PLANET
Networking & Communication

User's Manual

4-Bay SATA NAS RAID Server with iSCSI

► **NAS-7410**

www.PLANET.com.tw

Copyright

CE mark Warning

This is a class A device, in a domestic environment; this product may cause radio interference, in which case the user may be required to take adequate measures.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste; they should be collected separately.

Revision

User's Manual for PLANET 4-Bay SATA NAS RAID SERVER with iSCSI
Model: NAS-7410
Rev: 1.00 (June.2013)
Part No. EM-NAS-7410

Table of Contents

Chapter 1. Product Introduction

1.1. Package Contents

The package should contain the following items:

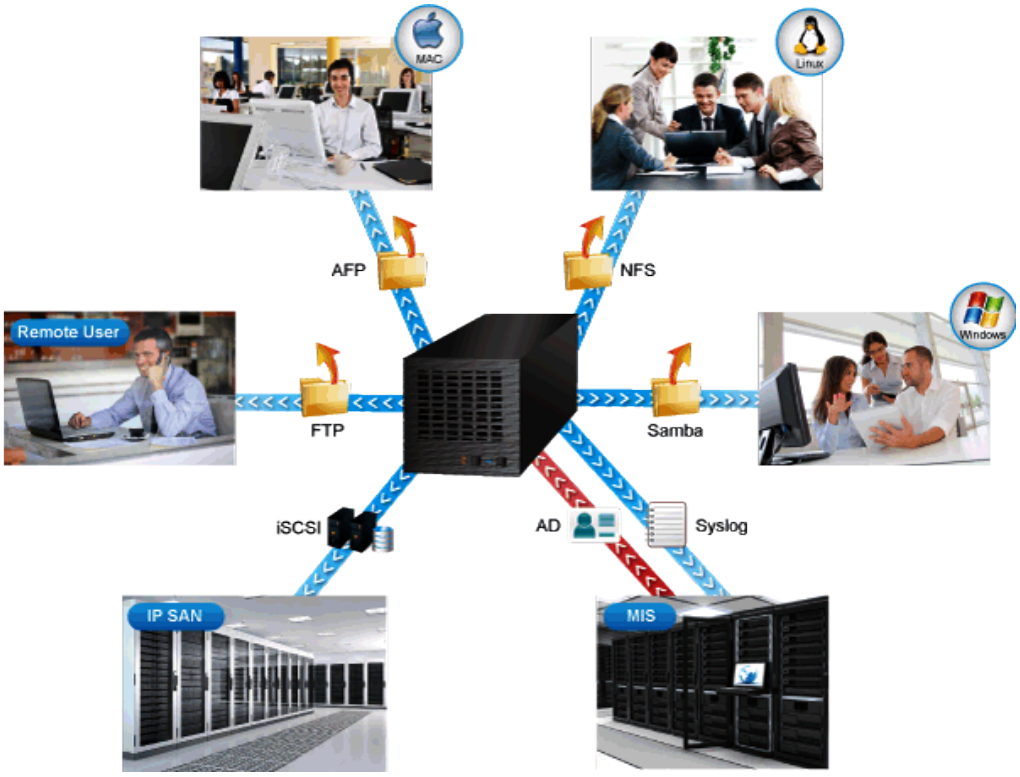
- NAS-7410 x 1
- HDD Key x 4
- Power Cord x 1
- 2.5 inch HDD Screw x 16
- 3.5 inch HDD Screw x 12
- Console Connector x 1
- User's Manual CD x 1
- Quick Installation Guide x 1

Note	1. If any of the above items are missing, please contact your dealer immediately. 2. Using the power supply that is not included in the package will cause damage, thus voiding the warranty for this product.

1.2. Overview

High Performance Shared Storage Server

PLANET NAS-7410, a reliable and high-performance business-class network storage is a 4-bay RAID network storage system for those seeking reliable and affordable server virtualization and file storage. The network storage unified architecture supports both NAS and IP-SAN applications and solves numerous data management problems with a single system. Support for major network file-system protocols enables cross-platform compatibility and file sharing among Windows, Mac and Unix/Linux operating systems. Integrated data protection and offsite replication features make managing complex business storage environments affordable.

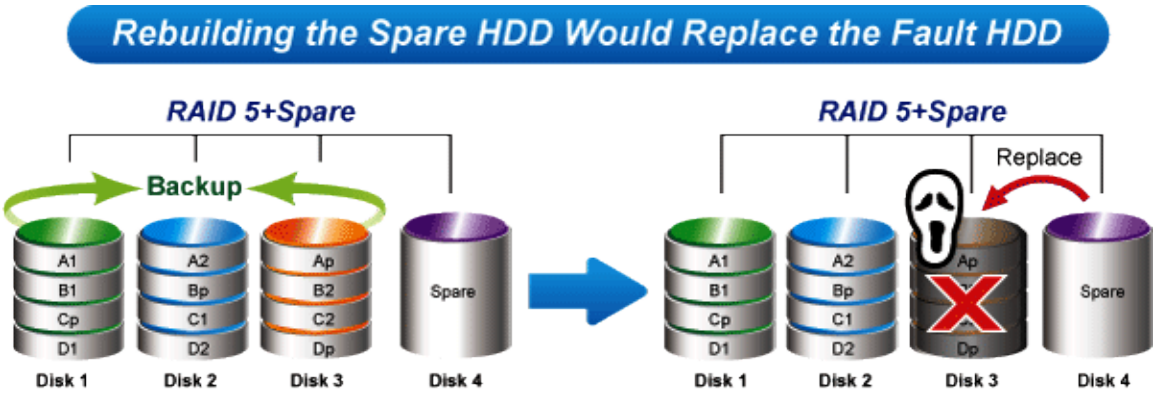


Space Saving & Tray-less Design

The NAS-7410 is designed to allow the installation of up to four 2.5”/3.5” SATA hard drives. Each hard drive door has a multi-locking latch mechanism in order to prevent a door from being opened easily. Each of these doors includes a tray and hard drive key that can be easily unlocked and pulled out. Then users can easily attach the hard drive to the hot-swap hard drive tray with the screws.

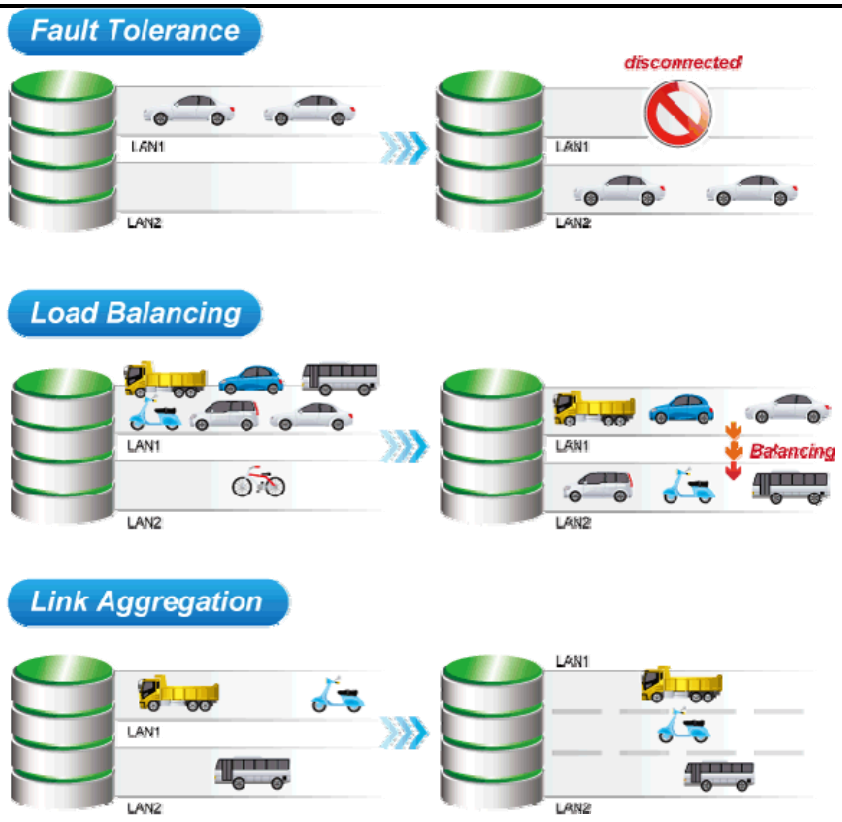
Automatic Data Protection by RAID & Hot Swap

The NAS-7410 provides advanced RAID configurations including RAID 0, 1, 5, 6 and 10 functions. You can get the perfect compromise between speed and disk-failure proof, hardware-level data protection. It also supports hot-swap design so that a failed drive can be replaced by hot swapping without turning off the server.



Multiple LAN for Better Efficiency

The NAS-7410 features multiple functions to support LAN storage for better efficiency.
Fault Tolerance：When LAN1 of the NAS-7410 fails to connect to the network, LAN2 would take over from LAN1 which is designed to ensure server availability to the network.
Load Balancing：When the traffic of LAN1 starts to get congested, then LAN2 would share the traffic until the traffic of both LAN ports starts to get balanced. Load Balancing also incorporates Fault Tolerance protection.
Link Aggregation：Combine LAN1 and LAN2 into a single channel to provide greater bandwidth. Must be used with Link Aggregation switch.

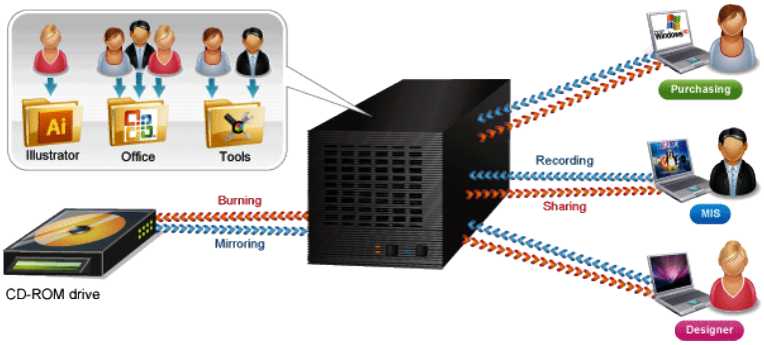


The Extension of Network Communication by WebDAV

The NAS-7410 supports WebDAV, which is an extension of the HTTP protocol for users to edit and manage documents and files that are stored on servers over the Internet. It also allows iOS and Android WebDAV clients to access files from NAS server.

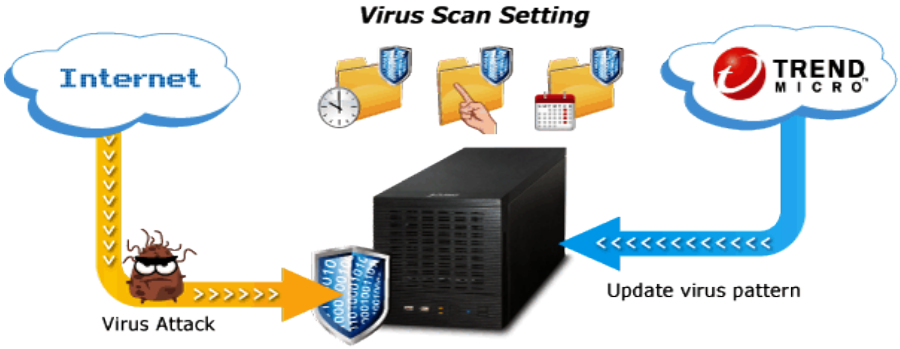
Powerful Disc Images Management and Sharing by Disc Server

Disc Server is our unique technology which is designed for CD/ DVD, Blu-ray disc images creation, burning and data archiving for central management. This feature saves the space for storing the physical discs, reduces the risk of data loss caused by disc wearing and tearing, and enhances the efficiency of data sharing on business network.



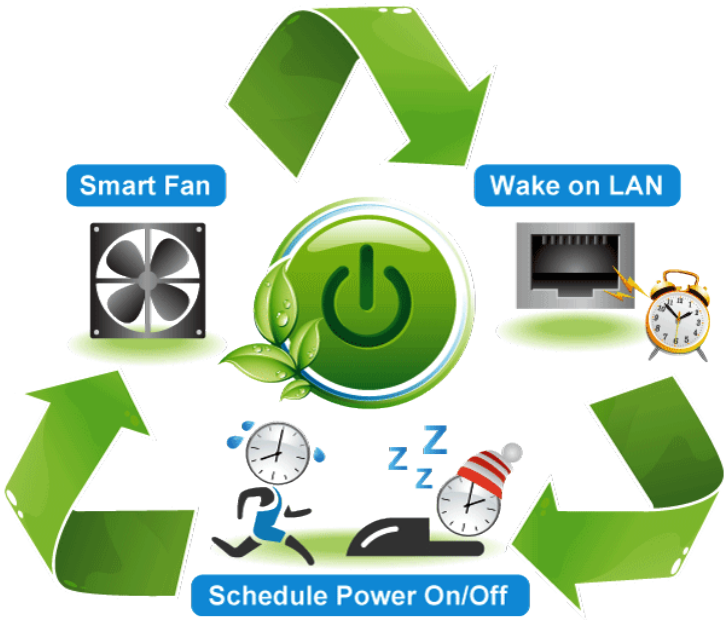
Always-on Data Security with Trend Micro

The NAS-7410 features virus engine scanning technology and cooperates with well-known Trend Micro Anti-virus Company. It updates the virus pattern information automatically via internet to protect NAS against new virus attacks. The real-time online scanning can warn and remove infected files to prevent users from distributing virus from NAS on the network.



Energy Efficient Design

The NAS-7410 features green technologies to protect the environment and save electricity. The smart fan monitors the system temperature of the NAS-7410 and automatically adjusts its speed to ensure quiet operation and power saving. Scheduled power on/off feature provides flexibility to only allow the NAS-7410 to operate in designated time and therefore minimize power usage. The NAS-7410 can be powered on remotely and reduce the power consumption by Wake on LAN.



1.3. Features

➢ **Hardware**

- High performance Intel Dual Core 1.8GHz processor
- Provides scalability up to 16TB (with 4TB per hard drive)
- Tray-less design for genuine plug & play and hot swap use
- Integrated dual Gigabit LAN with Fault Tolerance and Link Aggregation
- Adds storage capacity by connecting external USB / E-SATA hard disk drives

➢ **Network and Configuration**

- Compatible with Windows 2003 / 2008 / XP / Vista / 7, Mac OS 8.x or above, Linux / Unix
- Supports CIFS/SMB to allow Microsoft network remote users to easily retrieve files
- Supports VMware vSphere and Citrix XenServe at Server Virtualization & Clustering

➢ **Data Backup and Management**

- Linux based Samba OS provides EXT3 file system for securing data storage
- Supports RAID 0, 1, 5, 6, 10 and JBOD
- Bad Block Scan & hard drive by S.M.A.R.T.
- Supports NAS and iSCSI / IP-SAN for database and server virtualization applications
- Built-in FTP server allows users to conveniently transfer files
- Allows the administrator to allocate the amount of available disk space to individual users
- Provides password protected data access to all users
- Supports up to 2048 user accounts with individual access rights
- SmartSync backup for automatic client backup
- Snapshot for instant backup and restoration
- NAS to NAS replication for remote backup
- WebDAV enables viewing, adding, or deleting files from the web
- Instant Alert via Email, Buzzer, Trap, Web Reminder

➢ **General**

- Antivirus engine protection by Trend Micro
- Uninterruptible power supply (UPS) supports without data loss in the case of power failure
- Power Saving -- Wake on LAN, Scheduled Power On/Off, Smart-Fan

1.4. Product Specifications

Model	NAS-7410 4-Bay SATA NAS RAID SERVER with iSCSI
Hardware Platform	
CPU Frequency	Intel D525 1.8GHZ
Memory	DDR3 2GB
Supported hard drive	4 x 2.5”/3.5" SATA I/II/III hard drive (Hard drive not included) File System: EXT3
Buttons	1 x Power button 1 x Reset button
LAN Interface	2 x Gigabit Ethernet port with load balancing and fault tolerance
USB Interface	6 x USB2.0 port for external storage and UPS File System: FAT16/32, NTFS
E-SATA Interface	1 x E-SATA port for external storage

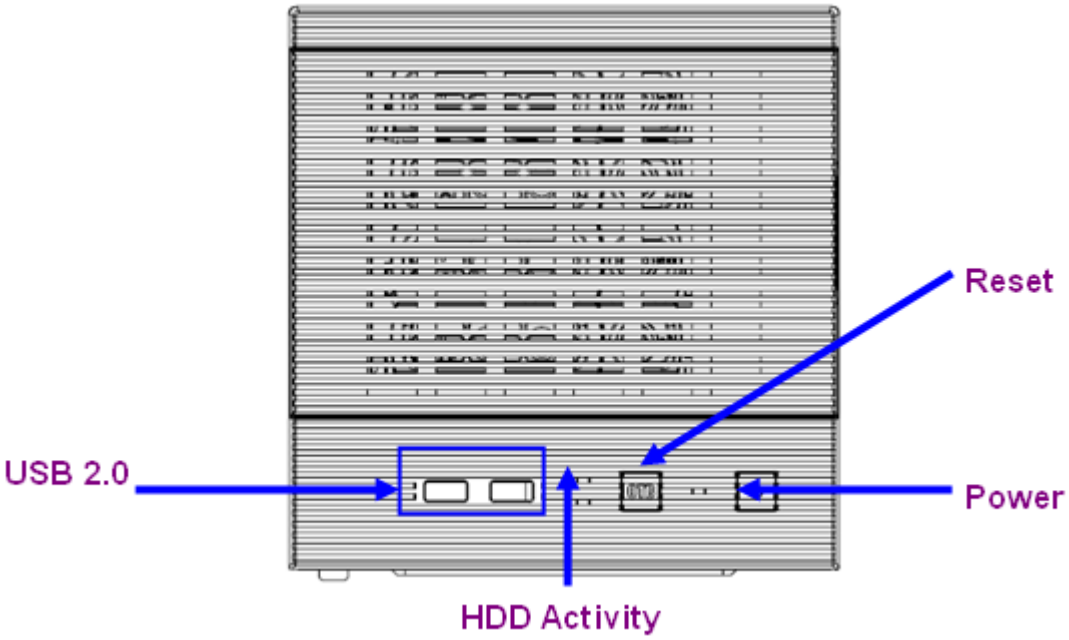
	File system: FAT16/32, NTFS
COM Interface	1 x COM port for UPS
Fan	1 x quiet cooling fan (12 cm, 12V DC, Max. 15400rpm)
Alarm Buzzer	System warning
Secure Design	Lock security slot for Hard drive prevention
Network and Configuration	
Network Standard	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3ab 1000Base-T IEEE 802.3ad for dual link aggregation
Protocol	IPv4 & IPv6, AppleTalk HTTPS, CIFS/SMB, AFP, NFS(v3/v4), FTP, FTPS (SSL, TLS), SSH, SMTP, SNMP, NTP, iSCSI
Security	Password protection IP address filtering HTTPS encrypted data transmission 802.1X Port-based authentication for network protection QoS / DSCP
Supported Languages	Unicode UTF-8
Supported Browsers	Microsoft Internet Explorer 8, 9, 10 Google Chrome Firefox
Supported Clients	Windows XP, Vista, Windows 7 (32-/64-bit), Windows Server 2003/2008 R2 Apple Mac OS 8.X / 9.X / 10.6X Linux & UNIX
Data Backup and Management	
RAID level	Single Disk, JBOD, RAID 0, 1, 1 + Hot Spare, 5, 5 + Hot Spare, 6, 6 + Hot Spare, 10, 10 + Hot Spare
Max. User/ Groups	2048 (including local/domain account/groups)
Max. Shared Folder	256
Max. Concurrent Connections	150
Max. iSCSI Target/LUNs	8
Disk Management	Bad Block Scan & hard drive S.M.A.R.T. Global hot spare drive RAID Recovery BSR (Bad Sector Remap)
Backup Solution	SmartSync: NAS-to-NAS, NAS-to-USB/E-SATA, USB/E-SATA-to-NAS Snapshot: Point-in-time Copy in a Flash System Profile: Recover from system failures Disc Server: Optical disc recording

	Data Backup to Multiple External Storage Devices
Security	Network Access：SSH, HTTPS, FTP, CIFS/SMB, AFP Encrypted Access: HTTPS, FTP with SSL/TLS, SSH/SFTP, Encrypted Remote Replication between NAS Servers Built-in Trend Micro antivirus software Access Control List (ACL) Secure Sockets Layer (SSL) 128-bit encryption Instant alert via email, buzzer, trap, web reminder
General	
Power Requirements	100~240V AC, 3.5A, 50~60Hz
Operating Temperature	0 ~ 40 degrees C
Operating Humidity	10 ~ 80% (non-condensing)
Weight	5.1Kg
Dimensions (W x D x H)	200 x 320 x 210 mm
Power Management	Wake on LAN Scheduled Power On/Off COM Port, USB and Network UPS Support
Antivirus	Protection against the latest known viruses, Trojans, and other threats Virus pattern update on manual or scheduled basis Email notification upon task completion or virus detection Quarantines or deletes infected files Real-time and scheduled scan setting
Emission	CE, FCC

Chapter 2. Hardware Interface

2.1 Physical Descriptions

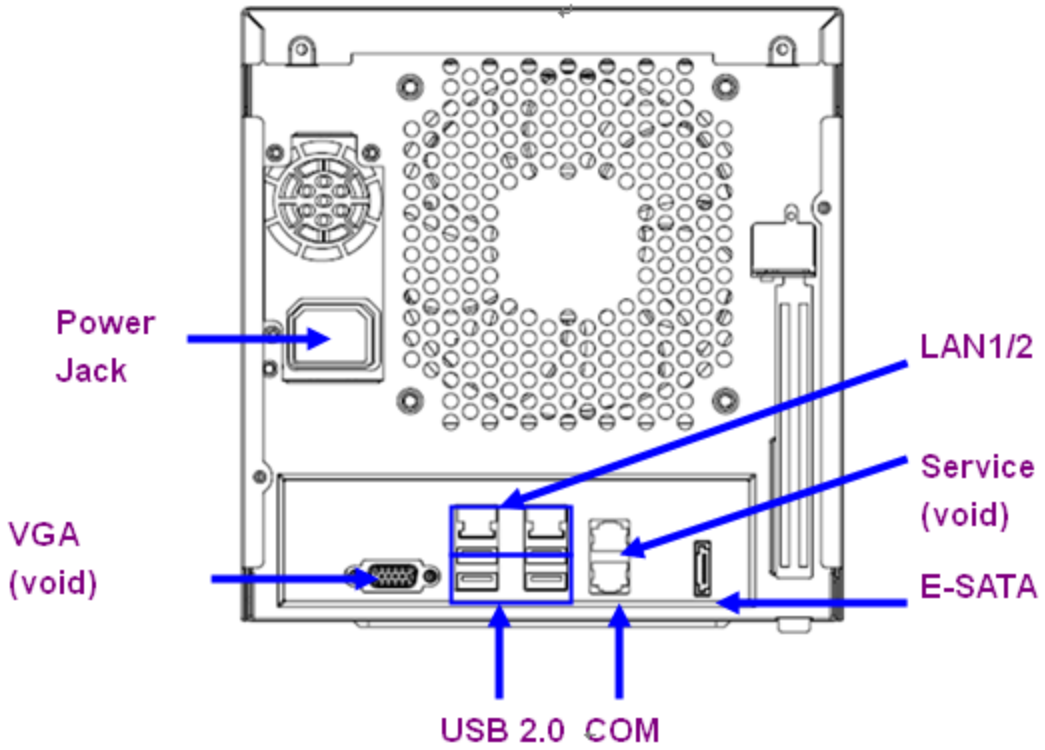
2.1.1 Front Panel



Interface	Description
Power Button	Press the button to start the NAS
Reset Button	This button is used to restore all the factory default settings
USB Socket	Connects to UPS and external HDD(FAT/FAT32/NTFS)

LED	Color	Description
Power	Blue	On: Power on Off: Power off
HDD Activity	Red	HDD is being accessed

2.1.2 Real Panel

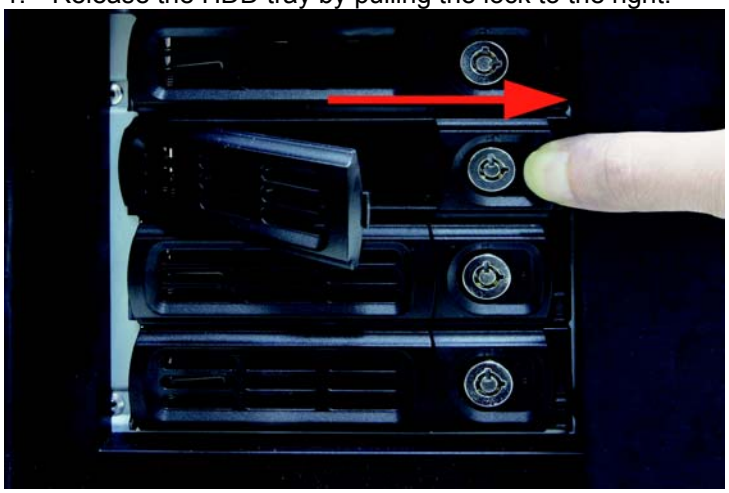


Interface	Description
Power Jack	Connect the two power supply cords shipped with the system
E-SATA	Connect to external hard drive case
COM	Connect to UPS
LAN Jack (LAN1)	These RJ-45 ports support auto negotiating Gigabit Ethernet interface. That allows your system to be connected to an Internet Access device, e.g. router, cable modem, or ADSL modem over a CAT.5 twisted pair Ethernet cable.
LAN Jack (LAN2)	
USB Socket	Connect to UPS and external HDD(FAT/FAT32/NTFS)
VGA	Future Feature
Service	Future Feature

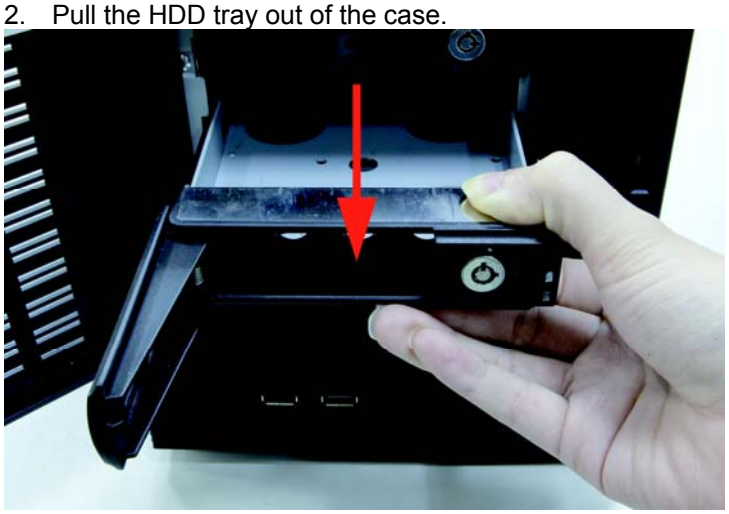
2.2 Hardware Installation

2.2.1 Installing the Hard Disk Drive

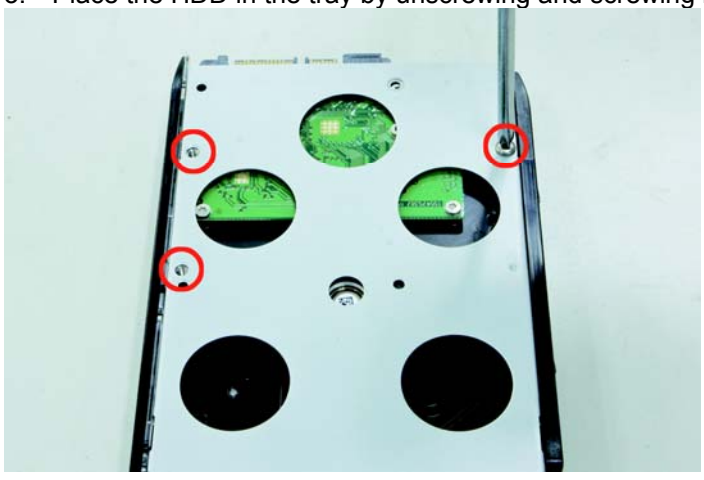
1. Release the HDD tray by pulling the lock to the right.



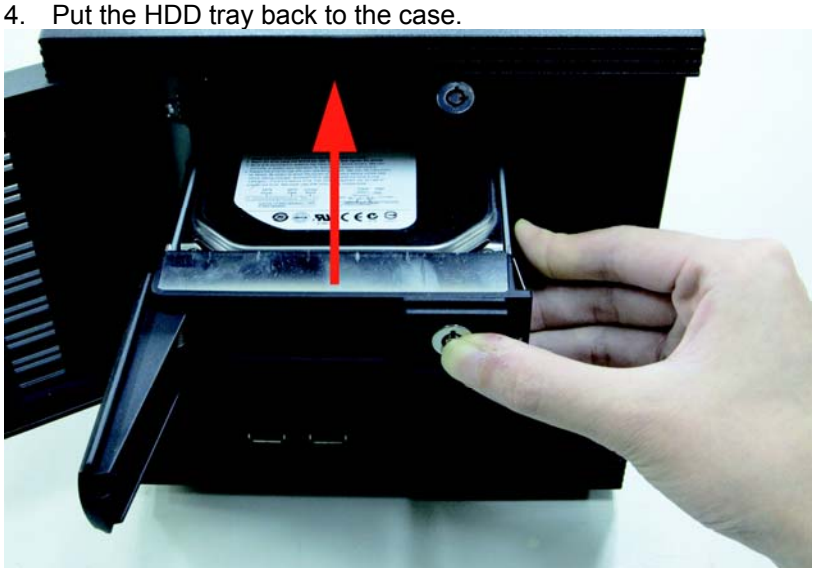
2. Pull the HDD tray out of the case.



3. Place the HDD in the tray by unscrewing and screwing it.



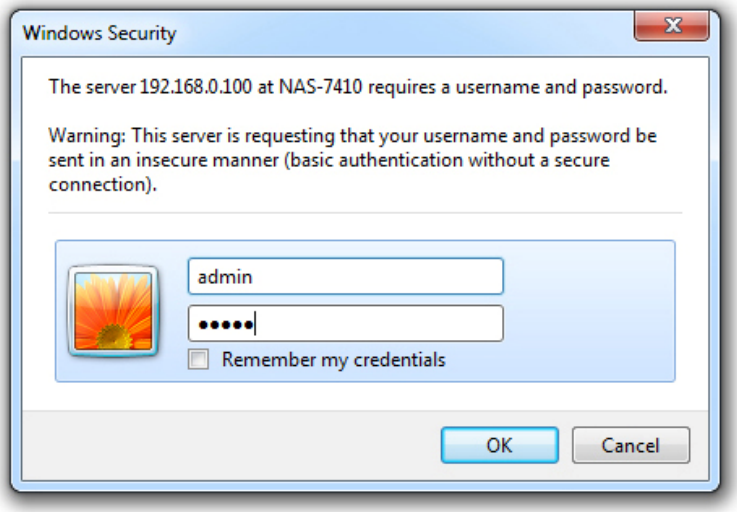
4. Put the HDD tray back to the case.



5. Push the tray door back to the case to secure it.

2.2.2. Network Installation

The NAS-7410 provides GUI (Web based, Graphical User Interface) for management and administration. The default IP address of NAS server is **192.168.0.100**. You may now open your web browser, and insert **http://192.168.0.100** in the address bar of your web browser to login web configuration page. The NAS server will prompt for login username / password. Please enter: **admin** / **admin** to continue the NAS Server administration.



Default DHCP Client	OFF
Default IP Address	**192.168.0.100**
Default Login User Name	**admin**
Default Login Password	**admin**
Search Tools	NAS Finder

Note

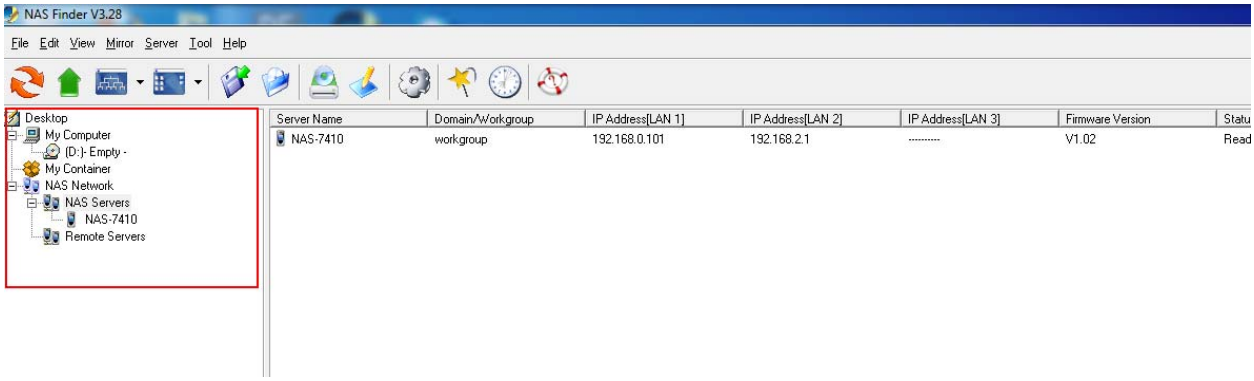
If the networked device's default IP Address (**192.168.0.100**) is already used by another device, the other device must be turned off until the device is allocated a new IP Address during configuration.

2.3 Initial Utility Installation

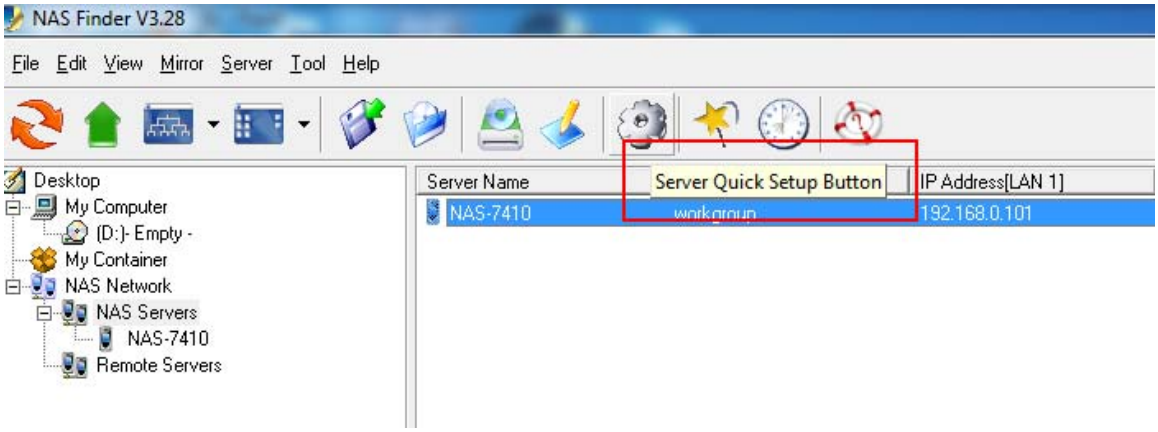
This chapter shows how to quickly set up your NAS system. The NAS is with the default settings. However to help you find the networked NAS quickly the windows utility PLANET NAS Finder can search the NAS in the network that will help you to configure some basic setting before you start advanced management and monitoring.

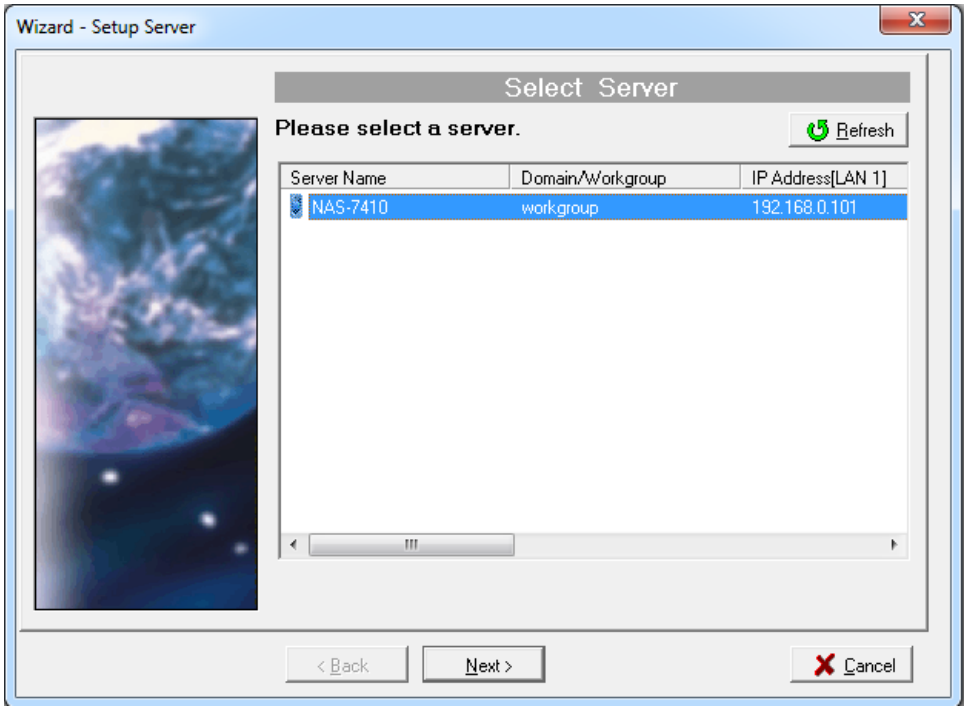
Configuring the IP addresses using NAS Finder
The utility is designed to perform a quick setup and put your NAS server online in just a few minutes. During startup, NAS Finder begins to discover the entire NAS server on the network. The default server name would be **NAS-7410**.

1. Highlight the server you want to configure from the left hand pane.

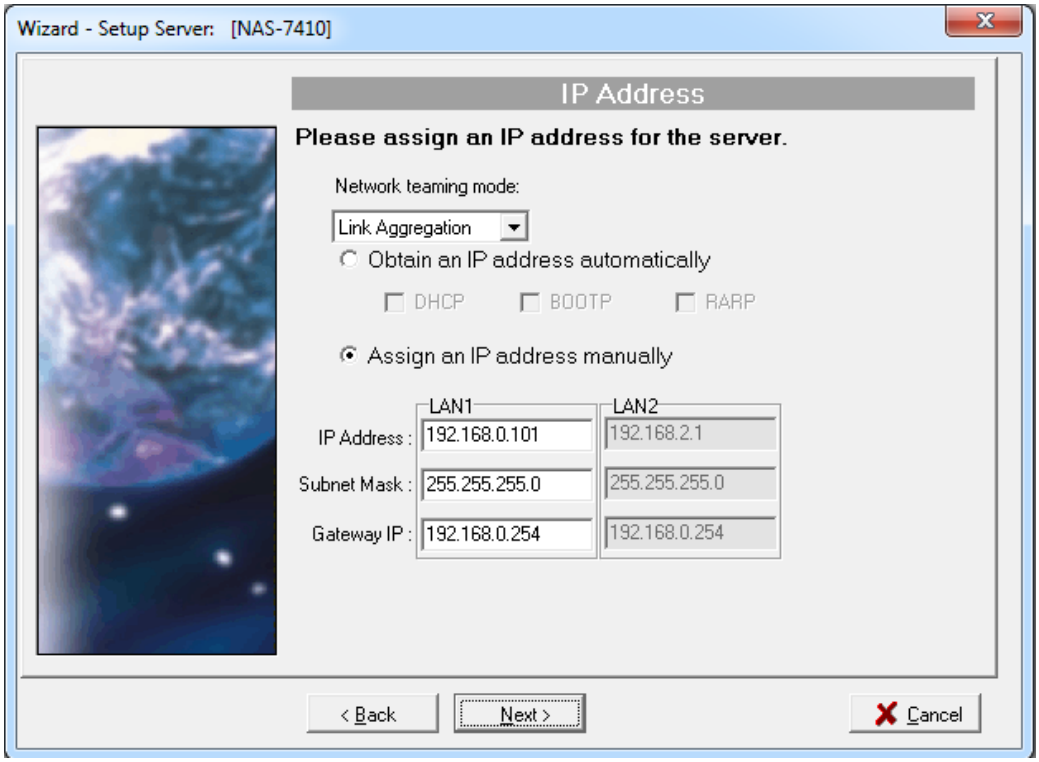


2. Click the setting button on the toolbar.

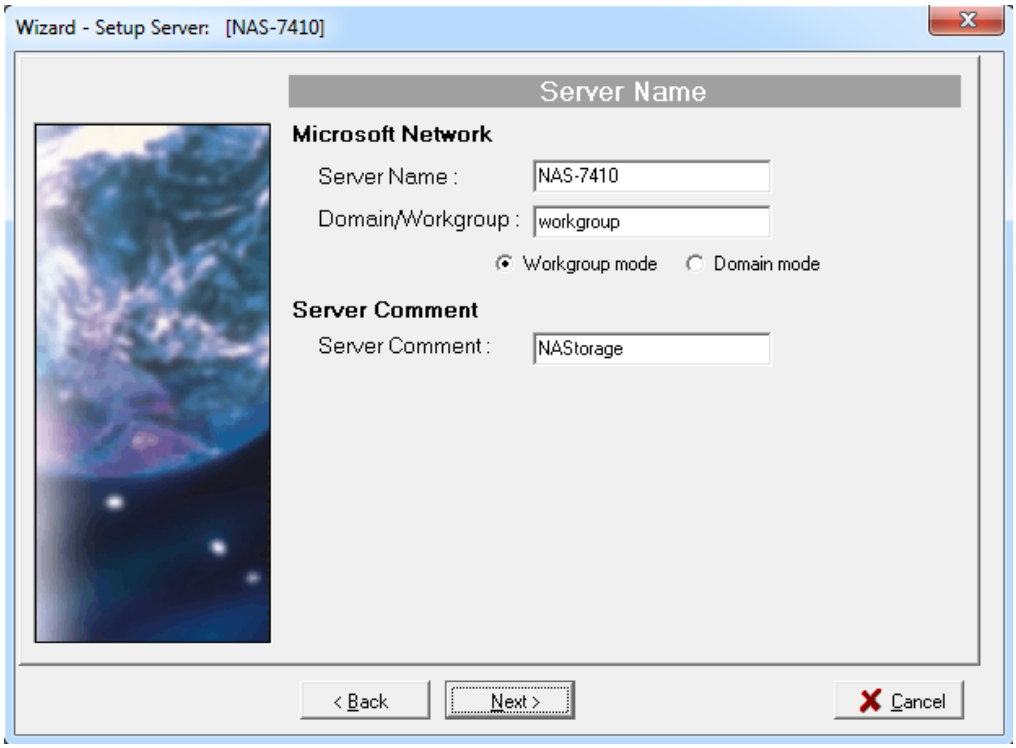




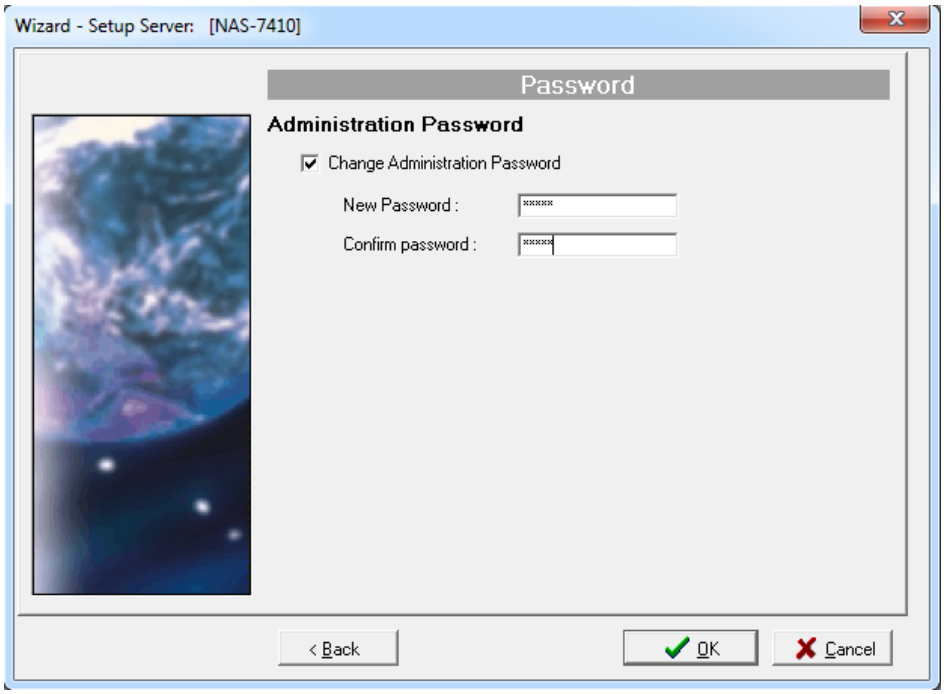
3. The default is Assign an IP address manually. If you want IP settings to be assigned automatically, click **Obtain IP settings automatically.**



4. Enter the **Server Name**, **Server Comment**, and **Workgroup/Domain Name** and select either the **Workgroup mode** or **Domain mode**.



6. Change the admin password if necessary.



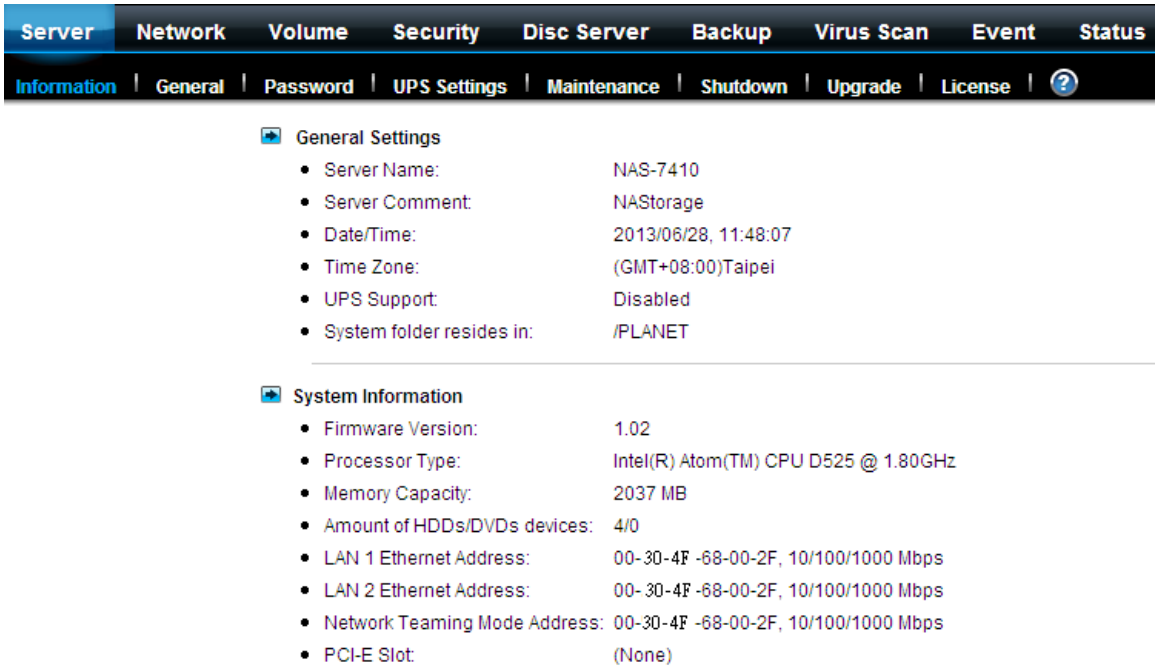
7. Click the **OK** button to save the settings.

Chapter 3. Server Configuration

This chapter describes how to name the server, specify the server date and time, upgrade the OS firmware, shut down the system and use UPS with the NAS server.

3.1. Server Information

Click **Server** from the administration homepage. You will see the **Information** page describing the summary information of the NAS server.



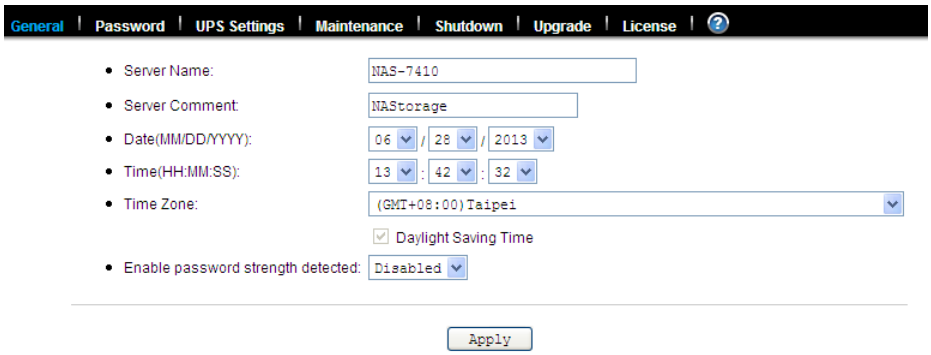
Item	Description
Server Name	Name of the NAS server. A NAS server has one unique name, applicable to all network protocols.
Server Comment	The text which is shown in the comment field when browsing network computers in Windows Network Neighborhood.
Date/Time	Server date and time in 24-hour format.
Time Zone	The time zone setting of the server relative to the Greenwich standard time.
UPS Support	Indicates whether the UPS support is enabled or not.
System Folder resides in	Display the volume name in which the system folder is located.

The **System Information** section shows the hardware and firmware status of the server.

Item	Description
Firmware Version	The version number of the OS firmware.
Processor Type	The CPU operating frequency.
Memory Capacity	The total size of the main memory.
No. of HDD/CD/tape	Display the number of HDD/CD/tape installed in the system.
LAN1/2 Ethernet Address	The Ethernet MAC addresses of the network controller chips and their types.
PCI-E Slot	Display the type of the add-on adaptor installed in the system. Note: The NAS-7410 cannot support this function.

3.2 General

The **General Settings** section shows the parameters which can be modified on the **Server→General** page.

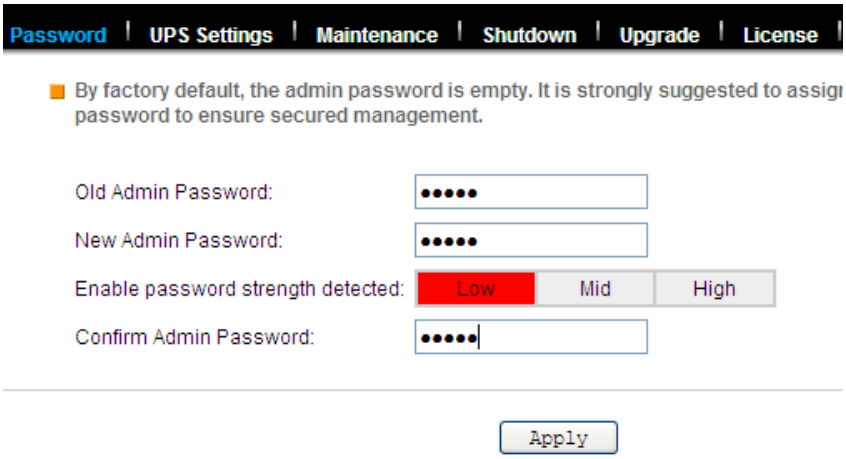


3.3 Modifying the administrator's password

Admin is a built-in user account for the administrator. It is like the **root** account in UNIX or the **administrator** account in Windows 2000 or XP. Using this account, users have access to the administration homepage and all the storage resources. By default, the password for this user account is empty. To prevent security vulnerability, it is strongly suggested to specify the password when performing the first-time setup of the NAS server.

To specify or modify the administrator's password, please select the **Server→Password** menu on the administration homepage. Input the current admin password in the **Old Admin Password** field, and the new password in the **New Admin Password** and **Confirm Admin Password** fields. Then click **Apply**.

The administrator can delegate the administrator's privilege to other users by including them into the **Admins** built-in group. Please select the **Security→Account** menu. Select **Admins*** in the **Local User/Group** window and click **Property**. Specify the users to have the privilege and click **Apply**.

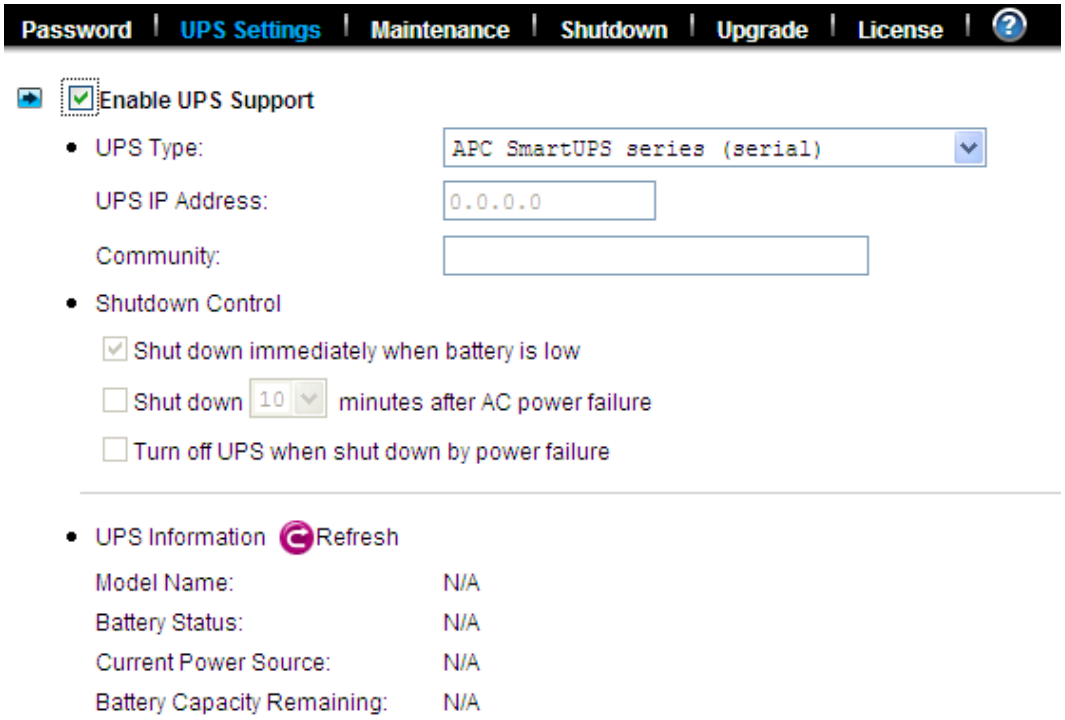


3.4 Enabling UPS support

The NAS server supports UPS and basic power management functions. It sends alerts when there are power events like utility power failure or low battery capacity. When power events occur, the NAS server can shut down itself automatically to prevent potential data loss.

To use smart-signaling UPS, connect UPS to the NAS server with an RS-232 or USB cable. Then go to the Server UPS Settings menu on the administration page to enable UPS support.

To use network-type UPS, connect the UPS to the LAN first. Then go to the Server UPS Settings page on the administration page. Enable APC Smart UPS series, such as USB UPS, and Generic serial UPS Type 1 and Type 2. Select Network UPS from the UPS Type menu and enter the UPS IP address and correct community.



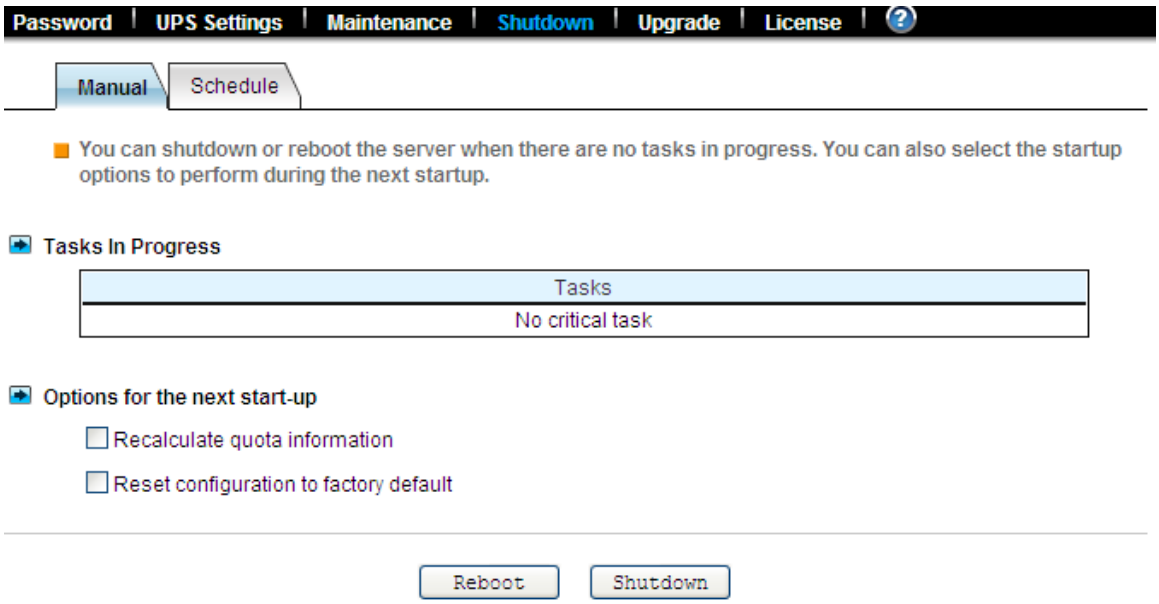
Item	Description
Shut down immediately when battery is low	Specify whether to shut down the server when UPS battery is low. Note: When utility power fails, the NAS server will always shut down.
Shut down in x minutes after AC power failure	Specify how many minutes to wait before shutting down the server when a power event occurs.
Turn off UPS when shut down by power failure	If checked, the NAS server will turn off the UPS while it is shutting down by power failure. If not, the UPS will still be working when the server is shut down.

3.5 Shutting down the server

Shutdown, reboot and startup actions

The NAS server can be shut down by pressing the power button twice on the front of the server case. The whole shutdown process might take seconds to minutes until data are all safely saved to the hard disks. To shut down the server from the **Administration Homepage**, select **Shutdown** from the **Server** menu and click the **Reboot** or **Shutdown** button.

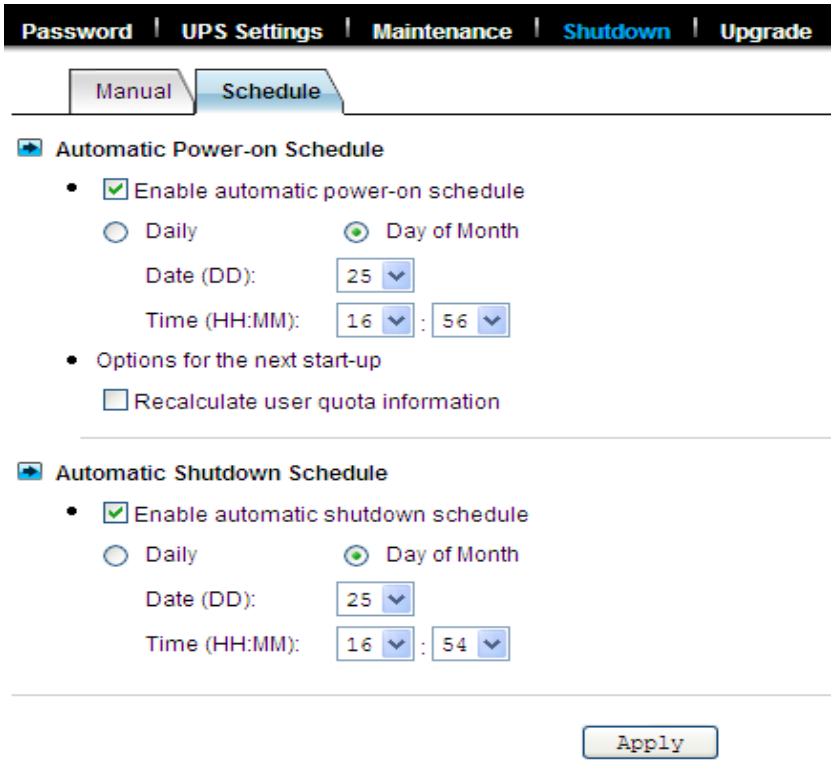
You can specify the actions to take during the next startup.



Item	Description
Recalculate user quota information	Recalculate the storage consumption per user during the next startup. It may take much time if there are a huge amount of files in disk.
Reset configuration to factory default	Reset all configurations to default.

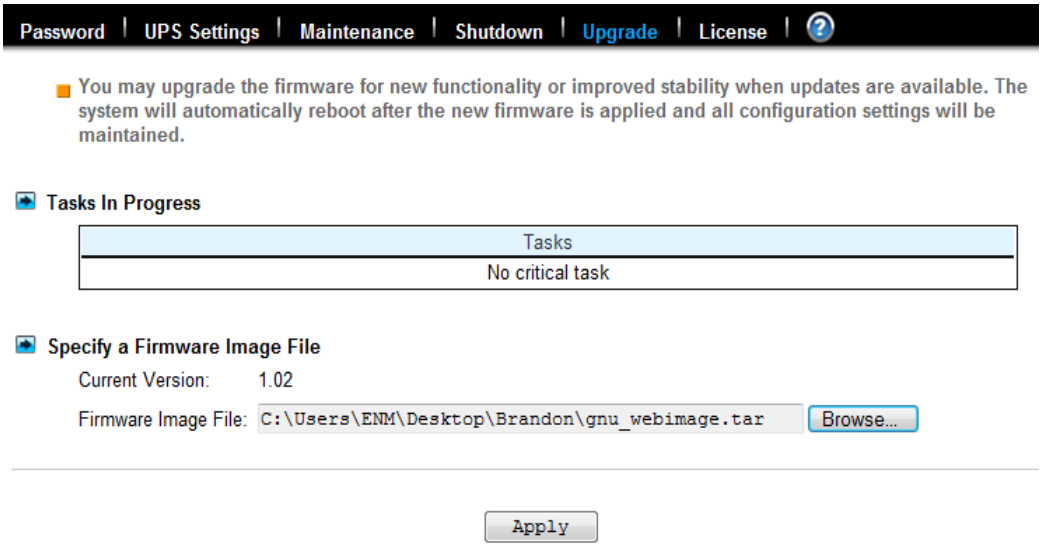
Scheduled shutdown and power-on

To set the automatic power-on and shutdown schedules, select the **Server→Shutdown** menu. Click the **Schedule** tab to modify the schedules. On the schedule settings page, you can set daily or day of month schedules. Check the **Enable** check-boxes and specify the time of powering on or shutting down. Remember to click the **Apply** button to submit the changes.



3.6 Upgrading the firmware

Updating OS firmware will accommodate new functions or bug-fixes. Once you get new releases of an OS firmware image, you can upgrade the OS firmware by using the web browser. The process is simple and fast. Once you get the image file of the new OS firmware from your vendor, open the **Administration Homepage** of the NAS server and select the **Server→Upgrade** menu. Specify the full path of the image file or click the **Browse**… button to find it. Click **Apply** to begin. The process might take several minutes. The server will reboot after the firmware is upgraded.



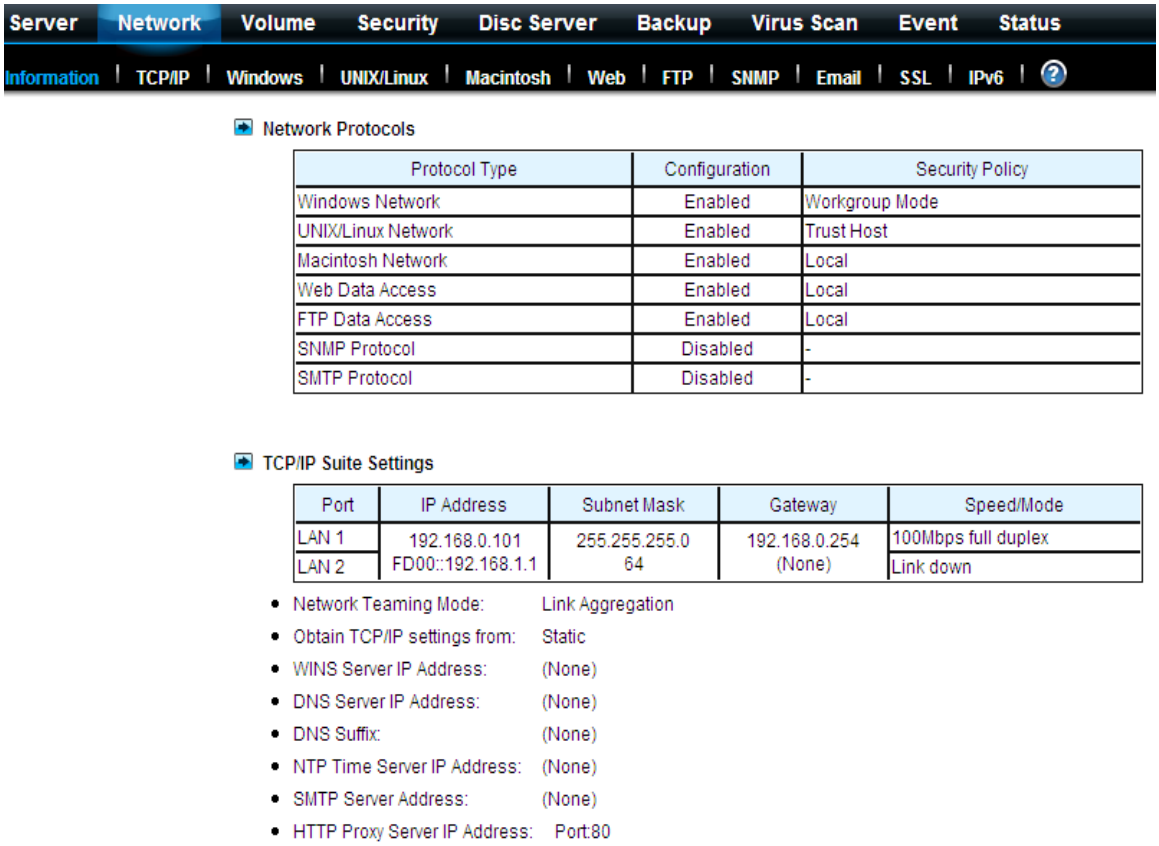
Chapter 4. Network Configuration

This chapter details concepts and procedures for configuring the NAS server and establishing the system that can communicate among various OS platforms. Management protocol and email notification setting are also covered in this chapter.

4.1 Network Information

The “Network Information” screen is the summary of the current network settings of the NAS server. It provides the administrator a quick look of the basic network setting of the NAS server.

The “Information” page is divided into two sections. The “Network” Protocols section displays the current network protocol settings of the server.



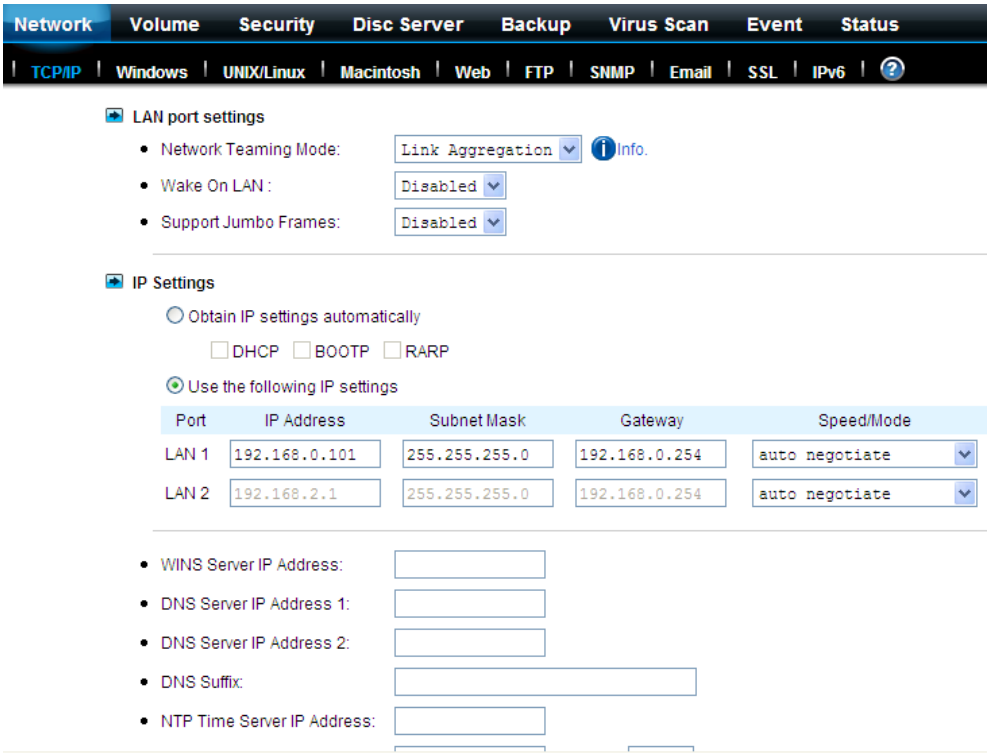
Item	Description
Protocol Type	Display network protocol supported by the server.
Configuration	Current status of the network protocol. Status: Enabled or Disabled
Security Policy	Display type of the security policy of the network protocol.

The “TCP/IP Suite Settings” section shows the various TCP/IP settings of the server.

Item	Description
Port	Display Ethernet port #.
IP Address	An identifier for a network resource on a TCP/IP network.
Subnet Mask	A subnet mask is used to determine what subnet an IP address belongs to.
Gateway	A node on a network that works as a point of entry to another network.
Speed/Mode	10/100/1000 Mbps and full/half duplex.
Network Teaming Mode	Display the current network teaming mode.
Obtain TCP/IP settings from	Display the IP settings that is either assigned automatically from DHCP or assigned manually.
WINS Server IP Address	Windows Internet Naming Service (WINS) manages the association of network resources name and its IP addresses without the user or an administrator having to be involved in each configuration change.
DNS Server IP Address	IP address of the domain name system (DNS) server which locates the domain names and translates it into IP addresses.
DNS Suffix	Display the DNS suffix.
NTP Time Server IP Address	The IP address of the NTP (Network Time Protocol) server is used to synchronize system time automatically over the net. The system time will be synchronized with the NTP server every 24 hours.
SMTP Server Address	IP address or server name of the SMTP (Simple Mail Transfer Protocol) server used in sending and receiving e-mail.
HTTP Proxy Server IP Address	IP address of the HTTP proxy server. Next to the IP address is the port number.

4.2 TCP/IP settings

TCP/IP handles network communications between network nodes that are connected to the network. It is important to set up correct TCP/IP setting for NAS server to function properly.



Item	Description
Network Teaming Mode	The NAS server provides two on-board 10/100/1000 or Gigabit Ethernet ports (LAN1 & LAN2). You can configure the Ethernet ports using the following operating modes: **Stand Alone:** Each LAN1 & LAN2 is configured with a unique IP address, which is independent to each other. **Fault Tolerance:** Uses LAN2 to take over LAN1 if LAN1 fails to connect to the network which is designed to ensure server availability to the network. **Load Balancing:** Offers increased network bandwidth by allowing transmission to multiple destination addresses using both LAN1 and LAN2. If the traffic of one of the LAN ports starts to get congested, requests are then forwarded to the other LAN port with more capacity until the traffic of both LAN ports start to get balanced. Note that only the LAN1 Ethernet port receives incoming traffic. **Load Balancing** also incorporates Fault Tolerance protection. **Link Aggregation:** Combines both LAN1 & LAN2 into a single channel, appearing to use a single MAC address to provide greater bandwidth. It must be used with a network switch having the **Link Aggregation** or **Trucking** function.
Wake-on-LAN	Allows administrators to remotely power on your NAS server to perform maintenance task on the server with no need to go to the server physically.

Configuring TCP/IPv4 settings

1. Select a **Network Teaming Mode** from the pull-down menu that suits your needs.

2. Enable or Disable **Wake on LAN (Available for LAN1 or LAN2)**.

3. Click the **Obtain IP settings automatically** radio button to obtain IP addresses of your NAS server from DHCP, BOOP or RARP server on the network.

4. Or, click the **Use the following IP settings** radio button to assign the IP addresses manually.

5. Note that LAN3 IP address field will appear only when the optional Gigabit Ethernet adapter is installed in your system.

6. Input the **WINS server IP address**.

7. Input the **DNS server IP address**.

8. Input the **DNS Suffix**.

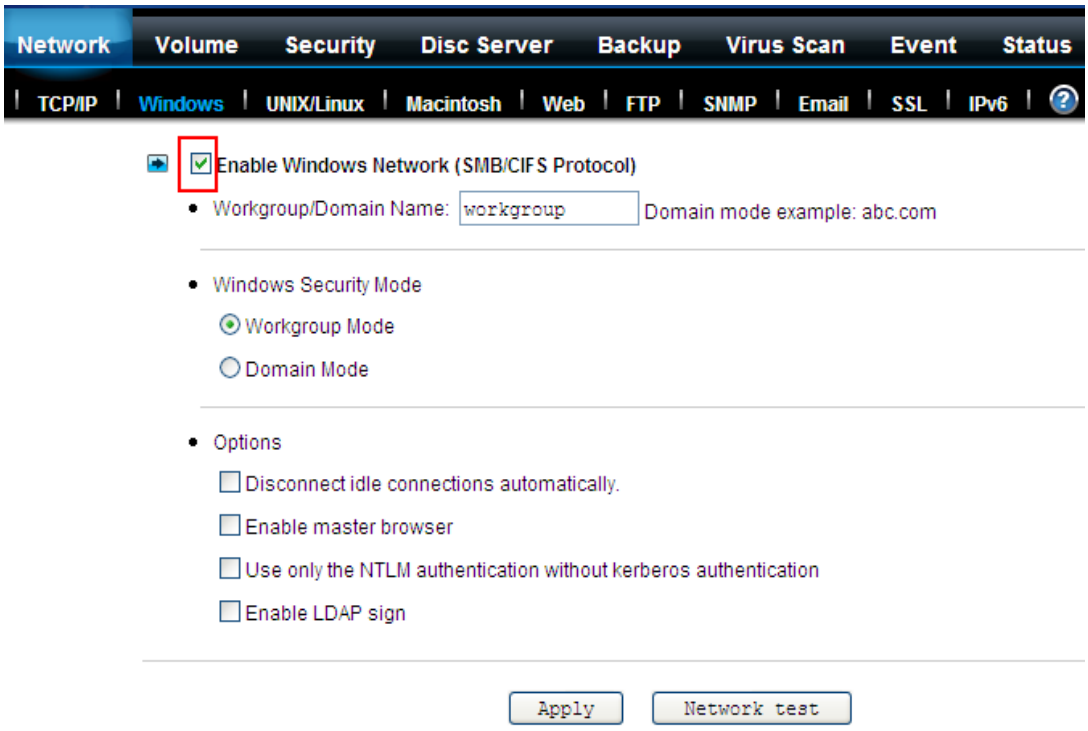
9. Input the **NTP Time Server IP Address** if available.

10. Click **Apply** to save the setting.

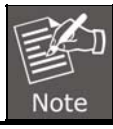
To disable a LAN port, enter 0.0.0.0 in its IP address field. If you happen to disable all LAN ports and cannot access the administration page, please use the LCD panel to change the IP address to non-zero values.

4.3 Windows settings

NAS server adopts the SMB (Server Message Block)/CIFS (Common Internet File System) protocol, used by Microsoft, to share files, directories and devices with the Windows client.



Item	Description

Workgroup Mode	NAS server becomes a member of a workgroup and communicates with the clients using its internal user database for authentication and does not require other authentication servers to be present in the network.
Domain Mode	NAS server becomes a member of a domain and communicates with the client using the user database stored in an authentication server which must be present in the network. Optionally, you can register the NAS server to the domain. Once registered, the NAS server will be created as a machine account on the domain controller. And it will use Kerberos as the authentication mechanism, which provides better integration into the Windows network environment.  As Kerberos has more tight security policy, NAS, Domain and Client's date/time are required to have a time difference of not more than 5 minutes.

Configuring windows network settings

1. Click the **Enable Windows Network (SMB/CIFS Protocol)** checkbox to enable access for SMB client.

2. Enter the Workgroup/Domain name. Use FQDN if you want to configure

   NAS server in Domain Mode e.g., Microsoft.com

3. Click the **Workgroup Mode** radio button if you want to configure NAS server in **Workgroup Mode**.

4. Or, click the **Domain Mode** radio button if you want to configure NAS server in **Domain Mode**.

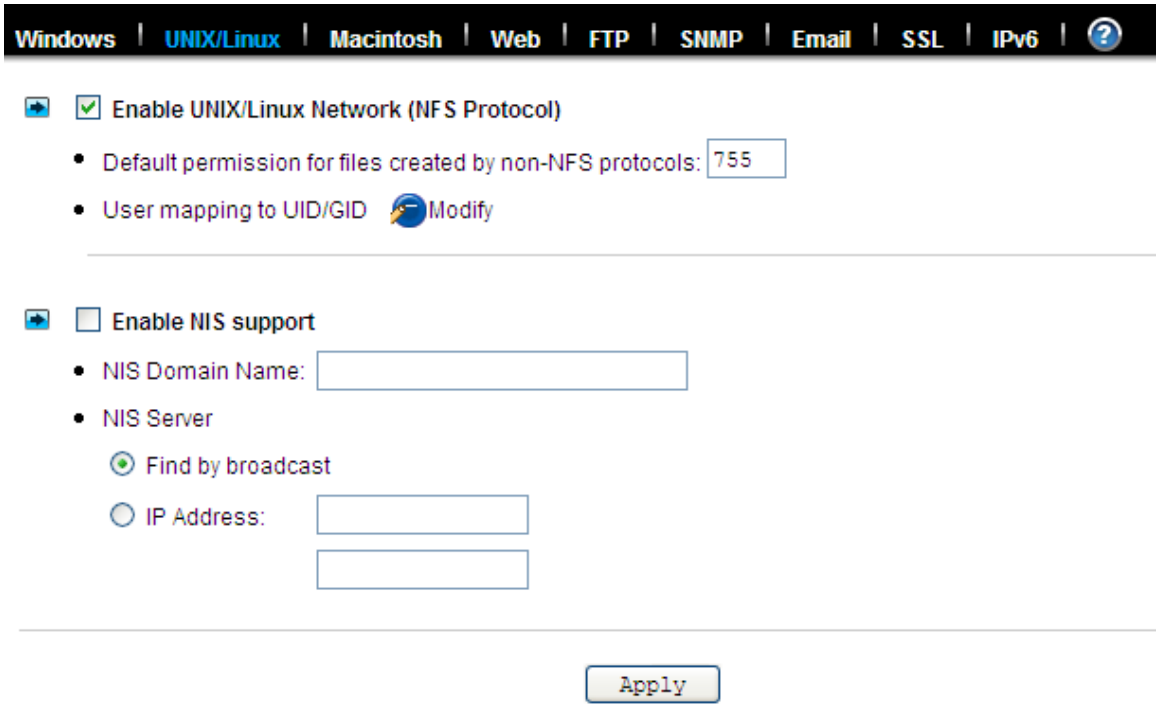
5. Input the domain manager's user name and password (Power Users at least)

6. Select the option to disconnect idle connection automatically. Server will disconnect the connections which have been idle for 5 minutes if this option is enabled.

7. Click **Apply** to save the setting.

4.4 UNIX/Linux settings

NAS server can export shares to UNIX/Linux client via NFS protocol. UNIX/Linux client then can mount the shares and gain access to the content of the shares. UNIX/Linux client uses UNIX user identification, typically consisting of User Identifier (UID) and Group Identifier (GID), for access control. Non-NFS clients do not use UIDs and GIDs for identification. Since NAS server is intended for working in a heterogeneous network, files created by non-NFS client could possess incorrect ownership information and generate inaccurate quota information for UNIX/Linux clients due to the unmatched UID and GID. A mapping is needed to maintain the correct identity of the user using multiple protocols to access NAS server, for example, Windows and UNIX/Linux clients. Windows based clients need to map the Windows user name to UID/GID before forwarding a request to retain the correct ownership information for UNIX/Linux clients. By default, the NAS server maps all non-NFS users, including local users and domain users, with the same UID/GID as defined on this page. If the administrator wants to have different UID/GID for different users, he should click the **Modify** button to modify the user mapping to UID/GID.



Item	Description
UID	User ID. The numeral is assigned to a user with Unix/Linux permissions. NFS uses UID to determine permissions on files and directories.
GID	Group ID. A part of POSIX permissions that determine groups of users. NFS files have a GID assigned to them.
Permission	Three numbers are used for setting the file permission. Each of the three numbers corresponds to the type of users -- Owner, Members of a group and Everyone Else.

Number	Read (R)	Write (W)	Execute (X)
0	No	No	No
1	No	No	Yes
2	No	Yes	No
3	No	Yes	Yes
4	Yes	No	No
5	Yes	No	Yes
6	Yes	Yes	No
7	Yes	Yes	Yes

For example, if the permission of a file is set to 777, this file has read, written and executed permissions for the owner, the group and for other users.

Configuring UNIX/Linux network settings

1. Click the **Enable UNIX/Linux Network (NFS Protocol)** checkbox to enable access for NFS client.

2. Enter the default permission for files created via non-NFS protocol. (Default setting = 755)

3. Click **Apply** to save the settings.

4. Click the Modify icon and enter the default UID and GID. (Default setting = 0)

5. Choose to map all users to the default UID/GID or assign UID/GID for each user manually.

6. Click **Set Default** link to set the UID/GID of all users to the default UID/GID. Note that the value '-1' represent that the UID/GID is equal to the default UID/GID configured above.

7. Click **Apply** to save the settings

Configuring NIS settings

The NIS (network information services), formerly known as Yellow Pages, is a UNIX standard for centralizing the management of UNIX resources. The NAS server supports the retrieval of user accounts and their UID/GID from an NIS server.

If the NIS support is enabled, the NAS server can auto-map NIS users with local/domain users. It matches user names and assigns the UID/GID of the matched NIS users to local/domain users. The user auto-mapping function provides better and tighter integration between NFS clients and other network operating systems.

The steps of enabling NIS support are as follows:

1. Check the **Enable NIS Support** checkbox.

2. The NIS domain name is required. Please fill in the correct name in **NIS Domain Name** field.

3. If you do not know the IP address of the NIS server, please specify **Find by broadcast**. Otherwise, specify the IP address in the fields.

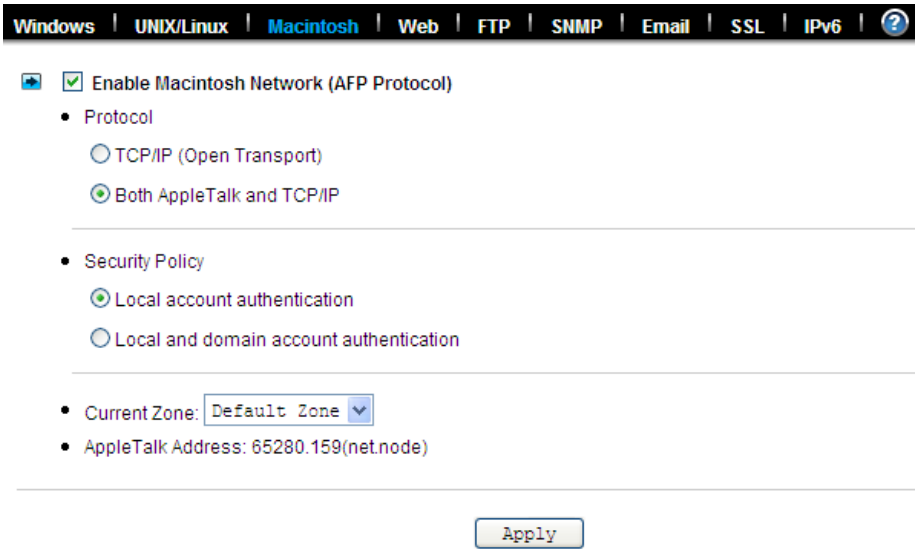
4. After enabling the NIS support, you can auto-map NIS users with local/domain users. In **UNIX/Linux** menu, click the **Modify** icon.

5. Select **Map users to UID/GID as defined below** to Apply**.**

6. Click the **Auto-map with NIS user's** link to map with the users in the configured NIS server.

4.5 Macintosh settings

NAS server supports two kinds of protocols used for Mac OS clients –**TCP/IP (Open Transport) and Both AppleTalk and TCP/IP**. Also, NAS server provides two kinds of security polices for Macintosh Network AFP client.



Item	Description
Local Account Authentication	Authenticate user using NAS server's internal user database.
Local and Domain Authentication	If **Windows Network** is enabled, you can enable both local and domain authentication for AFP client.
Current Zone	A division between groups of machines when viewed using AppleTalk. AppleTalk Zones can be seen in the Chooser, the AppleTalk Control Panel, and the Network Browser.
AppleTalk Address	It is a unique number that identify the server on the network. The number to the left of the dot is the network number. The number to the right of the dot is the node number.

Configuring Macintosh network settings

1. Click the **Enable Macintosh Network (AFP Protocol)** checkbox to enable access for AFP client.

2. Select a protocol and click the radio button beside it.

3. Click the **Local account authentication** radio button to authenticate user using the server's local user database.

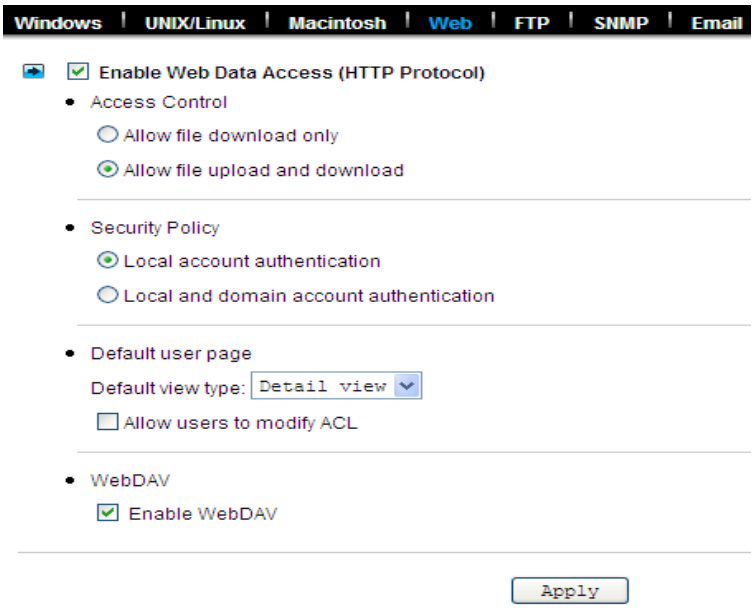
4. Or, click the **Local and domain account authentication** radio button to use both local account and Microsoft domain security authentication.

5. Select the **Current Zone** from the pull down menu or **Default Zone** is assigned by default.

6. Click **Apply** to save the setting.

4.6 Web data access settings

This section shows the parameters that you can set up for user to access NAS system user's home page. You can configure the user access constraint, authentication policy and default setting by defining the **Access Control**, **Security Policy** and **Default User Page** settings.



Configuring web data access

1. Click the **Enable Web Data Access (HTTP Protocol)** checkbox to enable Web data accessing.

2. Choose **Allow file download only** or **Allow file upload and download**.

3. Click the **Local account authentication** radio button to authenticate user using the server's local user database.

4. Or, click the **Local and domain account authentication** radio button to use both local account and Microsoft domain security authentication.

5. Select the default type of the folder display on the user page. You can choose from **Detail View**, **Large Icons** or **Small Icons**.

6. Click the checkbox beside the **Allow users to modify ACL** to give users the privilege to modify the ACL table entries.

7. Click **Apply** to save the setting.

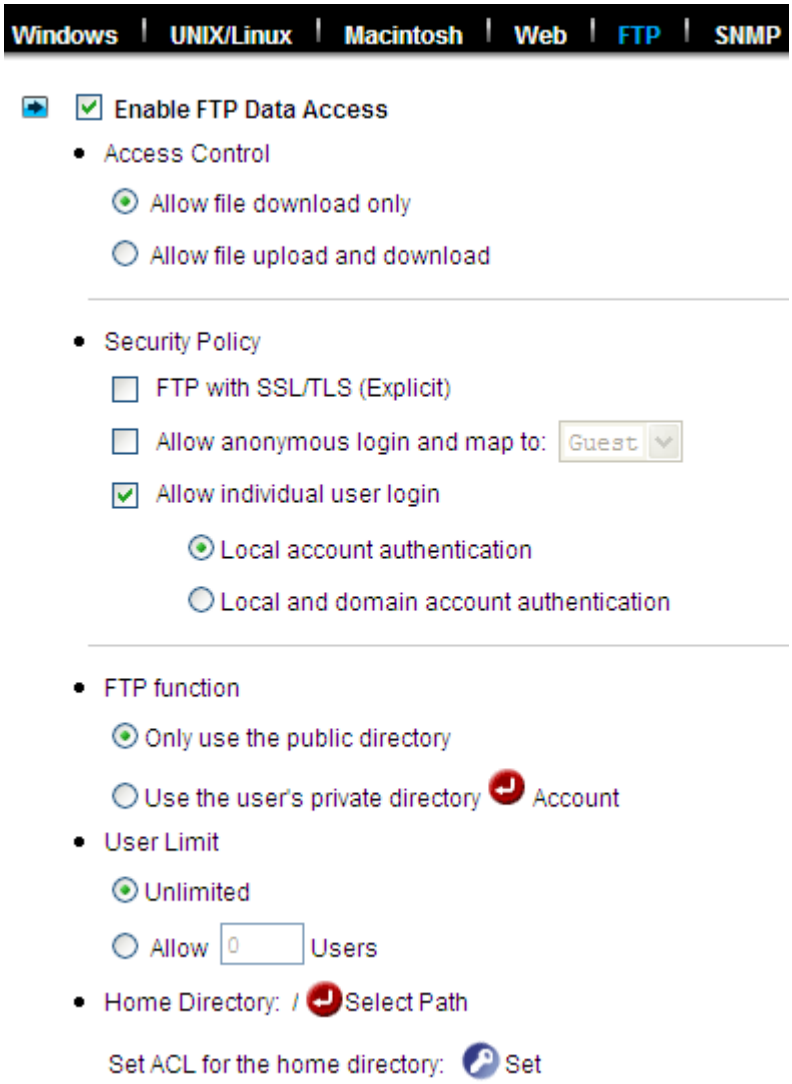
Configuring WebDAV Settings

1. Go to **Network→Web** page.

2. Click the **Enable WebDAV** checkbox to enable WebDAV function.

4.7 FTP data access settings

NAS system supports File Transfer Protocol (FTP) that allows users to transfer files via the Internet. By properly configuring the FTP settings, you can effectively control how users access the content in your NAS server via FTP.



Configuring FTP data access

1. Select Access Control option to determine whether FTP clients can download only or allow users to upload and download data after being connected with FTP protocol.

2. Select suitable Security Policy to fit the network environment

a. FTP with SSL/TLS (Explicit): Enable this option to encrypt data transfers when the FTP clients login with SSL/TLS mode to access data that will make the data more secure.

For example, use FileZilla as the FTP clients and select “Require explicit FTP over TLS”

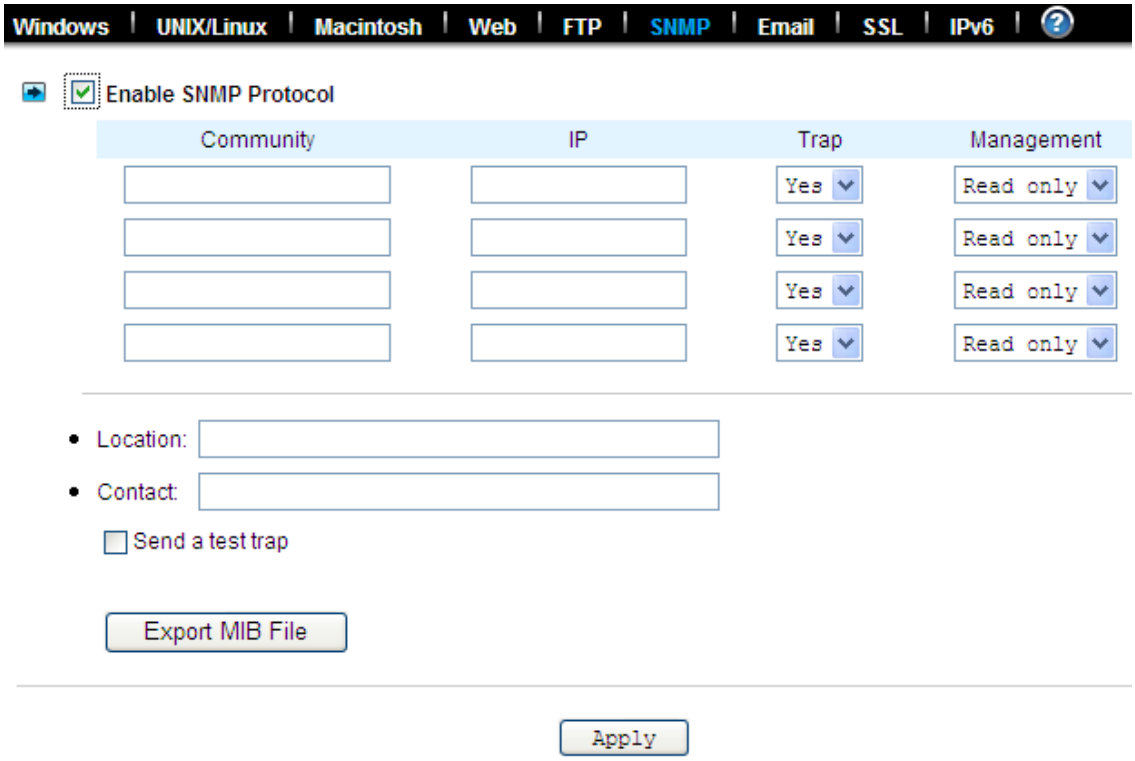
b. Allow anonymous login and map to: Enable this option to let anonymous login and map to local account for the access rights to someone who is in NAS-7410’s user database.

For example, use anonymous to login FTP server

c. Allow individual user login: You can allow Local accounts only for login NAS-7410 from FTP clients, or both Local accounts and Domain accounts have the access rights to the NAS-7410 via FTP protocol. For example, use domain account to login FTP server

4.8 SNMP settings

Simple network management protocol (SNMP) provides the ability to monitor and gives status information of the SNMP agent to the SNMP management console. NAS server behaves as an SNMP agent that answers requests from management console and sends trap information to it.



Item	Description
Community	A name serves as a simple authentication. The communication between the SNMP management console and the NAS server cannot be established if the community names are mismatched.
IP	IP address of the SNMP management console.
Trap	A trap is a voluntary message sent out from an SNMP agent (which is in this case your NAS server) when there is an event occurred.
Management	Configure the SNMP management console as **Read Only** or **Full Control**.
Location	Provides location information on the SNMP agent.
Contact	Provide name of the contact person who has the management information on the SNMP agent.

Configuring SNMP settings

1. Click the **Enable SNMP Protocol** checkbox to enable SNMP accessing.

2. Enter a **Community** name.

3. Enter the **IP** address of the management console.

4. Select "**Yes"** from the pull down menu if you want the corresponding management console to receive trap message.

5. Select "**Read Only"** from the pull down menu if you want the corresponding management console to have read only privilege.

6. Repeat Step 2 to Step 5 if more than one management console is available. NAS server supports up to 4 management consoles.

7. Enter the location information of your NAS server.

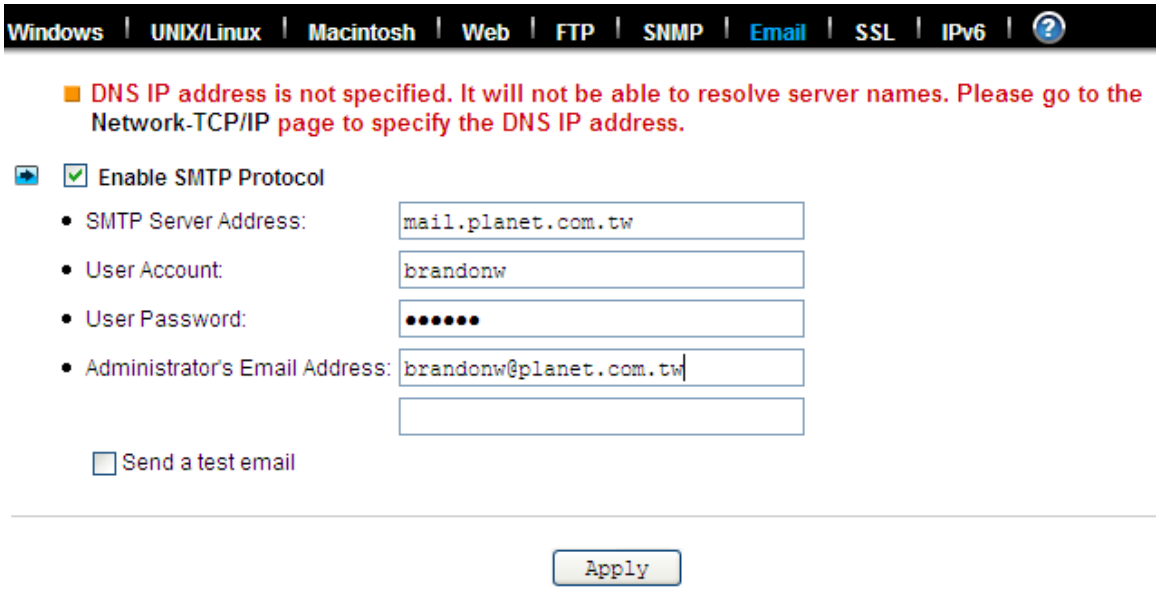
8. Enter the name of the contact person who has the management information of the NAS server.

9. You can check the checkbox beside **Send a test trap** to send sample trap information to validate your setting of the SNMP settings.

10. Click **Apply** to save the setting.

4.9 Email settings

You can configure email notification to notify you when there is an event occurred to the NAS server. Enter the information of the SMTP server on your network in this menu; you can configure what kind of event should trigger the email notification process in the **Event→Configuration→Advance** menu.



Configuring email settings

1. Click the **Enable SMTP Protocol** checkbox to enable SMTP protocol.

2. Enter the **SMTP Server Address**.

3. Enter an existing user account name of the SMTP server.

4. Enter the password of the account.

5. Enter up to two email addresses you want to send email notification to when event occurred.

6. Click the **Send a test email** checkbox if you want to send out a test email to validate your email

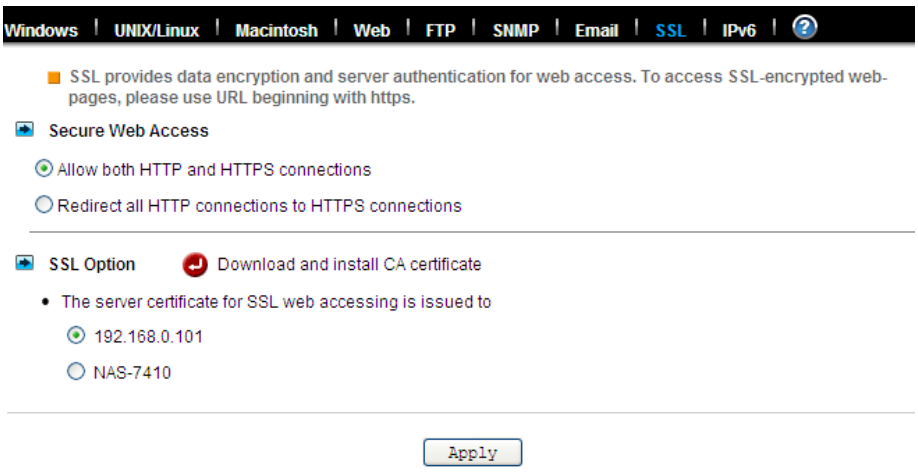
setting.

7. Click **Apply** to save the setting.

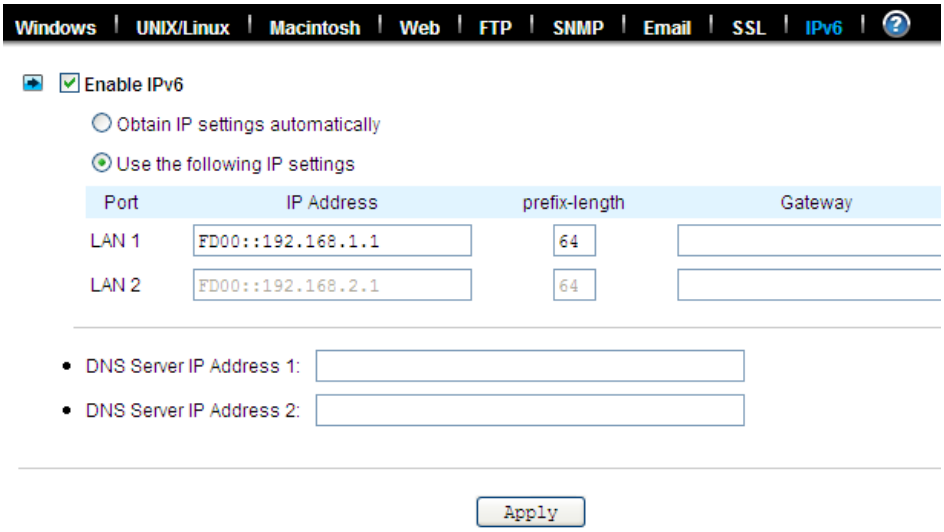
4.10 SSL settings

The NAS server enables secure web access by supporting SSL 3.0, both for the user homepage and the administration homepage. To use SSL 3.0, the NAS server will generate a server certificate for authentication and data encryption. By default, the server certificate is issued to the NAS server designated by its IP address. You can also specify to use the server's full name on the server certificate.

For clients to access server web-pages with secure connection, they have to install the CA certificate first. First to the **Network→SSL** page. Click **Download and install CA certificate** hyperlink. Choose to install the certificate when a dialog-box pops up. Once the CA certificate is installed, the client can access all NAS server s' web pages with SSL connection. Suppose that the server IP address is 192.168.1.100. To access the NAS system's web pages with SSL connection, please open https://192.168.1.100/ for the user homepage, or https://192.168.1.100/admin/ for the administration homepage. If the server certificate with the server name is chosen, please open https://[server_name] instead.



4.11 IPv6



Configuring TCP/IPv6 settings

1. Click the **IPv6** checkbox to enable IPv6 in **Web→IPv6.**
2. Select **Obtain IPv6 address automatically** or use self settings.
3. Input the LAN1 and LAN2 IPv6 address, prefix-length and gateway respectively if the self settings selected.

Input IPv6 address for DNA server 1and 2 if needed.

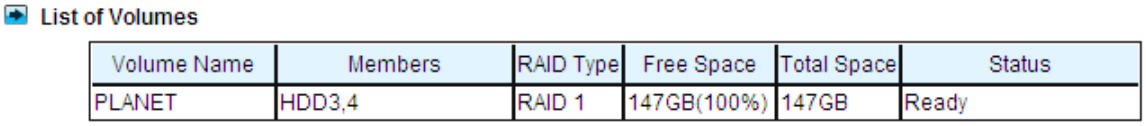
Chapter 5. Volume Configuration

This chapter describes how to create a single-disk volume or a RAID volume. It also outlines the steps of deleting a volume, expanding a RAID-5 volume and assigning hot-spare disks. After a volume is created, please refer to the next chapter for more information about sharing data and assigning permissions.

5.1 Volume Information

A volume is a logical storage unit. Each volume holds a complete file-system. A volume can exist on a single disk or a RAID group consisting of two or more disks.

Volume View


List of Volumes

Volume Name	Members	RAID Type	Free Space	Total Space	Status
PLANET	HDD3,4	RAID 1	147GB(100%)	147GB	Ready

Item	Description
Volume Name	Shows the volume name which is defined when creating a volume. Each volume name is also a hyperlink. It opens a page for showing the detailed information of that volume.
Members	Indicate the hard disks which comprise the volume.
RAID Type	Indicates whether this volume is JBOD (a single hard disk), RAID 0, RAID 1, RAID 5, RAID 6 or RAID 10. Please refer to the next section for more information about RAID.
Free Space	Indicates the volume usage by showing the free storage space in the volume and the percentage.
Status	Indicates the disk activity on the volume. The disk activity might be one of the following:

Item	Description
Ready	The volume is mounted and ready for data access.
Not Ready	The volume is not mounted successfully. It is not accessible.
Degraded	One of the volume members is defective. Data are still intact and accessible, but the volume is no longer protected by RAID. Data backup and RAID rebuilding are strongly suggested when a volume is in this state.
Critical	Two of the volume members are defective. Data are still intact and accessible, but the volume is no longer protected by RAID. Data backup and RAID rebuilding are strongly suggested when a volume is in this state

	Faulty	Two or more hard disks in the volume are not functional. It is not possible to perform any data access or recover any data.
	Faulty (RW)	Two or more volume members are defective. There might be data loss, but it is possible to recover some data. Please copy data to a safe place immediately when a volume is in this state.
	Inaccessible	Two or more volume members are missing. The volume is not mounted and data cannot be accessed.
	Apply (Ready) **Apply(Degraded)** **Apply(Critical)** **Apply (Faulty RW)** **Apply (Rebuild)** **Apply (Expand)**	The volume settings on the server and those on the hard disks are inconsistent. It means that the server has to read and apply the volume settings from the hard disks. After the volume settings are restored, it will return to the last known state, which is specified in parentheses.
	Checking	Checking the file-system.
	Mounting	Mounting the volume for data access.
	Create (xx%)	Creating a volume. The progress is shown in percentage.
	Rebuild (xx%)	Rebuilding a RAID. The progress is shown in percentage.
	Expand (xx%)	Expanding a RAID. The progress is shown in percentage.
	Scan (xx%)	Scanning hard disks for bad sectors. The progress is shown in percentage.

Hot-Spare Disks

A hot-spare disk will be used to rebuild a RAID automatically whenever a RAID volume is degraded because of a bad or missing hard disk.

Hot-spare Disks

Device	Location	Mode	Model Name	Capacity	Status
HDD1	CH1	SATA 2	Hitachi HDS72168..	73 GB	Off-line

Free disks

These hard disks are not used yet. They can be used to create volumes or assigned as hot-spare disks.

Free Disks

Device	Location	Mode	Model Name	Capacity	Status
HDD2	CH2	SATA 1	ST3160811AS	148GB	Defective

Device View

It is a list of all the storage devices connected with the NAS server, including hard disks, CD/DVD-ROM, CD/DVD writers and drives.

List of Hard Disks

Device	In Volume	Location	Model Name	Capacity	S.M.A.R.T.	Status
HDD1	(Hot Spare)	CH1	Hitachi HDS72168..	73GB	Good	Off-line
HDD2	-	CH2	ST3160811AS	148GB	Warning	Defective
HDD3	PLANET	CH3	Hitachi HDT72101..	930GB	Good	On-line
HDD4	PLANET	CH4	Hitachi HDS72161..	148GB	Warning	On-line

Item	Description
In Volume	Shows to which volume the hard disk belongs.
Location	Indicates the SATA channel position of the hard disk and USB position.
Model Name	Shows the model or the manufacturer of the hard disk.
Capacity	Shows the unformatted capacity of the hard disk.
Status	Indicates the disk status or disk activity, being one of the following.

Item	Description
On-line	The hard disk is a member of a mounted volume which is ready for data access.
No init	The hard disk is not initialized yet. A no-init disk must be a free disk, which can be used to create a volume or be assigned as a hot-spare disk.
Defective	The hard disk contains bad sectors.
Off-line	The hard disk is not mounted and not accessible.

Backup/Archiving devices

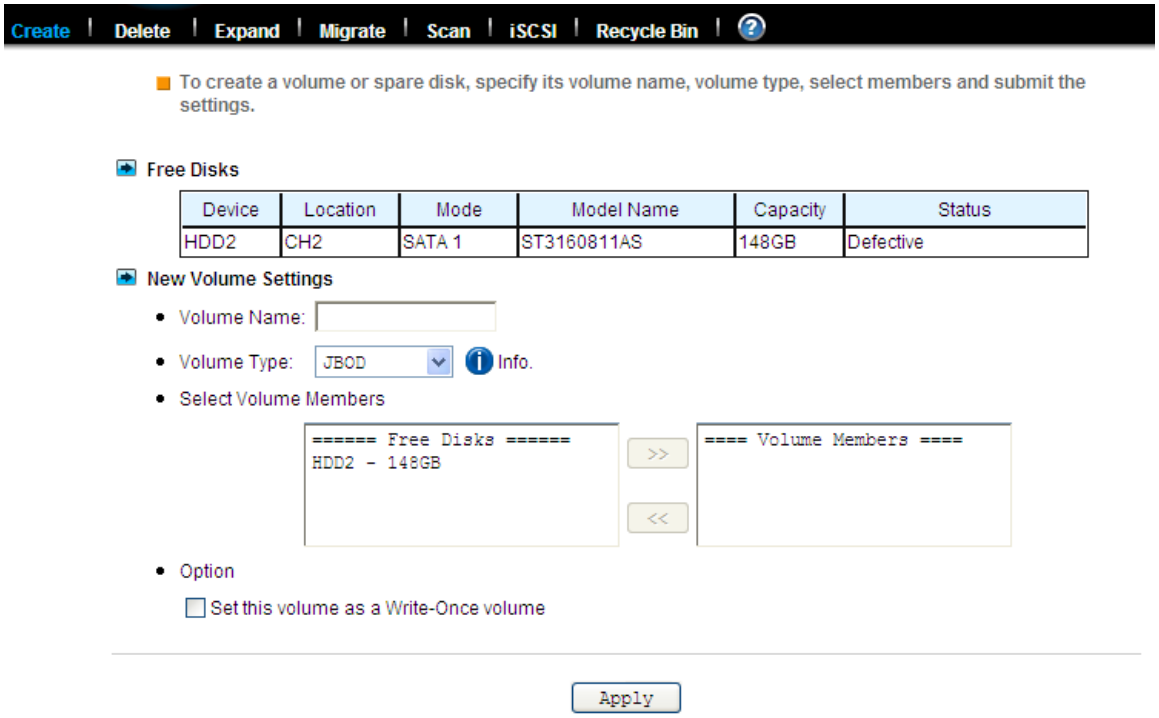
Backup/Archiving Devices

No Device

These are either CD/DVD-ROM drives, CD/DVD writers or drives. **Type** indicates what kind of device it is. **Mode** indicates the data transfer mode of the storage device interface. Device type could be CD-ROM, CD-R, CD-RW, DVD-ROM, DVD+R, DVD+RW or DVD-ROM+CD-RW.

5.2 Creating a volume

The first thing for the administrator to do with the storage is to create a volume on the hard disks. Then he or she can share the storage for user access and set security control. To create a volume, first go to the **Volume→Create** page. Specify the volume name in the **Volume Name** field and choose the volume type (JBOD, RAID 0, RAID 1, RAID 5, RAID 6 or RAID 10). Then choose the hard disks to be included in the volume. Last, click **Apply** to submit changes. The progress of volume creation is shown on the **Volume→Information** page. Below are the volume types.



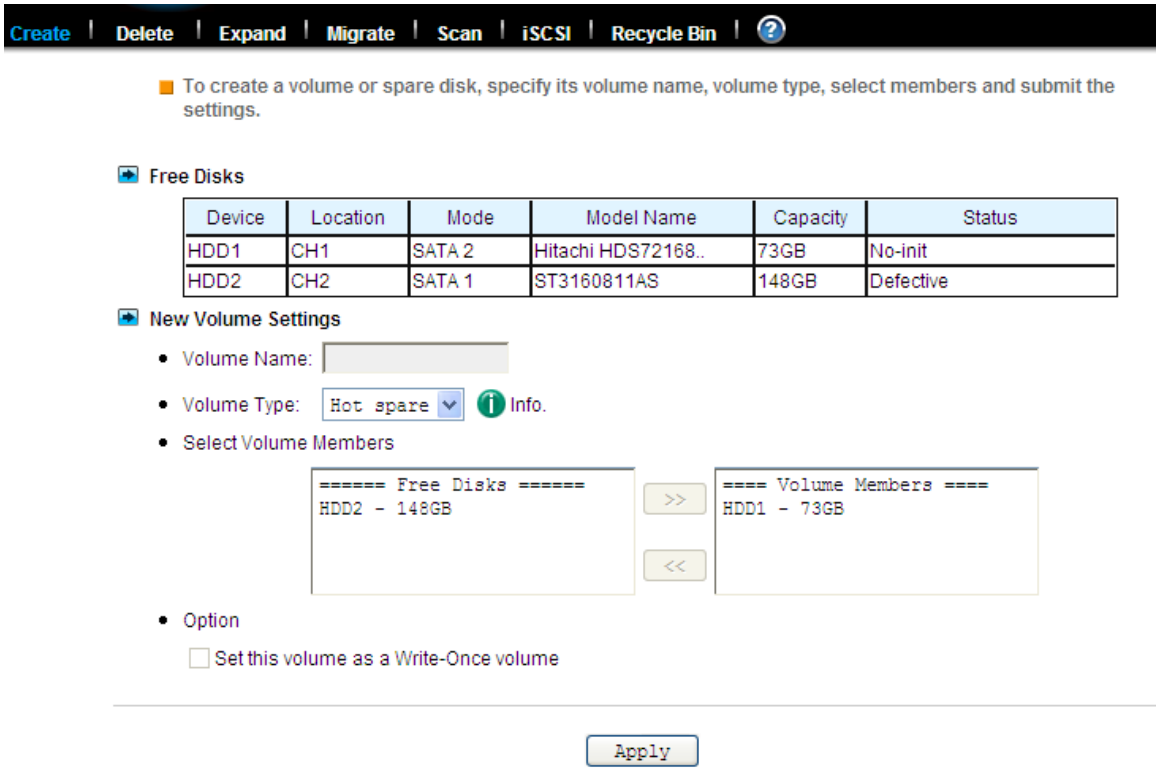
Item	Description
JBOD	Just a Bunch Of Disks. A JBOD-type volume contains only one hard disk as its member.
RAID 0	RAID level 0 is disk striping only, which distribute data evenly over multiple disks for better performance. It does not provide safeguards against failure. RAID level 0 uses two or more hard disks.
RAID 1	RAID level 1 uses disk mirroring, which provides 100% duplication of data. It offers high reliability, but doubles storage cost. RAID level 1 uses two hard disks.
RAID 5	RAID level 5 distributes data and parity bits over multiple disks for both performance and fault tolerance. A RAID volume can still work when a hard disk fails. RAID level 5 uses three or more hard disks. Building a RAID-5 volume may take hours depending on capacity.
RAID 6	RAID 6 (striped disks with dual parity) combines four or more disks in a way that protects data against loss of any two disks.
RAID 10	RAID 1+0 (or 10) is a mirrored data set (RAID 1) which is then striped (RAID 0), hence the “1+0” name. A RAID 1+0 array requires a minimum of four drives – two mirrored drives to hold half of the striped data, plus another two mirrored for the other half of the data. In Linux, MD RAID 10 is a non-nested RAID type like RAID 1 that only requires a minimum of two drives and may give read performance on the level of RAID 0.
Write-Once Volume	When setting a Write-Once volume, you are not allowed to erase or change what you have written on this volume. This setting CANNOT be reverted in any situation, please think it twice before you enable it.

Assigning Hot-spare disks

The hot-spare disks are global, which means they are not bound to any specific RAID volumes. Whenever a RAID volume goes degraded because of a bad hard disk, a hot-spare disk will be taken immediately to recover that RAID volume.

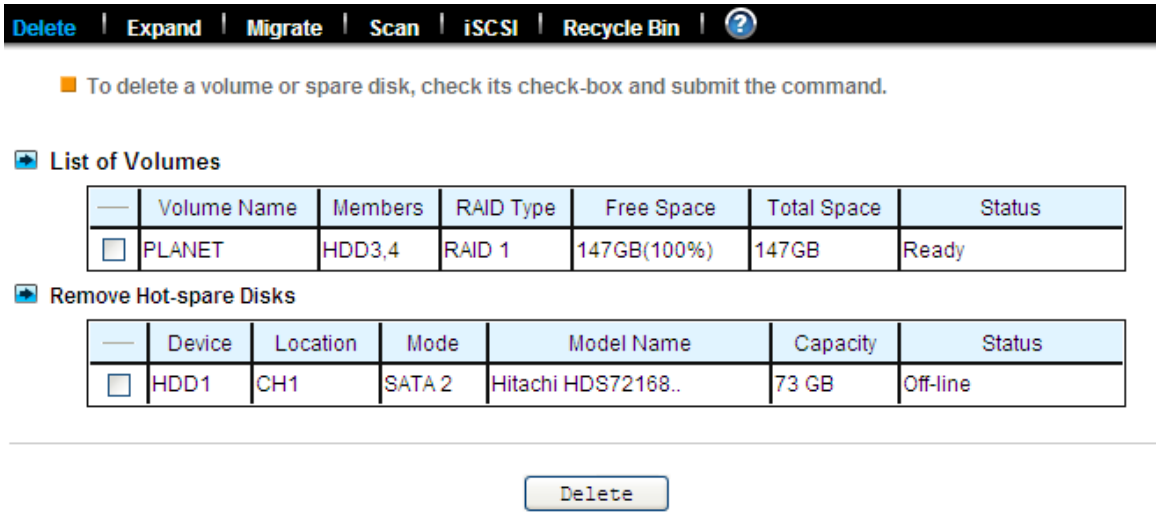
To assign hot-spare disks, please go to the **Volume→Create** page. Specify the volume type as Hot-spare. Assign the free disks as hot-spares by using the dual window panes. Click **Apply** to submit changes.

To remove disks from the hot-spare list, please go to the **Volume→Delete** page. Select the hot-spares to be deleted in the **Remove Hot-Spare Disks** table and click **Delete**.



5.3 Deleting a volume

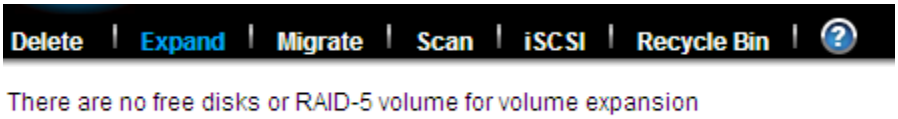
To delete a volume, go to the **Volume→Delete** page. Select the volume to be deleted and click the **Delete** button. Please be very careful because all data in the volume will be destroyed and the RAID configuration will be erased also. All hard disk members in this volume will become free disks after the deletion.



5.4 Expanding a RAID-5 volume

RAID-5 volume expansion makes it possible to enlarge volume capacity without rebooting the NAS server. Volume capacity grows on the fly. Moreover, you do not have to change any share permissions, security controls and quota settings after volume expansion. Storage management becomes much easier.

To expand a RAID-5 volume, please go to the **Volume→Expand** page. Select a RAID-5 volume to be expanded. Then choose the free disks as new members. Click **Apply** to submit changes. The progress of RAID expansion is shown on the **Volume→Information** page.

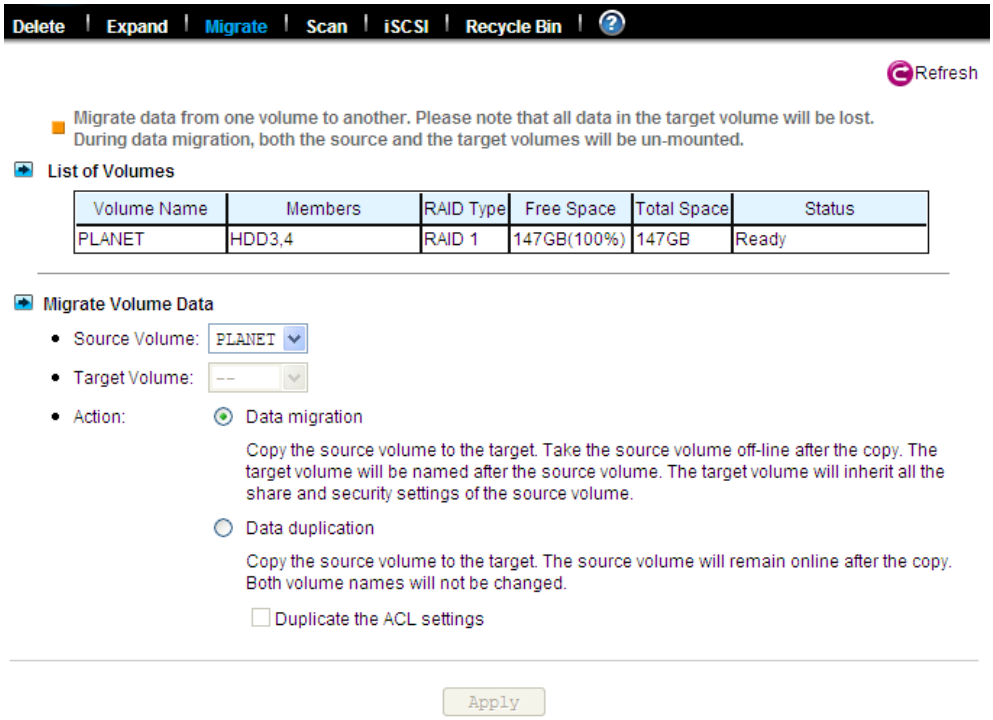


5.5 Migrating Data Volumes

Migrating a data volume is to duplicate a volume block by block. It helps administrators migrate or duplicate data between volumes of different RAID types or capacity. During data migration, both the source volume and the target volume will be un-mounted, not available for client access.

To migrate data, select a source volume, and the target volume to migrate to. Choose **Data migration** and click **Apply**. The target volume will inherit all the security and quota settings of the source volume. No differences will be observed by clients before and after the migration.

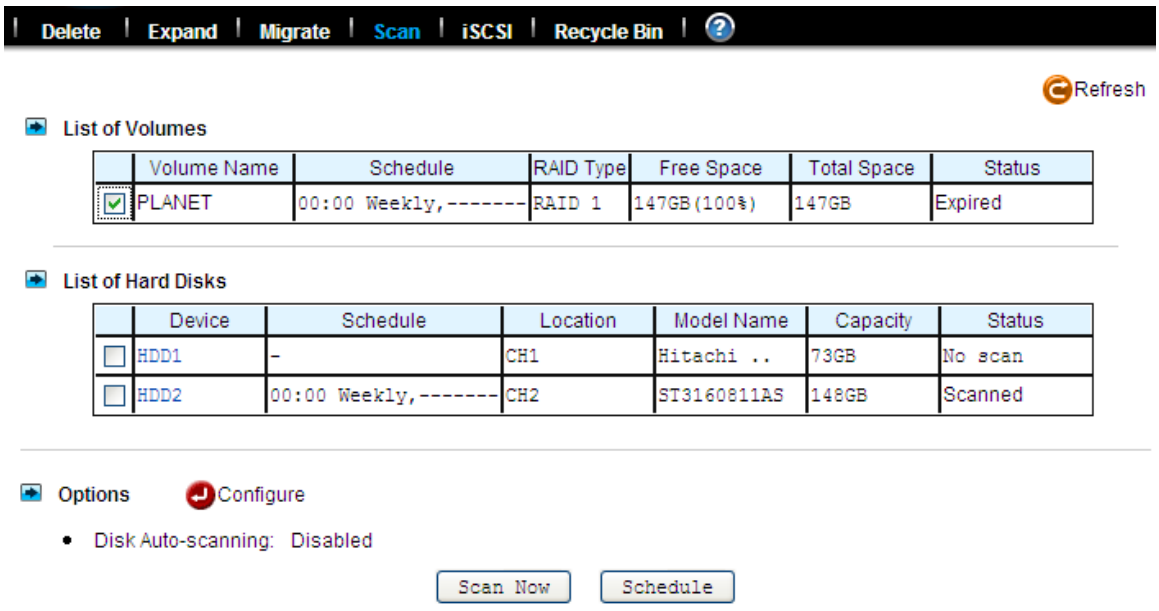
To duplicate a volume, select a source volume and the target volume. Choose **Data duplication** and click **Apply**. The target volume will stay on-line after the data duplication.



5.6 Volume/Disk scan

Volume/Disk scan is especially useful for disk diagnostics and repairs lost or cross linked clusters in Volume/Disk. All readable data will be placed in new clusters and defective cluster will mark as bad in the file system. All the newly added devices will be scanned before usage to ensure the data integrity in the NAS Server.

Select the volumes or disks you want to scan, click **Scan Now** button to start scanning. Or, click **Schedule** to set the time for NAS Server to perform scanning at the scheduled time.

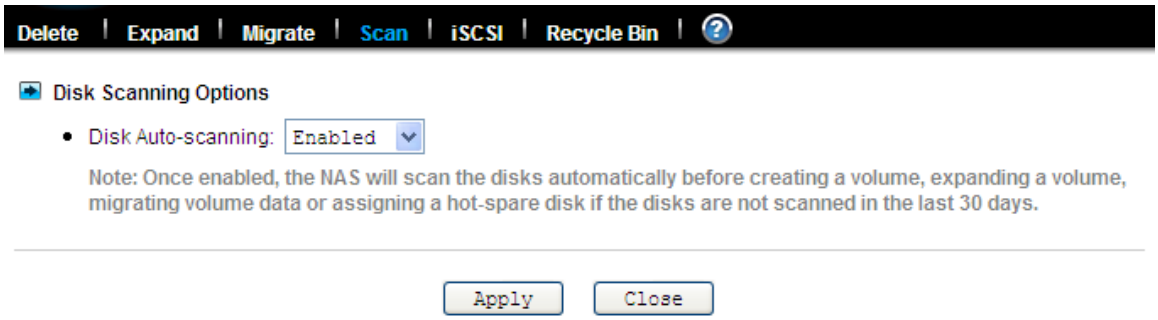


Disk Auto-scanning

To make sure that the hard disks contain no bad sectors before putting into use, it is suggested to

perform disk-scanning before taking such actions as creating a volume, expanding a volume, migrating data or assigning a hot-spare disks. If disk auto-scanning is enabled, the NAS server can scan disks automatically when you perform these actions. If the hard disks have ever been scanned in the last 30 days, the auto-scanning will be skipped so that the auto-scanning will not be activated too often.

To enable the feature, please click the **Configure** hyperlink on the **Volume→Scan** page. Set the **Disk Auto-scanning** item to **Enabled**.



5.7 iSCSI (IP SAN)

iSCSI, (Internet Small Computer System Interface), an Internet Protocol (IP)-based storage networking standard for linking data storage facilities. By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances. iSCSI can be used to transmit data over local area networks (LANs), wide area networks (WANs), or the Internet and can enable location-independent data storage and retrieval.

iSCSI Target

Follow the steps below to configure the iSCSI target service on the NAS server.

1. Click “iSCSI” tab and Click “Add” to create an iSCSI target on the NAS.

2. Enter the iSCSI target information for configuration

Item	Description
Target User Name	The name for the target.
iSCSI Target Lun	Select to create an iSCSI target with a mapped LUN and enter the size of LUN.
Comment	The comment for the target.
iSCSI Authentication	None or CHAP.
Target User Name	The name for target authentication.
Password	The password for target authentication.
Mutual CHAP	Two-way authentication mode.
Initiator Name	The name for initiator authentication.
Password	The password for initiator authentication.
CRC/Checksum	Data or Header Digest.

3. Apply the settings. Now, an iSCSI LUN is a logical volume mapped to the iSCSI target. The target and LUN are shown on the list under the “iSCSI” tab.

Note

The NAS supports 8 iSCSI devices at the maximum.

iSCSI target configuration

- iSCSI qualified name

Target user name: ENM

- iSCSI target LUN:

	Target Volume Name	RAID Type	Free Space	LUN size
◉	PLANET	RAID 1	138GB	100 MB

☑ Allocate the disk space now

Comment:

- iSCSI authentication

◉ None

○ CHAP

Target user name: (A~Z, a~z, 0~9)

Password: (A~Z, a~z, 0~9)

Re-enter password:

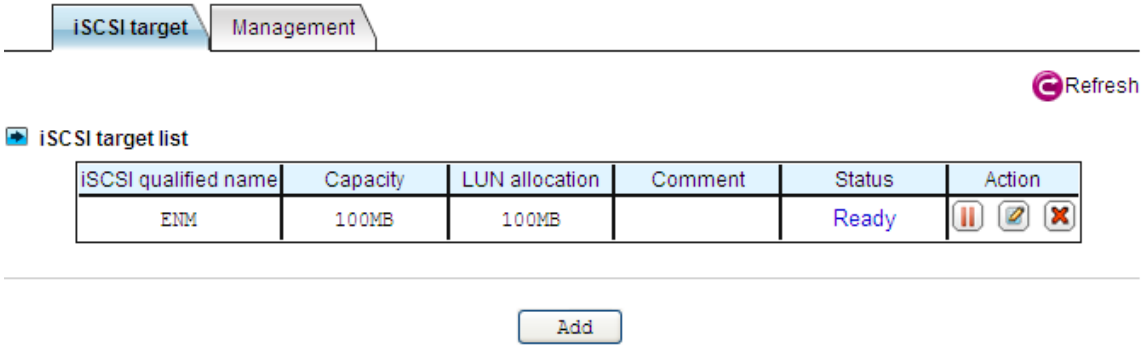
☐ Mutual CHAP:

Initiator name: (A~Z, a~z, 0~9)

Password: (A~Z, a~z, 0~9)

Re-enter password:

4. The LUNs created can be mapped to and unmapped from the iSCSI target anytime. You can deactivate or activate by clicking ⏸ or ▶ icon, respectively. You can delete a target by clicking ✖ icon.



Initiator Management: Add up to 32 Initiators to the Initiator Allow List. By default, all Initiators have no access permission.

Add a new initiator:

1. Enter initiator name or IP.

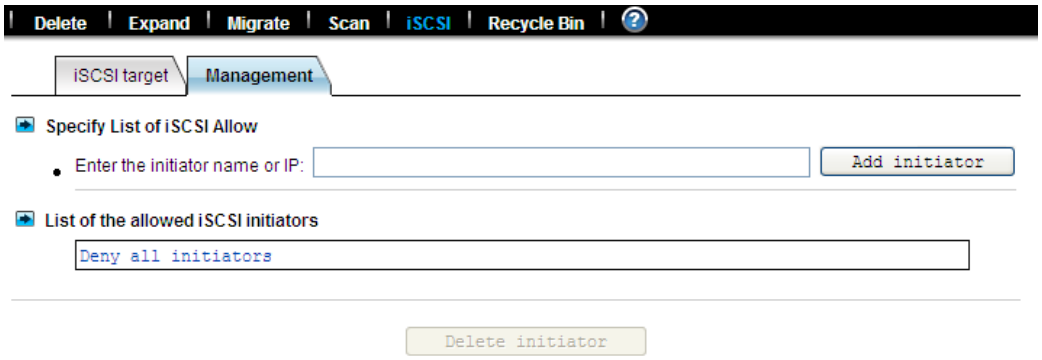
2. Click “**Add initiator**”.

3. New initiator will be displayed on the below allowed list.

Remove an initiator:

1. Click the checkbox in front of the name/IP of an initiator.

2. Click “**Delete initiator**” to remove the initiator from allowed list.



5.8 Recycle bin

This feature will take effect after the system re-start.

Recycle Bin function

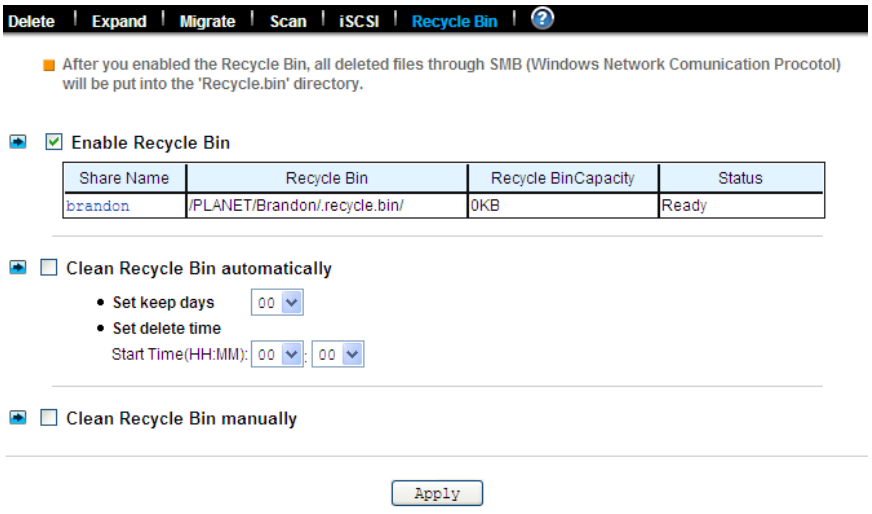
When you enable this function, NAS server will automatically create a dedicated folder named “Recycle.bin” in the share folder. When accessing the NAS server via SMB (Windows network protocol), all deleted files will be moved to this dedicated folder.

Clean Recycle Bin automatically

This function can prevent the Recycle Bin from taking too much space on your hard disk, leading to the occurrence of deficiencies in the volume space, and can save managers from time to time required to clean up the Recycle Bin. Delete time setting can be used to make adjustments to avoid affecting the overall performance of the NAS server; it is recommended that the delete time can be set in the off-peak time.

Clean Recycle Bin manually

Manually clear the data in the Recycle Bin of all Volumes. The data will be removed permanently.



Chapter 6. Security control

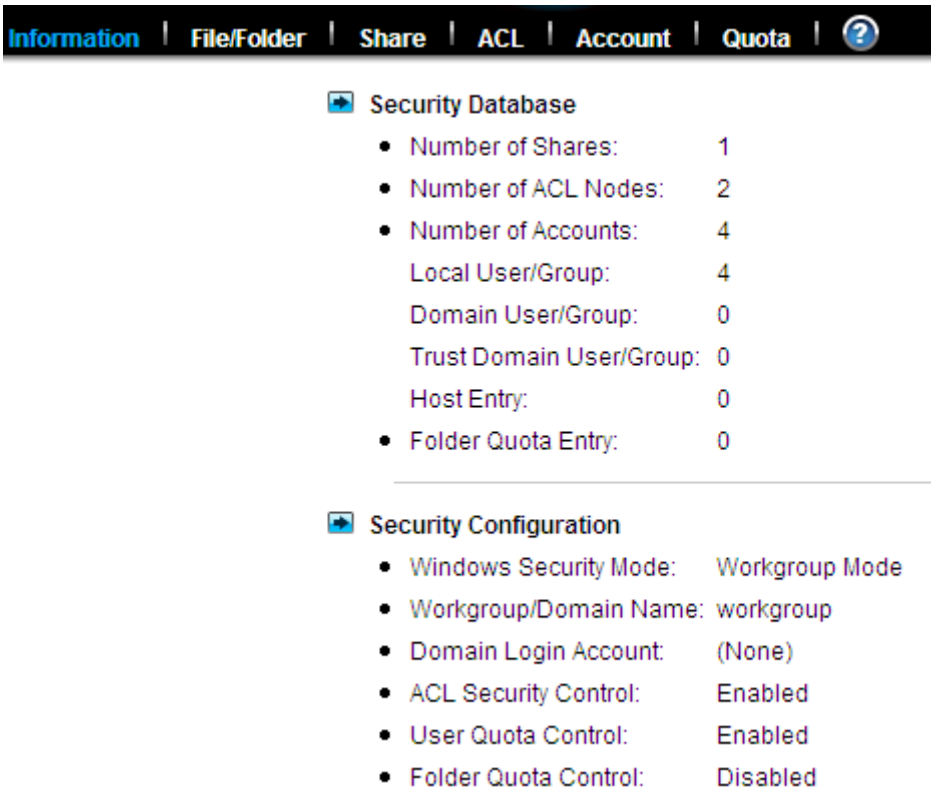
This chapter covers how to set up the security control of the files, folders and shares stored in NAS server. Managing Access Control List (ACL) file level security, file ownership and user quota are also covered in this chapter. You can configure the following types of security control on the NAS server:

1. Create, edit and delete user accounts in the local user database.
2. Create shares.
3. Configure Files, Folders and shares permission.
4. Configure local account, domain account and UNIX/Linux Hosts permission.
5. Maintain the ACL table.
6. Configure the local user and domain user quota limit.

6.1 Security information

The Security Information screen is the statistic of the current security setting of the NAS server. It provides administrator with a summary of the security database and the status of the operation mode.

The Information page is divided into two sections. The Security Database section displays the number of shares, number of ACL nodes and number of users/groups.



Item	Description

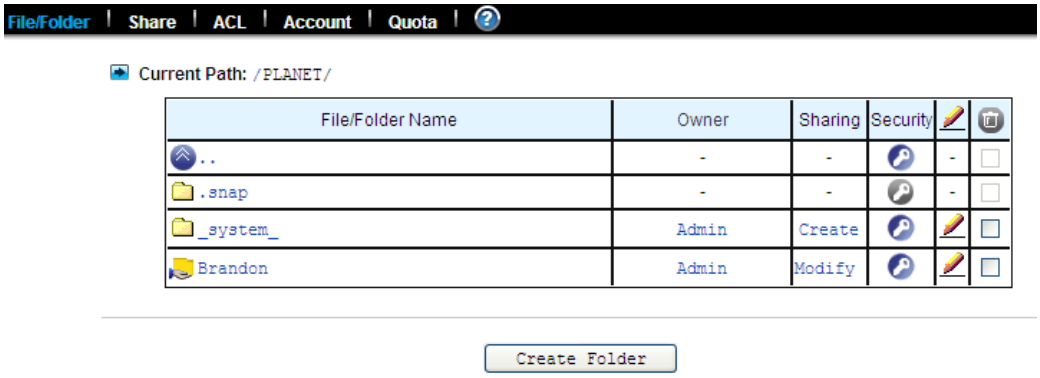
Number of Shares	Total number of shares created in NAS server.
Number of ACL Nodes	Total number of ACL nodes created. ACL tells NAS server which access right each user has to a folder or an individual file.
Number of Accounts	The total account number of the Local Users/Groups, Domain Users/Groups, Trust Domain Users/Groups and Unix/Linux Host Entries.
Local User/Group	Total number of local users/groups. A local user or group is an account that can be granted permissions and rights from NAS server.
Domain User/Group	Total number of domain users/groups. Domain users or groups are managed by the network administrator.
Trust Domain User/Group	Total number of trust domain users/groups.
Host Entry	Total number of Unix/Linux hosts entered.
Folder Quota	Total number of Unix/Linux hosts entered.

The “Security Configuration” section shows the current security configuration settings of the server.

Item	Description
Windows Security Mode	Display the status of the Windows Network operating mode. Status: “Domain Mode or Workgroup Mode”.
Workgroup/Domain Name	Display either the workgroup name or domain name.
Domain Login Account	Display the username for retrieving the domain user list in the domain.
ACL Security Control	Display the status of the ACL Security Control. Status: “Enabled” or “Disabled”.
User Quota Control	Display the status of the User Quota Control. Status: “Enabled” or “Disabled”.
Folder Quota Control	Display the status of the Folder Quota Control. Status: “Enabled” or “Disabled”.

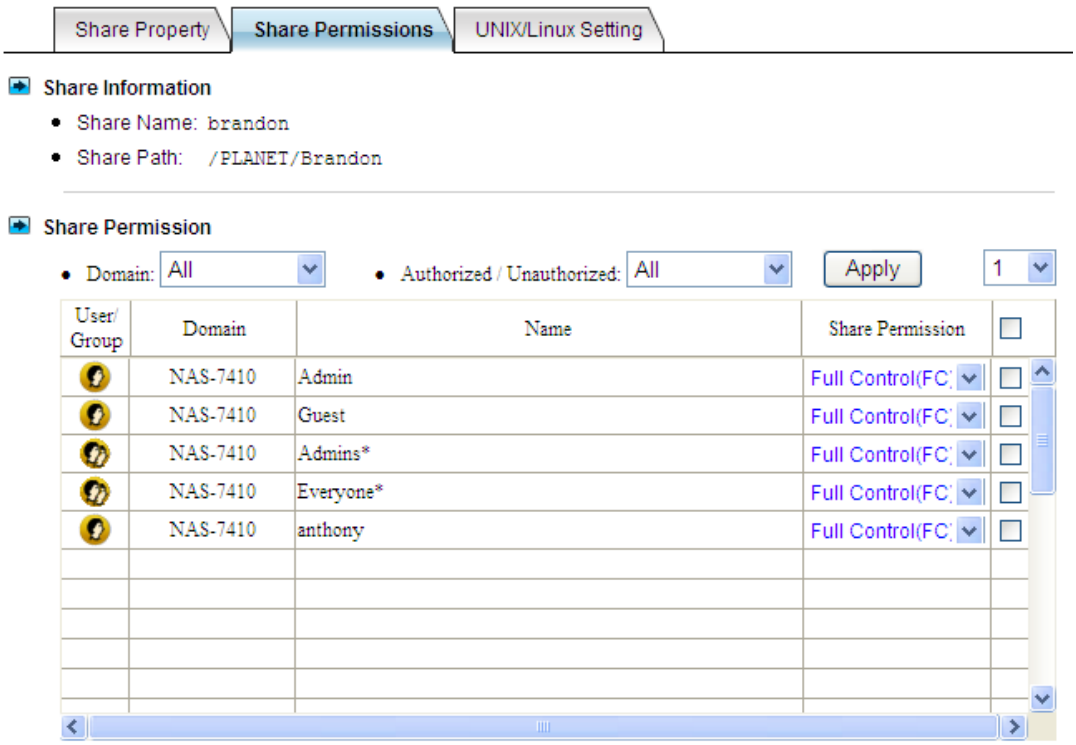
6.2 Creating share and assigning share permissions

You can share a specific folder in any volume created in the NAS server with others on the network. When you create a share, you can assign the permission to the share that other users will be allowed or denied when they access the share over the network.



To create a new share:

1. Go to Security→File/Folder menu.
2. Locate the volume you want to share on the volume lists.
3. Click the Create hyperlink to share the corresponding volume. Then go to Step 9.
4. If you want to share an existing folder under a volume, click the volume name hyperlink. Click the folder hyperlink until you reach the desired directory. Then, go to Step 8.
5. If you want to share a new folder under a volume, click the folder hyperlink until you reach the desired directory path.
6. Click the Create Folder button to create a new folder.
7. Enter a new folder name and click Apply.
8. Click the Create hyperlink to share the corresponding folder.
9. Enter a unique shared name in the Share Name field. The shared name is what user will see when they connect to this share. The actual name of the folder does not change.
10. To add a comment about the share, type the text in Comment.
11. To limit the number of users who can connect to the share, on the User limit, click Allow and enter a number of users.
12. Select the protocols you want to share.
13. Click Apply to save the setting.

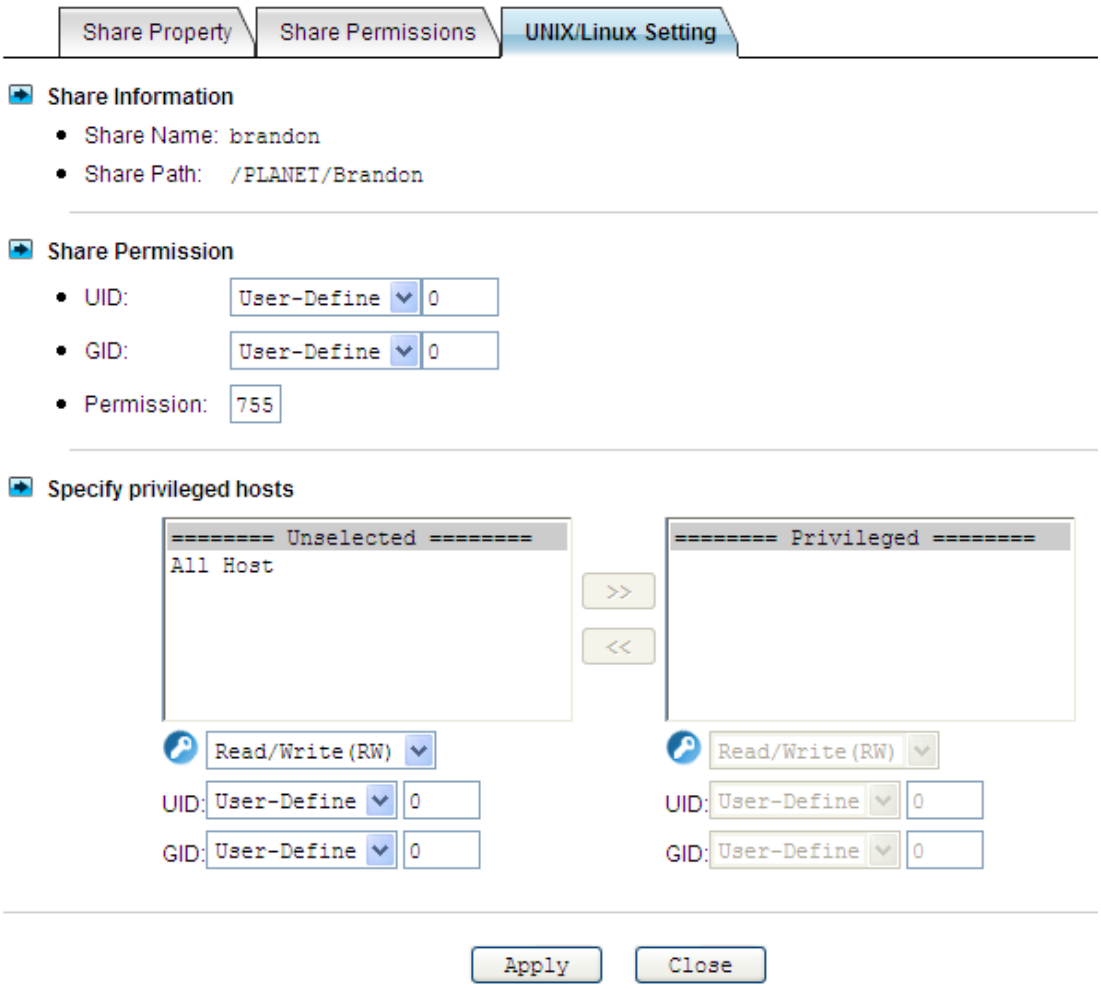


To assign share permission of a share for local account and domain account:
1. Go to **Security→Share** menu.
2. Locate the share and click permission icon to assign or modify share permission to this share.
3. Highlight the users or groups from user pool and click user's checkbox.
4. Select the appropriate permission from the pull down menu at the bottom.
6. You can modify the permission of the users or groups in the privileged list by first highlight the users or groups and then select the appropriate permission from the pull down menu at the bottom of the share permission item.
7. Click **Apply** to save the setting.

Note

You can also modify share permission in **Security→File/Folder** menu by clicking the **Modify** hyperlink of the corresponding shared folder.

You can assign the following share permissions to a user on NAS server:
No Access (NA) – Account has been denied access to the share.
Read Only (RO) – Account is allowed to read the share.
Change (CH) – Account is allowed to read and write to the share.
Full Control (FC) – Account is allowed to read both read and write and change permission to the file or folder.



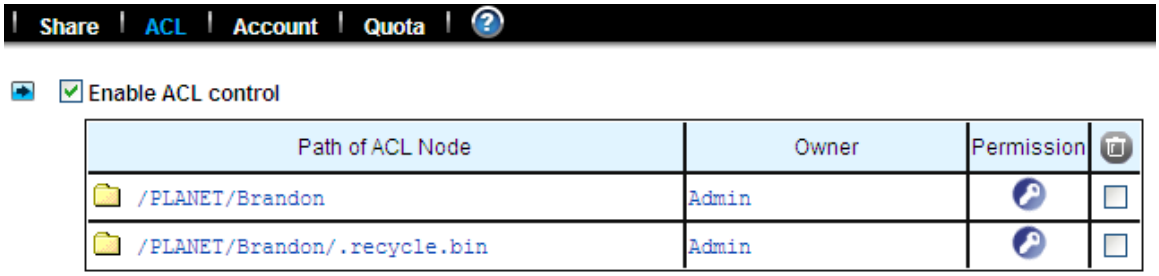
To assign share permission of a share for UNIX/Linux host:

1. Go to **Security→Share** menu.
2. Locate the share and click to assign share permission to this share.
3. Click the **UNIX/Linux Setting** tab.
4. Assign the UID, GID and Permission of this share. It will overwrite the ownership and permission of the mount point once the share is mounted by the NFS client. If the NIS support is enabled, the UID and GID pull-down menus will list all NIS users for you to choose.
5. You can allow all hosts to access the share with read/write or read only permission. Then go to Step 9.
6. Or, you can specify privileged hosts by highlighting the host IP from the left hand windows.
7. Select the appropriate permission from the pull down menu at the bottom of the left hand windows.
8. Assign which UID/GID the root account of the UNIX host should be converted into when accessing the share. This is the 'root squash' function.
9. Click the **>>** button to join the privileged list.
10. You can modify the permission of the hosts in the privileged list by first highlighting the privileged host and then select the appropriate permission from the pull down menu at the bottom of the right hand windows.
11. Click **Apply** to save the setting.
12. If you want to remove shares, check the corresponding checkbox located at the end of the row and click .

You can assign the following share permission to UNIX/Linux Hosts on NAS system:

Read Only (RO) –The host is allowed to read the share.
Read Write (RW) –The host is allowed to read and write to the share.

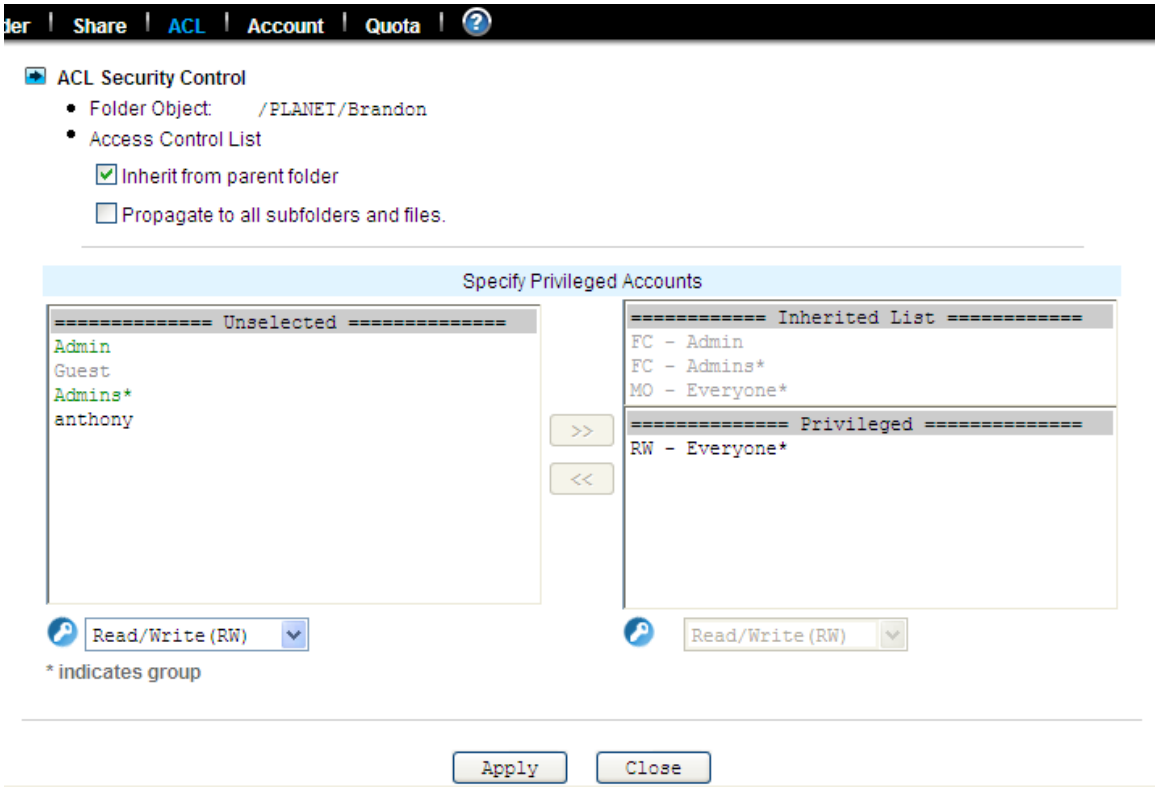
6.3 Configuring file and folder security and ACL



Access Control Lists (**ACL**) are associated with each file and folder, as well as the list of users and groups permitted to use that file or folder. When a user is granted access to the file or folder, an ACL node is created and added to the ACL for the file or folder. If you assign permissions to a local user, a Security ID (SID) created by NAS system will be referred by the ACL for the file and folder security. If the local user is then deleted, and the same name is created as the previous one, the new user does not have permissions to the file or folder, because the SID will not be the same. The administrator will have to re-configure all the group memberships and access rights to the files and folders.

Since the Security ID (**SID**) for domain user is issued and maintain by the domain controller on the network. Administrator does not need to re-configure all the group memberships and access rights to the files and folders if the domain user is deleted from the local user database and the same name is created as the previous one.

Note	If the administrator changes the permission on a file or folder that a user is currently accessing, the permission setting does not take immediate effect because of the local handle being used by the user. The new rights will only take effect when the user reconnects to the file or folder.



There are two built-in user accounts: **Admin** and **Guest**. And two built-in group accounts: **Admins** and **Everyone**.

Every user of NAS server including local and Domain user is the member of the **Everyone** group. By default, when a volume is created, **Admins** and **Admin and Everyone** will be granted Full Control permission. After you set permissions on a volume, all the new files and folders created under the volume inherit these permissions. If you do not want them to inherit permissions, uncheck the **Inherit from parent folder** when you set up the permissions for the files and folder.

Configuring file and folder security:

1. By default, **ACL control** is enabled.

2. Go to **Security→File/Folder** menu.

3. Locate the file or folder you want to configure the permission.

4. Click the icon. If the icon is disabled, go to **Security→ACL** menu to enable the **ACL Control**.

5. Clear the **Inherit from parent folder** check box.

6. Select the users or groups from the left hand windows and click the **>>** button to join the privileged user/group list.

7. If you want all the subfolders and files inherit the new permission you have just set, check the **Propagate to all subfolders and files** check box.

8. Click **Apply** to save the setting.

You can assign the following File/Folder permission to a user on NAS server:

No Access (NA) – Account has been denied access to the file or folder.

Read Only (RO) – Account is allowed to read the file or folder.

Write Only (WO) – Account is allowed to write to the file or folder.

Read Write (RW) – Account is allowed to read and write to the file or folder, but not to delete it.

Modify (MO) – Account is allowed to read, write and delete the file or folder

Full Control (FC) – Account is allowed to read both read and write and change permission to the file or folder. **Set file/folder permission in Windows Network** NAS server provides a simple, efficient way to set up and maintain file/folder security in Windows Network. To change permissions, you must be granted permission to do so by the administrator. Below is the permission mapping table of NAS server in Windows Network:

File/Folder Permission in NAS system	Folder Permission in Windows Network	File Permission in Windows Network
No Access (NA)	☐ Full Control ☐ Modify ☐ Read & Execute ☐ List Folder Contents ☐ Read ☐ Write	☐ Full Control ☐ Modify ☐ Read & Execute ☐ Read ☐ Write
Read Only (RO)	☐ Full Control ☐ Modify ☑ Read & Execute ☑ List Folder Contents ☑ Read ☐ Write	☐ Full Control ☐ Modify ☑ Read & Execute ☑ Read ☐ Write
Write Only (WO)	☐ Full Control ☐ Modify ☐ Read & Execute ☐ List Folder Contents ☐ Read ☑ Write	☐ Full Control ☐ Modify ☐ Read & Execute ☐ Read ☑ Write
Read/Write (RW)	☐Full Control ☐ Modify ☑ Read & Execute ☑ List Folder Contents ☑ Read ☑ Write	☐ Full Control ☐ Modify ☑ Read & Execute ☑ Read ☑ Write
Modify (MO)	☐ Full Control ☑ Modify ☑ Read & Execute ☑ List Folder Contents ☑ Read ☑ Write	☐ Full Control ☑ Modify ☑ Read & Execute ☑ Read ☑ Write
Full Control (FC)	☑ Full Control ☑ Modify ☑ Read & Execute ☑ List Folder Contents ☑ Read ☑ Write	☑ Full Control ☑ Modify ☑ Read & Execute ☑ Read ☑ Write

To set, view, change or remove file/folder permission in Windows Network:

1. Locate the file or folder you want to set permission

2. Right-click the file or folder, click **Properties** → **Security**

3. Change permission from an existing groups or users, click the **Allow** or **Deny** checkbox

4. Or, remove the groups or users by clicking the **Remove** button.

To change owner of a file or folder

1. Go to **Security→File/Folder** menu.

2. If you want to change the owner's name of the corresponding file and folder, click the owner's name hyperlink. Select a new owner from the user list.

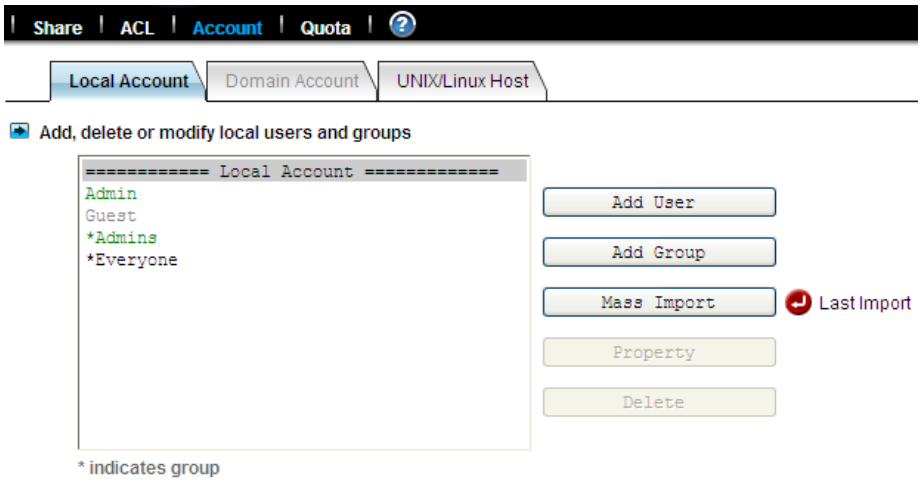
3. Check the checkbox beside **Apply to all sub folders and files** if you want to propagate the

ownership to all sub folders and files.

4. Click **Apply** to save the setting.

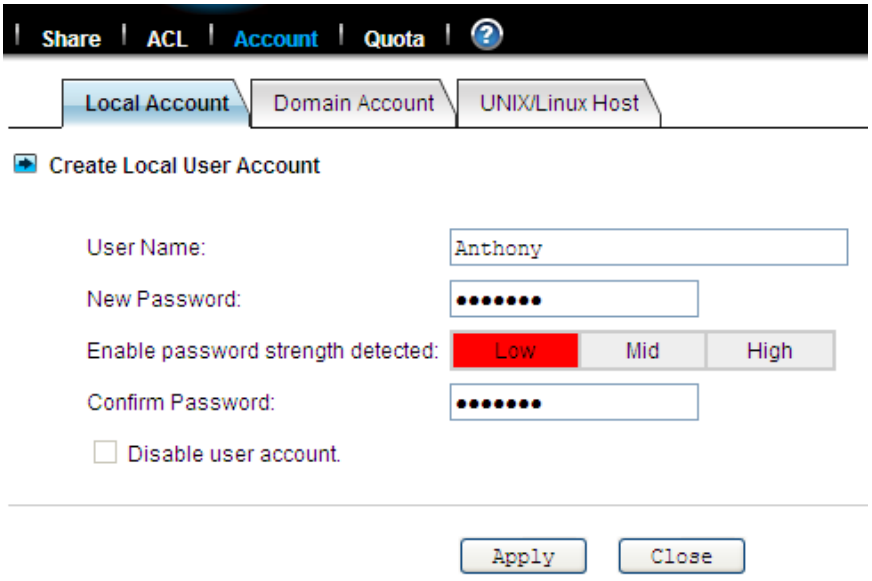
6.4 Creating the local user and local group accounts

A local user or group is an account that can be granted permissions and rights from your NAS server. You can add local user to a local group. Groups are indicated by a * sign at the suffix of the name. You can also grant administrator privilege to a local group. Groups with administrator privilege are indicated by a # sign at the suffix of the name.



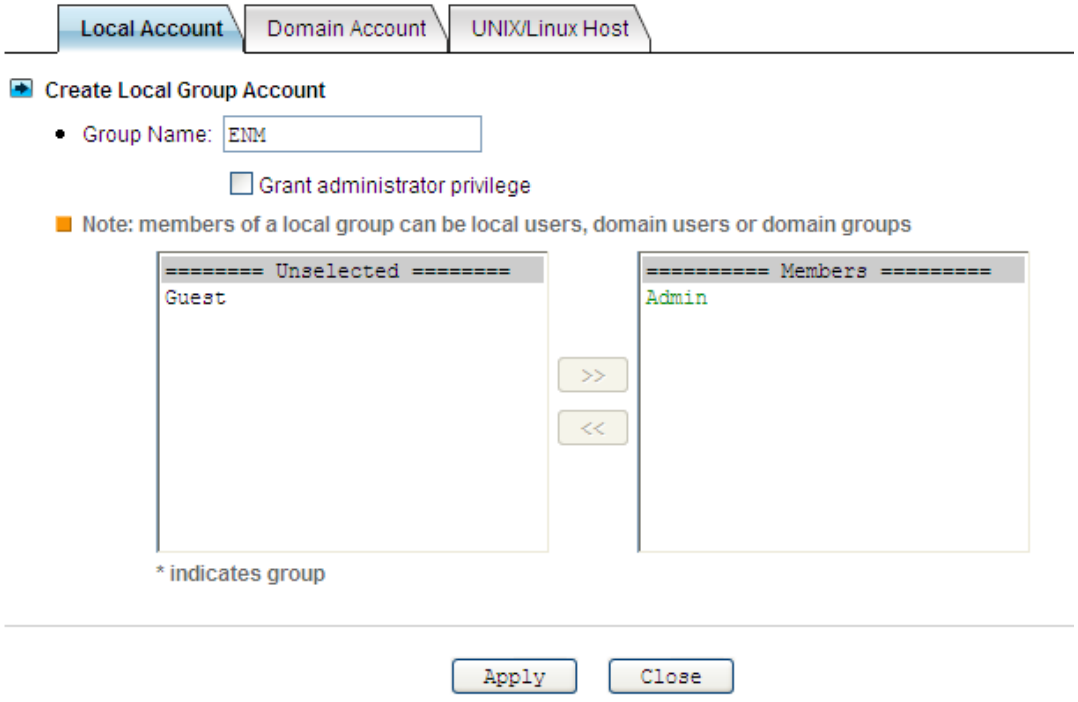
To create a local user:

1. Go to **Security→Account→Local Account** menu.
2. Click the **Add User** button.
3. Type in the user name and enter the password.
4. Re-type the password to confirm.
5. Click **Apply** to save the setting.



To create a local group:

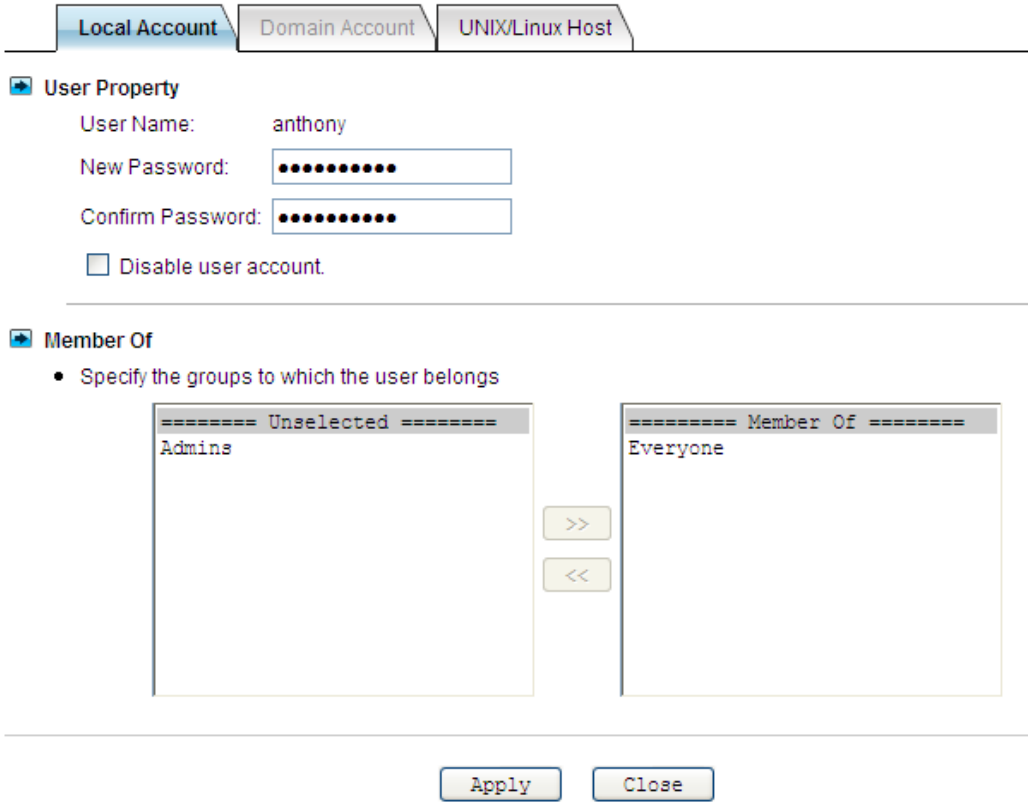
1. Go to **Security→Account→Local Account** menu.
2. Click the **Add Group** button.
3. Type in the group name.
4. If you want to grant the administrator privilege to this group, click the **Grand administrator privilege** check box.
5. Select the users from the left hand windows and click the **>>** button to join the group.
6. Click **Apply** to save the setting.



Note	If you want to grant administrator privilege to a user, simply add the user to the built-in group Admins which has administrator privilege. User with administrator privilege can access the administration home page.

To view and change local user property:

1. Go to **Security→Account→Local Account** menu.
2. Select a user.
3. Click the **Property** button.
4. If you want to change the password, enter a new password and confirm.
5. If you want to disable this user account, click the **Disable user account** checkbox.
6. Select a group from the left hand window and click the **>>** button to add the user as a member of this group in the **Member of** section.
7. Click **Apply** to save the setting, and view and change local group property.



The NAS server provides a mechanism for administrators to create multiple accounts at one time. It imports accounts from a text file and create local accounts accordingly. The text file defines some parameters related to the accounts, like passwords, user quotas, groups, etc. Also it can be used to create user folders in a batch. Below is an example of the text file.

username, password, group, user quota, user folder, folder quota, create default ACL

user001, aa1aa1, group A, 1GB, /vol-1/users/user001, 1GB, yes

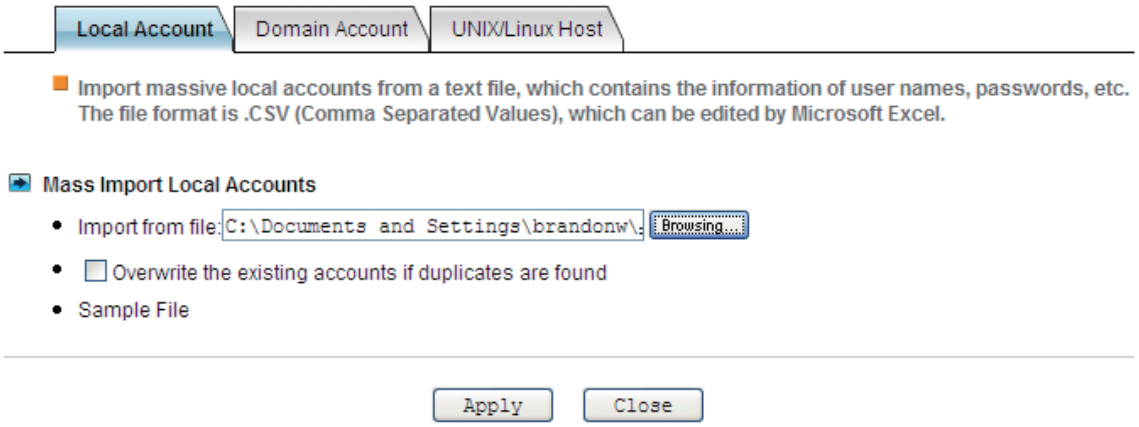
user002, bb2bb2, group A, 1GB, /vol-1/users/user002, 1GB, yes

user101, 101101, group B, 10GB, /vol-1/users/user101, 10GB, no

It is suggested that administrators use Microsoft Excel to maintain the account file, and then save it as .CSV files, in which fields are delimited by commas. Thus, the advance features of Microsoft Excel, like filling in a series of numbers or items, easy copy and paste, can be used.

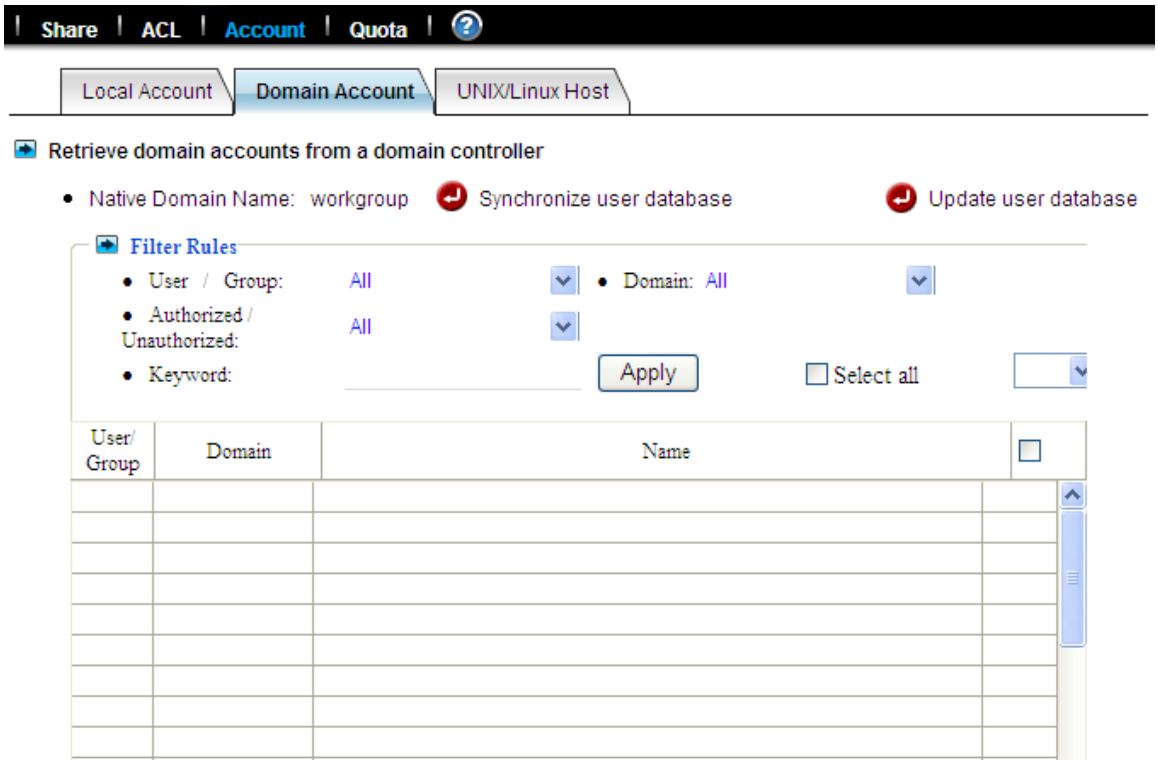
To mass import local accounts:

1. Go to **Security→Account→Local Account** menu.
2. Click the **Mass Import** button.
3. Select a file to import.
4. Click the **Apply** button.
5. If there are any errors, it will be displayed in the pop-up window after clicking the **Last Import** hyperlink.



6.5 Caching windows domain user accounts

Domain users and groups are managed by your network administrator. Windows network uses a domain controller to store the information of all the domain users and groups. When the **Windows Network** is set to use **Domain Mode** in your NAS server, you need to cache domain account in the NAS server's local user database. By caching domain accounts, it speeds up the process of setting permissions and quotas.



To retrieve Windows domain user/group:

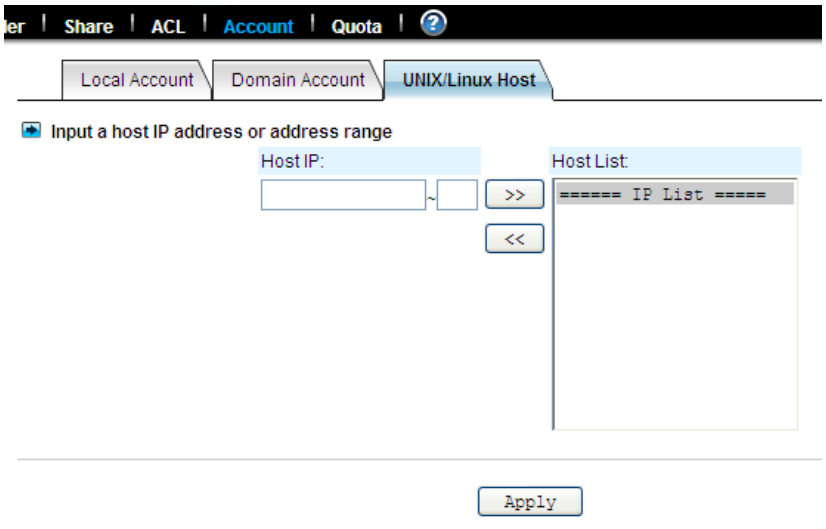
1. Go to **Security→Account** menu.
2. Click the **Domain Account** tab.
3. Select the domain users or groups from domain user pool and click domain user checkbox.
4. Click **Apply** to save the setting.

Filter Rules:

Item	Description
User/Group	You can filter windows domain pool that displays domain users or domain groups or all.
Domain	You can filter which one domain displays pool or all.
Authorized / Unauthorized	You can filter authorized or unauthorized domain accounts or all.
Keyword	You can filter domain accounts which you key in some keyword in field.
Synchronize User Database	This function synchronizes the domain accounts cached in the NAS user database with the native domain controller. New domain accounts in the domain controller will be added to the NAS user database, while the non-existent domain accounts will be removed from the NAS user database. Due to the limitation of system resource, the user database synchronization will be skipped if there are more than 20,480 domain accounts in the domain controller.
Update User Database	Changes of user accounts on the domain controller will not affect the NAS server automatically. You have to do it manually. The '**Update user database**' function on the **Domain Account** tab of the **Security→Account** menu helps you find the user accounts which have already been deleted from the domain controller, yet still remain in the NAS user database. You can choose to delete them from the database. ACL and share permission will be also updated by removing the entries related to those users.

6.6 Creating UNIX/Linux host

For NAS server, NFS client's mount privileges are granted specifically to UNIX/Linux host created by the administrator. If a UNIX/Linux host is granted access right to a share in the NAS server, user of the UNIX/Linux host can have access to the share. Administrator should create a UNIX/Linux host list prior to grant access right to them.



To create a list of the UNIX/Linux host:

1. Go to **Security→Account** menu.
2. Click the **UNIX/Linux Host** tab.
3. Enters a single host IP address in the first text box.
4. Or, enter the start IP address in the first text box and the last 3 digits of the end IP address in the second text box to input a range of the host IP addresses of the **Host IP** field.
5. Click the **Add** button to add the host IPs to the host list.
6. Click **Apply** to save the setting.

6.7 Managing quotas

Configuring user quota:

NAS server supports two types of quotas: user quota and folder quota. User quota monitors the disk space usage of each user. It is based on file ownership, and is independent to which volume that the file and folder located. Below are the descriptions of the parameters when setting up user quotas.

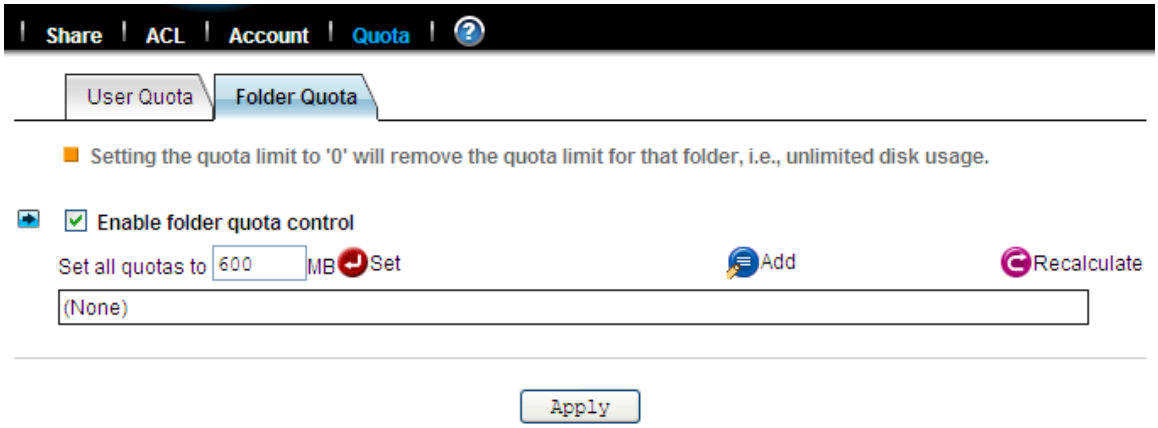
Item	Description
User Name	User name in the local user database.
UID	The user ID set in the user mapping table in “Network → UNIX/Linux” menu.
GID	The group ID set in the user mapping table in “Network → UNIX/Linux” menu.
Type	User type “Local” or “Domain”.
In Use	Total amount of disk space used by the user.
Quota Limit	The amount of disk space in MB a user is allowed to use.

1. Click the **Enable user quota control** checkbox to enable user quotas.
2. Enter quota limit in MB for the user under the **Quota Limit** column.

3. You can click the **Recalculate icon** to obtain the most updated information of the total amount of disk space used by each user.

4. Click **Apply** to save the setting.

To set all quotas to the same value, please specify the quota value in the **Set all quotas to xx MB** input field. Click the **Set** hyperlink to save settings.



Configuring folder quota:

Folder quota monitors the amount of data that can be stored on the folder on which folder quota is applied regardless of who saves there. It can limit the total amount of data stored in the NAS server to effectively control the proper consumption of the storage resources. Note that it is prohibited to set folder quota to the Volume root or “System folder” and its sub-folders.

Item	Description
Folder Name	The path and folder name that the folder quota has been applied.
In Use	Total amount of disk space used.
Quota Limit	The amount of data that can be stored in the respective folders.
	Delete quota entries by selecting the check box at the end of each quota entry and click this icon.

1. Click the “Enable folder quota control” checkbox to enable folder quotas.

2. Click the “Add” to add folder quota to a folder.

3. Click the “Select Path” to browse for target folder.

4. Enter the quota limit in MB.

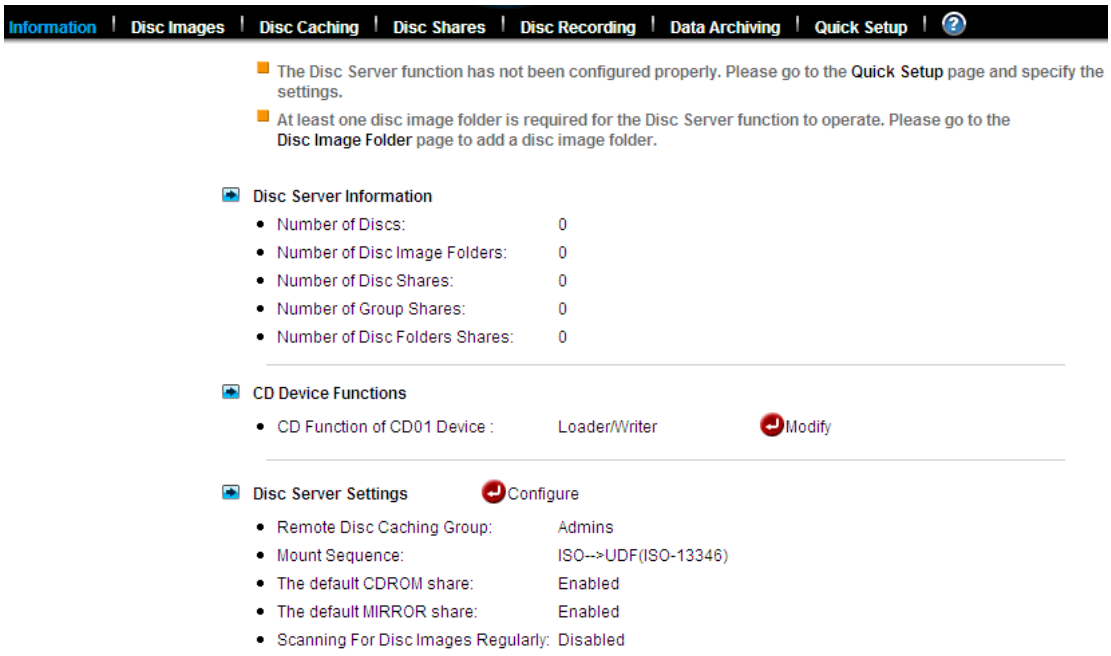
5. Click “Apply” to save the settings.

6. You can click the “Recalculate” to obtain the most updated information of the total amount of disk space in use on each folder.

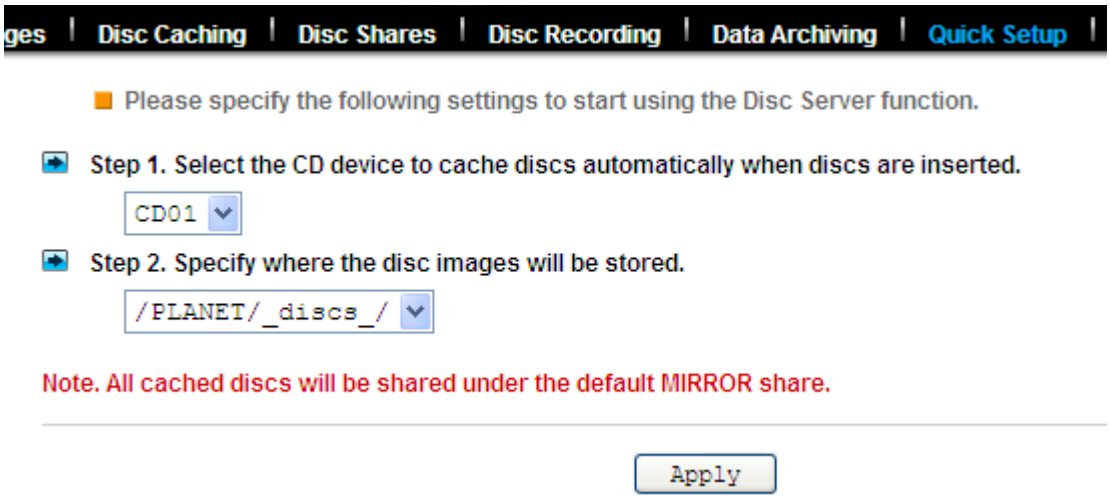
To set all quotas to the same value, please specify the quota value in the “Set all quotas to xx MB” input field. Click the “Set” hyperlink to save settings.

Chapter 7. Disc Sharing and Data Archiving

Disc Server creates and manages CD and DVD disc images for easy and fast disc sharing. It relieves the efforts of handling huge amount of discs. Thousands of discs can be kept online for user access. To protect those disc images, all NAS servers are equipped with a robust RAID sub-system, which features hot-spare disks and strong data protection.



7.1 Starting to use the disc server function



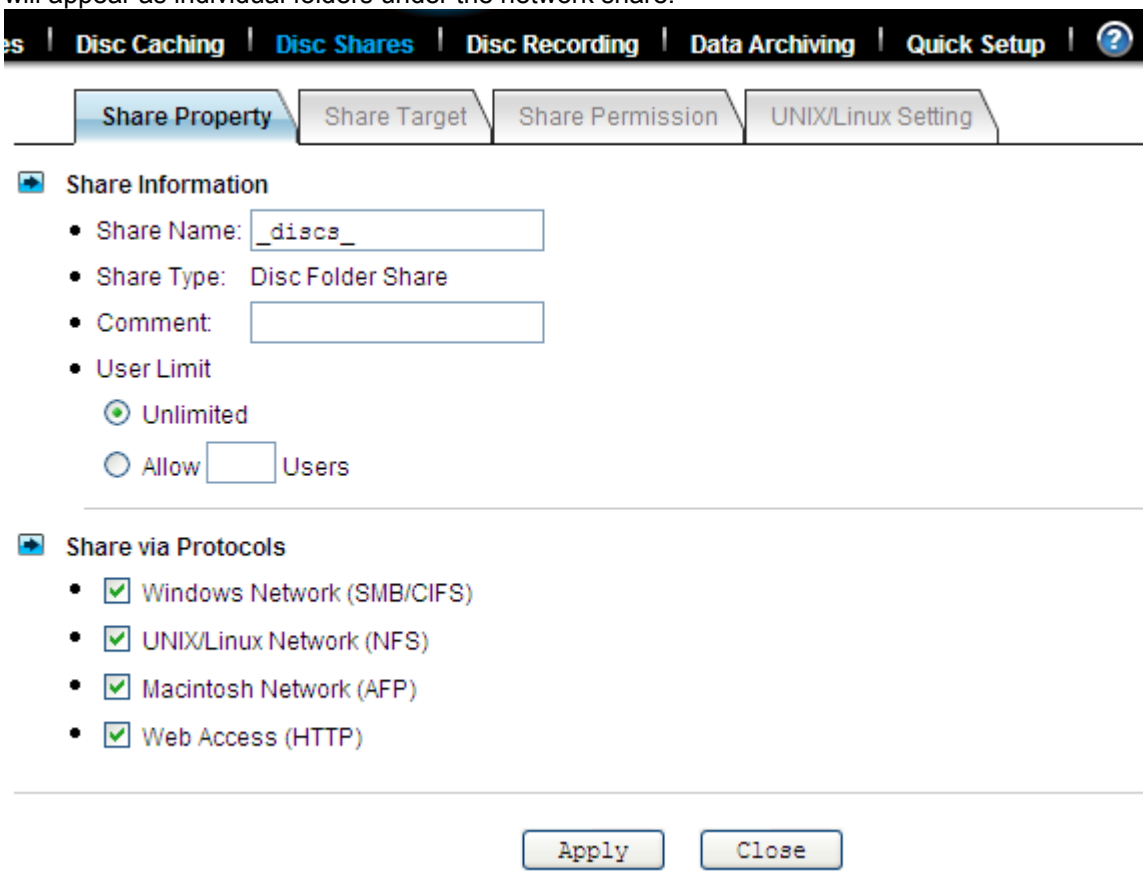
It requires some simple configuration before using the Disc Server function. Please open the administration page and select **Quick Setup** from the **Disc Server** menu. On the page, select the CD or DVD device which will duplicate the disc image automatically when a disc is inserted. Then specify the folder to store the duplicated disc images. Click **Apply** to save the settings.

Insert a disc into the CD or DVD device. It should start duplicating the disc image immediately. When it finishes, network users can access the disc by opening the MIRROR share of the NAS

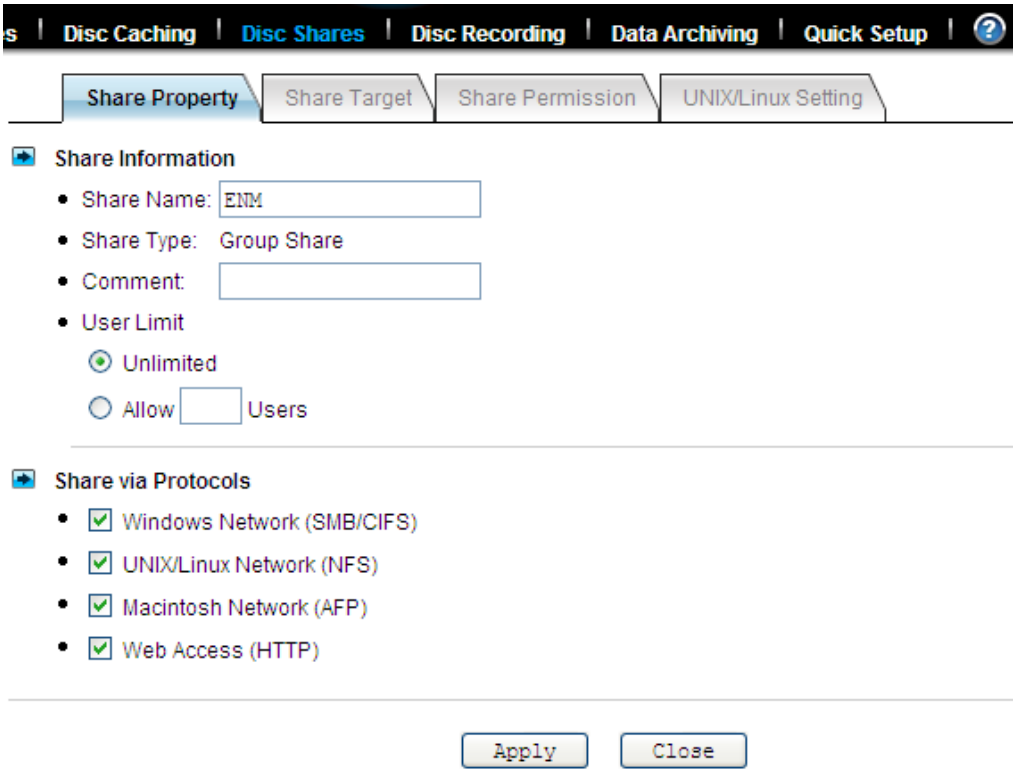
server.

7.2 Sharing discs

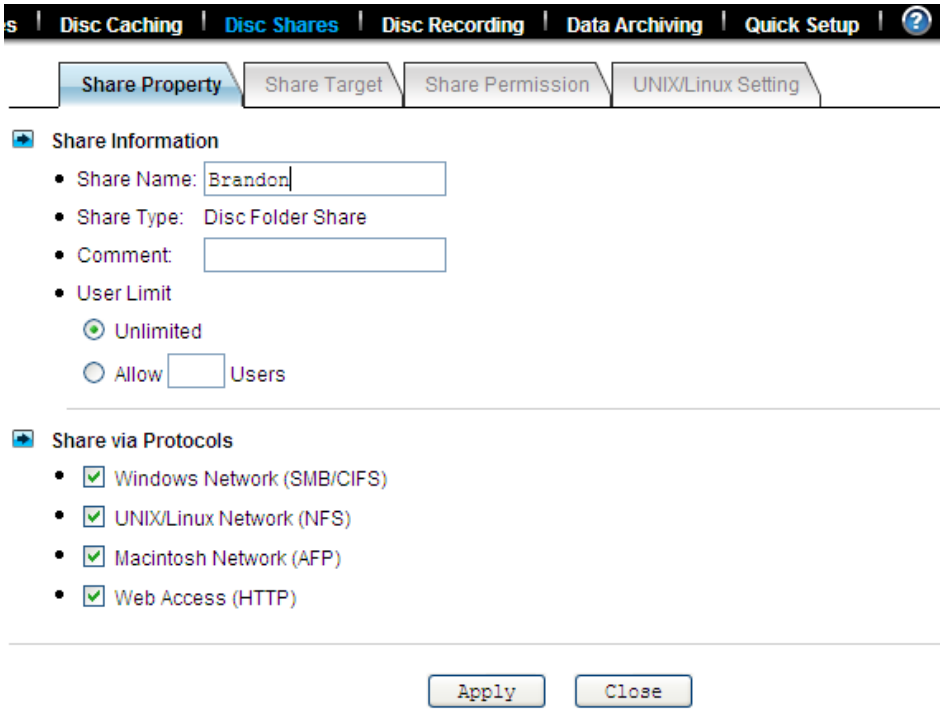
Administrators can choose to share a single disc, multiple discs or a disc image folder. If a single disc is shared, its content will be shown when users open the network share. If multiple discs are shared, the discs will appear as individual folders under the network share. The folder names are the same as the disc names. If a disc image folder is shared, all the discs in the disc image folder will appear as individual folders under the network share.



To share a single disc:
To share a single disc, go to the **Disc Server→Disc Images** menu of the administration page. Click the **Create** hyperlink in the **Share** column. Click **Apply** to share the disc. Enter the **Share Permissions** tab to assign user permissions if you want to restrict user access. The Unix/Linux Setting tab is for configuring NFS security settings. Please refer to section 6.5 - Creating Share and Assigning Share Permissions for the details of share permissions and NFS security settings. You can also go to the **Disc Server→Disc Shares** page to share a single disc. Click the **Create Disc Share** button. Specify the share name and click **Apply** to create the share. Select the disc to share in the **Share Target** tab and click **Apply**.



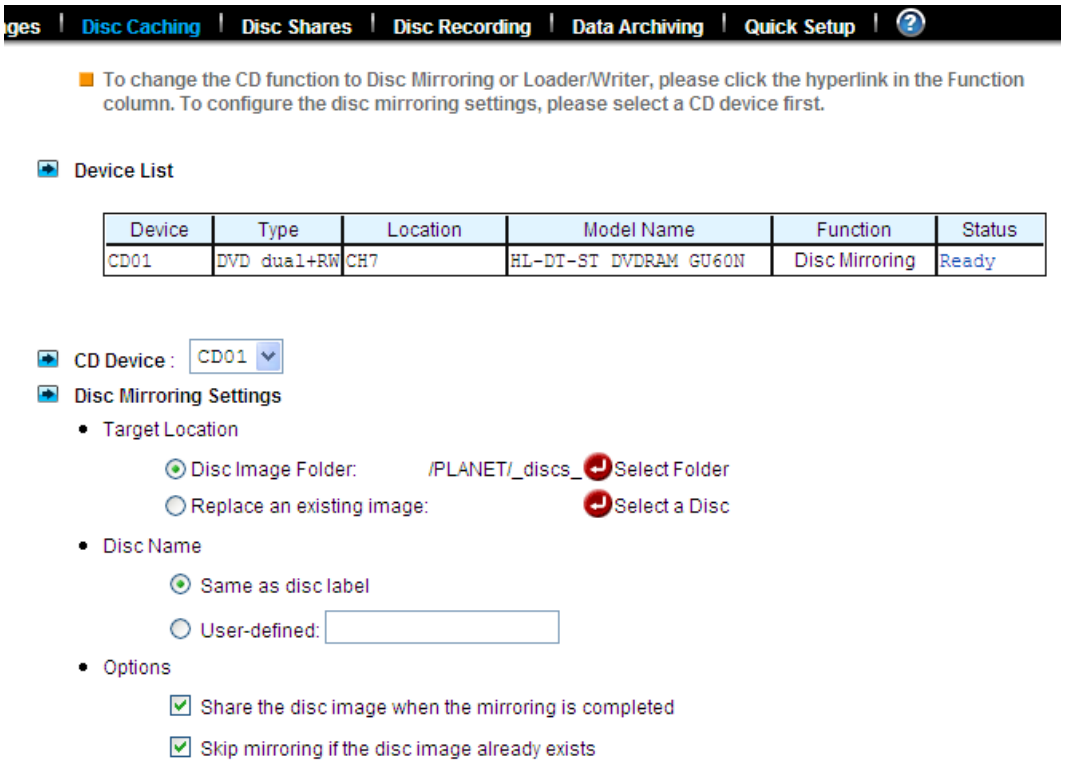
To share multiple discs:
To share multiple discs, go to the **Disc Server→Disc Shares** page. Click the **Create Group Share** button. Specify the share name and click **Apply** to save settings. Select the discs to share in the **Share Target** tab and click **Apply**. Use the **Share Permissions** tab or the **Unix/Linux Setting** tab if you want to restrict user access.



To share a disc image folder:
To share a disc image folder, go to the **Disc Server→Disc Images→Disc Image Folder** menu of the administration page. Click the **Create** hyperlink in the **Share** column. Specify the share name and click **Apply**. Use the **Share Permissions** tab or the **Unix/Linux Setting** tab if you want to restrict user access.

You can also go to the **Disc Server→Disc Shares** page to share a disc image folder. Click the **Create Disc Folder Share** button. Specify the share name and click **Apply** to create the share. Select the disc image folder to share in the **Share Target** tab and click **Apply**.

7.3 Creating disc images

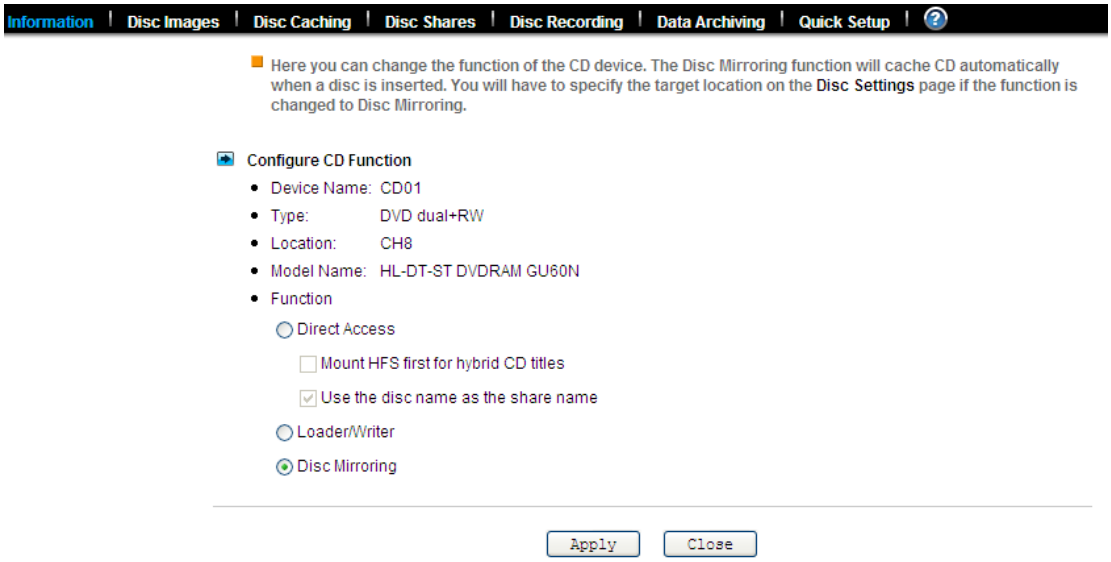


Using the local optical device to duplicate disc images

The simplest and fastest way to create a disc image is to use the CD or DVD device of NAS server to duplicate the inserted discs. Usually a CD can be duplicated in 5 to 10 minutes.

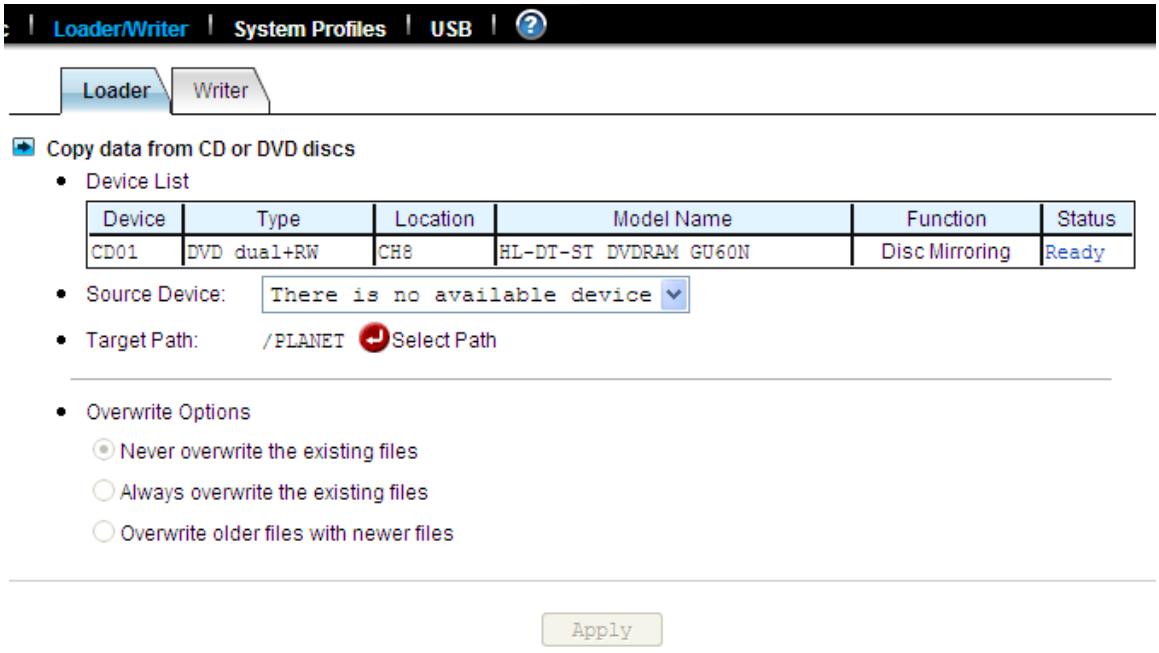
To configure a device so that it can automatically duplicate any inserted discs, please go to the **Disc Server→Disc Caching** menu page of the administration page. In the **Device List** table, click the hyperlink text in the CD Device's **Function** column and change the CD function to **Disc Mirroring**.

The Disc Mirroring Settings section will appear on the page. Select a folder as the target location. The folder is called **Disc Image Folder**, which is a folder especially for storing disc images. In addition to creating a new disc image, it can also replace an existing disc image with the duplicated one. If the disc image being replaced is shared, the duplicated disc image will inherit all the share settings and permissions. The CD replacement will happen once and it will return to the previous settings.



The disc image's name can be either inherited from the CD label or user-defined. A user-defined name will only apply once to the next duplicated disc image.

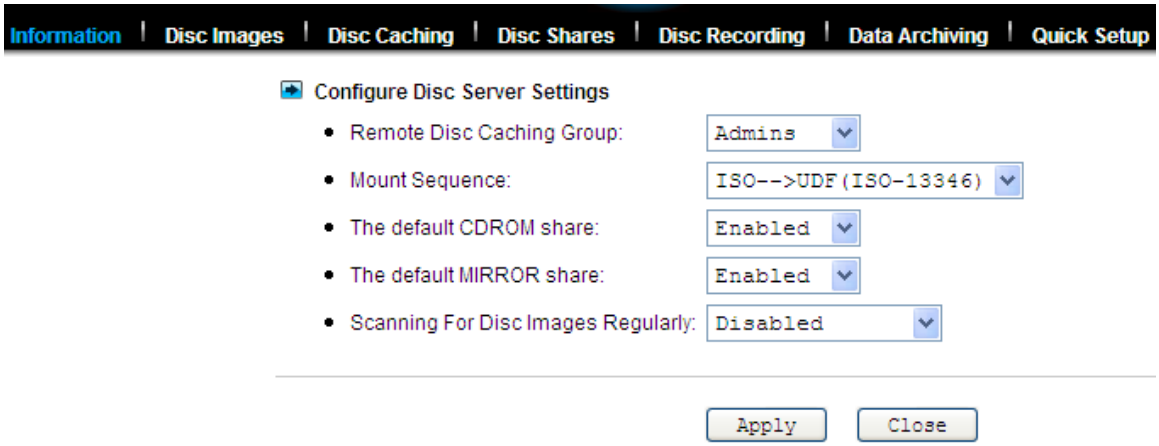
If you set the CD function to '**Direct Access**', it will mount any disc inserted in the CD/DVD device. The mounted disc will appear as a folder under the default CDROM share.



Copying disc images via network filing protocols or SmartSync

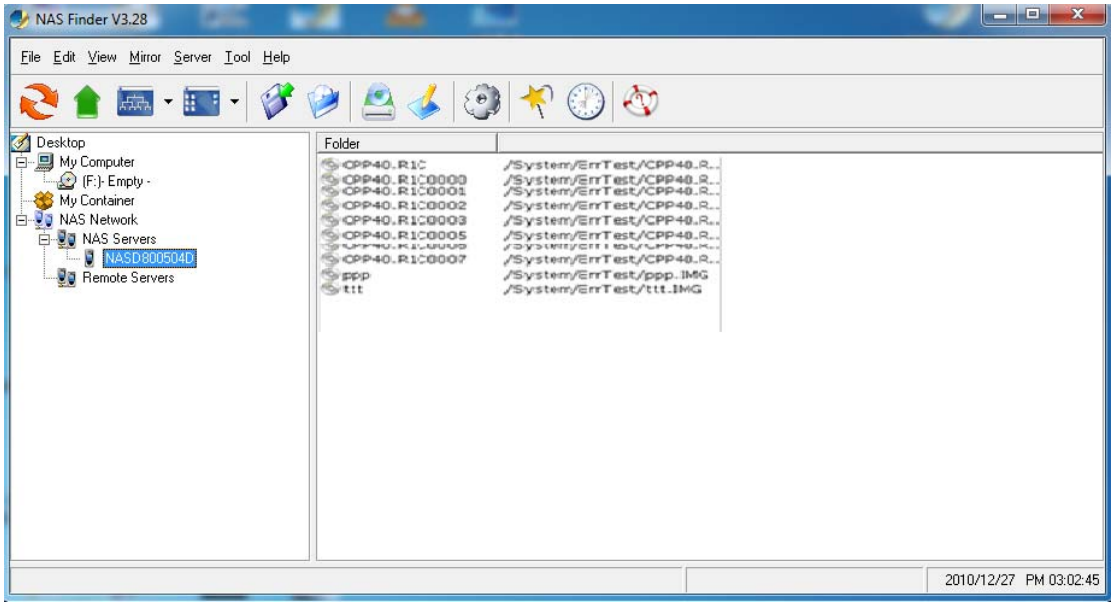
The disc images are stored in the disc image folders. Administrators can also copy or sync the disc images from one NAS server to another, using Windows Explorer, MacOS Finder or SmartSync.

When disc images are copied to a disc image folder, the NAS server will not recognize them immediately. Administrators must command the NAS server to discover disc images manually or set up the NAS server to discover disc image regularly.



To discover disc images manually, please open the **Disc Server→Disc Images** administration page and click the **Rescan images** hyperlink to the right of the page.

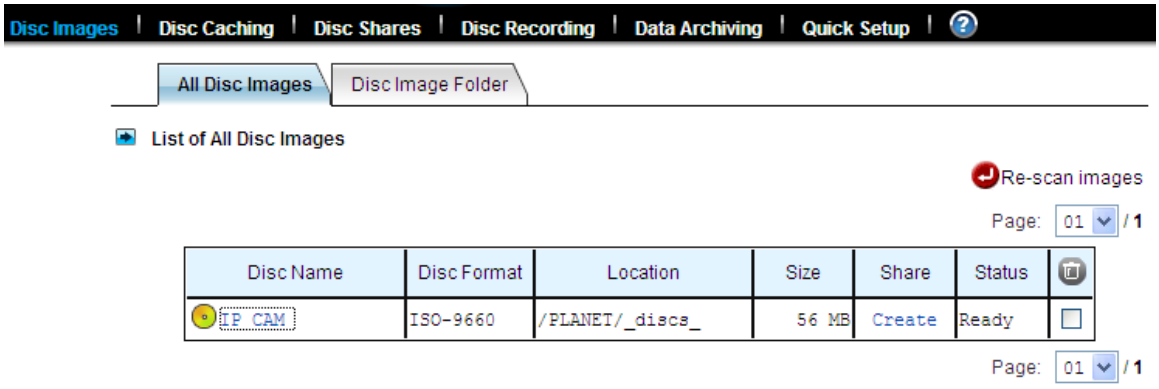
To set up the NAS server to discover disc images regularly, please open the **Disc Server→Information** page. Configure the **Disc Server Settings** to enable the NAS server to scan for disc images every one hour.



Using the remote mirroring software to create disc images

Please refer to Appendix B - Utility for NAS server for how to use the remote mirroring software.

7.4 Managing discs



Once the disc image is created in the NAS server, it can be seen on the **Disc Server→All Disc Images** menu of the administration page. If the disc images are not created or duplicated by the NAS server or by the remote mirroring software, administrators will have to re-scan the disc image folders for disc images manually. For example, if disc images are copied from another NAS server to a disc image folder over network using the Windows or other OS platforms, the NAS server will not be able to list them on the **Disc Images** page. In such cases, administrators have to click the **Re-scan images** hyperlink text to the right of the page.

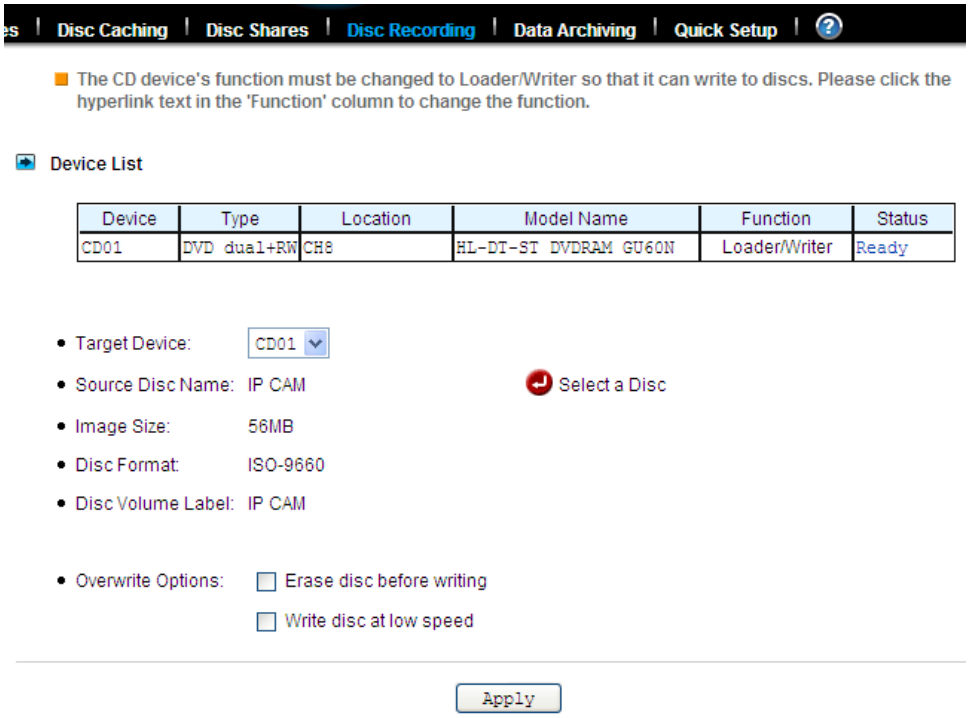
To change the disc name:

To change the disc name, click on the hyperlink text in the **Disc Name** column. On the same page, it also shows detailed information of the disc image.

To delete a disc image:

To delete a disc image, check the check-boxes to the right and click the **Delete** icon.

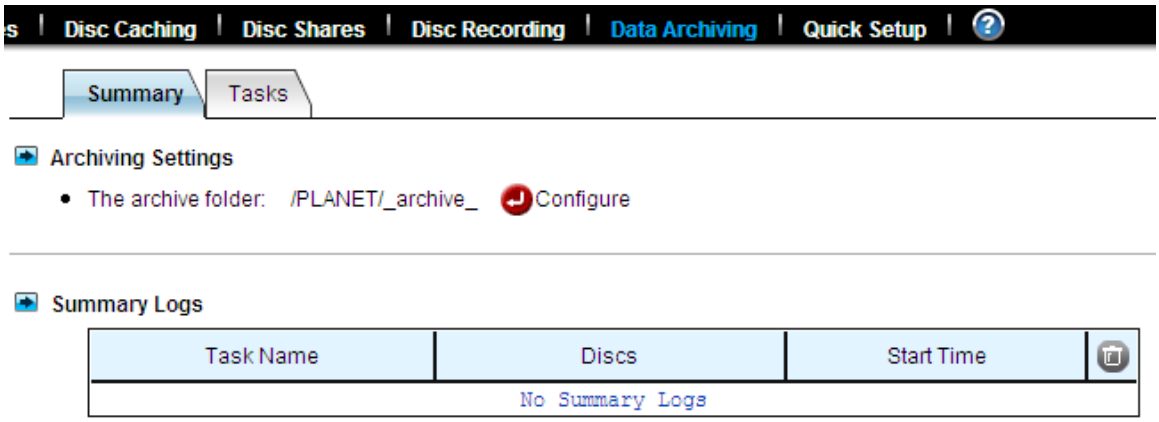
7.5 Burning disc images



To burn an existing disc image, select **Disc Recording** from the **Disc Server** menu on the administration page. To do disc recording, the CD function must be configured as **Loader/Writer**.

To change the CD function, please click the hyperlink in the **Function** column of the **Device List** table. Next, select a disc image by clicking the **Select a Disc** hyperlink. After the selection is made, the disc image information will be shown underneath, including image size, disc format and disc volume label. Check the **Erase disc before writing** option if it is a rewriteable disc which contains data. Click **Apply** to start the disc recording.

7.6 Archiving data to CD/DVD discs



Data archiving is to move or copy regularly NAS data to CD/DVD discs. Administrators can set file filters, mostly based on file date/time, to specify what to burn. One of the applications is to move obsolete data out of the NAS server so that disk space can be freed for future uses.

If used with the Disc Server function, the Data Archiving function becomes more versatile. You can choose to turn some less-frequently-used files to read-only disc images first, which can be mounted by the Disc Server function to share to network users in read-only forms. When the archived data are not in use for a long time, you can then choose to burn them to discs, freeing the hard disk space.

The archive folder

During data archiving, the NAS server will first create disc images in the **archive folder**, which is a disc image folder specifically for storing archived data in the form of disc images. Firstly specify the location of the archive folder on the **Disc Server→Data Archiving→Summary** page before you use the data archiving function.

Summary logs

On the **Disc Server→Data Archiving→Summary** page also shows the summary logs, which keep track of the execution summary of the data archiving tasks.

In addition, they keep records like which disc images are created, which are burned and which are not. Click the **View** hyperlink under the **Discs** column of the **Summary Logs** table to view the list of disc images. For those disc images not burnt yet, you can choose to burn them.

Setting up data archiving tasks

On the **Disc Server→Data Archiving→Tasks** page, you can create tasks to archive data manually or scheduled.

Item	Description
Task Name	Specifies the name of the data archiving task for management purposes.
Source Folders	Specify the data to be archived. The folders, not preserving the full paths, will be archived to CD/DVD discs.

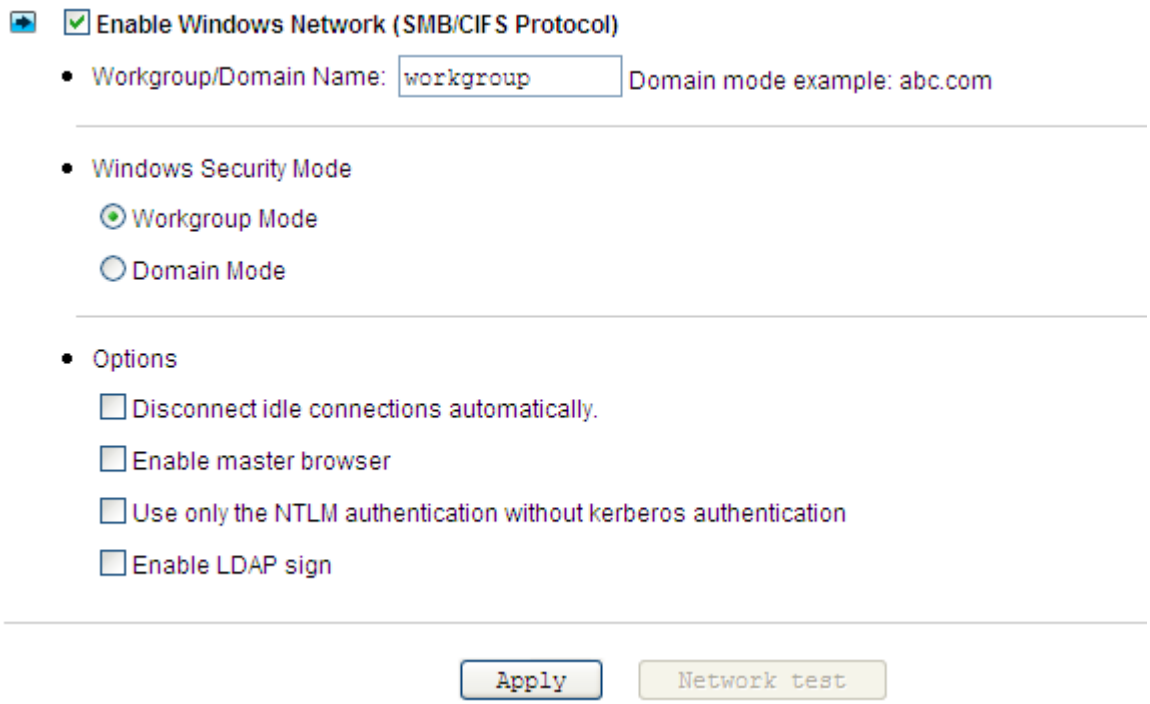
Disc Label	Specifies the labels of the CD/DVD discs.
Date Extension	If the date extension is enabled, it will append the date of archiving to the disc labels. For example, PLANET20041010_01 is the first disc created by the data archiving task on October 25, 2004 with the date extension. The second disc will be PLANET20041010_02 if more than one disc is created.
Disc Type	Specifies the media for burning. It can be a CD (650M/700M), a DVD, a blu-ray DVD or a dual-layer DVD. The NAS server will create disc images that match the size of the disc type, and then burn the disc images.
Advanced Settings – File Filtering	At first the settings are hidden. Please click the **Show** hyperlink to display the advanced settings. The file filters specify which files in the source folders to include for data archiving. You can choose to include only the files which are in the specified date range. Or, you can choose to include the files which are N days old. Or, you can choose to include only the files of which the archive bits are set. The NAS server will clear the archive bits of the source files which are archived, if not deleted.
Advanced Settings – Skip Archiving (Do archiving only if…)	You can set constraints so that the archiving task is activated only when one of the following conditions is met. **if the free volume space is lower than n%** – in other words, the data archiving will be skipped if the free volume space is high **if the archived data are over n MB/GB** – that is to say, the data archiving will be skipped if the archived data are below the threshold.
Archiving Schedule	Specifies the schedule of the archiving task. If the schedule is due, the NAS server will check if the conditions specified in the Advanced Settings are met. If met, then perform the data archiving task.
Options	**Delete source files after the archiving is completed** – if checked, the NAS server will delete the source files to free up disk space after data are successfully archived as disc image burned to discs. **Burn Disc** – if checked, it will archive data to CD or DVD discs. Multiple CD/DVD writers can be specified here. Please note that the CD/DVD functions must be set to Loader/Writer before putting into use for burning.

Chapter 8. User access

The NAS server fits into the network environment as soon as it is properly configured. This chapter describes how to get the NAS server ready for user access from various network operating systems.

Before reading on, please make sure that the NAS server is configured with an IP address and a volume is created successfully. For the rest of the sections, we assume that the server name is **NAS SERVER**, the IP address is **192.168.0.100** and there is a volume named **volume01**.

8.1 Workgroup or domain mode



The NAS server can work in either the workgroup mode or the domain mode. In the workgroup mode, the administrator creates accounts for the NAS server and maintains the user database per server. User authentication is done by checking the local user accounts. In the domain mode, the NAS server can retrieve user names from the domain controller and rely on the domain controller to authenticate users. It can also authenticate users by local accounts. In the domain mode, when a Windows user requests to access a shared folder, the user will be authenticated with the domain accounts first, then the local accounts. If the user is assigned with proper access rights in the share permissions and the ACL settings, the user will be allowed to access the shared folder.

For those using MacOS, web browsers or FTP to access the NAS server, the security control mechanism is similar. If set to the workgroup mode, the NAS server authenticates all users from various network operating systems with local accounts only. If set to the domain mode, the NAS server can be configured to use different security policies for different network file protocols – either authenticated by local accounts only, or by both local and domain accounts.

For example, the NAS server can authenticate Windows users by querying the domain controller, while at the same time check the MacOS users with local user accounts. The administrator can set the SMB/CIFS protocol to the domain mode and configure the AFP protocol to apply **Local account authentication**.

8.2 Accessing from windows

There are some configuration jobs to do before Windows users can access the NAS server. Please enter the administration homepage first.

1. Go to Server → Maintenance page select a volume as system folder then click Apply button

2. Please configure the NAS server to operate either in the workgroup mode or the domain mode. Go to the **Network→Windows** menu and select either **Workgroup Mode** or **Domain Mode**. Also specify the workgroup/domain name.

3. Create local accounts if the NAS server is in the workgroup mode. Go to the **Security→Account→Local Account** page and use the **Add User** or **Add Group** button to create local accounts.

4. Get domain accounts from the domain controller if the NAS server is in the domain mode. Go to the **Security→Account→Domain Account** page. Get domain user account for the domain controller. Next, tick some domain account to be cached in NAS server.

5. Share the volume to network users.

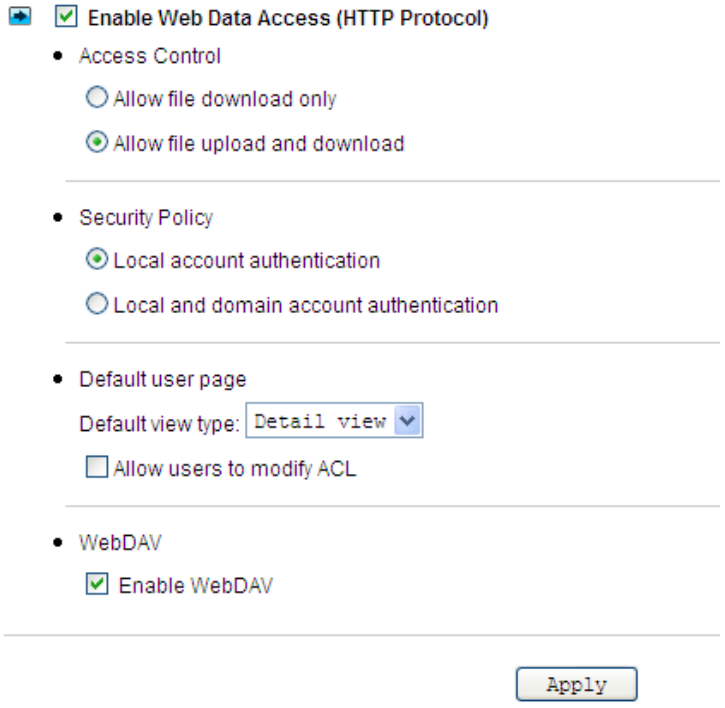
Go to the **Security→File/Folder** menu. Find the **volume01** entry and click **Create** in the **Sharing** column (or click **Modify** if the volume has been shared). On the **Property** page, check the **Windows Network (SMB/CIFS)** checkbox and click **Apply**.

6. Set the share permissions.

After sharing the volume, specify the access rights of local users/groups and domain users/groups.

Now Windows users can access the NAS server. They can run the Windows Explorer and open the path of **\\nasserver**. The shared folder **volume01** will appear in the window. Windows users can also map a network drive to **\\nasserver\volume01** or use the **net use** command in the **Command Prompt** window. The command will be like: net use n:\\nasserver\volume01

8.3 Accessing from web browsers



In addition to the administration homepage, the NAS server provides the user homepage for normal users to access data in the server. With a web browser, users can download files, create folders, upload files and modify ACL. To enable user access from web, please follow the steps.

1. Enable the user homepage.

Open the administration page and enter the **Network→Web** menu. Check the **Enable Web Data Access** check-box. Specify whether to allow local accounts only or allow both local and domain accounts to access the user page. Check other parameters and click **Apply**.

2. Create local user accounts or retrieve domain accounts from the domain controller, depending on whether the NAS server is in the workgroup mode or the domain mode.

3. Share the volume to network users.

Go to the **Security→File/Folder** menu. Find the **volume01** entry and click **Create** in the **Sharing** column (or click **Modify** if the volume has been shared). On the **Property** page, check the **Web Access (HTTP)** check-box and click **Apply**.

4. Set the share permissions.

After sharing the volume, click the **Share Permissions** tab to specify the access rights of local users/groups and domain users/groups.

Now users can run the web browser and open the IP address of 192.168.0.100 to browse the NAS server. When the user homepage is opened, it prompts for user name and password. Then it will display all shared folder after user login. The user homepage will be like:

In the top right corner of the user page are the tool-bar icons, which provide access to various functions like creating folder or uploading files. Below the tool-bar icons are the server name and the login user. Lower on the page is a file browsing area.

Tool-bar icons

Item	Description
	**Admin Page:** switches to the administration home page.
	**Change View Mode:** changes the views of the file browsing area between **Detail**, **Large Icons** and **Small Icons**.
	**Change Password:** modifies the password of the login user. It allows a local user to change the password.
	**Create Folder:** creates a new folder in the current path if the login user has the access right.

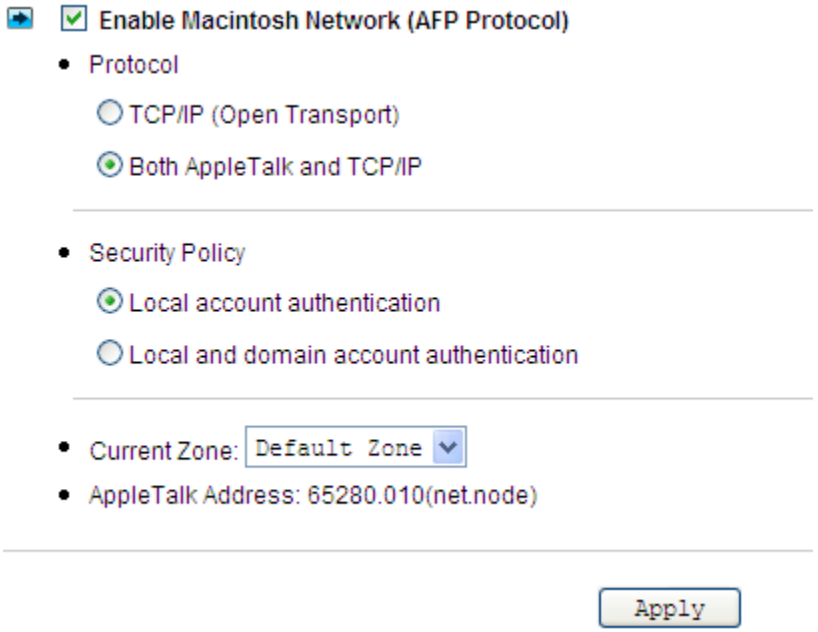
	**Upload File:** uploads files to the current path if the login user has the access right.
	**Help:** opens a new browser window with help information

File browsing

When the user page is opened, the file-browsing window shows all the shares in the server. All the folders and files are presented as hyperlinks. If a folder is clicked, it will show its content in the same window. When a file is clicked, it will either open the file in another browser window or pop up a dialog box for download. To move to the upper level of directory, click the  **Up Directory** icon.

To delete files or folders, check the checkboxes in the **Delete** column. And click the **Delete** icon  to delete them. To rename a file or folder, click the **Rename** icon  , input the name and press the **Enter** key. If a user has the **Full Control** access right for a file or folder, he can modify its ACL by clicking the ACL icon  in the  Permission column.

8.4 Accessing from MacOS



After setting the NAS server to operate in the workgroup mode or the domain mode, follow the steps below to configure for MacOS user access.

1. Enable the Macintosh Network support (the AFP protocol).

Open the administration page and enter the **Network→Macintosh** menu. Check the **Enable Macintosh Network** check-box and specify the security policy and the AppleTalk zone. Then click **Apply**. In the workgroup mode you can only select **Local account authentication** as the security policy. In the domain mode, you can select either one.

2. Create local user accounts or retrieve domain accounts from the domain controller, depending

on whether the NAS server is in the workgroup mode or the domain mode.

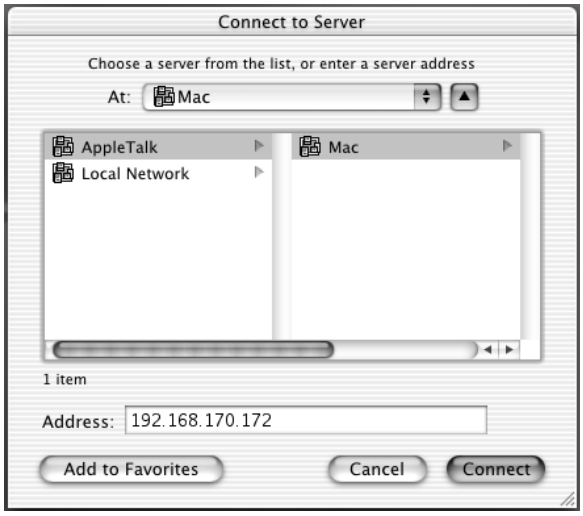
3. Share the volume to network users.

Go to the **Security→File/Folder** menu. Find the **volume01** entry and click **Create** in the **Sharing** column (or click **Modify** if the volume has been shared). On the **Property** page, check the **Macintosh Network (AFP)** check-box and click **Apply**.

4. Set the share permissions.

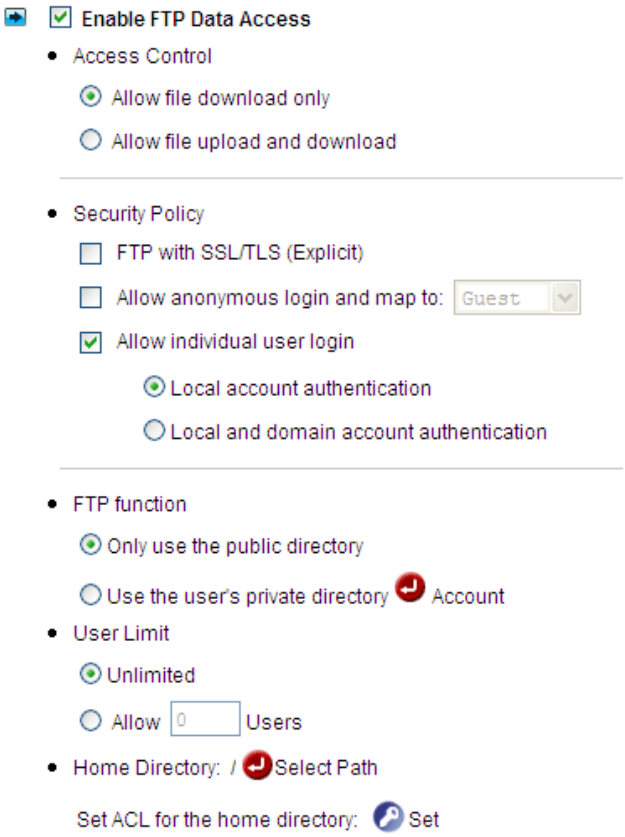
After sharing the volume, specify the access rights of local users/groups and domain users/groups. After the configuration is done, MacOS 8 or OS 9 users can use the MacOS Chooser or Network Browser to access the NAS server. Mac OS X users can use the Connect to Server function to open the NAS server.

For example, open the **Connect to Server** window in **Finder**.



You can either type the IP address of **NAS Server** in the **Address** field. And click **Connect** to put it on **Desktop**. Or you can click **AppleTalk** in the middle left window pane to find the zone and the server. Once you find the server, click **Connect** to put it on **Desktop**.

8.5 Accessing from FTP clients



You can set an FTP home directory in the NAS server for user access. Login authentication is done by checking the ACL of the FTP home directory. During an FTP session, the server always checks ACL when it receives any FTP requests, such as tls, put, get, etc. Local accounts and domain accounts are both supported, depending on the security policy.

After setting the NAS server to operate in the workgroup mode or the domain mode, follow the steps below to configure for FTP access.

1. FTP function is used for public folder only or create home directories to privileged accounts.

a. Only use the public directory: Select this option and FTP clients will enter public folder for accessing the same data.

For example, Use FileZilla as FTP client for login to public folder

b. Use the user's private directory: Select option can create a private directory for each privileged user for logging in to their private directory. For example, use FileZilla as FTP client for logging in to private directory

2. Determine the option of User Limit for limiting user's number or don't limit how many FTP clients to login NAS-7410 at the same time.

a. Unlimited: Don't limit how many FTP clients can login to NAS-7410 at the same time.

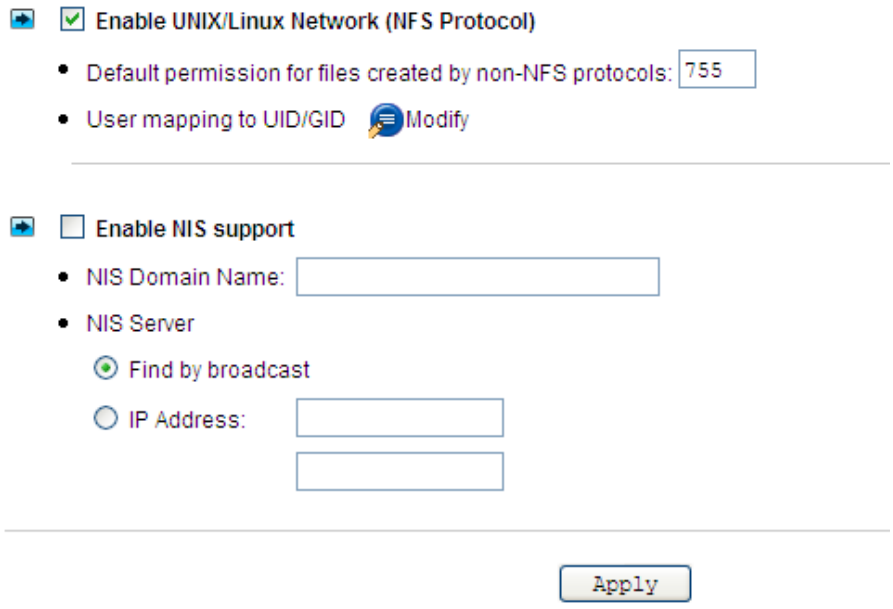
b. Allowed number of Users: Select this option and you can set a number to limit the total number of FTP clients to login to NAS-7410 at the same time for saving some network bandwidth or system resource.

3. Select a folder as the Home Directory of FTP clients and Set ACL for file base security management.

a. Home Directory: Select a folder under NAS-7410; it will be easier for you to manage all of FTP clients and to know how many data under the folder. ※ You have to create a folder first and then click Select Path button to select main Home Directory.

b. Set ACL for the home directory: User can set ACL node on the home directory. It has various permissions (N/A, RO, WO, RW, MO and FC) for each FTP client. You can set the ACL node to the home directory for determining different users with different permissions separately.

8.6 Accessing from NFS clients



The security control of the NAS server for NFS clients follows the traditional UNIX-style trust-host mechanism and UID/GID checking. Follow the steps below to enable NFS support and export the volume for NFS clients to mount.

1. Enable the UNIX/Linux Network support (the NFS protocol).

Open the administration page and enter the **Network→UNIX/Linux** menu. Check the **Enable UNIX/Linux Network** check-box and click **Apply**.

2. Go to the **Security→Account→UNIX/Linux Host** page and add the hosts that might be trusted to access the NAS server.

3. Export the volume to NFS clients.

Go to the **Security→File/Folder** menu. Find the **volume01** entry and click **Create** in the **Sharing** column (or **Modify** if the volume has been shared). On the **Property** page, check the **UNIX/Linux Network (NFS)** check-box and click **Apply**.

4. Enter the **UNIX/Linux Setting** tab. Add NFS clients to the privileged host list. And assign UID, GID and permission octets to the exported volume.

After the volume is exported, use one of the NFS clients in the privileged host list to mount the volume. Please login as the root and use the following command to mount **volume01** under the **/mnt** directory. Mount 192.168.0.100:/volume01 /mnt

Once mounted, the **/mnt** directory will link to **volume01** and inherit the same UID, GID and

permission as you specify in the configuration steps. The users on the NFS client with proper access rights will be able to access the **/mnt** directory and hence the NAS server.

Chapter 9. Backup and Recovery

9.1 Snapshot – Fast Point-In-Time copies

Snapshots are read-only copies of file-systems at a specific point in time. Snapshot distinguishes itself in its speed. Creating a snapshot is not involved with copying user data, thus usually taking less than a second.

The concept of snapshot is very different from backups. Data are not copied to any media during backup. Instead, it just informs the NAS that all the data blocks in use should be preserved, not being overwritten. That is why it can be so fast. The “copy” occurs during everyday file access. When a file is modified after a snapshot is created, its original data blocks are protected from being overwritten. The new updates are written to a new location. The file-system maintains records and pointers to keep track of the snapshot data and file changes.

Snapshot management

To manage snapshots, please open the administration page.

Enter the **Backup→Snapshot→Manage** page and select a volume.

Viewing Snapshot Information

On the page shows the snapshots existing on the volume and their information. **Snapshot Used Space** indicates the disk space used by snapshot data. In the table – **List of Snapshots**, **Space to Free** indicates the disk space which will be freed if a snapshot is deleted. **Activity** indicates whether the snapshot is being deleted or rolled back.

Configuring snapshot settings

Item	Description
Show the .snap folder	With the .snap folders enabled, end-users can access snapshot data without intervention of MIS people, retrieving previous versions of files from the .snap folders. Administrators can choose to show the .snap folders under the root of a volume, or under all folders.
Name the .snap folder as ~snap	Using the AFP protocol, the folders with names beginning with dot (.) will be hidden and not able to be accessed by Macintosh clients. To make the .snap folders visible, the administrators can choose to show the .snap folders as ~snap instead so that the folders can be accessed by Macintosh clients.
Delete snapshots if free space is low	If enabled, it will automatically delete the oldest snapshots to free more disk space when the free space is lower than the specified percentage.
Snapshot Policy	They specify how many hourly, daily, weekly and monthly snapshots to keep, respectively. If the limit is exceeded, the oldest snapshot of the same type will be deleted. If not specified, it will keep the snapshots until being manually deleted.

Creating snapshots

There are several ways to create snapshots. One is to create a snapshot manually by selecting a volume and clicking the **Create Snapshot** button on the **Snapshot→Manage** page. It will create a snapshot with a name like manual-20041010.190000, which indicates a snapshot created manually at 19:00 on October 10, 2004. Another method is to set schedules to create snapshots regularly. Moreover, the NAS server will create snapshots automatically when doing backup, SmartSync and CD/DVD-burning tasks. Then it reads in source data from the automatically

created snapshots, instead of the current active file-system, to prevent the open-file issue.

Deleting snapshots

To delete snapshots, check the check-boxes in the **List of Snapshots** table and click the **Delete** icon to delete the selected snapshots. You can make multiple selections to delete several snapshots at a time. The NAS server will delete the snapshots one by one.

Snapshot Roll-back

Snapshot roll-back is to restore the volume to the state when the selected snapshot was taken. Snapshot roll-back is useful if most data are lost or destroyed by virus attacks or human errors. Snapshot roll-back is much faster than restoring. Please note that the roll-back operation is dangerous because the whole volume will be restored to the previous state. If you want to restore only part of the data, please simply copy them from the .snap folders to the current file-system.

Snapshot scheduling

To manage snapshot schedules, please open the administration page. Enter the **Backup→Snapshot→Schedule** page.

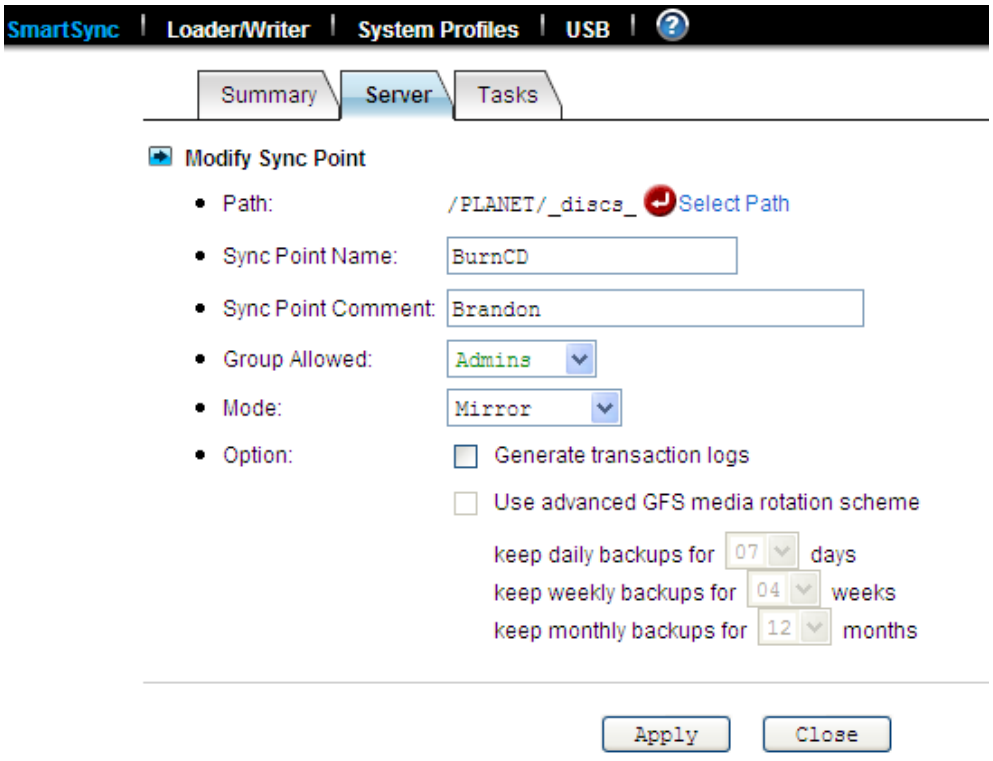
To add a snapshot schedule, either click the **Add Schedule** icons next to the volume names, or click on the **Add Schedule** button on the bottom of the page.

To delete snapshot schedules, check the check-boxes to the right and click the **Delete** icon.

To modify a snapshot schedule, click the hyperlink of the snapshot schedule in the **Schedule** column.

There are four types of schedules – hourly, daily, weekly and monthly. Each volume can have up to 16 schedules of any types.

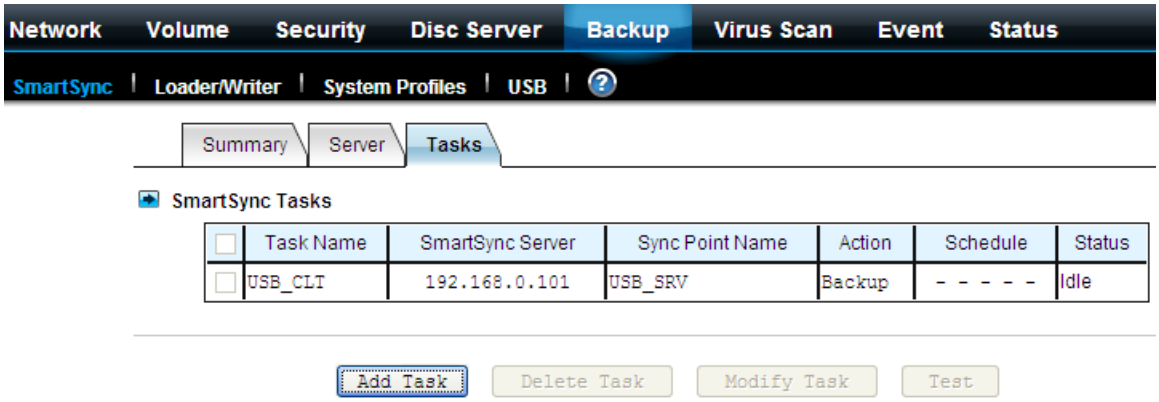
9.2 SmartSync – NAS-to-NAS data replication



The NAS server is integrated with the SmartSync function for NAS-to-NAS data replication. Two or more NAS server are required, one as the SmartSync server, others as the SmartSync clients. The

SmartSync server is like an ftp server. The SmartSync clients can either replicate their data to the SmartSync server, or copying data from the SmartSync server, depending on the task settings.

There are three operating modes of SmartSync - **"mirror"** for one-to-one data replication, **"backup"** for disk-based backup, **"distribute"** for one-to-many data distribution. The following sections describe the usage and applications of these operating modes.



On the NAS server which acts as the SmartSync client, set up a SmartSync task, which defines the schedule settings and the source folder.

To set up a SmartSync task, please go to the **Backup→SmartSync →Task** menu on the **Administration Page**. Click the **Add Task** button.

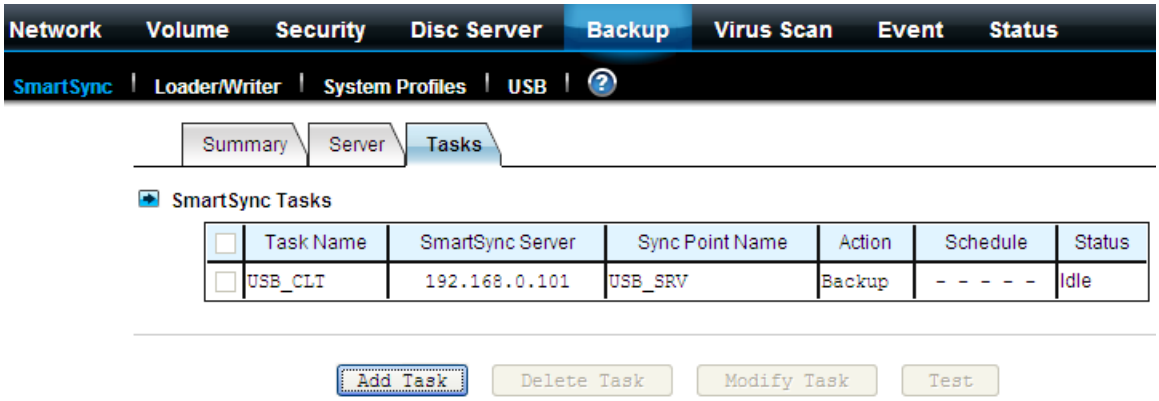
There are four steps to take when adding a SmartSync task. Step 1 is to specify the IP address of the SmartSync server. Please enter the IP address of the NAS server where you create the sync point.

Step 2 is to choose a sync point of **"Mirror"** mode in the SmartSync server. Please also provide a user account with the privilege to replicate data to the sync point.

Step 3 is to complete the task settings. On the page you should provide the task name, select the source folder to replicate, specify the schedule and configure the SmartSync options.

Step 4 is for confirmation, showing the brief information of the task settings.

Making Disk-to-disk backups



Two or more NAS servers are required, one as the SmartSync server, the rest as the SmartSync clients. It will backup data from the SmartSync clients to the SmartSync server.

On the NAS server which acts as the SmartSync server, create a sync point of **"Backup"** mode, which receives data from SmartSync clients and creates data backups in it.

To create a sync point, please go to the **Backup→SmartSync →Server** menu on the **Administration Page**. Click the **Add** button to open the page below. On the page you should provide the sync point name and specify which group is allowed to replicate data to this sync point. Set the mode to **"Backup"**.

The GFS media rotation mechanism is the policy of managing backup versions. The policy is described below. Basically it will check for obsolete versions and delete them when a new backup version is created. X, Y, Z are user-defined numbers.

a. It will keep all the backup versions today.

b. It will keep one backup version per day in the last X days, except today.

c. It will keep one backup version per week in the last Y weeks prior to the X days.

d. It will keep one backup version per month in the last Z months prior to the Y weeks.

On the NAS server which acts as the SmartSync client, set up a SmartSync task, which defines the schedule settings and the source folder.

To set up a SmartSync task, please go to the **Backup→SmartSync →Task** menu on the **Administration Page**. Click the **Add Task** button.

There are four steps to take when adding a SmartSync task.

Step 1 is to specify the IP address of the SmartSync server.

Step 2 is to choose a sync point of **"Backup"** mode in the SmartSync server. Specify the action as **"Backup to server"**. Please also provide a user account with the privilege to replicate data to the sync point.

Step 3 is to complete the task settings. On the page you should provide the task name, select the source folder to replicate, specify the schedule and configure the SmartSync options.

Step 4 is for confirmation, showing the brief information of the task settings.

Restoring files from the SmartSync backups

To restore data from the SmartSync server, please create a SmartSync task on the client. Open the **Administration Page** and enter the **Backup→SmartSync →Task** menu. Click the **Add Task** button.

Follow the steps to take to add the SmartSync task.

Step 1 is to specify the IP address of the SmartSync server.

Step 2 is to choose a sync point of **"Backup"** mode in the SmartSync server. Specify the action as **"Restore from server"**. Please also provide a user account with the privilege to replicate data to the sync point.

Step 3 is to complete the task settings. On the page you should provide the task name, select which backup version to restore, specify the target folder and configure the SmartSync options and the overwrite options. The overwrite options specify whether to overwrite the target with the files of the same names.

Step 4 is for confirmation, showing the brief information of the task settings.

Distributing file updates to multiple sites

Two or more NAS servers are required, one as the SmartSync server, others as the SmartSync clients. It will replicate data from the SmartSync server to the SmartSync client.

On the NAS server which acts as the SmartSync server, create a sync point of **"Distribute"** mode, which distributes data to the SmartSync clients as they request.

To create a sync point, please go to the **Backup→SmartSync →Server** menu on the

Administration Page. Click the **Add** button to open the page below. On the page you should provide the sync point name and specify which group is allowed to request data from this sync point. Set the mode to **"Distribute"**.

On the NAS server which acts as the SmartSync client, set up a SmartSync task, which defines the schedule settings and the target folder.

To set up a SmartSync task, please go to the **Backup→SmartSync →Task** menu on the **Administration Page**. Click the **Add Task** button.

Follow the steps to take to add the SmartSync task.

Step 1 is to specify the IP address of the SmartSync server.

Step 2 is to choose a sync point of **"Distribute"** mode in the SmartSync server. Please also provide a user account with the privilege to request data from the sync point.

Step 3 is to complete the task settings. On the page you should provide the task name, select the target folder to receive data, specify the schedule and configure the SmartSync options.

Step 4 is for confirmation, showing the brief information of the task settings.

The SmartSync options

When setting up a SmartSync task, you will see the following SmartSync options.

Item	Description
Compress the data stream during data transmission	When checked, it will compress data before transmitting to the SmartSync server. Sometimes it will make it faster to complete a task. However, it takes extra CPU time to compress data and may have performance penalty if compression ratio is low.
Contain security information	When checked, it will send ACL information to the SmartSync server.
Bandwidth control	Limits the maximum bandwidth for the task.
Include/exclude file pattern	For excluding or including certain file types in the synchronization. For example, to exclude WORD files, type -*.doc; To exclude all WORD files except those beginning with abc, type +abc*; - *.doc;
Perform quick synchronization	Quick synchronization will only check file date, time and size when matching files, instead of checking block-by-block. It will speed up the synchronization a lot, while taking the risk that files might not be made identical.
Generate transaction logs	When checked, it will record which files are added, updated or deleted during the data replication. The transaction logs are displayed on the SmartSync **Summary** page.

9.3 Loading and writing CD/DVD discs

Connecting a CD or DVD writer to the NAS server, you will be able to load data from CD/DVD discs or burn files on writeable CD/DVD discs. The CD and DVD burning feature turns the NAS server into a device that publishes data, beyond the powerful data storage function.

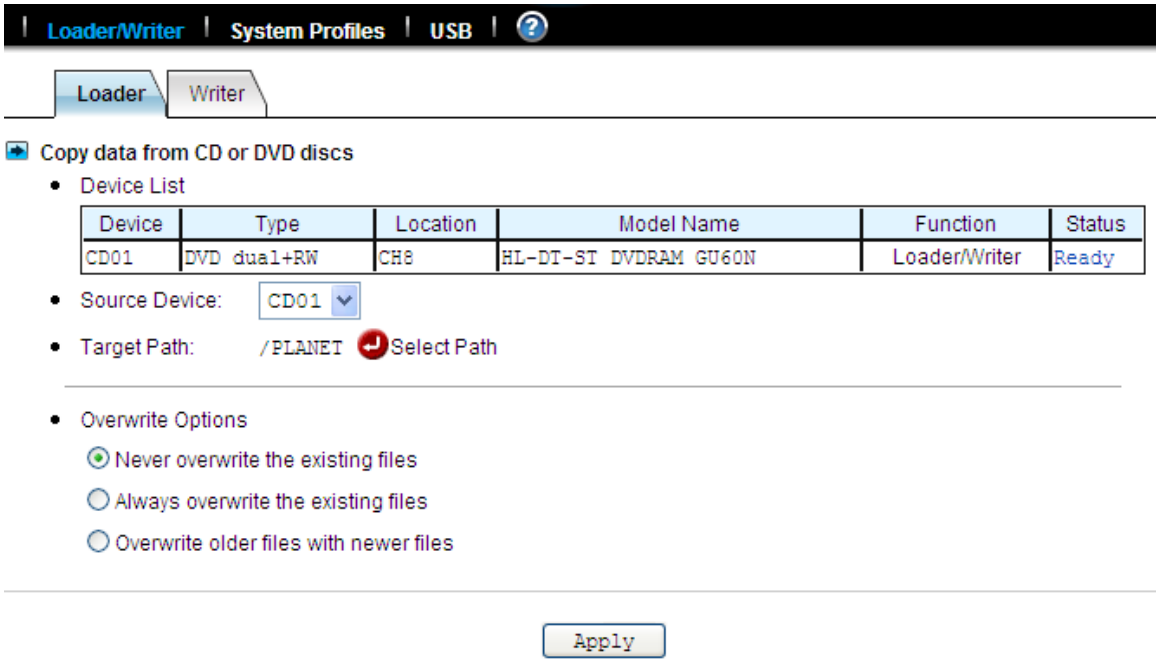
Loading CD/DVD data

The **Loader** function copies data from a CD or DVD disc to any location inside the NAS server. This function is useful when you try to restore the archived data on CD/DVD discs or simply copy files from discs to the server.

Note that the NAS server recognizes only data CD or DVD, such as ISO 9660 level 1, 2, 3 (including Romeo, Joliet and Rock-Ridge extension), CD HFS, CD/DVD UDF, High Sierra, Hybrid (ISO+HFS)

Multi-session CD Mixed Mode CD and UDF V1.5/V2.0. Multimedia CD formats such as audio CD or video CD are not supported.

To load data from CD/DVD discs, please insert the source disc into the CD or DVD device first. Open the **Administration Page** and select **Backup→Loader/Writer**.



1. Select a **Source Device** where you insert the disc to be loaded. Above the **Source Device** item you will see a device list for your reference.

2. Specify the destination. Click the **Select Path** hyperlink and select a target path.

3. Choose whether to overwrite the existing files. **"Overwrite with newer files"** means it will overwrite the target if the files on the CD/DVD disc are newer.

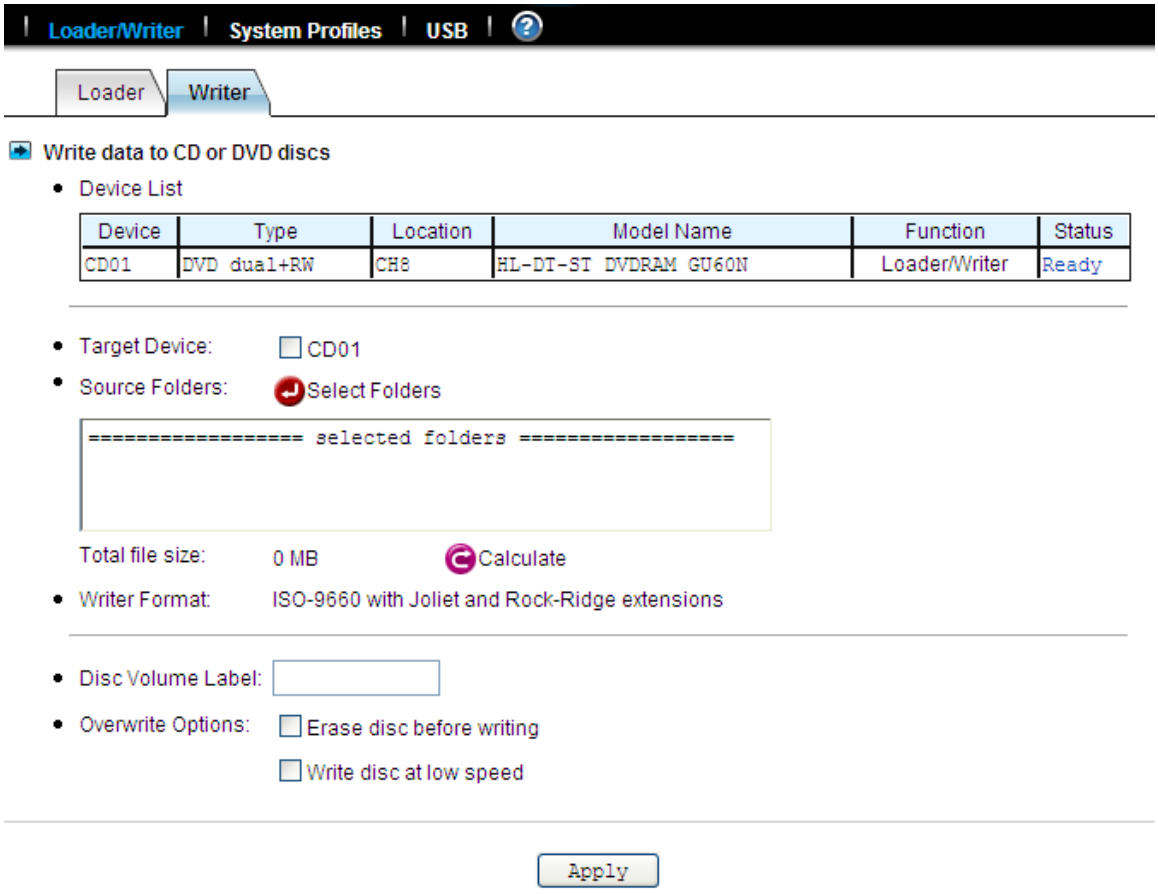
4. Click **Apply** to start copying data.

When it is copying disc, you can see the progress by clicking the hyperlink in the **Status** column of the **Device List**. A separate browser window will pop up. The progress is indicated by the progress bar, the **Processed Folders** item, the **Processed Files** item and the **Size Processed** item.

Writing CD/DVD discs

The NAS server supports CD or DVD burning. It can use ISO-9660 CD format to write data to CD or DVD discs. Supported devices are CD-RW, DVD-RW and DVD+RW writers and Blu-ray Disc. Dual-layer DVD writing is also supported.

To write data to CD/DVD discs, please insert a blank disc into the CD/DVD writer first. Next, open the **Administration Page** and enter the **Backup→Loader/Writer** page. Then follow the steps below.



1. Click the **Writer** tab in **Backup→Loader/Writer** menu

2. Select the **Target Device** where you want to burn the blank CD/DVD disc(s). Above the **Target Device** item you will see a device list for your reference.

3. Specify the source folders. Please click **Select Folders** and specify which folders to burn.

4. Specify the volume label of the CD or DVD disc.

5. Check the overwrite option if you want erase a rewriteable disc first before burning.

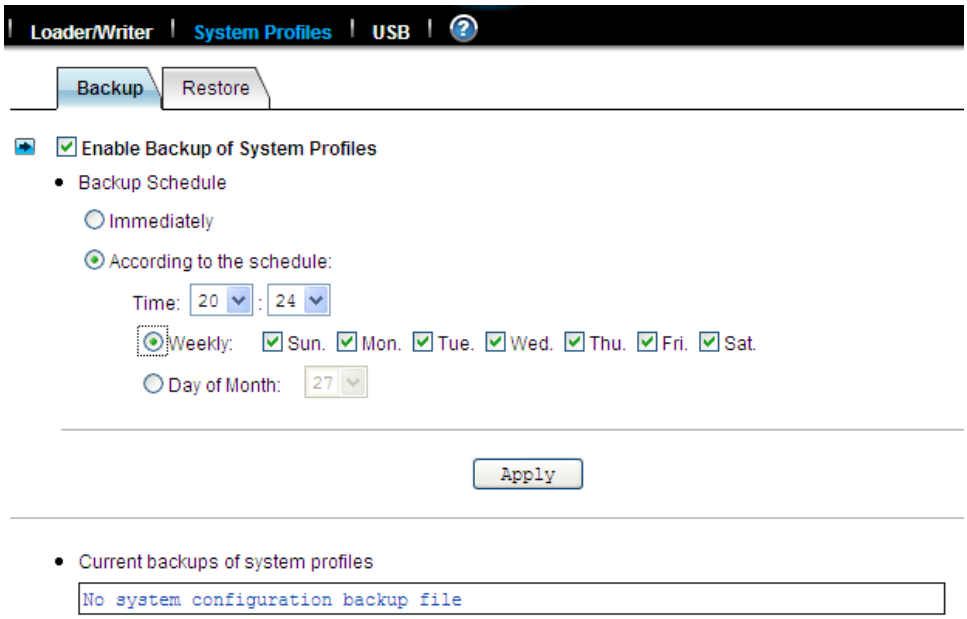
6. Click **Apply** to start burning CD or DVD discs.

When it is writing to disc, you can see the progress by clicking the hyperlink in the **Status** column of the **Device List**. A separate browser window will pop up. The progress is indicated by the progress bar, the **Processed Folders** item, the **Processed Files** item and the **Size Processed** item. You can also check the **Task Phase** to see what the CD/DVD writer is doing.

If it requires more than one disc to burn the source data, it will prompt for a new disc after the first disc is burned ok. In this case, the **Task %** progress bar indicates the total task progress, which means the percentage of the source data which have been burned to discs. The **Disc %** progress bar indicates the CD/DVD writing percentage of the current disc.

9.4 Backup and restore system profiles

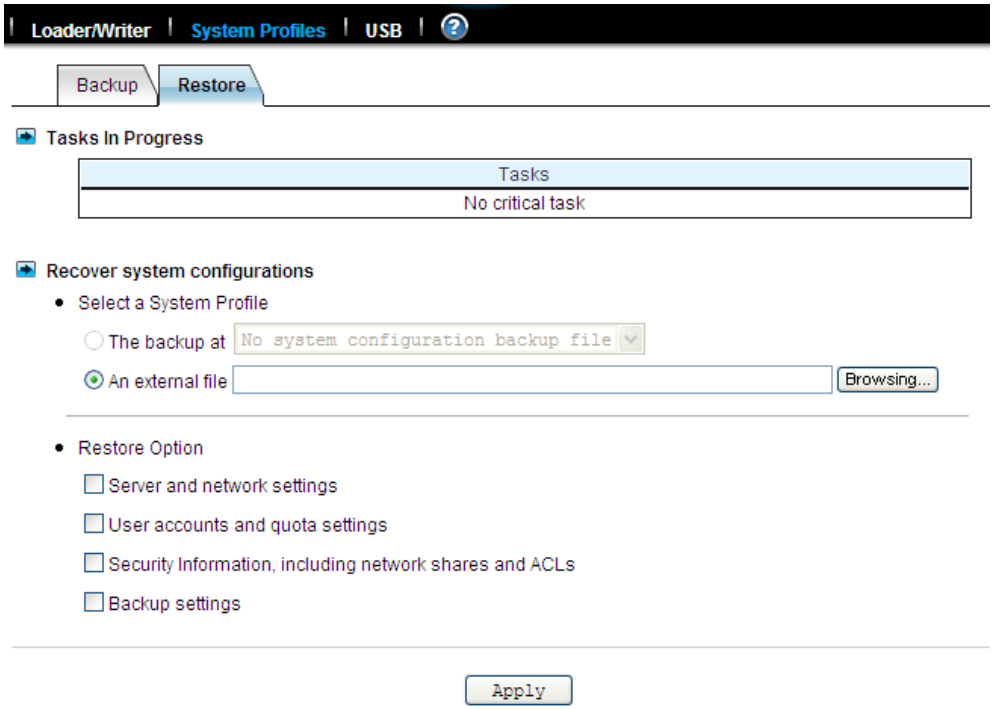
To recover from system failures, it requires restoring data and system configurations. Backup and SmartSync are for restoring data, while system profiles are used for recovering system configurations. System profiles are the backups of all system configurations, user database and security information.



Backing up system profiles

To back up system configurations, please open the administration page and go to **Backup→System Profile**. System profiles are saved manually or on a regular basis as defined on the page. System profiles will be saved locally on HD. The current backups are displayed on the lower page. To delete a system profile, check its check-box and click the **Delete** icon.

Recovering the system configurations when a disaster happens



If there is any system failure which causes corrupt system configurations, the first step is to reset the system configurations to factory default. Go to the **Server→Shutdown** page. Check the **Reset configuration to factory default** option and click the **Reboot** button. The second step is to restore system configurations using one of the system profiles. Go to the **Backup→System Profiles→Restore** page. Select a system profile and choose which part of the system settings to restore. Then click the **Apply** button.

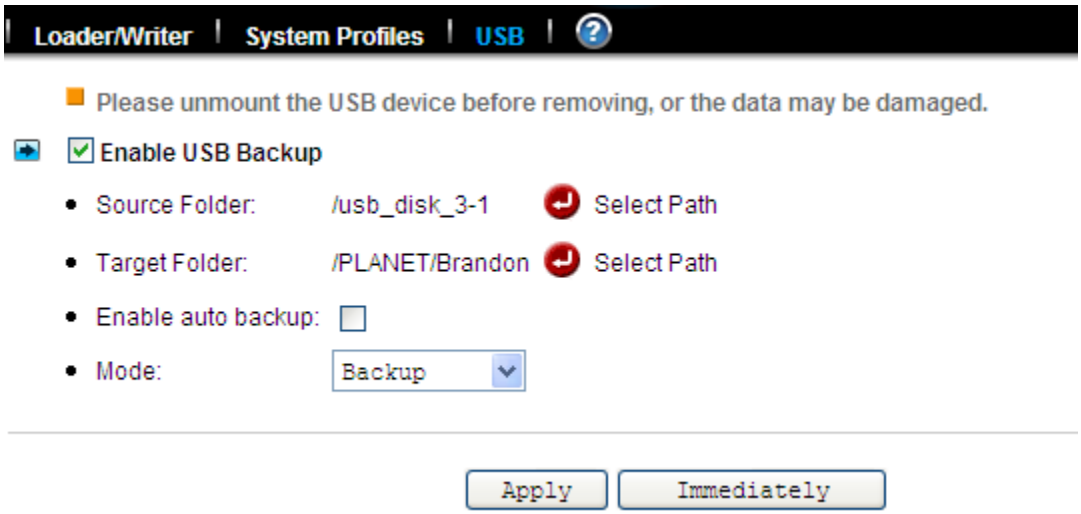
A system profile can also be created by the NAS Finder software. To recover from a system profile saved by NAS Finder, click **an external file** item and find the system profile. Specify restore options and click the **Restore** button.

Restore options are:

Item	Description
Server, network and backup settings	Includes all settings in the **Server**, **Network**, **Backup** and **Event→Configuration** menus. Please note that the admin password will not be restored during the recovery.
User accounts and quota settings	Includes local accounts, current domain accounts and trust domain accounts, together with their quota settings. User accounts will be appended to the existing user database – local accounts with the same names will be overwritten; domain accounts with the same SID will be overwritten; others will be added to the existing user database.
Security Information, including network shares and ACLs	Includes all network shares, share permissions and access control lists.

9.5 Backup USB device

NAS server supports the USB flash drive and external hard disk (support FAT/FAT32/NTFS) backup in optional models with USB ports. Press the button on the LCD front panel to activate the USB backup when plugging in a USB flash drive or hard drive. You can also activate this function via the web interface.



Enable USB Backup

Enable this check box to enable the USB backup support. Plug in the device; you will see a menu to select the "source folder" and the "target folder".

Item	Description
Source folder	When you insert a USB storage device, select the folder you want to back up.
Target folder	Select the file path you want to back up files.
Enable auto backup	When this feature is turned on, NAS server will perform backup automatically following the paths that you have set up. Backup can be divided into three modes. **Backup** – back up the entire content of the source folder to the target folder. Each backup is full backup and stored in a separate folder in the target folder. **Mirror** – back up the entire content of the source folder to the target folder. Any files in target folder that are not present in source folder will be erased. **Distribute** - copy files from the target folder to the source folder. After synchronization is complete, it does not automatically delete the extra files in the source folder.

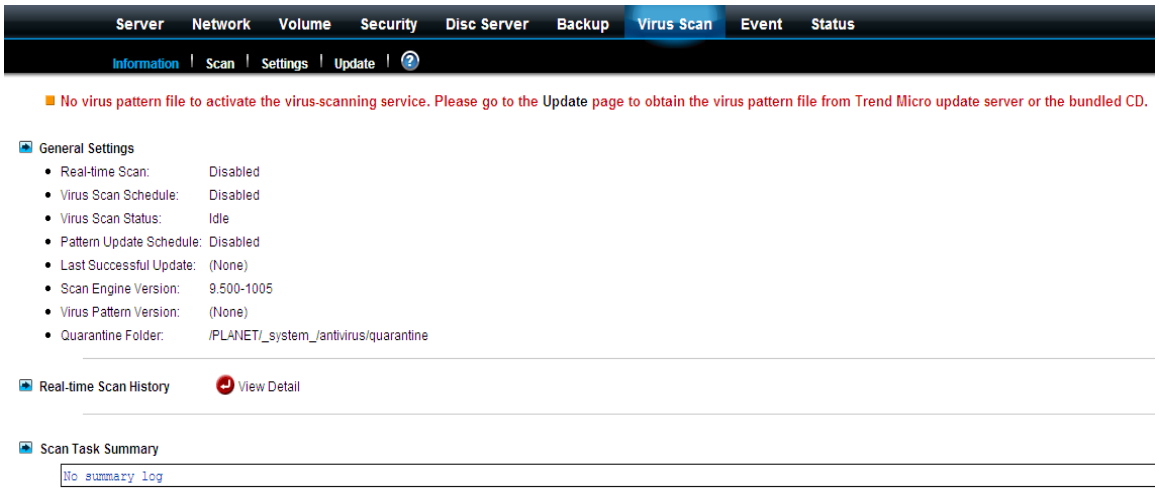
Note

1. This function doesn't support the Card Reader.
2. Do not support USB devices with more than 3 partitions.
3. Please un-mount the USB device before removing it or the data may be damaged.

Chapter 10. Virus Protection

Most storage systems are vulnerable to virus attacks. An infected file in you NAS server can be exchanged among the client systems in the network, resulting in corrupted data or causing productivity loss. The integrated Trend Micro antivirus software in NAS server is the best-of-breed security product that delivers the reliable antivirus protection to prevent virus from spreading before they get to you.

10.1 Information



The **Information** screen is the summary of the current antivirus settings. It gives you a comprehensive overview of the current status of antivirus general settings, real-time scans history and scan task summary of your NAS server. General settings display the present condition of the following items.

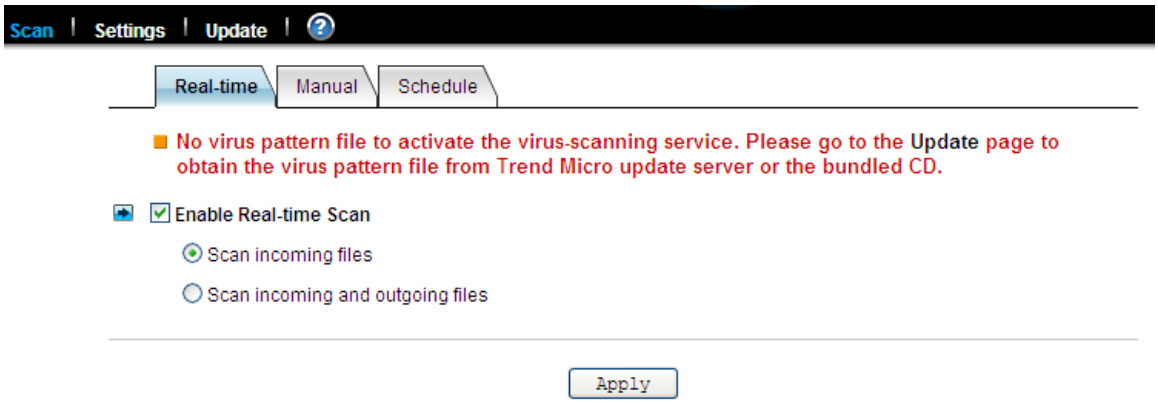
Item	Description
Real-time Scan	Display real-time scanning is either disabled or enabled.
Virus Scan Schedule	Display schedule virus scanning is either disabled or enabled.
Virus Scan Status	Display virus scanning is either idle or scanning.
Pattern Update Schedule	Display the status, schedule for the next virus pattern file update.
Last successful update	Display the date/time of the last successful virus pattern file update.
Scan engine version	Display the current scan engine version.
Virus pattern version	Display the current virus pattern file version

Quarantine Folder	Display the folder name and path where virus infected files are located and quarantine.

The real-time scan history displays the date and time where the virus is found. Action is then taken as to virus name and the full path name of the infected file. And, the scan task summary displays the start time of each manual or scheduled scan task.

10.2 Real-time, manual and schedule scanning

The embedded antivirus utility provides several options for virus protection, including real-time, manual and scheduled scanning to offer comprehensive antivirus and content security solutions for enterprise customers.



Note

1. Antivirus requires the system folder to operate. Please go to the **Server** → **Maintenance** page and specify the volume where the system folder resides.
2. For the first-time operation, please go to the **Virus Scan**→ **Update** page to obtain the most updated virus pattern file. Otherwise, the antivirus function cannot work.

Enabling real-time scanning

The real-time scanning function provides antivirus protection while users are reading or writing files to the NAS server.

1. Click the **Enable Real-time scan** checkbox to enable real-time scanning.

2. Select scan direction. Incoming files are those that are being stored in NAS server whereas outgoing files are copied or moved from NAS server to other location.

3. Click **Apply** to save the settings.

Configuring manual scanning

The manual and scheduled scanning function can scan any folders for infected files. The scan results will be listed as a scan task summary on the **Information** page.

1. Go to **Virus Scan**→ **Setting** page to configure the scan settings required. See “Configuring Scan Settings” on Section 11-3.

2. Click the **Manual** tab to go to the manual scanning page.

3. Click the **Select Folders** hyperlink to specify the folders you want to perform the manual scan.

4. Click **Apply** to save the settings.

Configuring schedule scanning

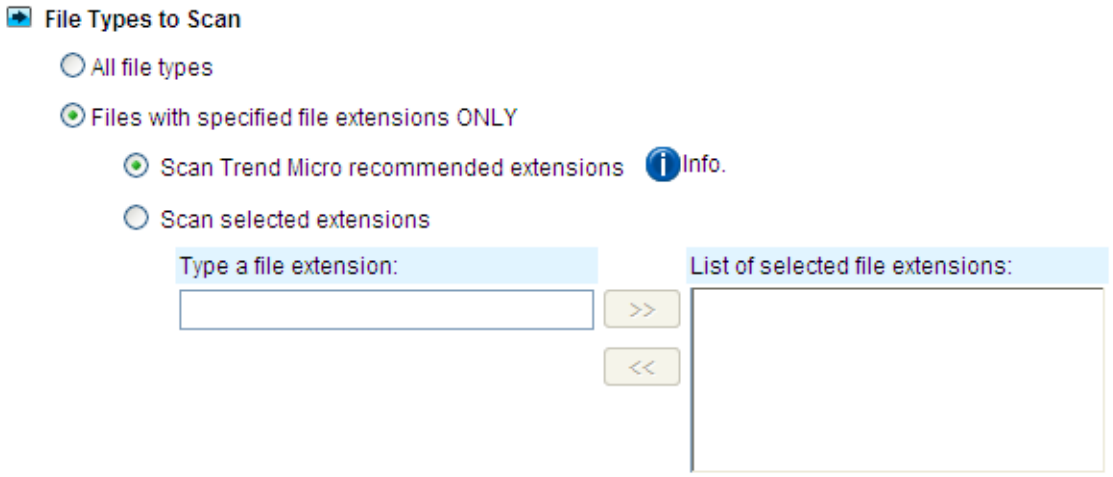
1. Click the **Enable Scheduled Scan for Infected Files** checkbox to enable scheduled scanning.

2. Click the **Select Folders** hyperlink to specify the folders you want to perform the scheduled scan.

3. Configure the start time and recurrence pattern for the scheduled scanning.

4. Click **Apply** to save the settings.

10.3 Configuring scan settings



All virus scan has two options that need to be configured.

Item	Description
File Type to Scan	You can limit scanning to specific file types.
Action When Virus Found	Three actions (quarantine, clean, delete) can be chosen from when virus is found.

File types to scan

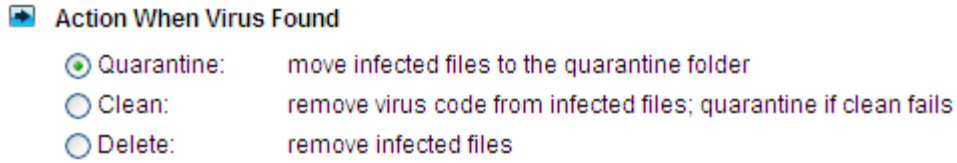
1. Click the desire scan file type.

2. If **all file types** is selected, all files regardless its file extension will be scanned.

3. If **Files with specified file extensions only** is selected, specify using the extensions recommended by Trend Micro or specify the file extension manually.

4. Note that the maximum scanning layer of a compressed file is set to 2 layers for all real-time manual and scheduled scan

Actions when virus found



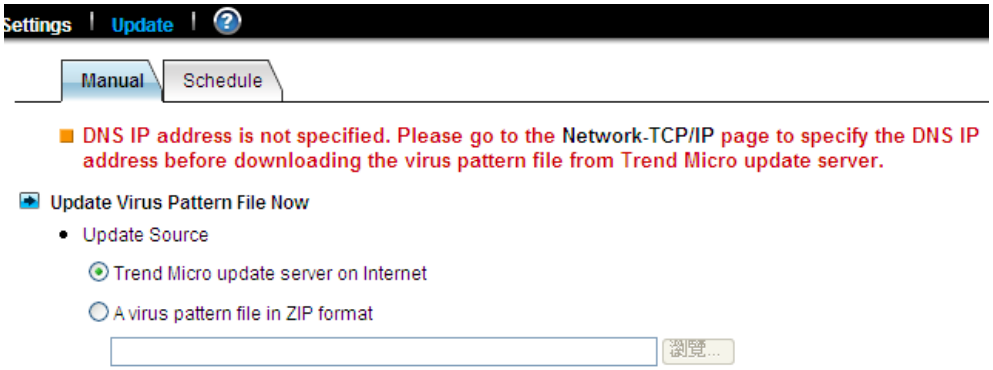
1. Click the desired action when virus is found.

2. Click **Apply** to save the settings.

10.4 Updating virus pattern file

Virus pattern update can be performed either manually or according to the schedule. It is required to perform a manual update immediately when the antivirus function is activated for the first time.

Configuring a manual update

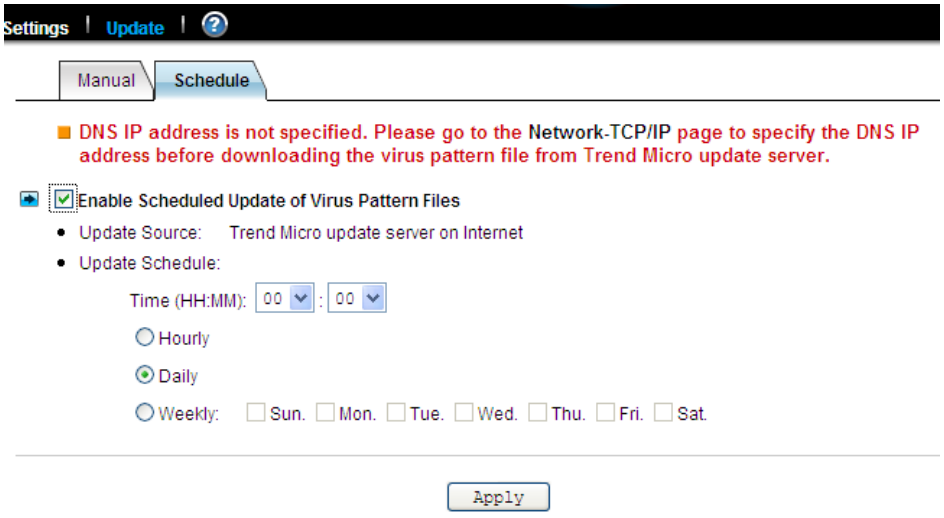


1. To download virus patterns from Internet, select **Trend Micro update server on internet**. Please note that you have to specify the DNS server IP address on the **Network→TCP/IP** menu of the Administration Page.

2. Or, you can download the virus pattern file in ZIP format from Trend Micro's website – http://www.trendmicro.com manually. Select **a virus pattern file in ZIP format** here and specify the location of the virus pattern file.

3. Click **Apply** to save the settings.

Configuring a scheduled update



1. Click the **Enable Scheduled Update of Virus Pattern Files** checkbox to enable scheduled update.

2. Configure the download schedule. Select the start time and recurrence pattern for the scheduled update.

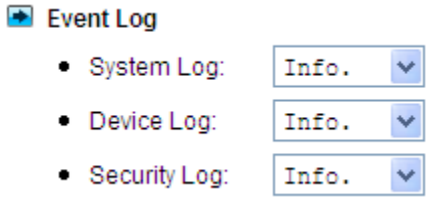
3. Click **Apply** to save the settings.

Chapter 11. Event Logs

This chapter covers the Event Notification. You can collect information about the system, hardware and security event of you NAS server.

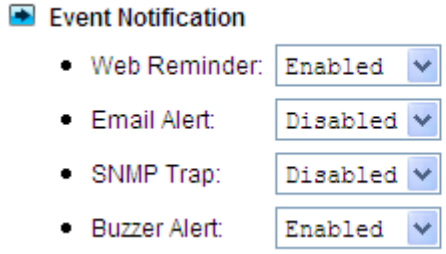
11.1 Event and Thermal settings

NAS server records three kinds of logs:



All the events are categorized into three levels: **Info**, **Warning** and **Error**. In **Event→Configuration** menu, you can configure the level of the logs. Use the **Advance** or **Basic** button to switch between the display of advance and basic information. The **Advance** view shows all the information in the Basic view plus additional event notification setting that may be of interest to the more advanced user. Various notification methods are provided by NAS server to ensure non-stop operation and data integrity:

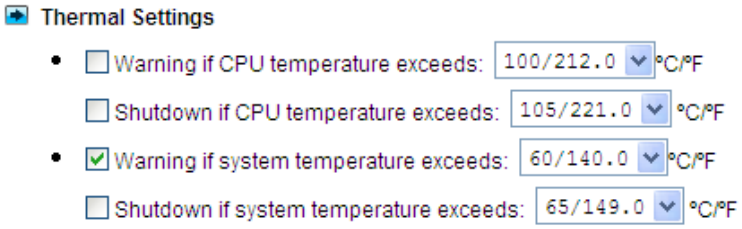
- Warning level notification such as very low disk space is detected on volume; Hot spare disk is consumed and so on.
- Error level notification such as CPU fan failed; Volume is degraded or faulty and so on.



Item	Description
Web Reminder	Provides instant notification in the administration homepage.
Email Alert	Provides notification via email.
SNMP Trap	Sends SNMP trap to the Network Manager System (NMS) such as HP Open View.
Buzzer Alert	An audio sound will goes off from the built-in buzzer in NAS system when event occurs. To turn off the buzzing sound, click the **Mute Buzzer** icon on the Administration Page. You can configure what kind of events should initiate the notification process in **Event→Configuration→Advance** menu.

Thermal settings

User can also define the thermal scheme of the NAS server so that NAS server can give off warning message or shutting down when the system or CPU temperature is over a predefined threshold temperature.



Configuring thermal settings:

1. Go to **Thermal Settings** in **Event→Configuration** menu.

2. You can set the NAS server to give off warning message or shutdown base on the CPU or System temperature. Check the **Warning** and **Shutdown** checkboxes and select the proper temperature from the pull down menu.

3. Click **Advance** button to configure the way of notification for various events.

4. Click **Apply** to save the setting.

The system and CPU fan would start to work over 25℃.

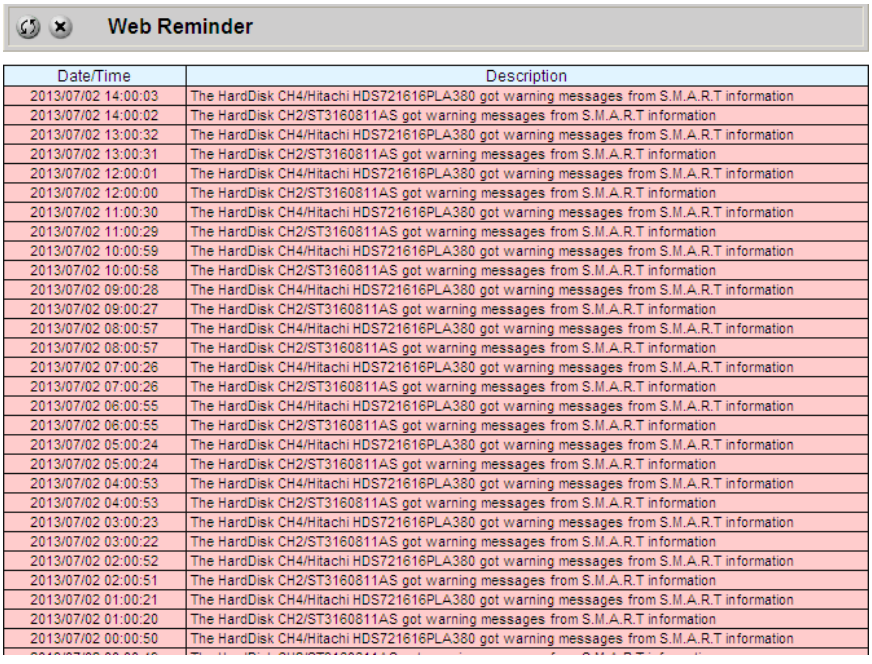
11.2 Checking the event logs

You can view a summary of all the events occurred on your

NAS server: **Web Reminder**, **System Log**, **Device Log** & **Security Log**. The severity of each event will be determined by NAS server and displayed in different colors:

Information = Green Warning = Yellow Error = Red

Viewing web reminder

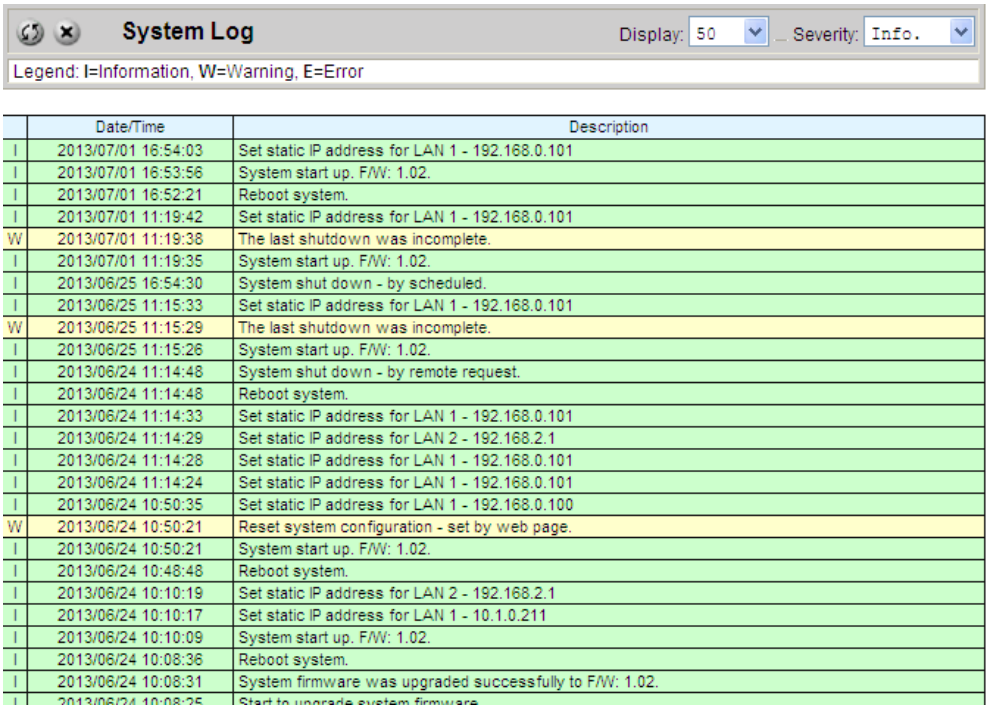


Date/Time	Description
2013/07/02 14:00:03	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 14:00:02	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 13:00:32	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 13:00:31	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 12:00:01	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 12:00:00	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 11:00:30	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 11:00:29	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 10:00:59	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 10:00:58	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 09:00:28	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 09:00:27	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 08:00:57	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 08:00:57	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 07:00:26	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 07:00:26	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 06:00:55	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 06:00:55	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 05:00:24	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 05:00:24	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 04:00:53	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 04:00:53	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 03:00:23	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 03:00:22	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 02:00:52	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 02:00:51	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 01:00:21	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
2013/07/02 01:00:20	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
2013/07/02 00:00:50	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information

Web Reminder is the warning message that appear at the first screen of the administrator home page to alert administrator that one or multiple critical events of your NAS server has been found. Administrator can, therefore be aware of the status of the NAS server immediately when entering the administrator home page. Click the hyper-link of the Web Reminder message and it will directly lead you to the Web Reminder summary menu.

Go to **Event→Web Reminder** menu to see a summary of all the critical events occurred on your NAS server.

Viewing system log



	Date/Time	Description
I	2013/07/01 16:54:03	Set static IP address for LAN 1 - 192.168.0.101
I	2013/07/01 16:53:56	System start up. F/W: 1.02.
I	2013/07/01 16:52:21	Reboot system.
I	2013/07/01 11:19:42	Set static IP address for LAN 1 - 192.168.0.101
W	2013/07/01 11:19:38	The last shutdown was incomplete.
I	2013/07/01 11:19:35	System start up. F/W: 1.02.
I	2013/06/25 16:54:30	System shut down - by scheduled.
I	2013/06/25 11:15:33	Set static IP address for LAN 1 - 192.168.0.101
W	2013/06/25 11:15:29	The last shutdown was incomplete.
I	2013/06/25 11:15:26	System start up. F/W: 1.02.
I	2013/06/24 11:14:48	System shut down - by remote request.
I	2013/06/24 11:14:48	Reboot system.
I	2013/06/24 11:14:33	Set static IP address for LAN 1 - 192.168.0.101
I	2013/06/24 11:14:29	Set static IP address for LAN 2 - 192.168.2.1
I	2013/06/24 11:14:28	Set static IP address for LAN 1 - 192.168.0.101
I	2013/06/24 11:14:24	Set static IP address for LAN 1 - 192.168.0.101
I	2013/06/24 10:50:35	Set static IP address for LAN 1 - 192.168.0.100
W	2013/06/24 10:50:21	Reset system configuration - set by web page.
I	2013/06/24 10:50:21	System start up. F/W: 1.02.
I	2013/06/24 10:48:48	Reboot system.
I	2013/06/24 10:10:19	Set static IP address for LAN 2 - 192.168.2.1
I	2013/06/24 10:10:17	Set static IP address for LAN 1 - 10.1.0.211
I	2013/06/24 10:10:09	System start up. F/W: 1.02.
I	2013/06/24 10:08:36	Reboot system.
I	2013/06/24 10:08:31	System firmware was upgraded successfully to F/W: 1.02.
I	2013/06/24 10:08:25	Start to upgrade system firmware.

In the **Event→System Log** menu, you can:

1. Select the number of most recent events show on a screen.

2. Select the severity level for the events you want to see.

3. Click **Refresh** button to refresh the screen.

4. Click **Clear** button to clear the log.

Viewing device log

	Date/Time	Description
W	2013/07/02 15:00:33	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
W	2013/07/02 15:00:33	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
W	2013/07/02 14:00:03	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
W	2013/07/02 14:00:02	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
W	2013/07/02 13:00:32	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
W	2013/07/02 13:00:31	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
W	2013/07/02 12:00:01	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
W	2013/07/02 12:00:00	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
I	2013/07/02 11:26:53	USB_CLT:sync complete successfully - backup to: server 192.168.0.101
I	2013/07/02 11:26:53	USB_CLT:sync complete successfully - backup from: client 192.168.0.101
I	2013/07/02 11:26:26	USB_CLT:sync start - backup from: client 192.168.0.101
I	2013/07/02 11:26:26	USB_CLT:sync start - backup to: server 192.168.0.101
I	2013/07/02 11:20:34	Mount volume successfully - usb_disk_3-1,USB,Ready
W	2013/07/02 11:00:30	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
W	2013/07/02 11:00:29	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
I	2013/07/02 10:07:38	The archive folder was set successfully - /PLANET/_archive_.
I	2013/07/02 10:07:38	/PLANET/_archive_: Disc image folder was created or assigned.
I	2013/07/02 10:05:30	CD01: The CD function was changed to Loader/Writer.
W	2013/07/02 10:00:59	The HardDisk CH4/Hitachi HDS721616PLA380 got warning messages from S.M.A.R.T information
W	2013/07/02 10:00:58	The HardDisk CH2/ST3160811AS got warning messages from S.M.A.R.T information
I	2013/07/02 09:48:27	CD01: The CD function was changed to Disc Mirroring.
I	2013/07/02 09:47:55	CD01: The CD function was changed to Loader/Writer.
I	2013/07/02 09:46:57	CD01: The CD function was changed to Direct Access.
I	2013/07/02 09:27:20	CD01: Disc caching completed successfully.
I	2013/07/02 09:26:07	CD01: Start disc caching - IP CAM to /PLANET/_discs_.
I	2013/07/02 09:23:00	CD01: The CD function was changed to Disc Mirroring.
I	2013/07/02 09:22:29	CD01: The CD function was changed to Loader/Writer.

In the **Event→Device Log** menu, you can:

1. Select the number of most recent events show on a screen.
2. Select the severity level for the events you want to see.
3. Click **Refresh** button to refresh the screen.
4. Click **Clear** button to clear the log.

Viewing security log

In the **Event→Security Log** menu, you can:

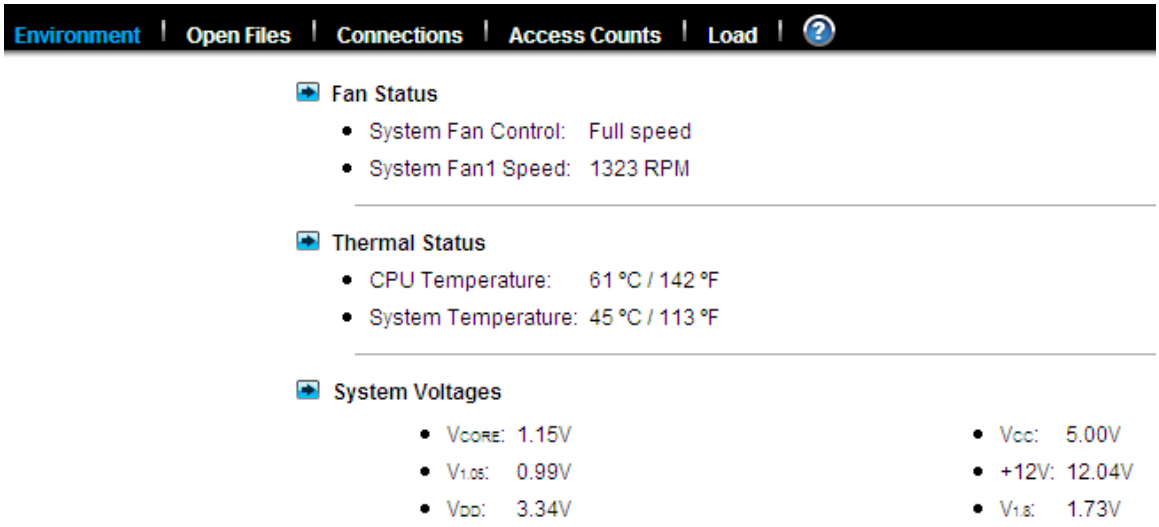
1. Select the number of most recent events shown on a screen.
2. Select the severity level for the events you want to see.
3. Click **Refresh** button to refresh the screen.
4. Click **Clear** button to clear the log.
5. Select the protocols and click the **Refresh** button to show the corresponding events. **Default** event represent general security event of your NAS server that is not related to any protocols.

Chapter 12. System Status

This chapter covers the System Status pages. You can collect information about the system, hardware and security event of your NAS server.

12.1 Viewing system status

System Status displays a comprehensive view of the system fan status, thermal status and system voltage. You can use this information to quickly find out the problem of your NAS server and take appropriate action. On **Status→Environment** page, you can monitor the CPU fan status, CPU and System temperature plus the System Voltages. Click **Refresh** to obtain the latest figure.



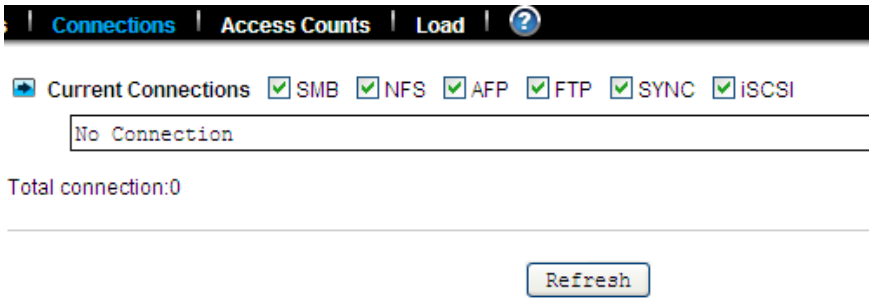
Viewing the open files

In **Status→Open Files** menu, it provides the following information about all the open files on NAS server:

Item	Description
R/W	Read/write privileges of the opened file.
User	The name of the user who has opened the file.
Protocol	The protocol used for the network connection: SMB, NFS, AFP or FTP.

File Name	Lists the name and path of the opened file.

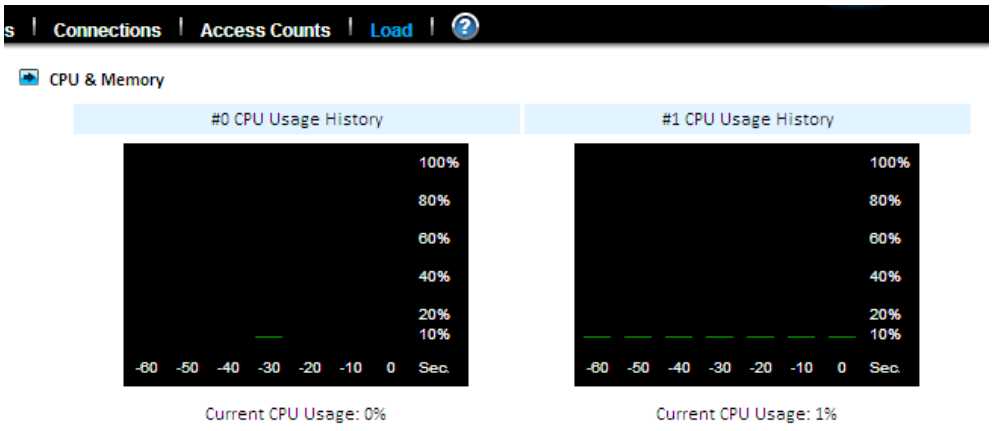
Viewing the active connections



In the **Status→Connections**:

Item	Description
Current Connections	Configure and show the protocol used by the client that is currently connecting to the NAS server by clicking the check box beside the protocol you want to show on the list.
User	The name of the user who has connected to NAS server.
Computer	The computer name of the client connecting to the NAS server.
Address	The IP address of the client connecting to the NAS server.
Protocol	The protocol used for the network connection: SMB, NFS, Sync, AFP or FTP.
Connected Time	The date / time that the connection is established.
Open Files	Total number of the opened files.
Disconnect	Disconnect a particular connection by checking the disconnect check box and click the icon.

Viewing the system load

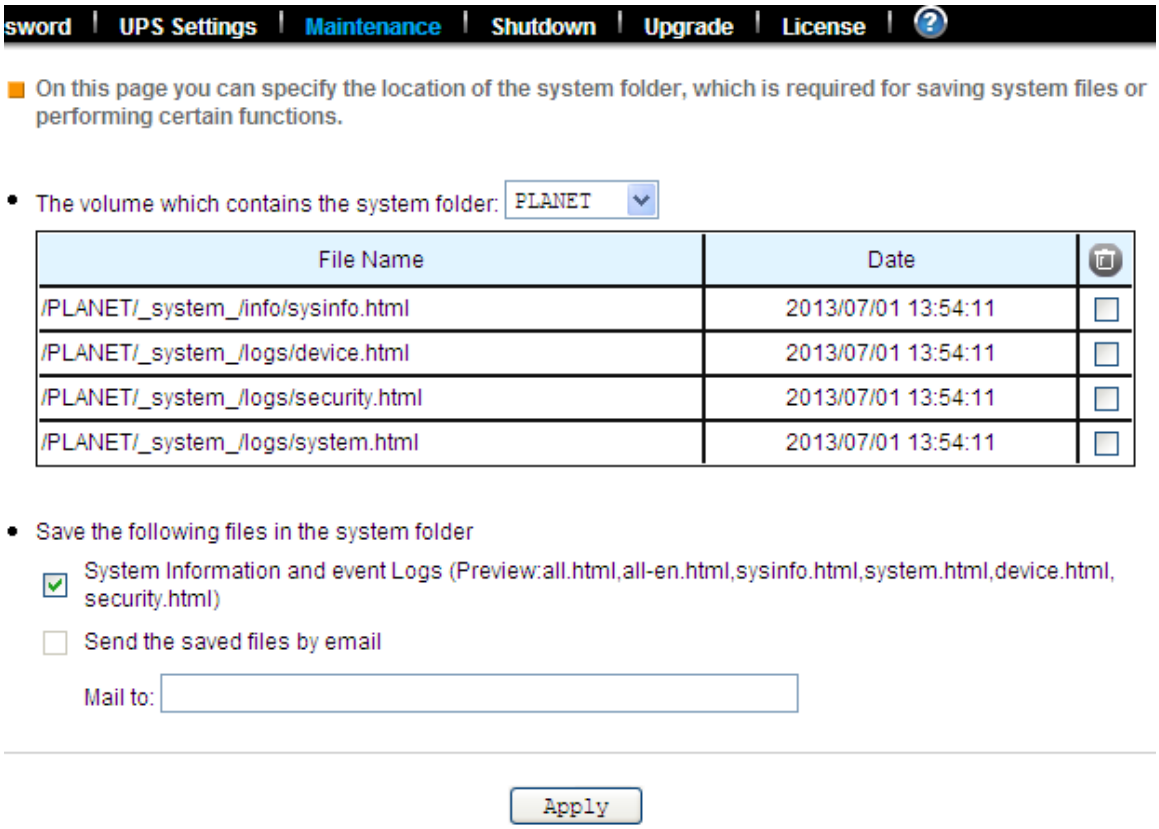


In the **Status→Load**:

Item	Description
CPU & Memory	You can see the CPU usage and memory usage here. Total memory and the current free memory are also shown here.
Network	The network throughput in percentage is showed on here.

12.2 Saving system settings and status as HTML files

For maintenance or technical support purpose, it is helpful and sometimes necessary to have an overview of all system settings, current system status and, even better, all event logs. It also helps a lot if a server itself can send out these files by email.



The NAS server does all the above within several mouse-clicks. First of all, you have to create a system folder, which is used for storing these files. The system folder is also required when performing SMB, permissions, DISC, and system profiles backup. To create the system folder, please open the **Administration Page** and go to the **Server→Maintenance** menu. On the menu page, select a volume to contain the system folder. And click **Apply** to create the system folder.

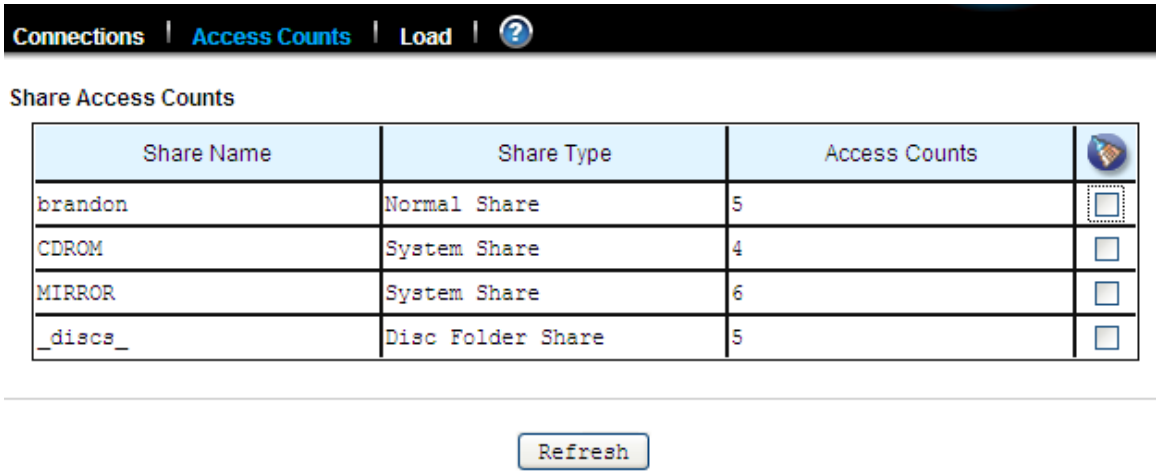
Once the system folder is created, you are able to save the system settings and event logs as HTML files. On the same page, choose the files to save and click the **Apply** button. Before saving the files, you can preview them by clicking the **Preview**:

Hyperlinks. Previewing will not create any files in the system folder.

After generating these files, you can see them appear in the table. Click any hyperlink to view the content of a file.

To email the saved files, choose the files to save and check the **Send the saved files by email** check-box. Enter the email address to send to. And click **Apply** to send them out by email, while saving copies in the system folder.

12.3 Share access counts



On the **Status→Access Counts** menu page it displays how many times the shares have been accessed. The count is added by one whenever a connection to the share is established by Windows clients, NFS clients, and MacOS clients.

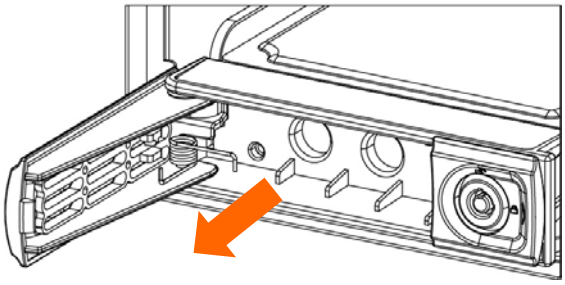
There are several share types.

Item	Description
Normal Share	Indicates a shared folder in any data volume.
System Share	Indicates the MIRROR share which holds all CD/DVD volumes.
Disc Share	Indicates a share of a single CD/DVD volume.
Group Share	Indicates a share of grouping of several CD/DVD volumes.
Disc Folder Share	Indicates a share of disc image folder.

Appendix A Hot-swapping

You may have to change hard disks in some situations, such as hard disk failure, degraded RAID, Critical RAID or general maintenance. The NAS server supports HDD hot-swapping. Below are the instructions of replacing hard disks when using the HDD module.

1. Identify which hard disk fails. The amber LED of the HDD tray will blink to indicate hard disk failure.



2. Unplug the HDD tray and replace the HDD with a good one.

3. Plug in the HDD tray. Wait until the Green LED is steady on.

Then you are done.

When a RAID volume is degraded and there is no available hot-spare disk for rebuilding, the RAID volume will stay in the degraded state. In this state, you can hot-unplug the failed hard disk and plug in a good one in the same HDD tray. The RAID volume will rebuild automatically with the new hard disk.

Appendix B Utility for NAS system

NAS Finder is powerful software that discovers and administers NAS Servers on the network, and remotely loads disc images into the NAS Server. You can either duplicate a whole CD or build an image from a group of files. Sharing and publishing data are never been so easy.

Use NAS Finder to display and modify the setting you have created. You can also perform server settings replication from a configured server to other NAS Servers on the network. Server parameters of a NAS Server can be imported into other NAS Server to avoid tedious setup process to each individual unit on the network.

Features:

Server Management

- Discovers all NAS Servers on the network
- Configures NAS Servers for the first-time setup or quick setup
- Export / Import NAS Servers system settings Creating CD Images Remotely -
- Remotely loads CD images from a local CD-ROM drive into a NAS Server
- Collect and duplicates files into NAS Servers as a single CD image
- Allows users to assign 6 different destination servers when building CD images
- Fully integrates the CD-R function of the NAS Server
- Supports up to 16 different tasks User Interface -
- Explorer-like user interface together with user friendly wizards
- Task Manager monitors all on-going and scheduled tasks

System Requirement

- IBM PC or compatible with 80486 processor or higher
- At least 8 MB of free memory (16 MB is recommended)
- Minimum 5MB of free hard disk space
- VGA or higher resolution monitor
- Microsoft Windows 95/98/98SE/ME, Windows NT/2000/XP

Installing TCP/IP Protocol for Microsoft Networks

NAS Finder communicates with NAS Servers through the TCP/IP protocol. You must install “Client for Microsoft Networks” and the “TCP/IP” protocol in Windows to use NAS Finder.

Installing NAS Finder

You are ready to install this utility if the TCP/IP protocol is installed in your computer. To install NAS Finder, insert the Utility CD into the CD-ROM drive. On the auto-run interface, click “Install NAS Finder”. If the auto-run interface does not appear, go to X:\NAS Finder and run” NAS Finder.exe”, where X is the drive letter of the CD-ROM drive.

Follow the instructions in the setup wizard to install NAS Finder. It will create shortcuts on Desktop and in the Programs folder of the Start me.

Discovering NAS system

When started, NAS Finder automatically discovers all the NAS systems on the network and displays a list of servers under the node Local Server. NAS Finder will automatically refresh the server list at a specified interval. The default interval is 10 minutes.

NAS Finder can also locate NAS servers by IP addresses. It is useful when NAS servers are on the Internet or located in different network segments from the NAS Finder. To locate NAS servers by IP addresses, select “Remote NAS List” from the “File” menu. Click the “Add” button and enter the IP address of the NAS server.

To set the automatic refresh interval

1. Go to “Tool → NAS Finder Options” menu.
2. Enter a number between 1 to 60 minutes.
3. Click “OK”.

Server Quick Setup Using NAS Finder

You can perform initial setup for your NAS system using NAS Finder.

1. Click the  button on the toolbar.
2. Or, go to “Server -> Server Quick Setup”.
3. Select a NAS Server from the server list and click “Next” button.
4. Choose the “Network Teaming Mode” from the pull down menu. If you are not clear about this feature, continue with the default value. (Refer to Chapter 4.2 TCP/IP Settings)
5. If you want the IP settings to be assigned automatically, click “Obtain IP settings automatically”.
6. Or, you can specify the IP settings manually.
7. Click “Next” button to go to the next page.
8. Enter the “Server Name, Server Comment”, and “Workgroup/Domain Name” and select either the “Workgroup mode” or “Domain mode”. Note that this is the server name as it appears on the network which is irrelevant to the network protocol used.
9. Click “Next” button to go to the next page.
10. Change the admin password if necessary. Click the “OK” button to save the settings. Note that server may need to reboot for certain parameters changes to take effect.

Importing and Exporting System Settings

This section describes how to export the system settings of a NAS Server into a file. This file can be read into another NAS Server on the network by using the import feature. “Import System Settings” and “Export System Settings” form a combined process of replicate system settings from one configured NAS Server to another NAS Server.

To export system settings of a NAS Server

1. Highlight the server from the server list.
2. Right click the server and select “Export System Settings”.
3. Or, go to “Server -> Export System Settings” menu.
4. You will prompt for the administrator password to proceed.
5. Select a location where you want to save and specify the name of the export file.
6. Click “Save”.

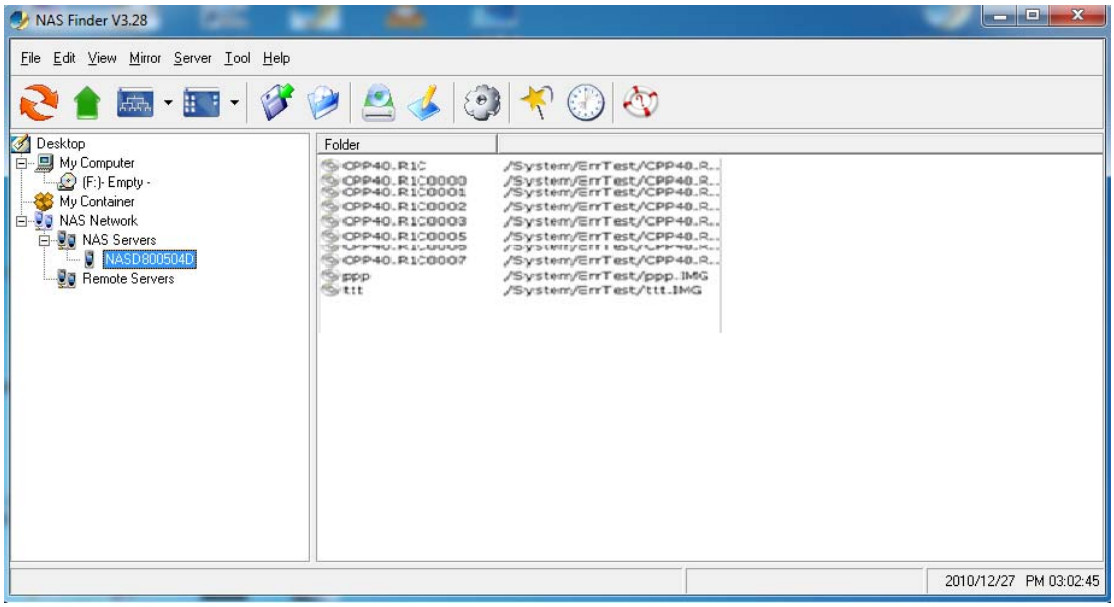
To import system settings into NAS Servers

1. Right click any NAS Server and select “Import System Settings”
2. Or, go to “Server -> Import System Settings” menu.
3. You will prompt for the administrator password to proceed.
4. You have the option to select a server or an export file as the source.
5. Click “Next”.
6. Select the type of system settings you want to import into the target server. The detail content of the system settings are displayed in the preview text box beside each selection.
7. Click “OK”. NAS Server will reboot automatically.

Browsing and Administering Servers

Browsing Servers

Below is the main window of NAS Finder. Upon execution, NAS Finder brings up Windows Explorer for you to drag and drop files into My Container for later image building. You can disable this option by choosing “Tool->NAS Finder Options” and un-checking the option - “Open Windows Explorer when NAS Finder starts”.



The main window consists of a file menu, a tool bar, a tree view pane on the left, a list view pane on the right and a status bar on the bottom.

Listed on the tree view pane are all the NAS Servers found by the NAS Finder on the network. Also included is “My Computer” as the one in Windows Explorer. “My Container” keeps information of the files/folders that can be built as a CD image in a NAS Server using the “Build Image” function. If you click on any item on the tree view pane, its content will be displayed in the list view pane.

The status bar indicates NAS Finder status and information. On the left side of the status bar shows function hint or item properties. On the right it displays the PC date and time.
You can browse the Domain Name, IP Addresses of each NAS Server just with a click of the mouse.

Note	If a NAS Server is protected by the admin password, you have to enter the password to set up or write to the server.

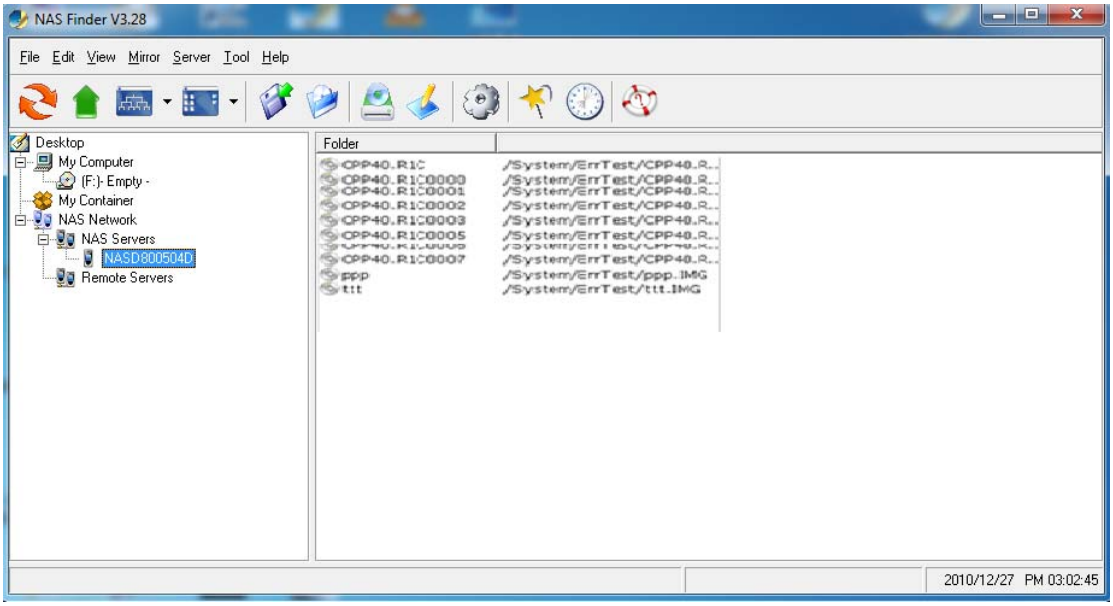
The following are some icon representations:

Item	Description
	**NAS Network**: display all the NAS Servers found on the LAN.

	**NAS Server**: represents a NAS Server
	**Disc Image Folder**: contains disc images of the NAS Server. You can double click to view its content.
	**Disc Image**: represents a mirrored CD/DVD image.

The following are some examples of browsing the servers.

Example 1. Content of a disc image folder



It displays all the disc images, path name, size, status and file system.

Tool Bar Functions

The tool-bar provides an easy access to the main functions of NAS Finder. The following explains what the tool-bar icons represent.

Item	Description
	**Refresh:** manually updates the directory content of My Computer or NAS Network.
	**Up Directory:** moves the cursor one level up.

	**Tree View Mode:** expands or shrinks the directory tree in the tree view pane (to the left).
	**List View Mode:** changes the view mode of items in the list view pane (to the right).
	**Save Container:** saves data in My Container into a container file.
	**Load Container:** loads a container file into My Container.
	**Mirror CD:** starts the “Mirror CD” wizard for duplicating CD images into the NAS Server.
	**Build Image:** starts the “Build Image” wizard to build a CD image from My Container into a NAS Server.
	**Server Quick Setup:** configures some fundamental parameters of a selected NAS Server. You can configure an un-initialized or initialized server.
	**Wizard:** brings up a wizard for access to major functions: “Mirror CD”, “Build Image” and “Server Quick Setup”.
	**Task Manager:** opens a task manager window which displays and controls all ongoing and scheduled tasks.
	**Help:** opens the Help window for display help information.

Mirroring CD/DVD Remotely

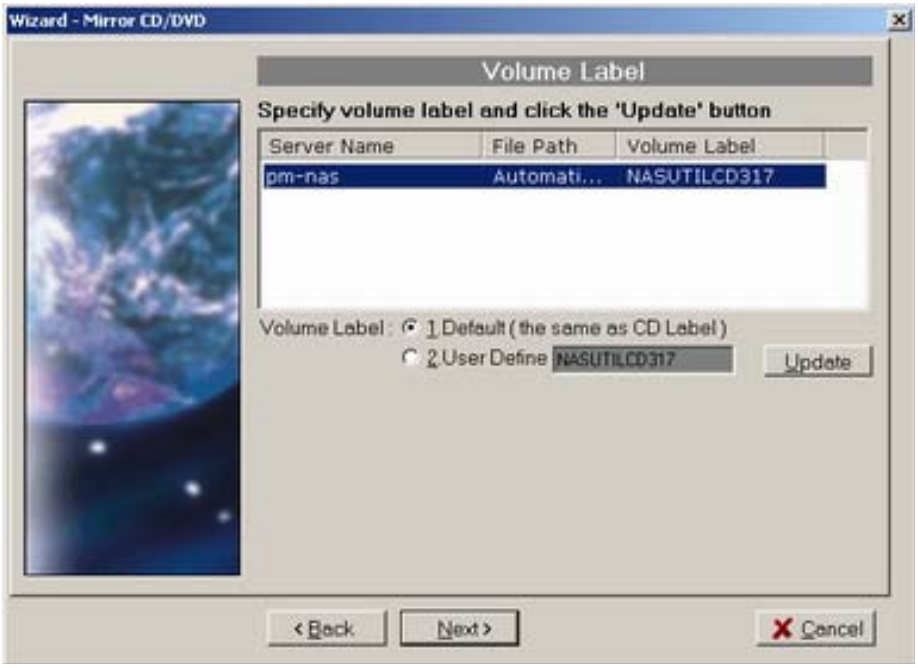
This chapter describes how to copy a CD from a PC CD-ROM drive to a NAS Server. Please follow the steps below.

1. To mirror a CD or a DVD remotely into a NAS Server, first click the  “Mirror CD” icon on the tool-bar. It invokes the “Mirror CD” wizard as shown below. Select a PC CDROM drive as the source. Press “Next” to continue.

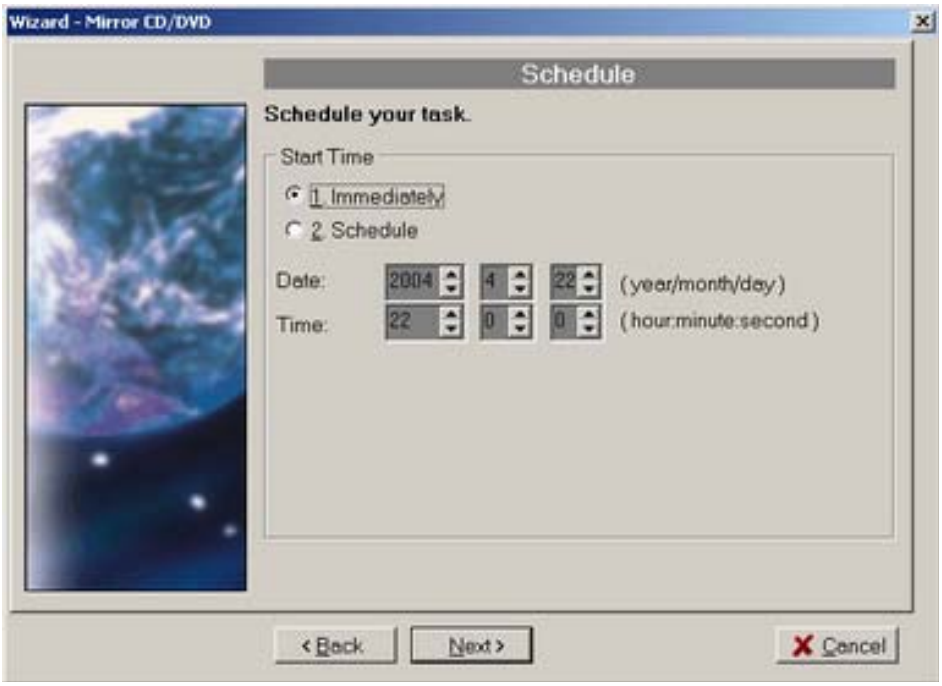
2. Choose one or more servers as the destination. Select a server in the “Target & File Path” list-box, select “Smart” mode for redundancy check of the CD image or select “Force” mode to allow a second copy of the same CD image.

   Then, click the >> button. You can see the task being added to the right-hand pane. Click the “Next” button to go to next page.

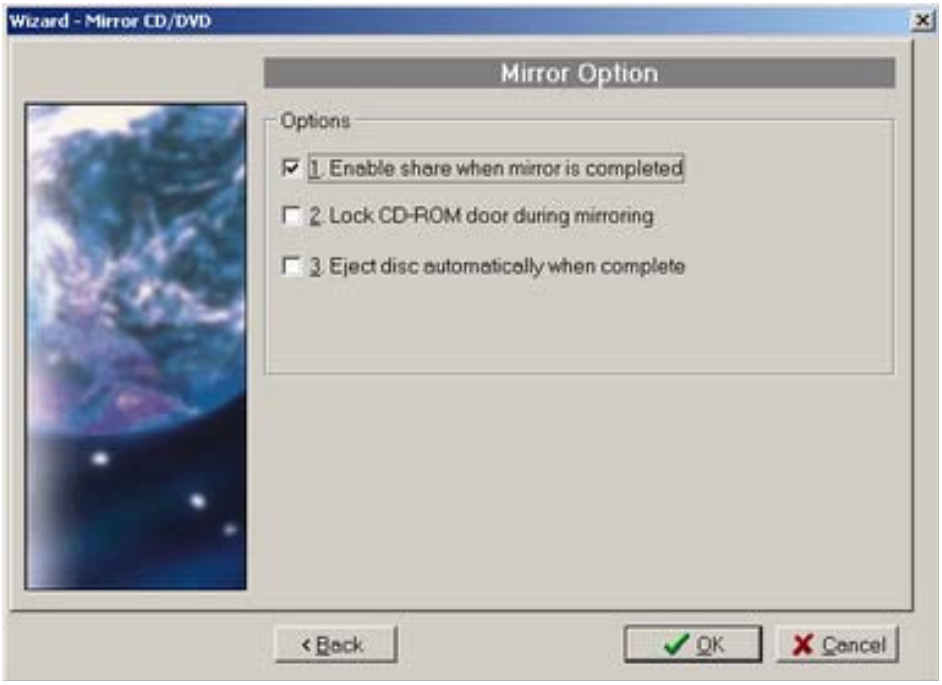
3. Change the volume label of the CD/DVD image if necessary. If you want to change the volume label, click “2” -- User Define -- and enter the volume label in the input-box. Then click the “Update” button. Click the “Next” button afterwards.



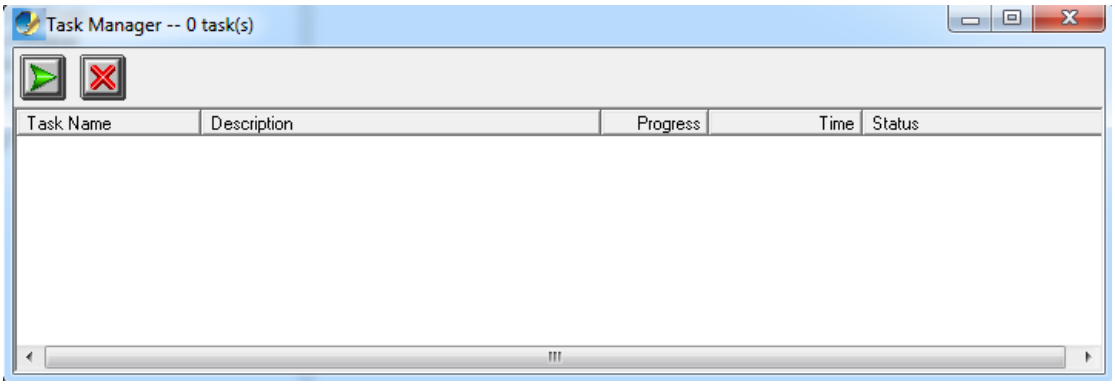
4. Specify the date/time to run the task. Then press “Next”.



5. Set the Mirror CD options if necessary.



6. Click “OK” to start the task. The Task Manager will show the progress.

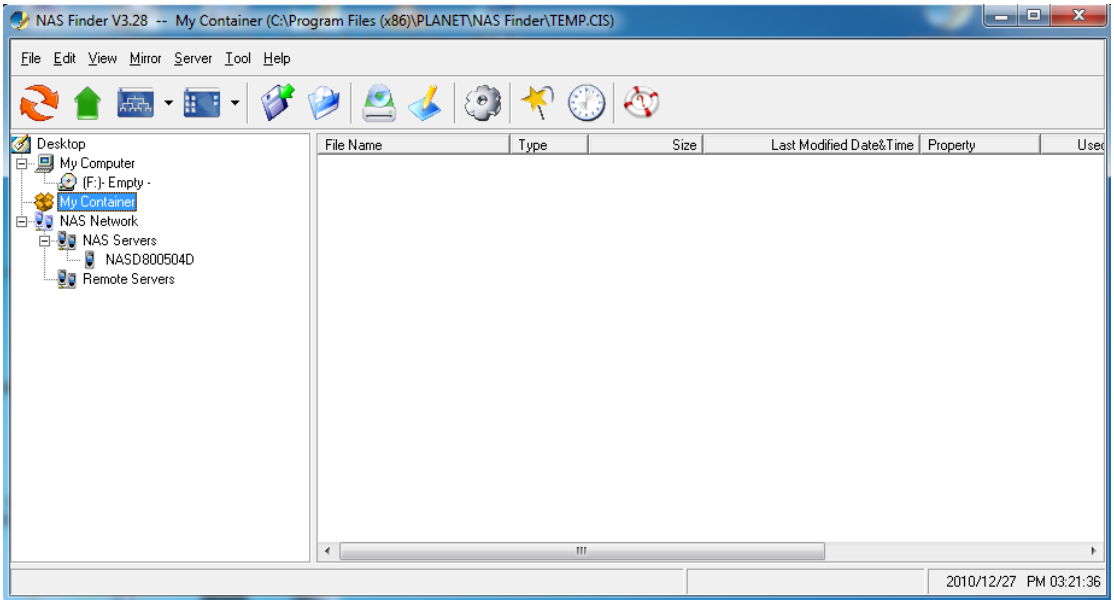


Archiving Files as a CD/DVD Image

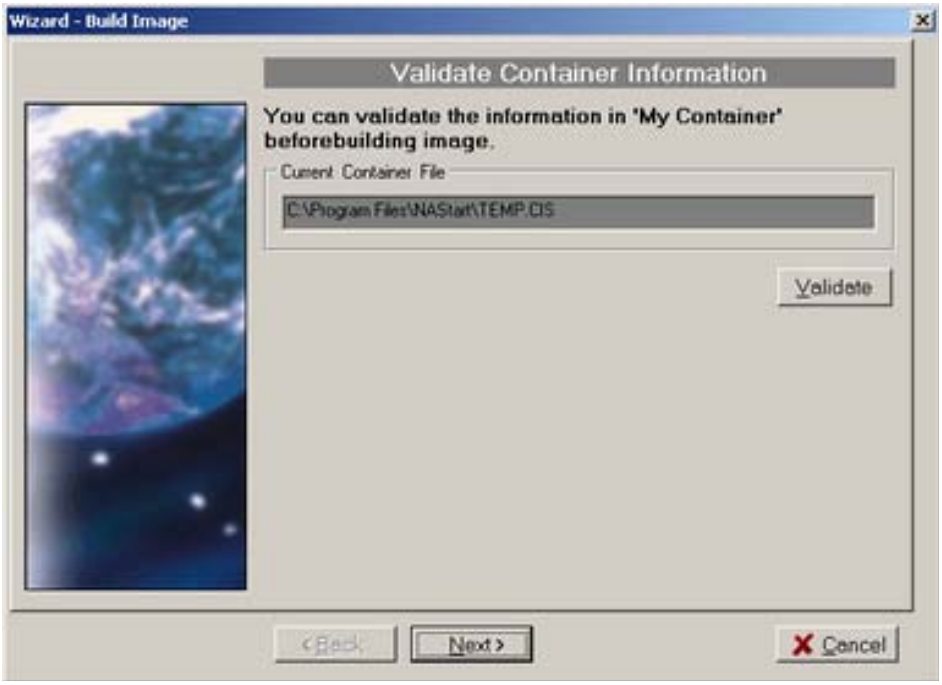
This chapter describes how to build CD image from “My Container” into a NAS Server. Please follow the steps below.

1. The first thing to build a CD/DVD image is to collect files.

   Open Windows Explorer and drag & drop files into My Container.

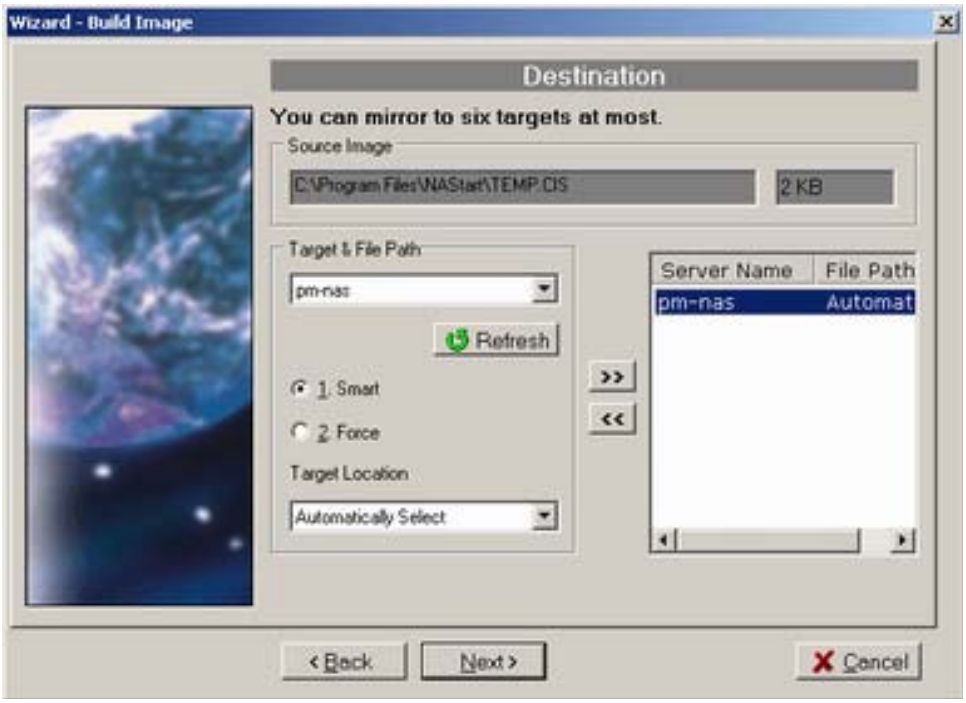


2. Click the  "Build Image" icon on the tool-bar to bring up the "Build Image" wizard. You can click the "Validate" button to check if the file/folder information in My Container is correct. If not, you can choose to update My Container.

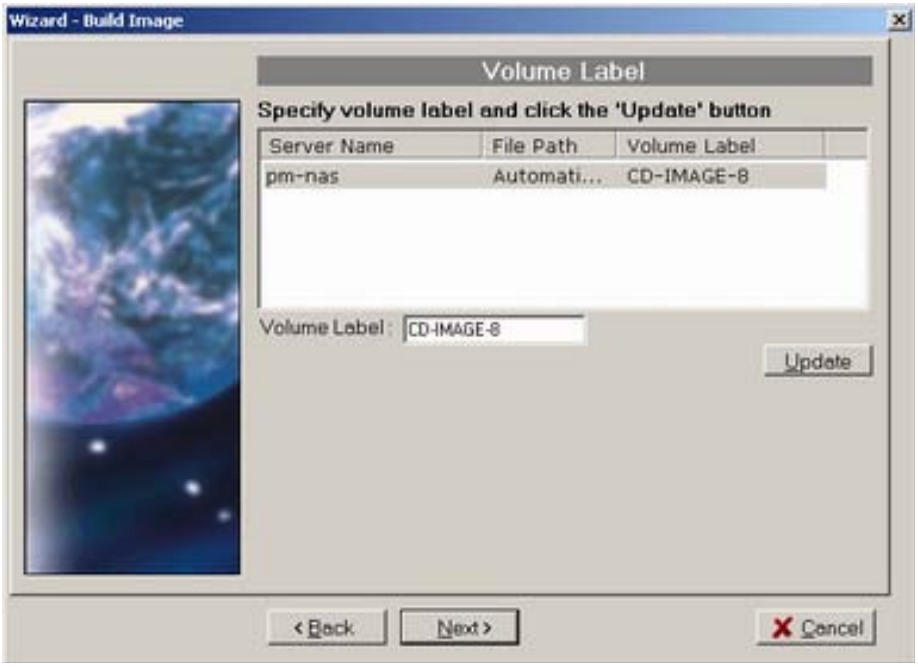


3. Choose one or more servers as the destination. Select a server in the "Target & File Path" list-box, select Smart mode for redundancy check of the CD image or select Force mode to allow a second copy of the same CD image. Then, click the >> button. You can see the task

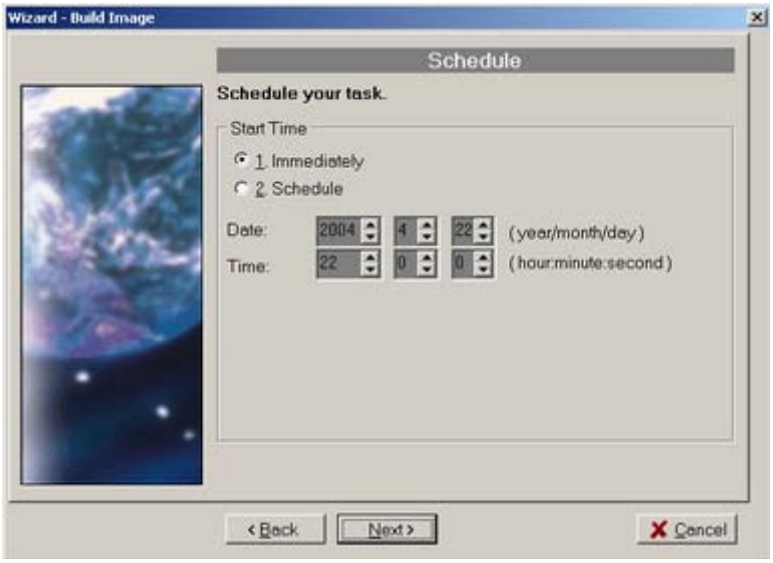
being added to the right-hand pane. Click the “Next” button to go to next page.



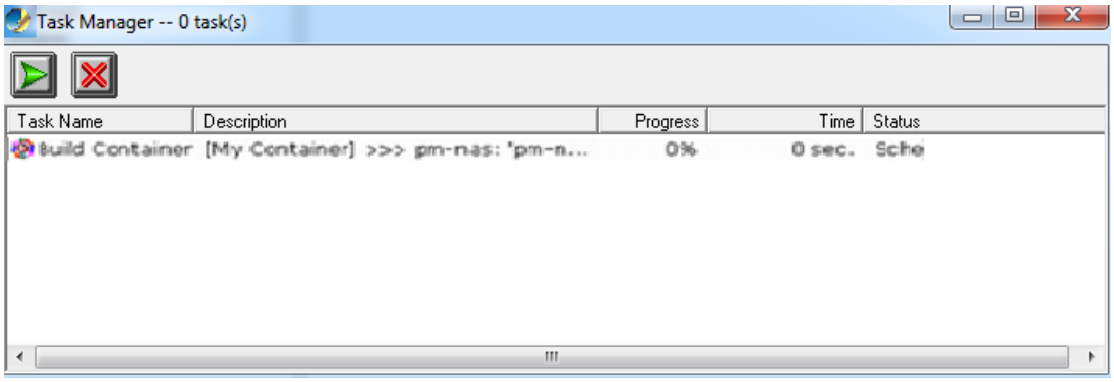
4. Name the CD/DVD image to be created. Enter the name in the “Volume label” input-box and click the “Update” button. Press “Next” afterwards.



5. Specify the date/time to run the task. Then press “OK”.



6. The Task Manager will show the progress.



Burning Disc Images
If the NAS server is equipped with CD or DVD writer, it can burn any existing disc image in it. Select a NAS server from the “NAS Servers” tree view pane of the NAS Finder main window. Select a disc image in the NAS server and right-click on it. Select “Record CD/DVD” from the right-click menu. Specify the parameters in the wizard and click the “Add CD-R Option” button. Click “Next” to continue. On the next page, specify the launch schedule and click “OK”.

Supported CD Formats
The “Mirror CD” function copies CD or DVD discs from a PC CD/DVD drive into a NAS Server. Below is a list of the supported CD formats that can be mirrored remotely.

- ISO 9660 level 1, 2, 3 (including Romeo, Joliet and Rock-Ridge extension)
- CD HFS
- CD/DVD UDF
- High Sierra
- Hybrid (ISO+HFS)
- Multi-session CD
- Mixed Mode CD
- DF V1.5, V2.0

Appendix C Troubleshooting & Frequently Asked Questions

<table>
<tr><th colspan="2">Features</th></tr>
<tr><td>What is NAS?</td><td>NAS is a term used to refer to storage elements that connect to a network and provide file access services to computer systems. A NAS storage element consists of an engine, which implements the file services, and one or more devices on which data is stored. NAS may be attached to any type of network.</td></tr>
<tr><td>What is the difference between NAS and SAN?</td><td>
<table>
<tr><th>NAS</th><th>SAN</th></tr>
<tr><td>Cost is lower</td><td>Cost is higher</td></tr>
<tr><td>Data typically is accessed by clients</td><td>Data typically is accessed by servers</td></tr>
<tr><td>File system resides in NAS</td><td>File system resides in server</td></tr>
<tr><td>For small business and workgroup</td><td>For large enterprise</td></tr>
<tr><td>Providing file-based data accessing</td><td>Providing block-based data transfer</td></tr>
<tr><td>Using standard file sharing protocol</td><td>Using encapsulated SCSI protocol</td></tr>
</table>
</td></tr>
<tr><td>How many nodes of ACL can be applicable in the NAS-7410?</td><td>NAS-7410 provides 10,239 nodes for ACL setting access control of client.</td></tr>
<tr><th colspan="2">Hardware Installation</th></tr>
<tr><td>Is the OS of NAS-7410 stored in the hard disk drive?</td><td>No, OS of NAS-7410 is not stored in hard disk drive. Instead, OS and system configuration information of NAS-7410 are stored in the CF Card.</td></tr>
<tr><td>Is there any storage management function provided for NAS-7410?</td><td>RAID management, disk quota and scan disk are management functions provided for NAS-7410.</td></tr>
<tr><td>How difficult is it to install a NAS-7410?</td><td>It only takes about 15 minutes to install NAS-7410 in the existing or start-up networking environments without any network downtime.</td></tr>
<tr><td>What benefits are available from the dual NIC?</td><td>The dual NIC in NAS-7410 can provide load-balance function to relieve network traffic. In addition, the dual NIC also provides the fail-over function to ensure consistent network connectivity.</td></tr>
<tr><th colspan="2">RAID Building</th></tr>
<tr><td>What RAID policy does NAS-7410 support?</td><td>NAS-7410 supports three RAID policies:
• RAID 0: Stripe/Span. (2 ~ 8 hard disk drives). It interleaves data</td></tr>
</table>

	across multiple disks for better performance. Safeguard function is not provided in RAID 0. • RAID 1: Mirror. (Multiplication of 2 hard disk drives). It provides 100% duplication of data into paired hard disks. This offers the highest reliability, but doubles the storage cost. • RAID 5: Striped with Rotating Parity (3 ~ 8 hard disk drives). Data is striped across three or more drives. Parity bits are used for fault tolerance. • RAID 6: RAID 6 (striped disks with dual parity) combines four or more disks in a way that protects data against loss of any two disks. • RAID 10: RAID 1+0 (or 10) is a mirrored data set (RAID 1) which is then striped (RAID 0), hence the "1+0" name. A RAID 1+0 array requires a minimum of four drives □V two mirrored drives to hold half of the striped data, plus another two mirrored for the other half of the data. In Linux, MD RAID 10 is a non-nested RAID type like RAID 1 that only requires a minimum of two drives and may give read performance on the level of RAID 0.
Can I use a different RAID type in NAS-7410 concurrently?	Yes. NAS-7410 provides the independent RAID group, which means you can group several different RAID groups at the same time in NAS-7410.
Generally RAID systems use either the hardware RAID controller or the software-only RAID system. Which one is used by NAS-7410?	NAS-7410 utilizes an innovative method of RAID management. It is hardware and software integrated solution, using a patent-pending technology for RAID management and access. This solution can provide more storage capacity while maintaining the RAID performance and improving RAID functionalities.
While creating RAID, must the hard disk drives installed in NAS-7410 be of the same brand and size?	Theoretically, the answer is negative. But for the performance concerns, the same brand drives will have the similar characteristics; it will help to maintain the overall performance especially on exchanging data. To have an optimized capacity of a RAID group, the similar size (or even same size) hard disk drives will be recommended. For example, if you use one 10GB hard drive and a 60GB hard drive to create RAID 1, only 10GB will be the available storage space instead of 60GB. If you use two 60GB hard drives to create RAID 1 group, the available storage space will be 60GB. Performance wise, this is also a fact, the similar capacity hard drives will mostly have the identical RPM speed. If the RPM of hard drives is different with each other, they will interfere each other and affect the overall performance a lot.
Should the hard disk drives be connected onto the same SATA channel while creating a RAID device?	No, you can group any hard disk drives (No Init) that are available on the SATA channels of the NAS-7410. In order to gain better performance for RAID device, we will suggest to group hard disk drives located in the different SATA channels. For example, you have 6 hard disk drives connected to the NAS-7410 and you want to create two RAID level 5 devices. RAID group A should consist of HD1, HD3, HD5 (all drives connected as "master" devices), and RAID group B should consist of HD2, HD4, HD6 (all drives connected as "slave"

	devices).
Can a "3-drive RAID-5" be dynamically being expanded to "4-drive RAID-5" without losing the existing data?	Yes. NAS-7410 provides a big and powerful function "Hot Expansion" now; you can set one hard drive in "Expand" web page for expand capacity of RAID group. It means that the data stored in the old RAID device will not be lost when you want to increase capacity of storage at no downtime. Dynamically changing the configuration of the RAID device is practicable in NAS-7410.
Will the data stored in the non-RAID drive be lost when I include this drive into a newly created RAID device?	Before a non-RAID drive being included into a RAID device, it has to be deleted as "No Init" state. It means that it will be formatted before being selected into this RAID device; the data stored in this drive will be lost.
When trying to build a RAID group in NAS-7410, why I do not see any available hard disk drive in the "Config RAID" page?	To avoid the user would accidentally include in-use hard disk drives into a RAID device, only the "No Init" (or so-called "Un-used Disks") hard disk drive(s) will be shown on this page for selection. Before you create a RAID device, these candidate drives have to be deleted as to the "No Init".
How will the performance difference be observed between non-RAID and RAID device?	It is difficult to measure precisely because it depends on several factors like "amount of memory installed", "amount of drives being included in the RAID device", etc. General speaking, the grades of performance should be classified "RAID level 0" > non-RAID > "RAID level 1" > "RAID level 5". And we believe the performance should not be the major consideration to decide whether you should create a RAID device or not; it should depend on your real-world application. According to our in-house test result, the performance difference among RAID level 0, non-RAID, and RAID level 1 should be within 5 ~ 10%. But for RAID level 5, the performance drop will be around 15 ~ 25% compared with non-RAID device. That is because RAID 5 service will consume more physical memory and CPU power for calculation.
Can I adjust the "strip size" in the RAID 0 or 5 groups of NAS-7410?	No, the RAID feature of the NAS-7410 does not provide a parameter to adjust the strip size.
Can you explain "global Hot Spare" briefly?	NAS-7410 uses the hot-spare disk(s) to recover a RAID group automatically and immediately when a RAID group is degraded with a bad disk. It ensures data protection and availability. The hot-spare disks in NAS-7410 are global because they are not associated with any specific RAID group. Any RAID group in NAS-7410 being degraded, a hot-spare disk will be consumed immediately to recover that RAID group.
What is the "Hot Expansion" function? On what occasions can it be used?	The hot-expansion function is used to enlarge the capacity of a RAID group without shutting down the system. With the hot-swappable HDDs and RAID hot-expansion, it is now possible to expand your storage capacity on demand while getting the maximum system uptime. For example, assume that you only need 480GB of storage capacity. You can connect five 120GB HDDs to NAS-7410 and create a RAID-5 group. A year later, 480GB might not be enough and

	you will need 240GB more. At this time, you just plug in two 120GB HDDs to NAS-7410 and join them into that RAID-5 group. You will get a RAID group with the capacity of (480GB + 240GB) = 720GB. All these are done while the system is still on-line.
What will happen if there is a power loss while writing data to NAS-7410?	The data will probably be lost and the file system corrupted because some files may still be kept open and not correctly closed before the system shuts down. If this happens, NAS-7410 will perform a detailed file system checking process at the next reboot to avoid corruption in the file system and to maintain the data integrity of the damaged files.
What will happen to the existing RAID groups at a restart that had a power loss in the rebuilding state?	When RAID group is still in the rebuilding state, once the power is lost or rebooted, NAS-7410 will continue previous rebuilding percentage to rebuild RAID group.
Why will several GB space of a hard disk drive be lost after being initialized in NAS-7410?	It is normally caused by the unit transformation problem. NAS-7410 always uses 1024 as the calculation basis; it means 1GB=1024MB, and 1MB=1024KB. The hard disk drive manufacturers would probably use 1000 as the unit transformation basis.
About SmartSync	
What is SmartSync? When to use it?	SmartSync is a backup option inside NAS-7410, and its main use is for Remote Data Synchronization. It is used when there is NAS-7410 set up on both local and remote areas. We create a synchronous connection of data stream between the matching volumes and folders on the two servers, enabling the synchronization of data on both sides. The benefit is that SmartSync allows the remote backup of large amount of data stored on NAS-7410 servers, ensuring the security of the data.
What are the needed components of SmartSync?	SmartSync consists of at least two NAS-7410 servers. One is on the client side (synchronizing side), while the other is on the server side (synchronized side). Of course, a connection between the two server ports is necessary.
Is the server on the synchronized side limited to the use of TCP/IP connection?	Yes. TCP/IP is known for its ability to pass through routers and to remotely connect through Internet, as well as its broad adoption and convenience. Therefore, we use TCP/IP as the communication protocol to search for the synchronized server.
How many tasks can SmartSync perform at the same time?	Each NAS-7410 can perform 8 tasks simultaneously, including immediate and scheduled ones. However, we do not recommend running too many tasks at the same time, since running more tasks means more system resources are required as well as the network bandwidth. This will greatly affect the performance of NAS-7410 and the network
What needs to be considered when setting up Bandwidth Control? Why?	If we do not control the bandwidth for the data stream when SmartSync is performing its tasks, the synchronous connection may occupy a lion share of the whole network bandwidth, making the server or network unable to provide other services to the clients at a

	good performance, especially those at the remote network area. Although most enterprises are now using broadband connections, they normally provide various services using these connections. To prevent SmartSync from occupying too much of the network bandwidth, it is recommended to set up Bandwidth Control during execution of the tasks. Some parameters to be considered are: 1. the total bandwidth and the distribution of bandwidth that the enterprise has in its network environment; 2. the frequency of accesses by the clients and the number of clients served by NAS-7410.
What does Quick Synchronization mean?	When SmartSync is performing the second task, we can choose the Quick Synchronization option. By selecting this option during synchronization, SmartSync will first check the file lists on both the source server and the destination server. Then, it checks the modify time and file size of those files. If the results of both items are identical, the system will simply bypass the synchronization of those sets of files and step to the next sets files. Thus it reduces the loading on the network bandwidth and the processing time.
What solutions for remote backup does NAS-7410 currently provide?	NAS-7410's solution for remote backup is SmartSync. Just like the other NAS storage systems on the market, current synchronization mode is remote mirroring. That is the client-side server can use SmartSync to make a mirrored image on the server side to achieve remote backup.
Does SmartSync support data synchronization from desktop to NAS-7410?	SmartSync currently supports data synchronization only from NAS-7410 to other NAS-7410 servers. We may consider implementing data synchronization from Windows platform to NAS-7410 at the second stage.
Sometimes the SmartSync task will be terminated by a reason "memory low", what's the possible cause?	Because SmartSync is a memory-consuming operation, memory utilization rate is critical when launching this task. When NAS-7410 detects the free memory is low, the program will terminate the synchronization task. To avoid this situation, we suggest checking the following configurations or timing before launching SmartSync task. 1. Set the SmartSync task to perform at non-rush hour to avoid memory conflict with routine network services. 2. Set a proper SmartSync source path. If the SmartSync source includes up to millions files/directories, that will occupy most of the memory capacity when creating check list, it is suggested assigning the source path in multiple sub-directory in different tasks.
What protocol is used for SmartSync? Is it CIFS/SMB, FTP or NFS network protocols?	SmartSync does not use CIFS/SMB, FTP or NFS as its communication protocol. It is based on SSL over TCP/IP. This also means SmartSync has its own security policy and won't refer to SMB, FTP or NFS security setting.
Which part of NAS-7410 will be mirrored to SmartSync Point? Data, Share Setting, ACL setting or User	SmartSync feature focuses on "Data" part remote backup. Thus only Data and ACL setting in the Data will be synchronized to remote servers, it does not synchronize User database and Share setting information to the SmartSync point. (Please refer to the FAQ section

database?	"Backup". NAS-7410 provides an advanced feature to Backup/Restore system configuration/User Database/Share setting in Backup -> System Profiles page)
If I use firewall or NAT device in my network environment. Which ports have to be opened for SmartSync tasks?	The default port number are 873 and 22. You have to open these two ports for SmartSync tasks.
Data Management	
Can the NAS-7410 behave itself as a stand-alone server without the existence of another file server?	Yes, when NAS-7410 is working in Microsoft, Macintosh, UNIX and HTTP network environments, the NAS-7410 behaves itself as a stand-alone server.
Will the NAS-7410 show me the home pages in different languages when I am using the different language web browsers?	Yes, a specific language home page of the NAS-7410 will be shown in your different language web browsers. It depends on the language version of web browser installed in your client.
Why did I cannot find NAS-7410 in "Network Neighborhood" or "My Network Place"?	Within TCP/IP of network environment, if your PC and NAS-7410 configure IP address to different IP segment, you won't find NAS-7410 appear in "Network Neighborhood". You can find four kinds of solution for your reference below: 1 Set up all of client PCs and NAS-7410 register to WINS server, you can use "Find Computer" to find NAS-7410. 2. Create "LMHosts" file in all of client PCs, you can create a relation between client PCs and NAS-7410. 3. You can use "DOS Prompt Command" under windows; perform "net use" command to map the shared folder inside NAS-7410. For example: net use z: \< Host IP >\< share >, "z:" means "network disk letter", "Host IP" is NAS-7410 IP address, "share" is a shared folder name inside NAS-7410.
Is there any limitation when I try to burn CD in the NAS-7410?	If your NAS-7410 is in the following situations, the recording task might fail: 1. During the recording process, the NAS-7410 is under heavy loading network traffic. 2. During the recording process, the same IDE channel's option device is performing a CD insert/eject operation. If the recording tasks continue to fail, we strongly recommend you to lower the recording speed or choose better quality recordable media
Can I perform multiple recording tasks simultaneously if I install two optical devices into	In order to increase the successful rate of burning CD, the NAS-7410 does not support multiple recording tasks simultaneously. It will however collect all the requested tasks and complete them one after another.

NAS-7410?	
How does NAS-7410 handle the repair of the flash system in the event of a crash?	NAS-7410 features with the system configuration backup/restore function to protect the system configuration from system crash.
Event Log and Notification	
Does the NAS-7410 support SNMP protocol for sending traps to the administrator?	Yes, you can manipulate the NMS software (For example, HP OpenView) to receive relative traps.
How can I send an email event to administrator?	You can follow the steps below to set up email event: 1. Go to NAS-7410 Admin Home page and select "Network Settings". 2. Select the sub menu "Email". 3. Enable SMTP Protocol. 4. Fill in correct SMTP server IP address or Fully Qualified Domain Name (FQDN). (* If you fill in FQDN, please make sure you have set DNS server IP address inside NAS-7410.) 5. Fill in a legal user account for login SMTP server purpose. 6. Based on your need, fill in one or two Email Addresses. 7. Click "Apply" and then select "Event" menu to configure further settings. 8. Click "Advance" button in "Configuration" sub menu of "Event". 9. Enable "Email Alert". 10. Check "Event List for Notification" to decide which events can be sent to administrator via email. 11. Click "Apply" button to complete settings.
How can I send Traps to my NMS?	You can follow the steps below to configure: 1. Go to NAS-7410 Admin Home page and select "Network Settings". 2. Select the sub menu "SNMP". 3. Enable SNMP Protocol. 4. Fill in your server IP address (with NMS installed) that you want to receive traps and then make sure the "Trap" column is set to "YES". 5. Click "Apply" and then select "Event" menu to configure further settings. 6. Click "Advance" button in "Configuration" sub menu of "Event". 7. Enable "SNMP Trap". 8. Check "Event List for Notification" to decide which events can be sent to NMS via trap. 9. Click "Apply" button to complete settings.

Configuration	
How to set all configurations of NAS-7410 back to factory default?	You can set it through web page or adjust hardware jumper on motherboard. Web page: 1. Go to Admin Home page. 2. Select Server Settings. 3. Select Shutdown of sub menu. 4. Enable "Reset configuration to factory default". 5. Click "Reboot" button for completing the process.
Why can't I add user account to NAS-7410 user database through mouse right-click (Windows native tools)?	Only the accounts that are of Admins group member can add user account to NAS-7410 user database through mouse right-click. If the login account does not belong to Admins group, although the login account has full control (FC) permission, he still only can see and modify permission, but cannot add any user account to NAS-7410 user database.