NAS System

User's Manual

Revision 1.7

P/N: PW0020000000324

Table of Contents

Preface 6

Before You Begin 7

Safety Guidelines 7

Packaging, Shipment and Delivery 7

Chapter 1 Introduction 8

1.1 Key Features 9

1.2 Technical Specifications 10

1.3 RAID Levels 11

Chapter 2 Installation 12

2.1 Packaging, Shipment and Delivery 12

2.2 Unpacking the NAS System 12

2.3 Identifying Parts of the NAS System 13

2.3.1 Front View 13

2.3.2 Rear View 14

2.3.3 HDD Status LEDs 14

2.3.4 Environmental Status LEDs 15

2.3.5 Lock Indicator 15

2.3.6 Front Panel 16

2.3.7 LCD Menu Diagram 17

2.4 Getting Started with the NAS System 18

2.4.1 NAS Hardware Setup 18

2.4.2 Installing Hard Drives 18

2.4.3 Using the QLaunch NAS Quick Finding Utility 20

2.4.4 Connecting to NAS Management GUI 23

2.4.5 Quick Setup 25

2.5 Overview of the NAS Setup Phases 29

2.5.1 Relationship between RAID disks, Storage Pool, Volumes, and Shares 30

Chapter 3 proNAS Manager 34

3.1 Storage/Share 34

3.1.1 RAID / Disk Information 34
3.1.1.1 Create New RAID and Join Disk to Storage Pool 36
3.1.1.2 Delete RAID 42
3.1.1.3 Extend RAID 44
3.1.1.4 Set a Spare Disk 46
3.1.2 Volume 47
3.1.2.1 Join a Disk to Storage Pool 48
3.1.2.2 Create a Volume 49
3.1.2.3 Delete a Volume 50
3.1.2.4 Extend a Volume Capacity 51
3.1.2.5 Setup Volume as iSCSI Target 52
3.1.2.6 Disable iSCSI Configuration in a Volume 56
3.1.2.7 Remove iSCSI Configuration and Restore to NAS Volume 57
3.1.3 Share/Security 59
3.1.3.1 Create New Share Folder 60
3.1.3.2 Assign Permission to Share 65
3.1.3.3 Edit Share Folder 68
3.1.3.4 Delete Share Folder 69
3.1.3.5 Accessing Share Folder from Windows Clients via Samba 70
3.1.3.6 Accessing Share Folder from Linux/UNIX Clients via NFS 72
3.1.3.7 Accessing Share Folder from Mac Clients 74
3.1.3.8 How to Setup Rsync 76
3.1.3.9 How to Setup Time Machine 82
3.2 Network 88
3.2.1 Device Configuration 88
3.2.1.1 Configure Network Trunking 90
3.2.1.2 Cancel Network Trunking 92
3.2.2 ADS/NIS 93
3.2.2.1 Join NAS to Windows AD Domain 94
3.2.2.2 Join NAS to NIS Domain 97
3.2.3 DHCP (Internet Gateway) 98
3.2.4 P2P 99
3.2.4.1 Status 100
3.2.4.2 Server 101
3.2.4.3 Option 102
3.2.4.4 Shares 103
3.2.4.5 Example of Download from Link and Torrent 104

3.3 System 108
3.3.1 System Information 108
3.3.2 Service 110
3.3.2.1 How to Use iTunes Service 117
3.3.2.2 How to Use WEB Service 120
3.3.2.3 How to Use DHCP (Internet Gateway) Service 123
3.3.2.4 How to Use Media Server Service 125
3.3.2.5 How to Use Photo Service 130
3.3.3 Time/UPS 134
3.3.4 Boot/Shutdown 136
3.3.5 Upgrade 143
3.3.5.1 Remote Upgrade 143
3.3.5.2 Local Upgrade 144
3.3.6 Log 145
3.3.7 Notification 146
3.3.7.1 Event Option 146
3.3.7.2 Email Setting 147
3.3.8 System Tools 148
3.4 Account 152
3.4.1 Account 152
3.4.1.1 Create Account 153
3.4.1.2 Delete Account 154
3.4.1.3 Edit Account 155
3.4.1.4 Import Account 156
3.4.2 Group 157
3.4.2.1 Create Group 158
3.4.2.2 Delete Group 159
3.4.2.3 Edit Group 160
3.5 Data Backup 161
3.5.1 Backup List 161
3.5.1.1 Create Backup Plan 162
3.5.1.2 Create Immediate Backup 166
3.5.1.3 Delete Backup Plan 167
3.5.1.4 Edit Backup Plan 167
3.5.1.5 Delete a Backup Log 168
3.5.1.6 Restore a Backup 168
3.5.1.7 Backup to Local Disk 169

3.5.2 Schedule....171
3.5.2.1 Setup Scheduled Backup Task....172
3.5.2.2 Edit Scheduled Backup Task....173
3.6 File Manager....175
3.6.1 Introduction to File Manager....175
3.6.2 Login to File Manager....177
3.6.2.1 Admin Login....177
3.6.2.2 Ordinary User Login....178
3.6.3 Folder....179
3.6.3.1 Create Folder....179
3.6.3.2 Delete Folder....180
3.6.3.3 Rename Folder....180
3.6.3.4 Set Folder Permission....181
3.6.3.5 Top....182
3.6.4 File....183
3.6.4.1 Upload File....183
3.6.4.2 Download File....184
3.6.4.3 Rename File....184
3.6.4.4 Delete File....185
3.6.4.5 Set File Permission....186
3.6.4.6 Refresh File List....187
3.6.5 System....188
3.6.5.1 Preview Function....188
3.6.5.2 Logout....189

Preface

About this manual

This manual provides information regarding the quick installation and hardware features of the **NAS system**. This document also describes how to use the storage management software. Information contained in the manual has been reviewed for accuracy, but not for product warranty because of the various environment/OS/settings. Information and specifications will be changed without further notice.

This manual uses section numbering for every topics being discussed for easy and convenient way of finding information in accordance with the user's needs. The following icons are being used for some details and information to be considered in going through with this manual:

NOTES:
These are notes that contain useful information and tips that the user must give attention to in going through with the subsystem operation.

IMPORTANT!
These are the important information that the user must remember.

WARNING!
These are the warnings that the user must follow to avoid unnecessary errors and bodily injury during hardware and software operation of the subsystem.

CAUTION:
These are the cautions that user must be aware to prevent damage to the equipment and its components.

Copyright

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent.

Trademarks

All products and trade names used in this document are trademarks or registered trademarks of their respective owners.

Changes

The material in this document is for information only and is subject to change without notice.

NOTE: Some screen shots may differ from actual NAS system model.

Before You Begin

Before going through with this manual, you should read and focus to the following safety guidelines. Notes about the subsystem product packaging and delivery are also included.

Safety Guidelines

To provide reasonable protection against any harm on the part of the user and to obtain maximum performance, user is advised to be aware of the following safety guidelines particularly in handling hardware components:

Upon receiving of the product:

- Place the product in its proper location.
- To avoid unnecessary dropping out, make sure that somebody is around for immediate assistance.
- It should be handled with care to avoid dropping that may cause damage to the product. Always use the correct lifting procedures.

Upon installing of the product:

- Ambient temperature is very important for the installation site. It must not exceed 30°C. Due to seasonal climate changes; regulate the installation site temperature making it not to exceed the allowed ambient temperature.
- Before plugging-in any power cords, cables and connectors, make sure that the power switches are turned off. Disconnect first any power connection if the power supply module is being removed from the enclosure.
- Outlets must be accessible to the equipment.
- All external connections should be made using shielded cables and as much as possible should not be performed by bare hand. Using anti-static hand gloves is recommended.
- In installing components, secure all the mounting screws and locks. Make sure that all screws are fully tightened. Follow correctly all the listed procedures in this manual for reliable performance.

Packaging, Shipment and Delivery

- Before removing the subsystem from the shipping carton, you should visually inspect the physical condition of the shipping carton.
- Unpack the subsystem and verify that the contents of the shipping carton are all there and in good condition.
- Exterior damage to the shipping carton may indicate that the contents of the carton are damaged.
- If any damage is found, do not remove the components; contact the dealer where you purchased the subsystem for further instructions.

Chapter 1 Introduction

The NAS System

Storage networks become more and more complex. If you need to easily expand storage capacity while providing uninterrupted high-performance data access across your LAN, you may want to consider a NAS (Network Attached Storage) appliance. When budgets are tight and a quick fix is required, a NAS appliance is a low-cost, efficient solution to dodge that network-to-storage logjam. That's why more and more users select NAS architecture as their storage networking.

The NAS system is a reliable, cost-effective way to add storage to the network. It comes with 5 drive trays accommodating 3.5" SATA II drives while SCA-II single connector architecture enables true hot swap capability. Built-in Intel Celeron 1.6GHz CPU (or above), up to 2GB DDR2-667MHz SDRAM and two Gigabit Ethernet ports offers high performance NAS platform. With Linux-based embedded OS design, it can boot without HDD, FDD or CD-ROM to guarantee reliability and quick boot. The NAS system is managed and configured by Flex/Ruby browser-based software, and some features include pre-configure disk capacity, users setting, volume management, quick installation on popular network platform, and multi-protocol support. It is equipped with software RAID to offer fault tolerant data protection. It offers full featured data protection supporting RAID levels 0, 1, 5, 6, 10, Linear.

System reliability is ensured by an environmental monitoring unit, which tracks the enclosure temperature as well as individual disk temperatures. If any irregularity in the system occurs, the monitoring unit alerts the administrator.

1.1 Key Features

- Supports up to five hot-swappable SATA II hard drives
- Equipped with software RAID function and supports RAID levels 0, 1, 5, 6, 10, Linear
- Linux-based embedded OS design
- Provides file access services to multiple users over the LAN, the intranet and / or the internet
- Multi-protocol support (TCP/IP, DHCP, AppleTalk, Mac Zone, SMB, NFS, CIFS, AFP over TCP/IP, HTTP)

1.2 Technical Specifications

Hardware Platform ▪ Intel Celeron 1.6G CPU (or above) ▪ Cache memory: 1GB ~ 2GB DDR2-667MHz ▪ Supports 5 SATA II hard drives ▪ Two Gigabit Ethernet port ▪ Environmental monitoring unit ▪ 270W power supply with PFC	**Macintosh Support** ▪ AFP over AppleTalk ▪ AFP over TCP/IP ▪ Mac Zone ▪ iTunes service
Storage ▪ Equipped with software RAID function to offer fault tolerant data protection ▪ Supports RAID levels 0, 1, 5, 6, 10, Linear ▪ Volume Management ▪ Disk usage statistics ▪ Hot spare capability	**Connectivity** ▪ SMB over TCP / IP ▪ NFS over UDP / IP ▪ CIFS over TCP / IP ▪ NAT ▪ DHCP ▪ FTP ▪ Internet Server ▪ Unit acts as a DHCP server ▪ Unit act as a master browser ▪ Share level security ▪ User ID security for NFS
General ▪ Supports Volume as iSCSI Target ▪ File Server Independent ▪ Peer-to-peer operation ▪ Localized language support ▪ With Quick Setup function ▪ Supports trunking / load balance / fail over / LACP(802.3ad) ▪ Support UPS monitoring	**System Management** ▪ Automatic IP address configuration ▪ Self-contained unit; no extras needed ▪ Management through Web browser ▪ Flash upgradeable unit ▪ Supports Microsoft ADS/PDC and Unix NIS accounts import ▪ Fail-free online firmware upgrade ▪ Unicode support

1.3 RAID Levels

Below is the list of RAID Levels available for configuration in the NAS.

RAID Level	No. of Allowed Failed Drives	Description	Minimum Required Number of Drives
0	**None**	Block striping is provided and yields higher performance than with individual drives. There is no redundancy.	**1**
1	**1**	Drives are mirrored. All data is 100% duplicated on an equivalent drive. Fully redundant.	**2**
5	**1**	Data is striped across several physical drives. Parity protection is used for data redundancy.	**3**
6	**2**	Data is striped across several physical drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives. RAID 6 provides for an extremely high data fault tolerance and can sustain multiple simultaneous drive failures.	**4**
10	**2**	Striping over two RAID1 RAID sets. This level provides mirroring and redundancy through striping.	**4**
Linear (JBOD)	**None**	Linear (JBOD) is similar to RAID 0 in that it concatenates the capacity of all member drives. The data is written linearly starting with the first disk drive. When first disk drive becomes full, the next disk drive is used. Linear can have 1 or more disk drives. There is no data redundancy.	**1**

Chapter 2 Installation

2.1 Packaging, Shipment and Delivery

- ❖ Before removing the system from the shipping carton, you should visually inspect the physical condition of the shipping carton.
- ❖ Unpack the system and verify that the contents of the shipping carton are all there and in good condition.
- ❖ Exterior damage to the shipping carton may indicate that the contents of the carton are damaged.
- ❖ If any damage is found, do not remove the components; contact the dealer where you purchased the system for further instructions.

2.2 Unpacking the NAS System

The package contains the following items:

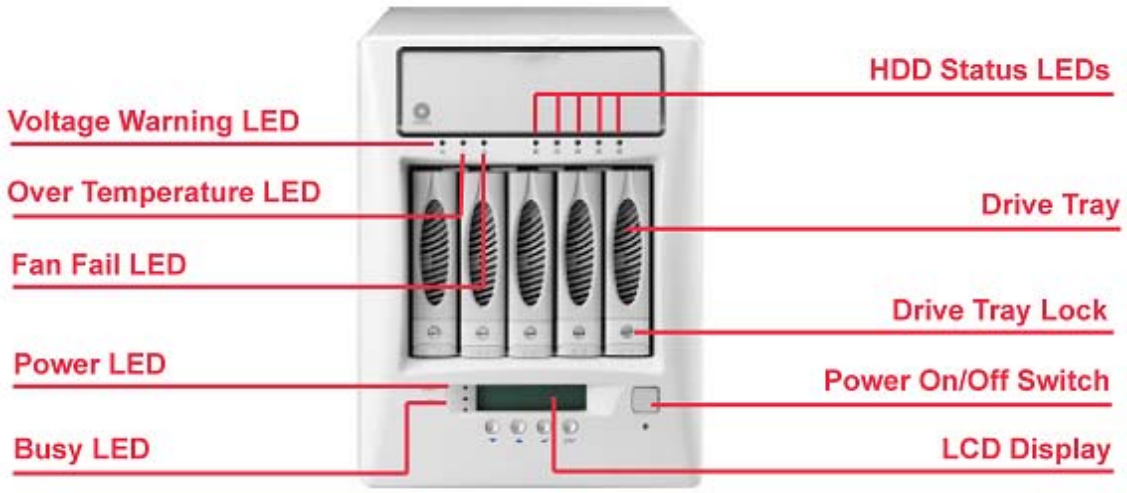
- System unit
- One power cord
- Two Ethernet LAN cables
- Installation Reference Guide

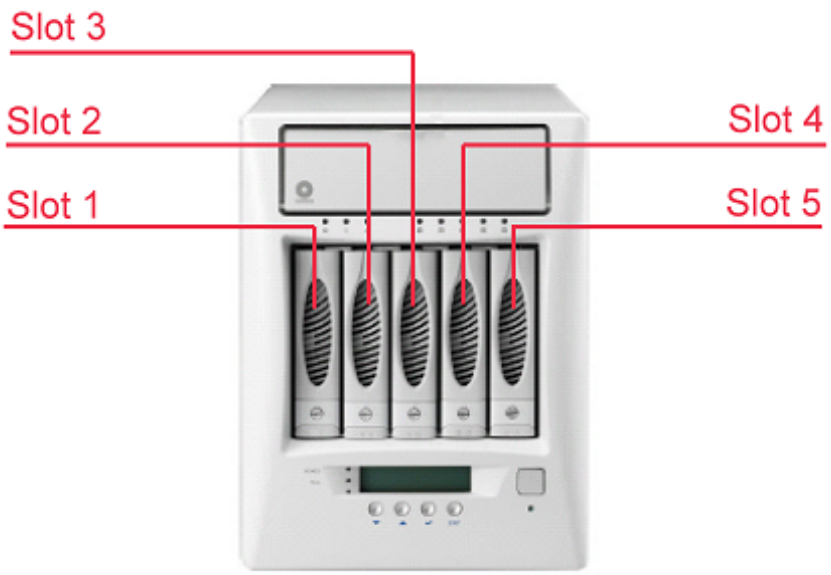
If any of these items are missing or damaged, please contact your dealer or sales representative for assistance.

2.3 Identifying Parts of the NAS System

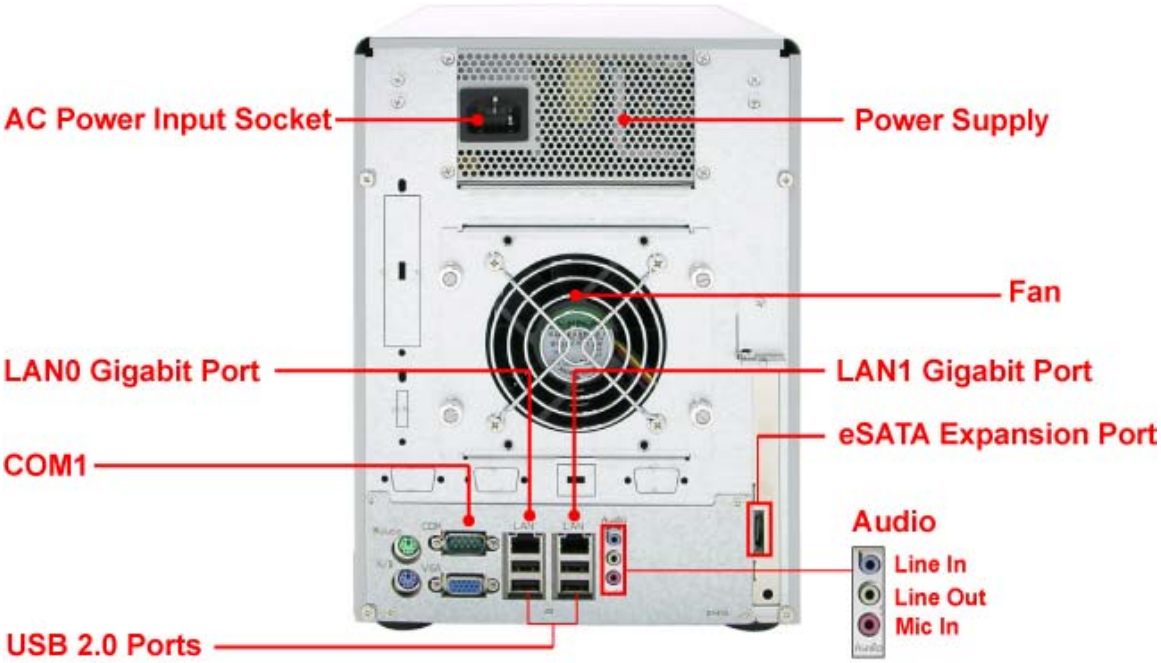
The illustrations below identify the various parts of the NAS system.

2.3.1 Front View

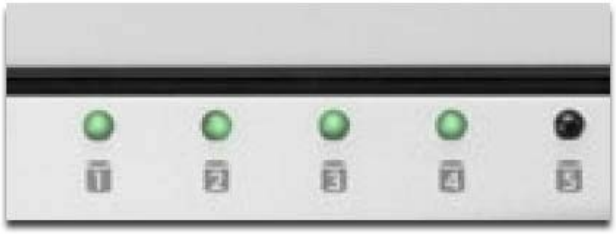




2.3.2 Rear View

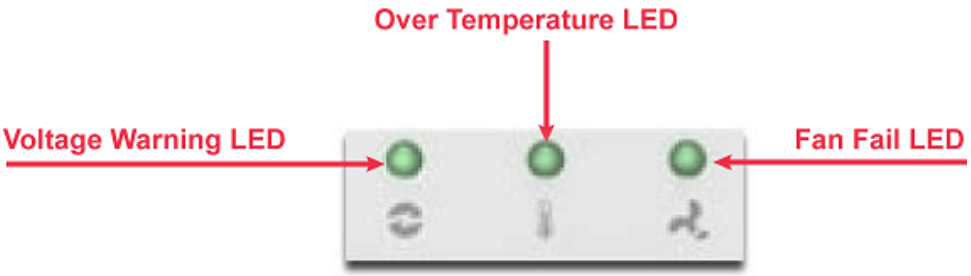


2.3.3 HDD Status LEDs



Green LED indicates power is on and the hard disk drive status is good for this slot. Blinking Orange and Green LED indicates the hard disk drive is in rebuilding state.

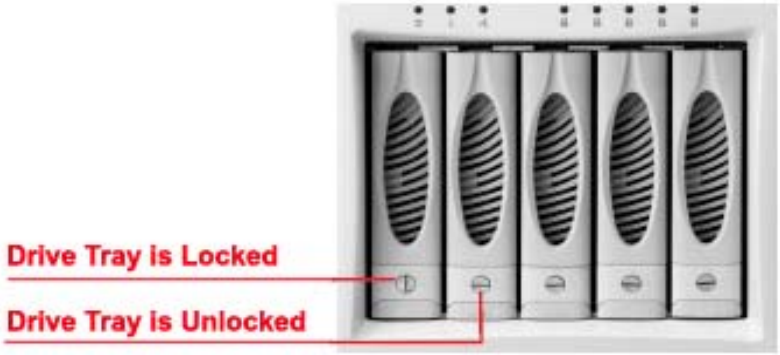
2.3.4 Environmental Status LEDs



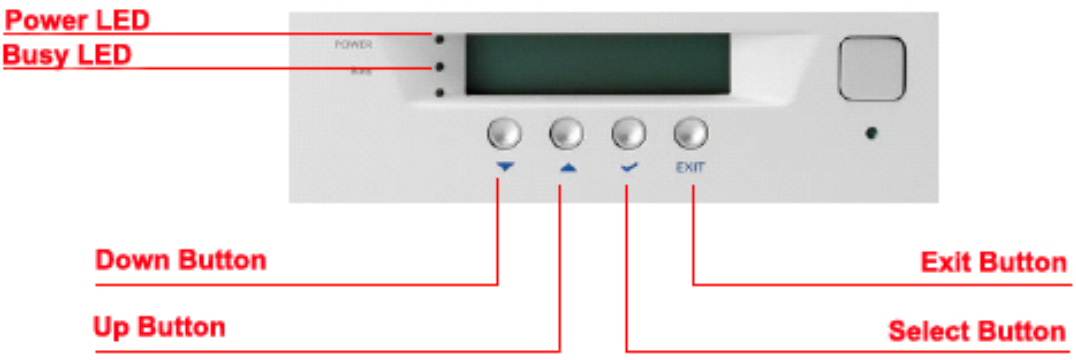
Parts	Function
Voltage Warning LED	An alarm will sound warning of a voltage abnormality and this LED will turn red.
Fan Fail LED	When fan fails, this LED will turn red and an alarm will sound.
Over Temperature LED	If temperature irregularities in the system occurs (HDD slot temperature over 55°C), this LED will turn RED and alarm will sound.

2.3.5 Lock Indicator

Every Drive Carrier is lockable and is fitted with a lock indicator to indicate whether or not the carrier is locked into the chassis. Each carrier is also fitted with an ergonomic handle for easy carrier removal.

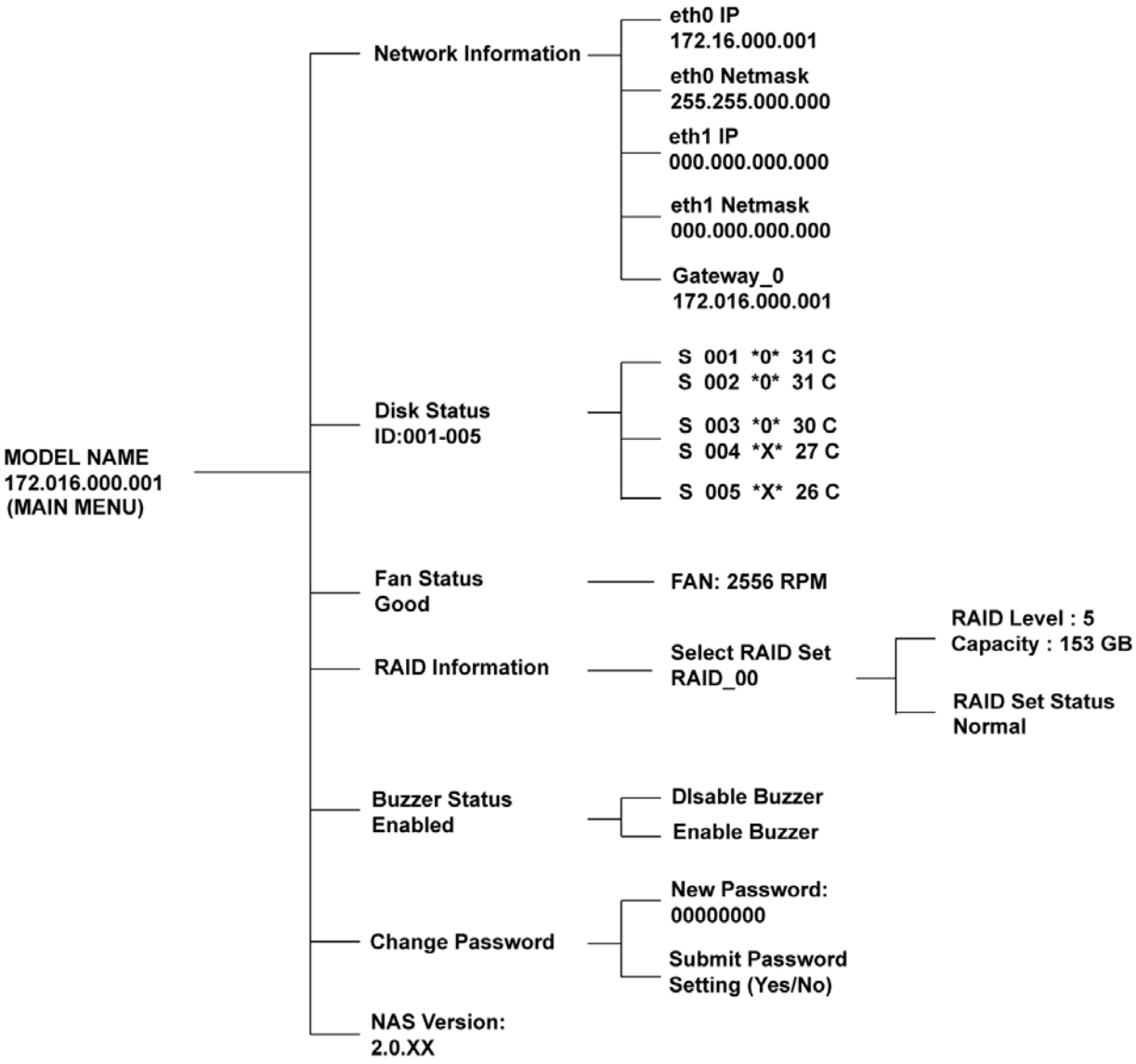


2.3.6 Front Panel



PARTS	FUNCTION
Power LED	Green LED indicates power is on.
Busy LED	Orange blinking indicates system is busy or data is being accessed.
Up and Down Arrow buttons ▲ ▼	Use the Up or Down arrow keys to go through the information on the LCD screen. This is also used to move between each menu when you configure the subsystem.
Select button ✔	This is used to enter the option you have selected.
Exit button **EXIT**	Press this button to return to the previous menu.

2.3.7 LCD Menu Diagram



Disk Status Information:

S 001 - means slot number 1
O - means disk drive in slot is Online or detected
X - means no disk drive in slot or disk drive not detected

2.4 Getting Started with the NAS System

2.4.1 NAS Hardware Setup

1. Attach network cable to LAN0 Ethernet port. Connect the other end of network cable to your network hub or switch. You may also connect the other Ethernet ports if needed.
2. Plug in the power cord into the AC Power Input Socket located at the rear of the subsystem.
3. To turn on the NAS, press the Power On/Off Switch.
4. The Power LED on the front panel will turn green.

2.4.2 Installing Hard Drives

This section describes the location of the hard drives in the NAS system and gives instructions on installing a hard drive. The system supports hot-swapping allowing you to install or replace a hard drive while the system is running.

a. Make sure the lock indicator is in unlocked position. To pull out a disk tray, press the Lock Indicator Button. Pull the handle outwards to remove the disk tray from the enclosure.

b. Place the hard drive in the disk tray.

c. Make sure the holes of the disk tray align with the holes of the hard drive. Install the mounting screws on the bottom part to secure the drive in the disk tray.

d. Slide the tray into a slot and push the Lock Indicator Button.

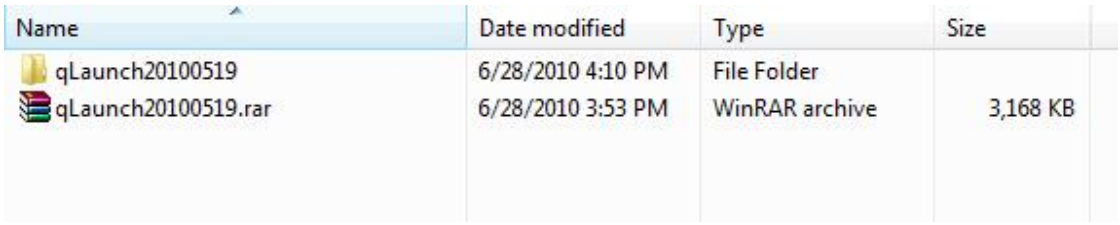
e. Press the handle until you hear the latch click into place. The HDD status LED will turn green if subsystem is on.

2.4.3 Using the QLaunch NAS Quick Finding Utility

The shipping CD contains a QLaunch application that helps find NAS systems in the network. To open QLaunch, copy the Qlaunch archive file (latest version as of this writing is 171SP1 / 20100519) to a computer that will be used to manage the NAS system.

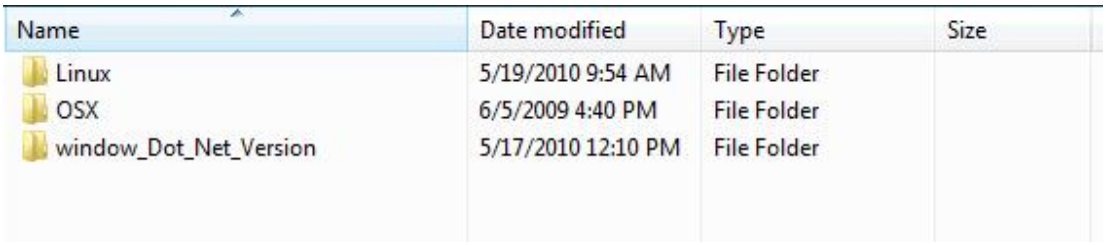
NOTE: The QLaunch Utility can also be downloaded from vendor website: http://www.proware.com.tw/support/support_software_nas.html. Check your vendor for latest available Qlaunch version.

1. Extract the Qlaunch archive file.



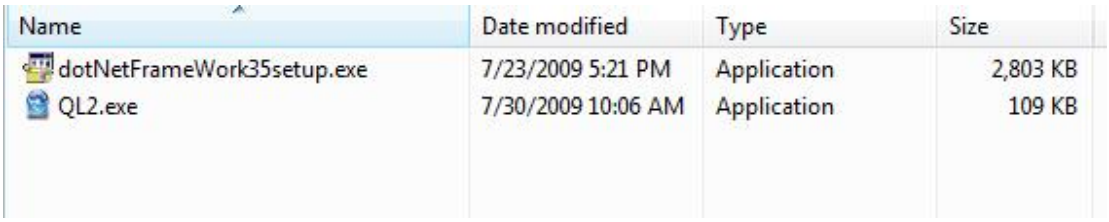
2. Open the Qlaunch folder. There are three subfolders. For computer with Windows OS, open the window_Dot_Net_Version folder.

   For Linux or Mac OS, copy the Linux or OSX directory to a Linux or Mac OS computer.

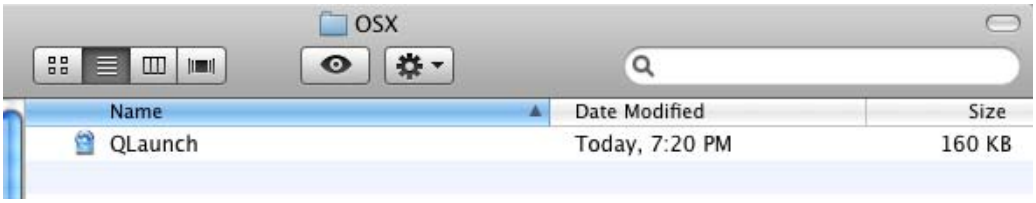


3. After opening the folder, the QL2.exe file will be displayed. Open (double-click) the **QLaunch** application program QL2.exe.

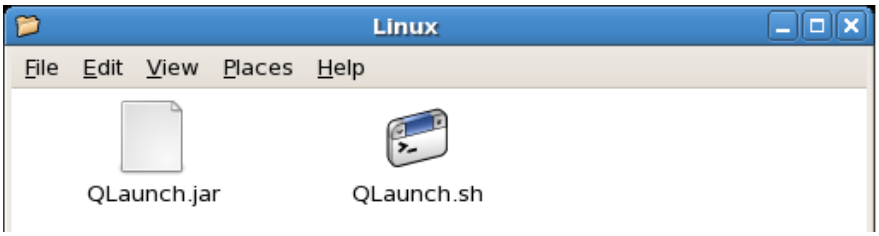
Windows OS:

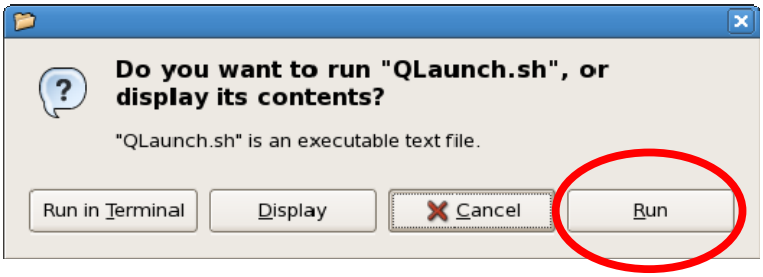


Mac OS X: (QLaunch application)

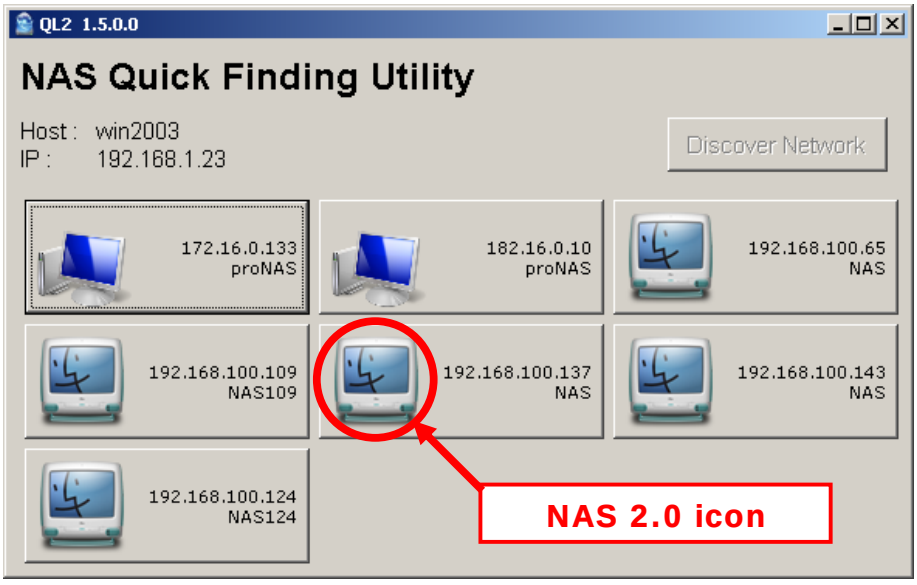


Linux OS: (QLaunch script)



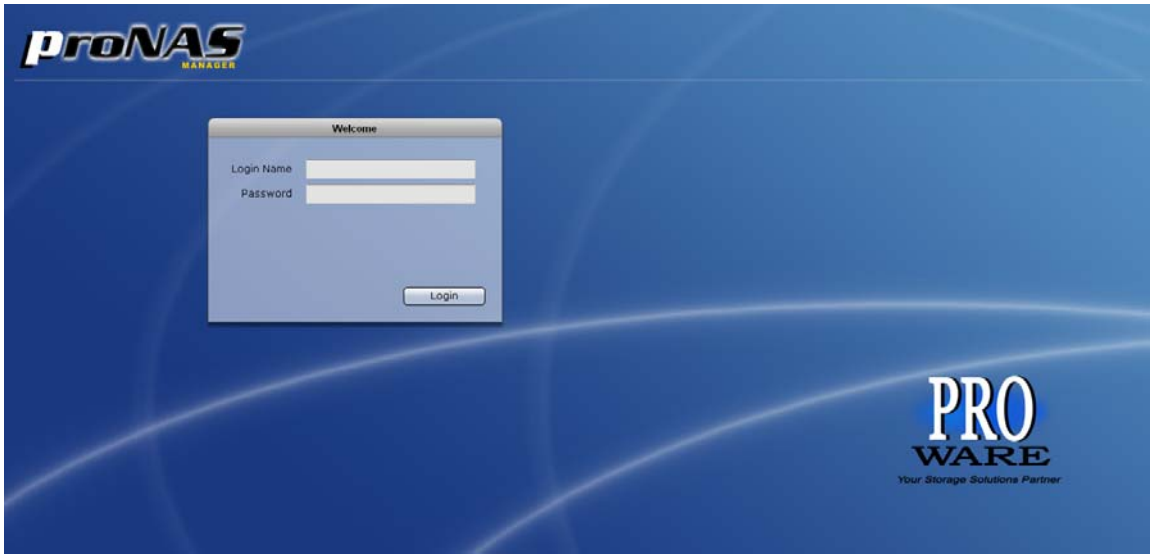


4. The QLaunch GUI will be displayed. It will show all available NAS systems on the network.



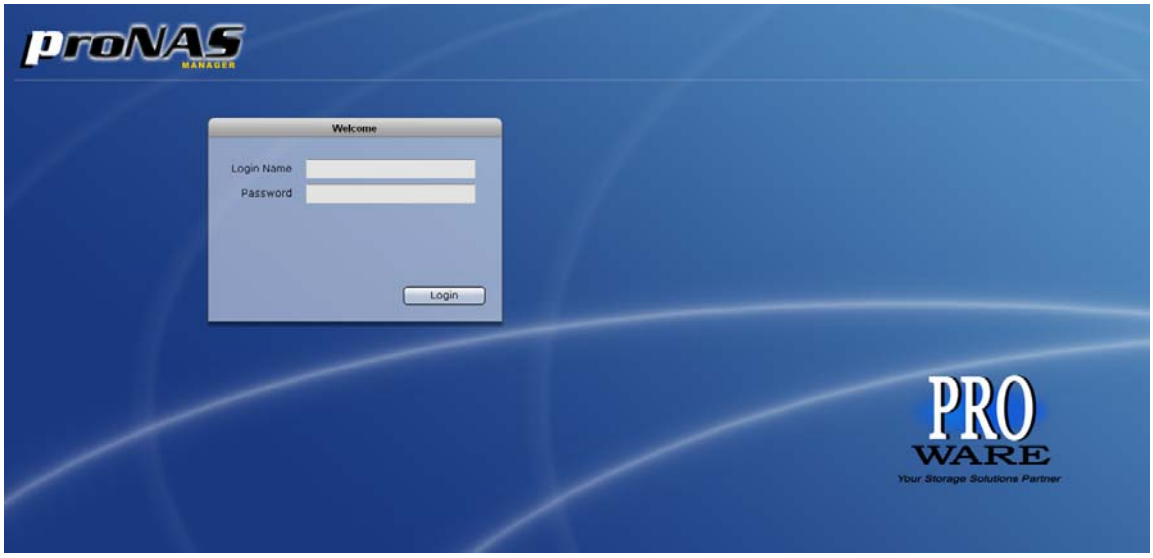
5. Select (double-click) the NAS system that you want to manage.

6. The proNAS login page will be displayed.



2.4.4 Connecting to NAS Management GUI

1. Configure the network setting of your host system (computer that will be used to manage the NAS)), i.e. add network IP address such as 172.16.0.5 subnet 255.255.0.0, to enable connection to NAS default IP 172.16.0.1, (if there is no DHCP server in your network). Refer to Table below.
2. Open web browser and type in the address bar http://172.16.0.1:3000, or use the dynamic IP assigned to the NAS, if a DHCP server is available.
3. The proNAS Login Page will be displayed.



4. Enter the Login Name account and Password. See default settings in the table below.

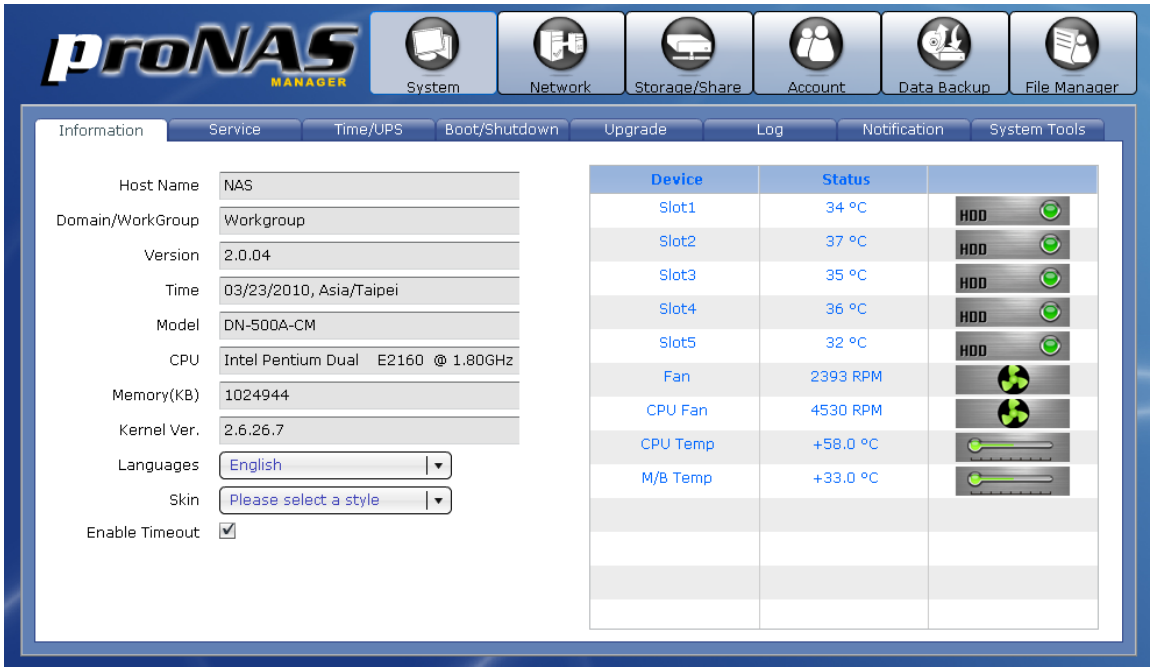
Entity	Default Value
LAN0 (eth0) IP address	172.16.0.1
TCP port	3000
Net Mask	255.255.0.0
Hostname	NAS
Login Name	admin
Password	00000000

NAS Default Settings

NOTE: When the system initially has no NAS configuration (Unit is new and drives have just been used and inserted in the disk slots), after login to GUI, the Quick Setup option will be displayed. Refer to the Quick Setup information in the next section.
NOTE: The admin password for NAS management GUI login can be changed in Account → Account tab.

5. A warning message will be displayed. Select “Yes” to configure the NAS for the first time using Quick Setup (see next Section how to configure with Quick Setup).

6. If you select “No” in the message shown in item #5 (no existing NAS configuration, or NAS system has been configured already), after login, the proNAS Manager GUI will be displayed.



NOTE: “Enable Timeout” is enabled by default. When there is no activity in the proNAS Manager GUI, admin will be automatically logged out after 15 minutes. To disable timeout, remove check mark in Enable Timeout.

NOTE: The Language options supports: English, Traditional Chinese, Simplified Chinese, Japanese, Korean, and Spanish.

2.4.5 Quick Setup

NOTE: The Quick Setup provides a quick and easy way to setup the basic NAS configuration. This function will create the NASVG, which is a Volume Group that holds the NAS configurations and must be created or initialized the first time the NAS is used. The Quick Setup will make use of all available disk drives in the NAS.

The Quick Setup options are listed below:

1. **RAID**
   This is used for selecting the RAID Level.
2. **Storage/Share**
   This shows the default Home share capacity which can be changed. It also shows default share named "share" which can be renamed and whose size can be changed.
3. **Network Adapter**
   This is for configuring the primary Ethernet interface LAN0 (eth0) network settings. After changing the settings, admin need to login using the new IP address.
4. **Service**
   This is for enabling the basic Services provided by proNAS. Windows (Samba) service is enabled by default.

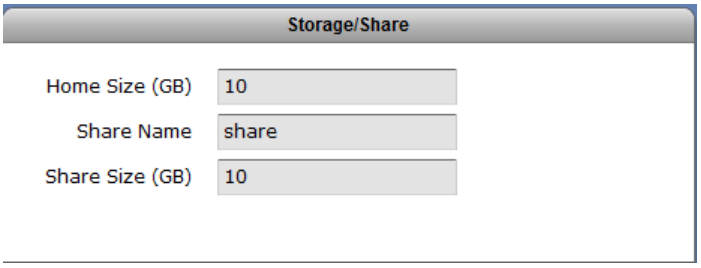
The Quick Setup Steps:

1. Configure the software RAID by selecting the RAID Level.

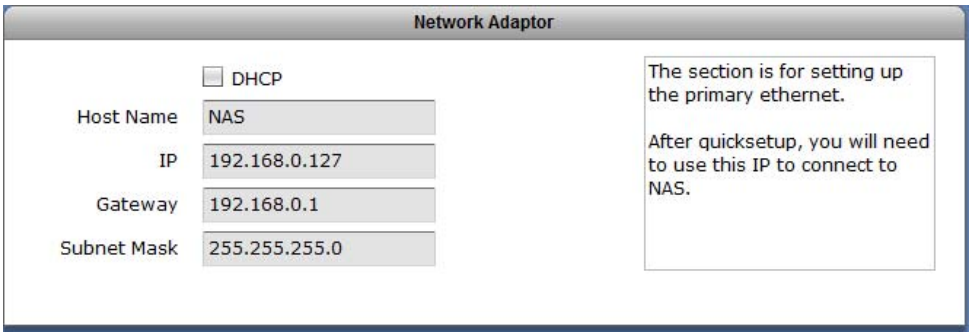
   The RAID Level options are:
   (a) Max. Capacity (RAID0)
   (b) Clone Data (RAID1)
   (c) Security (RAID5)
   (d) Max. Security (RAID6)

NOTE: To initialize the RAID, remove the check mark in the "Without initializing" option. Initializing the RAID will ensure the previous RAID data in the disks are cleared.

2. Configure the Storage/Share.
    a. Change the “home” size default capacity if needed.
    b. Rename the default share if necessary.
    NOTE: The share folder name does not allow space in-between characters.
    c. Change the size of the default share if needed.



3. Configure the Network Adaptor settings. Select “DHCP” option, or configure static IP.
    a. Enter the new NAS Host Name in the Host Name box.
    b. Enter the new IP address.
    c. Edit the Subnet Mask and Gateway.



The configuration options in Network Adaptor:

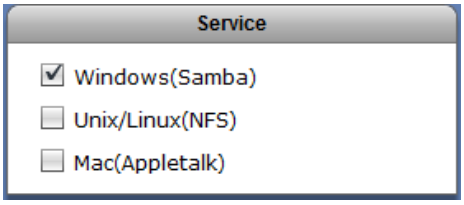
- **Host Name**
  The Host Name is the NetBIOS name of NAS system. This name should be unique.

- **IP**
  This is the IP address of primary Ethernet port LAN0 (eth0) used for NAS management or share folder access. If not set or no DHCP server, it will use the default IP 172.16.0.1.

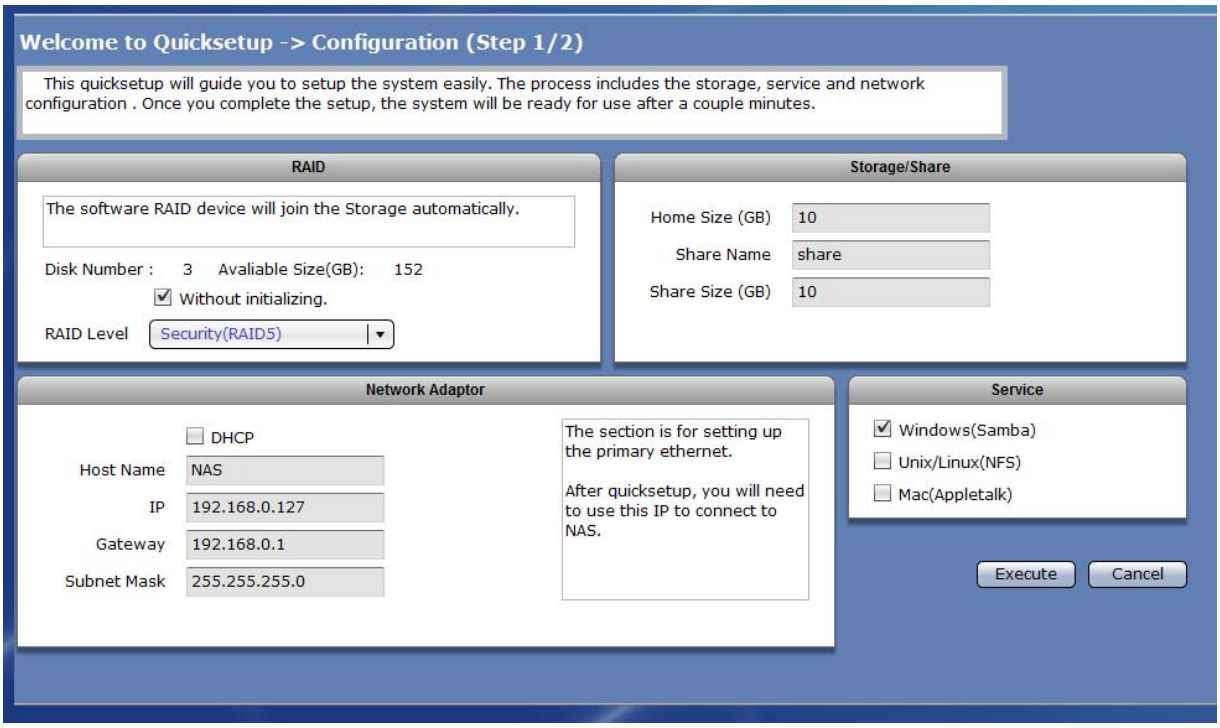
- **Subnet Mask**
  The Subnet Mask used. If not set, it will use the default Subnet Mask 255.255.0.0.

- **Gateway**
  The Gateway used. If not set, it will use the default Gateway 172.16.0.1.

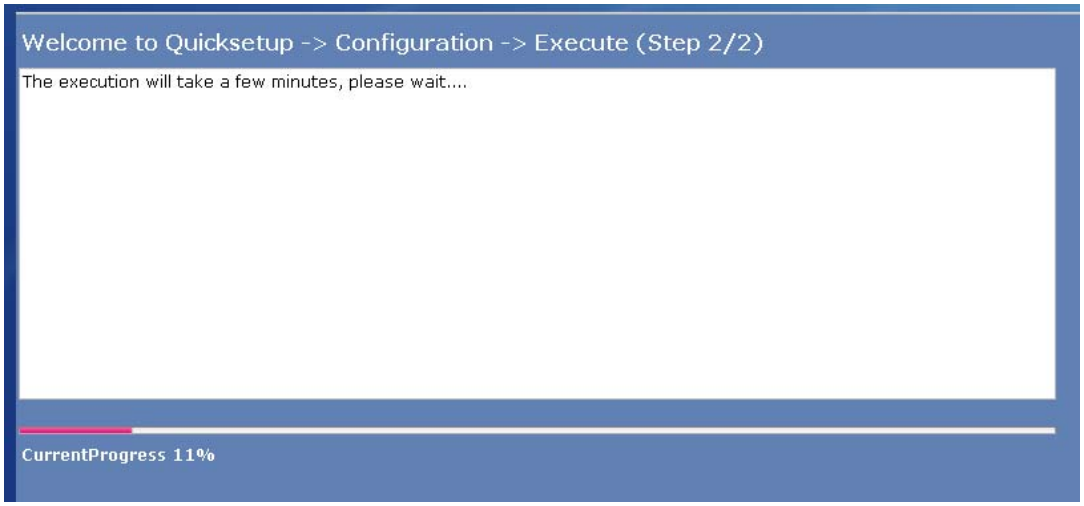
4. Configure the Service options.
    a. Enable the proNAS Service options as needed.



5. Click the “Execute” button.

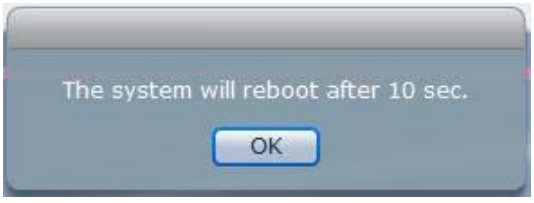


6. The configurations will be set.



7. A warning message will be displayed. Select “Yes” to reboot the NAS and free some memory used by the system.

8. A message will be displayed. Click “OK”.



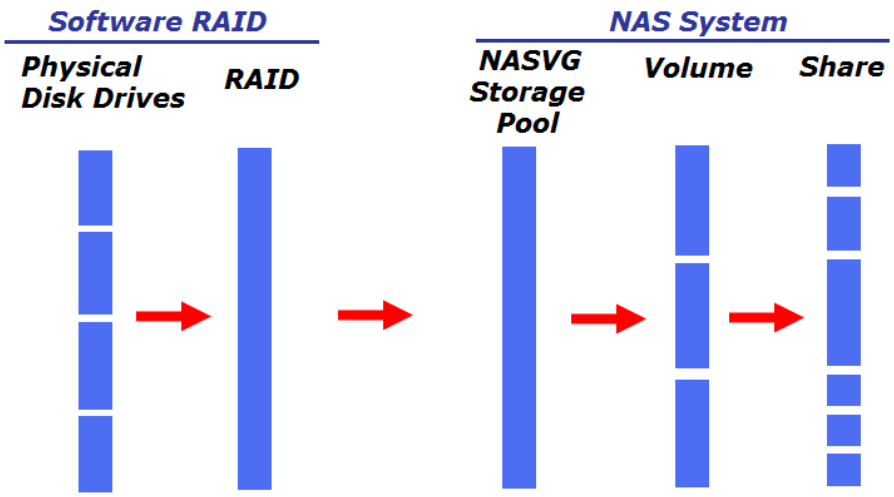
9. The NAS will restart. Wait for about 3 to 4 minutes then login again. If IP address was changed in Network Adapter settings, re-login to proNAS administration page using the new IP address.

2.5 Overview of the NAS Setup Phases

The Setup Phases include configuring proNAS components with proNAS Manager. The basic steps are:

- Create RAID Disk from Hard Disk Drives
- Join RAID Disk to Volume Group's Storage Pool
- Setup the Network Environment
- Enable Services for Windows clients, Linux/UNIX clients, and MAC clients
- Create and Setup Logical Volume and Share Folder.
- Create Accounts or Groups or Join ADS/NIS Domain and assign Share Folder Permission

2.5.1 Relationship between RAID disks, Storage Pool, Volumes, and Shares

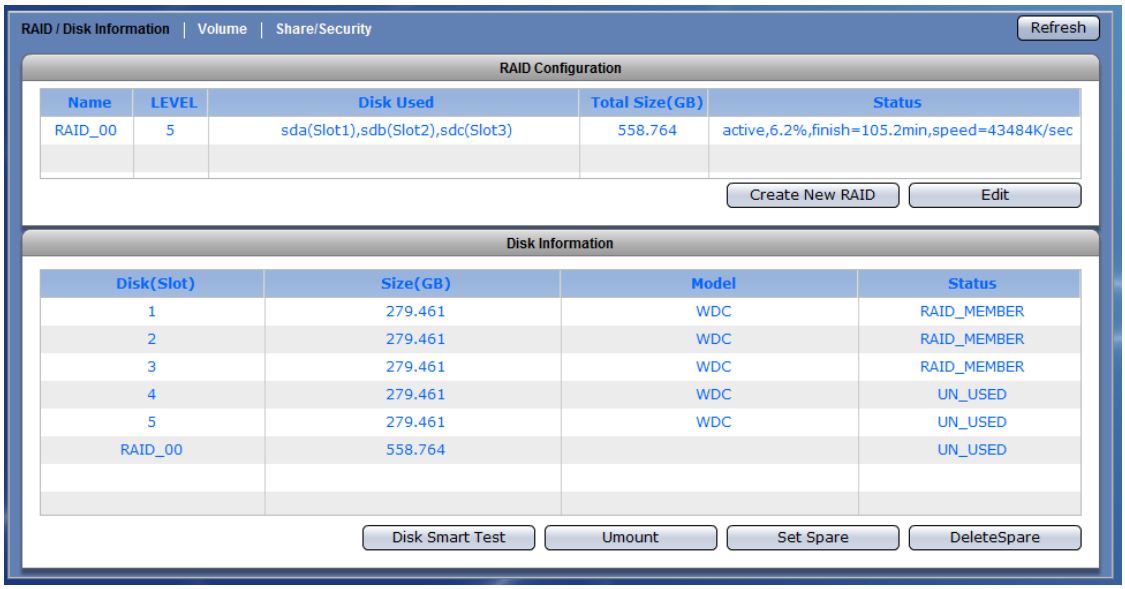


RAID disks

RAID disks are basically logical disks created using the “Create New RAID” button by selecting the physical disk drives to be included as RAID member. When physical disk drives are included in RAID, the status will show as “RAID_MEMBER”. When a physical disk drive is free (neither a RAID member nor a hot-spare), its status will show “UN_USED”.

When a RAID disk is created, the RAID level is assigned. Select your preferred RAID level. Please note that the RAID level options available for selection depends on the number of physical disk drives in the NAS.

Please refer to Section 1.3 RAID Levels for more information about the different RAID levels available in the NAS, and to Section 3.1.1 RAID/Disk Information for creating RAID.

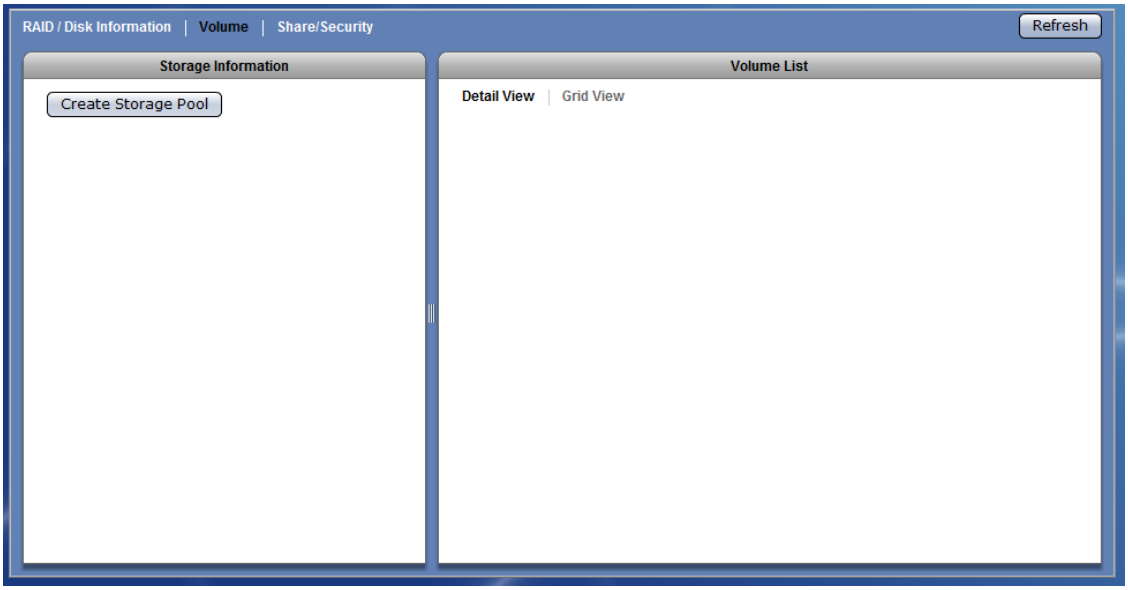


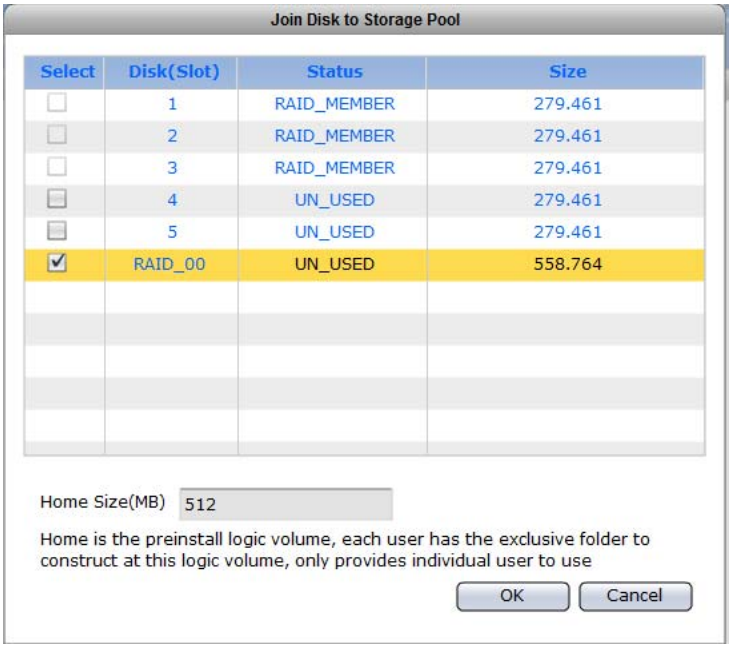
Storage Pool

The Storage Pool is a collection of storage devices, such as RAID disk, which have been joined to NASVG (NAS Volume Group). At least one RAID disk must be joined to NASVG Storage Pool.

After one RAID disk is joined to Storage Pool, the NASVG is initialized and the basic NAS configuration is setup. All other NAS configurations can be done, such as creating Volumes, Shares, and Accounts, and configuring different NAS services.

Please refer to Section 3.1.1 RAID/Disk Information for more information.

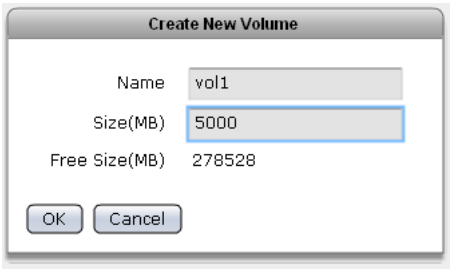


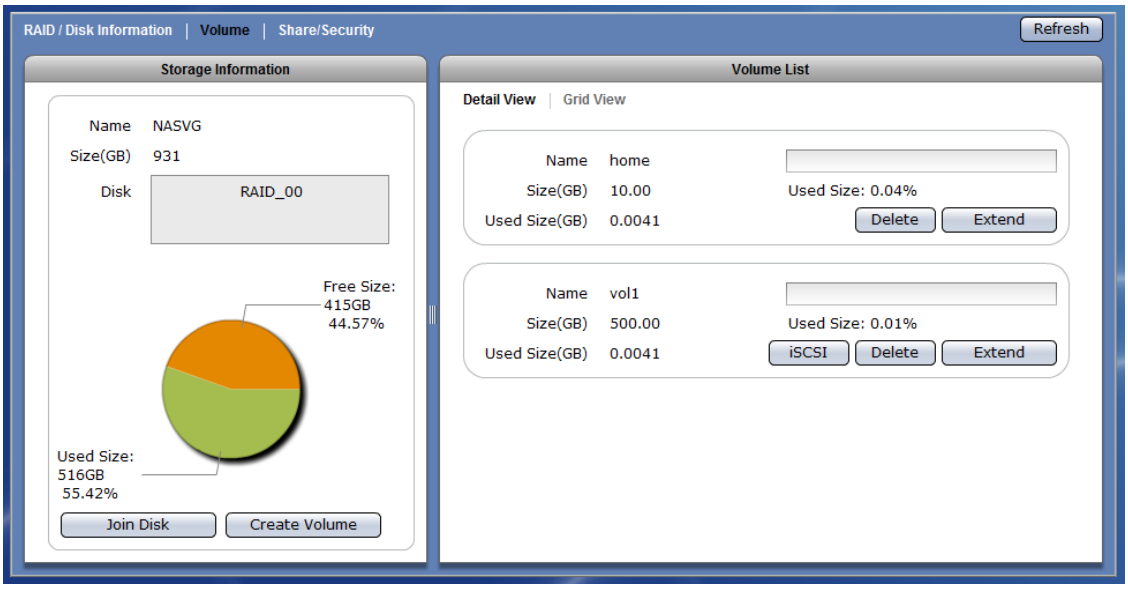


Volumes

Volumes are logical disks created from the NASVG (NAS Volume group). The NASVG total capacity will be almost equal to the capacity of a RAID disk joined to the NASVG Storage Pool. When Volume is created, the Volume capacity will be taken from the available capacity of the NASVG. After a Volume is created, Share folders can also be created. The iSCSI volume can also be configured for a particular Volume. Note that the capacity of a Volume can be extended.

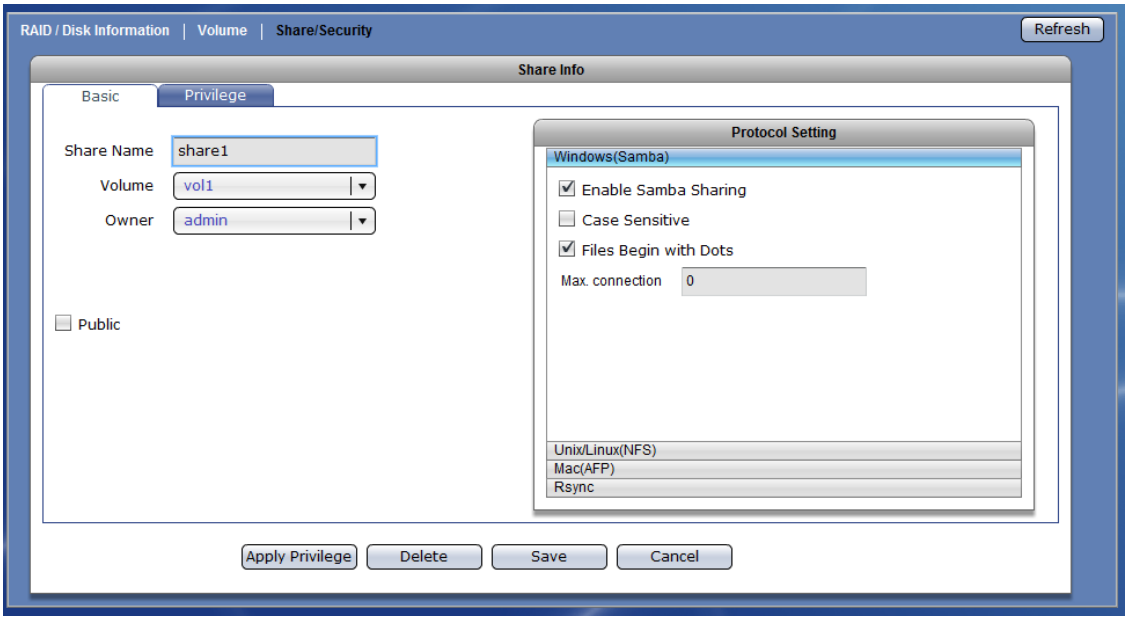
Please refer to Section 3.1.2 Volume for more information.

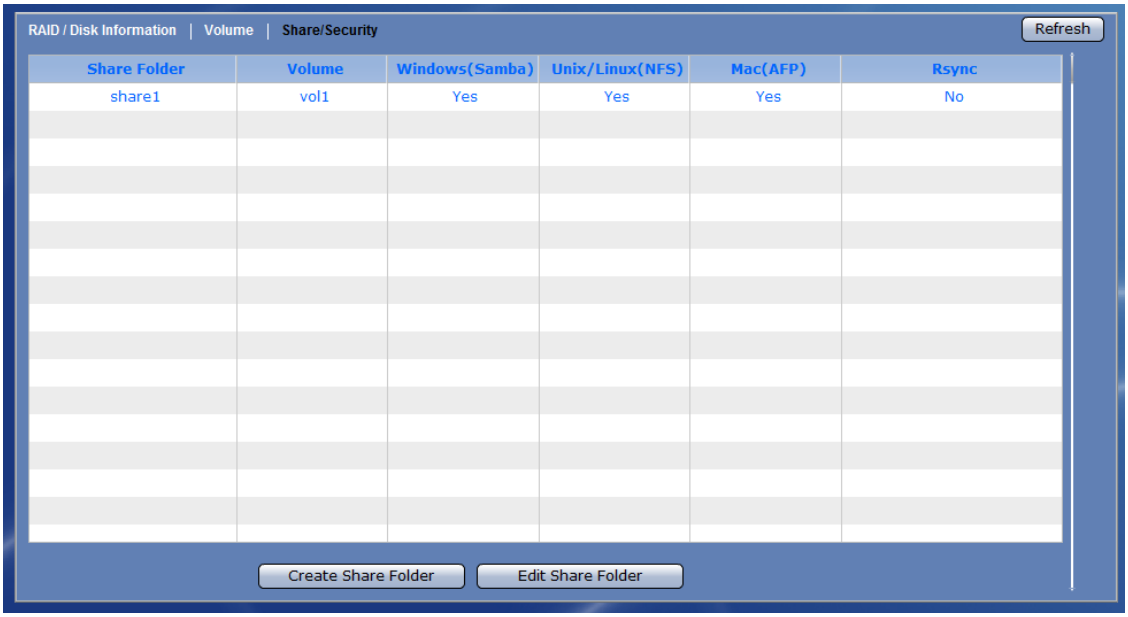




Shares

Shares are the shared folders that are accessed by users in the network. Shares that are created within the same Volume will share or use the total capacity of the Volume.
It is also in the Share where account or group permission is assigned, to allow read-only or read-write access, and where different Protocol Settings for the selected Share can be enabled and configured, or disabled.
Please refer to Section 3.1.3 Share for more information.





Chapter 3 proNAS Manager

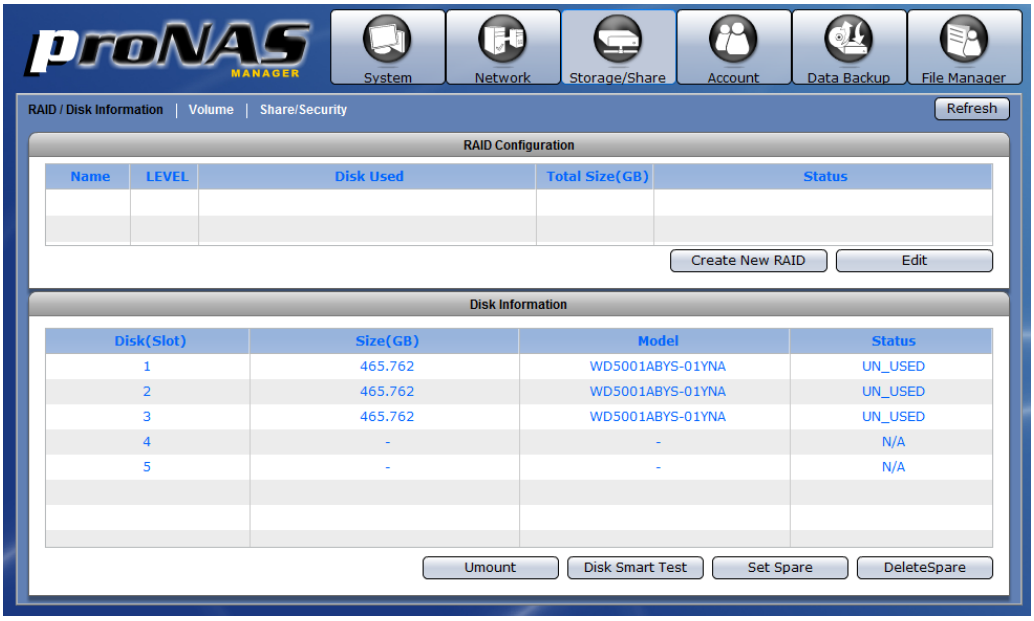
There are six management functions used to configure or manage the NAS.

- **Network**
- **System**
- **Storage / Share**
- **Account**
- **Data Backup**
- **File Manager**

3.1 Storage / Share

3.1.1 RAID / Disk Information

Click the Storage/Share icon then select RAID tab. The RAID Configuration and Disk Information window will be displayed.



NOTE: The Storage / Share → RAID function is normally used when creating a customized RAID configuration. This can be used when the Quick Setup has not been done yet, or Quick Setup has already been done but the RAID will be expanded using new disk drives.

RAID Configuration Screen:

Name – The RAID disk name. This defaults to "RAID_00" if this is the first RAID disk created.

LEVEL – The RAID level used by the RAID disk.

Disk Used – The hard disk drives (slots) joined to the RAID disk.

Total Size (GB) – The capacity size of the RAID disk.

Status – The current status of the RAID disk. Status can be active, degraded, rebuilding, or failed.

RAID Configuration Options:

Create New RAID – Use to create a RAID disk using the hard disk drives.

Edit RAID – Used to edit an existing RAID disk, such as extend the RAID (add another hard disk drive).

Disk Information Screen:

Slot – The hard disk drive slot number.

Disk – The hard disk drive device name. The first disk drive is named "/dev/sda".

Size (GB) – The capacity size of the hard disk drive.

Model – The hard disk drive model name.

Status – The current status of the hard disk drive. Status can be "RAID_MEMBER", "UN_USED", or "SPARE".

Disk Information Options:

Disk Smart Test – Use to perform SMART test on a selected disk drive.

There are two types:

Long Test - does extended/in-depth test on the disk drive which can run in about an hour (more or less 60 minutes).

Short Test – does short test on the disk which can run in more or less 2 minutes.

NOTE: To display the SMART Information of a disk drive, double-click on the disk drive in the Disk Information list.

Umount – Use to un-mount a disk.

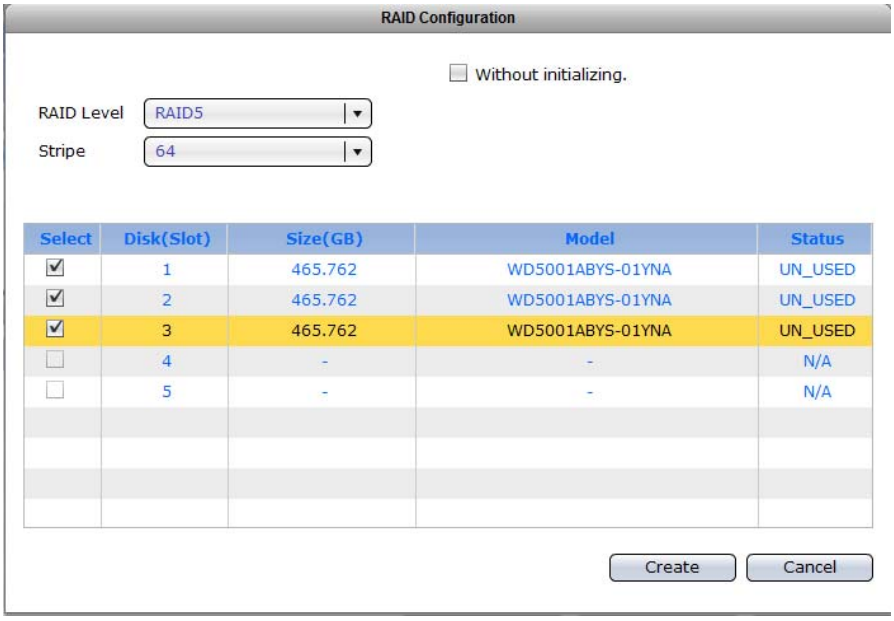
Set Spare – Use to set a selected hard disk drive as a Spare Disk.

Delete Spare – Use to remove the Spare Disk setting on a hard disk drive.

3.1.1.1 Create New RAID and Join Disk to Storage Pool

Steps to Create a New RAID and Join Disk to Storage Pool:

1. Click “Create New RAID”.
2. Set the RAID Level and Stripe size, and select the hard disk drives to be included in the RAID disk. To initialize the RAID, remove the check mark in “Without initializing” option.



RAID Configuration Options:

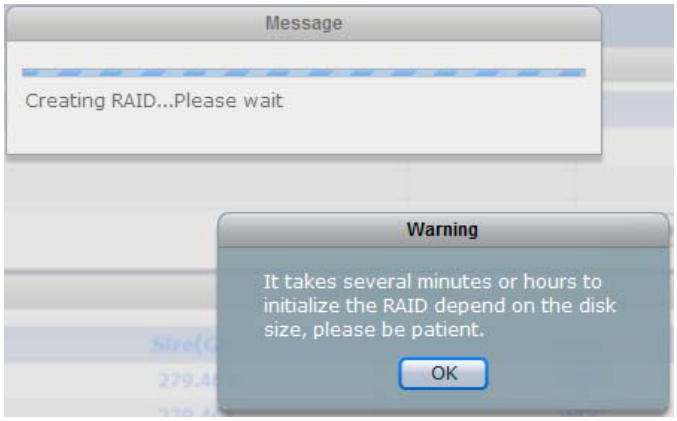
RAID Level – Select the RAID Level you want for the RAID configuration. Available options, depending on number of disk drives, are: JBOD, 0, 1, 5, 6, and 10.

Stripe Size – Set the size of the stripe (block size or chunk size) written to each disk drive. Default is 64KB. Other options are: 128KB, 256KB, 512KB and 1024KB.

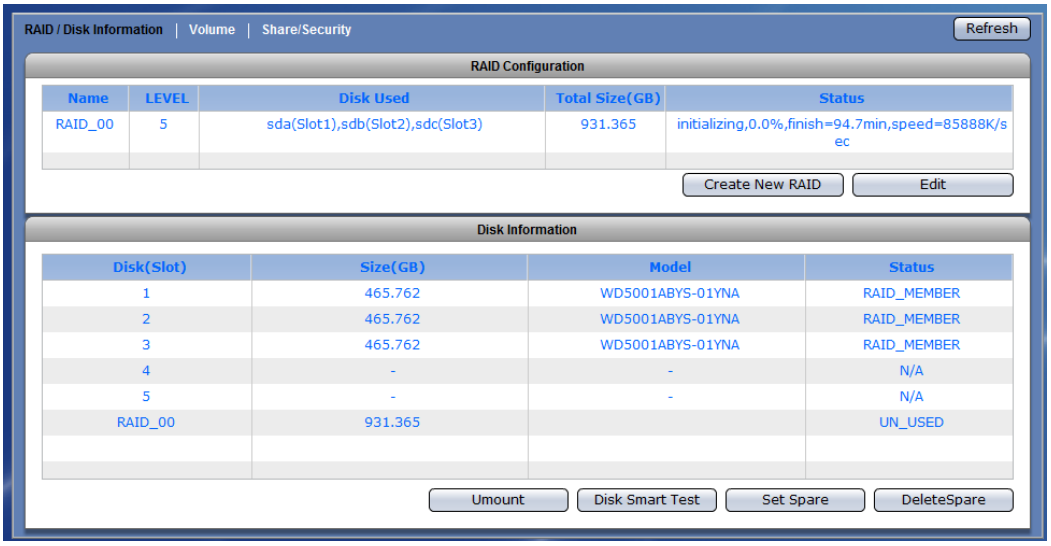
Without initializing – Use this initialize or not initialize the RAID. Default is not to initialize the RAID (with check mark). For first time use, it is recommended to initialize the RAID to ensure the previous RAID data in the disk drives are cleared.

NOTE: A large stripe size produces better read performance if the NAS does mostly sequential reads. If the NAS will do mostly random reads, small stripe size is recommended.

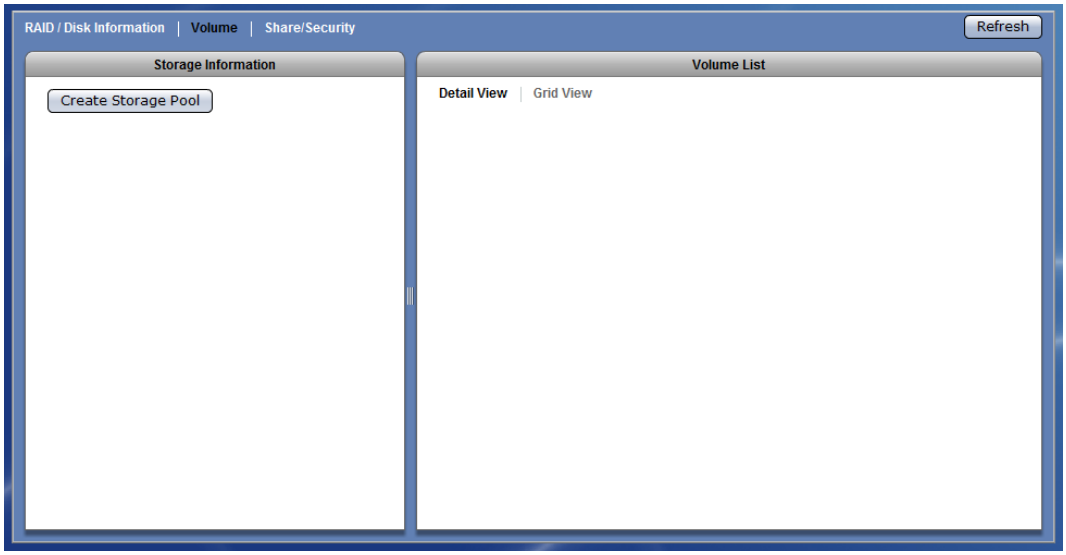
3. A message will be displayed. A warning message is also displayed. Click “OK” to close the warning message.



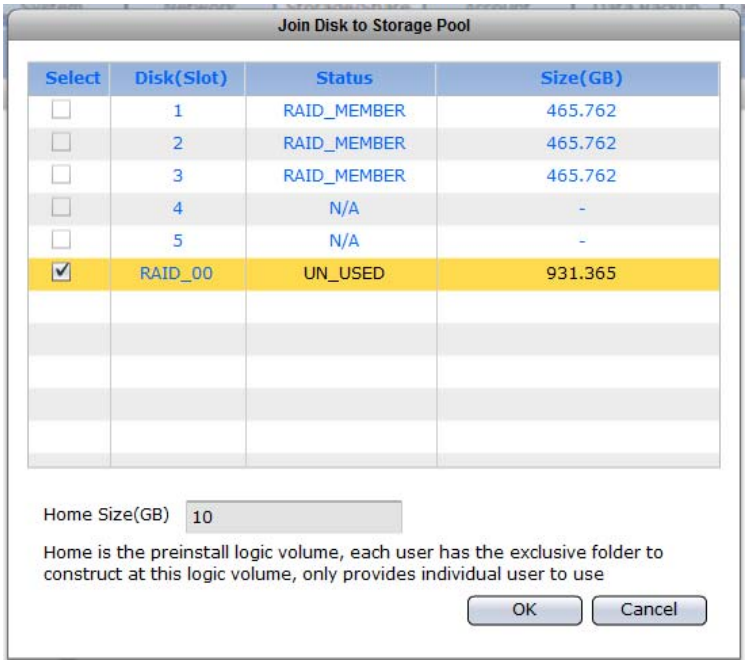
4. The RAID disk will be initialized. Verify in the Status information the current initialization process.



5. While the RAID disk in initializing, the status will show active and the Disk Information will show “UN_USED”. The RAID disk can be joined to NASVG in Volume tab using “Create Storage Pool” button. Click “Create Storage Pool”.



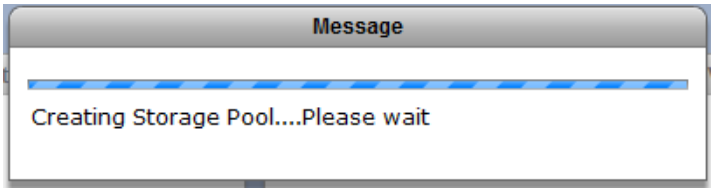
6. Select the disk (must be RAID disk, such as RAID_00) that will be added to storage pool. Click “OK” when done.



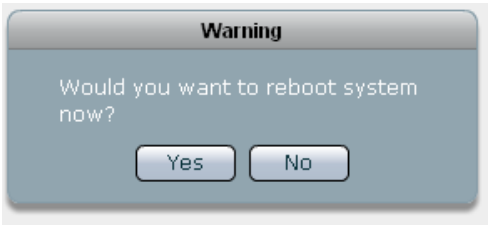
NOTE: NASVG, which is a Volume Group that holds the NAS configurations, will be created when at least one disk (RAID disk) is joined to Storage Pool. At the same time, the default Home volume is also created. The Home volume holds the individual share folders of all user accounts. The default Home volume size is 10GB. If necessary, change the Home size to a larger size.

7. A warning message will be displayed. Select “Yes” to proceed.

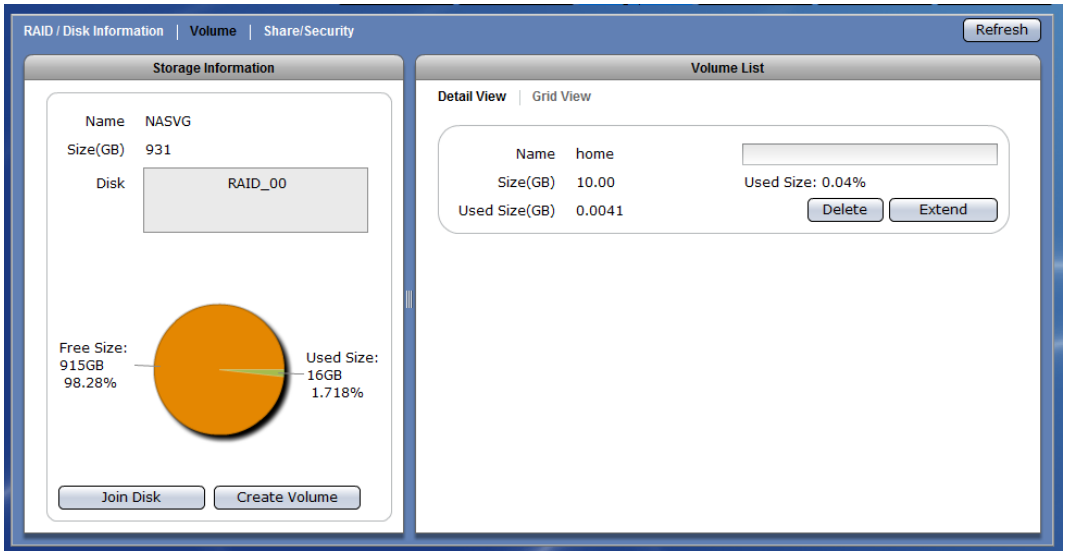
8. A message will be displayed.



9. When warning message is displayed, select “Yes” to free some memory used by the system. The NAS system will reboot.



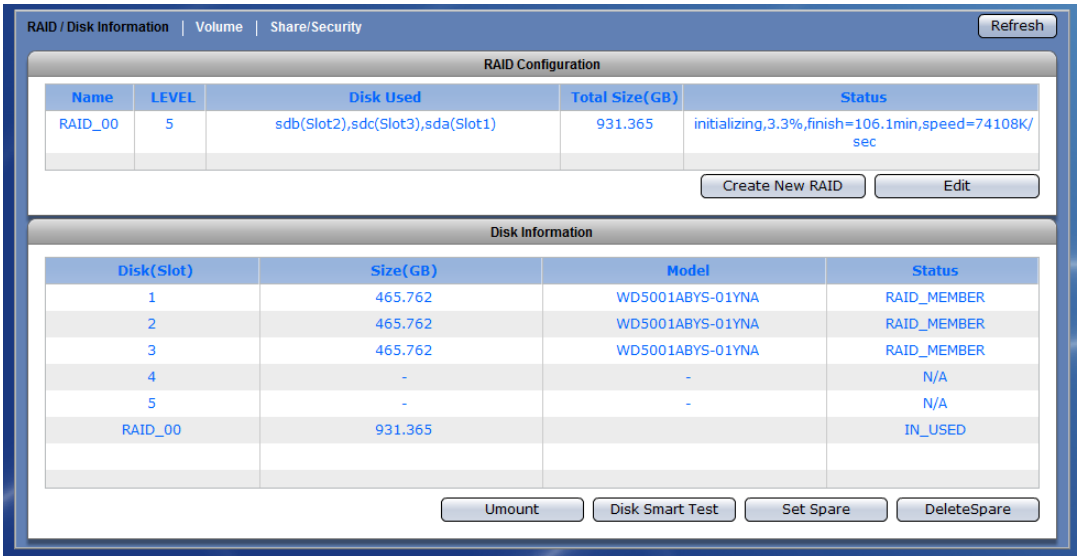
10. Re-login to the system then select Storage/Share. The NASVG and the default “home” volume are created.



NOTE: After NASVG is initialized, the Storage Information screen will show a pie chart with amount of Free Size and Used Size. Volumes can be created from the NASVG.

NOTE: The default “home” volume cannot be deleted.

11. After the RAID disk is joined to NASVG, the RAID status in Disk Information will show “IN_USED”.



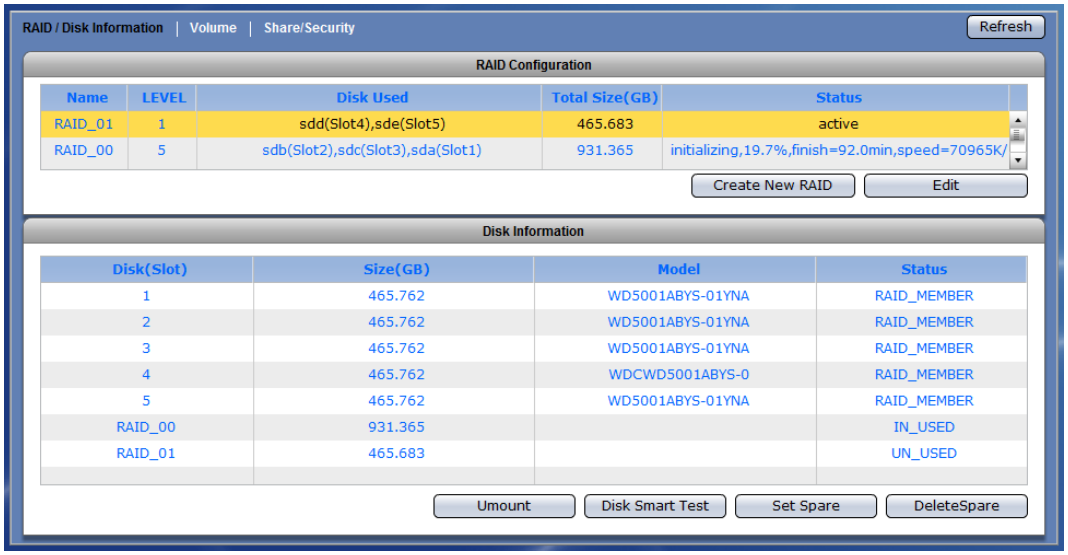
NOTE: Once a RAID disk has been joined to the NASVG Storage Pool, the RAID disk can no longer be deleted. Once joined, the RAID disk status will be shown as “IN_USED” which means the NAS system is already using the RAID disk.
The way to delete existing RAID disks which are already joined to Storage Pool is to reset NAS to factory default in “System” → “Boot/Shutdown” → “Reboot to Default”. WARNING! Using this option will delete all existing RAID configuration and data, and the NAS will be reset to factory default settings.

3.1.1.2 Delete RAID

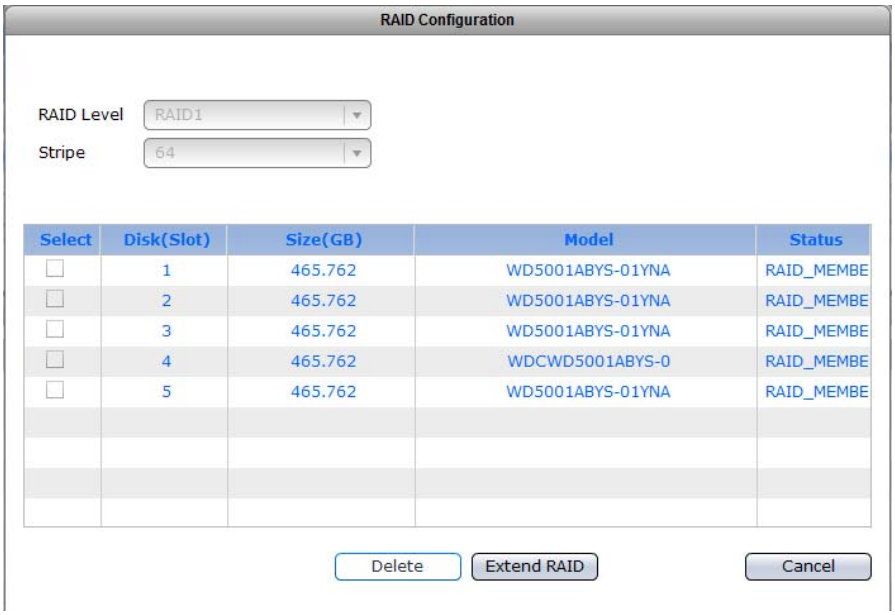
NOTE: Once a RAID disk has been joined to the NASVG Storage Pool, the RAID disk can no longer be deleted. Once joined, the RAID disk status will be shown as "IN_USED" which means the NAS system is already using the RAID disk.
The way to delete existing RAID disks which are already joined to Storage Pool is to reset NAS to factory default in "System" → "Boot/Shutdown" → "Reboot to Default". WARNING! Using this option will delete all existing RAID configuration and data, and the NAS will be reset to factory default settings.

Steps to delete an existing RAID:

1. Select the RAID disk to be deleted. The RAID disk will be highlighted.



2. Click “Edit”. The RAID Configuration window will be displayed.



3. Click “Delete”. A warning message will be displayed.

4. Select “Yes” to confirm deleting selected RAID disk.

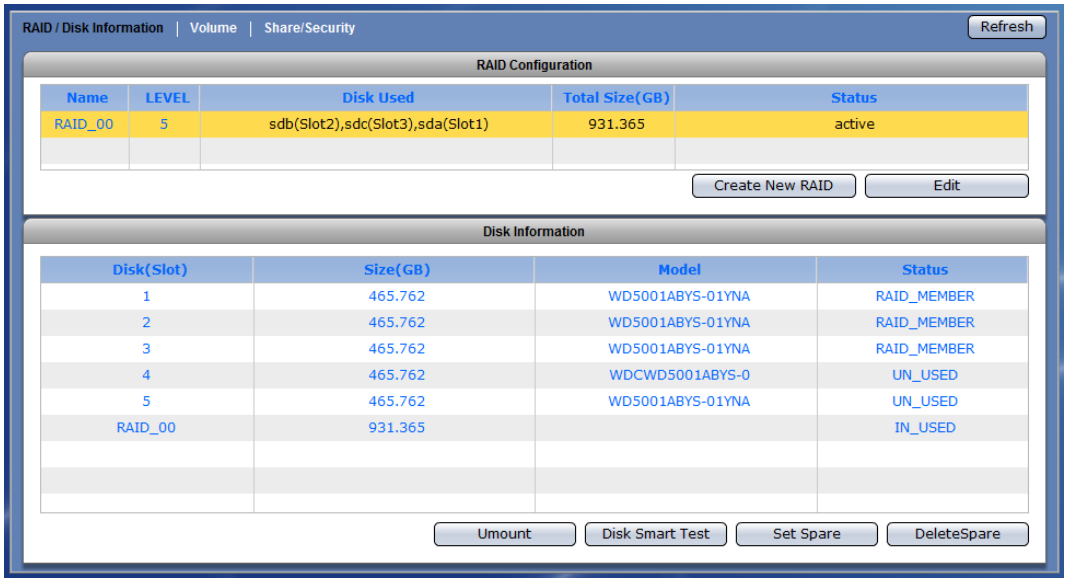
5. The status of the member disks of the deleted RAID will be shown as “UN_USED”.

3.1.1.3 Extend RAID

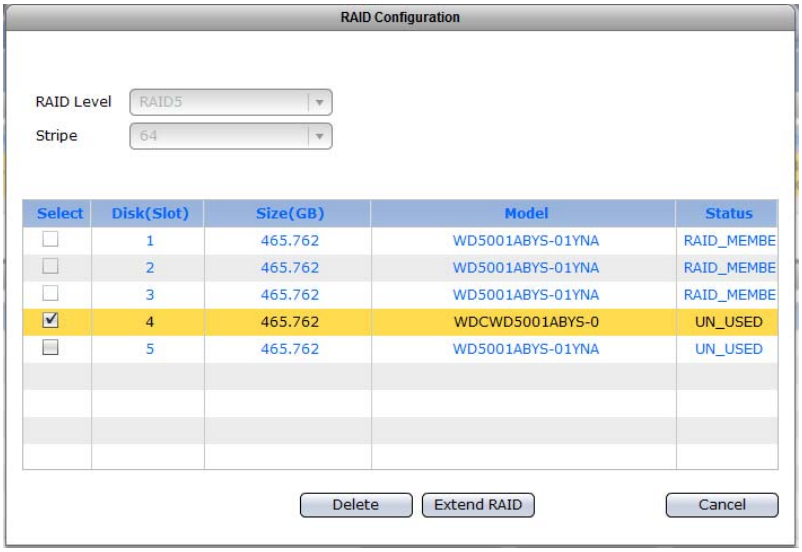
NOTE: A RAID cannot be extended if the RAID is busy, such as when the RAID is in Initializing or Rebuilding state. Wait until the RAID status becomes normal then do the RAID extension.

Steps to add drive(s) or extend an existing RAID:

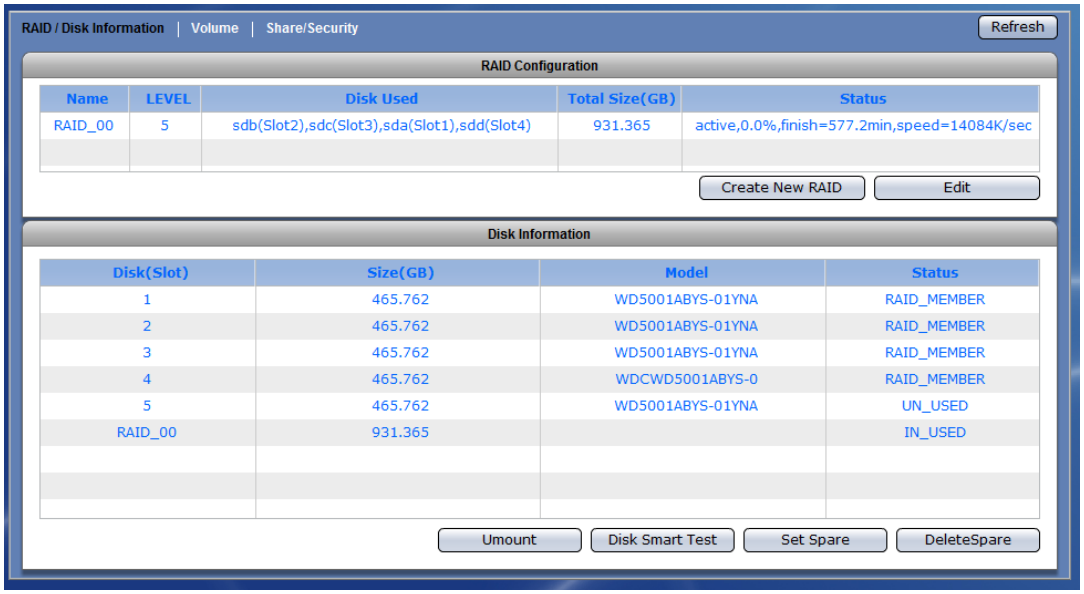
1. Select the RAID disk to be extended. The RAID disk will be highlighted. Click "Edit".



2. The RAID Configuration window will be displayed. Select the disk(s) that will be used for extending the RAID. Click “Extend RAID”.



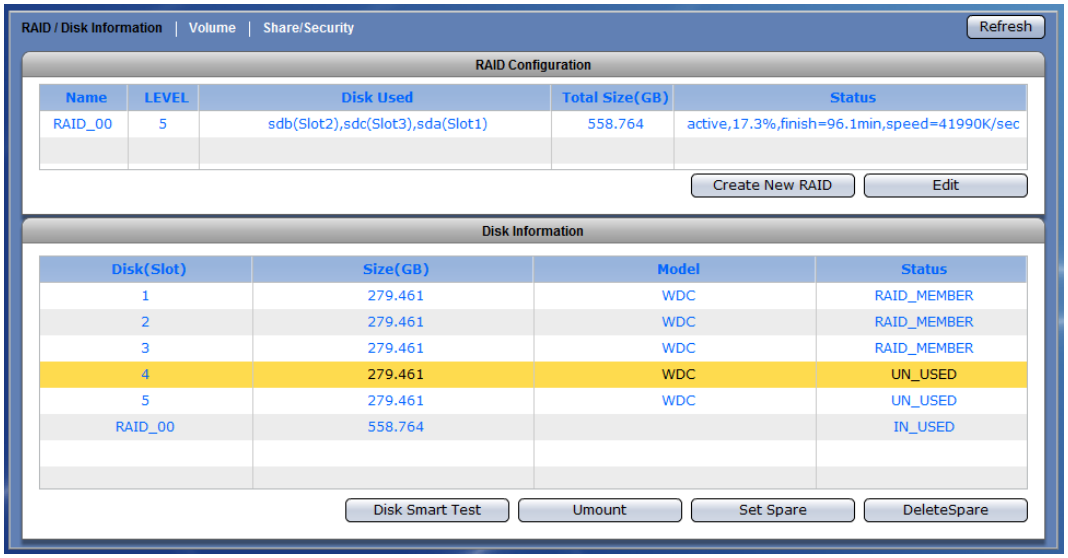
3. The RAID will be extended. The disk that was added to the RAID will now have “RAID_MEMBER” status.



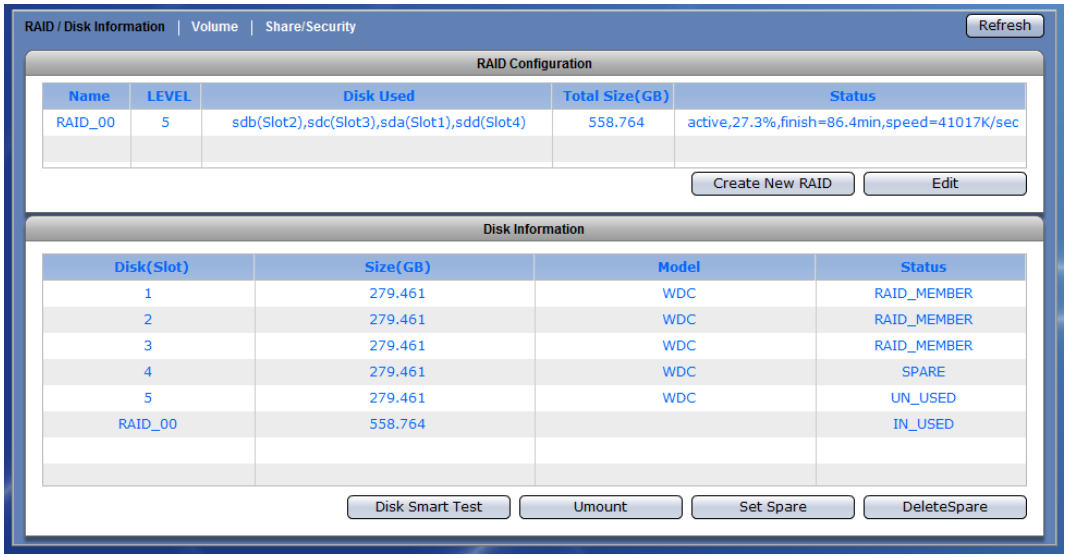
3.1.1.4 Set a Spare Disk

Steps to Set a Spare Disk:

1. Select the hard disk drive to be made a spare disk and click “Set Spare”.

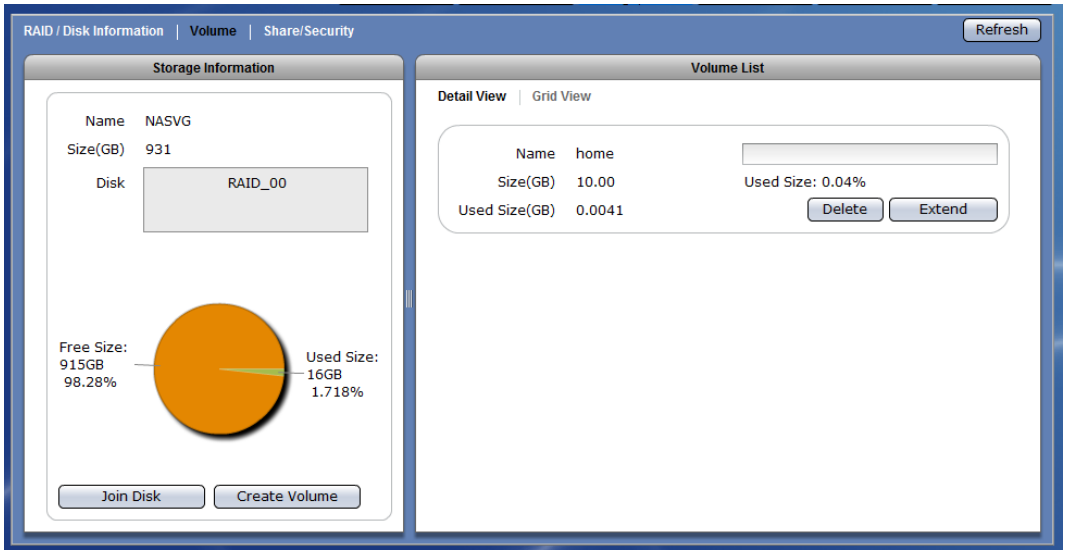


2. The selected hard disk drive will become a Spare Disk. The Status in Disk Information will show “SPARE”.



3.1.2 Volume

Click the Volume tab. The Volume Configuration screen will be displayed.



Storage Information Screen:

Name – The NAS Volume Group default name "NASVG".
Size (GB) – The total capacity of the NASVG
Disk – The list of RAID disk(s) joined to the NASVG.

Storage Information Options:

Join Disk – Used to join a RAID disk to the NASVG.
Create Volume – Used to create a new Volume. A Volume is storage space which is shared by several Share Folders (several Share Folders can be created under a single Volume).

Volume List Screen:

There are two types of view provided to display the Volume information: Detail View and Grid View.

Detail View: has Delete, Extend, and iSCSI buttons

Name – The Volume name.
Size (GB) – The total Volume capacity in GB.
Used (GB) – The Volume used capacity in GB.
Used Size – The Volume used capacity as a percentage of the total Volume capacity.

Grid View: displays Volume List in table format

Name – The Volume name.
Size (GB) – The total Volume capacity in GB.
Used Size (GB) – The Volume used capacity in GB.

Volume List Options:

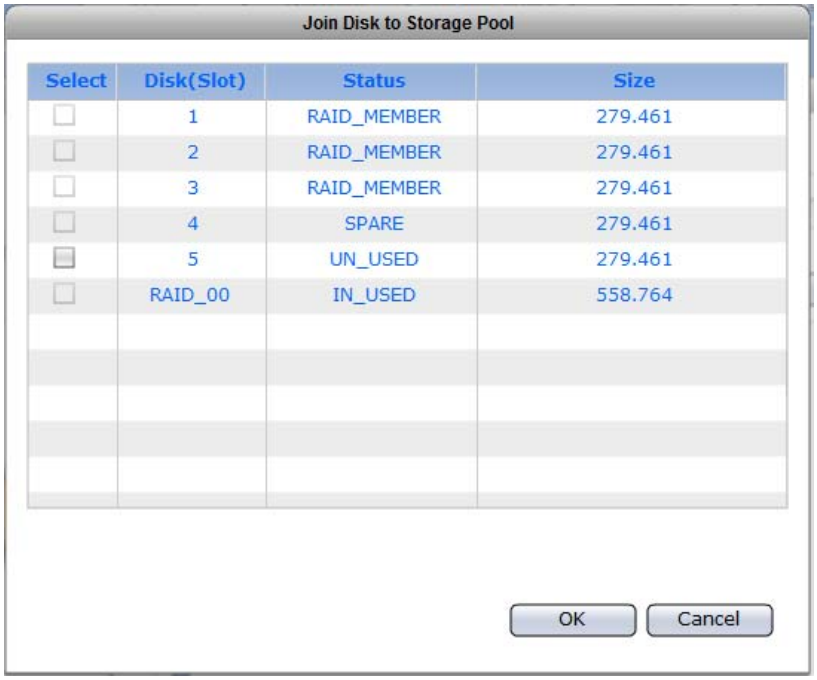
Delete – Used to erase the Volume.
Extend – Used to extend the total Volume capacity.
iSCSI – Used to setup the Volume as iSCSI target.

3.1.2.1 Join a Disk to Storage Pool

Steps to Join a Disk to Storage Pool:

1. Click “Join Disk”.
2. A dialog box will be displayed. Select a RAID logical disk (an unused/newly created RAID disk) to be joined to the Storage Pool of NASVG. Click “OK” when done.

NOTE: If a new (UN_USED) RAID logical disk has not been created yet, create first the RAID disk using the available free physical disk drives.



3. The RAID logical disk will be joined to the NASVG.

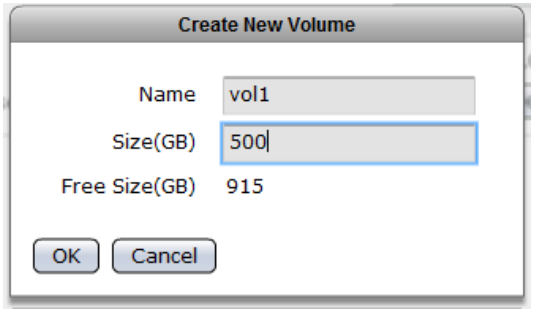
NOTE: An un-used physical disk drive can be used to join to the Storage Pool of NASVG but it is not recommended because the physical disk drive does not have RAID Level nor provide data redundancy. Select only a RAID disk to add into the Storage Pool for better data security.

3.1.2.2 Create a Volume

Steps to Create a Volume:

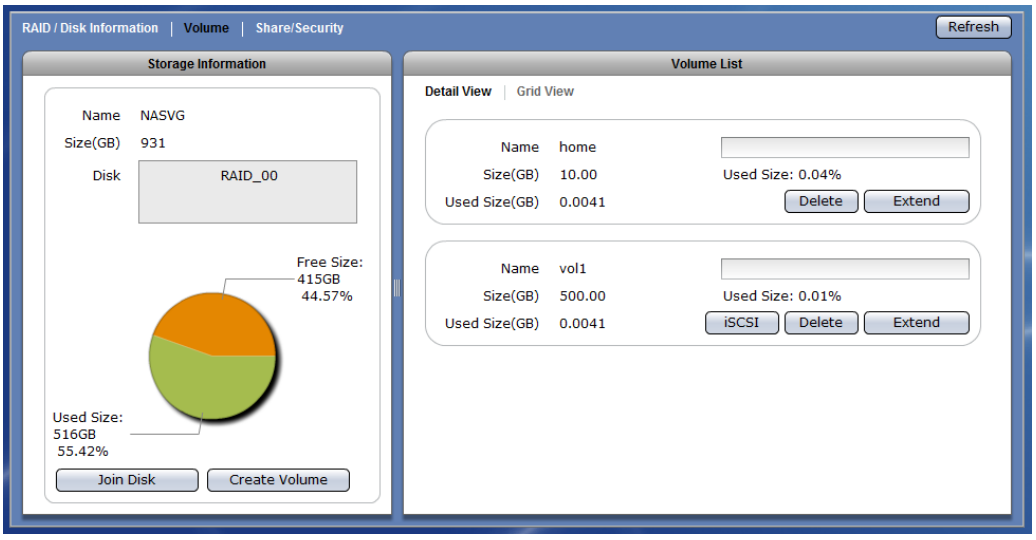
1. Click “Create Volume”.
2. In the Create New Volume dialog box, enter the Volume Name and Size in GB. The Free NASVG capacity will show the available capacity that can be used. Click “OK” when done.

NOTE: The volume name does not allow space in-between characters. Valid characters are A-Z, a-z, and 0-9.



3. A message will be displayed.

4. The new Volume will be created.



3.1.2.3 Delete a Volume

Steps to Delete a Volume:

WARNING! Be careful when using this function. Make sure the data in the volume and all its share folders are no longer needed or a backup has been made before deleting the volume.

1. Click the “Delete” button of the Volume to be deleted.
2. A warning message will be displayed. Click “Yes” to proceed with deletion.

3. A message window will be displayed.

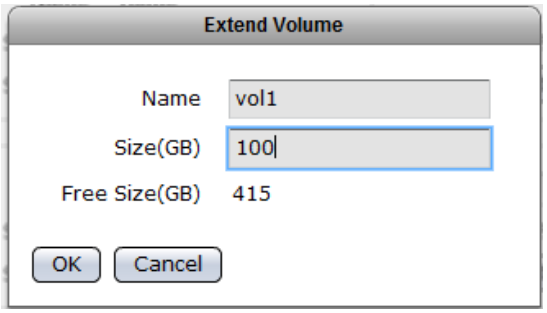
4. The Volume will be deleted.

3.1.2.4 Extend a Volume Capacity

NOTE: The capacity of a Volume can be extended many times as long as there is available free space in the NASVG.

Steps to Extend a Volume:

1. Click the “Extend” button of the Volume to be extended.
2. A dialog box will be displayed. Enter the additional capacity that will be added to the Volume in the “Size(GB)” box. Click “OK” when done.



3. A message will be displayed.

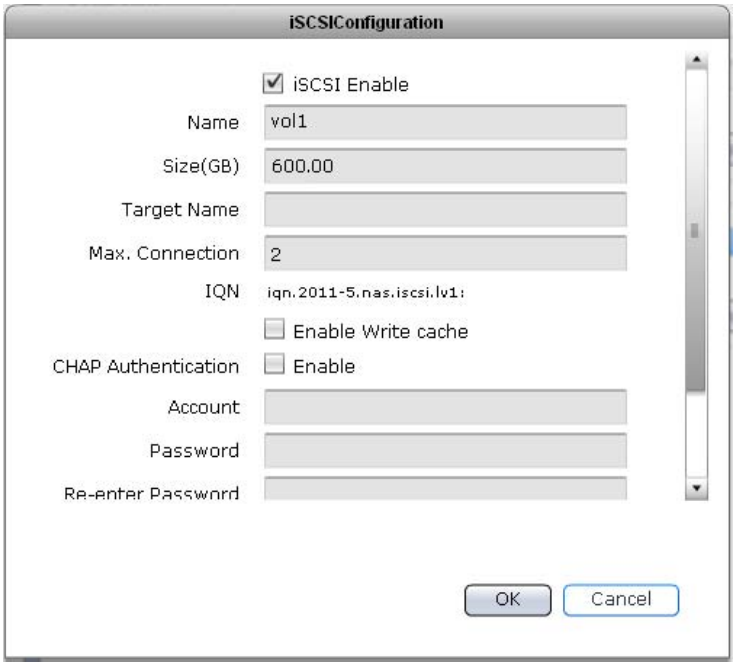
4. The total Volume capacity will be increased.

3.1.2.5 Setup Volume as iSCSI Target

Steps to Setup Volume as iSCSI Target:

1. Click the “iSCSI” button of the Volume to be setup.

2. A dialog box will be displayed. Tick the “iSCSI Enable” option to enable iSCSI function. Enter the Target name. To enable authentication, tick the “Enable” box in Authentication then enter an Account name. Enter the password in Password box and Password Confirm box. To enable iSCSI MPIO, set Max Connection to 2. Click “OK” when done.



NOTE: When Authentication is used, the same Account and Password must also be used in iSCSI initiator to successfully connect to the NAS iSCSI target device. Password length must be 12 to 16 characters.

NOTE: By default, the iSCSI Volume (LUN) write cache option is disabled. To enable write cache on iSCSI target LUN, tick the “Enable Write Cache” option.

NOTE: Max Connections is the number of separate connections per initiator on the target iSCSI Volume. This is useful when setting MPIO on iSCSI initiator.

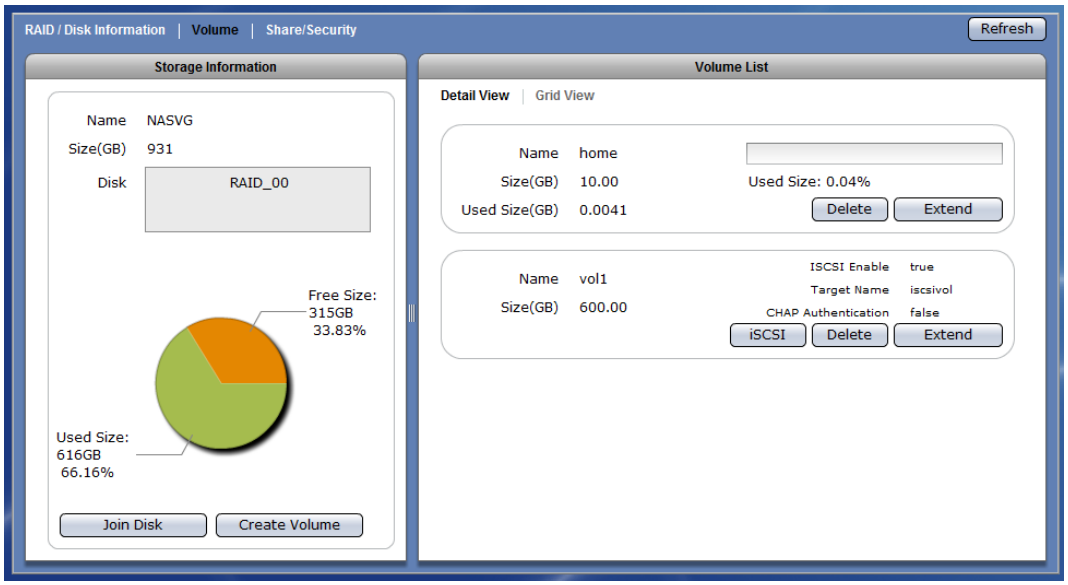
3. A warning message will be displayed. Select “Yes” to proceed.

4. Another warning message will be displayed. Select “Yes” to proceed.

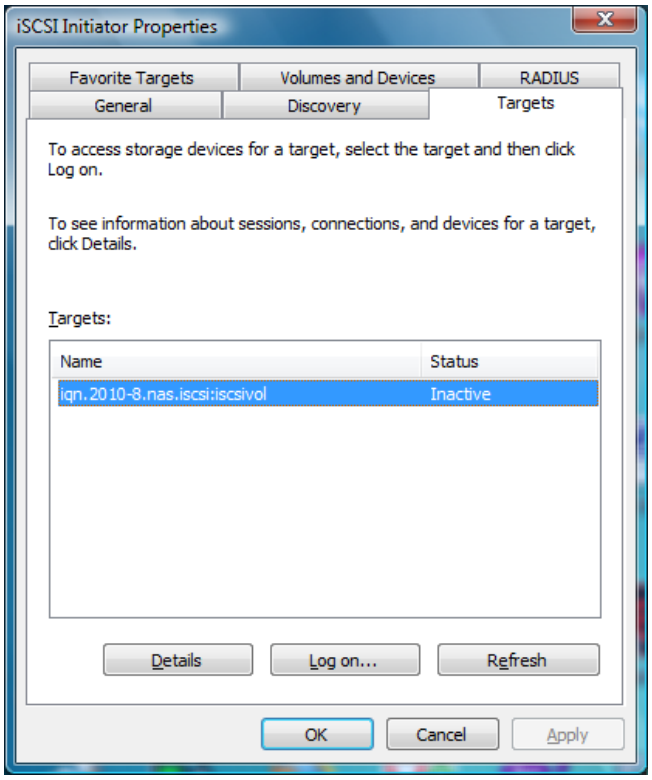
NOTE: Make sure the volume does not contain important data in its share folders. Select “Yes” in this step will confirm formatting the volume for iSCSI use, all data in this volume will be deleted.

5. A message will be displayed.

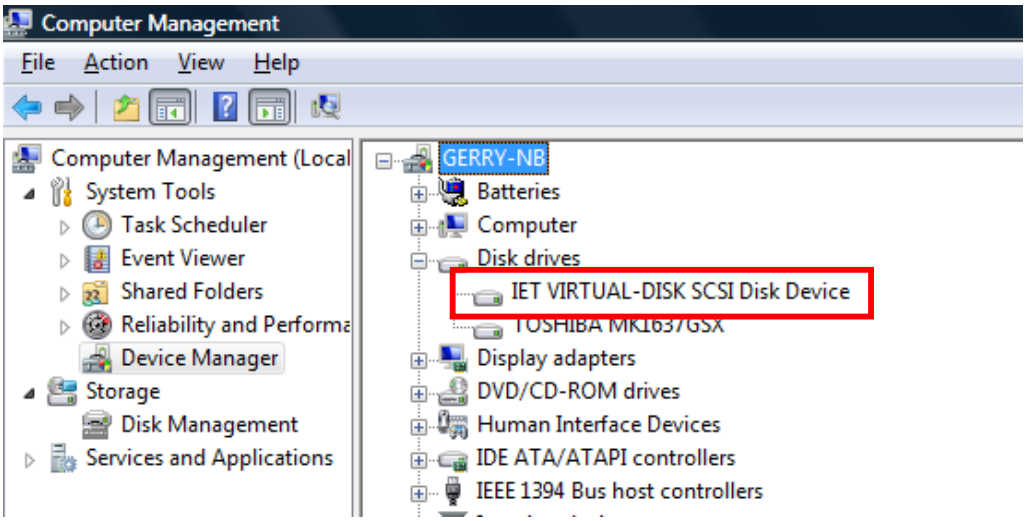
6. The Volume iSCSI function is ready.



7. Connect to iSCSI Target Volume from host computer with iSCSI Initiator. Log on to target device. Use the account and password if set in iSCSI Configuration.



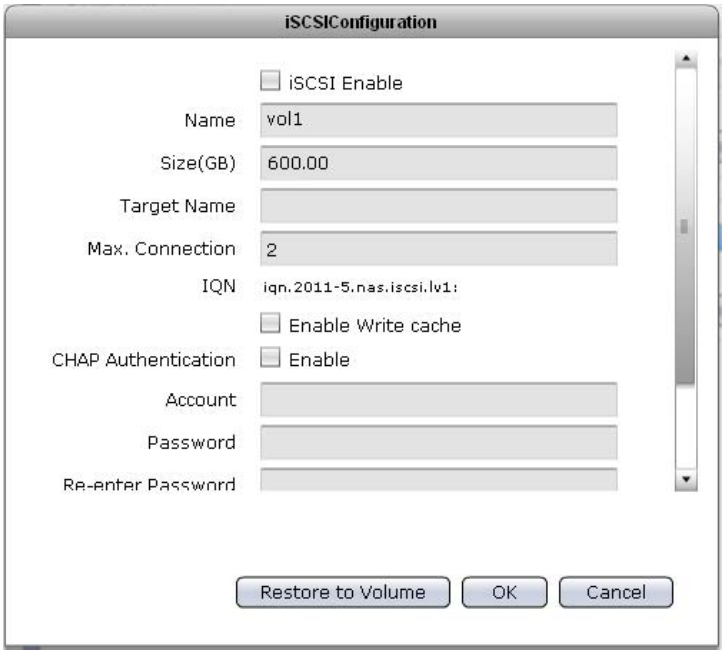
8. After successful connection, the iSCSI device will be shown in Disk Drives list.



3.1.2.6 Disable iSCSI Configuration in a Volume

Steps to Disable the iSCSI Configuration in a Volume:

1. Select the Volume with iSCSI Configuration and click the “iSCSI” button. Remove the check mark on the “iSCSI Enable” box. Click “OK” when done.



2. A warning message will be displayed. Select “Yes” to proceed.

3. A message will be displayed.

4. The iSCSI function of the Volume will be disabled.

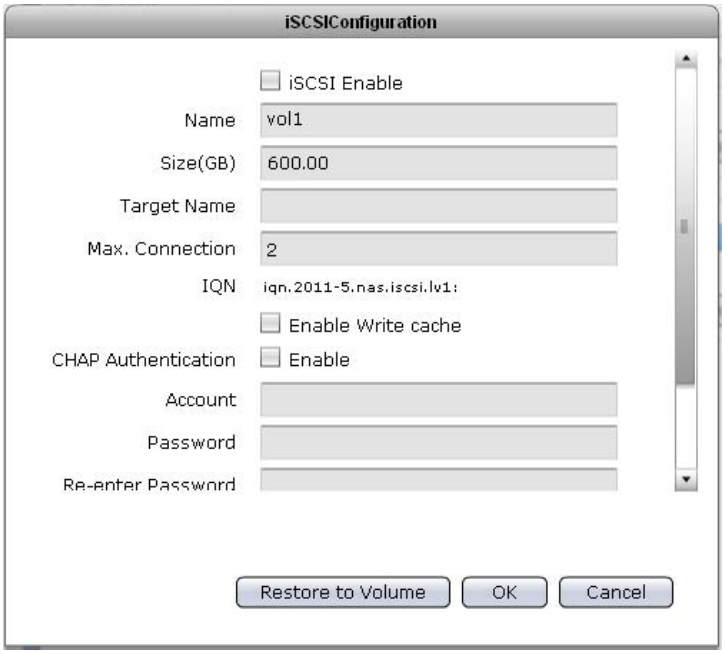
3.1.2.7 Remove iSCSI Configuration and Restore to NAS Volume

Steps to Remove iSCSI Configuration and Restore to NAS Volume:

WARNING: When iSCSI Configuration is removed and volume is restored as basic NAS volume, all the data in the volume previously configured as iSCSI Target are deleted.

NOTE: The iSCSI Configuration must be disabled first before the Volume can be restored as basic NAS volume. See previous Section on how to disable iSCSI configuration.

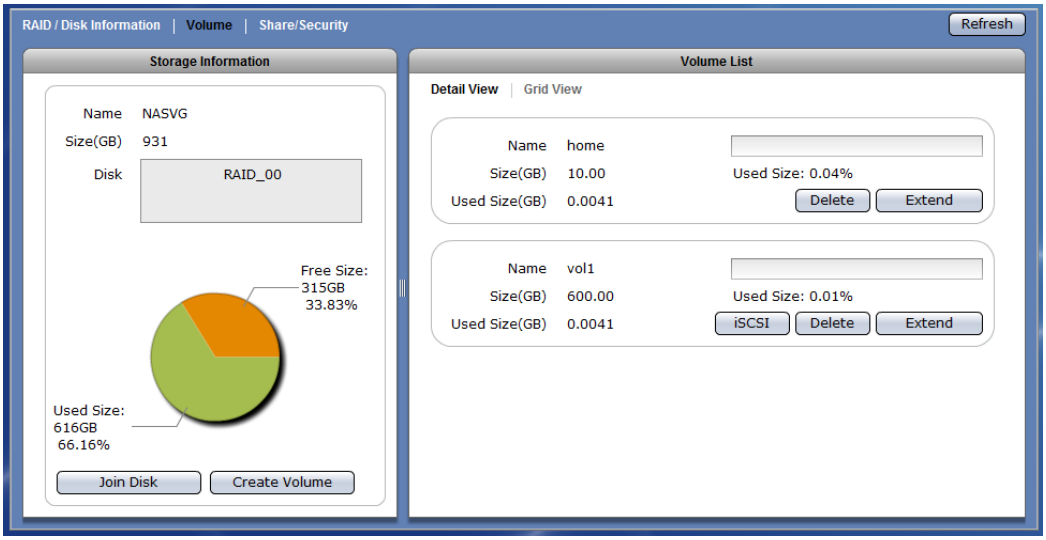
1. Select the Volume with iSCSI Configuration and click the “iSCSI” button. Click the “Restore to Volume” button.



2. A warning message will be displayed.

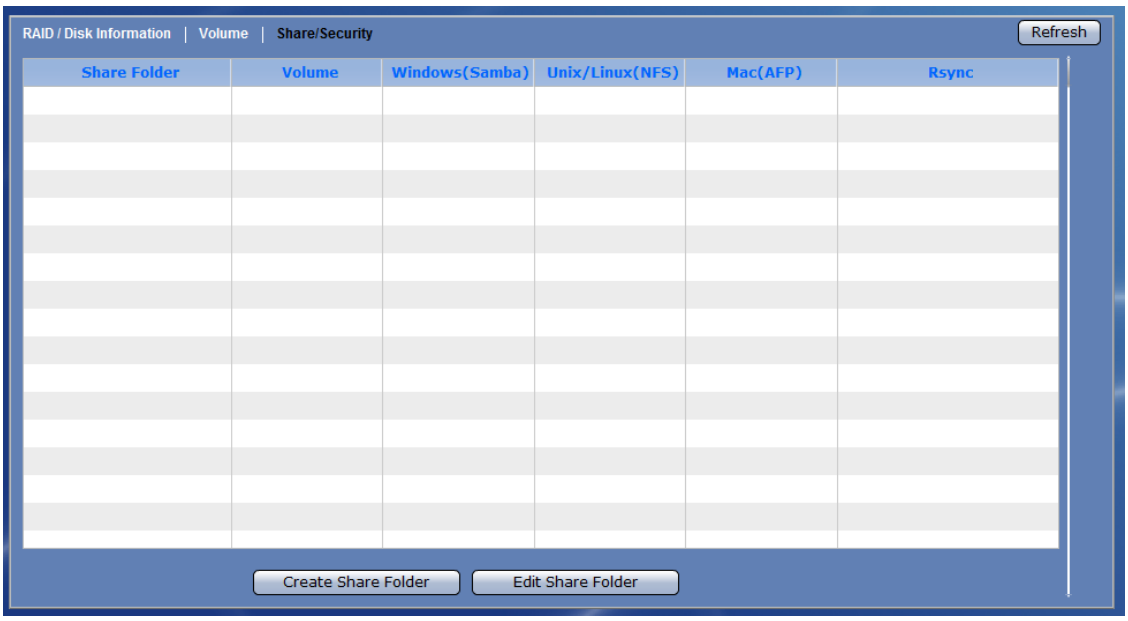
3. A message will be displayed.

4. The iSCSI Configuration will be removed and the volume is restored as basic NAS volume.



3.1.3 Share/Security

Click the Share/Security tab. The Share and Security Configuration window will be displayed. In this window, you can configure the protocol settings as well as assign share access permission.



Share/Security Information Screen:

Share Folder – Displays the share folder name.
Volume – Shows the volume name where the share was created.
Windows (Samba) – Shows the status if Samba / CIFS protocol is enabled (Yes) or not (No) in the share folder.
UNIX/Linux (NFS) – Shows the status if NFS protocol is enabled (Yes) or not (No) in the share folder.
Mac (AFP) – Shows the status if AppleTalk protocol is enabled (Yes) or not (No) in the share folder.
Rsync – Shows the status if Rsync is enabled (Yes) or not (No) in the share folder.

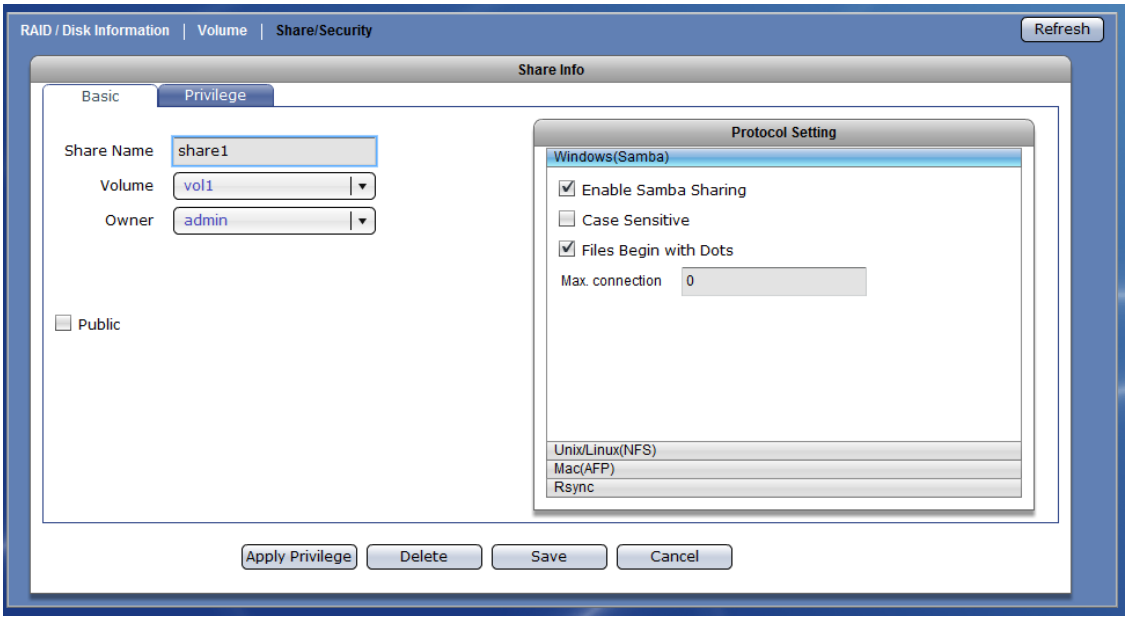
Share/Security Options:

Create Share Folder – Used to create a new share folder.
Edit Share Folder – Used to edit settings of an existing share folder.
Refresh – Used to update the information displayed in the screen.

3.1.3.1 Create New Share Folder

Steps to Create New Share Folder:

1. Click “Create Share Folder”.
2. The Share Folder Basic Configuration screen will be displayed. Configure the necessary options.



Share Configuration Options:

Share Name – Enter the share folder name.

NOTE: The share folder name does not allow space in-between characters.
NOTE: If the share folder is designated as WEB target share folder, do not enable “Public” option.

Volume – Select the Volume where the share folder will be created.
Owner – Set the owner of the share folder. By default, admin owns all share folders.
Public – When enabled (checked), the share folder is accessible to all users.

Share Configuration Buttons:

Apply Privilege – Use this to propagate the ACL from the parent share folder (the share name created in this GUI) into its child directories or sub-directories (sub-folders) and files. For example, if user1 has read/write permission on a sub-directory but read-only on the main share folder, after applying privilege, user1 will now have a read-only permission on the sub-directory.
Delete – Use this to delete the share folder.
Save – Use this to save changes made.
Cancel – Use this to undo changes made.

3. In the Protocol Setting window, setup the Windows (Samba) protocol options.

Windows (Samba) Configuration Options:

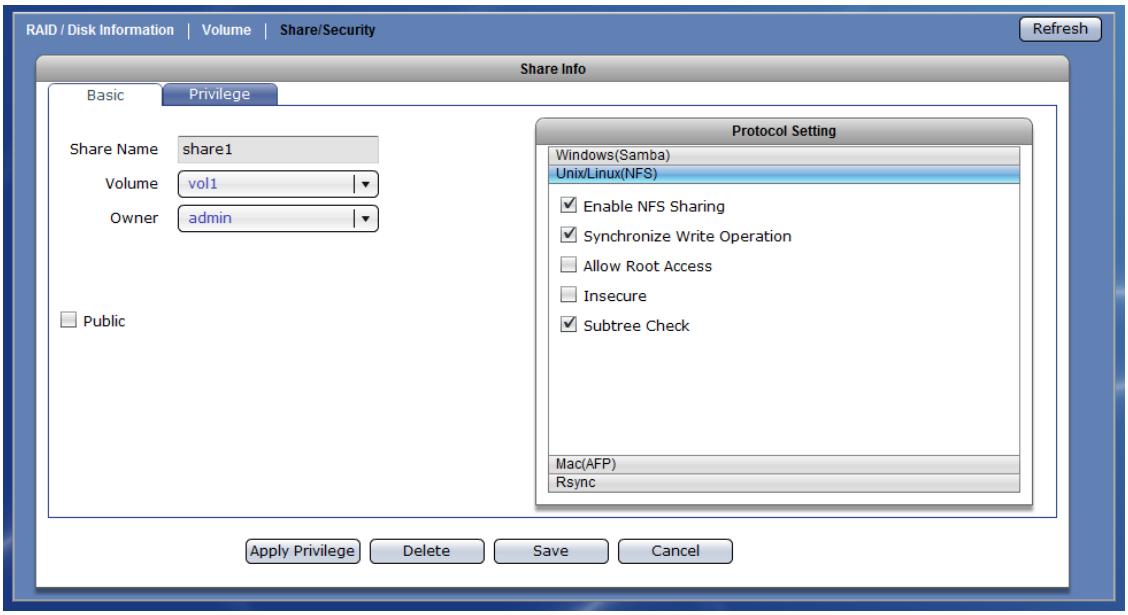
Enable Samba Sharing – Used to enable Samba protocol. When checked, the share folder can be accessed via Samba protocol.

Case Sensitive – This controls whether filenames are case sensitive or not. Default is disabled.

Files Begin with Dots – This controls whether files that begin with a dot will become hidden files. Default is disabled.

Max connection - This option limits the number of simultaneous connections at a certain time. A value of zero (default) means an unlimited number of connections will be possible in this share.

4. Select "Unix/Linux(NFS)" option in Protocol Setting window. The NFS protocol configuration screen is displayed. If share will be accessed by UNIX/Linux clients, setup the necessary options.



Unix/Linux (NFS) Configuration Options:

Enable NFS Sharing – Used to enable or disable NFS protocol. When enabled (checked), the share folder can be accessed via NFS protocol.

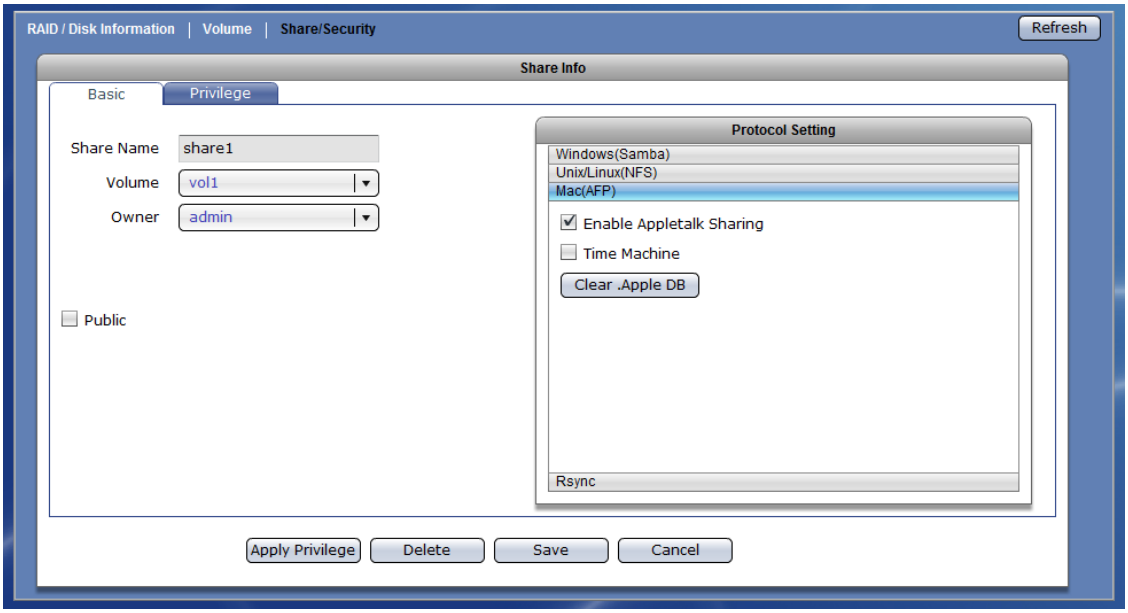
Synchronize Write Operation - Use this option to enable or disable write caching.

Allow Root Access – Use this option to allow or disallow access by root super-user account.

Insecure - This option provides higher security. If this option is enabled, only the ports under 1024 are allowed access to the share folder.

Subtree Check - Use this option to enable or disable subtree checking. A subtree check happens if a subdirectory of a filesystem is exported but the whole filesystem isn't, then whenever a NFS request arrives the server must check not only that the accessed file is in the appropriate filesystem (which is easy) but also that it is in the exported tree (which is harder).

5. Select “Mac(AFP)” option in Protocol Setting window. The AppleTalk protocol configuration screen is displayed. If share will be accessed by Mac clients, setup the necessary options.



Mac (AFP) Configuration Options:

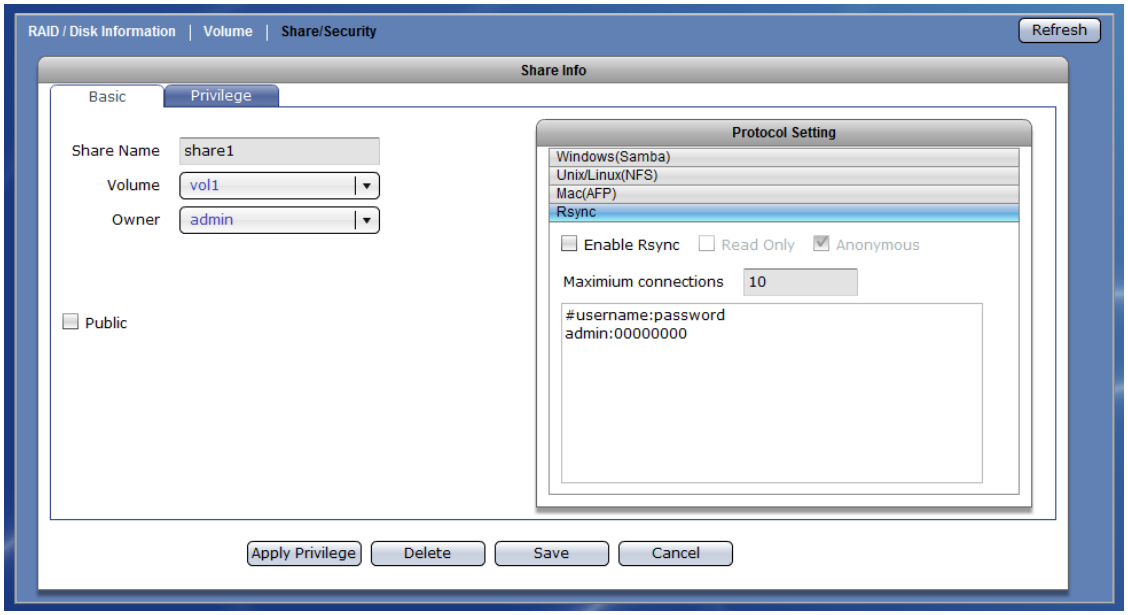
Enable AppleTalk Sharing – Used to enable or disable AppleTalk protocol. When enabled, the share folder can be accessed via AppleTalk protocol.

Note that newer Mac OS X versions support SMB protocol, and therefore will be able to connect to NAS share folder using SMB protocol, without enabling “Mac (AFP)”.

Time Machine – Used this option to enable Time Machine function on the share folder. The NAS share folder will become Time Machine backup target destination.

Clear .AppleDB – Use this button to delete the .AppleDB hidden folder (including all files in it) on the share folder.

6. Select “Rsync” option in Protocol Setting window. The Rsync configuration screen is displayed. If share will be used for Rsync, setup the necessary options.



Rsync Configuration Options:

Enable Rsync – Used to enable or disable Rsync Server function on this share folder. When enabled (checked), an Rsync client can connect to this share folder and upload or download files via Rsync.

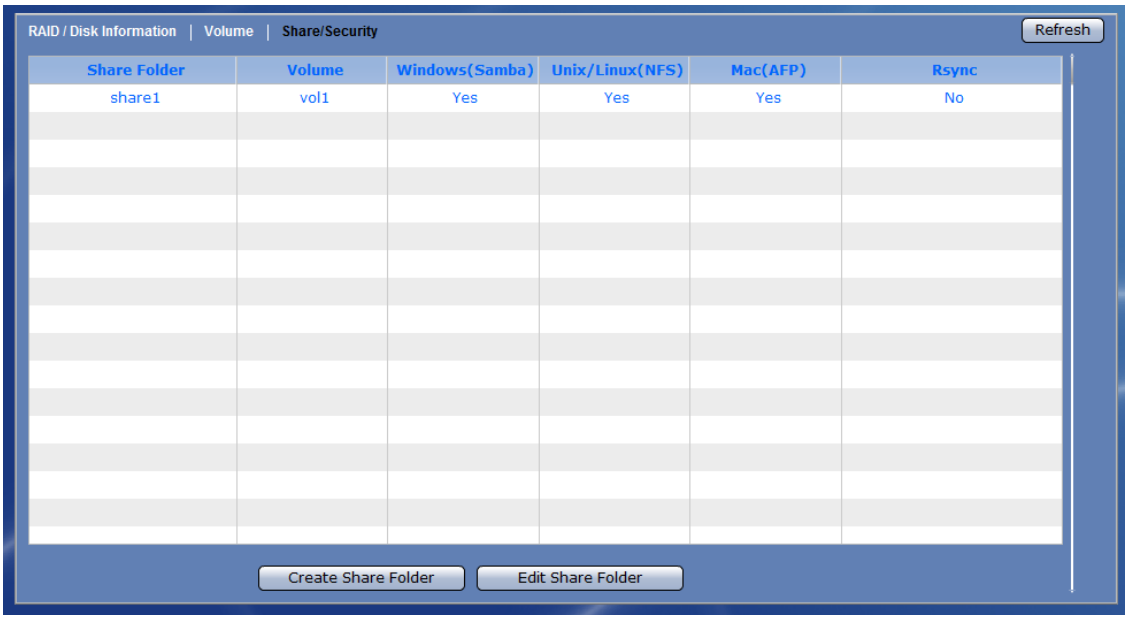
Read Only - When checked, all files within this share will be read only to any Rsync client.

Anonymous – When checked, anonymous connections will be accepted.

Maximum connections - This specifies the maximum number of Rsync client that can connect to this share at a certain time.

#username:password – Use this option to edit Rsync account and password list. These accounts are the accounts that will be supplied by the Rsync client when connecting to this server.

7. Click “Save” when done. Then Share Folder will be created.



3.1.3.2 Assign Permission to Share

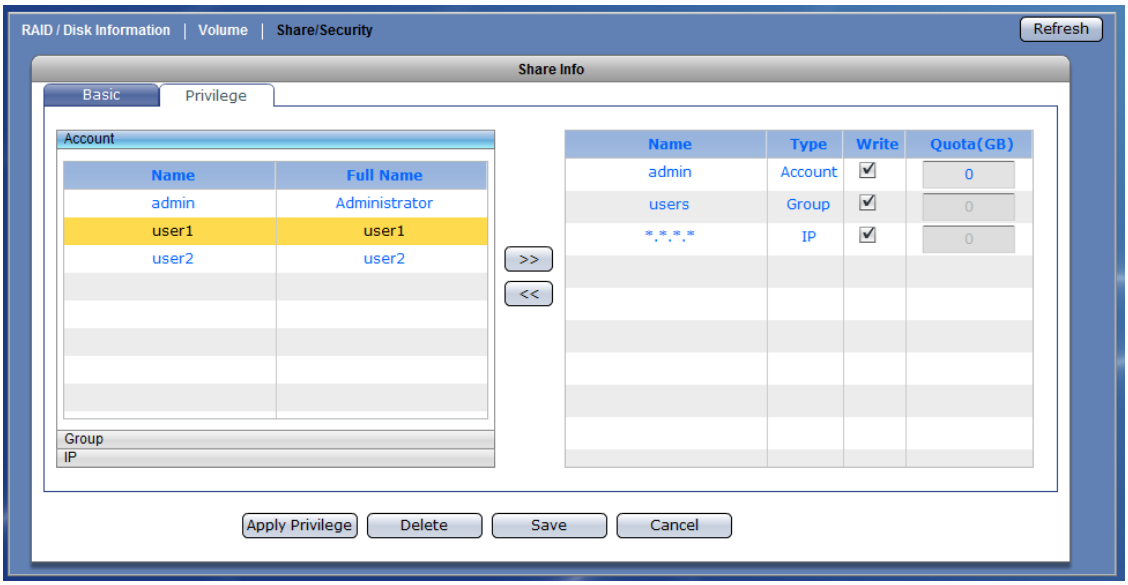
Steps to Assign User or Group Account Permission to the Share Folder:

NOTE: User or Group Accounts must have been created or NAS must have been joined to Windows AD or NIS domain.

1. Select (highlight) the share folder then click “Edit Share Folder”, or double-click the share folder name.

2. Select the Privilege tab. In the Account option, select the user accounts that will be given access permission to the share folder, then click “>>”.The accounts will appear on the right screen. Set the Write and Quota(GB) options as needed.

NOTE: Use the “<<” to remove an account from share folder privilege. Select the account then click “<<”. The account will be removed from the right column. By default, admin account and users group (group account for local NAS users) have permission to a share folder.



Account Privilege Options:

Write – By default, this option is checked and the account is given Read and Write permission to the share folder. To assign Read-Only permission, remove the check mark.

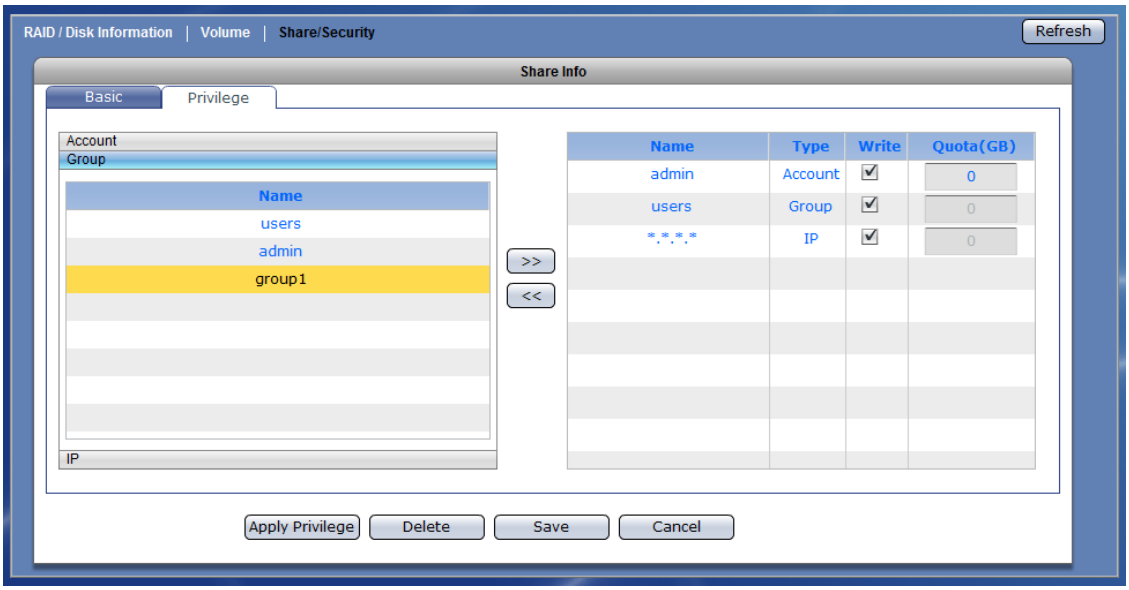
Quota(GB) – This option is used to assign user account quota to the share folder. Default is zero which means no limit (limit is volume capacity).

NOTE: The Account quota set in Privilege section of Share folder applies only to the share folder itself. Other share folders can have different account quota. Also, this quota is different from the user account’s home folder.

3. Click the Group option. Select the groups that will be given access permission to the share folder, then click “>>”.The groups will appear on the right screen. Set the Write and Quota(GB) options as needed.

NOTE: Use the “<<” to remove a group from share folder privilege. Select the group then click “<<”. The group will be removed from the right column.

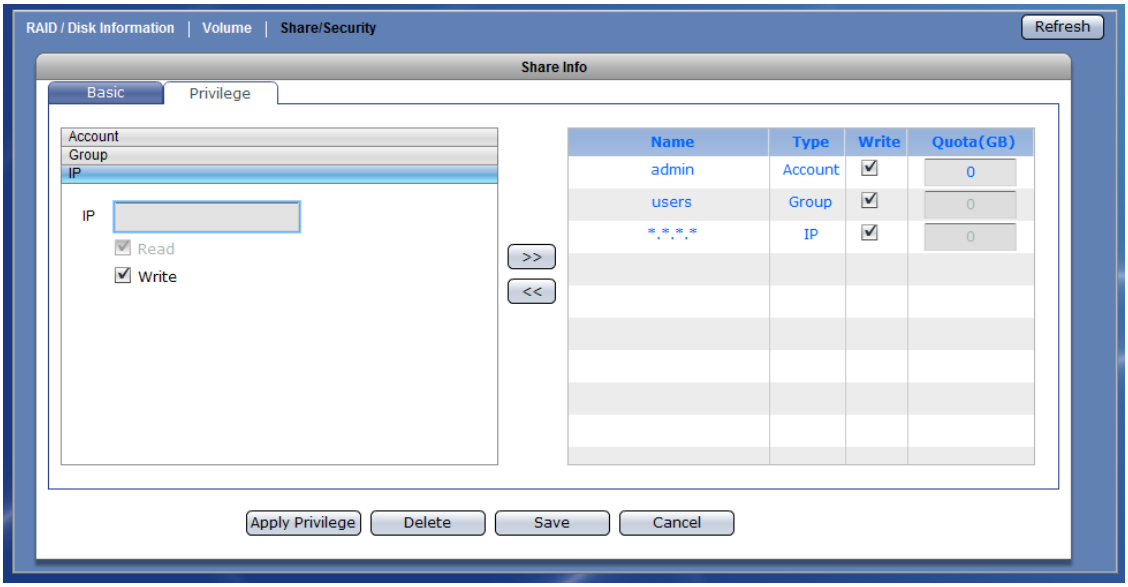
NOTE: By default, all local NAS accounts belong to “users” group and have share read/write access permission.



Group Privilege Options:

Write – By default, this option is checked and the group is given Read and Write permission to the share folder. To assign Read-Only permission, remove the check mark.

4. Click the IP option. Set up the IP address or addresses that will be allowed connections to the share folder, then click “>>”.The IP address will appear on the right screen.



NOTE: This option allows setting certain range of hosts to have an access to the NAS. By default, NAS will accept connections from any host (*.*.*.*). To allow connections only from certain IP address, remove *.*.*.* then add the IP address/range. For example, add 192.168.100.*. This will only allow connections from your private network 192.168.100 and all other connection will be refused.

NOTE: To remove an IP address from share folder privilege, select the IP address then click “<<”.

IP Privilege Setup Options:

Read – This option allows Read access from the specified IP address or address range.

Write –This option allows Write access from the specified IP address or address range.

IP Privilege Edit Option:

Write – By default, this option is checked and the IP address or range of IP address is given Read and Write permission to the share folder. To assign Read-Only permission, remove the check mark.

5. Click “Save” when done. The permissions will be set in the share folder.

3.1.3.3 Edit Share Folder

Steps to Edit Share Folder:

1. Select the share folder name then click “Edit Share Folder”.
2. Change the necessary options. Click “Save” when done.

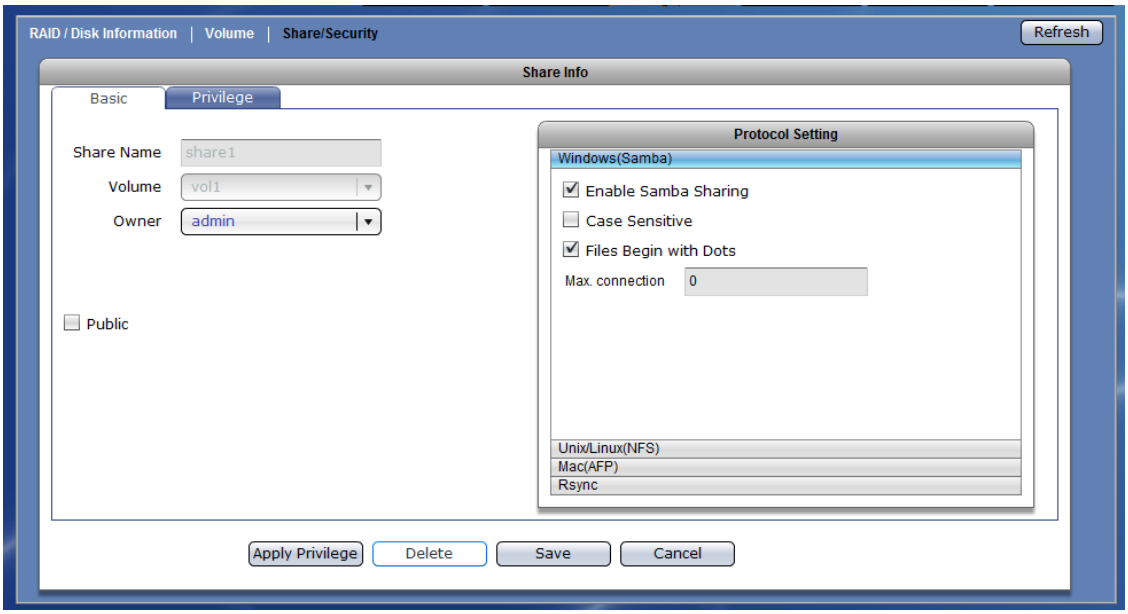
NOTE: The Share Name cannot be modified.

NOTE: If you want the same share folder privilege / permission to be propagated to existing sub-folders and files under the share folder, use the “Apply Privilege” button. A warning message will be displayed. Select “Yes” to confirm.

3.1.3.4 Delete Share Folder

Steps to Delete Share Folder:

1. Select the share folder name then click “Edit Share Folder”. Click “Delete”.



2. A warning message will be displayed. Select “Yes” to proceed. The share folder will be deleted.

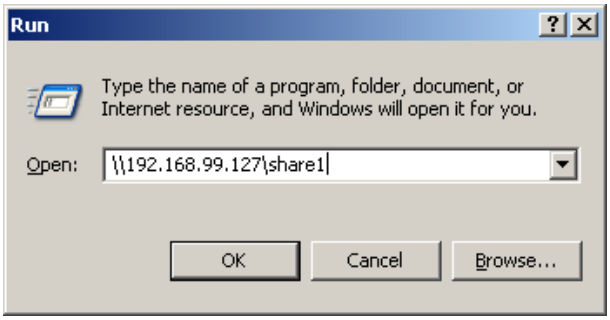
WARNING! Be careful when using the “Delete” button. Make sure your data in the share is no longer needed or a backup has been made before deleting the share folder.

3.1.3.5 Accessing Share Folder from Windows Clients via Samba

NOTE: Make sure Samba service is enabled in System → Service, and Samba protocol is enabled in Storage / Share → Share / Security → Share → Protocol Setting → Windows(Samba).
Make sure the account that will be used to login the share folder has permission or already added in Storage / Share → Share / Security → Share → Privilege. By default, all local NAS accounts, which belong to "users" group, have read / write permission to share folders.

1. To access the share folder from Windows client PC, click "Start" then "Run". Enter in the Open input box as follows: \\x.x.x.x\share-name, where x.x.x.x is the NAS IP.

   For example: \\192.168.99.127\share1

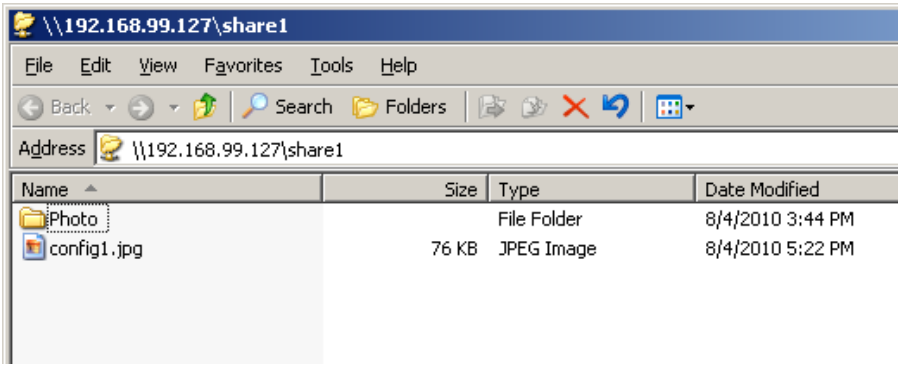


   NOTE: You can also use the NAS host name, if DNS is setup in Network → Device Configuration and in DNS server (NAS host name is added).

2. Enter the login account and password. If login account is a Windows domain account, use the domain name followed by account name, such as Domain-name\Account-name. For example: testdom\user1

NOTE: If NAS is not joined to Windows domain and you will use a NAS local account, enter only the NAS account name and password.

3. Login to share is successful.



3.1.3.6 Accessing Share Folder from Linux/UNIX Clients via NFS

NOTE: Make sure NFS service is enabled in System → Service, and NFS protocol is enabled in Storage/Share → Share/Security → Share → Protocol Setting → Unix/Linux(NFS).

1. Login to console of Linux client. Change to root user, if necessary.

2. To check which share folders of NAS are accessible via NFS protocol and which path will be used for mounting, use the command "showmount –e x.x.x.x", where x.x.x.x is the NAS IP.

   For example: showmount –e 192.168.99.127

```
bash-3.00# showmount -e 192.168.99.127
Export list for 192.168.99.127:
/mnt/NAS/home         *
/mnt/NAS/vol1/share1 *.*.*.*
bash-3.00#
```

3. Create local mount point, if not yet created.

```
-bash-3.00# mkdir /nfstest
-bash-3.00#
```

4. Mount the share folder via NFS.

   The format for the mount command is:
   mount -t nfs x.x.x.x:/mnt/NAS/volume/share /local-mount-point

   x.x.x.x is the NAS IP.
   Note that /mnt/NAS/volume-name/share-name is the complete path to NFS share as shown using the showmount command (step 2).

   For example: **mount –t nfs 192.168.99.127:/mnt/NAS/vol1/share1 /nfstest**

```
bash-3.00# mount -t nfs 192.168.99.127:/mnt/NAS/vol1/share1 /nfstest
bash-3.00#
```

5. The share folder is mounted via NFS protocol. To check, use “mount” or “df –h” command.

mount

```
192.168.99.127:/mnt/NAS/vol1/share1 on /nfstest type nfs (rw,addr=192.168.99.127)
bash-3.00#
```

df -h

```
192.168.99.127:/mnt/NAS/vol1/share1
                      600G  4.3M  600G   1% /nfstest
bash-3.00#
```

3.1.3.7 Accessing Share Folder from Mac Clients

NOTE: By default, new Mac OS versions such as 10.4.x or later versions, support SMB protocol.

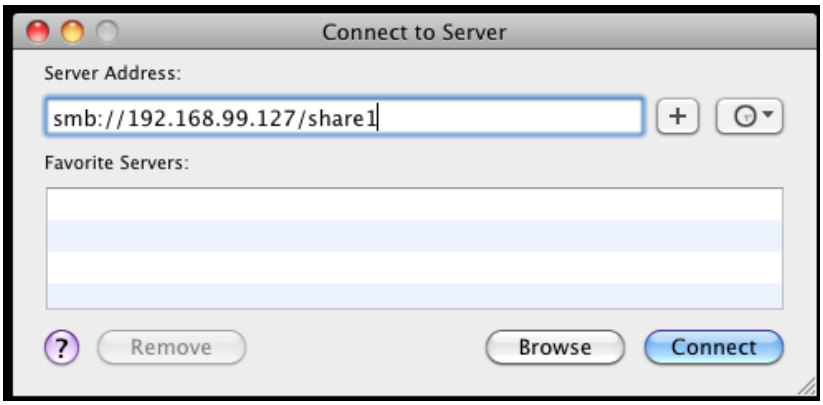
If Mac OS is older version, such as Mac OS 9, and will use AFP protocol to connect, the AFP protocol must be enabled in System → Service. Enable also Mac(AFP) in Storage/Share → Share/Security → Share → Protocol Setting.

Make sure the account that will be used to login the share folder has permission (already added in Storage/Share → Share/Security → Share → Privilege).

1. To connect to share folder via SMB protocol, in the Finder, select “Connect to Server” from the Go menu. The Connect to Server dialog box will be displayed.

2. In Server Address box, enter the path to the NAS share. Use the format: smb://x.x.x.x/share-name or smb://NAS-host-name/share-name.

   For example: **smb://192.168.99.127/share1**



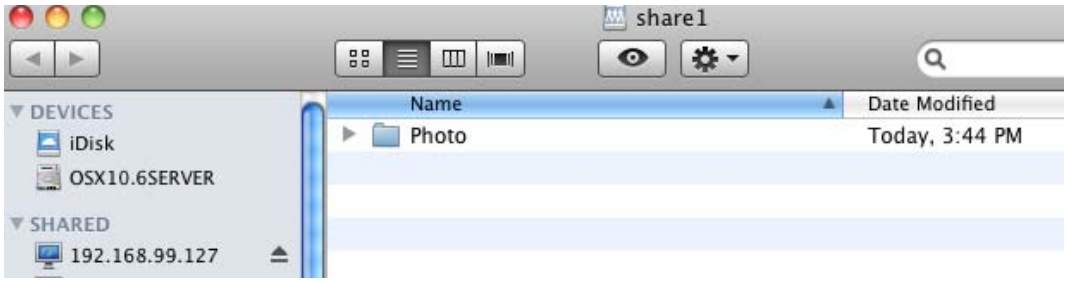
NOTE: You can also use the NAS host name instead of IP address, if DNS setting is configured in NAS → Network → Device Configuration, in Mac OS, and in DNS server.

If you enabled AFP service and Mac(AFP) Protocol Setting, and wanted to connect to NAS share folder via AFP, use the format: afp://x.x.x.x/share-name.
For example: afp://192.168.99.127/share1

3. Click the “Connect” button. The OS X system will contact the NAS, and display the SMB/CIFS File System Authentication screen.

4. Enter the Workgroup or Domain name, if there is (and if required), and a valid user name (for example: NAS local account) with permission to the share folder, and the password for the user name.

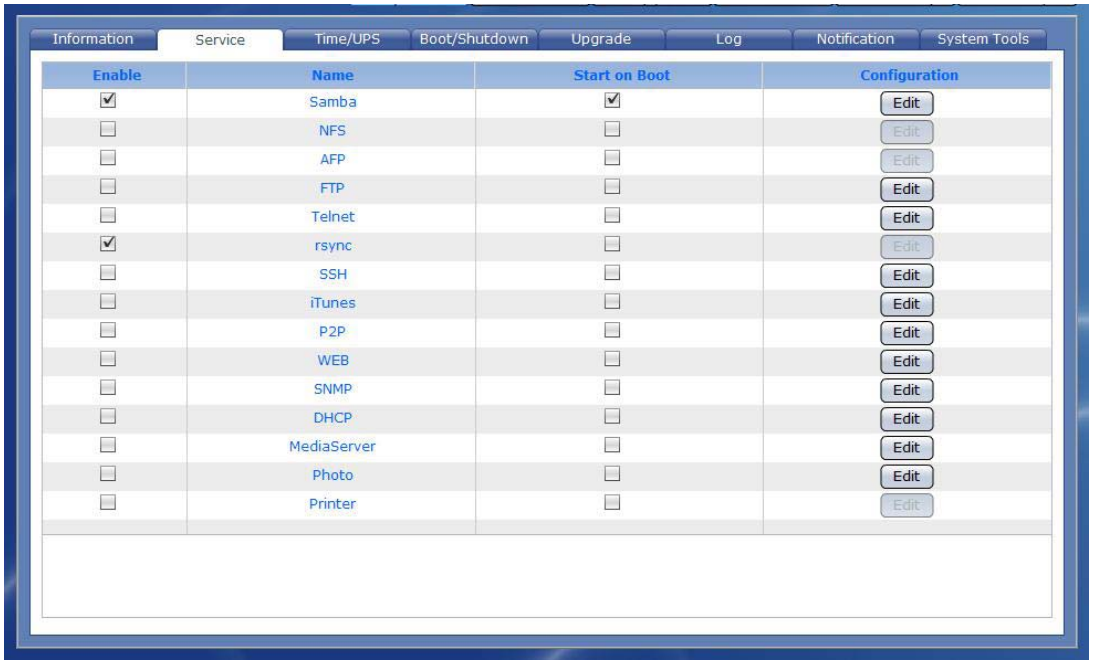
5. Click “OK” button. Once the Mac OS has connected to the share folder via SMB, you can see the directories/files under the share folder using Finder.



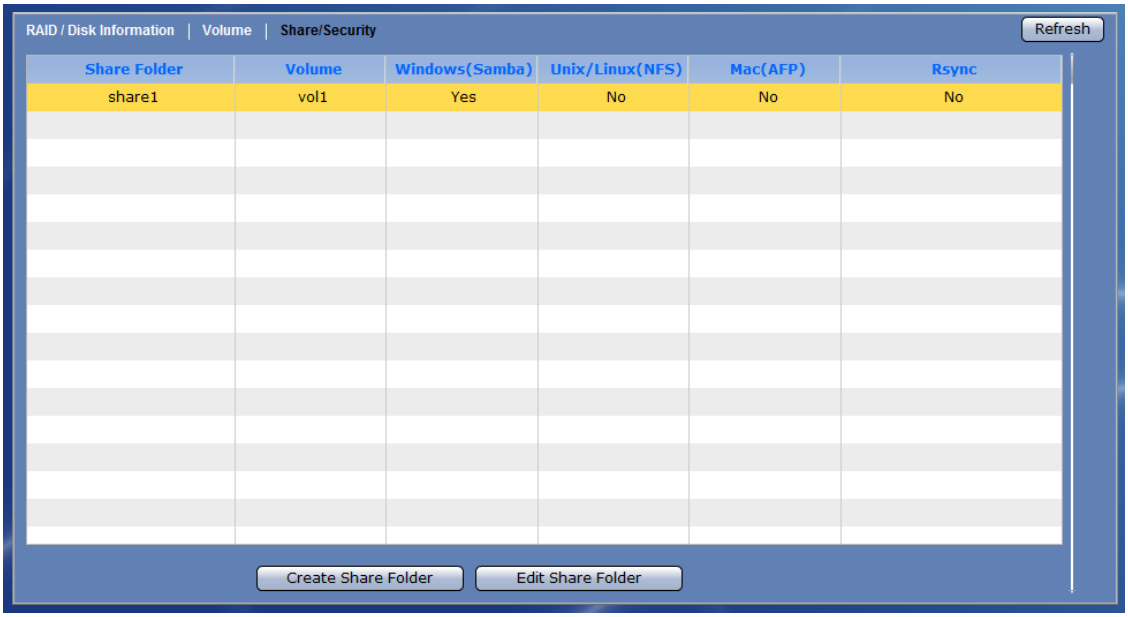
3.1.3.8 How to Setup Rsync

A. How to Setup the NAS as Rsync Server

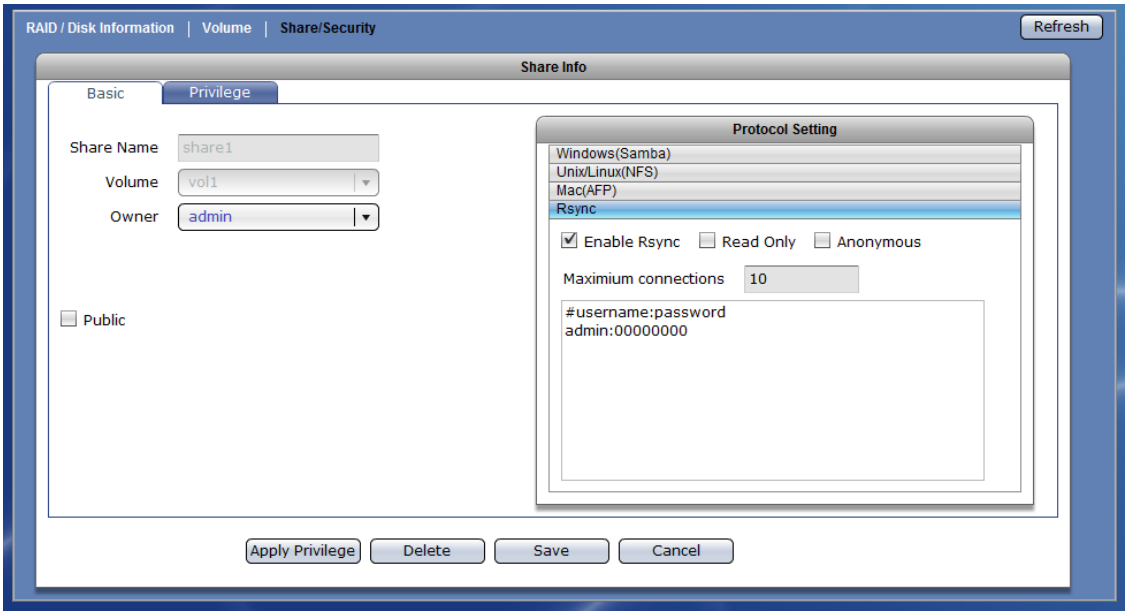
1. In System → Service, enable SSH and Rsync services.



2. In Storage/Share → Share/Security, select the share folder that will be used as Rsync Server target share folder. Click “Edit Share Folder”.



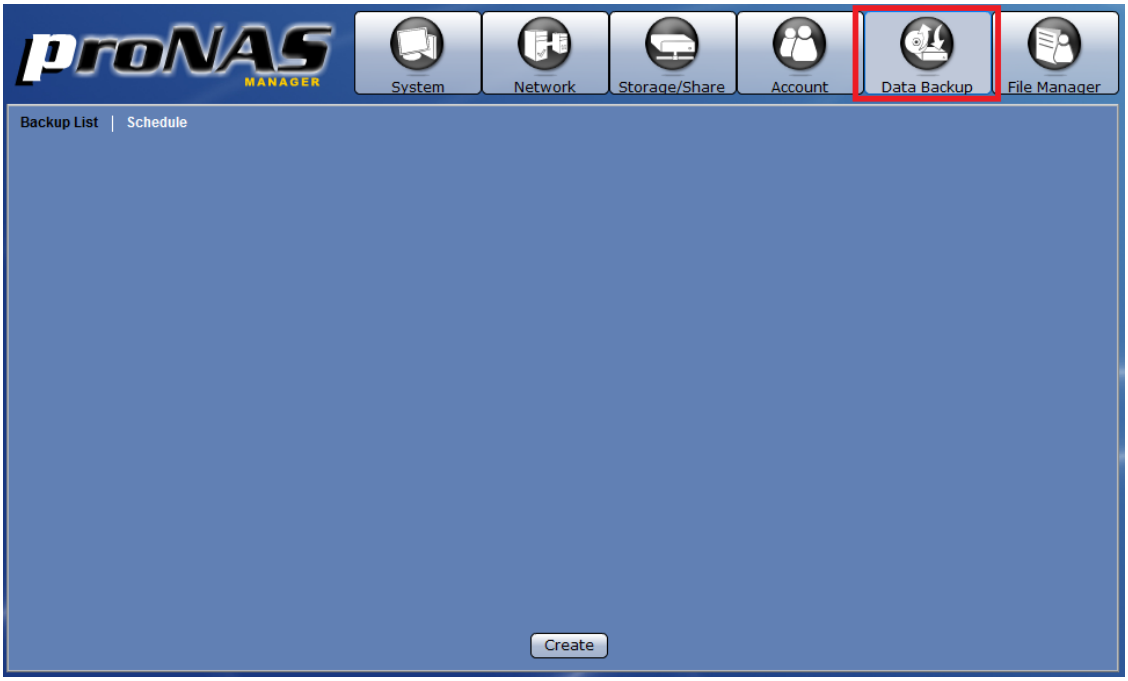
3. In Basic tab, select “Rsync” in Protocol Setting. Then tick “Enable Rsync”. Remove check mark in “Anonymous” option. Click “Save”.



B. How to Setup the NAS as Rsync Client:

The NAS can function as Rsync client using the Data Backup feature. To setup the NAS as Rsync client:

1. Select Data Backup. Click “Create”.



2. Setup Rsync client options. Enter the Backup Name and select the Backup Method as Rsync. Select the share (only one share) that will be used for back up using Rsync. In the Client Options, setup the IP, Remote Path, Account, Password, and Mode.

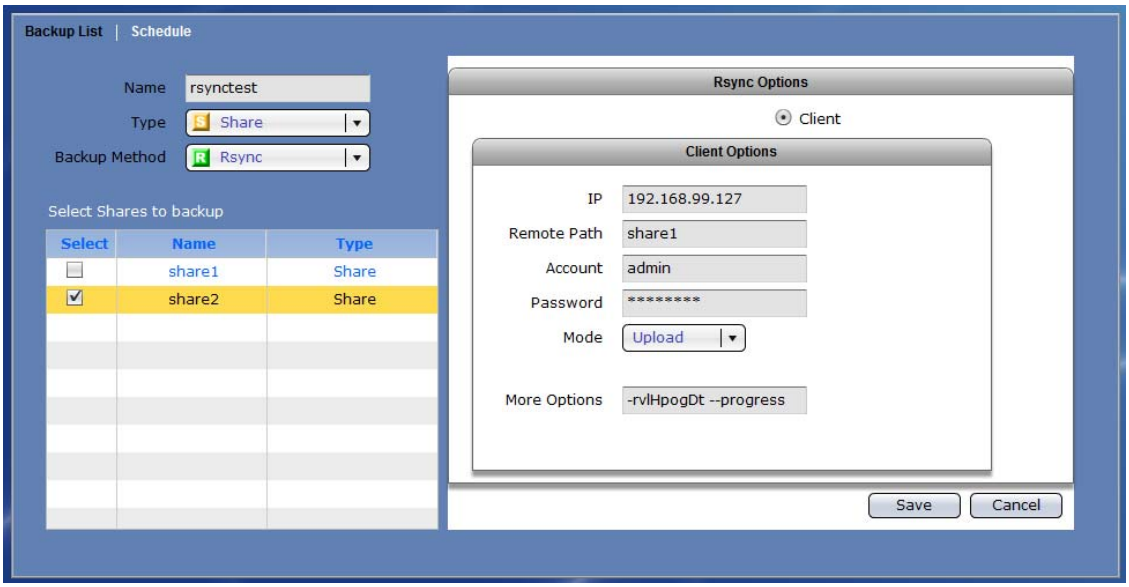
Rsync Client Options:

IP – the IP address of the remote Rsync server
Remote Path – the share name on the remote Rsync server
Account – the account name that will be required by the Rsync server for authentication
Password –the password of the account
Mode – Select the mode of file transfer, whether to upload to Rsync server or to download from Rsync server.
More Options – Specify here the Rsync options to be used. For more information about Rsync options, please visit http://samba.org/ftp/rsync/rsync.html.

NOTE: Only one share folder can be selected and used for Rsync backup, since the remote path is also single share folder.

Sample Setting:

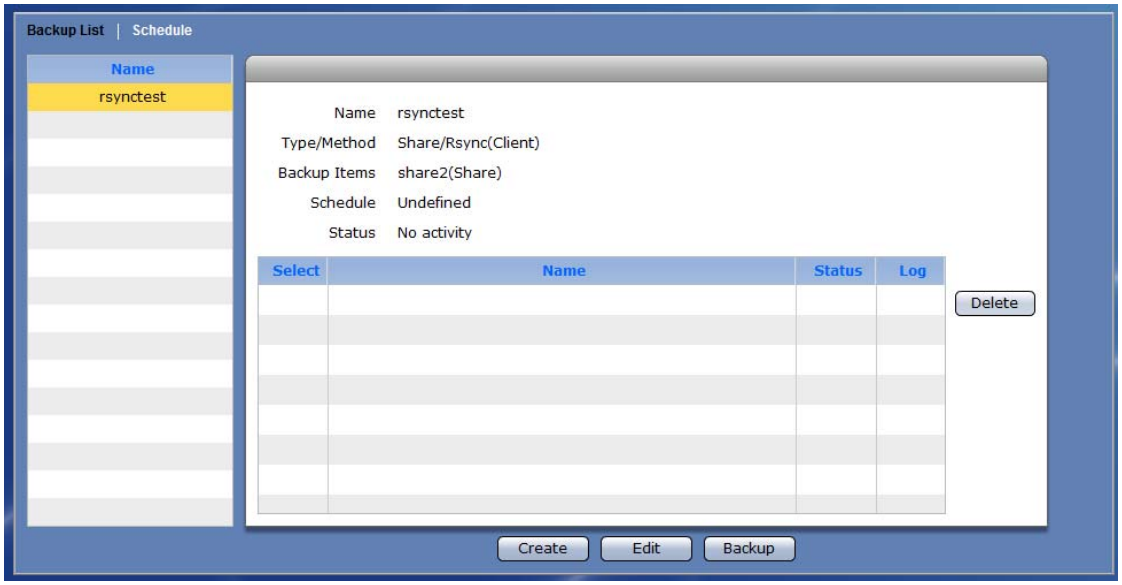
Name: rsynctest
Type: Share
Backup Method: Rsync
Select Shares to backup: share2 (selected)
Rsync Client Options
IP: 192.168.99.127
Remote Path: share1
Account: admin
Password: 00000000
Mode: Upload
More Options: -rvlHpogDt –progress



Summary of Rsync default options:

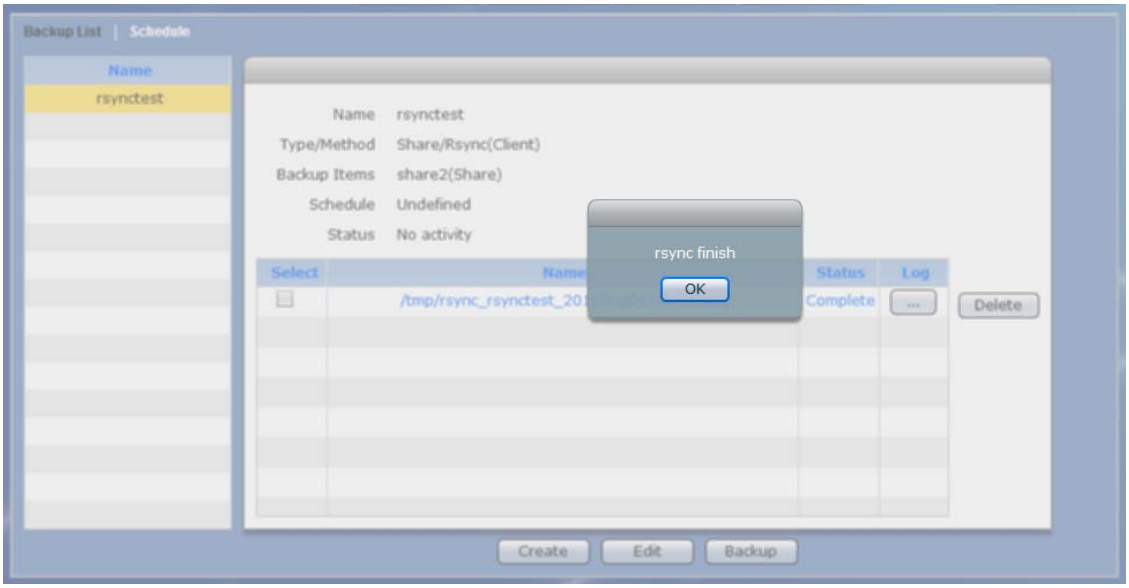
-r, --recursive	Recurse into directories
-v, --verbose	Increase verbosity. This option increases the amount of information given during the transfer
-l, --links	Copy symlinks as symlinks
H, --hard-links	Preserve hard links
-p, --perms	Preserve permissions. This option causes the receiving Rsync to set the destination permissions to be the same as the source permissions.
-o, --owner	Preserve owner (super-user only). This option causes Rsync to set the owner of the destination file to be the same as the source file
-g, --group	Preserve group. This option causes Rsync to set the group of the destination file to be the same as the source file.
-D, --devices	Preserve device files
-t, --times	Preserve times
--progress	Show progress during transfer (shown in the Rsync log)

3. Click “Save”.



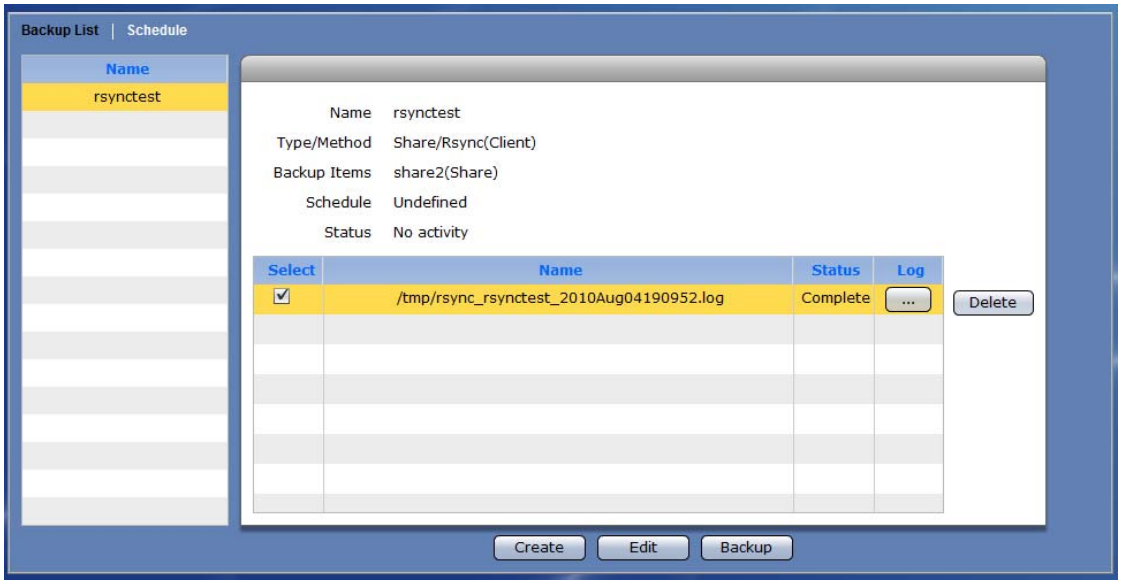
4. To execute the Rsync backup that was just created, select the backup name from the backup List, if not yet selected, and then click “Backup”.

5. When backup is finished, a pop-up message will be displayed. Click OK.

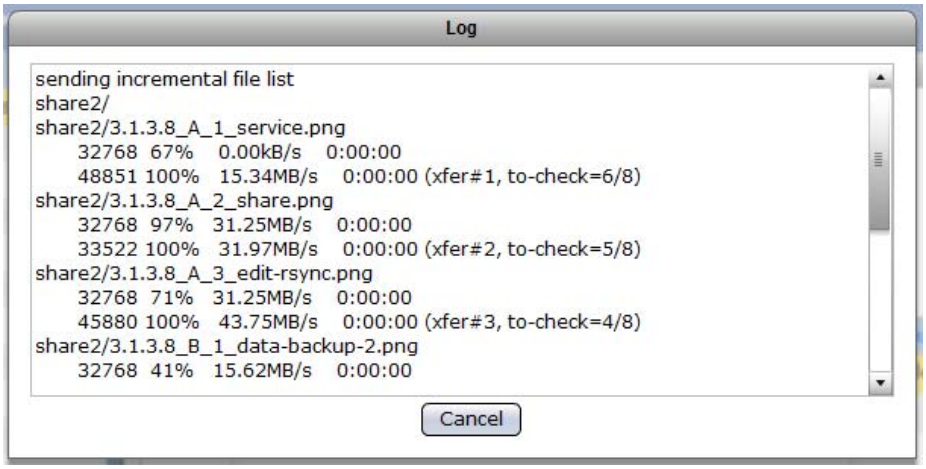


NOTE: The Rsync backup process can take a while if there are many files to be updated / uploaded or downloaded.

6. To view the Rsync log, select the backup log from the log list and click "…" button in the Log column.



7. The Rsync log for the selected log file will be displayed. Click "Cancel" to close.



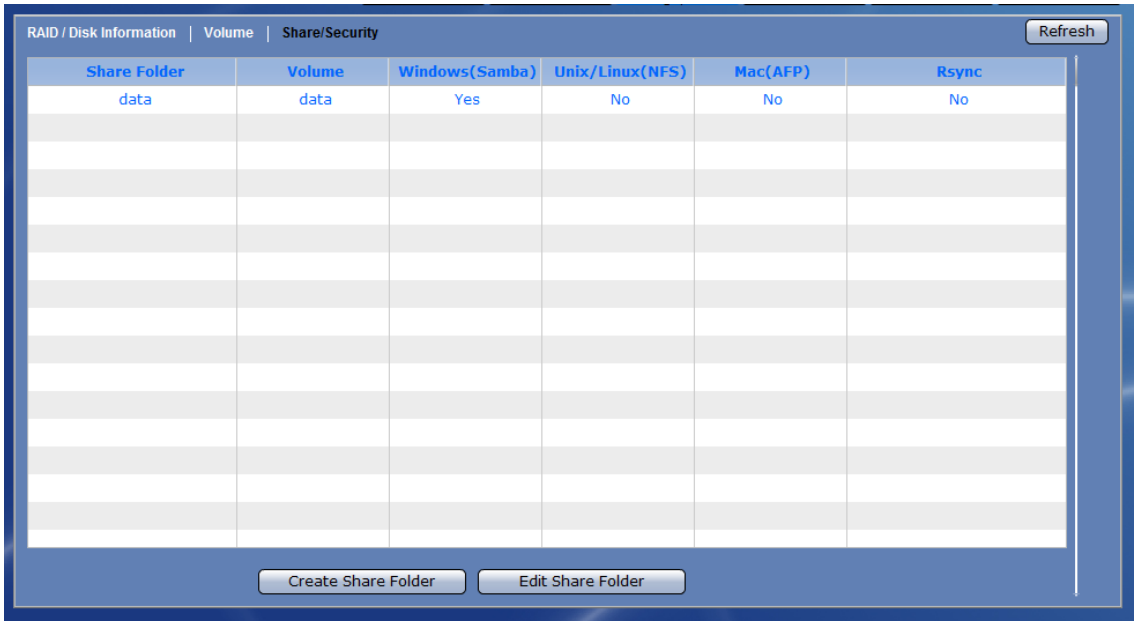
8. The Rsync backup can also be run on schedule. For more information how to setup backup by schedule, refer to Section 3.5.2.

3.1.3.9 How to Setup Time Machine

The NAS supports Time Machine to backup data from Mac to NAS share folder automatically. For more information about Time Machine, please visit Apple's website at http://www.apple.com/macosx/what-is-macosx/time-machine.html

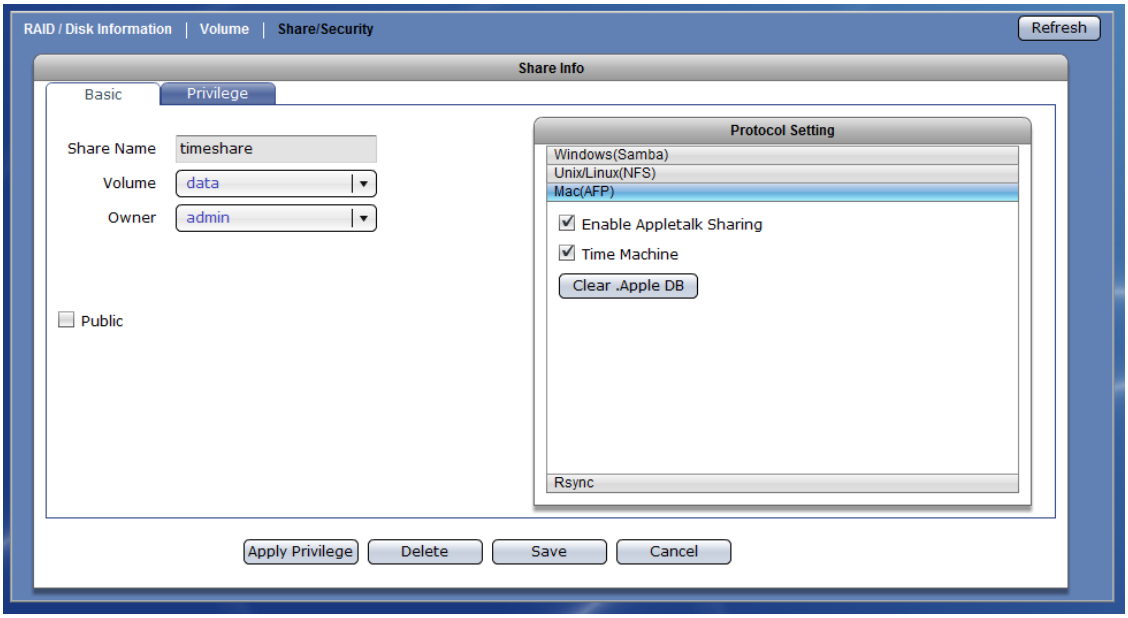
To setup Time Machine:

1. In NAS management GUI, select "Storage/Share" icon. Then select the "Share/Security" menu. Create a new share, if necessary, or edit an existing share.

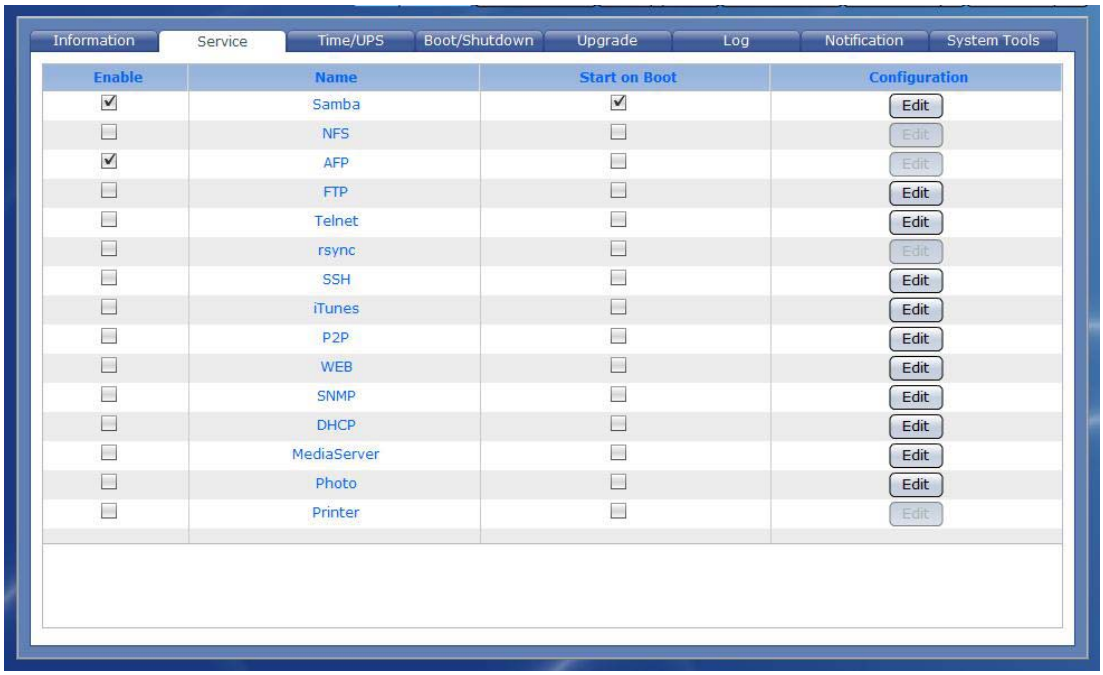


2. To create a new share folder for use with Time Machine, click "Create Share Folder".

3. Enter the share folder name, for example: timeshare. In the Protocol Setting on the right pane, select “Mac(AFP)”, and then tick “Enable AppleTalk Sharing” and “Time Machine” options. Click “Save”.

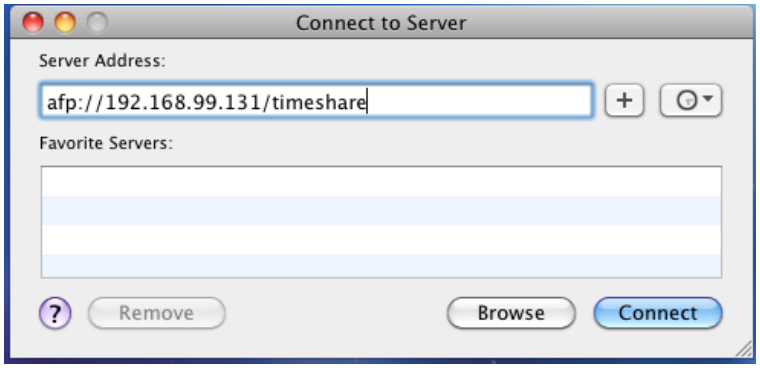


4. In System → Service menu, make sure the AFP service is enabled. If not, enable the service.



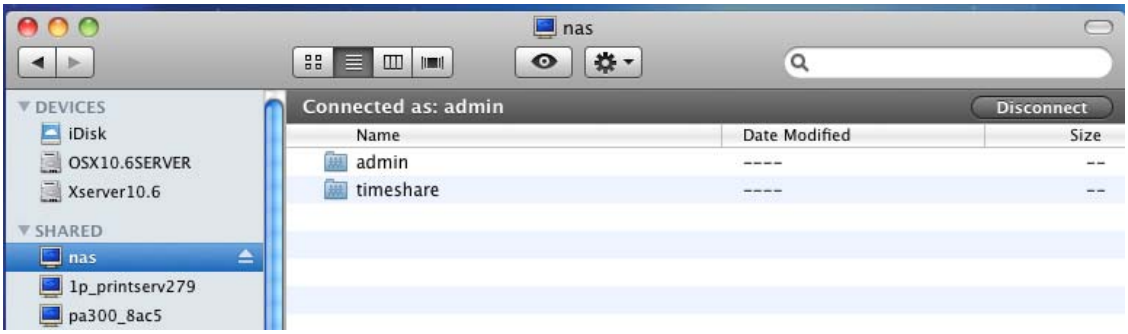
5. On Mac machine, to login to the NAS share folder via AFP, select “Go” then “Connect to Server”.

6. In Server Address, enter “afp://x.x.x.x/timeshare”, where x.x.x.x is the NAS IP address and timeshare is the share folder previously configured for Time Machine use. Then click “Connect”.



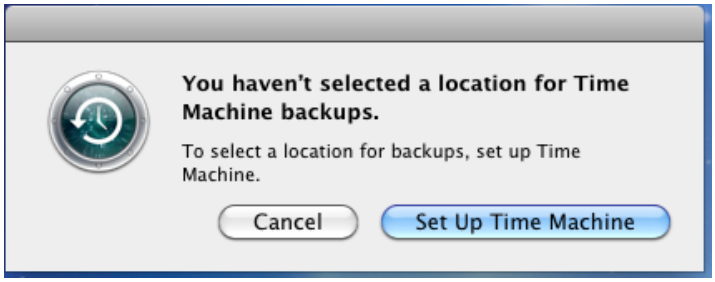
7. Enter a valid Account Name and Password; use account which has permission to the NAS share folder. In this example, admin account is used. Then click “Connect”.

8. The Mac will be connected to the NAS share folder.



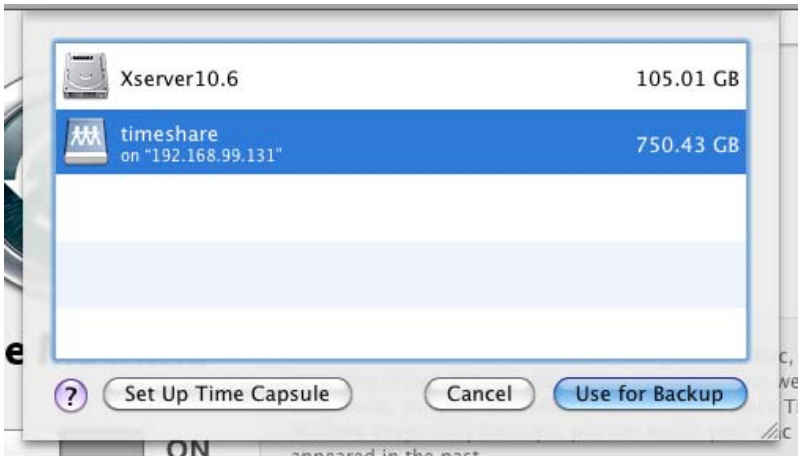
9. To setup Time Machine in Mac, open Time Machine.

10. If the Time Machine has not been previously setup, a message will be shown as below. Then select “Set Up Time Machine”.

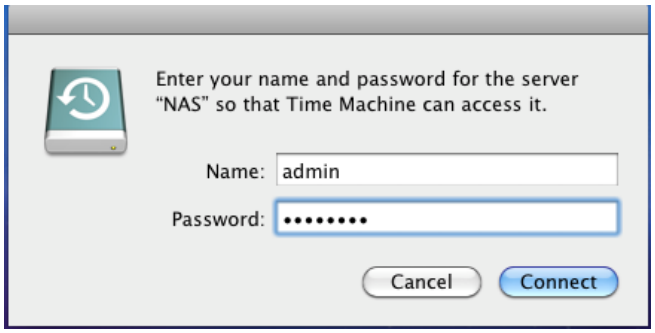


11. The Time Machine screen will be displayed. Click “Select Backup Disk…”.

12. Select the “timeshare” disk and click “Use for Backup”.



13. Enter the account name and account password to access the NAS share folder via Time Machine, and then click “Connect”.



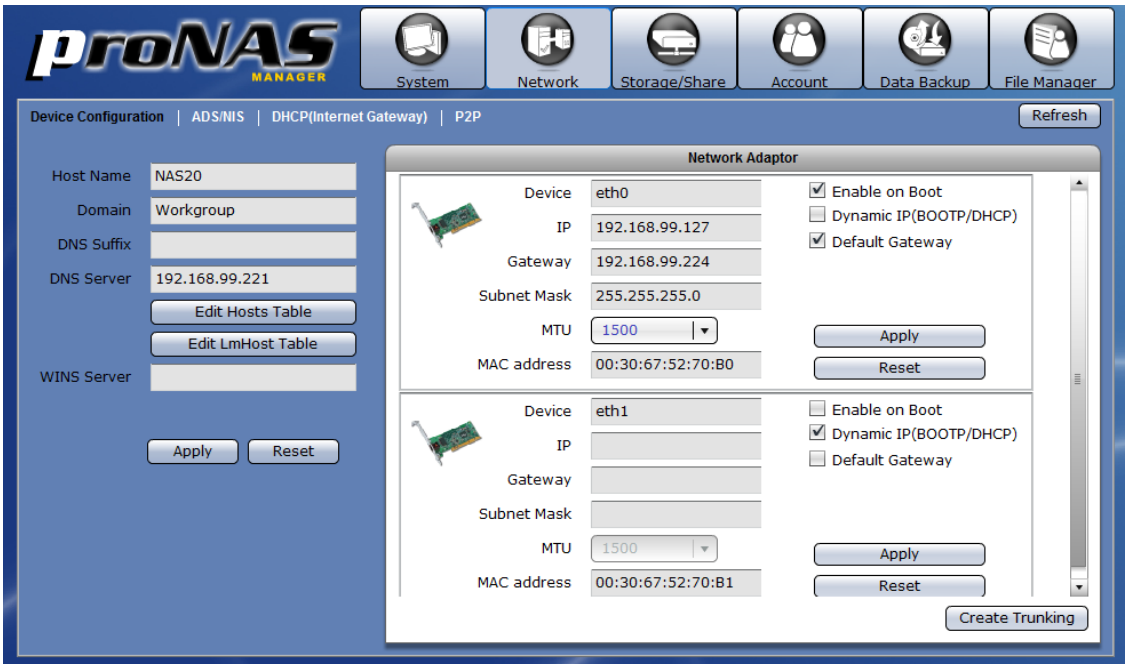
14. After successful connection, the Time Machine is setup. The available space on the NAS share folder will be shown. The Next Backup time is also displayed.

15. Done. The Time Machine will automatically backup to the designated NAS share folder.

3.2 Network

3.2.1 Device Configuration

Click the Network icon to display the Network Device Configuration screen.



Device Configuration Options:

Host Name – The NetBIOS name of NAS. It should be unique.

Domain – Enter the Windows domain name or workgroup name. For example: MYDOMAIN. Default is "Workgroup".

DNS Suffix – The DNS suffix is the name appended to server name to complete the server's FQDN. For example: MYDOMAIN.LOCAL

DNS Server – Enter the DNS Server IP address. DNS server is responsible for mapping the machine name and IP address.

WINS Server – Enter the WINS Server IP address. WINS Server is responsible for the setting NetBIOS name resolution.

Edit Hosts Table - Use this button to edit machine name and IP address mapping in the Hosts table. This is optional.
NOTE: After you edit host table configuration and click "OK", you still need to click "Apply" for changes to be saved.

Edit LmHost Table - Use this button to define the resolution of NetBIOS in the Lmhosts table. This is optional.
NOTE: After you edit lmhost table configuration and click "OK", you still need to click "Apply" for changes to be saved.

Reset – Use this button to undo or clear any changes made.

Apply – Use this button to save the changes made.

Network Adaptor Configuration Options:

Device – Shows the network device name. eth0 is the device name for LAN0 gigabit port.

IP - Shows the current IP address of the network device. Configure the IP address as necessary.

Gateway – Show the current IP address of the Gateway. To edit, enter the Gateway IP address.

Subnet Mask - Shows the current subnet mask setting. To edit, type in the new subnet mask number.

MTU - The MTU size (Maximum Transmission Unit) in bytes. To modify the MTU size for this interface, select the new MTU size. Options are: 1500 (default), 2000, 3000, 4000, 5000, 6000, 7000, 8000, and 9000.

MAC address – Shows the MAC address of network device.

Enable on Boot - If enabled, this adapter will be active when proNAS starts up.

Dynamic IP (BOOTP/DHCP) - If checked, this specifies that this network device will dynamically obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server or from a Bootstrap Protocol (BOOTP) server.

Default Gateway - If checked, the default gateway will be enabled in this adapter. A default gateway is a local IP router that is used to forward packets to destination beyond the local network. Only one default gateway in the NAS can be enabled in a certain time.

Reset – Use this button to undo or clear any changes made.

Apply – Use this button to save the changes made.

Create Trunking – Use this button to configure network trunking.

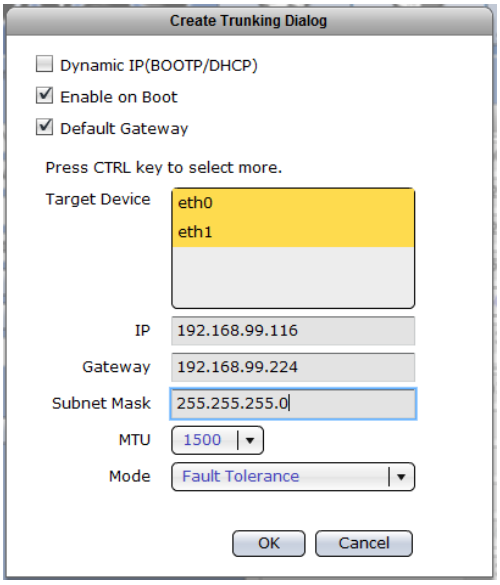
3.2.1.1 Configure Network Trunking

Steps to Configure Trunking Function:

NOTE: It is necessary that the network switch supports the type of trunking mode that will be used. Otherwise, the network connections may become unstable.

1. In Network → Device Configuration screen, click “Create Trunking”.

2. The Create Trunking Dialog window will be displayed. Configure the necessary options.



Create Trunking Configuration Options:

Target Device – Shows the network device names that can be included in Trunking. To select, press the “Ctrl” key and at the same time click the network device names.

Mode – Select the Trunking Mode that will be used.

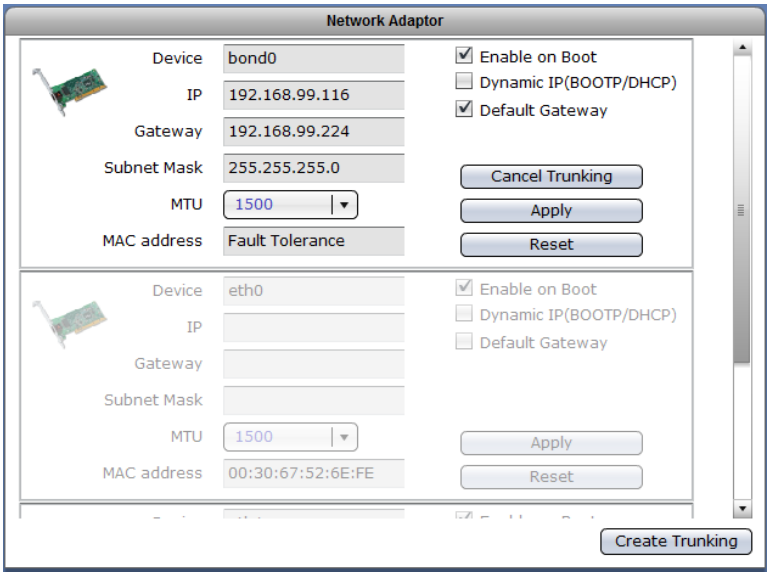
Trunking Mode Options:

- **Fault Tolerance** – Active-Backup policy: If the active Ethernet port fails, the standby Ethernet port will become active. This enhances the availability of access to the NAS.
- **Load Balance / Fault Tolerance** - XOR policy: Transmit based on source MAC address XOR with destination MAC address. This selects the same slave for each destination MAC address. This mode provides load balance and fault tolerance.
- **Dynamic Link Aggregation** - 802.3ad policy: Combines multiple physical network links into a single logical link for increased performance. Transmits and receives on all slaves in the active aggregator. Pre-requisite: the network switch must support IEEE 802.3ad.
- **Load Balance** - ALB (Adaptive Load Balancing) policy: The receive load balancing is achieved by ARP negotiation and does not require special switch support.

3. Click “OK” when done. A warning message will be displayed. Click “Yes” to proceed.

4. The NAS network configuration will be restarted. Re-login to NAS GUI.

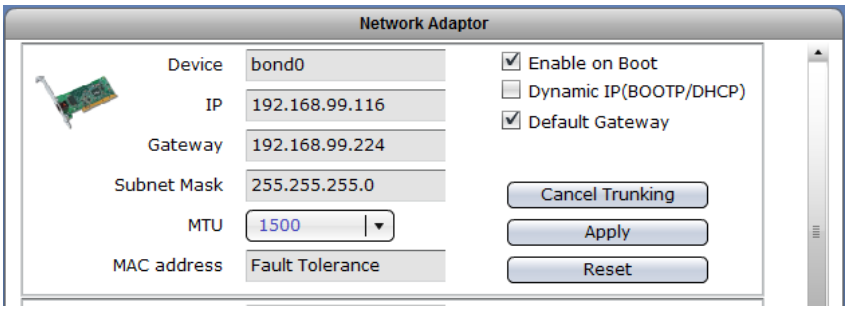
5. The Trunking function is configured. The member network devices will be shown as deactivated and cannot be configured. A new network device name “bond0”, which is the Trunking device, will be shown.



3.2.1.2 Cancel Network Trunking

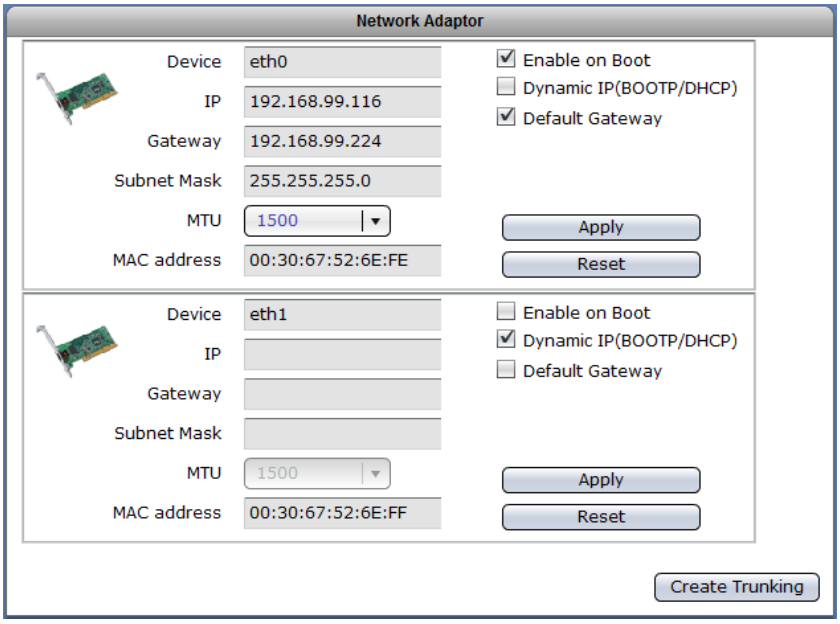
Steps to Cancel Trunking Function:

1. Find the device name “bond0” then click “Cancel Trunking”.



2. A warning message will be displayed. Click “Yes” to proceed.

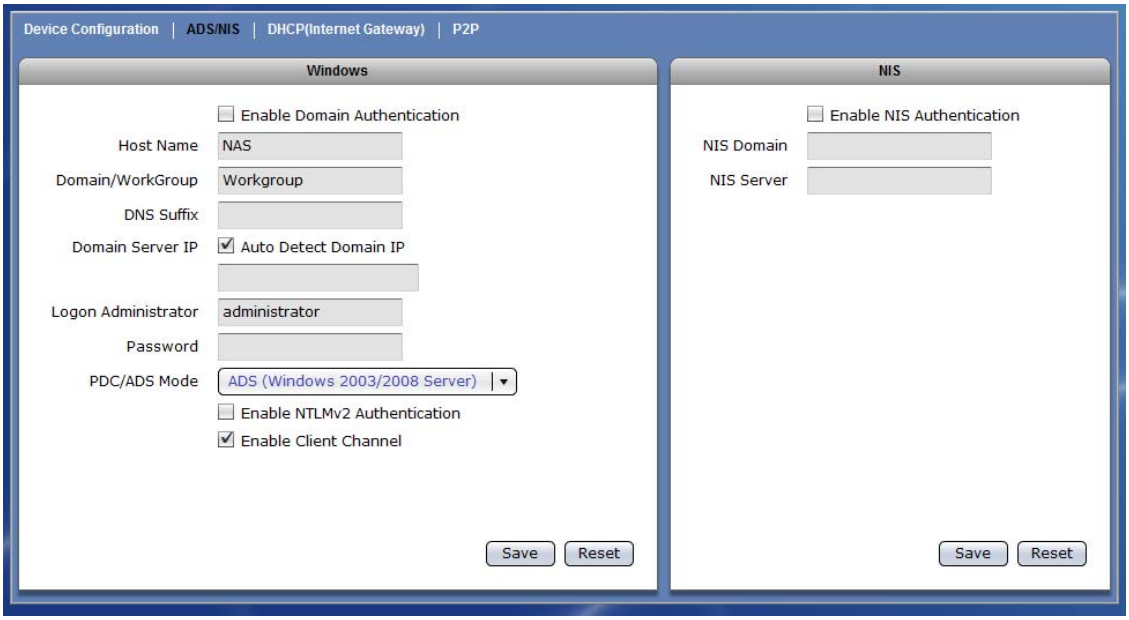
3. The Trunking function will be cancelled and the network configuration will be restarted. Re-login to NAS GUI. The network device eth0 will be automatically configured and get the IP address previously assigned to the Trunking device.



3.2.2 ADS/NIS

Windows ADS/PDC or NIS domain accounts can be imported and integrated into the NAS.

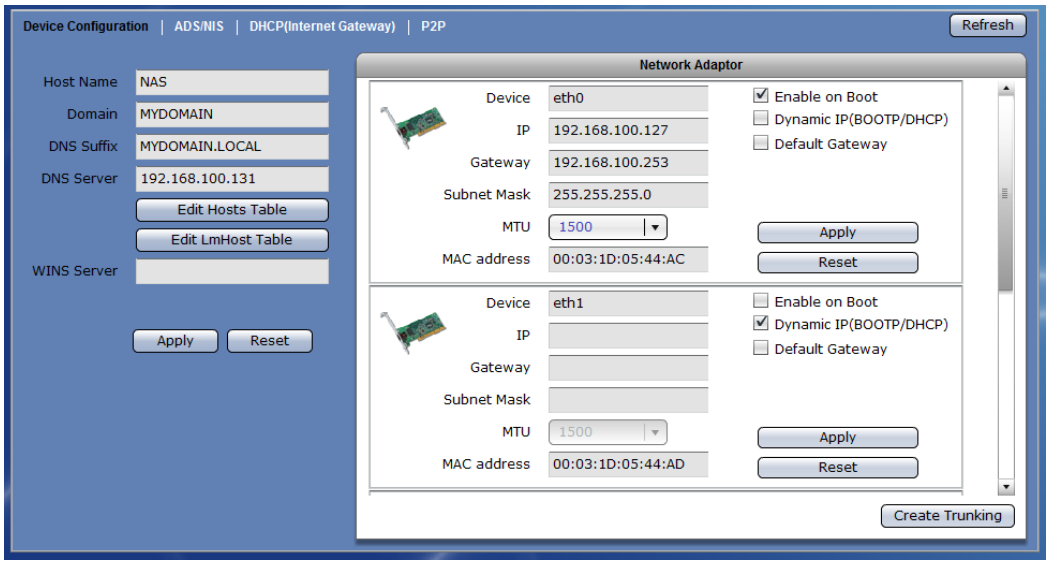
NOTE: Some network settings required in configuring the Windows Domain Authentication option must have been configured in Network ➔Device Configuration, such as Domain/Workgroup name, DNS Suffix, and DNS Server.



3.2.2.1 Join NAS to Windows AD Domain

Steps to Join NAS in the Windows AD Domain:

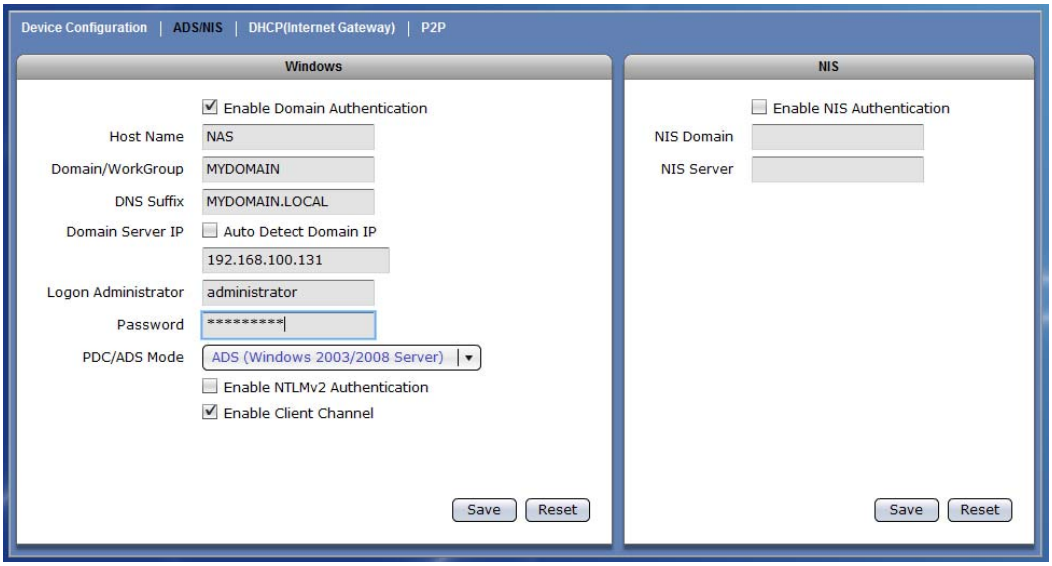
1. Select Network → Device Configuration. Enter the Domain Name and DNS Suffix. A DNS Server IP can also be entered if necessary. Refer to Section 3.2.1 for the Device Configuration options.



2. A warning message will be displayed. Select “Yes” to apply new settings.

3. Select Network → ADS/NIS tab.

4. In Windows screen, check the “Enable Domain Authentication” option. Configure the necessary options.
   a. If Domain Server IP is automatically detected, the Domain Server IP will be displayed. If you want to join NAS to a specific Domain Server IP, remove the check mark in “Auto Detect Domain IP” and manually enter the Domain Server IP address.
   b. Enter the Domain Administrator account.
   c. Enter the Domain Administrator’s password.
   d. Select the PDC/ADS mode.
   e. Click “Save” when done.



Windows Domain Authentication Options:

Enable Domain Authentication – Use this option to enable or disable Windows Domain Authentication.

Host Name – Indicates the NetBIOS name of NAS as configured in Network → Device Configuration tab.

Domain / Workgroup – Shows the domain/workgroup name as configured in Network → Device Configuration tab.

DNS Suffix – Shows the DNS Suffix as configured in Network → Device Configuration tab.

Domain Server IP – Shows the IP address of the domain server which is automatically detected when “Auto Detect Domain IP” option is enabled. If “Auto Detect Domain IP” option is disabled, manually type the domain server IP address.

Logon Administrator – Enter the administrator’s logon account in the domain server.

Password – Enter the password of administrator’s logon account in the domain server.

PDC/ADS Mode – Select the mode type of the domain server. This can be "ADS (Windows 2003/2008 Server)" or "PDC (Windows NT Server)".

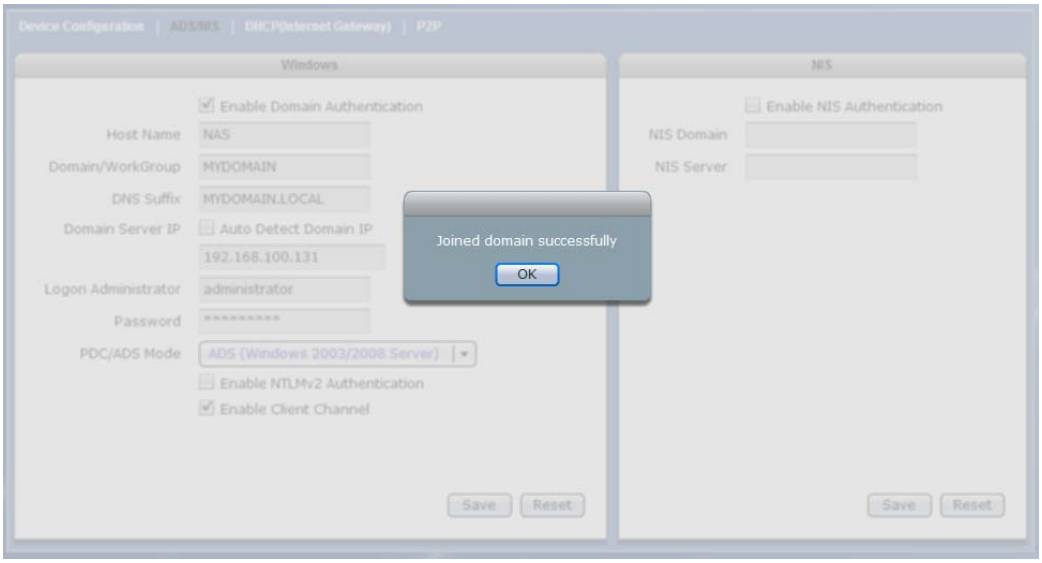
Enable NTLMv2 Authentication – This parameter determines whether or not smbclient will attempt to authenticate itself using the NTLMv2 encrypted password. If enabled, NAS will only sent NTLMv2 and LMv2 responses. NTLMv2 authentication protocol is available only on WindowsNT4 with SP4 and Windows 2000 or later. Default is disabled.

Enable Client Channel - This controls whether the client offers or even demands the use of the netlogon schannel. Default is auto, means it offers the schannel but does not enforce it.

Reset – Use this button to undo or clear any changes made.

Save – Use this button to save the changes made.

5. A message will be displayed when NAS is successfully joined the domain. Click "OK".



NOTE: When NAS is successfully joined to the Windows domain, the domain user accounts will appear in Account list.

NOTE: The NAS cannot be joined to the Windows domain if NASVG does not exist (NASVG is not yet initialized).

3.2.2.2 Join NAS to NIS Domain

Steps to Join NAS in the NIS Domain:

1. Select Network → ADS/NIS tab.
2. In NIS screen, check the "Enable NIS Authentication" option. Configure the necessary options.
    a. Enter the NIS Domain name.
    b. Enter the NIS Server IP address.
3. Click "Save" when done.

NIS Authentication Options:

Enable NIS Authentication – Use this option to enable or disable NIS Domain Authentication.
NIS Domain – Enter the NIS domain name.
NIS Server – Enter the IP Address of NIS server.
Reset – Use this button to undo or clear any changes made.
Save – Use this button to save the changes made.

NOTE: When NAS is successfully joined to the NIS domain, the domain user accounts will appear in Account list.
NOTE: The NAS cannot be joined to the NIS domain if NASVG does not exist (NASVG is not yet initialized).

3.2.3 DHCP (Internet Gateway)

NAS provides Internet gateway function for administrator to easily enable and disable the Internet access for users. This function integrates with DHCP service, routing and NAT.

DHCP (Internet Gateway) Options:

IP range starting from – Means the starting address of range of private IP addresses for DHCP.

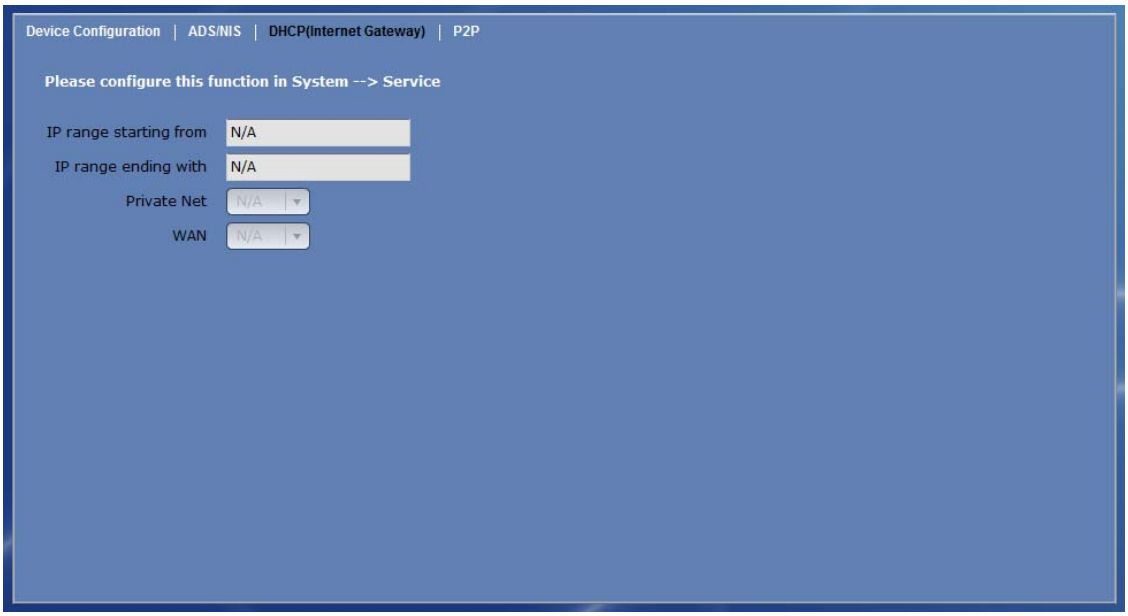
IP range ending with – Means the ending address of range of private IP address for DHCP.

Private Net – The network device connected to the private network.

WAN – The network device connected to the Internet / WAN.

NOTE: This function must be configured in System ➔ Service tab. Select DHCP service.

NOTE: Please refer to Section 3.3.2.3 on how to use DHCP (Internet Gateway).

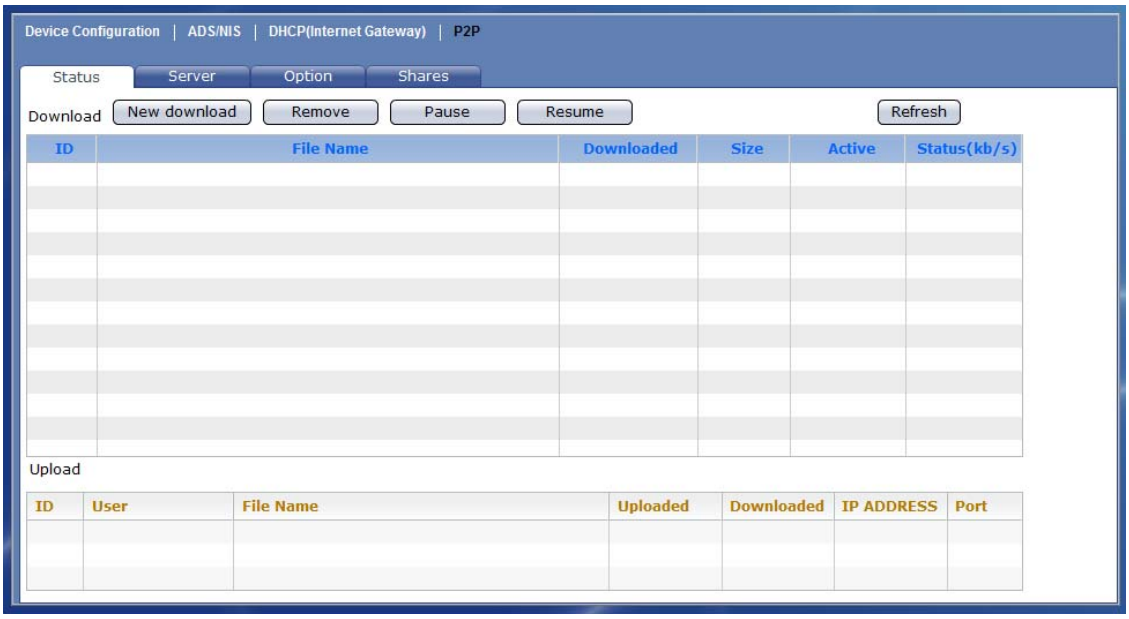


3.2.4 P2P

The NAS system supports P2P (peer-to-peer) file sharing protocol.

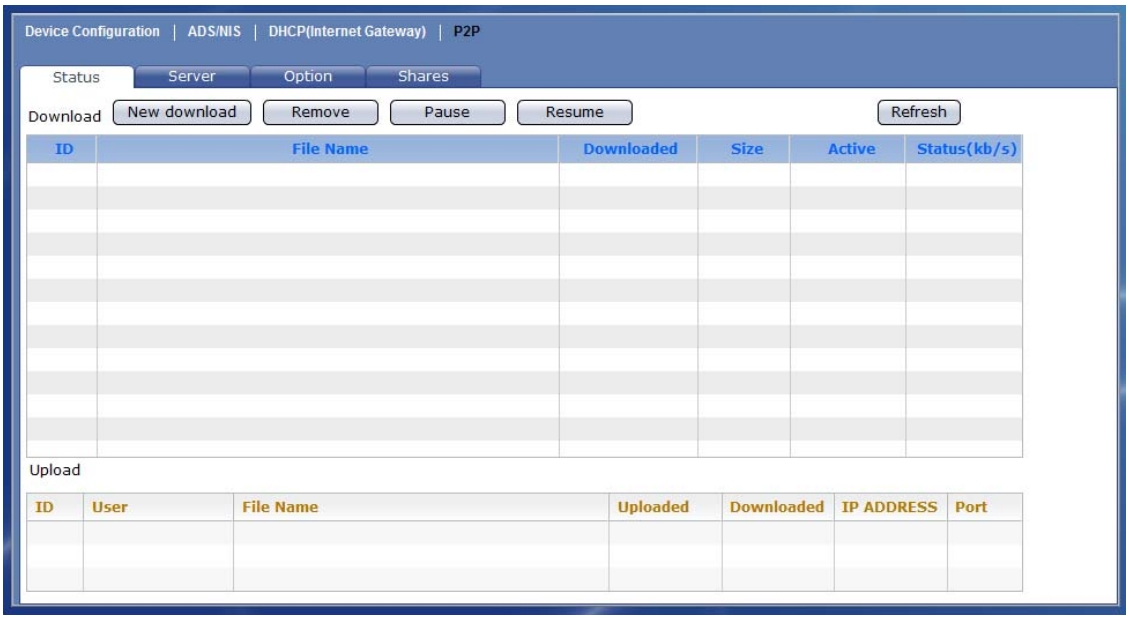
NOTE: Enable the P2P Service (System ➔ Service). Also setup the P2P Service 'Download file location' (System ➔ P2P ➔ Edit ➔ Quick Setup). Refer to Section 3.3.2 Service.

NOTE: DNS settings must be configured first before starting P2P service.



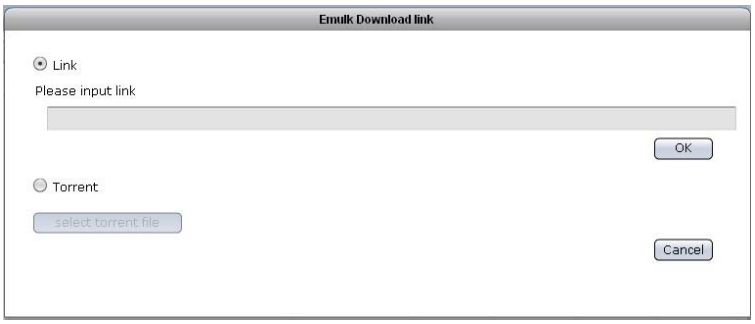
3.2.4.1 Status

This screen will show current download or upload connections.



Options:

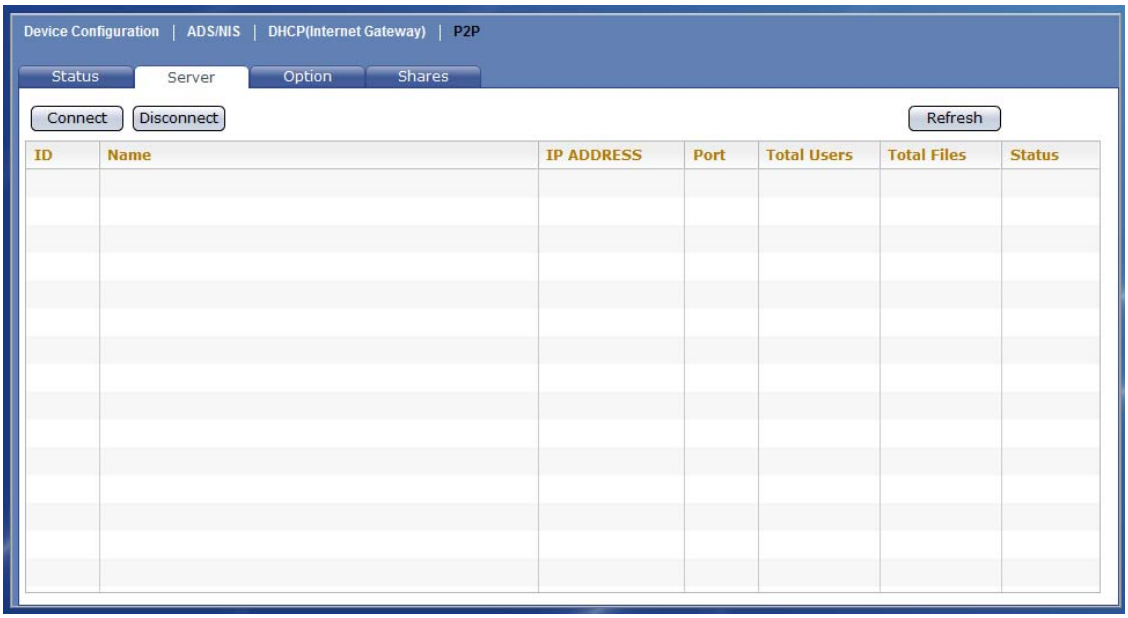
New download – Use this button to add download item. Then select either download link or torrent file.



Remove – Use this button to remove a selected download item.
Pause – Use this to pause the downloading of selected item.
Resume – Use this to resume downloading of selected item.
Refresh – use this to refresh current download status.

3.2.4.2 Server

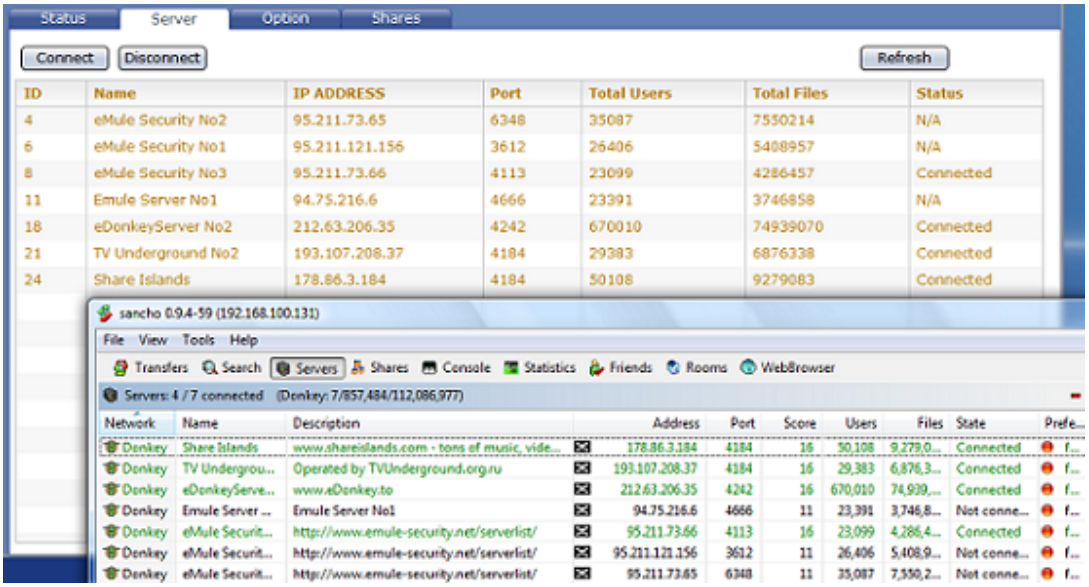
This screen allows connection to and disconnection from server.



Options:

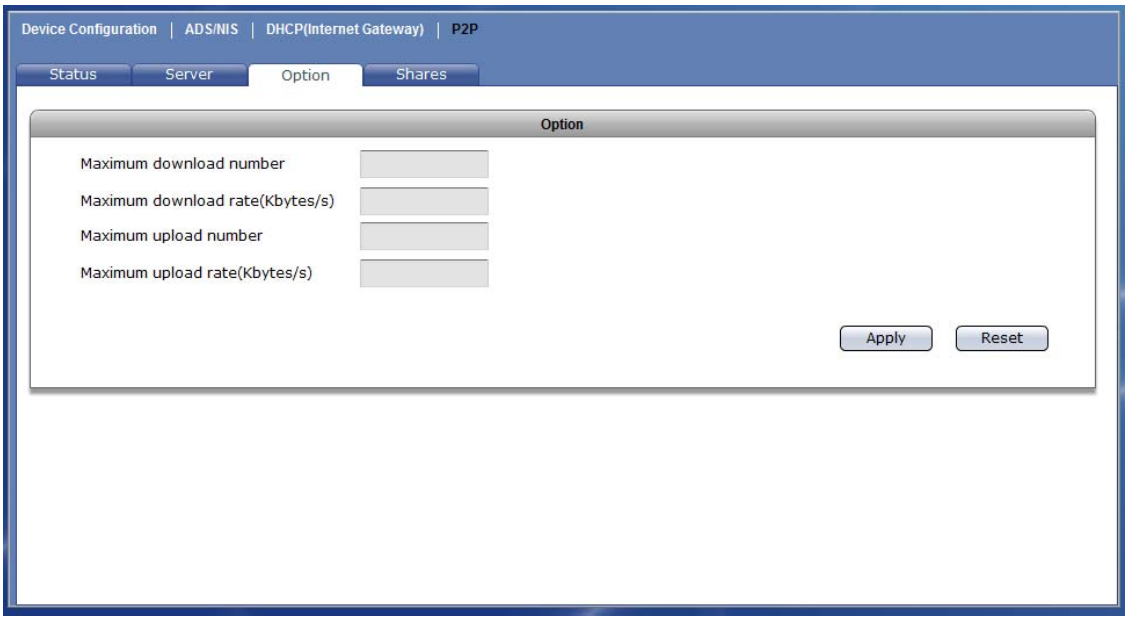
Connect – Use this button to connect to a selected server.
Disconnect – Use this button to disconnect to a selected server.
Refresh – Use this to refresh current connection status.

NOTE: You can use sancho http://sancho.awardspace.com/ (latest version is 0.9.4-59) to edit the server list.



3.2.4.3 Option

Use this screen to configure download options.



Options:

Maximum download number – Use this option to set the maximum number of download connections.

Maximum download rate – Use this option to set the maximum download transfer rate.

Maximum upload number – Use this option to set the maximum number of upload connections.

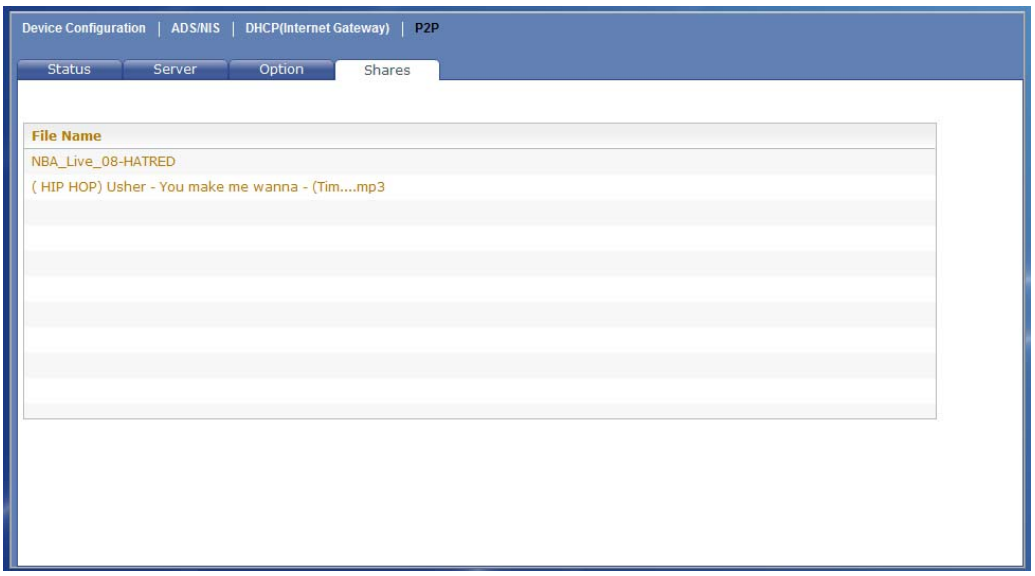
Maximum upload rate – Use this option to set the maximum upload transfer rate.

Apply – Use this button to save changes made.

Reset – Use this button undo any changes made and load previously saved setting.

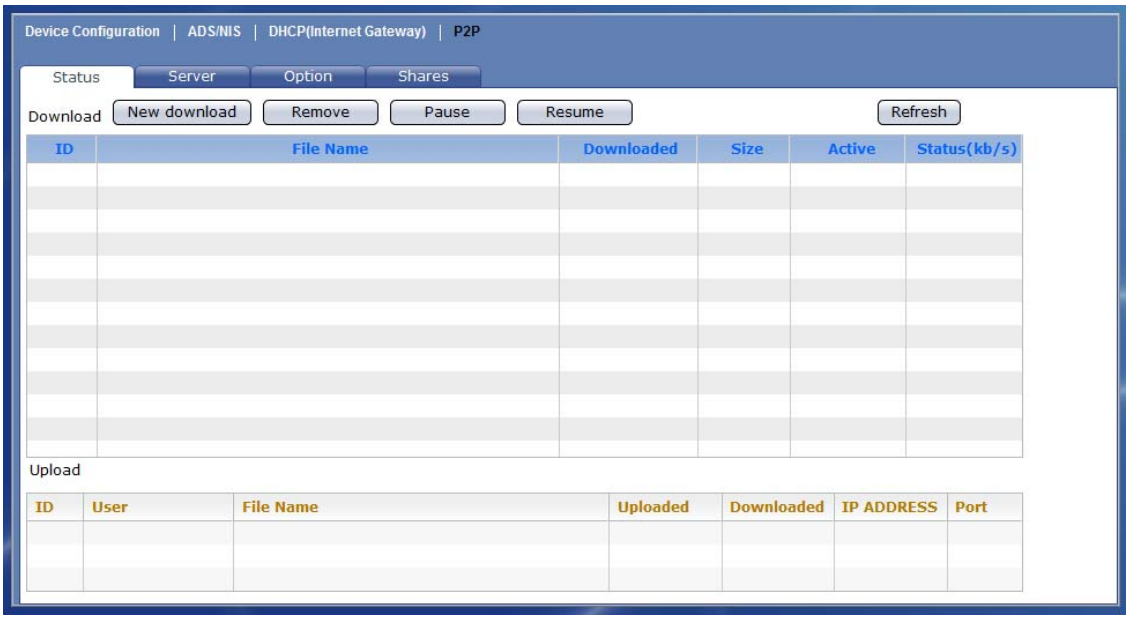
3.2.4.4 Shares

This screen displays the list of files downloaded or being downloaded in the target share.

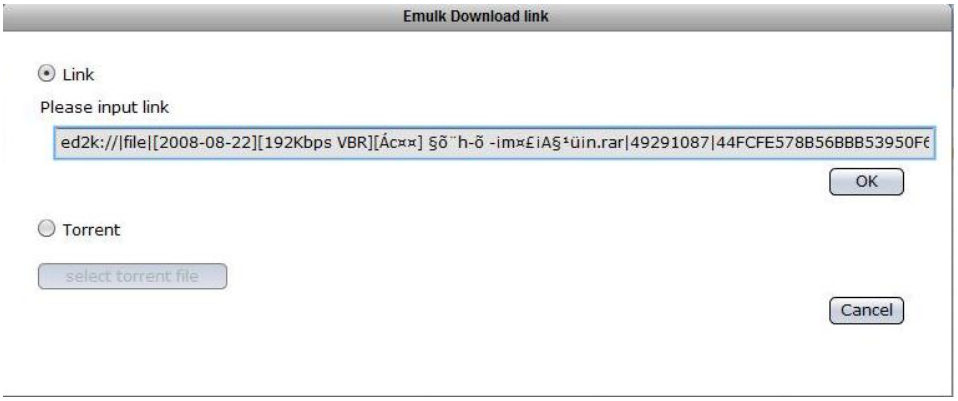


3.2.4.5 Example of Download from Link and Torrent

1. Click “New download”.

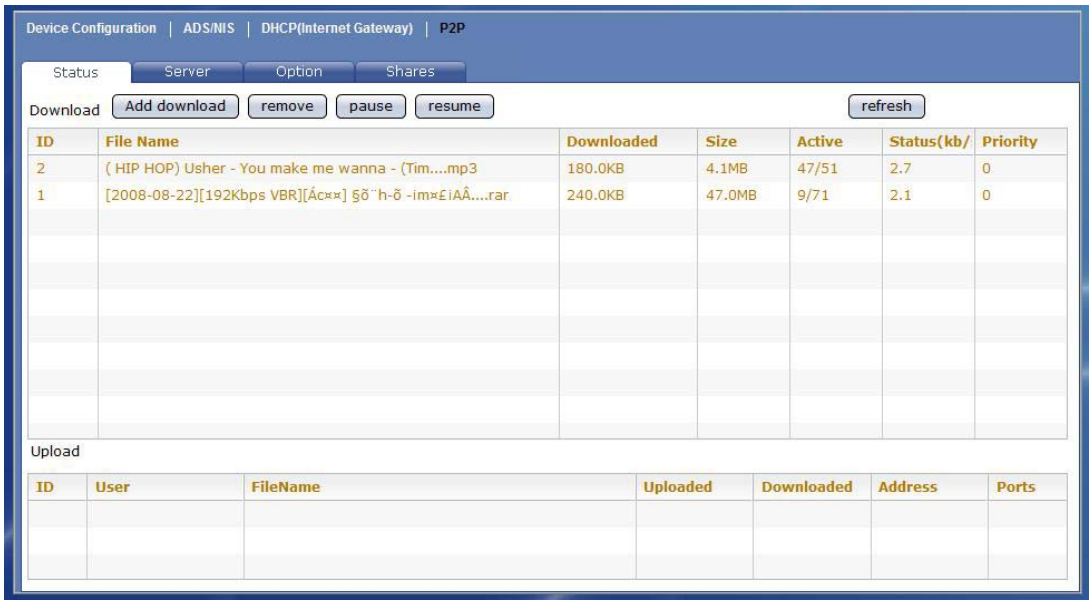


2. To download using link, enter the download link or paste the link in the box provided. Click “OK”.

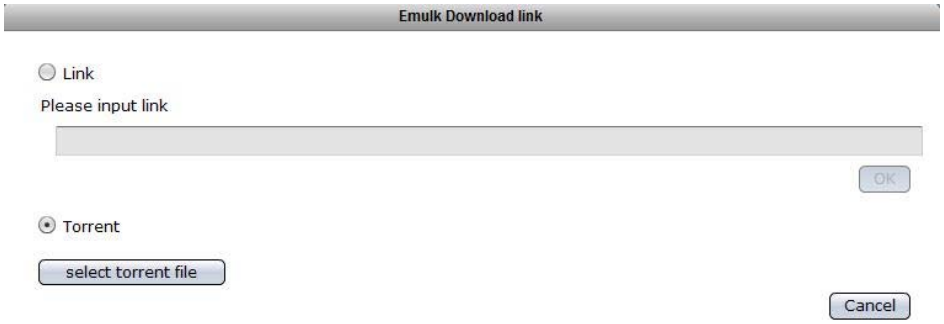


3. To download from another link, enter the link or paste the link in the box then click "OK".

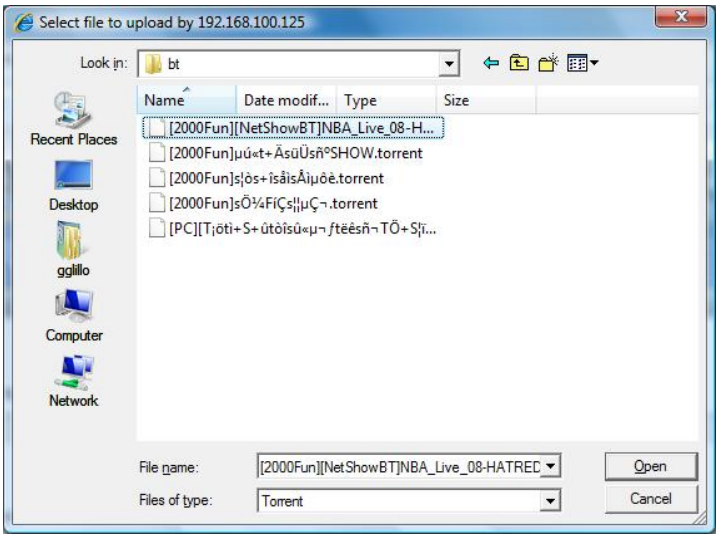
4. Two items will be displayed under Download.



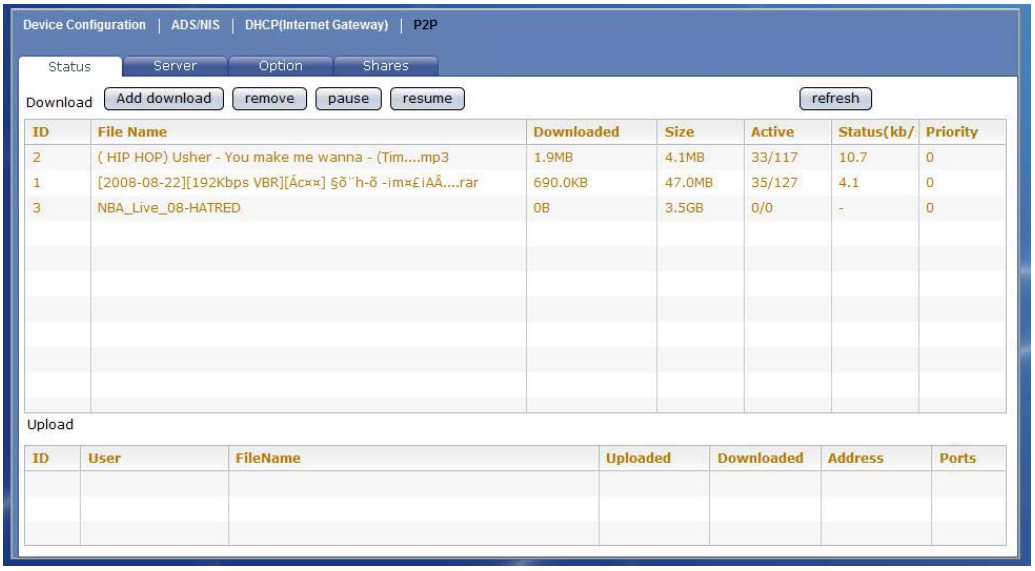
5. To download using torrent, click “New download” then select “Torrent” option. Click “select torrent file”.



6. Select the torrent file. Click “Open”.



7. The download item will be added in the Download list.

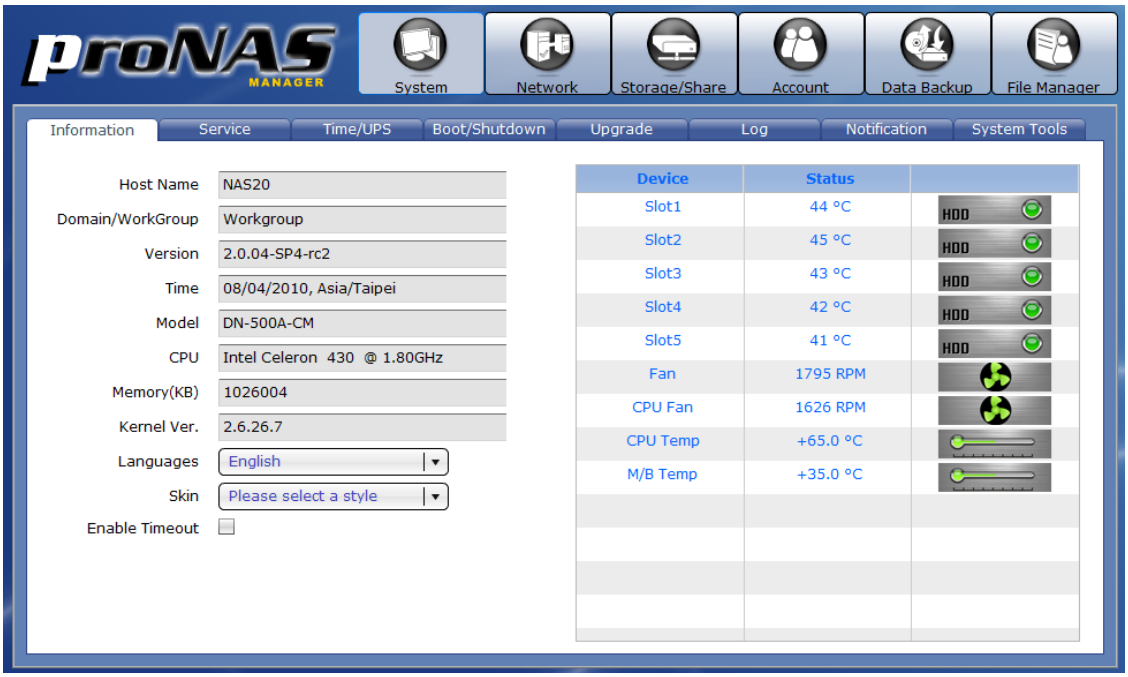


8. To remove an item, select the item and click “Remove”.
9. To pause downloading, select an item and click “Pause”.
10. To resume downloading, select a paused item then click “Resume”.

3.3 System

The System function is used to configure different NAS system settings and services, such as: Service configurations, Date and Time Zone setting, Serial Port setting, NAS Firmware Upgrade, Reboot and Shutdown functions, Log Information, Event Notification via email, and various System Tools.

3.3.1 System Information



The System Information screen shows the following:

Host Name – Indicates the NetBIOS name of NAS as configured in Network → Device Configuration.

Domain / Workgroup – Shows the domain/workgroup name as configured in Network → Device Configuration.

Version – Shows the NAS firmware version.

Time – Shows the NAS system time and time zone.

Model – Shows the NAS system model.

CPU - Shows the NAS system processor type.

Memory (KB) – Shows the amount of NAS system memory (RAM) in KB.

Kernel Ver. – Shows the NAS kernel version.

Languages – Choose the preferred language from available options: English, Traditional Chinese, Simplified Chinese, Japanese, Korean, and Spanish.

Skin – Shows the color schemes available as skin color. Current options are: Black, Blue (default), and Green.

Enable Timeout – This is enabled by default. When there is no activity in the proNAS Manager GUI, admin will be automatically logged out after 15 minutes. To disable timeout, remove check mark in Enable Timeout.

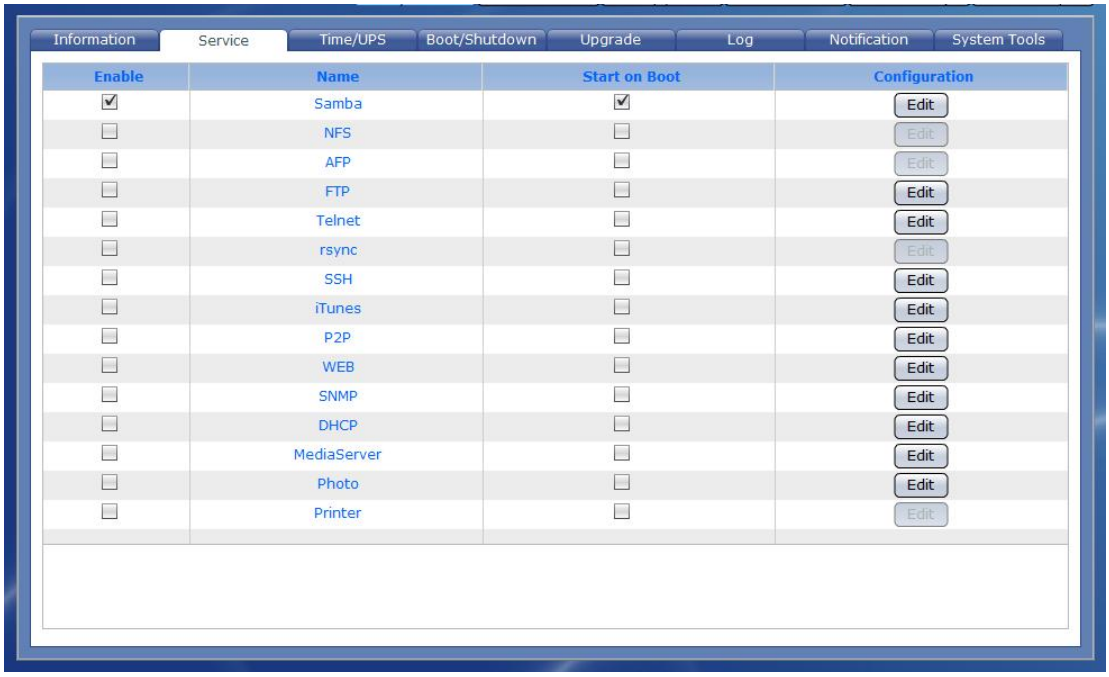
Device – Shows the device information such as Slot number, system fan, CPU fan, CPU temperature, and motherboard temperature.

Status – Shows the current status of each device, such as slot temperature, system fan and CPU fan speed in RPM, and CPU and motherboard temperature reading.

The System Information screen also shows the number of disk drives detected by the NAS system. The device icon is green when device is in good condition, and shows red when device is failed.

3.3.2 Service

The administrator can manage and enable/disable the various NAS system services. At the same time, some service can be configured in the Service tab.



Service Name:

Samba – Provides CIFS file sharing. MS Windows users need this service "Enabled" to be able to access the NAS share folders. By default, this service is enabled.
The "Windows(Samba)" Protocol Setting for the specific Share folder should also be enabled. Refer to Section 3.1.3.1 for more details on how to configure Samba protocol setting in a Share folder.

NFS - Provides Network File System (NFS) file sharing. UNIX and Linux users need this service "Enabled" to be able to access the NAS share folders. The "Unix/Linux(NFS)" Protocol Setting for the specific Share folder should also be enabled. Refer to Section 3.1.3.1 for more details on how to configure NFS protocol setting in a Share folder.

AFP - Provides Apple Filing Protocol. Mac OS users can use AFP to access the NAS share folders, and need this service "Enabled".

The “Mac(AFP)” Protocol Setting for the specific Share folder should also be enabled. Refer to Section 3.1.3.1 for more details on how to configure Mac(AFP) protocol setting.

FTP – Provides users with access to NAS using File Transfer Protocol (FTP). After enabling this service, NAS accounts can login to NAS via FTP using their account and password. Use an FTP client application to login to NAS and transfer files via FTP.

Telnet – Provides users with access to NAS using Telnet. After enabling this service, NAS accounts can remote login to NAS console via Telnet using their account and password. Use a Telnet client application, such as PuTTY http://www.putty.org/ to login via Telnet.
NOTE: Admin can limit access via Telnet by disabling this service. It is recommended to access the NAS console only when needed, such as when troubleshooting the NAS. NAS configuration should be done in the GUI and not in the console.

Rsync - Provides Rsync Server function to NAS. Rsync client can connect to NAS, such as another NAS with Rsync client function configured. Refer to Section 3.1.3.1 Step 6 for Rsync Server setup options. Data can be backed up to NAS using Data Backup function. Refer to Section 3.5.1.1 Create Backup Plan how to configure Rsync client to do backup via Rsync backup method. For more information about Rsync function, please visit http://samba.org/rsync/.

SSH – Provides remote management connection to NAS using Secure Shell (SSH) with more secure level. Use an SSH client application, such as PuTTY http://www.putty.org/ to remotely login to NAS console.

iTunes – Enable music files in the NAS share to be directly accessed by iTunes programs in the network.

P2P – Provides P2P (peer-to-peer) client program. This also supports sancho as its P2P GUI on a Windows computer in the network. Refer to Section 3.2.4 for more information how to setup P2P.

WEB – Provide web server program. Need to be enabled if photo service is to be used.
If NAS will be used as web server, need to copy the html file, example: index.html, file to the share folder (designated in Target Share in Quick Setup) and under WEB subfolder. In web browser, enter http://x.x.x.x/index.html, where is x.x.x.x is the NAS IP.

Note that a default index.html file will be created in the WEB subfolder of the designated share folder when the service is enabled. You can delete the default index.html file and copy your own index.html file, or copy a different html filename, for example mytest.html then to open this from web browser, use http://xxx.xxx.xxx.xxx/mytest.html

NOTE: Do not enable "Public" option on the share folder designated as WEB target share folder.

SNMP – The SNMP gives users independence from the proprietary network management schemes of some manufacturers and SNMP is supported by many WAN and LAN manufacturers enabling true LAN/ WAN management integration.

DHCP – Provides DHCP service, and make proNAS act as DHCP server. Click the "Edit" button under Configuration and setup the DHCP options. Refer to Configuration Options in the succeeding pages.

Media Server – Provides NAS DLNA multimedia File Server. Allow NAS to share files to Sony PlayStation3 and XBOX360.
When a share folder is set as Media Server library, the share folder is accessible from a DLNA/media client.

Photo – Provide easy to use Photo gallery service. This service requires WEB service enabled.
Note that the WEB service will be automatically enabled when Photo service is enabled.

Printer – Provide print server service. It allows a printer installed in the NAS to be shared by computers on the network. Supported model is HP Deskjet F4280 printer. Connect USB cable from printer to USB port of NAS.

Service Options:

Enable – Allows you to enable/disable the selected service.

NOTE: You cannot enable a selected service if VG does not exist (NASVG is not yet initialized).

Name – Shows the service name.

Start on Boot – Allows the service to auto-start when the NAS starts.

Configuration – This contains basic configuration options (Quick Setup) which can be set by clicking the "Edit" button.

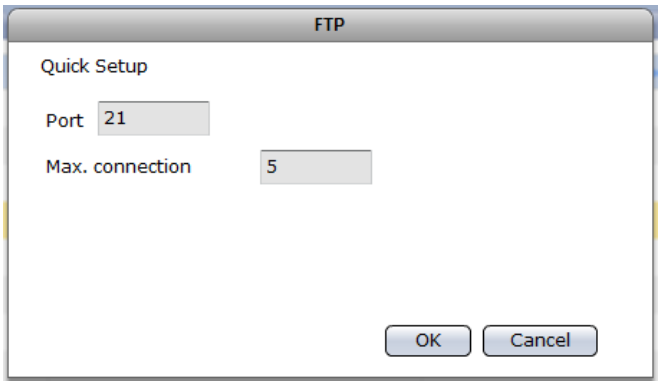
Edit – Click this button to configure the service.

Configuration (Quick Setup):

FTP Option:

Port – Use this option to set the FTP port number. Default FTP port used by the NAS is 21.

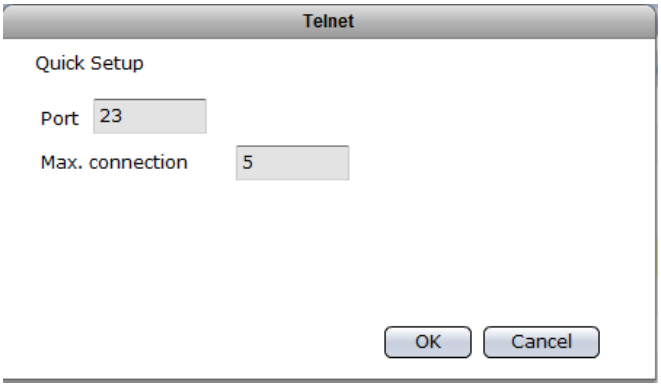
Max. connection – Specify the maximum number of allowed connections. Default is 5.



Telnet Option:

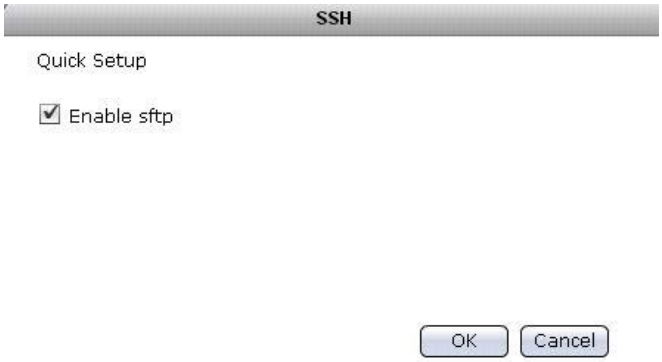
Port – Use this option to set the Telnet port number. Default Telnet port used by the NAS is 23.

Max. connection – Specify the maximum number of allowed connections. Default is 5.



SSH Option:

Enable sftp – Use this option to enable or disable SFTP in SSH. SFTP (Secure FTP) provides secure file transfer in SSH.

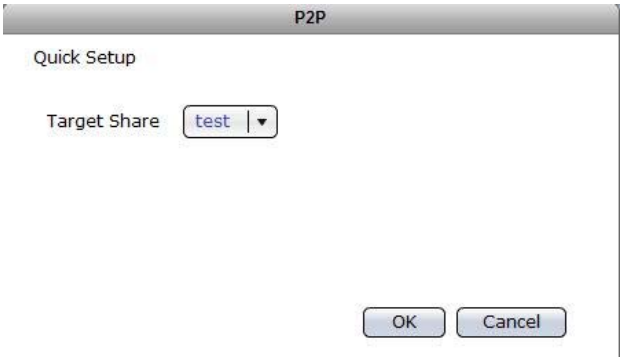


iTunes Option:

Set Share as iTunes Library – Select the share folder name that will be used as iTunes library from the list.

P2P Option:

Target Share – Select the share folder name that will be used as download location.



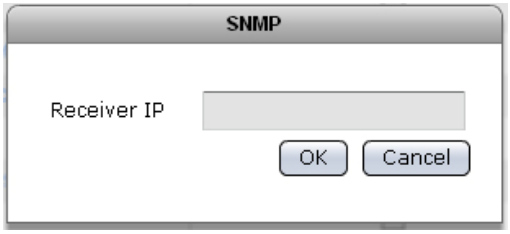
WEB Options:

Target Share – Select the share folder name that will be used as target location for web server files.

Enable SSL – Tick the box to enable SSL option.

SNMP Option:

Receiver IP – Means the SNMP trap IP address



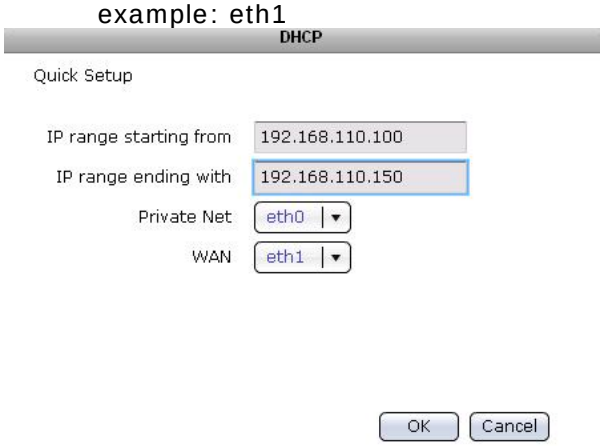
DHCP Options:

IP range starting from – Means the starting address of range of private IP addresses for DHCP.

IP range ending with – Means the ending address of range of private IP addresses for DHCP.

Private Net – The network device connected to the private network. For example: eth0

WAN – The network device connected to the Internet / WAN. For example: eth1



Media Server Options:

Target Share – Select the share folder where Media Server service will be enabled.

Please select LAN device – Select the network device to be used by Media Server service. The LAN device will be the dedicated path for media access.

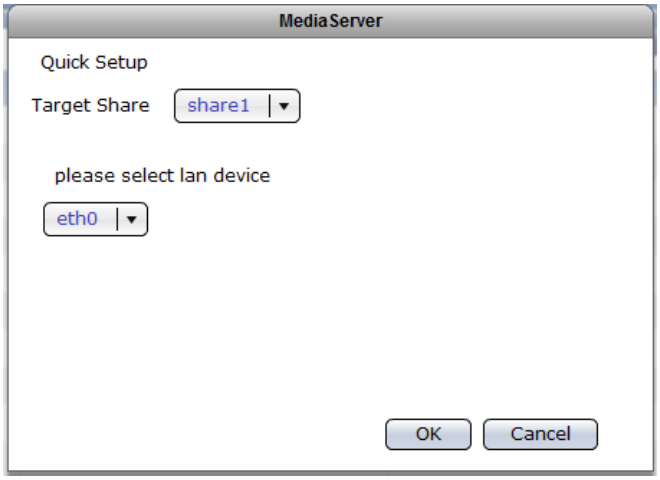
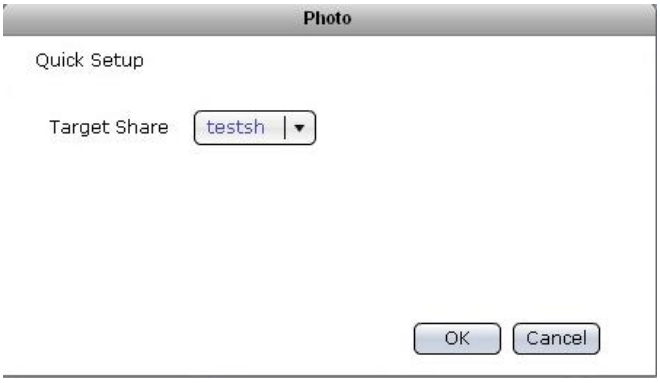


Photo Options:

Target Share – Select the share folder that will be used as target location of photo/images.



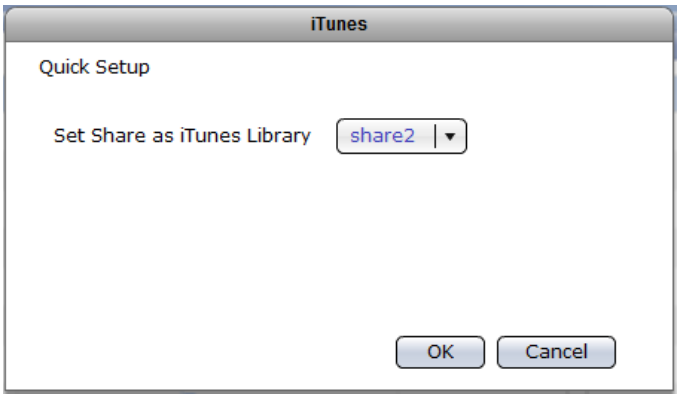
3.3.2.1 How to Use iTunes Service

NOTE: This section provides a simple example of how to use a NAS share folder as iTunes media folder. For more information about iTunes and how to use it, please visit http://www.apple.com/itunes/what-is/.

To use a NAS share folder as iTunes media folder:

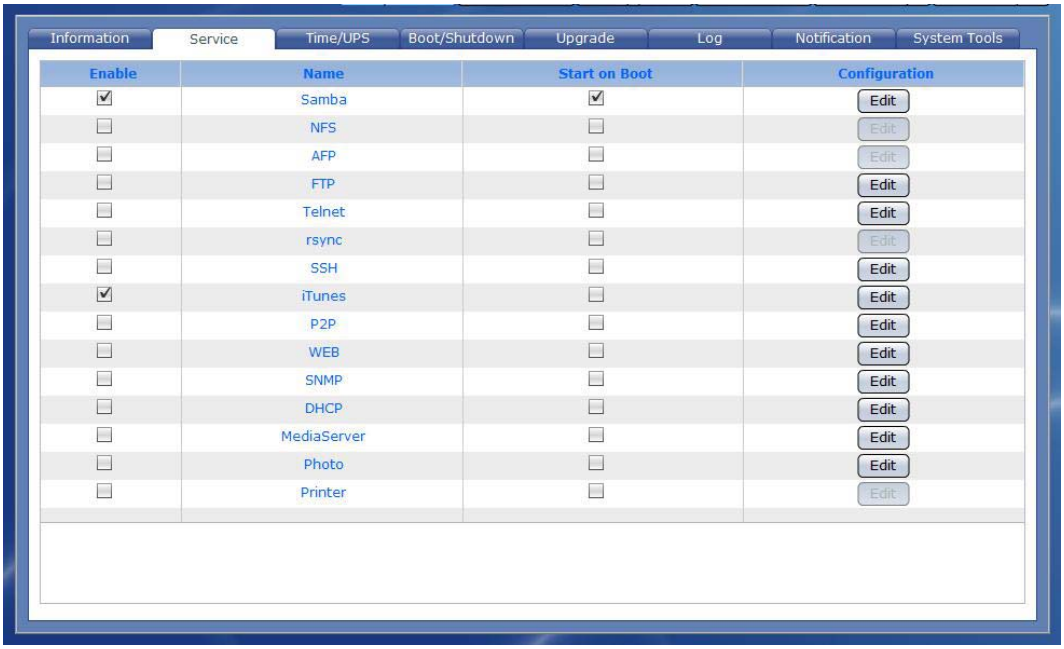
1. Select the iTunes service in "System" → "Service".
2. Click "Edit". Select the share folder that will be used by iTunes service.

   Set Share as iTunes Library – Select the share folder name that will be used as iTunes library from the list.

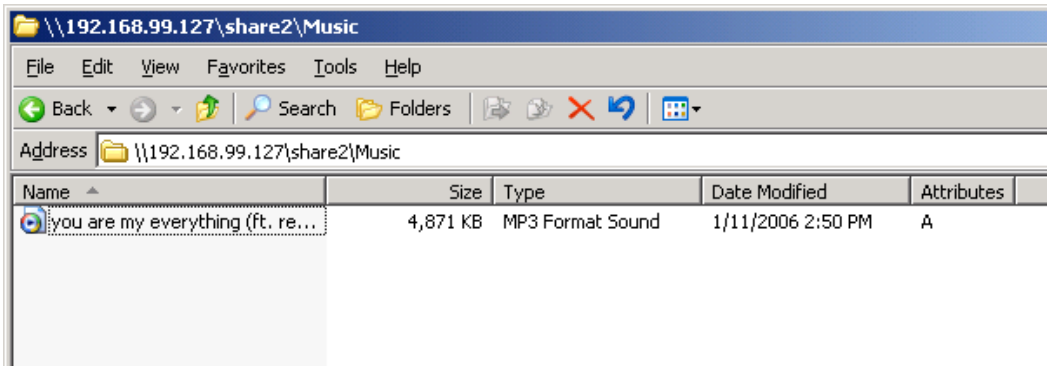


3. Click "OK" to save.

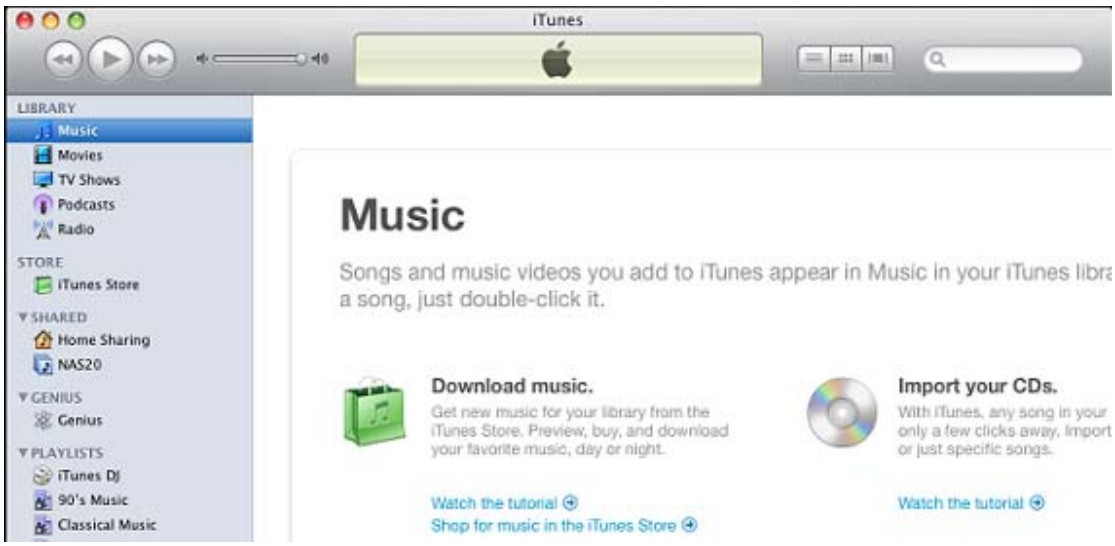
4. Click “Enable” option to enable iTunes service.



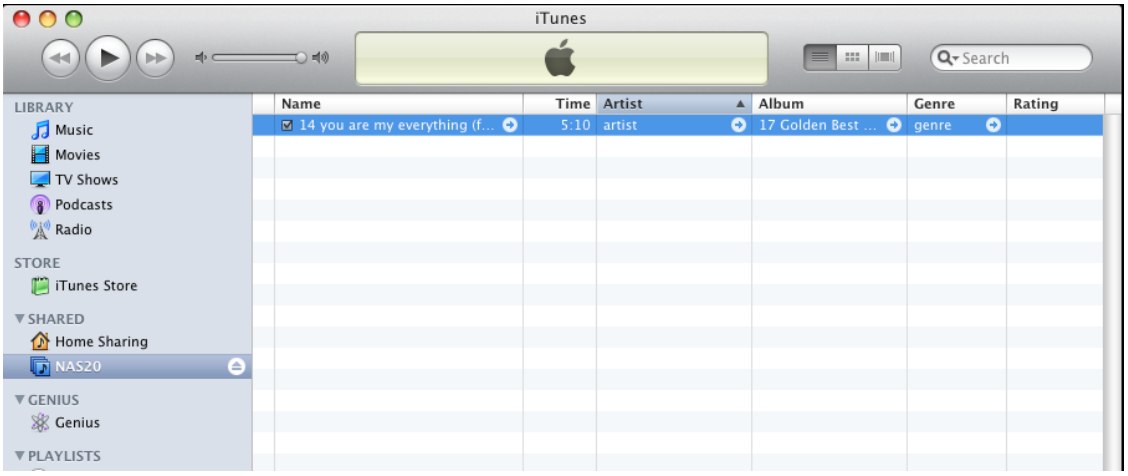
5. Copy some digital audio files to the share folder designated as iTunes Library and under the Music sub-folder. This can be done by accessing the NAS share folder via network (SMB protocol) and copying the audio files.



6. To play the digital music, open iTunes application in remote PC or Mac. Note that the NAS object name will appear in the SHARED list.



7. Select the NAS object in the shared library list. Then select the music to play from the list.



3.3.2.2 How to Use WEB Service

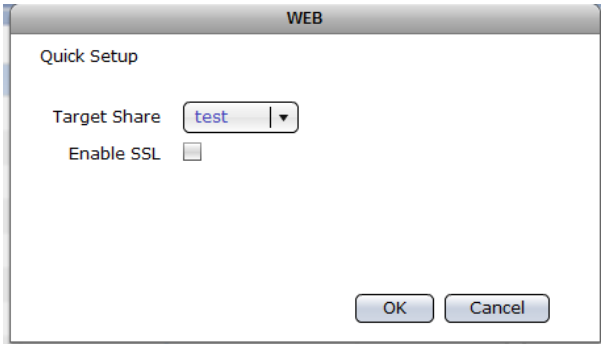
This section provides a simple example of how to setup WEB service and use a NAS share folder as repository of WEB files.

NOTE: Do not enable "Public" option on the share folder designated as WEB target share folder.

To use WEB service:

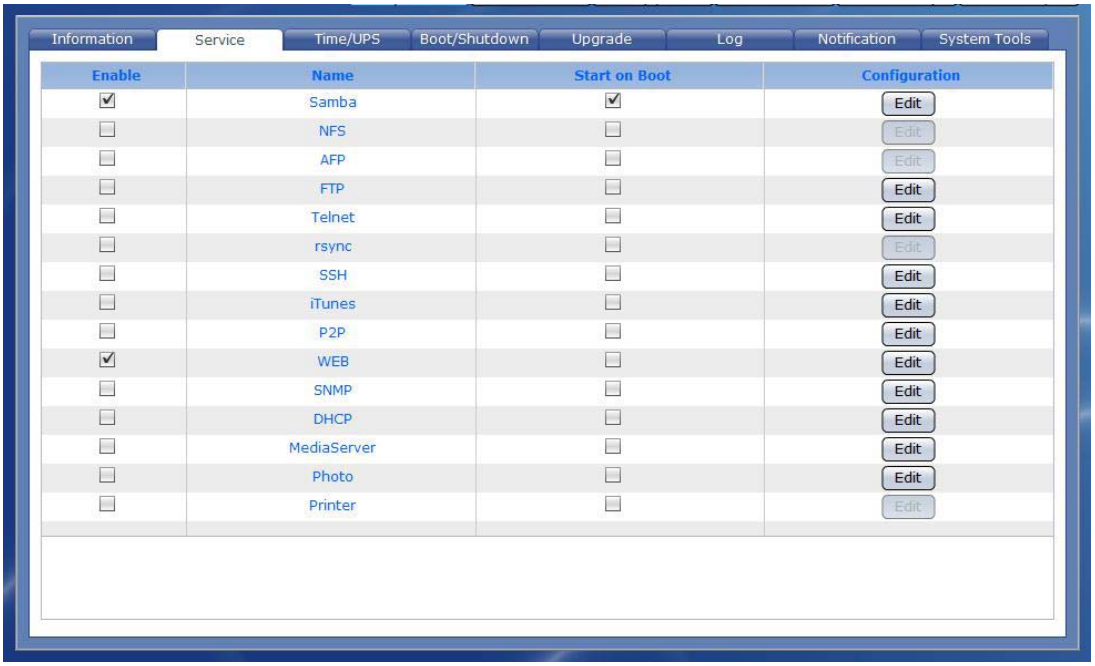
1. Select the WEB service in "System" → "Service".
2. Click "Edit". Configure the Target Share and select a share folder. If needed, enable SSL.

Target Share – Select the share folder name that will be used as target location for web server files.
Enable SSL – Tick the box to enable SSL option.

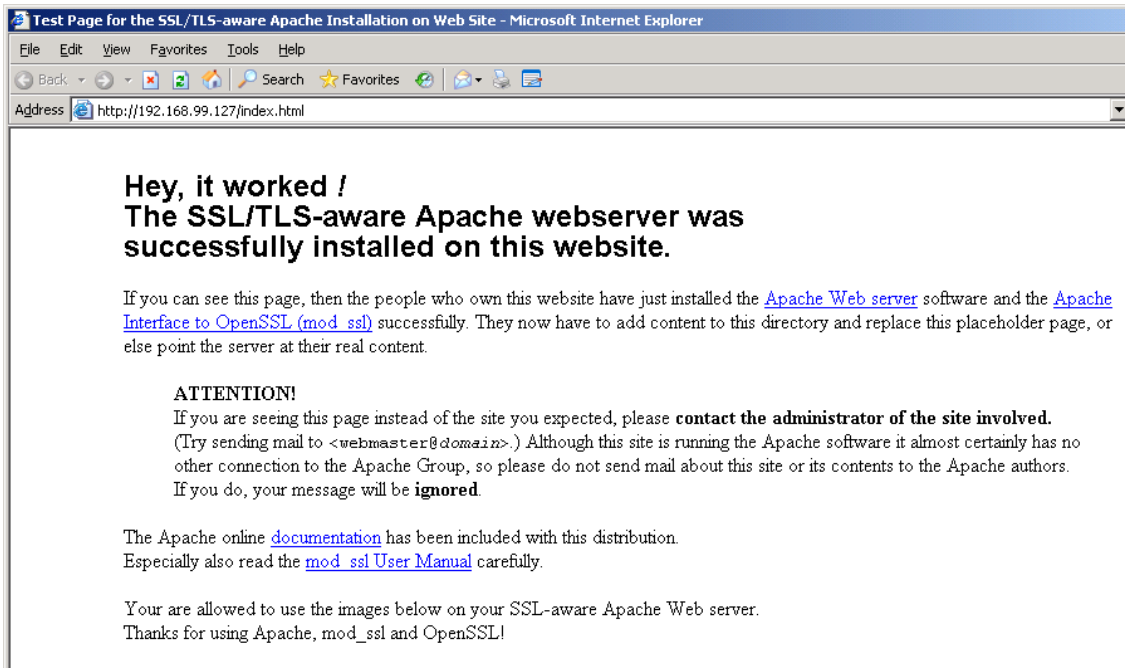


3. Click "OK" to save.

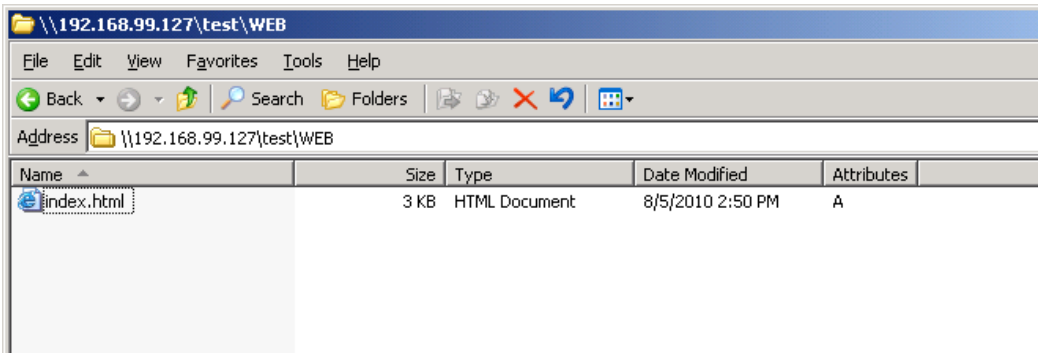
4. Click “Enable” option to enable WEB service.



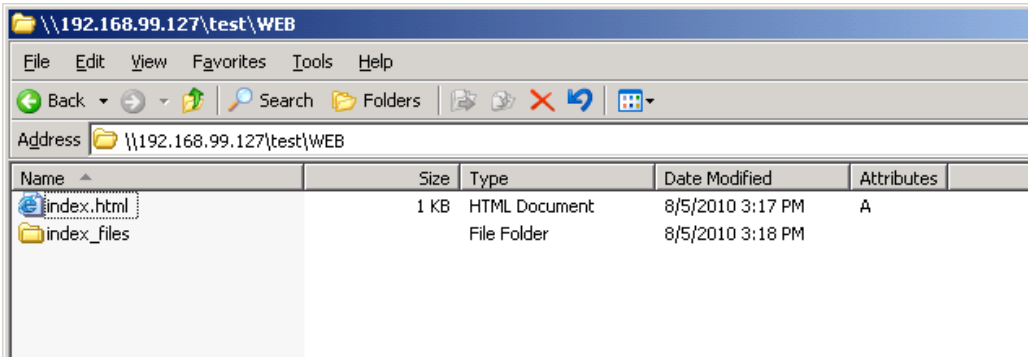
5. To test if web service is working, open web browser and enter http://x.x.x.x/index.html where x.x.x.x is the NAS IP. The default web page will be displayed.



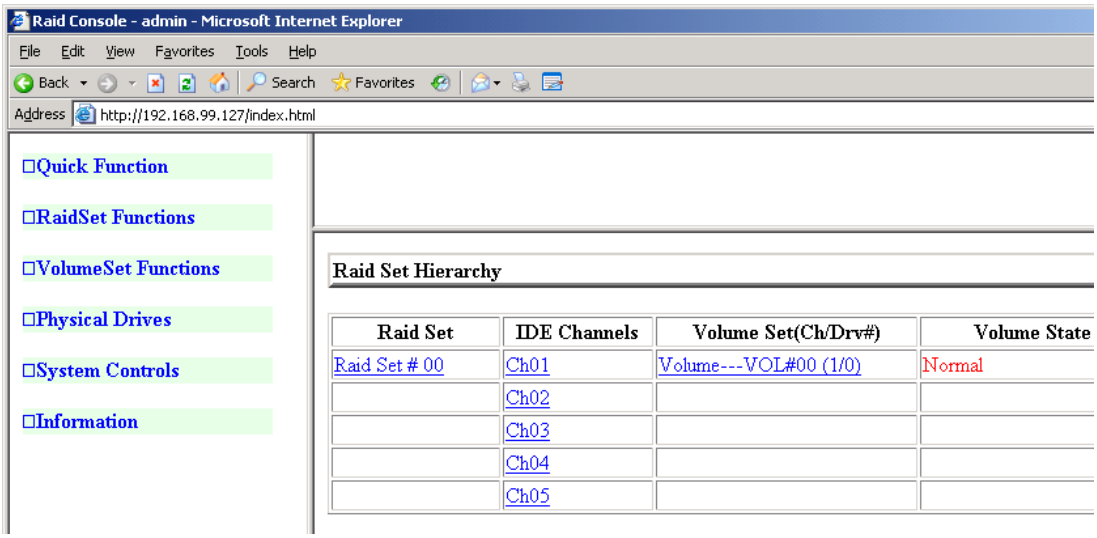
6. The default index.html file can be accessed via SMB/CIFS connection, and is saved in the WEB-designated share folder under WEB sub-folder. Delete the default index.html file.



7. Copy your own index.html file including the supporting folder/files.



8. Open web browser and enter http://x.x.x.x/index.html to verify if your web page will be displayed.

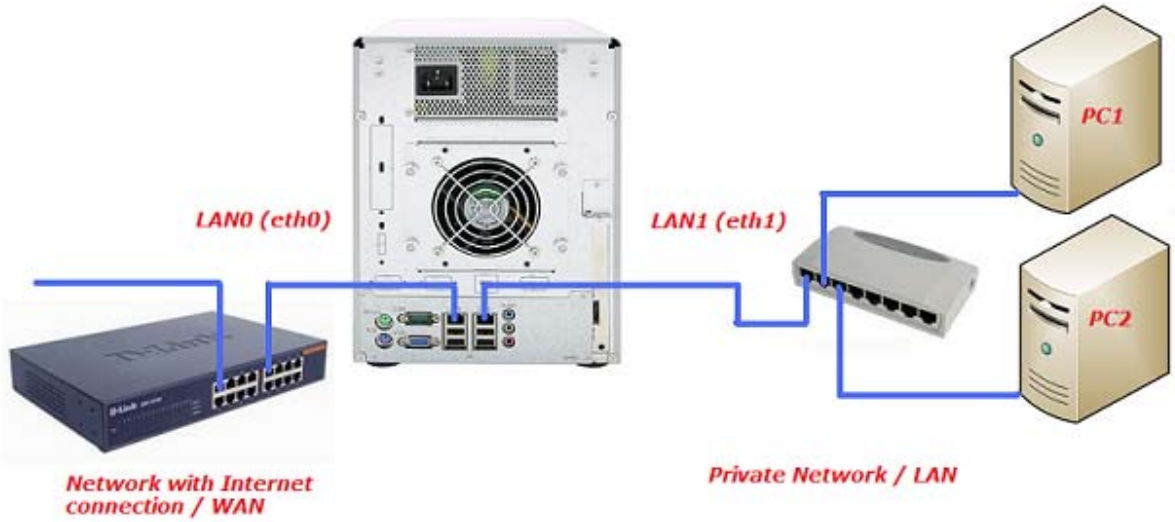


A sample web page

3.3.2.3 How to Use DHCP (Internet Gateway) Service

NAS provides DHCP / Internet Gateway function for administrator to easily enable and disable the Internet access for users on a private network. At the same time, the computers can get dynamic IP provided by the NAS which acts as DHCP server.

The diagram below shows an example of how to use the NAS as DHCP server and Internet Gateway.

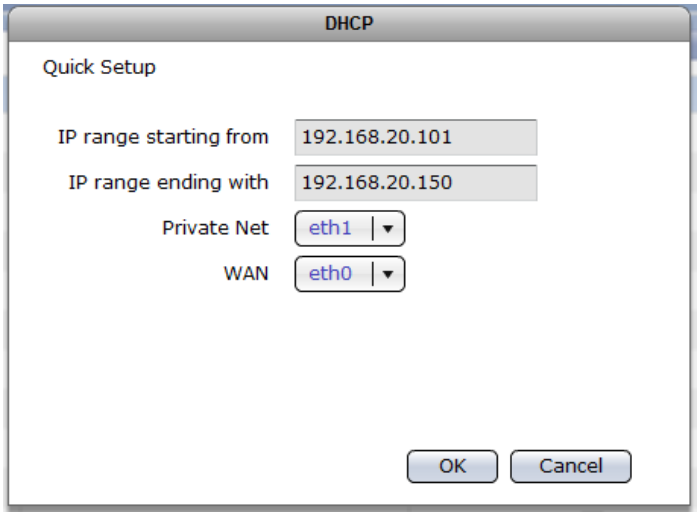


Before configuring the DHCP service, make sure the network devices eth0 and eth1 are already assigned the proper IP address in Network → Device Configuration.

To use the NAS as a DHCP server / Internet Gateway:

1. Select the DHCP service in "System" → "Service".
2. Click "Edit". Configure the following:

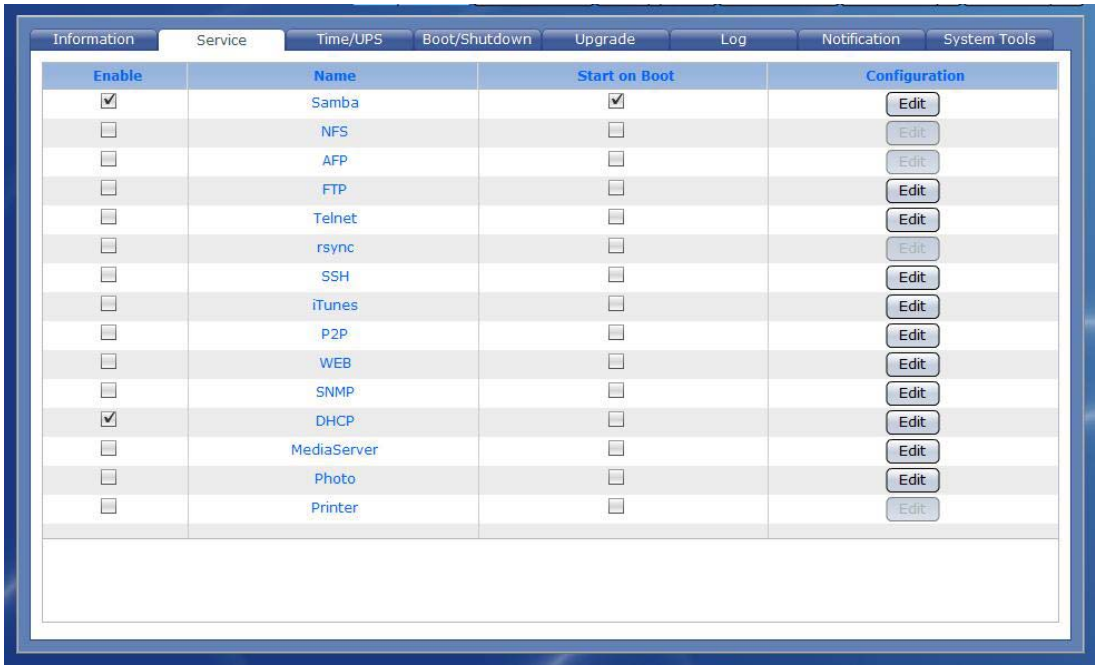
IP range starting from – Means the starting address of range of private IP addresses for DHCP.
IP range ending with – Means the ending address of range of private IP addresses for DHCP.
Private Net – The network device connected to the private network. For example: eth1
WAN – The network device connected to the Internet / WAN. For example: eth0



NOTE: In this example, eth1 is assigned to Private Net and must have an IP in the same subnet, for example: as 192.168.20.2

3. Click “OK” to save.

4. Tick the DHCP service to enable it.



5. Verify if the computers on the Private Network can get dynamic IP when configured with DHCP, and if there is internet access (eth0 should have internet access).

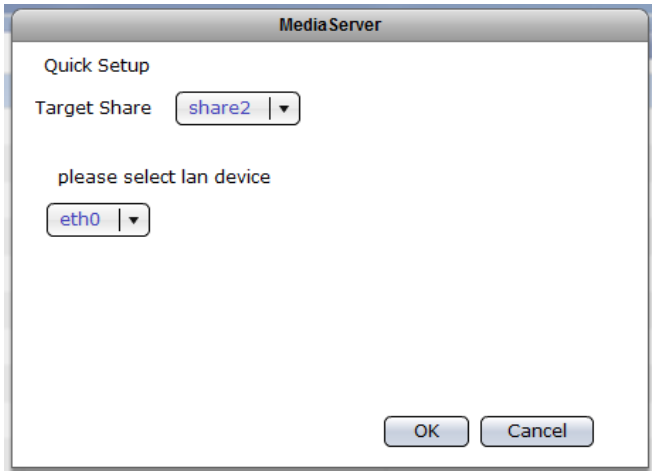
3.3.2.4 How to Use Media Server Service

This section provides a simple example of how to setup the NAS as DLNA (Digital Living Network Alliance) Media Server, and use a share folder as central repository of media files. DLNA compatible players must be used to access or play the media files.

To use Media Server Service:

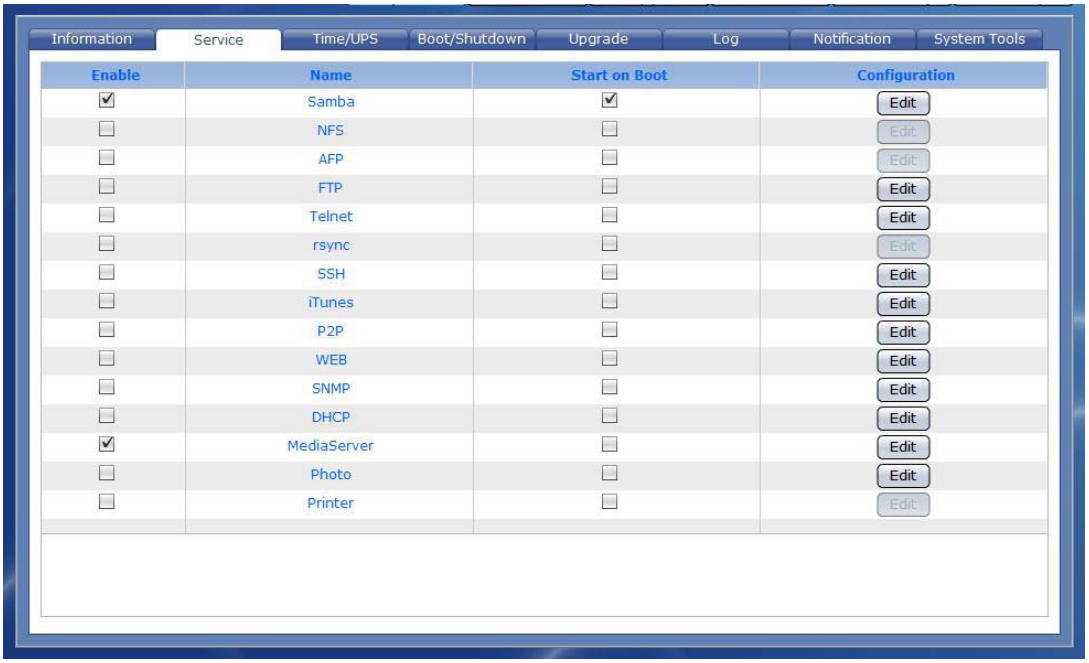
1. Select the Media Server service in “System” → “Service”.
2. Click “Edit”. Configure the Target Share and LAN device.

Target Share – Select the share folder where Media Server service will be enabled.
Please select LAN device – Select the network device to be used by Media Server service. The LAN device will be the dedicated path for media access.

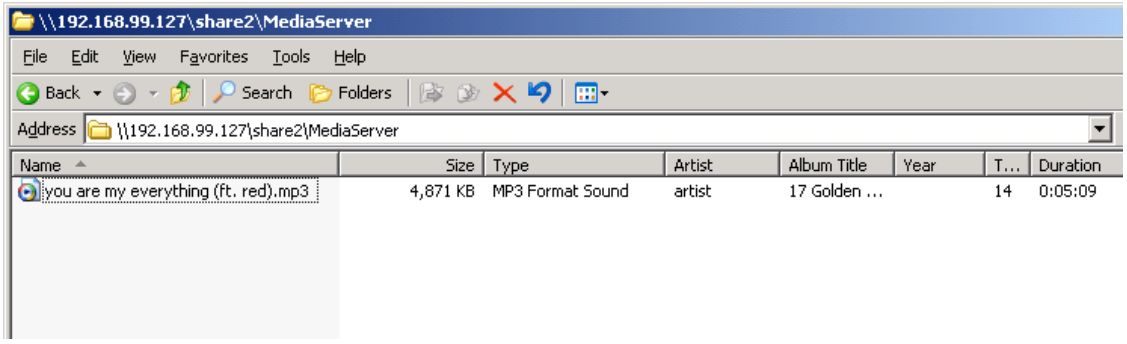


3. Click “OK” to save.

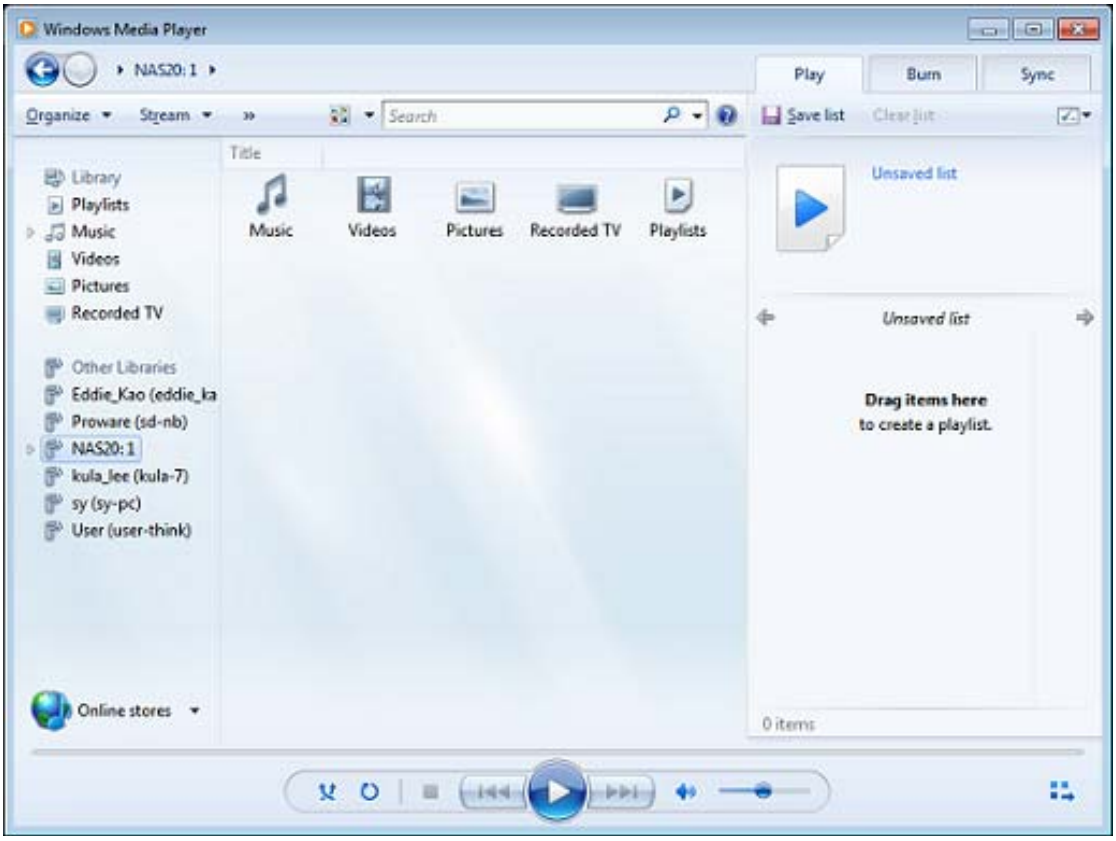
4. Tick the Media Server service to enable it.



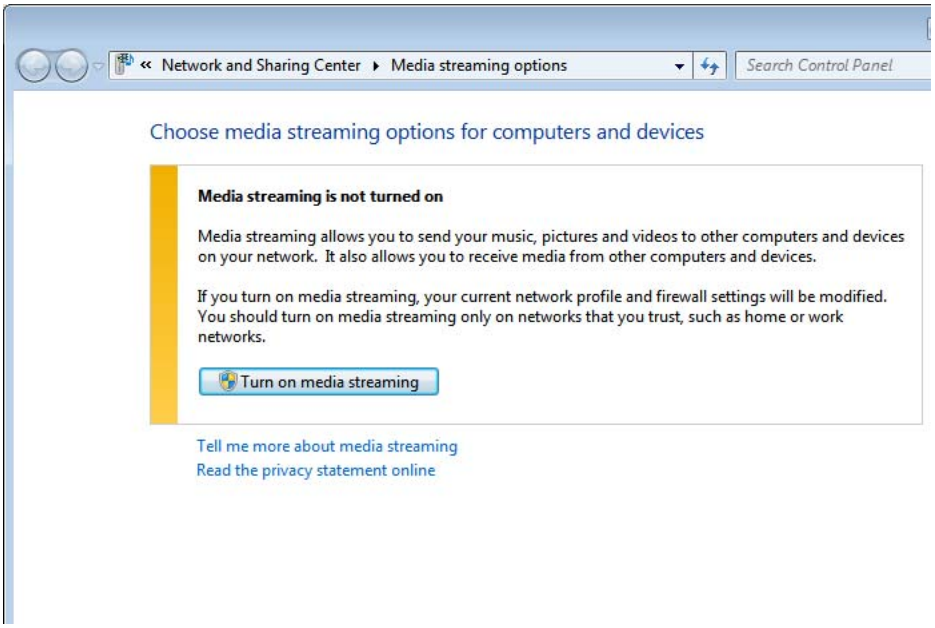
5. Copy the media file(s) to the share folder designated as Media Server Target Share under the MediaServer sub-folder. This can be done by accessing the NAS share folder via network (SMB/CIFS protocol) and copying the media file(s).

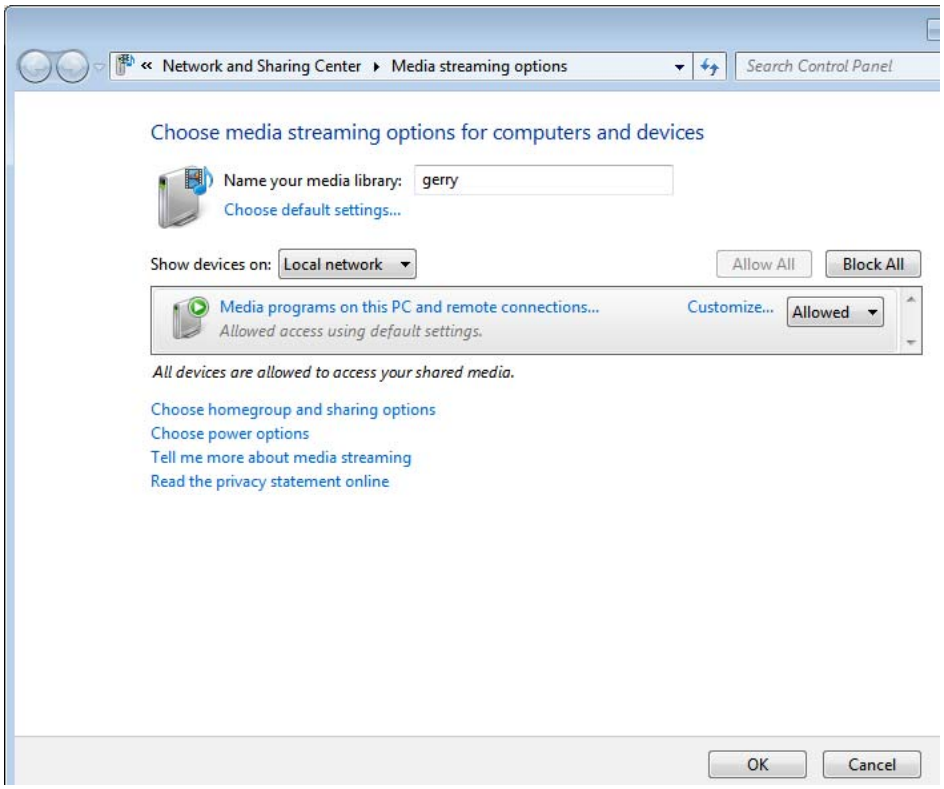


6. Open a DLNA compatible player. For example, Windows Media Player 12 in a PC with Windows 7 OS. The NAS object name should appear in the Other Libraries list.

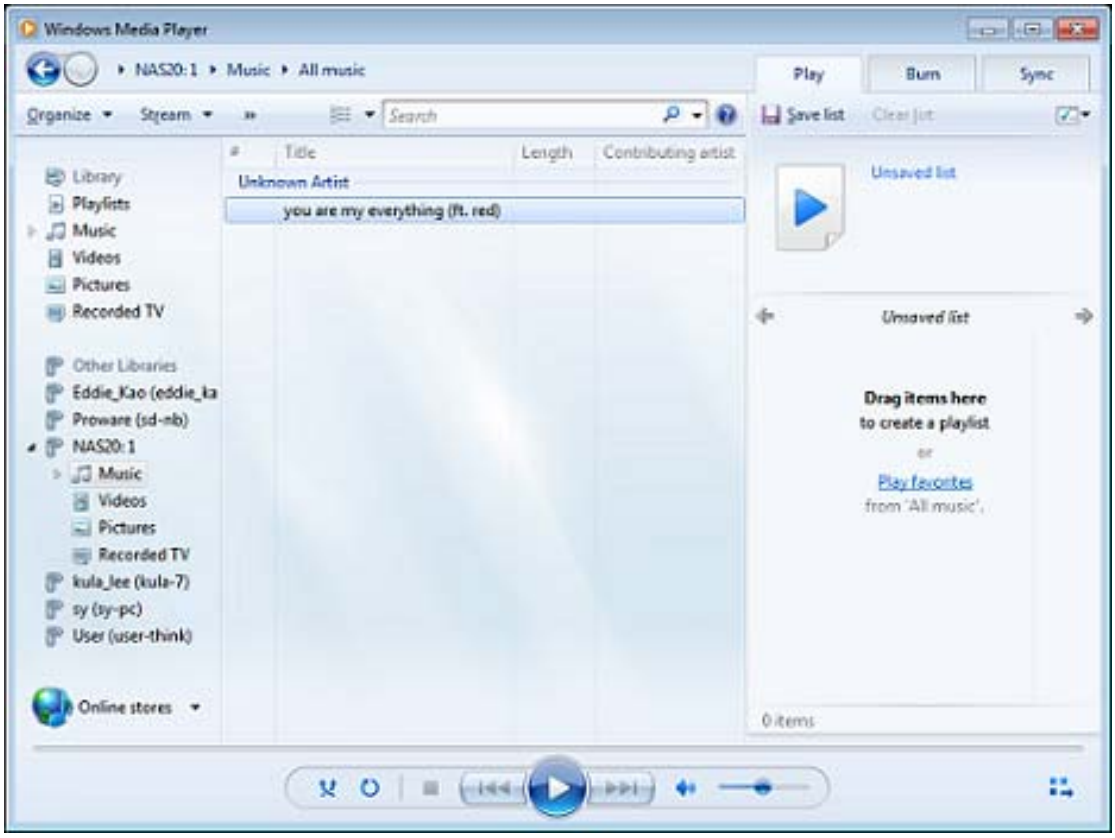


7. If you don't see the NAS object name in Other Libraries list of Windows Media Player, please check if Media Streaming is turned on. If not, turn it on.





8. Play the media (music).



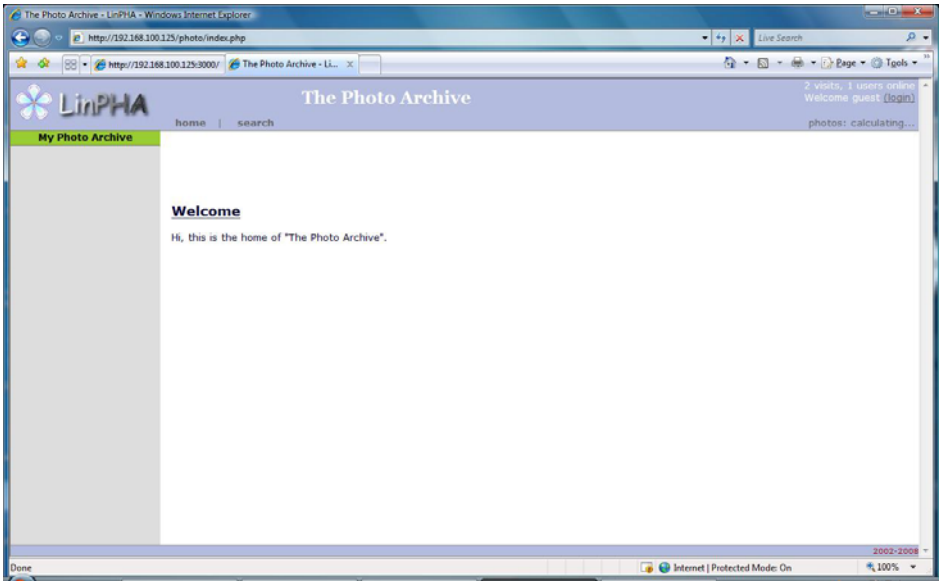
9. For other applications, copy the media files to the designated Media Server share folder under the MediaServer sub-folder, and use other DLNA compatible players to access or connect to NAS Media Server.

3.3.2.5 How to Use Photo Service

To use the Photo service:

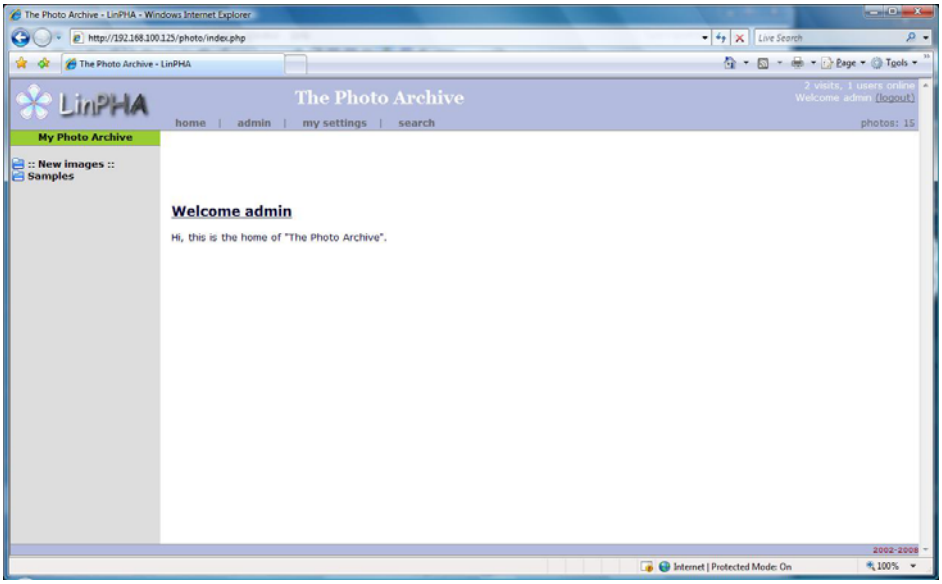
1. Enable the Photo Service, if not yet enabled, by selecting Photo service in System → Service tab. Click “Edit” and select the target share. Enable the Photo service by selecting the “Enable” check box on the left of the service name.

2. Open web browser and type **http://xxx.xxx.xxx.xxx/photo/** where xxx.xxx.xxx.xxx is the NAS IP address. The LinPHA Photo Archive page will be displayed.

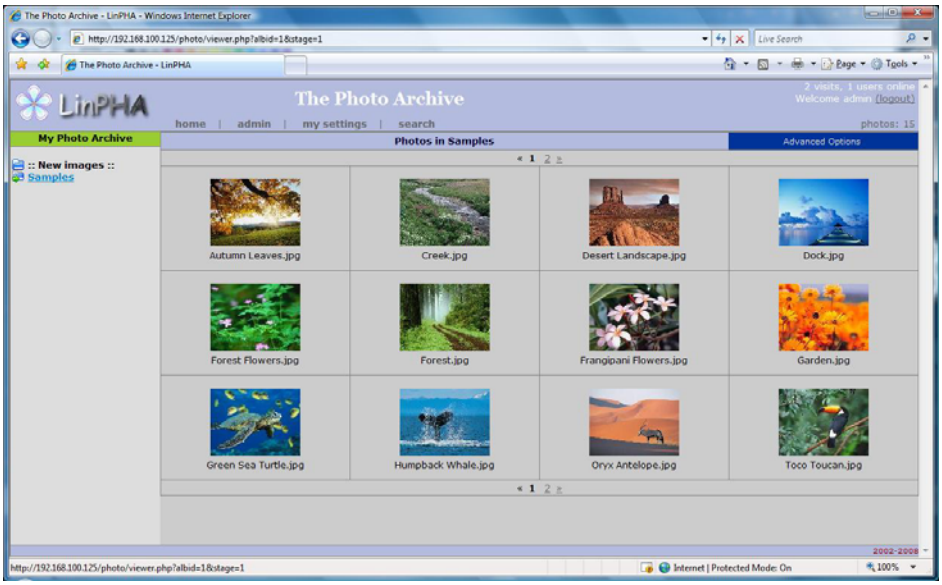


3. Click the “login” link in the upper right side then login as admin and enter admin’s password.

4. The Photo Archive home page will be displayed.

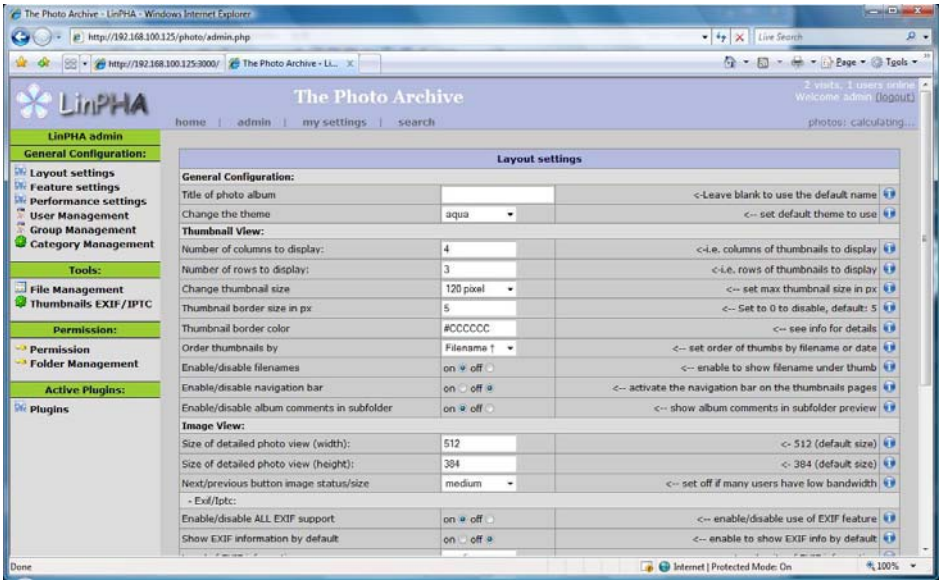


5. To view photos and images, select the folder links under “My Photo Archive”.

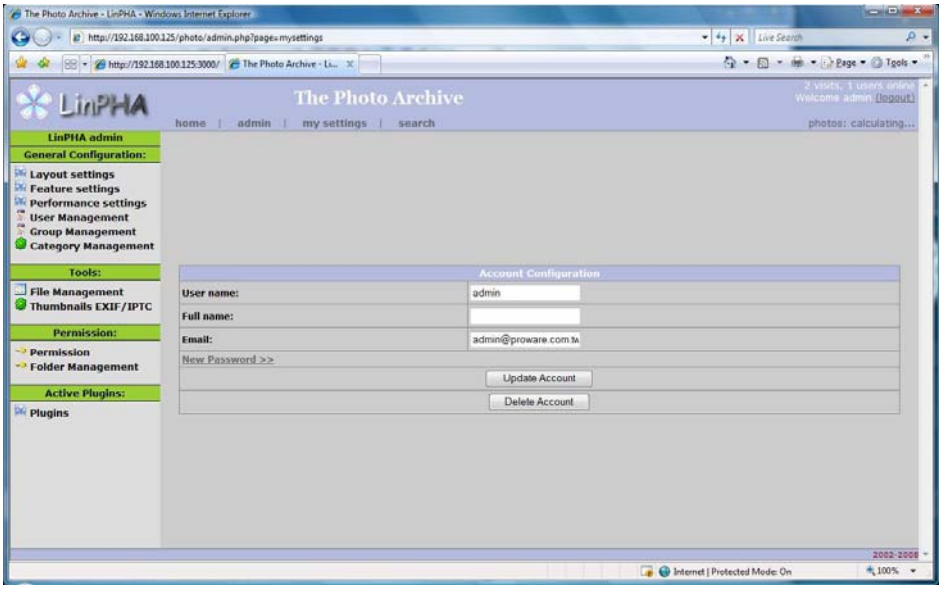


NOTE: The picture files must be saved in the NAS share designated as target location of Photo service and must be inside a subfolder. For example: share1\Photo\Samples, where share1 is the share name, Photo is the folder created by Photo service, and Samples is the subfolder containing photos or images.

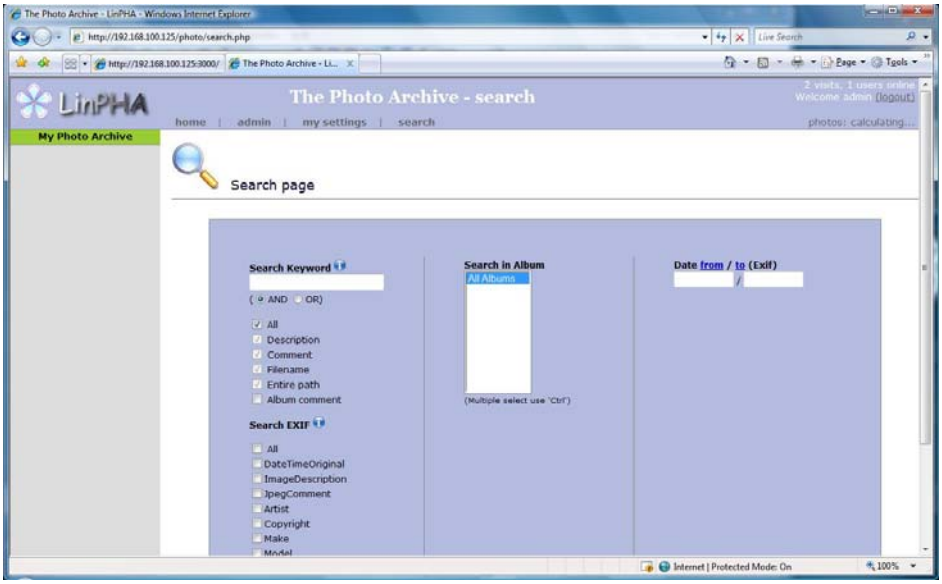
6. Select the “admin” tab to configure settings and options.



7. Select “my settings” to configure account details.



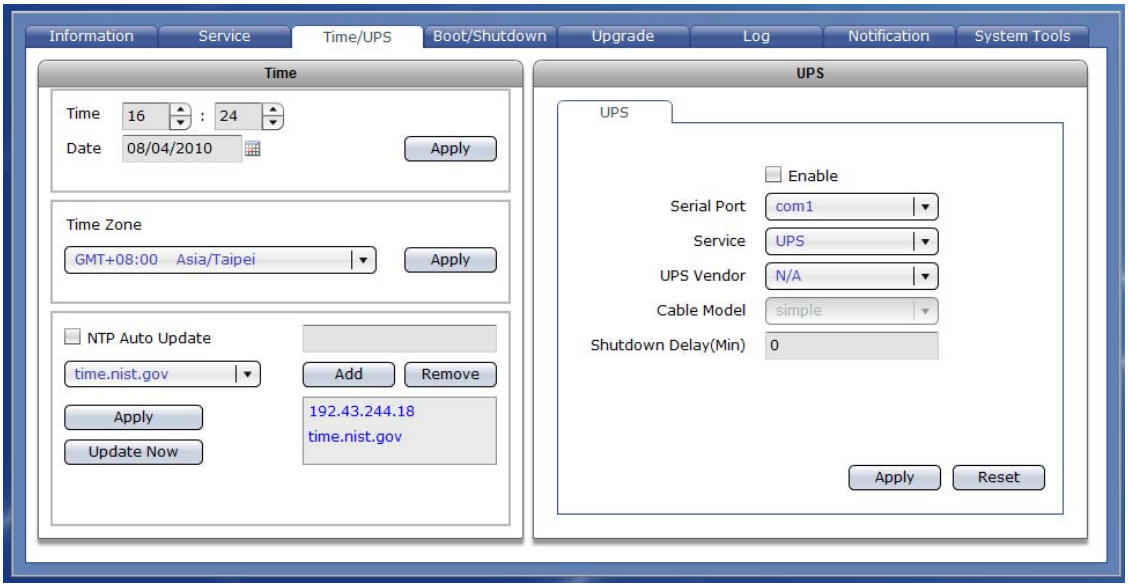
8. Select “search” tab for search options.



9. Click the “logout” link to logout.

3.3.3 Time/UPS

The system time, date, time zone, NTP option, and UPS can be configured here.



Time

To set Time, press up/down arrow in the hour and seconds boxes. To set Date, click the calendar icon on the right side and select the preferred date. To set Time Zone, click the down arrow and select the preferred time zone.

Apply – Use this button to save the changes made.

NTP Option

To select the NTP server, click the down arrow and select the preferred NTP server.

To immediately synchronize the system time from NTP server, press the “Update Now” button. To enable automatic update of system time from NTP server, check the “Auto Update” option.

NTP Auto Update – Check this option to enable automatic update of system time from NTP server.
Apply – Use this button to save the changes made.
Update Now – Use this button to manually update the system time and synchronize from NTP server.
Add – Use this button to add an NTP server. Enter the NTP server IP address in the box provided then click this button.
Remove – Use this button to remove an NTP server. Select the NTP server from the list then click this button.

UPS

Use the settings here to configure the UPS.

Enable – Use the option to enable or disable UPS support for serial port.

Serial Port – Use this option to select serial port option. Available option is **com1** only.

NOTE: In NAS models with com2 serial port, com2 is reserved for SES use.

Service – Use this option to select the type of UPS, whether **UPS** (smart) or **Dumb UPS**.

UPS Vendor – Use this option to select the UPS vendor. Currently, only **APC** and **Beam-Tech** UPS models are supported.

NOTE: Users/customers must use only the supported UPS vendor models: APC and Beam-Tech. If other UPS models are used, there is no guarantee that the NAS will be able to communicate to the UPS. The basic UPS function (to provide uninterrupted power supply to the NAS) will probably work but the Shutdown Delay might not work using the UPS cable from the "unsupported" UPS vendor model.
Other UPS vendor models will be added to the approved models in the future.

Cable Model – Use this option to select the UPS cable type.
Options for **APC** are: **simple**, **smart**, **ether**, and **usb**.
Please refer to the APC UPS specification for the UPS cable type used in the particular APC UPS model.

Shutdown Delay (Min) – Use this option to set the delay time in minutes. After a power failure, UPS will shutdown the NAS when the Shutdown Delay time has expired.

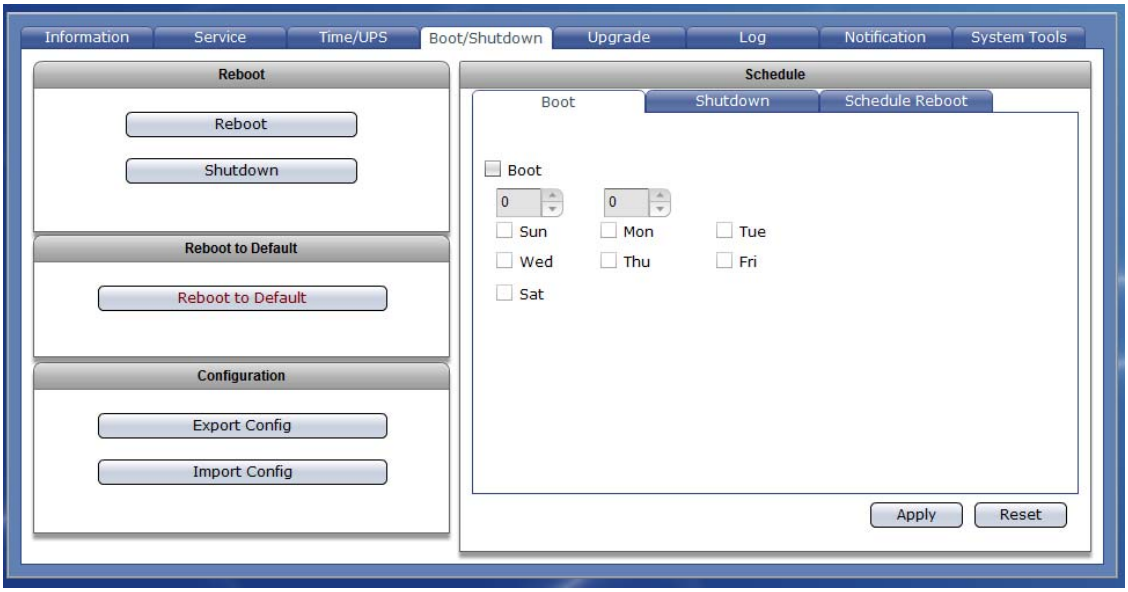
NOTE: For most cases, it is recommended to use a value of 1 instead of 0 (zero) in Shutdown Delay.
When set to 0, the timer is disabled and the UPS will shutdown the NAS depending on the battery level and/or remaining runtime, or when the UPS battery is exhausted.
However, some types of UPS cables, which do not support low battery detection, might not work when Shutdown Delay is set to 0.

Reset – Use this button to undo or clear any changes made.

Apply – Use this button to save the changes made.

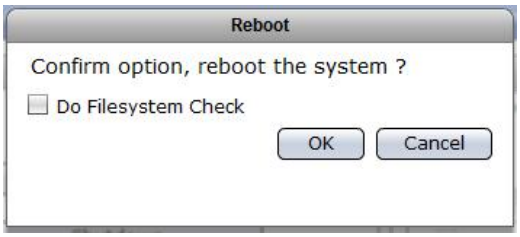
3.3.4 Boot/Shutdown

The NAS can be restarted or shutdown manually or based on schedule.



Reboot:

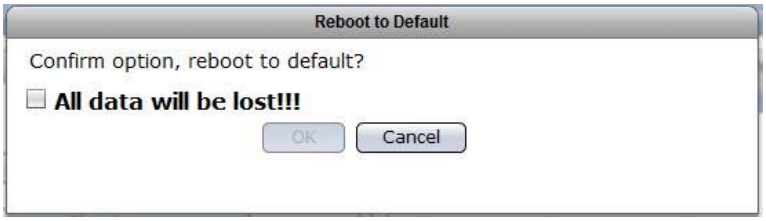
Reboot – Use the button to immediately reboot the NAS. If needed, you can also enable “Do Filesystem Check” option to perform filesystem check after reboot.



Shutdown – Use this button to immediately shutdown the NAS. When a warning message is displayed, select “Yes” to shutdown the system.

Reboot to Default:

Reboot to Default – Use this button to reboot the NAS and restore to default configuration.

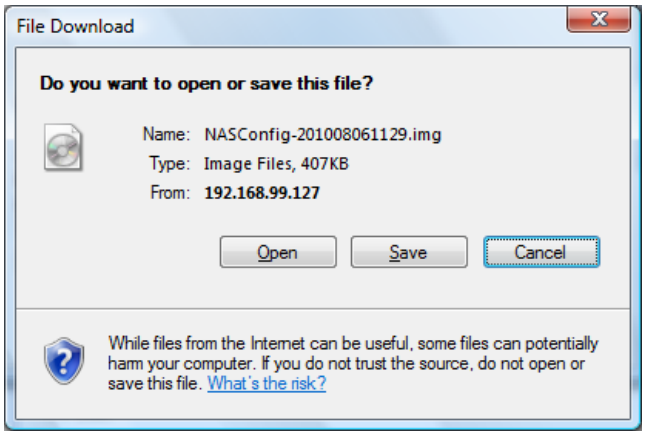


WARNING! Use the "Reboot to Default" function with care. Resetting the NAS to default configuration will delete the current NAS settings and erase all existing data.

NOTE: If you have made a Data Backup to Local Disk (or external eSATA disk), shutdown the NAS and remove the Local Disk (or eSATA disk) with Data Backup, then power on the NAS and do "Reboot to Default". If the Local Disk with Data Backup is in the NAS when "Reboot to Default" is executed, the data on the Local Disk will also be cleared.

Configuration:

Export Config – Use this button to export the NAS system configuration and save as image file, which can be used later for restoration. After clicking "Export Config", click "Save" to save the configuration image file.



NOTE: Your web browser might be configured to block pop-ups. You need to allow pop-ups (temporarily) to be able to download and save the configuration file.

Import Config – Use this button to import and restore a previously saved (exported) NAS system configuration.

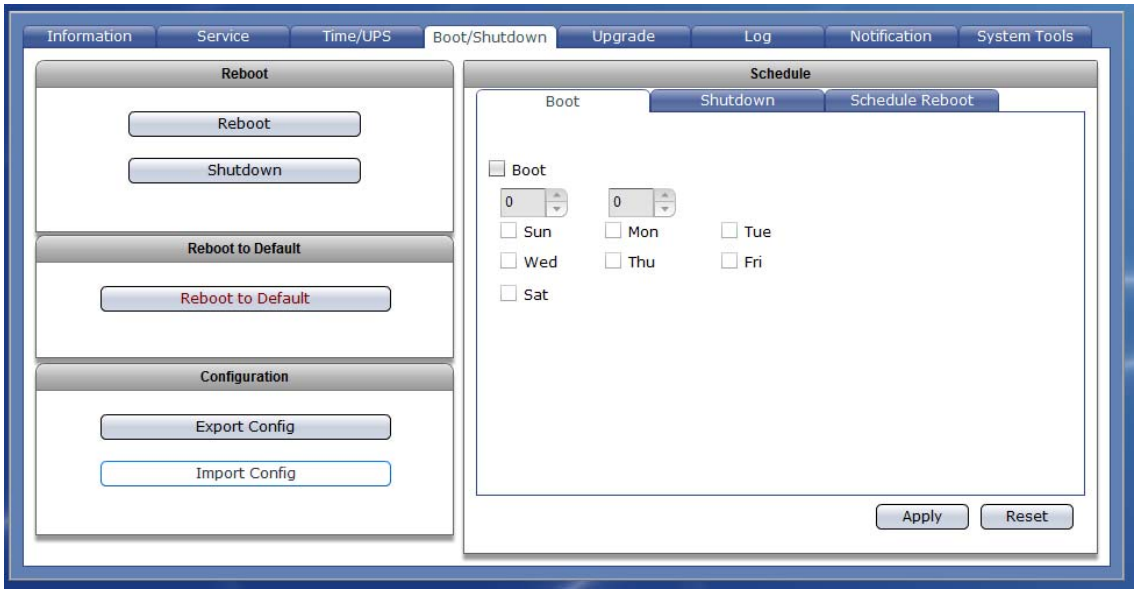
NOTE: Import Config function requires that the NAS be reset to factory default setting before a saved configuration file can be restored.

NOTE: If you have made a Data Backup to Local Disk (or external eSATA disk), shutdown the NAS and remove the Local Disk (or eSATA disk) with Data Backup, then power on the NAS and do "Reboot to Default". If the Local Disk with Data Backup is in the NAS when "Reboot to Default" is executed, the data on the Local Disk will also be cleared.

To import configuration:

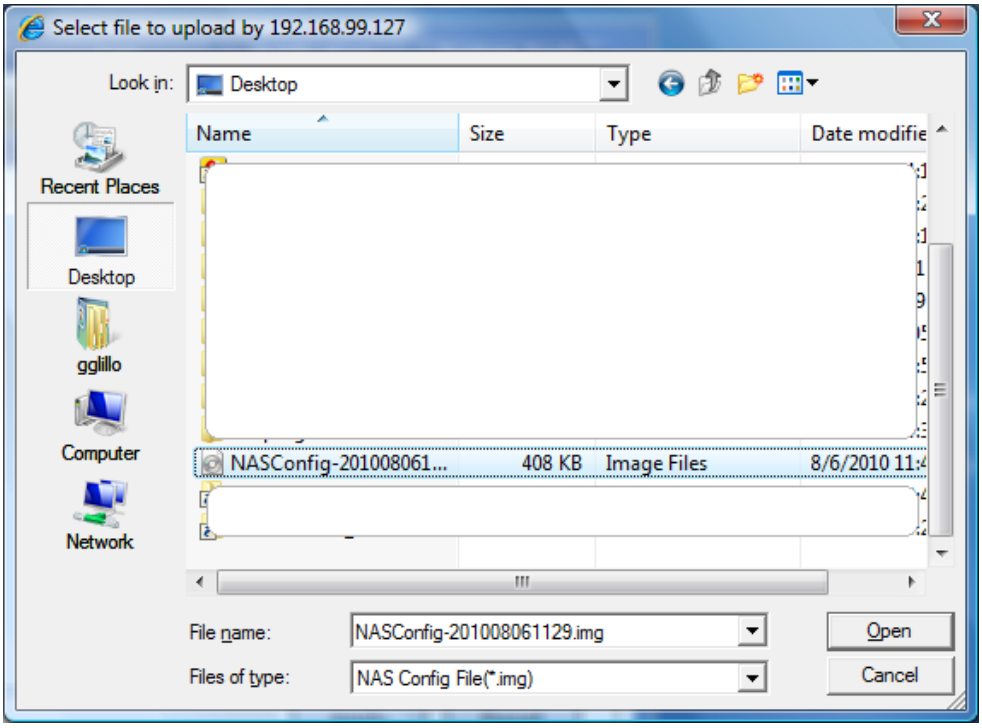
1. Use "Reboot to Default" to reset the NAS to factory default settings.
2. After reset to default, login to NAS GUI. You may need to verify the assigned IP of the NAS.
3. When the warning message below appears, select "No".

4. Select “System” → “Boot/Shutdown” → “Import Config”.

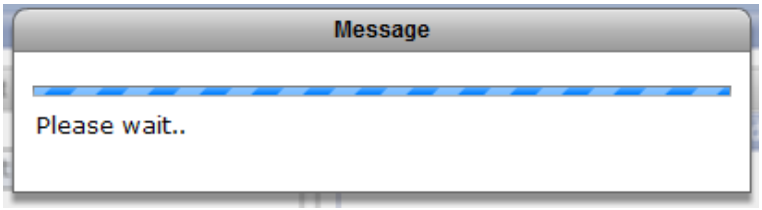


5. A warning message will be displayed. Make sure the NAS where configuration will be imported has the same environment as the NAS configuration that will be restored, such as same number of disk drives, same NAS firmware version, etc. Click “Yes” to continue.

6. Select the NAS configuration file to be imported. Click “Open”.



7. A process status message will be displayed.



8. A reboot warning message will be displayed. Select “Yes” to reboot.

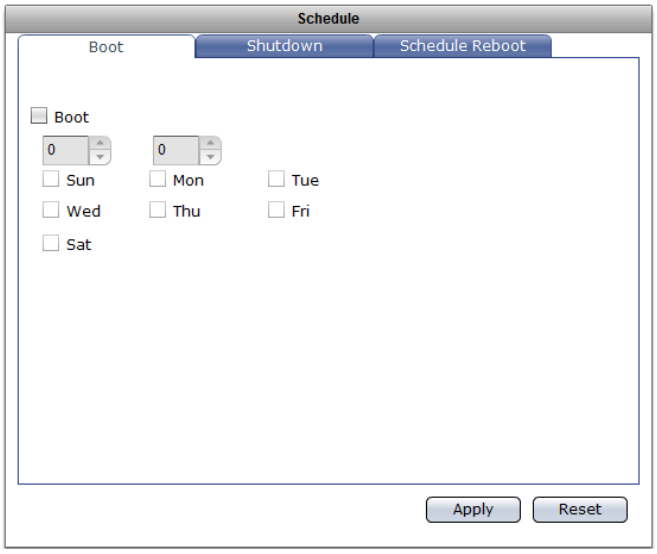
9. The imported configuration file will be restored to the NAS. Login to NAS GUI.

Schedule:

Use the options here to boot, shutdown, or reboot the NAS based on schedule.

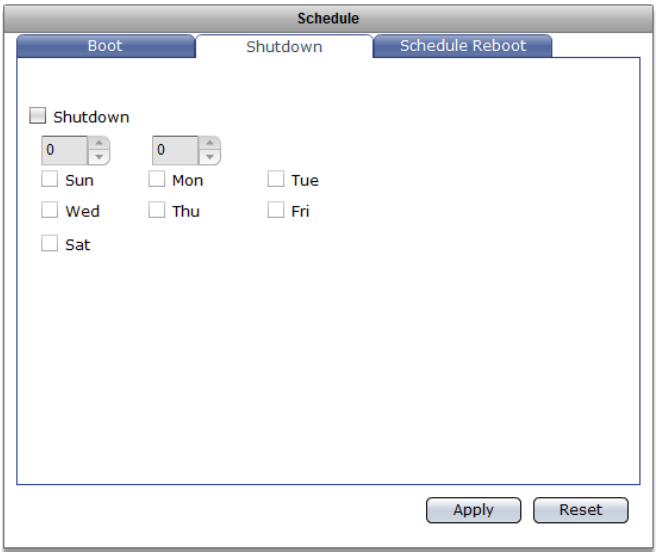
Boot

Boot – Use the option to enable or disable scheduled boot of NAS.
Set the time (hour and minutes) in the up/down arrow boxes.
Select the day or days when the scheduled boot will happen.



Shutdown

Shutdown – Use this option to enable or disable scheduled shutdown of NAS.
Set the time (hour and minutes) in the up/down arrow boxes.
Select the day or days when the scheduled shutdown will happen.

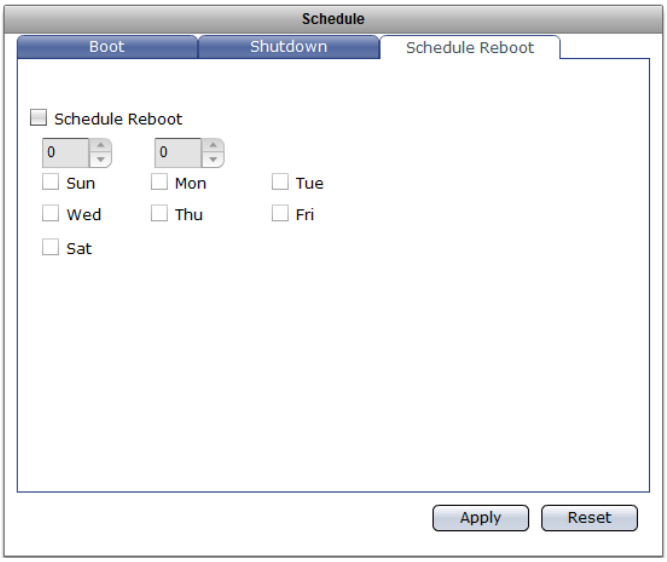


Schedule Reboot

Schedule Reboot – Use this option to enable or disable scheduled reboot of NAS.

Set the time (hour and minutes) in the up/down arrow boxes.

Select the day or days when the scheduled reboot will happen.



Apply – Use this button to save the changes made.

Reset – Use this button to undo or clear any changes made.

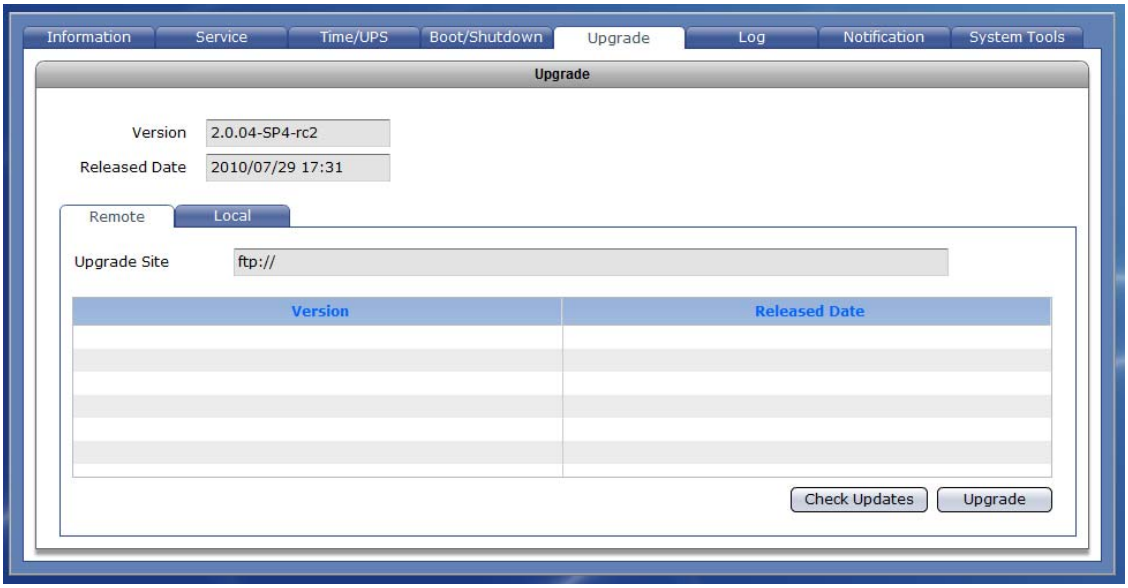
3.3.5 Upgrade

The NAS firmware can be upgraded remotely from FTP server or manually from local directory.

3.3.5.1 Remote Upgrade

Remote

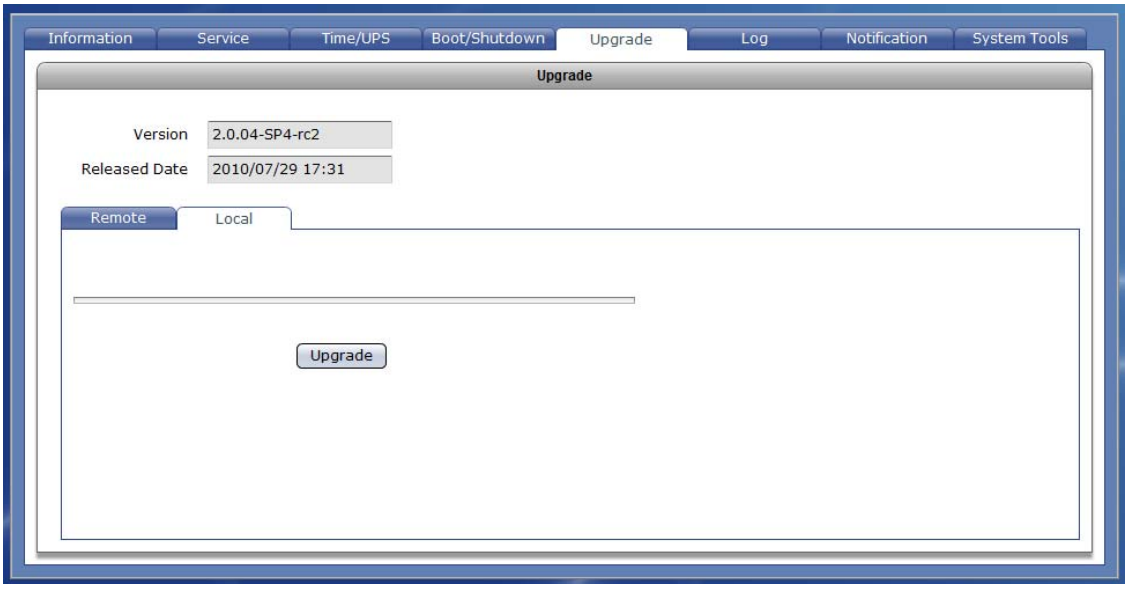
To upgrade remotely, press the “Check Updates” button. The available NAS firmware version will be listed. Select the firmware version then click the “Upgrade” button. The NAS firmware version will be updated. NAS will restart to load the updates.

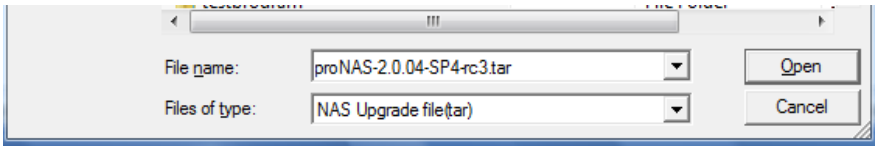


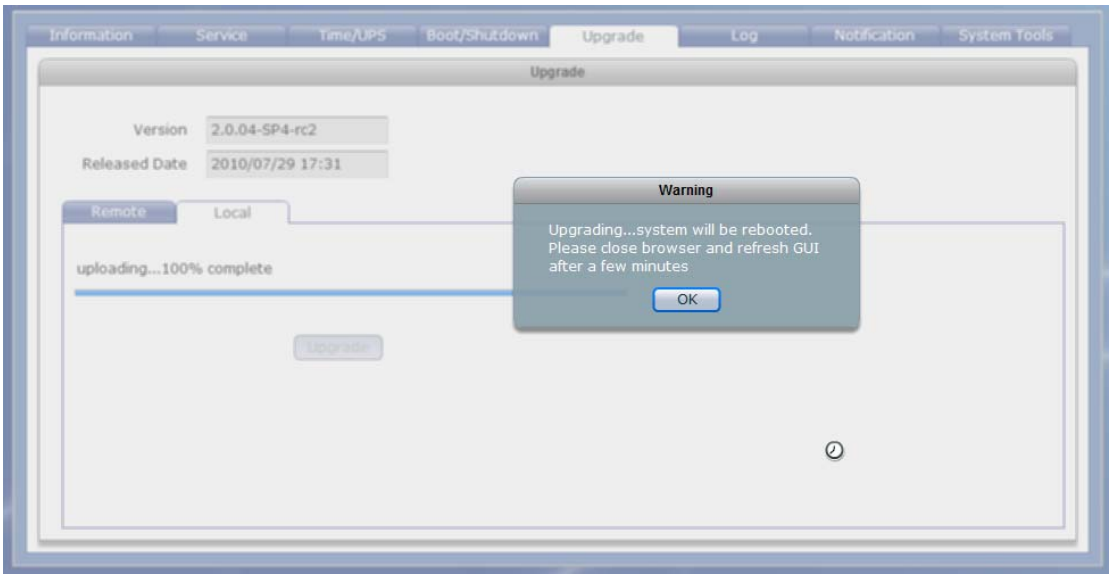
3.3.5.2 Local Upgrade

Local

To upgrade locally, the NAS firmware must have been downloaded from vendor's FTP site and saved into local directory. Click the "Upgrade" button, select the NAS upgrade file (tar file), and click Open. The NAS firmware version will be updated. NAS will restart to load the updates.







3.3.6 Log

NAS logs can be viewed in this tab.

Log Options:

Date – Shows the date and time when the particular log happened. Use the down arrow to select the day or days that will be used to display the log. Options are: Today, Past 7 Days, Past 14 Days, Past 30 Days, and All.

Type – Shows the type of log. Use the down arrow to select the type of log to display. Options are: All, System, Storage, Share, and Account.

Level – Shows the log level. Use the down arrow to select the level of log to display. Options are: All, DEBUG, INFO, WARN, and ERROR.

Message – Shows information about the log.

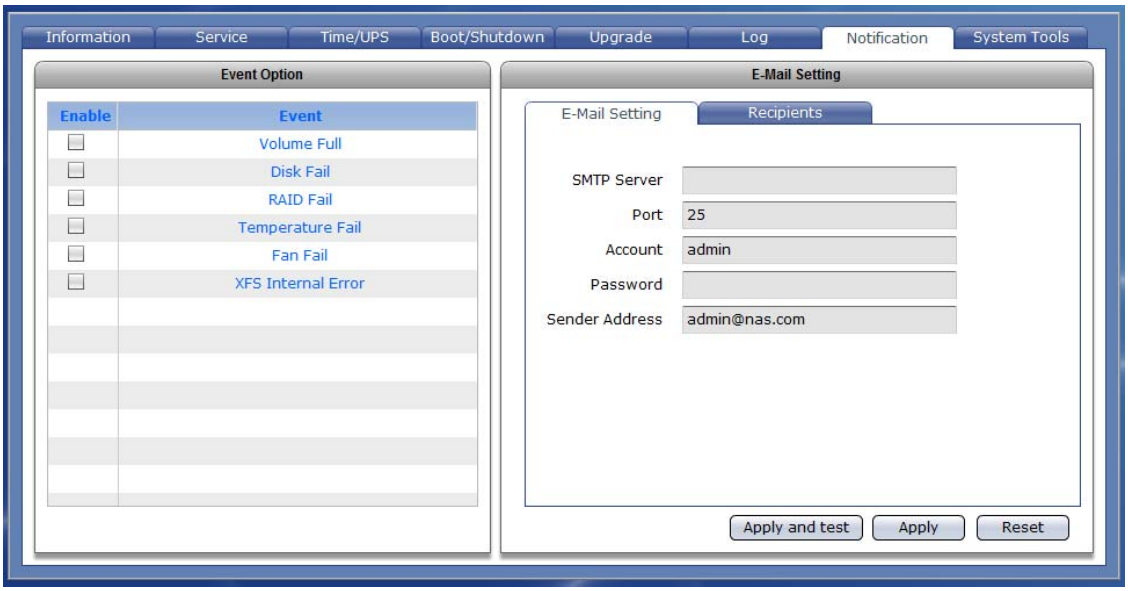
Download system logs – Use this button to save all proNAS logs to a log file in local directory. The log file will be given ".tar" extension name. Rename the log file if needed.

Refresh – Use this button to update the log information displayed.

3.3.7 Notification

3.3.7.1 Event Option

Use this function to enable event notification via email.



Event Option

Enable - Check the event(s) that will be included in list of events that will be monitored. Once the selected event happened, the email recipient(s) will receive a notification mail.

Event List:
Volume Full
Disk Fail
RAID Fail
Temperature Fail
Fan Fail
XFS Internal Error

3.3.7.2 Email Setting

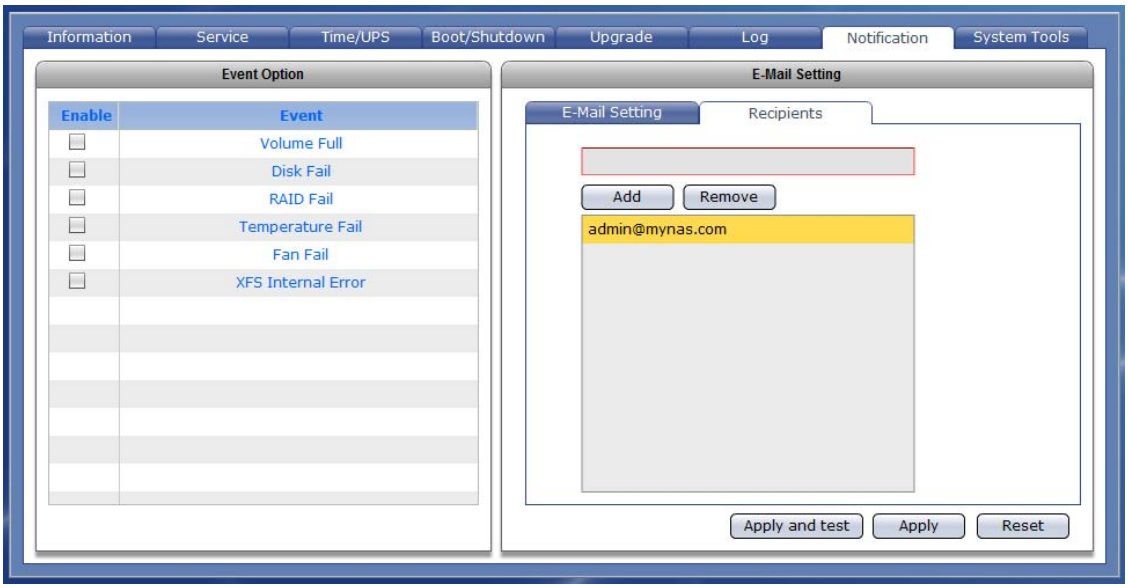
Email Setting Options:

SMTP Server – Use this option to enter the SMTP server IP address.
Port – Use this option to set the SMTP port number. Default is port 25.
Account – Use this option to enter a valid email account in the SMTP server.
Password – Use this option to enter the password of the email account.
Sender Address – Use this option to specify the sender's email address.

Recipients Options:

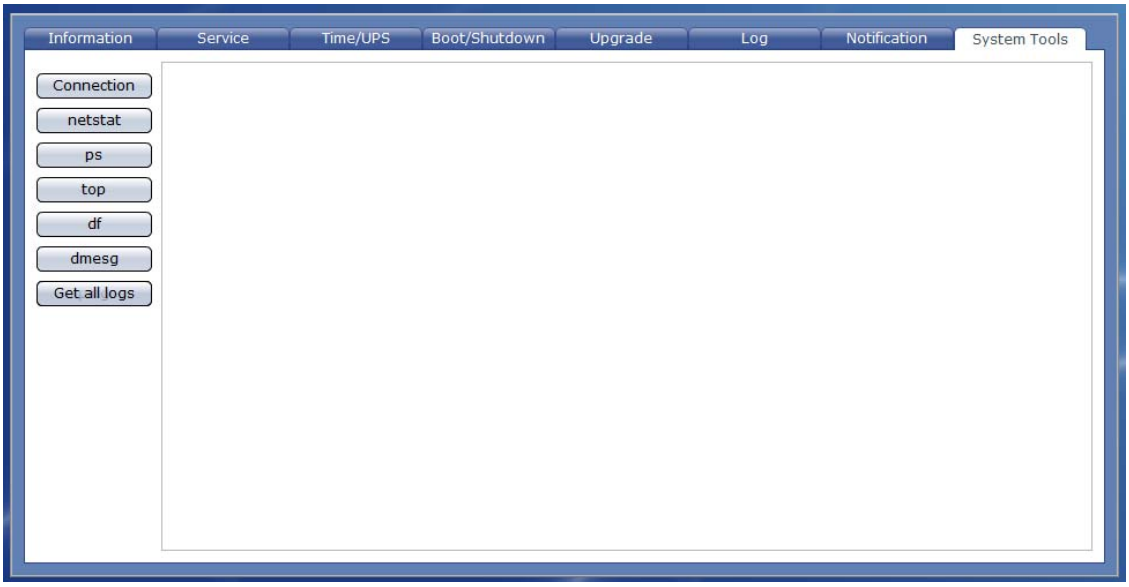
Add – Use this button to add a recipient email address in the list of recipients. Type in the text box the recipient email address.
Remove – Use this button to remove an email address from the list of recipients. Select first the email address then click "Remove".

Apply and test – Use this button to save the changes made and send test mail to the e-mail recipient(s).
Apply – Use this button to save the changes made.
Reset – Use this button to undo or clear any changes made.

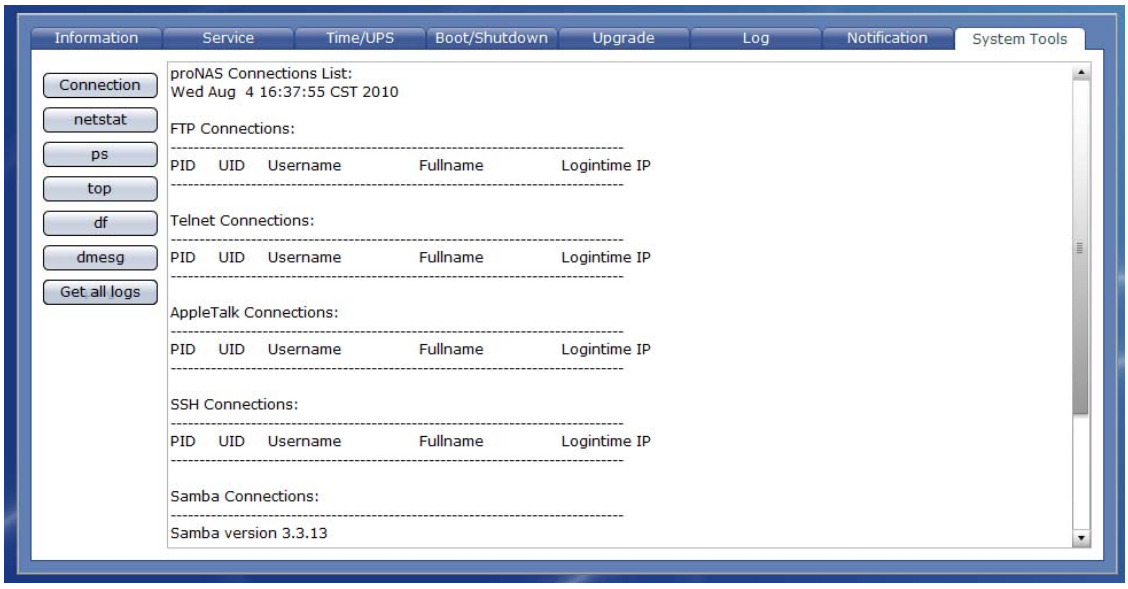


3.3.8 System Tools

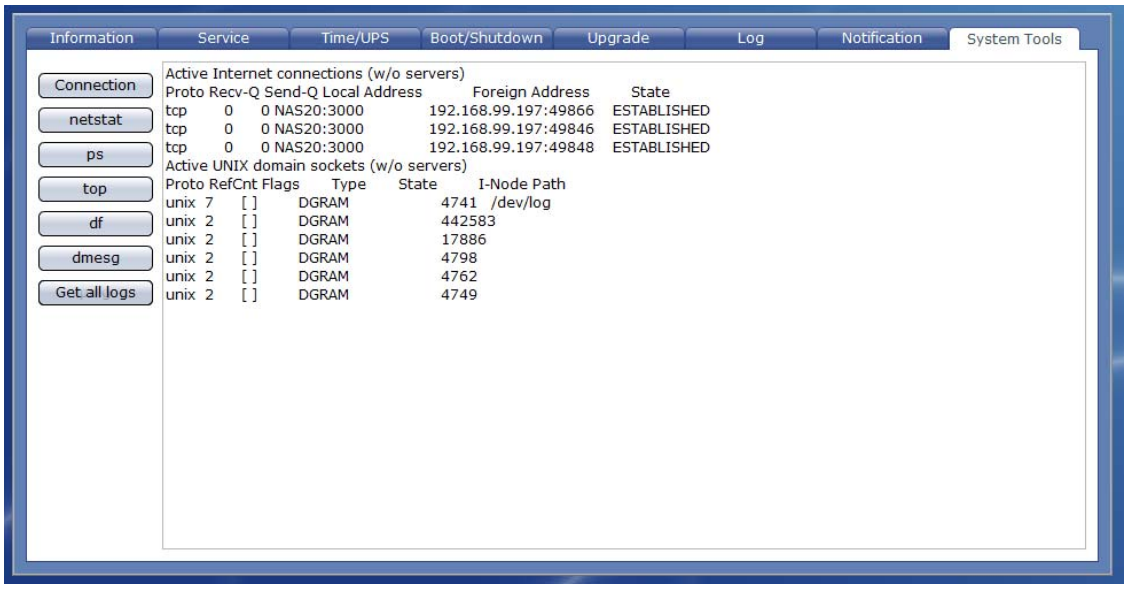
NAS provides various system tools which help the administrator monitor the system.



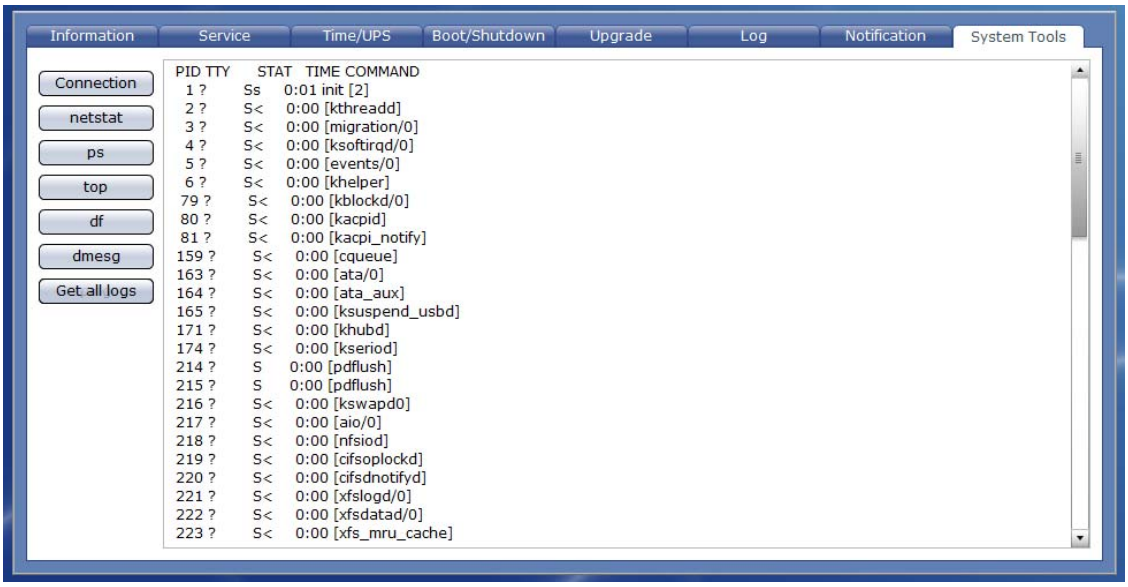
Connection – Use this button to display information about client active connections.



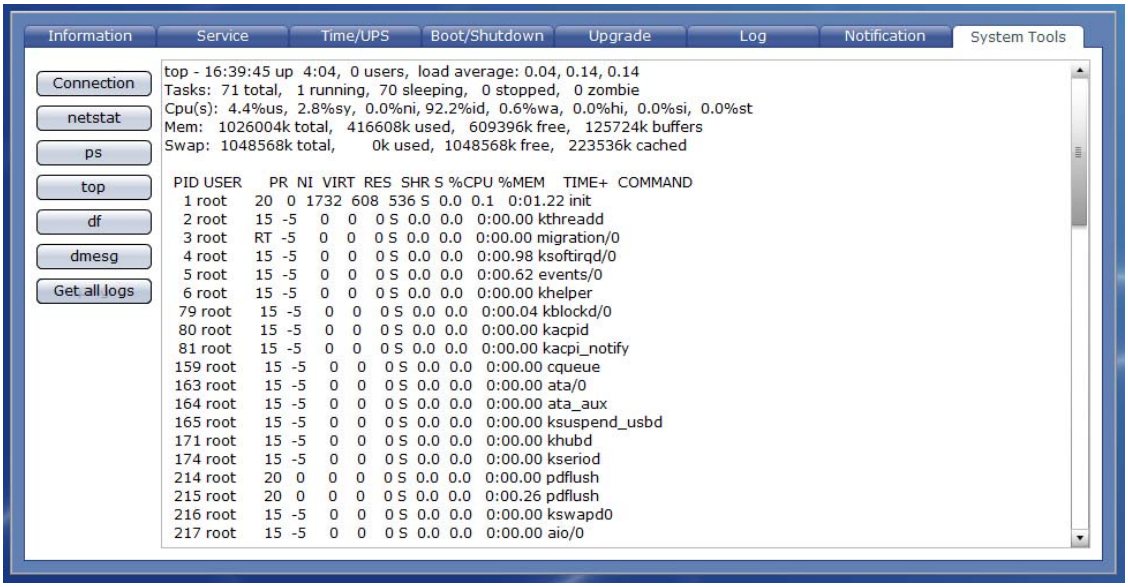
netstat – Use this button to display network connections and statistics information.



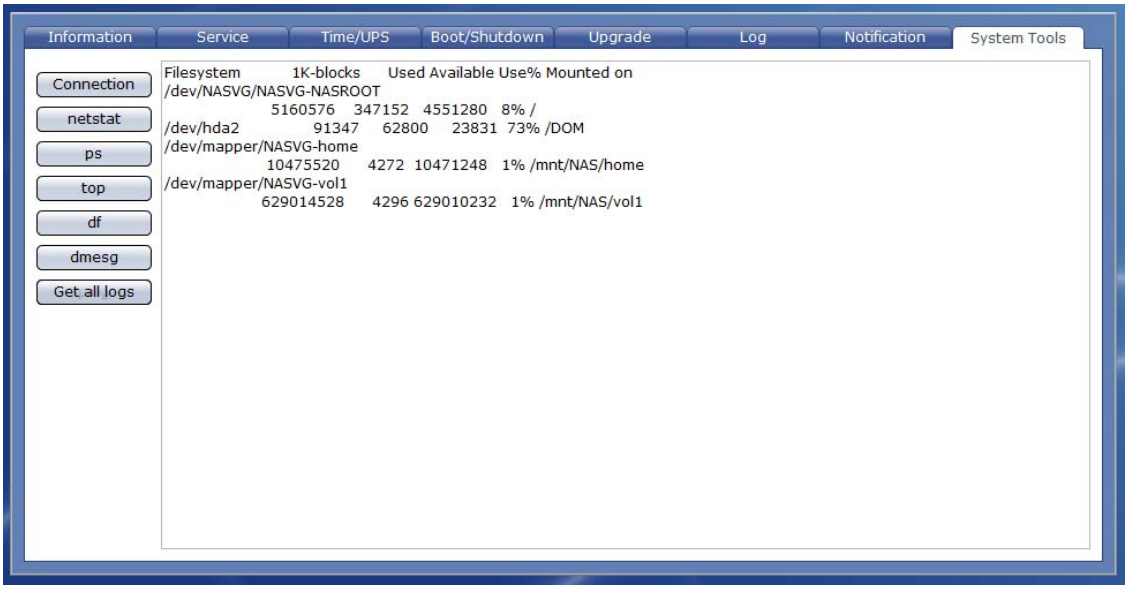
ps – Use this button to display current running processes.



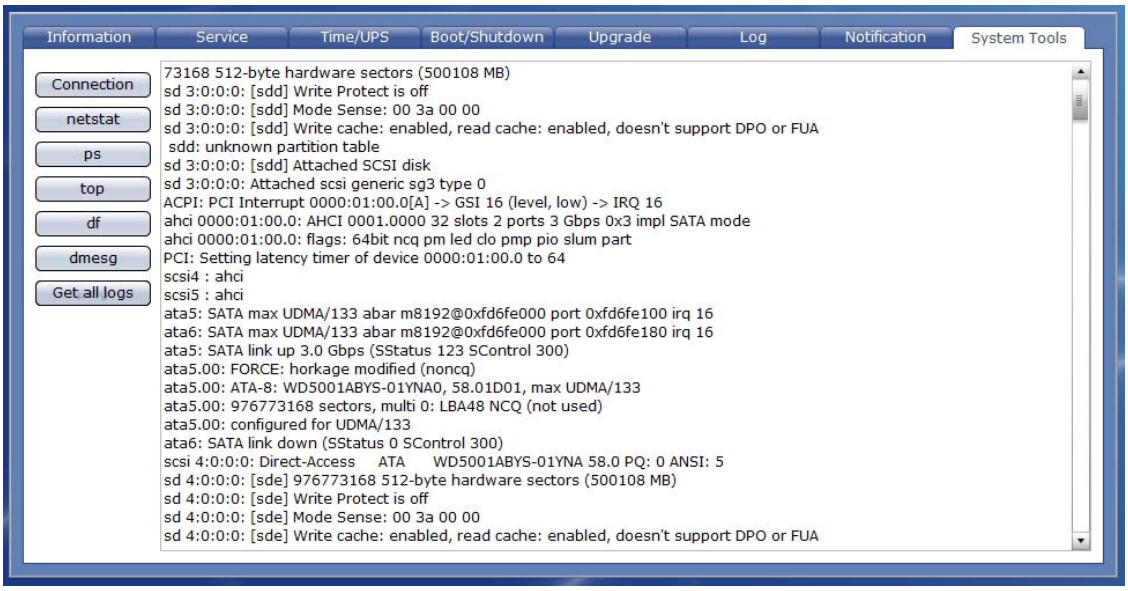
top – Use this button to display current running processes and system usage information.



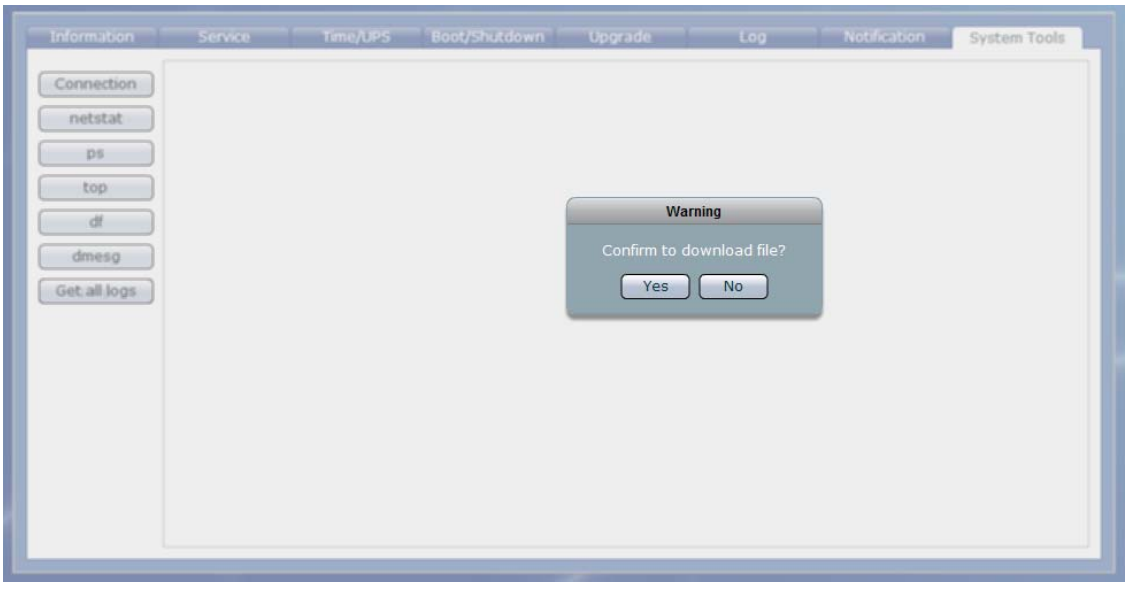
df – Use this button to display disk free information or the amount of available disk space in mounted file systems.



dmesg – Use this button to display NAS boot up messages.



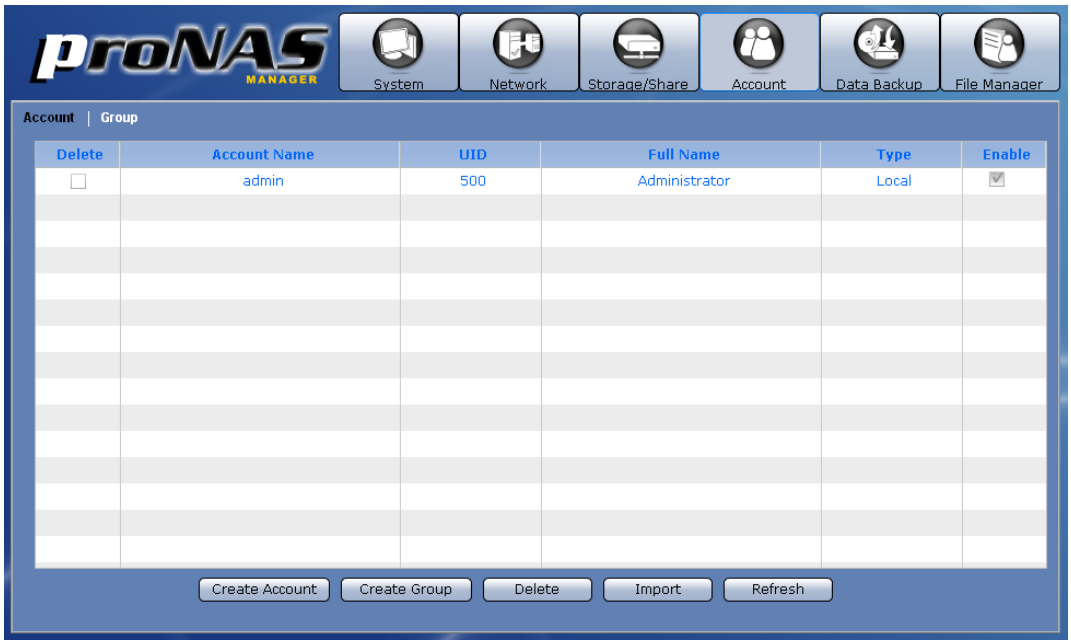
Get all logs – Use this button to save all proNAS logs to a log file in local directory. The log file will be given ".tar" extension name. Rename the log file if needed.



3.4 Account

Using the Account function, the administrator can create and administer local user and group accounts, as well as import large number of accounts.

3.4.1 Account



Account Information and Options:

Delete – Used to option to delete the selected account. After checking this option, click the "Delete" button.
Account Name – Shows the user account name.
UID – Shows the user account ID number.
Full Name – Shows the user account full name.
Type – Shows the type of account, which can be local, Windows or NIS.
Enable – Use this option to enable or disable an account. When an account is disabled, the account is prohibited to access the NAS.

Create Account – Use this button to create a user account.
Create Group – Use this button to create a group account.
Delete – Use this button to delete the selected user account or group account.
Import – Use this option to import large number of accounts instead of adding an account one by one. The administrator can type multiple user accounts in the Import Account input box.
Refresh – Use this button to update the information displayed in the Account and Group list.

3.4.1.1 Create Account

Steps to Create Account:

1. Click “Create Account” button.
2. A dialog box will be displayed. Enter the necessary information.

Create / Edit Account Options:

Name – Used this option to enter the user account name. It should be unique.

NOTE: The account name does not allow space in-between characters. Duplicate account name is also not allowed. Names used by the system, such as root, nobody, mail, adm, etc., are reserved names and cannot be used as account name.

Type – Displays the type. Shows Account for user account.
Full Name – Use this option to enter user account full name.
UID – Use this option to manually assign a UID for the account. Use a valid UID starting from 500. If this option is not set (UID is 0), the system will automatically assign UID starting from 500. Domain accounts will have UID from 10000 to 30000.
Quota (GB) – Use this option to assign quota to the user account’s home folder. Default quota is 0, which means no limit (or will use the total capacity of home folder).
Usage (GB) – read-only information which shows the user account’s current usage of home folder.
Password – Enter the user account’s password.
Password Confirm – Enter again the user account’s password.

NOTE: The setting for “Quota (GB)” when creating or editing a user account applies only to the home folder of the user account. This is different from the user account’s quota for other share folders. The setting of a user account quota for a share folder is done in the Share folder itself, in the Privilege section.

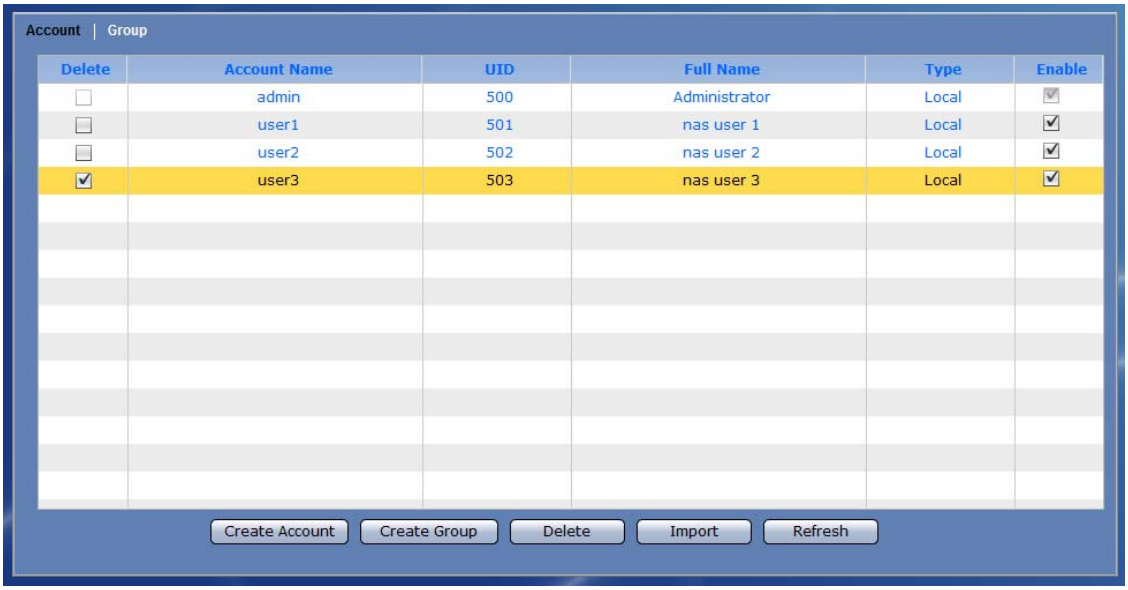
3. Click “OK” when done. The new user account will added to the Account list.

NOTE: If you try to create an Account without an existing VG (NASVG is not yet initialized), a warning message will be displayed.

3.4.1.2 Delete Account

Steps to Delete Account:

1. In the Account list, check the “Delete” option for the account to be deleted.



2. Click the “Delete” button.

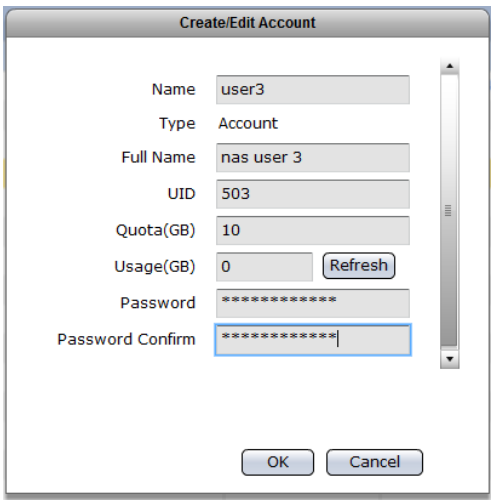
3. A warning message will be displayed. Select “Yes” to proceed. The account will be deleted.

3.4.1.3 Edit Account

Steps to Edit Account:

1. Double-click the Account name in the Account List.
2. Edit the necessary options.

NOTE: Only the Full Name, Quota, Password, and Password Confirm can be changed. Account Name, UID, and Usage cannot be changed.

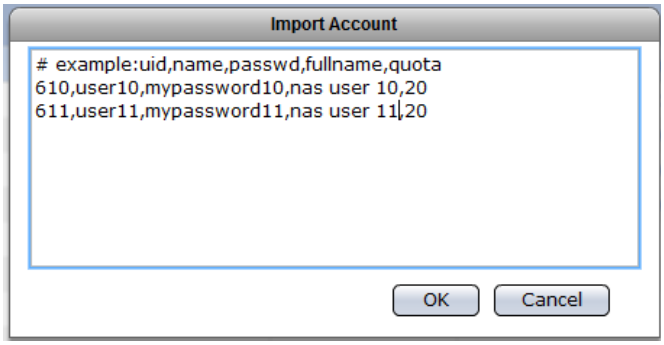


3. Click “OK” when done. The account will be updated with the changes made.

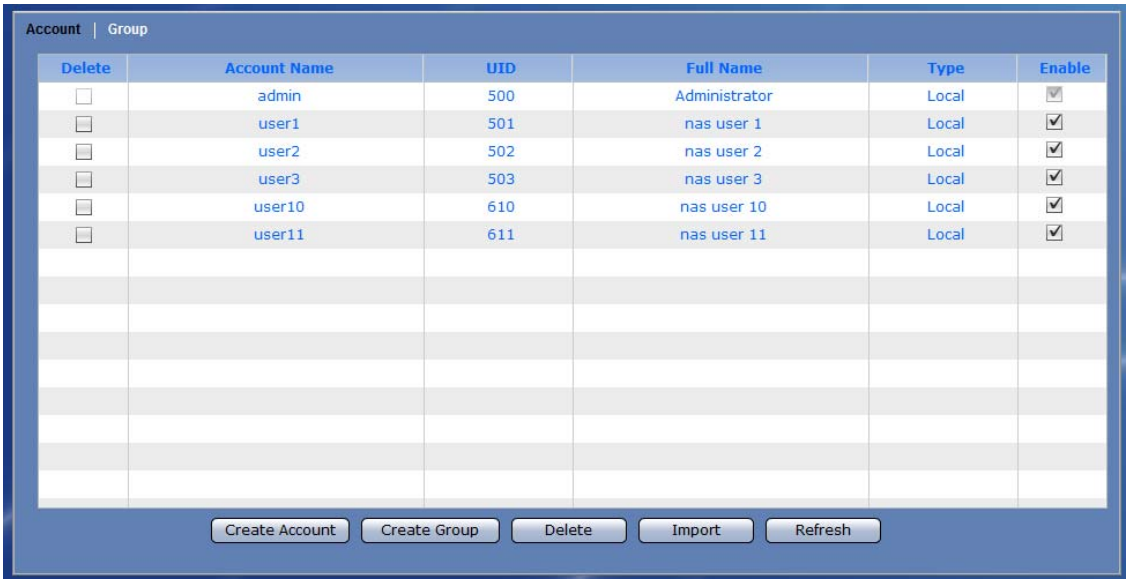
3.4.1.4 Import Account

Steps to Import Account:

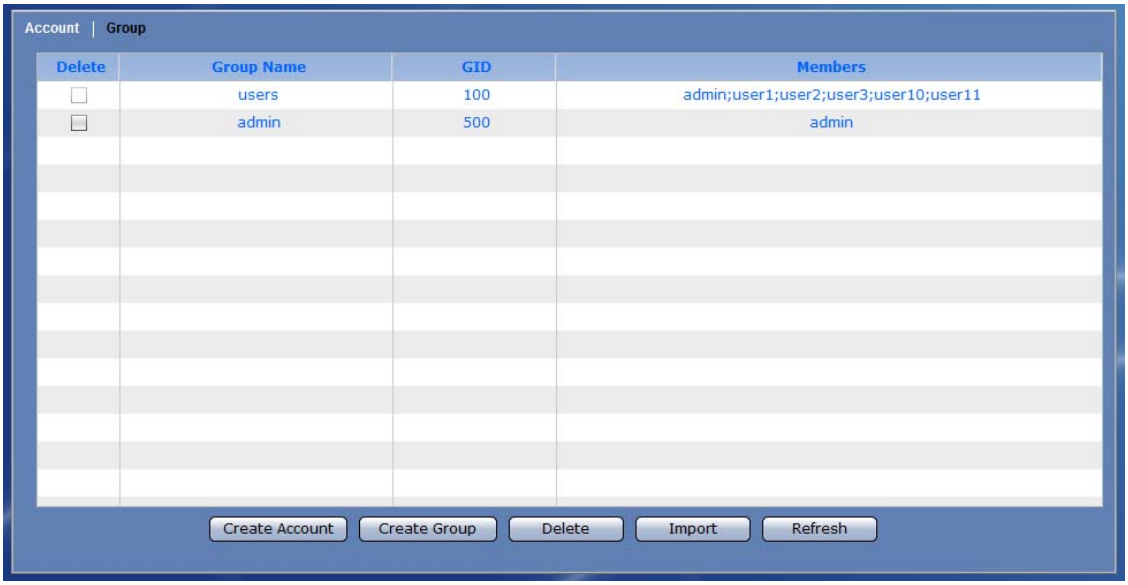
1. Click “Import” button.
2. An input box will displayed. Type the account information using the following format: UID,Name,Password,FullName,Quota. Click “OK” when done.



3. The new accounts will appear in the Account list.



3.4.2 Group



Group Information and Options:

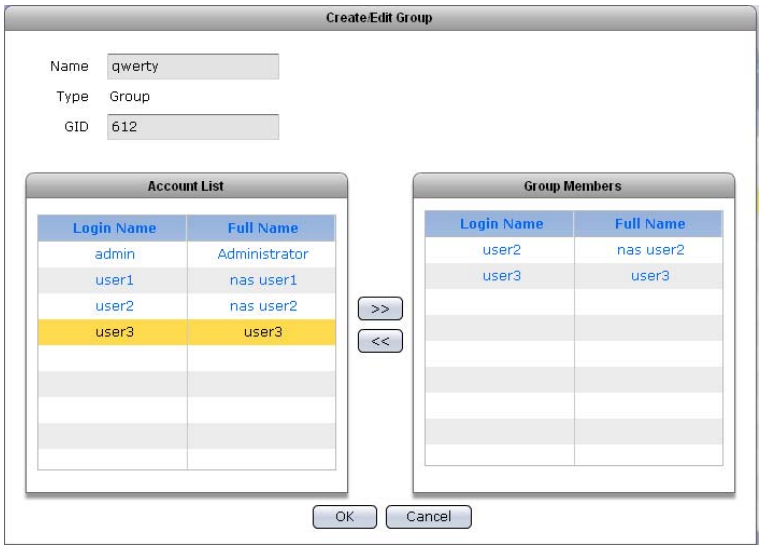
Delete – Used to option to delete the selected group. After checking this option, click the "Delete" button.
Group Name – Shows the group account name.
GID – Shows the group ID number.
Members – Shows the group's user account members.

Create Account – Use this button to create a user account.
Create Group – Use this button to create a group account.
Delete – Use this button to delete the selected user account or group account.
Import – Use this option to import large number of accounts instead of adding an account one by one. The administrator can type multiple user accounts in the Import Account input box.
Refresh – Use this button to update the information displayed in the Account and Group list.

3.4.2.1 Create Group

Steps to Create Group:

1. Click the “Create Group” button.
2. A dialog box will be displayed. Enter the necessary information.



Create/Edit Group Options:

Name – Used this option to enter the group account name. It should be unique.

NOTE: The group name does not allow space in-between characters. Duplicate group name is not allowed. Names used by the system, such as root, nobody, mail, adm, etc., are reserved names and cannot be used as account name.

Type – Displays the account type; shows Group for group account.
GID - Use this option to manually assign a GID for the group. Use a valid GID starting from 500. If this option is not set (GID is 0), the system will automatically assign GID starting from 500.

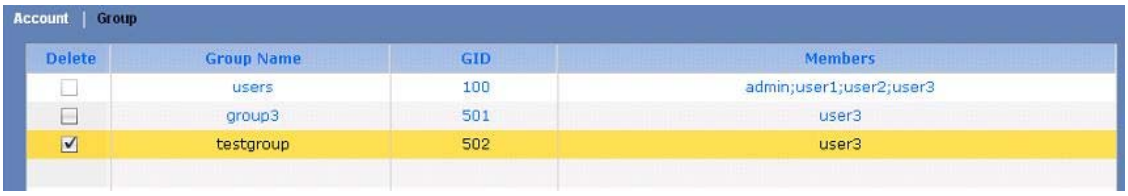
3. Select the account that will become member of the group from the Account List. Then click the “>>” button. The selected account will be displayed in the Group Members list.
4. Click “OK” when done. The group will be created.

NOTE: If you try to create a Group without an existing VG (NASVG is not yet initialized), a warning message will be displayed.

3.4.2.2 Delete Group

Steps to Delete Group:

1. In the Group list, check the “Delete” option for the group to be deleted.



2. Click the “Delete” button.

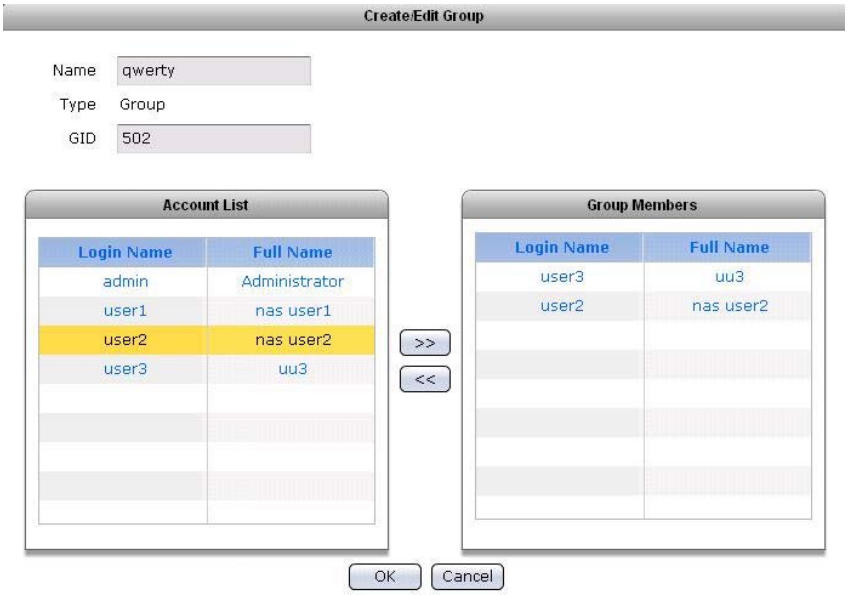
3. A warning message will be displayed. Select “Yes” to proceed. The group will be deleted.

3.4.2.3 Edit Group

Steps to Edit Group:

1. Double-click the Group name in the Group List.
2. Edit the necessary options.

NOTE: Only the Group Name and Group Members can be changed.



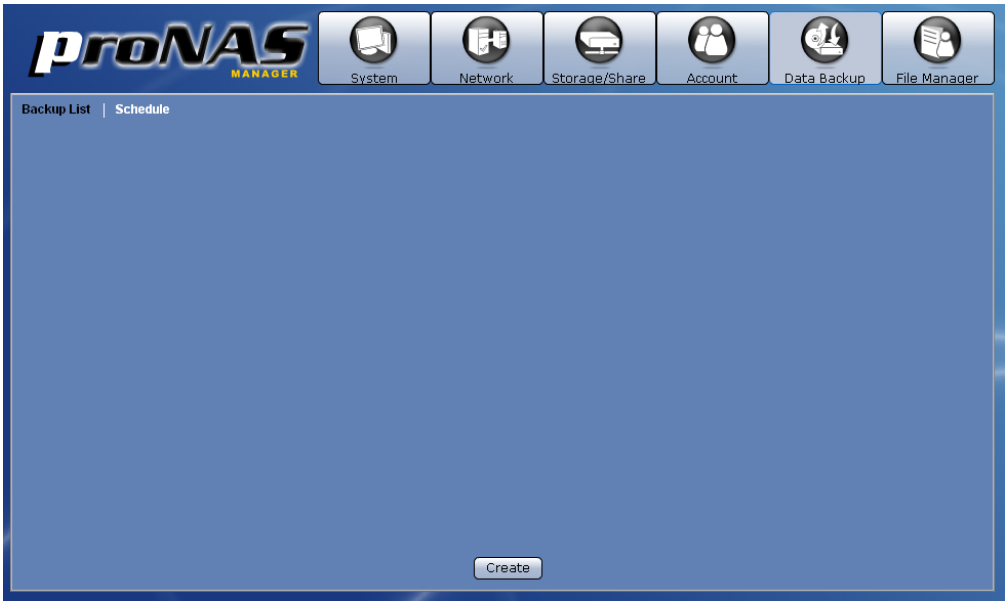
3. Click “OK” when done. The group will be updated with the changes made.

3.5 Data Backup

The administrator can backup NAS data to remote destination or to local disk.

NOTE: The Data Backup function is not available in the iSCSI target Volume. Only share folders (created under non-iSCSI Volume) can be included in the backup source. iSCSI Volume cannot be selected as backup source.

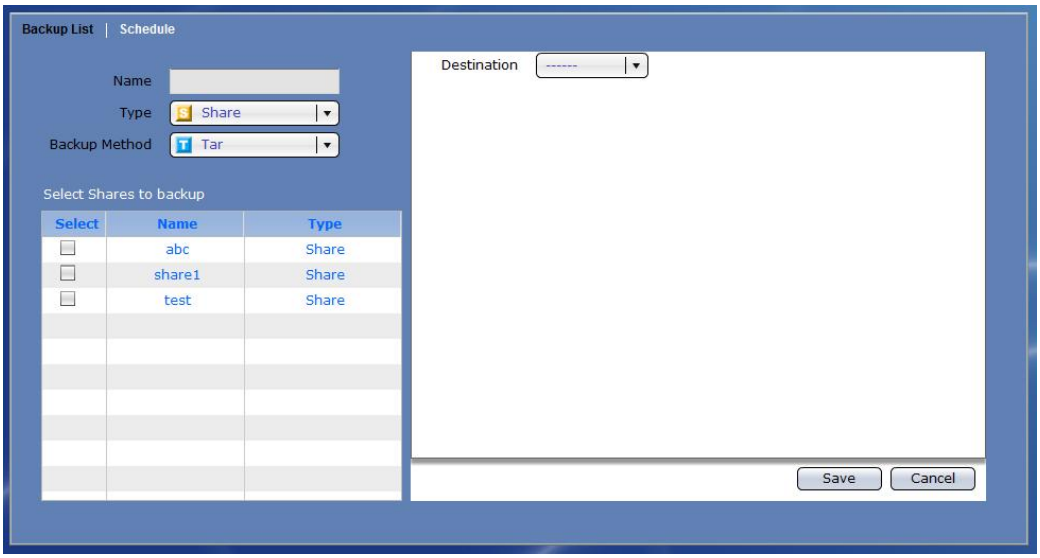
3.5.1 Backup List



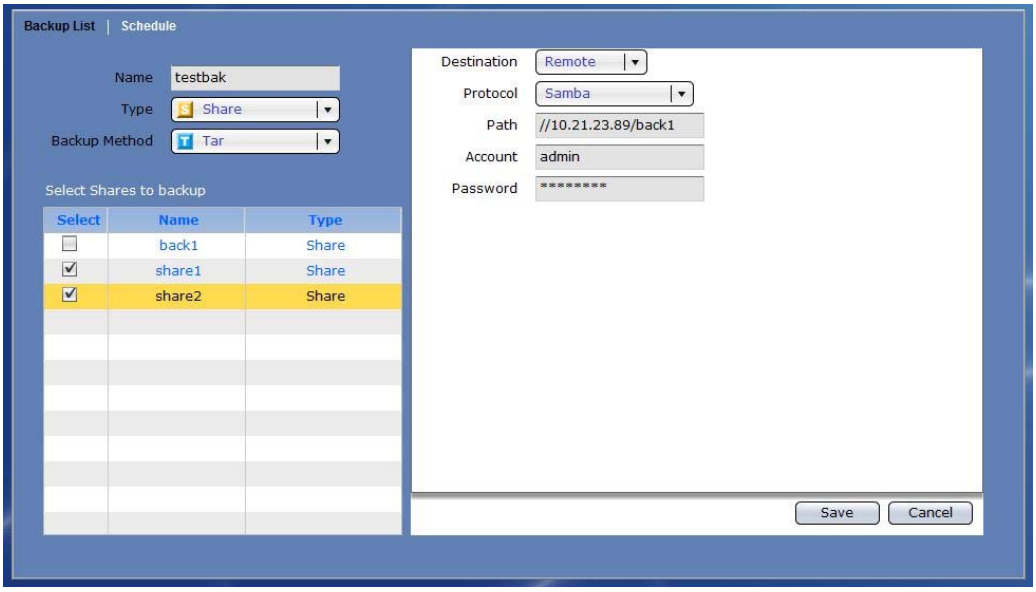
3.5.1.1 Create Backup Plan

Steps to Create a Backup Plan:

1. Click the “Create” button. The screen below will be shown.



2. Configure the necessary options.



Create Backup Options:

Name – Used this option to enter the backup name.
NOTE: Duplicate backup name is not allowed.
Type – Select the type of backup source; for example: Share.
Backup Method – Select the backup method that will be used, such as Tar or Rsync.

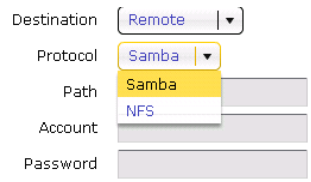
Select Shares to backup – Select from the list the share folders that will be backed up.

Tar Options:

Destination – Select the destination option for the backup. Options can be: Local Disk or Remote. Local Disk is an un-used disk drive. Remote is a remote CIFS/Samba share or NFS file system.

Local Disk:

Remote:



NOTE: When a local disk is selected as backup destination, the disk status in Storage / Share ➔ RAID screen will be shown as "BACKUP".

Protocol - Select the type of protocol to be used for backup. Options are: Samba and NFS.

NOTE: For NFS, it will be assumed that the root account will be used. Please verify that root account can access the remote NFS file system.

Path – Type the path for the remote destination.

Format for Samba:

//remote-IP/remote-share

Example:

//172.16.0.211/backupfolder

Format for NFS:

remote-IP:/Path-to-Remote-NFS-file-system

Example:

172.16.0.9/mnt/proNAS/volume/share

Account – Type the account name with access to the remote share.

Password – Type the password for the account with access to the remote share.

Rsync Options (Client Options):

IP – Type here the IP address of the remote Rsync server.

Remote Path – Type here the share name on the remote Rsync server.

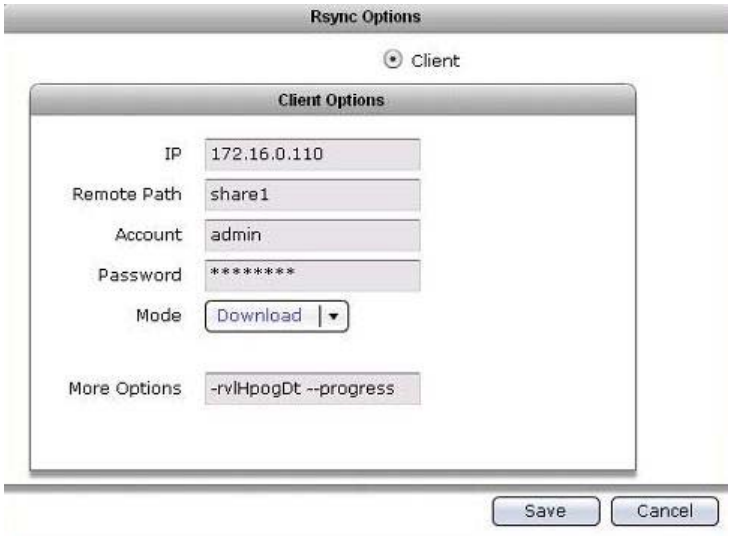
Account – Type here the account name that will be required by the Rsync server for authentication.

Password – Type here the password of the account.

Mode – Select the mode of file transfer, whether to upload to Rsync server or to download from Rsync server.

More Options – Specify here the Rsync options to be used. For more information about Rsync options, please visit http://samba.org/ftp/rsync/rsync.html.

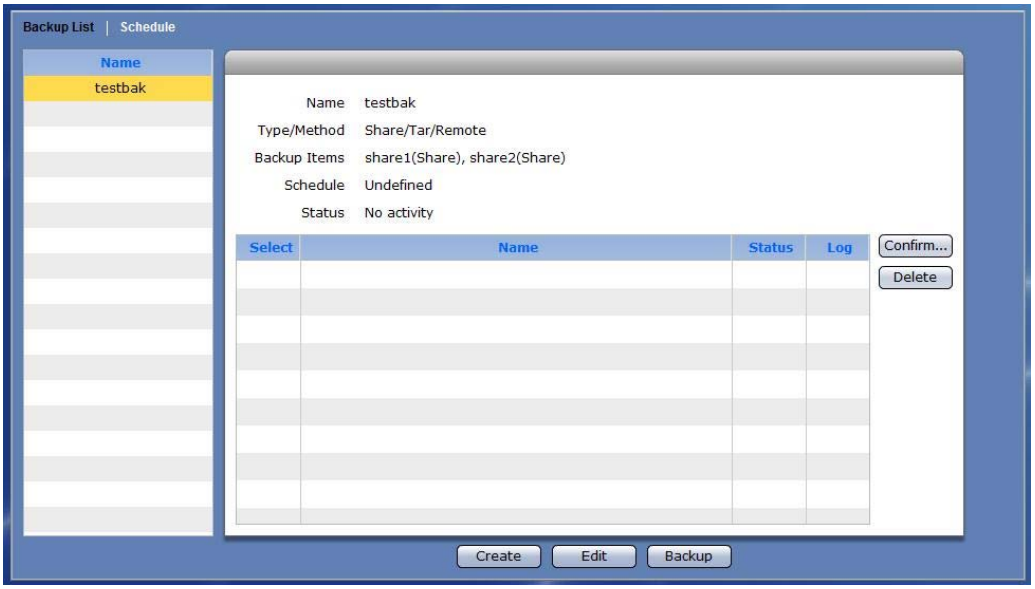
Refer to Section 3.1.3.8–B on how to setup NAS as Rsync client.



Save – Use this button to apply the changes made.

Cancel – Use this button to undo or clear any changes made.

3. Click the “Save” button. The backup plan will be created and shown in the Backup List.



Backup List Options:

Name – Shows the list of backup plans. When a backup plan is selected, information about the backup plan will be displayed, such as name of backup plan, type/method of backup, backup items, schedule (Enabled or Undefined), and completed backups.

Select – Use this option to select a completed backup then delete or restore the backup.

Name – Show the backup name.

Status – Shows the status of the particular backup. Status can be: Incomplete or Complete.

Log – Use this option to view the detailed information about the completed backup. Click the “…” button.

Backup List Buttons:

Confirm… – Use this button to restore a selected backup.

Delete – Use this button to delete the selected backup.

Create – Use this button to create a new backup plan.

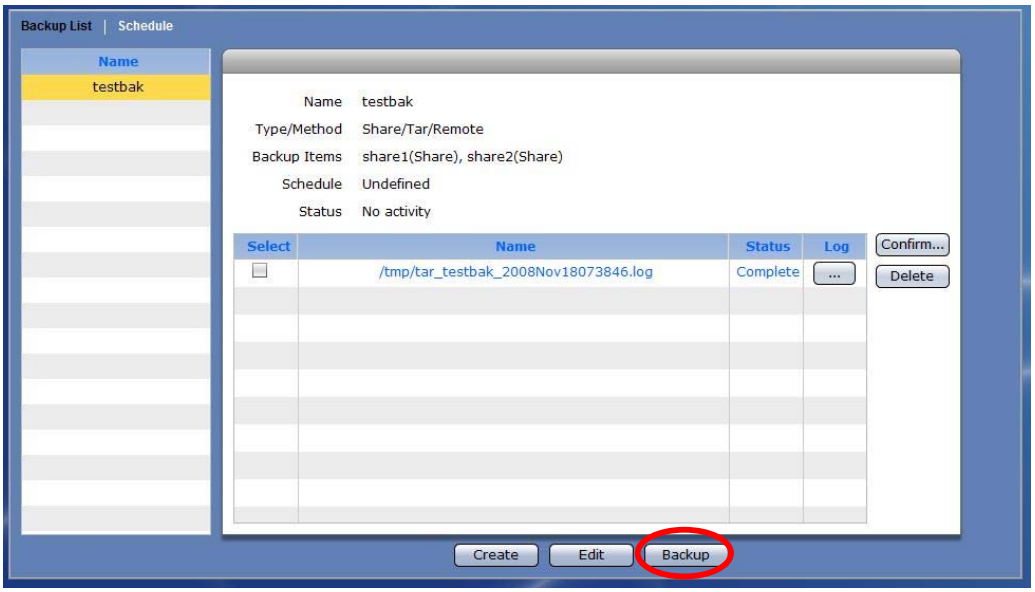
Edit – Use this to button edit or delete a selected backup plan.

Backup – Use this button to perform immediate backup.

3.5.1.2 Create Immediate Backup

Steps to Create Immediate Backup:

1. Select the particular backup plan from the Backup List. Click the “Backup” button.



2. A message will be displayed. The backup is completed and a backup name will be added to the log list.

3.5.1.3 Delete Backup Plan

Steps to Delete a Backup Plan:

1. Select the particular backup plan from the Backup List.
2. Click the “Edit” button.
3. Click the “Delete” button.
4. A warning message will be displayed. Select “Yes” to delete the backup plan.

3.5.1.4 Edit Backup Plan

Steps to Edit a Backup Plan:

1. Select the particular backup plan from the Backup List.
2. Click the “Edit” button.
3. Change the necessary options. Click “Save” when done.

NOTE: A backup plan cannot be modified if a backup log exists.

3.5.1.5 Delete a Backup Log

Steps to Delete a Backup Log:

1. Select (check) the backup log to be deleted from the log List.
2. Click the “Delete” button. A warning message will be displayed.

3. The backup will be deleted from backup destination and removed from log list.

3.5.1.6 Restore a Backup

Steps to Restore a Backup:

1. Select (check) the particular backup from the log List.
2. Click the “Confirm…” button. A warning message will be displayed. Select “Yes” to restore backup.

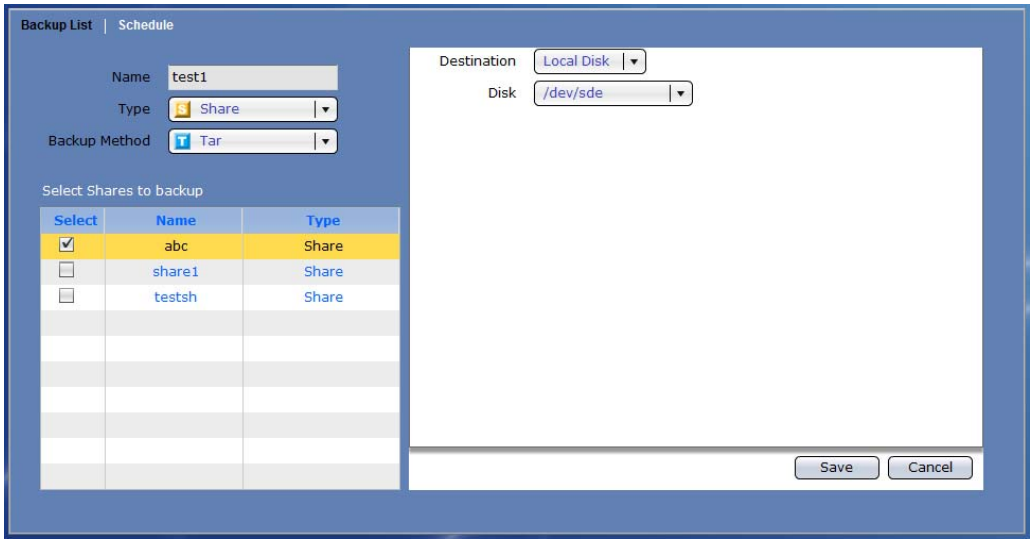
3. The original data will be restored.

3.5.1.7 Backup to Local Disk

Here is an example of how to backup to local disk.

6. Create a Backup Plan by using the “Create” button while in Backup List tab of Data Backup function.

7. Setup the Backup Plan. Enter the Backup Name and select the shares to backup. Leave the Type and Backup Method as is. In the Destination option, select Local Disk. The Disk option will display the available (free or un-used) local disk. Select the disk you want as destination for backup, if more than one free disk are available. Click “Save” when done.

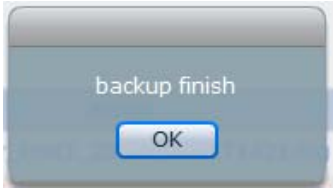


8. To perform immediate backup, click “Backup” button. A warning message will be displayed. To proceed and confirm formatting the disk, select “Yes”.

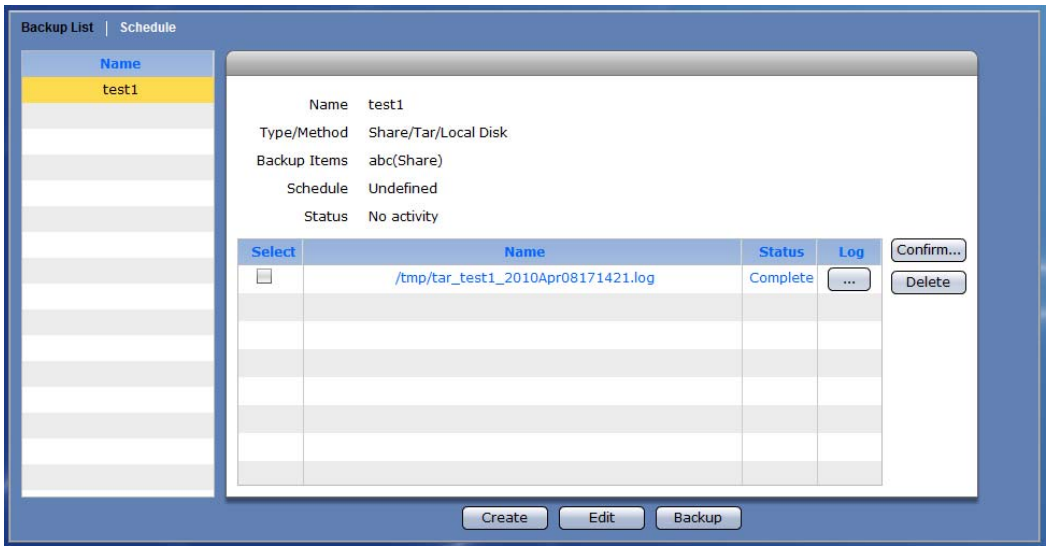
NOTE: After the local disk is formatted, the succeeding backup processes will no longer require formatting the disk.

9. Another warning message will be displayed. Select “Yes” to continue.

10. The backup process will be started. When backup is completed, a message will be displayed. Click “OK”.



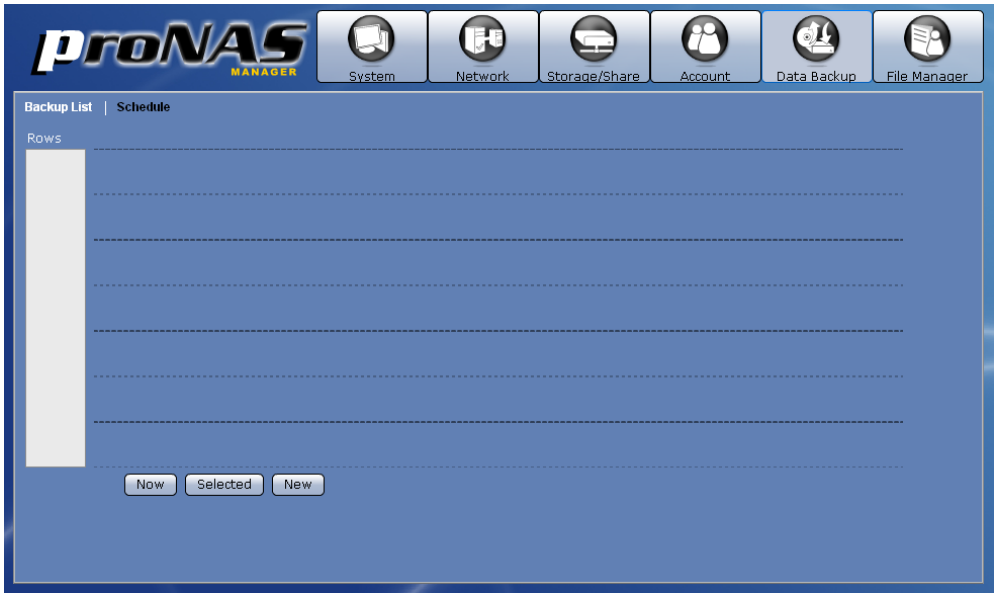
11. The backup to local disk is done. A log will be shown in the log list.



3.5.2 Schedule

A backup plan can be run based on schedule. Select the Schedule tab. This will show a graphical view of the scheduled backup tasks.

Each row shows the day of the week. Each column shows the time in very 30 minutes interval.



Schedule Options:

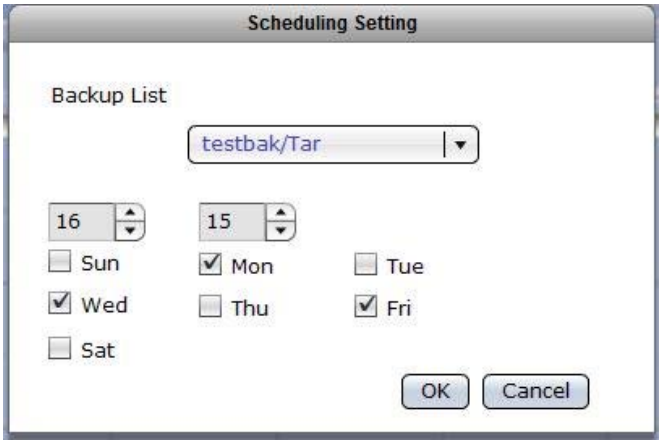
Now – Use this option to display available backup tasks on the current time.
Selected - Use this button to edit a scheduled backup task. Select first the scheduled backup task then click this button.
New – Used this button to create a new scheduled backup task.

NOTE: It is not allowed to have duplicated or overlapping backup time. Only one backup process can be running at a time. A scheduled backup is set to run within 30 minutes time frame. Scheduling another backup within a scheduled time is not allowed.

3.5.2.1 Setup Scheduled Backup Task

Steps to Setup Scheduled Backup:

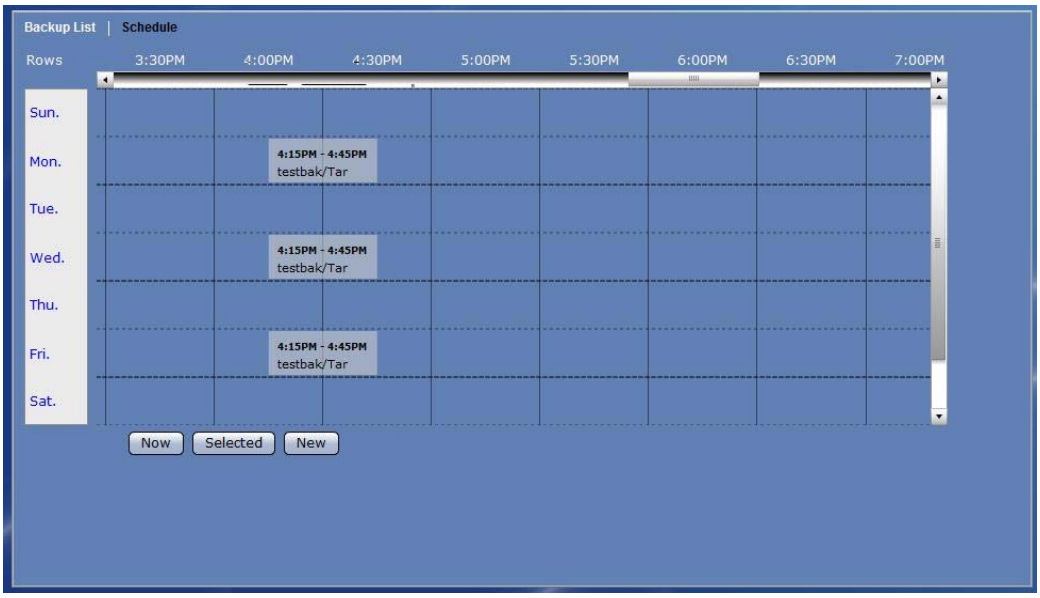
1. Select the “Schedule” tab then click the “New” button.
2. Edit the options in Schedule Setting.



Schedule Setting Options:

Backup List – Select the backup plan from the list.
Time – Set the hour and minutes when the backup will be run.
Day – Select the day or days when the backup will be run.
OK – Use this button to save the backup settings. The backup schedule will be automatically enabled.
Cancel – Use this button to clear or undo any changes made.

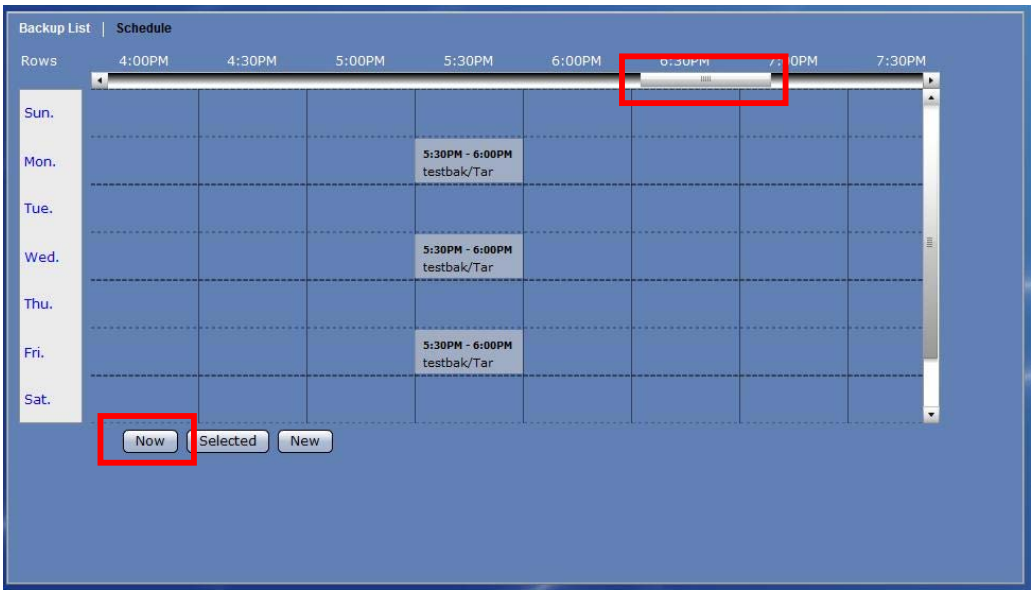
3. The backup task will appear in the schedule.



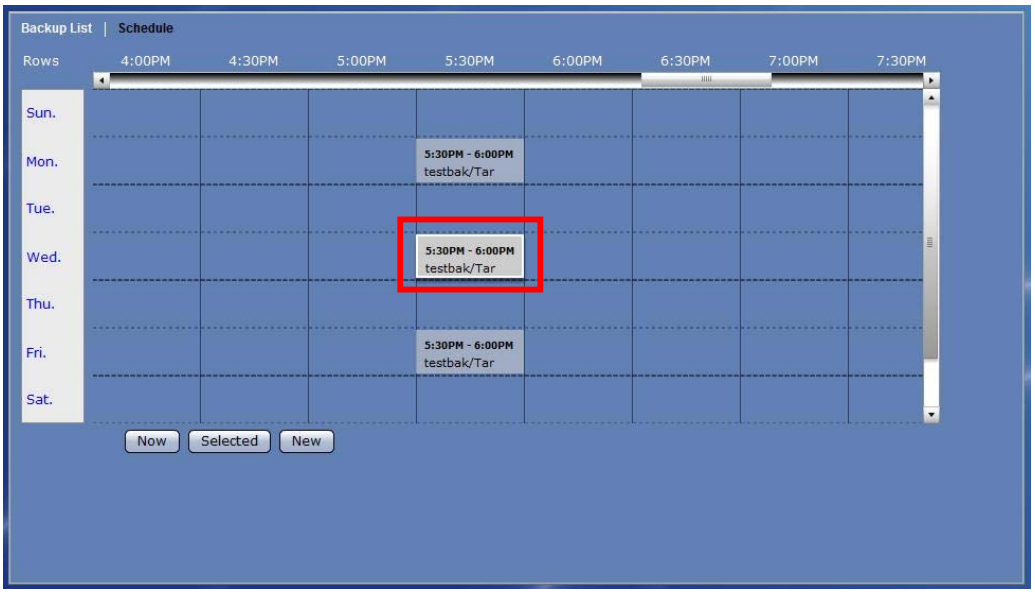
3.5.2.2 Edit Scheduled Backup Task

Steps to Edit Scheduled Backup Task:

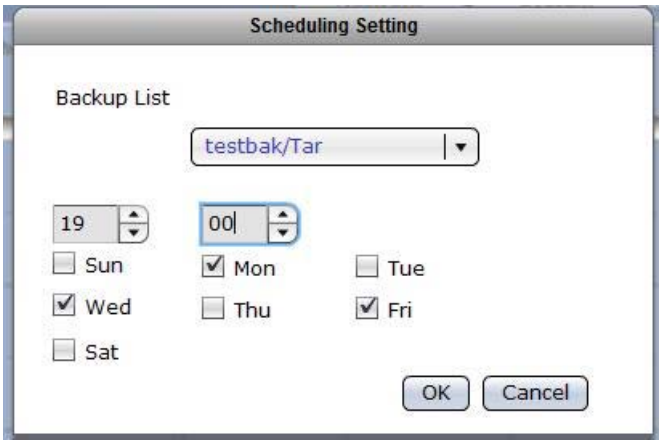
1. Move the scroll bar then locate the scheduled backup task to be changed, or click "Now" to see current scheduled backup.



2. Select the backup task to edit. The backup task will be highlighted.



3. Click the “Selected” button. Edit the necessary options.



NOTE: It is not allowed to have duplicated or overlapping backup time. Only one backup process can be running at a time. A scheduled backup is set to run within 30 minutes time frame. Scheduling another backup within a scheduled time is not allowed.

4. Click “OK” to save the changes made.

3.6 File Manager

3.6.1 Introduction to File Manager

File Manager is a web-based file system management utility for admin and ordinary users to do the following actions:

Create, Delete, Rename a Folder: User needs to have read and write permission to the share folder and the folder itself in order to create, delete, or rename the folder.

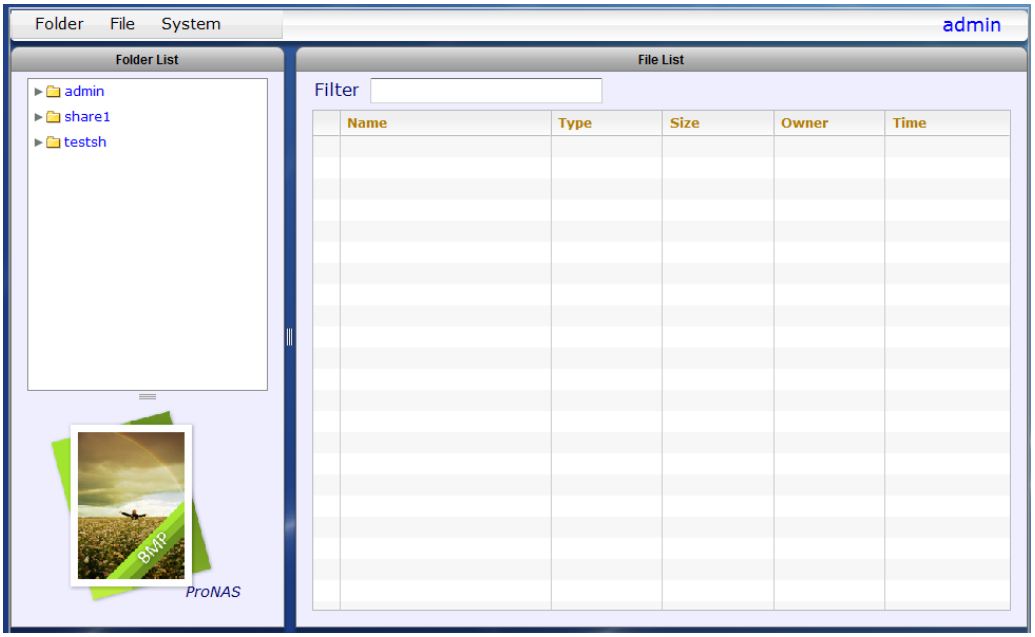
Set Folder Permission: User needs to have read and write permission to the share folder and the folder itself in order to set the permission of the folder.

Upload a file: User needs to have read and write permission to the share folder/ sub-folder. A browser's upload window will show up and user needs to locate the file from local computer to be uploaded to the current folder.

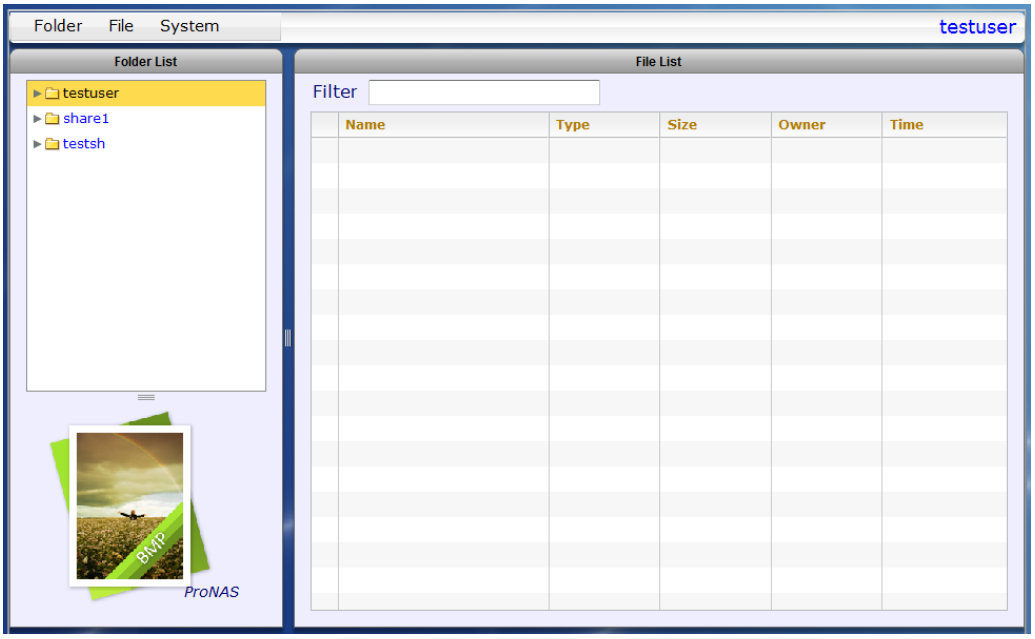
Download a file: User needs to have at least read permission to the folder and the file itself. After selecting the file to be downloaded and clicking "Download", a browser's download window will show up and user can (open or) save the file to local directory.

Rename a file: User needs to have read and write permission to the folder and the file itself. Select the file to be renamed. A pop up window will show up and user needs to enter the new file name.

Delete a file: User needs to have rear and write permission to the folder and the file itself. Select the file to be deleted. A pop up message will show up and user needs to select "Yes" to delete the selected file.



Admin is logged-in

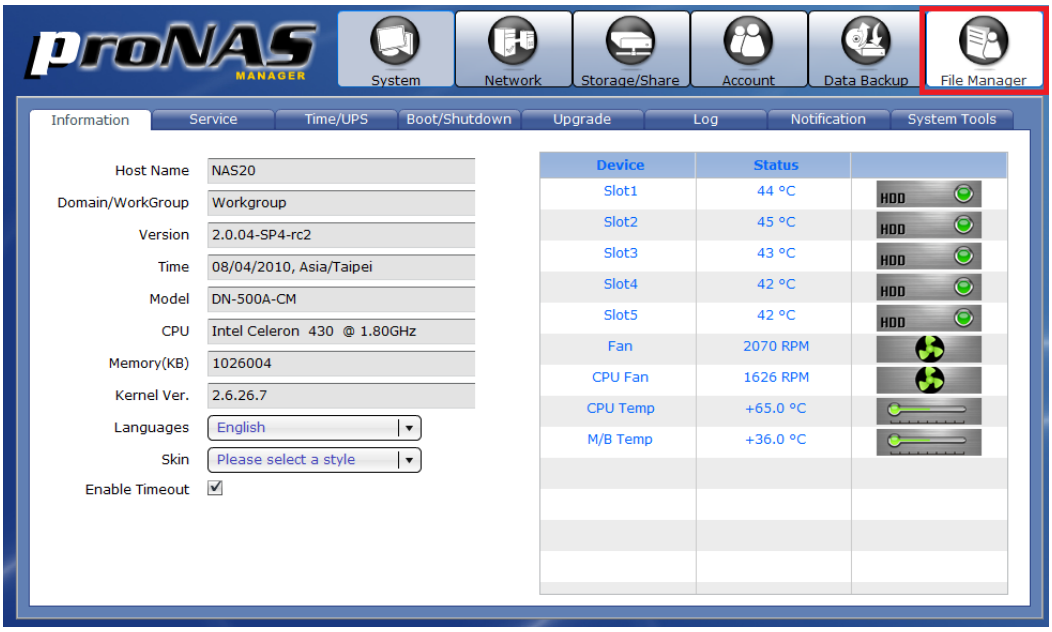


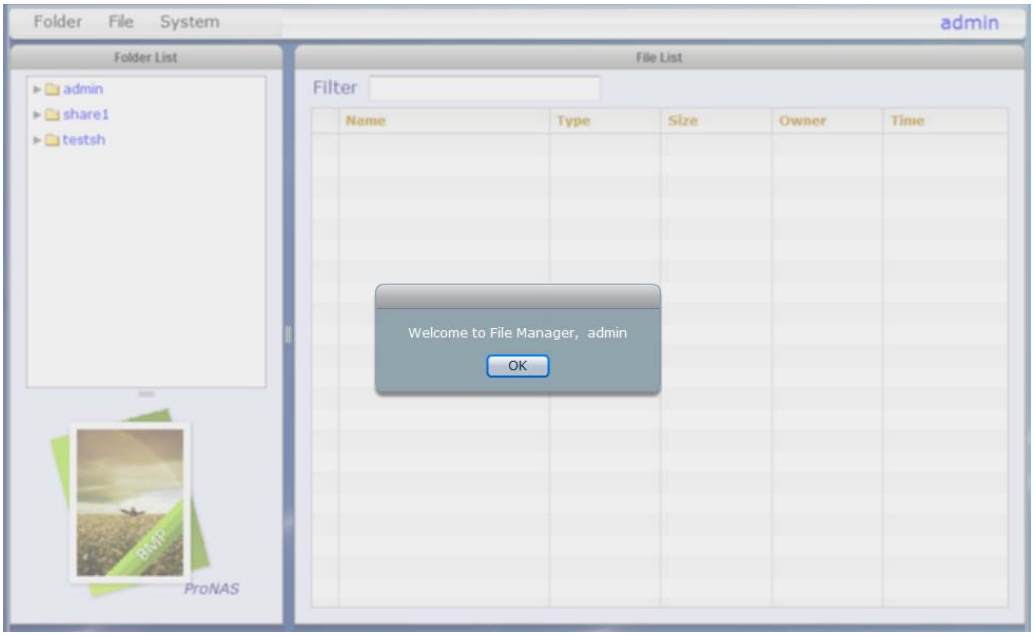
Local user “testuser” is logged-in

3.6.2 Login to File Manager

3.6.2.1 Admin Login

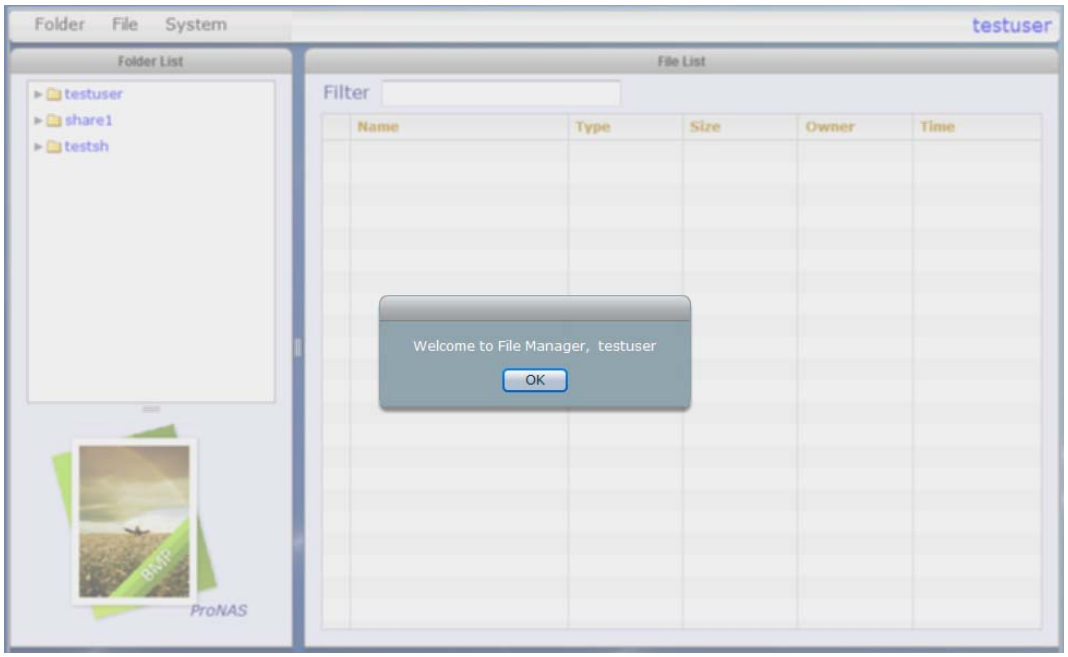
Admin can login to File Manager while in proNAS Manager GUI. Select the File Manager icon on the upper right corner. The File Manager window will be displayed.





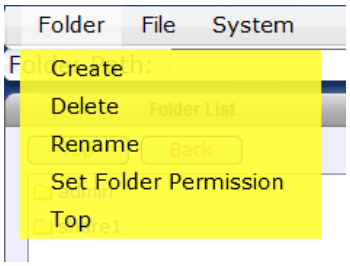
3.6.2.2 Ordinary User Login

Ordinary user can login to File Manager from main login screen. After login, the File Manager window will be displayed.



3.6.3 Folder

Under Folder menu, user can select the following functions: Create, Delete, Rename, Set Folder Permission, and Refresh Folder List.

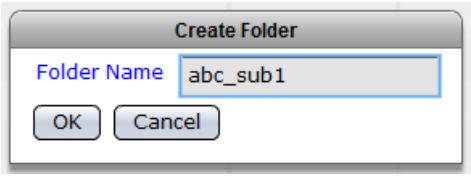


3.6.3.1 Create Folder

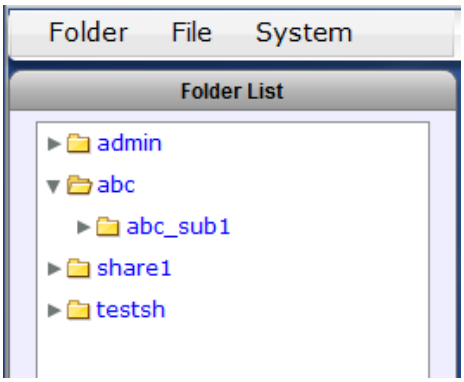
NOTE: User needs to have read and write permission to the share folder/sub-folder in order to create a new sub-folder.
NOTE: Some characters, such as (, #, $, ^, “, and -, are not allowed to be used as folder name.

To create a folder or sub-folder:

12. Select the share folder or sub-folder where a sub-folder will be created, then select the Folder menu and click Create.
13. Enter the folder name in the Folder Name box. Click “OK” when done.



14. The folder will be created.



3.6.3.2 Delete Folder

NOTE: User needs to have read and write permission to the share folder and the sub-folder itself in order to delete the sub-folder.

To delete a folder or sub-folder:

9. Select the folder or sub-folder that will be deleted, then select Folder menu and click Delete.
10. When a message is displayed, click “Yes” to confirm deletion.

11. The folder will be deleted.

3.6.3.3 Rename Folder

NOTE: User needs to have read and write permission to the share folder and the sub-folder itself in order to rename the sub-folder.
NOTE: Some characters, such as (, #, $, ^, ”, and -, are not allowed to be used as folder name.

To rename a folder or sub-folder:

1. Select the folder or sub-folder, then click Folder menu then select Create.
2. Enter the new folder name in the New Folder Name box. Click “OK” when done.

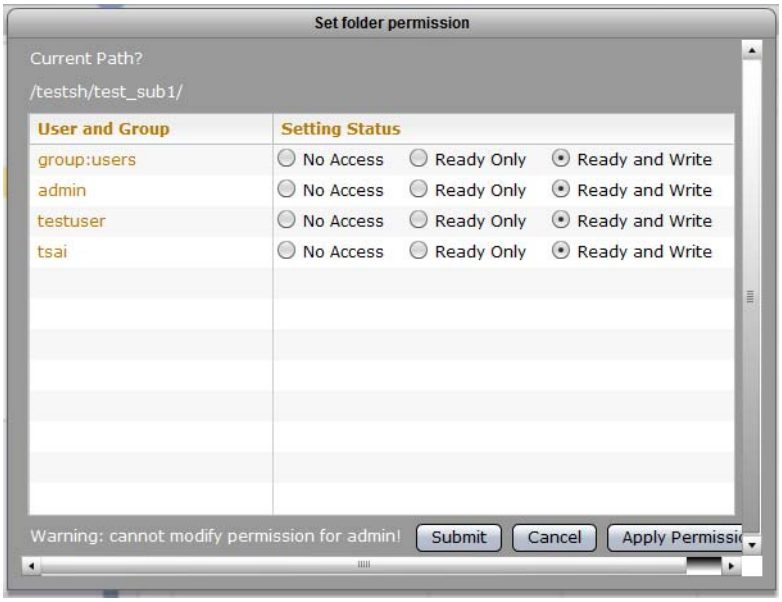
3. The folder will be renamed.

3.6.3.4 Set Folder Permission

NOTE: User needs to have read and write permission to the share folder and the sub-folder itself in order to set the permission on the sub-folder.
NOTE: Admin and user cannot set the permission of the share folder (top level share folder) in File Manager. Admin can do this in proNAS GUI → Storage / Share → Share / Security. Only sub-folders created under the share folder can be set.

To set the permission on a folder or sub-folder:

1. Select the folder or sub-folder whose permission will be set, then select Folder menu and click Set Folder Permission.
2. The Set folder permission window will be displayed. Modify the permission as needed.



Options:

No Access - User or Group is denied access to the folder.
Read Only – User or Group is allowed Read-Only access to the folder.
Read and Write – User or Group is allowed Read and Write access to the folder.

Buttons:

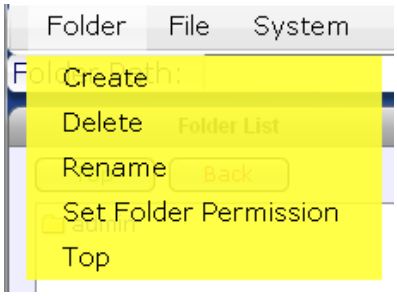
Submit – Use this button to save the changes made.
Cancel – Use this button to undo any changes made.
Apply Permission – Use this button to propagate the current ACL (access control list) from the selected folder into all sub-folders and files under it.

3. Click “Submit” to save the changes. The folder permission is set.

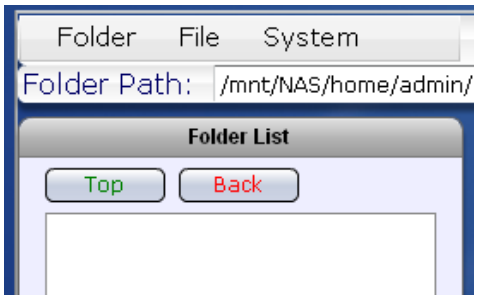
NOTE: If you need to propagate the same permission (ACL) to the sub-folders and files under the current folder, use the “Apply Permission” button.

3.6.3.5 Top

Use the Top option in the Folder menu to go up to the top most level of share folder list from the current sub-folder.



You can also use the Top and Back buttons.

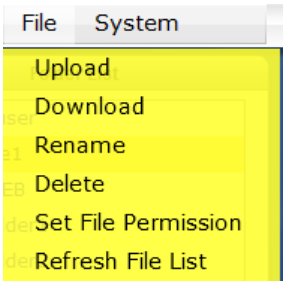


Top – Use this button to go up to the top most level of share folder list from the current sub-folder

Back - Use this button to go up one folder level higher from the current sub-folder

3.6.4 File

Under File menu, user can select the following functions: Upload, Download, Rename, Delete, Set File Permission, and Refresh File List.



3.6.4.1 Upload File

NOTE: User needs to have read and write permission to the share folder and the sub-folder itself in order to upload a file.

NOTE: The file size limit for uploading file via File Manager is 25MB only.

To upload a file:

1. Select a folder or sub-folder where a file will be uploaded, then select File menu and click Upload.
2. A pop up window will be displayed. Select the file that will be uploaded to the folder. Click “Open”.
3. The selected file will be uploaded.
4. A message will be displayed when upload is completed.

3.6.4.2 Download File

NOTE: User needs to have at least read permission to the share folder / sub-folder and to the file itself in order to download the file.

To download a file:

1. Select a folder or sub-folder where the file to be downloaded is located.
2. Select the file.
3. Select File menu and click “Download”.
4. Save (or open) the file.

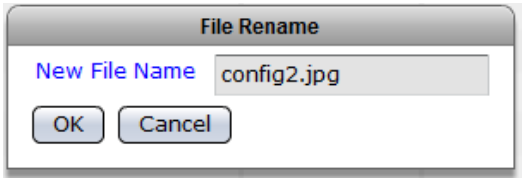
3.6.4.3 Rename File

NOTE: User needs to have read and write permission to the share folder / sub-folder and to the file itself in order to rename the file.

NOTE: Some characters, such as (, #, $, ^, and ”, are not allowed to be used as file name.

To rename a file:

1. Select a folder or sub-folder where the file to be renamed is located.
2. Select the file.
3. Select File menu and click “Rename”.
4. Enter the new file name.



5. Click “OK” when done.

3.6.4.4 Delete File

NOTE: User needs to have read and write permission to the share folder / sub-folder and to the file itself in order to delete the file.

To delete a file:

1. Select a folder or sub-folder where the file to be deleted is located.
2. Select the file.
3. Select File menu and click “Delete”.
4. A message will be displayed.

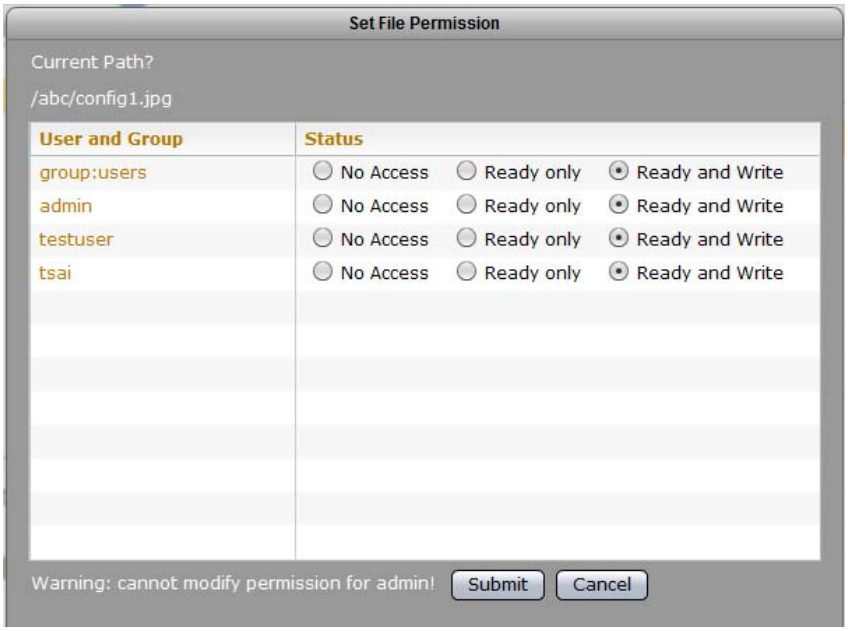
5. Select “Yes” to delete the file.

3.6.4.5 Set File Permission

NOTE: User needs to have read and write permission to the share folder / sub-folder and to the file itself in order to set file permission.

To set file permission:

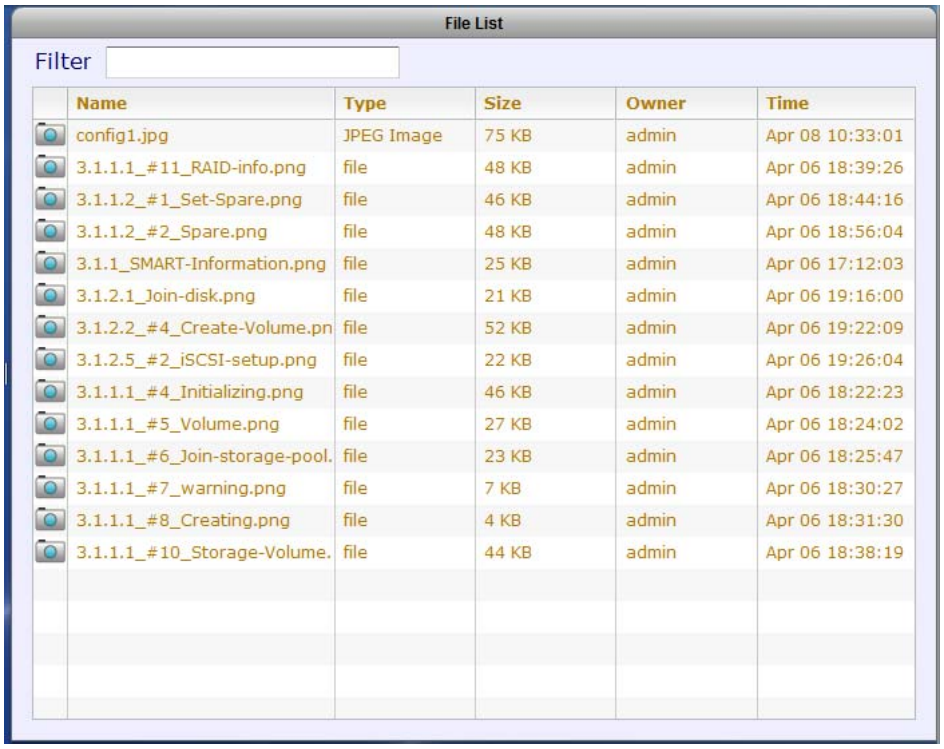
1. Select a folder or sub-folder where the file is located.
2. Select the file.
3. Select File menu and click “Set File Permission”.
4. The Set File Permission window will be displayed.



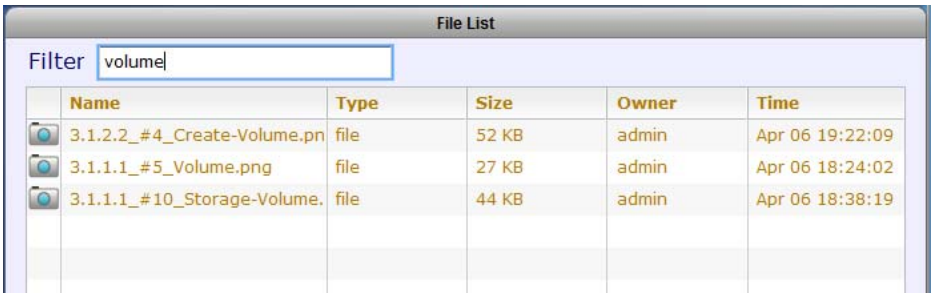
5. Modify the permission as needed.
6. Click “Submit” when done.
7. A Complete message will be displayed. Click “OK”.

3.6.4.6 Refresh File List

Use the Refresh File List option to update the list of files displayed in the File List on the right pane.

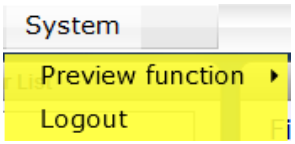


NOTE: Use the Filter function to display specific files. For example, if you want to display files with characters “volume”, enter the word volume in the Filter text box. The list of files containing the word “volume” will be displayed. Note that the text is not case-sensitive.



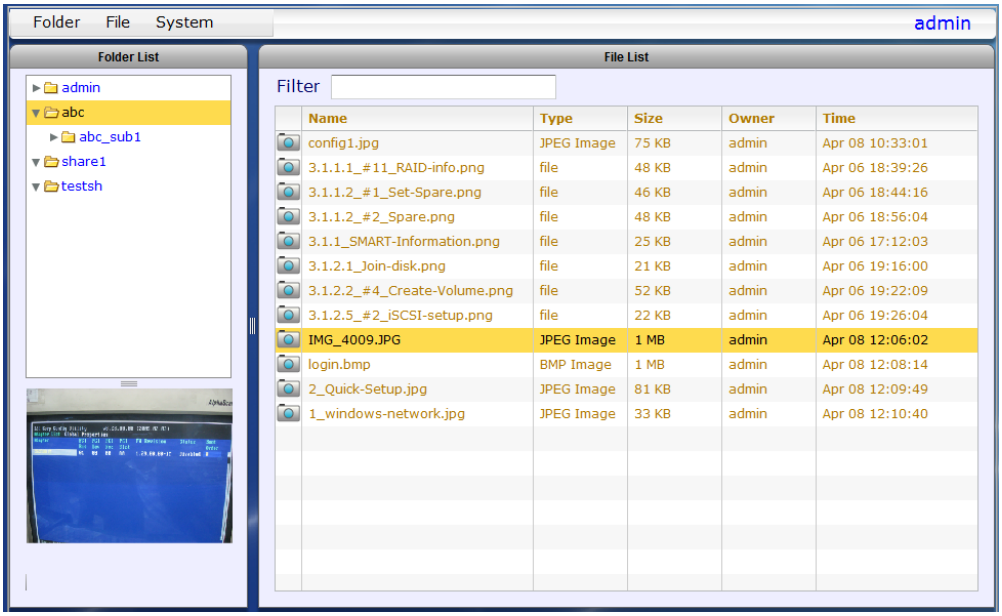
3.6.5 System

Under System menu, user can select the following functions: Preview function and Logout.



3.6.5.1 Preview Function

The Preview function enables the user to see a sample view of a picture file on the left lower pane. The supported file format is JPEG Image (.JPG).



By default, the Preview function is enabled (set to “Yes”).

To disable the Preview function, select System Menu and Preview function, and click “NO”.

3.6.5.2 Logout

Use the Logout function to logout from File Manager.

To logout:

1. Select System menu and click “Logout”.
2. A message will be displayed. Click “Yes” to confirm logout.