

READYNAS INSTANT STORAGE

# User Guide

---



Copyright © 2005, **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-04

# Contents

<b>About This Guide</b>	<b>7</b>
<b>1 FrontView Advanced Control</b>	<b>8</b>
<b>Clock</b>	<b>10</b>
System Time	10
NTP Option	10
<b>Network</b>	<b>11</b>
Ethernet	11
Wireless	12
DNS	13
WINS	13
DHCP	14
Route	15
<b>Security</b>	<b>16</b>
Share Mode	17
▶ Specify a Workgroup	17
User Mode	17
▶ Specify a Workgroup	18
▶ Setting up Accounts	18
▶ Managing Groups	18
▶ Managing Users	19
▶ Setting Accounts Defaults	21
Domain Mode	22
▶ Domain/ADS Authentication	22
<b>Shares</b>	<b>23</b>
Services	23
Adding Shares	24
Managing Shares	26
▶ Setting Share Access in Share Mode	27
▶ Setting Share Access in User and Domain Modes	27
▶ Recycle Bin	28

▶ Advanced Share Permission	29
Snapshot	30
▶ Taking and Scheduling Snapshot	31
Volume Management	33
▶ Advantages of ReadyNAS Models 600/1000	33
▶ Advantages of ReadyNAS X Series	34
Volume Management for ReadyNAS Models 600/1000	34
▶ Deleting a Volume	34
▶ Adding a Volume	35
▶ RAID Settings	36
Volume Management for ReadyNAS X Series	37
▶ X-RAID Redundancy Overhead	37
▶ X-RAID Has one data volume	37
▶ Adding a 2 <sup>nd</sup> DISK for Redundancy	37
▶ Adding a 3 <sup>rd</sup> and 4 <sup>th</sup> DISK for MORE Capacity	37
▶ Replacing All Your Disks for Even MORE Capacity	38
USB	38
▶ USB Storage	38
▶ USB Printers	40
<b>System</b>	<b>43</b>
Alerts	43
▶ Alerts Contacts	43
▶ Alerts Settings	43
▶ SNMP	44
▶ SMTP	45
Admin Password	46
Performance	47
▶ Adding a UPS for performance	48
Language	49
Updating ReadyNAS	50
▶ Remote Update	50
▶ Local Update	52
▶ Settings	52
▶ Factory Default	53
Shutdown	53
<b>Status</b>	<b>55</b>
Logs	55
Health	55
<b>Backup</b>	<b>56</b>
Adding a New Backup Job	56

▶ Step 1 – Select Backup Source	56
▶ Step 2 – Select Backup Destination	57
▶ Step 3 – Choose Backup Schedule	58
▶ Step 4 – Choose Backup Options	58
Viewing the Backup Schedule	58
Viewing the Backup Log	59
Editing a Backup Job	60
<b>2 Accessing Shares</b>	<b>61</b>
Windows	62
MAC OS X	63
MAC OS 9	66
Linux / UNIX	67
Web Browser	68
FTP	70
Rsync	71
Networked DVD Players and UPnP AV Media Adapters	72
<b>3 Replacing a Failed Disk</b>	<b>73</b>
Locate the Failed Disk	73
Order Replacement Disk	73
Replace the Failed Disk	74
Re-synchronize the Volume	74
<b>4 System Reset Switch</b>	<b>75</b>
<b>5 Changing User Passwords</b>	<b>76</b>
<b>A RAID Levels Simplified</b>	<b>77</b>
RAID Level 0	77
RAID Level 1	77
RAID Level 5	77
<b>B Input Field Format</b>	<b>78</b>
Domain/Workgroup Name	78
Host	78
Host Name	78
ReadyNAS Host Name	78
Host Expression	79
Share Name	79
Share Password	79
SNMP Community	79
User/Group Name	79
User Password	79

<b>C Glossary</b>	<b>80</b>
<b>D If You Need Help...</b>	<b>82</b>

## 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”.

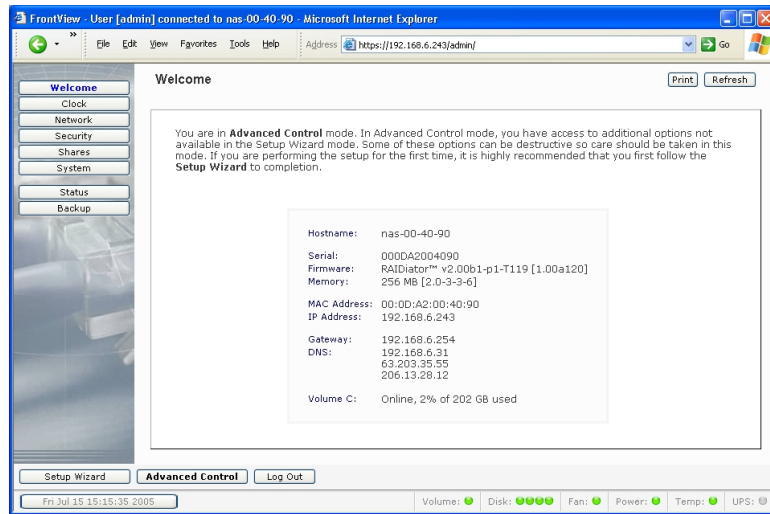
If you have questions on what constitutes a valid input for host name, workgroup, or password, [Appendix B](#), “Input Field Format”, describes these and more.

[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.



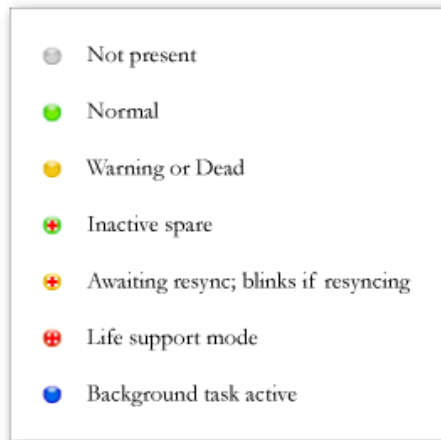
When you first switch to this mode, you'll notice the menus on the left that allow you to quickly jump to the desired menu page. Towards the bottom left, you'll notice buttons that allow you to switch back and forth between the Setup Wizard mode and the Advanced Control mode..

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 status represent:

- **Not present** – No disk or device attached.
- **Normal** – Device in normal operating mode.
- **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; blinks if re-syncing** – This disk is waiting to re-sync to the RAID volume. 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.
- **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.

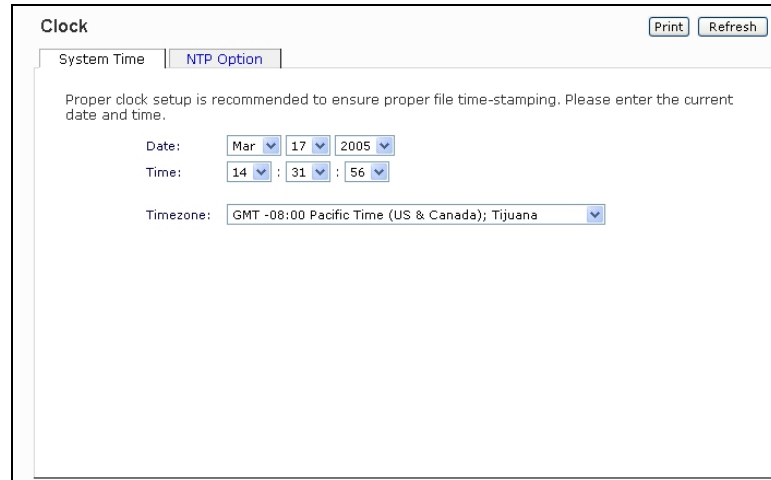
Move the mouse cursor over the LED to display more information on the device, or click on it to display the status in more detail.

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.

## Clock

### System Time

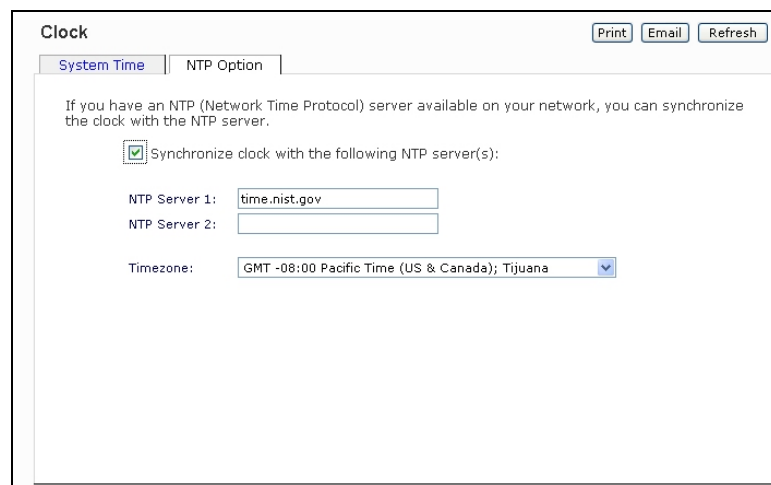
The System Time tab in the Clock page allows you to set the date, time, and time zone. Set appropriately to ensure files maintain proper timestamp.



The screenshot shows the 'Clock' page with the 'System Time' tab selected. The page title is 'Clock' and it includes 'Print' and 'Refresh' buttons. Below the tabs, there is a message: 'Proper clock setup is recommended to ensure proper file time-stamping. Please enter the current date and time.' The form contains three rows of input fields: 'Date' with dropdowns for 'Mar', '17', and '2005'; 'Time' with dropdowns for '14', '31', and '56'; and 'Timezone' with a dropdown menu showing 'GMT -08:00 Pacific Time (US & Canada); Tijuana'.

### NTP Option

You can elect to synchronize the system time on the device with a remote NTP (Network Time Protocol) server. Click on the **NTP Options** tab to designate the host name or IP address of the NTP server. You can elect to keep the default server or enter a NTP server closer to your locale. Available public NTP servers can be found by searching the web.

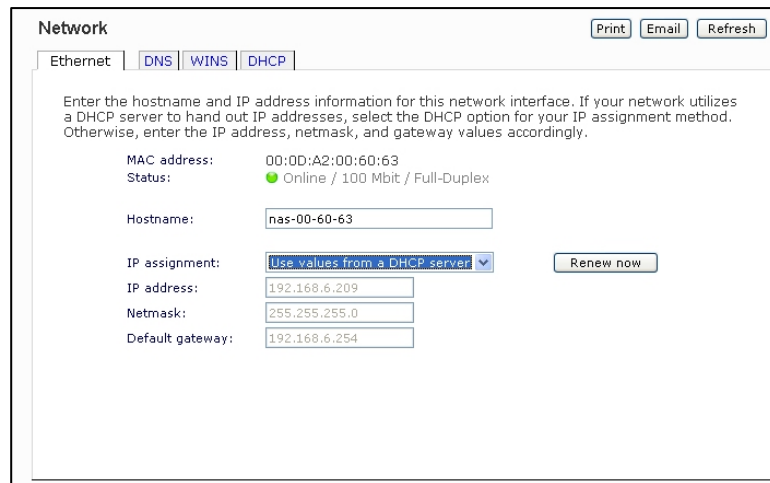


The screenshot shows the 'Clock' page with the 'NTP Option' tab selected. The page title is 'Clock' and it includes 'Print', 'Email', and 'Refresh' buttons. Below the tabs, there is a message: 'If you have an NTP (Network Time Protocol) server available on your network, you can synchronize the clock with the NTP server.' There is a checked checkbox labeled 'Synchronize clock with the following NTP server(s):'. Below this, there are two input fields for 'NTP Server 1' (containing 'time.nist.gov') and 'NTP Server 2' (empty). At the bottom, there is a 'Timezone' dropdown menu showing 'GMT -08:00 Pacific Time (US & Canada); Tijuana'.

## Network

### Ethernet

The Ethernet tab allows you to set the hostname, IP address, network mask, and default gateway for your ReadyNAS device. 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 three parameters.



The screenshot shows a web interface for configuring the Ethernet network. At the top, there are tabs for 'Ethernet', 'DNS', 'WINS', and 'DHCP'. The 'Ethernet' tab is selected. Below the tabs, there are buttons for 'Print', 'Email', and 'Refresh'. A text box contains instructions: 'Enter the hostname and IP address information for this network interface. If your network utilizes a DHCP server to hand out IP addresses, select the DHCP option for your IP assignment method. Otherwise, enter the IP address, netmask, and gateway values accordingly.'

MAC address: 00:0D:A2:00:60:63  
Status: ● Online / 100 Mbit / Full-Duplex

Hostname:

IP assignment:

IP address:

Netmask:

Default gateway:

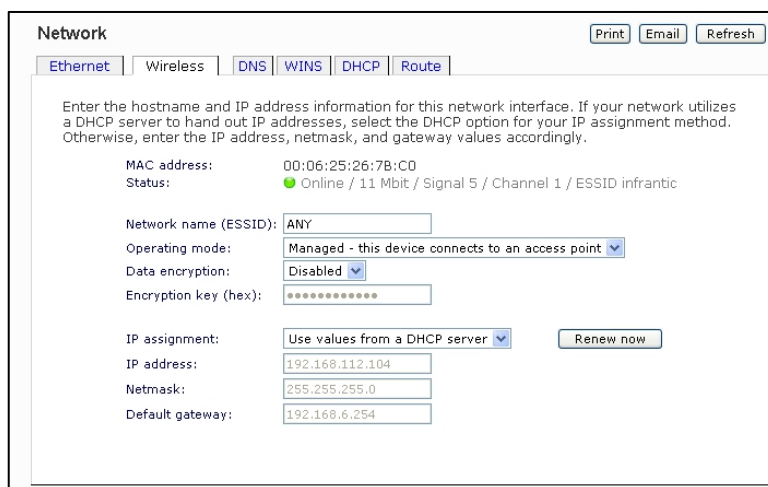
If you assign a static IP address, be aware that the browser will lose connection to the ReadyNAS device after the IP address has been changed. You can click Rescan in RAIDar to locate the device and reconnect from there.

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

## Wireless

There are a couple of ways in which you can use this NAS device over a wireless network. You can either connect the NAS to your wireless access point with a Cat-5 Ethernet cable, or you can connect a USB wireless adapter directly to the USB port on the NAS device.

The wireless network tab shows up in the Network menu when a supported USB wireless adapter is connected. 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 USB adapter.



**Network** Print Email Refresh

[Ethernet](#) | [Wireless](#) | [DNS](#) | [WINS](#) | [DHCP](#) | [Route](#)

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

MAC address: 00:06:25:26:7B:C0  
Status: ● Online / 11 Mbit / Signal 5 / Channel 1 / ESSID infrantic

Network name (ESSID):

Operating mode: Managed - this device connects to an access point ▼

Data encryption: Disabled ▼

Encryption key (hex):

IP assignment: Use values from a DHCP server ▼ Renew now

IP address:

Netmask:

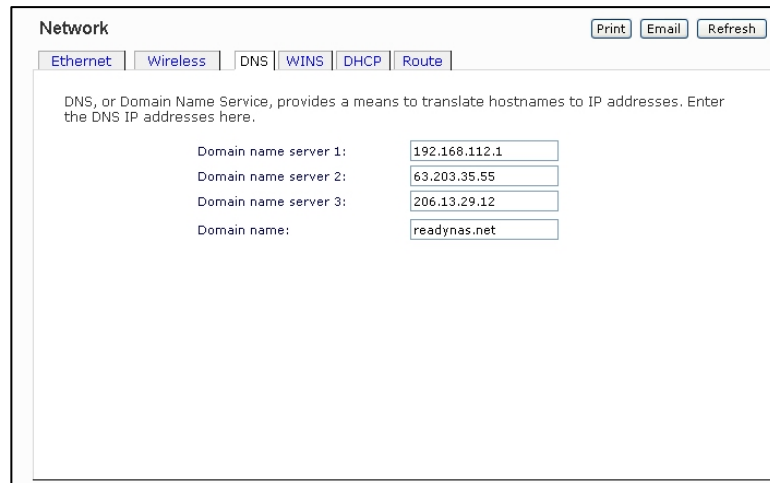
Default gateway:

### Note

Please note that support for USB 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.

## DNS

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

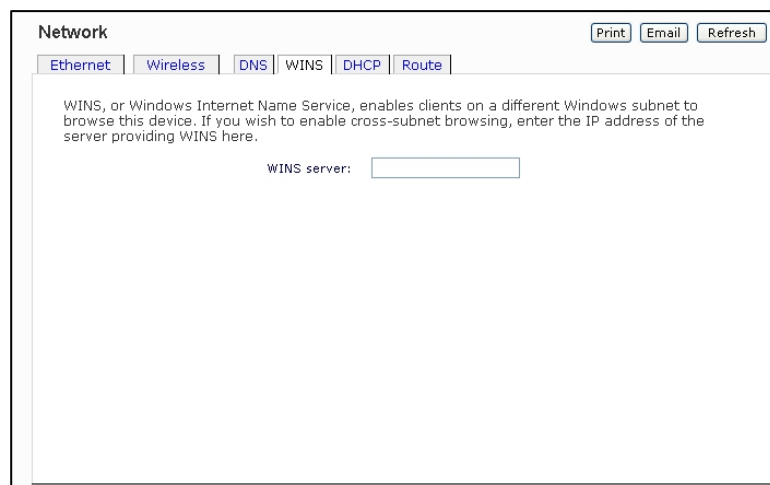


The screenshot shows the 'Network' configuration window with the 'DNS' tab selected. The window title is 'Network' and it has 'Print', 'Email', and 'Refresh' buttons. The 'DNS' tab is active, and the 'WINS' tab is also visible. The text reads: 'DNS, or Domain Name Service, provides a means to translate hostnames to IP addresses. Enter the DNS IP addresses here.' Below this, there are four input fields: 'Domain name server 1:' with the value '192.168.112.1', 'Domain name server 2:' with '63.203.35.55', 'Domain name server 3:' with '206.13.29.12', and 'Domain name:' with 'readynas.net'.

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

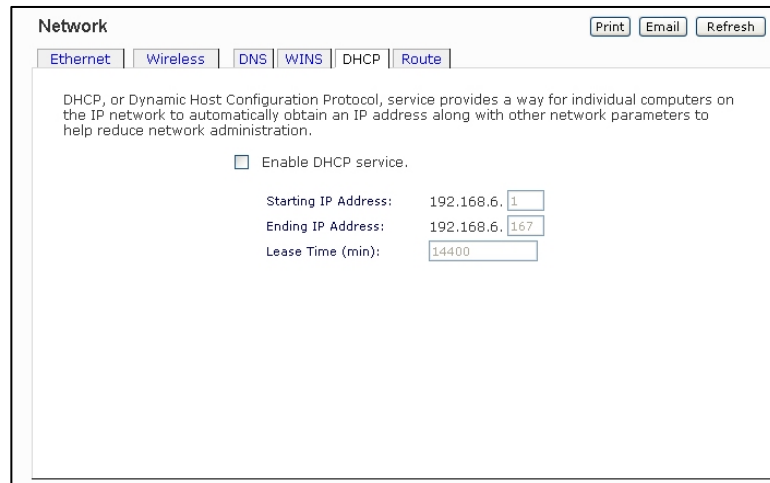
The WINS tab allows you to specify the IP address of the WINS (Windows Internet Naming Service) server. A WINS server is typically a Windows server on the network that will allow the ReadyNAS to be (Windows) browsable from other subnets. Leave this blank if you are unsure.



The screenshot shows the 'Network' configuration window with the 'WINS' tab selected. The window title is 'Network' and it has 'Print', 'Email', and 'Refresh' buttons. The 'WINS' tab is active, and the 'DNS' tab is also visible. The text reads: '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.' Below this, there is a single input field labeled 'WINS server:' which is currently empty.

## 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.



The screenshot shows a web interface for network configuration. At the top, there's a 'Network' title and three buttons: 'Print', 'Email', and 'Refresh'. Below the title is a navigation bar with tabs: 'Ethernet', 'Wireless', 'DNS', 'WINS', 'DHCP', and 'Route'. The 'DHCP' tab is selected. The main content area contains a paragraph explaining DHCP: '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.' Below this is a checkbox labeled 'Enable DHCP service.' which is currently unchecked. Underneath the checkbox are three input fields: 'Starting IP Address:' with the value '192.168.6.1', 'Ending IP Address:' with the value '192.168.6.167', and 'Lease Time (min):' with the value '14400'.

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.

Network configuration page, Route tab. The page title is "Network" and it includes "Print", "Email", and "Refresh" buttons. The "Route" tab is selected among other options like "Ethernet", "Wireless", "DNS", "WINS", and "DHCP".

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

Network	Netmask	Gateway	Interface
192.168.0.0	255.255.255.0	192.168.0.1	Ethernet

Buttons: "Add new route"

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

## Security

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.

**Security** Print Email Refresh

Windows | **Workgroup**

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

- Share.** Fit for home or small office. Select this option if you would like to restrict share access with the use of an optional share password. Each user accesses the shares on the device as a common guest user and will have the same read/write privilege as other users. This option supports setting disk quotas on a per-share basis.
- User.** Fit for medium-size office or workgroup. Select this option if you would like to control access to shares based on user or group accounts and your network does not utilize a domain controller for authentication. If you select this option, you will need to create a user account for anyone accessing this device. This option supports setting disk quotas on a per-user or per-group basis.
- 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 supports setting disk quotas on a per-user or per-group basis. Do not select this option otherwise or if you are unsure.

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

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

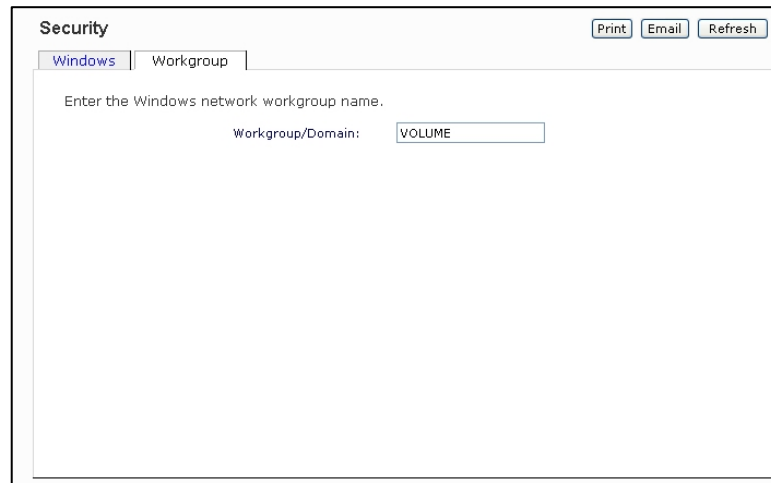


## Share Mode

The **Share security mode** is the easiest security option to set up. You only need to specify a workgroup if you wish to change it from the default.

### ► SPECIFY A WORKGROUP

To change the workgroup name, click on the **Workgroup** tab and enter a new name.



The screenshot shows a window titled "Security" with three tabs: "Windows", "Workgroup", and "Refresh". The "Workgroup" tab is selected. Below the tabs, there is a text prompt: "Enter the Windows network workgroup name." Below this prompt, there is a label "Workgroup/Domain:" followed by a text input field containing the word "VOLUME". In the top right corner of the window, there are three buttons: "Print", "Email", and "Refresh".

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.

## User 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 private share is accessible only by that user and the administrator who needs the privilege to perform backups of these private shares.

## Note

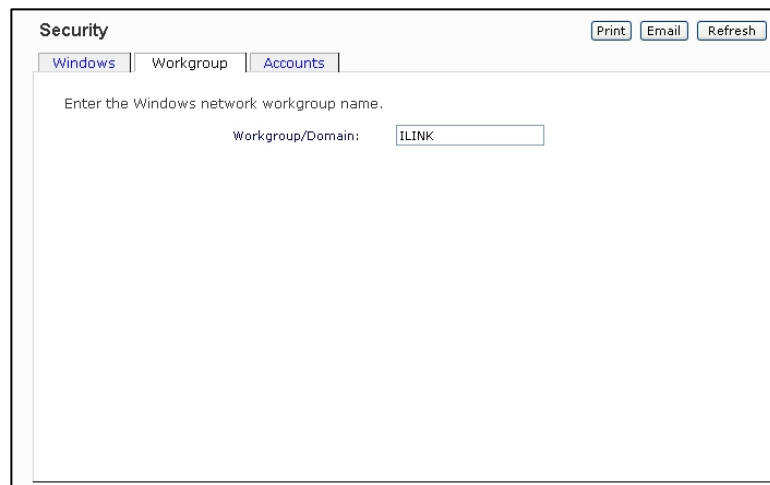
Private user shares are only accessible by users using CIFS (Windows) or AppleTalk file protocols.

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 specify a workgroup name, click on the Workgroup tab and enter the name. The name can be the workgroup name that is already used on your Windows network.



The screenshot shows a web interface titled "Security" with three tabs: "Windows", "Workgroup", and "Accounts". The "Workgroup" tab is selected. Below the tabs, there is a text input field labeled "Workgroup/Domain:" with the value "ILINK" entered. Above the input field, there is a prompt: "Enter the Windows network workgroup name." In the top right corner of the page, there are three buttons: "Print", "Email", and "Refresh".

### ► SETTING UP ACCOUNTS

In this security mode, the Accounts tab is available where you can manage user and group accounts on the ReadyNAS device. 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.

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.

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
engr		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.

The current security mode requires user and group accounts for share access.

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

Name	GID	Disk Used	Quota (MB)	Delete
accounting	101	0 MB	1000	<input type="checkbox"/>
engr	103	0 MB	2000	<input type="checkbox"/>
general	104	0 MB	2000	<input type="checkbox"/>
marketing	102	0 MB	1000	<input type="checkbox"/>
users	100	0 MB	0	<input type="checkbox"/>

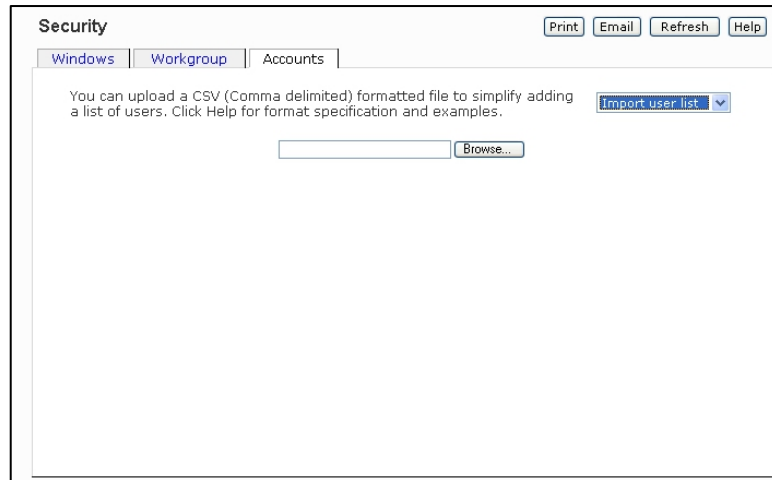
### ► MANAGING USERS

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.
- Password must be 1 to 8 characters in length.
- 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
```

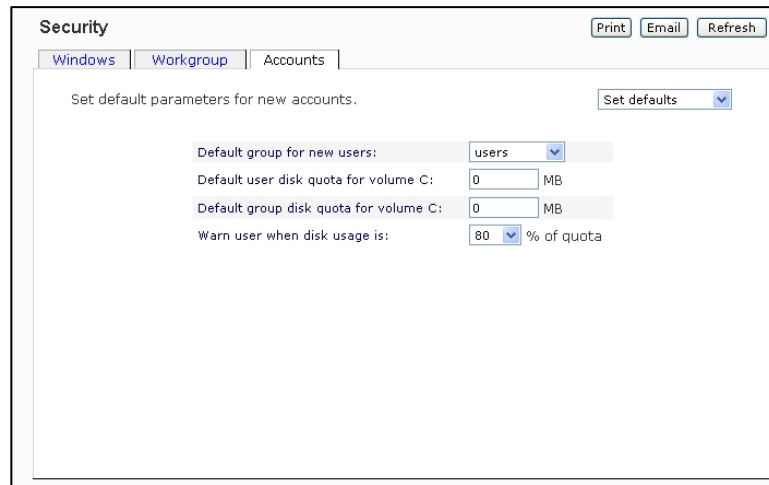
In this example, user **barney** will have password set to *23stone*, belongs to the default group, will be sent email notification to *barney@bedrock.com*, automatic UID assigned, and default quota.

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

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

► **SETTING ACCOUNTS DEFAULTS**

You can set account defaults by selecting the Set defaults option in the drop-down box. Here you can set up a default group for new users, a default user disk quota, and a default warning point when email alerts should be sent to users approaching quota limits. If multiple volumes are configured, you can select on which volume the user private home share will be located.

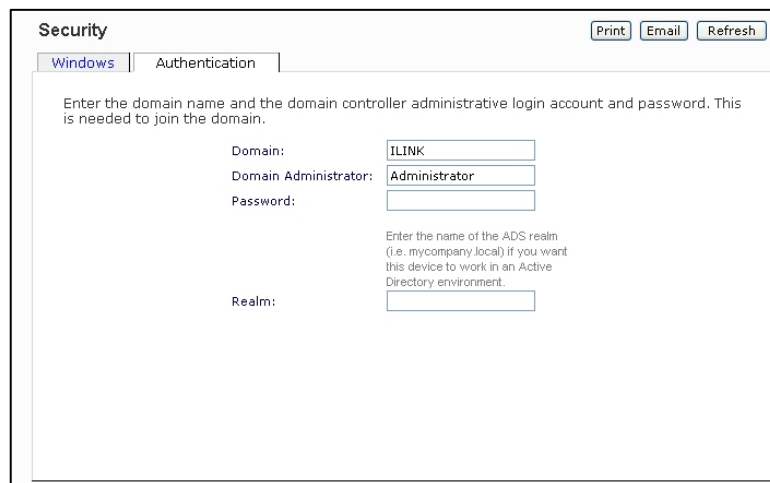


## Domain Mode

### ► 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 the 'Security' configuration page with the 'Authentication' tab selected. The page contains the following fields and instructions:

- Domain:** ILINK
- Domain Administrator:** Administrator
- Password:** (empty field)
- Realm:** (empty field)

Instructions on the page include: 'Enter the domain name and the domain controller administrative login account and password. This is needed to join the domain.' and 'Enter the name of the ADS realm (i.e. mycompany.local) if you want this device to work in an Active Directory environment.'

Enter these items in the Authentication tab and click Apply. If successful, the ReadyNAS device will have joined the domain and all users and groups from the domain will have login access to the shares on this device.

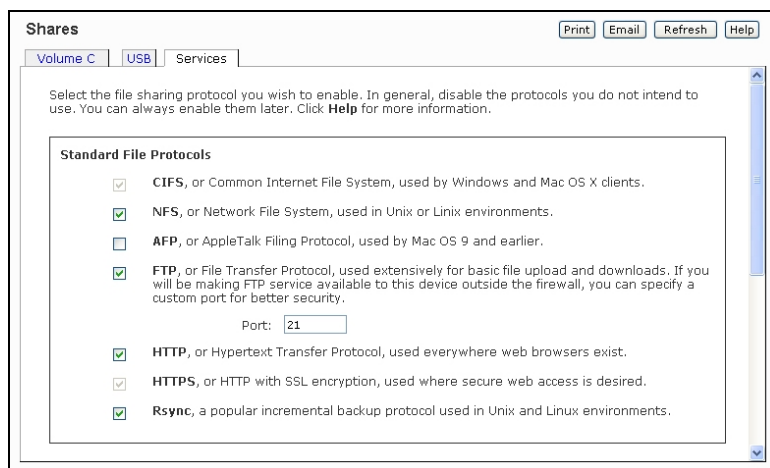
## Shares

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.

## Services

The Services tab allows you to manage the file protocols for share access. This in effect controls the type of clients you wish to enable share access.

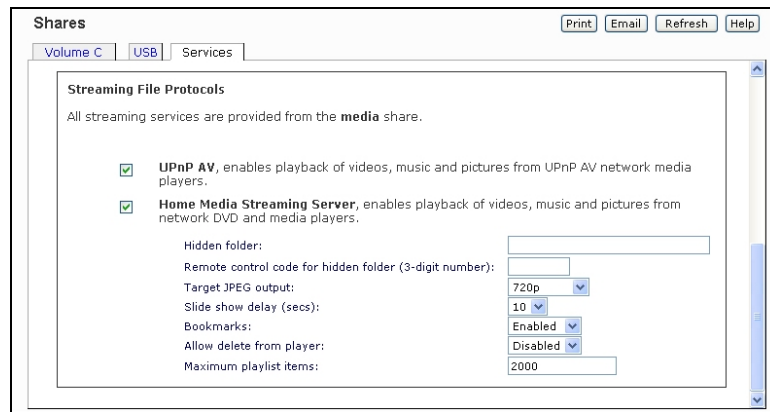


At the top are the file protocols, a bunch of daunting acronyms if you are not familiar with them, but we'll try to explain them here:

- **CIFS**, or Common Internet File Service. This protocol is used by Microsoft Windows and 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.
- **AFP**, or AppleTalk File Protocol. Mac OS 9 uses this protocol. Mac OS X supports this but it now defaults to using CIFS.
- **FTP**, or File Transfer Protocol. Widely used in public file upload and download sites. ReadyNAS supports anonymous or user access for FTP clients, depending on the security mode selected. If you wish, you can elect to set up port-forwarding to a non-standard port 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.

- **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.
- **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.

Next are Streaming File Protocols, a list of built-in streaming servers available straight from the ReadyNAS to serve the growing number of network media players without ever having to turn on your PC or Mac.



- **UPnP AV**, a standard streaming server allowing compatibility with stand-alone networked home media adapters and some networked DVD players. 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.
- **Home Media Streaming Server**, a service used to stream videos, music, and pictures to popular networked DVD players. Similar to UPnP AV, this service is used to stream videos, music, and pictures from the reserved *media* share to these adapters.

## 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.



**Shares** Print Email Refresh Help

Volume C USB Services

Disk space: 32 MB of 202 GB used (0%)  
Additional 10 GB reserved for snapshots

Share List Add Share Snapshot RAID Settings

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

Share Name	Description	Password (optional)	Disk Quota
Brochure	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.

**Shares** Print Email Refresh Help

Volume C USB Services

Disk space: 32 MB of 202 GB used (0%)  
Additional 10 GB reserved for snapshots

Share List Add Share Snapshot RAID Settings

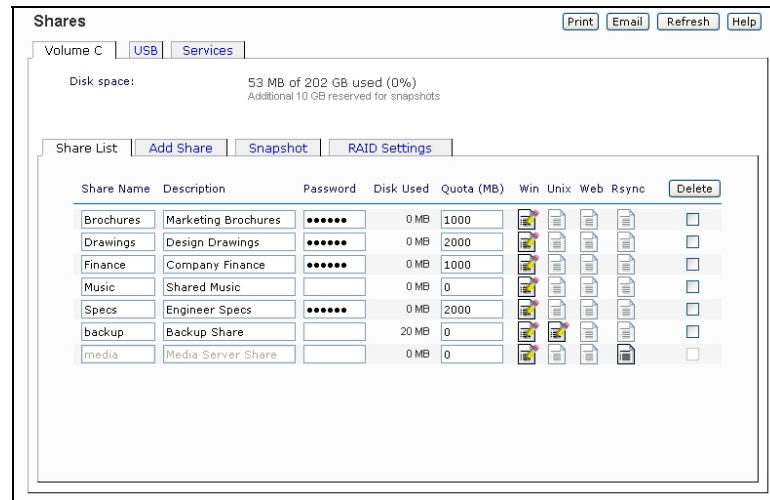
Enter the share names and descriptions you wish to add.

Share Name	Description
Brochure	Marketing Brochure
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.

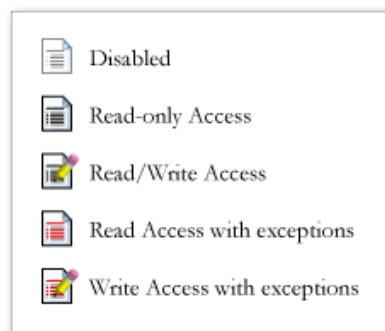
## Managing Shares

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

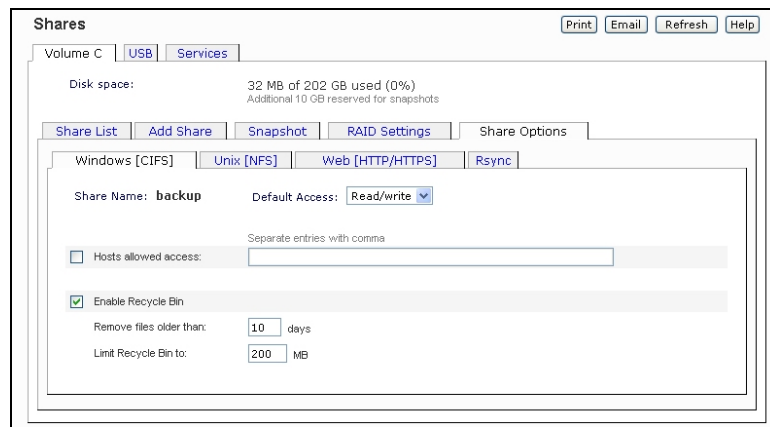
that are granted read/write permission, or (3) access is disabled except for one or more users or groups that are granted read-only privilege.

- **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 specify the host(s) that you wish to allow. 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:

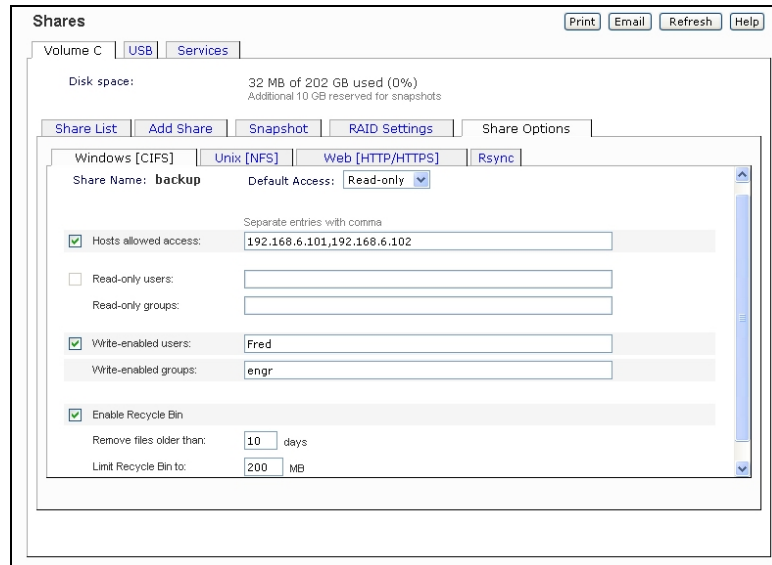
```
192.168.2., 192.168.2.0/255.255.255.0, 192.168.2.0/24
```

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 **Enable Recycle Bin** option. Refer to the Recycle Bin following the next section for information on this feature.

#### ► **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):



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
```

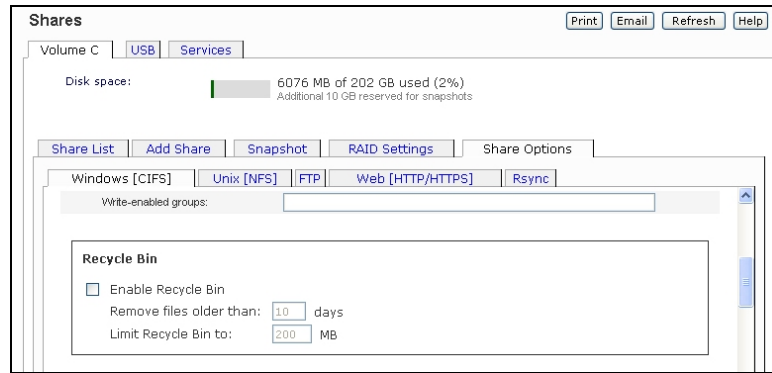
If you wish to specify some users and groups for read-only access and some for read/write access, and disallow all other users and groups, enter the following:

```
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
```

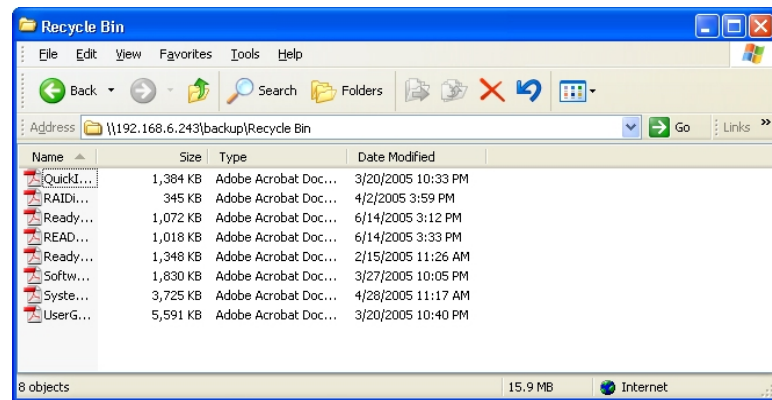
Note that access control will differ slightly from service to service.

#### ► 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.



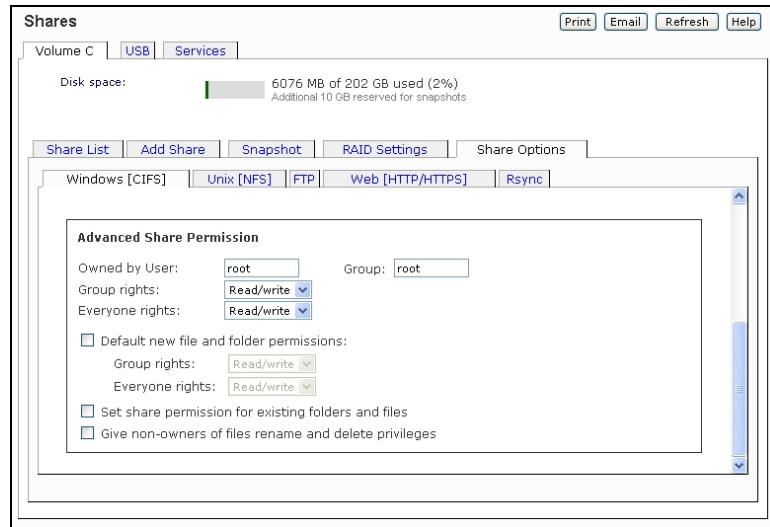
When enabled, whenever you delete a file, the file gets inserted into the Recycle Bin folder in the Share rather than being permanently deleted. This allows for a grace period where users can restore deleted files.



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 SHARE PERMISSION**

In the Advanced Share Permission box, you can change the ownership and permissions of the share base directory along with specify default permission of files and directories that are created in the share.



The **Owned by User** and **Group** fields specifies the ownership of the share directory. The **Group rights** field specifies the permission that the group owner has. This can be Read/Write, Read-only, or Disabled. Likewise, **Everyone rights** specify the permission of other users.

The **Default new file and folder permissions** allow you to set up default permission granted for newly created files and folders. This can be useful where you may want to increase or decrease security based on whether you can trust the users accessing and modifying files in the share. For instance, if you set Group and Everyone rights to Read-only, only the creator of the file will have modify privileges. In a more trusted environment, you can set up Group rights and maybe Everyone rights to Read-only.

The **Set share permission for existing folders and files** option is a one-shot method of changing the permission of all files and folders in the share to that of the share owner specified above. This can be useful in cases where you may have changed the security level and find that users no longer have access to files they had before due to permission problems.

The **Give non-owners of files rename and delete privileges** relaxes the security to allow users the capability to rename and delete files not belonging to them. Consider the security implication before enabling this option.

## 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

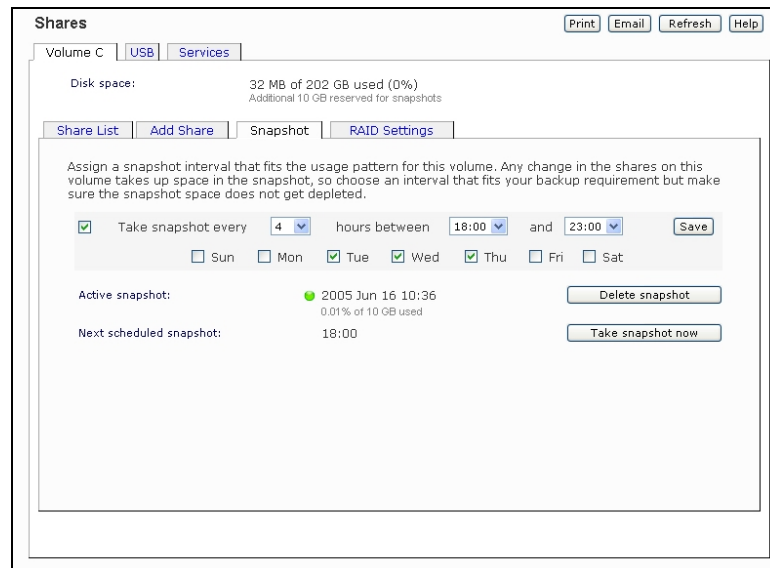
If you do not see a Snapshot tab within your volume tab, you did not reserve any space for snapshots when you added the volume. The ReadyNAS ships with a snapshot reserved space of 5% for volume C.

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.

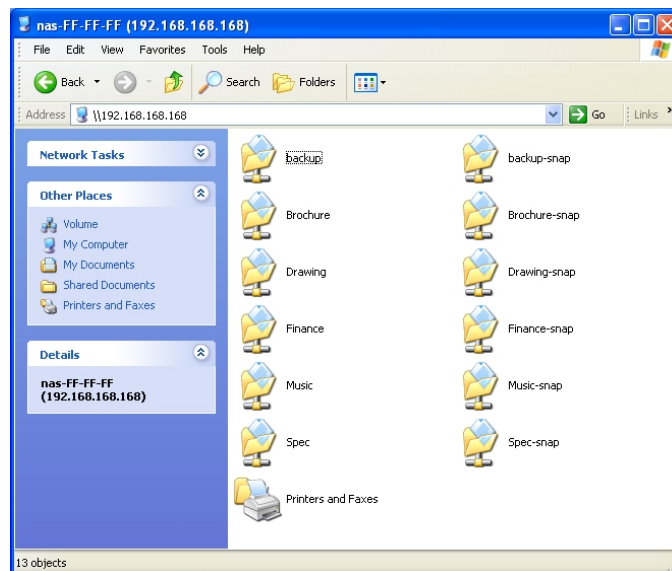
Specify the frequency and the days that you wish to schedule a snapshot. A start and end-time of 00:00 will take one snapshot at midnight. A start time of 00:00 and end-time of 23:00 will take snapshots between midnight and 11pm the next day at the interval you specify. Once you save the snapshot schedule,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

The screenshot shows the 'Shares' management interface for 'Volume C'. At the top, there are tabs for 'USB' and 'Services'. Below the tabs, the 'Disk space' section shows '32 MB of 202 GB used (0%)' and 'Additional 10 GB reserved for snapshots'. The 'Snapshot' tab is selected, and it contains a 'Share List', 'Add Share', 'Snapshot', and 'RAID Settings' sub-tabs. A warning message states: 'Assign a snapshot interval that fits the usage pattern for this volume. Any change in the shares on this volume takes up space in the snapshot, so choose an interval that fits your backup requirement but make sure the snapshot space does not get depleted.' The configuration area includes a checked checkbox for 'Take snapshot every', a dropdown menu set to '4', the text 'hours between', a dropdown menu set to '18:00', the text 'and', a dropdown menu set to '23:00', and a 'Save' button. Below this, there are checkboxes for days of the week: Sun (unchecked), Mon (unchecked), Tue (checked), Wed (checked), Thu (checked), Fri (unchecked), and Sat (unchecked). At the bottom, it shows 'Next scheduled snapshot: 18:00' and a 'Take snapshot now' button. Utility buttons for 'Print', 'Email', 'Refresh', and 'Help' are located at the top right of the interface.

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



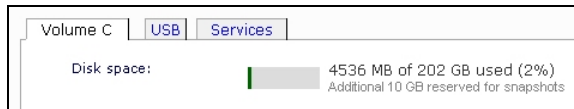
When a snapshot is taken, snapshots of shares appear in your browse list alongside the original shares, except the snapshot share names have *-snap* appended to the original share names. For example, a snapshot taken of share **backup** will be available as **backup-snap**.



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. If you are constantly getting this notification, you may want to either increase the frequency of the snapshot, or consider re-creating the volume with a larger snapshot reserved space. This is covered in the next section.

### 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 and any scheduled snapshots should be disabled.

## Volume Management

The ReadyNAS family consists of two RAID volume technologies. The ReadyNAS Models 600 and 1000 utilize the industry standard RAID levels 0, 1, and 5. The ReadyNAS X Series utilize the Infrant patent-pending X-RAID technology.

There are advantages to both technologies.

### ► ADVANTAGES OF READYNAS MODELS 600/1000

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.

- Multiple volumes are supported, each with a different RAID level, snapshot schedule and disk quota definition.
- 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 READYNAS X SERIES**

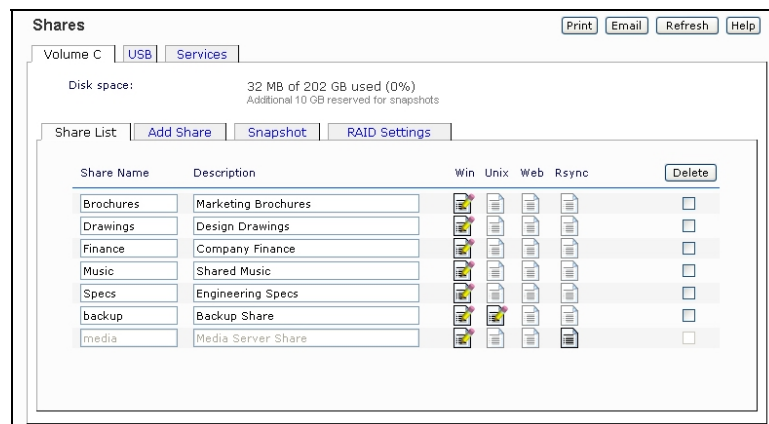
- One volume technology, but supports volume expansion, either by adding more disks or by replacing existing disk with larger capacity disks.
- You can start out with one disk, and add up to 3 more disks when you need them or can afford them.
- Volume management is automatic. Add a 2<sup>nd</sup> disk; it becomes a mirror to the 1<sup>st</sup>. Add a 3<sup>rd</sup>, your capacity doubles; add a 4<sup>th</sup>, 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 ReadyNAS Models 600/1000

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.

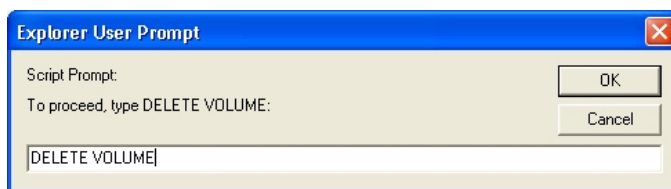
► **DELETING A VOLUME**

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!**



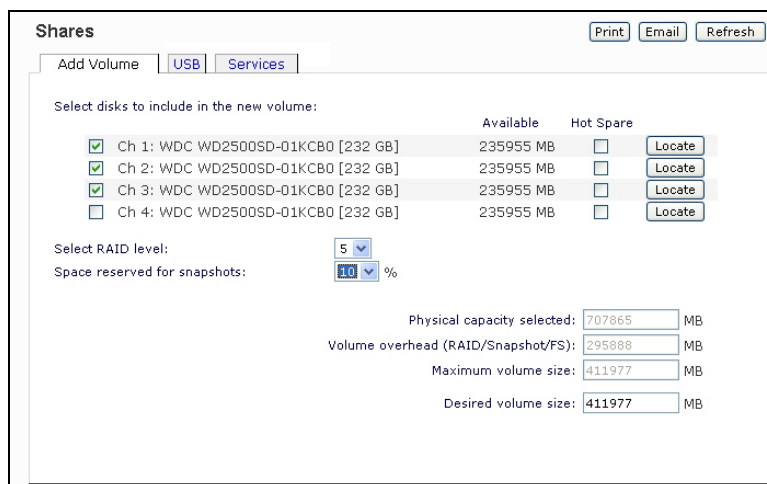
Click **Delete Volume** in the Volume C tab.

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.

The screenshot displays the RAID Settings for Volume C. At the top, there are buttons for 'Print', 'Email', 'Refresh', and 'Help'. Below this, the 'Volume C' tab is active, showing 'Add Volume', 'USB', and 'Services' sub-tabs. The 'Disk space' section indicates '0% of 408 GB used' and 'Additional 46 GB reserved for snapshots', with a 'Delete volume' button. The 'RAID Settings' tab is selected, showing 'Configuration: RAID Level 5, 3 disks' and 'Status: Redundant'. Under 'RAID Disks', three channels are listed: Ch 1, Ch 2, and Ch 3, each with '230 GB allocated' and 'Remove' and 'Locate' buttons. Under 'Available Disks', Ch 4 is listed with '230 GB free' and a 'Make hot spare' button.

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 ReadyNAS X Series**

The ReadyNAS with 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 any complexity. 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 2<sup>ND</sup> 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 3<sup>RD</sup> AND 4<sup>TH</sup> 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 3<sup>rd</sup> and perhaps 4<sup>th</sup> 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 2<sup>nd</sup> disk with another larger capacity disk, and boot. The process will be the same as the 1<sup>st</sup> disk. You will do this also for the 3<sup>rd</sup> and 4<sup>th</sup> disk.

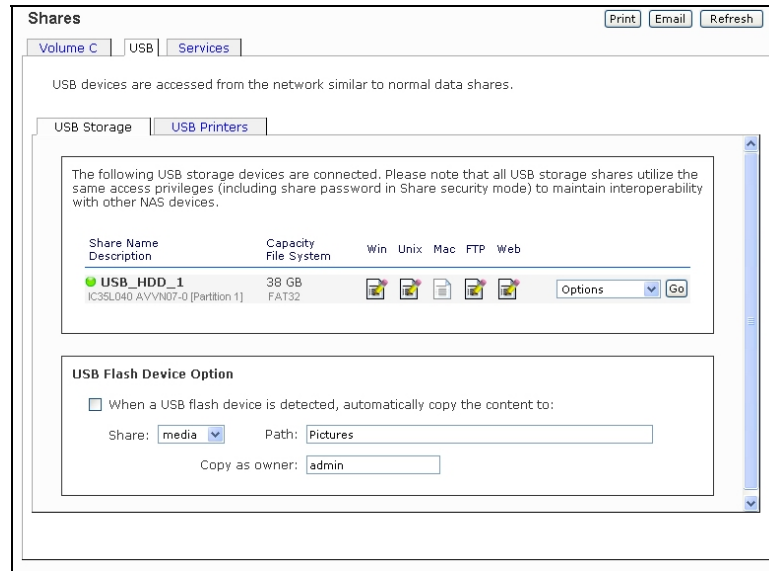
Once you get the completion notification for the 4<sup>th</sup> disk, reboot the ReadyNAS. During boot, volume capacity is expanded with the additional capacity from each disk. For instance, if you had replaced four 250GB disks with four 600GB disks, the capacity of the volume will increase by approximately 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.

## **USB**

USB storage and printer devices are accessed from the network as a normal data or print share. You can assign access restrictions and password-protect a USB storage share just as you would a normal data share, and access to the share is almost identical. The Print shares appear as remote printer devices to Windows and OS X users, and setting up to print on the printers connected to the ReadyNAS is as simple as setting up a network printer.

#### ► **USB STORAGE**

The USB Storage tab displays the USB disk and flash devices connected to the ReadyNAS, and offers various options for these devices. At the top, each partition of storage devices appear in a share list, similar to the way data shares are presented. The automatically generated share names, i.e. USB\_HDD\_1, USB\_HDD\_2, USB\_FLASH\_1, represents the type of device connected, and the partition number on that device.



When browsing for shares on the ReadyNAS, these USB device share names appear alongside the data shares and access to them are just the same.

Do note that only recognized partitions will be listed and available as a share. Partitions must be one of the following file system formats:

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

Identical to data shares, in Share security mode, you can optionally protect the USB share with a password. Advanced share restrictions, such as limiting share access to only particular hosts, is available by clicking on the access icons.

In non-Share mode, you can restrict access by clicking on the access icon and entering users or groups you wish to limit access to.

### 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.

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.
- 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 USB share entry, 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.

#### **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.

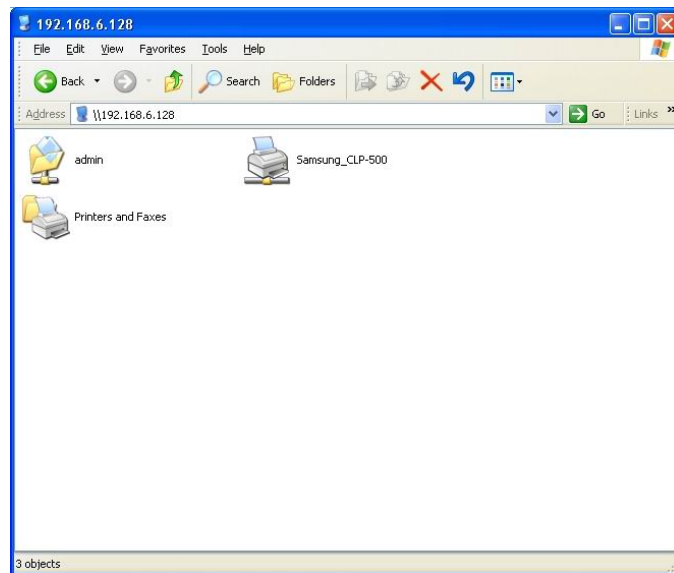
#### **► USB PRINTERS**

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 on the **USB Printers** tab or **Refresh** the page to display detected printers. The print share name will automatically reflect the manufacturer and model of your printer and will list in the USB Printers tab.





The 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.

### 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.

**Shares** Print Email Refresh

Volume C | USB | **Services**

USB devices are accessed from the network similar to normal data shares.

USB Storage | **USB Printers**

The following USB printers are connected. The printers appear as print shares to Windows and Mac users. If print jobs have been queued, job info will be displayed as well as an option to delete the print job(s) in queue.

Share Name	Job	Status	User	Size	Time	Delete Print Job
<b>Samsung_CLP-500</b>						
Samsung_CLP-5						
	1	Active	nobody	492142	16:33:49	<input checked="" type="checkbox"/>
	2	Queued	nobody	20933	16:34:43	<input type="checkbox"/>
	3	Queued	nobody	125980	16:35:12	<input type="checkbox"/>

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

## System

### 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 'System' configuration page with the 'Alerts' tab selected. The page title is 'System' and it includes 'Print', 'Email', and 'Refresh' buttons. The 'Alerts' tab is active, and the sub-tab 'Contacts' is selected. The main content area contains the following text: 'In the event of device or enclosure failure, quota violation, low disk space, and other system events requiring attention, email alerts will be sent.' Below this, there are sub-tabs for 'Contacts', 'Settings', 'SNMP', and 'SMTP'. The 'Contacts' sub-tab is active, and the text reads: 'Enter the alert contact email addresses where alert messages should be sent.' There are three input fields for 'Alert Contact 1', 'Alert Contact 2', and 'Alert Contact 3'. The first field contains 'mike@abcd.com', the second contains 'marry@abcd.com', and the third is empty. A 'Send Test Message' button is located to the right of the input fields.

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.

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 the **Power-off NAS when a disk fails or no longer responds** option. Enabling this option will cause the ReadyNAS to gracefully power off itself in the event that a disk failure or a disk remove event is detected.

#### ► 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.

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

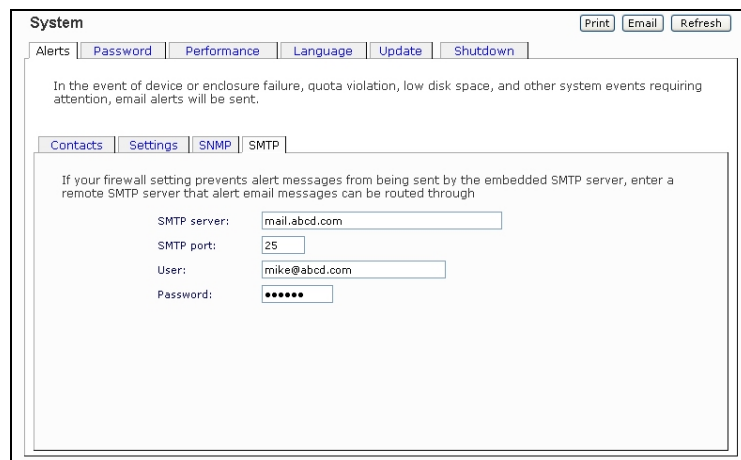
If you wish to limit SNMP access to only a secure list of hosts, please specify the hosts in the **Hosts allowed access** field.

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 a web interface for system configuration. At the top, there are tabs for Alerts, Password, Performance, Language, Update, and Shutdown. Below these tabs, there is a section for SMTP settings. The text reads: "If your firewall setting prevents alert messages from being sent by the embedded SMTP server, enter a remote SMTP server that alert email messages can be routed through". Below this text, there are four input fields: SMTP server (with the example value "mail.abcd.com"), SMTP port (with the example value "25"), User (with the example 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.

## Admin Password

The **Password** tab allows you to change the **admin** user password. 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 wipe out the data on the ReadyNAS.

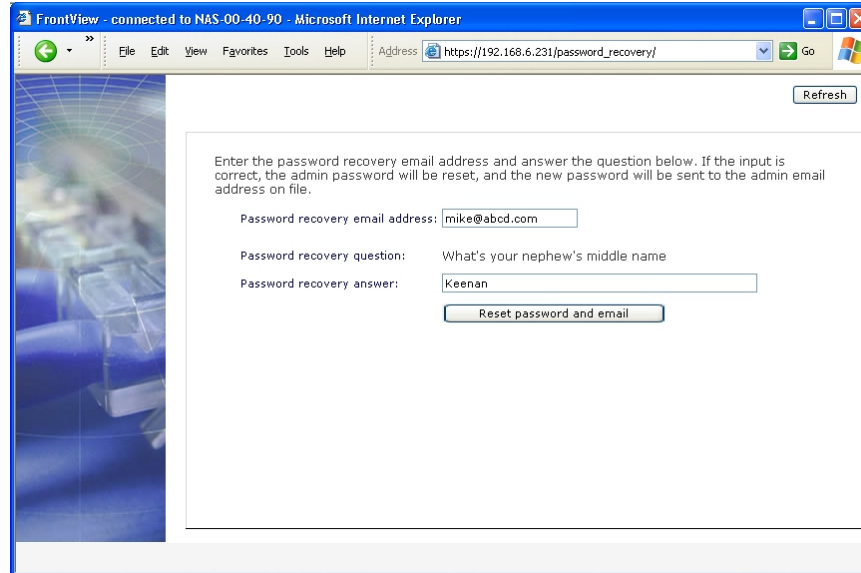


The screenshot shows the 'System' configuration page with the 'Password' tab selected. A 'Refresh' button is in the top right corner. Below the navigation tabs (Alerts, Password, Performance, Language, Update, Shutdown), there is a text block explaining the password change process: 'To change a password 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 this text are five input fields: 'New admin password:' (masked with dots), 'Retype admin password:' (masked with dots), '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'). A 'Change Password' button is located at the bottom of the form.

### Note

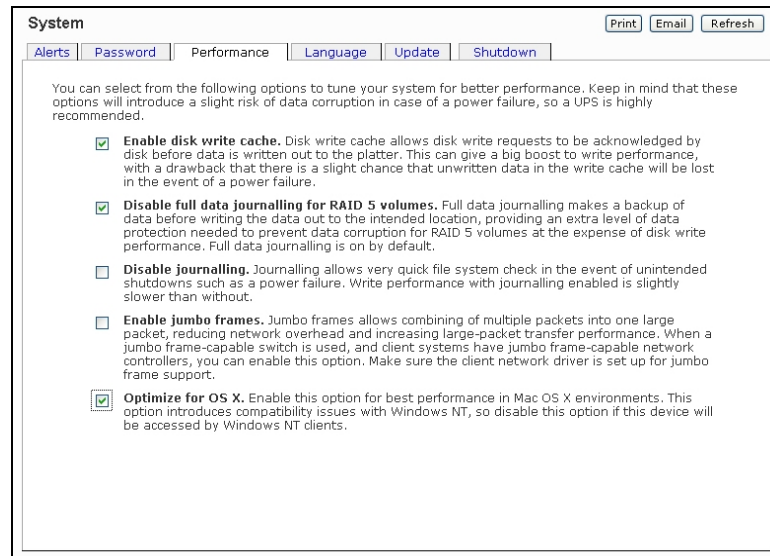
In User or Domain security mode, you can use the **admin** account to login to a Windows share, and perform maintenance on any file or folder in that share. The admin user also has permission to access all user private home shares to perform backups.

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



## 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 for RAID 5 volumes** 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 5 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 2<sup>nd</sup> 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 versus 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 **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.

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.

#### Warning

Whenever you enable or disable jumbo frames support, please make sure to do this when there is no activity to the ReadyNAS. The ReadyNAS supports a 9K frame size, so a switch capable of this frame size should also be used.

#### ► ADDING A UPS FOR PERFORMANCE

Adding a UPS to the NAS is an easy way to protect against power failures, but as mentioned in the **System Performance** section, a UPS can also safely allow for a more aggressive performance setting. Simply connect the NAS power cable to the UPS and connect the UPS USB monitoring cable between the UPS and the NAS<sup>1</sup>. The UPS will be detected automatically and will show up in

---

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



the Status bar. You can move the mouse pointer over the UPS LED icon to display the current UPS information and battery life.

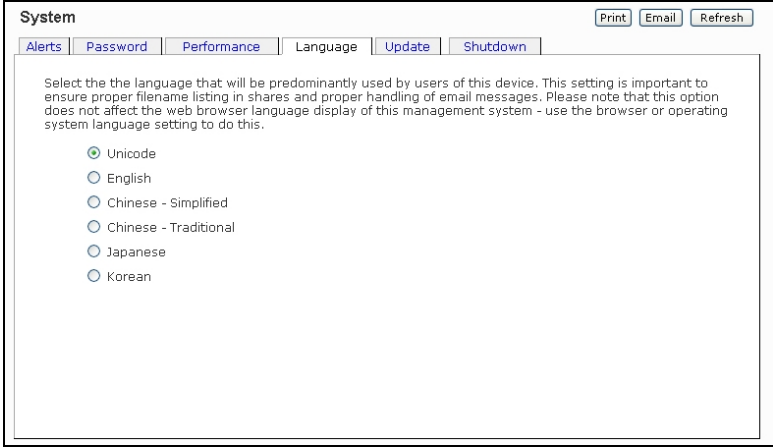


You will be notified by email whenever the status of the UPS changes, i.e. when a power failure forces the UPS to be in battery mode or when the battery is low. When the battery is low, the NAS device will automatically shutdown safely.

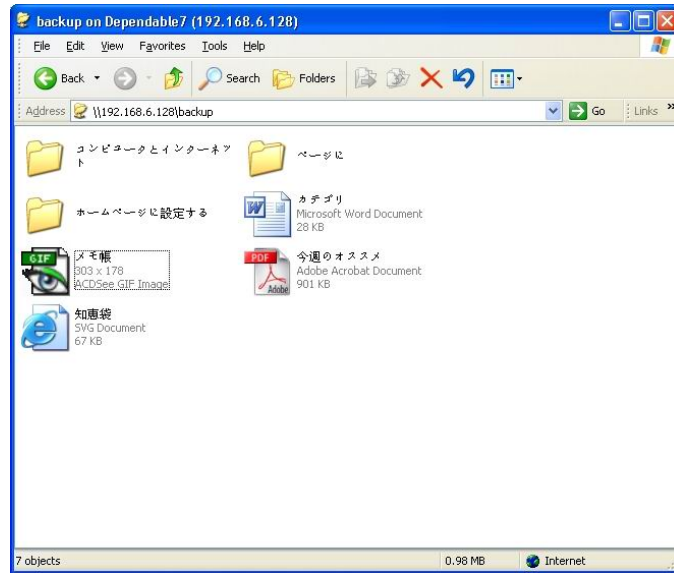
Make sure to adjust the optimization settings in the Performance tab if you wish to take advantage of the available options.

## Language

The **Language** tab offers the option of setting the ReadyNAS device to the appropriate character set for file names when files are shared with non-unicode supported operating systems.



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.

## Updating ReadyNAS

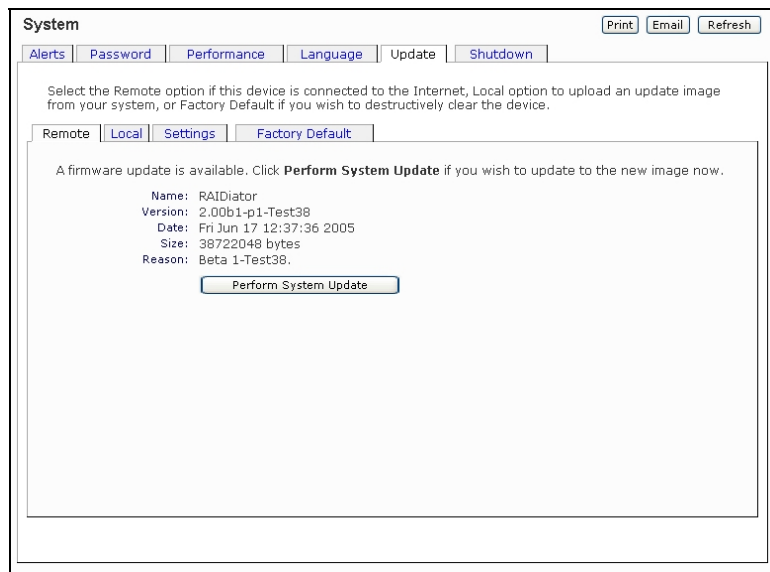
The ReadyNAS device offers the option of upgrading the operating firmware either automatically using the Remote Update option or manually loading an update image downloaded from the Infrant Support website.

### ► REMOTE UPDATE

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



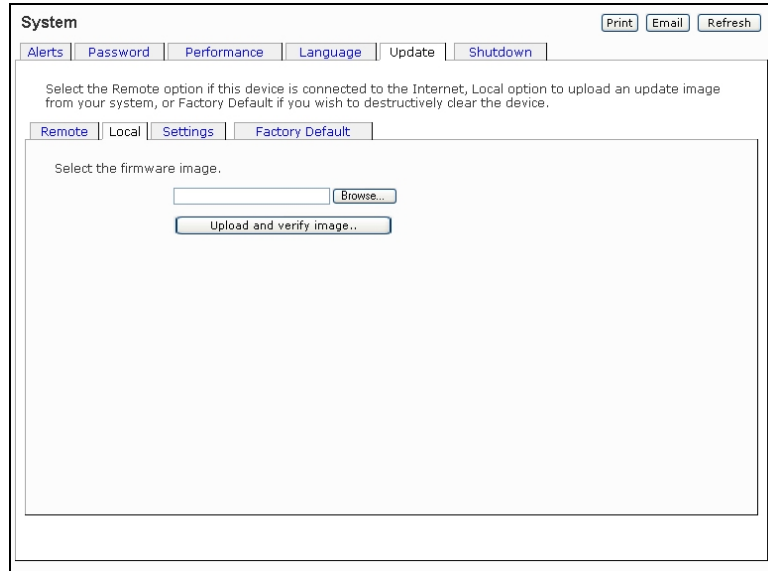
Simply click **Check for Update** to check for updates on the Infrant update server.



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.

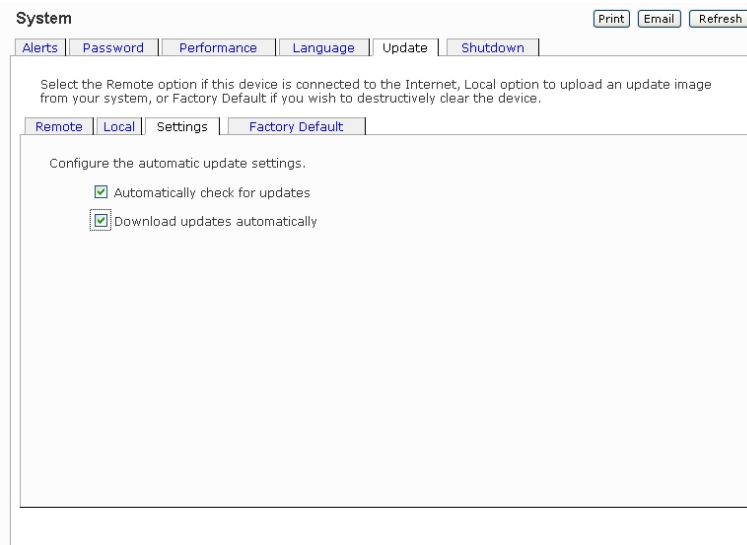


The screenshot shows the 'System' configuration page with the 'Update' tab selected. The 'Local' sub-tab is active. The page contains a text box with instructions: 'Select the Remote option if this device is connected to the Internet, Local option to upload an update image from your system, or Factory Default if you wish to destructively clear the device.' Below this, there are four tabs: 'Remote', 'Local', 'Settings', and 'Factory Default'. The 'Local' tab is selected. The main content area says 'Select the firmware image.' and features a 'Browse...' button next to a text input field, and an 'Upload and verify image..' button below it. At the top right of the page are 'Print', 'Email', and 'Refresh' buttons.

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.



The screenshot shows the 'System' configuration page with the 'Update' tab selected. The 'Settings' sub-tab is active. The page contains a text box with instructions: 'Select the Remote option if this device is connected to the Internet, Local option to upload an update image from your system, or Factory Default if you wish to destructively clear the device.' Below this, there are four tabs: 'Remote', 'Local', 'Settings', and 'Factory Default'. The 'Settings' tab is selected. The main content area says 'Configure the automatic update settings.' and features two checked checkboxes: 'Automatically check for updates' and 'Download updates automatically'. At the top right of the page are 'Print', 'Email', and 'Refresh' buttons.

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.

#### **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.

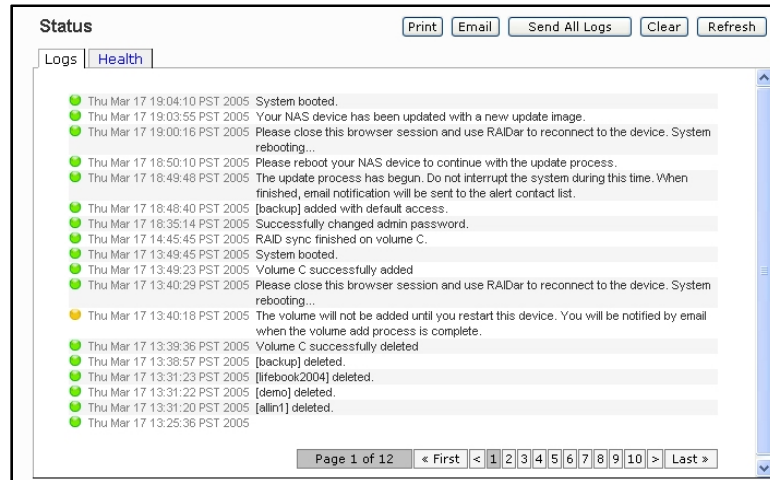
When you reboot or shutdown the ReadyNAS, you will need to close the browser window and use RAIDar to re-connect to FrontView.

## Status

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

### Logs

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

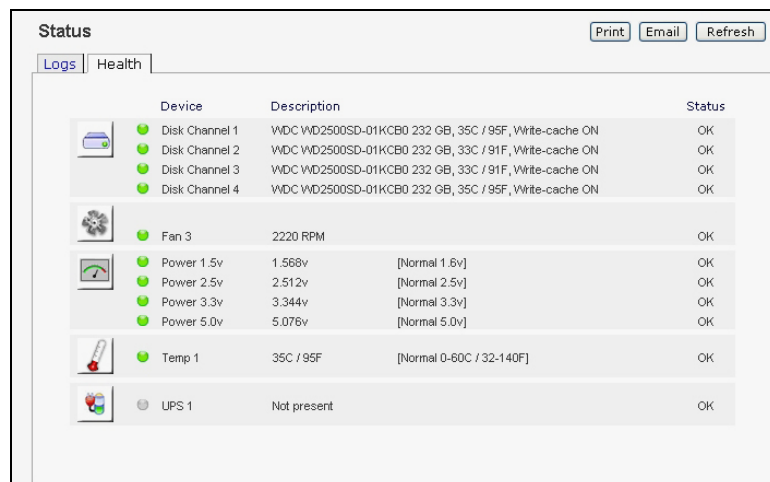


The screenshot shows the 'Status' page with the 'Logs' tab selected. At the top right, there are buttons for 'Print', 'Email', 'Send All Logs', 'Clear', and 'Refresh'. Below the tabs, a list of log entries is displayed, each with a green status icon, a timestamp, and a description. The entries include system booting, updates, password changes, RAID sync, volume management, and file deletions. At the bottom, there is a pagination control showing 'Page 1 of 12' and navigation buttons for 'First', '1', '2', '3', '4', '5', '6', '7', '8', '9', '10', and 'Last'.












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.

### Health

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



The screenshot shows the 'Status' page with the 'Health' tab selected. At the top right, there are buttons for 'Print', 'Email', and 'Refresh'. Below the tabs, a table displays system health metrics. The table has four columns: 'Device', 'Description', 'Status', and 'Status'. The rows include disk channels, fan speed, power supply voltages, temperature, and UPS status.

Device	Description	Status	Status
 Disk Channel 1	WDC WD2500SD-01KCB0 232 GB, 35C / 95F, Write-cache ON	OK	OK
 Disk Channel 2	WDC WD2500SD-01KCB0 232 GB, 33C / 91F, Write-cache ON	OK	OK
 Disk Channel 3	WDC WD2500SD-01KCB0 232 GB, 33C / 91F, Write-cache ON	OK	OK
 Disk Channel 4	WDC WD2500SD-01KCB0 232 GB, 35C / 95F, Write-cache ON	OK	OK
 Fan 3	2220 RPM	OK	OK
 Power 1.5v	1.568v [Normal 1.6v]	OK	OK
 Power 2.5v	2.512v [Normal 2.5v]	OK	OK
 Power 3.3v	3.344v [Normal 3.3v]	OK	OK
 Power 5.0v	5.076v [Normal 5.0v]	OK	OK
 Temp 1	35C / 95F [Normal 0-60C / 32-140F]	OK	OK
 UPS 1	Not present	OK	OK

## Backup

The **Backup** manager integrated with the ReadyNAS allows it 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 'Backup' configuration page with the 'Add a New Backup Job' tab selected. The interface is titled 'STEP 1 - Select backup source'. Below the title, there is a paragraph of instructions: '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 main sections for configuration. The first section has a dropdown menu labeled 'Select this NAS or remote' with a list of options: 'Select this NAS or remote', 'Remote: Windows/NAS', 'Remote: Website', 'Remote: FTP Site', 'Remote: NFS Server', 'Remote: Rsync Server', 'Share: USB\_HDD\_1', 'Share: backup', and 'Share: media'. To the right of this dropdown are input fields for 'Path:', 'Login:', and 'Password:', along with a 'Test connection' button. The second section is partially visible and also contains similar input fields and a 'Test connection' button.

#### ► STEP 1 - SELECT BACKUP SOURCE

The backup source can be located remotely or it can be a share 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** – select this if you wish to backup a share from a Windows PC or another ReadyNAS device.
- **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 share on the current 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 interface titled "Backup" with a navigation bar containing "Backup Schedule" and "Add a New Backup Job". There are utility buttons for "Print", "Email", "Refresh", and "Help".

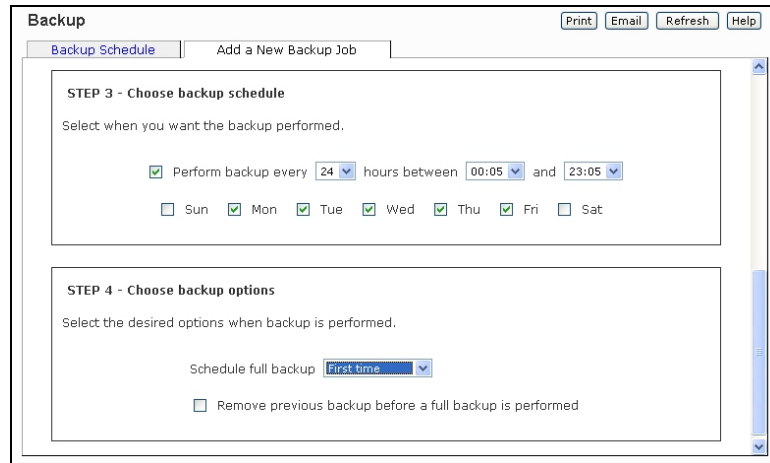
**STEP 1 - Select backup source**  
 Specify what you want to backup. The path you want to backup can be in a share on this device (a USB disk attached to this device will show up as a share) or located remotely. At least one of backup source or destination path must be local to this device.  
 Share: backup (dropdown) Path: [text field]  
 Login: [text field] Password: [text field]  
 Test connection button

**STEP 2 - Select backup destination**  
 Specify where you want your backup data saved. As with the backup source, the destination path can be a share on this device or a path on a remote PC or device.  
 Remote: Windows/NAS (dropdown) Path: //192.168.6.197/MyBackup [text field]  
 Login: admin [text field] Password: [masked text field]  
 Test connection button

The remote backup destination can be a Windows PC/ReadyNAS system, NFS server, or a Rsync server.

### ► 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 and perform backups on those snapshots.



The screenshot shows a web-based configuration window titled "Backup". At the top right, there are buttons for "Print", "Email", "Refresh", and "Help". Below the title bar, there are two tabs: "Backup Schedule" (which is active) and "Add a New Backup Job".

**STEP 3 - Choose backup schedule**  
Select when you want the backup performed.

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

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**STEP 4 - Choose backup options**  
Select the desired options when backup is performed.

Schedule full backup: First time

Remove previous backup before a full backup is performed

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.

### ► STEP 4 - CHOOSE BACKUP OPTIONS

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

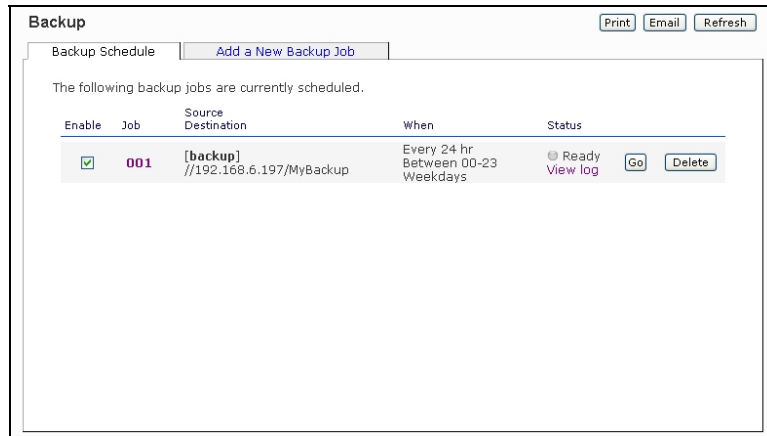
First, select when you want full backups to be performed. You can elect to do this just at the first time, every week, every two weeks, every three weeks, every four weeks, or every time this backup job is invoked. The first full backup is performed at the next scheduled occurrence of the backup depending 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 cycle.

Next, select if you want to erase the destination path contents before the backup is performed.

Before trusting that your backup will succeed, 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.



Here, you will see a summary of the backup jobs that have been scheduled. Jobs are numbered starting from 001.

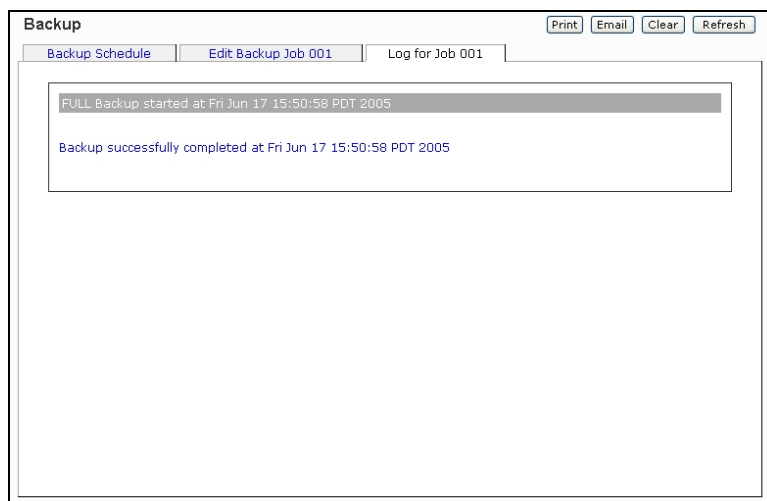
If you wish, you can enable or disable the job scheduling by clicking on the **Enable** checkbox. Disabling the job will not delete the job, but rather take it out of the automatic scheduling. If you wish to delete the job, click the **Delete** button.

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.

## 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

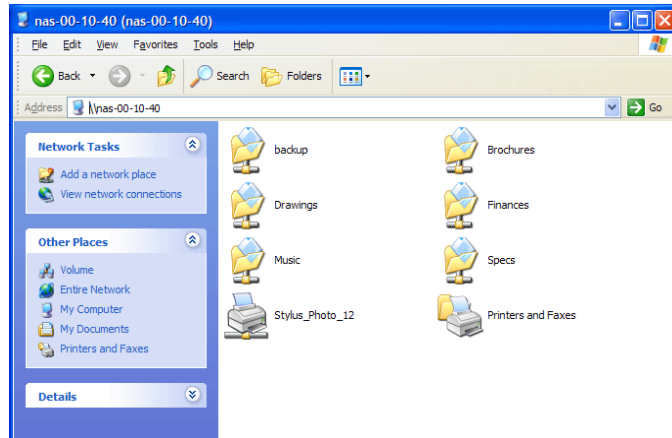
To edit a backup job, you can either click on the 3-digit **job number** in the Backup Schedule tab, or you can click on the **Edit Backup Job** tab while viewing that job's log. You can make appropriate changes or adjustments to the job there.

## Accessing Shares

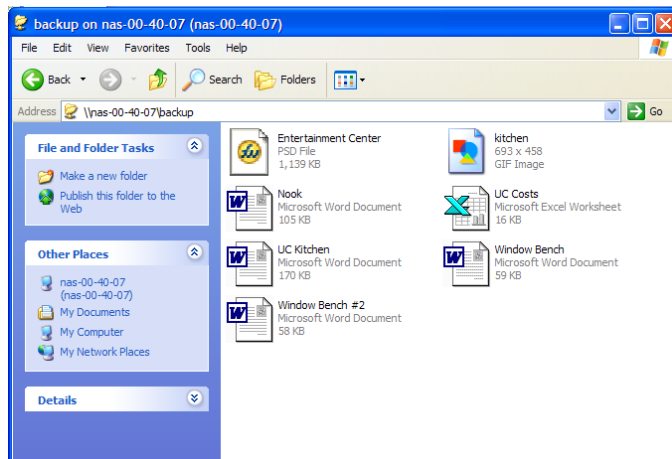
This chapter presents examples of how shares on the ReadyNAS device can be accessed by the various operating systems. If you have problems accessing your shares, make sure to enable the corresponding service in the **Shares Services** tab. Also make sure the default access of the share is set to **Read-only**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

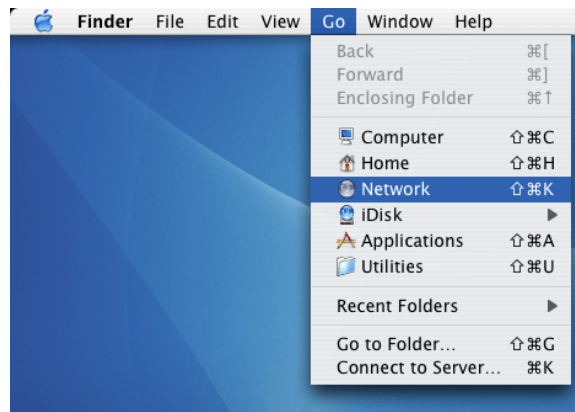


To access the share under Windows, specify the hostname followed by the share name in the Explorer address bar, i.e. `\\hostname\backup`, as follows:

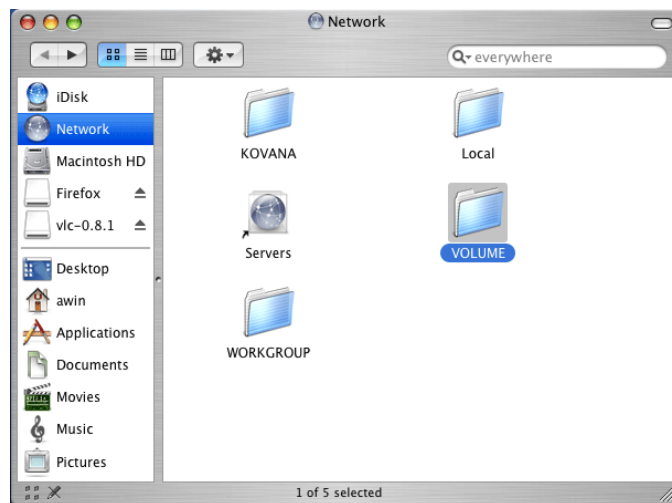


## MAC OS X

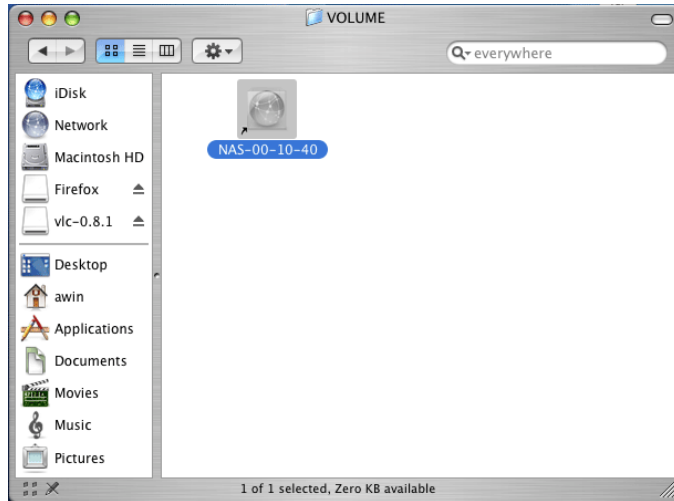
To access the same share under Mac OS X, select **Network** from the Finder **Go** menu.



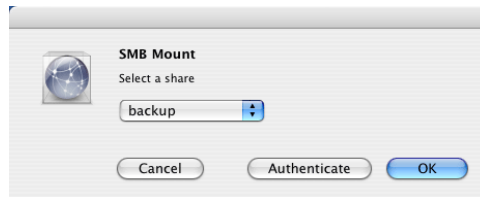
You will see a listing of available networks. The workgroup or domain name of the ReadyNAS system will appear in the listing. If you left the name unchanged, you should see **Volume**.



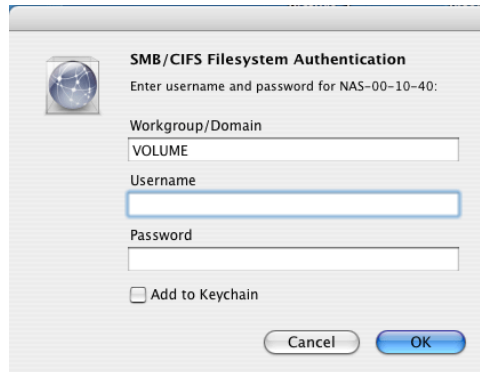
Double-click the workgroup or domain name icon to display the ReadyNAS host name.



Double-click on the host name icon to display the share listing.



Select the share you wish to connect to and click **OK** to get the login prompt.



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.



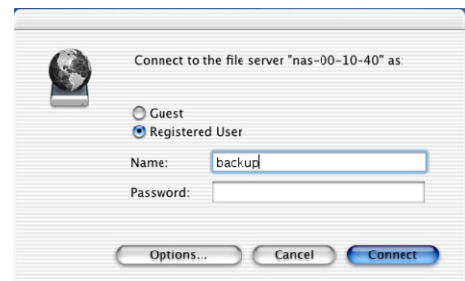
## MAC OS 9

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**.

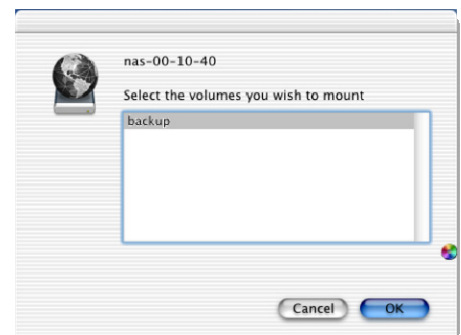


When you are prompted to login, enter the **share name** and **password** if the NAS is configured for **Share** security mode, or enter a valid user account and password otherwise.

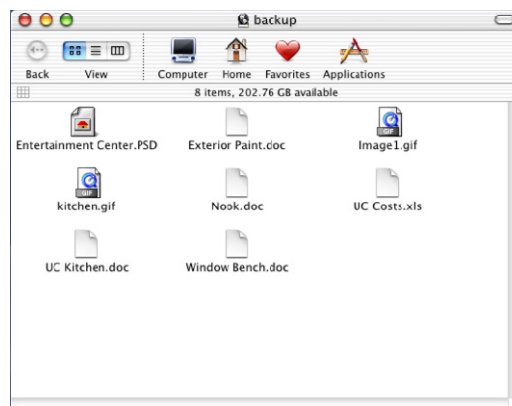
If no share password is set in **Share** mode, you can select **Guest** user and leave the password field blank.



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.

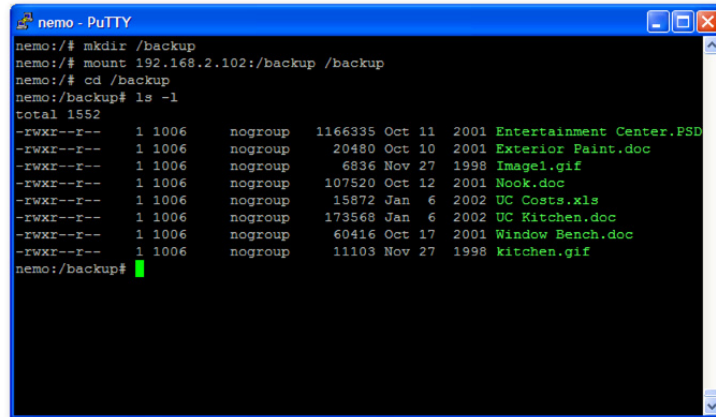


## Linux / UNIX

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.



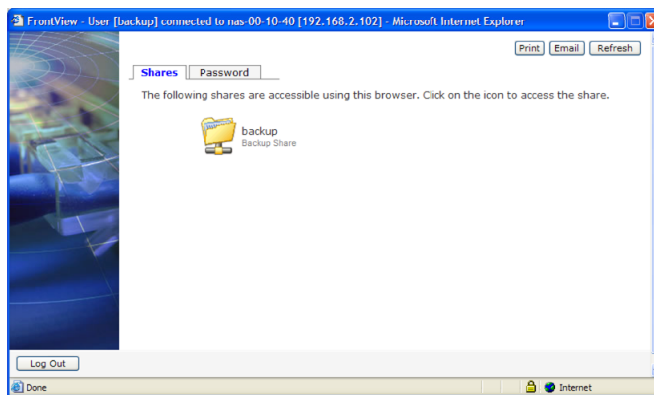
```
nemo - PuTTY
nemo:/$ mkdir /backup
nemo:/$ mount 192.168.2.102:/backup /backup
nemo:/$ cd /backup
nemo:/backup# ls -l
total 1552
-rwxr--r-- 1 1006 nogroup 1166335 Oct 11 2001 Entertainment.Center.PSD
-rwxr--r-- 1 1006 nogroup 20480 Oct 10 2001 Exterior.Paint.doc
-rwxr--r-- 1 1006 nogroup 6836 Nov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

## Web Browser

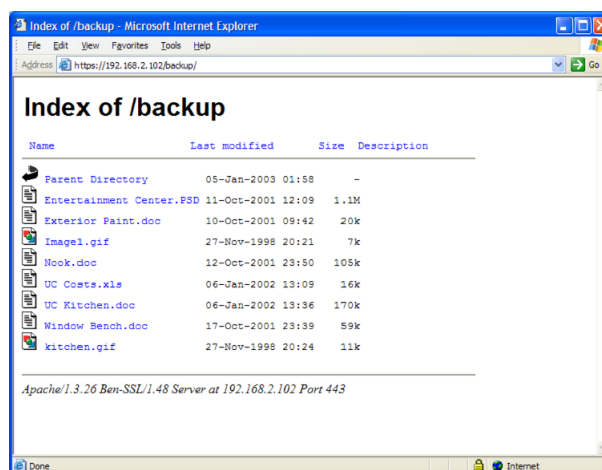
To access the same share using a web browser, enter <http://ipaddr> in the browser address bar. You can use **https** if you want a secure encrypted connection. You will be prompted to login.



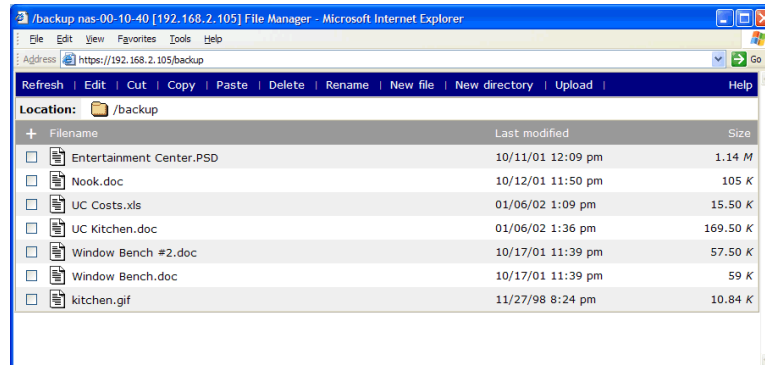
Enter the share name and share password if the ReadyNAS is in **Share** security mode. Otherwise, login with a valid user and password if the ReadyNAS is in **User** or **Domain** mode.



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.

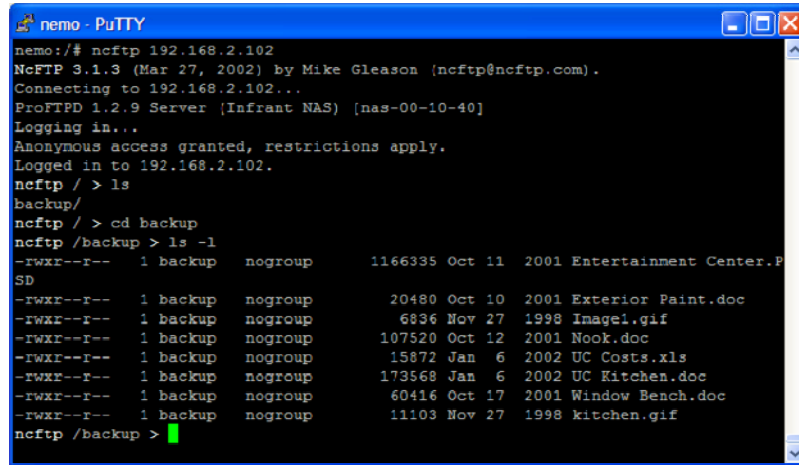
### Note

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

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 Image1.gif
-rwxr--r--  1 backup  nogroup    107520 Oct 12  2001 Nook.doc
-rwxr--r--  1 backup  nogroup     15872 Jan  6  2002 UC Costs.xls
-rwxr--r--  1 backup  nogroup    173568 Jan  6  2002 UC Kitchen.doc
-rwxr--r--  1 backup  nogroup     60416 Oct 17  2001 Window Bench.doc
-rwxr--r--  1 backup  nogroup     11103 Nov 27  1998 kitchen.gif
ncftp /backup >
```

Note 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.

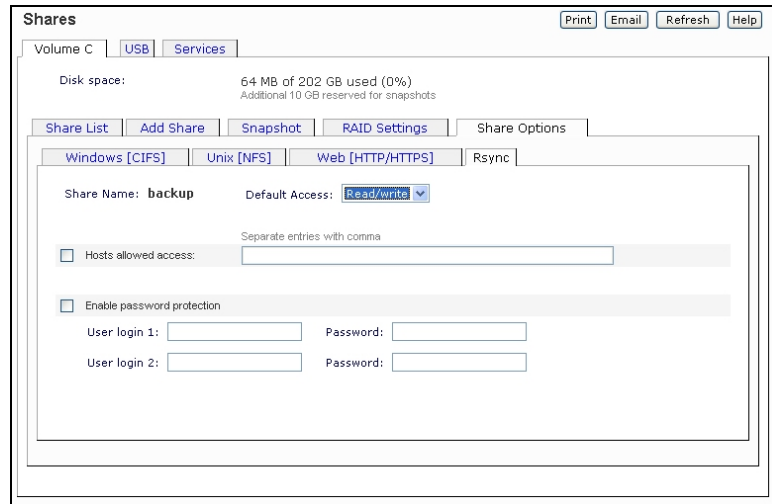
### Warning

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.

## 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'. It includes tabs for 'USB' and 'Services'. The 'Share List' tab is active, showing a table with columns for 'Share Name', 'Default Access', 'Hosts allowed access', and 'Enable password protection'. The 'backup' share is listed with 'Read/write' access. Below the table, there are input fields for 'User login 1', 'User login 2', 'Password', and 'Hosts allowed access'.

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  
Password: *****
```

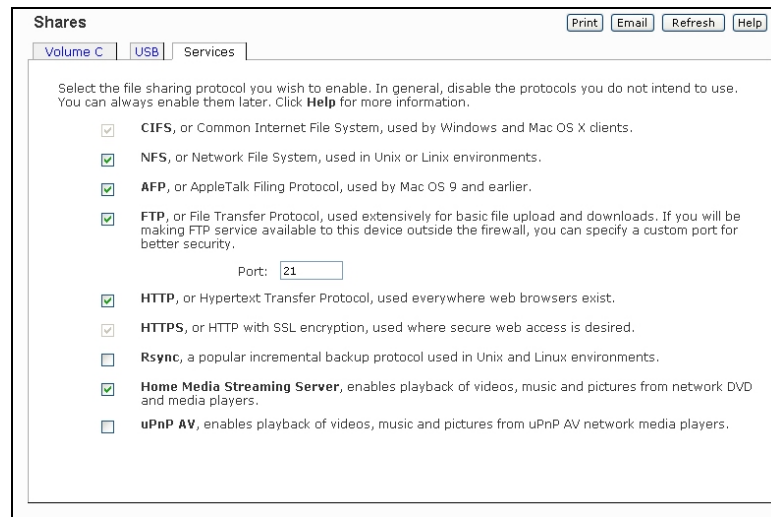
### Note

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 a window titled "Shares" with tabs for "Volume C", "USB", and "Services". The "Services" tab is selected. At the top right are buttons for "Print", "Email", "Refresh", and "Help". Below the tabs, there is a text box with instructions: "Select the file sharing protocol you wish to enable. In general, disable the protocols you do not intend to use. You can always enable them later. Click **Help** for more information." Below this are several protocols with checkboxes:

- CIFS**, or Common Internet File System, used by Windows and Mac OS X clients.
- NFS**, or Network File System, used in Unix or Linux environments.
- AFP**, or AppleTalk Filing Protocol, used by Mac OS 9 and earlier.
- FTP**, or File Transfer Protocol, used extensively for basic file upload and downloads. If you will be making FTP service available to this device outside the firewall, you can specify a custom port for better security.  
Port:
- HTTP**, or Hypertext Transfer Protocol, used everywhere web browsers exist.
- HTTPS**, or HTTP with SSL encryption, used where secure web access is desired.
- Rsync**, a popular incremental backup protocol used in Unix and Linux environments.
- Home Media Streaming Server**, enables playback of videos, music and pictures from network DVD and media players.
- UPnP AV**, enables playback of videos, music and pictures from uPnP AV network media players.

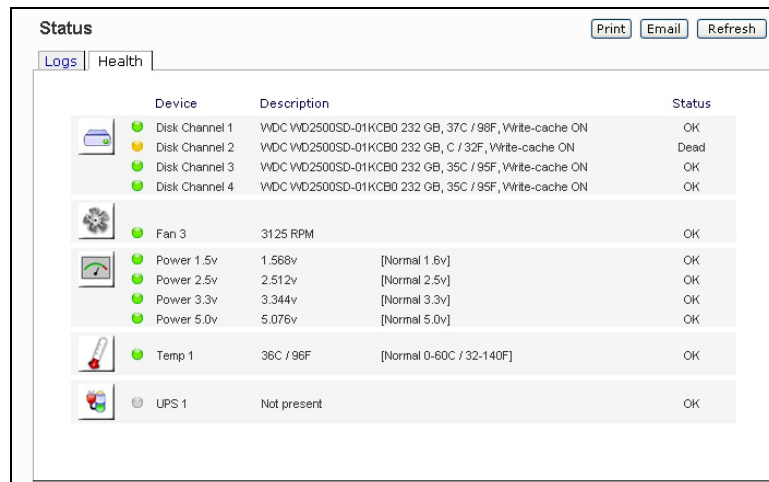
Consult the Device Compatibility list for information on which DVD players and media adapters will work with the ReadyNAS.



## 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.



Status			
Device	Description		Status
Disk Channel 1	WDC WD2500SD-01KCB0 232 GB, 37C / 98F, Write-cache ON		OK
Disk Channel 2	WDC WD2500SD-01KCB0 232 GB, C / 32F, Write-cache ON		Dead
Disk Channel 3	WDC WD2500SD-01KCB0 232 GB, 35C / 95F, Write-cache ON		OK
Disk Channel 4	WDC WD2500SD-01KCB0 232 GB, 35C / 95F, Write-cache ON		OK
Fan 3	3125 RPM		OK
Power 1.5v	1.568v	[Normal 1.6v]	OK
Power 2.5v	2.512v	[Normal 2.5v]	OK
Power 3.3v	3.344v	[Normal 3.3v]	OK
Power 5.0v	5.076v	[Normal 5.0v]	OK
Temp 1	36C / 96F	[Normal 0-60C / 32-140F]	OK
UPS 1	Not present		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

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.

You will need to 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.

## Re-synchronize the Volume

Power-on the ReadyNAS. The RAID volume will automatically re-synchronize the new disk in the background. The process may take up to several hours depending on disk size. During the re-sync process, the ReadyNAS can be used as normal, although access will 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 two tasks: (1) re-install the ReadyNAS firmware and (2) reset the ReadyNAS back to the factory default settings. Typically, you should not need to resort to either option 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:

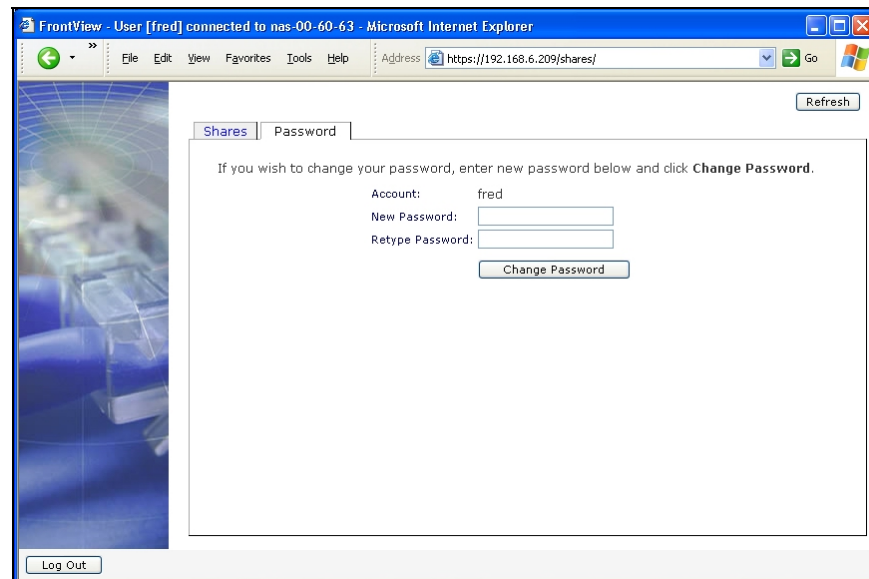
- **To re-install the ReadyNAS firmware**, use a paper clip to depress the switch while the system is off. Continue to depress the reset switch while powering on the system and continue to hold the reset switch for 5 seconds afterward. The disk LED's will flash once to signify that the command has been 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 twice 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.

For both 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/](https://ip_addr/) to access the web share listing page. Then select the **Password** tab, and follow the prompts to set a new 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.

## 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 24 characters or less.
- A fully-qualified domain name (FQDN) must have no more than 24 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 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.

## 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. During off-hours, you can post questions on the message board at <http://www.infrant.com/forum.htm> which is frequented by advanced users and Infrant engineering support and design staff.