NAS-7450 / NAS-7850

User's manual

Version 1.0.0

Copyright

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B 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.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

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.

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 and have to collect such WEEE separately.

Revision

User's Manual for PLANET 4-Bay/8-Bay SATA NAS RAID Server
Model: NAS-7450/7850
Rev: 1.0 (Dec. 2010)
Part No. EM-NAS-7450/7850

Chapter 1 Introduction

1.1 NAS-7450 overview

The reliable and high-performance business-class network storage, PLANET NAS-7450 is a 1U 4-Bay rack-mountable unified network storage system designed 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. Integrated data protection and offsite replication features make managing complex business storage environments affordable.

The NAS-7450 provides advanced RAID configurations including RAID 0, 1, 5, 6 and 10 functions. The HDD space in use can easily increases up to double with RAID-0 or real-time data backup to prevent data lost with RAID-1. The basic RAID function will ask user to install two hard drives in the same model when storing data, however, it also supports hot-swap design so that a failed drive can be replaced by hot swapping without turning off the server. Besides, the best-in-class RAID on the NAS brings users a higher level of data security by allowing one more hard drive failure than other NAS with similar functions.

The NAS-7450 is equipped with the Intel Celeron processor, and it is a powerful 4-Bay network attached storage (NAS) server, which is designed to provide a cost-efficient and easy-to-use solution. It supports advanced user management functions such as private HDD space and login account. It not only shares HDD space, but also positions as the central management device managing each user of the device. With the NAS-7450, business-class office or home users will get a simple yet effective way to expand the client side or the network data storage.

1.1.1 Features

- High-density **1U rack-mount**, extreme energy efficiency and simple serviceability
- Multiple volume support for **RAID 0, 1, 5, 6, 10** background sync and Smart Sync resume
- Simultaneously supports **NAS** and **iSCSI SAN** for database and server virtualization applications
- **Two 10/100/1000** Ethernet ports with **load balancing** and failover
- High-end Data Protection adopts the most advanced SATA RAID technology and fully integrates **Anti-virus** engine to protect valuable data on the fly
- Multi-Protocol system support for Windows, MAC, Solaric, FreeBSD, Linux and other UNIX derivatives
- Revolutionary dual-function NAS server integrates both On-line file service into one centralized storage server
- **High Performance:** Using single device connection which eliminates the master/ slave issues and allows faster transfer rate without latency and delay
- **High Data Integrity:** Offers error checking and error correcting capabilities

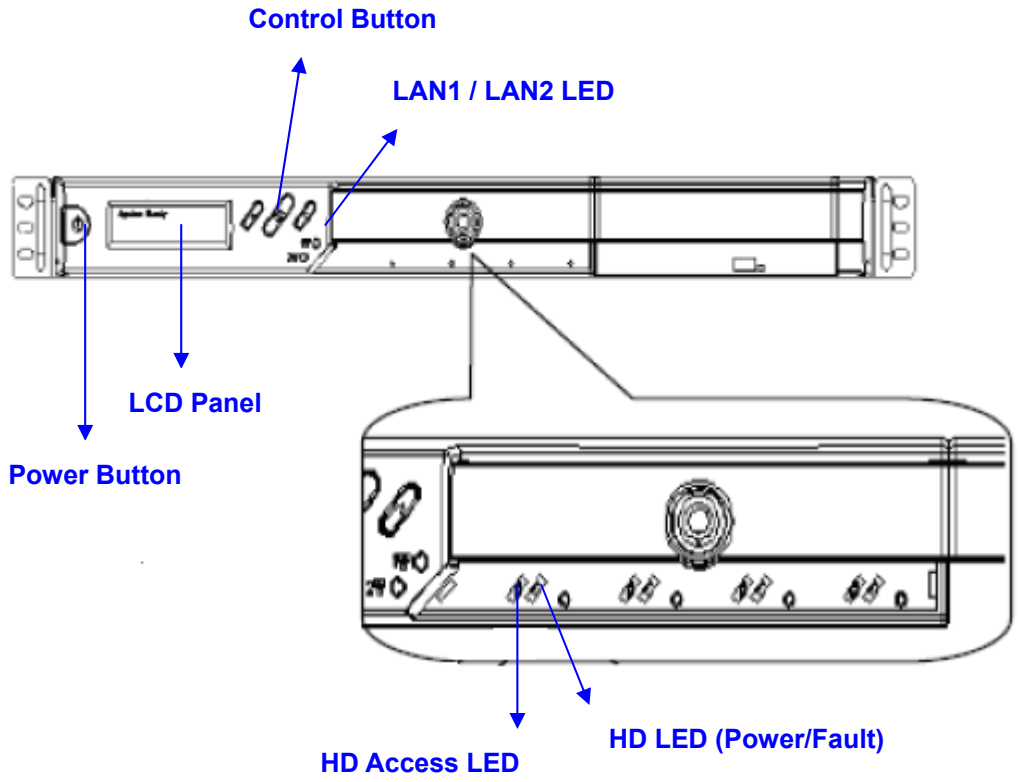
- The end-to-end integrity of transferred commands and data can be guaranteed across the serial bus
- **High System Reliability:** A dedicated port for each disk drive, providing greater system reliability through individual drive and cable fault isolation
- **High Usability:** Easier configuration and design with cables that are thinner, have smaller connectors, and are simpler to route and install

1.1.2 Package Content

- NAS-7450 x 1
- Key x 2
- Power Cord x 1
- Screw Package x 1
- User's Manual CD x 1
- Sliding Rail x 1 set
- Quick Installation Guide x 1

1.1.3 Physical Detail

NAS-7450 Front View

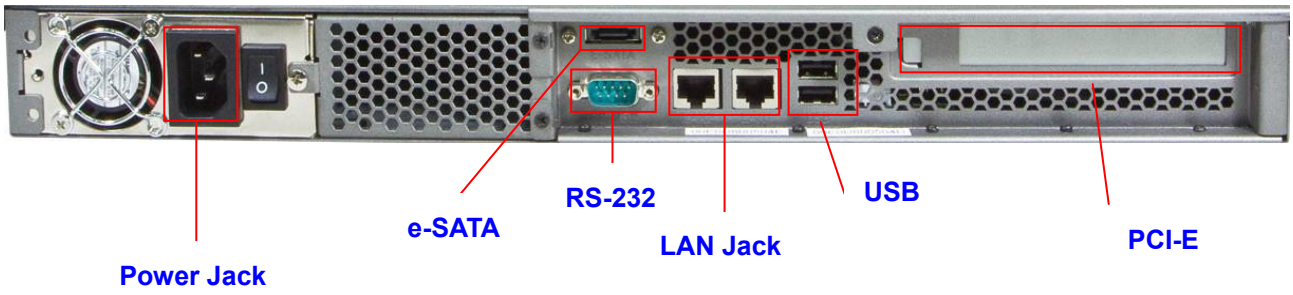


Interface	Description
Power Button	Green(power on)、Yellow(default)
LCD Panel	Display LAN1/LAN2 IP Information
Control Button	Press the Control button to configure LAN1/LAN2 IP address.

LAN1	Yellow(10M link)、Green(100M link)、Amber(1000M link)
LAN2	

HD Access LED	HD LED(Power/Fault)	Description
Red on	Green Blinks	Powering up
Red On during access	Green On	HDD is being accessed
Red Blinks (Fast)	Green Blinks (Fast)	RAID building, rebuilding, expanding
Red off	Amber on	Volume un-mounted and HDD is ready for being hot-up plugged
Off	Amber Blinks (Slowly)	Disk faulty. Blinking interval is about 2 seconds

NAS-7450 Rear View



Interface	Description
Power Jack	Connect the two power supply cord shipped with the system
e-SATA	Connect to External hard drive case
RS-232	Connect to UPS
LAN Jack (LAN1)	These RJ-45 ports support auto negotiating Fast Ethernet 10/100/1000 Base-TX networks. That allows your system to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a CAT.5 twisted pair Ethernet cable.
LAN Jack (LAN2)	
USB Socket	Connect to UPS and external HDD(FAT/FAT32)
PCI-E Port (optional)	Connect to Tape Backup or Tape Library or Network card

1.2 NAS-7850 overview

The reliable and high-performance business-class network storage, PLANET NAS-7850 is a 2U 8-Bay rack-mountable with redundant power supplies network storage system designed 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. Integrated data protection and offsite replication features make managing complex business storage environments affordable.

The NAS-7850 provides advanced RAID configurations including RAID 0, 1, 5, 6 and 10 functions. The HDD space in use can easily increase up to double with RAID-0 or real-time data backup to prevent data lost with RAID-1. The basic RAID function will ask user to install two hard drives in the same model when storing data, however, it also supports hot-swap design so that a failed drive can be replaced by hot swapping without turning off the server. Besides, the best-in-class RAID on the NAS brings users a higher level of data security by allowing one more hard drive failure than other NAS with similar functions.

The NAS-7850 is equipped with the Intel Core 2 Duo processor, and it is a powerful 8-Bay network attached storage (NAS) server, which is designed to provide a cost-efficient and easy-to-use solution. It supports advanced user management functions such as private HDD space and login account. It not only shares HDD space, but also positions as the central management device managing each user of the device. With the NAS-7850, business-class office or home users will get a simple yet effective way to expand the client side or the network data storage.

1.2.1 Features

- High-density **2U 8-bay rack-mount** with redundant power supplies for reliability and business continuity
- Multiple volume support for **RAID 0, 1, 5, 6, 10** background sync and Smart Sync resume
- Simultaneously supports **NAS** and **iSCSI SAN** for database and server virtualization applications
- **Two 10/100/1000** Ethernet ports with **load balancing** and failover
- High-end Data Protection adopts the most advanced SATA RAID technology and fully integrates **Anti-virus** engine to protect valuable data on the fly
- Multi-Protocol system support for Windows, MAC, Solaric, FreeBSD, Linux and other UNIX derivatives
- Revolutionary dual-function NAS server integrates both On-line file service into one centralized storage server
- **High Performance:** Using single device connection which eliminates the master/ slave issues and allows faster transfer rate without latency and delay
- **High Data Integrity:** Offers error checking and error correcting capabilities
- The end-to-end integrity of transferred commands and data can be guaranteed across the

serial bus

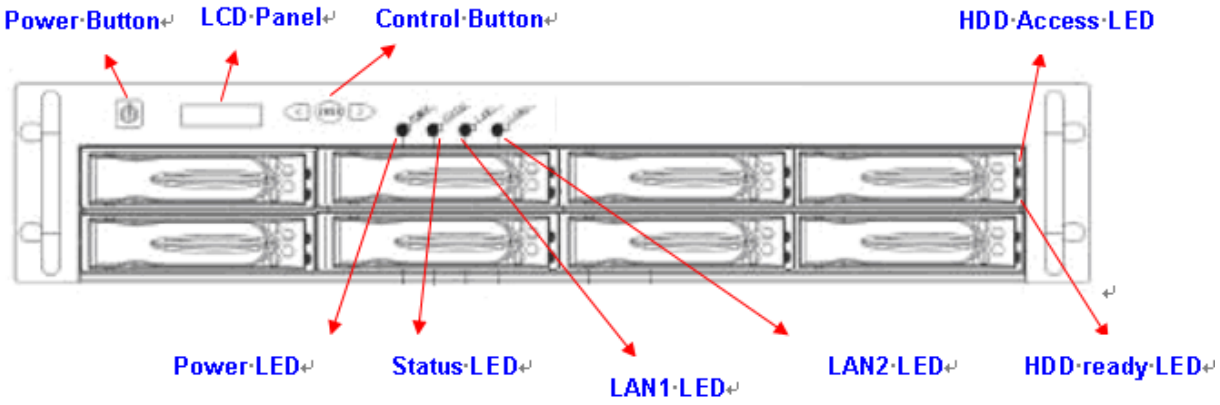
- **High System Reliability:** A dedicated port for each disk drive, providing greater system reliability through individual drive and cable fault isolation
- **High Usability:** Easier configuration and design with cables that are thinner, have smaller connectors, and are simpler to route and install

1.2.2 Package Content

- NAS-7850 x 1
- User's Manual CD x 1
- Power Cord x 2
- Screw Package x 1
- Sliding Rail x 1 set
- Quick Installation Guide x 1

1.2.3 Physical Detail

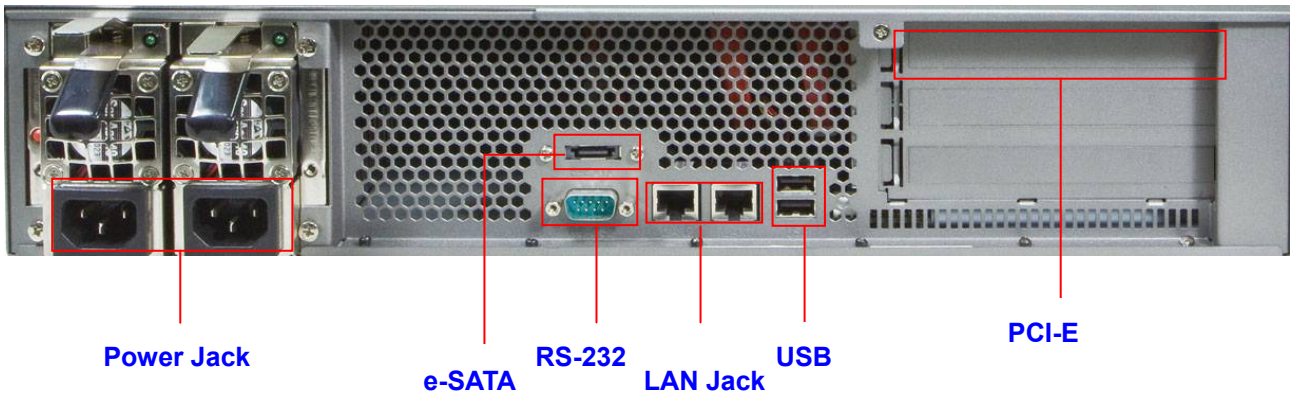
NAS-7850 Front View



Interface	Description
Power Button	Power on/off
LCD Panel	Display LAN1/LAN2 IP Information
Control Button	Press the Control button to configure LAN1/LAN2 IP address.
Power LED	Green(power on)、Yellow(default)
Status LED	Yellow(default)
LAN1 LED	Yellow(10M link)、Green(100M link)、Amber(1000M link)
LAN2 LED	

HDD Access LED	HDD ready LED	Description
Red on during access	Green Blinks	Power is being accessed
Red on	Green Blinks (FAST)	RAID building, rebuilding, expending
Off	Amber on	Volume un-mounted and HDD is ready for being hot-unplugged
Off	Amber Blink (Slowly)	Disk fault Blinking interval is 2 second
Off	Off	Hard disk is absent or SATA cable is not connected

NAS-7850 Rear View



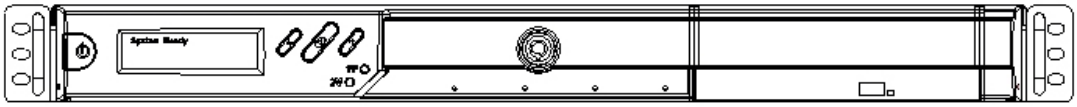
Interface	Description
Power Jack	Connect the two power supply cord shipped with the system
e-SATA	Connect to External hard drive case
RS-232	Connect to UPS
LAN Jack (LAN1)	These RJ-45 ports support auto negotiating Fast Ethernet 10/100/1000 Base-TX networks. That allows your system to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a CAT.5 twisted pair Ethernet cable.
LAN Jack (LAN2)	
USB Socket	Connect to UPS and external HDD(FAT/FAT32)
PCI-E Port (optional)	Connect to Tape Backup or Tape Library or Network card

Chapter 2 Installing and Starting NAS system

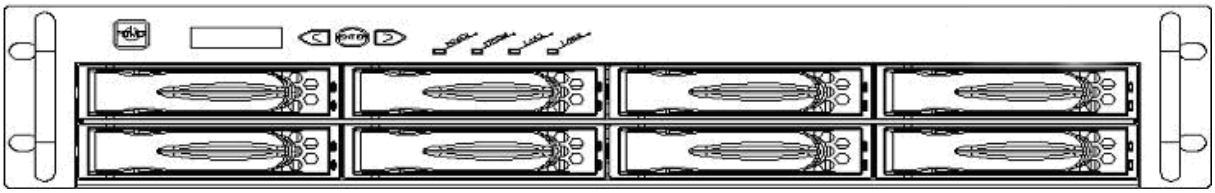
This chapter covers the installation procedure of different form factors of NAS server as well as the NAS-7450/NAS-7850 Mobile Rack. Instruction on how to startup the NAS server by setting up the basic configuration through the Admin Home page or provided software tool – NAS Finder is also outlined in this chapter.

2.1 Installing the NAS-7450/NAS-7850 rack-mount Model

NAS-7450



NAS-7850



Hot swap hard disk tray installation

1. To unlock the hot swap hard disk tray, pull the tab behind the end of the lever to release the latch and then lift the lever up as far as it can go to disengage the hard disk tray from the chassis.

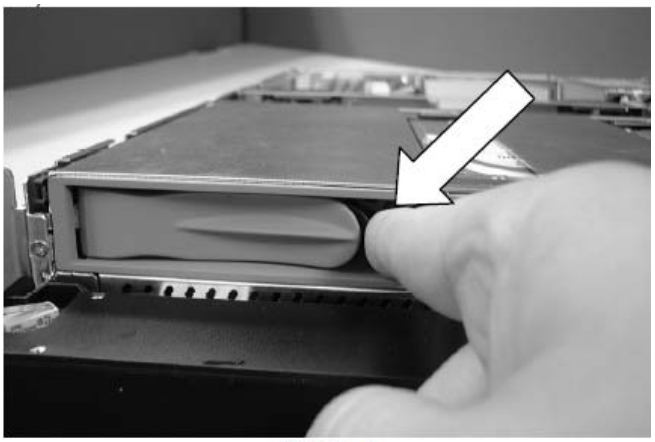


Figure 1

2. Pull the hard disk drive tray out.
3. Attached the HDD to the hot swap hard disk tray with the screws provided shown in Figure 2.

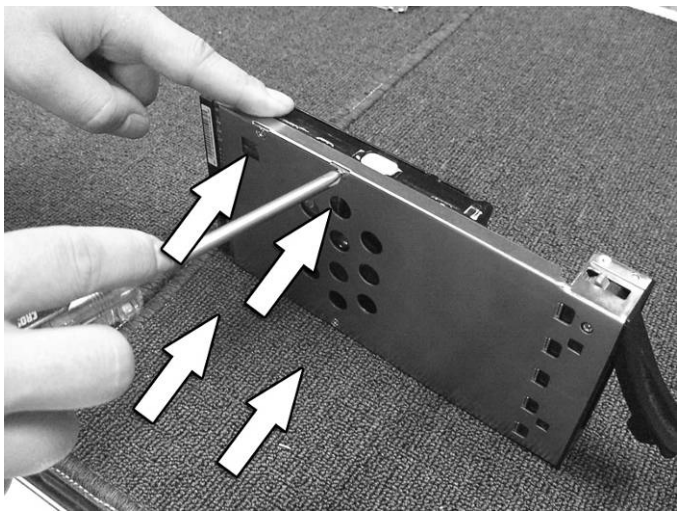


Figure 2

4. Slide the hot swap hard disk tray slowly into the chassis, push the outer rim of the tray as shown in Figure 3 until the lever retract slowly toward the tray. Then, push the level down as far as it can go to connect the hot swap hard disk tray to the chassis.

Figure 3

NAS-7450/NAS-7850 rack-mount server installation

1. Pull out a HDD tray from the server.
2. Secure and mount a hard disk onto the HDD tray using four screws under the tray.
3. Insert the HDD tray back in the server. Make sure the lever of the HDD tray is properly in place.
4. Repeat Step 1 to Step 3 if necessary for the other HDD tray.
5. Install the provide rack mounting handles at both side of the NAS server.
6. Install the NAS server in the rack. (Refer to the paragraph “Sliding Rails Installation” in Chapter 2 section 5)
7. Connect your NAS server to the network by attach a LAN cable from the LAN port located at the back of your NAS server.(At least one network connection is required)
8. Plug the power cord into the power connector on you NAS server.
9. Make sure the power switch on the power supply is in on position.

10. Press the power button on the left hand corner of your NAS server.

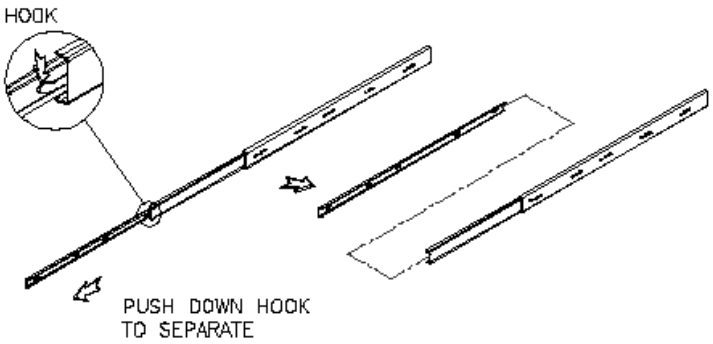
11. Wait for the server to boot up. The boot up process takes approximately 2 minutes.

2.2 Sliding Rails Installation

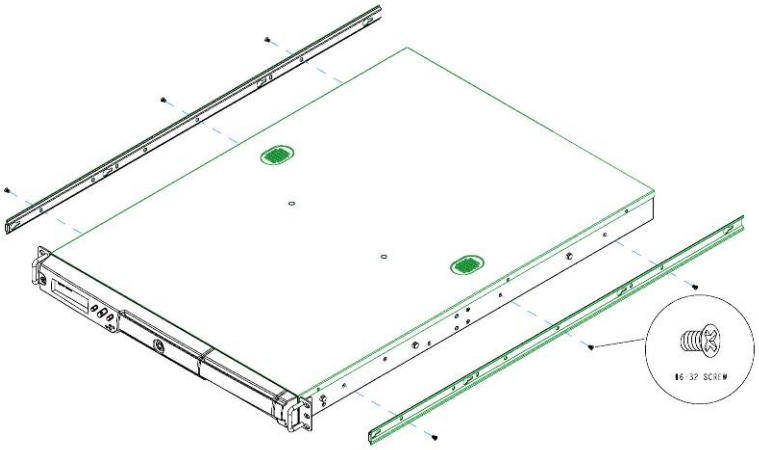
1.Make sure that you have the following the mounting parts for the sliding rails.

- 4 L-shaped brackets (see the left side of the photo)
- 8 x "**M4**" size screws, 8 x "**M5**" size screws and 6 x "**#6-32**" size screws.

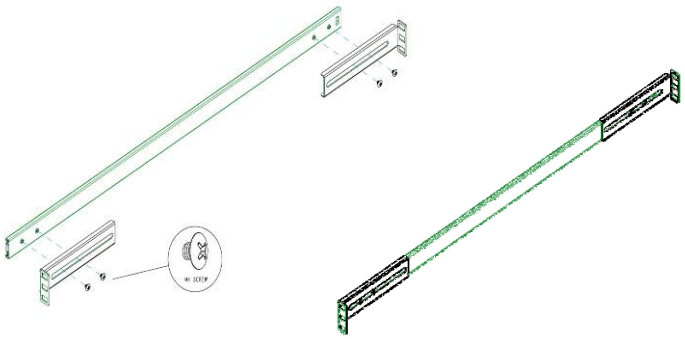
2.Take the sliding rail apart by sliding out the center slide. Push down the hook to separate them. Pull the center slide all the way until it reaches the end.



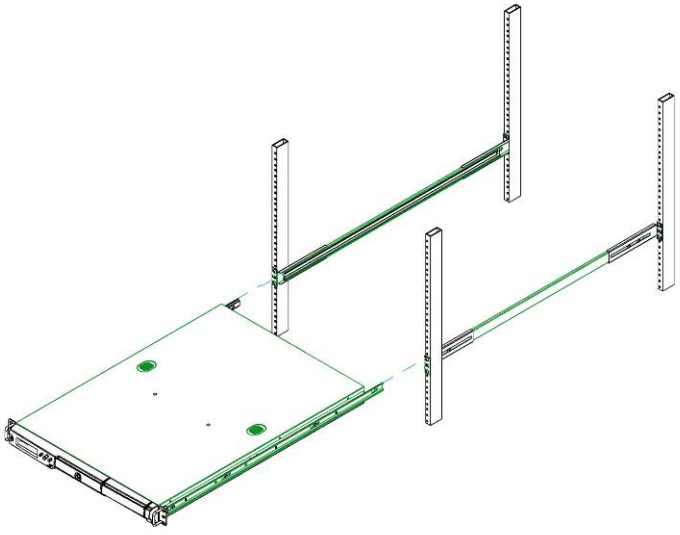
3. Now install the center slide to the rack-mount chassis. Find the screw holes on both sides of the rack-mount chassis, which are used for mounting the center slide. Fasten the "**#6-32**" screws to fix the center slides onto chassis. Later, the center slides will be used for attaching to the sliding rail.



4. Next, attach the two L-shaped mounting brackets on to a sliding rail. Use the "**M4**" screws to secure the L-shaped bracket on to the sliding rail.

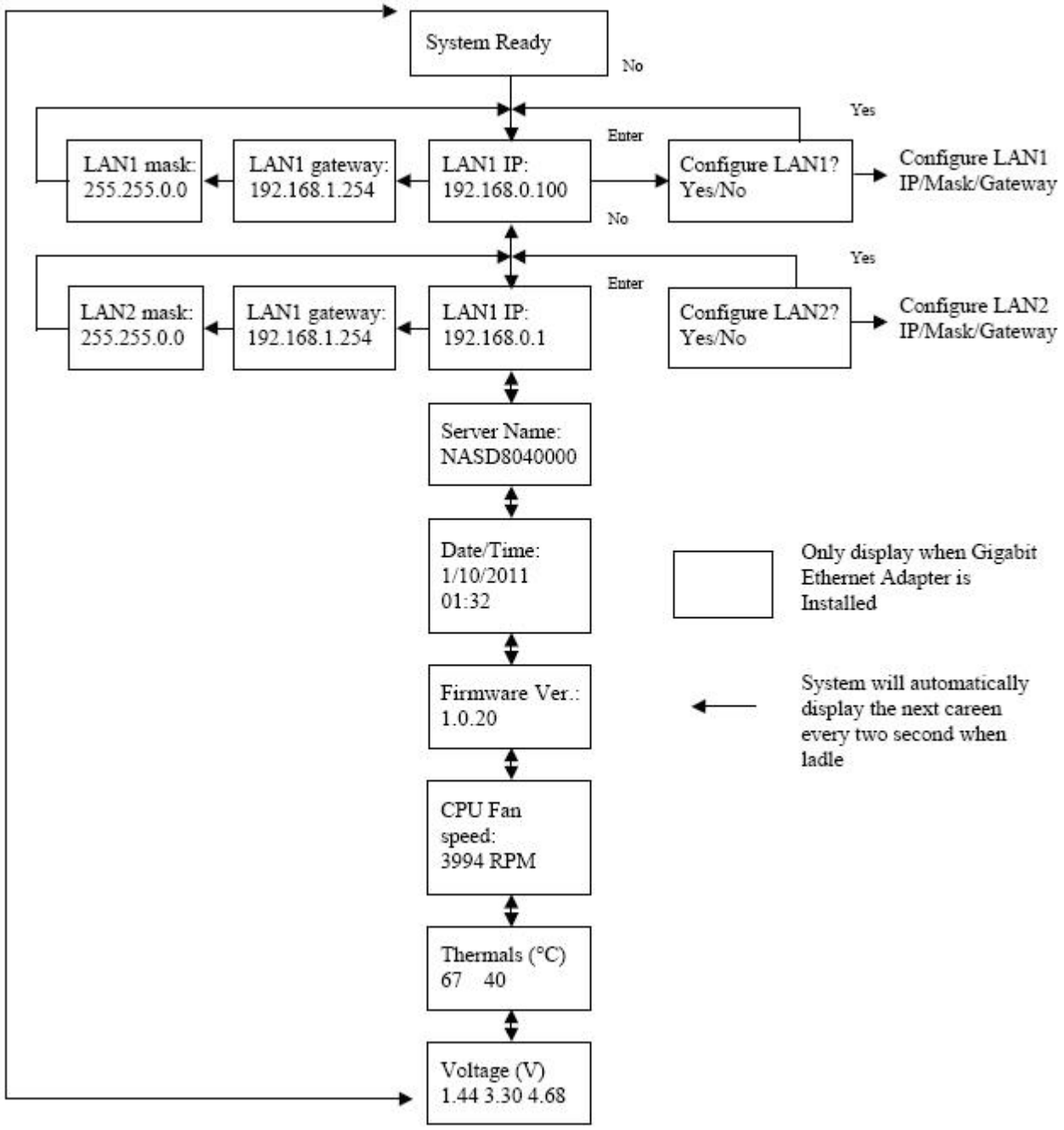


5. Attach the sliding rail onto a rack-mount cabinet. Secure the sliding rail onto the rack-mount cabinet via the screw holes on the L-shaped brackets



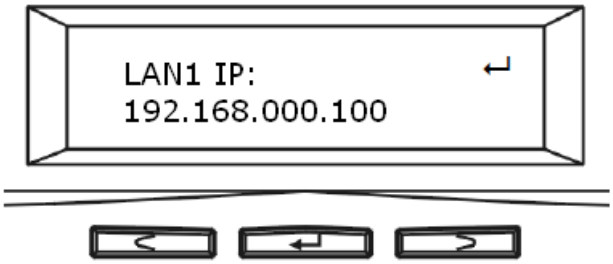
After properly attaching both sliding rails to the rack-mount cabinet, you may slide the rack-mount chassis (mounting) in to the cabinet.

Configuring the NAS using the LCD console



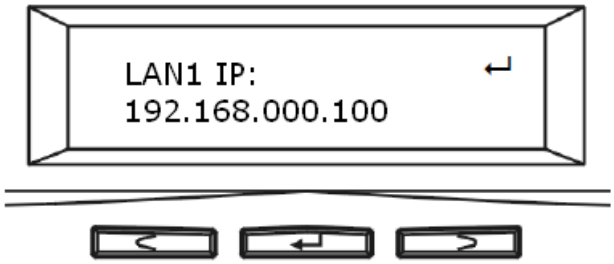
Configuring the IP addresses using the LCD console

1. After NAS server is boot up, the LCD console shows **System Ready**. Press the right button.

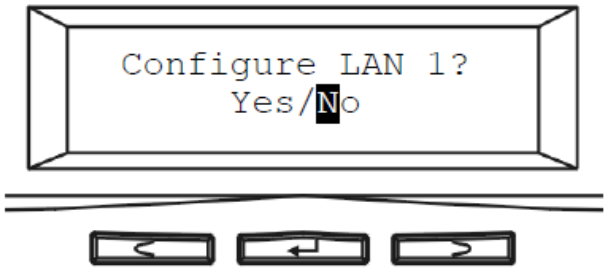


2. The IP address of LAN1 is shown. Press the middle button to configure LAN1 IP address.

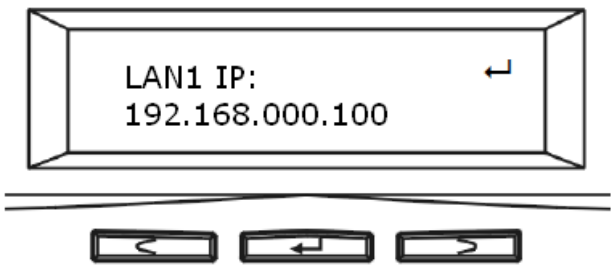
Note that the ↵ symbol at the right hand upper corner indicates that the IP address can be configured using the LCD console.



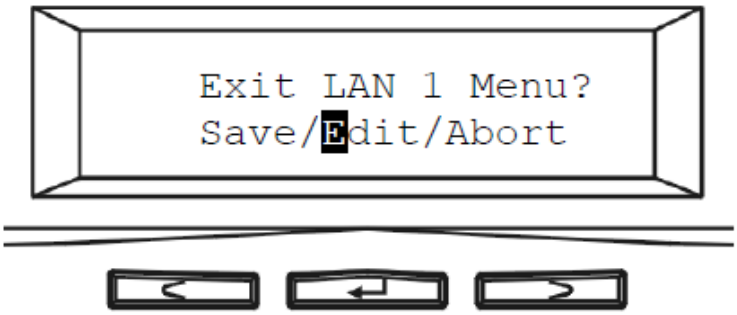
3. Move the cursor to "**Yes**" by pressing the left button and then press the middle button to confirm.



4. Move the cursor to the correct position using the left or right button. Then press the middle button to change that number.



5. After you edit the last digit of the IP address, press the right button and configure the **Subnet Mask** address.
6. Repeat Steps 4 to Steps 5 to configure the **Subnet Mask** and **Gateway** address.
7. After you edit the last digit of the **Gateway** address, press the right button. Move the cursor to **Save** and save the setting or **Edit** to repeat the above process or **Abort** to quit the configuration process without saving.



8. Repeat the above process to configure the other LAN port.

Configuring the IP addresses using NAS Finder

You can use the provided utility NAS Finder to perform the initial setup of your newly arrived NAS server. The utility designed to perform a quick set up 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 “NASxxxxxxxx”**,** where “xxxxxxxx” is the last eight digits of the Ethernet address of LAN1.

1. Highlight the server you want to configure from the left hand pane.
2. Click the  button on the toolbar
3. Or, right click the server and select “Configure”
4. Enter the “Server Name”, “Server Comment”, and “Workgroup/Domain Name” and select either the “Workgroup mode” or “Domain mode”.
5. Click “Next” button to go to the next page.
6. Choose the “Network Teaming Mode” from the pull down menu. If you are not clear about this feature, continue with the default value.
7. If you want IP settings to be assigned automatically, click “Obtain IP settings automatically”.
8. Or, you can specify IP settings manually.
9. Click “Next” button to go to the next page.
10. Change the admin password if necessary.
11. Click the “Finish” button to save the settings. Note that server may need to reboot for certain parameters changes to take effect.

2.3 Accessing the Administration Home Page

You can configure the detail settings of your NAS server in the administration home page. To access the administration home page of NAS server, type the URL name of your NAS server in the address field of the web browser: http://192.168.1.100 /admin/ or run the utility “NAS Finder” provided in the CD-ROM, right-click on a NAS server on the left-hand tree-view pane. Select “Admin page” item from the right-click menu to open the administration page. It will prompt for username and password. By factory default, the username is admin and password is admin.

Note:	It is recommended that user change the admin password immediately to keep your NAS server secure and to protect resources from inappropriate access by other users on the network.

2.4 Detection of Chassis Intrusion

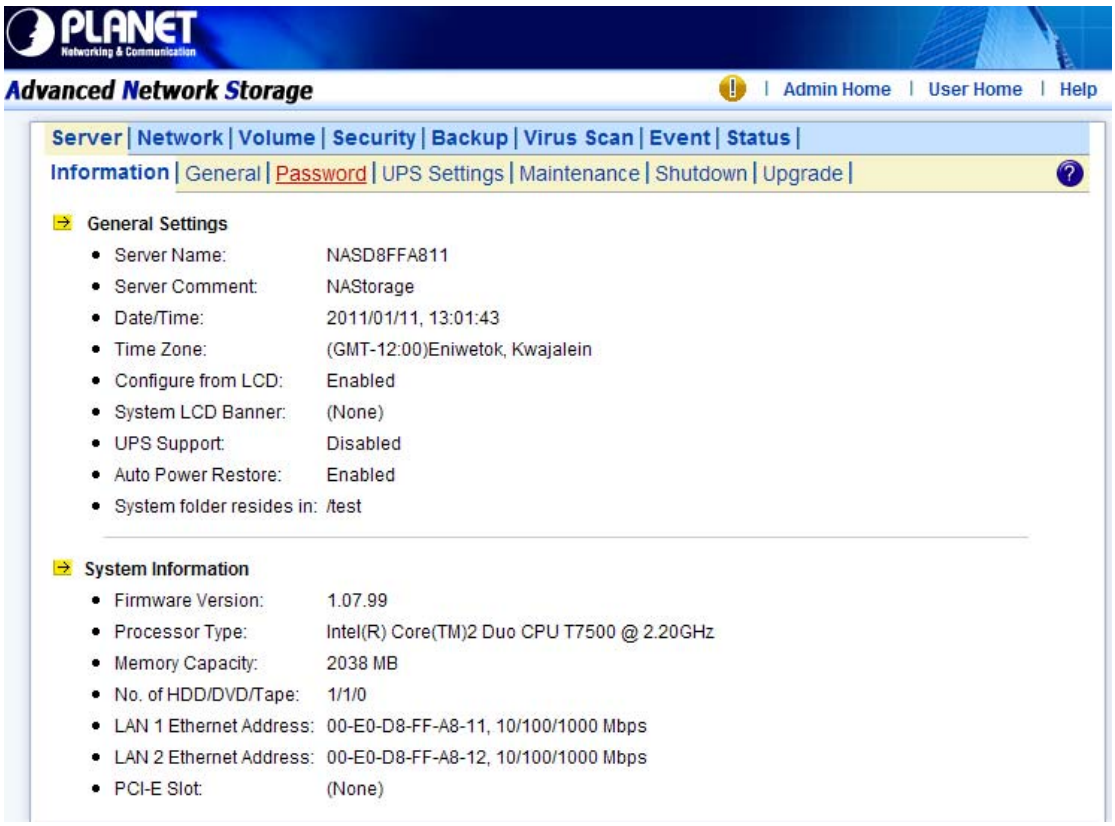
Model NAS-7450/7850 NAS server supports the detection of chassis intrusion and door intrusion. When the chassis is opened or chassis door is opened, the system will send email alerts or SNMP traps. To enable the function, please go to the “Event → Configuration” menu on the administration page. Click the “Advanced” button and check the “Chassis intrusion detected” item.

Please note that the sensor must be connected to the main boards correctly for the function to work.

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 and Settings



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

The **Information** page is divided into two sections. The “General Settings” section shows the parameters which can be modified on the “Server → General” page.

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

Configure from LCD	Indicates whether users can configure the server from the LCD console
System LCD Banner	Indicates the banner text which is displayed on the LCD console when it receives no user input or event messages for a period of time
UPS Support	Indicates whether the UPS support is enabled or not
Auto Power Restoration	If enabled, the server will power on automatically when the power restores after abnormal shutdown
System folder resides in	Display the volume name of 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

3.2 Upgrading the Firmware

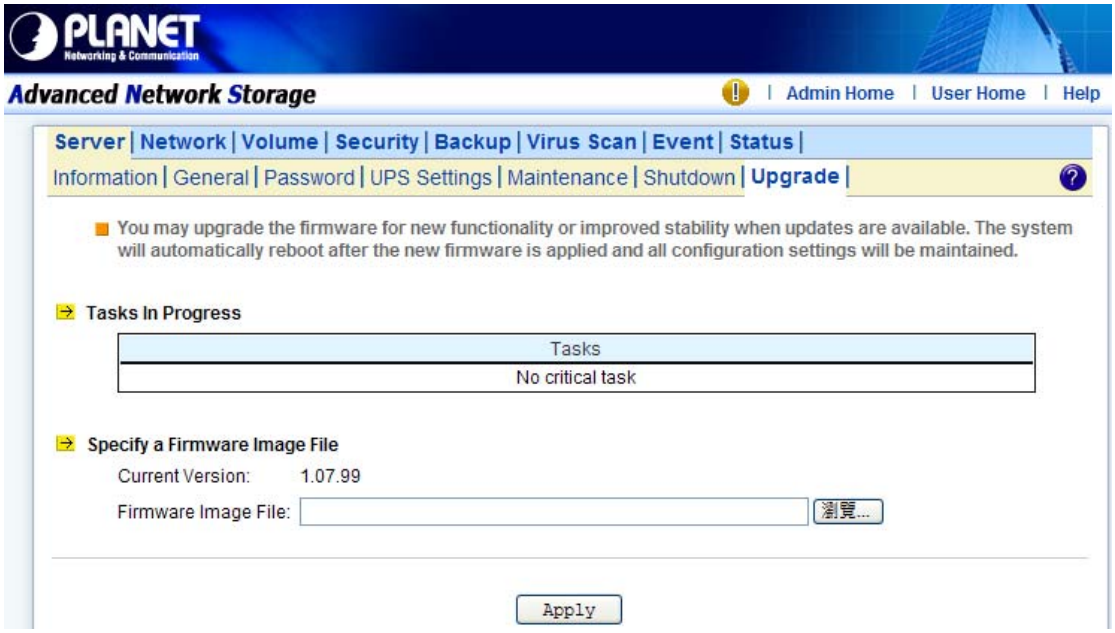
Updating OS firmware will accommodate new functions or bug-fixes. Once you get new releases of an OS firmware image, you can upgrade the OS firmware by using the web browser. The process is simple and fast. Once you get the image file of the new OS firmware from your vendor, open the “Administration 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.

3.3 Shutting Down the Server

Shutdown, reboot and startup actions

The NAS server can be shut down by pressing the power button twice at 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.

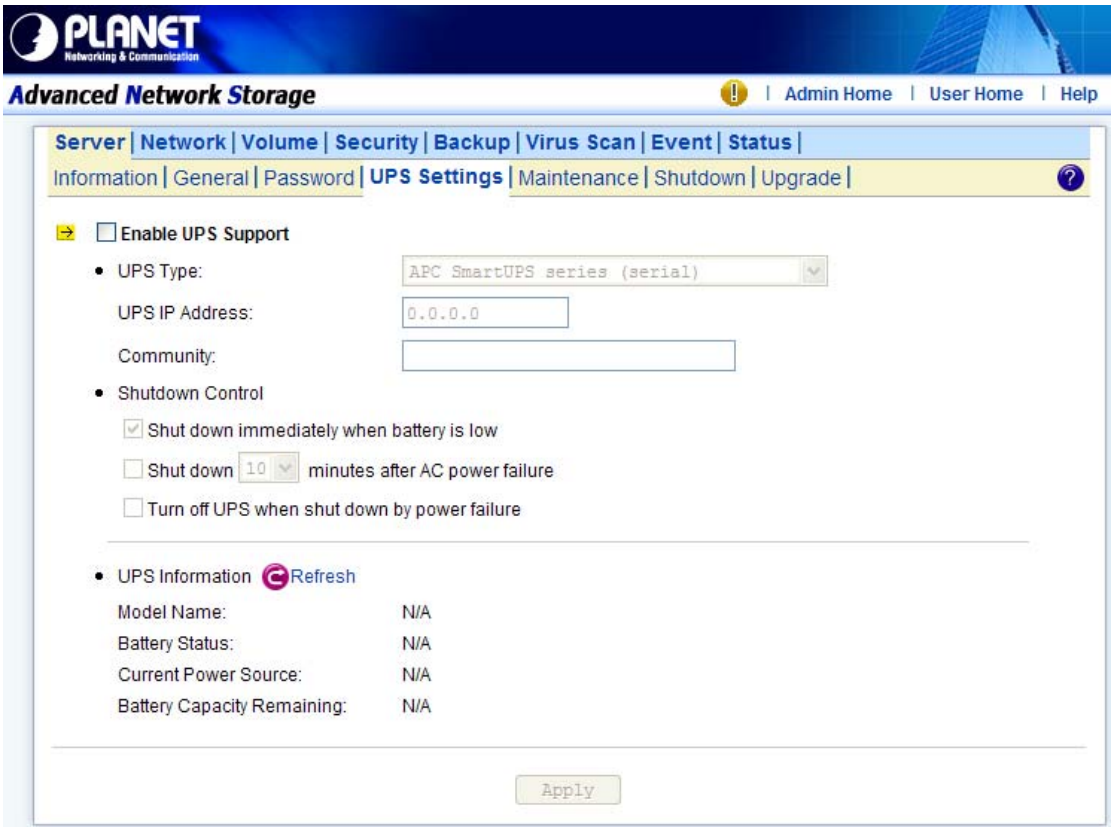
3.4 Enabling UPS Support

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、 USB UPS、 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.

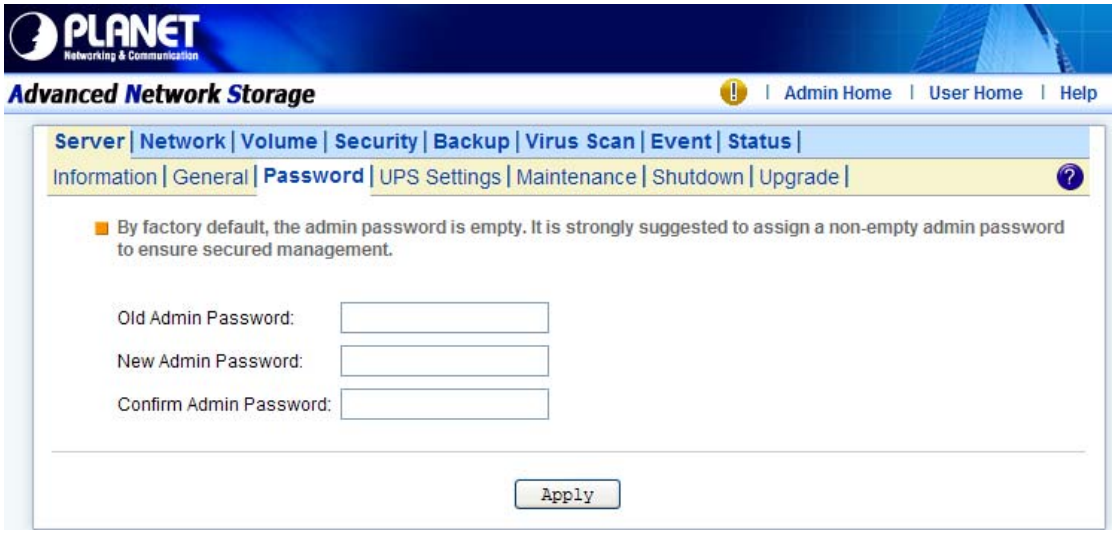


Below are the shutdown options on the page.

Item	Description
Shut down immediately when battery is low	Specify whether to shut down the server when UPS battery is low.
Shut down in x minutes when AC fails	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.

Note:	When utility power fails, the NAS server will always shut down.

3.5 Modifying the Administrator's Password



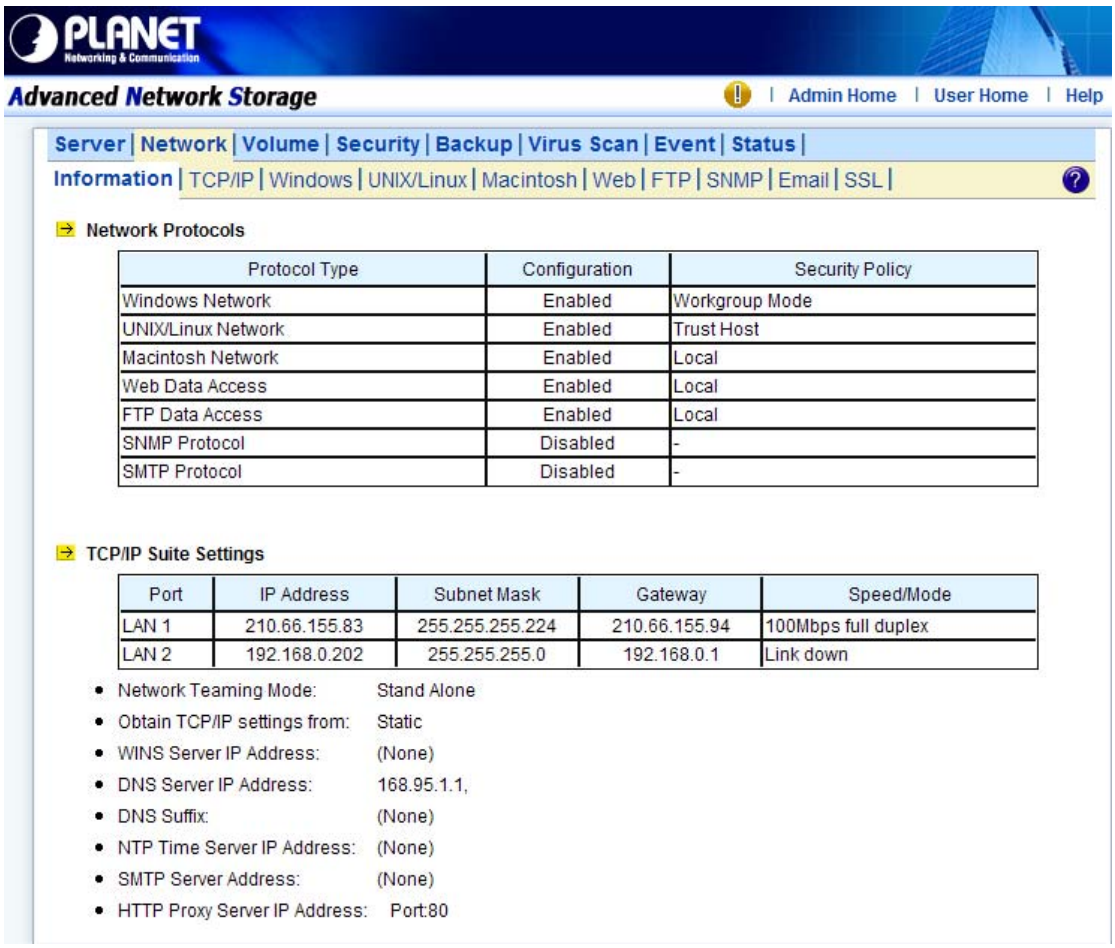
"Admin" is a built-in user account for the administrator. It is like the "root" account in UNIX or the "administrator" account in Windows 2000 or XP. Using this account, users have access to the administration homepage and all the storage resources. By default, the password for this user account is empty. 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".

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 used to determine what subnet an IP address belongs to.
Gateway	A node on a network that work 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 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 located 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, which 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 setting up correct TCP/IP setting that for NAS server to function properly.

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 are configured with a unique IP address, which are independent to each other.

Fault Tolerance: Uses LAN2 to take over for the LAN1 if LAN1 is fail to connect to the network which 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 port 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 balance. Note that only the LAN1 Ethernet port receives incoming traffic.

Load Balancing: also incorporates Fault Tolerance protection.

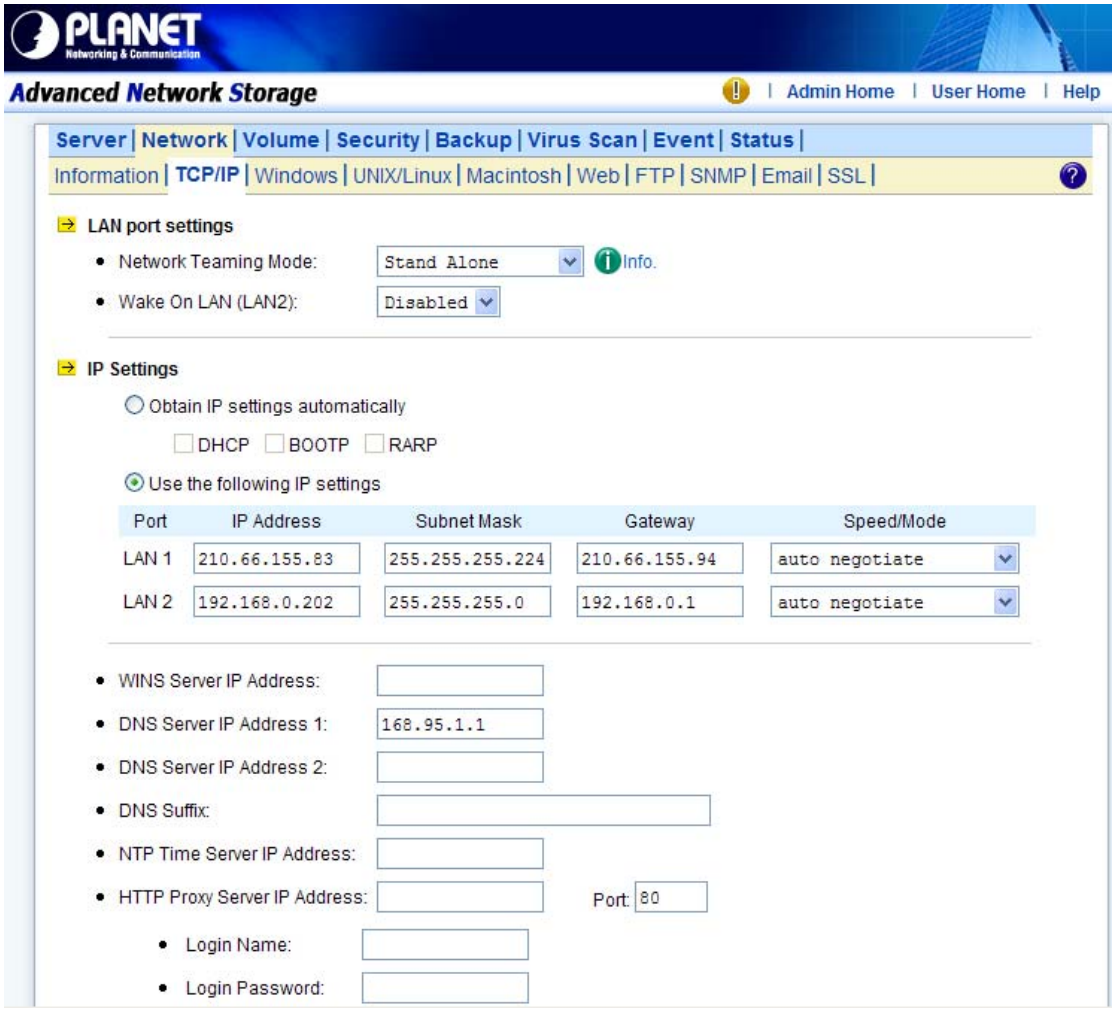
Link Aggregation: combines both LAN1 & LAN2 into a single channel, appearing to use a single MAC address to provide greater bandwidth. It must be used with a network switch having the Link Aggregation or Trucking function.

Wake-On-LAN:

NAS server also supports Wake-On-LAN (available for LAN2 only). 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/IP Settings

1. Select a “Network Teaming Mode” from the pull-down menu that suit you need.
2. Enable or Disable “Wake On LAN” (Available for LAN2 only).
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 using SMB/CIFS protocol- short for Server Message Block/Common Internet File System, a protocol used by Microsoft to share files, directories and devices with the Windows client.

You can configure the Windows Network Settings using the following operating mode:

Workgroup Mode: NAS server becomes a member of a workgroup and communicates with the clients using its internal user database for authentication and do not require other authentication server present in the network.

Domain Mode: NAS server become 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.

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 Ex: 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

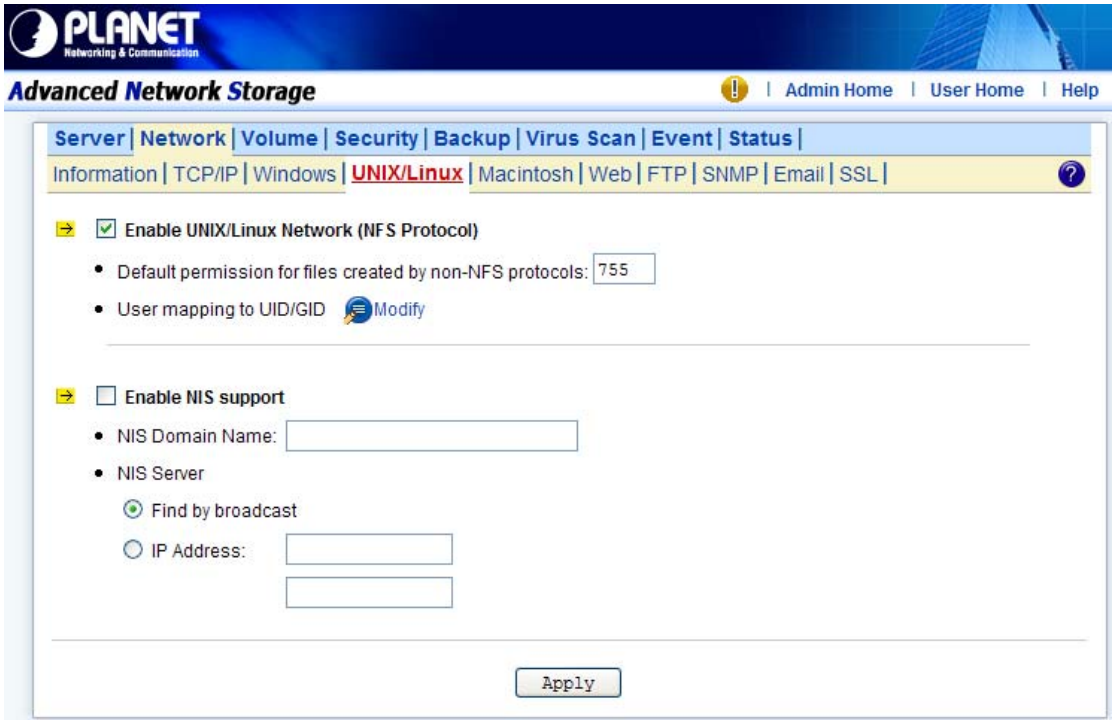
NAS server can export shares to UNIX/Linux client via NFS protocol. UNIX/Linux client then can mount the shares and gain access to the content of the shares. UNIX/Linux client uses UNIX user identification, typically consisting of User Identifier (UID) and Group Identifier (GID), for access control. 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.
UID: User ID. The numerical number assigned to a user in 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

Example: If the permission of a file is set to 777, this file has read, write and execute 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 a NIS server.

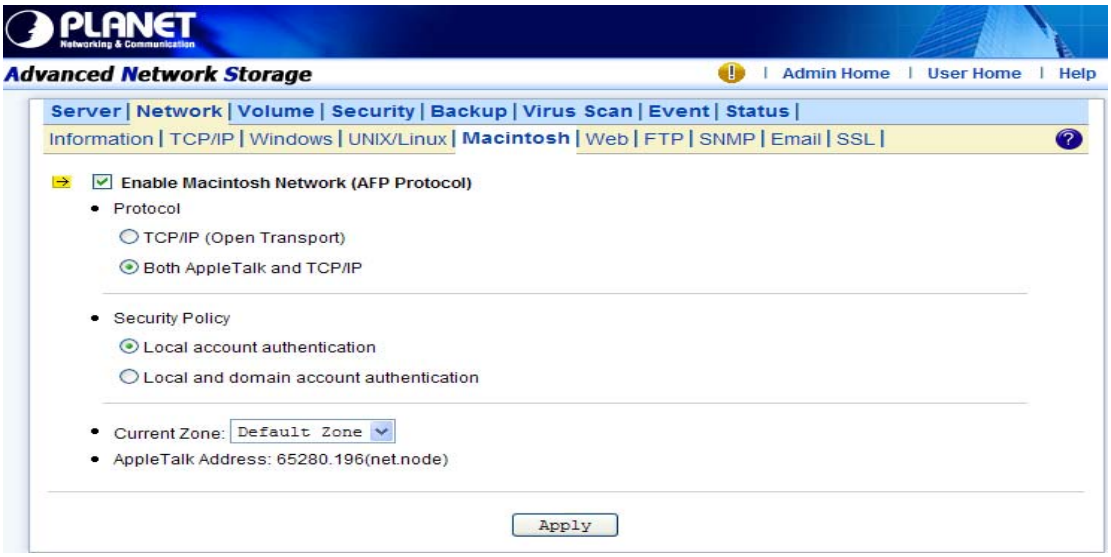
If the NIS support is enabled, the NAS server cans auto-map NIS users with local/domain users. It matches user names and assigns the UID/GID of the matched NIS users to local/domain users. The user auto-mapping function provides better and tighter integration between NFS clients and other network operating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



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.

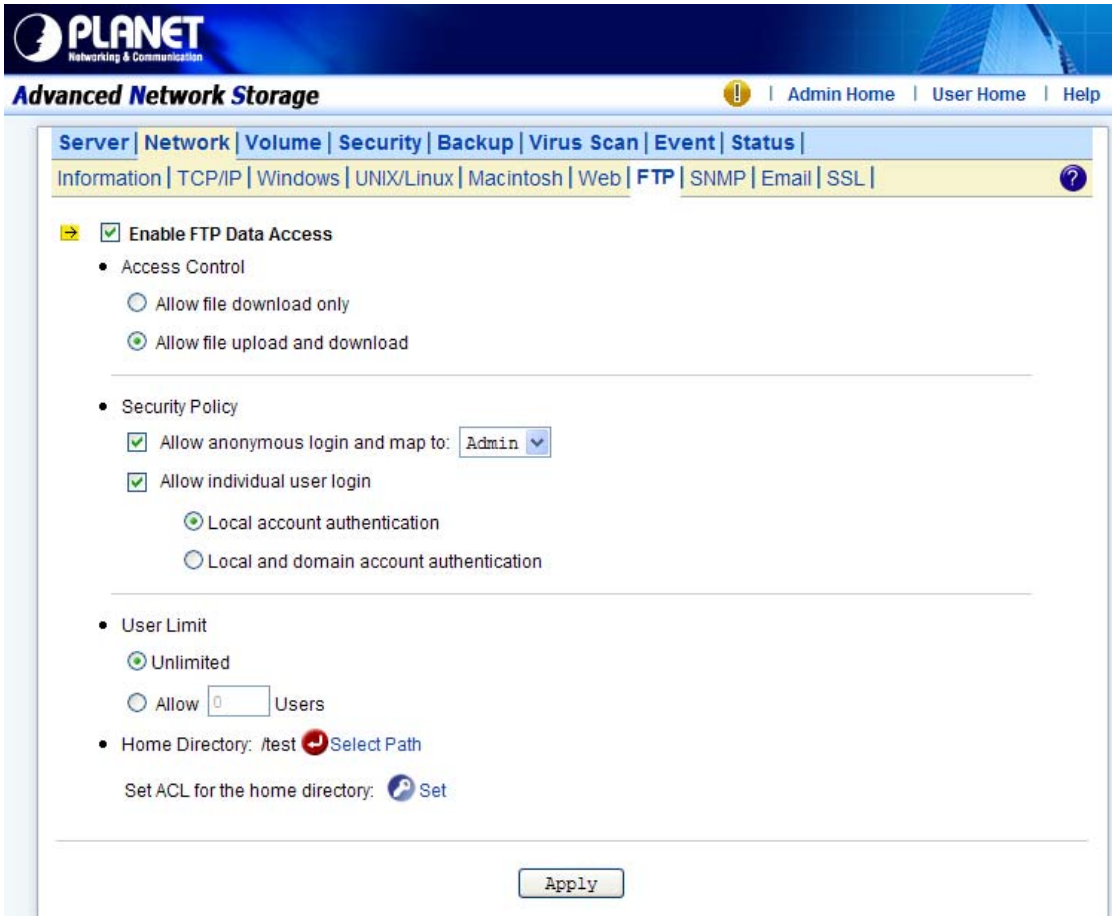
Configuring Web Data Access

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.

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.



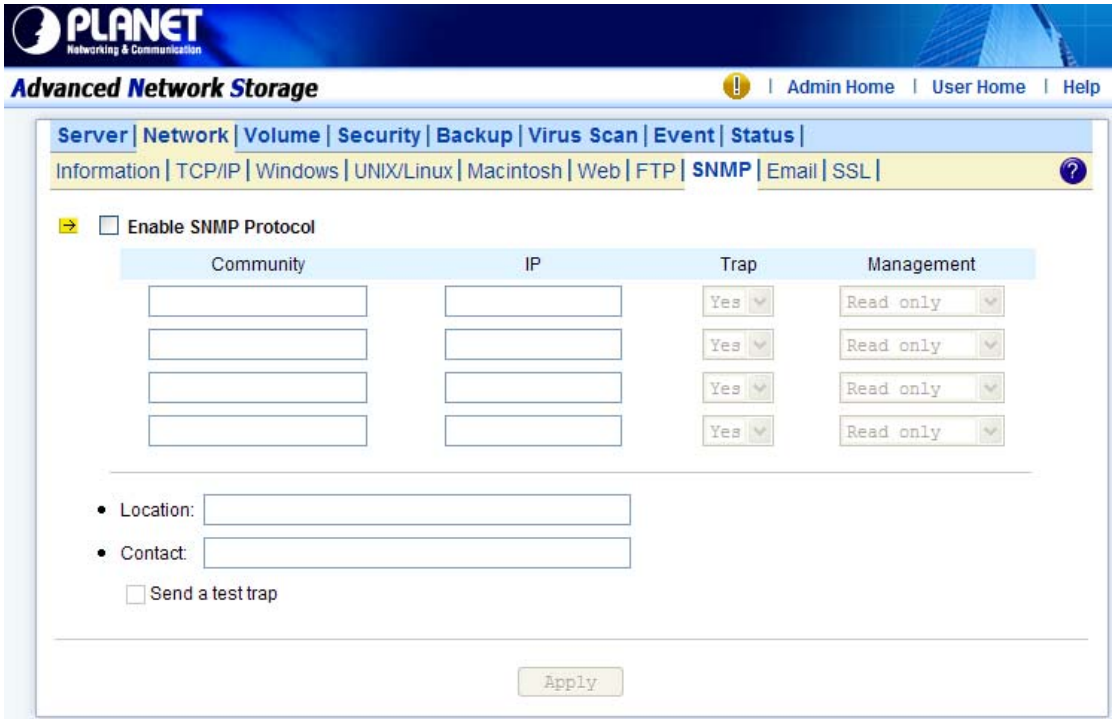
Configuring FTP Data Access

1. Click the “Enable FTP Data Access” checkbox to enable FTP data accessing.
2. Select the “Access” Control type. Click the “Allow file download only” or “Allow file upload and download” radio button.
3. Select the appropriate “Security Policy”. Check the “Allow anonymous login and map to”**:** check-box, and select a local user from the pull down menu. User using the anonymous login will then possess the same security privilege as the selected local user.

4. Or, click “Allow individual user login”. Select “Local account authentication” to authenticate user using the local user database or click the “Local and domain account authentication” radio button to use both local account and Microsoft domain security authentication.
5. Select the “User Limit”. Click the “Unlimited” radio button or specify the maximum number of users allowed to access the content in your NAS server via FTP.
6. Specify the “Home Directory” when user connects to the NAS server via FTP. Note that you must select a volume to create a FTP home directory.
7. Specify the permission of the home directory by clicking the “Set” icon.
8. Click “Apply” to save the setting.

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. The following options should be configured to using SNMP protocol:



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 mismatch.

IP: IP address of the SNMP management console

Trap: A trap is a voluntary message send out from a 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: Provide location information of the SNMP agent.

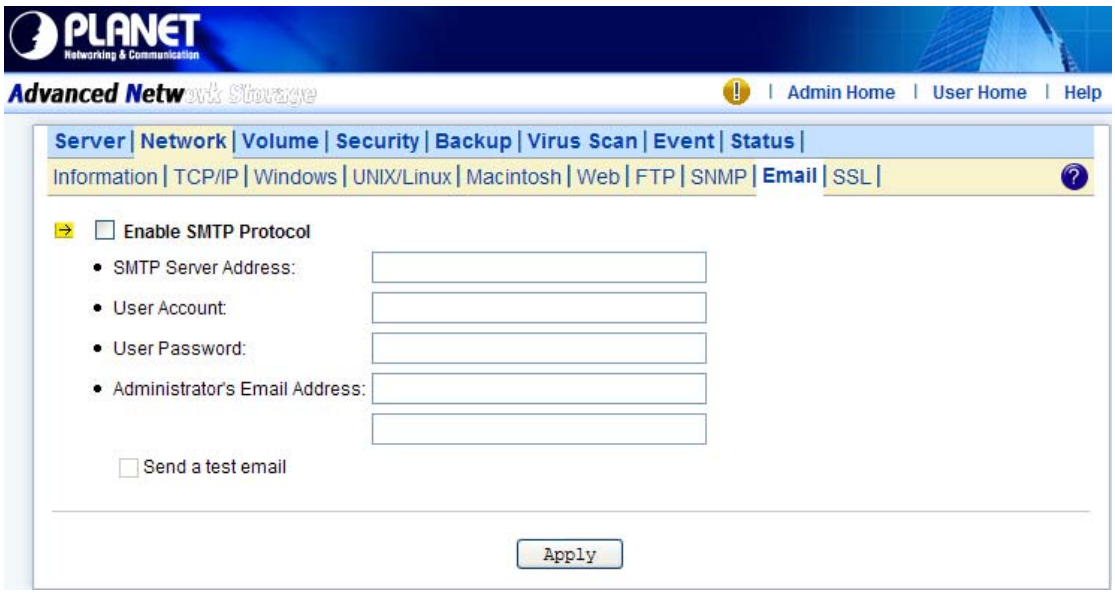
Contact: Provide name of the contact person who has the management information of the SNMP agent.

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 has 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 of to the “Network → SSL” page. Click

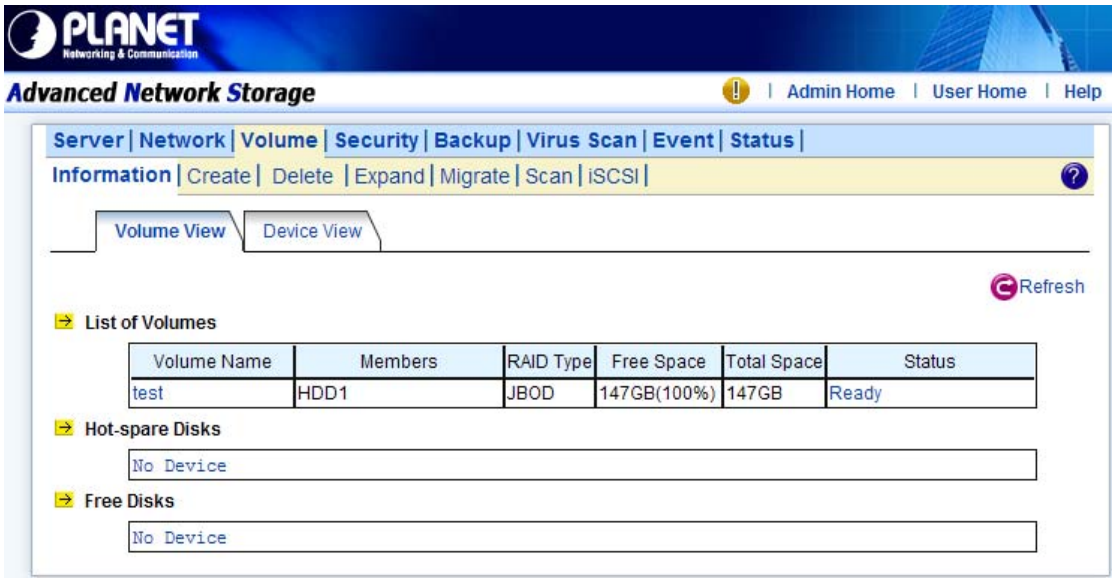
“Download and install CA certificate“ hyperlink. Choose to install the certificate when a dialog-box pops up. Once the CA certificate is installed, the client can access all NAS server s' web pages with SSL connection. Suppose that the server IP address is 192.168.1.100. To access the NAS system's web 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.

Chapter 5 Storage Management

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 Usage and Status

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

1. List of Volumes

It displays all the volumes in the NAS server. “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.

2. Members indicate the hard disks which compose the volume.

3. 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.

4. Free Space indicates the volume usage by showing the free storage space in the volume and the percentage.

5. Total Space indicates the volume size.

6. Status indicates the disk activity on the volume. The disk activity may 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 member 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
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.

7. 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.

8. Free disks

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

9. Volume Details and Renaming a Volume

To change the name of a volume, click its Volume Name hyperlink in the List of Volumes table. It brings to another page for displaying detailed information of the volume. You can modify the volume name on that page.

10. 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 tape drives.

11. List of hard disks

12. In Volume shows to which volume the hard disk belongs.

13. Location indicates the SATA channel position of the hard disk and USB position.

14. Model Name shows the model or the manufacturer of the hard disk. Capacity shows the unformatted capacity of the hard disk.

15. 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.

16. Backup/Archiving Devices (optional)

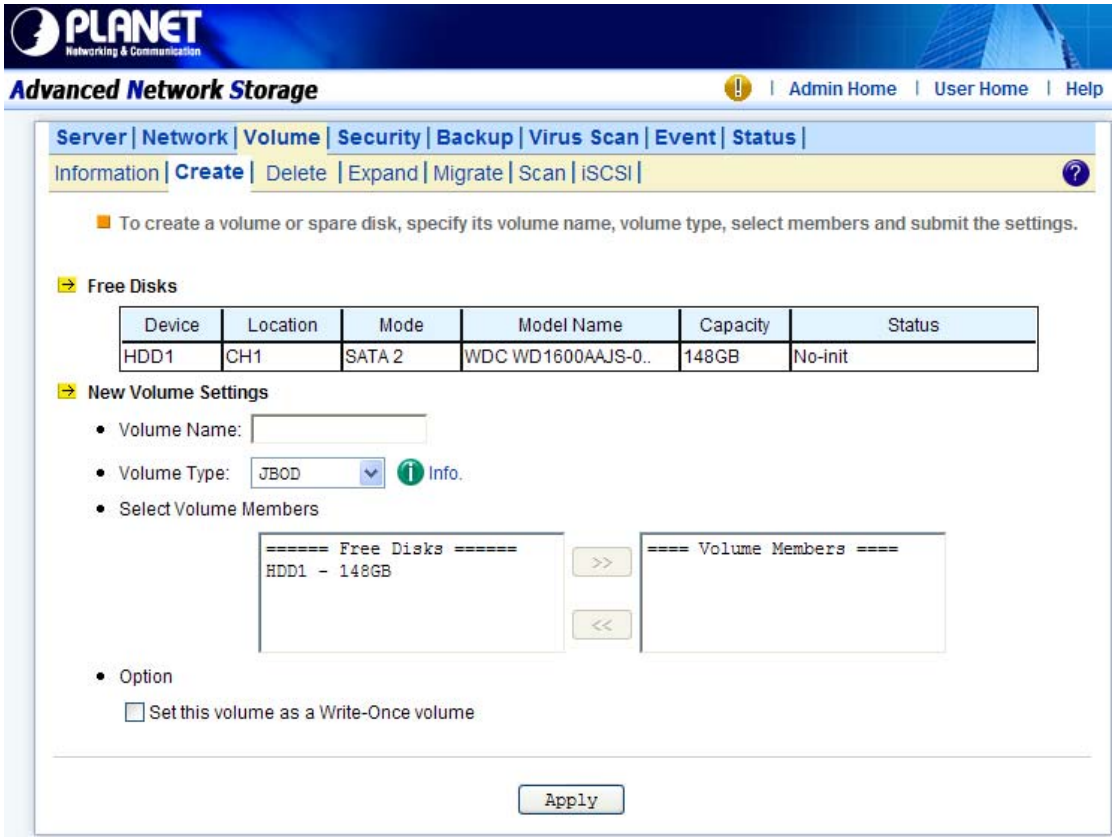
These are either CD/DVD-ROM drives, CD/DVD writers or tape drives. Type indicates what kind of device it is. Mode indicates the data transfer mode of the storage device interface. Device type could be CD-ROM, CD-R, CD-RW, DVD-ROM, DVD+R, DVD+RW, DVD-ROM+CD-RW or Tape.

17. Data Transfer Modes

SATA 1 or SATA 2.

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

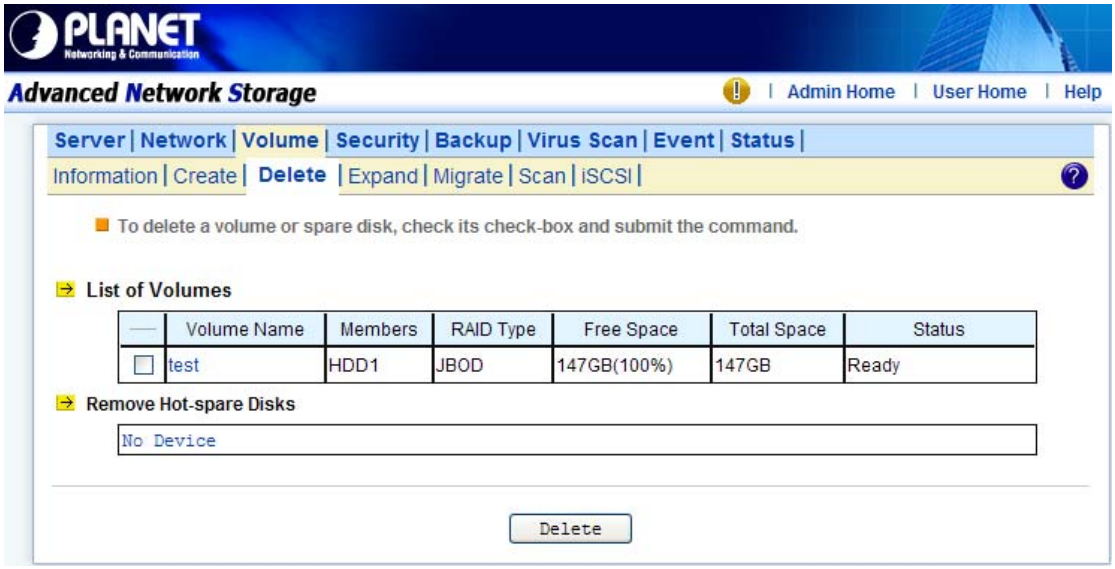
	performance on the level of RAID 0.

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.

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 Volume/Disk Scan

Volume/Disk scan is especially useful for disk diagnostics and repairs lost or cross linked

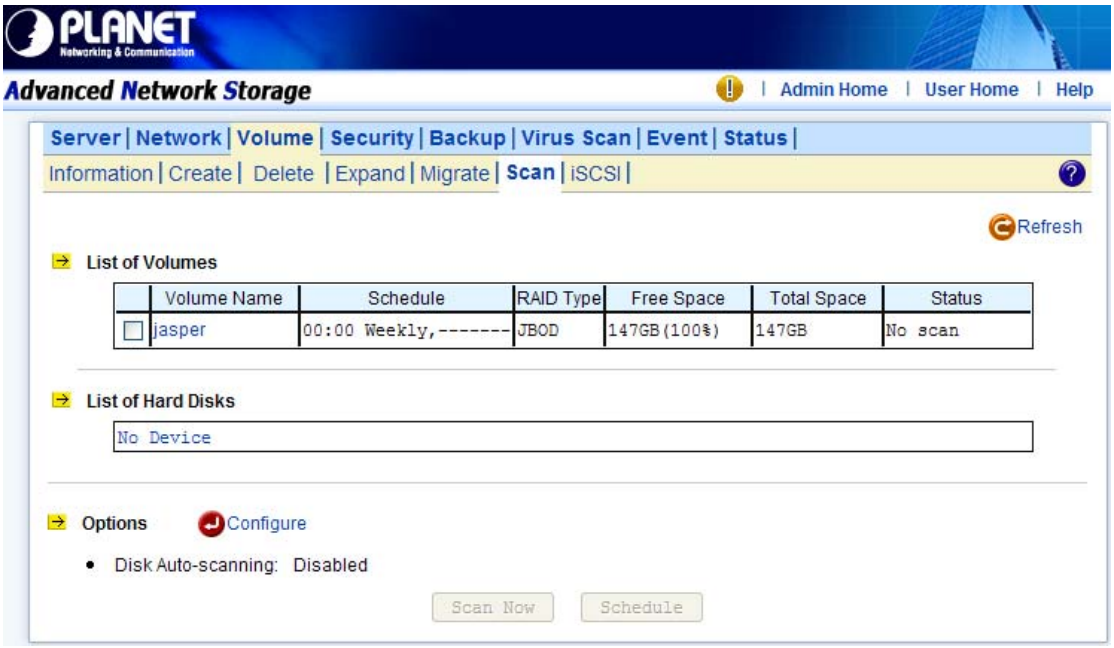
clusters in Volume/Disk. All readable data will be placed in new clusters and defective cluster will mark as bad in the file system. All the newly added devices will be scanned before usage to ensure the data integrity in the NAS Server.

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”.



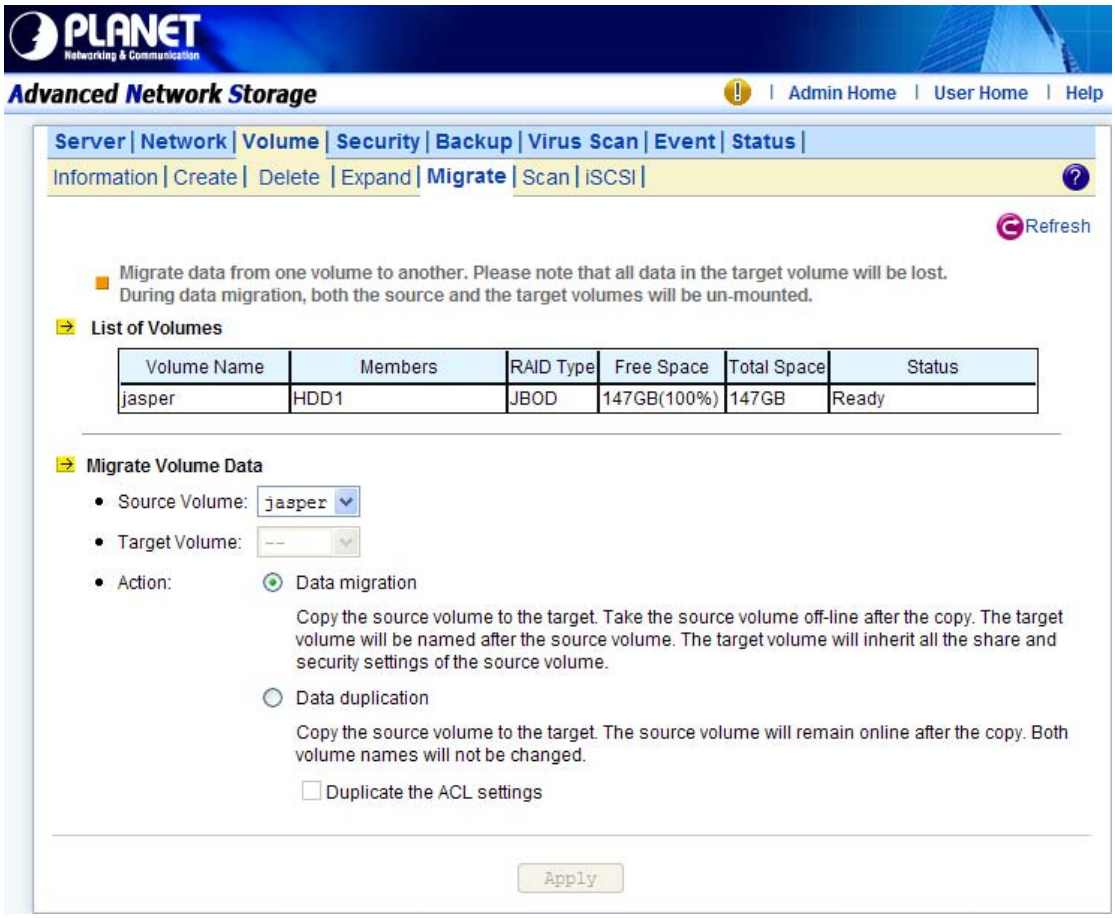
5.6 Assigning Hot-spare Disks

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”.

5.7 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.

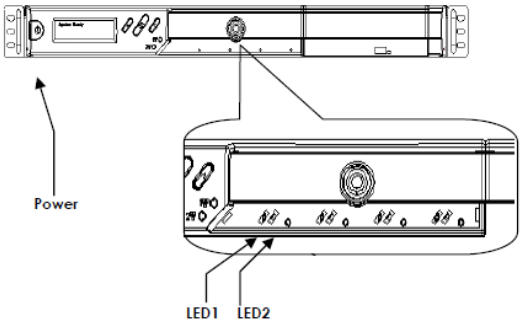
To migrate data, select a source volume, and the target volume to migrate to. Choose “Data migration” and click “Apply”. The target volume will inherit all the security and quota settings of the source volume. No differences will be observed by clients before and after the migration.

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.

5.8 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 if used with NAS-7450 hot-swappable HDD module. Below are the instructions of replacing hard disks when using the HDD module.

For NAS-7450 rack mount model:



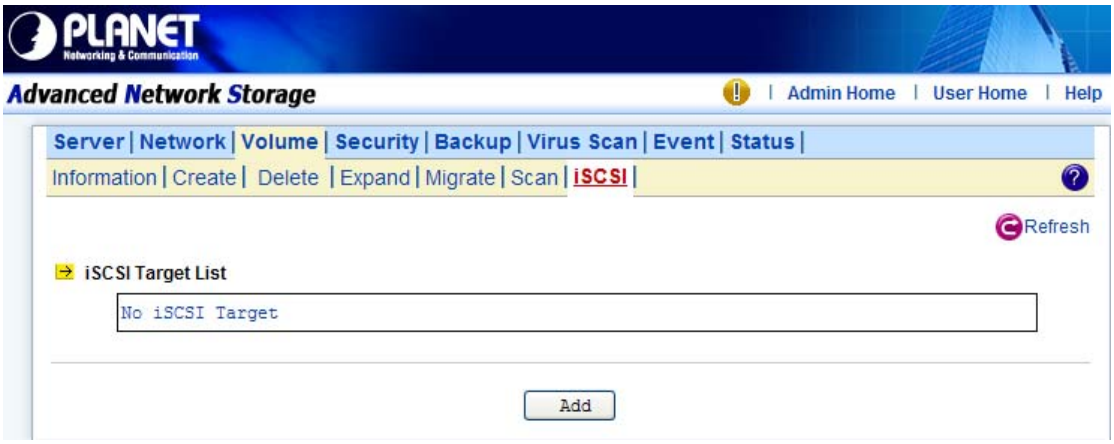
1. Identify which hard disk fails. The amber LED2 will blink to indicate hard disk failure.
2. Unplug the HDD tray and replace the HDD with a good one.
3. Plug in the HDD tray. Wait until the Green LED is steady on.

Then you are done.

5.9 iSCSI

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.

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.

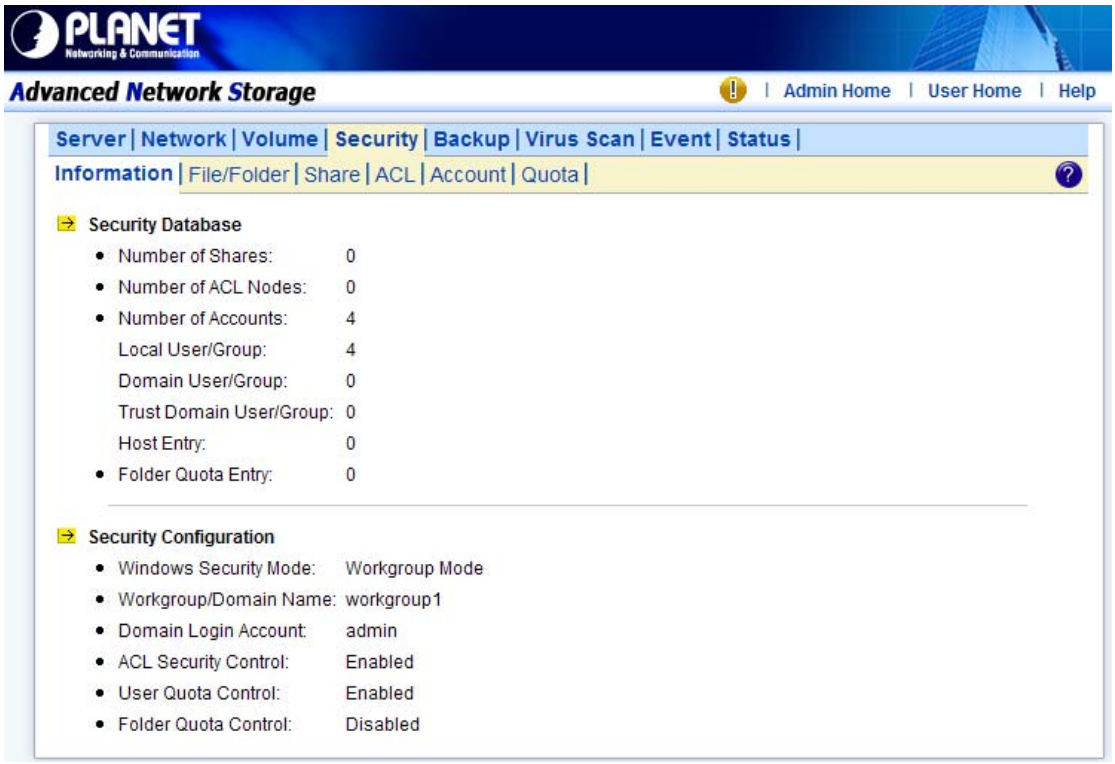
Note:	The NAS supports 8 iSCSI devices at maximum.

4. The LANs 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.

Chapter 6 Security Control

This chapter covers how to setting 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 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 display the number of shares, number of ACL nodes and number of user/group.

Item	Description

Number of Shares	Total number of share created in NAS server.
Number of ACL Nodes	Total number of ACL node 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 User/Group, Domain User/Group, Trust Domain User/ Group and Unix/Linux Host Entry.
Local User/Group	Total number of local user/group. 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 user/group. Domain users or groups are managed by the network administrator.
Trust Domain User/Group	Total number of trust domain user/group.
Host Entry	Total number of Unix/Linux host entered.
Folder Quota	Total number of Unix/Linux host 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 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. To 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, groupA, 1GB, /vol-1/users/user001, 1GB, yes
user002, bb2bb2, groupA, 1GB, /vol-1/users/user002, 1GB, yes
user101, 101101, groupB, 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.

6.3 Caching Windows Domain User Accounts

Domain users and groups are managed by your network administrator. Windows network use a domain controller to store the information of all the domain users and groups. When the Windows Network is set to using 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.
7. Select the domain users or groups from domain user pool and click domain user checkbox.

8. Click “Apply” to save the setting.

Filter Rules:

1. User/Group: You can filter windows domain pool displays domain users or domain groups or all.
2. Domain: You can filter which one domain displays in pool or all.
3. Authorized / Unauthorized: You can filter authorized or unauthorized domain accounts or all
4. Keyword: You can filter domain accounts which you key in some keyword in field.

Synchronize user database

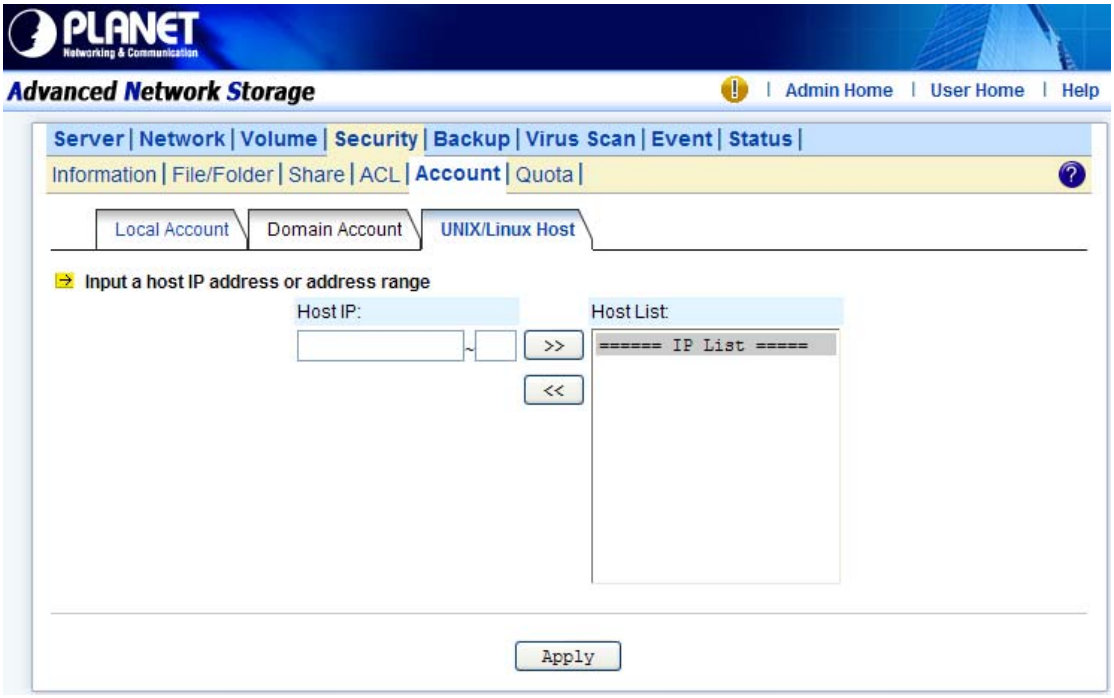
This function synchronizes the domain accounts cached in the NAS user database with the native domain controller. New domain accounts in the domain controller will be added to the NAS user database, while the non-existent domain accounts will be removed from the NAS user database. Due to the limitation of system resource, the user database synchronization will be skipped if there are more than 10,240 domain accounts in the domain controller. To synchronize with 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” functions 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.

6.4 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.

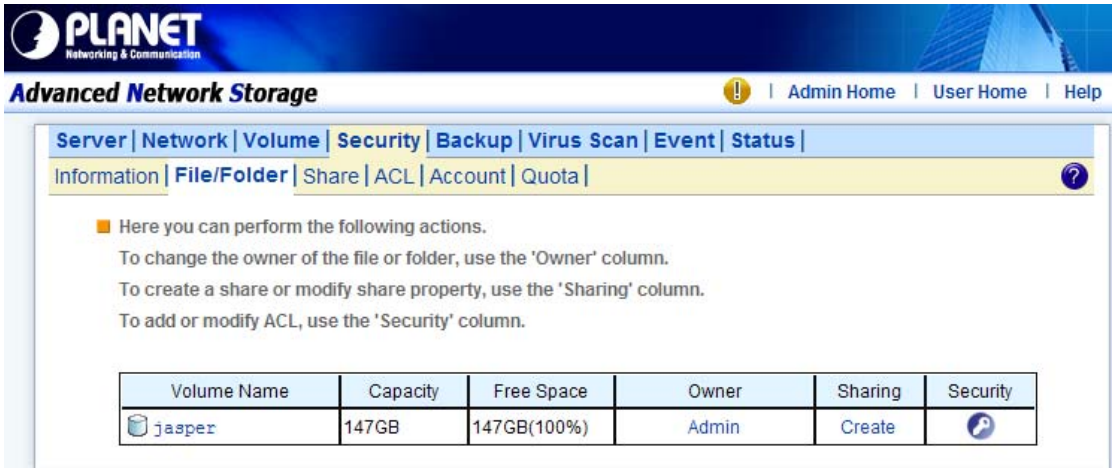


To create a list of the UNIX/Linux host:

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.

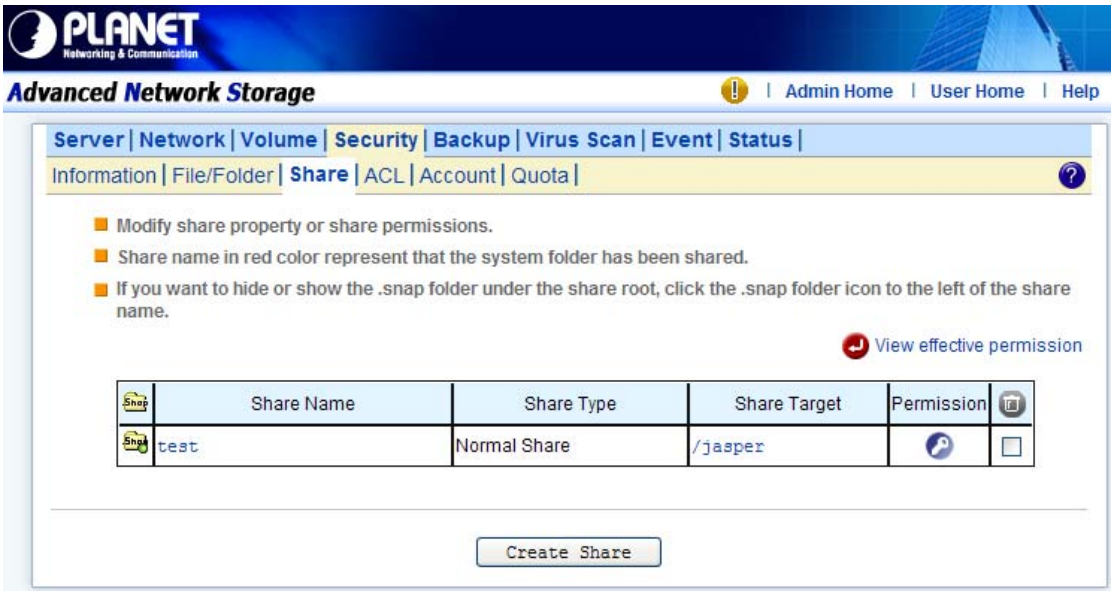
6.5 Creating Share and Assigning Share Permissions

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 desire 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 desire 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 share name in the “Share Name” field. The share 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 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 click the “Modify” hyperlink of the corresponding shared folder.

You can assign the following share permission 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 highlight 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 highlight 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.

6.6 Configuring File and Folder Security and ACL

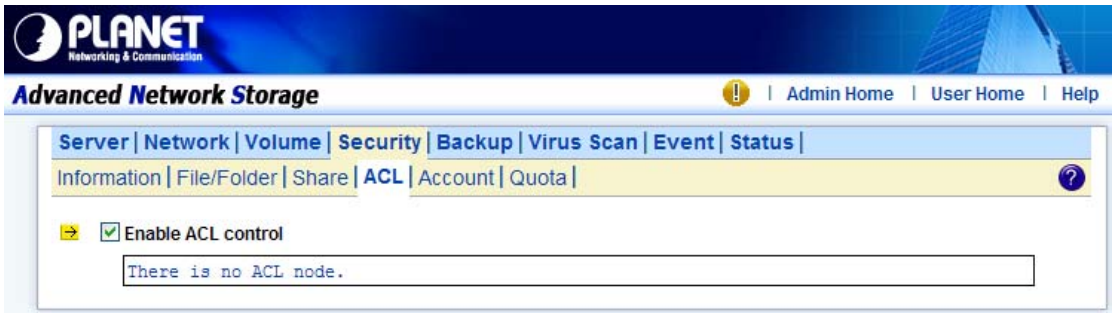
Access Control Lists (**ACL**) are associated with each file and folder, as well as the list of users and groups permitted to use that file or folder. When a user is granted access to the file or folder, an ACL node is created and added to the ACL for the file or folder. If you assign permissions to 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 do 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 do 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.

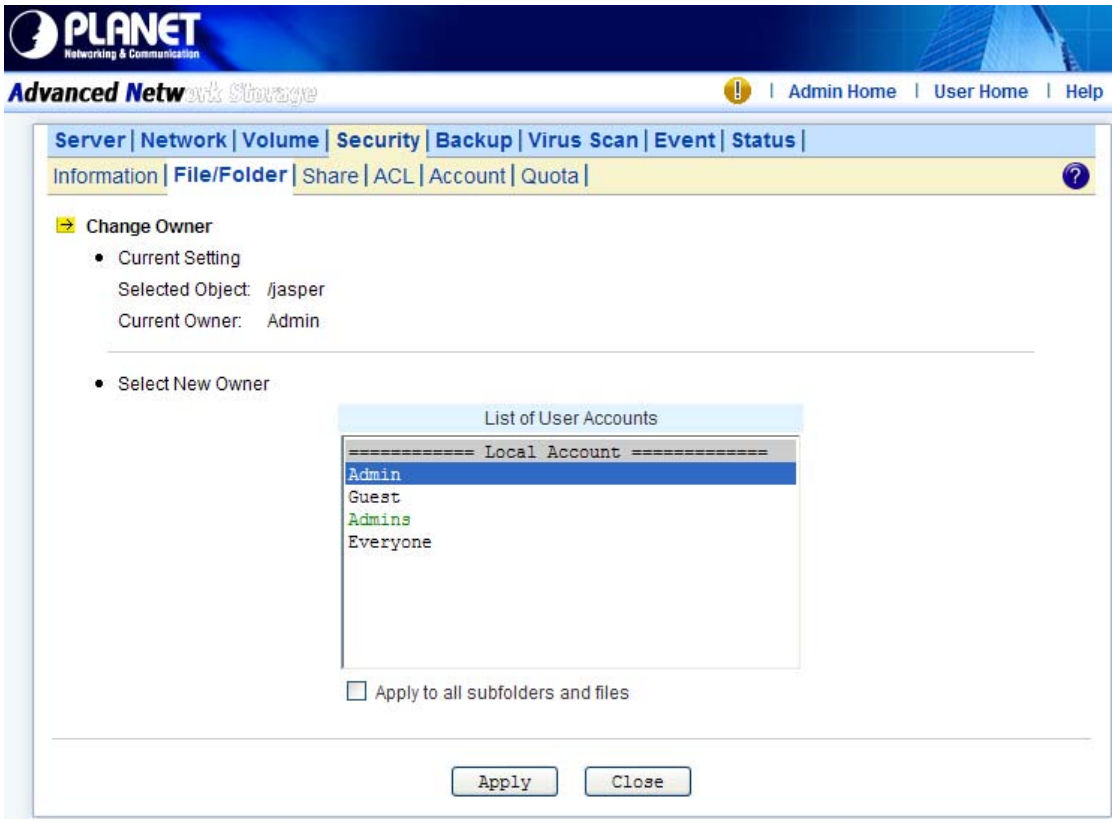
Read Write (RW) – Account is allowed to read and write to the file or folder, but not to delete it.
Modify (MO) – Account is allowed to read, write and delete the file or folder
Full Control (FC) – Account is allowed to read both read and write and change permission to the file or folder. “Set file/folder 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 have been 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

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

Windows Network:

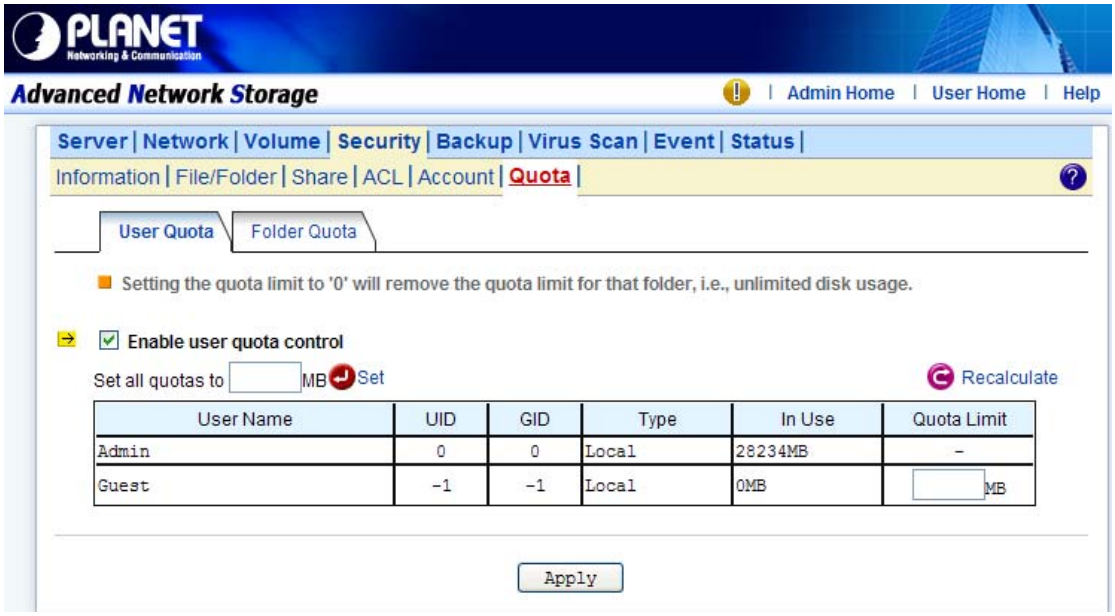
1. Locate the file or folder you want to set permission
2. Right-click the file or folder, click “Properties → Security”
3. Change permission from an existing groups or users; click the “Allow” or “Deny” checkbox
4. Or, remove the groups or users by clicking the “Remove” button.



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.

6.7 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” 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 is it 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 entries 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 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 OS. 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**.

7.1 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.

7.2 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. 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.
2. 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.
3. 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.
4. 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”.
5. 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

7.3 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 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.

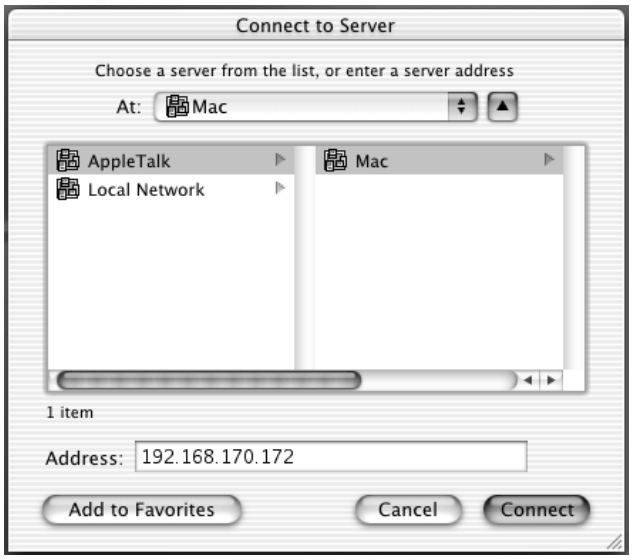
To delete files or folders, check the checkboxes in the "Delete" column. And click the "Delete" icon  to delete them. To rename a file or folder, click the "Rename" icon  , input the name and press the Enter key. If a user has the "Full Control" access right for a file or folder, he can modify its ACL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

7.4 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”.

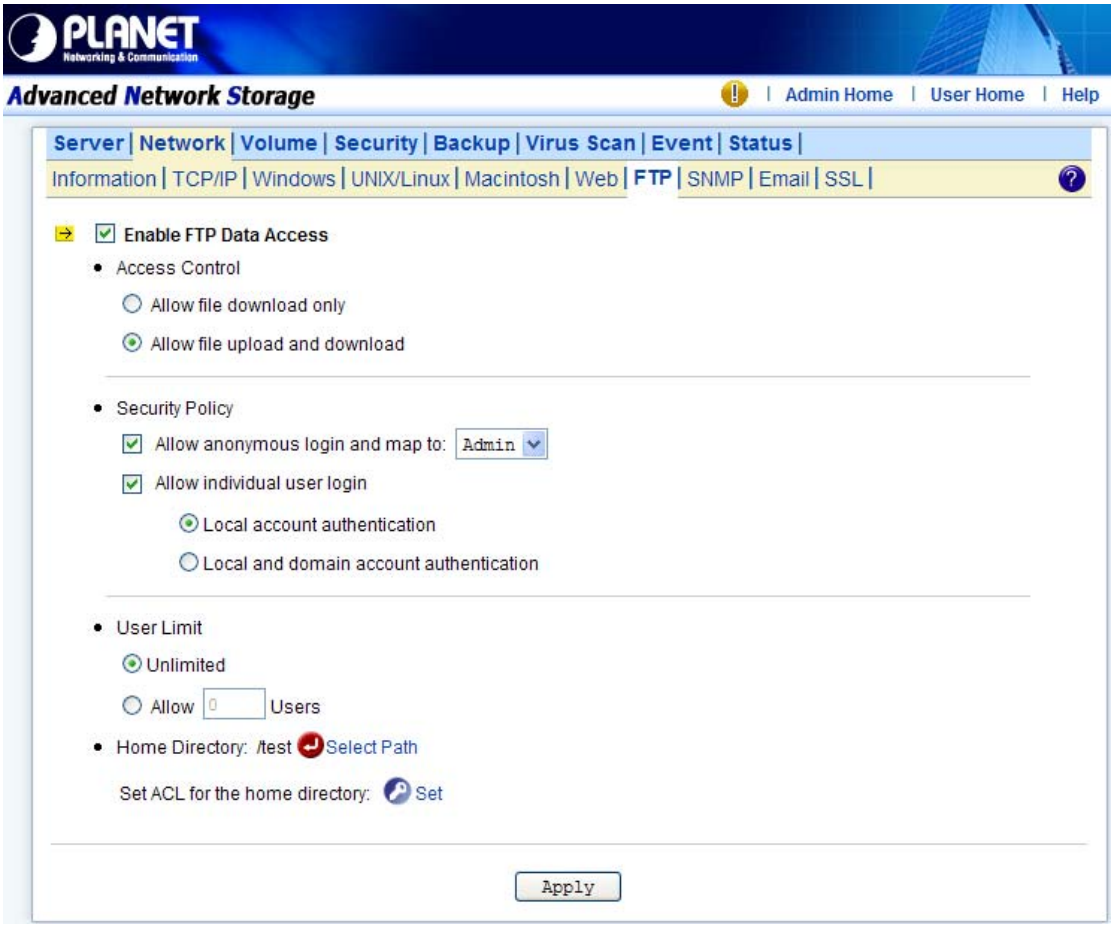


You can either type the IP address of NAS Server in the Address field. And click Connect to put it on Desktop. Or you can click AppleTalk in the middle left window pane to find the zone and

the server. Once you find the server, click **Connect** to put it on Desktop.

7.5 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 ls, 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. Enable the FTP Data Access feature.
   Open the administration page and enter the “Network → FTP” menu. Check the “Enable FTP Data Access” check-box and specify the security policy. In the workgroup mode you can only select “Local account authentication” as the security policy. In the domain mode, you can select either one. Then specify the FTP home directory as “volume01” and click “Apply” to save the settings.
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. Configure the folder security settings of “volume01” to control user access.

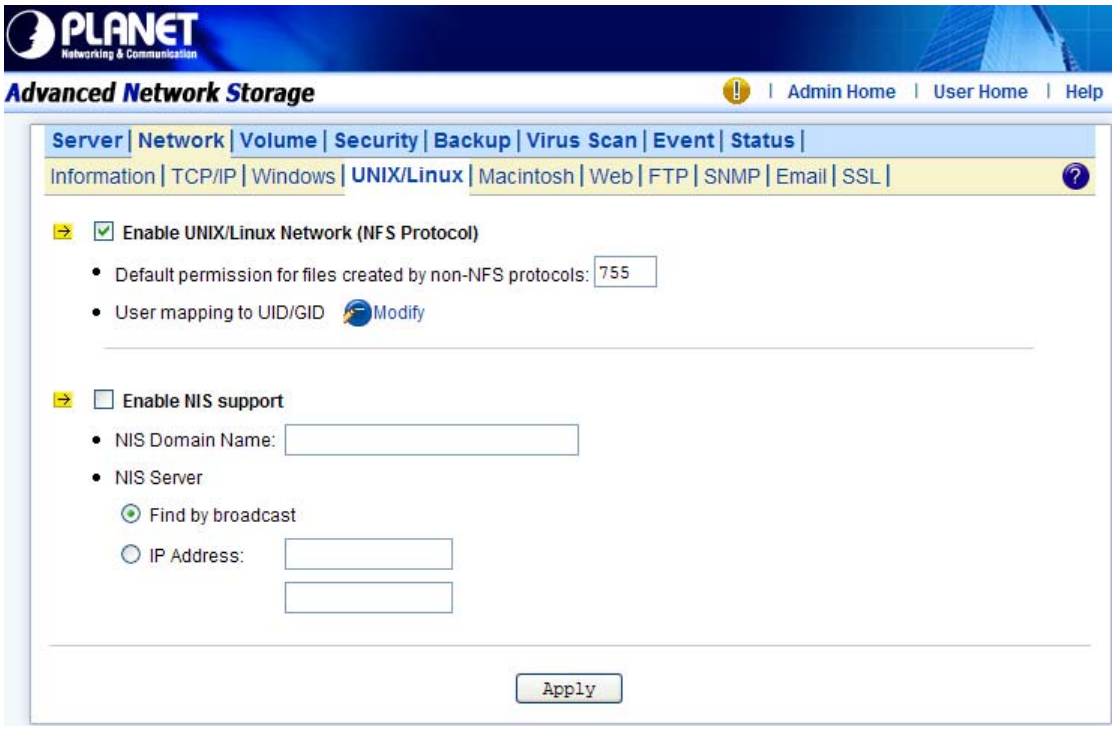
Click the “Set” hyperlink to specify the access rights (ACL) for the FTP home directory –

volume01. These will be the accounts which are allowed to login the NAS using ftp software. Note that the Inherited List will be cleared if you uncheck the Inherit from parent folder check-box and click “Apply” button.

Now, run an FTP client to connect to 192.168.170.172. Login as the user you assign in step 3 above. Then you will be able to access volume01.

7.6 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.



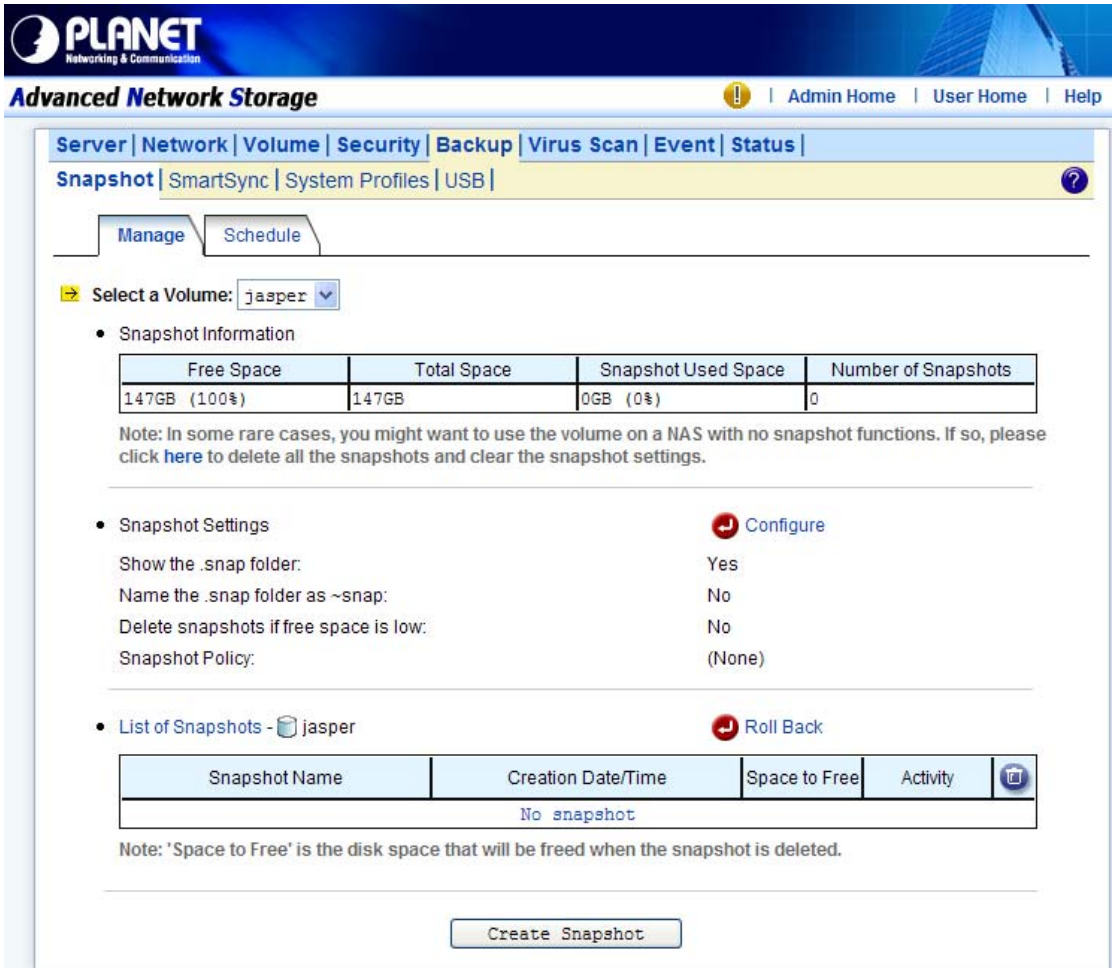
1. Enable the UNIX/Linux Network support (the NFS protocol).
   Open the administration page and enter the “Network → UNIX/Linux” menu. Check the “Enable UNIX/Linux Network” check-box and click “Apply”.
2. Go to the “Security → Account → UNIX/Linux Host” page and add the hosts that might be trusted to 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 8 Backup and Recovery

8.1 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 tape 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.

1. Snapshot Management

To manage snapshots, please open the administration page.

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

2. 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.

3. 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.

4. 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 19:00:00 of October 10, 2004. Another method is to set schedules to create snapshots regularly. Moreover, the NAS server will create snapshots automatically when doing tape 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.

5. 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.

6. 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 from tapes. 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.

7. 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.

8.2 SmartSync – NAS-to-NAS Data Replication

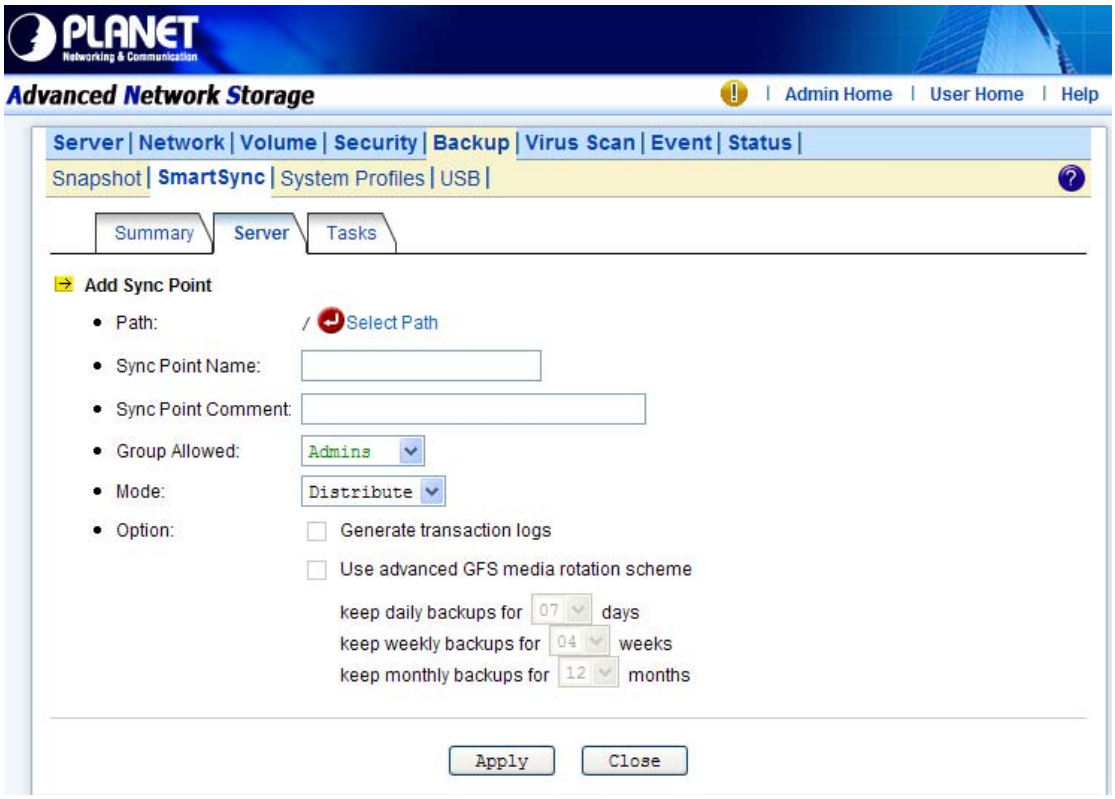
The NAS server is integrated with the SmartSync function for NAS-to-NAS data replication. Two or more NAS server are required, one as the SmartSync server, others as the SmartSync clients. The SmartSync server is like an ftp server. The SmartSync clients can either replicate their data to the SmartSync 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.

Building a Mirror Site

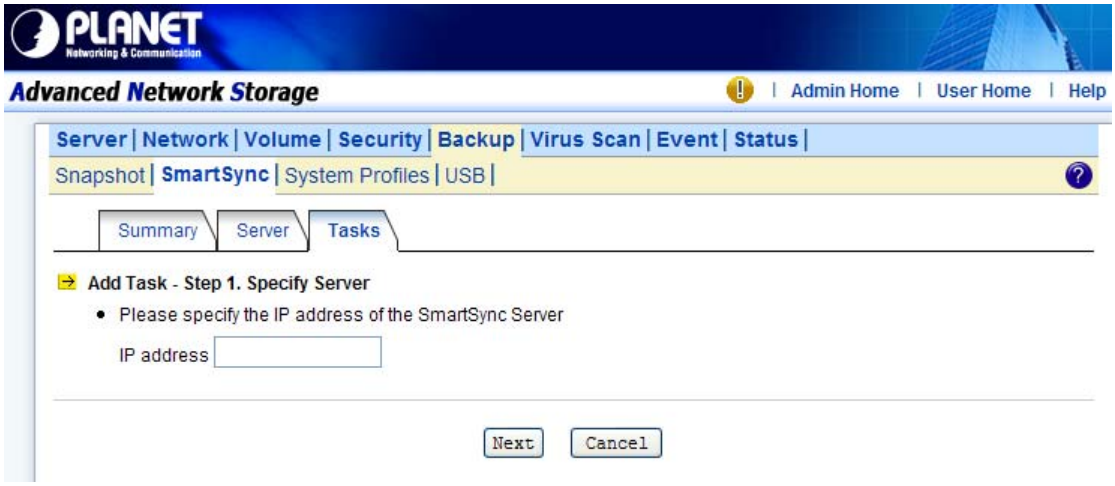
Two NAS server are required, one as the SmartSync server, another as the SmartSync client. It will replicate data from the SmartSync client to the SmartSync server.

On the NAS server which acts as the SmartSync server, create a sync point in it. A sync point is a folder in the SmartSync server which is exposed to SmartSync clients for data replication. A sync point of mirror mode receives data from a SmartSync client and builds an identical data copy 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 "Mirror".



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.

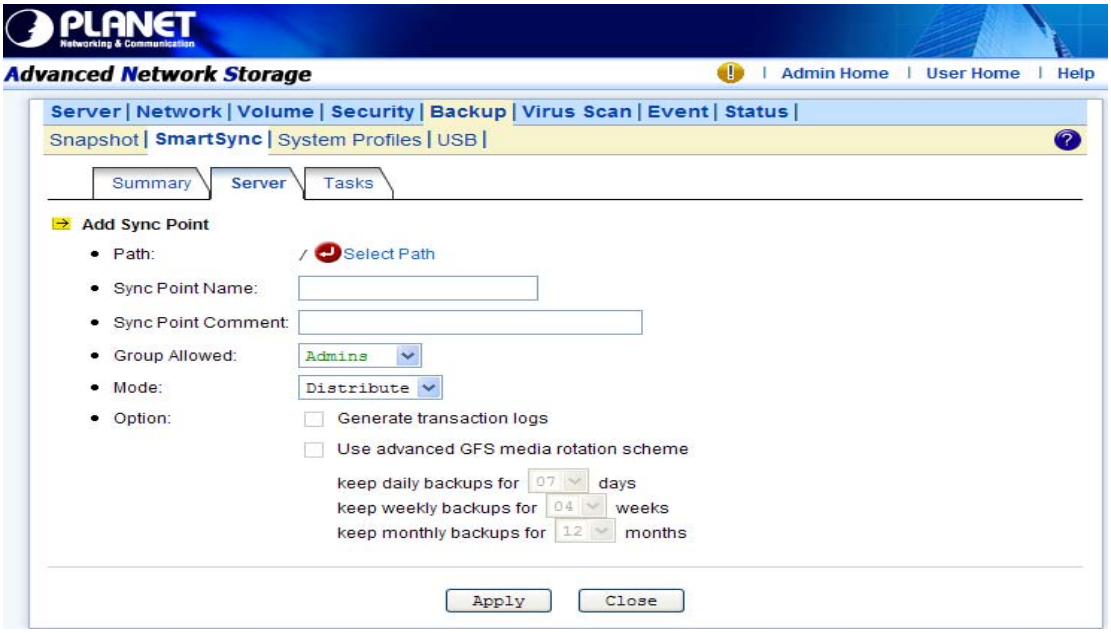
Step 4 is for confirmation, showing the brief information of the task settings.

Making Disk-to-disk Backups

Two or more NAS server 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 as 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.

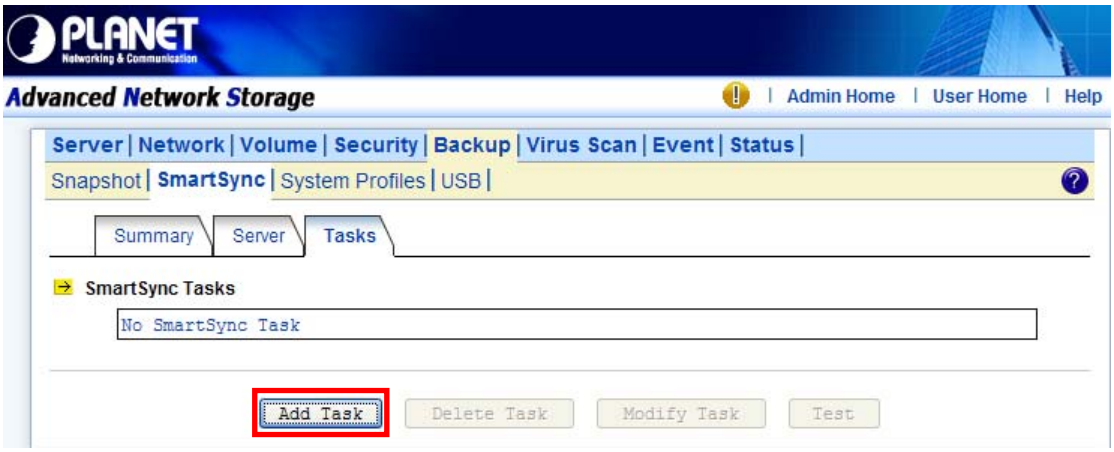
b. It will keep one backup version per day in the last X days, except today.

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.

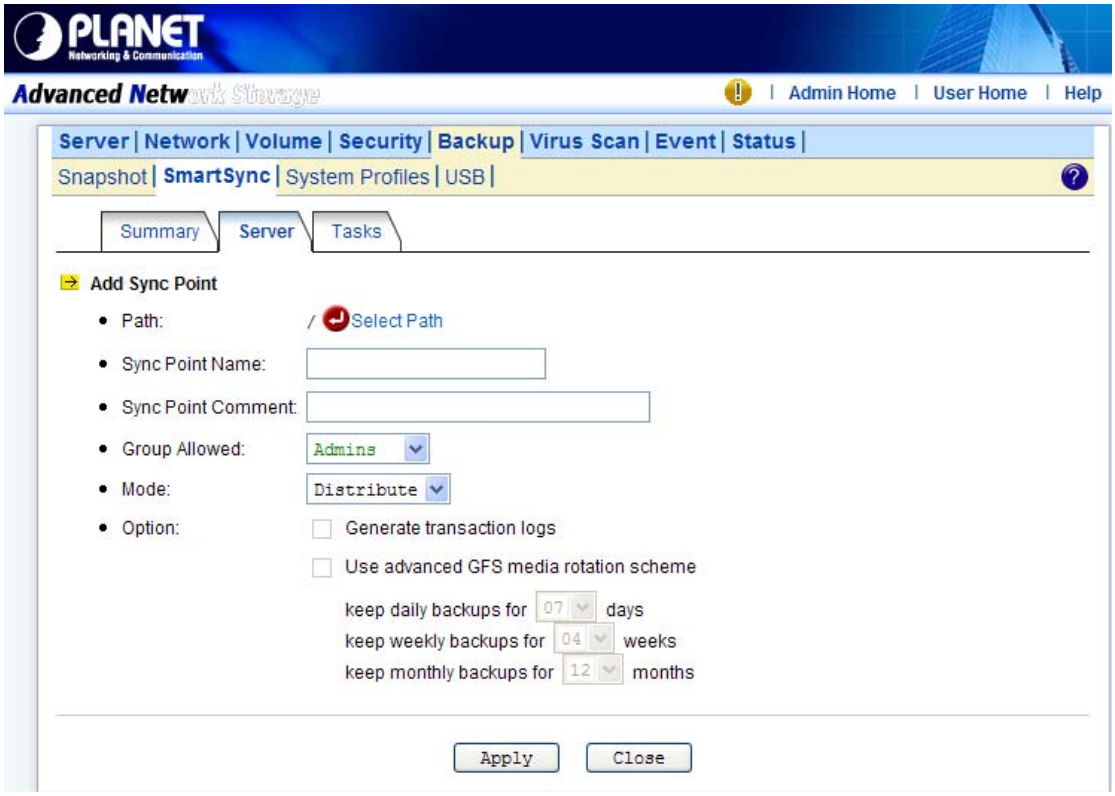
Restoring Files from the SmartSync Backups

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.

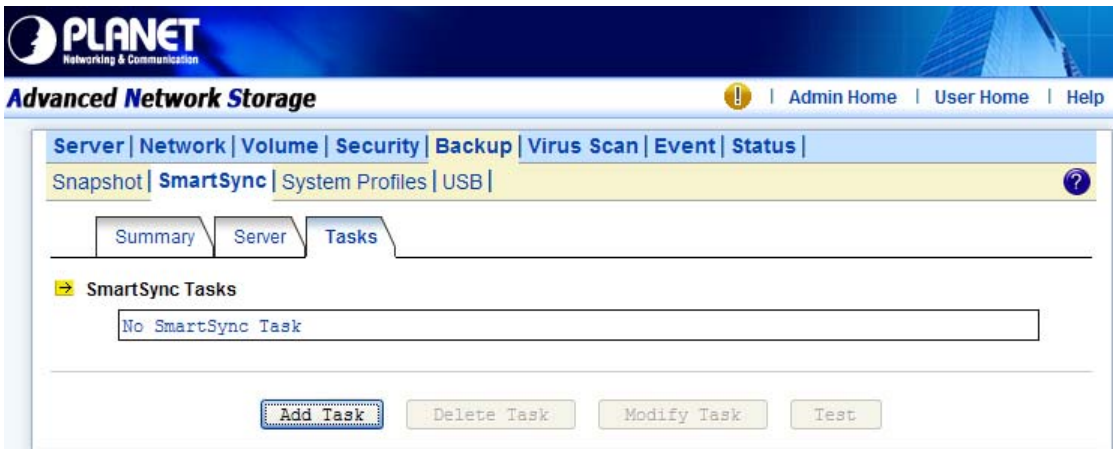
Distributing File Updates to Multiple Sites

Two or more NAS server 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.

• **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.

8.3 Backup and Restore System Profiles

To recover from system failures, it requires restoring data and system configurations. Tape 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 the “An external file” item and find the system profile. Specify restore options and click the “Restore” button.

Restore options are:
• 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.

8.4 Backup USB Device

NAS server supports USB pen drive and external hard disk (support FAT/FAT32 only) backup in optional models with USB ports. The front penal will display to ask if you want to process USB backup or not when plugging in a device. System will jump out the display without any inputs in 60 seconds. You can also activate this function via web interface.

Enable USB Backup

Plug in the device and check the 'Enable USB Backup'. You will see the menu for selecting the source folder and the target folder.

Click 'Select Path' by Source Folder to select the entire drive or individual folder in device you want to backup.

Limitation

• This function doesn't support the CARD Reader.

• One drive supports 3 partitions.

• Please unmeant the USB device before removing, or the data may be damaged

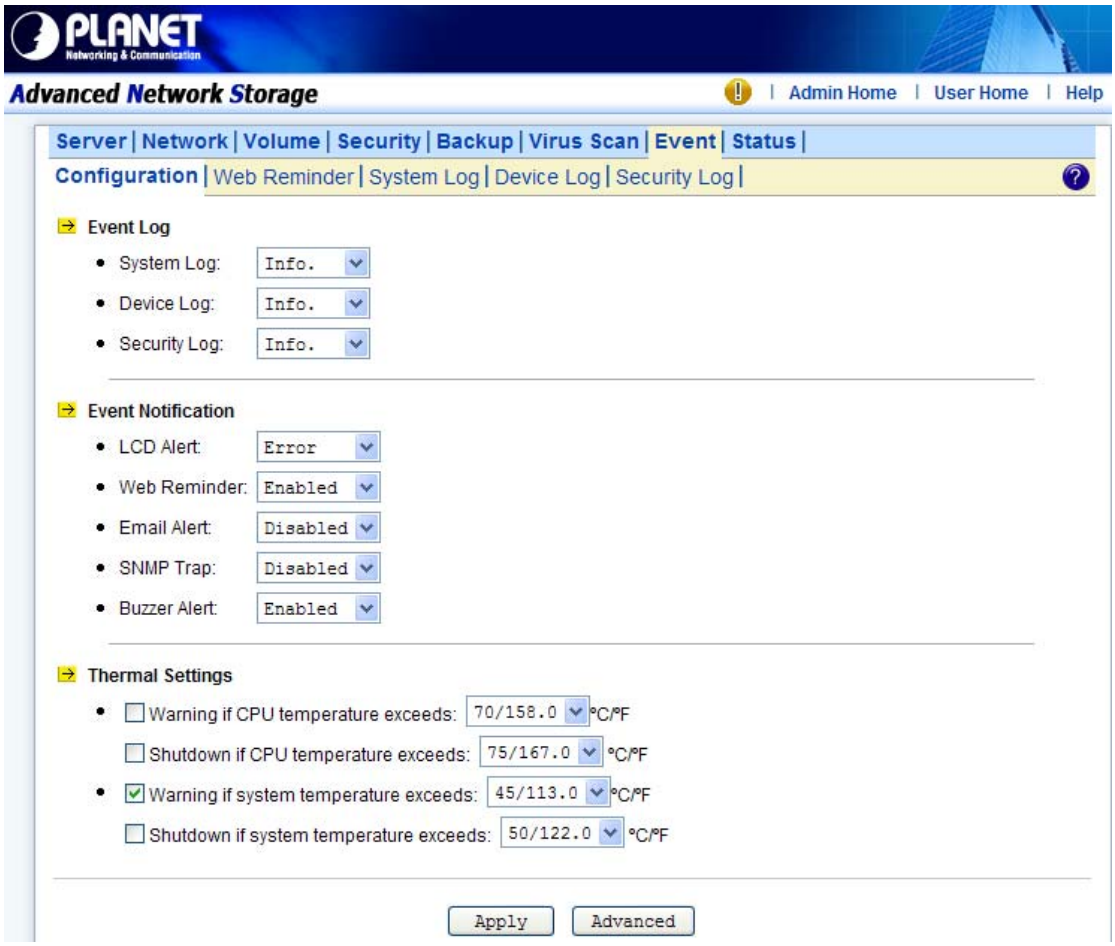
Chapter 9 Event Logs and System Status

This chapter covers the Event Notification and System Status pages. You can collect information about the system, hardware and security event of you NAS server. NAS server records three kinds of logs:

• **System Log**

• **Device Log**

• **Security Log**



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:

• LCD alert – provides warning and error level notification:

- 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.

• 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 build-in buzzer in NAS system when event occurred. To turn off the buzzing sound, either press any button on the LCD front-panel or 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.

9.1 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 Fan Control” functions only on NAS-7450/NAS-7850.

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

9.2 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

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

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”  or button to refresh the screen.
4. Click “Clear” or  button to clear the log.

Viewing Device Log

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”  or button to refresh the screen.
4. Click “Clear” or  button to clear the log.

Viewing Security Log

In the “Event → Security 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”  or button to refresh the screen.
4. Click “Clear” or  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.

9.3 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. In “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:

• **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”:

• **Current Connections** – configure and show the protocol used by the client that is currently connecting to the NAS server by click 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 open files.

• **Disconnect** – disconnect a particular connection by check the disconnect check box and click the  icon.

Viewing the System Load

In the “Status → Load”:

• **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 are showed on here.

9.4 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, event 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 tape, 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 save 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.

9.5 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, MacOS clients.

There are several share types.

Normal Share – indicates a shared folder in any data volume.

System Share – indicates the MIRROR share which holds all CD/DVD volumes.

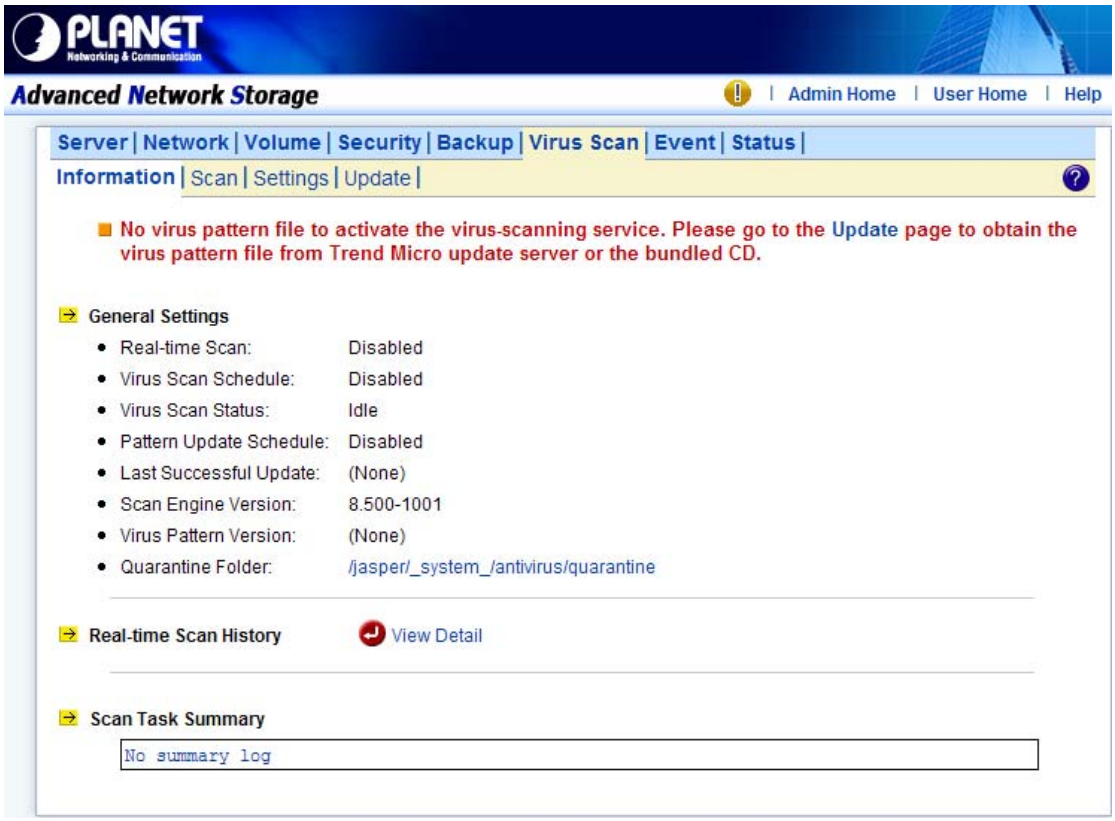
Disc Share – indicates a share of a single CD/DVD volume.

Group Share – indicates a share of grouping of several CD/DVD volumes.

Disc Folder Share - indicates a share of disc image folder.

Chapter 10 Virus Protection

Most storage systems are vulnerable to virus attacks. An infected file in you NAS server can be exchanged among the clients system in the network and 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 display the date time that the virus is found, virus name, action taken and the full path name of the infected file. And, the scan task summary display 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

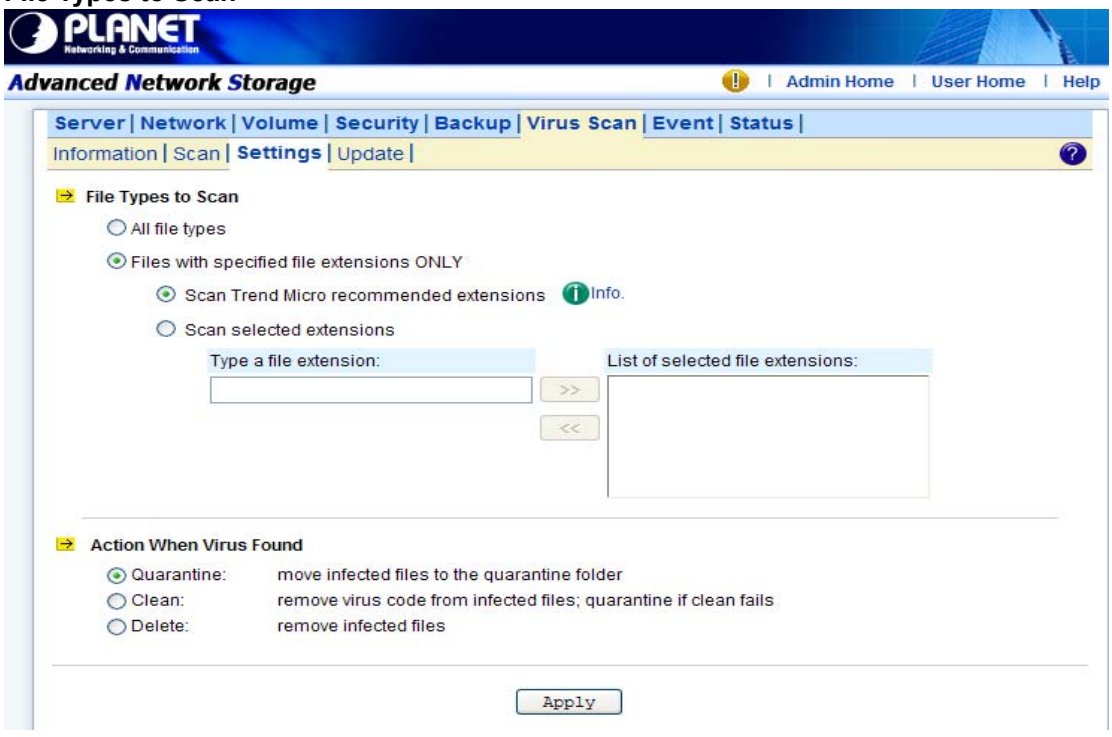
1. Click the “Enable Scheduled Scan for Infected Files” checkbox to enable scheduled scanning.
2. Click the “Select Folders” hyperlink to specify the folders you want to perform the scheduled scan.
3. Configure the start time and recurrence pattern for the scheduled scanning.
4. Click “Apply” to save the settings.

10.3 Configuring Scan Settings

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

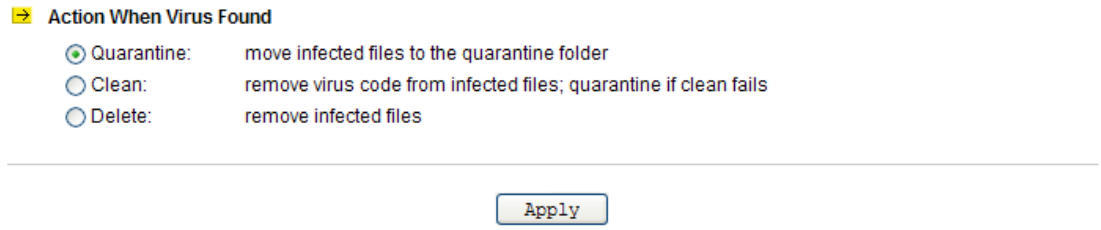
- File Type to Scan – you can limit scanning to specific file types.
- Action When Virus Found – three actions (quarantine, clean, delete) can be chose from when virus is found

File Types to Scan



1. Click the desire scan file type.
2. If “All file types” is selected, all files regardless to its file extension will be scanned.
3. If “Files with specified file extensions Only” is selected, specify using the recommended 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 desire action when virus was 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.

Appendix A Troubleshooting & Frequently Asked Questions

Device	
What kind of OS is used in NAS-7450 / 7850?	NAS-7450 / 7850 are equipped with the Linux-based OS that is optimized for networking storage. Planet develops the OS to be seamlessly integrated with its own SlimServer technology.
Are the OS of NAS-7450 / 7850 stored in the hard disk drive?	No, OS of NAS-4750/7850 are not stored in hard disk drive. Instead, OS and system configuration information of NAS-7450/7850 are stored in the CF Card.
Is there any storage management function provided of NAS-7450/ 7850?	RAID management, disk quota and scan disk are management functions provided for NAS-7450/7850.
What about user license of NAS-7450 / 7850?	Unlike other OS, there is no user license fee based on the user number. What you pay includes the hardware and OS of NAS-7450/7850 that can be used in any kind of networking environment.
RAID	
What RAID policy dose NAS-7450 / 7850?	NAS-7450/7850 supports three RAID policies: **RAID 0:** Stripe/Span. (2 ~ 8 hard disk drives). It interleaves data 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 – 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.
Should the hard disk drives be connected onto the same SATA channel while creating a	No, you can group any hard disk drives (No Init) that are available on the SATA channels of the NASt-7450/7850. 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-7450/7850 and you want to create two RAID level 5 devices. RAID group A should

RAID device?	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).
Device management	
What kind of device interfaces can NAS-7450 / 7850 support?	NAS-7450/7850 supports CD/DVD-ROM, CD-R/RW, DVD+-R/RW, Blu-ray, Dual-layer and hard disk drives of SATA interface.
How to operate CD-R/RW devices and DVD+-R/RW devices on NAS-7450 / 7850?	You can find two functions within Admin Home page of NAS-7450 / 7850 that are “Writer” and “Loader” for backup or restore data.
Event Log and Notification	
What is “Web Reminder”?	When the NAS-7450/7850 occurs some critical events, you will find a message “There are critical events. Please Check Web Reminder page.” in Admin Home page. The intention is reminding administrator to check those critical events as most quick.
How can I send an email event to administrator?	You can follow the steps below to set up email event: 1. Go to NAS-7450 /7850 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 had set DNS server IP address inside NAS-7450 / 7850.) 5. Fill in a legal user account for login SMTP server purpose. 6. Base on your need; fill in one or two Email Address. 7. Click “Apply” 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.
Power management	
Doss NAS-750 / 7850 supports UPS system?	Yes, NAS-7450 / 7850 can integrate with UPS power management via smart signaling as well.
What power management features dose the NAS-7450 / 7850 support?	The NAS-7450 / 7850 have supported the following outstanding features on power management if an ATX power supply is engaged. For example, “UPS control to shutdown”, “safe shutdown”, “schedule shutdown”, and “schedule power ON”.

Security	
Dose NAS-7450 / 7850 support "file level" security control?	NAS-7450 / 7850 can set security permission via ACL (Access Control List) and applicable to shared folders and files.
How many user accounts can be stored in user database of the NAS-7450 / 7850?	Up to 20,480 accounts information can be stored in the NAS-7450 / 7850, which include local accounts and domain accounts.

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 was 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

Installation

◆ 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 startups, NAS Finder automatically discover all the NAS systems on the network and display a list of server 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”

Or, go to “Server -> Import System Settings” menu.

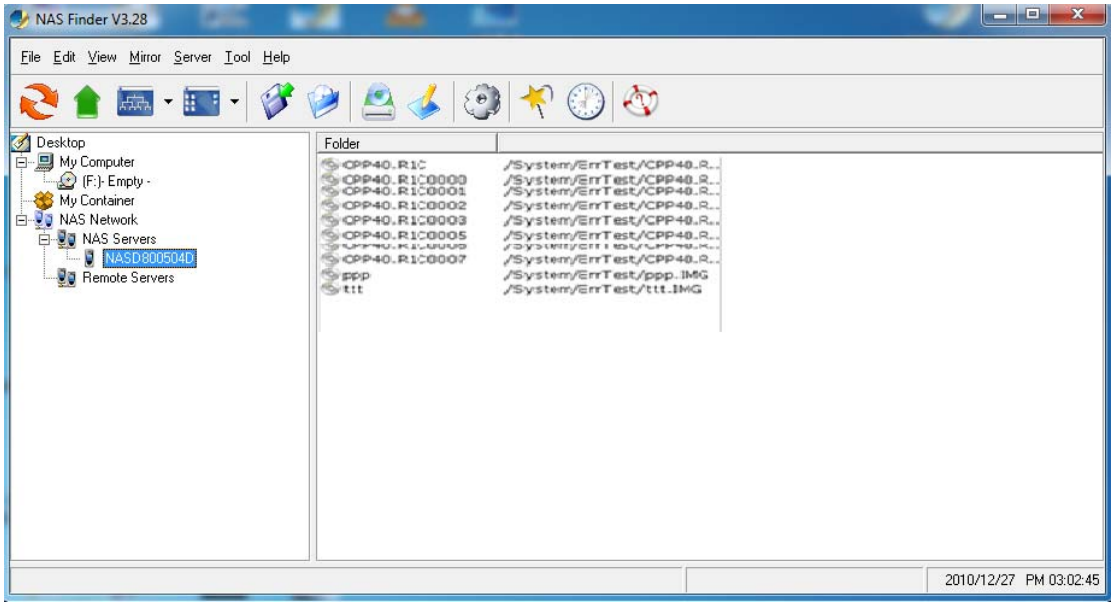
3. You will prompt for the administrator password to proceed.
4. You have the option to select a server or an export file as the source.
5. Click “Next”.
6. Select the type of system settings you want to import into the target server. The detail content of the system settings are displayed in the preview text box beside each selection.
7. Click “OK”. NAS Server will reboot automatically.

● **Browsing & Administering Servers**

◆ **Browsing Servers**

Below is the main window of NAS Finder. Upon execution, NAS Finder brings up Windows Explorer for you to drag & 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.

On the tree view pane are listed 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 & information. The left of the status bar shows function hint or item properties. To the right it displays the PC date and time.

You can browse the Domain Name, IP Addresses of each NAS Server just by mouse over it.

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:

NAS Network: display all the NAS Servers found on the LAN.

NAS Server: represents a NAS Server

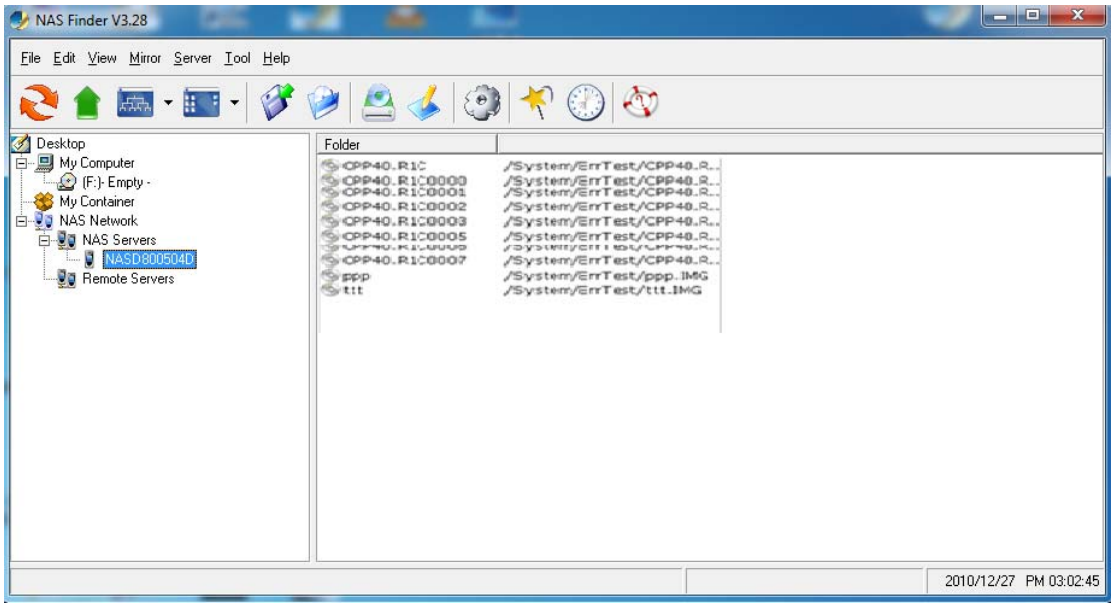
Disc Image Folder: contains disc images of the NAS Server. You can double click to

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.


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 shrink 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.

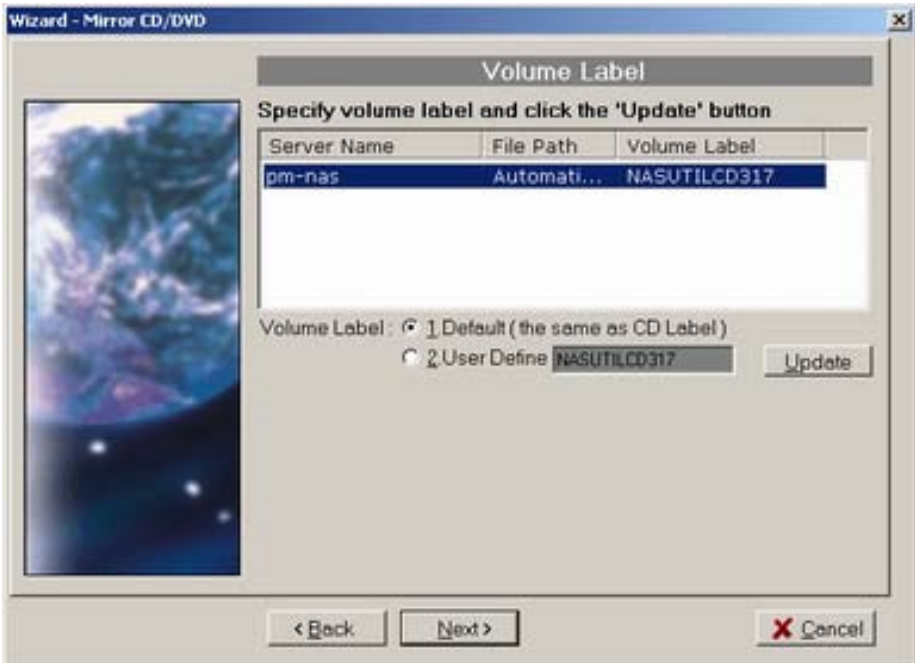
● Mirroring CD/DVD Remotely

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.

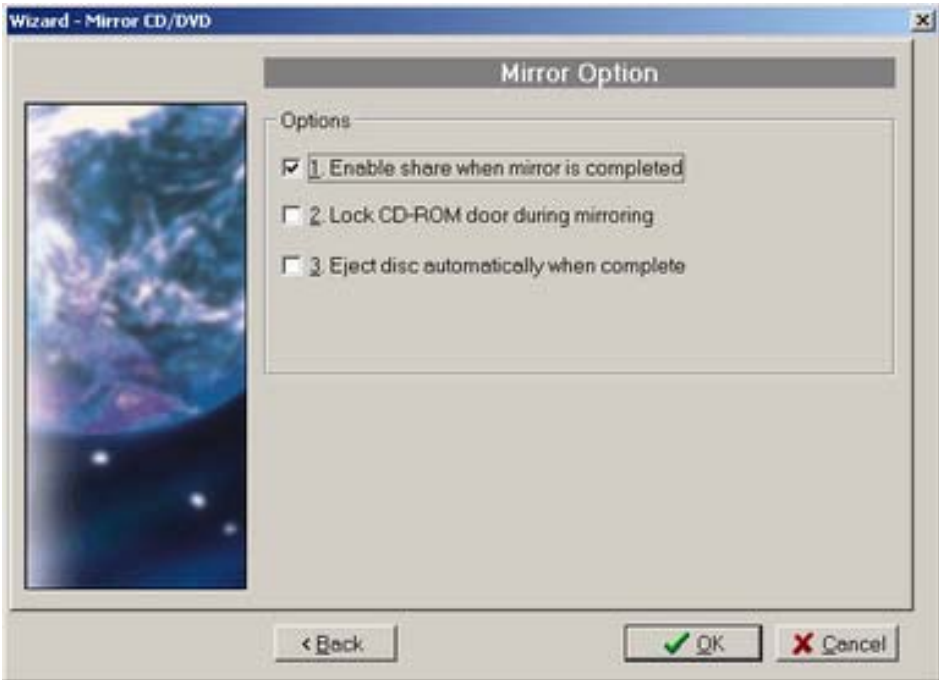
2. Choose one or more servers as the destination. Select a server in the “Target & File Path” list-box, select “Smart” mode for redundancy check of the CD image or select “Force” mode to allow a second copy of the same CD image.
   Then, click the >> button. You can see the task being added to the right-hand 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 the “2. User Define” radio button and enter the volume label in the input-box. Then click the “Update” button. Click the “Next” button afterwards.

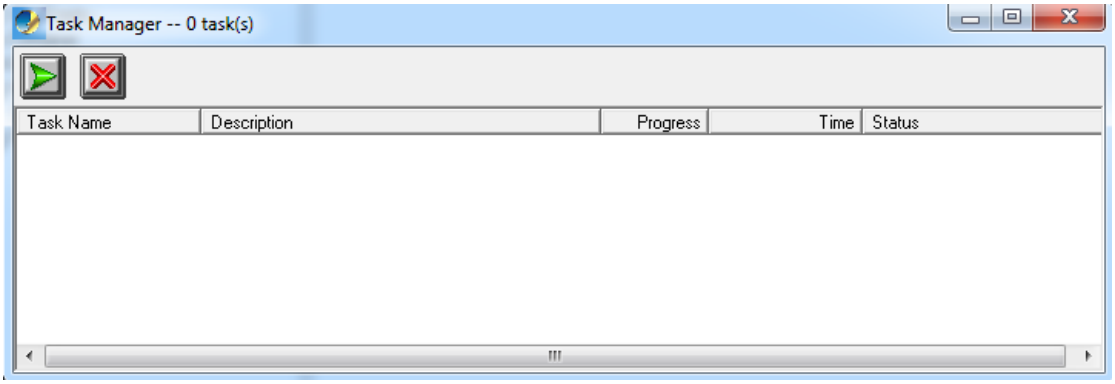


4. Specify the date/time to run the task. Then press “Next”.

5. Set the Mirror CD options if necessary.



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

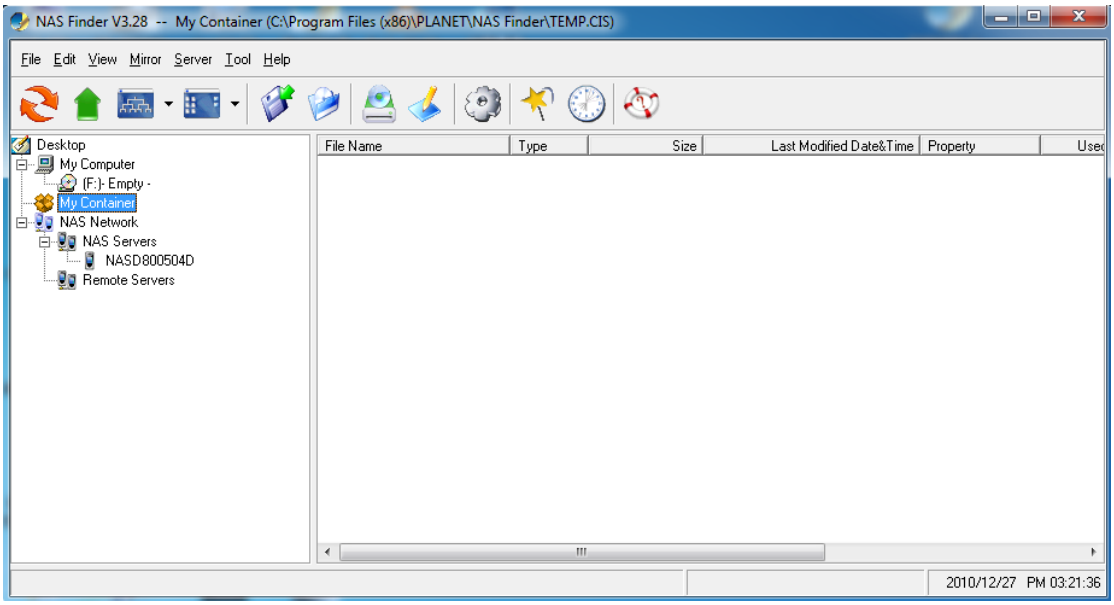


- **Archiving Files as a CD/DVD Image**

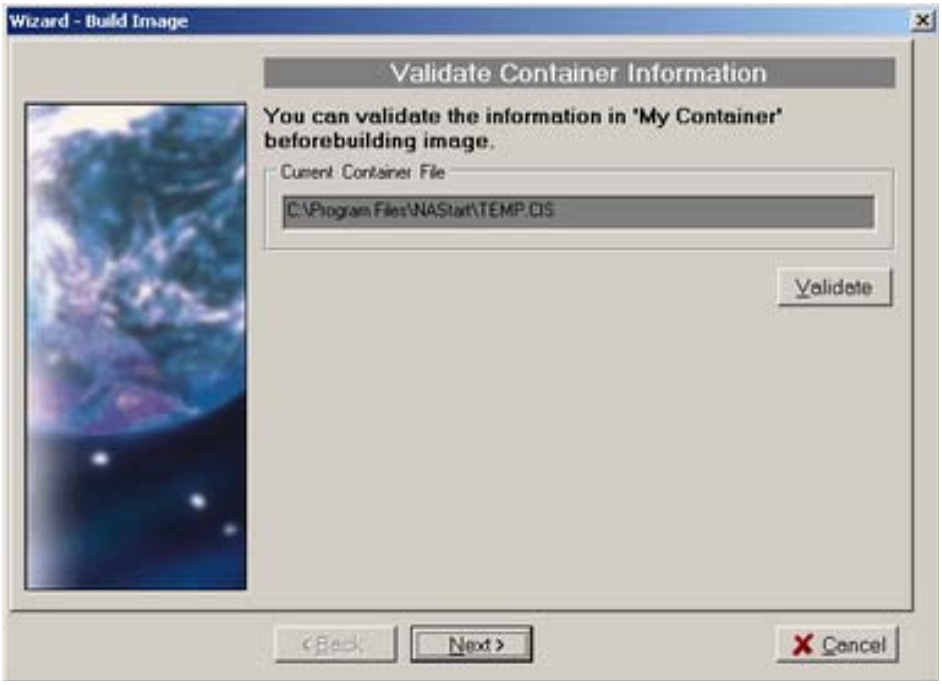
This chapter describes how to build CD image from “My Container” into a NAS Server. Please follow the steps below.

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

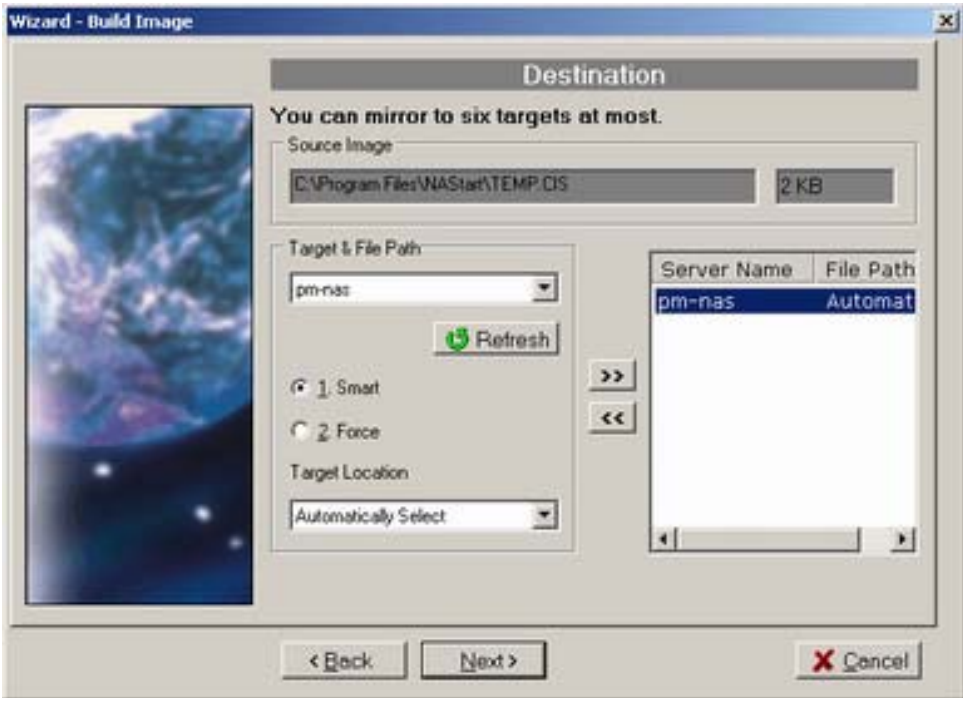
   Open Windows Explorer and drag & drop files into My Container.



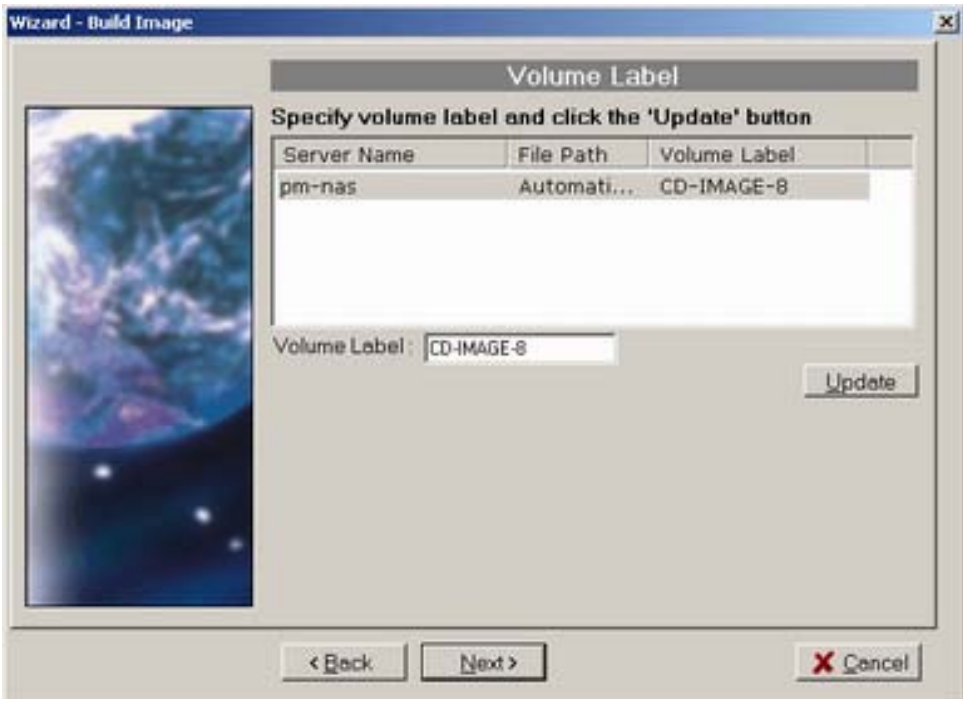
2. Click the  “Build Image” icon on the tool-bar to bring up the “Build Image” wizard. You can click the “Validate” button to check if the file/folder information in My Container is correct. If not, you can choose to update My Contained.



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.

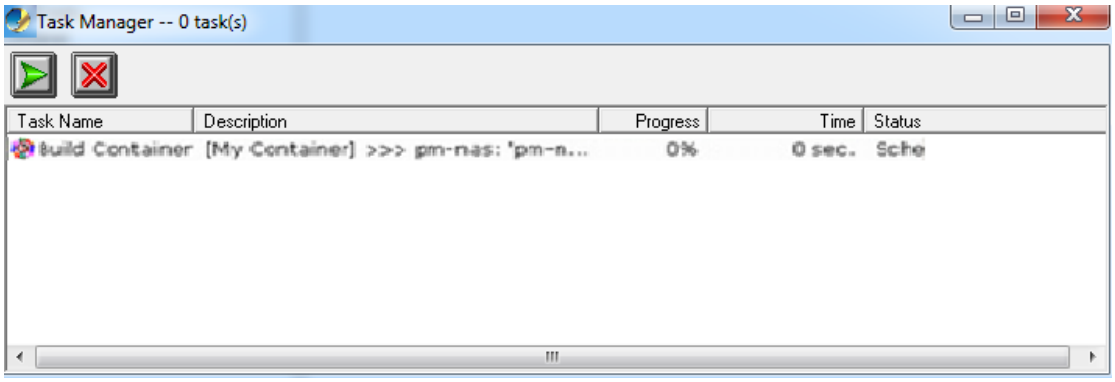


4. Name the CD/DVD image to be created. Enter the name in the “Volume label” input-box and click the “Update” button. Press “Next” afterwards.



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
- UDF V1.5, V2.0

Appendix C LED Indicators

- **LED indicator**

		On	Off	Blink
1 LAN 1	Amber*	1000M link	no link	1000M activity
	Green	100M link	no link	100 M activity
	Yellow	10M link	no link	10 M activity
2 LAN 2	Amber*	1000M link	no link	1000M activity
	Green	100M link	no link	100M activity
	Yellow	10M link	no link	10 M activity
HD Access	Red	–	–	SATA activity
Power/Fault	Green	Power on	–	–
	Yellow	Fault	–	Disk fault(Blink)

Appendix D Product Specification

Hardware Specification for NAS-7450

Specification	
CPU	Intel Celeron 2.0G/1M/533MHz
Memory	1GB RAM
Flash	1GB RAM
HDD	3.5” SATA I/II HDD x4 NOTE: The system is shipped without HDD.
HDD Tray	1U / 4 x Hot-swappable and lockable tray
LAN Port	2 x 10/100/1000 M Gigabit Ethernet ports with load balancing and failover
USB	2 x USB 2.0 port (Back)
eSATA	1 x eSATA port (Back)
Buttons	1 x Power button, 3 x System operation button
Alarm Buzzer	System warning
LCD panel	Mono-LCD display with backlight and buttons for configuration
Max. User Accounts	20480 (include local/domain account/groups)
Max. Groups	20480 (include local/domain account/groups)
Max. Shared Folder	512
Max. Concurrent Connections	200
Supported Operating System	• Microsoft Windows 95/98/ME/NT/2000/XP/VISTA/Server 2003/2008/7 • Solaric, FreeBSD, Linux, and other UNIX derivatives • Mac OS 8.x, 9.x, OS X
Network Protocols	• TCP/IP, AppleTalk • HTTP, CIFS/SMB, NFS v3/v4, FTP, AFP • BOOTP, RARP, DHCP, DNS, WINS, SMTP, SNMP, NTP, SSL
Data Protection	• RAID 0,1,5,6,10 and JBOD with global hot-spare and RAID expansion • NAS-to-NAS data synchronization with SmartSync

	• Advanced RAID bad sector recovery mechanism • Support smart-signaling UPS, USB UPS and network UPS • Local tape backup with SCSI tape drive support
Network Security	• Built-in Trend Micro antivirus software • Integrate with Microsoft Windows NT/2000/2003/2008/7 Domain and Active Directory environment • Support UNIX Network Information Service (NIS) • Support Access Control List (ACL) • Secure Sockets Layer (SSL) 128-bit encryption
System Management	• Multi-lingual web-based interface for system administration • LCD console for setting IP addresses and displaying system information • User quota and folder quota control • Environmental monitoring of system/CPU temperature, CPU fan speed and CPU voltages • System monitoring of CPU/ memory usage and LAN1/LAN2 throughput • Snapshot technology for maintaining consistent backup images of file system up to 256 snapshot standard • E-mail notification, SNMP management (MIB II) and system buzzer alerts • NAS Finder software utility for quick setup and system configuration backup
Multilingual Support	• Localized web-pages: English, Traditional Chinese, Simplified Chinese, Korean, Japanese, French, German, Italian, Spanish • Unicode UTF-8
Operating	Ttemperature: 0°C ~ 40°C (32°F ~ 104°F) Humidity: 10% ~ 80%, (non-condensing)
Storage	Temperature: -20°C ~ 70°C (-4°F ~ 158°F); Humidity: 0% ~ 90%, non-condensing
Dimension (L x W x H)	658mm x 439mm x 45mm
Weight	10.2Kg

Power Adapter	INPUT: 100-240V AC, 3-6A FUSE: 6.3A, 250V
Secure Design	Lock security slot for HDD prevention
Regulatory	FCC, CE, RoHS, WEEE compliance

Hardware Specification for NAS-7850

Specification	
CPU	Intel Core 2 Duo 2.2G/4M/800MHz
Memory	2GB RAM
Flash	1GB RAM
HDD	3.5” SATA I/II HDD x8 NOTE: The system is shipped without HDD.
HDD Tray	2U / 8 x Hot-swappable and lockable tray
LAN Port	2 x 10/100/1000 M Gigabit Ethernet ports with load balancing and failover
USB	2 x USB 2.0 port (Back)
eSATA	1 x eSATA port (Back)
Buttons	1 x Power button, 3 x System operation button
Alarm Buzzer	System warning
LCD panel	Mono-LCD display with backlight and buttons for configuration
Max. User Accounts	20480 (include local/domain account/groups)
Max. Groups	20480 (include local/domain account/groups)
Max. Shared Folder	512
Max. Concurrent Connections	400
Supported Operating System	• Microsoft Windows 95/98/ME/NT/2000/XP/VISTA/Server 2003/2008/7 • Solaric, FreeBSD, Linux, and other UNIX derivatives • Mac OS 8.x, 9.x, OS X
Network Protocols	• TCP/IP, AppleTalk • HTTP, CIFS/SMB, NFS v3/v4, FTP, AFP • BOOTP, RARP, DHCP, DNS, WINS, SMTP, SNMP, NTP, SSL

Data Protection	• RAID 0,1,5,6,10 and JBOD with global hot-spare and RAID expansion • NAS-to-NAS data synchronization with SmartSync • Advanced RAID bad sector recovery mechanism • Support smart-signaling UPS, USB UPS and network UPS • Local tape backup with SCSI tape drive support
Network Security	• Built-in Trend Micro antivirus software • Integrate with Microsoft Windows NT/2000/2003/2008/7 Domain and Active Directory environment • Support UNIX Network Information Service (NIS) • Support Access Control List (ACL) • Secure Sockets Layer (SSL) 128-bit encryption
System Management	• Multi-lingual web-based interface for system administration • LCD console for setting IP addresses and displaying system information • User quota and folder quota control • Wake On LAN • Environmental monitoring of system/CPU temperature, CPU fan speed and CPU voltages • System monitoring of CPU/ memory usage and LAN1/LAN2 throughput • Snapshot technology for maintaining consistent backup images of file system up to 256 snapshot standard • E-mail notification, SNMP management (MIB II) and system buzzer alerts • NAS Finder software utility for quick setup and system configuration backup
Multilingual Support	• Localized web-pages: English, Traditional Chinese, Simplified Chinese, Korean, Japanese, French, German, Italian, Spanish • Unicode UTF-8
Operating	Ttemperature: 0°C ~ 40°C (32°F ~ 104°F) Humidity: 10% ~ 80%, (non-condensing)
Storage	Temperature: -20°C ~ 70°C (-4°F ~ 158°F);

	Humidity: 0% ~ 90%, non-condensing
Dimension (L x W x H)	669mm x 480mm x 88mm
Weight	16.2kg
Power Adapter	INPUT: 100-240V AC, 5-8A FUSE: 8A, 250V
Secure Design	Lock security slot for HDD prevention
Regulatory	FCC, CE, RoHS, WEEE compliance