

READYNAS INSTANT STORAGE

User Guide



Updated for RAIDiator 3.01c1-p5

Copyright © 2006, **Infrant Technologies Inc.** All rights reserved.

<http://www.infrant.com>

ReadyNAS, X-RAID, FrontView, RAIDar, RAIDiator, Network Storage Processor, and NSP are trademarks or registered trademarks of Infrant Technologies Inc. All other product names are the property of their respective owner.

P/N: IT-05-1-1040-U-08

Contents

About This Guide	7
1 FrontView Advanced Control	8
Network	10
Ethernet	10
▶ Speed/Duplex Mode	11
▶ MTU	11
▶ VLAN Setting	11
▶ Performance Setting	12
Wireless	13
Global Network Settings	14
▶ Hostname	14
▶ Default Gateway	14
▶ DNS	14
WINS	15
DHCP	16
Route	17
Security	18
Admin Password	18
Security Mode Selection	19
Share Security Mode	20
▶ Specify a Workgroup	20
▶ Share Accounts	21
User Security Mode	21
▶ Specify a Workgroup	21
▶ Setting up Accounts	21
▶ Managing Groups	22
▶ Managing Users	24
▶ Setting Accounts Preferences	26
Domain Security Mode	27
▶ Domain/ADS Authentication	27

▶ Setting up Accounts	28
Services	29
Standard File Protocols	29
Streaming Services	30
Discovery Services	31
Volumes	32
Volume Management	32
▶ Advantages of Flex-RAID	32
▶ Advantages of X-RAID	32
Volume Management for Flex-RAID	32
▶ Deleting a Volume	33
▶ Adding a Volume	34
▶ RAID Settings	35
Volume Management for X-RAID	36
▶ X-RAID Redundancy Overhead	36
▶ X-RAID Has one data volume	36
▶ Adding a 2 nd DISK for Redundancy	36
▶ Adding a 3 rd and 4 th DISK for MORE Capacity	36
▶ Replacing All Your Disks for Even MORE Capacity	37
Changing Between X-RAID and Flex-RAID Modes	37
Snapshot	37
▶ Taking and Scheduling Snapshot	38
▶ Resizing Snapshot Space	40
USB Storage	40
Shares	43
Adding Shares	43
Managing Shares	44
▶ Setting Share Access in Share Mode	45
▶ Setting Share Access in User and Domain Modes	46
▶ Advanced Options	48
USB Shares	49
Printers	50
Print Shares over CIFS/SMB	50
IPP Printing	51
Managing Print Queues	51
Backup	52
Adding a New Backup Job	52
▶ Step 1 – Select Backup Source	52
▶ Step 2 – Select Backup Destination	53
▶ Step 3 – Choose Backup Schedule	54

▶ Step 4 – Choose Backup Options	54
Viewing the Backup Schedule	55
Programming the Backup Button	56
Viewing the Backup Log	56
Editing a Backup Job	56
System	57
Clock	57
▶ System Time	57
▶ NTP Option	57
Alerts	58
▶ Alerts Contacts	58
▶ Alerts Settings	58
▶ SNMP	59
▶ SMTP	60
Performance	61
▶ Adding a UPS for performance	62
Language	63
Unicode for User, Group, and Share Names	64
Updating ReadyNAS	64
▶ Remote Update	64
▶ Local Update	65
▶ Settings	65
▶ Factory Default	66
Power Management	67
▶ Disk Spin-down Option	67
▶ Power Timer	67
Shutdown	68
Status	70
Health	70
Logs	71
2 Accessing Shares	73
Windows	74
MAC OS X	75
AFP over Bonjour	75
AFP over AppleTalk	77
MAC OS 9	79
Linux/Unix	81
Web Browser	82
FTP / FTPS	84
Rsync	85

Networked DVD Players and UPnP AV Media Adapters	86
3 Replacing a Failed Disk	87
Locate the Failed Disk	87
Order Replacement Disk	87
Replace the Failed Disk	88
Re-synchronize the Volume	88
4 System Reset Switch	89
5 Changing User Passwords	91
A RAID Levels Simplified	92
RAID Level 0	92
RAID Level 1	92
RAID Level 5	92
RAID Level “X” (X-RAID)	93
B Input Field Format	94
Domain/Workgroup Name	94
Host	94
Host Name	94
ReadyNAS Host Name	94
Host Expression	95
Share Name	95
Share Password	95
SNMP Community	95
User/Group Name	95
User Password	95
C Glossary	96
D If You Need Help...	98

About This Guide

Congratulations and thank you for purchasing a ReadyNAS Instant Storage system from Infrant Technologies. If you haven't already done so, please read the Getting Started guide provided in the shipping box and the Quick Installation Guide on the CD-ROM.

The Quick Installation Guide takes you step-by-step through the FrontView Setup Wizard and quickly prepares the ReadyNAS for your network. The User Guide explains each of the available options in detail, including a lot of advanced options not available during the Setup Wizard process.

[Chapter 1](#), “FrontView Advanced Control”, describes all the menus and tabs available in the Advanced Control mode.

If you have already configured the ReadyNAS and you need help in accessing the shares on the ReadyNAS, 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 ReadyNAS supports, please refer to [Appendix A](#), “RAID Levels Simplified”.

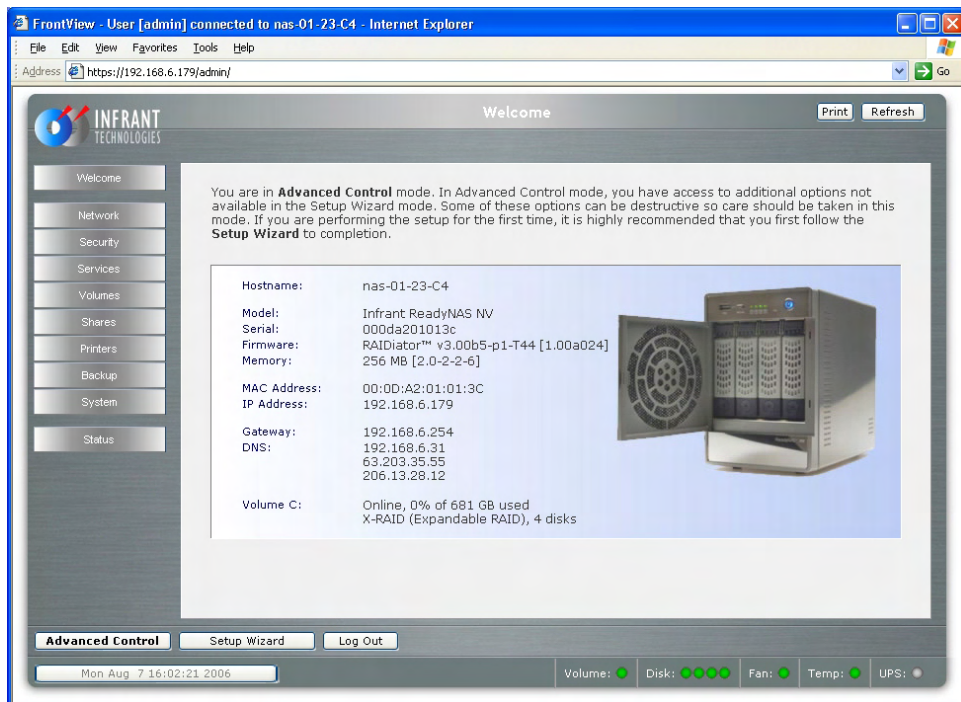
If you have questions on what constitutes a valid input for host name, workgroup, or password, [Appendix B](#), “Input Field Format”, describes these and more.

[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...”.

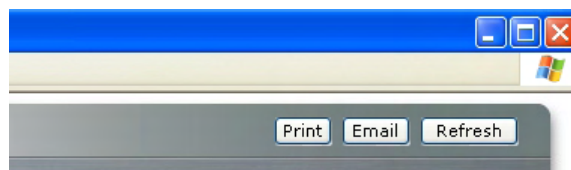
FrontView Advanced Control

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

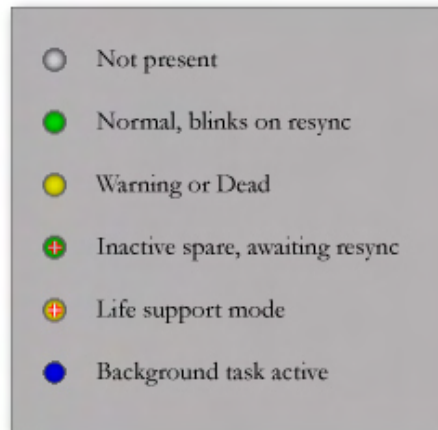


When you first switch to this mode, you'll see the menus on the left that allow you to quickly jump to the desired menu page. Towards the bottom left, you'll notice buttons that allow you to switch back and forth between the Setup Wizard mode and the Advanced Control mode..

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 print or email the page, refresh the browser window, or display help where available.



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 ReadyNAS 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 ReadyNAS immediately, reconnect the disk, and power-on the ReadyNAS. If you reconnect the disk during runtime, the ReadyNAS 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 is the Logout button. 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. To the right is the Apply button. Use this to save any changes in the current menu page.

Network

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.

The screenshot displays the configuration page for Ethernet 1. At the top, there are tabs for 'Global Network Settings', 'WINS', 'DHCP', and 'Route'. The 'Standard Setting' section includes fields for MAC address (00:0D:A2:10:00:02), Status (Online / 100 Mbit / Full-Duplex), IP assignment (Use values from a DHCP server), IP address (192.168.6.167), Netmask (255.255.255.0), Speed/Duplex mode (Auto-negotiation), and MTU (1500). The 'VLAN Setting' section has an unchecked checkbox for 'Enable VLAN support' and a 'VLAN Tag' field set to 0. The 'Performance Setting' section has an unchecked checkbox for 'Enable jumbo frames'.

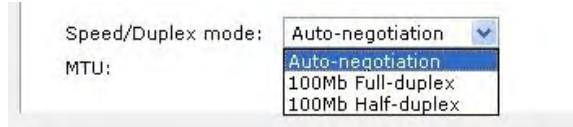
If you assign a static IP address, be aware that the browser will lose connection to the ReadyNAS device after the IP address has been changed. You can click Rescan in RAIDar to locate the device and reconnect from there.

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 ReadyNAS 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 ReadyNAS 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.



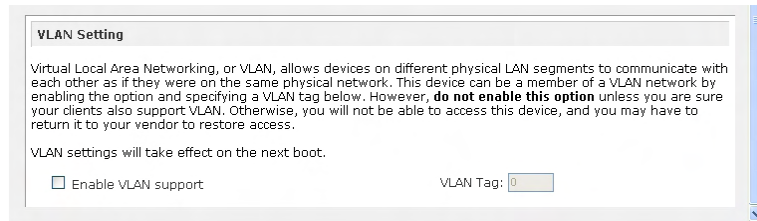
► MTU

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



► 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.



If you wish to use the ReadyNAS in a VLAN environment, select the **Enable VLAN support** checkbox and input a numeric VLAN tag. You will need to reboot the ReadyNAS 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 ReadyNAS 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 ReadyNAS for large data transfers such as multiple streams of video playback. Select this option if your NIC and your gigabit switch support jumbo frames.

Note

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

If your ReadyNAS device comes with multiple Ethernet interfaces, you will see a separate configuration tab for each interface.

Wireless

There are several ways in which you can use this NAS device over a wireless network. You can either connect the NAS to your wireless access point (preferred) with a Cat-5 Ethernet cable, connect a USB wireless adapter directly to the USB port on the NAS device, or use a supported wireless PCI adapter if a PCI slot exists on your ReadyNAS.

The wireless network tab shows up in the Network menu when a supported USB or PCI wireless adapter is detected. Enter the network name (ESSID), operating mode (typically Managed if you have an access point), data encryption mode, and encryption key values from your wireless access point. Select the desired IP assignment method (DHCP or static) and save the changes to start using your ReadyNAS device with the wireless adapter.

The screenshot shows the 'Wireless' tab in the network settings. At the top, there are tabs for 'Ethernet', 'Wireless', 'Global Network Settings', 'WINS', 'DHCP', and 'Route'. The 'Standard Setting' section contains the following fields and options:

- MAC address: 00:12:17:86:AB:36
- Status: Online / 54 Mbit / Signal -37 dBm / Channel 11 / ESSID STUDIO54
- Network name (ESSID): ANY
- Operating mode: Managed - this device connects to an access point
- Data encryption: Enabled
- Network Authentication: Shared Key Mode
- Encryption key (hex): *****
- IP assignment: Use values from a DHCP server
- IP address: 192.168.7.191
- Netmask: 255.255.255.0

A 'Renew now' button is located to the right of the IP assignment dropdown.

Note

Please note that support for USB and PCI wireless devices is limited. Consult the hardware device compatibility list for a list of devices that are currently supported. Future updates may support additional adapters.

Global Network Settings

Ethernet 1 | 2 | Global Network Settings | WINS | DHCP | Route

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:

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. This has been automatically set by your DHCP server.

Default gateway:

DNS Settings

DNS, or Domain Name Service, addresses are automatically assigned when DHCP service is used. This has been automatically set by your DHCP server.

Domain name server 1:

Domain name server 2:

Domain name server 3:

Domain name:

► HOSTNAME

The Hostname you specify is used to advertise the ReadyNAS on your network. You can use the hostname to address the ReadyNAS in place of the IP address when accessing the ReadyNAS 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 or Wireless 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.

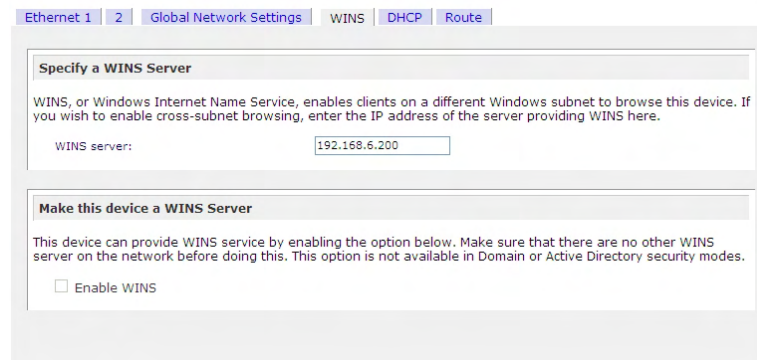
► DNS

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 or Wireless 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 ReadyNAS or other devices on the network to be (Windows) browsable from other subnets.



Ethernet 1 | 2 | Global Network Settings | WINS | DHCP | Route

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.

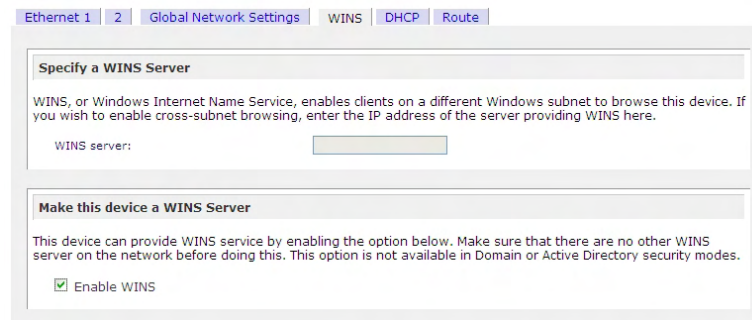
WINS server:

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.

Enable WINS

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



Ethernet 1 | 2 | Global Network Settings | WINS | DHCP | Route

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.

Enable WINS

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.

Ethernet 1 | 2 | Global Network Settings | WINS | DHCP | Route

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: 192.168.6.1

Ending IP Address: 192.168.6.167

Lease Time (min): 15

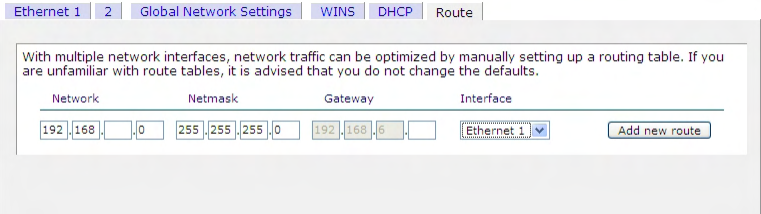
Click on the **Enable DHCP service** checkbox if you want the ReadyNAS device to act as a DHCP server. This is convenient in networks where DHCP service is not already available.

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 ReadyNAS. In some environments, you can optimize your network traffic by manually setting up a routing table.



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.

Admin Password

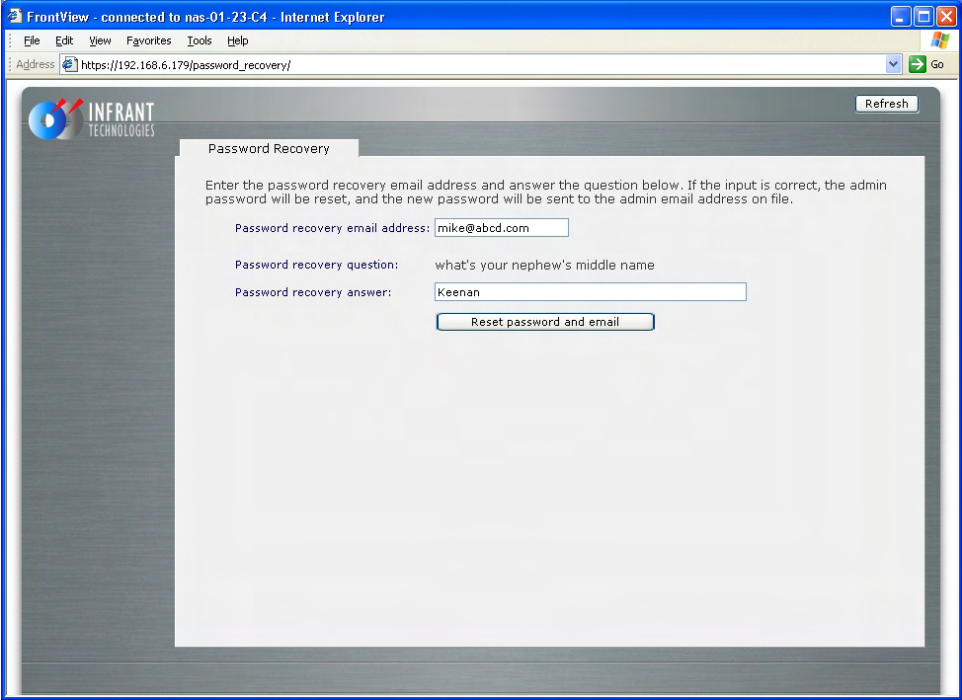
The **Admin Password** tab allows you to change the **admin** user password. The **admin** user is the only user that can access FrontView and this user has administrative privileges when accessing shares. Be sure to set a password different from the default password and make sure this password is kept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

The screenshot shows a web interface with three tabs: "Admin Password", "Security mode", and "Accounts". The "Admin Password" tab is active. Below the tabs is a text box containing the following instructions: "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.**" Below the text are five input fields: "New admin password:" (masked with asterisks), "Retype admin password:" (masked with asterisks), "Password recovery question:" (containing "what's your nephew's middle name"), "Password recovery answer:" (containing "keenan"), and "Password recovery email address:" (containing "mike@abcd.com").

Note

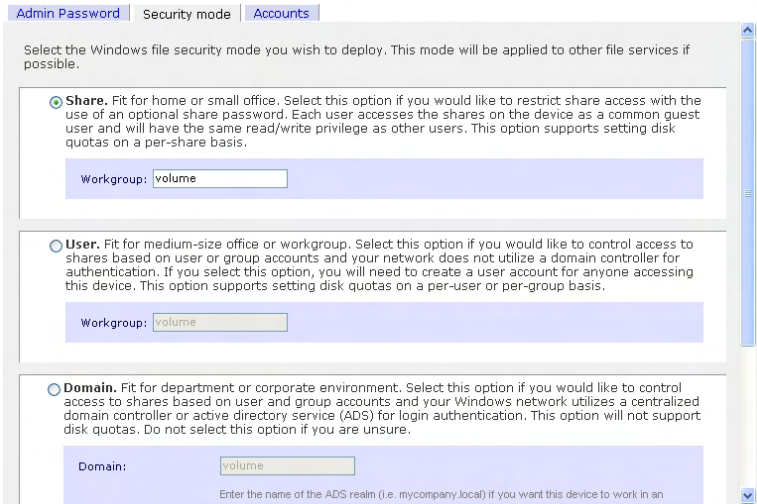
In User or Domain security mode, you can use the **admin** account to login to a Windows share, and perform maintenance on any file or folder in that share. The admin user also has permission to access all user private home shares to perform backups.

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. 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 ReadyNAS 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.



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 ReadyNAS device itself. In addition, each user account will be automatically set up with a private home share on the ReadyNAS.

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 ReadyNAS 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 ReadyNAS.

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 ReadyNAS 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.

A screenshot of a software interface showing a text input field. The label 'Workgroup:' is on the left, and the input field contains the text 'link'.

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 ReadyNAS. 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 ReadyNAS 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 ReadyNAS 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.

Workgroup:

► SETTING UP ACCOUNTS

In this security mode, the Accounts tab allows you to manage user and group accounts on the ReadyNAS. 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.

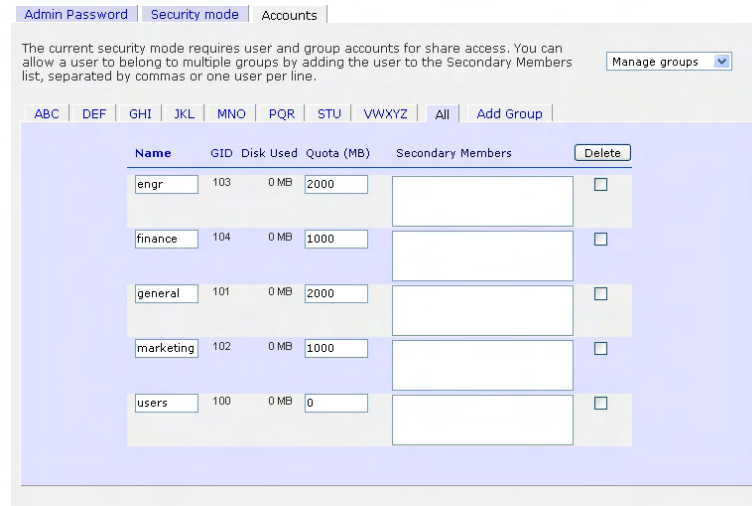
The current security mode requires user and group accounts for share access. You can allow a user to belong to multiple groups by adding the user to the Secondary Members list, separated by commas or one user per line. [Manage groups](#)

ABC | DEF | GHI | JKL | MNO | PQR | STU | VWXYZ | All | Add Group

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. Quota value of 0 disables disk quota enforcement.

Group	GID	Quota (MB)
finance		1000
enr		2000
marketing		1000
general		2000
		0

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



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



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 is 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**.

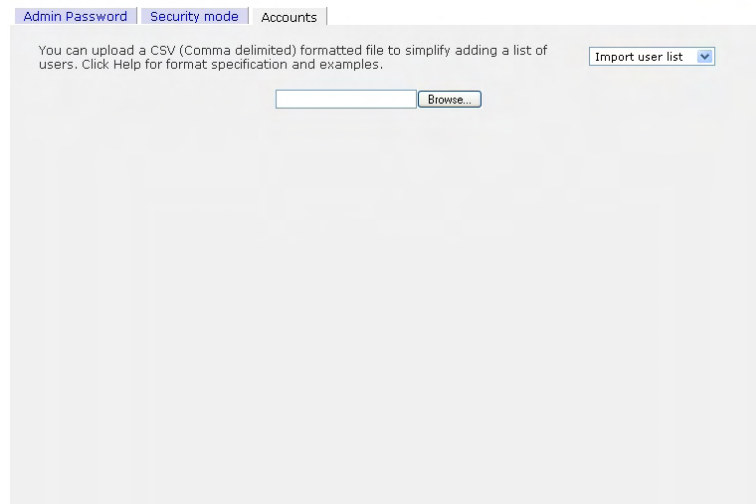
► MANAGING USERS

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.

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.



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 omitted 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 omit 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.

Admin Password | Security mode | Accounts

Set default parameters for new accounts. Preferences

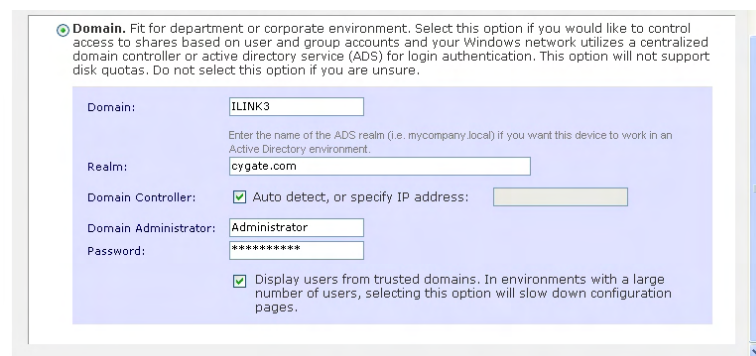
Default group for new users:	users
Private home shares for users:	Enabled
Recycle Bin for private home shares:	Disabled
Remove Recycle Bin files older than this many days:	10
Limit Recycle Bin to this many MB:	100
Allow users to change their passwords:	Enabled
Warn user when disk usage is:	80 % of quota

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 ReadyNAS device. You will need the following information:

- Domain name
- Domain administrator login
- Domain administrator password
- DNS name of the ADS realm (if using ADS)



The screenshot shows a configuration window for 'Domain' security mode. At the top, there is a radio button selected for 'Domain'. Below this, a text box explains: '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 form contains several fields: 'Domain:' with the value 'ILINK3'; 'Realm:' with the value 'cygate.com'; 'Domain Controller:' with a checked checkbox for 'Auto detect, or specify IP address:' and an empty text box; 'Domain Administrator:' with the value 'Administrator'; and 'Password:' with a masked password '*****'. At the bottom, there is a checked checkbox for '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 ReadyNAS 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.

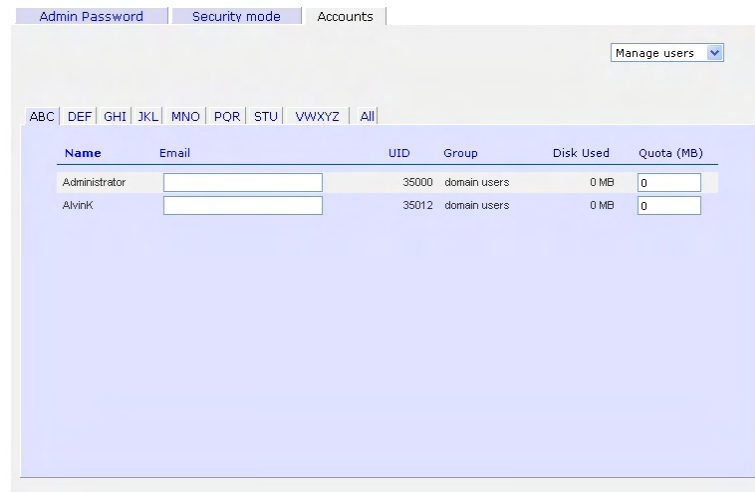
Note

Use of the ReadyNAS 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

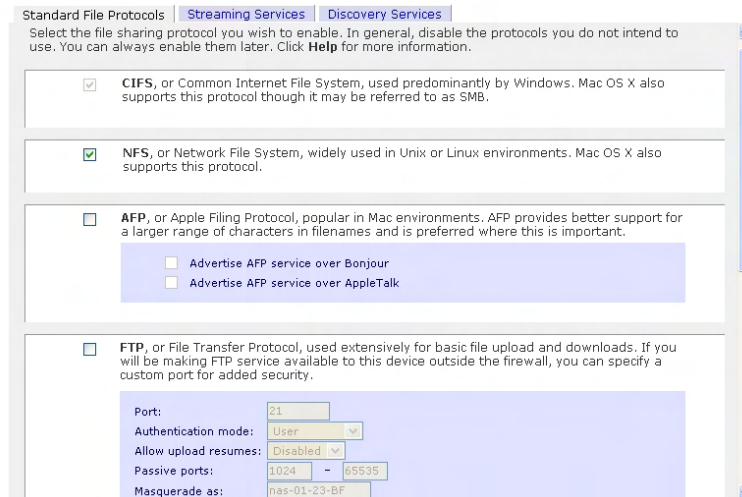
Accounts are managed on the domain controller. The ReadyNAS simply pulls the account information from the controller and displays them in the Accounts tab if you have the **Display users from trusted domains...** option enabled.



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 ReadyNAS.



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 ReadyNAS using built-in file manager over network file protocols on the client operating system. The available services are:

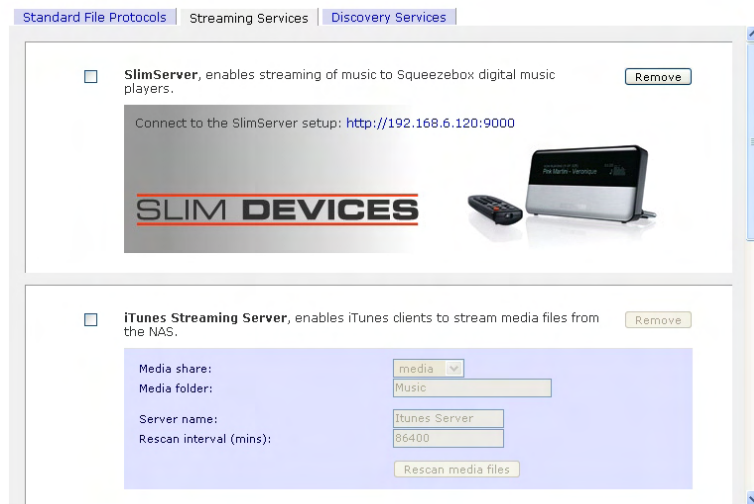
- **CIFS**, or Common Internet File Service, and often referred to as SMB. This protocol is a predominant protocol used by Microsoft Windows clients, and sometimes used by Mac OS X clients. Under Windows, when you click on My Network Places or Network Neighborhood, you're going across CIFS. This service is enabled by default and cannot be disabled.
- **NFS**, or 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 ReadyNAS supports NFS v3 over UDP.
- **AFP**, or Apple File Protocol. Mac OS 9 and OS X works best using this protocol as it handles a large range of character set. The ReadyNAS supports AFP 3.1.
- **FTP**, or File Transfer Protocol. Widely used in public file upload and download sites. ReadyNAS 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 a non-standard ports for better security when accessed over the Internet.
- **HTTP**, or Hypertext Transfer Protocol. Used by web browsers. ReadyNAS 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://readynas_ip` to `http://readynas_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**, or 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 ReadyNAS. This allows you to bypass the default dummy certificate warnings whenever you access the ReadyNAS.
- **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 ReadyNAS will allow clients to use Rsync to initiate backups to and from the ReadyNAS.

Streaming Services

Next are the Streaming File Protocols, a list of built-in streaming services available straight from the ReadyNAS, without the need to have your PC or Mac powered on.



- **SlimServer** provides music streaming to the popular Squeezebox music players from Slim Devices. You can click on the setup link for more detail configuration options.
- **iTunes Streaming Server** enables iTunes clients to stream media files straight from the ReadyNAS. You can specify the share and folder path where your music files reside, and you can specify a name for the service that will appear in your iTunes application as well as how often your music files will be rescanned on the ReadyNAS. Rescanning is required to update your music list, and you can opt to rescan your files manually.

- **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 ReadyNAS 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 are often utilizing 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** provides a simple way of discovering various services on the ReadyNAS. 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** service provides a means for UPnP-enabled clients to discover the ReadyNAS on your LAN.

Volume Management

The ReadyNAS family consists of two RAID volume technologies – **Flex-RAID**, utilizing the industry-standard RAID levels 0, 1, and 5, and **X-RAID**, Infrant Technologies' patented expandable RAID technology. Your system defaults to one or the other, 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.

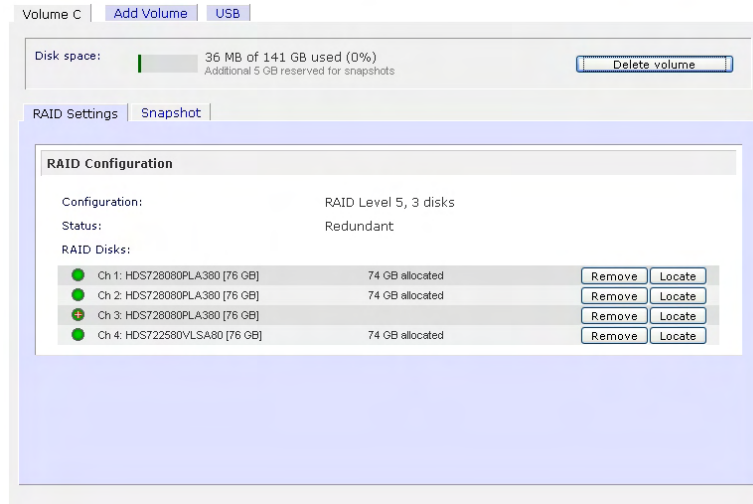
At a future point in time, each disk can be replaced one by one, have it finish rebuilding, and after the last disk is replaced, your volume automatically expands utilizing the new capacity.

Volume Management for Flex-RAID

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

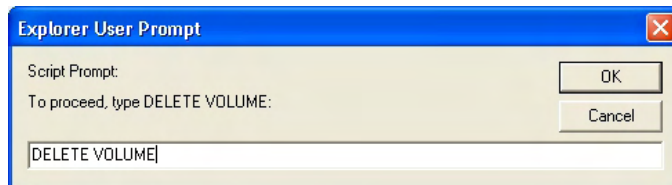
► DELETING A VOLUME

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!**



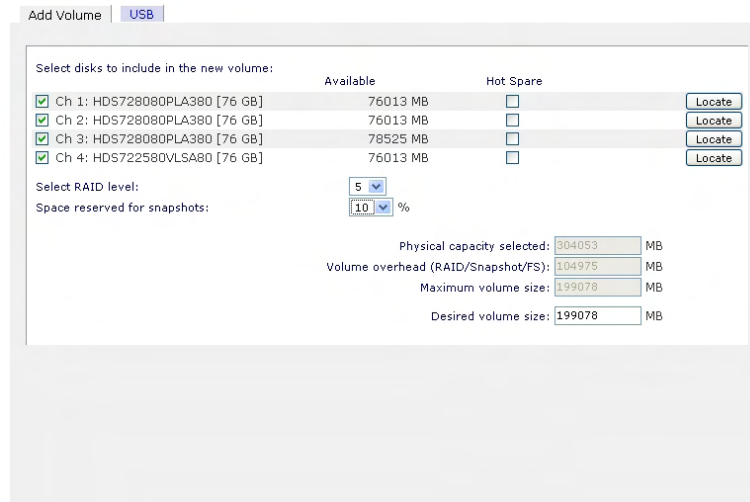
Click **Delete Volume** in the Volume C tab.

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



► ADDING A 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 is enough disks to fulfill the required minimum plus one.



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 percentage 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 percentage in 5% increment from 5 to 50%.

The percentage 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 previous 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 10% of the volume to be reserved for snapshots.

Note

If you do not reserve any space for snapshots, the snapshot tab will not be displayed within the volume tab.

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 instruction to reboot the system. It typically takes about a minute before you are notified to reboot.

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.

Volume C | Add Volume | USB

Disk space: 33 MB of 131 GB used (0%)
Additional 14 GB reserved for snapshots

RAID Settings | Snapshot

RAID Configuration

Configuration: RAID Level 5, 3 disks
Status: Redundant

RAID Disks:

● Ch 1: HDS728080PLA380 [76 GB]	74 GB allocated	Remove	Locate
● Ch 2: HDS728080PLA380 [76 GB]	74 GB allocated	Remove	Locate
● Ch 3: HDS728080PLA380 [76 GB]	74 GB allocated	Remove	Locate

Available Disks:

● Ch 4: HDS722580VLSA80 [76 GB]	74 GB free	Make hot spare	Locate
---------------------------------	------------	----------------	--------

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 ReadyNAS 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 ReadyNAS is not permitted during this time. You will be notified by email when the process is complete.

After you receive your email, the ReadyNAS 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 600GB 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 out your old disks.

First, power down the ReadyNAS, replace the first disk with the larger capacity disk, and boot. The ReadyNAS 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 ReadyNAS. 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 ReadyNAS 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 ReadyNAS 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

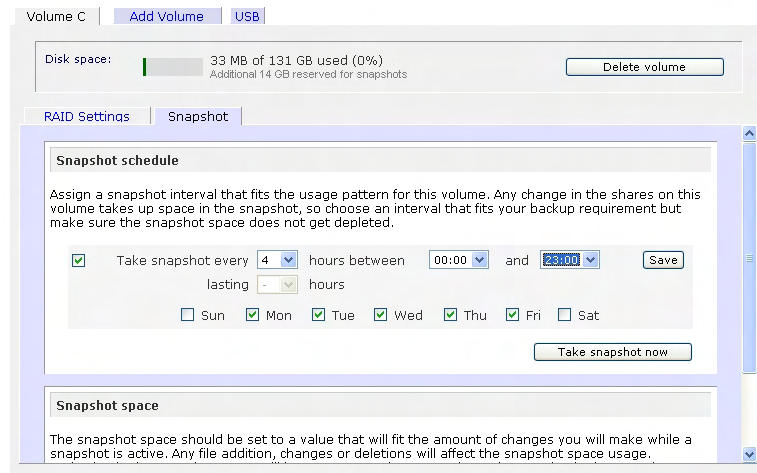
To take or schedule a snapshot, click on the **Snapshot** tab.

Note

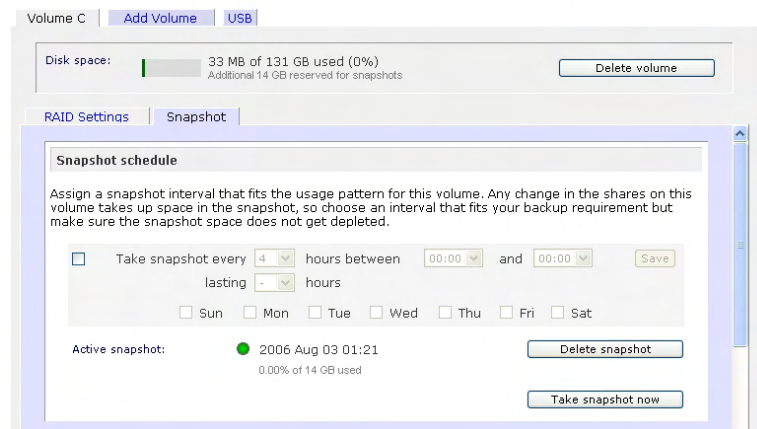
If you do not see a Snapshot tab within your volume tab, you did not reserve any space for snapshots when you added the volume. The ReadyNAS ships with a snapshot reserved space of 5 GB.

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.

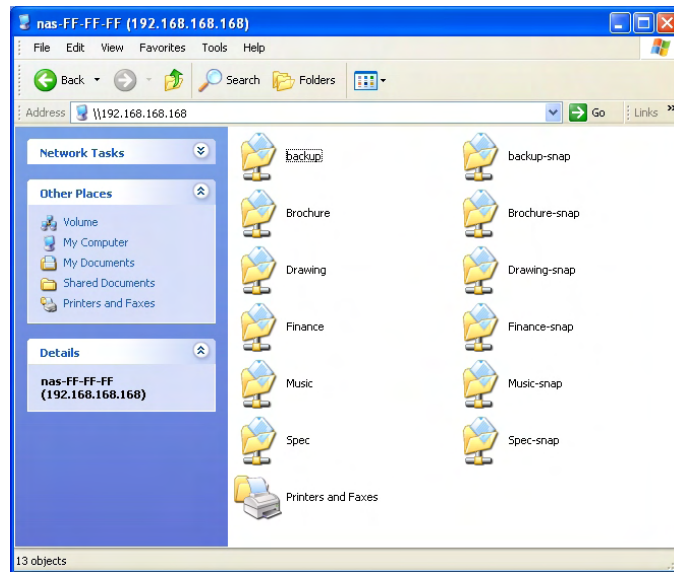


If you prefer, you can manually take a snapshot – just click on **Take snapshot now**.



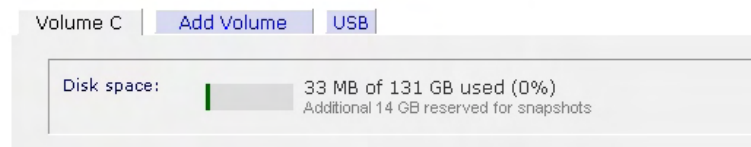
You can also specify how long a snapshot should last. If you will be using snapshots for backups, you can schedule the snapshot to last slightly longer than the expected duration of the backup. Having an active snapshot can affect the write performance to the ReadyNAS, so deactivating it when not needed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

Do note that 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.



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

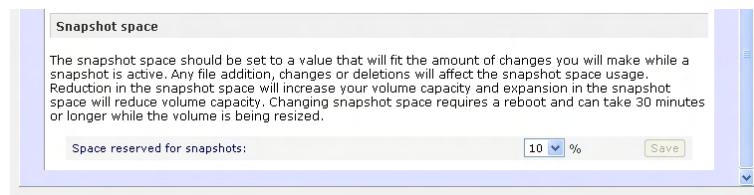
Note

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.



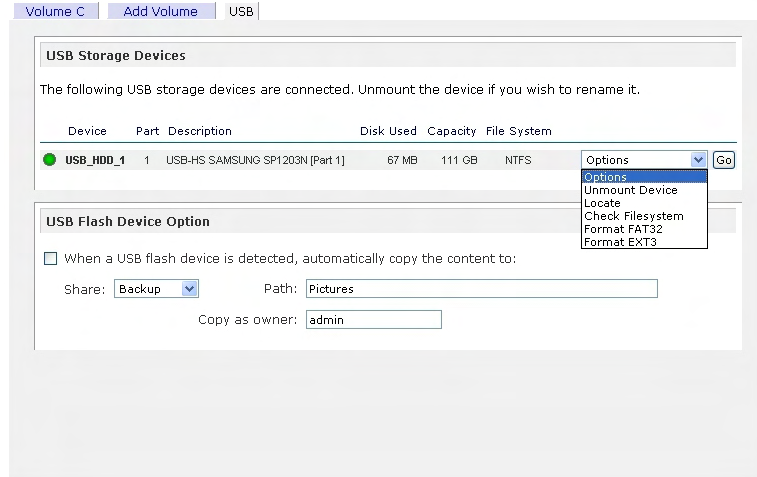
The process of resizing the snapshot space can take awhile depending on your data volume size and the number of files in your volume. Expanding the snapshot space will reduce your data volume size, and reducing the snapshot space will expand it.

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 be live.

USB Storage

The USB tab displays the USB disk and flash devices connected to the ReadyNAS, 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.



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

- FAT32
- NTFS (read-only)
- Ext2
- Ext3

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

- Unmount:** 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 Unmount command ensures that any data still in the write-cache is written out to the disks and the file system is properly closed. The Unmount option will unmount all partitions on the device.
- Mount:** If an **Unmount** operation was performed, the **Mount** command re-mounts the partitions and makes the USB share accessible again.
- 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 ReadyNAS 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_# or USB_HDD_# 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 ReadyNAS 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.

Add Shares

No shares exist. If you wish to enable file sharing, enter the share names you wish to add below and click Apply. You can specify a share password and share-level disk quota if this device is configured for **Share** security mode.

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

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.

Add Shares

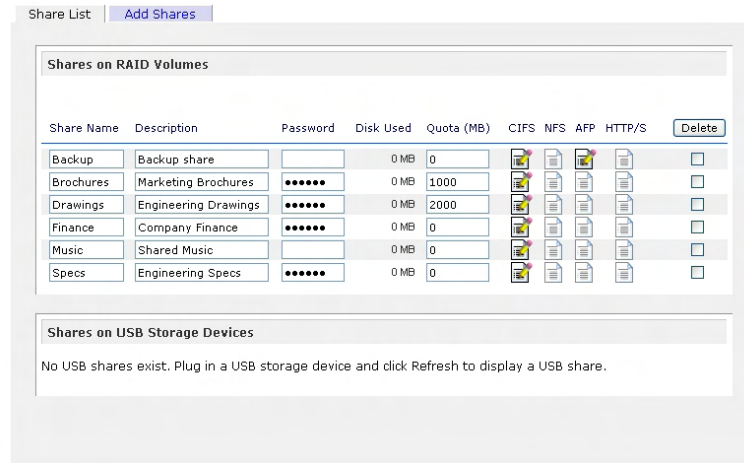
No shares exist. If you wish to enable file sharing, enter the share names you wish to add below and click Apply. You can specify a share password and share-level disk quota if this device is configured for **Share** security mode.

Share Name	Description
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.

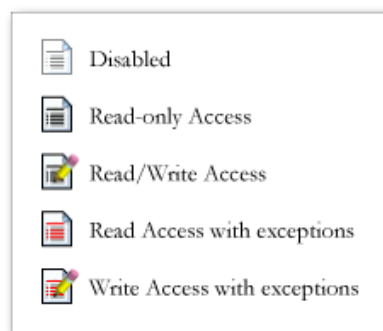
Managing Shares

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.



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:

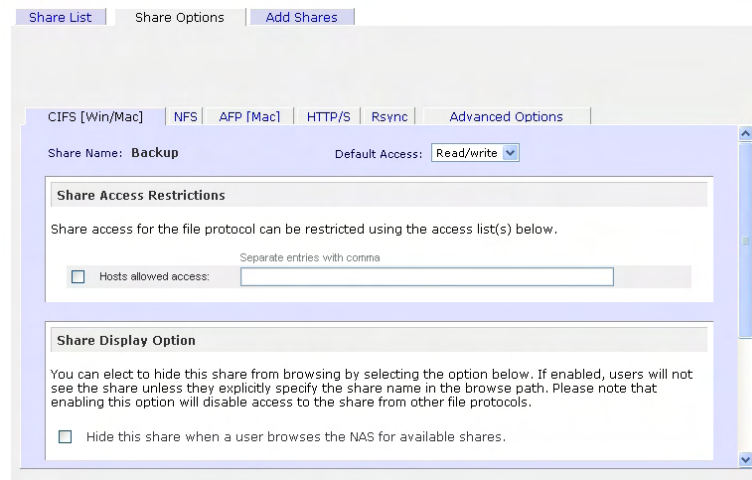
- **Disabled** – Access to this share is disabled.
- **Read-only Access** – Access to this share is read-only.
- **Read/Write Access** – Access to this share is read/write.

- **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:



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:

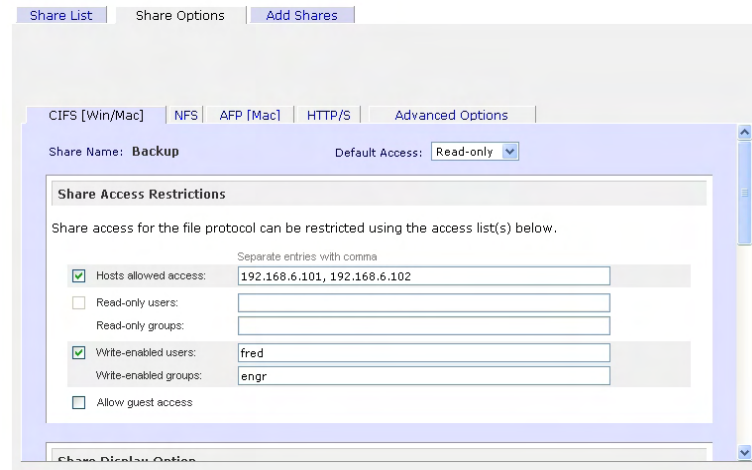
```
192.168.2. , 192.168.2.0/255.255.255.0 , 192.168.2.0/24
```

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 **Advanced CIFS Permission** options. Refer to the description for these options below.

► 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 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 ReadyNAS 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
```

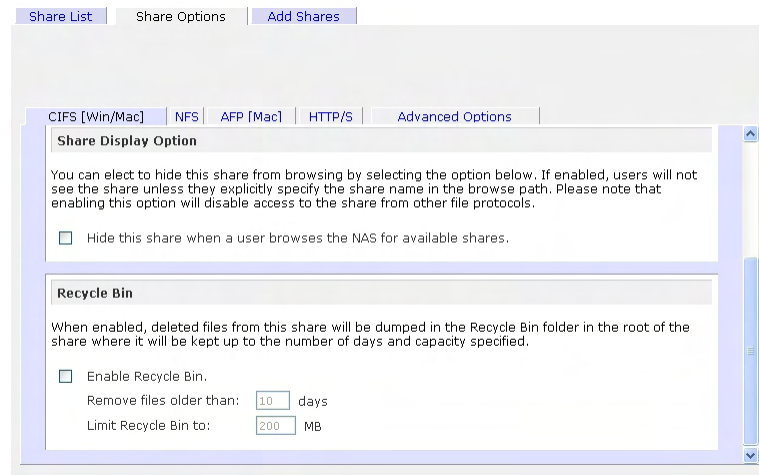
If you wish to specify some users and groups for read-only access and some for read/write access, and disallow all other users and groups, enter the following:

```
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

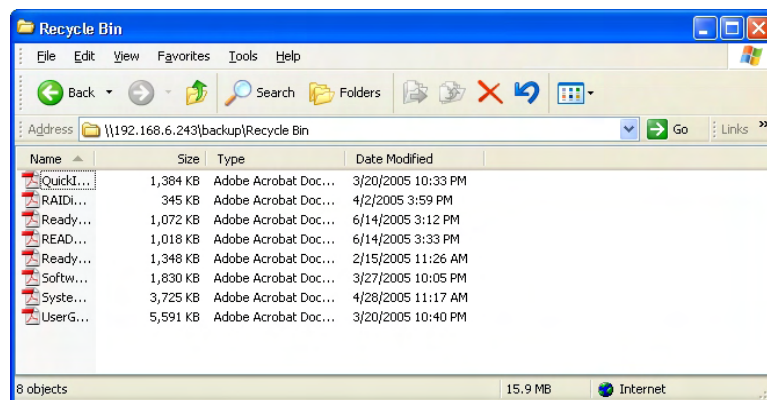
Restricting access to a share will not prevent users from seeing the share in the browse list. In certain instances, this might not be desirable, such as for backup shares that you may want to prevent users from seeing. To hide a share, select the **Hide this share...** option. Users who have access 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 ReadyNAS 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.

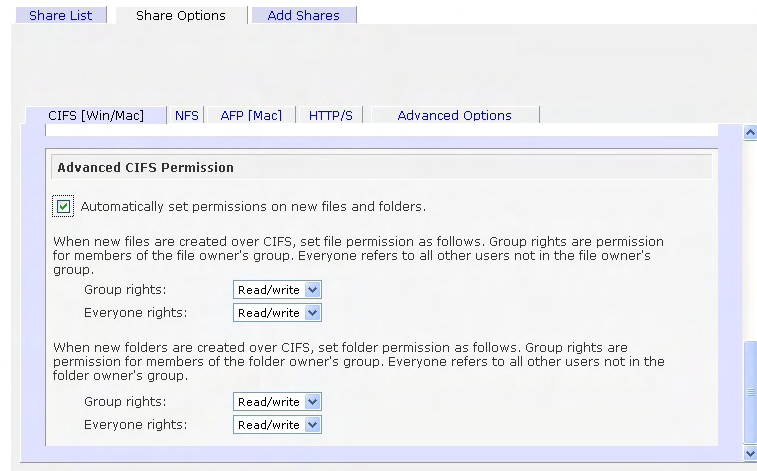
When enabled, whenever you delete a file, the file gets inserted into the Recycle Bin folder in the Share rather than being permanently deleted. This allows for a grace period where users can restore deleted files.



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.

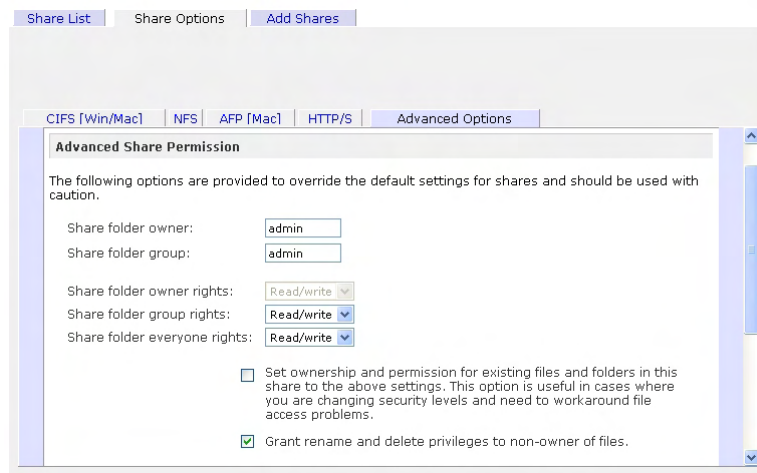
Advanced CIFS Permission

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.



► 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.



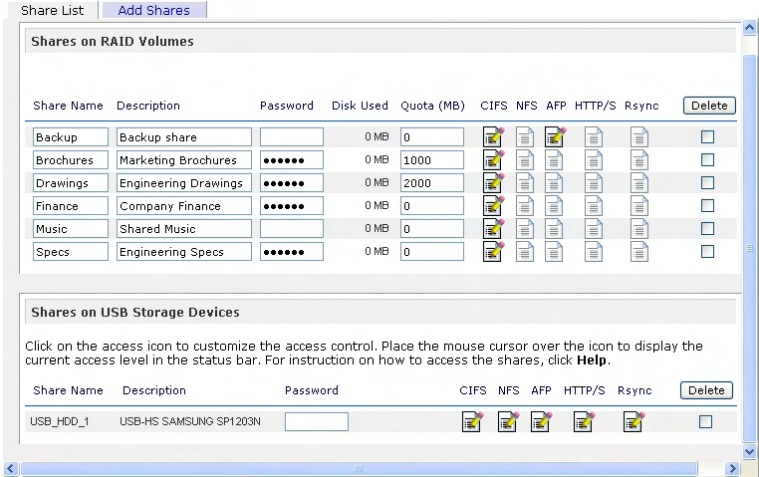
Advanced Share Permission

The Advanced Share Permission box 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 ReadyNAS 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.

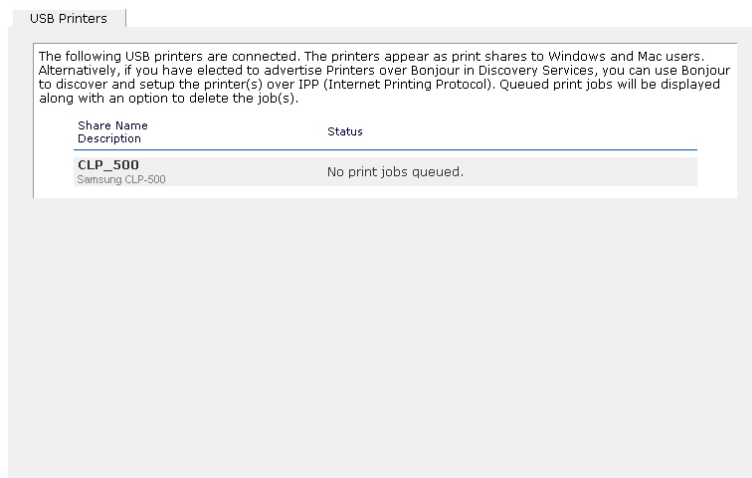


Note

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 ReadyNAS and PC systems.

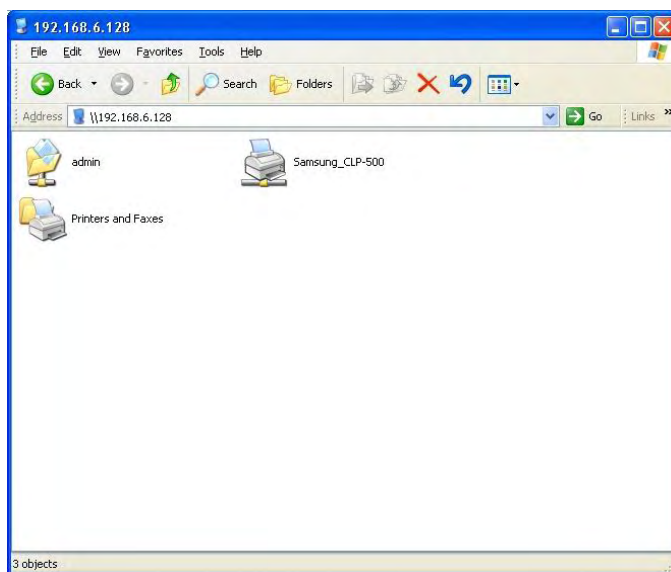
Printers

The ReadyNAS 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.



Print Shares over CIFS/SMB

The ReadyNAS 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 ReadyNAS.



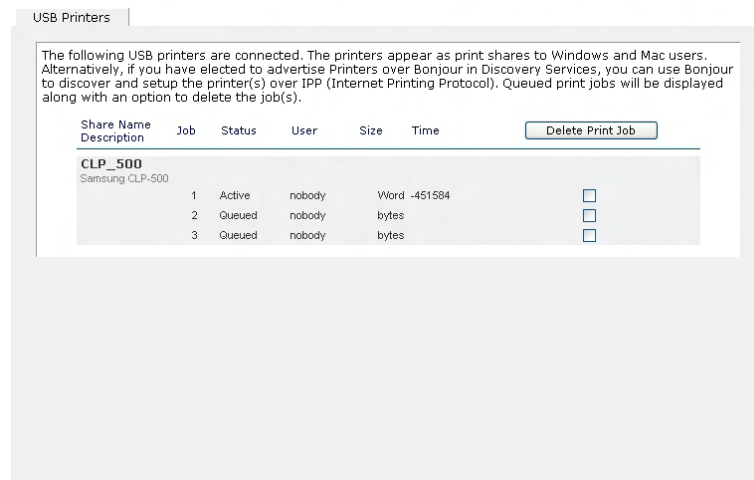
Double-click the printer icon to assign a Windows driver.

IPP Printing

The ReadyNAS also supports the IETF standard Internet Printing Protocol (IPP) over HTTP. Any client supporting IPP Printing (IPP is available natively on the latest Windows XP and OS X) can now use this protocol to utilize printers connected to the ReadyNAS. 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 ReadyNAS 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 screenshot shows a web interface titled "USB Printers". It contains a text box explaining that USB printers are connected and appear as print shares. Below this is a table with columns: Share Name, Description, Job, Status, User, Size, Time, and a "Delete Print Job" button. The table lists three jobs for the "CLP_500" printer (Samsung CLP-500). Job 1 is "Active", Job 2 is "Queued", and Job 3 is "Queued". Each job has a checkbox in the "Delete Print Job" column.

Share Name	Description	Job	Status	User	Size	Time	Delete Print Job
CLP_500	Samsung CLP-500	1	Active	nobody	Word	-451584	<input type="checkbox"/>
		2	Queued	nobody	bytes		<input type="checkbox"/>
		3	Queued	nobody	bytes		<input type="checkbox"/>

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

Backup

The **Backup** manager integrated with the ReadyNAS allows the ReadyNAS to act as a powerful backup appliance. Backup tasks can be controlled directly from the ReadyNAS 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 ReadyNAS can act as a simple central repository for both home and office environments.

And with multiple ReadyNAS systems, you can set up one ReadyNAS to backup another directly. The built-in **rsync** incremental backup support allows you to optimize an incremental backup schedule close enough in time to implement a remote data mirroring system.

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.

The screenshot shows the 'Add a New Backup Job' wizard in the ReadyNAS interface. The current step is 'STEP 1 - Select backup source'. The instructions state: '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. At least one of backup source or destination path must be local to this device.' There are two sections for selecting a source. The first section has a dropdown menu with options: 'Select this NAS or remote', 'Remote: Windows/NAS (Timestamp)', 'Remote: Windows (Archive Bit)', 'Remote: Website', 'Remote: FTP Site', 'Remote: NFS Server', and 'Remote: Rsync Server'. Below this are fields for 'Path:', 'Login:', and 'Password:', along with a 'Test connection' button. The second section is partially visible, showing similar options and fields.

► 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 ReadyNAS.

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 ReadyNAS 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 this if you wish to backup a website or a directory off the website. Files that will be backed up are the files referred to in the default index file and all the files associated with it, including image files referred by web pages linked to from the index file.
- **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 backup 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.

Once you have selected a backup source, you can enter the path from that source. If you selected a ReadyNAS 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 selection box shows an example format of the path. You can also click **Help** for more examples.

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 ReadyNAS 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 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 ReadyNAS (either the source or destination must be local to the ReadyNAS). If you had chosen a ReadyNAS share for the source, you can either enter another local ReadyNAS share for the destination, or you can specify a remote backup destination.

The screenshot shows a web-based interface for adding a new backup job. It is divided into three steps:

- STEP 1 - Select backup source:** This step includes a dropdown menu for 'Share' (set to 'Backup'), a 'Path' field, 'Login' and 'Password' fields, and a 'Test connection' button.
- STEP 2 - Select backup destination:** This step includes a dropdown menu for 'Remote' (set to 'Windows/NAS (Timestamp)'), a 'Path' field containing '//192.168.1.4/documentation', 'Login' (set to 'admin') and 'Password' (masked with dots) fields, and a 'Test connection' button.
- STEP 3 - Choose backup schedule:** This step is partially visible at the bottom of the window.

The remote backup destination can be a Windows PC/ReadyNAS system, NFS server, or a Rsync server. Note that you can select Rsync for a remote ReadyNAS 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.

The screenshot shows a web-based configuration interface for setting up a backup job. It is divided into two main sections: 'STEP 3 - Choose backup schedule' and 'STEP 4 - Choose backup options'. In Step 3, the user has selected 'Perform backup every 24 hours between 00:05 and 23:05' and has checked the days 'Mon', 'Tue', 'Wed', 'Thu', and 'Fri'. In Step 4, the 'Schedule full backup' is set to 'First time', and the option to 'Send backup log' is set to 'errors only'. There are also several unchecked checkboxes for advanced options like cleaning the destination and changing ownership.

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...** option. You may want to do this if you will be starting the backup from a Backup Button on ReadyNAS systems with this feature.

► STEP 4 - CHOOSE BACKUP OPTIONS

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

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 will 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 completes. 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).

Remove files from destination first

Next, 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, this new job will appear in the **Backup Schedule** tab.

The screenshot shows the Backup Manager interface with the 'Backup Listing' tab selected. The 'Backup Schedule' section displays a table of scheduled jobs. The table has columns for 'Enable', 'Job', 'Source Destination', 'When', and 'Status'. A single job is listed with job number '001', source destination '//192.168.1.4/documentation', and a schedule of 'Every 24 hr Between 00-23 Weekdays'. The status is 'Ready' with 'View log' and 'Clear log' links. Below the table is the 'Backup Button Setup' section, which includes a 'View' link, a 'Clear default backup button job logs' link, and a dropdown menu with the number '1' selected.

Enable	Job	Source Destination	When	Status
<input checked="" type="checkbox"/>	001	[Backup] //192.168.1.4/documentation	Every 24 hr Between 00-23 Weekdays	Ready View log Clear log Go Delete

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.

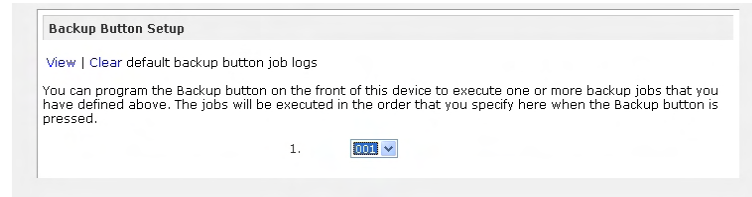
If you wish, you can enable or disable the job scheduling by clicking on the **Enable** checkbox. Disabling the job will not delete the job, but rather take it out of the automatic scheduling. If you wish to delete the job, click the **Delete** button.

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 Log** if you wish to check a detailed status of the backup.

Programming the Backup Button

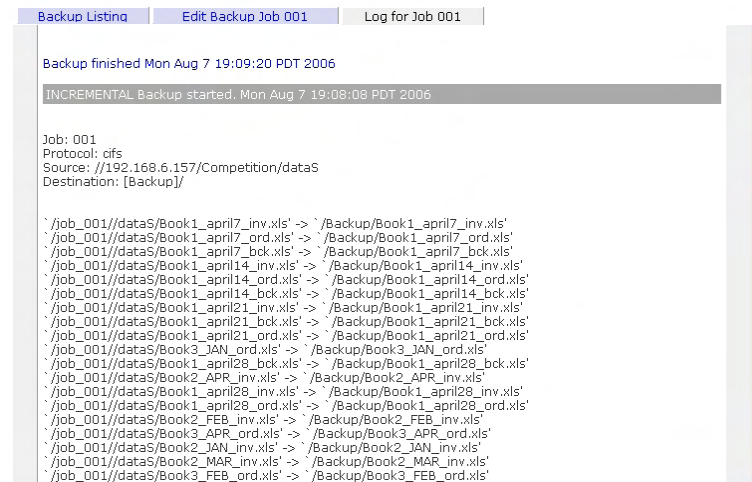
On ReadyNAS systems with the backup button feature, you can program the button to execute one or more pre-defined backup jobs.



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).

Viewing the Backup Log

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



The log format may differ depending on the backup source and destination type that was selected, but you can see when the job was started and finished, whether 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 Listing tab, or you can click on the **Edit Backup Job** tab while viewing that job's log. You can make appropriate changes or adjustments to the job there.

System

Clock

► 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.

The screenshot shows the 'Clock' configuration page with several tabs: 'Clock', 'Alerts', 'Performance', 'Language', 'Update', 'Power Management', and 'Shutdown'. The 'Clock' tab is active. A message at the top states: 'Accurate clock setting is required to ensure proper file timestamps.' Below this, there are three main sections: 'Select Timezone', 'Select Current Time', and 'NTP Option'. The 'Select Timezone' section has a dropdown menu set to 'GMT -08:00 Pacific Time (US & Canada); Tijuana'. The 'Select Current Time' section has date pickers for 'Aug', '3', and '2006', and time pickers for '03', '38', and '34'. The 'NTP Option' section has a checked checkbox for 'Synchronize clock with the following NTP server(s):' and two input fields for 'NTP Server 1' (192.168.6.84) and 'NTP Server 2' (0.pool.ntp.org).

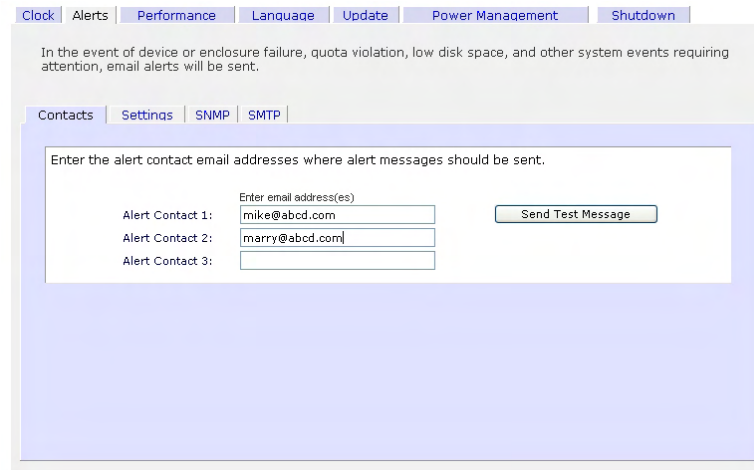
► NTP OPTION

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 ReadyNAS 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.

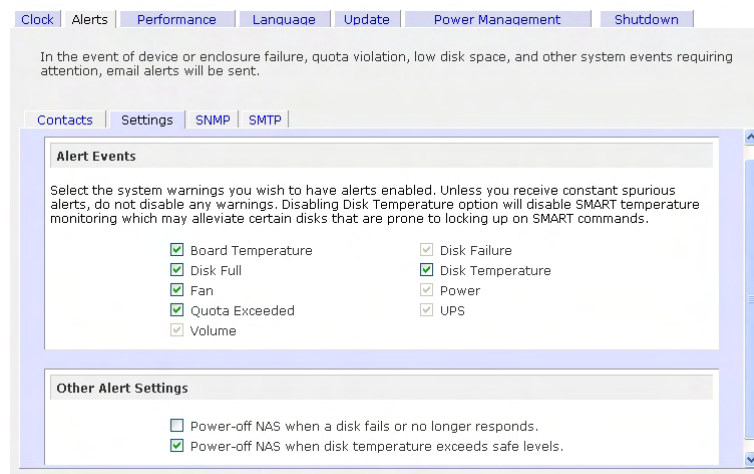


The screenshot shows the 'Alerts' tab in the ReadyNAS web interface. The 'Contacts' sub-tab is selected. The page contains a form for entering alert contact email addresses. The form includes a header: 'Enter the alert contact email addresses where alert messages should be sent.' Below this, there are three input fields labeled 'Alert Contact 1:', 'Alert Contact 2:', and 'Alert Contact 3:'. The first two fields contain the email addresses 'mike@abcd.com' and 'marry@abcd.com' respectively. A 'Send Test Message' button is located to the right of the input fields. The page also features a navigation menu at the top with tabs for 'Clock', 'Alerts', 'Performance', 'Language', 'Update', 'Power Management', and 'Shutdown'.

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



The screenshot shows the 'Alerts Settings' sub-tab in the ReadyNAS web interface. The page contains a section titled 'Alert Events' with the following text: '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.' Below this text, there are two columns of checkboxes, all of which are checked. The first column includes: Board Temperature, Disk Full, Fan, Quota Exceeded, and Volume. The second column includes: Disk Failure, Disk Temperature, Power, and UPS. Below the 'Alert Events' section, there is a section titled 'Other Alert Settings' with two checkboxes: 'Power-off NAS when a disk fails or no longer responds.' (unchecked) and 'Power-off NAS when disk temperature exceeds safe levels.' (checked). The page also features a navigation menu at the top with tabs for 'Clock', 'Alerts', 'Performance', 'Language', 'Update', 'Power Management', and 'Shutdown'.

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.

Other Alert Settings

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 ReadyNAS 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 ReadyNAS 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 ReadyNAS 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.

Contacts Settings **SNMP** SMTP

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:

Trap destination:

Separate entries with comma

Hosts allowed access:

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

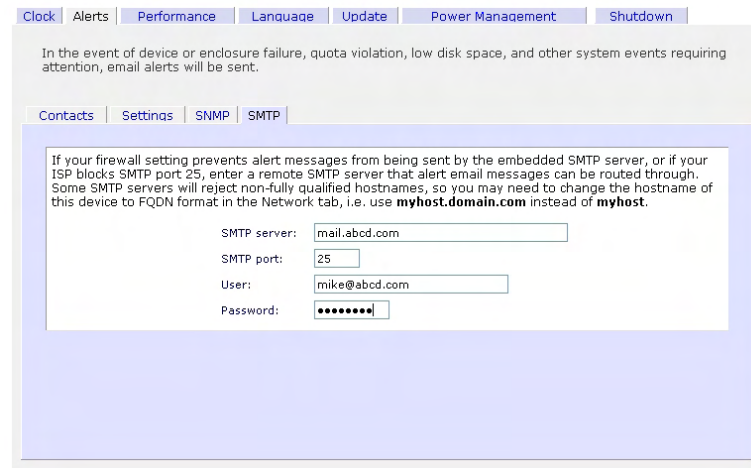
If you wish to limit SNMP access to only a secure list of hosts, please specify the hosts in the **Hosts allowed access** field.

When you have saved the SNMP settings on the ReadyNAS, you can import the Infrant SNMP MIB to your SNMP client application. The Infrant MIB can be obtained from the included Installation CD-ROM or downloaded from the Infrant Support site at <http://www.infrant.com>.

► SMTP

The ReadyNAS device 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, please specify an appropriate SMTP server in this tab.

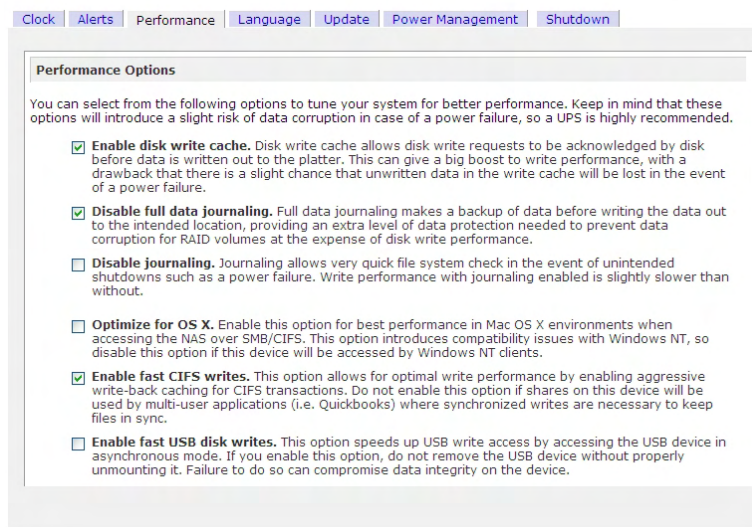


The screenshot shows the 'SMTP' configuration tab within the 'Alerts Settings' section. At the top, there are navigation tabs: 'Clock', 'Alerts', 'Performance', 'Language', 'Update', 'Power Management', and 'Shutdown'. Below these, a message states: 'In the event of device or enclosure failure, quota violation, low disk space, and other system events requiring attention, email alerts will be sent.' The 'SMTP' tab is selected, and a sub-tab bar shows 'Contacts', 'Settings', 'SNMP', and 'SMTP'. A text box contains the following instructions: '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**.' Below this text are four input fields: 'SMTP server:' with the value 'mail.abcd.com', 'SMTP port:' with the value '25', 'User:' with the value 'mike@abcd.com', and 'Password:' with a masked field of seven dots.

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.



Select **Enable disk write cache** if you want to utilize the performance advantages of write caching on the hard disks. For the utmost protection of data, you should utilize a UPS to back up the ReadyNAS because there is a slight chance that data queued up in the cache will be lost should a power failure occur while the system is writing data to the disk.

The **Disable full data journaling** is also recommended only if the NAS has UPS protection. 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 if a power failure suddenly occurs, possibly causing incorrect data to be recovered if one disk fails. Without full data journaling, disk write performance will increase substantially.

Select **Disable journaling** altogether if you understand the consequences of the 2nd option above, and you also don't 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 for less than \$50 (US dollars). By safely allowing the performance options to be checked, you can effectively double your write performance and provide uninterrupted service of your ReadyNAS for a very low price.

The **Optimize for OS X** option provides the best performance in Mac OS X environments when connected to the ReadyNAS via 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.

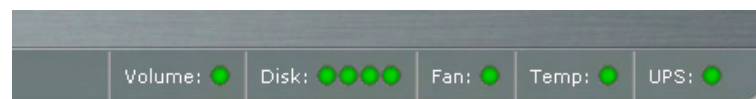
The **Enable fast CIFS writes** option allows for fast write performance by enabling aggressive write-back caching over CIFS. Do not enable this option multi-user application environments such as Quickbooks where synchronized writes are necessary to keep files in sync.

The **Force CIFS filename case-sensitivity** option provides substantial performance improvement when accessing CIFS shares when many files are being copied; however, before enabling this option, please understand the ramifications. Windows runs in case-insensitive mode, and one side-effect of enabling this option is that two filenames with different cases (i.e. ABC and abc) will appear as two files but opening one may actually open the wrong one. Another effect of this option is that you will now need to enter the exact case for search strings for the Find option in Explorer (i.e. find on abc will no longer return file ABC). Also, some Windows applications that assume case-insensitive operations (i.e. BackupExec) may have problems. Do not enable this option if you will have clients running Windows NT/95 or earlier accessing the NAS.

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 NAS¹. 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.



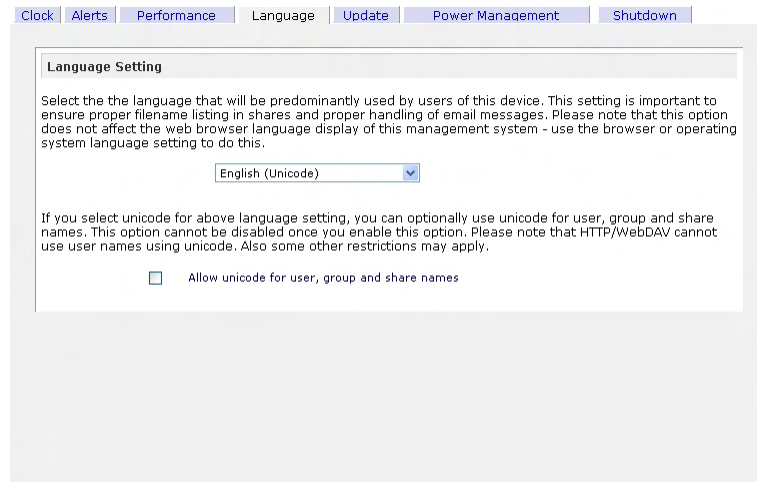
You will be notified by email whenever the status of the UPS changes, i.e. when a power failure forces the UPS to be in battery mode or when the battery is low. When the battery is low, the NAS device will automatically shutdown safely.

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

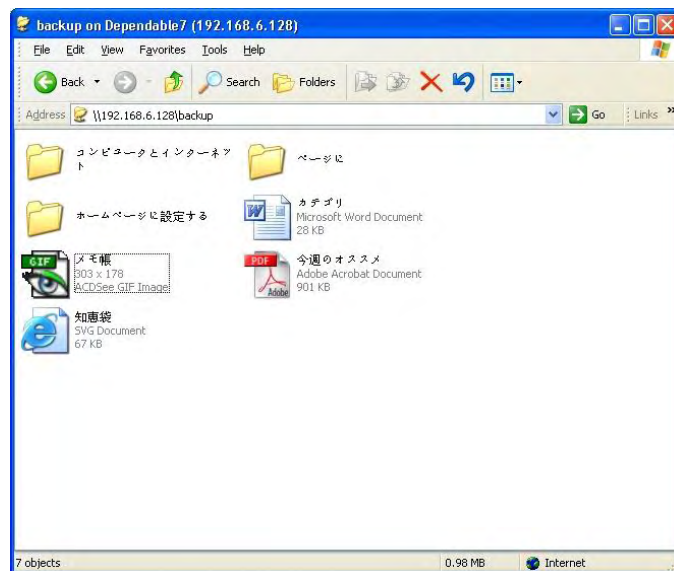
¹ Note that alert notification and automatic system optimization is available only with UPS utilizing a USB monitoring interface.

Language

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



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



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

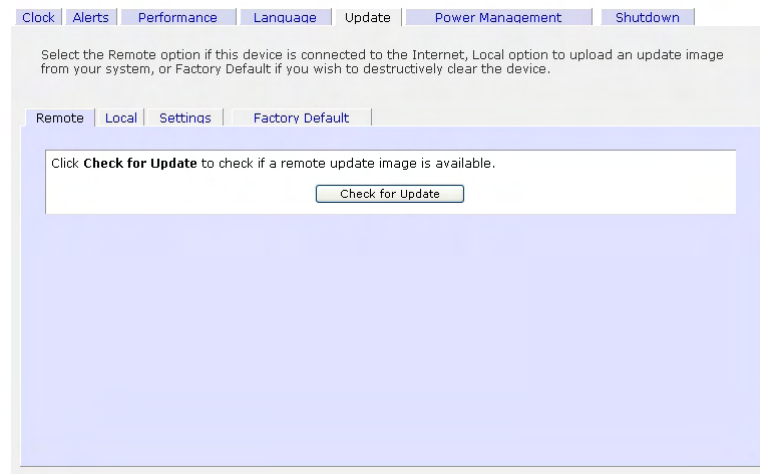
HTTP and WebDAV access will not work with Unicode user names. Other restrictions may exist.

Updating ReadyNAS

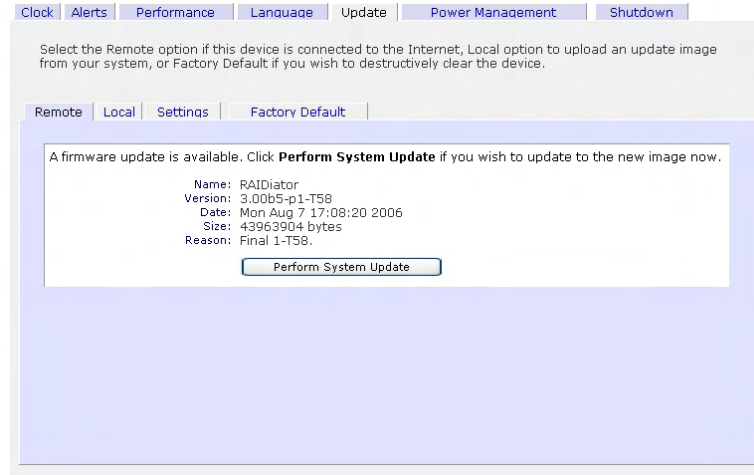
The ReadyNAS device offers the option of upgrading the operating firmware either automatically using the Remote Update option or manually loading an update image downloaded from the Infrant Support website.

► REMOTE UPDATE

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



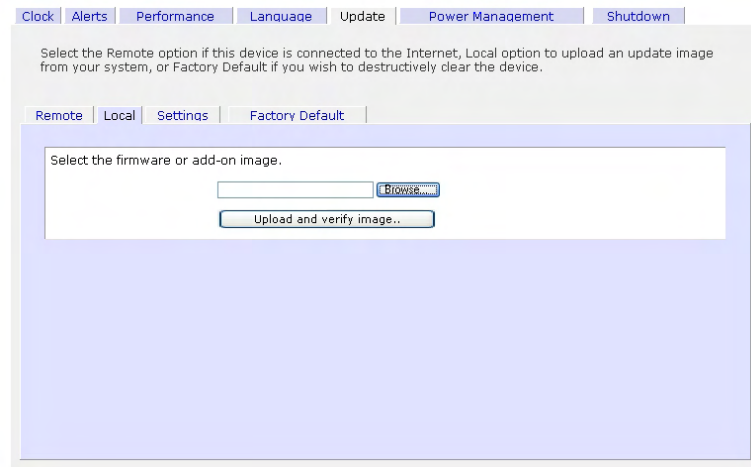
Simply click Check for Update to check for updates on the Infrant update server.



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

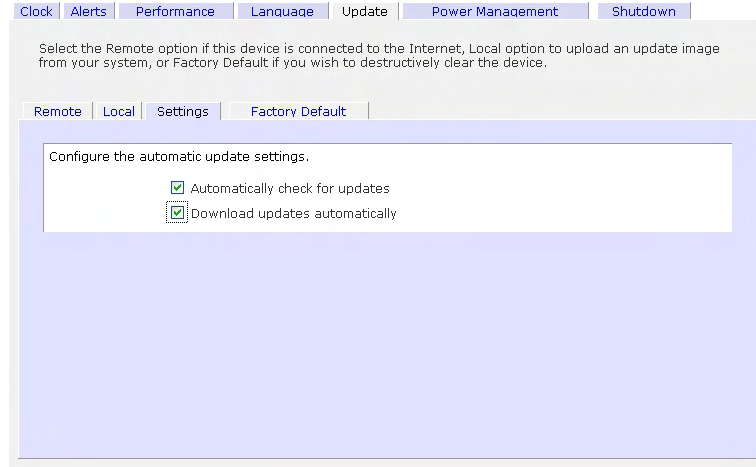
When the ReadyNAS device is not connected to the Internet, or Internet access is blocked, you can download an update file from the Support site and upload that file to the ReadyNAS in the **Local** update tab.



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 you will be requested to reboot the system to proceed with the upgrade. **DO NOT click on the browser Refresh button** during the update.

► SETTINGS

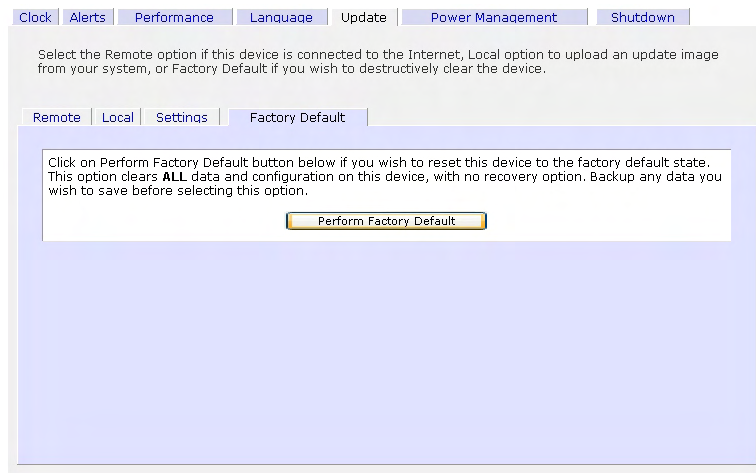
If you do have reliable Internet connection, you can enable the automatic update check and download options in the Settings tab.



If you enable the **Automatically check for updates** option, the ReadyNAS 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 ReadyNAS 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.



You will be asked to confirm the command by typing: **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 ReadyNAS 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 ReadyNAS disks after a specified time of inactivity. The disks will spin-up as needed.

The screenshot shows the 'Power Management' tab in the ReadyNAS web interface. It contains two main sections: 'Disk Spin-down Option' and 'Power Timer'.

Disk Spin-down Option: This section includes a checkbox labeled 'Enable disk spin-down after' which is checked. Next to it is a dropdown menu set to '5' minutes of inactivity. A note above the checkbox states: '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.'

Power Timer: This section includes a checkbox labeled 'Enable power timer' which is unchecked. Below it is a table for scheduling power actions.

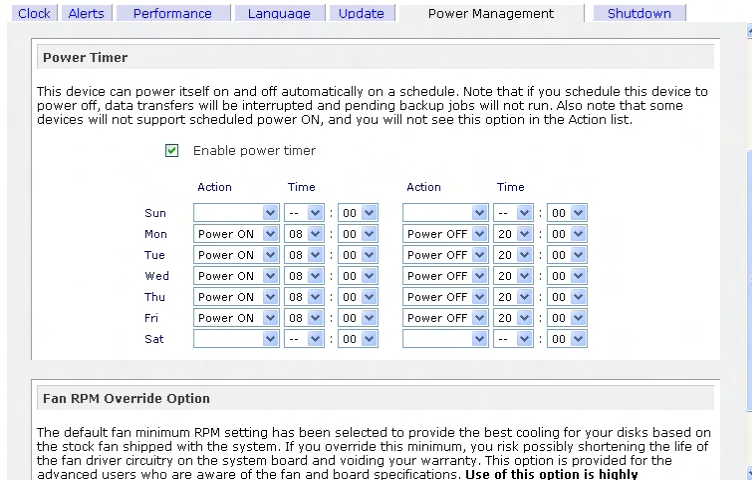
	Action	Time	Action	Time
Sun	---	:00	---	:00
Mon	---	:00	---	:00
Tue	---	:00	---	:00
Wed	---	:00	---	:00

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 ReadyNAS can be scheduled to power off and power back on (on certain models) automatically. Select the **Enable power timer** checkbox and enter the desired action and time. The **Power ON** option is available on the ReadyNAS NV through an add-on package due to certain limitations. Please refer to the Release Notes for RAIDiator 3 on the Infrant Support site for more information.



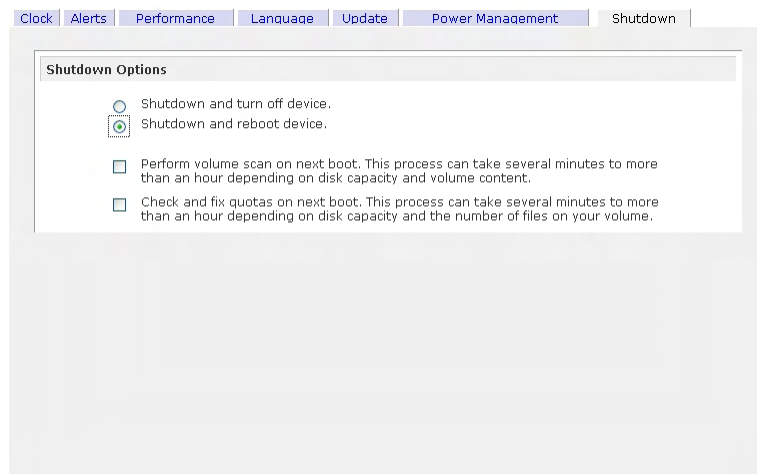
The **Power ON** option will not appear if the ReadyNAS hardware does not support this feature.

Note

When the ReadyNAS 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.

Shutdown

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



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 ReadyNAS, you will need to close the browser window and use RAIDar to re-connect to FrontView.

Status

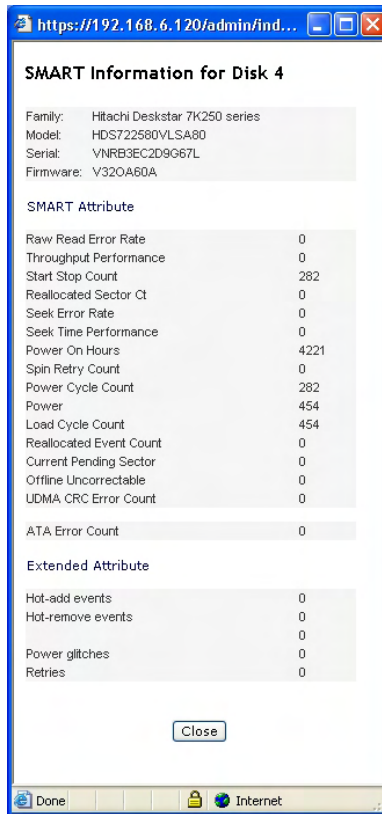
The Status page consists of the **Health** and **Logs** tabs providing system status information.

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	HDS728080PLA380 76 GB, 38C / 100F, Write-cache ON, SMART+	OK
Disk 2	HDS728080PLA380 76 GB, 40C / 104F, Write-cache ON, SMART+	OK
Disk 3	HDS728080PLA380 76 GB, 40C / 104F, Write-cache ON, SMART+	OK
Disk 4	HDS722580VLSA80 76 GB, 38C / 100F, Write-cache ON, SMART+	OK
Fan 1	1470 RPM Recalibrate	OK
Temp 1	33.5C / 92F [Normal 0-60C / 32-140F]	OK
UPS 1	Not present	OK

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



Logs

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



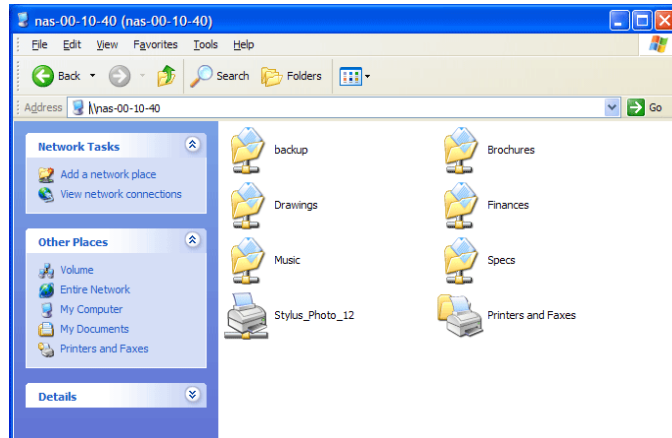
The **Send All Logs** button is available in case of problems where technical support personnel may be of assistance in analyzing low-level log information. Alternatively, if you have problems with the ReadyNAS sending out email through your firewall, you can download a zip of all the logs by clicking the **Download All Logs** link.

Accessing Shares

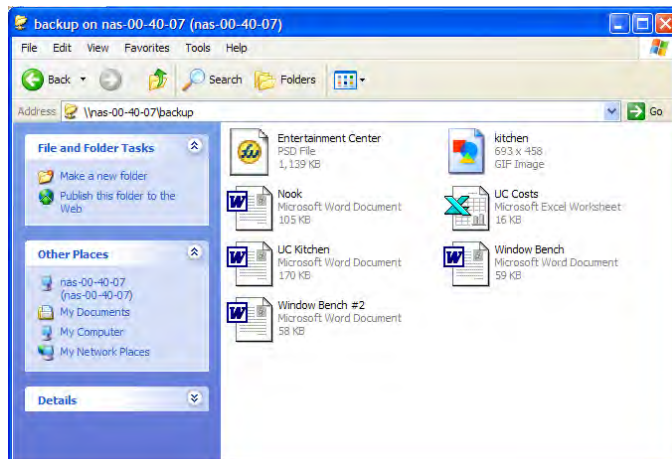
This chapter presents examples of how shares on the ReadyNAS device can be accessed by the various operating systems. If you have problems accessing your shares, make sure to enable the corresponding service in the **Shares Services** tab. Also make sure the default access of the share is set to **Read-only**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

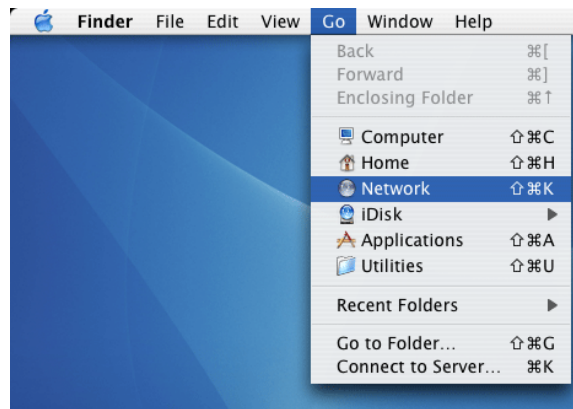


To access the share under Windows, specify the hostname followed by the share name in the Explorer address bar, i.e. `\\hostname\backup`, as follows:



MAC OS X

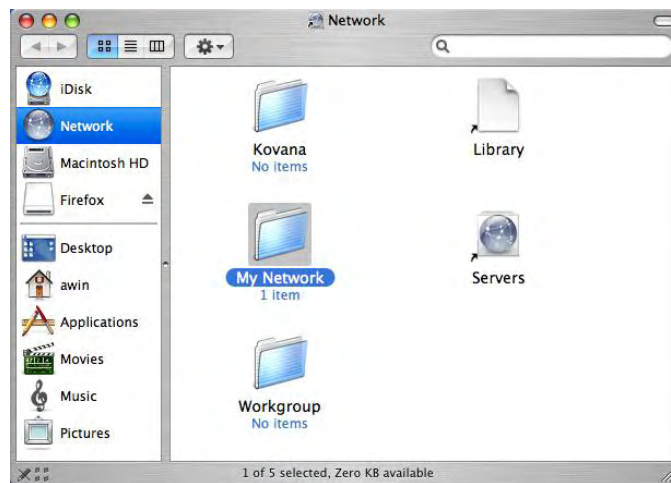
To access the same share over AFP with OS X, select **Network** from the Finder **Go** menu.



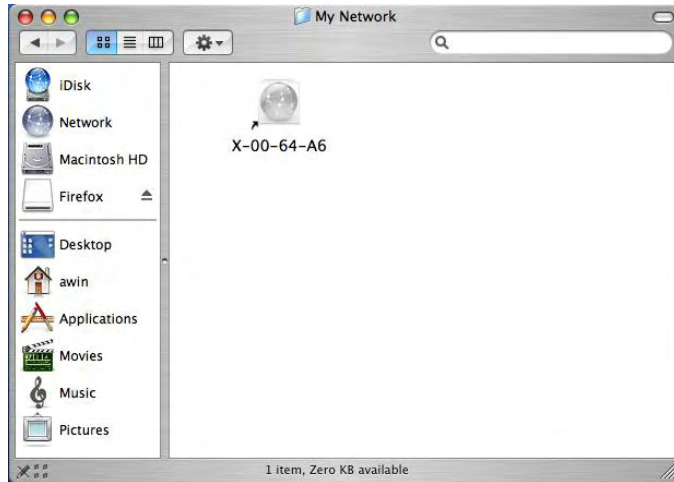
At this point, there are two ways in which you can access your AFP share, depending on how you have chosen to advertise your AFP share.

AFP over Bonjour

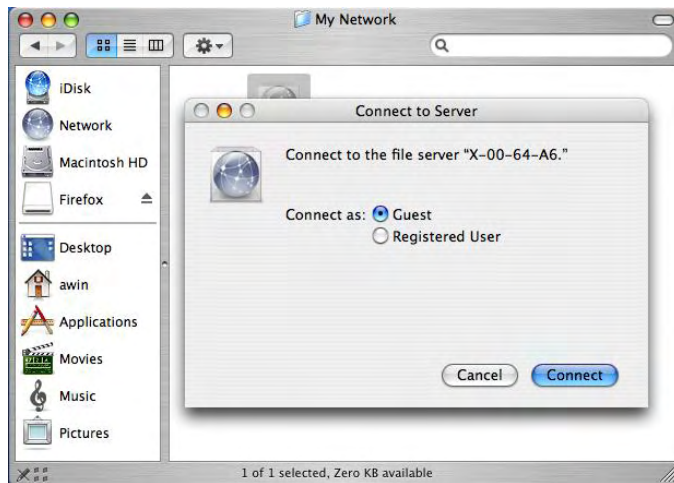
To access the AFP share advertised over **Bonjour** on Mac OS X, select **Network** from the Finder **Go** menu to see a listing of available networks.



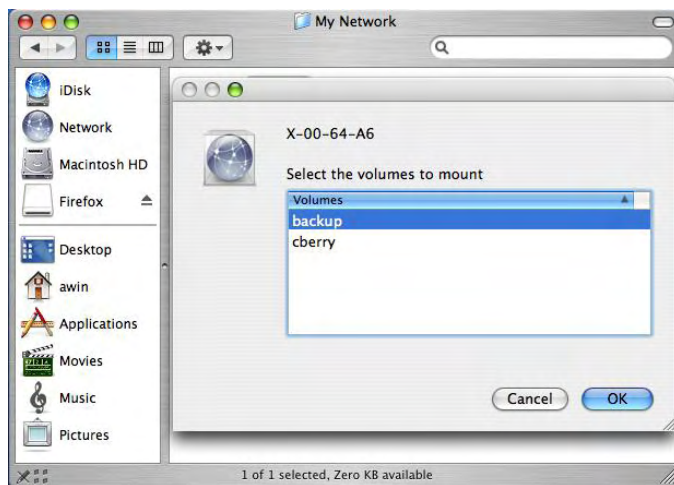
Open the **My Network** folder to display the ReadyNAS hostname.



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



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 ReadyNAS as.



Select the Share you would like to view.

AFP over AppleTalk

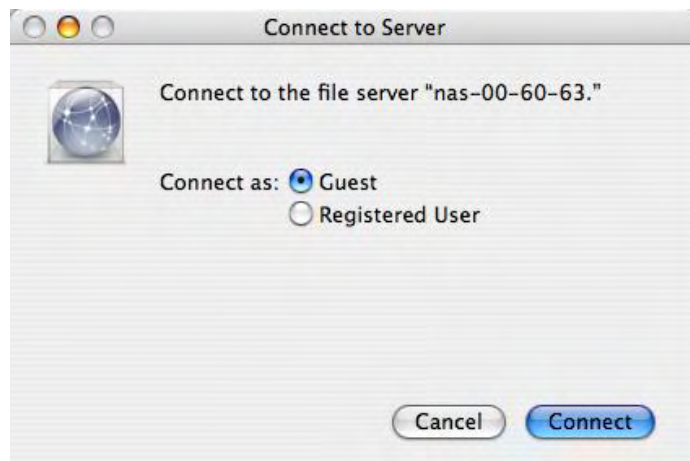
If you had chosen to advertise your AFP service over AppleTalk, you will see a listing of available networks.



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



You'll be prompted with a connection box.



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



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 ReadyNAS as.

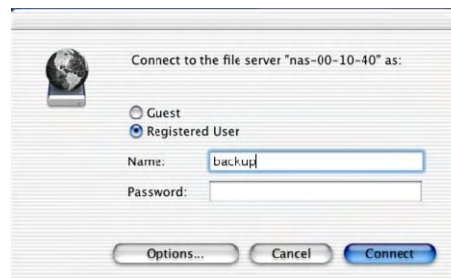
You should see the same file listing as you would in Windows Explorer.

MAC OS 9

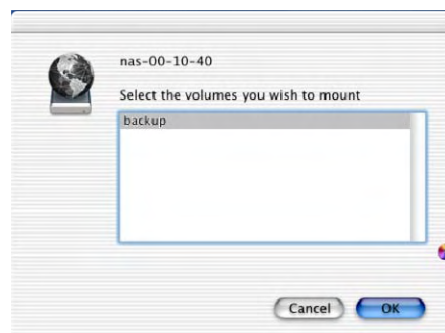
To access the same share under Mac OS 9, select **Connect to Server** from the Finder menu, choose the NAS device entry from the AppleTalk selection, and click **Connect**.



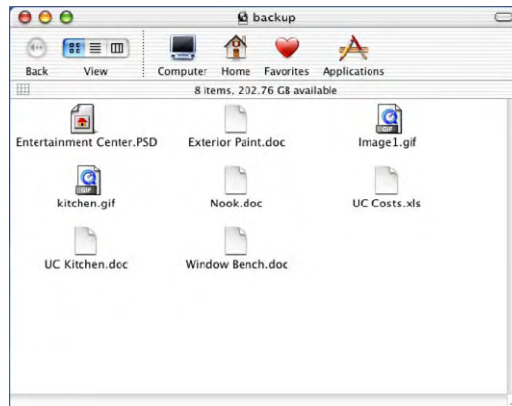
When you are prompted to login, enter the **share name** and **password** if the ReadyNAS is configured for **Share** security mode, or enter a valid **user account** and **password** otherwise.



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.



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

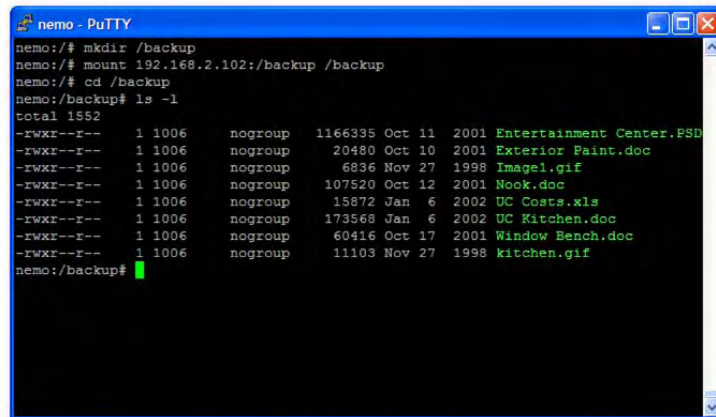


Linux/Unix

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.



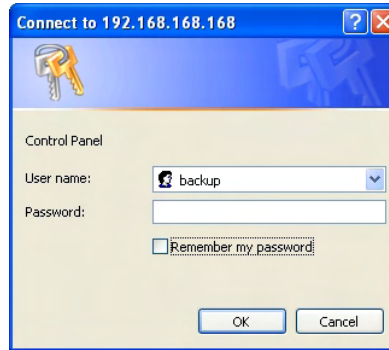
```
nemo - PuTTY
nemo:/$ mkdir /backup
nemo:/$ mount 192.168.2.102:/backup /backup
nemo:/$ cd /backup
nemo:/backup# ls -l
total 1552
-rwxr--r-- 1 1006 nogroup 1166335 Oct 11 2001 Entertainment.Center.PSD
-rwxr--r-- 1 1006 nogroup 20480 Oct 10 2001 Exterior.Paint.doc
-rwxr--r-- 1 1006 nogroup 6836 Nov 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

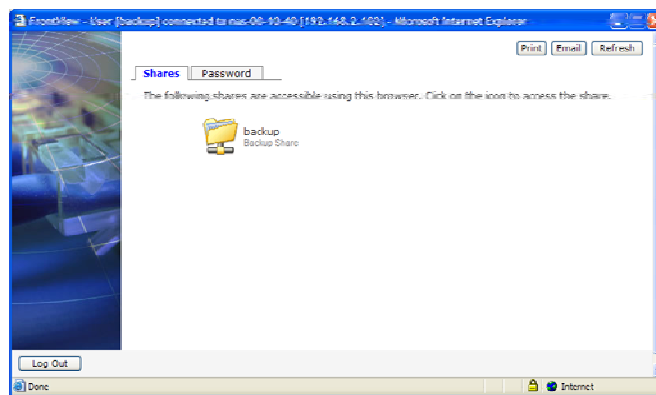
Please note that the ReadyNAS does not support NIS as it is unable to correlate NIS information with CIFS logins. In mixed environments where CIFS and NFS integration is desired, you can set the security to User mode and manually specify the UID and GID of the user and group accounts to match your NIS or other Linux/Unix server settings. The ReadyNAS 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

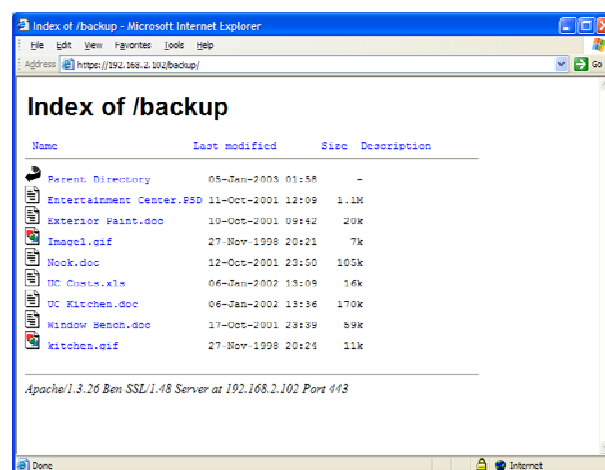
To access the same share using a web browser, enter <http://ipaddr> in the browser address bar. You can use **https** if you want a secure encrypted connection. You will be prompted to login.



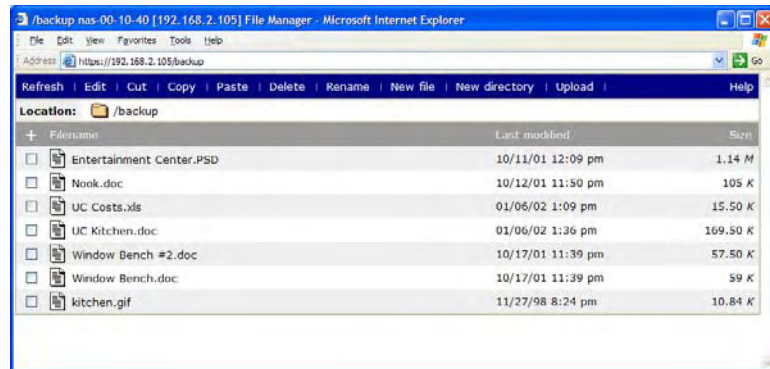
Enter the share name and share password if the ReadyNAS is in **Share** security mode. Otherwise, login with a valid user and password if the ReadyNAS is in **User** or **Domain** mode.



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



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



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.

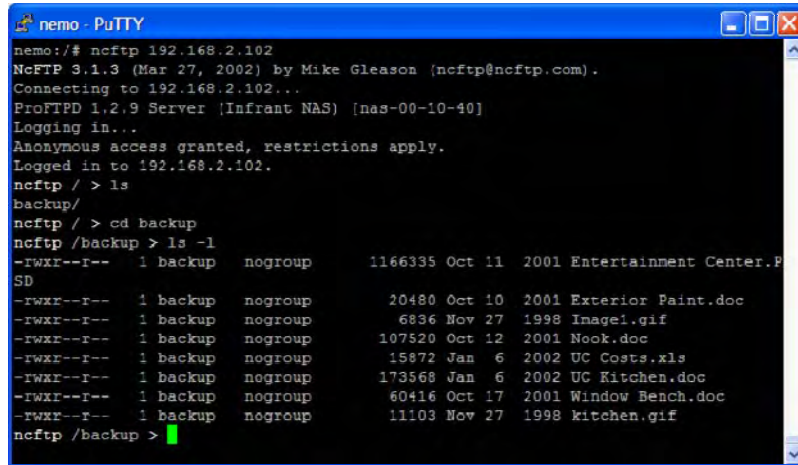
Note

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 - PuTTY
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 Inage1.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 that enabling FTP access in Share mode opens up the share to anyone who has a FTP client on your network. It is best to enable FTP access only to shares you are comfortable making public on your network.

Warning

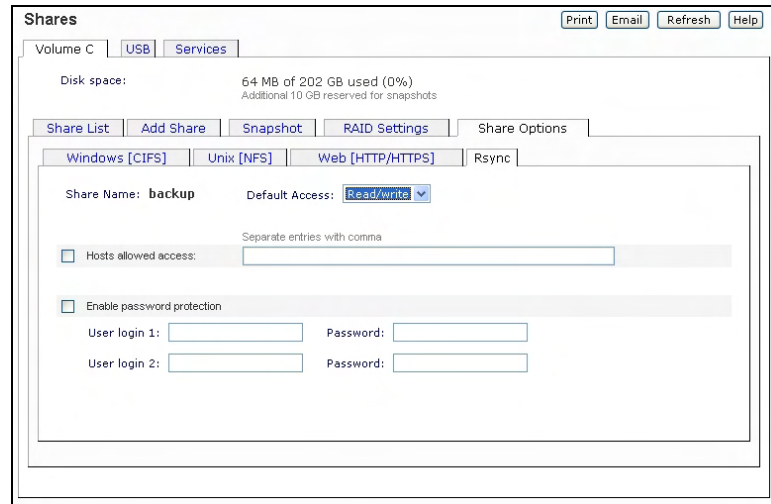
Disk usage using FTP in Share mode **WILL NOT** count towards the share disk quota, so carefully choose how you advertise a FTP Share.

To access the share in User or Domain security mode, use the appropriate user login and password used to access the ReadyNAS.

For better security, you can use a FTPS (FTP-SSL) client to connect to the ReadyNAS 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 ReadyNAS or a domain controller.



The screenshot shows the 'Shares' configuration page for 'Volume C'. The 'Rsync' tab is selected. The share name is 'backup' and the default access is 'Read/write'. There are checkboxes for 'Hosts allowed access' and 'Enable password protection'. Below these are input fields for 'User login 1', 'User login 2', 'Password', and 'Password'.

An example way for a Linux client to list the content of a ReadyNAS 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 ReadyNAS does not support rsync over SSH.

Networked DVD Players and UPnP AV Media Adapters

Networked DVD players and UPnP AV Media adapters will detect the ReadyNAS if the Home Media Streaming Server or the UPnP AV services are enabled. The content of the *media* share on the ReadyNAS 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 ReadyNAS and can play the media files concurrently.

Do make sure to enable the appropriate service in the Services tab.

The screenshot shows the 'Discovery Services' tab in the ReadyNAS configuration interface. It features two service configuration sections:

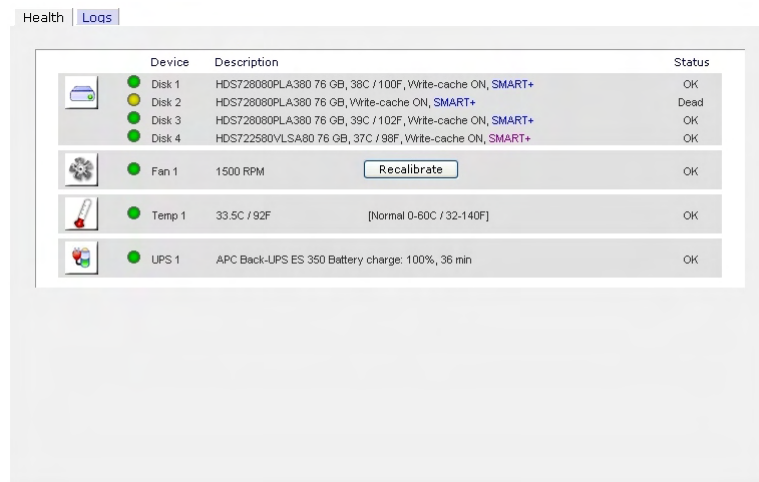
- UPnP AV:** This section is currently disabled, indicated by an unchecked checkbox. It includes a 'Media share' dropdown menu set to 'Backup', a 'Media folder' text input field, and a 'Rescan media files' button. A note below states: '* Home Media Streaming Server and UPnP AV services share the same media path.'
- Home Media Streaming Server:** This section is enabled, indicated by a checked checkbox. It includes a 'Media share' dropdown menu set to 'Backup', a 'Media folder' text input field, and a 'Hidden folder' text input field. Below these are several settings: 'Remote control code for hidden folder (3-digit number):' (text input), 'Target JPEG output:' (dropdown menu set to '720p'), 'Slide show delay (secs):' (dropdown menu set to '10'), 'Bookmarks:' (dropdown menu set to 'Enabled'), 'Allow delete from player:' (dropdown menu set to 'Disabled'), and 'Maximum playlist items:' (text input field set to '2000').

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

Replacing a Failed Disk

Locate the Failed Disk

When a disk fails in your ReadyNAS 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.



The screenshot shows the 'Health' tab in the ReadyNAS FrontView interface. It displays a table of system components and their status. The 'Disk 2' entry is highlighted in red, indicating a failure. The status bar also includes icons for a failed disk, a fan, a temperature gauge, and a UPS.

Device	Description	Status
Disk 1	HDS728080PLA380 76 GB, 38C / 100F, Write-cache ON, SMART+	OK
Disk 2	HDS728080PLA380 76 GB, Write-cache ON, SMART+	Dead
Disk 3	HDS728080PLA380 76 GB, 39C / 102F, Write-cache ON, SMART+	OK
Disk 4	HDS722580VLSA80 76 GB, 37C / 98F, Write-cache ON, SMART+	OK
Fan 1	1500 RPM <input type="button" value="Recalibrate"/>	OK
Temp 1	33.5C / 92F [Normal 0-60C / 32-140F]	OK
UPS 1	APC Back-UPS ES 350 Battery charge: 100%, 36 min	OK

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

Order Replacement Disk

Go to the Status menu and click on the Health tab. Take note of the disk vendor and model utilized on your ReadyNAS system. It is best to replace a failed disk with the same disk model. Contact the disk vendor and arrange to have the disk replaced if the disk is still under warranty. Disk RMA from the vendor will require that you provide the serial number of the disk, so you will need to open the case and take out the failed disk to get this info. See the next section on how to do this.

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

Replace the Failed Disk

Refer to the **Getting Started** guide for hardware-specific instructions on replacing a failed disk in your ReadyNAS system.

On the ReadyNAS 600/X6 system, shutdown the ReadyNAS and open up the enclosure as instructed in the **Getting Started** guide. If you view the disks from the front of the enclosure, the left-most disk is channel 1; the next disk is channel 2; and so on.

On the Rev A ReadyNAS 600/X6 system, remove the drive cage and disconnect the power and SATA cable from the failed disk. Insert the new replacement disk, reconnect the cables, insert the drive cage, and secure the enclosure.

Warning

When replacing the cables, make sure the connectors fit **square-on** and **securely**. After the drive cage is re-inserted, double-check the connectors to make sure they have not come loose. Loose connection may cause spurious drive failure events that may render the data volume inoperable.

On the Rev B ReadyNAS 600/X6 system, you can replace the failed disk in power off mode by removing the disk from the top and sliding the new disk in place.

On ReadyNAS systems with hot-swap drive bays, you do not need to power off the ReadyNAS to replace a failed disk. You can replace the disk while the system is on. After removing the failed disk, wait at least 10 seconds until the disk LED blinks, and then insert the new disk.

Re-synchronize the Volume

If you had to power-off to replace the failed disk, turn on the power on the ReadyNAS.

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 ReadyNAS 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.

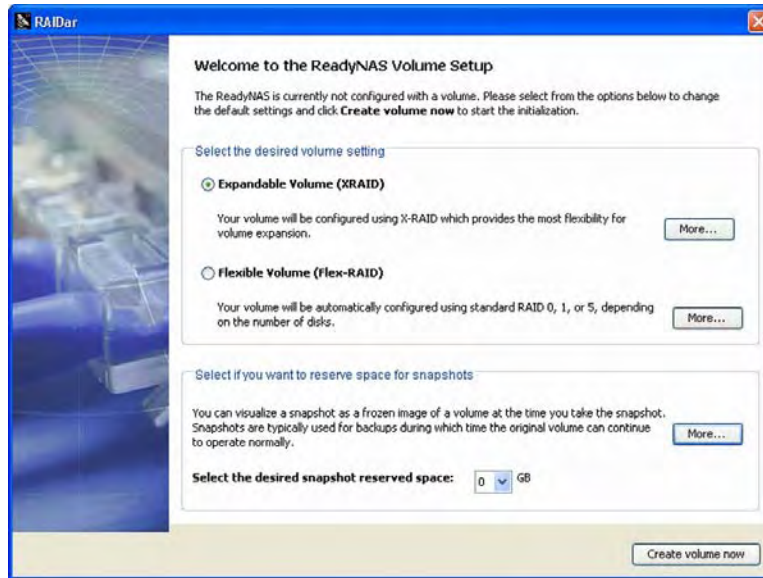
System Reset Switch

Refer to the **Getting Started** guide included in the shipping box for the location of the **System Reset** switch on the back of the ReadyNAS.

The System Reset switch allows you to perform three functions: (1) re-install the ReadyNAS firmware, (2) reset the ReadyNAS 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 ReadyNAS firmware as a first step, if the ReadyNAS had been working normally but a configuration change makes it inaccessible. If this does not work and/or you wish to set the ReadyNAS back to a factory default state, you can do so following the instructions below:

- **To re-install the ReadyNAS 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 ReadyNAS, **but make sure not to press the reset switch for too long, otherwise a destructive Factory Default process will be done instead** (see below).
- **To set the ReadyNAS 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 all disk configurations, **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 ReadyNAS 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.



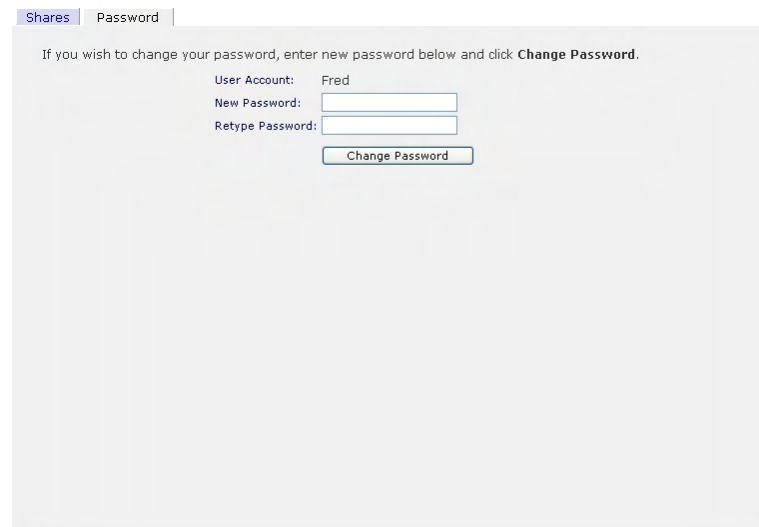
Select the desired mode along with the desired snapshot size and click **Create volume now**. The ReadyNAS will proceed with a reboot to re-configure your volume to the desired specification.

For any of the above activities, please make sure to back up important data before starting.

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.



The screenshot shows a web interface with two tabs: "Shares" and "Password". The "Password" tab is active. Below the tabs, there is a message: "If you wish to change your password, enter new password below and click **Change Password**." Below this message, there are three input fields: "User Account:" with the value "Fred", "New Password:" with an empty text box, and "Retype Password:" with an empty text box. At the bottom of these fields is a button labeled "Change 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.



RAID Levels Simplified

RAID can be somewhat daunting, so without going into too much detail, 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.

Input Field Format

Domain/Workgroup Name

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

- Name must only 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.

Host

A valid IP address or a host name.

Host Name

A valid host name must conform to the following restrictions:

- Name must only consist 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.

ReadyNAS 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 only consist 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 only 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 32 characters or less.

User/Group Name

- Name must only consist 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).

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 will abuse 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: Infrant Technologies patent-pending Expandable RAID technology.

If You Need Help...

If you have questions or you encounter problems with the setup, you can visit our support site at <http://www.infrant.com>. There, you'll find links to FAQs, message board, and live online support. Infrant also has a lively community forum at <http://www.infrant.com/forum> which is often monitored by advanced users and Infrant support and engineering staff.