which an RMA number has not been issued, will be returned to you at your expense. Authorized returns are to be shipped prepaid and insured to the address on the RMA in an approved shipping container. To request an RMA, please refer to the ioSafe web site at www.iosafe.com.

Extended Warranty

Customers can purchase an extended warranty on eligible ioSafe products with less than a 5-year warranty. The maximum warranty period for these products, including any warranty extension, cannot be longer than 5 years from the date of purchase. Extended warranty is currently available for purchase online.

LIMITATION OF REMEDIES

YOUR EXCLUSIVE REMEDY FOR ANY DEFECTIVE PRODUCT IS LIMITED TO THE REPAIR OR REPLACEMENT OF THE DEFECTIVE PRODUCT.

ioSafe may elect which remedy or combination of remedies to provide in its sole discretion. ioSafe shall have a reasonable time after determining that a defective Product exists to repair or replace a defective Product. ioSafe's replacement Product under its limited warranty will be manufactured from new and serviceable used parts. ioSafe's warranty applies to repaired or replaced Products for the balance of the applicable period of the original warranty or ninety days from the date of shipment of a repaired or replaced Product, whichever is longer.

LIMITATION OF DAMAGES

IOSAFE'S ENTIRE LIABILITY FOR ANY DEFECTIVE PRODUCT SHALL IN NO EVENT EXCEED THE PURCHASE PRICE FOR THE DEFECTIVE PRODUCT. THIS LIMITATION APPLIES EVEN IF IOSAFE CANNOT OR DOES NOT REPAIR OR REPLACE ANY DEFECTIVE PRODUCT AND YOUR EXCLUSIVE REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

NO CONSEQUENTIAL OR OTHER DAMAGES

NOTWITHSTANDING ANYTHING ELSE IN THIS POLICY OR OTHERWISE, IOSAFE WILL NOT BE LIABLE WITH RESPECT TO THE PRODUCTS UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY (I) FOR ANY AMOUNT IN EXCESS OF THE PURCHASE PRICE FOR THE DEFECTIVE PRODUCT OR (II) FOR ANY GENERAL, CONSEQUENTIAL, PUNITIVE, INCIDENTAL OR SPECIAL DAMAGES. THESE INCLUDE LOSS OF RECORDED DATA, INTERRUPTION OF USE, THE COST OF RECOVERY OF LOST DATA, LOST PROFITS AND THE COST OF THE INSTALLATION OR REMOVAL OF ANY PRODUCTS, THE INSTALLATION OF REPLACEMENT PRODUCTS, AND ANY INSPECTION, TESTING, OR REDESIGN CAUSED BY ANY DEFECT OR BY THE REPAIR OR REPLACEMENT OF PRODUCTS ARISING FROM A DEFECT IN ANY PRODUCT. THIS SECTION DOES NOT LIMIT LIABILITY FOR BODILY INJURY OF A PERSON.

IN THE UNITED STATES, SOME STATES DO NOT ALLOW EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE LIMITATIONS ABOVE MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

Your Use of the Product

ioSafe will have no liability for any Product returned if ioSafe determines that:

- The product was stolen from ioSafe.
- The asserted defect:
  - A. is not present,
  - B. cannot reasonably be fixed because of damage occurring when the Product is in the possession of someone other than ioSafe, or
  - C. is attributable to misuse, improper installation, alteration (including removing or obliterating labels and opening or removing external covers (unless authorized to do so by ioSafe or an authorized Service Center)), accident or mishandling while in the possession of someone other than ioSafe.
- The Product was not sold to you as new.

Additional Limitations on Warranty

ioSafe’s limited warranty does not cover Products which have been received improperly packaged, altered, or physically damaged. Products will be inspected upon receipt. You can view additional examples of the warranty limitations below by clicking on the available links.

ioSafe Disaster Recovery Service Terms and Conditions

As applicable during the warranty period and proper registering of an ioSafe product, ioSafe will assist the original purchaser who has experienced a “qualified disaster” to restore the data that was stored on their ioSafe product by the following ways:

1. ioSafe will provide phone or email based support to assist in recovering the data, or

2. ioSafe will pay for the disaster exposed product to be shipped back to ioSafe headquarters for data recovery. If data recovery is successful, a replacement product will be loaded with the original data and shipped back to the original user, or

3. if the data recovery by ioSafe is not successful, ioSafe will pay up to the amount shown in the table below for the specific ioSafe product to a third party disk recovery service of ioSafe's choice to extract the data. Any data extracted will be loaded on a replacement product and shipped back to the original user. ioSafe has the right to use a factory refurbished product as the replacement product.

Product Line	U.S. Dollars per disk
ioSafe S2, ioSafe R4	$5,000

ioSafe's good faith attempts to restore and recover the data in accordance with these terms and conditions shall be the purchaser's sole and exclusive remedy and ioSafe shall not be liable for any damages whatsoever. ioSafe cannot guarantee that any data will be recoverable nor can it guarantee which data files are on the ioSafe product. Data restoration or recovery shall be strictly limited to whatever files are restorable or recoverable and not what the purchaser believes to exist on the ioSafe product. Only one instance of data extraction per ioSafe product is covered by this program. Other exclusions may apply. See web site for details: www.iosafe.com.

A “qualified disaster” is defined as a disaster by which a police or fire incident report is written to describe the disaster event. The disaster event would include, but is not limited to: fire, flood, theft and acts of God.

Contents

About This Guide

Congratulations and thank you for purchasing an ioSafe disaster proof backup and storage system from ioSafe Inc. This ioSafe system represents the latest technology in disaster-proof computer hardware.

Chapter 1, "FrontView Advanced Control", describes all the menus and tabs available in the Advanced Control mode.

If you have already configured the ioSafe R4 and you need help in accessing the shares on the ioSafe R4, skip to **Chapter 2**, "Accessing Shares".

In the event of a disk failure, the proper procedure for replacing the failed disk is in **Chapter 3**, "Replacing a Failed Disk".

Sometimes it may be necessary to re-install the firmware or reset the system back to the factory default configuration. **Chapter 4**, "System Reset Switch", explains the process for doing both.

Chapter 5, "Changing User Passwords", covers how non-admin users can access FrontView to change their password.

For an explanation of the RAID levels that the ioSafe R4 supports, please refer to **Appendix A**, "RAID Levels Simplified".

If you have questions on what constitutes a valid input for host name, workgroup, or password, **Appendix B**, "Input Field Format", describes these and more.

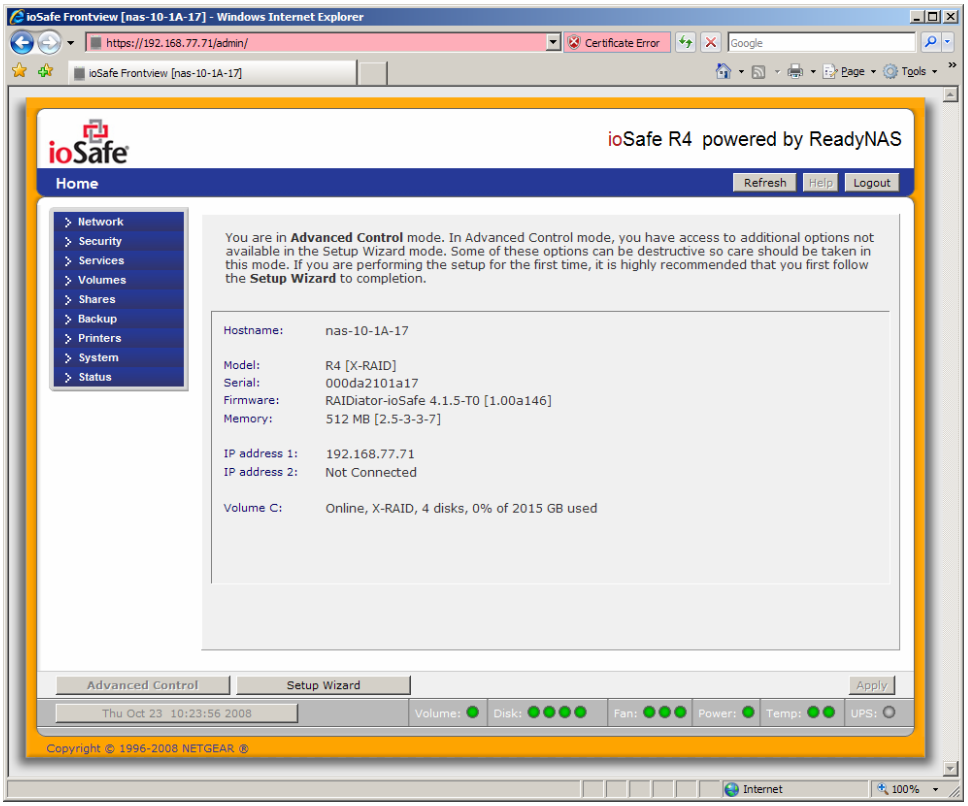
Appendix C, "Glossary", provides definitions for some of the technical terminologies used in this document.

If you need help during setup, refer to **Appendix D**, "If You Need Help…".

Chapter 1

FrontView Advanced Control

The Advanced Control mode offers the all settings available in the Setup Wizard plus more.

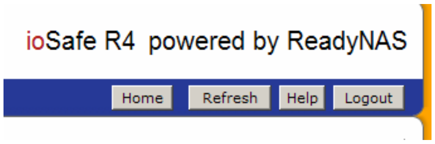


You are in **Advanced Control** mode. In Advanced Control mode, you have access to additional options not available in the Setup Wizard mode. Some of these options can be destructive so care should be taken in this mode. If you are performing the setup for the first time, it is highly recommended that you first follow the **Setup Wizard** to completion.

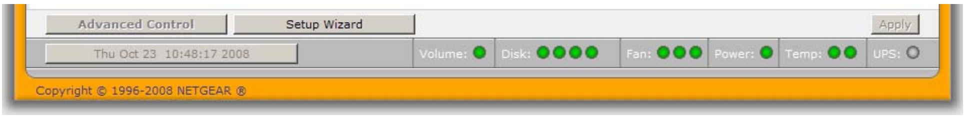
Hostname:	nas-10-1A-17
Model:	R4 [X-RAID]
Serial:	000da2101a17
Firmware:	RAIDiator-ioSafe 4.1.5-T0 [1.00a146]
Memory:	512 MB [2.5-3-3-7]
IP address 1:	192.168.77.71
IP address 2:	Not Connected
Volume C:	Online, X-RAID, 4 disks, 0% of 2015 GB used

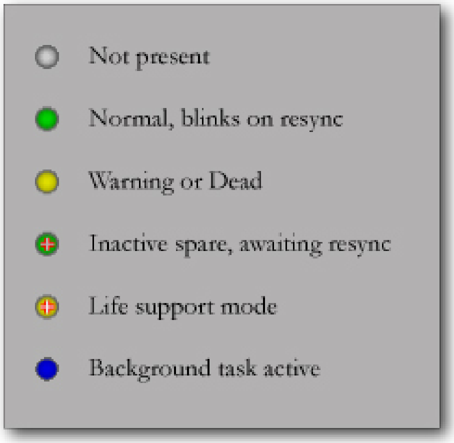
When you first switch to this mode, you'll see the menus on the left that allow you to quickly jump to the desired menu page. Towards the bottom left, you'll notice buttons that allow you to switch back and forth between the Setup Wizard mode and the Advanced Control mode.

As you click on the menu buttons, you'll notice a similar theme across all menu pages. At the top right corner is the command bar which typically provides options to return to the home page, refresh the browser window, display help where available, or to log out of the session. Due to security reasons, the **Logout** button only acts as a reminder to close the current browser session which is necessary to securely log out.



At the furthest bottom is the status bar with the date button which doubles its duty as a clock and a link to the Clock page. The status LEDs to the right gives a quick glimpse of the system device status.





The statuses represent:

- **Not present** – No disk or device attached.
- **Normal** – Device in normal operating mode. If the LED is blinking, this disk is currently re-syncing. During the re-sync process, the performance is temporarily in a "degraded" mode and another disk failure in the volume will render it dead.
- **Warning or Dead** – The device has failed or requires attention.
- **Inactive spare** – This disk is a "hot spare" on standby. When a disk fails, this disk will take over automatically.
- **Awaiting re-sync** – This disk is waiting to re-sync to the RAID volume.
- **Life support mode** – The volume has encountered multiple disk failures and is in the state of being marked dead. However, the ioSafe R4 has blocked it from being marked dead in the event that someone may have accidentally pulled out the wrong disk during runtime. If the wrong disk was pulled out, shutdown the ioSafe R4 immediately, reconnect the disk, and power-on the ioSafe R4. If you reconnect the disk during runtime, the ioSafe R4 will mark it as a newly added disk and you will no longer be able to access the data on it.
- **Background task active** – A lengthy background task such as a system update is in progress.

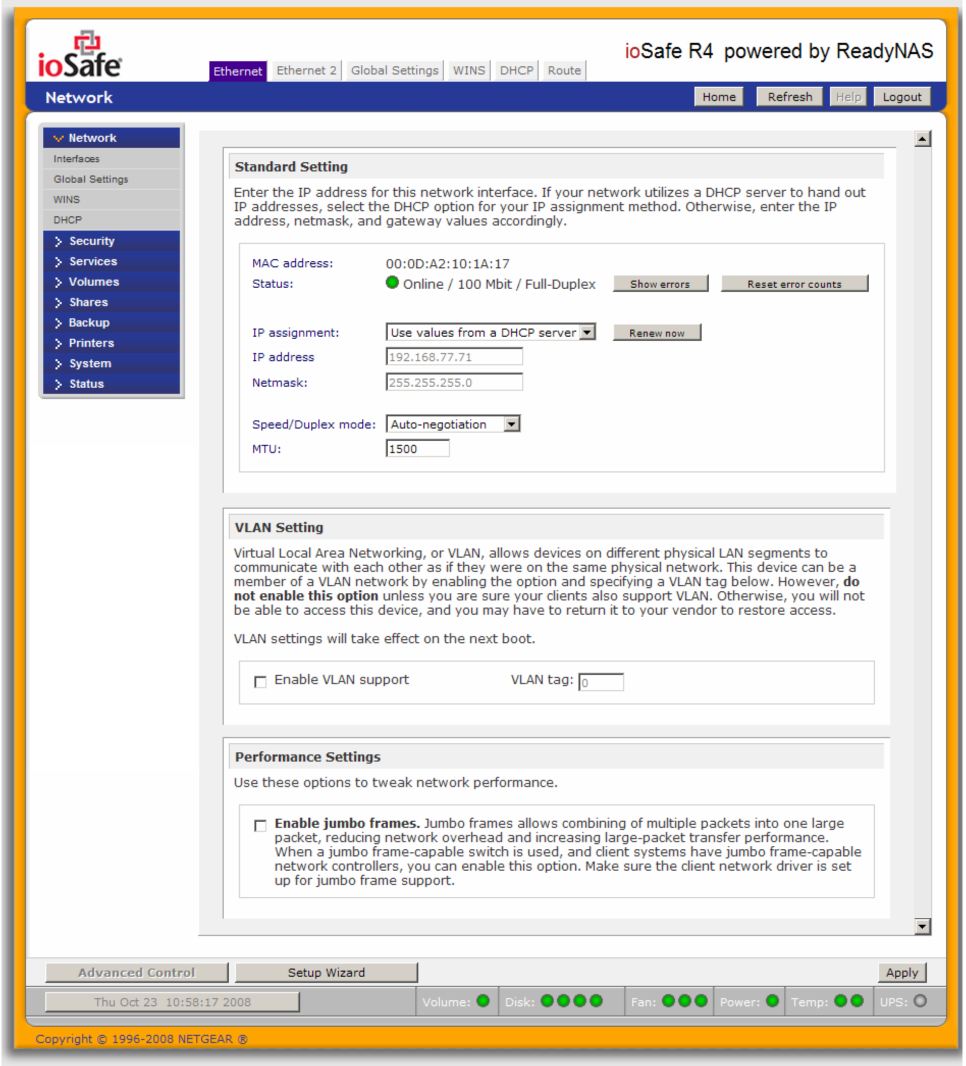
Move the mouse cursor over the LED to display more information on the device, or click on it to display the status in more detail.

Right above the status bar is the action bar. To the left are the Advanced Control and Setup Wizard buttons. To the right is the Apply button. Use this to save any changes in the current menu page.

Ethernet

The Ethernet tab allows you to specify network interface-specific settings.

In the **Standard Setting** box, you can specify the IP address, network mask, speed/duplex mode, and MTU settings. In most networks where a DHCP server is enabled, you can simply specify the "Use values from a DHCP server" option to automatically set the IP address and network mask.



Standard Setting

Enter the IP address for this network interface. If your network utilizes a DHCP server to hand out IP addresses, select the DHCP option for your IP assignment method. Otherwise, enter the IP address, netmask, and gateway values accordingly.

MAC address: 00:0D:A2:10:1A:17
Status: ● Online / 100 Mbit / Full-Duplex

IP assignment: Use values from a DHCP server
IP address: 192.168.77.71
Netmask: 255.255.255.0

Speed/Duplex mode: Auto-negotiation
MTU: 1500

VLAN Setting

Virtual Local Area Networking, or VLAN, allows devices on different physical LAN segments to communicate with each other as if they were on the same physical network. This device can be a member of a VLAN network by enabling the option and specifying a VLAN tag below. However, **do not enable this option** unless you are sure your clients also support VLAN. Otherwise, you will not be able to access this device, and you may have to return it to your vendor to restore access.

VLAN settings will take effect on the next boot.

☐ Enable VLAN support VLAN tag: 0

Performance Settings

Use these options to tweak network performance.

☐ **Enable jumbo frames.** Jumbo frames allows combining of multiple packets into one large packet, reducing network overhead and increasing large-packet transfer performance. When a jumbo frame-capable switch is used, and client systems have jumbo frame-capable network controllers, you can enable this option. Make sure the client network driver is set up for jumbo frame support.

Thu Oct 23 10:58:17 2008 Volume: ● Disk: ●●●● Fan: ●●● Power: ● Temp: ●● UPS: ○

Copyright © 1996-2008 NETGEAR ®

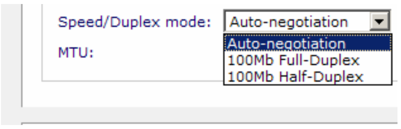
If you assign a static IP address, be aware that the browser will lose connection to the ioSafe R4 device after the IP address has been changed. You can click Rescan in RAIDar to locate the device and reconnect from there.

Note

If you elect to assign the IP address using DHCP, it is advisable to set the lease time on the DHCP server/router to a value of at least a day. Otherwise, you may notice that the ioSafe R4 IP address may change even when it has been powered down for only a few minutes. Most DHCP servers allow you to assign a static IP address for specified MAC addresses. If you have this option, this would be a good way to ensure your ioSafe R4 maintains the same IP address even in DHCP mode.

► SPEED/DUPLEX MODE

If you have a managed switch that works best if the devices are forced to a particular speed or duplex mode, you can select the desired setting. It's advisable to keep the setting in auto-negotiation mode otherwise.

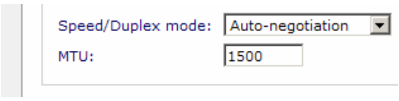


Speed/Duplex mode: Auto-negotiation

MTU:

► MTU

In some network environments, changing the default MTU value may fix throughput problems. It's advisable to leave the default setting otherwise.

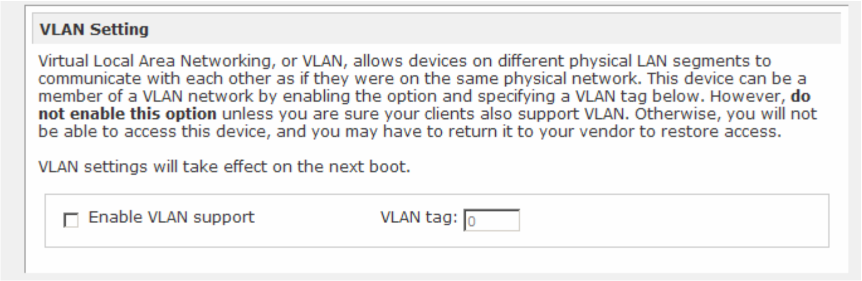


Speed/Duplex mode: Auto-negotiation

MTU: 1500

► VLAN SETTING

Virtual Local Area Network, or VLAN, allows devices residing on different segments of a LAN to appear in the same segment, or conversely allows devices on the same switch to behave as though they belong to a different LAN.



VLAN Setting

Virtual Local Area Networking, or VLAN, allows devices on different physical LAN segments to communicate with each other as if they were on the same physical network. This device can be a member of a VLAN network by enabling the option and specifying a VLAN tag below. However, **do not enable this option** unless you are sure your clients also support VLAN. Otherwise, you will not be able to access this device, and you may have to return it to your vendor to restore access.

VLAN settings will take effect on the next boot.

□ Enable VLAN support VLAN tag: 0

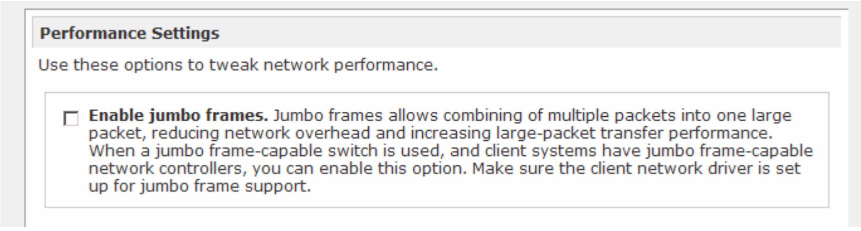
If you wish to use the ioSafe R4 in a VLAN environment, select the **Enable VLAN support** checkbox and input a numeric VLAN tag. You will need to reboot the ioSafe R4 for the VLAN function to take effect.

Warning

Do not enable VLAN support unless you are sure your clients also support VLAN. Otherwise, you can lose network access to the ioSafe R4 and you may need to perform a firmware re-installation to disable the VLAN setting.

► PERFORMANCE SETTING

The **Enable jumbo frames** option allows you to optimize the ioSafe R4 for large data transfers such as multiple streams of video playback. Select this option if your NIC and your gigabit switch support jumbo frames.



Performance Settings

Use these options to tweak network performance.

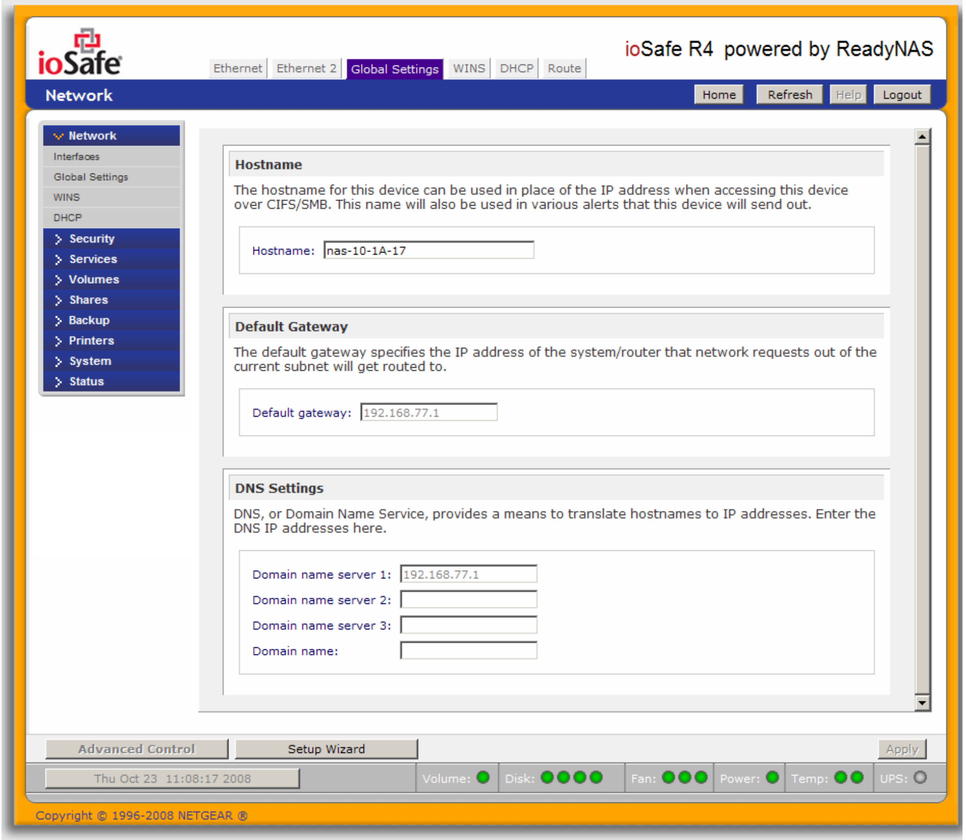
□ **Enable jumbo frames.** Jumbo frames allows combining of multiple packets into one large packet, reducing network overhead and increasing large-packet transfer performance. When a jumbo frame-capable switch is used, and client systems have jumbo frame-capable network controllers, you can enable this option. Make sure the client network driver is set up for jumbo frame support.

Note

The ioSafe R4 supports a 7936 byte frame size, so for optimal performance, a switch capable of this frame size or larger should also be used.

Your ioSafe R4 device comes with multiple Ethernet interfaces, you will see a separate configuration tab for each interface.

Global Network Settings



Hostname

The hostname for this device can be used in place of the IP address when accessing this device over CIFS/SMB. This name will also be used in various alerts that this device will send out.

Hostname: nas-10-1A-17

Default Gateway

The default gateway specifies the IP address of the system/router that network requests out of the current subnet will get routed to.

Default gateway: 192.168.77.1

DNS Settings

DNS, or Domain Name Service, provides a means to translate hostnames to IP addresses. Enter the DNS IP addresses here.

Domain name server 1: 192.168.77.1

Domain name server 2:

Domain name server 3:

Domain name:

► HOSTNAME

The Hostname you specify is used to advertise the ioSafe R4 on your network. You can use the hostname to address the ioSafe R4 in place of the IP address when accessing the ioSafe R4 from Windows, or over OS X using SMB. This is also the name that will appear in the RAIDar scan list.

The default hostname is **nas-** followed by the last three bytes of your primary MAC address.

► DEFAULT GATEWAY

The Default Gateway specifies the IP address of the system where your network traffic is routed to if the destination is outside of your subnet. In most homes and smaller offices, this is the IP address of the router connected to the cable modem or your DSL service.

If you had selected the DHCP option in the Ethernet tab, the Default Gateway field will be automatically populated with the setting from your DHCP server. If you had selected the Static option, you can manually specify the IP addresses of the default gateway server here.

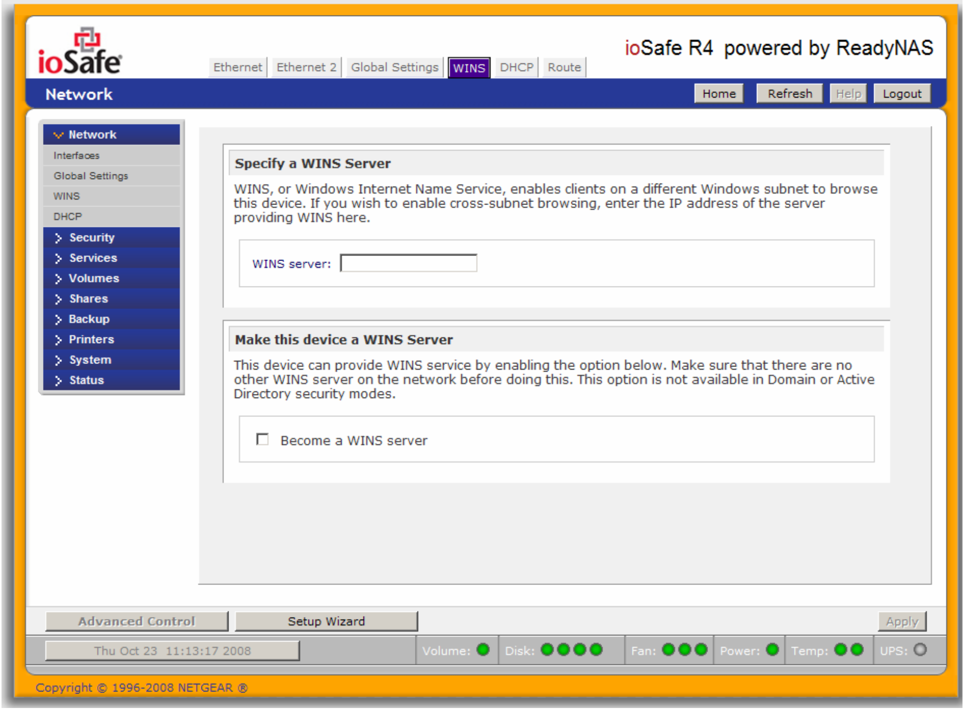
► DNS

The DNS box allows you to specify up to three Domain Name Service servers for host name resolution. If you are unfamiliar with DNS, the service translates host names into IP addresses.

If you had selected the DHCP option in the Ethernet tab, the domain name server fields will be automatically populated with the DNS settings from your DHCP server. If you had selected the Static option, you can manually specify the IP addresses of the DNS servers and the domain name here.

WINS

The WINS option allows you to specify the IP address of the WINS (Windows Internet Naming Service) server. A WINS server is typically a Windows server on the network that will allow the ioSafe R4 or other devices on the network to be (Windows) browsed from other subnets.



Specify a WINS Server

WINS, or Windows Internet Name Service, enables clients on a different Windows subnet to browse this device. If you wish to enable cross-subnet browsing, enter the IP address of the server providing WINS here.

WINS server:

Make this device a WINS Server

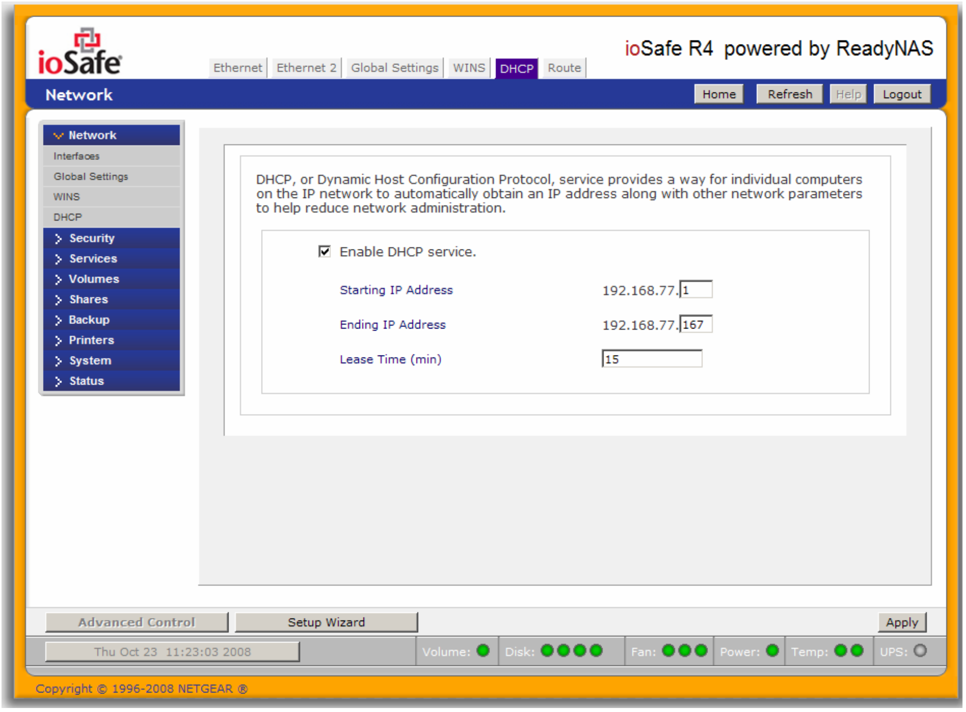
This device can provide WINS service by enabling the option below. Make sure that there are no other WINS server on the network before doing this. This option is not available in Domain or Active Directory security modes.

☐ Become a WINS server

If you do not have an existing WINS server, you can designate the ioSafe R4 to be one. Simply select the **Become a WINS server** checkbox and configure your Windows PC to specify the ioSafe R4 IP address as the WINS server. This can be useful if you wish to browse by hostname across multiple subnets, i.e. over VPN.

DHCP

The DHCP tab allows this device to act as a DHCP (Dynamic Host Configuration Protocol) server. DHCP service simplifies management of a network by dynamically assigning IP addresses to new clients on the network.



DHCP, or Dynamic Host Configuration Protocol, service provides a way for individual computers on the IP network to automatically obtain an IP address along with other network parameters to help reduce network administration.

☑ Enable DHCP service.

Starting IP Address 192.168.77.1

Ending IP Address 192.168.77.167

Lease Time (min) 15

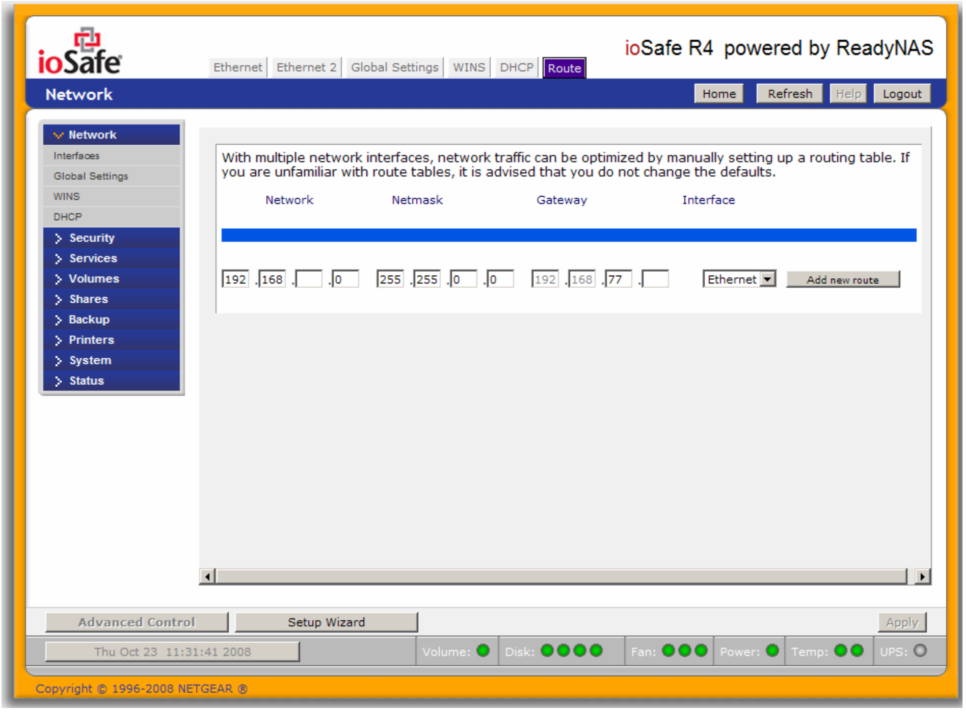
Click on the **Enable DHCP service** checkbox if you want the ioSafe R4 device to act as a DHCP server. This is convenient in networks where DHCP service is not already available.

Note

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

Route

The **Route** tab is available if you have two or more network interfaces (Ethernet or Wireless combined) on your ioSafe R4. In some environments, you can optimize your network traffic by manually setting up a routing table.



With multiple network interfaces, network traffic can be optimized by manually setting up a routing table. If you are unfamiliar with route tables, it is advised that you do not change the defaults.

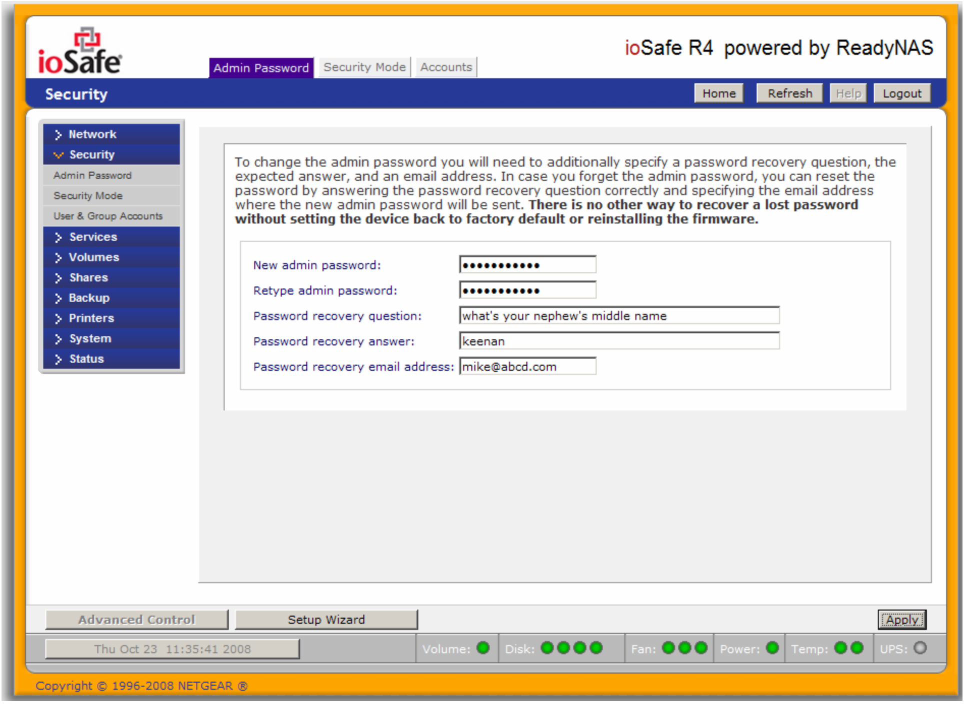
Network	Netmask	Gateway	Interface
192.168. .0	255.255.0.0	192.168.77.	Ethernet

Route table management is beyond the scope of this manual, and this option is provided only for advanced users who understand routing and wish to deviate from the default routes.

Security

Admin Password

The **Admin Password** tab allows you to change the **admin** user password. The **admin** user is the only user that can access FrontView and this user has administrative privileges when accessing shares. Be sure to set a password different from the default password and make sure this password is kept in a safe place. Anyone who obtains this password can effectively change or erase the data on the ioSafe R4. The default **admin** user password is "iosafe1" .



To change the admin password you will need to additionally specify a password recovery question, the expected answer, and an email address. In case you forget the admin password, you can reset the password by answering the password recovery question correctly and specifying the email address where the new admin password will be sent. **There is no other way to recover a lost password without setting the device back to factory default or reinstalling the firmware.**

New admin password:	●●●●●●●●●●●
Retype admin password:	●●●●●●●●●●●
Password recovery question:	what's your nephew's middle name
Password recovery answer:	keenan
Password recovery email address:	mike@abcd.com

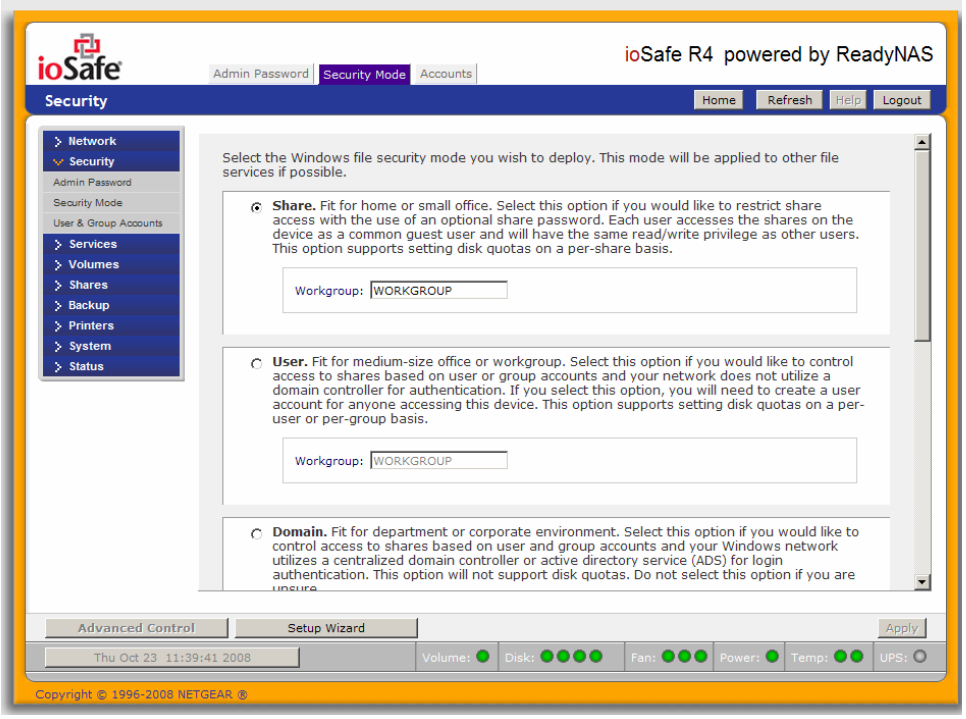
Note

In User or Domain security mode, you can use the **admin** account to login to a Windows share, and perform maintenance on any file or folder in that share. The admin user also has permission to access all user private home shares to perform backups.

As a safeguard, you will be requested to enter a password recovery question, the expected answer, and an email address. If, in the future, you forget the password, you can go to [https://*ip_address*/password_recovery](https://ip_address/password_recovery). Successfully answering the questions there will reset the admin password, and that new password will be sent to the email address you enter in this tab.

Security Mode Selection

The ioSafe R4 device offers three security options for your network environment. Read the quick overview below to help select the most appropriate option based on the required level of security and your current network authentication scheme.



Select the Windows file security mode you wish to deploy. This mode will be applied to other file services if possible.

● **Share.** Fit for home or small office. Select this option if you would like to restrict share access with the use of an optional share password. Each user accesses the shares on the device as a common guest user and will have the same read/write privilege as other users. This option supports setting disk quotas on a per-share basis.

Workgroup: WORKGROUP

○ **User.** Fit for medium-size office or workgroup. Select this option if you would like to control access to shares based on user or group accounts and your network does not utilize a domain controller for authentication. If you select this option, you will need to create a user account for anyone accessing this device. This option supports setting disk quotas on a per-user or per-group basis.

Workgroup: WORKGROUP

○ **Domain.** Fit for department or corporate environment. Select this option if you would like to control access to shares based on user and group accounts and your Windows network utilizes a centralized domain controller or active directory service (ADS) for login authentication. This option will not support disk quotas. Do not select this option if you are unsure.

The Share security mode is suitable for most home and small office environments, providing a simple way for people in a trusted environment to share files without the necessity of setting up separate user and group accounts. Shares that you create in this environment can be password-protected if desired.

A more appropriate selection for the medium-size office or workgroup environment is the User security mode. This mode allows you to set up user and group accounts to allow for more specific share access restrictions. Access to shares requires proper login authentication, and you can specify which users and/or groups you wish to offer access. As an example, you may want to restrict company financial data to just users belonging to one particular group. In this security mode, the administrator will need to set up and maintain user and group accounts on the ioSafe R4 device itself. In addition, each user account will be automatically set up with a private home share on the ioSafe R4.

The Domain security mode is most appropriate for larger department or corporate environments, where a centralized Windows-based domain controller or active directory server is present. The ioSafe R4 device integrates in this environment by creating a trusted relationship with the domain/ADS authentication server and allowing all user authentications to occur there, eliminating the need for separate account administration on the device itself. Also, in this security mode, each domain/ADS user will be automatically set up with a private home share on the ioSafe R4.

Note

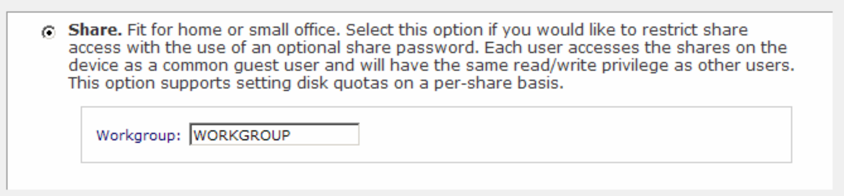
The FrontView management system will slow down in proportion to the number of users in the domain. It is not advisable to use the ioSafe R4 in a domain environment with more than 1000 users.

Share Security Mode

The **Share security mode** is the easiest security option to set up.

► SPECIFY A WORKGROUP

You only need to specify a workgroup if you wish to change it from the default.



● **Share.** Fit for home or small office. Select this option if you would like to restrict share access with the use of an optional share password. Each user accesses the shares on the device as a common guest user and will have the same read/write privilege as other users. This option supports setting disk quotas on a per-share basis.

Workgroup: WORKGROUP

A valid workgroup name must conform to the following restrictions:

- Name must consist of characters a-z, A-Z, 0-9, and the symbols _ (underscore), – (dash), and . (period).
- Name must start with a letter.
- Name length must be 15 characters or less.

► SHARE ACCOUNTS

You will notice the Accounts tab which consists of share accounts which match the current share names on the ioSafe R4. These share accounts are listed to allow you the option of changing the UID and quota assigned to the share. The share quota can be changed from the Share Listing in the Share menu as well. The UID does not need to be changed unless you wish to avoid a UID conflict with an existing NFS user.

User Security Mode

In User security mode, you specify a workgroup name just as you would in the previous security option, and create user and group accounts. You will have control over how much disk space is allocated for each user or group.

In this security mode, each user will be given a home share on the ioSafe R4 device that the user can use to keep private data such as backups of the user's PC. This home share is accessible only by that user and the administrator who needs the privilege to perform backups of these private shares. The option to automatically generate the private home share is controlled in the Accounts/Preferences tab, and you can disable it if you wish.

Note

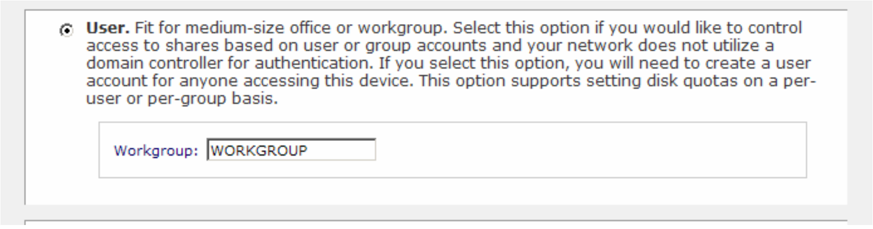
Private user shares are only accessible by users using CIFS (Windows) or AppleTalk file protocols.

To set up the ioSafe R4 for this security mode, you will need the following information:

- Workgroup name
- Group names you wish to create (i.e. Marketing, Sales, Engineering)
- User names you wish to create (plus email addresses if you will be setting disk quotas)
- Amount of disk space you would like to allocate to users and groups (optional)

► SPECIFY A WORKGROUP

To change or set a workgroup name, enter the desired name in the Workgroup field in the User option box. The name can be the workgroup name that is already used on your Windows network.



● **User.** Fit for medium-size office or workgroup. Select this option if you would like to control access to shares based on user or group accounts and your network does not utilize a domain controller for authentication. If you select this option, you will need to create a user account for anyone accessing this device. This option supports setting disk quotas on a per-user or per-group basis.

Workgroup: WORKGROUP

► SETTING UP ACCOUNTS

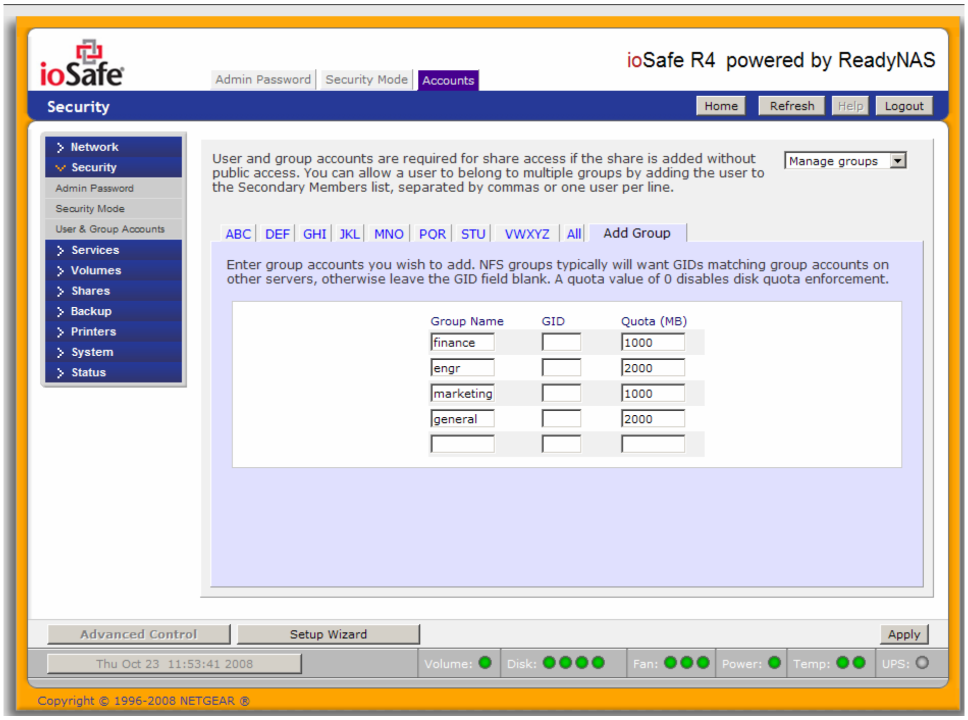
In this security mode, the Accounts tab allows you to manage user and group accounts on the ioSafe R4. A good starting point would be to select the **Manage groups** option from the drop-down box in the upper right corner.

▶ MANAGING GROUPS

To add a new group, click on the Add Group tab if it is not already selected. You can add up to five groups at a time. If you expect to have just one big set of users for one group, you can forego adding a new group and accept the default **users** group.

If desired, a user can belong to multiple groups. Once you have created user accounts, you can specify secondary groups that the user can belong to. This allows for finer-grain settings for share access. For instance, you can have user **joe** in group **marketing** also belong to group **sales** so **joe** can access shares restricted to only **marketing** and **sales** groups.

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

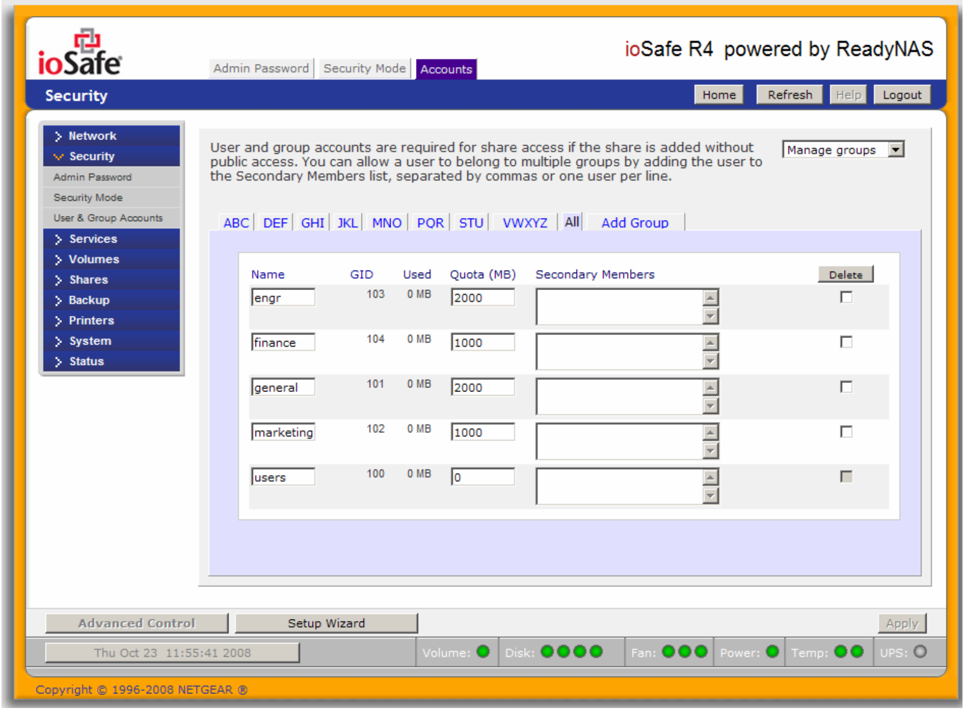


User and group accounts are required for share access if the share is added without public access. You can allow a user to belong to multiple groups by adding the user to the Secondary Members list, separated by commas or one user per line.

Enter group accounts you wish to add. NFS groups typically will want GIDs matching group accounts on other servers, otherwise leave the GID field blank. A quota value of 0 disables disk quota enforcement.

Group Name	GID	Quota (MB)
finance		1000
engr		2000
marketing		1000
general		2000

After adding your groups, you can view or change your groups by clicking on the alphabetical index tab, or **All** to list all groups.



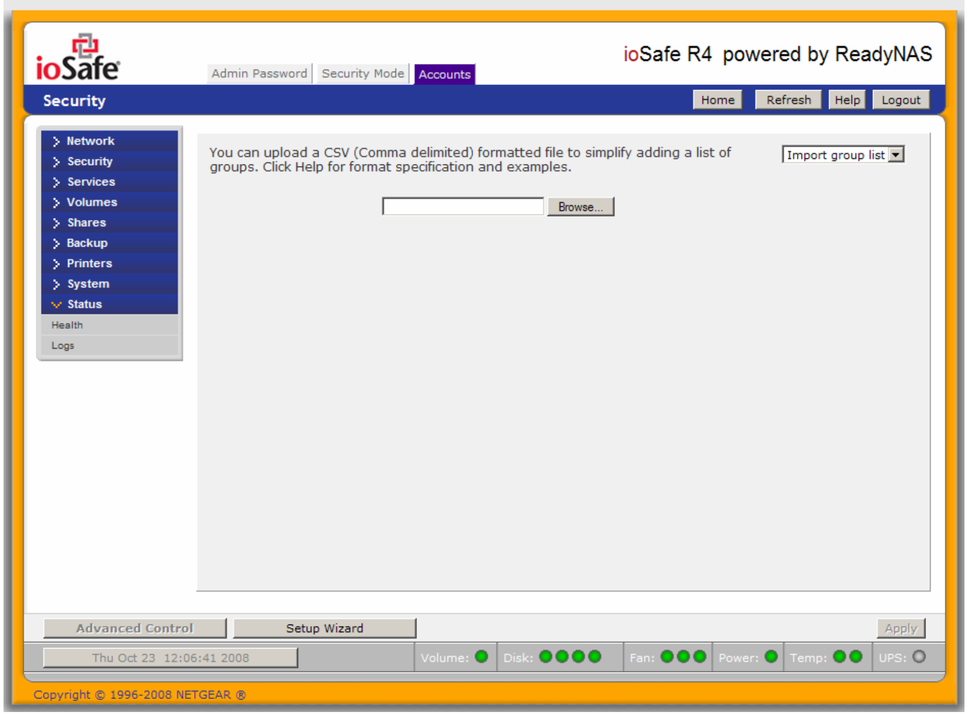
User and group accounts are required for share access if the share is added without public access. You can allow a user to belong to multiple groups by adding the user to the Secondary Members list, separated by commas or one user per line.

Name	GID	Used	Quota (MB)	Secondary Members	Delete
engr	103	0 MB	2000		☐
finance	104	0 MB	1000		☐
general	101	0 MB	2000		☐
marketing	102	0 MB	1000		☐
users	100	0 MB	0		☐

Thu Oct 23 11:55:41 2008

Copyright © 1996-2008 NETGEAR ®

If you wish to add a large number of groups, select **Import group list** from the selection box.



You can upload a CSV (Comma delimited) formatted file to simplify adding a list of groups. Click Help for format specification and examples.

Thu Oct 23 12:06:41 2008

Copyright © 1996-2008 NETGEAR ®

Here, you can upload a CSV (Comma Separated Value) formatted file containing the group account information. The format of the file is:

```
name1,gid1,quota1,member11:member12:member13
name2,gid2,quota2,member21:member22:member23
name3,gid3,quota3,member31:member32:member33
```

Please note the following:

- Spaces around commas are ignored.
- The name fields are required.
- Quota will be set to default if not specified.
- GID will be automatically generated if not specified.
- Empty fields are replaced with accounts defaults.
- Group members are optional.

Examples of acceptable formats are as follows (note that you can omit follow-on commas and fields if you wish to accept the system defaults for those fields, or you can leave the fields empty):

```
flintstones
```

In this example, group **flintstones** will be created with an automatically assigned GID, and default quota.

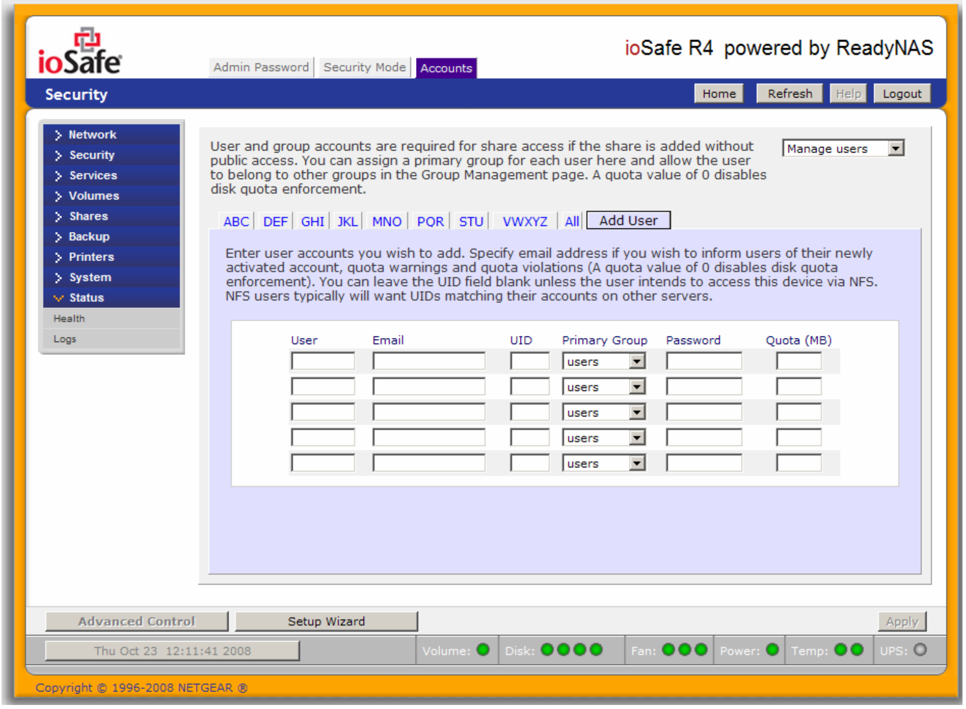
```
rubble,1007,5000,barney:betty
```

In this example, group **rubble** will have GID 1007, quota of 5000 MB, with members **barney** and **betty**.

▶ MANAGING USERS

To manage user accounts, select the Manage users option in the drop-down box.

To add a user, click on the Add User tab. You can add up to five users at a time.



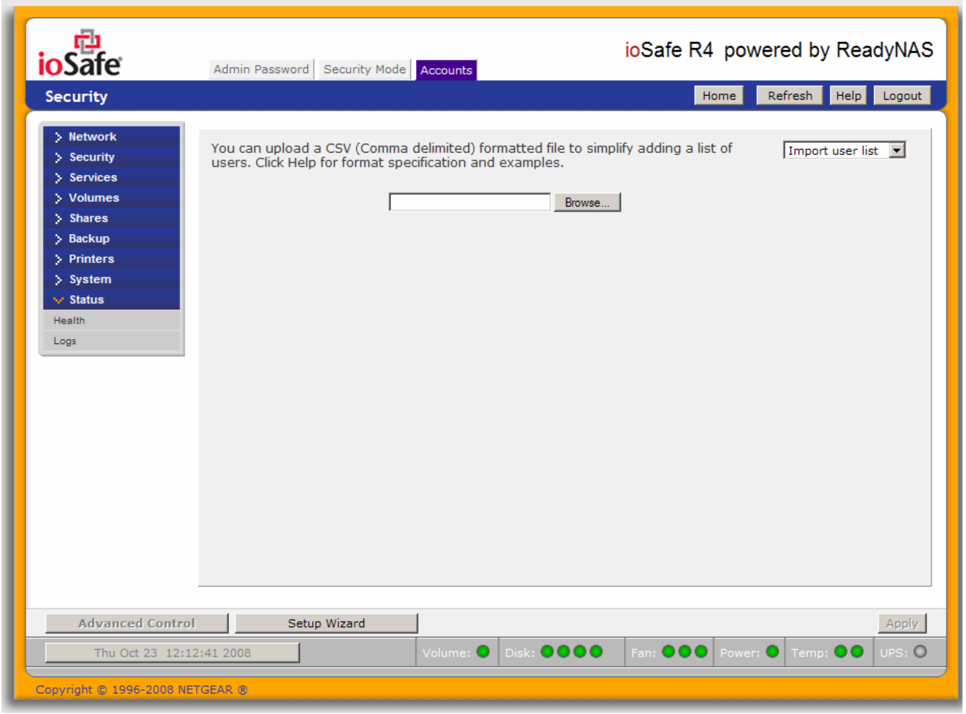
User and group accounts are required for share access if the share is added without public access. You can assign a primary group for each user here and allow the user to belong to other groups in the Group Management page. A quota value of 0 disables disk quota enforcement.

Enter user accounts you wish to add. Specify email address if you wish to inform users of their newly activated account, quota warnings and quota violations (A quota value of 0 disables disk quota enforcement). You can leave the UID field blank unless the user intends to access this device via NFS. NFS users typically will want UIDs matching their accounts on other servers.

User	Email	UID	Primary Group	Password	Quota (MB)
			users		
			users		
			users		
			users		
			users		

You can enter a user name, email address, user ID, select a group, password, and disk quota for the user. Only the user name and password fields are required, however, you should specify the user email address if you intend to set up disk quotas. Without an email address, the user will not be warned when disk usage approaches the specified disk quota limit. If you do not wish to assign a disk quota, enter 0.

If you wish to add a large number of users, select **Import user list** from the selection box.



You can upload a CSV (Comma delimited) formatted file to simplify adding a list of users. Click Help for format specification and examples.

Here, you can upload a CSV (Comma Separated Value) formatted file containing the user account information. The format of the file is:

```
name1,password1,group1,email1,uid1,quota1
name2,password2,group2,email2,uid2,quota2
name3,password3,group3,email3,uid3,quota3
```

Please note the following:

- Spaces around commas are ignored.
- The name and password fields are required.
- If a listed group account does not exist, it will be automatically created.
- Group and quota will be set to the defaults if not specified.
- Email notification will not be sent to the user if the field is ommitted or left blank.
- UID will be automatically generated if not specified.
- Empty fields are replaced with accounts defaults.

Examples of acceptable formats are as follows (note that you can ommit follow-on commas and fields if you wish to accept the system defaults for those fields, or you can leave the fields empty):

```
fred,hello123
```

In this example, user **fred** will have password set to *hello123*, belongs to the default group, no email notification, automatic UID assigned, and default quota.

```
barney,23stone,,barney@bedrock.com
```

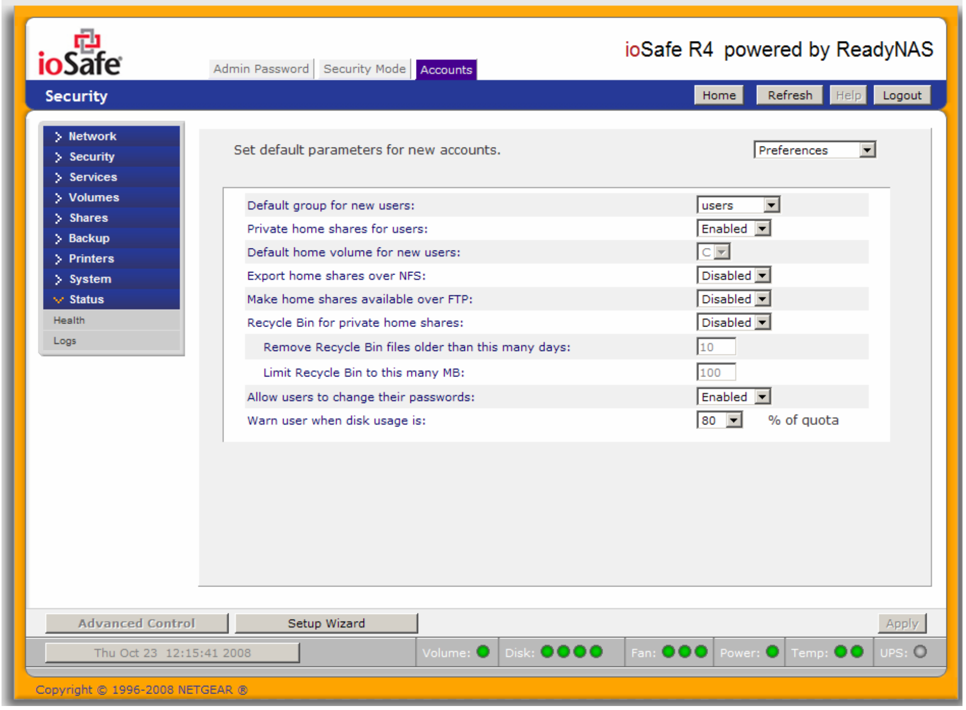
In this example, user **barney** will have password set to *23stone*, belongs to the default group, will be sent email notification to *barney@bedrock.com*, automatic UID assigned, and default quota.

```
wilma,imhiswif,ourgroup,wilma@bedrock.com,225,50
```

In this example, user **wilma** will have password *imhiswif*, belongs to group *ourgroup*, email notification sent to *wilma@bedrock.com*, UID set to *225*, and quota set to *50MB*.

► SETTING ACCOUNTS PREFERENCES

You can set various account defaults by selecting the Preferences option in the drop-down box.



Set default parameters for new accounts. Preferences

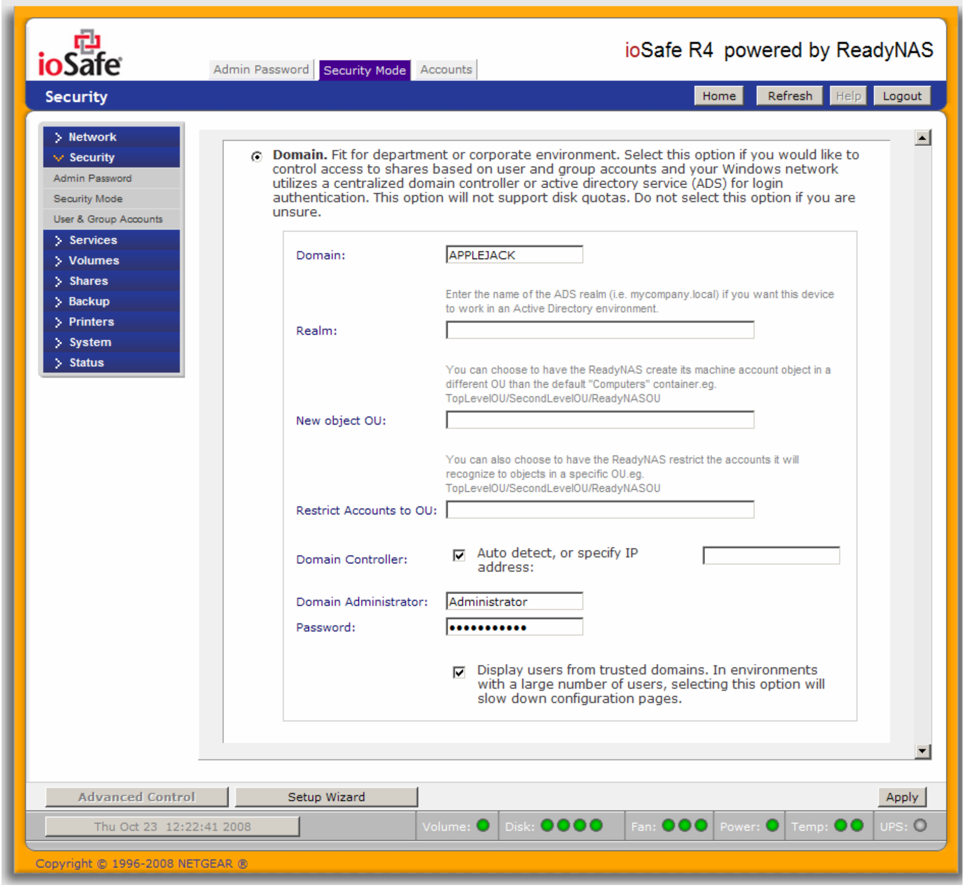
Default group for new users:	users
Private home shares for users:	Enabled
Default home volume for new users:	C
Export home shares over NFS:	Disabled
Make home shares available over FTP:	Disabled
Recycle Bin for private home shares:	Disabled
Remove Recycle Bin files older than this many days:	10
Limit Recycle Bin to this many MB:	100
Allow users to change their passwords:	Enabled
Warn user when disk usage is:	80 % of quota

Domain Security Mode

▶ DOMAIN/ADS AUTHENTICATION

If you choose the Domain security mode option, you will need to create a trusted relationship with the domain controller or the active directory server (ADS) that will act as the authentication server for the ioSafe R4 device. You will need the following information:

- Domain name
- Domain administrator login
- Domain administrator password
- If using ADS:
  - DNS name of the ADS realm
  - OU (Organization Unit). You can specify nested OU's by separating OU entries with commas. The lowest level OU must be specified first.



● **Domain.** Fit for department or corporate environment. Select this option if you would like to control access to shares based on user and group accounts and your Windows network utilizes a centralized domain controller or active directory service (ADS) for login authentication. This option will not support disk quotas. Do not select this option if you are unsure.

Domain: APPLEJACK

Enter the name of the ADS realm (i.e. mycompany.local) if you want this device to work in an Active Directory environment.

Realm:

You can choose to have the ReadyNAS create its machine account object in a different OU than the default "Computers" container.eg. TopLevelOU/SecondLevelOU/ReadyNASOU

New object OU:

You can also choose to have the ReadyNAS restrict the accounts it will recognize to objects in a specific OU.eg. TopLevelOU/SecondLevelOU/ReadyNASOU

Restrict Accounts to OU:

Domain Controller: ☑ Auto detect, or specify IP address:

Domain Administrator: Administrator

Password: •••••••••••

☑ Display users from trusted domains. In environments with a large number of users, selecting this option will slow down configuration pages.

You can elect to have the ioSafe R4 automatically auto-detect the domain controller, or you can specify the IP address. Sometimes auto-detect will fail, and you will need to supply the IP address of the domain controller to join the domain.

If you have a large number of users in your domain, you may need to deselect the **Display users from trusted domains**… checkbox. Otherwise, FrontView management system may slow down to an unusable state.

Note

Use of the ioSafe R4 in a domain environment with more than 1000 users is not recommended at this time.

Click Apply to join the domain. If successful, users and groups from the domain will have login access to the shares on this device.

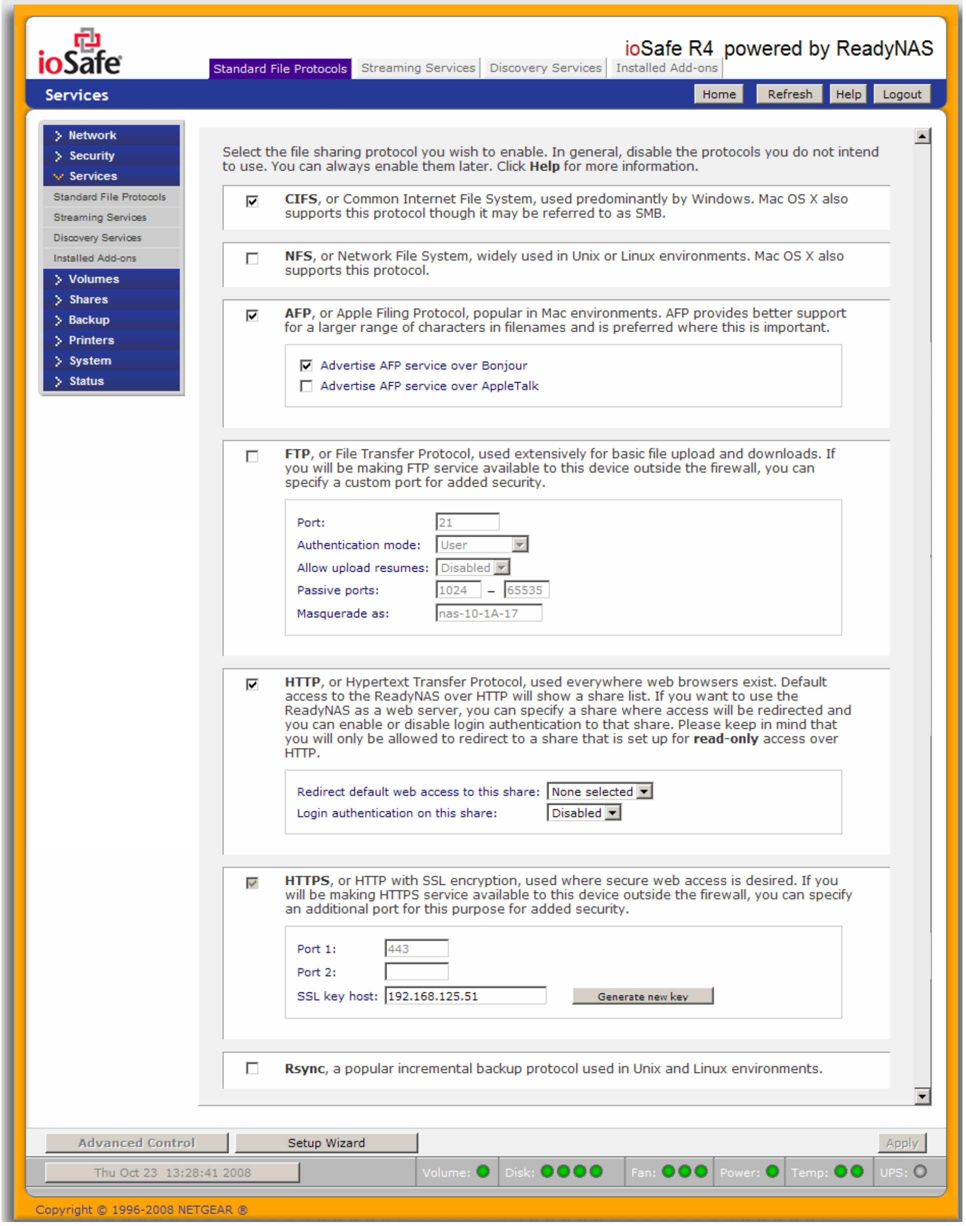
► SETTING UP ACCOUNTS

Accounts are managed on the domain controller. The ioSafe R4 simply pulls the account information from the controller and displays them in the Accounts tab if you have the **Display users from trusted domains…** option enabled.

If you wish, you can assign a disk quota to the domain users and groups. If email addresses are specified, users will be automatically notified when approaching and reaching their quotas.

Services

The Services menu allows you to manage various services for share access. This in effect controls the type of clients you wish to allow access to the ioSafe R4.



Select the file sharing protocol you wish to enable. In general, disable the protocols you do not intend to use. You can always enable them later. Click **Help** for more information.

☑ **CIFS**, or Common Internet File System, used predominantly by Windows. Mac OS X also supports this protocol though it may be referred to as SMB.

☐ **NFS**, or Network File System, widely used in Unix or Linux environments. Mac OS X also supports this protocol.

☑ **AFP**, or Apple Filing Protocol, popular in Mac environments. AFP provides better support for a larger range of characters in filenames and is preferred where this is important.

- ☑ Advertise AFP service over Bonjour
- ☐ Advertise AFP service over AppleTalk

☐ **FTP**, or File Transfer Protocol, used extensively for basic file upload and downloads. If you will be making FTP service available to this device outside the firewall, you can specify a custom port for added security.

Port: 21
Authentication mode: User
Allow upload resumes: Disabled
Passive ports: 1024 – 65535
Masquerade as: nas-10-1A-17

☑ **HTTP**, or Hypertext Transfer Protocol, used everywhere web browsers exist. Default access to the ReadyNAS over HTTP will show a share list. If you want to use the ReadyNAS as a web server, you can specify a share where access will be redirected and you can enable or disable login authentication to that share. Please keep in mind that you will only be allowed to redirect to a share that is set up for **read-only** access over HTTP.

Redirect default web access to this share: None selected
Login authentication on this share: Disabled

☑ **HTTPS**, or HTTP with SSL encryption, used where secure web access is desired. If you will be making HTTPS service available to this device outside the firewall, you can specify an additional port for this purpose for added security.

Port 1: 443
Port 2:
SSL key host: 192.168.125.51

☐ **Rsync**, a popular incremental backup protocol used in Unix and Linux environments.

Thu Oct 23 13:28:41 2008

Copyright © 1996-2008 NETGEAR ®

You will notice three tabs at the top: **Standard File Protocols**, **Streaming Services**, and **Discovery Services**. These different services are explained below.

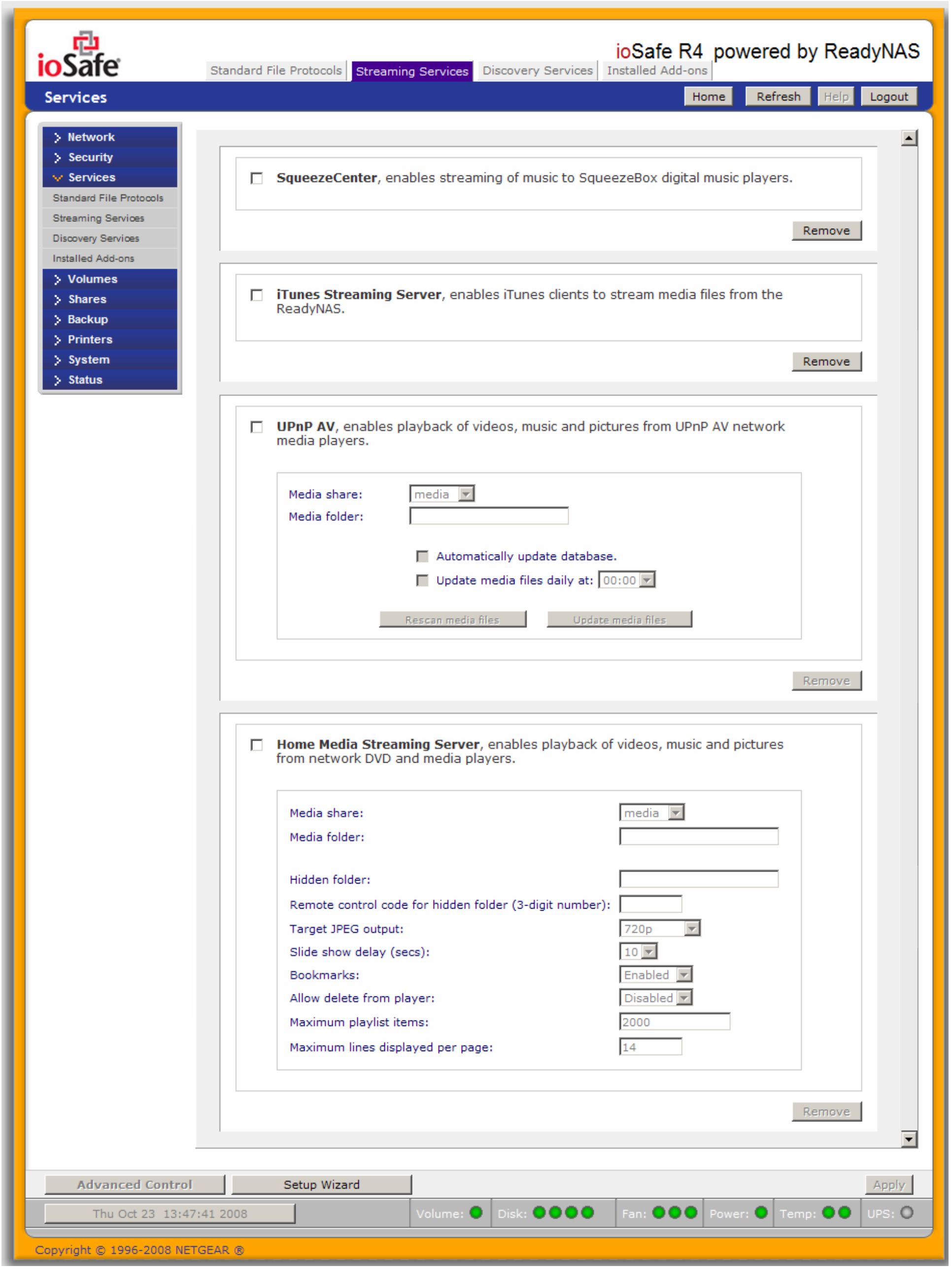
Standard File Protocols

The standard file protocols are common file sharing services that allow your workstation clients file transfer to and from the ioSafe R4 using built-in file manager over network file protocols on the client operating system. The available services are:

- **CIFS** (Common Internet File Service). Sometimes referred to as SMB. This protocol is used mainly by Microsoft Windows clients, and sometimes used by Mac OS X clients. Under Windows, when you click on My Network Places or Network Neighborhood, you're going across CIFS. This service is enabled by default and cannot be disabled.
- **NFS** (Network File Service.) NFS is used by Linux and Unix clients. Mac OS 9/X users can access NFS shares as well through console shell access. The ioSafe R4 supports NFS v3 over UDP and TCP.
- **AFP** (Apple File Protocol). Mac OS 9 and OS X works best using this protocol as it handles an extensive character set. The ioSafe R4 supports AFP 3.1.
- **FTP** (File Transfer Protocol). Widely used in public file upload and download sites. The ioSafe R4 supports anonymous or user access for FTP clients, regardless of the security mode selected. If you wish, you can elect to set up port-forwarding to non-standard ports for better security when accessing files over the Internet.
- **HTTP** (Hypertext Transfer Protocol). Used by web browsers. The ioSafe R4 supports HTTP file manager, allowing web browsers to read and write to shares using the web browser. This service can be disabled in lieu of HTTPS to allow for a more secure transmission of passwords and data. With the option to redirect default web access to a specified share, you can transparently force access to http://*iosafe_ip* to http://*iosafe_ip*/*share* . This is useful if you do not want to expose your share listing to outsiders as well as allowing you to redirect all default web access to a share dedicated to be your website. All you need in the target share is an index file such as **index.htm** or **index.html**. You have the option of enabling or disabling login authentication to this share.
- **HTTPS** (HTTP with SSL encryption). This service is enabled by default and cannot be disabled. Access to FrontView is strictly through HTTPS for this reason. If you want remote web access to FrontView or your HTTPS shares, you have the option of specifying a non-standard port that you can forward on your router for better security. You can also regenerate the SSL key based on the hostname or IP address that users will address the ioSafe R4. This allows you to bypass the default dummy certificate warnings whenever you access the ioSafe R4 over HTTPS.
- **Rsync**. An extremely popular and efficient form of incremental backup made popular in the Linux platform but is now available for various other Unix systems as well as Windows and Mac. Enabling rsync service on the ioSafe R4 will allow clients to use rsync to initiate backups to and from the ioSafe R4.

Streaming Services

The built-in streaming services on the ioSafe R4 allow you to stream multi-media content directly from the ioSafe R4, without the need to have your PC or Mac powered on.



□ **SqueezeCenter**, enables streaming of music to SqueezeBox digital music players.

□ **iTunes Streaming Server**, enables iTunes clients to stream media files from the ReadyNAS.

□ **UPnP AV**, enables playback of videos, music and pictures from UPnP AV network media players.

Media share: media
Media folder:
□ Automatically update database.
□ Update media files daily at: 00:00

□ **Home Media Streaming Server**, enables playback of videos, music and pictures from network DVD and media players.

Media share: media
Media folder:
Hidden folder:
Remote control code for hidden folder (3-digit number):
Target JPEG output: 720p
Slide show delay (secs): 10
Bookmarks: Enabled
Allow delete from player: Disabled
Maximum playlist items: 2000
Maximum lines displayed per page: 14

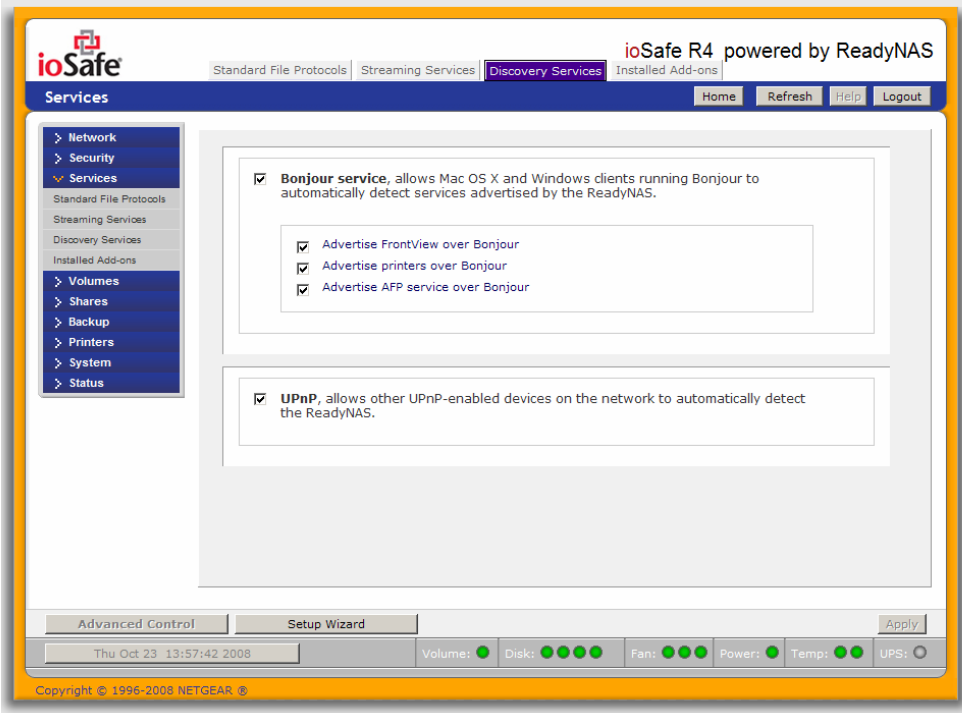
Thu Oct 23 13:47:41 2008 Volume: ● Disk: ●●●● Fan: ●●● Power: ● Temp: ●● UPS: ○

Copyright © 1996-2008 NETGEAR ®

- **SquezeCenter** (SlimServer) provides music streaming to the popular Squeezebox music players from Slim Devices.
- **iTunes Streaming Server** enables iTunes clients to stream media files straight from the ioSafe R4.
- **UPnP AV** provides media streaming service to stand-alone networked home media adapters and networked DVD players that support the UPnP AV protocol or are Digital Living Network Alliance (DLNA) standard compliant. The ioSafe R4 comes with a reserved *media* share that is advertised and recognized by the players. Simply copy your media files to the Videos, Music, and Pictures folders in that share to display them on your player. If you wish, you can specify a different media path where your files reside.

- **Home Media Streaming Server** provides streaming of videos, music, and pictures to popular networked DVD players. The streaming players often utilize the streaming client developed by Syabas. Similar to UPnP AV, this service is used to stream videos, music, and pictures from the reserved *media* share to these adapters. If you wish to change the location where the media files are stored, you can specify a different share and folder path. Note that this path is shared between the UPnP AV and this service.

Discovery Services



☑ **Bonjour service**, allows Mac OS X and Windows clients running Bonjour to automatically detect services advertised by the ReadyNAS.

☑ Advertise FrontView over Bonjour

☑ Advertise printers over Bonjour

☑ Advertise AFP service over Bonjour

☑ **UPnP**, allows other UPnP-enabled devices on the network to automatically detect the ReadyNAS.

- **Bonjour Service** provides a simple way of discovering various services on the ioSafe R4. Bonjour currently provides an easy way to connect to FrontView, IPP Printing, and AFP services. OS X has built-in Bonjour support and you can download Bonjour for Windows from Apple's website.
- **UPnP** provides a means for UPnP-enabled clients to discover the ioSafe R4 on your LAN.

Volume Management

The ioSafe R4 consists of two RAID volume technologies – **Flex-RAID**, utilizing the industry-standard RAID levels 0, 1, and 5, and **X-RAID**, NETGEAR-patented expandable RAID technology. Your system defaults to **X-RAID**, however, you can switch between the two modes through a factory default reset process described in **Chapter 4 – System Reset Switch**.

There are advantages to both technologies.

► ADVANTAGES OF FLEX-RAID

1. The default volume can be deleted and recreated, with or without the snapshot reserved space.
2. Hot spare disk is supported.
3. Full volume management is available – you can create a volume utilizing RAID level 0, 1, or 5, specify the size of the volume, delete a disk from a volume, assign a hot spare, etc.
4. Multiple volumes are supported, each with a different RAID level, snapshot schedule and disk quota definition.
5. Each disk can be replaced, one by one, then rebuilt; after the last disk is replaced, another data volume utilizing the newly added capacity can be configured.

► ADVANTAGES OF X-RAID

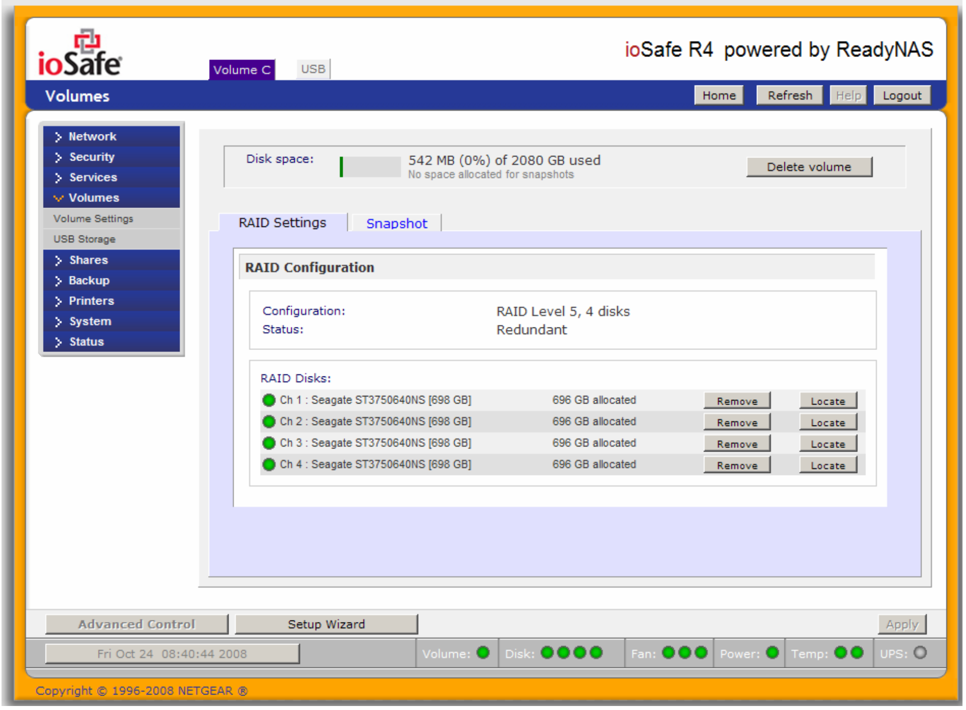
1. One volume technology, but supports volume expansion, either by adding more disks or by replacing existing disk with larger capacity disks.
2. You can start out with one disk, and add up to 3 more disks when you need them or can afford them.
3. Volume management is automatic. Add a 2nd disk; it becomes a mirror to the 1st. Add a 3rd, your capacity doubles; add a 4th, and your capacity triples – the expansion occurring while maintaining redundancy.
4. At a future point in time, each disk can be replaced one by one, have it finish rebuilding, and after the last disk is replaced, your volume automatically expands utilizing the new capacity.

Volume Management for Flex-RAID

If you wish to reconfigure the default volume C, wish to split it into multiple volumes, or specify a different RAID level, you will need to reconfigure your volume. The first step is to delete the existing volume you wish to replace.

▶ DELETING A VOLUME

To delete a volume, click on the volume tab of the volume you wish to delete or Volume C if only one volume is configured. Make sure if you have data in that volume that you back up the files you wish to keep first. All shares, files, and snapshots residing on that volume **WILL BE DELETED AND ARE NON-RECOVERABLE!**



Disk space: 542 MB (0%) of 2080 GB used
No space allocated for snapshots

RAID Configuration

Configuration: RAID Level 5, 4 disks
Status: Redundant

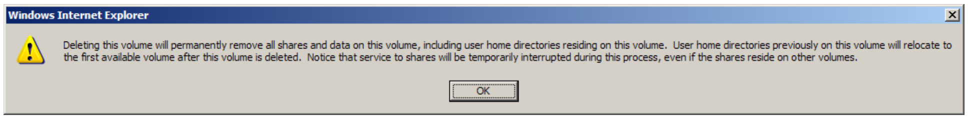
RAID Disks:

● Ch 1 : Seagate ST3750640NS [698 GB]	696 GB allocated	Remove	Locate
● Ch 2 : Seagate ST3750640NS [698 GB]	696 GB allocated	Remove	Locate
● Ch 3 : Seagate ST3750640NS [698 GB]	696 GB allocated	Remove	Locate
● Ch 4 : Seagate ST3750640NS [698 GB]	696 GB allocated	Remove	Locate

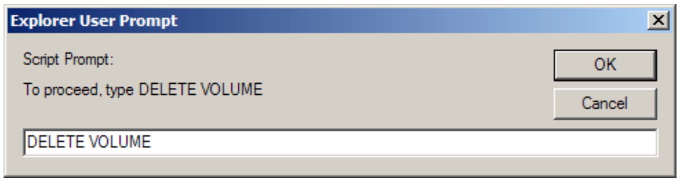
Fri Oct 24 08:40:44 2008

Click **Delete Volume** in the Volume C tab.

You will be asked to confirm your intention by typing: **`DELETE VOLUME`**



Deleting this volume will permanently remove all shares and data on this volume, including user home directories residing on this volume. User home directories previously on this volume will relocate to the first available volume after this volume is deleted. Notice that service to shares will be temporarily interrupted during this process, even if the shares reside on other volumes.

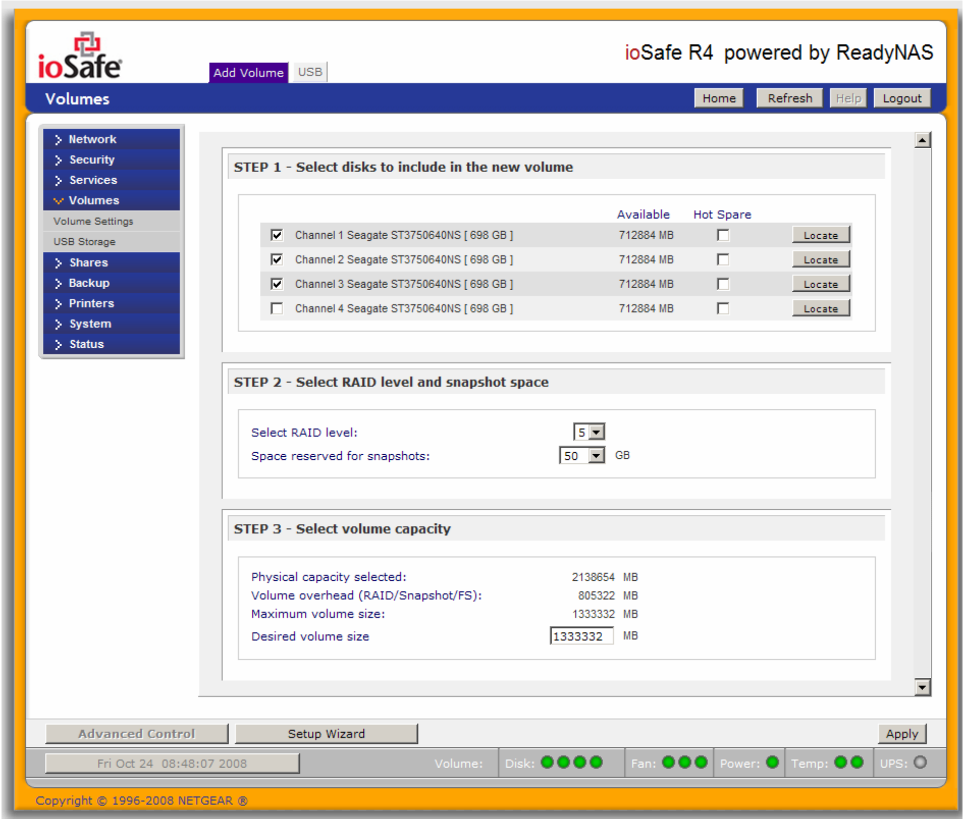


Script Prompt:

To proceed, type DELETE VOLUME

DELETE VOLUME

You will then be presented with the **Add Volume** tab listing the available configurable space on the hard disks. All the disks will be selected by default. You can elect to specify a hot spare disk if you wish. A hot spare remains in standby mode and will automatically regenerate the data from a failed disk from the volume. A hot spare disk is only available for RAID level 1 and RAID level 5 if there are enough disks to fulfill the required minimum plus one.



STEP 1 - Select disks to include in the new volume

		Available	Hot Spare	
☑	Channel 1 Seagate ST3750640NS [698 GB]	712884 MB	□	Locate
☑	Channel 2 Seagate ST3750640NS [698 GB]	712884 MB	□	Locate
☑	Channel 3 Seagate ST3750640NS [698 GB]	712884 MB	□	Locate
□	Channel 4 Seagate ST3750640NS [698 GB]	712884 MB	□	Locate

STEP 2 - Select RAID level and snapshot space

Select RAID level: 5

Space reserved for snapshots: 50 GB

STEP 3 - Select volume capacity

Physical capacity selected:	2138654 MB
Volume overhead (RAID/Snapshot/FS):	805322 MB
Maximum volume size:	1333332 MB
Desired volume size	1333332 MB

Select Hard Disks

In our example here, we'll select the first three disks and elect not to specify any of them as a hot spare.

Select RAID level

RAID level determines how the redundancy, capacity utilization, and performance is implemented for the volume. See Appendix A, "RAID Levels Simplified", for more information. Typically in a three or more disk configuration, RAID level 5 is recommended.

In our example above, we selected RAID level 5 for the three selected disks.

Specify reserve space for snapshot

Next, select the amount of the volume you wish to allocate for snapshots. You can elect to specify 0 if you wish to disable snapshot capability, or you can specify a 5GB increment from 5 to 100GB.

This represents the amount of data you feel would be changing while the snapshot is active. This typically depends on how often you schedule your snapshot (see following section on snapshot), and the maximum amount of data (plus padding) you feel will change during that time. Make sure to allocate enough space for worse case as the snapshot becomes unusable when its reserved space runs out.

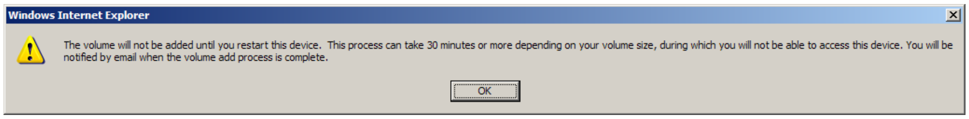
In our example above, we selected 50GB of the volume to be reserved for snapshots.

Specify desired volume size

After you've specified the above volume parameters, enter the desired volume size if you wish to configure a smaller volume size than the maximum displayed. The resulting volume will be approximately the size that is specified.

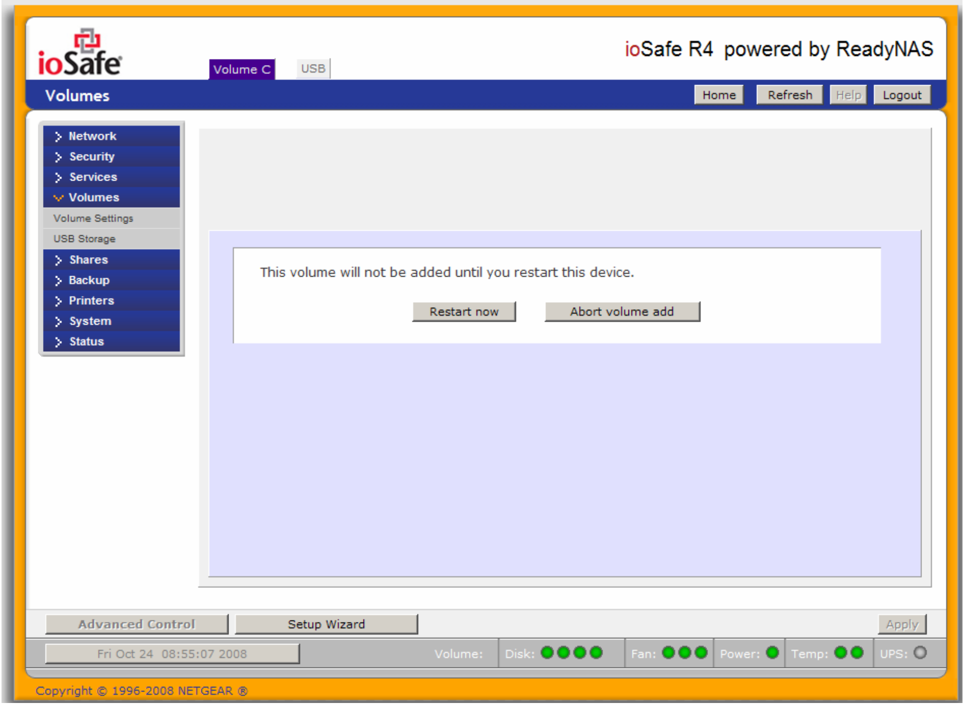
In our example above, we kept the maximum size that was calculated.

Click **Apply** and wait for the instruction to reboot the system. It typically takes about 1 minute before you are notified to reboot.



Windows Internet Explorer

The volume will not be added until you restart this device. This process can take 30 minutes or more depending on your volume size, during which you will not be able to access this device. You will be notified by email when the volume add process is complete.



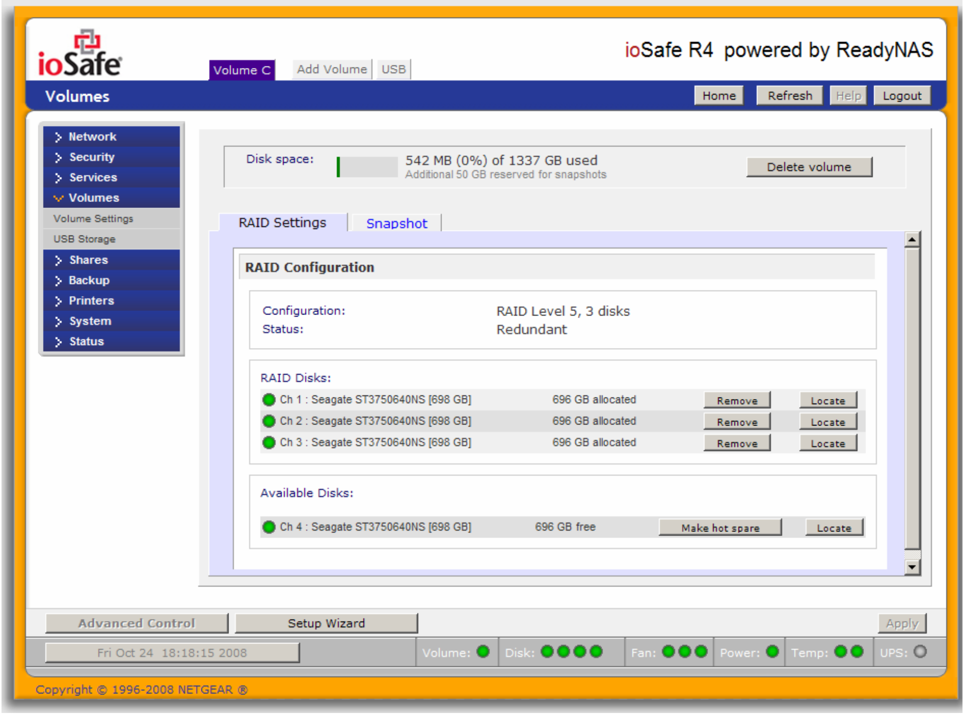
This volume will not be added until you restart this device.

After rebooting, you will then be notified by email when the volume has been added. Use RAIDar to reconnect to the NAS device.

► RAID SETTINGS

After you have added a volume, you can revisit the Volume tab and click on the **RAID Settings** tab to display the current RAID information and configuration options for the volume.

Notice the disk on channel 4 that we did not configure is listed in the Available Disks section. We can add this disk as a hot spare by clicking on the **Make hot spare** button.



Disk space: 542 MB (0%) of 1337 GB used
Additional 50 GB reserved for snapshots

RAID Configuration

Configuration: RAID Level 5, 3 disks
Status: Redundant

RAID Disks:

● Ch 1 : Seagate ST3750640NS [698 GB]	696 GB allocated	Remove	Locate
● Ch 2 : Seagate ST3750640NS [698 GB]	696 GB allocated	Remove	Locate
● Ch 3 : Seagate ST3750640NS [698 GB]	696 GB allocated	Remove	Locate

Available Disks:

● Ch 4 : Seagate ST3750640NS [698 GB]	696 GB free	Make hot spare	Locate

Fri Oct 24 18:18:15 2008

We can also remove a disk from the volume by clicking on the **Remove** button. The volume will still be available but in a non-redundant state. An additional disk failure would render this volume unusable.

Warning

The Remove operation is a maintenance feature and is not recommended in a live environment. Its function is equivalent to hot-removing the disk or simulating a disk failure.

The **Locate** option is a way to verify that a disk is correctly situated in the expected disk slot. Clicking on **Locate** will blink the LED of the disk for 15 seconds.

Volume Management for X-RAID

The X-RAID technology offers a simplified approach to volume management. X-RAID works on the premise that what most people want to do with their data volume over time is either adding redundancy or expanding it without the headaches usually associated with doing that. By using simple rules, X-RAID is able to hide all the complexities yet provide volume management features only previously available in enterprise-level storage solutions.

► X-RAID REDUNDANCY OVERHEAD

To maintain redundancy from disk failure, X-RAID requires a one-disk overhead. In a two-disk X-RAID volume, the usable capacity is one disk. In a three-disk X-RAID volume, the usable capacity is two disks. In a four-disk X-RAID volume, the usable capacity is three disks.

► X-RAID HAS ONE DATA VOLUME

X-RAID devices only have one data volume. This volume encompasses one to four disks, utilizing the capacity of the smallest disk from each disk. For instance, if you had one 80GB disk and two 250GB disks, only 80GB from each disk will be used in the volume. (The leftover space on the 250GB disks will be reclaimed only when the 80GB disk is replaced with a 250GB or greater capacity disk. See "Replacing All Your Disks for Even More Capacity" below.)

► ADDING A 2ND DISK FOR REDUNDANCY

A one-disk X-RAID device has no redundancy and provides no protection from a disk failure. However, if and when you feel the need for redundancy, simply power down the device, add a new disk with at least the capacity of the first disk, and power on. Depending on the size of the disk, within a few hours, your data volume will be fully redundant. The process occurs in the background, so access to the ioSafe R4 is not interrupted.

► ADDING A 3RD AND 4TH DISK FOR MORE CAPACITY

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

Not so with X-RAID. Simply power down the device, add the 3rd and perhaps 4th disk and power on. The X-RAID device will initialize and scan the newly added disk(s) for bad sectors in the background. You can continue working normally with the device during this process without any lag in performance. When the process finishes, you will be alerted by email to reboot the device.

During the boot process, your data volume is expanded. This process typically takes about 15-30 minutes per disk, perhaps more, depending on the size of your disks. A 250GB disk takes approximately 30 minutes. Access to the ioSafe R4 is not permitted during this time. You will be notified by email when the process is complete.

After you receive your email, the ioSafe R4 will have been expanded with the capacity from your new disk(s).

► REPLACING ALL YOUR DISKS FOR EVEN MORE CAPACITY

A couple years down the line, you find the need more disk space, and 1 TB disks are available at an attractive price. Again, you can expand your volume capacity quite easily, although you will need to power down several times to replace your old disks.

First, power down the ioSafe R4, replace the first disk with the larger capacity disk, and boot. The ioSafe R4 will detect that a new disk was put in place and will resync the disk with data from the removed disk. This process will take several hours, depending on disk capacity. The disk will be initialized and scanned for bad sectors first before the resync is started. The total time from the start of initialization to the end of resync can be around 5 hours or more, depending on disk capacity. You will be notified when this resync process is complete.

Upon completion, power down, replace the 2nd disk with another larger capacity disk, and boot. The process will be the same as the 1st disk. You will do this also for the 3rd and 4th disk.

Once you get the completion notification for the 4th disk, reboot the ioSafe R4. During boot, volume capacity is expanded with the additional capacity from each disk. For instance, if you had replaced four 250GB disks with four 600GB disks, the capacity of the volume will increase by approximately 350GB x 3 (the fourth disk is reserved for parity). The expansion process will take several hours depending on the capacity expanded, and you will be notified by email when the process is complete. There is no access to the ioSafe R4 during this time.

Changing Between X-RAID and Flex-RAID Modes

You can switch between X-RAID and Flex-X-RAID modes. The process involves setting the ioSafe R4 to factory default and using RAIDar to configure the volume during a 10-minute delay window during boot. Please see **Chapter 4 – System Reset Switch** for more information.

Snapshot

The Volume page offers the ability to schedule and take snapshots. You can visualize a snapshot as a frozen image of a volume at the time you take the snapshot. Snapshots are typically used for backups during which time the original volume can continue to operate normally. As primary storage becomes larger, offline backups tend to become increasingly difficult as backup time increases beyond offline hours. Snapshots allow backups to occur without taking systems offline.

Snapshots also can be used as temporary backups as well, perhaps as a means to backup data against viruses. As an example, if a file becomes infected with a virus on the NAS device, the uninfected file can be restored from a prior snapshot taken before the attack.

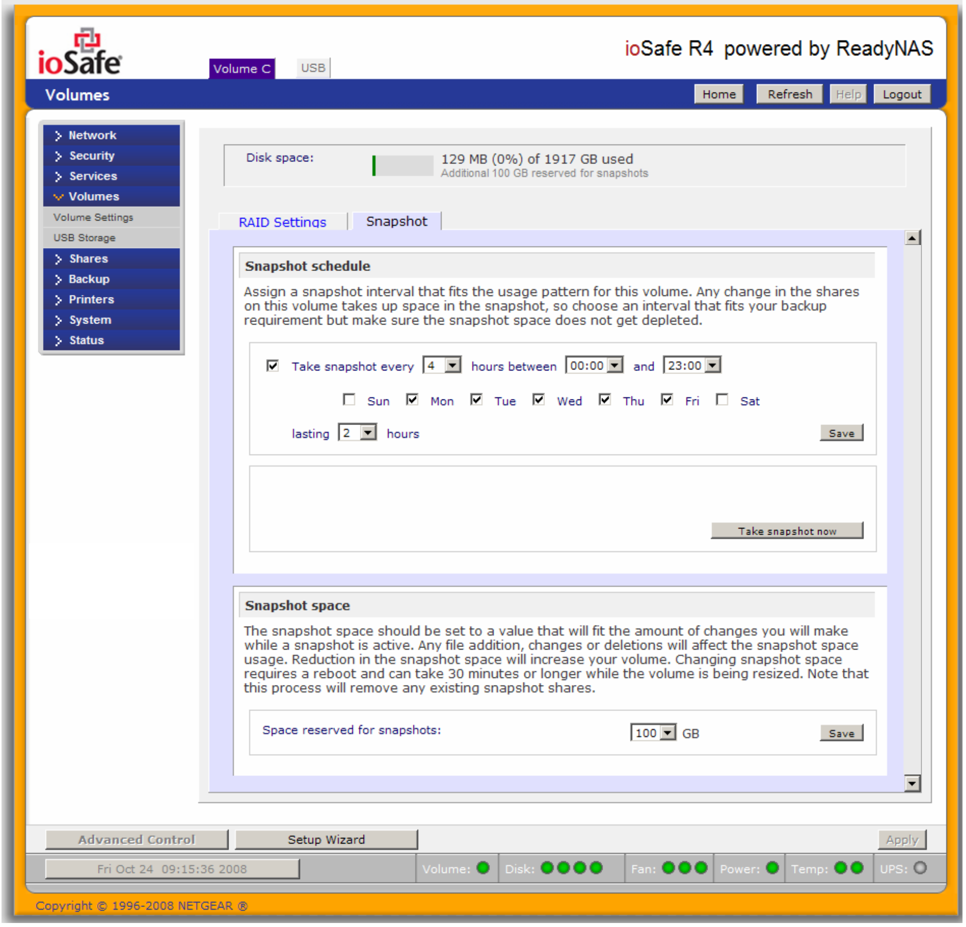
► TAKING AND SCHEDULING SNAPSHOT

To take or schedule a snapshot, click on the **Snapshot** tab.

> Note
>
> The ioSafe R4 ships with a snapshot reserved space of 0 GB.

In the tab, you can specify how often a snapshot should be taken. Snapshots can be scheduled in intervals from once every 4 hours to once a week.

Specify the frequency and the days that you wish to schedule a snapshot. A start and end-time of 00:00 will take one snapshot at midnight. A start time of 00:00 and end-time of 23:00 will take snapshots between midnight and 11pm the next day at the interval you specify. Once you save the snapshot schedule, the time of the next snapshot will be displayed. When the next snapshot is taken, the previous one is replaced.



Disk space: 129 MB (0%) of 1917 GB used
Additional 100 GB reserved for snapshots

Snapshot schedule

Assign a snapshot interval that fits the usage pattern for this volume. Any change in the shares on this volume takes up space in the snapshot, so choose an interval that fits your backup requirement but make sure the snapshot space does not get depleted.

☑ Take snapshot every 4 hours between 00:00 and 23:00

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

lasting 2 hours

Snapshot space

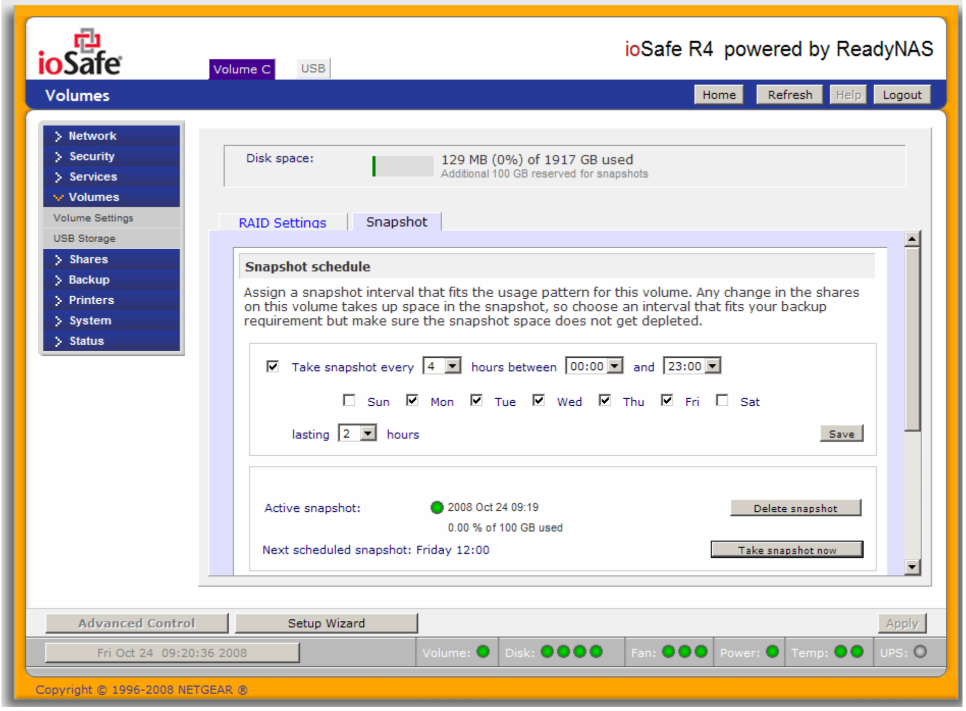
The snapshot space should be set to a value that will fit the amount of changes you will make while a snapshot is active. Any file addition, changes or deletions will affect the snapshot space usage. Reduction in the snapshot space will increase your volume. Changing snapshot space requires a reboot and can take 30 minutes or longer while the volume is being resized. Note that this process will remove any existing snapshot shares.

Space reserved for snapshots: 100 GB

Fri Oct 24 09:15:36 2008 Volume: ● Disk: ●●●● Fan: ●●● Power: ● Temp: ●● UPS: ○

Copyright © 1996-2008 NETGEAR ®

If you prefer, you can manually take a snapshot – just click on **Take snapshot now**.



Disk space: 129 MB (0%) of 1917 GB used
Additional 100 GB reserved for snapshots

Snapshot schedule

Assign a snapshot interval that fits the usage pattern for this volume. Any change in the shares on this volume takes up space in the snapshot, so choose an interval that fits your backup requirement but make sure the snapshot space does not get depleted.

☑ Take snapshot every 4 hours between 00:00 and 23:00

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

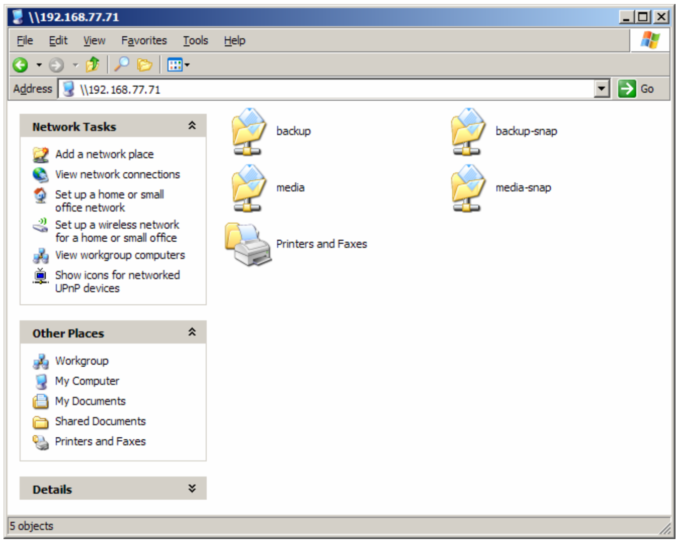
lasting 2 hours

Active snapshot: ● 2008 Oct 24 09:19
0.00 % of 100 GB used

Next scheduled snapshot: Friday 12:00

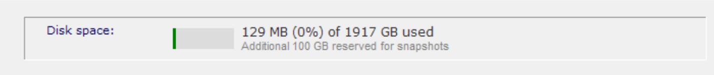
You can also specify how long a snapshot should last. If you will be using snapshots for backups, you can schedule the snapshot to last slightly longer than the expected duration of the backup. Having an active snapshot can affect the write performance to the ioSafe R4, so deactivating it when not needed may be advantageous in write-intensive environments.

When a snapshot is taken, snapshots of shares appear in your browse list alongside the original shares, except the snapshot share names have –*snap* appended to the original share names. For example, a snapshot taken of share **backup** will be available as **backup-snap**.



You can traverse a snapshot share just as you would a normal share except that the snapshot share is read-only. If you wish, you can select a detailed listing to show the snapshot time in the description field.

Snapshots can expire when the snapshot reserved space is filled. The snapshot mechanism keeps track of data that has been changed from the original volume starting at the point when the snapshot is taken. All these changes are kept in the snapshot reserved space on the volume. If you look at the **Disk space** utilization information just below the **Volume** tab, you will see how much space has been reserved for snapshots.



Disk space: 129 MB (0%) of 1917 GB used
Additional 100 GB reserved for snapshots

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

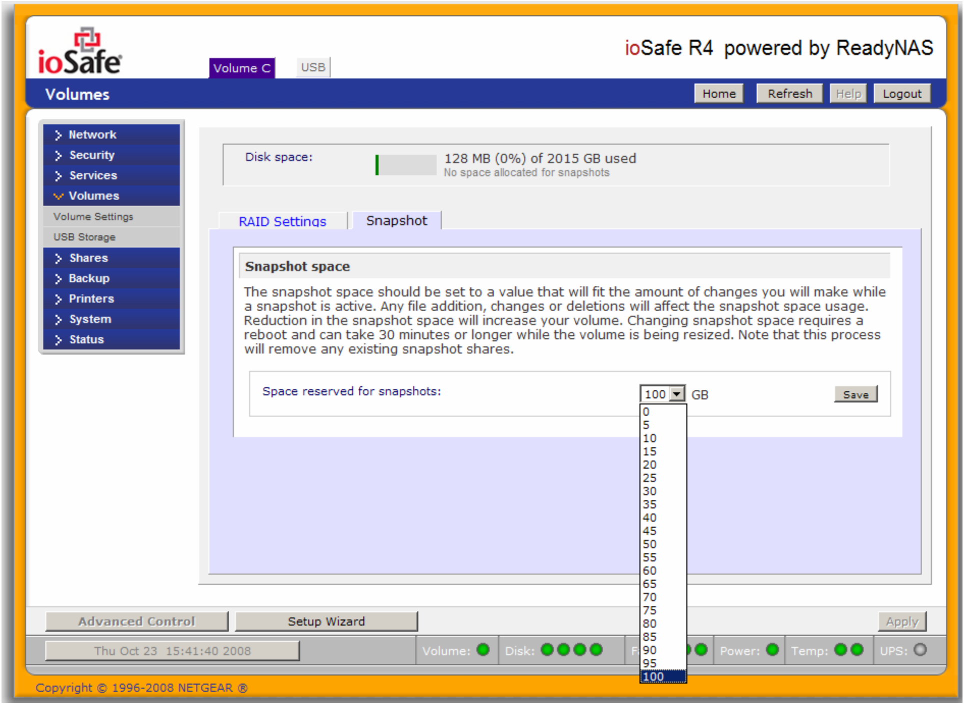
Note

Changes that occupy space in the snapshot reserved space include new file creation, modifications, and deletions; for instance, any time you delete a 1MB file, the change caused by the deletion will use up 1MB of reserved space.

When the snapshot does become invalidated, an email alert will be sent and the status will be reflected in the Snapshot tab. The snapshot is no longer usable at this stage.

► RESIZING SNAPSHOT SPACE

If you are constantly getting snapshot invalidation alerts, you may want to either increase the frequency of the snapshot, or consider increasing the snapshot reserved space. To do this, or to eliminate your existing snapshot space (thus increasing your usable volume space), you can specify the desired snapshot space in the Snapshot Space box. Simply select a value from the selection box and click **Save**. Your snapshot space will be limited to approximately 100GB.



Disk space: 128 MB (0%) of 2015 GB used
No space allocated for snapshots

Snapshot space

The snapshot space should be set to a value that will fit the amount of changes you will make while a snapshot is active. Any file addition, changes or deletions will affect the snapshot space usage. Reduction in the snapshot space will increase your volume. Changing snapshot space requires a reboot and can take 30 minutes or longer while the volume is being resized. Note that this process will remove any existing snapshot shares.

Space reserved for snapshots: 100 GB Save

0
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100

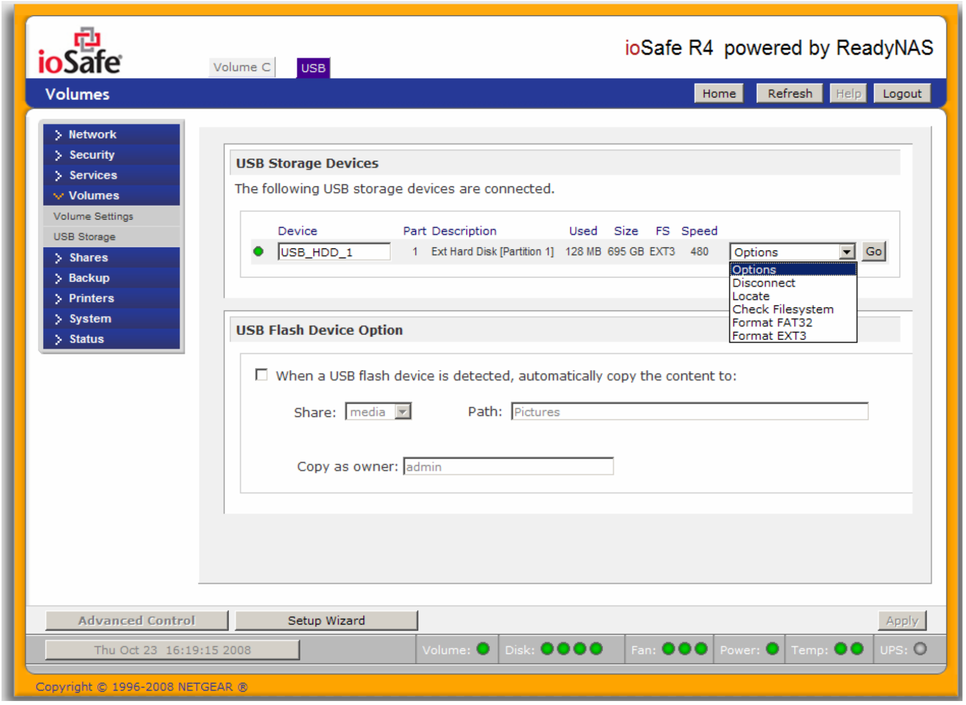
The process of resizing the snapshot space can take awhile depending on your data volume size and the number of files in your volume. Expanding the snapshot space will reduce your data volume size, and reducing the snapshot space will expand it.

Note

Due to the nature of how snapshots work, you will encounter a drop in write performance when a snapshot is active. If your environment requires the highest throughput in performance, the active snapshot should be deleted, or you should set a limit on how long the snapshot should last.

USB Storage

The USB tab displays the USB disk and flash devices connected to the ioSafe R4, and offers various options for these devices. A flash device will appear as USB_FLASH_1 and a disk device will appear as USB_HDD_1. If you have multiple devices, they will appear appended by an increasing device number, i.e. USB_HDD_2. If the device contains multiple partitions, the partitions will be listed beneath the main device entry.



USB Storage Devices

The following USB storage devices are connected.

	Device	Part	Description	Used	Size	FS	Speed	
●	USB_HDD_1	1	Ext Hard Disk [Partition 1]	128 MB	695 GB	EXT3	480	Options

USB Flash Device Option

☐ When a USB flash device is detected, automatically copy the content to:

Share: media Path: Pictures

Copy as owner: admin

Partitions on the storage devices must be one of the following file system formats:

- FAT32
- NTFS
- Ext2
- Ext3

To the right of the access icons are command options for the device. The following commands are available:

Disconnect: This option prepares the USB partition for disconnection by properly unmounting the file system. In most cases, you can safely disconnect the device without first unmounting; however, the Disconnect command ensures that any data still in the write-cache is written out to the disks and the file system is properly closed. The Disconnect option unmounts all partitions on the device. Once disconnected, physically remove and re-connect to the ioSafe R4 to regain access to the USB device.

Locate: In cases where you attach multiple storage devices and wish to determine which device corresponds to the device listing, the **Locate** command will blink the device LED, if present.

Format FAT32: This option formats the device as a FAT32 file system. FAT32 format is easily recognizable by most newer Windows, Linux and Unix operating systems.

Format EXT3: This option formats the device as an EXT3 file system. Select this option if you will be accessing the USB device mainly from Linux systems or ioSafe R4 devices. The advantage of EXT3 over FAT32 is that file ownership and mode information can be retained using this format whereas this capability is not there with FAT32. Although not natively present in the base operating system, Ext3 support for Windows and OS X can be added. The installation images can be downloaded from the web.

When the USB device is unmounted, you have the option of renaming it. The next time the same device is connected, it will use the new name rather than the default USB_FLASH_*n* or USB_HDD_*n* naming scheme.

The USB storage shares are listed in the Share menu, and access restrictions can be specified there. The share names will reflect the USB device names.

USB Flash Device Option

Towards the lower portion of the USB Storage tab, you'll notice the USB Flash Device Option. There, you can elect to copy the content of a USB flash device automatically on connect to a specified share. Files are copied into a unique timestamp folder to prevent overwriting previous contents. This is useful for uploading pictures from digital cameras and music from MP3 players without needing to power-on a PC.

In User security mode, an additional option to set the ownership of the copied files is available.

Shares

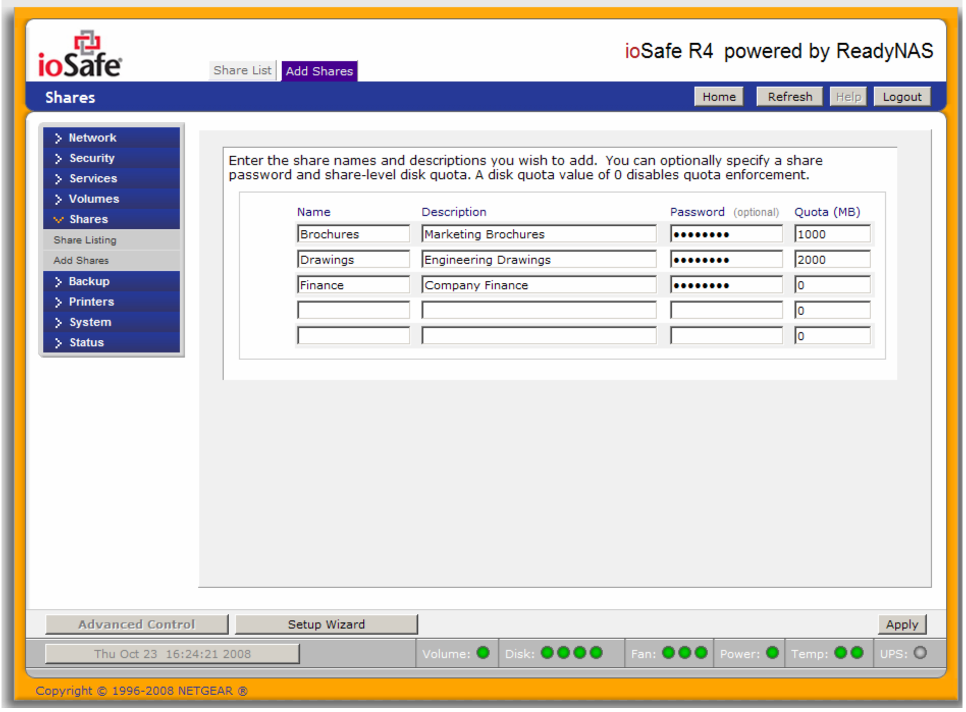
The Shares menu provides all the options pertaining to share services for the ioSafe R4 device. This entails share management (including data and print shares), volume management, and share service management.

We'll first look at how we can control the services.

Adding Shares

To add a share, click on the **Volume** tab. If more than one volume is configured, click on the volume you wish to add the share.

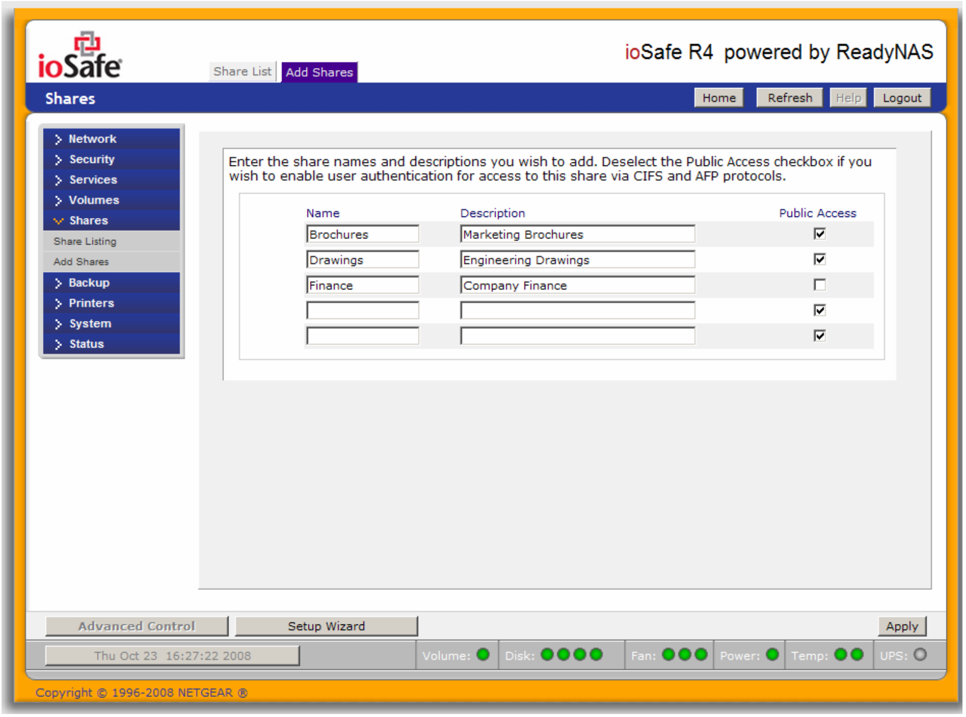
The **Add Share** tab has two looks, depending on the security mode. In the **Share** mode, you will enter the share name, description, and optional password and disk quota. The share password and share disk quota is available only in this security mode.



Enter the share names and descriptions you wish to add. You can optionally specify a share password and share-level disk quota. A disk quota value of 0 disables quota enforcement.

Name	Description	Password (optional)	Quota (MB)
Brochures	Marketing Brochures	••••••••	1000
Drawings	Engineering Drawings	••••••••	2000
Finance	Company Finance	••••••••	0
			0
			0

In the User or Domain security modes, the Add Share tab consists only of fields for the share name and description. Password and disk quotas are account-specific.



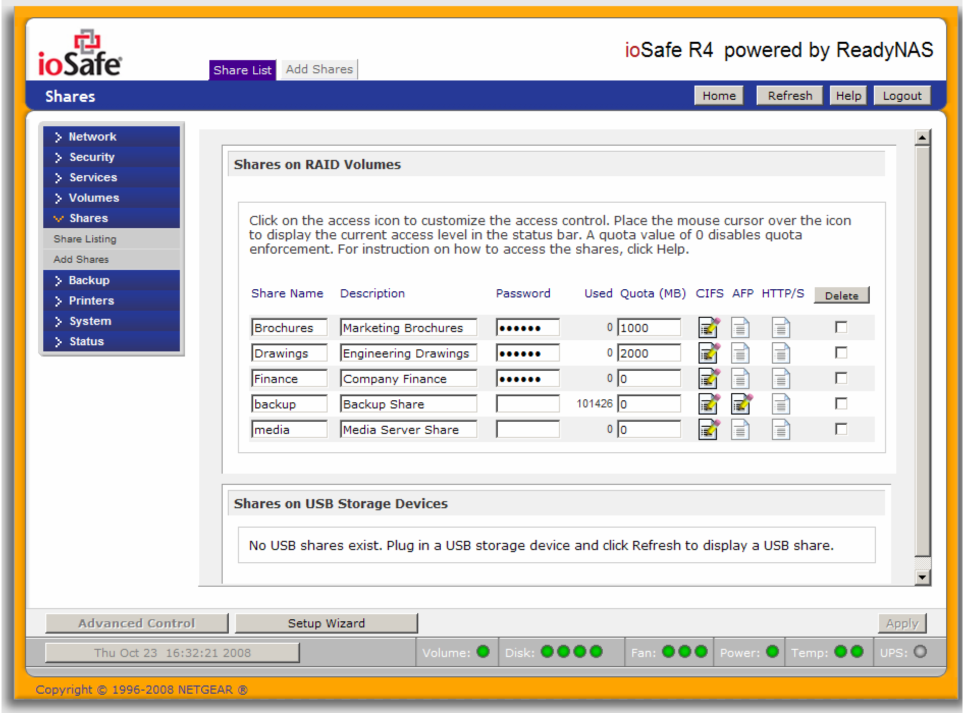
Enter the share names and descriptions you wish to add. Deselect the Public Access checkbox if you wish to enable user authentication for access to this share via CIFS and AFP protocols.

Name	Description	Public Access
Brochures	Marketing Brochures	☑
Drawings	Engineering Drawings	☑
Finance	Company Finance	□
		☑
		☑

In either case, you can add up to five shares at a time. Once you finish adding the shares, you can refer to Chapter 2 for instructions on how to access them from different client interfaces.

Managing Shares

Once you have added shares, you may want to manually fine-tune share access in the **Share List** tab. This tab has two looks, one for **Share** security mode and one for **User and Domain** mode. They're both similar except for the password and disk quota prompts which only appear in Share mode.



Shares on RAID Volumes

Click on the access icon to customize the access control. Place the mouse cursor over the icon to display the current access level in the status bar. A quota value of 0 disables quota enforcement. For instruction on how to access the shares, click Help.

Share Name	Description	Password	Used	Quota (MB)	CIFS	AFP	HTTP/S	Delete
Brochures	Marketing Brochures	••••••	0	1000	Read/Write Access	Disabled	Disabled	□
Drawings	Engineering Drawings	••••••	0	2000	Read/Write Access	Disabled	Disabled	□
Finance	Company Finance	••••••	0	0	Read/Write Access	Disabled	Disabled	□
backup	Backup Share		101426	0	Read/Write Access	Read/Write Access	Disabled	□
media	Media Server Share		0	0	Read/Write Access	Disabled	Disabled	□

Shares on USB Storage Devices

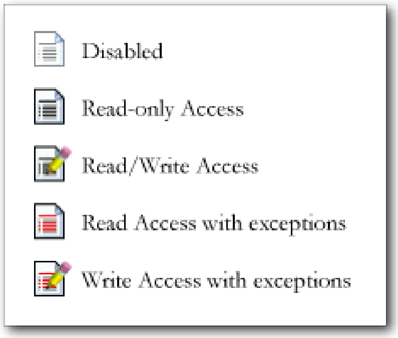
No USB shares exist. Plug in a USB storage device and click Refresh to display a USB share.

Thu Oct 23 16:32:21 2008 Volume: ● Disk: ●●●● Fan: ●●● Power: ● Temp: ●● UPS: ○

Copyright © 1996-2008 NETGEAR ®

If you want to delete a share, click on the checkbox to the far right of the share listing and click **Delete**. You have the option of deleting up to five shares at a time.

The columns to the left of the Delete checkbox represent the services that are currently enabled, and the access icons in those columns summarize the access rights to the share for each of the services. You can move the mouse pointer over the access icons to get a quick glimpse of the access settings.



The settings represent:

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

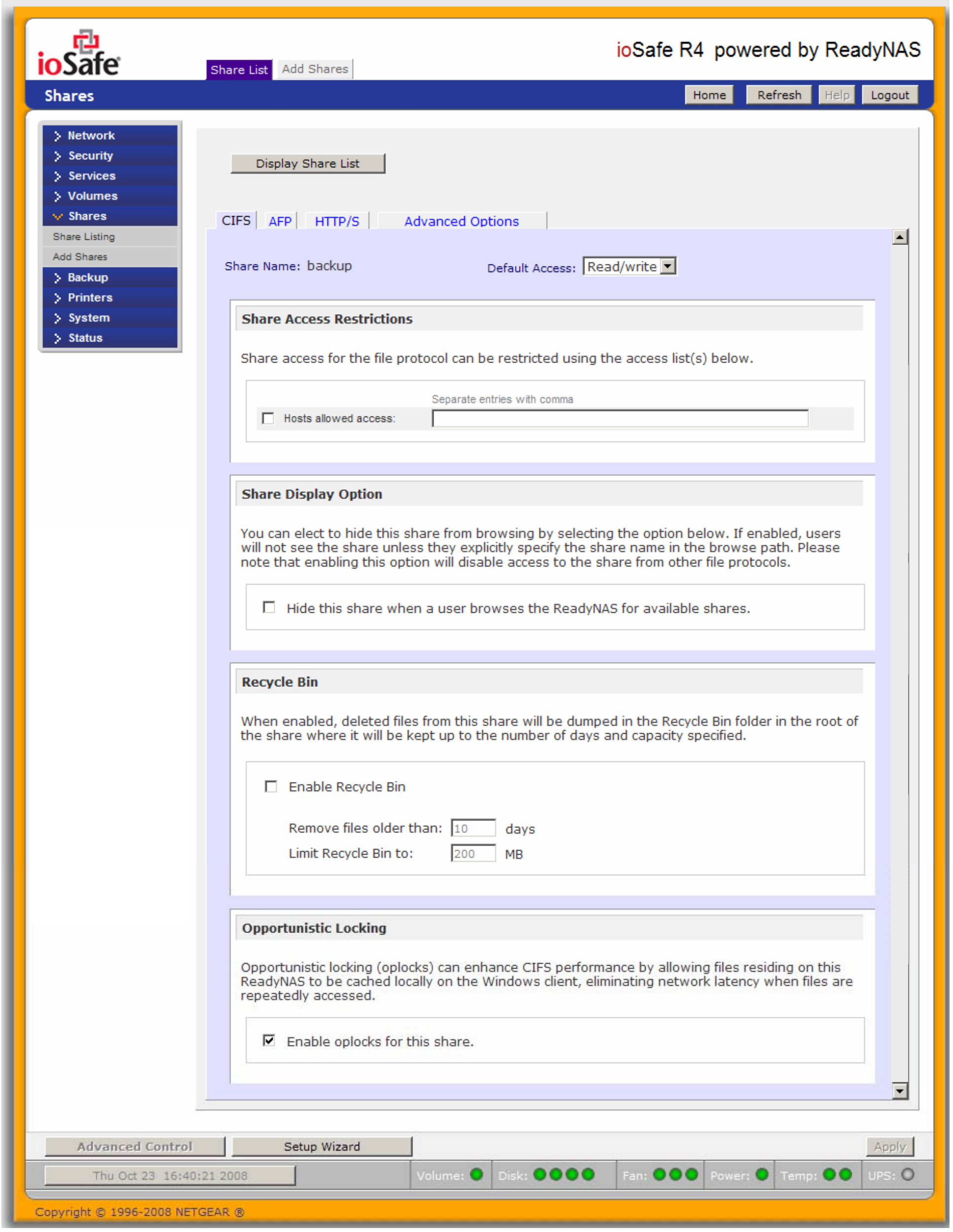
that are granted read/write permission, or (3) access is disabled except for one or more users or groups that are granted read-only privilege.

- **Write Access with exceptions** – Either (1) access to this share is read/write and only allowed for specified hosts, (2) access is read/write except for one or more users or groups that are restricted to read-only access, or (3) access is disabled except for one or more users or groups that are granted read/write privilege.

You can click on the access icons to bring up the Share Options tab where you can set the access rules for each file protocol. Keep in mind that access options will differ between protocols.

► SETTING SHARE ACCESS IN SHARE MODE

In Share mode, the CIFS/Windows share options tab will look as follows:



Share Name: backup

Default Access: Read/write

Share Access Restrictions

Share access for the file protocol can be restricted using the access list(s) below.

Separate entries with comma

☐ Hosts allowed access:

Share Display Option

You can elect to hide this share from browsing by selecting the option below. If enabled, users will not see the share unless they explicitly specify the share name in the browse path. Please note that enabling this option will disable access to the share from other file protocols.

☐ Hide this share when a user browses the ReadyNAS for available shares.

Recycle Bin

When enabled, deleted files from this share will be dumped in the Recycle Bin folder in the root of the share where it will be kept up to the number of days and capacity specified.

☐ Enable Recycle Bin

Remove files older than: 10 days

Limit Recycle Bin to: 200 MB

Opportunistic Locking

Opportunistic locking (oplocks) can enhance CIFS performance by allowing files residing on this ReadyNAS to be cached locally on the Windows client, eliminating network latency when files are repeatedly accessed.

☑ Enable oplocks for this share.

In this tab, you can select the default access at the top and optionally specify the host(s) that you wish to allow restrict access to in the Share Access Restriction box.

Share Access Restriction

For instance, select **read-only** for default access and list the hosts you wish to allow access to. Access from all other hosts will be denied. For example, to allow only host *192.168.2.101* read-only access to the share, specify the following:

```
Default:                Read-only
Hosts allowed access:   192.168.2.101
```

Multiple hosts can be separated with commas (see **Appendix B** for more description of valid host formats.) For example, if you wish to limit access to the share to particular hosts, you can enter host IP addresses or valid DNS hostnames in the **Host allowed** access field. In addition, you can enter a range of hosts using common IP range expressions such as:

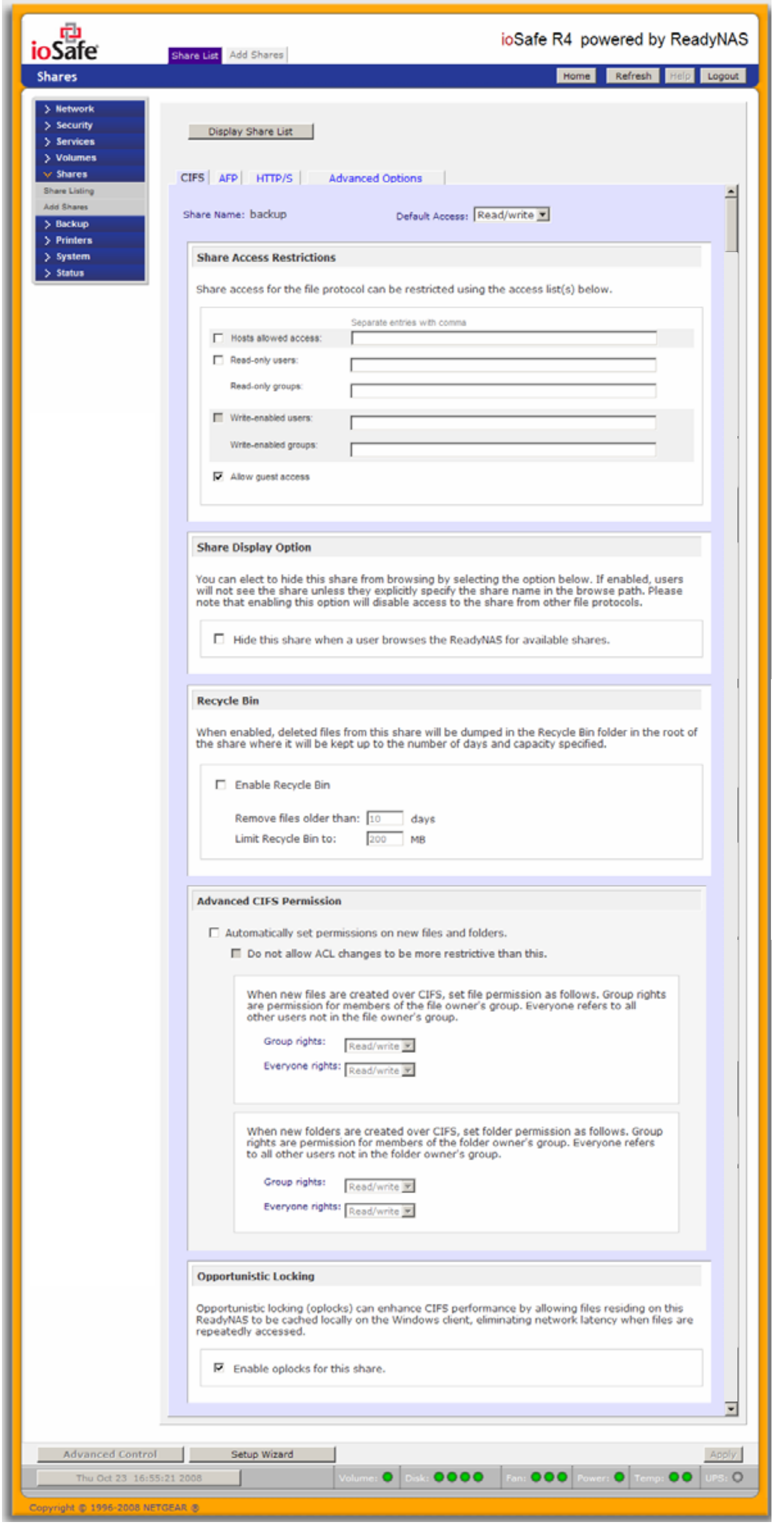
```
192.168.2., 192.168.2.0/255.255.255.0, 192.168.2.0/24
```

The above designations all allow hosts with IP addresses *192.168.2.1* through *192.168.2.254*.

Towards the bottom of the **Windows [CIFS]** tab, you'll notice the **Share Display**, **Recycle Bin**, and **Opportunistic Locking** options.

► SETTING SHARE ACCESS IN USER AND DOMAIN MODES

In User or Domain modes, the same tab would look as follows (note the addition of read-only and write-enabled user and group fields):



Share Name: backup

Default Access: Read/write

Share Access Restrictions

Share access for the file protocol can be restricted using the access list(s) below.

Separate entries with comma

□ Hosts allowed access:

□ Read-only users:

Read-only groups:

□ Write-enabled users:

Write-enabled groups:

☑ Allow guest access

Share Display Option

You can elect to hide this share from browsing by selecting the option below. If enabled, users will not see the share unless they explicitly specify the share name in the browse path. Please note that enabling this option will disable access to the share from other file protocols.

□ Hide this share when a user browses the ReadyNAS for available shares.

Recycle Bin

When enabled, deleted files from this share will be dumped in the Recycle Bin folder in the root of the share where it will be kept up to the number of days and capacity specified.

□ Enable Recycle Bin

Remove files older than: 10 days

Limit Recycle Bin to: 200 MB

Advanced CIFS Permission

□ Automatically set permissions on new files and folders.

□ Do not allow ACL changes to be more restrictive than this.

When new files are created over CIFS, set file permission as follows. Group rights are permission for members of the file owner's group. Everyone refers to all other users not in the file owner's group.

Group rights: Read/write

Everyone rights: Read/write

When new folders are created over CIFS, set folder permission as follows. Group rights are permission for members of the folder owner's group. Everyone refers to all other users not in the folder owner's group.

Group rights: Read/write

Everyone rights: Read/write

Opportunistic Locking

Opportunistic locking (oplocks) can enhance CIFS performance by allowing files residing on this ReadyNAS to be cached locally on the Windows client, eliminating network latency when files are repeatedly accessed.

☑ Enable oplocks for this share.

Thu Oct 23 16:55:21 2008

Copyright © 1996-2008 NETGEAR ®

Share Access Restriction

If you wish to limit share access to particular users and/or groups, you can enter their names in the **Read-only users**, **Read-only groups**, **Write-enabled users**, and **Write-enabled group** fields. The names must be valid accounts, either on the ioSafe R4 or on the domain controller.

For instance, if you wish to allow read-only access to all and read/write access only user *fred* and group *engr*, you would set the following:

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

If you wish to limit the above access only to hosts *192.168.2.101* and *192.168.2.102*, set the following:

```
Default:               Read-only
Hosts allowed access:  192.168.2.101, 192.168.2.102
Write-enabled users:   fred
Write-enabled groups:  engr
```

If you wish to specify some users and groups for read-only access and some for read/write access, and disallow all other users and groups, enter the following:

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

Note that access control will differ slightly from service to service.

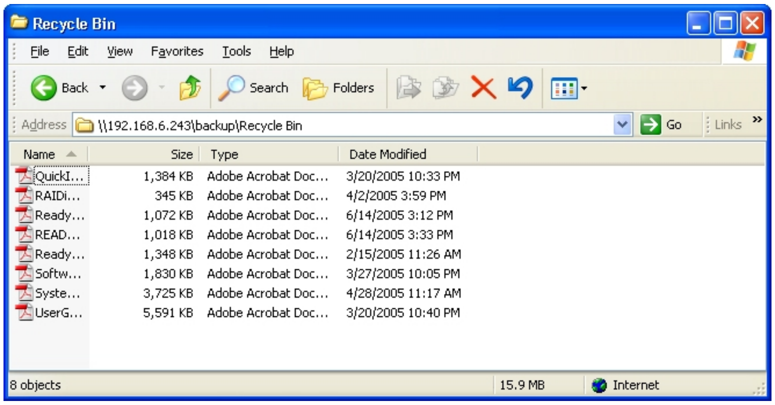
Share Display Option

Restricting access to a share will not prevent users from seeing the share in the browse list. In certain instances, this might not be desirable, such as for backup shares that you may want to prevent users from seeing. To hide a share, select the **Hide this share…** option. Users who have access to this share must specify the path explicitly. For example, to access a hidden share, enter \\host\share in the Windows Explorer.

Recycle Bin

The ioSafe R4 can have a Recycle Bin for each share for Windows users. You will see the **Enable Recycle Bin** option at the bottom of the **Windows [CIFS]** access tab.

When enabled, whenever you delete a file, the file gets inserted into the Recycle Bin folder in the Share rather than being permanently deleted. This allows for a grace period where users can restore deleted files.



Address \\192.168.6.243\backup\Recycle Bin

Name	Size	Type	Date Modified
QuickI…	1,384 KB	Adobe Acrobat Doc…	3/20/2005 10:33 PM
RAIDi…	345 KB	Adobe Acrobat Doc…	4/2/2005 3:59 PM
Ready…	1,072 KB	Adobe Acrobat Doc…	6/14/2005 3:12 PM
READ…	1,018 KB	Adobe Acrobat Doc…	6/14/2005 3:33 PM
Ready…	1,348 KB	Adobe Acrobat Doc…	2/15/2005 11:26 AM
Softw…	1,830 KB	Adobe Acrobat Doc…	3/27/2005 10:05 PM
Syste…	3,725 KB	Adobe Acrobat Doc…	4/28/2005 11:17 AM
UserG…	5,591 KB	Adobe Acrobat Doc…	3/20/2005 10:40 PM

You can specify how long to keep the files in the Recycle Bin and how large the Recycle Bin can get before files get permanently erased.

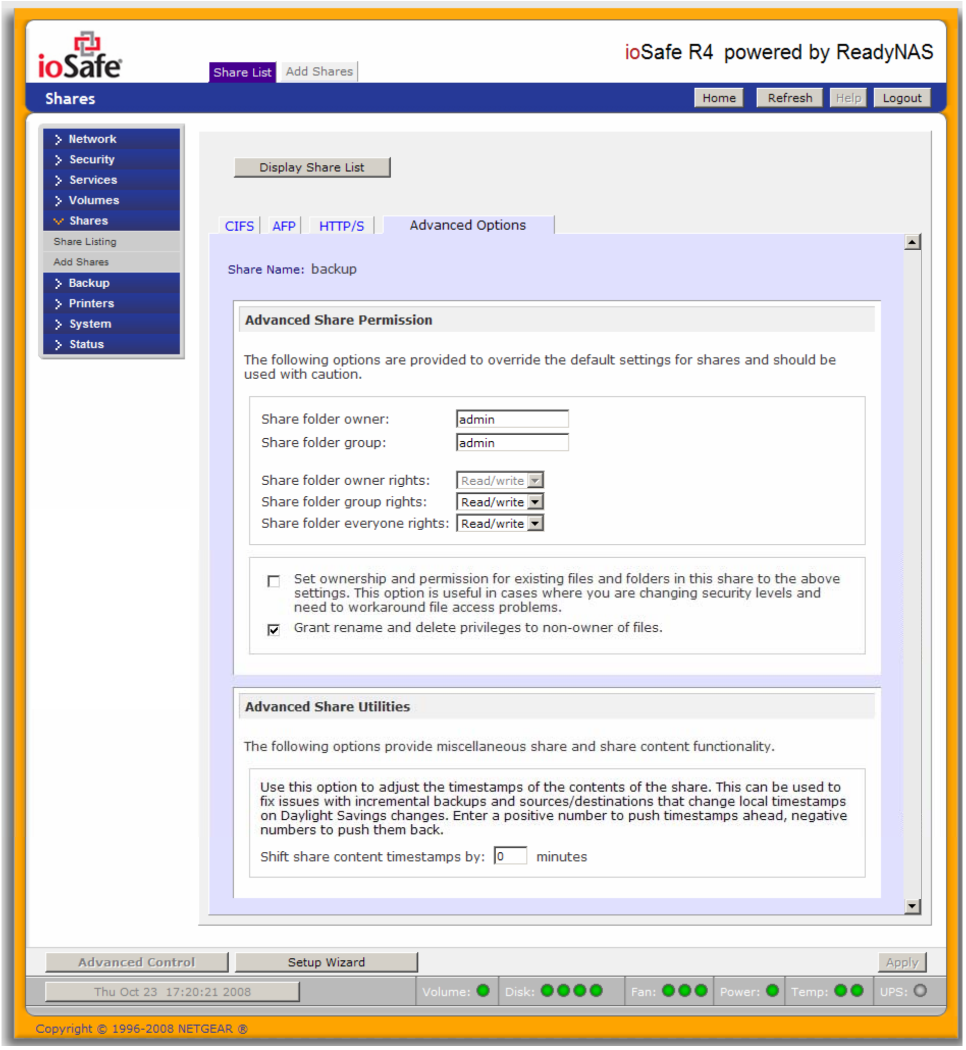
Advanced CIFS Permission

The Advanced CIFS Permission box offers options for setting the default permission of new files and folders created via CIFS. The default permission of newly created files is read/write for the owner and owner's group and read-only for others (i.e. everyone). Permission for newly created folders is read/write for everyone. If the default doesn't satisfy your security requirement, you can change it here.

Opportunistic locking (often referred to as oplocks) enhances CIFS performance by allowing files residing on the NAS to be cached locally on the Windows client, thus eliminating network latency when the files are constantly accessed.

► ADVANCED OPTIONS

The Advanced Options tab offers advanced low-level file manipulation options that can affect remote file access through all file protocol interfaces. Care should be taken before using these options as anything that changes ownership and permissions may not be easily reversible.



Share Name: backup

Advanced Share Permission

The following options are provided to override the default settings for shares and should be used with caution.

Share folder owner: admin
Share folder group: admin

Share folder owner rights: Read/write
Share folder group rights: Read/write
Share folder everyone rights: Read/write

☐ Set ownership and permission for existing files and folders in this share to the above settings. This option is useful in cases where you are changing security levels and need to workaround file access problems.

☑ Grant rename and delete privileges to non-owner of files.

Advanced Share Utilities

The following options provide miscellaneous share and share content functionality.

Use this option to adjust the timestamps of the contents of the share. This can be used to fix issues with incremental backups and sources/destinations that change local timestamps on Daylight Savings changes. Enter a positive number to push timestamps ahead, negative numbers to push them back.

Shift share content timestamps by: 0 minutes

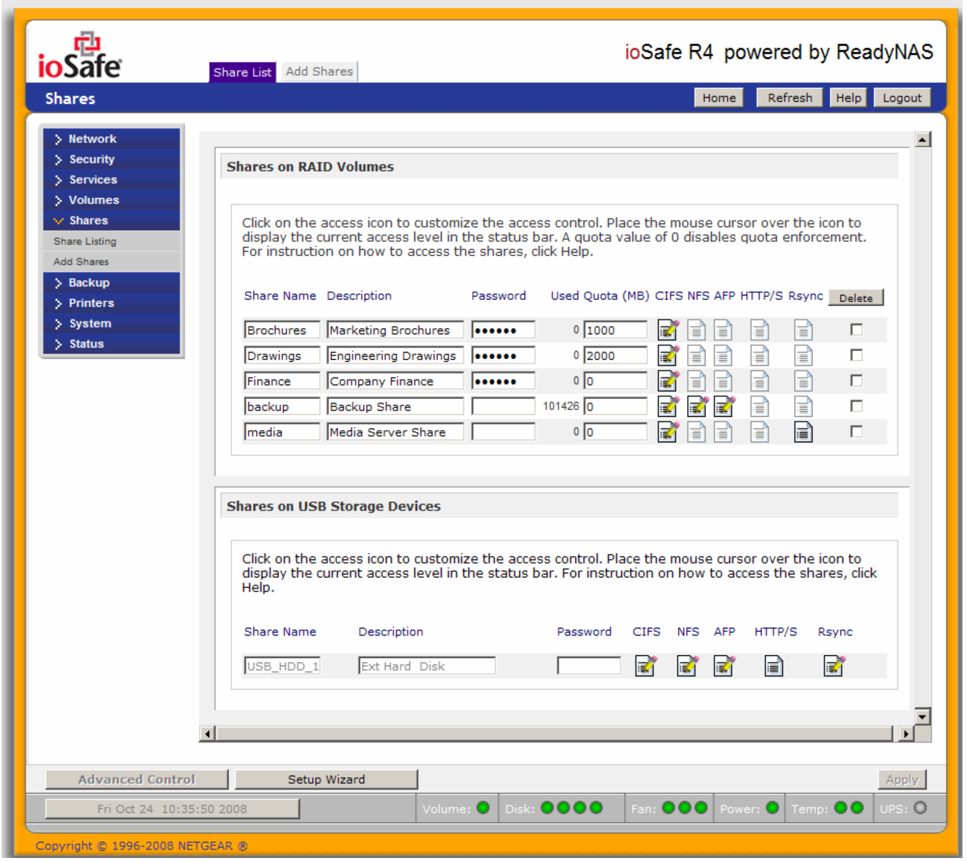
Advanced Share Permission

The Advanced Share Permission section offers the options to override the default ownership and permission of the share folder on the embedded file system and to permeate these settings to all files and folders residing on the selected share. The **Set ownership and permission for existing files and folders…** option will perform a one-time change. Depending on the size of the share, this can take awhile to finish.

You can also **grant rename and delete privilege to non-owners of the files** option. In a collaborative environment, it may be desirable to enable this option. In a more security-conscious environment, it may be desirable to disable this option.

USB Shares

USB storage devices are shared using the name of the device appended by the partition number. The base device name can be changed in the Volumes/USB tab if desired. The ioSafe R4 attempts to remember the name as long as there's a unique ID associated with the USB device so that the next time the device is connected, the same share name(s) will be available. Share access restrictions are not saved across disconnects, however.



Shares on RAID Volumes

Click on the access icon to customize the access control. Place the mouse cursor over the icon to display the current access level in the status bar. A quota value of 0 disables quota enforcement. For instruction on how to access the shares, click Help.

Share Name	Description	Password	Used	Quota (MB)	CIFS	NFS	AFP	HTTP/S	Rsync	Delete
Brochures	Marketing Brochures	••••••	0	1000	✎	🗎	🗎	🗎	🗎	☐
Drawings	Engineering Drawings	••••••	0	2000	✎	🗎	🗎	🗎	🗎	☐
Finance	Company Finance	••••••	0	0	✎	🗎	🗎	🗎	🗎	☐
backup	Backup Share		101426	0	✎	✎	✎	🗎	🗎	☐
media	Media Server Share		0	0	✎	🗎	🗎	🗎	🗎	☐

Shares on USB Storage Devices

Click on the access icon to customize the access control. Place the mouse cursor over the icon to display the current access level in the status bar. For instruction on how to access the shares, click Help.

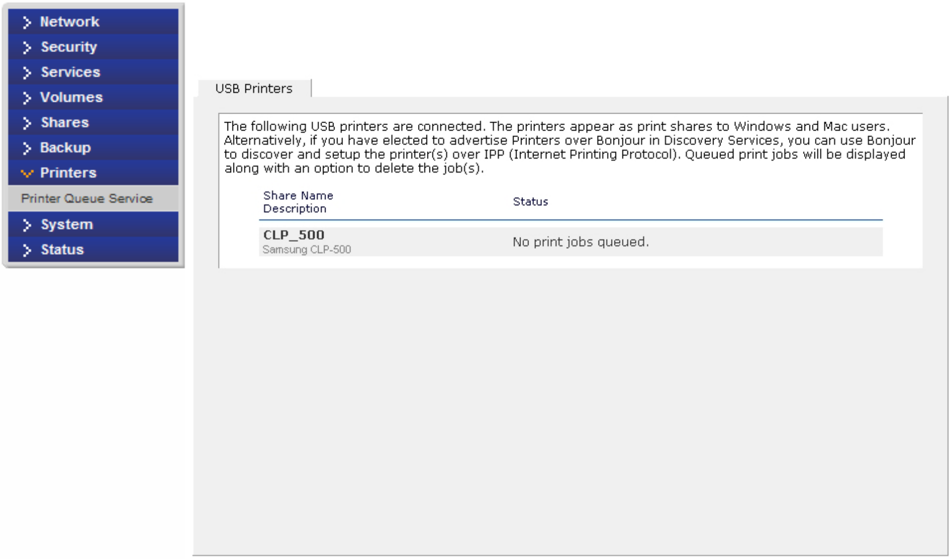
Share Name	Description	Password	CIFS	NFS	AFP	HTTP/S	Rsync
USB_HDD_1	Ext Hard Disk		✎	✎	✎	🗎	✎

Note

Although access authorization is based on user login in non-Share mode, files saved on the USB device, regardless of the user account, are with UID 0. This is to allow easy sharing of the USB device with other ioSafe R4 and PC systems.

Printers

The ioSafe R4 device supports automatic recognition of USB printers. If you have not already done so, you can connect a printer now, wait a few seconds, and click **Refresh** to display detected printers. The print share name will automatically reflect the manufacturer and model of your printer and will list in the USB Printers tab.

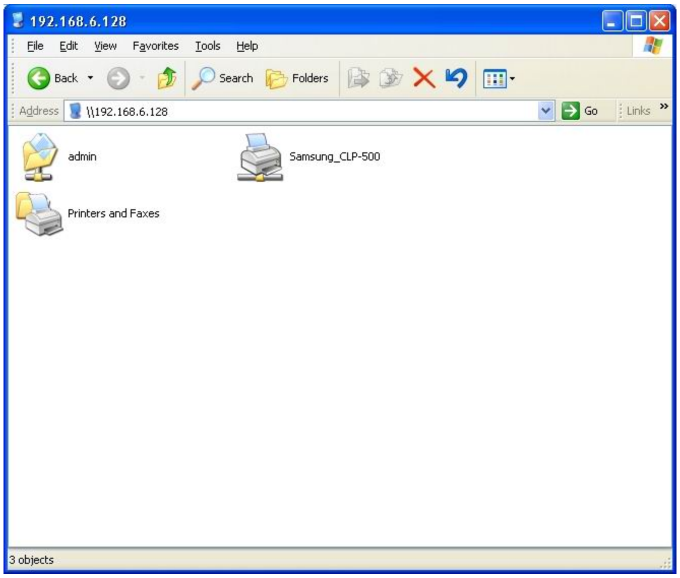


The following USB printers are connected. The printers appear as print shares to Windows and Mac users. Alternatively, if you have elected to advertise Printers over Bonjour in Discovery Services, you can use Bonjour to discover and setup the printer(s) over IPP (Internet Printing Protocol). Queued print jobs will be displayed along with an option to delete the job(s).

Share Name Description	Status
CLP_500 Samsung CLP-500	No print jobs queued.

Print Shares over CIFS/SMB

The ioSafe R4 can act as a print server for up to two USB printers for your Windows or Mac clients. For example, to setup a printer under Windows, click Browse in RAIDar or simply enter \\hostname in the Windows Explorer address bar to list all data and printer shares on the ioSafe R4.



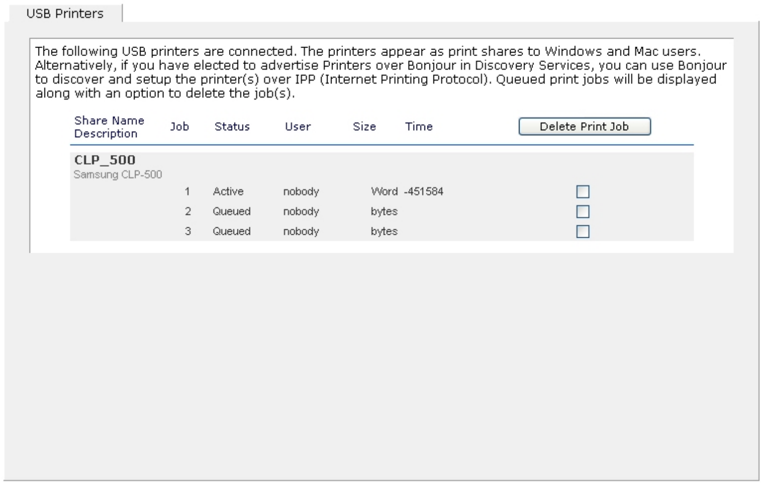
Double-click the printer icon to assign a Windows driver.

IPP Printing

The ioSafe R4 also supports the IETF standard Internet Printing Protocol (IPP) over HTTP. Any client supporting IPP Printing (IPP is available natively on the latest Windows Versions and OS X) can now use this protocol to utilize printers connected to the ioSafe R4. The simplest way to utilize IPP Printing is to use **Bonjour** to discover and setup the print queue. Bonjour is built into OS X and can be installed on Windows (Bonjour for Windows is available for download from Apple's website at http://www.apple.com/macosx/features/bonjour/).

Managing Print Queues

From time to time, printers may run out of ink, paper, or simply jam up, forcing you to deal with the print jobs stuck in a queue. The ioSafe R4 has a built-in print queue management to handle this. Simply go to the **USB Printers** tab or click **Refresh** to display the printers and the jobs queued up for any "stuck" printers.



The following USB printers are connected. The printers appear as print shares to Windows and Mac users. Alternatively, if you have elected to advertise Printers over Bonjour in Discovery Services, you can use Bonjour to discover and setup the printer(s) over IPP (Internet Printing Protocol). Queued print jobs will be displayed along with an option to delete the job(s).

Share Name Description	Job	Status	User	Size	Time	Delete Print Job
CLP_500 Samsung CLP-500						
	1	Active	nobody	Word	-451584	□
	2	Queued	nobody	bytes		□
	3	Queued	nobody	bytes		□

Click on the checkbox next to the print jobs and click **Delete Print Job** to remove them from the print queue.

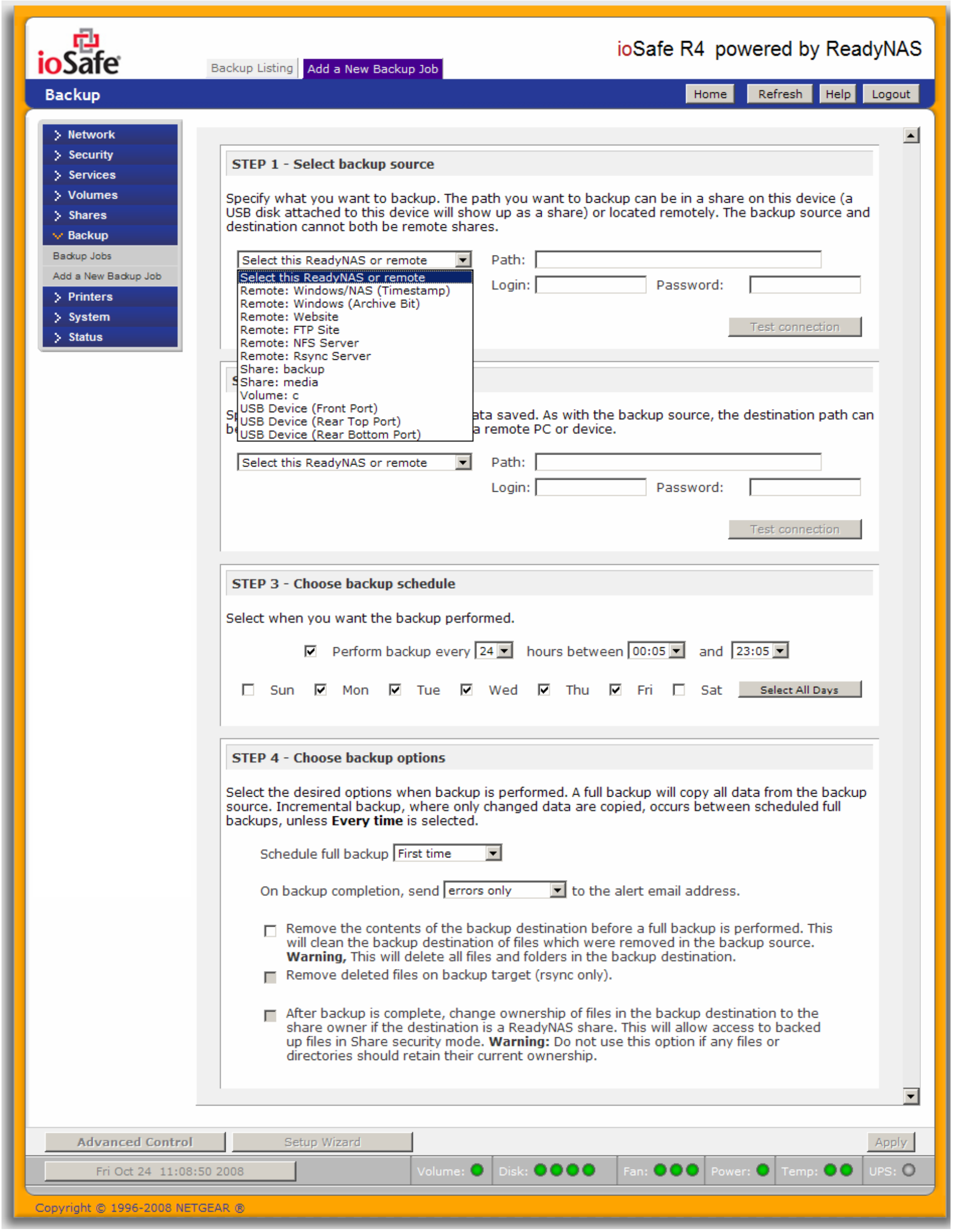
Backup

The **Backup** manager integrated with the ioSafe R4 allows the ioSafe R4 to act as a backup appliance. Backup tasks can be controlled directly from the ioSafe R4 without the need for a client-based backup application.

With the flexibility to support full and incremental backups across FTP, HTTP, CIFS/SMB, and NFS protocols, the ioSafe R4 can act as a simple central repository for both home and office environments. And with multiple ioSafe R4 systems, you can set up one ioSafe R4 to backup another directly.

Adding a New Backup Job

To create a new backup job, click on the **Add a New Backup Job** tab. You will notice a 4-step procedure on creating a job.



ioSafe R4 powered by ReadyNAS

Backup Listing | Add a New Backup Job

Backup

Home | Refresh | Help | Logout

STEP 1 - Select backup source

Specify what you want to backup. The path you want to backup can be in a share on this device (a USB disk attached to this device will show up as a share) or located remotely. The backup source and destination cannot both be remote shares.

Select this ReadyNAS or remote ▾ Path: Login: Password:

- Select this ReadyNAS or remote
- Remote: Windows/NAS (Timestamp)
- Remote: Windows (Archive Bit)
- Remote: Website
- Remote: FTP Site
- Remote: NFS Server
- Remote: Rsync Server
- Share: backup
- Share: media
- Volume: c
- USB Device (Front Port)
- USB Device (Rear Top Port)
- USB Device (Rear Bottom Port)

Test connection

S

Sp ata saved. As with the backup source, the destination path can
b a remote PC or device.

Select this ReadyNAS or remote ▾ Path: Login: Password:

Test connection

STEP 3 - Choose backup schedule

Select when you want the backup performed.

☑ Perform backup every 24 ▾ hours between 00:05 ▾ and 23:05 ▾

☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat Select All Days

STEP 4 - Choose backup options

Select the desired options when backup is performed. A full backup will copy all data from the backup source. Incremental backup, where only changed data are copied, occurs between scheduled full backups, unless **Every time** is selected.

Schedule full backup First time ▾

On backup completion, send errors only ▾ to the alert email address.

☐ Remove the contents of the backup destination before a full backup is performed. This will clean the backup destination of files which were removed in the backup source. **Warning,** This will delete all files and folders in the backup destination.

☐ Remove deleted files on backup target (rsync only).

☐ After backup is complete, change ownership of files in the backup destination to the share owner if the destination is a ReadyNAS share. This will allow access to backed up files in Share security mode. **Warning:** Do not use this option if any files or directories should retain their current ownership.

Advanced Control | Setup Wizard | Apply

Fri Oct 24 11:08:50 2008 | Volume: ● | Disk: ●●●● | Fan: ●●● | Power: ● | Temp: ●● | UPS: ○

Copyright © 1996-2008 NETGEAR ®

▶ STEP 1 – SELECT BACKUP SOURCE

The backup source can be located remotely or it can be a public, a private home share, or all home shares on the ioSafe R4.

A USB device will appear as a share, so if you want to backup a USB device, select on a share name starting with USB. If you want to backup data from a remote source, you will need to select from one of the following:

- **Windows/NAS (Timestamp)** – select this if you wish to backup a share from a Windows PC or another ioSafe R4 device. Incremental backups use timestamps to determine whether files should be backed up.

- **Windows/NAS (Archive Bit)** – select this if you wish to backup a share from a Windows PC. Incremental backups use the archive bit of files, similar to Windows, to determine whether they should be backed up.
- **Website** – select thi if you wish to back up a website or a website directory. The backed up files include files in the default index file and all associated files, as well as all index file links to web page image files.
- **FTP site** – select this if you wish to back up an FTP site or a path from that site.
- **NFS server** – select this option if you wish to back up from a Linux/Unix server across NFS. Mac OS X users can also use this option by setting up a NFS share from the console terminal.
- **Rsync server** – select this if you wish to perform backups from a rsync server. Rsync was originally available for Linux and other flavors of Unix, but has lately become popular under Windows and Mac for its efficient use of incremental file transfers. This is the preferred backup method between two ioSafe R4 systems.

Once you have selected a backup source, you can enter the path from that source. If you selected a ioSafe R4 share, you can either leave the path blank to backup the entire share, or enter a folder path. Note that you should use forward slashes, '/', in place of backslashes (\).

If you selected a remote source, each remote protocol uses a slightly different notation for the path. If the path field is empty, selecting the remote source in the pull-down menu shows an example format of the path. Following are some examples:

Examples of a FTP path
ftp://myserver/mypath/mydir
ftp://myserver/mypath/mydir/myfile

Examples of a Website path
http://www.mywebsite.com
http://192.168.0.101/mypath/mydir

Examples of a Windows or remote NAS path
//myserver/myshare
//myserver/myshare/myfolder
//192.168.0.101/myshare/myfolder

Examples of NFS path
myserver:/mypath
192.168.0.101:/mypath/myfolder

Examples of Rsync path
myserver::mymodule/mypath
192.168.0.101::mymodule/mypath

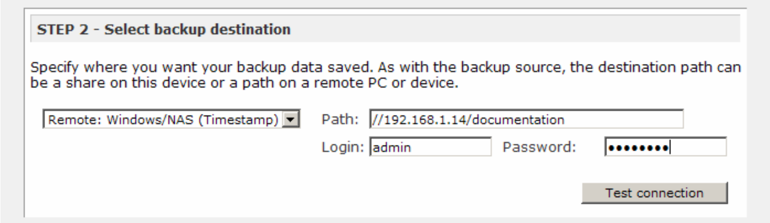
Examples of local path
myfolder
media/Videos
My Folder
My Documents/My Pictures

With a remote source, you may need to enter a login and password to access the share. If you are accessing a password-protected share on a remote ioSafe R4 server configured for Share security mode, enter the name of the share name for login.

You should click on the **Test Connection** button to make sure you have proper access to the remote backup source before continuing.

► STEP 2 – SELECT BACKUP DESTINATION

The **Step 2** process is almost identical to Step 1 except that you are now specifying the backup destination. If you had selected a remote backup source, you will need to select a public or a private home share on the ioSafe R4 (either the source or destination must be local to the ioSafe R4). If you selected an ioSafe R4 share for the source, you can either enter another local ioSafe R4 share for the destination, or you can specify a remote backup destination.



STEP 2 - Select backup destination

Specify where you want your backup data saved. As with the backup source, the destination path can be a share on this device or a path on a remote PC or device.

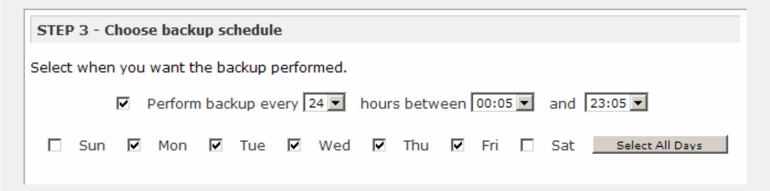
Remote: Windows/NAS (Timestamp) ▾ Path: //192.168.1.14/documentation

Login: admin Password: ••••••••

The remote backup destination can be a Windows PC/ioSafe R4 system, NFS server, or a Rsync server. Note that you can select Rsync for a remote ioSafe R4 if it is configured to serve data over Rsync.

► STEP 3 – CHOOSE BACKUP SCHEDULE

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



STEP 3 - Choose backup schedule

Select when you want the backup performed.

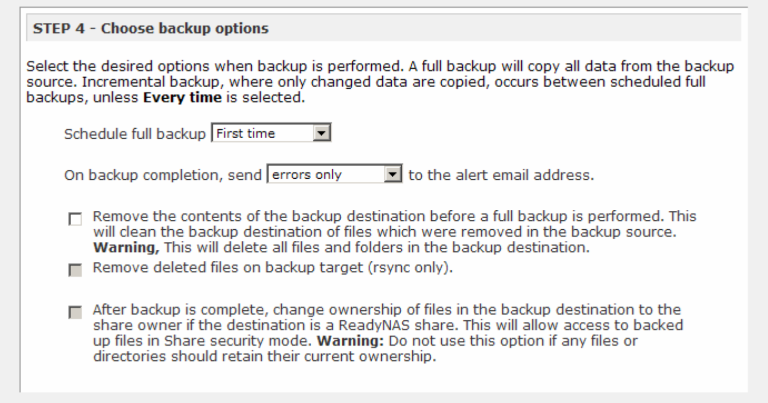
☑ Perform backup every 24 ▾ hours between 00:05 ▾ and 23:05 ▾

☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat

If you wish, you can elect not to schedule the backup job so that you can invoke it manually instead by not selecting the **Perform backup every…** check box. You may want to do this if you will be starting the backup from the Backup Button on ioSafe R4 system.

► STEP 4 – CHOOSE BACKUP OPTIONS

In this last step, select how you would like backups to be performed.



STEP 4 - Choose backup options

Select the desired options when backup is performed. A full backup will copy all data from the backup source. Incremental backup, where only changed data are copied, occurs between scheduled full backups, unless **Every time** is selected.

Schedule full backup: First time

On backup completion, send errors only to the alert email address.

□ Remove the contents of the backup destination before a full backup is performed. This will clean the backup destination of files which were removed in the backup source. **Warning,** This will delete all files and folders in the backup destination.

□ Remove deleted files on backup target (rsync only).

□ After backup is complete, change ownership of files in the backup destination to the share owner if the destination is a ReadyNAS share. This will allow access to backed up files in Share security mode. **Warning:** Do not use this option if any files or directories should retain their current ownership.

Schedule full backup

First, select when you want full backups to be performed. You can elect to do this just at the first time, every week, every two weeks, every three weeks, every four weeks, or every time this backup job is invoked. The first full backup is performed at the next scheduled occurrence of the backup depending on the schedule you specify, and the next full backup is performed at the weekly interval you choose calculated from this first backup. Incremental backup is performed between the full backup cycles.

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

Send backup log

Backup logs can be sent to the users on the Alert contact list when the backup is complete. It is a good idea to select this option to make sure files are backed up as expected. You can elect to send only errors encountered during backup, full backup logs consisting of file listing (can be large), or status and errors (*status* refers to completion status).

> **Note**
>
> Backup log e-mails are restricted to approximately 10K lines. To view the full backup log (regardless of length), select Status > Logs and click the **Download All Logs** link.

Remove files from destination first

Select if you want to erase the destination path contents before the backup is performed. Be careful not to reverse your backup source and destination as doing so can delete your source files for good. It is safer to not select this option unless your device is running low on space. Do experiment with a test share to make sure you understand this option.

Remove deleted files on backup target for Rsync

By default, files deleted in the backup source will not get deleted in the backup destination. With Rsync, you have the option of simulating *mirror* mode by removing files in the backup destination deleted from the backup source since the last backup. Select this option if you wish to do this. Do experiment with a test share to make sure you understand this option.

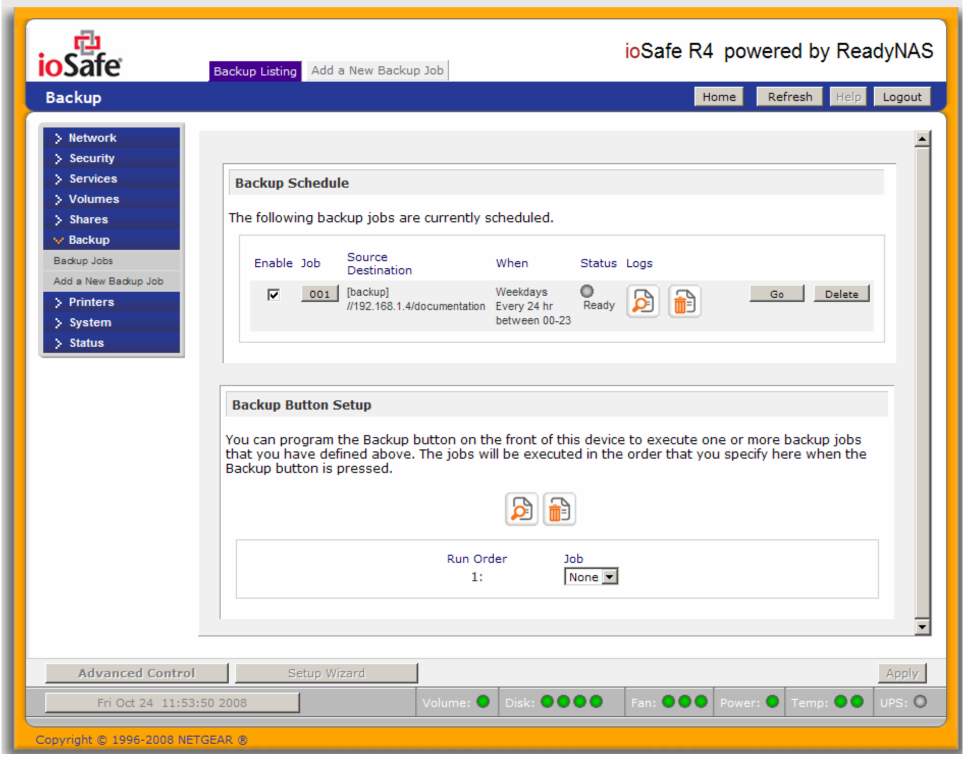
Change ownership of backup files

The Backup Manager attempts to maintain original file ownership whenever possible; however, this may cause problems in Share security mode when backup files are accessed. To work around this, you have the option of automatically changing the ownership of the backed up files to match the ownership of the share. This allows anyone who can access the backup share to have full access to the backed up files.

Before trusting that your backup job to a schedule, it is always a good idea to manually perform the backup to make sure access to the remote backup source or destination is granted, and the backup job can be done within the backup frequency you selected. You can do this after clicking **Apply** to save the backup job.

Viewing the Backup Schedule

After saving the backup job, a new job appears in the Backup Schedule section of the Backup Jobs screen.



Backup Schedule

The following backup jobs are currently scheduled.

Enable	Job	Source Destination	When	Status	Logs		
☑	001	[backup] //192.168.1.4/documentation	Weekdays Every 24 hr between 00-23	○ Ready		Go	Delete

Backup Button Setup

You can program the Backup button on the front of this device to execute one or more backup jobs that you have defined above. The jobs will be executed in the order that you specify here when the Backup button is pressed.

Run Order	Job
1:	None

Here, you will see a summary of the backup jobs that have been scheduled. Jobs are numbered starting from 001. You can modify the backup job by clicking the Job number button.

If you wish, you can enable or disable the job scheduling by clicking on the **Enable** checkbox. Disabling the job will not delete the job, but rather take it out of the automatic scheduling. If you wish to delete the job, click the **Delete** button.

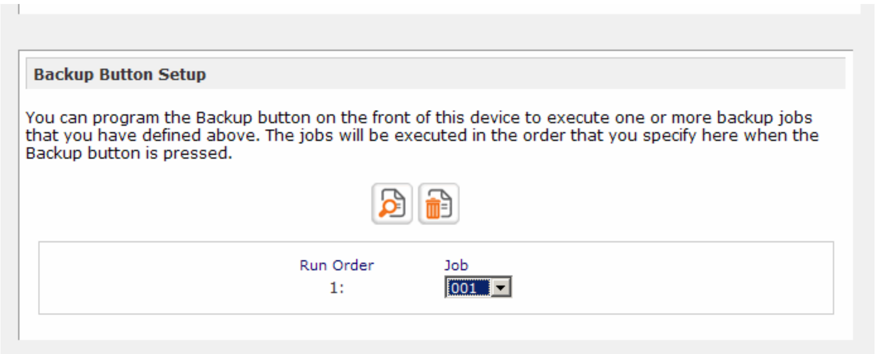
You can manually start the backup job by clicking **Go**. You will see the status change as the backup is started, encounters an error, or is finished.

Click **View Logs** 🔍 to check a detailed status of the backup.

Click **Clear Logs** 🗑 to clear the current log detail.

Programming the Backup Button

On ioSafe R4 systems you can program the backup button to execute one or more pre-defined backup jobs. Simply select the backup jobs in the order that you want them run and click **Apply**. Pressing the Backup Button once will start the job(s).



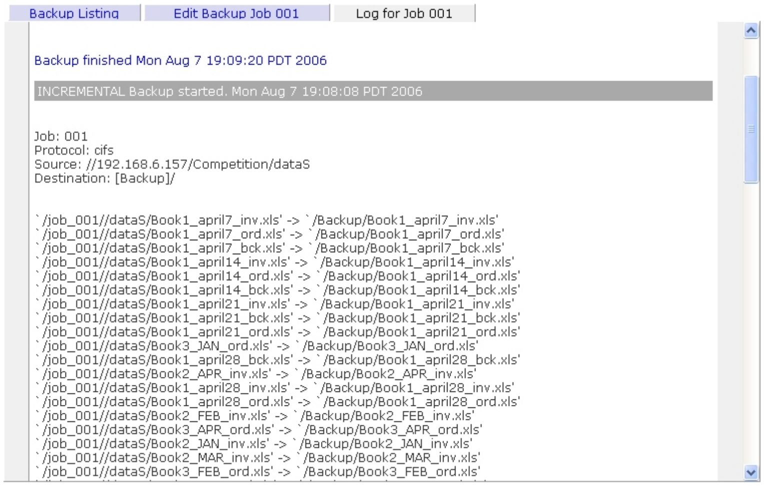
Backup Button Setup

You can program the Backup button on the front of this device to execute one or more backup jobs that you have defined above. The jobs will be executed in the order that you specify here when the Backup button is pressed.

Run Order	Job
1:	001

Viewing the Backup Log

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



```
Backup finished Mon Aug 7 19:09:20 PDT 2006

INCREMENTAL Backup started. Mon Aug 7 19:08:08 PDT 2006


Job: 001
Protocol: cifs
Source: //192.168.6.157/Competition/dataS
Destination: [Backup]/


`/job_001//dataS/Book1_april7_inv.xls' -> `/Backup/Book1_april7_inv.xls'
`/job_001//dataS/Book1_april7_ord.xls' -> `/Backup/Book1_april7_ord.xls'
`/job_001//dataS/Book1_april7_bck.xls' -> `/Backup/Book1_april7_bck.xls'
`/job_001//dataS/Book1_april14_inv.xls' -> `/Backup/Book1_april14_inv.xls'
`/job_001//dataS/Book1_april14_ord.xls' -> `/Backup/Book1_april14_ord.xls'
`/job_001//dataS/Book1_april14_bck.xls' -> `/Backup/Book1_april14_bck.xls'
`/job_001//dataS/Book1_april21_inv.xls' -> `/Backup/Book1_april21_inv.xls'
`/job_001//dataS/Book1_april21_bck.xls' -> `/Backup/Book1_april21_bck.xls'
`/job_001//dataS/Book1_april21_ord.xls' -> `/Backup/Book1_april21_ord.xls'
`/job_001//dataS/Book3_JAN_ord.xls' -> `/Backup/Book3_JAN_ord.xls'
`/job_001//dataS/Book1_april28_bck.xls' -> `/Backup/Book1_april28_bck.xls'
`/job_001//dataS/Book2_APR_inv.xls' -> `/Backup/Book2_APR_inv.xls'
`/job_001//dataS/Book1_april28_inv.xls' -> `/Backup/Book1_april28_inv.xls'
`/job_001//dataS/Book1_april28_ord.xls' -> `/Backup/Book1_april28_ord.xls'
`/job_001//dataS/Book2_FEB_inv.xls' -> `/Backup/Book2_FEB_inv.xls'
`/job_001//dataS/Book3_APR_ord.xls' -> `/Backup/Book3_APR_ord.xls'
`/job_001//dataS/Book2_JAN_inv.xls' -> `/Backup/Book2_JAN_inv.xls'
`/job_001//dataS/Book2_MAR_inv.xls' -> `/Backup/Book2_MAR_inv.xls'
`/job_001//dataS/Book3_FEB_ord.xls' -> `/Backup/Book3_FEB_ord.xls'
```

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

Editing a Backup Job

To edit a backup job, you can either click on the 3-digit **job number** button in the Backup Jobs screen. You can make appropriate changes or adjustments to the job.

System

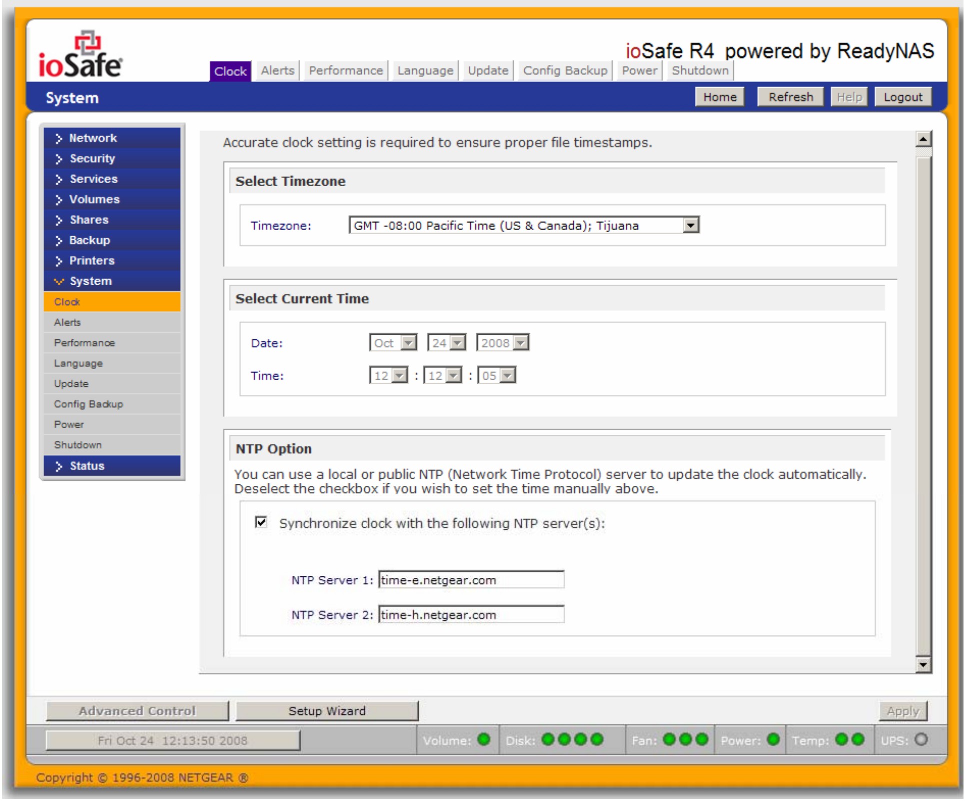
To set up and manage your ioSafe R4 system effectively, review the settings in the following sections and make any necessary changes.

Clock

An accurate time setting on the Clock screen is required to ensure proper file timestamps. You can access the Clock screen by selecting System > Clock from the main menu.

▶ SYSTEM TIME

The System Time tab in the Clock page allows you to set the date, time, and time zone. Set appropriately to ensure files maintain proper timestamp.



Accurate clock setting is required to ensure proper file timestamps.

Select Timezone

Timezone: GMT -08:00 Pacific Time (US & Canada); Tijuana

Select Current Time

Date: Oct 24 2008

Time: 12 : 12 : 05

NTP Option

You can use a local or public NTP (Network Time Protocol) server to update the clock automatically. Deselect the checkbox if you wish to set the time manually above.

☑ Synchronize clock with the following NTP server(s):

NTP Server 1: time-e.netgear.com

NTP Server 2: time-h.netgear.com

Fri Oct 24 12:13:50 2008

Copyright © 1996-2008 NETGEAR ®

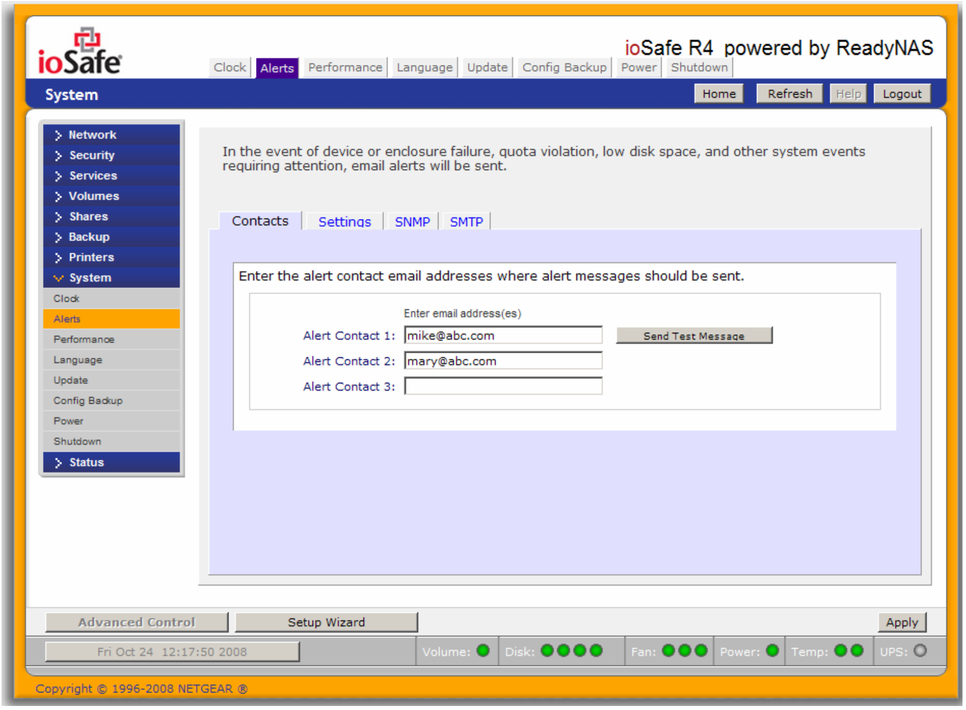
▶ NTP OPTION

You can elect to synchronize the system time on the device with a remote NTP (Network Time Protocol) server. You can elect to keep the default servers or enter up to two NTP servers closer to your locale. Available public NTP servers can be found by searching the web.

Alerts

▶ ALERTS CONTACTS

The **Contacts** tab allows you to specify up to three email addresses where system alerts will be sent. The ioSafe R4 device has a robust system monitoring feature and sends email alerts if something appears to be wrong or when a device has failed. Make sure to enter a primary email address and a backup one if possible.



In the event of device or enclosure failure, quota violation, low disk space, and other system events requiring attention, email alerts will be sent.

Enter the alert contact email addresses where alert messages should be sent.

Enter email address(es)

Alert Contact 1: mike@abc.com

Alert Contact 2: mary@abc.com

Alert Contact 3:

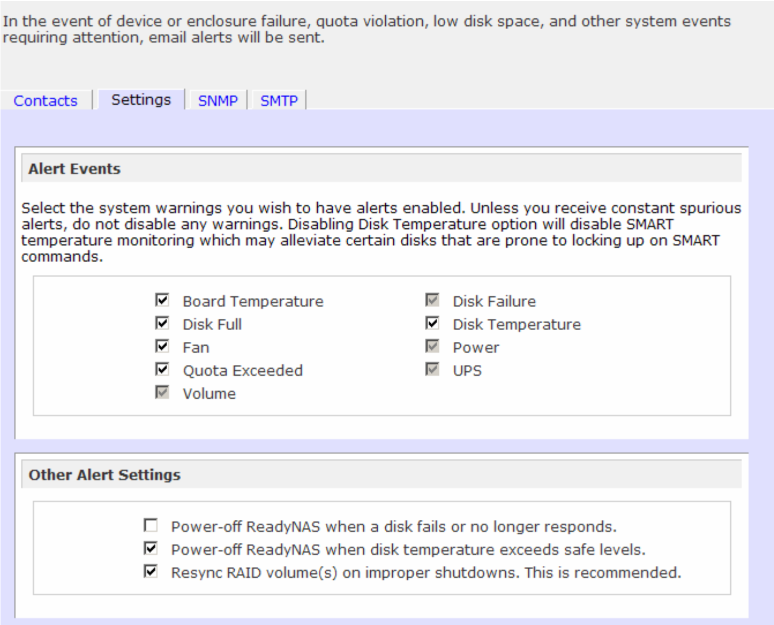
Fri Oct 24 12:17:50 2008

Copyright © 1996-2008 NETGEAR ®

Some email addresses can be tied to a mobile phone. This is a great way to monitor the device when you are away from your desk.

► ALERTS SETTINGS

This ioSafe R4 device has been pre-configured with mandatory and optional alerts for various system device warnings and failures. The **Settings** tab allows you to control the settings for the optional alerts.



In the event of device or enclosure failure, quota violation, low disk space, and other system events requiring attention, email alerts will be sent.

Alert Events

Select the system warnings you wish to have alerts enabled. Unless you receive constant spurious alerts, do not disable any warnings. Disabling Disk Temperature option will disable SMART temperature monitoring which may alleviate certain disks that are prone to locking up on SMART commands.

☑ Board Temperature
☑ Disk Full
☑ Fan
☑ Quota Exceeded
☑ Volume
☑ Disk Failure
☑ Disk Temperature
☑ Power
☑ UPS

Other Alert Settings

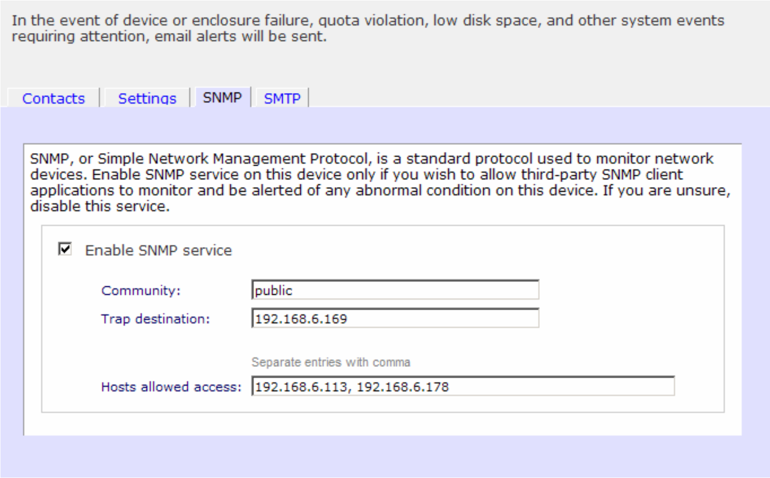
☐ Power-off ReadyNAS when a disk fails or no longer responds.
☑ Power-off ReadyNAS when disk temperature exceeds safe levels.
☑ Resync RAID volume(s) on improper shutdowns. This is recommended.

It is highly recommended that all alerts are kept enabled; however, you may choose to disable an alert if you are aware of a problem and wish to temporarily disable it.

At bottom of the tab, under the **Other Alert Settings** heading, you'll notice a couple additional options. Selecting the **Power-off NAS when a disk fails or no longer responds** option will gracefully power off the ioSafe R4 in the event that a disk failure or a disk remove event is detected. Selecting the **Power-off NAS when disk temperature exceeds safe level** will gracefully power off the ioSafe R4 when the disk temperature exceeds nominal range.

► SNMP

If you utilize a SNMP management system such as HP OpenView or CA UniCenter to monitor devices on your network, you can set up the ioSafe R4 device to work within this infrastructure.



In the event of device or enclosure failure, quota violation, low disk space, and other system events requiring attention, email alerts will be sent.

SNMP, or Simple Network Management Protocol, is a standard protocol used to monitor network devices. Enable SNMP service on this device only if you wish to allow third-party SNMP client applications to monitor and be alerted of any abnormal condition on this device. If you are unsure, disable this service.

☑ Enable SNMP service

Community: public

Trap destination: 192.168.6.169

Separate entries with comma

Hosts allowed access: 192.168.6.113, 192.168.6.178

To set up SNMP service, check the **Enable SNMP service** checkbox in the **SNMP** tab. You can leave the **Community name** as *public*, or specify a private name if you have opted for a more segregated monitoring scheme.

Next, enter a host name or an IP address for **Trap destination**. This is where all trap messages will be sent. The following system events will generate a trap:

- Abnormal power voltage
- Abnormal board enclosure temperature
- Fan failure
- UPS connected
- UPS detected power failure
- RAID disk sync started and finished
- RAID disk added, removed, and failure
- Snapshot invalidated

If you wish to limit SNMP access to only a secure list of hosts, specify the hosts in the **Hosts allowed access** field.

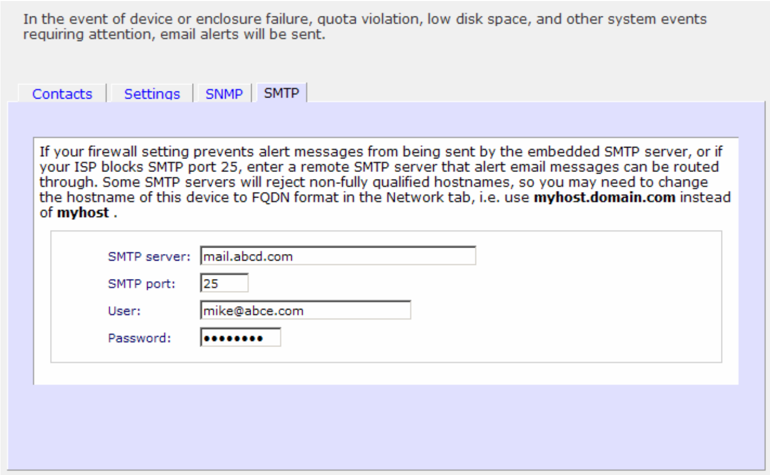
Click **Apply** to save your settings.

When you have saved the SNMP settings on the ioSafe R4, you can import the ioSafe SNMP MIB to your SNMP client application. The ioSafe MIB can be from the ioSafe Support site at http://www.iosafe.com.

► SMTP

The ioSafe R4 system has a built-in email message transfer agent (MTA) that is set up to send alert email messages from the device. Some corporate environments, however, may have a firewall that blocks untrusted MTA's from sending out messages.

If you were unable to receive the test message from the **Alerts Settings** tab, it may have been blocked by the firewall. In that case, specify an appropriate SMTP server in this tab.



In the event of device or enclosure failure, quota violation, low disk space, and other system events requiring attention, email alerts will be sent.

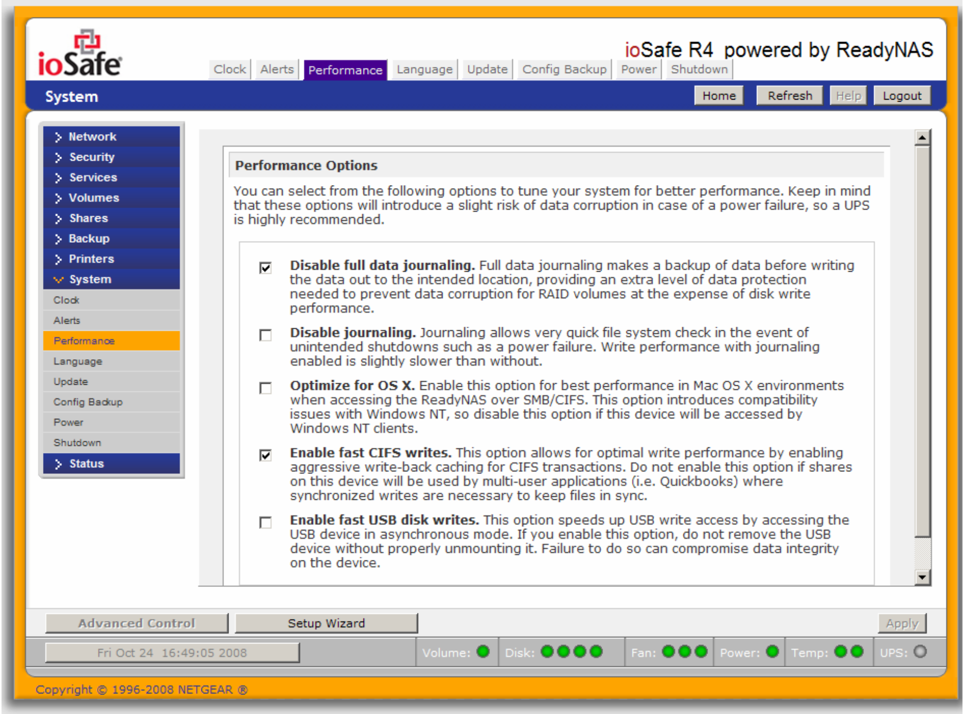
If your firewall setting prevents alert messages from being sent by the embedded SMTP server, or if your ISP blocks SMTP port 25, enter a remote SMTP server that alert email messages can be routed through. Some SMTP servers will reject non-fully qualified hostnames, so you may need to change the hostname of this device to FQDN format in the Network tab, i.e. use **myhost.domain.com** instead of **myhost** .

SMTP server: mail.abcd.com
SMTP port: 25
User: mike@abce.com
Password: ••••••••

Internet Service Providers (ISP) for home may also block untrusted MTA's. Furthermore, they may allow you to specify their SMTP server but require you to enter a user login and password to send out email – this is common with most DSL services. If this is the case, simply enter the user name and password in the fields provided.

Performance

If you wish to tweak the system performance, select the **Performance** tab in the **System** menu. Note that some of the settings suggest that you utilize an Uninterruptible Power Supply (UPS) before enabling that option.



Performance Options

You can select from the following options to tune your system for better performance. Keep in mind that these options will introduce a slight risk of data corruption in case of a power failure, so a UPS is highly recommended.

☑ **Disable full data journaling.** Full data journaling makes a backup of data before writing the data out to the intended location, providing an extra level of data protection needed to prevent data corruption for RAID volumes at the expense of disk write performance.

□ **Disable journaling.** Journaling allows very quick file system check in the event of unintended shutdowns such as a power failure. Write performance with journaling enabled is slightly slower than without.

□ **Optimize for OS X.** Enable this option for best performance in Mac OS X environments when accessing the ReadyNAS over SMB/CIFS. This option introduces compatibility issues with Windows NT, so disable this option if this device will be accessed by Windows NT clients.

☑ **Enable fast CIFS writes.** This option allows for optimal write performance by enabling aggressive write-back caching for CIFS transactions. Do not enable this option if shares on this device will be used by multi-user applications (i.e. Quickbooks) where synchronized writes are necessary to keep files in sync.

□ **Enable fast USB disk writes.** This option speeds up USB write access by accessing the USB device in asynchronous mode. If you enable this option, do not remove the USB device without properly unmounting it. Failure to do so can compromise data integrity on the device.

Select **Disable full data journaling** to substantially improve disk write performance. During an unexpected power down without battery backup, there is a small chance that parity written to a disk in a RAID set may become out of sync with the data disks, possibly causing incorrect data to be recovered if one disk fails.

Select **Disable journaling** if you understand the consequences of this action, and you do not mind a long file system check (only after unexpected power failures). File system journaling allows disk checks of only a few seconds verses possibly an hour or longer without journaling. Disabling journaling will improve disk write performance slightly.

Note

You can buy a UPS with USB monitoring at a very reasonable cost. By safely allowing the performance options to be checked, you can effectively double your write performance and provide uninterrupted service of your ioSafe R4 for a very low price.

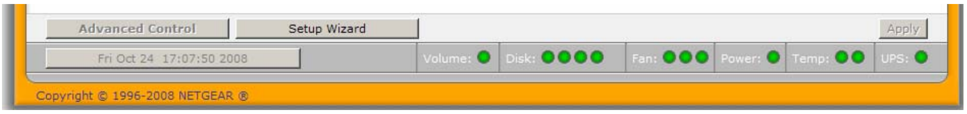
The **Optimize for OS X** option provides the best performance in Mac OS X environments when connected to the ioSafe R4 through the SMB/CIFS protocol. This option however introduces compatibility issues with Windows NT 4.0; do not enable this option if this device will be accessed by Windows NT 4.0 clients.

The **Enable fast CIFS writes** option allows for fast write performance by enabling aggressive write-back caching over CIFS. Do not enable this option in multi-user application environments such as Quickbooks where synchronized writes are necessary to keep files in sync.

The **Enable fast USB disk writes** option speeds up USB write access by accessing the USB device in asynchronous mode. If you enable this option, do not remove the USB device without properly unmounting it. Failure to do so can compromise data integrity on the device.

► ADDING A UPS FOR PERFORMANCE

Adding a UPS to the NAS is an easy way to protect against power failures, but as mentioned in the **System Performance** section, a UPS can also safely allow for a more aggressive performance setting. Simply connect the NAS power cable to the UPS and connect the UPS USB monitoring cable between the UPS and the NAS. The UPS will be detected automatically and will show up in the Status bar. You can move the mouse pointer over the UPS LED icon to display the current UPS information and battery life.



Note

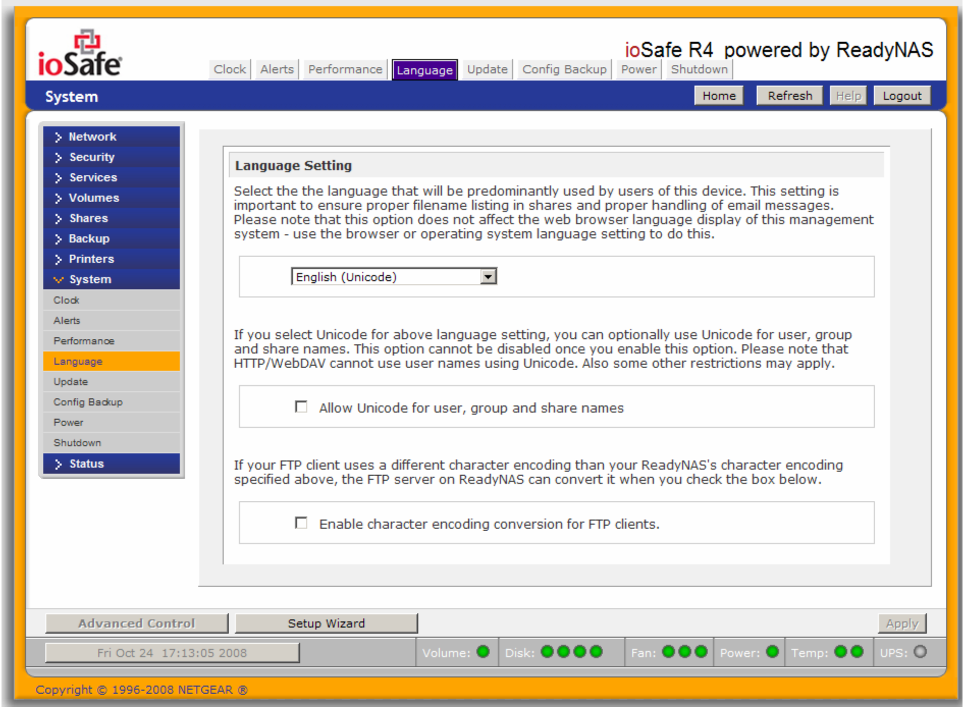
Alert notification and automatic system optimization is available only with a UPS that utilizes a USB monitoring interface.

You are notified by email whenever the status of the UPS changes; for example, when a power failure forces the UPS to be in battery mode or when the battery is low. When the battery is low, the NAS device automatically shuts down safely.

Make sure to adjust the optimization settings in the Performance tab if you wish to take advantage of the available options.

Language

The **Language** tab offers the option of setting the ioSafe R4 device to the appropriate character set for file names.



Language Setting

Select the the language that will be predominantly used by users of this device. This setting is important to ensure proper filename listing in shares and proper handling of email messages. Please note that this option does not affect the web browser language display of this management system - use the browser or operating system language setting to do this.

English (Unicode)

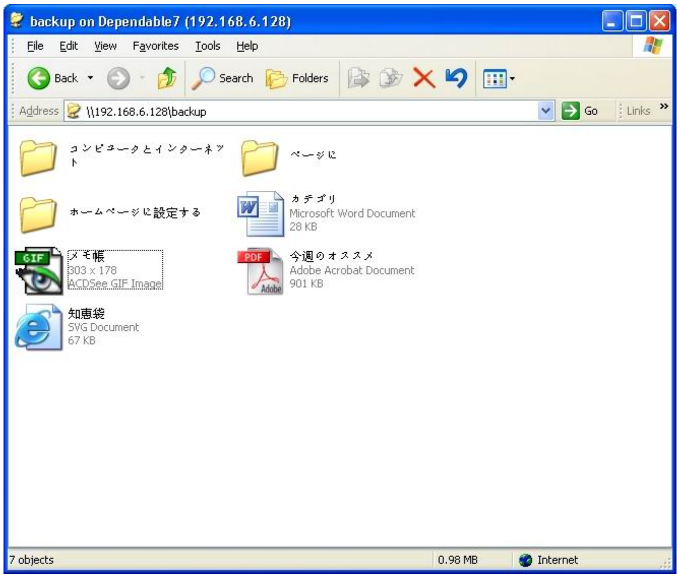
If you select Unicode for above language setting, you can optionally use Unicode for user, group and share names. This option cannot be disabled once you enable this option. Please note that HTTP/WebDAV cannot use user names using Unicode. Also some other restrictions may apply.

☐ Allow Unicode for user, group and share names

If your FTP client uses a different character encoding than your ReadyNAS's character encoding specified above, the FTP server on ReadyNAS can convert it when you check the box below.

☐ Enable character encoding conversion for FTP clients.

For example, selecting Japanese allows sharing of files with Japanese names in Windows Explorer.



Address: \\192.168.6.128\backup

コンピュータとインターネット

ページに

ホームページに設定する

カテゴリ
Microsoft Word Document
28 KB

メモ帳
303 x 178
ACDSee GIF Image

今週のオススメ
Adobe Acrobat Document
901 KB

知恵袋
SVG Document
67 KB

7 objects | 0.98 MB | Internet

It is best to select the appropriate language based on the region that this device will operate in.

> Note
>
> This option does not set the web browser language display – browser settings must be done using the browser language option.

Unicode for User, Group, and Share Names

If desired, you can elect to enable use of Unicode for user, group, and share names, allowing for greater flexibility in non-English speaking regions. This option, once selected, cannot be reversed.

> Note
>
> HTTP and WebDAV access will not work with Unicode user names. Other restrictions may exist.

Enable Character encoding conversion for FTP clients

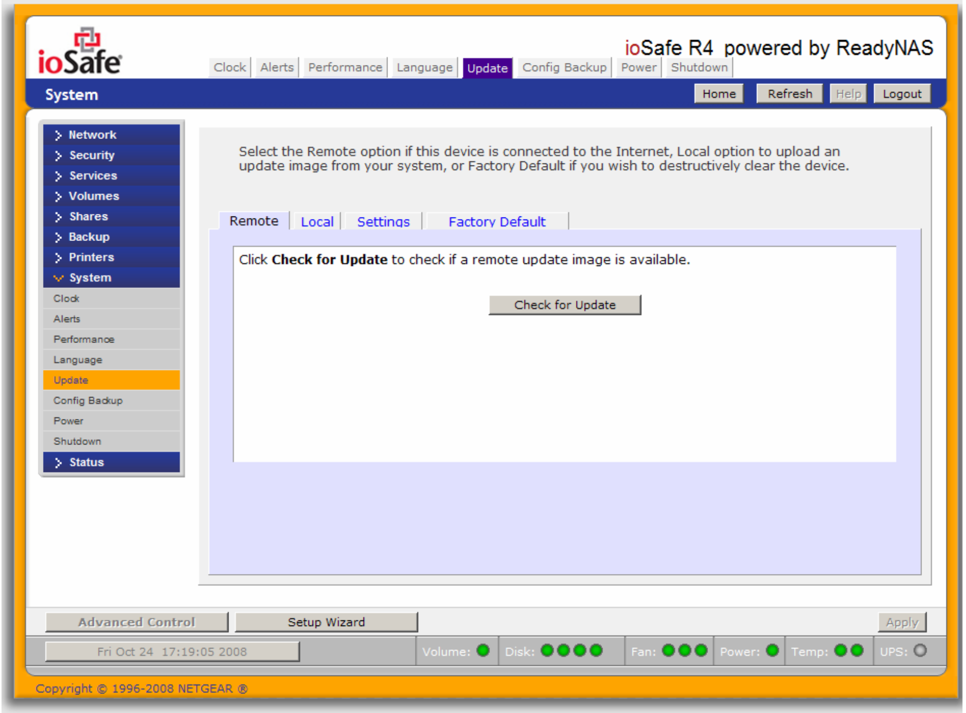
If your FTP client uses different character encoding from the NAS character encoding specified in Unicode, the NAS FTP server will convert to it if this option is selected.

Updating ioSafe R4

The ioSafe R4 device offers the option of upgrading the operating firmware either automatically using the Remote Update option or manually loading an update image downloaded from the ioSafe Support website.

► REMOTE UPDATE

The preferred and quicker method if the ioSafe R4 has Internet access is the **Remote** update option.



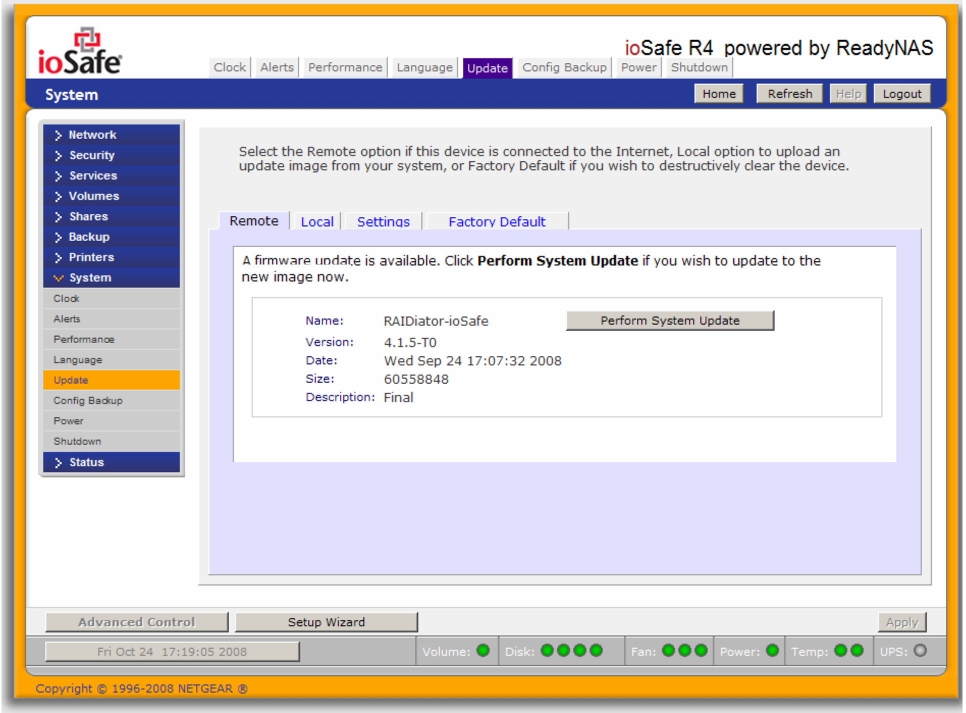
Select the Remote option if this device is connected to the Internet, Local option to upload an update image from your system, or Factory Default if you wish to destructively clear the device.

Click **Check for Update** to check if a remote update image is available.

Fri Oct 24 17:19:05 2008

Copyright © 1996-2008 NETGEAR ®

Simply click Check for Update to check for updates on the ioSafe update server.



Select the Remote option if this device is connected to the Internet, Local option to upload an update image from your system, or Factory Default if you wish to destructively clear the device.

A firmware update is available. Click **Perform System Update** if you wish to update to the new image now.

Name: RAIDiator-ioSafe
Version: 4.1.5-T0
Date: Wed Sep 24 17:07:32 2008
Size: 60558848
Description: Final

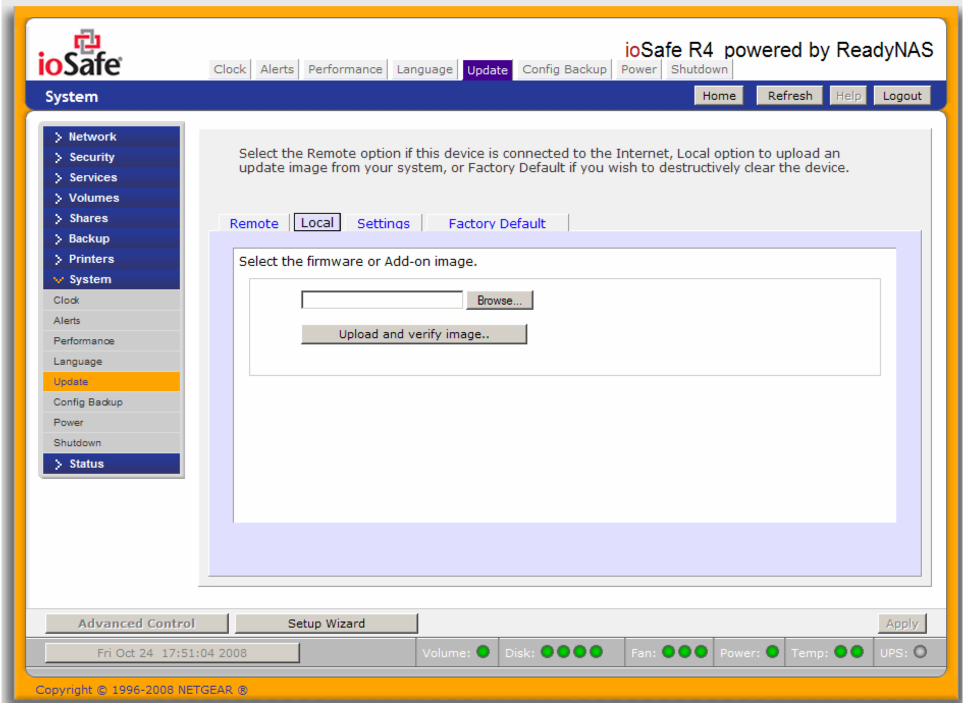
Fri Oct 24 17:19:05 2008

Copyright © 1996-2008 NETGEAR ®

If you wish to continue, click **Perform System Update**. After the update image has been downloaded, you will be asked to reboot the system. The update process only updates the firmware image and does not modify your data volume. However, it is always a good idea to backup your important data whenever you perform an update.

► LOCAL UPDATE

When the ioSafe R4 device is not connected to the Internet, or Internet access is blocked, you can download an update file from the Support site and upload that file to the ioSafe R4 in the **Local** update tab.



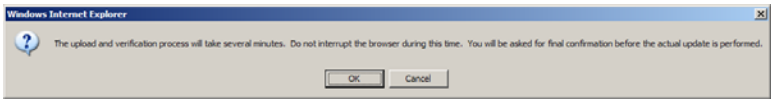
Select the Remote option if this device is connected to the Internet, Local option to upload an update image from your system, or Factory Default if you wish to destructively clear the device.

Select the firmware or Add-on image.

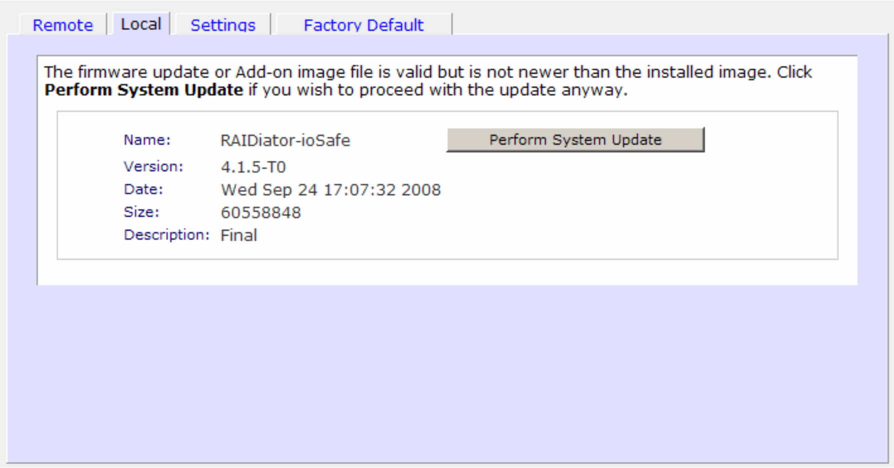
Fri Oct 24 17:51:04 2008

Copyright © 1996-2008 NETGEAR ®

Click on the Browse button to select the update file and click the **Upload and verify image** button. The process will take several minutes at which time can click the **Perform System Update** button. You will be requested to reboot the system to proceed with the upgrade. **DO NOT click on the browser Refresh button** during the update process.



The upload and verification process will take several minutes. Do not interrupt the browser during this time. You will be asked for final confirmation before the actual update is performed.

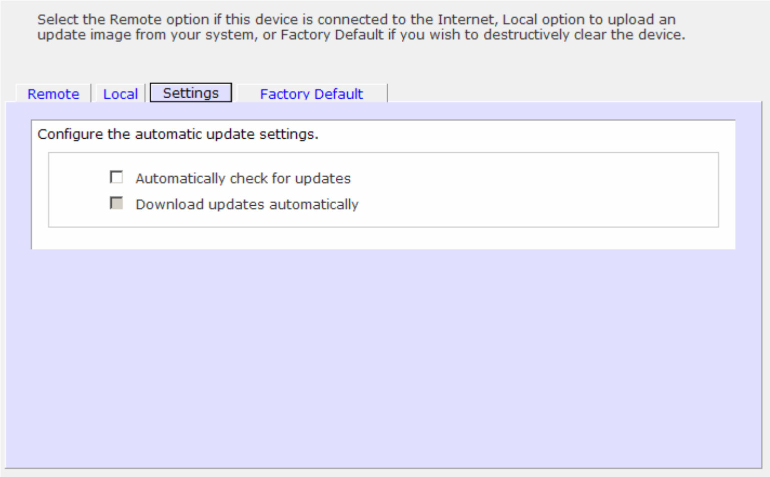


The firmware update or Add-on image file is valid but is not newer than the installed image. Click **Perform System Update** if you wish to proceed with the update anyway.

Name: RAIDiator-ioSafe
Version: 4.1.5-T0
Date: Wed Sep 24 17:07:32 2008
Size: 60558848
Description: Final

► SETTINGS

If you do have reliable Internet connection, you can enable the automatic update check and download options in the Settings tab.



Select the Remote option if this device is connected to the Internet, Local option to upload an update image from your system, or Factory Default if you wish to destructively clear the device.

Configure the automatic update settings.

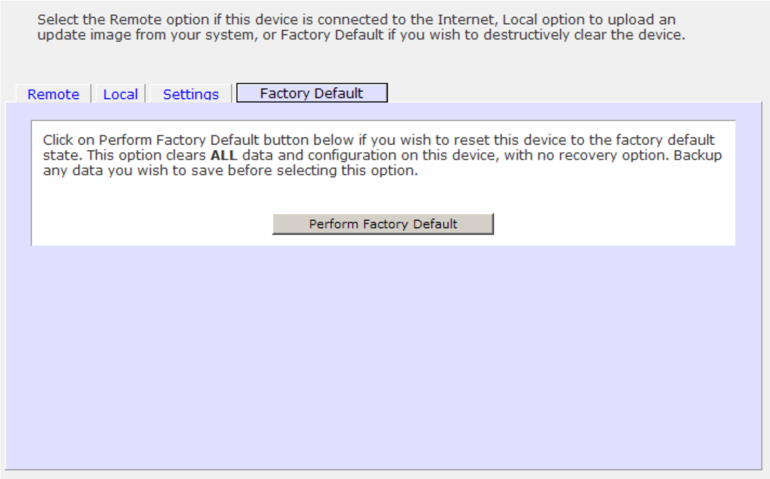
☐ Automatically check for updates

☐ Download updates automatically

If you enable the **Automatically check for updates** option, the ioSafe R4 will not download the actual firmware update, but will notify you when an update is available. If you enable the **Download updates automatically** option, the update image will be downloaded, and you will be notified by email to reboot to the device to perform the update.

► FACTORY DEFAULT

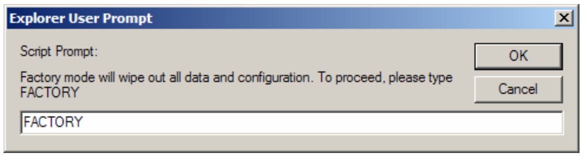
The **Factory Default** tab allows you to set the ioSafe R4 device back to factory default. Choose this option carefully as **ALL DATA WILL BE LOST**, and remember to back up any data that you wish to keep.



Select the Remote option if this device is connected to the Internet, Local option to upload an update image from your system, or Factory Default if you wish to destructively clear the device.

Click on Perform Factory Default button below if you wish to reset this device to the factory default state. This option clears **ALL** data and configuration on this device, with no recovery option. Backup any data you wish to save before selecting this option.

You will be asked to confirm the command by typing: **FACTORY**



Script Prompt:

Factory mode will wipe out all data and configuration. To proceed, please type FACTORY

FACTORY

Warning

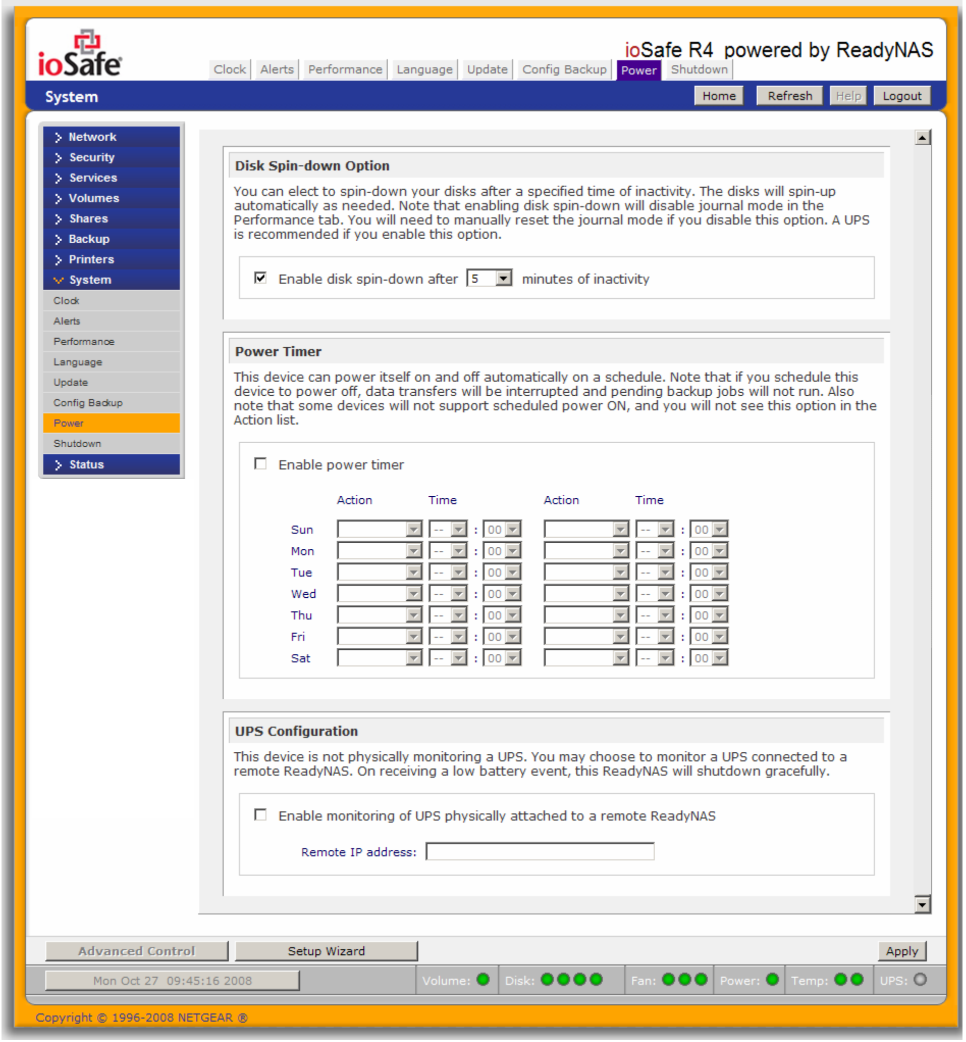
Resetting to Factory Default will erase everything, including data shares, volume(s), user and group accounts, and configuration information. There is **no way to recover** after you confirm this command.

Power Management

The ioSafe R4 offers a couple of power management options to reduce the system's power consumption while it is in use and when it is expected to not be in use.

▶ DISK SPIN-DOWN OPTION

You can elect to spin-down your ioSafe R4 disks after a specified time of inactivity. The disks will spin-up as needed.



Disk Spin-down Option

You can elect to spin-down your disks after a specified time of inactivity. The disks will spin-up automatically as needed. Note that enabling disk spin-down will disable journal mode in the Performance tab. You will need to manually reset the journal mode if you disable this option. A UPS is recommended if you enable this option.

☑ Enable disk spin-down after 5 minutes of inactivity

Power Timer

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

☐ Enable power timer

	Action	Time	Action	Time
Sun		-- : 00		-- : 00
Mon		-- : 00		-- : 00
Tue		-- : 00		-- : 00
Wed		-- : 00		-- : 00
Thu		-- : 00		-- : 00
Fri		-- : 00		-- : 00
Sat		-- : 00		-- : 00

UPS Configuration

This device is not physically monitoring a UPS. You may choose to monitor a UPS connected to a remote ReadyNAS. On receiving a low battery event, this ReadyNAS will shutdown gracefully.

☐ Enable monitoring of UPS physically attached to a remote ReadyNAS

Remote IP address:

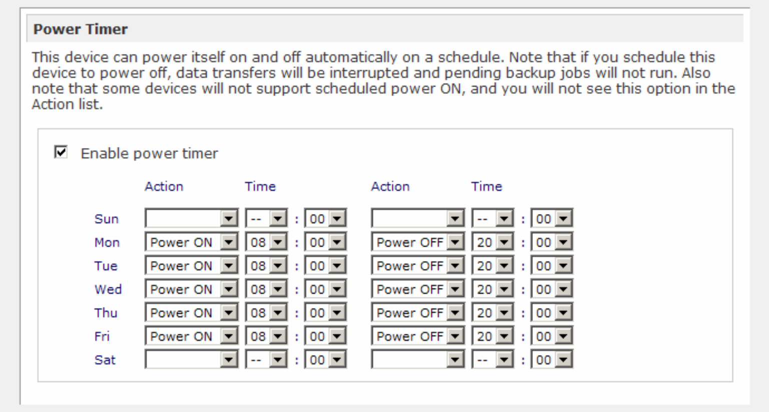
Mon Oct 27 09:45:16 2008

Note

Enabling disk spin-down will disable journal mode. Once enabled, if you decide to disable disk spin-down, you will need to manually re-enable journal mode if desired. A UPS is recommended if you utilize this option.

► POWER TIMER

The ioSafe R4 can be scheduled to power off and power back on automatically. Select the **Enable power timer** checkbox and enter the desired action and time.



Power Timer

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

☑ Enable power timer

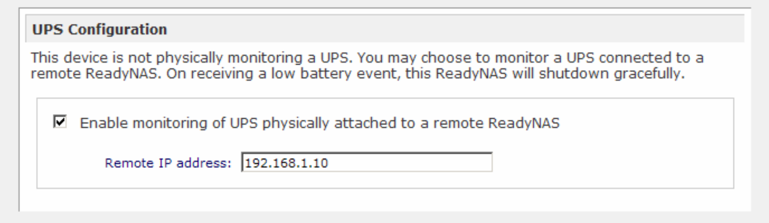
	Action	Time		Action	Time	
Sun		--	00		--	00
Mon	Power ON	08	00	Power OFF	20	00
Tue	Power ON	08	00	Power OFF	20	00
Wed	Power ON	08	00	Power OFF	20	00
Thu	Power ON	08	00	Power OFF	20	00
Fri	Power ON	08	00	Power OFF	20	00
Sat		--	00		--	00

Note

When the ioSafe R4 is powered off, any file transfers and backup jobs will be interrupted, and backup jobs scheduled during the power off state will not be run.

► UPS CONFIGURATION

If this device is sharing a UPS with another ioSafe R4 system, but not directly monitoring the battery status through a USB connection, you may elect to **Enable monitoring of UPS physically attached to a remote ReadyNAS**. To use this feature, check the box and enter the IP Address in the **Remote IP address** field of the ioSafe R4 system that is monitoring the UPS battery status.



UPS Configuration

This device is not physically monitoring a UPS. You may choose to monitor a UPS connected to a remote ReadyNAS. On receiving a low battery event, this ReadyNAS will shutdown gracefully.

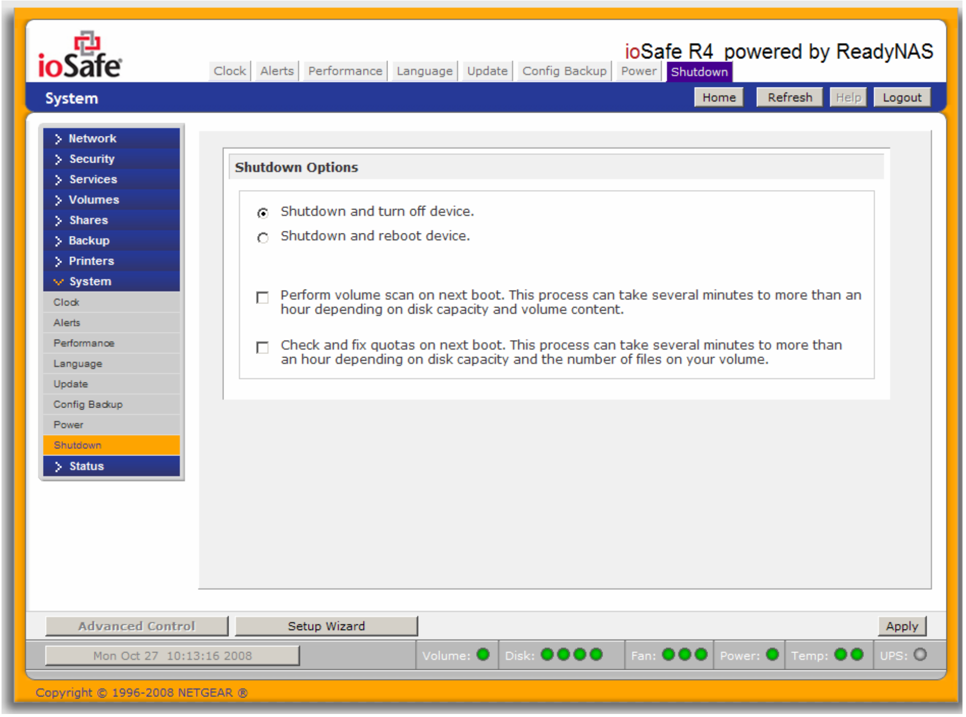
☑ Enable monitoring of UPS physically attached to a remote ReadyNAS

Remote IP address: 192.168.1.10

As an option, the ioSafe R4 can remotely monitor the UPS when connected to a PC running Network UPS Tools (NUT). For more information about NUT, see http://www.networkupstools.org/.

Shutdown

The Shutdown tab offers the option to power-off or reboot the ioSafe R4 device.



Shutdown Options

● Shutdown and turn off device.

○ Shutdown and reboot device.

□ Perform volume scan on next boot. This process can take several minutes to more than an hour depending on disk capacity and volume content.

□ Check and fix quotas on next boot. This process can take several minutes to more than an hour depending on disk capacity and the number of files on your volume.

You have the option of performing a full file system check or quota check on the next boot. Both these options can take several minutes to several hours depending on the size of your volume and the number of files in the volume. You do not need to select these options unless you suspect there might be data or quota integrity problems.

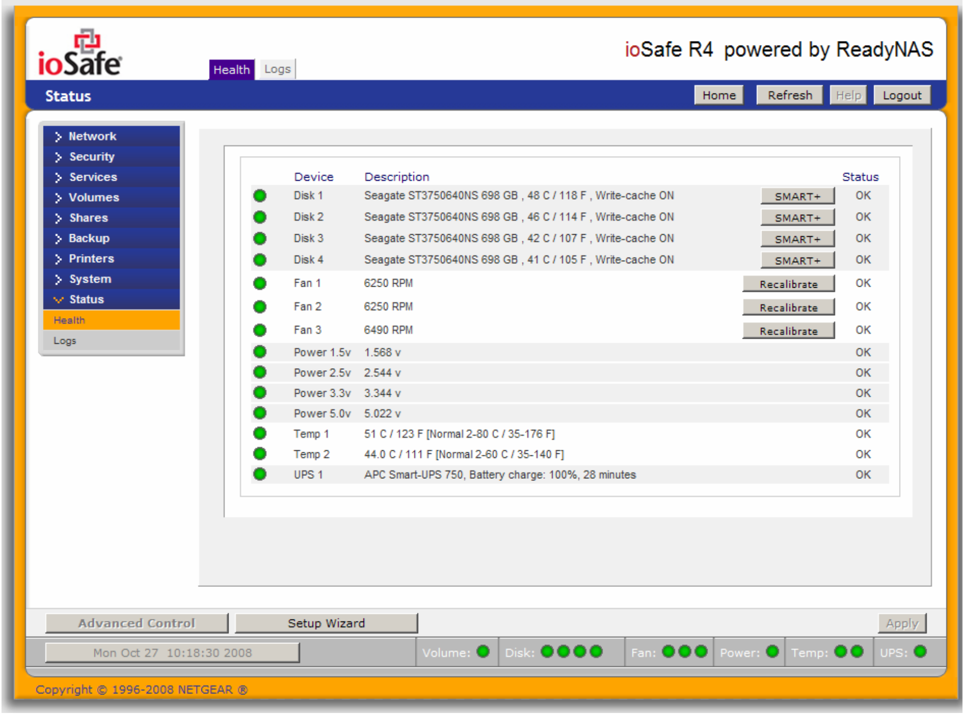
When you reboot or shutdown the ioSafe R4, you will need to close the browser window and use RAIDar to reconnect to FrontView.

Status

The Status page consists of the **Health** and **Logs** tabs providing system status information.

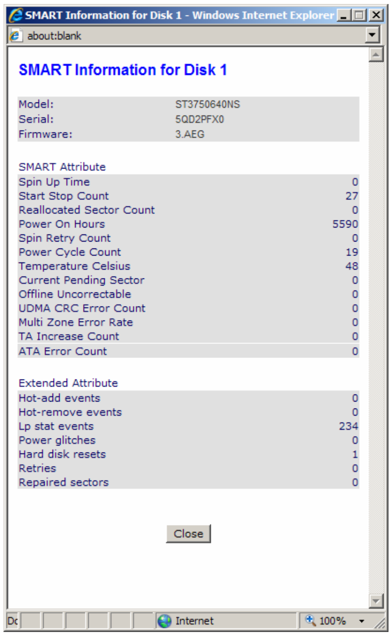
Health

The **Health** page displays the disk, fan, power, temperature, and UPS status in detail. When available, normal expected values are provided.



	Device	Description		Status
●	Disk 1	Seagate ST3750640NS 698 GB , 48 C / 118 F , Write-cache ON	SMART+	OK
●	Disk 2	Seagate ST3750640NS 698 GB , 46 C / 114 F , Write-cache ON	SMART+	OK
●	Disk 3	Seagate ST3750640NS 698 GB , 42 C / 107 F , Write-cache ON	SMART+	OK
●	Disk 4	Seagate ST3750640NS 698 GB , 41 C / 105 F , Write-cache ON	SMART+	OK
●	Fan 1	6250 RPM	Recalibrate	OK
●	Fan 2	6250 RPM	Recalibrate	OK
●	Fan 3	6490 RPM	Recalibrate	OK
●	Power 1.5v	1.568 v		OK
●	Power 2.5v	2.544 v		OK
●	Power 3.3v	3.344 v		OK
●	Power 5.0v	5.022 v		OK
●	Temp 1	51 C / 123 F [Normal 2-80 C / 35-176 F]		OK
●	Temp 2	44.0 C / 111 F [Normal 2-60 C / 35-140 F]		OK
●	UPS 1	APC Smart-UPS 750, Battery charge: 100%, 28 minutes		OK

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



SMART Information for Disk 1

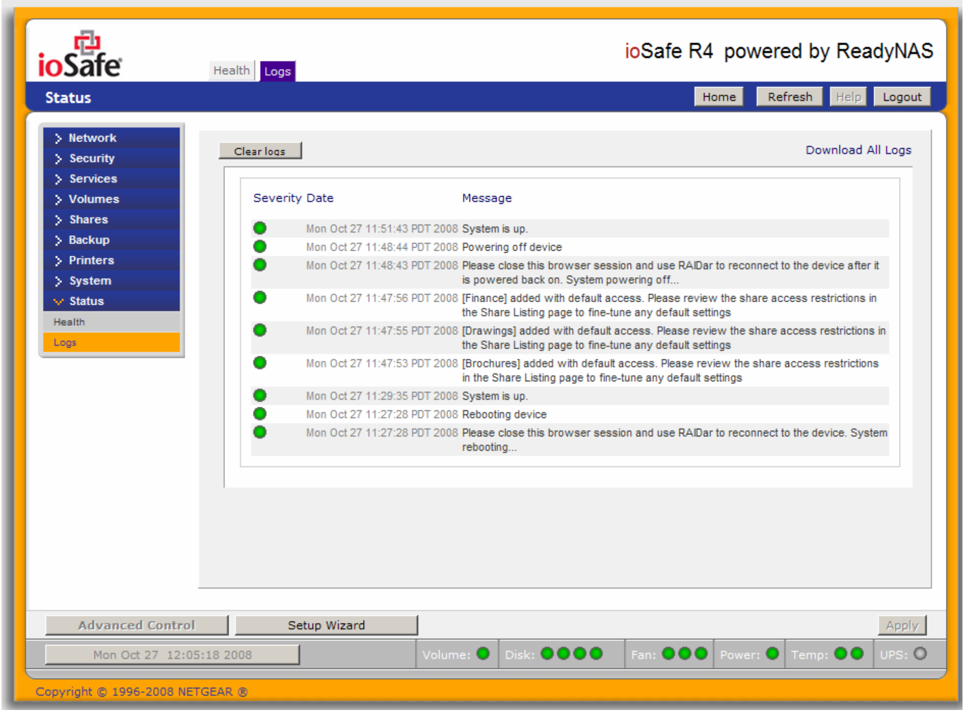
Model:	ST3750640NS
Serial:	5QD2PFX0
Firmware:	3.AEG

SMART Attribute	
Spin Up Time	0
Start Stop Count	27
Reallocated Sector Count	0
Power On Hours	5590
Spin Retry Count	0
Power Cycle Count	19
Temperature Celsius	48
Current Pending Sector	0
Offline Uncorrectable	0
UDMA CRC Error Count	0
Multi Zone Error Rate	0
TA Increase Count	0
ATA Error Count	0

Extended Attribute	
Hot-add events	0
Hot-remove events	0
Lp stat events	234
Power glitches	0
Hard disk resets	1
Retries	0
Repaired sectors	0

Logs

The Logs tab provides status information of management tasks along with a timestamp.



Severity	Date	Message
●	Mon Oct 27 11:51:43 PDT 2008	System is up.
●	Mon Oct 27 11:48:44 PDT 2008	Powering off device
●	Mon Oct 27 11:48:43 PDT 2008	Please close this browser session and use RAIDar to reconnect to the device after it is powered back on. System powering off...
●	Mon Oct 27 11:47:56 PDT 2008	[Finance] added with default access. Please review the share access restrictions in the Share Listing page to fine-tune any default settings
●	Mon Oct 27 11:47:55 PDT 2008	[Drawings] added with default access. Please review the share access restrictions in the Share Listing page to fine-tune any default settings
●	Mon Oct 27 11:47:53 PDT 2008	[Brochures] added with default access. Please review the share access restrictions in the Share Listing page to fine-tune any default settings
●	Mon Oct 27 11:29:35 PDT 2008	System is up.
●	Mon Oct 27 11:27:28 PDT 2008	Rebooting device
●	Mon Oct 27 11:27:28 PDT 2008	Please close this browser session and use RAIDar to reconnect to the device. System rebooting...

The **Download All Logs** link is available in case of problems where technical support personnel may be of assistance in analyzing low-level log information. A zip file of all logs is downloaded and can be attached to an email for further technical support.

Chapter

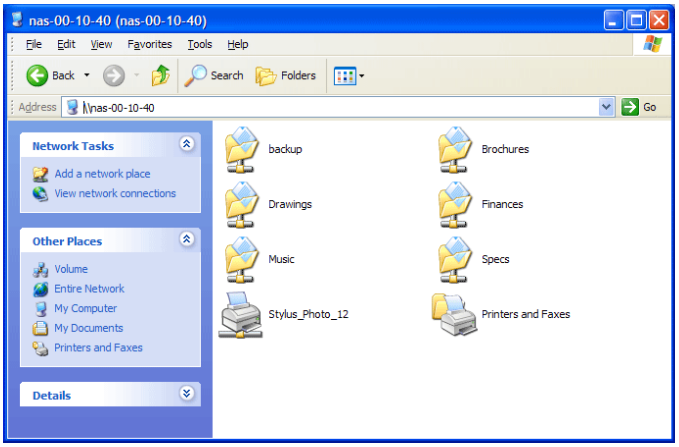
2

Accessing Shares

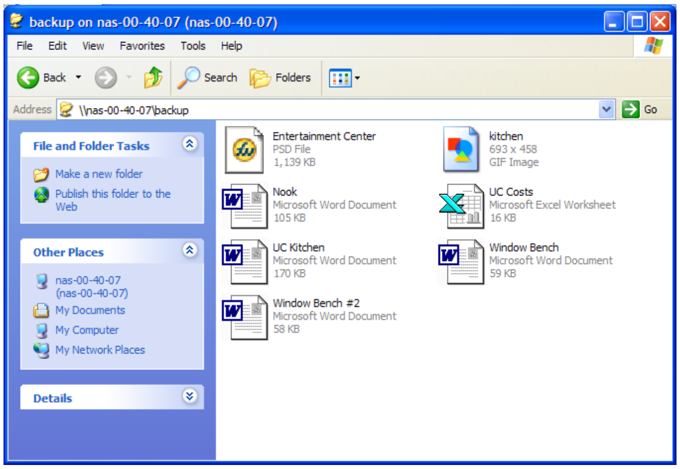
This chapter presents examples of how shares on the ioSafe R4 device can be accessed by the various operating systems. If you have problems accessing your shares, make sure to enable the corresponding service in the **Shares Services** tab. Also make sure the default access of the share is set to **Read-only** or **Read/write**.

Windows

To see a share listing under Windows, either click **Browse** in **RAIDar** or enter \\hostname or \\ip_address in the Explorer address bar. *Hostname* is the NAS hostname assigned in the Network tab. The default hostname is set to *nas-* followed by the last three hex bytes of the device MAC address.

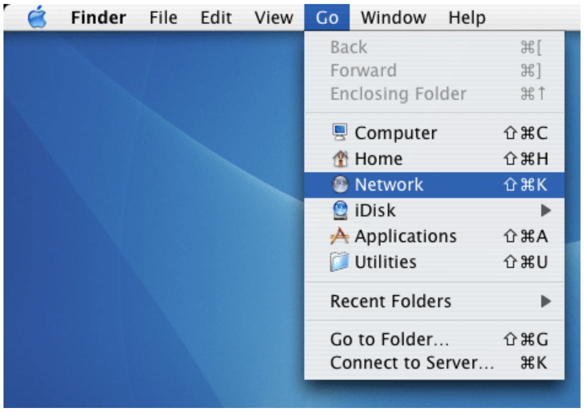


To access the share under Windows, specify the hostname followed by the share name in the Explorer address bar, i.e. \\hostname\backup, as follows:



MAC OS X

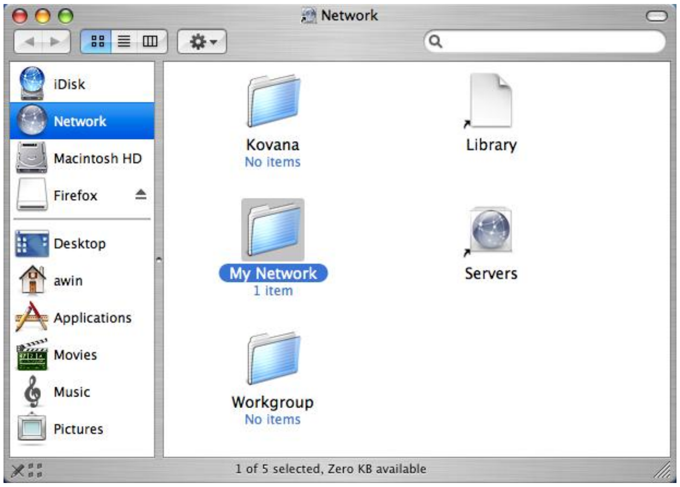
To access the same share over AFP with OS X, select **Network** from the Finder **Go** menu.



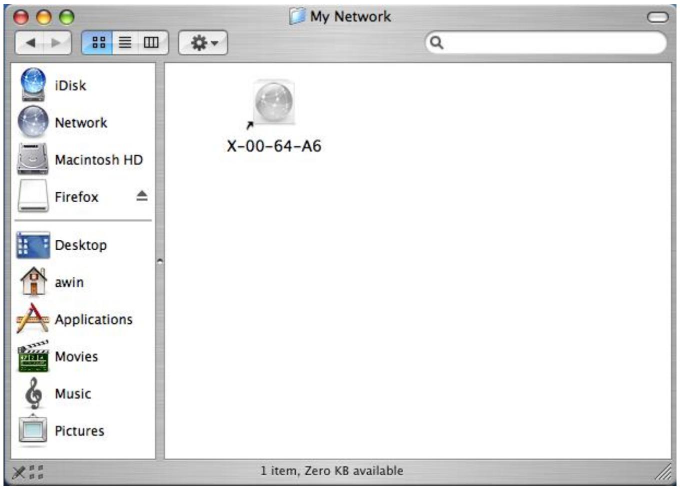
At this point, there are two ways in which you can access your AFP share, depending on how you have chosen to advertise your AFP share.

AFP over Bonjour

To access the AFP share advertised over **Bonjour** on Mac OS X, select **Network** from the Finder **Go** menu to see a listing of available networks.

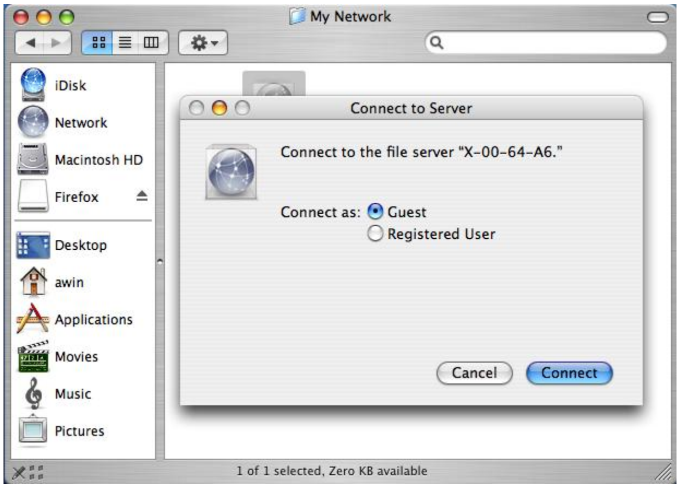


Open the **My Network** folder to display the ioSafe R4 hostname.



1 item, Zero KB available

Double-click on the hostname icon to display the share listing.



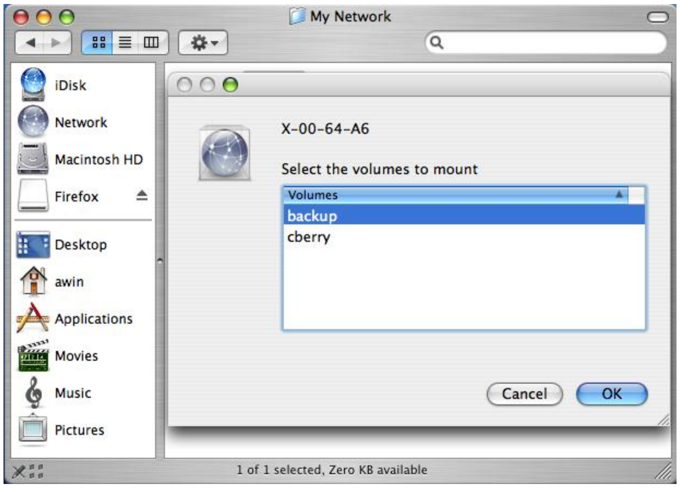
Connect to Server

Connect to the file server "X-00-64-A6."

Connect as: ● Guest
○ Registered User

1 of 1 selected, Zero KB available

In **Share** security mode, simply select **"Guest"** to access the shares. In **User** or **Domain** security mode, enter the user name and password you wish to connect to the ioSafe R4 as.



X-00-64-A6

Select the volumes to mount

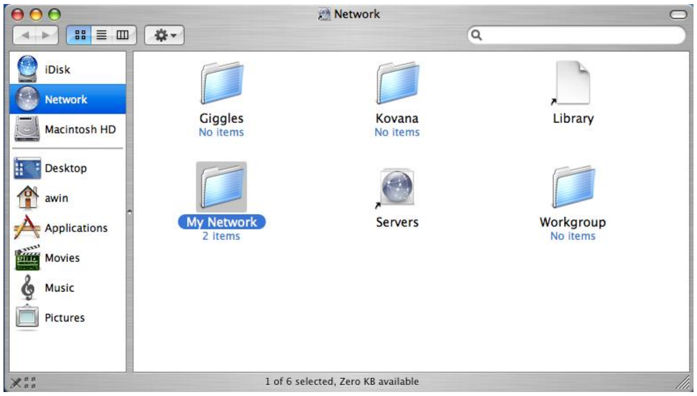
Volumes
backup
cberry

1 of 1 selected, Zero KB available

Select the Share you would like to view.

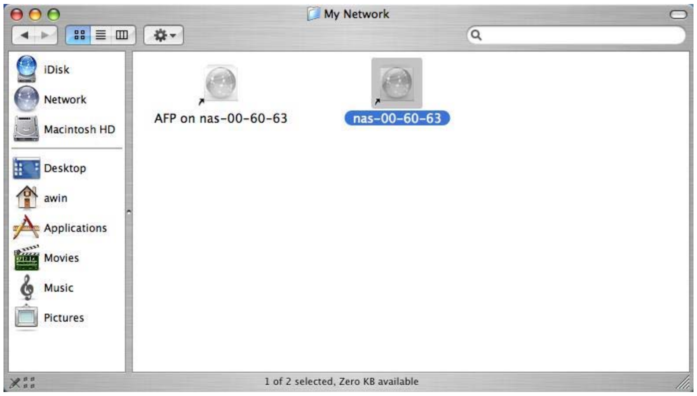
AFP over AppleTalk

If you had chosen to advertise your AFP service over AppleTalk, you will see a listing of available networks.



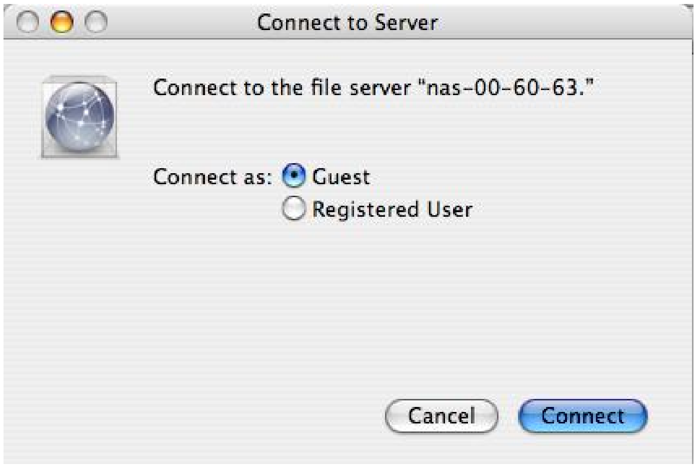
1 of 6 selected, Zero KB available

Open the **My Network** folder to display the ioSafe R4 hostname. Select the one that has the hostname only.



1 of 2 selected, Zero KB available

You'll be prompted with a connection box.

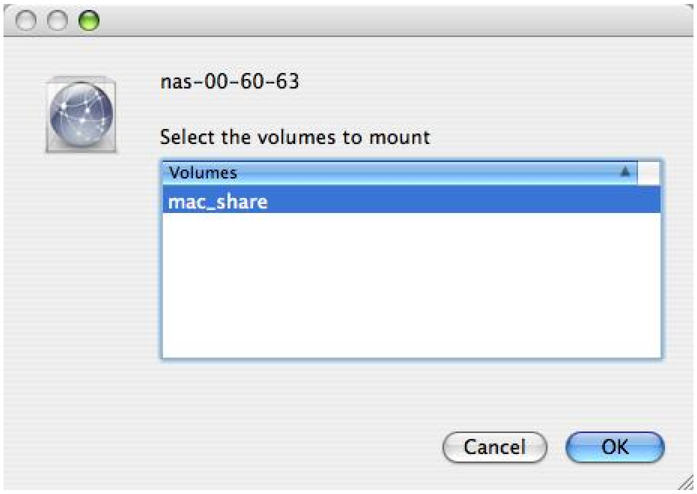


Connect to Server

Connect to the file server "nas-00-60-63."

Connect as: ● Guest
○ Registered User

Select **Guest** and then the share you wish to connect to, and click **OK**.



nas-00-60-63

Select the volumes to mount

Volumes

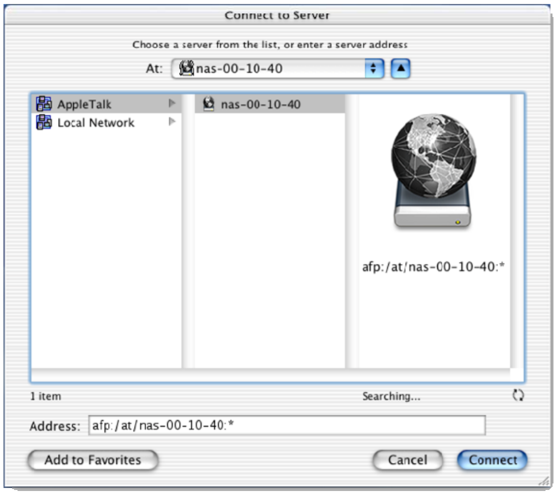
mac_share

In **Share** security mode, you will need to only specify user name and password if you have set up a password for your share. Enter the share name in place of the user name. In **User** or **Domain** security mode, enter the user name and password you wish to connect to the ioSafe R4 as.

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

MAC OS 9

To access the same share under Mac OS 9, select Connect to Server from the Finder menu, choose the NAS device entry from the AppleTalk selection, and click **Connect**.



Connect to Server

Choose a server from the list, or enter a server address

At: nas-00-10-40

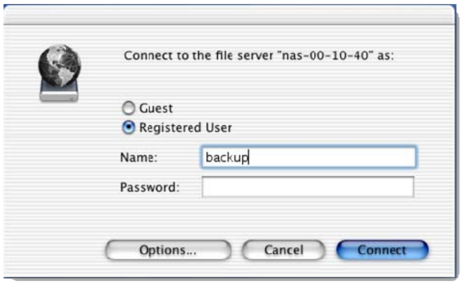
afp:/at/nas-00-10-40:*

1 item

Searching...

Address: afp:/at/nas-00-10-40:*

When you are prompted to login, enter the **share name** and **password** if the ioSafe R4 is configured for **Share** security mode, or enter a valid **user account** and **password** otherwise, and click **Commect.**



Connect to the file server "nas-00-10-40" as:

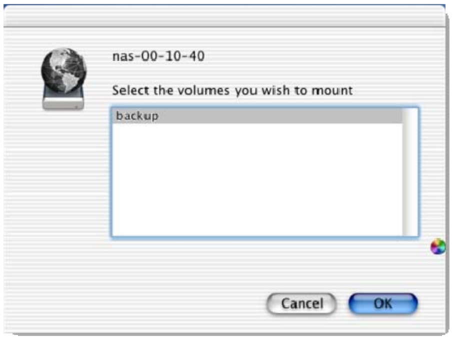
○ Guest

● Registered User

Name: backup

Password:

If no share password is set in Share mode, you can select Guest user and leave the password field blank. If your login is successful, you will be given a listing of one or more shares. Select the share you wish to connect to and click **OK**.

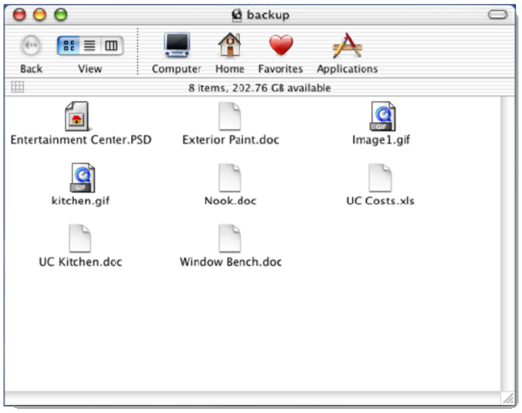


nas-00-10-40

Select the volumes you wish to mount

backup

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

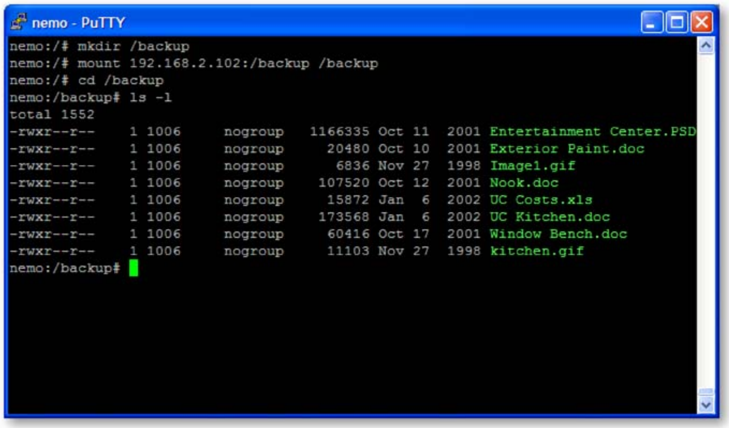


Linux/Unix

To access this share from a Linux or Unix client, you will need to mount the share over NFS, i.e. type:

```
mount ipaddr:/backup /backup
```

where **backup** is the share name. Running the **ls** command in the mounted path displays the share content.



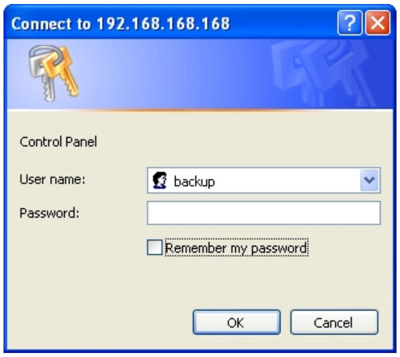
```
nemo:/# mkdir /backup
nemo:/# mount 192.168.2.102:/backup /backup
nemo:/# cd /backup
nemo:/backup# ls -l
total 1552
-rwxr--r--    1 1006     nogroup   1166335 Oct 11  2001 Entertainment Center.PSD
-rwxr--r--    1 1006     nogroup     20480 Oct 10  2001 Exterior Paint.doc
-rwxr--r--    1 1006     nogroup      6836 Nov 27  1998 Image1.gif
-rwxr--r--    1 1006     nogroup    107520 Oct 12  2001 Nook.doc
-rwxr--r--    1 1006     nogroup     15872 Jan  6  2002 UC Costs.xls
-rwxr--r--    1 1006     nogroup    173568 Jan  6  2002 UC Kitchen.doc
-rwxr--r--    1 1006     nogroup     60416 Oct 17  2001 Window Bench.doc
-rwxr--r--    1 1006     nogroup     11103 Nov 27  1998 kitchen.gif
nemo:/backup# 
```

Note

The ioSafe R4 does not support NIS as it is unable to correlate NIS information with CIFS logins. In mixed environments where CIFS and NFS integration is desired, you can set the security to User mode and manually specify the UID and GID of the user and group accounts to match your NIS or other Linux/Unix server settings. The ioSafe R4 provides the ability to import a comma-delimited file containing the user and group information to coordinate Linux/Unix login settings. Please see the **Managing Users** section for more information.

Web Browser

To access the same share using a web browser, enter *http://ipaddr* in the browser address bar. You can use **https** if you want a secure encrypted connection. You will be prompted to login.



Connect to 192.168.168.168

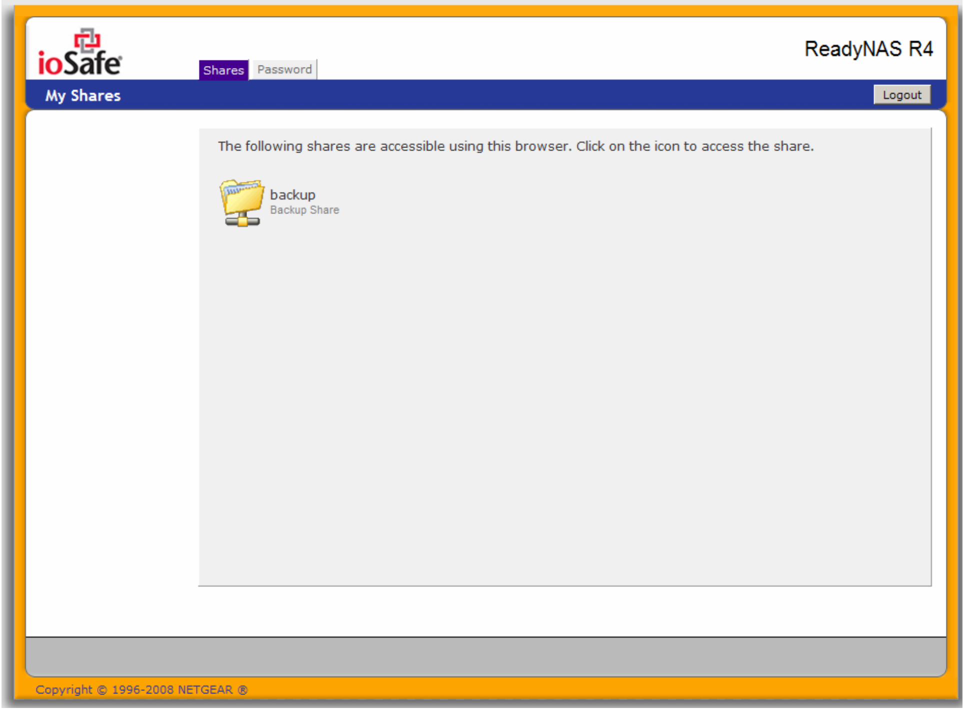
Control Panel

User name: backup

Password:

☐ Remember my password

Enter the share name and share password if the ioSafe R4 is in **Share** security mode. Otherwise, login with a valid user and password if the ioSafe R4 is in **User** or **Domain** mode.

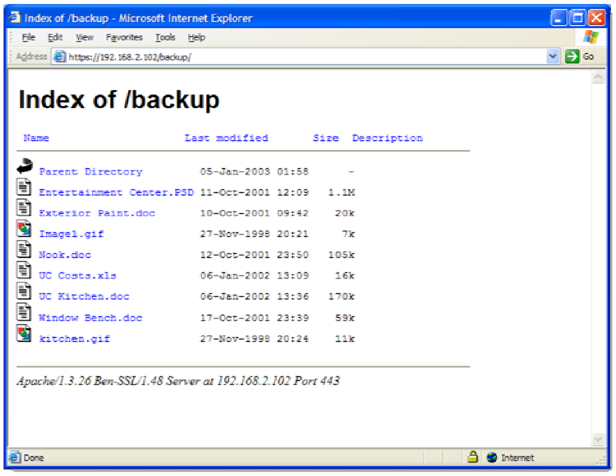


The following shares are accessible using this browser. Click on the icon to access the share.

backup
Backup Share

Copyright © 1996-2008 NETGEAR ®

If the share access is read-only, the file manager will only display:

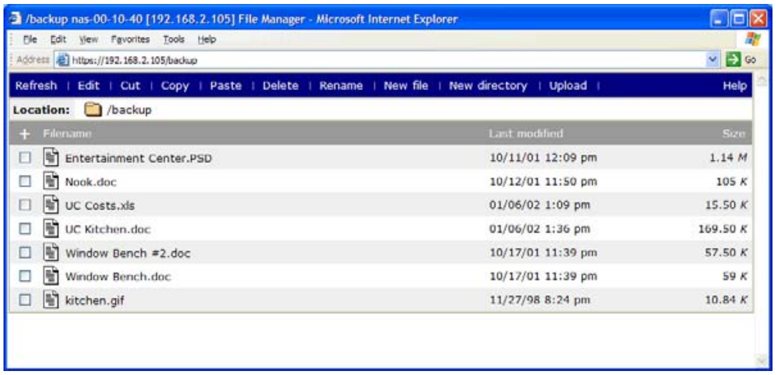

Index of /backup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.2.102/backup/
Go
Done
Internet

Index of /backup

```
Name                          Last modified      Size  Description
Parent Directory              05-Jan-2003 01:58     -
Entertainment Center.PSD 11-Oct-2001 12:09   1.1M
Exterior Paint.doc            10-Oct-2001 09:42   20k
Image1.gif                    27-Nov-1998 20:21    7k
Nook.doc                      12-Oct-2001 23:50  105k
UC Costs.xls                  06-Jan-2002 13:09   16k
UC Kitchen.doc                06-Jan-2002 13:36  170k
Window Bench.doc              17-Oct-2001 23:39   59k
kitchen.gif                   27-Nov-1998 20:24   11k
```

Apache/1.3.26 Ben-SSL/1.48 Server at 192.168.2.102 Port 443

If the share is also writable, the file manager will have options for creating, modifying, and deleting files, as follows:


/backup nas-00-10-40 [192.168.2.105] File Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.2.105/backup
Go
Refresh | Edit | Cut | Copy | Paste | Delete | Rename | New file | New directory | Upload |
Help

Location: /backup

	Filename	Last modified	Size
□	Entertainment Center.PSD	10/11/01 12:09 pm	1.14 M
□	Nook.doc	10/12/01 11:50 pm	105 K
□	UC Costs.xls	01/06/02 1:09 pm	15.50 K
□	UC Kitchen.doc	01/06/02 1:36 pm	169.50 K
□	Window Bench #2.doc	10/17/01 11:39 pm	57.50 K
□	Window Bench.doc	10/17/01 11:39 pm	59 K
□	kitchen.gif	11/27/98 8:24 pm	10.84 K

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

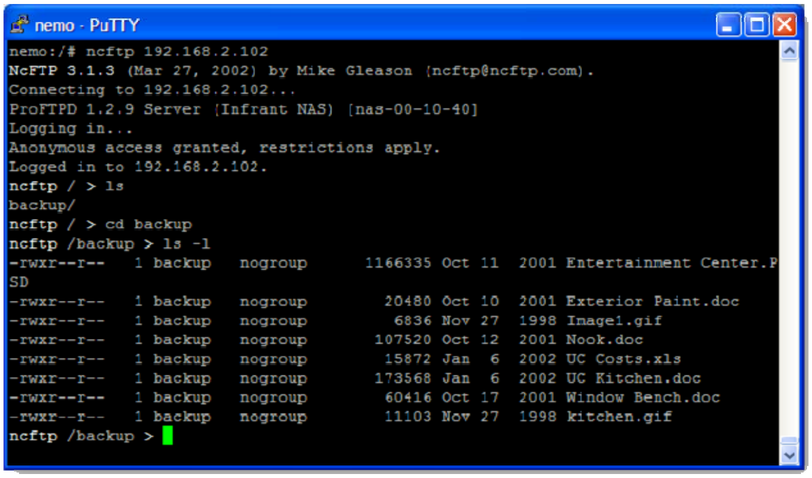
Note

Files created under the Web file manager can only be deleted under this file manager. The only exception is the admin user, who can change or delete any files created through the web.

Files not created from this file manager can be modified within the file manager but cannot be deleted here.

FTP / FTPS

To access the share via FTP in Share security mode, use "anonymous" as the login and your email address as the password.



```
nemo:/# ncftp 192.168.2.102
NcFTP 3.1.3 (Mar 27, 2002) by Mike Gleason (ncftp@ncftp.com).
Connecting to 192.168.2.102...
ProFTPD 1.2.9 Server (Infrant NAS) [nas-00-10-40]
Logging in...
Anonymous access granted, restrictions apply.
Logged in to 192.168.2.102.
ncftp / > ls
backup/
ncftp / > cd backup
ncftp /backup > ls -l
-rwxr--r--   1 backup   nogroup      1166335 Oct 11  2001 Entertainment Center.P
SD
-rwxr--r--   1 backup   nogroup        20480 Oct 10  2001 Exterior Paint.doc
-rwxr--r--   1 backup   nogroup         6836 Nov 27  1998 Image1.gif
-rwxr--r--   1 backup   nogroup       107520 Oct 12  2001 Nook.doc
-rwxr--r--   1 backup   nogroup        15872 Jan  6  2002 UC Costs.xls
-rwxr--r--   1 backup   nogroup       173568 Jan  6  2002 UC Kitchen.doc
-rwxr--r--   1 backup   nogroup        60416 Oct 17  2001 Window Bench.doc
-rwxr--r--   1 backup   nogroup        11103 Nov 27  1998 kitchen.gif
ncftp /backup >
```

Note

Enabling FTP access in Share mode opens up the share to anyone who has an FTP client on your network. It is best to enable FTP access only to shares you are comfortable making public on your network.

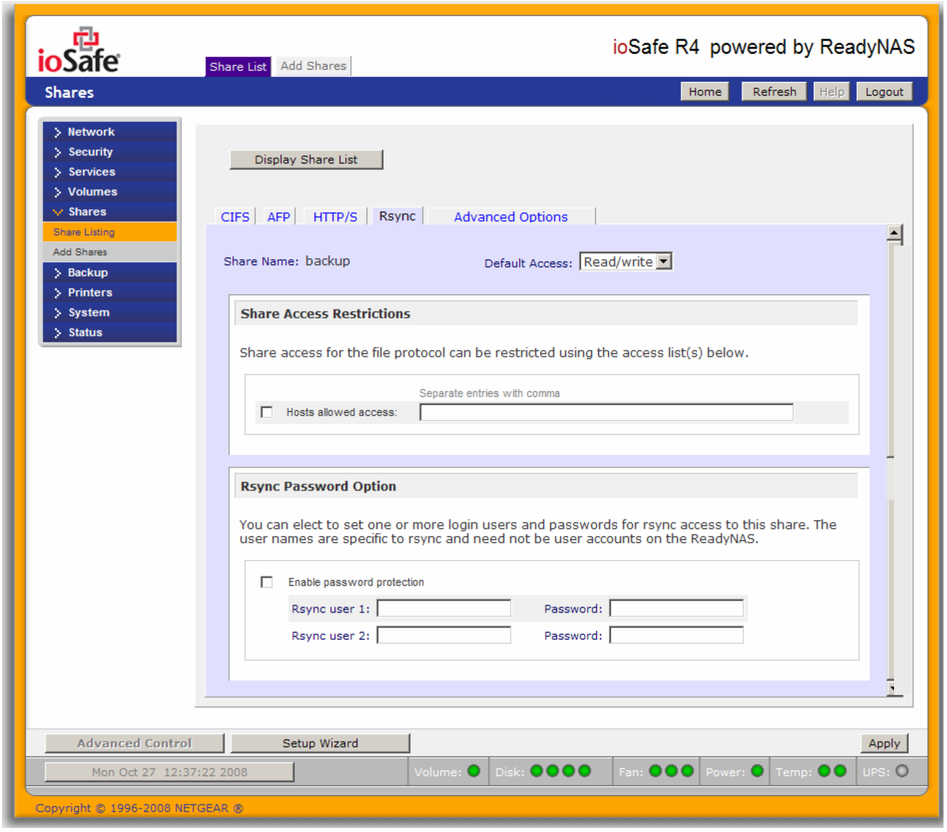
Warning

Disk usage using FTP in Share mode **does not** count towards the share disk quota, so carefully choose how you advertise a FTP Share.

To access the share in User or Domain security mode, use the appropriate user login and password used to access the ioSafe R4. For better security, you can use a FTPS (FTP-SSL) client to connect to the ioSafe R4 FTP service. With FTPS, password and data is encrypted.

Rsync

Access to the share via rsync is identical regardless of the security mode. If you had specified a user or password in the rsync share access tab, you will need to specify this when accessing the rsync share. Unlike other protocols, rsync uses arbitrary user name and password that is specific only for rsync access. The user account you specify does not need to exist on the ioSafe R4 or a domain controller.



Share Name: backup

Default Access: Read/write

Share Access Restrictions

Share access for the file protocol can be restricted using the access list(s) below.

Separate entries with comma

□ Hosts allowed access:

Rsync Password Option

You can elect to set one or more login users and passwords for rsync access to this share. The user names are specific to rsync and need not be user accounts on the ReadyNAS.

□ Enable password protection

Rsync user 1: Password:

Rsync user 2: Password:

Hers is an example of a way for a Linux client to list the content of an ioSafe R4 rsync share with no user name and password defined:

```
# rsync ipaddr::backup
```

To recursively copy the content of a share to /tmp:

```
# rsync –a ipaddr::backup /tmp
```

To do the same except with a login **user** and password **hello**:

```
# rsync –a user@ipaddr::backup /tmp
Passowrd: *****
```

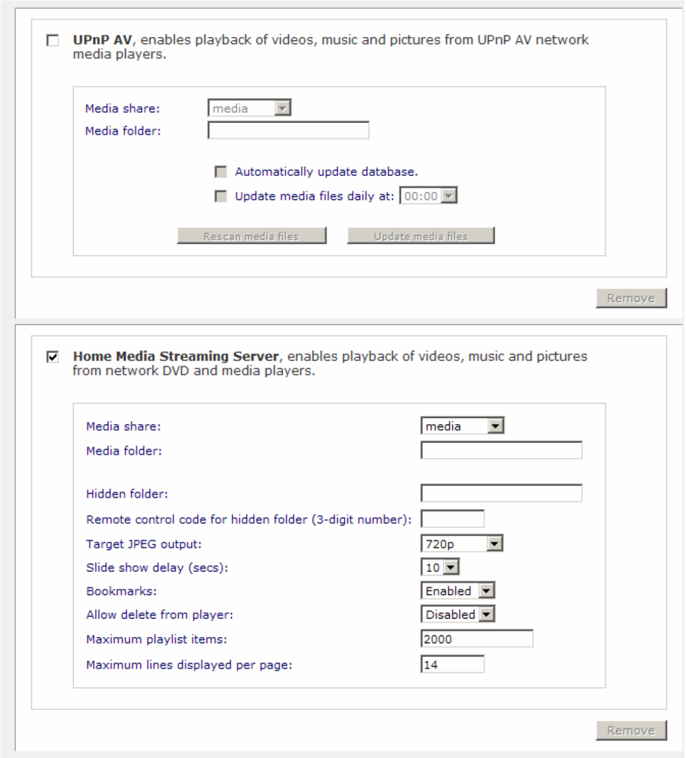
Note

The ioSafe R4 does not support rsync over SSH.

Networked DVE Players and UPnP AV Media Adapters

Networked DVD players and UPnP AV Media adapters will detect the ioSafe R4 if the Home Media Streaming Server or the UPnP AV services are enabled. The content of the Streaming Services *media* share on the ioSafe R4 is available to these players for playback. Please consult the player manual for information on the file formats that it supports. Multiple players can be connected to the ioSafe R4 and can play the media files concurrently.

Make sure that you enable the appropriate service in the Services tab before invoking this service.



□ **UPnP AV**, enables playback of videos, music and pictures from UPnP AV network media players.

Media share: media
Media folder:

□ Automatically update database.
□ Update media files daily at: 00:00

☑ **Home Media Streaming Server**, enables playback of videos, music and pictures from network DVD and media players.

Media share: media
Media folder:
Hidden folder:
Remote control code for hidden folder (3-digit number):
Target JPEG output: 720p
Slide show delay (secs): 10
Bookmarks: Enabled
Allow delete from player: Disabled
Maximum playlist items: 2000
Maximum lines displayed per page: 14

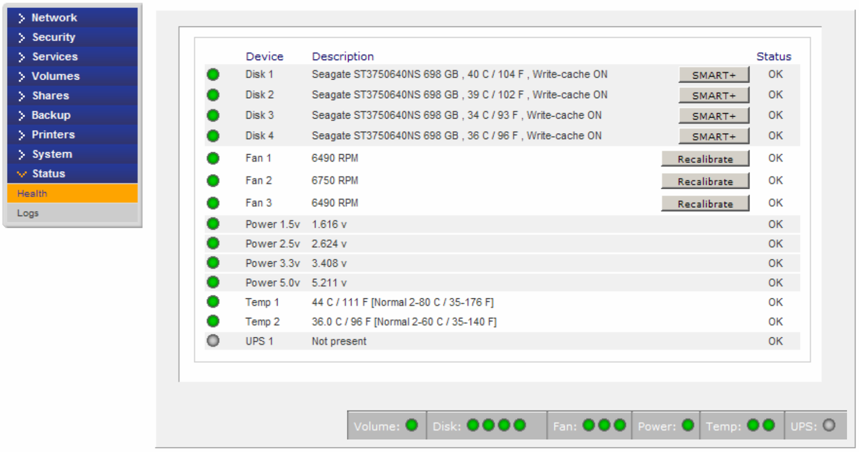
Consult the Device Compatibility list for information on which DVD players and media adapters will work with Netgear's ReadyNAS technology.

Chapter 3

Replacing a Failed Disk

Locate the Failed Disk

When a disk fails in your ioSafe R4 device, you will be notified of the failure by email. The failed disk location can be seen in the FrontView status bar at the bottom.



	Device	Description		Status
●	Disk 1	Seagate ST3750640NS 698 GB , 40 C / 104 F , Write-cache ON	SMART+	OK
●	Disk 2	Seagate ST3750640NS 698 GB , 39 C / 102 F , Write-cache ON	SMART+	OK
●	Disk 3	Seagate ST3750640NS 698 GB , 34 C / 93 F , Write-cache ON	SMART+	OK
●	Disk 4	Seagate ST3750640NS 698 GB , 36 C / 96 F , Write-cache ON	SMART+	OK
●	Fan 1	6490 RPM	Recalibrate	OK
●	Fan 2	6750 RPM	Recalibrate	OK
●	Fan 3	6490 RPM	Recalibrate	OK
●	Power 1.5v	1.616 v		OK
●	Power 2.5v	2.624 v		OK
●	Power 3.3v	3.408 v		OK
●	Power 5.0v	5.211 v		OK
●	Temp 1	44 C / 111 F [Normal 2-80 C / 35-176 F]		OK
●	Temp 2	36.0 C / 96 F [Normal 2-60 C / 35-140 F]		OK
○	UPS 1	Not present		OK

If you look at the front of the ioSafe R4 device, the failed disk will have also have a corresponding LED which will be amber in color. The top or left-most LED is disk channel 1; the next one is disk channel 2; and so on. Please take note of the failed channel.

Ordering Replacement Disk

Go to the Status menu and click on the Health tab. Take note of the disk size and model utilized on your ioSafe R4 system. It is best to replace a failed disk with the same disk model. Contact ioSafe and arrange to have the disk replaced.

If the disk is no longer under warranty, you can obtain a disk of the same capacity or larger from your ioSafe retailer.

Replace the Failed Disk

Contact ioSafe technical support for hardware-specific instructions on replacing a failed disk in your ioSafe R4 system.

On the ioSafe R4 system open up the front vent door using the four thumbscrews on the front of the unit. All the disk positions are labeled accordingly, identify which disk needs to be replaced. Remove the failed disk, wait approximately 30 seconds, then install the replacement disk and replace the front vent door. The front vent door can only be attached in one orientation. If the door doesn't seem to fit, try rotating the door to a different orientation.

Warning

> Proper seating and latching of the drive is essential to proper operation. Verify the replacement drive is fully seated and properly latched before reinstalling the front vent door.

The ioSafe R4 system has hot-swap drive bays, you do not need to power off the ioSafe R4 to replace a failed disk. You can replace the disk while the system is on. After removing the failed disk, wait at least 30 seconds until the disk LED blinks, and then insert the new disk.

Re-synchronize the Volume

If you powered off the R4 system to replace the failed disk, turn the power back on. The RAID volume will automatically re-synchronize the new disk in the background. The process will take several hours depending on disk size. During the re-sync process, the ioSafe R4 can be used as normal, although access will be slower until the volume is done re-synchronizing.

You will be notified by email when the re-sync process is complete.

Disaster Recovery Procedure

This section instructs how to recover data following a natural disaster such as fire, water, and/or physical damage. The first step in any disaster recovery is to contact your ioSafe disaster recovery team leader. For the most recent version of this document or to locate a team leader go to:

www.iosafe.com/drsupport or call 888-984-6723 x430

Typical steps to recovering from a disaster:

CAUTION: The presence of fire, heat, smoke, unstable structures, or liquid and electricity can create significant risk of bodily harm. Take care to ensure that your disaster recovery effort is only performed in safe working conditions.

1) The first step in recovering data from your ioSafe product is to contact a ioSafe disaster response team leader: 888-984-6723 x430

2) Inspect the R4 for physical damage. Remove all cables and inspect the receptacles. Remove the front and back doors and inspect the inside of the unit. See below for descriptions of what indicates damage to the R4. If there is no evidence of damage to the R4, plug the cables back in, power up the unit, and verify proper boot and the presence of your data. During normal boot, the blue LED will blink and then show steady on.

Fire Damage:

Moderate –Deformation of plastic parts due to heat. Minor areas of discoloration or paint damage. Doors easy to remove.

Extreme – Extensive paint damage, plastic parts are completely melted or gone, structural components appear visibly warped or compromised. Doors are difficult to remove.

Water/moisture exposure:

Moderate – Exposure to moisture or liquid for a short period of time due to splash, spray or flood. The R4 has minimal moisture present and no corrosion on the connectors. No moisture present on inside of unit.

Extreme – R4 has been exposed to extended moisture due to submersion or splash/spray without prompt recovery procedures being followed. Corrosion or other contaminates may be present. Moisture is present on inside of unit.

Physical Damage:

Moderate – The R4 may have experienced a low impact event. The exterior of the enclosure may have some minor dents or scratches. The doors are easily removable. The electronic core and hard drives are in visibly pristine condition.

Extreme – The R4 has experienced a high impact event. The outside enclosure is visibly damaged, the sides are no longer square, the doors do not readily come off, the electronic core or hard drives show evidence of damage.

3) If there is evidence of damage to the R4 in step 2, evaluate the extent of damage. If the damage is extreme, proceed no further and contact ioSafe to arrange the next steps of the recovery effort. If the damage is moderate with evidence of exposure to fire, moisture, or physical damage then remove all hard drives. **BE CAREFUL TO NOTE THEIR POSITION.** Inspect all surfaces and connectors of each drive.
4) Clean the hard drive connectors with Isopropyl Alcohol (P/N: 500-10511-00).
5) Inspect the connectors again for dirt, damage, or moisture. Repeat if required.
6) Install the hard drives in the recovery core (P/N: 700-10371-00). Make sure that the hard drives are installed in the same positions as in the original core.
7) Connect the jumper cable (P/N: 455-10372-00) to both DB-15 connectors on the rear the recovery core (opposite side from the drive bays).
8) Connect the CAT 6 network cable (P/N: 455-10512-00) to either of the network cable connectors on the recovery core. Connect the other end of the CAT 6 network cable into an available network.
9) Install the spare R4 fan assembly (P/N: 300-10337-00) into the recovery core. Firmly slide the fan assembly into the fan bay until seated.

10) Connect the AC power cable (P/N: 455-10370-00) to the recovery core, then connect the other end to AC power. Be aware that the recovery core will immediately initiate boot when the power cable is connected.

11) Verify LEDs are flashing during power up. Verify 4 solid green lights indicate all 4 hard drives have booted. Verify one solid blue light to indicate the core has properly booted. Two flashing green lights may indicate drive activity and network activity.

12) Using the RAIDar software installed on a computer on the network, locate the recovery core and recover data.

13) Contact an ioSafe disaster recovery team leader for help determining if the original R4 enclosure needs to be replaced. If the original enclosure is viable, affix the MAC address label (P/N: 380-10521-00) to the back of the enclosure in place of the old MAC address label. Verify that the MAC address label on the enclosure matches the MAC address label on the enclosed core.

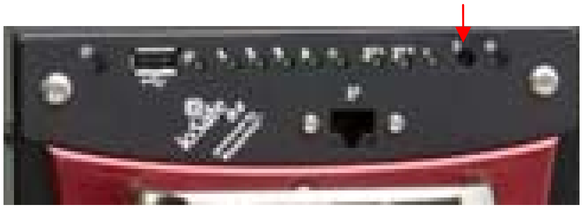
14) Order any replacement parts required for a complete R4 Disaster Recovery Kit (P/N: 700-10501-00). Reference the R4 Disaster Recovery Bill of Materials (P/N: 380-10520-00) for a complete list of parts.

Chapter

4

System Reset Switch

The **System Reset** switch on the front of the ioSafe R4 next to the power button.

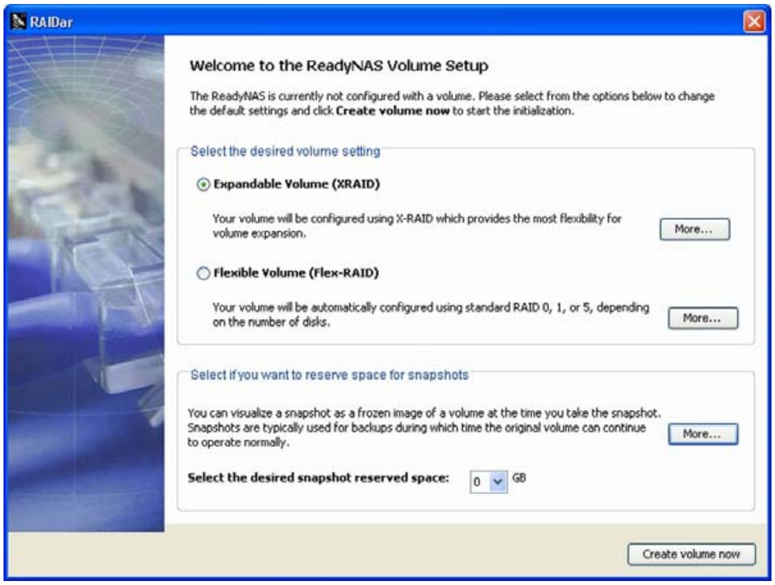


The System Reset switch allows you to perform three functions: (1) re-install the ioSafe R4 firmware, (2) reset the ioSafe R4 back to the factory default settings, and (3) change between **X-RAID** and **Flex-RAID** mode.

Typically, you should not need to resort to options (1) and (2) unless you have exhausted all other means of recovering your system. You may want to re-install the ioSafe R4 firmware as a first step, if the ioSafe R4 had been working normally but a configuration change makes it inaccessible. If this does not work and/or you wish to set the ioSafe R4 back to a factory default state, you can do so following the instructions below:

- **To re-install the ioSafe R4 firmware**, use a paper clip to depress the switch while the system is off. Continue to depress the reset switch while powering on the system and continue to hold the reset switch for 5 seconds afterward. The disk LED's will flash once to signify that the command has been accepted. The firmware installation will take several minutes to complete. The Status LED in the front will also be solid when the process is complete. The installation will not affect the data on the ioSafe R4. **Make sure not to press the reset switch for too long, otherwise a destructive Factory Default process will be started instead** (see below).
- **To set the ioSafe R4 device to Factory Default**, use the same process, except you must hold the System Reset Switch for 30 seconds after powering on the system. You should see the disk LED's flash for a second time to signify that the command has been accepted. Note that this process re-installs the firmware and resets the disk configuration, **WIPING OUT ANY DATA** you may have had on the NAS.
- **To change between X-RAID and Flex-RAID mode**, you will need to perform a Factory Default using the method described above. Note that changing RAID modes will not preserve your data, so make sure to perform a backup before doing this. During the boot process during Factory Default, there will be a 10-minute window where you can use RAIDar to select the desired volume setup. RAIDar will display your ioSafe R4 with **Click**

Setup in the Info column. It may take a couple of minutes for RAIDar to display this. At this point, click the **Setup** button to enter the Volume Setup screen.



Welcome to the ReadyNAS Volume Setup

The ReadyNAS is currently not configured with a volume. Please select from the options below to change the default settings and click **Create volume now** to start the initialization.

Select the desired volume setting

● **Expandable Volume (XRAID)**

Your volume will be configured using X-RAID which provides the most flexibility for volume expansion.

○ **Flexible Volume (Flex-RAID)**

Your volume will be automatically configured using standard RAID 0, 1, or 5, depending on the number of disks.

Select if you want to reserve space for snapshots

You can visualize a snapshot as a frozen image of a volume at the time you take the snapshot. Snapshots are typically used for backups during which time the original volume can continue to operate normally.

Select the desired snapshot reserved space: 0 GB

Select the desired mode along with the desired snapshot size and click **Create volume now**. The ioSafe R4 will proceed with a reboot to re-configure your volume to the desired specification. If no action is taken within 10 minutes, the system defaults to X-RAID and begins its initialization process.

Before beginning any of these activities, make sure to back up all important data.

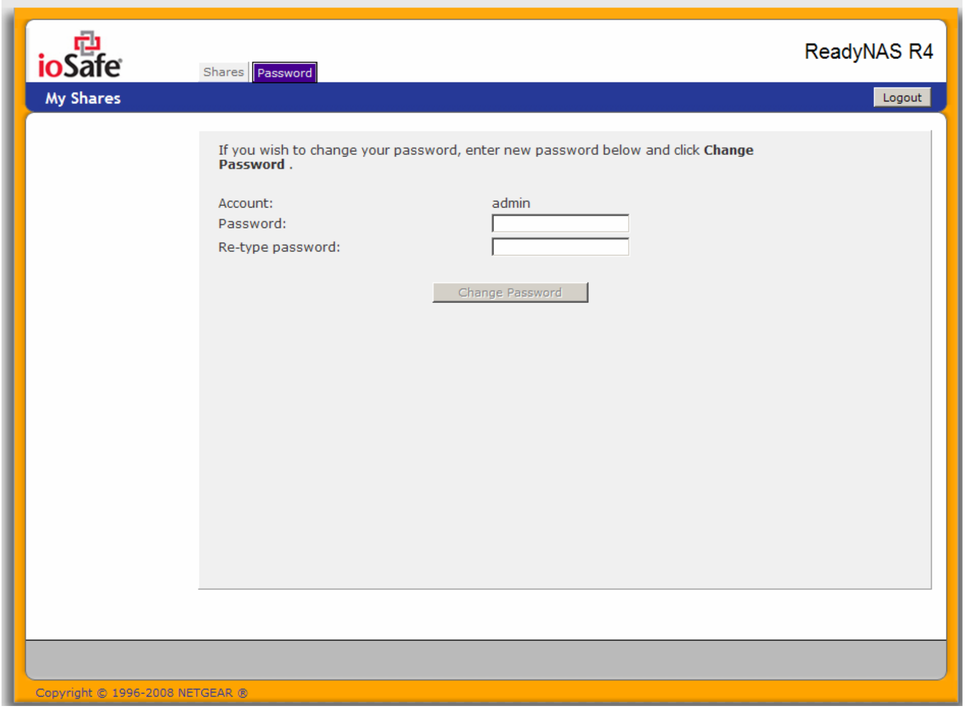
Chapter

5

Changing User Passwords

There are two ways in which user passwords can be changed in the **User security mode**. The first way is for the admin user to change the passwords in the **Accounts** tab in the **Security** menu. The other and preferred way is to allow users to change their own passwords. This relieves the admin from this task and hopefully, encourages users to change their passwords on a more regular basis for enhanced security.

Users can use the web browser and their existing password to log in to *https://ip_addr/* to access the web share listing page. Then select the **Password** tab, and follow the prompts to set a new password.



If you wish to change your password, enter new password below and click **Change Password** .

Account: admin
Password:
Re-type password:

In **Share** and **Domain** security mode, the **Password** tab will not appear. Note: User passwords in **Domain** mode must be set on the domain or ADS server.

Appendix A

RAID Levels Simplified

RAID can be somewhat daunting; this appendix will help simplify RAID for you.

RAID is an acronym for **R**edundant **A**rray of **I**ndependent **D**isks. Basically, if properly configured, it can store data on multiple disks in a way that if one disk fails, the data can still be accessed from the surviving disk(s). A RAID level selects how data will be kept redundant, the most popular ones being levels 0, 1, and 5. Contrary to the RAID acronym, RAID level 0 does not provide any redundancy.

RAID Level 0

RAID level 0 provides the best write performance of all the RAID levels as it stripes data across all disks so that data can be written to all disks in parallel. Unfortunately, it is not redundant, so if one disk fails the entire volume will fail. RAID level 0 can be configured with one or more disks, and its capacity is the size of the smallest disk in the RAID set multiplied by the number of disks in the set. For example, a four disk RAID 0 will yield the capacity of all four disks, assuming they are identical in size.

RAID Level 1

RAID level 1 consists of 2 or more disks, all disk(s) other than the first being an exact mirror of the first. RAID level 1 can sustain disk failure up to the total number of disks in the RAID set minus one. For example, a two-disk RAID 1 volume can sustain a one-disk failure and continue running. A three-disk RAID 1 volume can sustain up to two disk failures. If a disk fails, the data is retrieved from the surviving disk. Unfortunately, RAID 1 capacity utilization is not optimal in a three or more disk configuration. The capacity is limited to the size of the smallest disk in the RAID set.

RAID Level 5

RAID level 5 provides the best balance of capacity and performance while providing data redundancy. RAID 5 provides redundancy by striping data across three or more disks and keeping the parity information on one of the disks in each stripe. In case of disk failure, the surviving disks and the parity disk are used to reconstruct the lost data, providing that data transparently to the user application. Upon replacing the failed disk with a good disk, the reconstructed data is written out to the new disk, and when the reconstruction (or sometimes referred as re-sync) process is complete, the volume returns to a redundant state. The capacity of a RAID 5 volume is the smallest disk in the RAID set multiplied by one less than the number of disks in the RAID set. For example, a four-disk RAID 5 set will provide the capacity of three disks, assuming all four disks are identical in size.

RAID Level "X" (X-RAID)

RAID level "X", or **X-RAID**, is similar to RAID level 5, is optimized for large sequential access for the best possible media streaming performance. The "X" also refers to its natural volume eXpandability. In X-RAID mode, with one disk, the volume is non-redundant and has the capacity of the single disk. By adding a 2nd disk, the capacity remains the same, but the data is now mirrored between the two disks. With redundancy, your data will not be lost in the event of a disk failure. By adding a 3rd disk, the capacity doubles while maintaining redundancy. By adding a 4th disk, the capacity triples with redundancy. The process of volume expansion is automatic. When a disk has been added, you will be notified of the steps being taken, and you will be notified when you will need to reboot to continue with the expansion process.

Appendix

B

Input Field Format

Domain/Workgroup Name

A valid domain or workgroup name must conform to the following restrictions:

- Name must consist only of characters a-z, A-Z, 0-9, and the symbols _ (underscore), – (dash), and . (period).
- Name must start with a letter.
- Name length must be 15 characters or less.

Host

A valid IP address or a host name.

Host Name

A valid host name must conform to the following restrictions:

- Name must consist only of characters a-z, A-Z, 0-9, and the symbols – (dash) and . (period).
- Name must start with a letter.
- A short host name length must be 15 characters or less.
- A fully-qualified domain name (FQDN) must have no more than 63 characters in each section separated by . (period), and cannot end with a – (dash). Example of a valid FQDN: firstpart.secondpart.thirdpart.com.

ioSafe R4 Host Name

A valid host name except the first part or short host name must be 15 characters or less due to NetBIOS name length restriction.

Host Expression

A valid host expression is either a valid host or the common IP expression form specifying a range of addresses in a network; for example:

- 192.168.2.
- 192.168.2.0/255.255.255.0
- 192.168.2.0/24

Share Name

- Name must consist only of characters a-z, A-Z, 0-9, and the symbols – (dash) and . (period).
- Name cannot be an existing user name.
- Name cannot end in *–snap*.
- Name cannot be any one of the following reserved names:

```
bin boot cdrom dev etc floppy frontview home initrd lib lost+found mnt
opt proc root sbin tmp usr var admin administrator images language
quota.user quota.group shares global homes printers diag c d e f g h i
j
```

- Share name can contain Unicode characters if this option is specified in the Language tab.

Share Password

- Any character except for ' (single quote).
- Share passwords are limited to 8 characters.

SNMP Community

- Name must consist only of characters a-z, A-Z, 0-9, and the symbols _ (underscore), – (dash) and . (period).
- Name must start with a letter.
- Name length must be 32 characters or less.

User/Group Name

- Name must consist only of characters a-z, A-Z, 0-9, and the symbols _ (underscore), – (dash), @, and . (period).
- Name cannot be an existing share name.
- Name can contain Unicode characters if this option is specified in the Language tab.

User Password

- Any character except for ' (single quote).

Appendix C

Glossary

AFP: AppleTalk Filing Protocol, is the standard way Mac OS 9 and earlier share files across the network.

CIFS: Common Internet File System, a standard protocol that Windows users use to share files across the network. Mac OS X also has the capability to share files using CIFS.

FTP: File Transfer Protocol, a common protocol adopted by many OS to enable remote file download and upload for public sharing.

HTTP: Hypertext Transfer Protocol, the protocol web browsers use to connect to web servers for file access, typically web pages.

HTTPS: HTTP with SSL encryption, is used where secure web access is desired.

NFS: Network File System, a common way Unix and Linux systems share files by making remote file systems appear to reside locally.

Quota: Amount of volume space allocated to a particular user or group account, or to a particular share. The user, group, or share with a set quota cannot exceed disk usage beyond this limit. Quota is typically specified to ensure no one user, group, or share abuses the available storage space.

RAID: Acronym for **R**edundant **A**rray of **I**ndependent **D**isks. Basically it is a method of storing data on multiple disks in a way that if one disk fails, data can still be accessed from the other disk(s). A RAID level selects how data will be kept redundant, the most popular of which are levels 0, 1, and 5. Contrary to the RAID acronym, RAID level 0 does not provide any redundancy. For more info, see **RAID Levels Simplified** in **Appendix A**.

Share: A folder on a NAS volume that can be shared amongst different network file services such as CIFS for Windows, AFP (AppleTalk File Protocol) for Macs, NFS for Unix/Linux, FTP, and HTTP. Access to the share can be customized on a user/group/host-level basis.

Snapshot: An instantaneous, non-changing, read-only image of a volume. Snapshots are useful for backups during which time the original volume can continue to operate normally. Snapshots can also be utilized as a temporary backup against viruses. Files can be restored from the snapshot volume if current files are corrupted.

Volume: A filesystem built on top of a RAID set. This filesystem consists of shares that are made available through various network file services.

X-RAID: NETGEAR patent-pending Expandable RAID technology.

Appendix D

If You Need Help…

If you have questions or you encounter problems with the setup, you can visit our support site at http://www.iosafe.com. There, you'll find links to FAQs, ioSafe support and engineering staff can be reached at

Phone: 1.888.98.IOSAFE (984.6723) x400
Phone: 530.886.1578 x400
Fax: 888.FAX.IOSAFE
Email: customerservice@iosafe.com