Turbo NAS

User Manual (Version: 3.2.0)

Thank you for choosing QNAP products! This user manual provides detailed instructions of using the Turbo NAS. Please read carefully and start to enjoy the powerful functions of the Turbo NAS!

NOTE

- "Turbo NAS" is hereafter referred to as "NAS".
- This manual provides the description of all functions of the Turbo NAS. The product you purchased may not support certain functions dedicated to specific models.
- All features, functionality, and other product specifications are subject to change without prior notice or obligation.
- Information presented is subject to change without notice.
- All brands and products names referred to are trademarks of their respective holders.

DISCLAIMER

In no event shall the liability of QNAP Systems, Inc. (QNAP) exceed the price paid for the product from direct, indirect, special, incidental, or consequential software, or its documentation. QNAP makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. QNAP reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

CAUTION

1. Back up your system periodically to avoid any potential data loss. QNAP disclaims any responsibility of all sorts of data loss or recovery.
2. Should you return any components of the NAS package for refund or maintenance, make sure they are carefully packed for shipping. Any form of damages due to improper packaging will not be compensated.

Table of Contents

Safety Warnings

1. The NAS can operate normally in the temperature of 0ºC-40ºC and relative humidity of 0%-95%. Please make sure the environment is well-ventilated.
2. The power cord and devices connected to the NAS must provide correct supply voltage (100W, 90-264V).
3. Do not place the NAS in direct sunlight or near chemicals. Make sure the temperature and humidity of the environment are in optimized level.
4. Unplug the power cord and all connected cables before cleaning. Wipe the NAS with a dry towel. Do not use chemical or aerosol to clean the NAS.
5. Do not place any objects on the NAS for the server's normal operation and to avoid overheat.
6. Use the flat head screws in the product package to lock the hard disks in the NAS when installing hard disks for proper operation.
7. Do not place the NAS near any liquid.
8. Do not place the NAS on any uneven surface to avoid falling off and damage.
9. Make sure the voltage is correct in your location when using the NAS. If you are not sure, please contact the distributor or the local power supply company.
10. Do not place any object on the power cord.
11. Do not attempt to repair your NAS in any occasions. Improper disassembly of the product may expose you to electric shock or other risks. For any enquiries, please contact the distributor.
12. The chassis NAS models should only be installed in the server room and maintained by the authorized server manager or IT administrator. The server room is locked by key or keycard access and only certified staff is allowed to enter the server room.

Chapter 1 Install the NAS

For the information of the hardware installation, please refer to the "Quick Installation Guide" in the product package.

1.1 Hard Disk Compatibility List

This product works with 2.5-inch/ 3.5-inch SATA hard disk drives from major hard disk brands. For the HDD compatibility list, please visit http://www.qnap.com/.

QNAP disclaims any responsibility for product damage/ malfunction or data loss/ recovery due to misuse or improper installation of hard disks in any occasions for any reasons.

Note that if you install a hard drive (new or used) which has never been installed on the NAS before, the hard drive will be formatted and partitioned automatically and all the disk data will be cleared.

1.2 Check System Status

LED Display & System Status Overview

LED	Colour	LED Status	Description
USB	**Blue**	Flashes blue every 0.5 sec	1) A USB device (connected to front USB port) is being detected 2) A USB device (connected to front USB port) is being removed from the NAS 3) The USB device (connected to the front USB port) is being accessed 4) The data is being copied to or from the external USB or eSATA device
		Blue	1) A front USB device is detected (after the device is mounted) 2) The NAS has finished copying the data to or from the USB device connected to the front USB port
		Off	No USB device can be detected
eSATA*	**Orange**	Flashes	The eSATA device is being accessed
		Off	No eSATA device can be detected
System Status	**Red/ Green**	Flashes green and red alternately every 0.5 sec	1) The hard drive on the NAS is being formatted 2) The NAS is being initialised 3) The system firmware is being updated 4) RAID rebuilding is in process* 5) Online RAID Capacity Expansion is in process* 6) Online RAID Level Migration is in process*

		Red	1) The hard drive is invalid 2) The disk volume has reached its full capacity 3) The disk volume is going to be full 4) The system fan is out of function* 5) An error occurs when accessing (read/write) the disk data 6) A bad sector is detected on the hard drive 7) The NAS is in degraded read-only mode (2 member drives fail in a RAID 5 or RAID 6 configuration, the disk data can still be read)* 8) (Hardware self-test error)
System Status	**Red/ Green**	Flashes red every 0.5 sec	The NAS is in degraded mode (one member drive fails in RAID 1, RAID 5 or RAID 6 configuration)
		Flashes green every 0.5 sec	1) The NAS is starting up 2) The NAS is not configured 3) The hard drive is not formatted
		Green	The NAS is ready
		Off	All the hard drives on the NAS are in standby mode
HDD	**Red/ Green**	Flashes red	The hard drive data is being accessed and a read/ write error occurs during the process
		Red	A hard drive read/ write error occurs
		Flashes green	The hard drive data is being accessed
		Green	The hard drive can be accessed
LAN	**Orange**	Orange	The NAS is connected to the network
		Flashes orange	The NAS is being accessed from the network

* This function is applicable to some models only. Please refer to the comparison table for more details:

http://www.qnap.com/images/products/comparison/Comparison_NAS.html

Beep Alarm (beep alarm can be disabled in "System Tools" > "Hardware Settings")

Beep sound	No. of Times	Description
Short beep (0.5 sec)	1	1) The NAS is starting up 2) The NAS is being shut down (software shutdown) 3) The user presses the reset button to reset the NAS 4) The system firmware has been updated
Short beep (0.5 sec)	3	The user tries to copy the NAS data to the external storage device from the front USB port, but the data cannot be copied.
Short beep (0.5 sec), long beep (1.5 sec)	3, every 5 min	The system fan is out of function*
Long beep (1.5 sec)	2	1) The disk volume is going to be full 2) The disk volume has reached its full capacity 3) The hard drives on the NAS are in degraded mode 4) The user starts the HDD rebuilding process
	1	1) The NAS is turned off by force shutdown (hardware shutdown) 2) The NAS has been turned on successfully and is ready

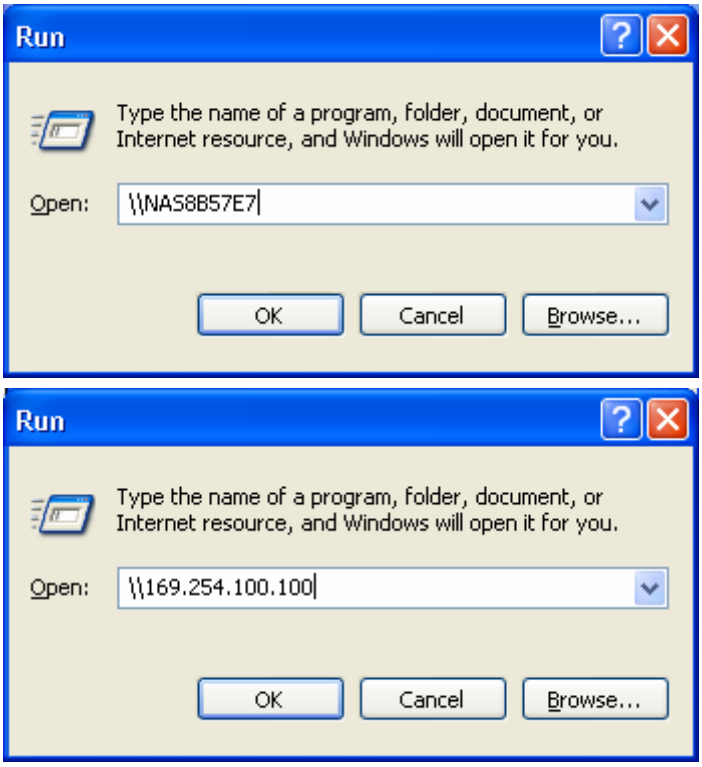
* This function is applicable to some models only. Please refer to the comparison table for more details:

http://www.qnap.com/images/products/comparison/Comparison_NAS.html

Chapter 2 Use the Powerful Services of NAS

A. Use the network shares

1. You can access the network shares of the NAS by the following means:
   a. Open My Network Places and find the workgroup of the NAS. If you cannot find the server, browse the whole network to search for the NAS. Double click the name of the NAS for connection.
   b. Use Run function in Windows. Enter **\\[NAS name]** or **\\[NAS IP]** to access the share folders on the NAS.



2. Enter the default user name and password.

Default user name: **admin** Password: **admin**

3. You can upload files to the network shares.

B. Manage the NAS

- **Manage the NAS using web browser by Windows® or Mac**

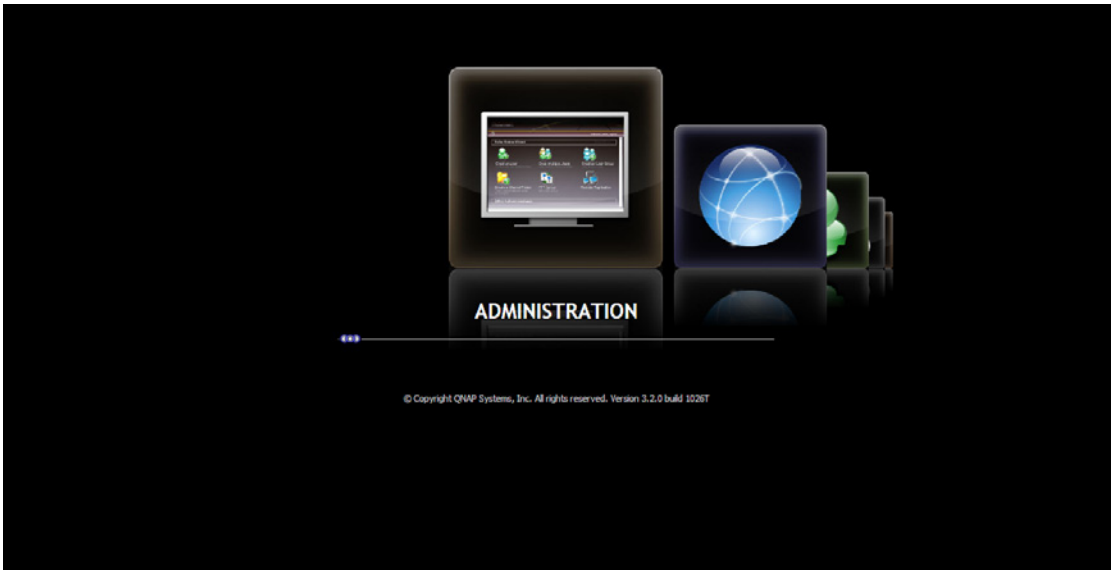
1. You can access the NAS web administration page by the following methods:
   a. Use the Finder to find the NAS.
   b. Open a web browser and enter **http://[NAS IP]:8080**

> The default NAS IP is 169.254.100.100:8080. If you have configured the NAS to use DHCP, you can use the Finder to check the IP address of the NAS. Make sure the NAS is connected to the same subnet of your computer that runs the Finder. If you cannot search for the NAS IP, please try to connect the NAS to your computer directly and run the Finder again.

2. When the administration page of the NAS is shown, click "ADMINISTRATION". Enter the user name and password to login.

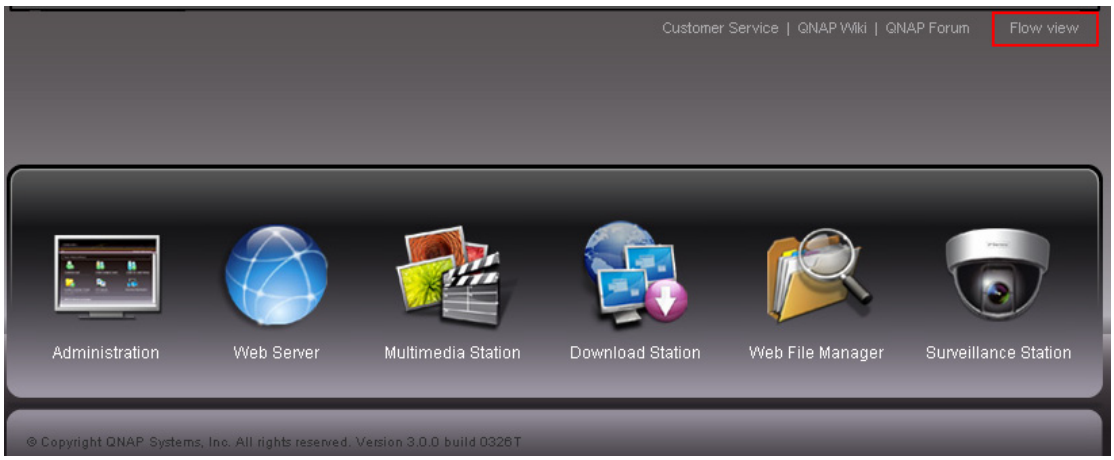
Default user name: **admin** Password: **admin**

Note that if you login the administration interface with a user account without administration right, you can only change your login password.



3. You can select to browse the NAS UI with Standard view or Flow view.

Standard view:

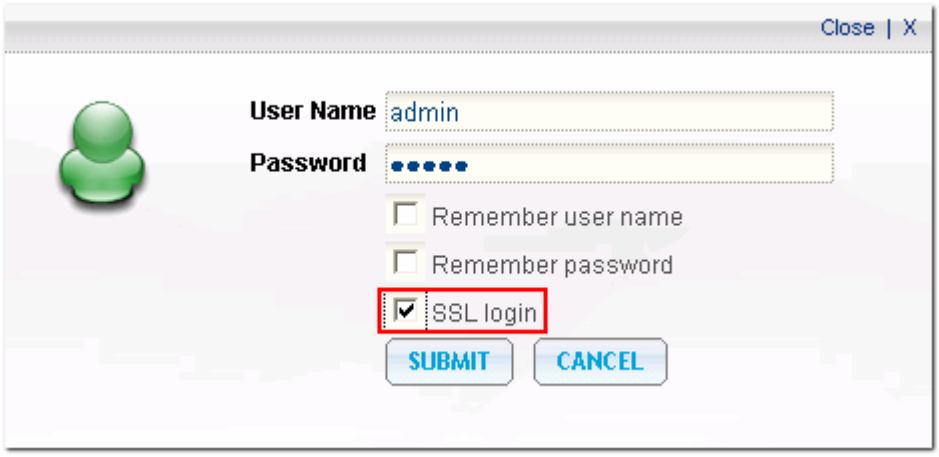


Flow view:

4. You can select the display language on the drop-down menu on the login page of the NAS or after you login the NAS.

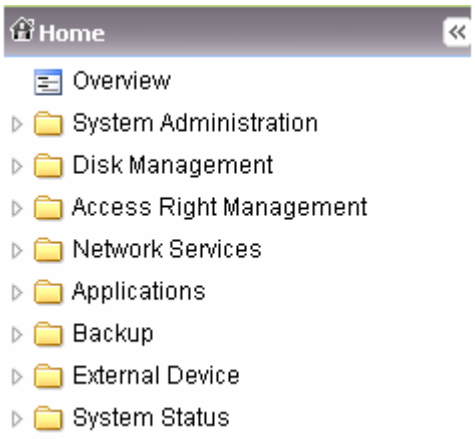
5. The NAS supports SSL secure login which enables you to configure and manage the server by encrypted transfer. To use this function, check the box "SSL login" on the administration page and login the server.

> **Note:** If your NAS is placed behind an NAT gateway and you want to access the NAS by secure login from the Internet, you must open the port 443 on your NAT and forward this port to LAN IP of the NAS.

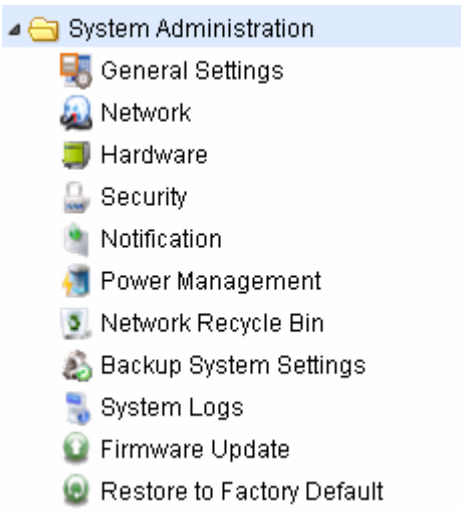


Chapter 3 Server Administration

There are 8 main sections in server administration.



Click the triangle icon next to the section name to expand the tree and view the items listed under each section.

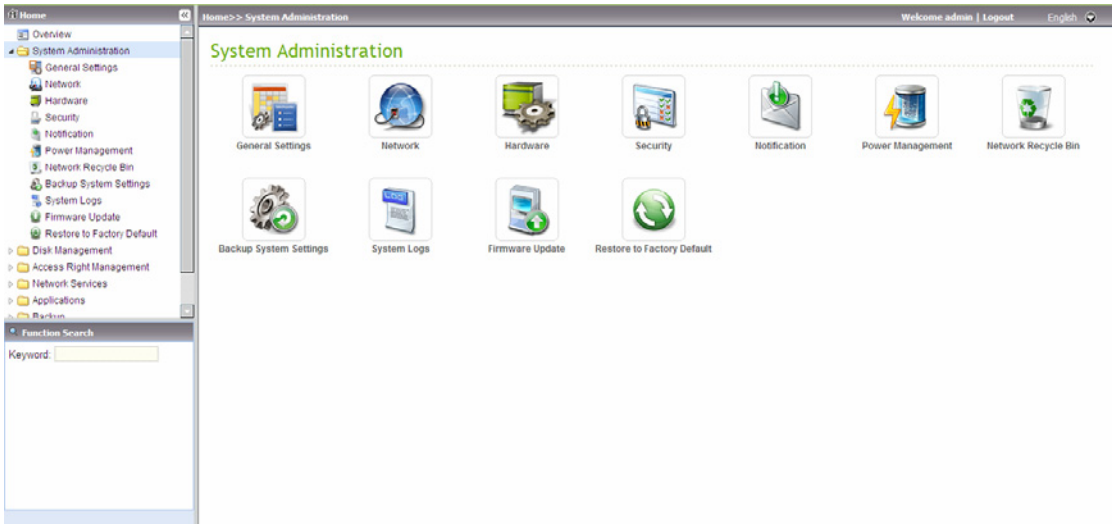


To access the services such as Web File Manager, Download Station, Multimedia Station, and Surveillance Station, you can select the services from the drop-down menu or click the icons on the login page.

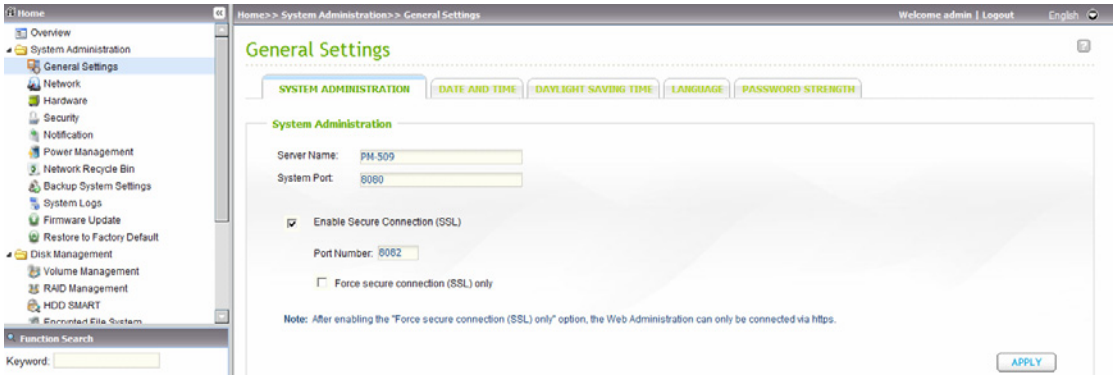
After you login the NAS, you can click the icons on top of the page to access the services.

3.1 System Administration

You can configure the general system settings, network settings, and hardware settings, update the firmware, etc. in this section.



3.1.1 General Settings



3.1.1.1 System Administration

Enter the name of the NAS. The server name can be 14 characters long at maximum, which supports alphabets, numbers, and hyphen (-). The server does not accept names with space, period (.), or names in pure number.

Assign a port for the system management. The default port is 8080. The services which use this port include: System Management, Web File Manager, Multimedia Station, and Download Station.

- ✓ **Enable Secure Connection (SSL)**
  To allow the users to access the NAS by https, enable secure connection (SSL) and enter the port number. If you enable the option "Force secure connection (SSL) only", the users can only access the web administration page by https connection.

3.1.1.2 Date and Time

Set the date, time, and time zone according to your location. If the settings are incorrect, the following problems may occur:

- When using a web browser to access the server or save a file, the display time of the action will be incorrect.
- The time of event log displayed will be inconsistent with the actual time when an action occurs.

✓ **Synchronize with an Internet time server automatically**

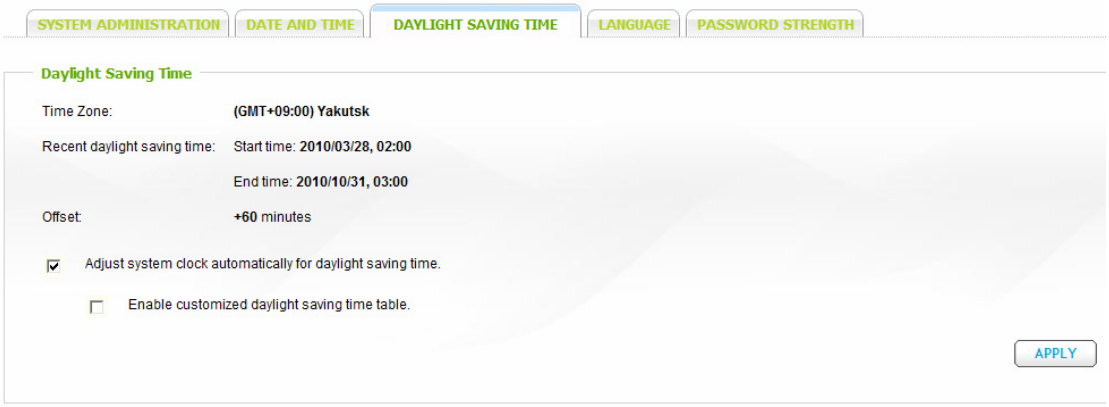
You can enable this option to update the date and time of the system automatically with specified NTP (Network Time Protocol) server. Enter the IP address or domain name of the NTP server, e.g. time.nist.gov, time.windows.com. Then enter the time interval for adjusting the time.

> **Note:** The first time you enable NTP server, it may take several minutes for time synchronization before the time is correctly adjusted.

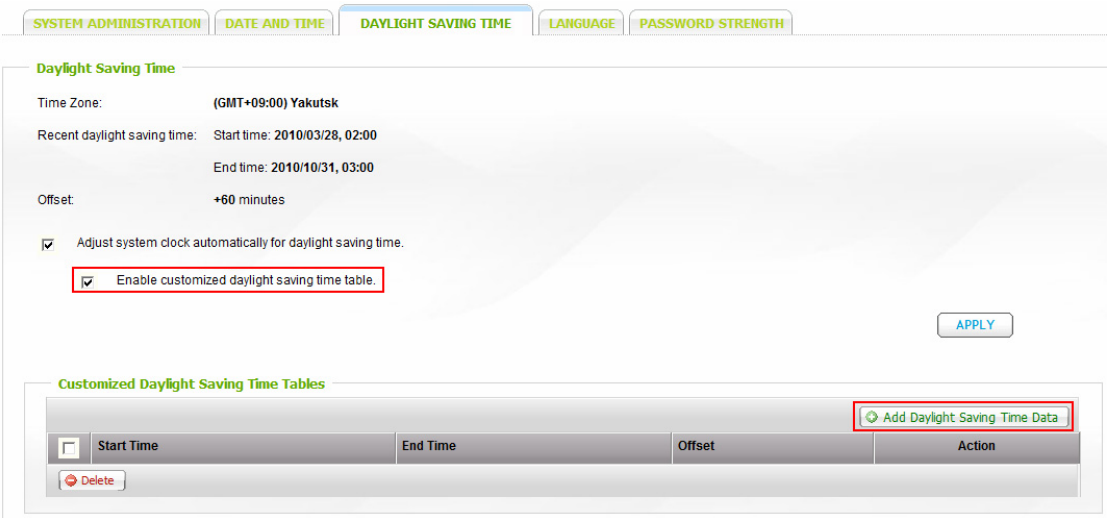
3.1.1.3 Daylight Saving Time

If your region adopts daylight saving time (DST), you can enable "Adjust system clock automatically for daylight saving time". Click "Apply". The latest DST schedule of the time zone you select in the "Date and Time" section will be shown. The system time will be adjusted automatically according to the DST.

Note that if your region does not adopt DST, the options on this page will not be available.



To enter the daylight saving time table manually, check the option "Enable customized daylight saving time table". Click "Add Daylight Saving Time Data" and enter the daylight saving time schedule. Then click "Apply" to save the settings.



3.1.1.4 Language

Select the language the NAS uses to display files and directories.

Note: All the files and directories on the NAS will be created using Unicode encoding. If your FTP clients or the OS of your PC does not support Unicode, e.g. Windows® 95/98/ME, select the language the same as your OS here in order to view the files and directories on the server properly.

3.1.1.5 Password Strength

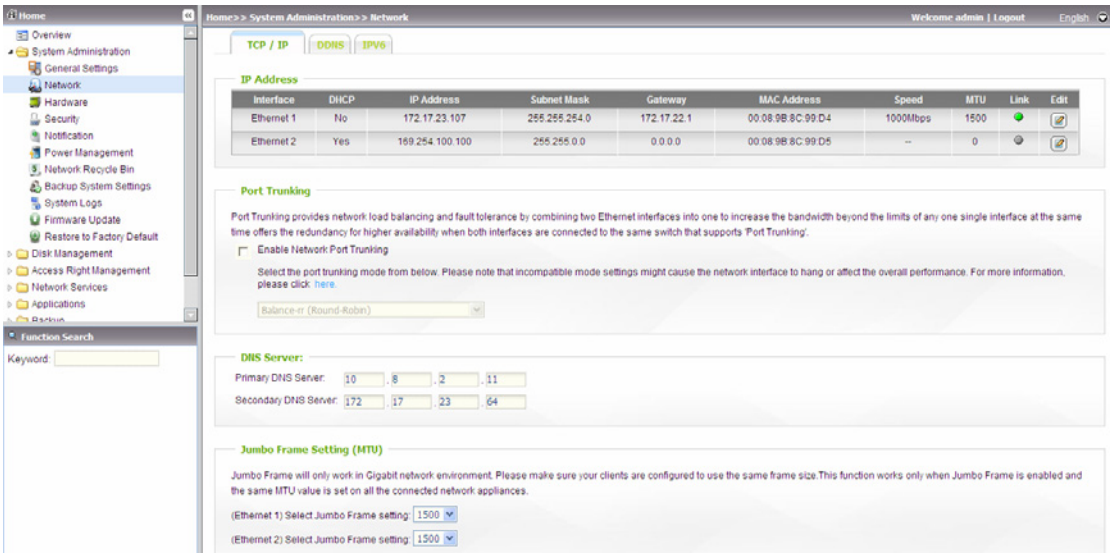
You can specify the password setting rules here. After the setting has been applied, the system will automatically check the validity of the password.

3.1.2 Network

3.1.2.1 TCP/IP

i. IP Address

You can configure the TCP/IP settings of the NAS on this page. Click  to edit the network settings.



- **Obtain the IP address settings automatically via DHCP**
  If your network supports DHCP, the NAS will use DHCP protocol to retrieve the IP address and related information automatically.

- **Use static IP address**
  To use fixed IP address for network connection, enter the IP address, subnet mask, and default gateway.

- **Enable DHCP Server**
  If no DHCP is available on the LAN where the NAS locates, you can enable this function to enable the NAS as a DHCP server. The NAS will allocate dynamic IP address to the DHCP clients on the LAN.

  You can set the range of IP addresses allocated by the DHCP server and the lease time. The lease time refers to the time that an IP address is leased to the clients by the DHCP server. When the lease time expires, the client has to

acquire an IP address from the DHCP server again.

For example, to establish a DLNA network and share the multimedia files on the NAS to the DLNA digital media players via UPnP while there is no NAT gateway that supports DHCP server, you can enable the DHCP server feature of the NAS. The NAS will allocate dynamic IP address to the media players or other clients automatically.

Note: If there is an existing DHCP server on your LAN, do not enable this function. Otherwise, there will be IP address allocation and network access errors.

ii. Port Trunking

Applicable to the models with two LAN ports only.

Port Trunking provides network load balancing and fault tolerance by combining two Ethernet interfaces into one to increase the bandwidth beyond the limits of any one single interface at the same time offers the redundancy for higher availability when both interfaces are connected to the same switch that supports 'Port Trunking'.

Field	Description
Balance-rr (Round-Robin)	The packets are transmitted in sequential order from the first available slave to the last. This mode provides load balancing and fault tolerance.
Active Backup	Only one active slave is used to transmit packets. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance.
Balance XOR	The packets are transmitted based on the hash policy. The default policy is a simple [(source MAC address XOR'd with destination MAC address) modulo slave count]. Alternate transmit policies may be selected via the xmit_hash_policy option. This mode provides load balancing and fault tolerance.
Broadcast	The packets are transmitted on all slave interfaces. This mode provides fault tolerance.

IEEE 802.3ad	The Ethernet interfaces are aggregated in a group and each slave shares the same speed. This mode provides load balancing and fault tolerance. Make sure the switch supports IEEE 802.3ad standard and the correct LACP mode is configured.
Balance-tlb (Adaptive Transmit Load Balancing)	Channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave. This mode provides load balancing and fault tolerance.
Balance-alb (Adaptive Load Balancing)	Include balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The receive load balancing is achieved by ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware address for the server. This mode provides load balancing and fault tolerance.

iii. DNS Server

- **Primary DNS Server:** Enter the IP address of the primary DNS server.
- **Secondary DNS Server:** Enter the IP address of the secondary DNS server.

Note:

1. Please contact your ISP or network administrator for the IP address of the primary and the secondary DNS servers. When the NAS plays the role as a terminal and needs to perform independent connection, e.g. BT download, you must enter at least one DNS server IP for proper URL connection. Otherwise, the function may not work properly.
2. If you select to obtain the IP address via DHCP, there is no need to configure the primary and the secondary DNS servers. In this case, enter "0.0.0.0".

iv. Jumbo Frame Settings (MTU)

"Jumbo Frames" refer to the Ethernet frames that are larger than 1500 bytes. It is designed to enhance Ethernet networking throughput and reduce the CPU utilization of large file transfers by enabling more efficient larger payloads per packet.

Maximum Transmission Unit (MTU) refers to the size (in bytes) of the largest packet that a given layer of a communications protocol can transmit.

The NAS uses standard Ethernet frames: **1500 bytes** by default. If your network appliances support Jumbo Frame setting, select the appropriate MTU value for your network environment. The NAS supports 4074, 7418, and 9000 bytes for MTU.

Note: The Jumbo Frame setting is valid in Gigabit network environment only. All the network appliances connected must enable Jumbo Frame and use the same MTU value.

3.1.2.2 DDNS

To set up a server on the Internet and enable the users to access it easily, a fixed and easy-to-remember host name is often required. However, if the ISP provides only dynamic IP address, the IP address of the server will change from time to time and is difficult to recall. You can enable the DDNS service to solve the problem.

After enabling the DDNS service of the NAS, whenever the NAS restarts or the IP address is changed, the NAS will notify the DDNS provider immediately to record the new IP address. When the user tries to connect the NAS via the host name, the DDNS will transfer the recorded IP address to the user.

The NAS supports the DDNS providers: members.dyndns.org, update.ods.org, members.dhs.org, www.dyns.cx, www.3322.org, www.no-ip.com.

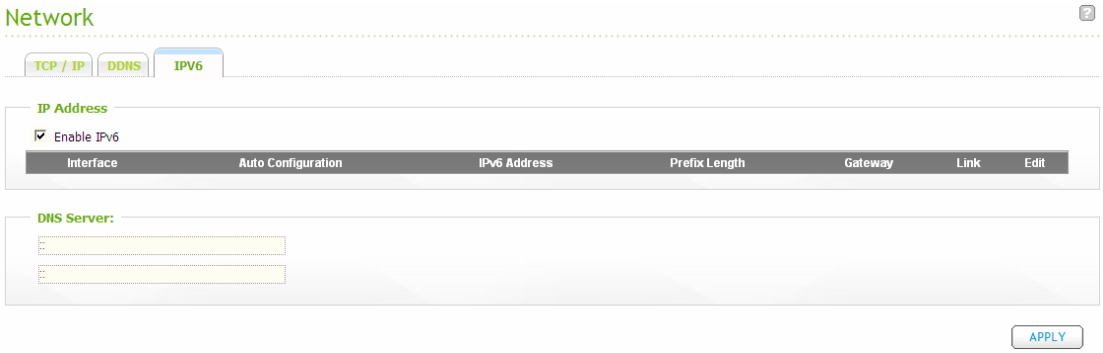
Check the External IP Address Automatically: Enable this option if your NAS is located behind a gateway. The NAS checks the external (WAN) IP automatically and if the IP address is changed, the NAS will inform the DDNS provider automatically to ensure it can be accessed via the host name.

For the information of setting up the DDNS and port forwarding on the NAS, please refer to the online tutorial: http://www.qnap.com/pro_features.asp.

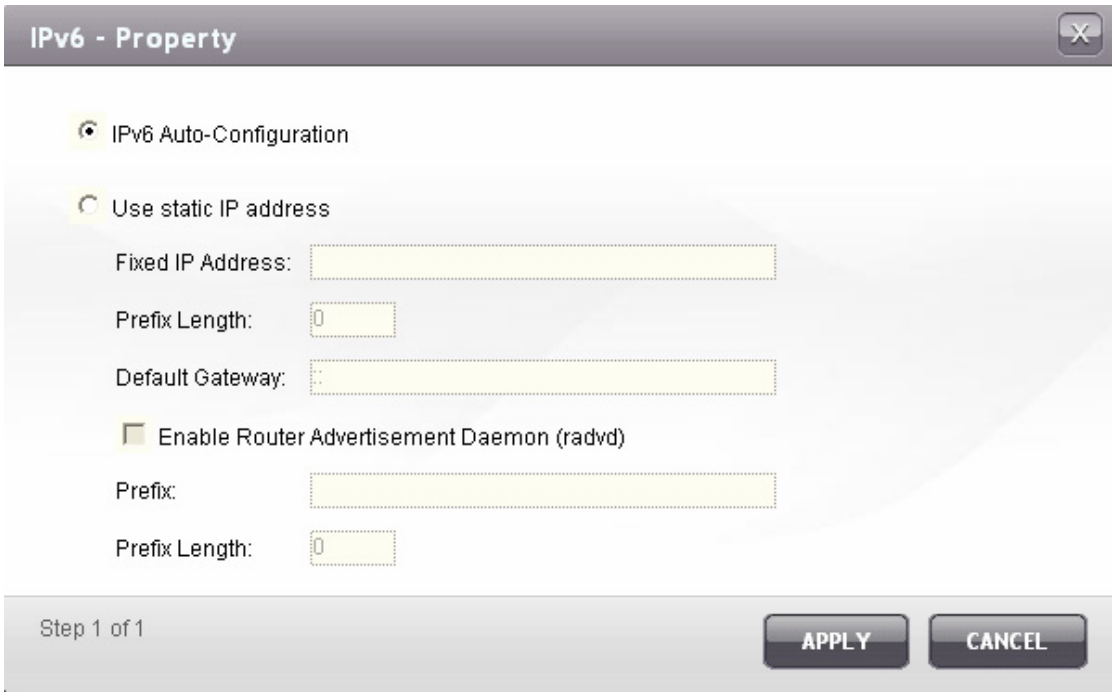
3.1.2.3 IPv6

The NAS supports IPv6 connectivity with "stateless" address configurations and RADVD (Router Advertisement Daemon) for IPv6, RFC 2461 to allow the hosts on the same subnet to acquire IPv6 addresses from the NAS automatically. The services on the NAS that support IPv6 include:

- Remote replication
- Web Server
- FTP
- iSCSI (Virtual disk drives)
- SSH (putty)



To use this function, check the box "Enable IPv6" and click "Apply". The NAS will restart. After the system restarts, login the IPv6 page again. The settings of the IPv6 interface will be shown. Click  to edit the settings.



- **IPv6 Auto Configuration**

  If you have an IPv6 enabled router on the network, select this option to allow the NAS to acquire the IPv6 address and the configurations automatically.

- **Use static IP address**

  To use a static IP address, enter the IP address (e.g. 2001:bc95:1234:5678), prefix length (e.g. 64), and the gateway address for the NAS. You may contact your ISP for the information of the prefix and the prefix length.

  - ✓ **Enable Router Advertisement Daemon (radvd)**

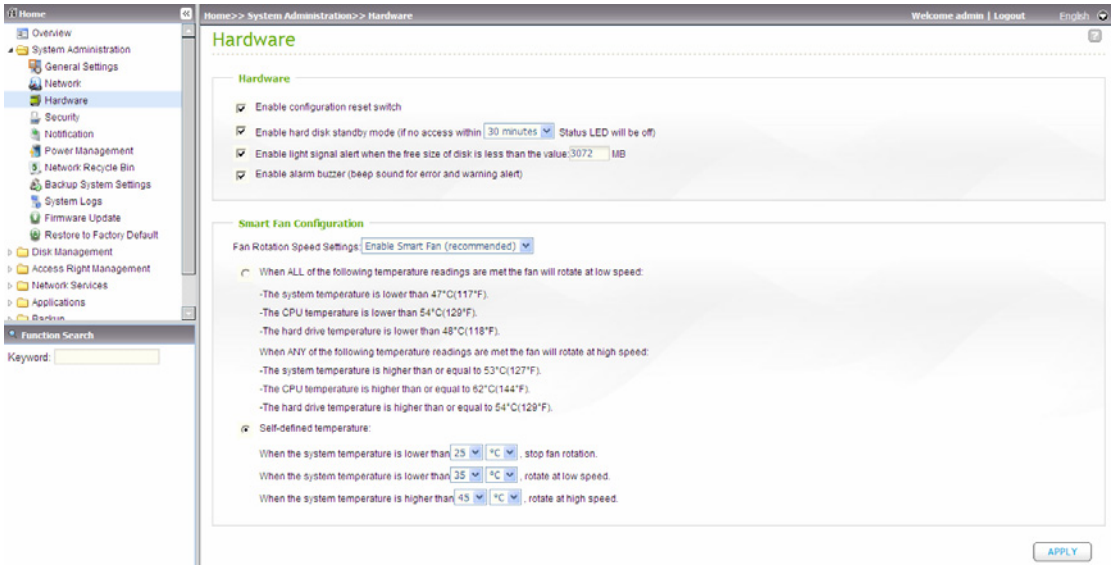
    To configure the NAS as an IPv6 host and distribute IPv6 addresses to the local clients which support IPv6, enable this option and enter the prefix and prefix length.

- **IPv6 DNS server**

  Enter the preferred DNS server in the upper field and the alternate DNS server in the lower field. You may contact your ISP or network administrator for the information. If you select IPv6 auto configuration, leave the fields as "::".

3.1.3 Hardware

You can enable or disable the hardware functions of the NAS.



- Enable configuration reset switch
  You can press the reset button for 3 seconds to reset the administrator password and the system settings to default.
- Enable hard disk standby mode
  When this function is enabled, the hard disk(s) will go to standby mode if there is no access within the specified period.
- Enable light signal alert when the free size of SATA disk is less than the value:
  The status LED flashes red and green when this function is enabled and the free space of the SATA disk is less than the value. The range of the value is 1-51200 MB.
- Enable alarm buzzer
  Enable this option. The system will sound when an error occurs.
- Smart Fan configuration
  (i) Enable smart fan (recommended)
  Select to use the default smart fan settings or define the settings manually. When the system default settings are selected, the fan rotation speed is automatically adjusted when the server temperature, CPU temperature, and hard drive temperature meet the criteria. It is recommended to enable this option.
  (ii) Set fan rotation speed manually
  By manually setting the fan rotation speed, the fan rotates at the defined

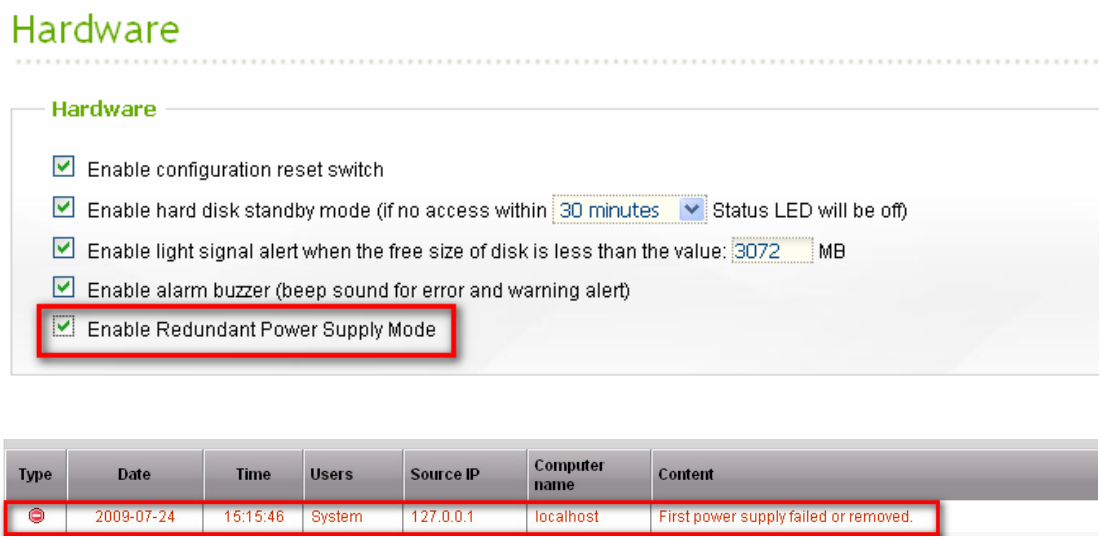
speed continuously.

Enable redundant power supply on the web-based interface:

If you have two power supply units installed on the NAS, follow the steps below to enable redundant power supply. Redundant power supply allows the NAS to operate normally when the primary power supply unit fails or is removed accidentally. The secondary (redundant) power supply unit will take over to supply the entire system in such case.

1. Login the Turbo NAS.
2. Go to "System Administration" > "Hardware".
3. Enable redundant power supply mode*. When this function is enabled, the system will start to record error messages about the power supply units in "System Logs".

* This function is disabled by default.

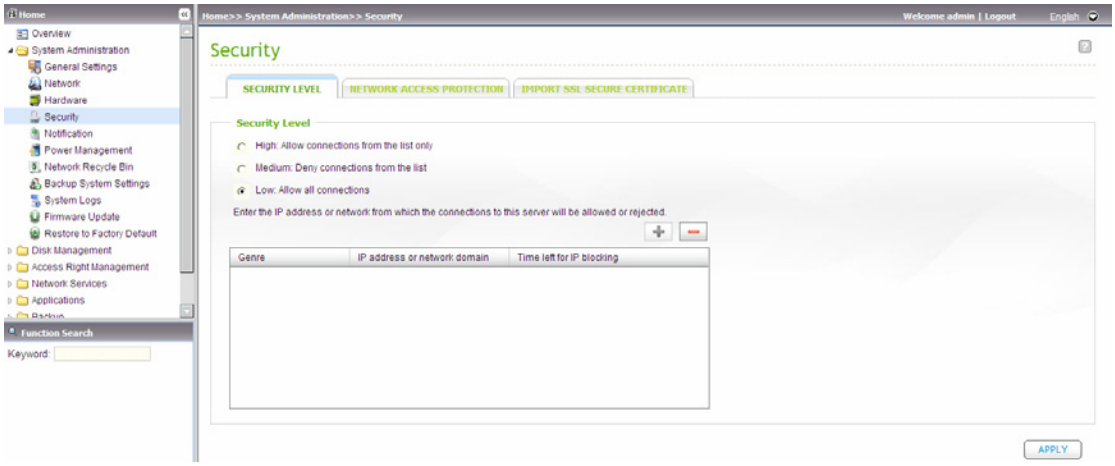


3.1.4 Security

3.1.4.1 Security Level

Enter the IP address or network from which the connections to this server are allowed or rejected. When the connection of a host server is denied, all protocols of that server are not allowed to access the local server.

After changing the settings, click "Apply" to save the changes. The network services will be restarted and current connections to the server will be disconnected.

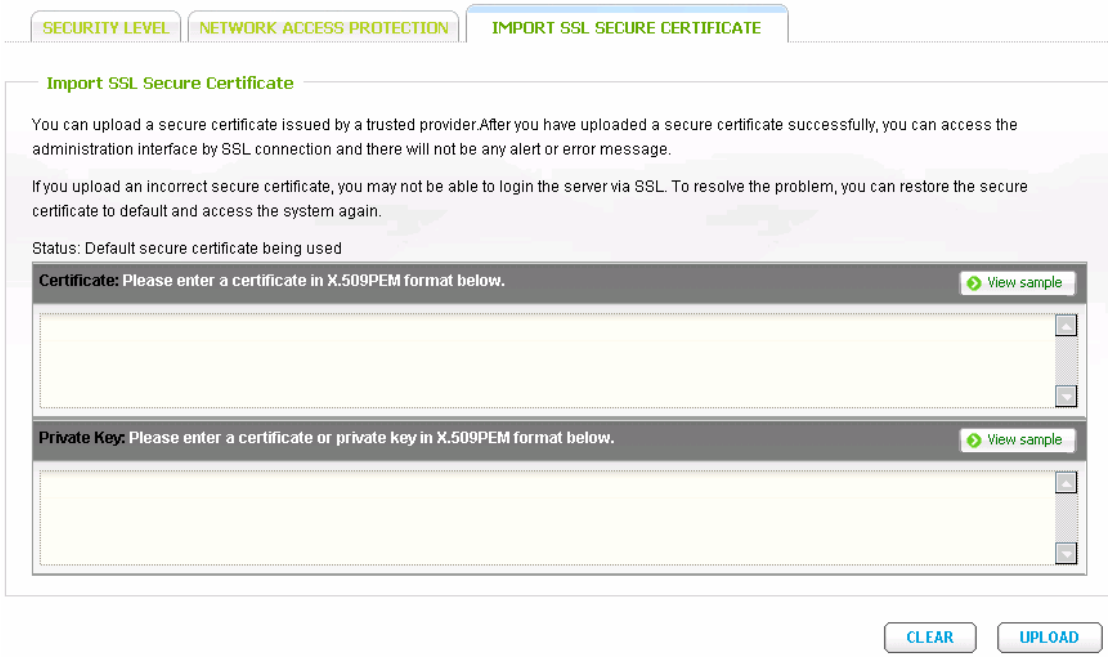


3.1.4.2 Network Access Protection

The network access protection enhances the security of the system and prevents unwanted intrusion. You can select to block the IP for a certain period of time or forever if the IP fails to login the server from a particular connection method.

3.1.4.3 Import SSL Secure Certificate

The Secure Socket Layer (SSL) is a protocol for encrypted communication between web servers and browsers for secure data transfer. You can upload a secure certificate issued by a trusted provider. After you have uploaded a secure certificate, you can access the administration interface by SSL connection and there will not be any alert or error message. The system supports X.509 certificate and private key only.

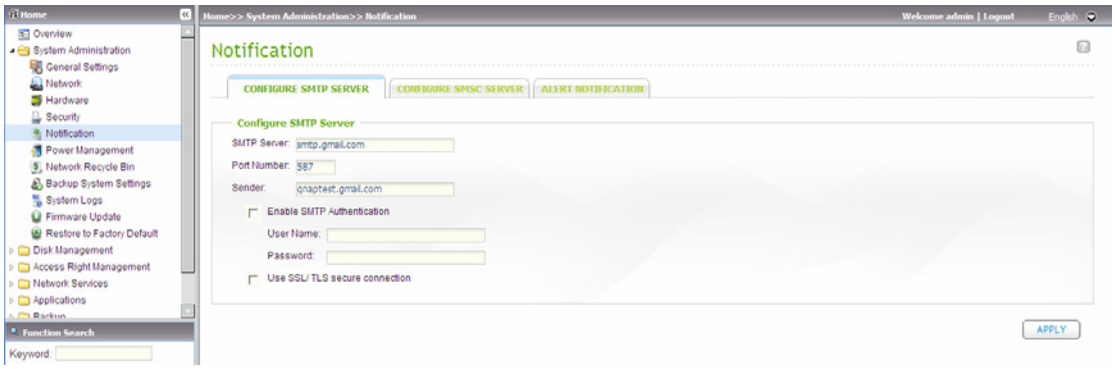


3.1.5 Notification

3.1.5.1 Configure SMTP Server

The NAS supports email alert to inform you about the system errors and warning. To receive the alert by email, configure the SMTP server.

- SMTP Server: Enter the SMTP server name, e.g. smtp.gmail.com.
- Port Number: Enter the port number for the SMTP server. The default port number is 25.
- Sender: Enter the sender information.
- Enable SMTP Authentication: If this function is enabled, the system would request the authentication of the mail server before the message is sent.
- User Name and Password: Enter your login information of your email account, e.g. your Gmail login name and password.
- Use SSL/ TLS secure connection: If the SMTP server supports this function, you can enable it.



3.1.5.2 Configure SMSC Server

You can configure the SMS server settings to send SMS messages from the NAS. The default SMS service provider is Clickatell. You may also add your own SMS service provider by selecting "Add SMS Provider" on the drop down menu.

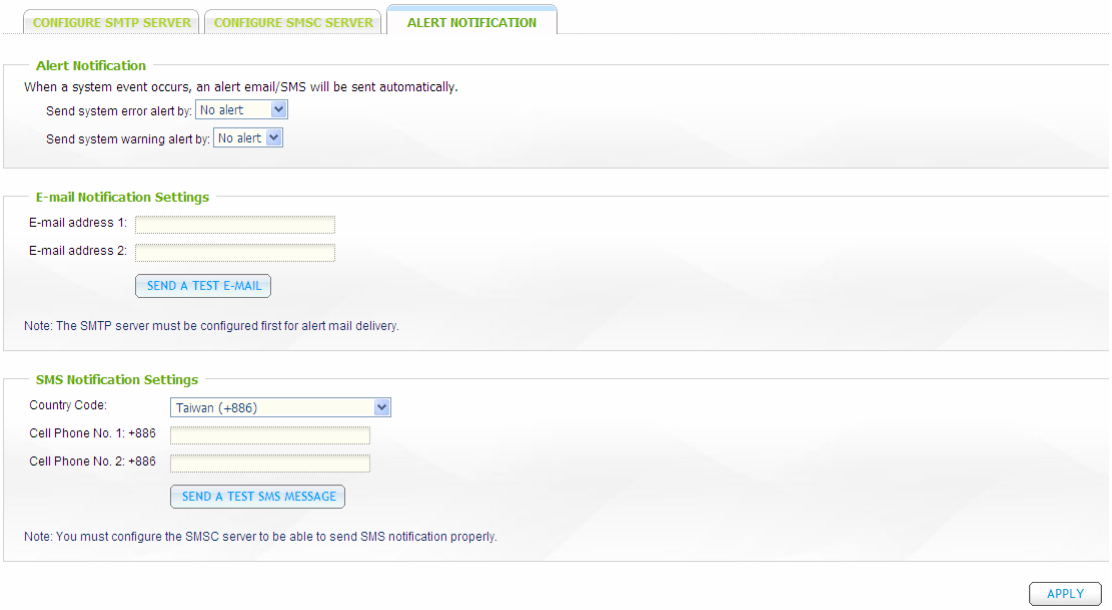
When you select "Add SMS service provider", you need to enter the name of the SMS provider and the URL template text.

Note: You will not be able to receive the SMS properly if the URL template text entered does not follow your SMS service provider's standard.

3.1.5.3 Alert Notification

You can configure to receive instant SMS or email alert when a system error or warning occurs. Enter the email address and mobile phone number to receive the alerts. Make sure you have entered the correct SMTP server and the SMSC server settings. If you do not want to receive any alerts, select "No alert" for both settings.

For the online tutorial, please visit http://www.qnap.com/pro_features.asp.



3.1.6 Power Management

This section enables you to restart or shut down the server immediately, define the behavior of the server when the power resumes after a power outage, and set schedule for automatic system power on/ off/ restart.

- **Restart/ Shutdown**
  Restart or shut down the server immediately.
  If you try to restart or turn off the NAS from the web-based interface or the LCD panel when a remote replication job is in process, the system will prompt you to ignore the running replication job or not.

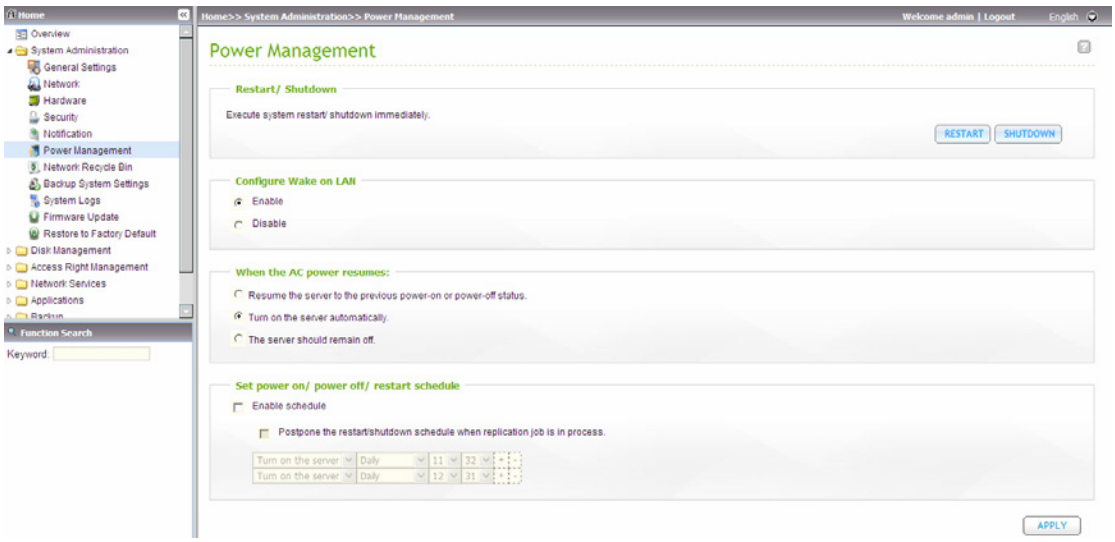
  Enable the option "Postpone the restart/shutdown schedule when replication job is in process" to allow the scheduled system restart or shutdown to be carried out after a running replication job completes. Otherwise, the system will ignore the running replication job and execute scheduled system restart or shutdown.

- **Wake on LAN**
  Enable this option to power on the NAS remotely by Wake on LAN. Note that if the power connection is physically removed when the NAS is turned off, Wake on LAN will not function whether or not the power supply is reconnected afterwards.

  This function is applicable to certain models only. Please refer to the comparison table for more details:
  http://www.qnap.com/images/products/comparison/Comparison_NAS.html

- **Power resumption settings**
  Configure the NAS to resume to the previous power-on or power-off status, turn on or remain off when the AC power resumes after a power outage.

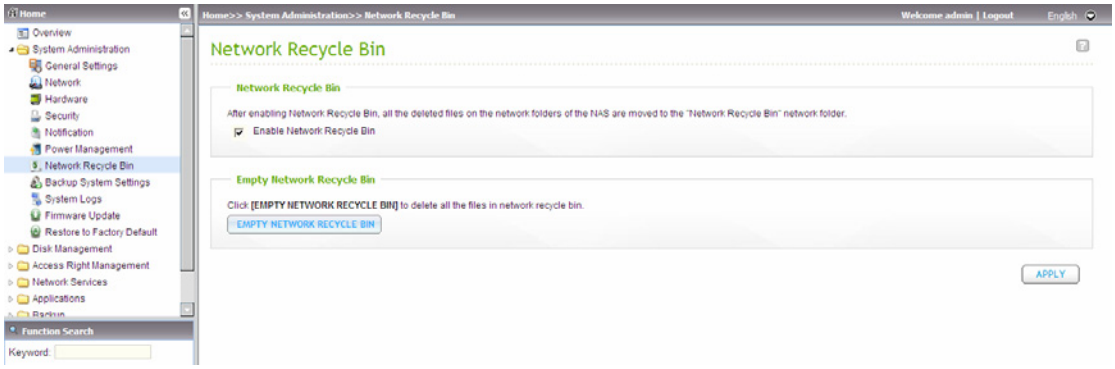
- **Power on/ power off/ restart schedule**
  You can select every day, weekdays, weekend, or any days of the week and set the time for automatic system power on, power off, or restart. Weekdays stand for Monday to Friday; weekend stands for Saturday and Sunday. Up to 15 schedules can be set.


Home
Overview
System Administration
General Settings
Network
Hardware
Security
Notification
Power Management
Network Recycle Bin
Backup System Settings
System Logs
Firmware Update
Restore to Factory Default
Disk Management
Access Right Management
Network Services
Applications
Function Search
Keyword:
Home>> System Administration>> Power Management
Welcome admin | Logout
English
Power Management
Restart/ Shutdown
Execute system restart/ shutdown immediately.
RESTART
SHUTDOWN
Configure Wake on LAN
Enable
Disable
When the AC power resumes:
Resume the server to the previous power-on or power-off status.
Turn on the server automatically.
The server should remain off.
Set power on/ power off/ restart schedule
Enable schedule
Postpone the restart/shutdown schedule when replication job is in process.
Turn on the server
Daily
11
32
Turn on the server
Daily
12
31
APPLY

3.1.7 Network Recycle Bin

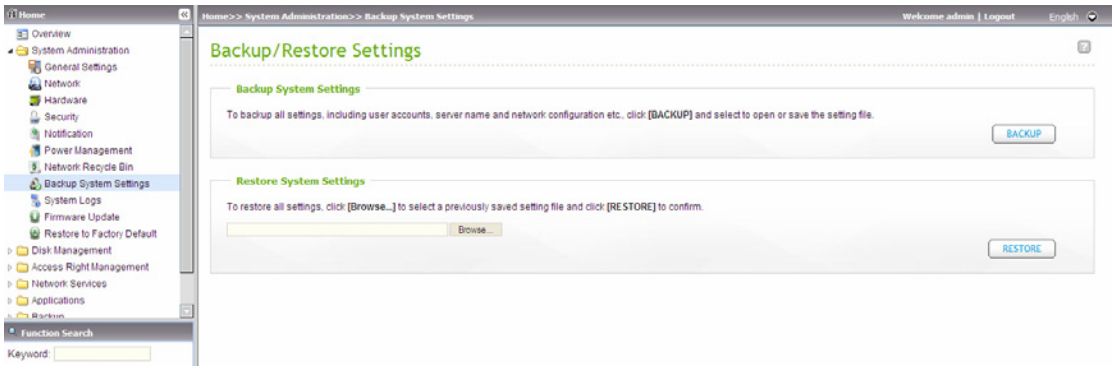
This function enables the files deleted on the shares of the NAS to be removed to Network Recycle Bin to reserve the files temporarily. To enable this function, check the box "Enable Network Recycle Bin" and click "Apply". The system will create a network share "Network Recycle Bin" automatically.

To delete all the files in network recycle bin, click "Empty Network Recycle Bin".



3.1.8 Backup/ Restore Settings

- To back up all the settings, including the user accounts, server name and network configuration etc., click “Backup” and select to open or save the setting file.
- To restore all the settings, click “Browse” to select a previously saved setting file and click “Restore”.

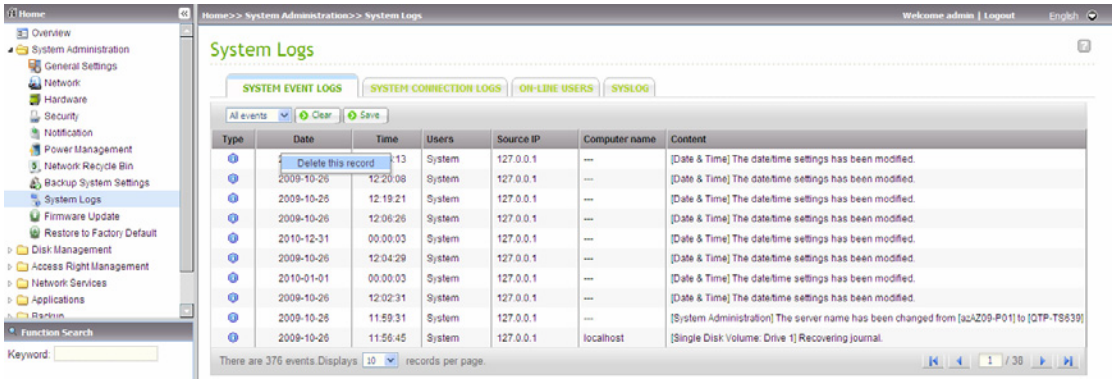


3.1.9 System Logs

3.1.9.1 System Event Logs

The NAS can store 10,000 recent event logs, including warning, error, and information messages. In case of system malfunction, the event logs can be retrieved to analyze the system problems.

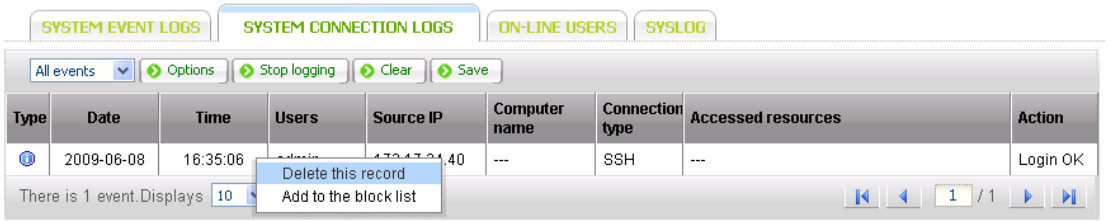
Tip: You can right click a log and delete the record.



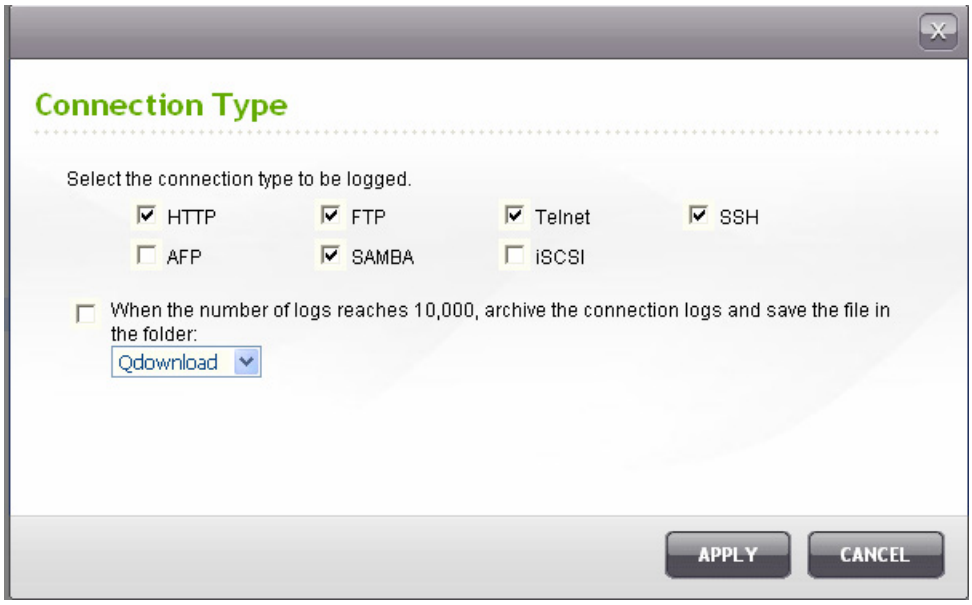
3.1.9.2 System Connection Logs

The system supports logging HTTP, FTP, Telnet, SSH, AFP, NFS, SAMBA, and iSCSI connections. Click "Options" to select the connection type to be logged.
The file transfer performance can be slightly affected by enabling the event logging.

Tip: You can right click the log on the list of connection logs and select to delete the record or add the IP to banned list and select how long the IP should be banned.



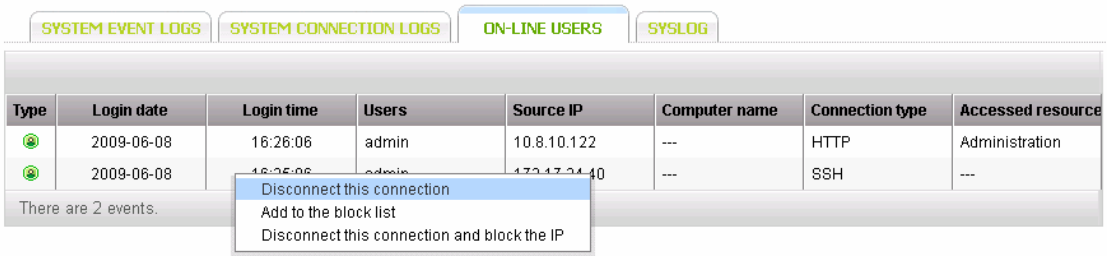
Archive logs: Enable this option to archive the connection logs. The system generates a csv file automatically and saves it to a specified folder when the number of logs reaches the upper limit.



3.1.9.3 On-line Users

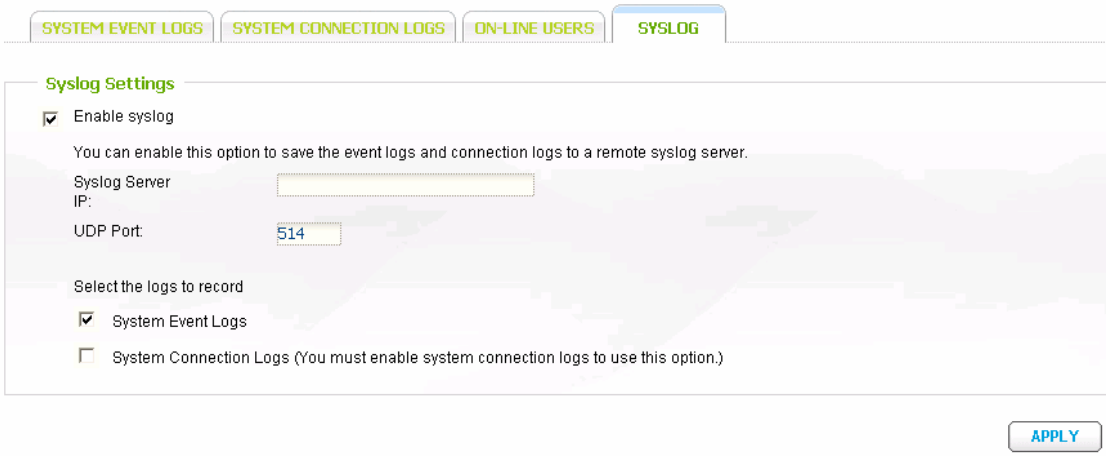
The information of the on-line users accessing the system via networking services is shown in this page.

Tip: You can right click a log and select to disconnect the IP connection and/or add the IP to the block list.

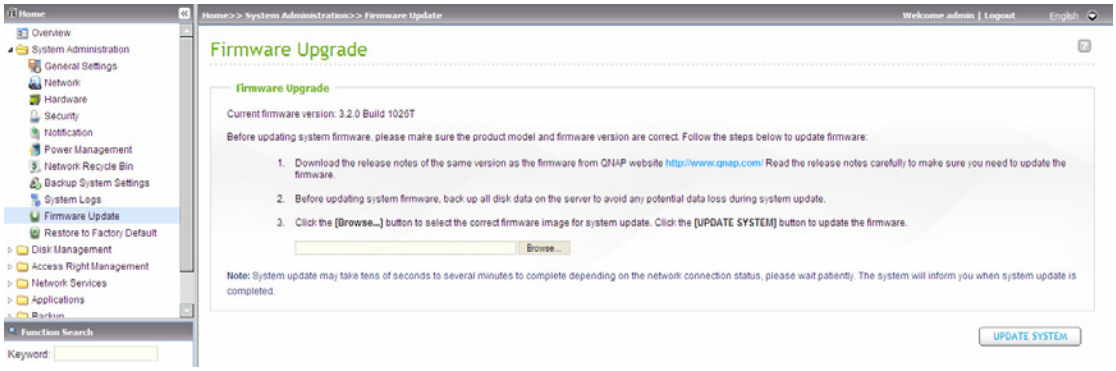


3.1.9.4 Syslog

Syslog is a standard for forwarding log messages in an IP network. You can enable this option to save the event logs and connection logs to a remote syslog server.



3.1.10 Firmware Update



Note: If the system is running properly, you do not need to update the firmware.

Before updating the system firmware, make sure the product model and firmware version are correct. Follow the steps below to update firmware:

Step 1: Download the release notes of the same version as the firmware from QNAP website http://www.qnap.com. Read the release notes carefully to make sure you need to upgrade the firmware.

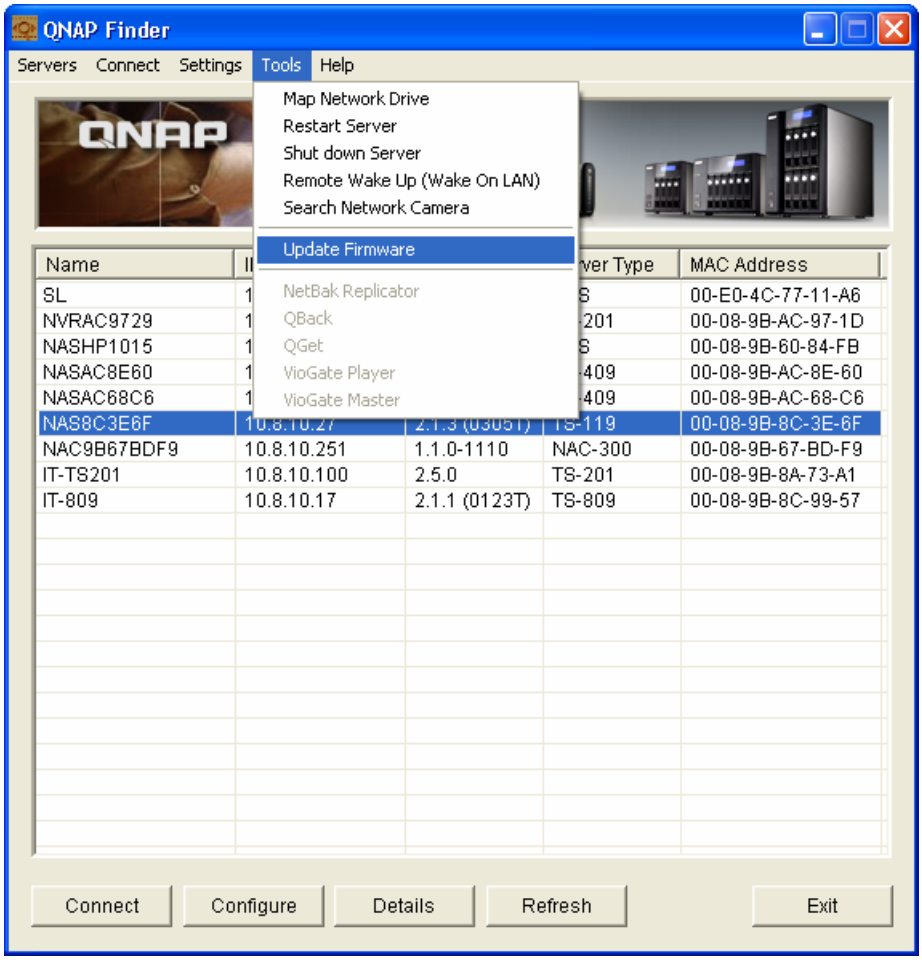
Step 2: Before upgrading system firmware, back up all disk data on the server to avoid any potential data loss during system update.

Step 3: Click "Browse" to select the correct firmware image for system update. Click "Update System" to update the firmware.

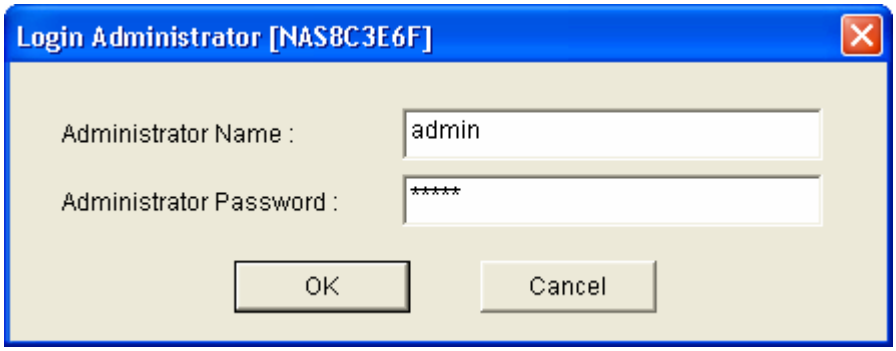
The system update may take tens of seconds to several minutes to complete depending on the network connection status. Please wait patiently. The system will inform you when system update is completed.

Update the system firmware by Finder

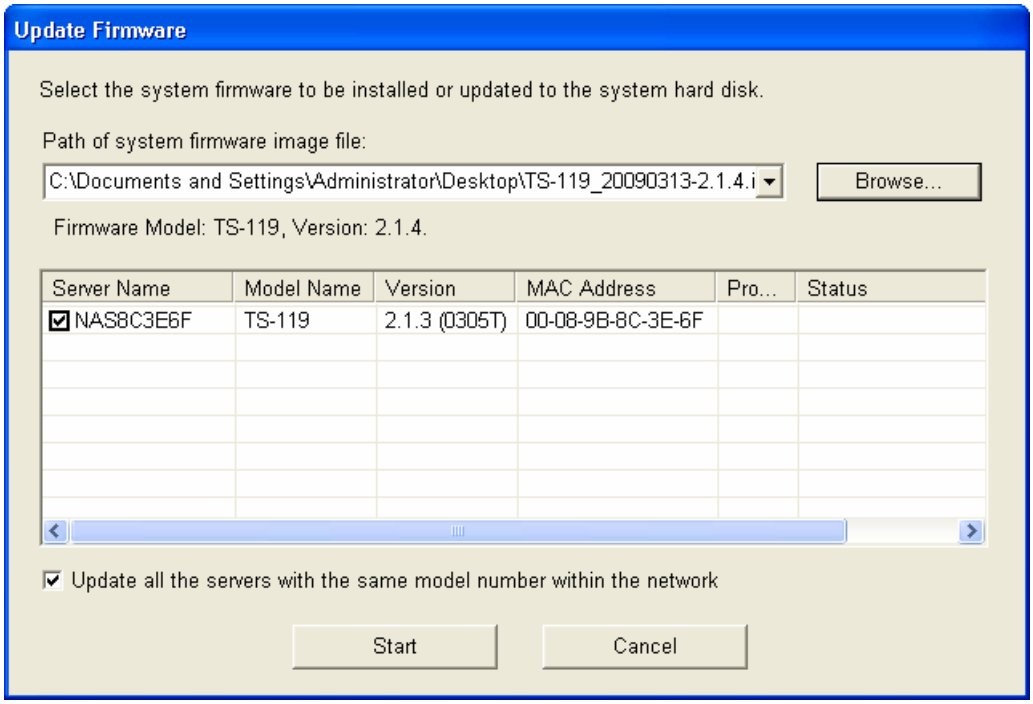
You can update the system firmware by QNAP Finder. Select a NAS model and click "Update Firmware" from the "Tools" menu.



Login as the administrator.



Browse and select the firmware for the NAS. Click "Start" to update the system.

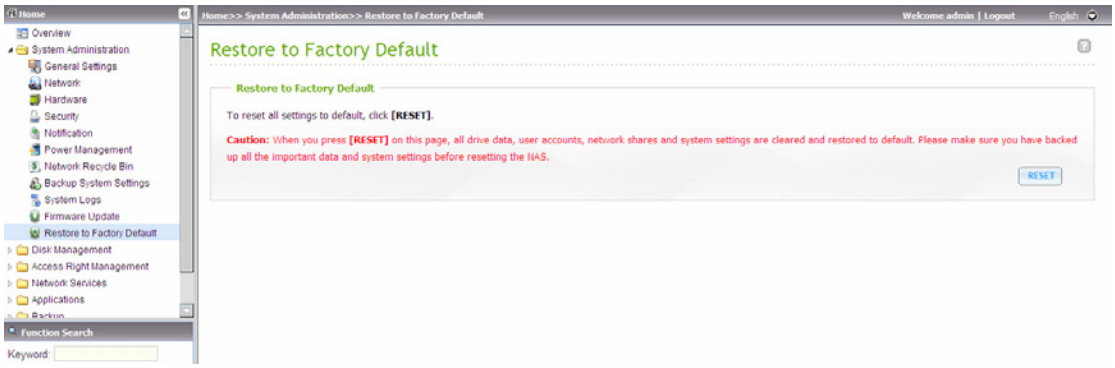


Note: You can use the Finder to update all the servers of the same model on the same local network. Make sure you have administrator access to all the servers you want to update.

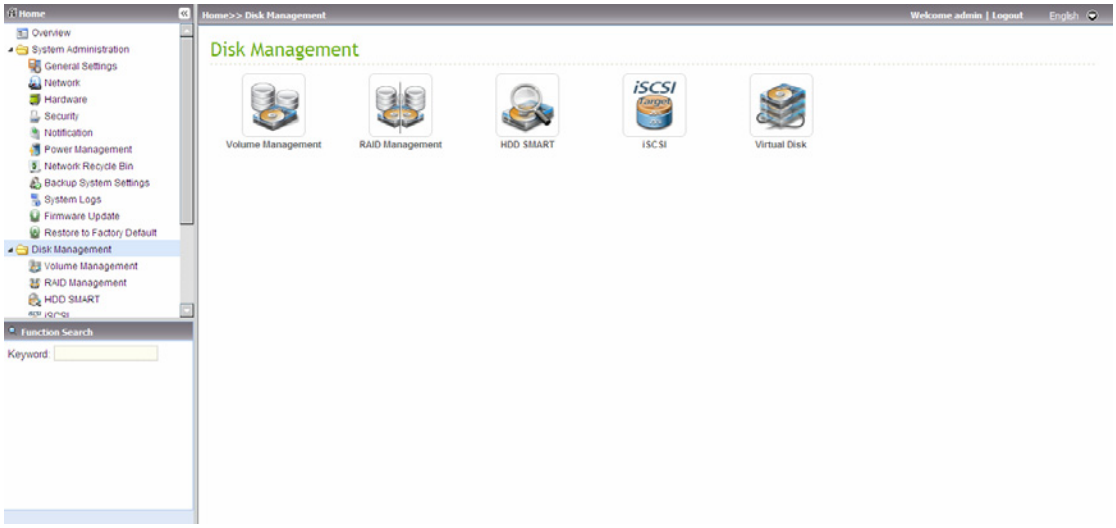
3.1.11 Restore to Factory Default

To reset all settings to default, click “RESET”.

Caution: When you press “RESET” on this page, all the drive data, user accounts, network shares, and system settings are cleared and restored to default. Please make sure you have backed up all the important data and system settings before resetting the NAS.



3.2 Disk Management



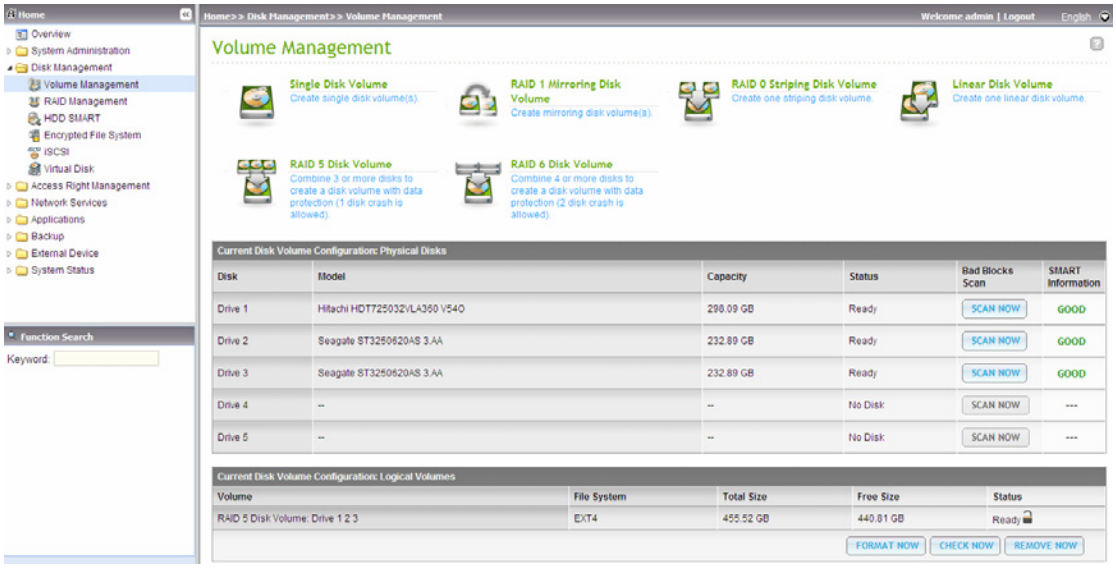
3.2.1 Volume Management

This page shows the model, size, and current status of the disk on the NAS. You can format and check disk, and scan bad blocks on the disk. When the disk is formatted, the NAS will create the following default share folders:

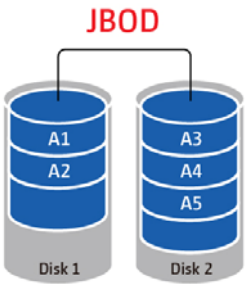
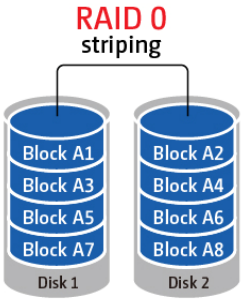
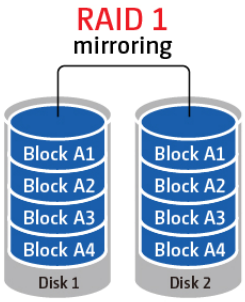
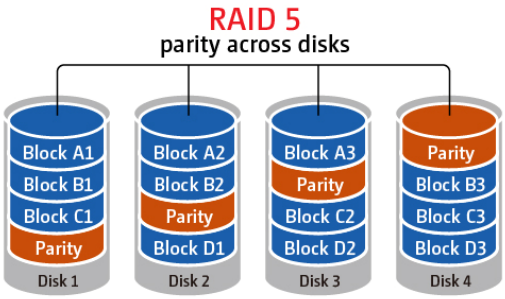
- ✓ Public: Network share for file sharing
- ✓ Qdownload/ Download*: The default network share for Download Station.
- ✓ Qmultimedia/ Multimedia*: The default network share for Multimedia Station.
- ✓ Qusb/ Usb*: The default network share for data copy function via USB ports.
- ✓ Qweb/ Web*: The default network share for Web Server.
- ✓ Qrecordings/ Recordings*: The default network share of Surveillance Station.

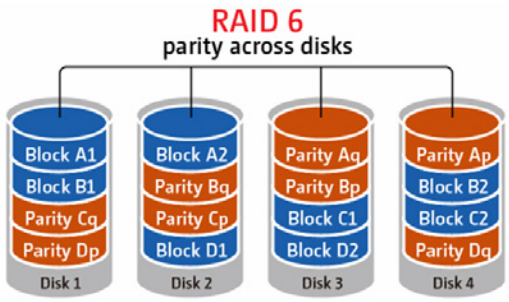
*TS-259/ TS-459/ TS-659/ TS-859 series only.

Note: The default shares are created on the first disk volume and the directory cannot be changed.



Disk Configuration	**Applied NAS Models**
Single disk volume	All models
RAID 1, JBOD (just a bunch of disks)	2-bay models or above
RAID 5, RAID 6, RAID 5+hot spare,	4-bay models or above
RAID 6+hot spare	5-bay models or above

Single Disk Volume Each hard disk drive is used as a standalone disk. If a disk is damaged, all the data will be lost.	
JBOD (Just a bunch of disks) JBOD is a collection of hard disk drives that does not offer any RAID protection. The data are written to the physical disks sequentially. The total storage capacity equals to the sum of the capacity of all the member drives.	
RAID 0 Striping Disk Volume RAID 0 (striping disk) combines 2 or more hard disk drives into one larger volume. The data is written to the hard disk drives without any parity information and no redundancy is offered. The disk capacity equals the number of hard disk drives in the array times the size of the smallest hard drive.	
RAID 1 Mirroring Disk Volume RAID 1 duplicates the data between two hard disk drives to provide disk mirroring. To create a RAID 1 array, a minimum of 2 hard drives are required.	
RAID 5 Disk Volume The data are striped across all the drives in a RAID 5 array. The parity information is distributed and stored across each drive. If a member drive fails, the array enters degraded mode. After installing a new drive to replace the failed one, the data can be rebuilt from other member drives that contain the parity information.	

To create a RAID 5 disk volume, a minimum of 3 hard disks are required. The storage capacity of a RAID 5 array equals (N-1). N is the total number of drive members in the array.	
RAID 6 Disk Volume The data are striped across all the drives in a RAID 6 array. RAID 6 differs from RAID 5 that a second set of parity information is stored across the member drives in the array. It tolerates failure of two member drives. To create a RAID 6 disk volume, a minimum of 4 hard disks are required. The storage capacity of a RAID 6 array equals (N-2). N is the total number of drive members in the array.	

3.2.2 RAID Management

* This function does not apply to one-bay model, and TS-210.

You can perform RAID capacity expansion (RAID 1/ 5/ 6), RAID level migration (single disk/ RAID 1/ RAID 5), or configure the spare drive (RAID 5/ 6) with the data retained.

Bitmap improves the time for RAID rebuilding after a crash, or removing or re-adding a member drive of the RAID configuration. If an array has a bitmap, the member drive can be removed and re-added and only blocks changes since the removal (as recorded in the bitmap) will be re-synchronized.

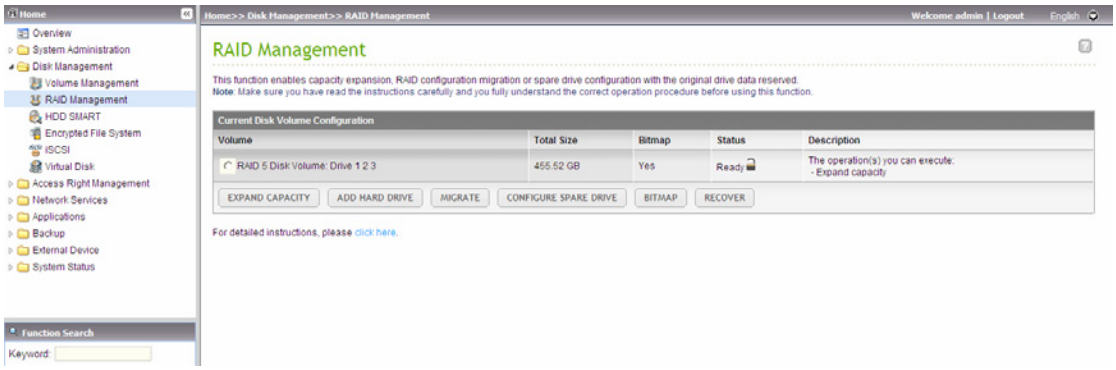
Note: Bitmap support is only available for RAID 1, 5, and 6.

RAID Recovery: When the NAS is configured as RAID 5 (or RAID 6) and 2 (or 3) hard drives are uplugged from the server accidentally, you can plug in the same hard drives into the same drive slots and click "Recover" to recover the volume status from "Not active" to "Degraded mode".

If the disk volume is configured as RAID 0 or JBOD and one or more of the drive members are disconnected, you can use this function to recover the volume status from "Not active" to "Normal". The disk volume can be used normally after successful recovery.

Note: If the disconnected drive member is damaged, the RAID recovery function will not work.
RAID recovery is not supported by TS-110, TS-210, TS-119.

For the online tutorial, please visit http://www.qnap.com/pro_features.asp.



RAID Level / RAID Status	Traditional RAID 5	QNAP RAID 5	Traditional RAID 6	QNAP RAID 6
Degraded mode	N-1	N-1	N-1 & N-2	N-1 & N-2
Read Only Protection (for immediate data backup & HDD replacement)	N/A	N-1, bad blocks found in the surviving drives of the array.	N/A	N-2, bad blocks found in the surviving drives of the array.
RAID Recovery (RAID Status: Not Active)	N/A	If re-inserting all the original hard disk drives to the NAS and they can be spun up, identified, accessed, and the HDD superblock is not damaged.	N/A	If re-inserting all the original hard disk drives to the NAS and they can be spun up, identified, accessed, and the HDD superblock is not damaged).
RAID Crash	N-2	N-2 failed HDD and any of the remaining HDD cannot be spun up/ identified/ accessed.	N-3	N-3 and any of the remaining HDD cannot be spun up/ identified/ accessed.

N = Number of hard disk drives in the array

The NAS supports the following actions according to the number of hard drives and disk configurations supported. Please refer to the following table for the details.

Original Disk Configuration * No. of HDD	No. of New HDD	Action	New Disk Configuration * No. of HDD
RAID 5 * 3	1	Add HDD member	RAID 5 * 4
RAID 5 * 3	2	Add HDD member	RAID 5 * 5
RAID 5 * 3	3	Add HDD member	RAID 5 * 6
RAID 5 * 3	4	Add HDD member	RAID 5 * 7
RAID 5 * 3	5	Add HDD member	RAID 5 * 8
RAID 5 * 4	1	Add HDD member	RAID 5 * 5
RAID 5 * 4	2	Add HDD member	RAID 5 * 6
RAID 5 * 4	3	Add HDD member	RAID 5 * 7
RAID 5 * 4	4	Add HDD member	RAID 5 * 8
RAID 5 * 5	1	Add HDD member	RAID 5 * 6
RAID 5 * 5	2	Add HDD member	RAID 5 * 7
RAID 5 * 5	3	Add HDD member	RAID 5 * 8
RAID 5 * 6	1	Add HDD member	RAID 5 * 7
RAID 5 * 6	2	Add HDD member	RAID 5 * 8
RAID 5 * 7	1	Add HDD member	RAID 5 * 8
RAID 6 * 4	1	Add HDD member	RAID 6 * 5
RAID 6 * 4	2	Add HDD member	RAID 6 * 6
RAID 6 * 4	3	Add HDD member	RAID 6 * 7
RAID 6 * 4	4	Add HDD member	RAID 6 * 8
RAID 6 * 5	1	Add HDD member	RAID 6 * 6
RAID 6 * 5	2	Add HDD member	RAID 6 * 7
RAID 6 * 5	3	Add HDD member	RAID 6 * 8
RAID 6 * 6	1	Add HDD member	RAID 6 * 7
RAID 6 * 6	2	Add HDD member	RAID 6 * 8
RAID 6 * 7	1	Add HDD member	RAID 6 * 8
RAID 1 * 2	1	Online RAID Capacity Expansion	RAID 1 * 2
RAID 5 * 3	1	Online RAID Capacity Expansion	RAID 5 * 3
RAID 5 * 4	1	Online RAID Capacity Expansion	RAID 5 * 4

RAID 5 * 5	1	Online RAID Capacity Expansion	RAID 5 * 5
RAID 5 * 6	1	Online RAID Capacity Expansion	RAID 5 * 6
RAID 5 * 7	1	Online RAID Capacity Expansion	RAID 5 * 7
RAID 5 * 8	1	Online RAID Capacity Expansion	RAID 5 * 8
RAID 6 * 4	1	Online RAID Capacity Expansion	RAID 6 * 4
RAID 6 * 5	1	Online RAID Capacity Expansion	RAID 6 * 5
RAID 6 * 6	1	Online RAID Capacity Expansion	RAID 6 * 6
RAID 6 * 7	1	Online RAID Capacity Expansion	RAID 6 * 7
RAID 6 * 8	1	Online RAID Capacity Expansion	RAID 6 * 8
Single * 1	1	Online RAID Level Migration	RAID 1 * 2
Single * 1	2	Online RAID Level Migration	RAID 5 * 3
Single * 1	3	Online RAID Level Migration	RAID 5 * 4
Single * 1	4	Online RAID Level Migration	RAID 5 * 5
Single * 1	5	Online RAID Level Migration	RAID 5 * 6
Single * 1	6	Online RAID Level Migration	RAID 5 * 7
Single * 1	7	Online RAID Level Migration	RAID 5 * 8
Single * 1	3	Online RAID Level Migration	RAID 6 * 4
Single * 1	4	Online RAID Level Migration	RAID 6 * 5
Single * 1	5	Online RAID Level Migration	RAID 6 * 6

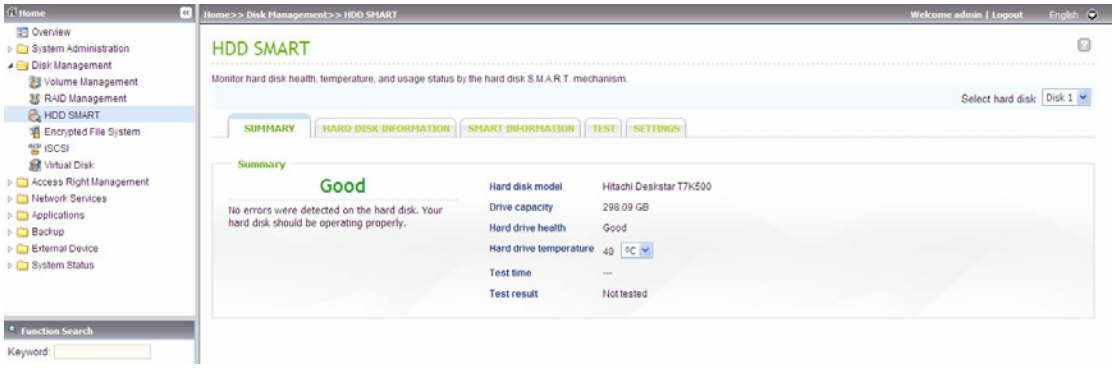
Single * 1	6	Online RAID Level Migration	RAID 6 * 7
Single * 1	7	Online RAID Level Migration	RAID 6 * 8
RAID 1 * 2	1	Online RAID Level Migration	RAID 5 * 3
RAID 1 * 2	2	Online RAID Level Migration	RAID 5 * 4
RAID 1 * 2	3	Online RAID Level Migration	RAID 5 * 5
RAID 1 * 2	4	Online RAID Level Migration	RAID 5 * 6
RAID 1 * 2	5	Online RAID Level Migration	RAID 5 * 7
RAID 1 * 2	6	Online RAID Level Migration	RAID 5 * 8
RAID 1 * 2	2	Online RAID Level Migration	RAID 6 * 4
RAID 1 * 2	3	Online RAID Level Migration	RAID 6 * 5
RAID 1 * 2	4	Online RAID Level Migration	RAID 6 * 6
RAID 1 * 2	5	Online RAID Level Migration	RAID 6 * 7
RAID 1 * 2	6	Online RAID Level Migration	RAID 6 * 8
RAID 5 * 3	1	Online RAID Level Migration	RAID 6 * 4
RAID 5 * 3	2	Online RAID Level Migration	RAID 6 * 5
RAID 5 * 3	3	Online RAID Level Migration	RAID 6 * 6
RAID 5 * 3	4	Online RAID Level Migration	RAID 6 * 7
RAID 5 * 3	5	Online RAID Level Migration	RAID 6 * 8

3.2.3 HDD SMART

This page enables the users to monitor the hard drive health, temperature, and the usage status by the hard disk S.M.A.R.T. mechanism.

Select the hard drive and you can view the following information by clicking the corresponding buttons.

Field	Description
Summary	Displays the hard drive S.M.A.R.T. summary and the latest test result.
Hard disk information	Displays the hard drive details, e.g. model, serial number, drive capacity.
SMART information	Displays the hard drive S.M.A.R.T. Any items that the values are lower than the threshold are regarded as abnormal.
Test	To perform quick or complete hard drive S.M.A.R.T. test and display the results.
Settings	Configure the temperature alarm. When the hard drive temperature is over the preset values, the system records the error logs. You can also configure quick and complete test schedule. The latest test result is shown on the Summary page.



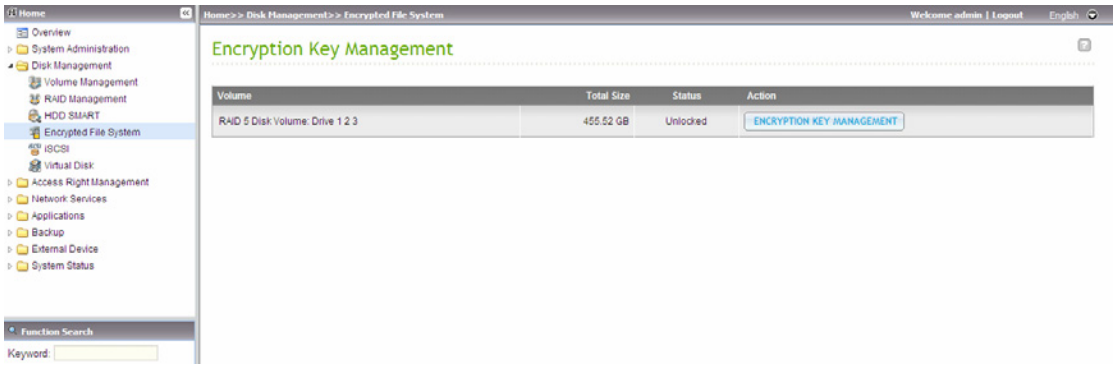
3.2.4 Encrypted File System

This function is applicable to certain models only. Please refer to the comparison table for more details:
http://www.qnap.com/images/products/comparison/Comparison_NAS.html

You can manage the encrypted disk volumes on the NAS on this page. Each encrypted disk volume is locked by a particular key. The encrypted volume can be unlocked by the following methods:

- Encryption Password: Enter the encryption password to unlock the disk volume. The default password is "admin". The password must be 8-16 characters long. Symbols (! @ # $ % ^ & * ( )_+ = ?) are supported.
- Encryption Key File: You can upload the encryption file to the server to unlock the disk volume. The key can be downloaded from "Encryption Key Management" page after you have unlocked the disk volume successfully.

The data encryption functions may not be available in accordance to the legislative restrictions of some countries.



3.2.5 iSCSI

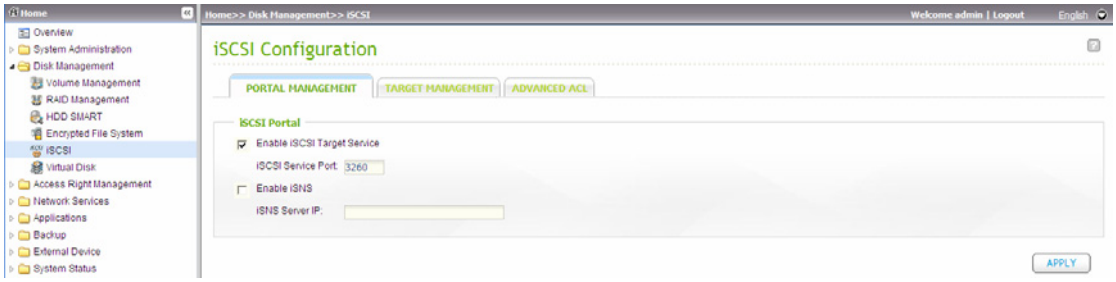
The NAS supports built-in iSCSI service for server clustering and virtualized environments.

Note: The NAS supports 8 iSCSI devices at maximum.

3.2.5.1 iSCSI Target

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

1. Click "Portal Management" tab and enable iSCSI target service. Apply the settings.



2. When the service is enabled, go to "Target Management" tab to create iSCSI targets on the NAS.

If you have not created any iSCSI targets, the Quick Installation Wizard will show up and prompt you to create iSCSI targets and/or LUN (Logical unit number). Click "OK".

3. When the wizard is shown, select to create an iSCSI target with a mapped LUN, an iSCSI target only, or an iSCSI LUN only. Click "Next".

4. Create iSCSI target with a mapped LUN:

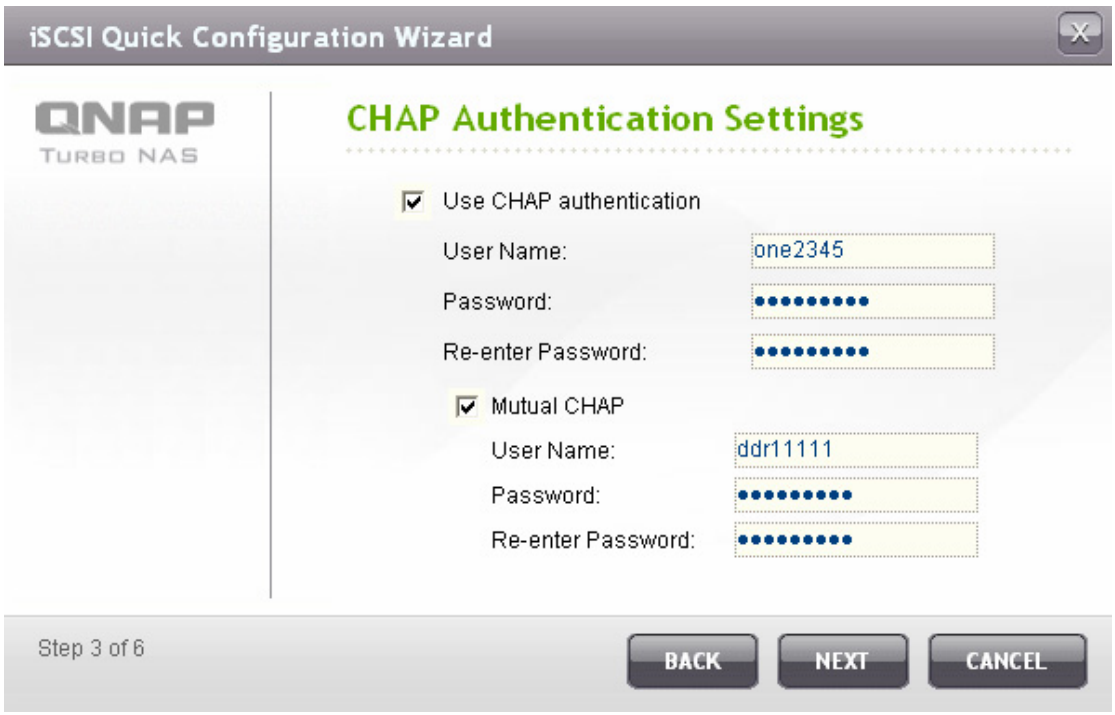
Click "Next".

5. Enter the target name and target alias. You may check the options "Data Digest" and/or "Header Digest" (optional). These are the parameters that the iSCSI initiator will be verified when it attempts to connect to the iSCSI target.

6. Enter the CHAP authentication settings. If you enter the user name and password settings under "Use CHAP authentication" only, only the iSCSI target authenticates the initiator, i.e. the initiators have to enter the user name password settings here to access the target.

Mutual CHAP: Enable this option for two-way authentication between the iSCSI target and the initiator. The target authenticates the initiator using the first set of user name and password. The initiator authenticates the target using the "Mutual CHAP" settings.

Field	User name limitation	Password limitation
Use CHAP authentication	• The only valid characters are 0-9, a-z, A-Z • Maximum length: 256 characters	• The only valid characters are 0-9, a-z, A-Z • Maximum length: 12-16 characters
Mutual CHAP	• The only valid characters are 0-9, a-z, A-Z, : (colon), . (dot), and - (dash) • Maximum length: 12-16 characters	• The only valid characters are 0-9, a-z, A-Z, : (colon), . (dot), and - (dash) • Maximum length: 12-16 characters



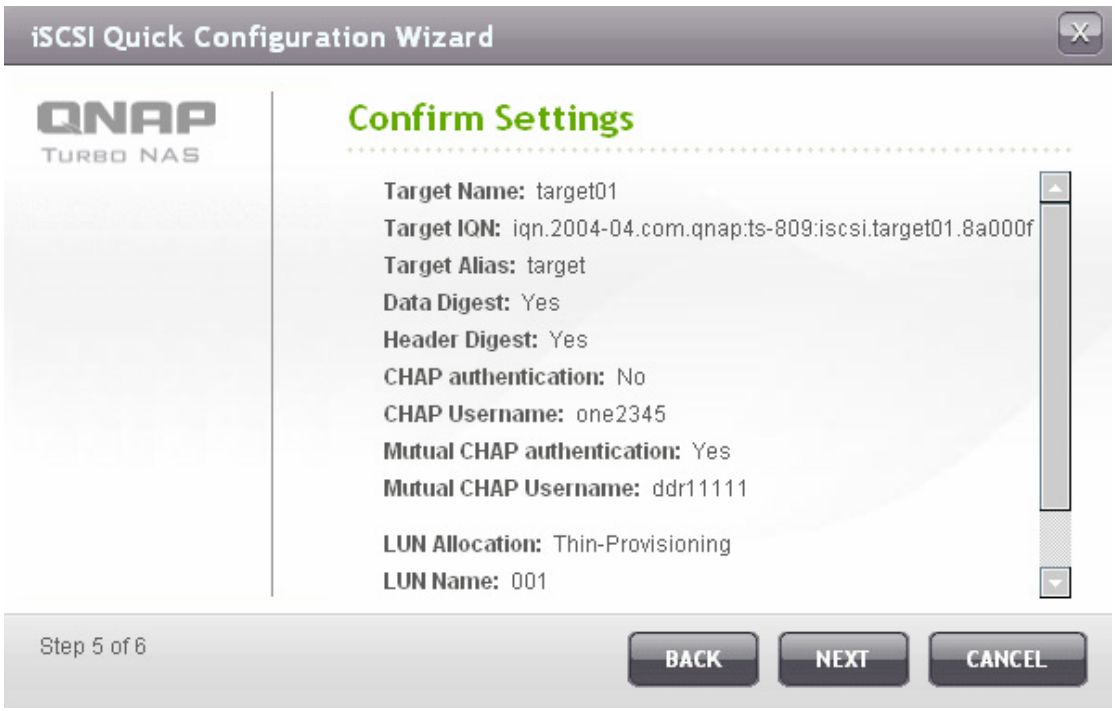
7. Create an iSCSI LUN

An iSCSI LUN is a logical volume mapped to the iSCSI target. Select one of the following modes to allocate the disk space to the LUN:

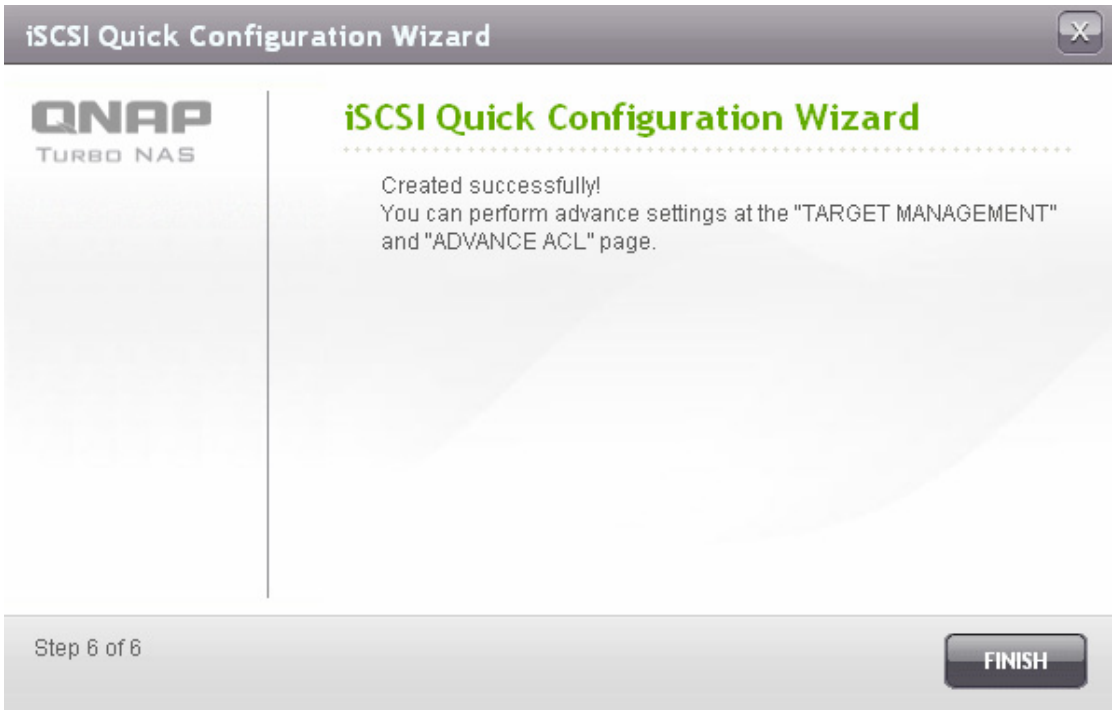
- Thin Provisioning: Select this option to allocate the disk space in a flexible manner. You can allocate the disk space to the target anytime regardless of the current storage capacity available on the NAS. Over-allocation is allowed since the storage capacity of the NAS can be expanded by Online RAID Capacity Expansion.
- Instant Allocation: Select this option to allocate the disk space to the LUN instantly. This option guarantees the disk space assigned to the LUN but may take a longer while to create the LUN.

Enter the LUN name and specify the LUN location (disk volume on the NAS). Enter the capacity for the LUN. Click "Next".

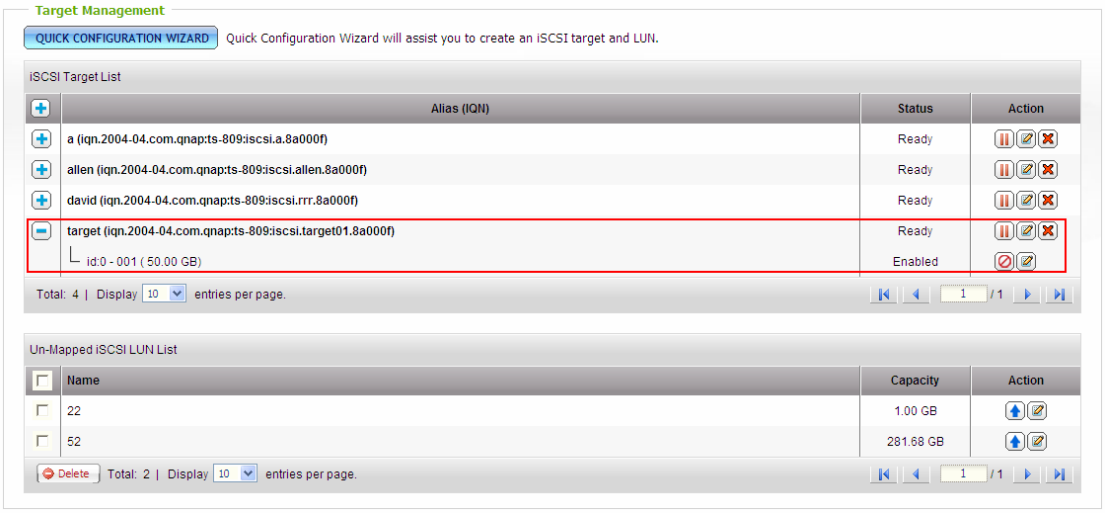
8. Confirm the settings and click “Next”.



9. When the target and the LUN have been created, click “Finish”.



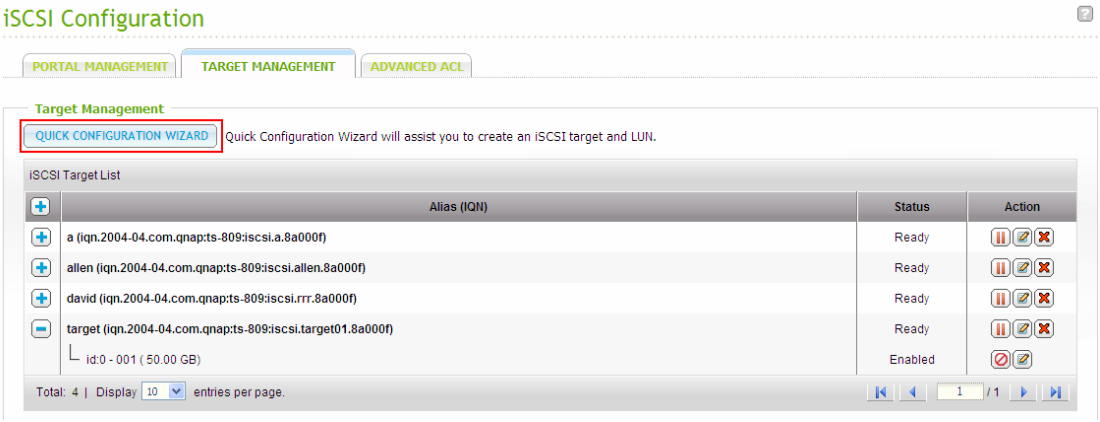
10. The target and LUN are shown on the list under the "Target Management" tab.



Create more LUN for a target

You can create multiple LUN for an iSCSI target. Follow the steps below to create more LUN for an iSCSI target.

1. Click "Quick Configuration Wizard" under "Target Management".

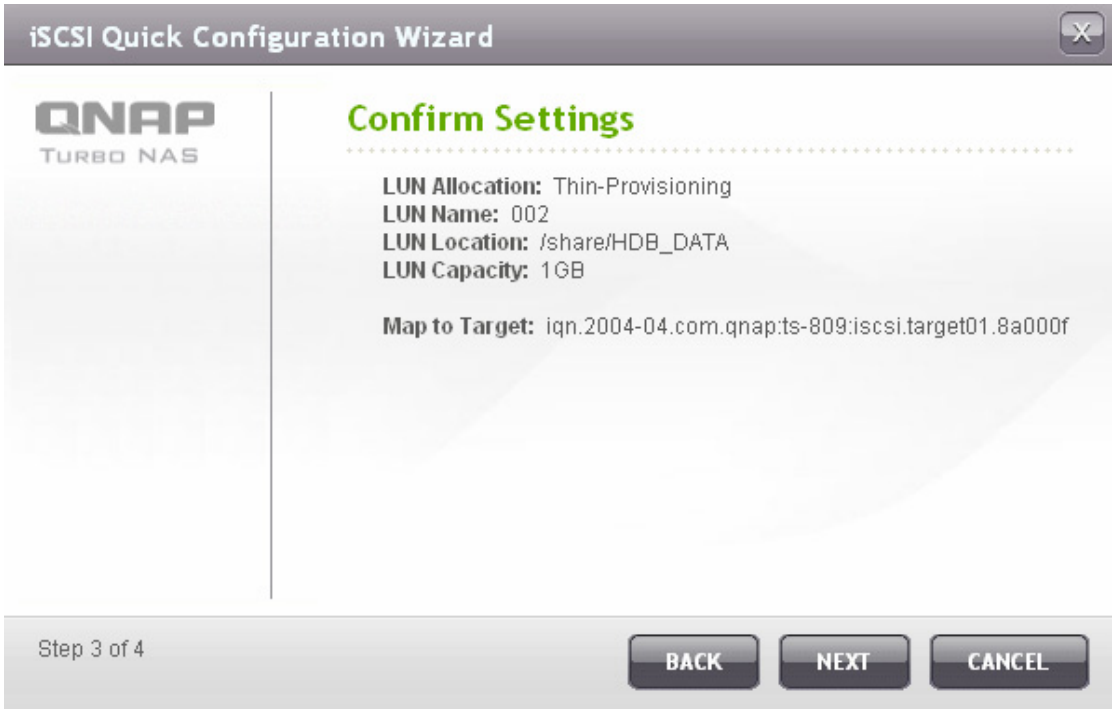


2. Select “iSCSI LUN only” and click “Next”.

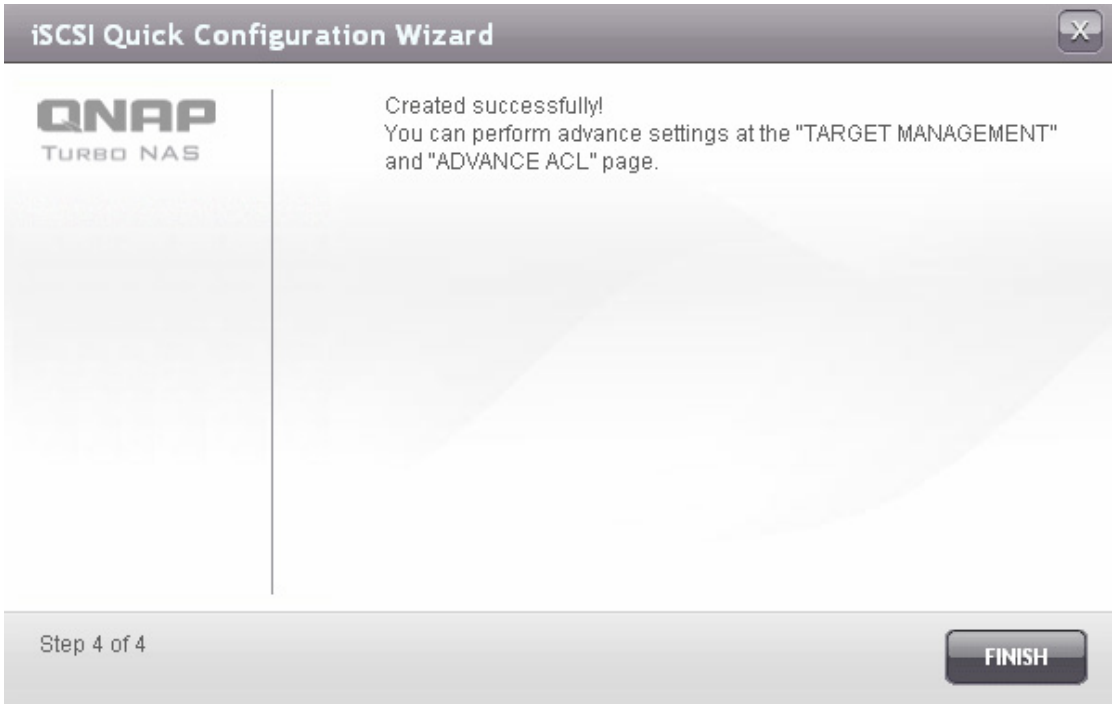
3. Select the LUN allocation method. Enter the LUN name, select the LUN directory, and specify the capacity for the LUN. Click “Next”.

4. Select the target to map the LUN to. You can also select not to map the LUN for now.

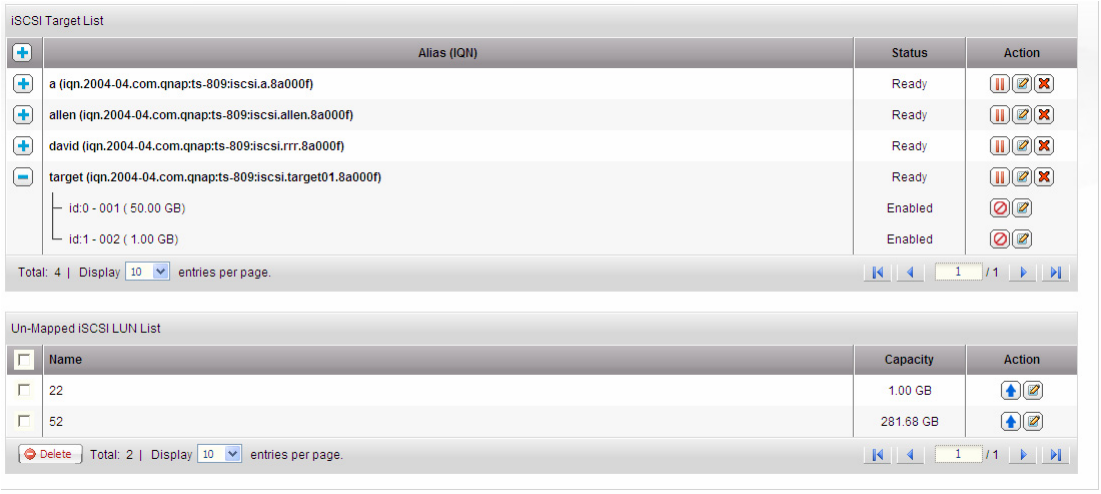
5. Confirm the settings and click "Next".



6. When the LUN has been created, click “Finish” to exit the wizard.



7. The LUNs created can be mapped to and unmapped from the iSCSI target anytime. You can also unmap the LUN from a target and map it to another target.



Item	Status	Description
iSCSI target	Ready	The iSCSI target is ready but no initiator has connected to it yet.
	Connected	The iSCSI target has been connected by an initiator.
	Disconnected	The iSCSI target has been disconnected
	Offline	The iSCSI target has been deactivated and cannot be connected by the initiator.
LUN	Enabled	The LUN is active for connection and is visible to authenticated initiators.
	Disabled	The LUN is inactive and is invisible to the initiators.

Button	Description
	Deactivate a ready or connected target. Note that the connection from the initiators will be removed.
	Activate an offline target.
	Modify the target settings: target alias, CHAP information, and checksum settings. Modify the LUN settings: LUN allocation, name, disk volume directory, etc.
	Delete an iSCSI target. All the connections will be removed.
	Disable an LUN. All the connections will be removed.
	Enable an LUN.
	Unmap the LUN from the target. Note that you must disable the LUN first before unmapping the LUN. When you click this button, the LUN will be moved to "Un-Mapped iSCSI LUN List".
	Map the LUN to an iSCSI target. This option is only available on the "Un-Mapped iSCSI LUN List".
	View the connection status of an iSCSI target.

Switch the mapping of an LUN

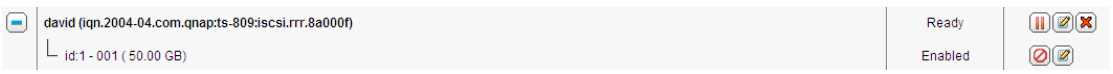
Follow the steps below to switch the mapping of an LUN.

1. Select an LUN to unmap from an iSCSI target and click (Disable).

2. Next, click to unmap the LUN. The LUN will appear on the Un-Mapped iSCSI LUN List. Click to map the LUN to another target.

3. Select the target to map the LUN to and click "Apply".

4. The LUN is mapped to the target.

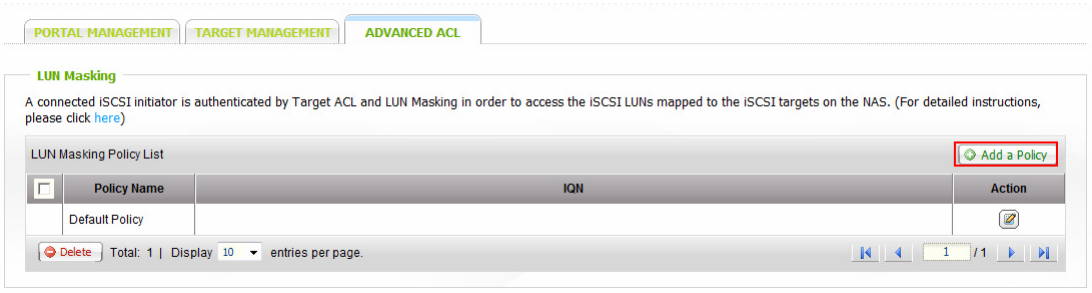


After creating the iSCSI targets and LUN on the NAS, you can use the iSCSI initiator installed on your computer (Windows PC, Mac, or Linux) to connect to the iSCSI targets and LUN and use the disk volumes as the virtual drives on your computer.

For the online tutorial, please refer to http://www.qnap.com/pro_features.asp.

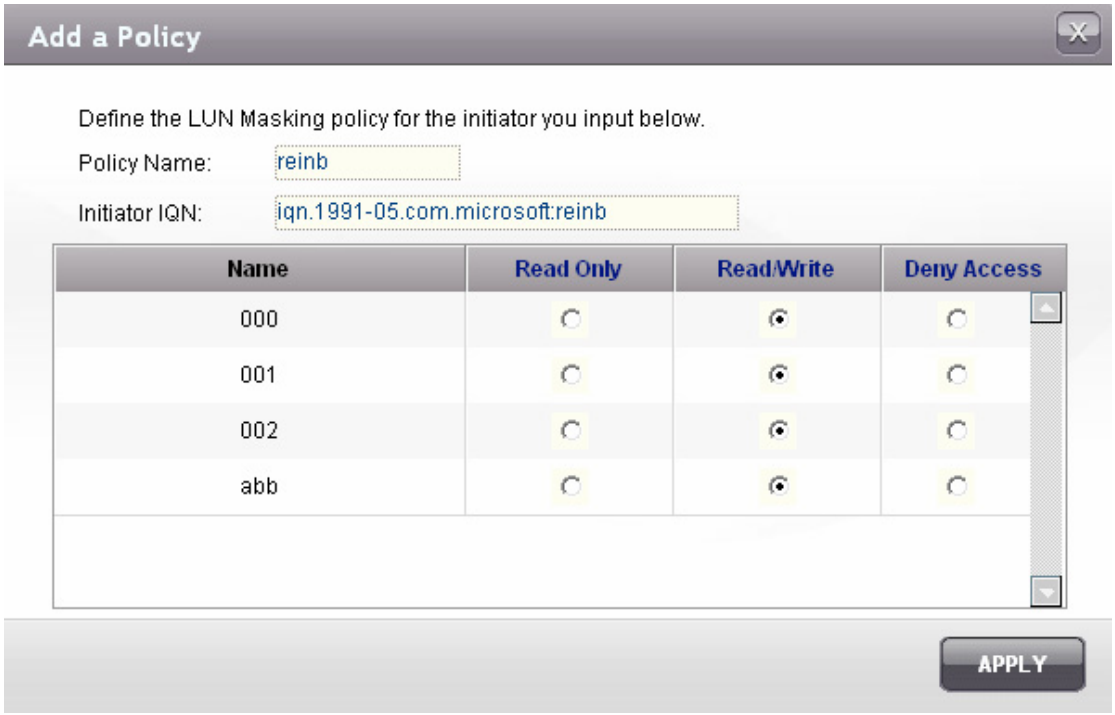
3.2.5.2 ADVANCED ACL

You can create LUN masking policy to configure the permission of the iSCSI initiators which attempt to access the LUN mapped to the iSCSI targets on the NAS. To use this feature, click "Add a Policy" on "ADVANCED ACL".



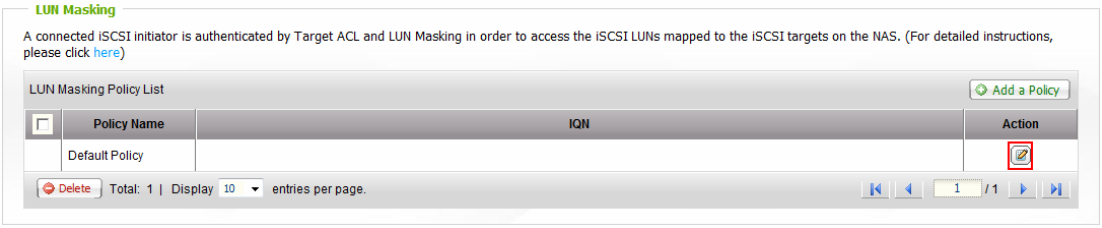
Enter the policy name, the initiator IQN, and assign the access right for each LUN created on the NAS.

- Read-only: The connected initiator can only read the data from the LUN.
- Read/Write: The connected initiator has read and write access to the LUN.
- Deny Access: The LUN is invisible to the connected initiator.



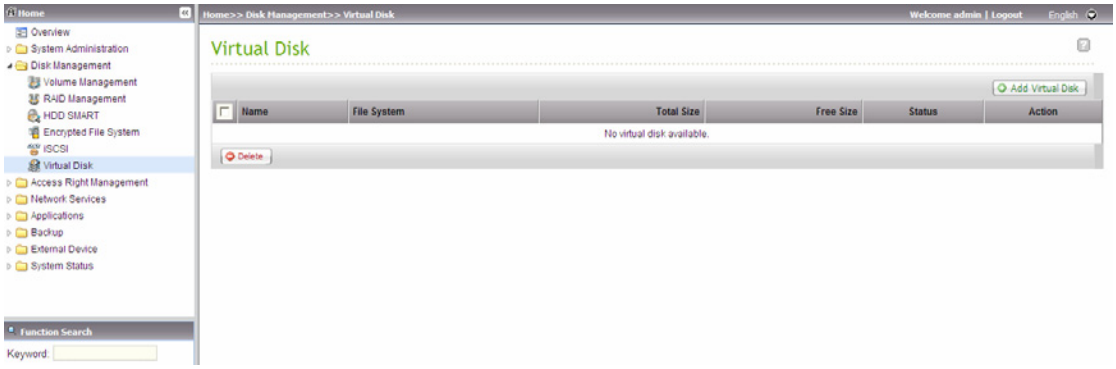
If no LUN masking policy is specified for a connected iSCSI initiator, the default policy will be applied. The system default policy allows read and write access from all the connected iSCSI initiators. You can click  on the LUN masking list to edit the default policy.

Note: Make sure you have created at least one LUN on the NAS before editing the default LUN policy.

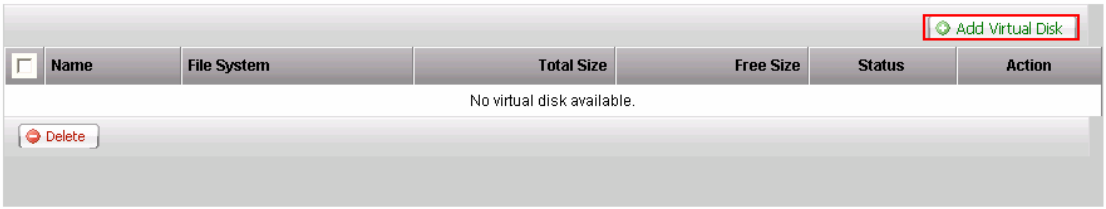


3.2.6 Virtual Disk

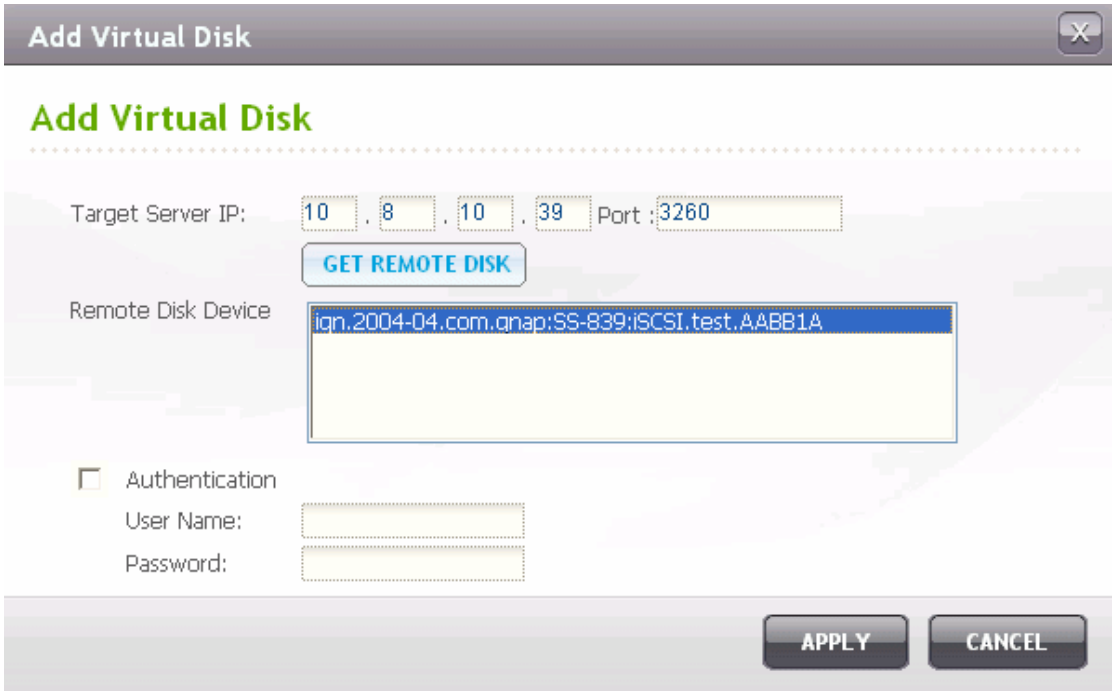
You can use this function to add the iSCSI targets of other QNAP NAS or storage servers to the NAS as the virtual disks for storage capacity expansion.



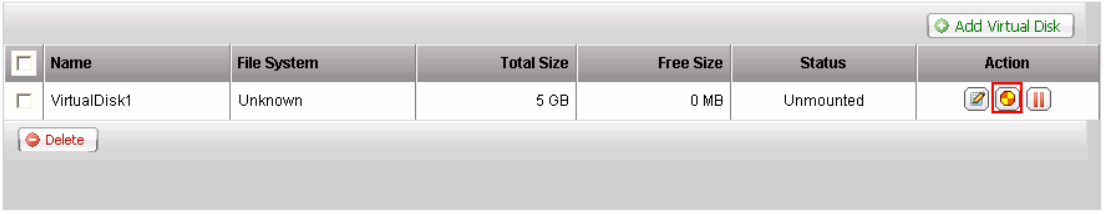
To add a virtual disk to the NAS, make sure an iSCSI target has been created. Click "Add Virtual Disk".



Enter the target server IP and port number (default: 3260). Click "Get Remote Disk". If authentication is required, enter the user name and the password. Then, click "Apply".



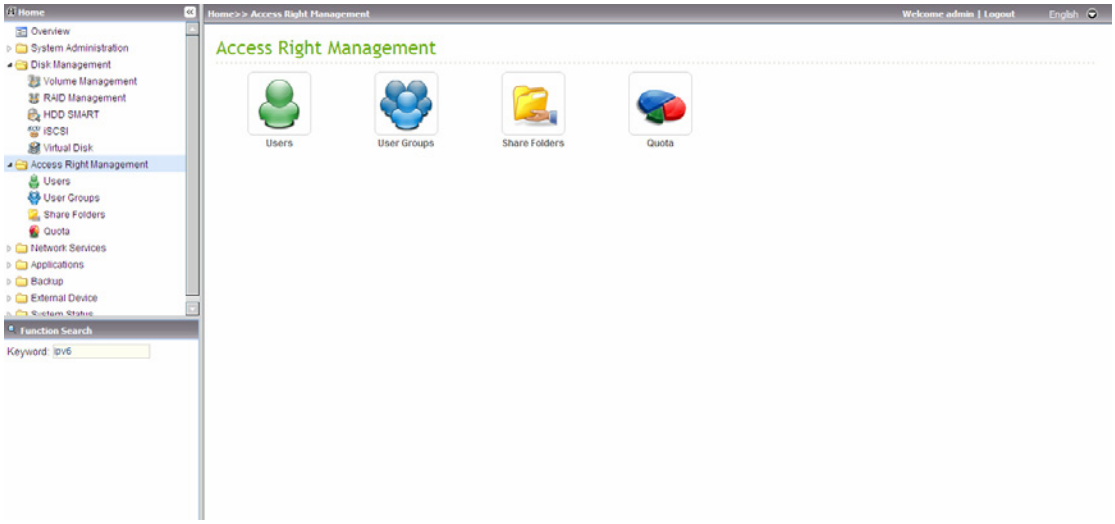
Click  to format the virtual disk.



When the status of the virtual disk is "Ready", you can start to use the virtual disk as a disk volume of the NAS. The NAS supports maximum 8 virtual disks.

3.3 Access Right Management

The files on the NAS can be shared among multiple users. For easier management and better control of users' access right, you have to organize the users, user groups and their access right control.



3.3.1 Users

The system has created the following users by default:

- **admin**
  By default, the administrator "admin" has access right to the system administration and cannot be deleted.
- **guest**
  This is a built-in user and will not be displayed on the "User Management" page. A guest does not belong to any user group. The login password for the guest is "guest".
- **anonymous**
  This is a built-in user and will not be displayed on the "User Management" page. When you connect to the server by the FTP service, you can use this name to login as a guest.

The number of users you can create on the NAS varies according to the NAS models. Please refer to http://www.qnap.com/images/products/comparison/Comparison_NAS.html for further information.

The following information is required to create a new user:

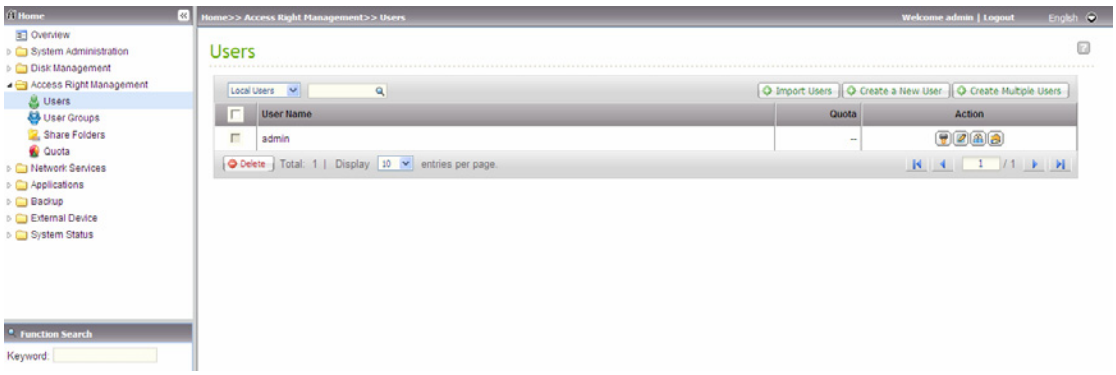
- ✓ **User name**

  The user name must not exceed 32 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean. The invalid characters are listed below:

  " / \ [ ] : ; | = , + * ? < > ` '

- ✓ **Password**

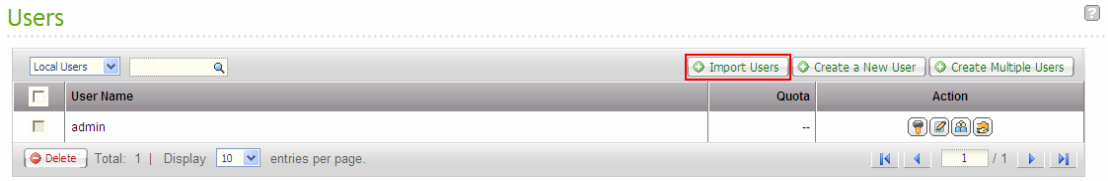
  The password is case-sensitive and can be 16 characters long at maximum. It is recommended to use a password of at least 6 characters.



Import Users

You can import multiple user accounts to the NAS with this feature. To import multiple users, follow the steps below:

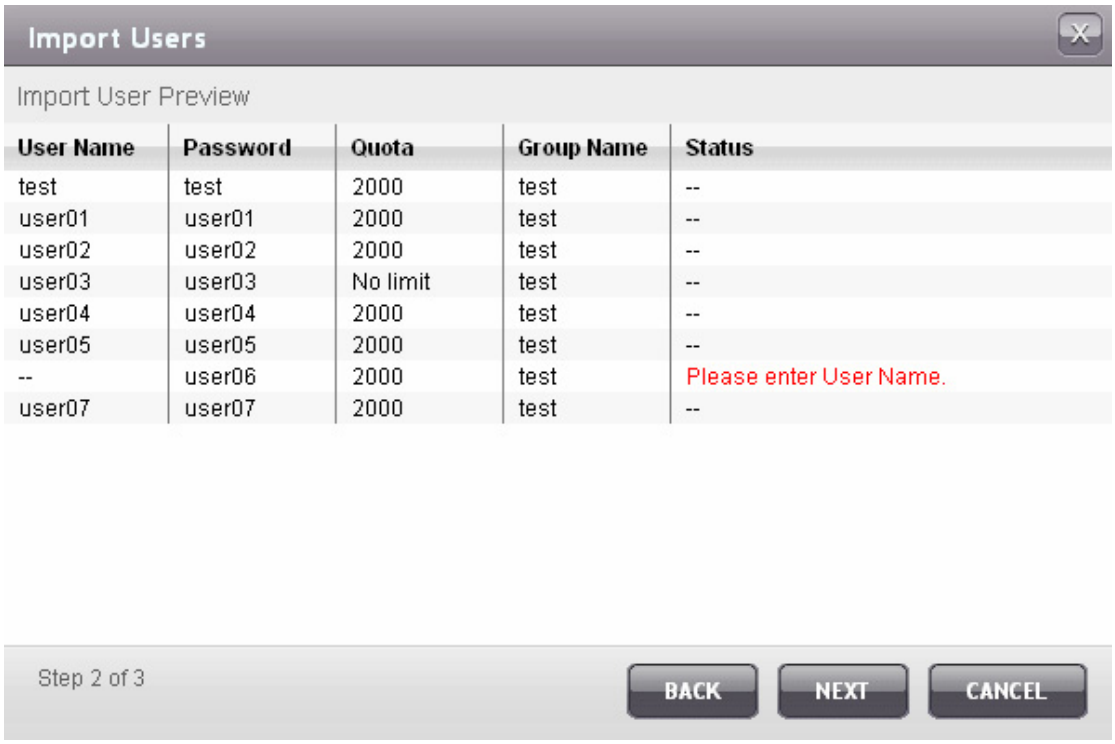
1. Click "Import Users".



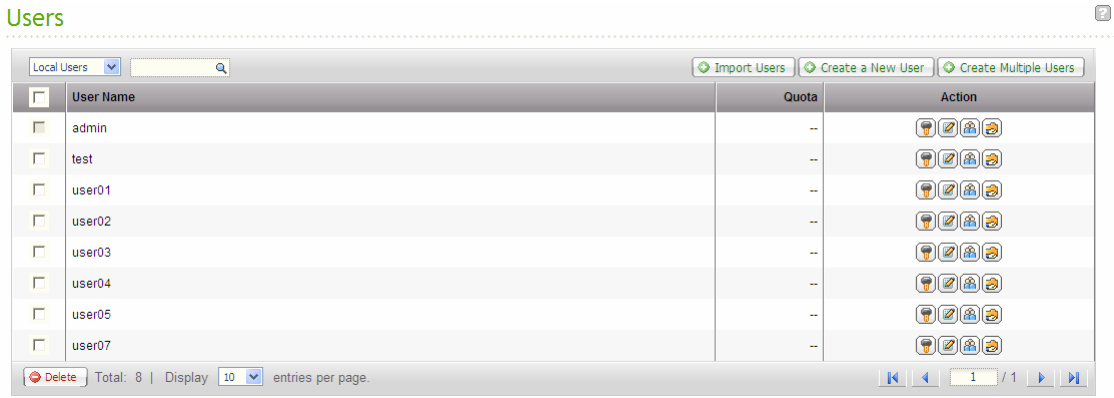
2. Check the option "Overwrite duplicate users" if you want to replace the existing users.

3. Select the file of users and click "Next".

4. A list of imported users will be shown. Abnormal or incorrect entries will be skipped. Click "Next".



5. The imported user accounts will be shown.

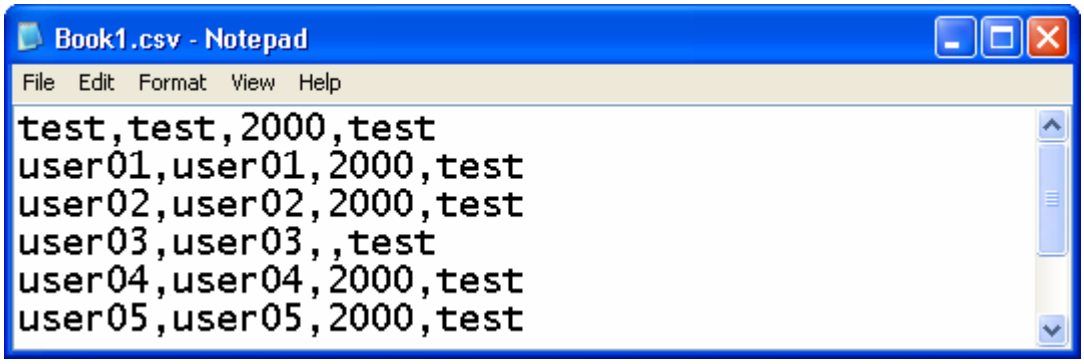


The NAS supports importing user accounts from txt or csv files. To create a list of user accounts with these file types, follow the steps below.

txt

1. Open a new file with a text editor.
2. Enter a user's information in the following order and separate them by ",": Username, Password, Quota (MB), Group Name
3. Go to the next line and repeat the previous step to create another user account. Each line indicates one user's information.
4. Save the file in **UTF-8 encoding** if it contains double-byte characters.

An example is shown as below. Note that if the quota is left empty, the user will have no limit in using the disk space of the NAS.



csv (Excel)

1. Open a new file with Excel.
2. Enter a user's information in the same row in the following order:
   Column A: Username
   Column B: Password
   Column C: Quota(MB)
   Column D: Group name
3. Go to the next row and repeat the previous step to create another user account.
   Each row indicates one user's information. Save the file in csv format.
4. Open the csv file with Notepad and save it in **UTF-8 encoding** if it contains double-byte characters.

An example is shown as below:

	A	B	C	D
1	test	test	2000	test
2	user01	user01	2000	test
3	user02	user02	2000	test
4	user03	user03		test
5	user04	user04	2000	test
6	user05	user05	2000	test

3.3.2 User Groups

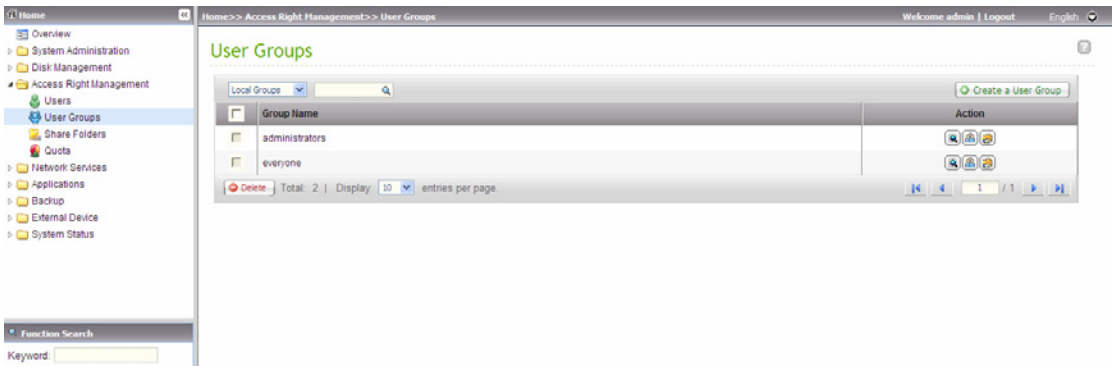
User group is a collection of users with the same access right to files or folders. The NAS has created the following user groups by default:

- **administrators**
  All members in this group have administration right. You cannot delete this group.
- **everyone**
  All registered users belong to everyone group. You cannot delete this group.

The number of user groups you can create on the NAS varies according to the NAS models. Please refer to http://www.qnap.com/images/products/comparison/Comparison_NAS.html for further information.

A group name must not exceed 256 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean, except the following ones:

" / \ [ ] : ; | = , + * ? < > ` '

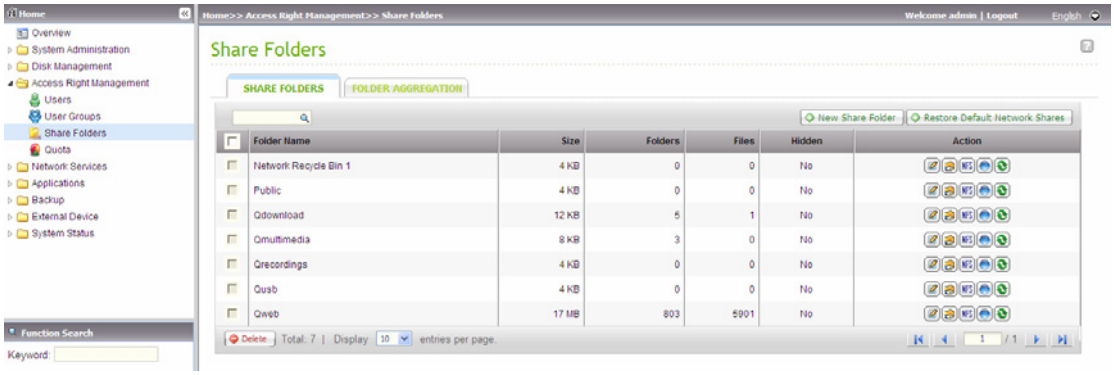


3.3.3 Share Folders

3.3.3.1 Share Folder

You can create different network share folders for various types of files, and provide different file access rights to users or user groups.

The number of share folders you can create on the NAS varies according to the NAS models. Please refer to http://www.qnap.com/images/products/comparison/Comparison_NAS.html for further information.



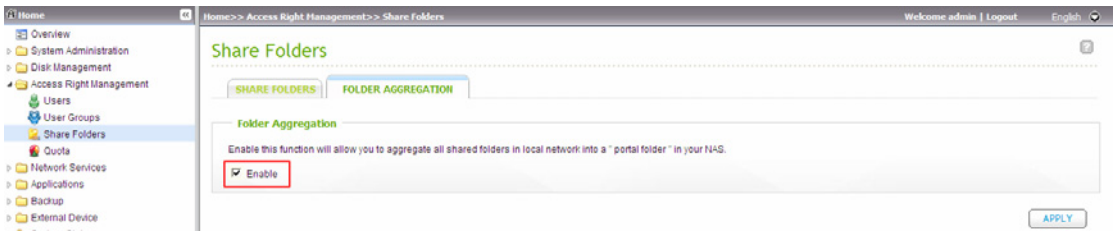
3.3.3.2 Folder Aggregation

You can aggegate the share folders on Microsoft network as a portal folder on the NAS and let the NAS users access the share folders through your NAS. Up to 10 share folders can be linked to a portal folder on the NAS.

Note: This function is supported only in Microsoft networking service.

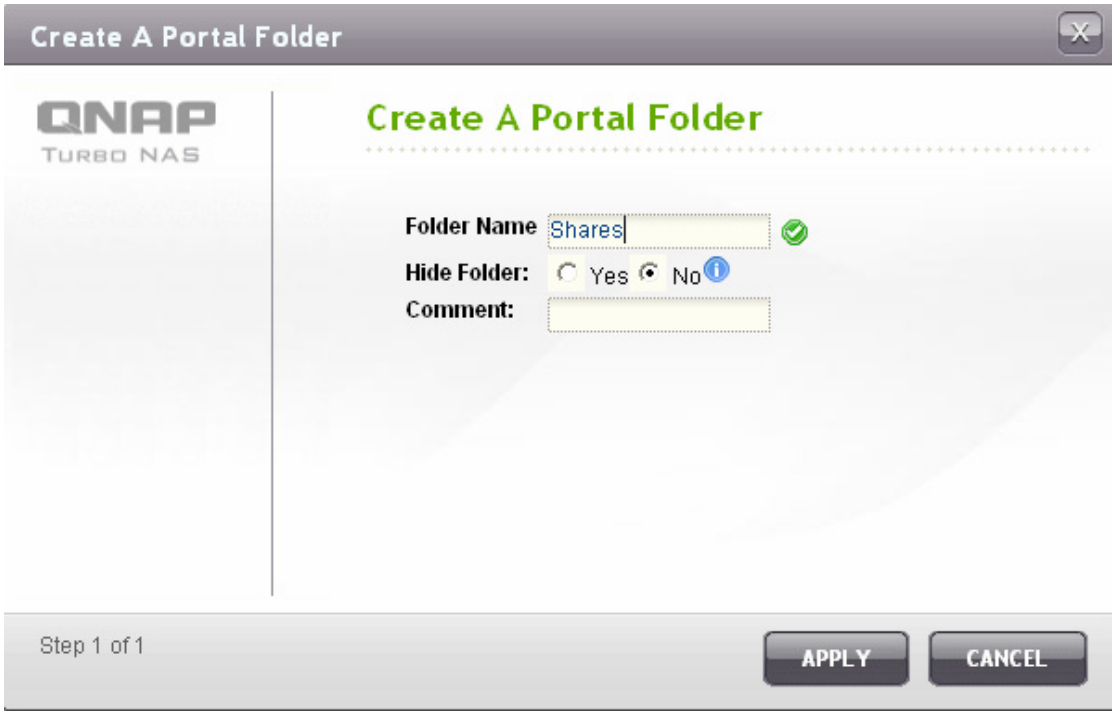
To use this function, follow the steps below.

1. Enable folder aggregation.



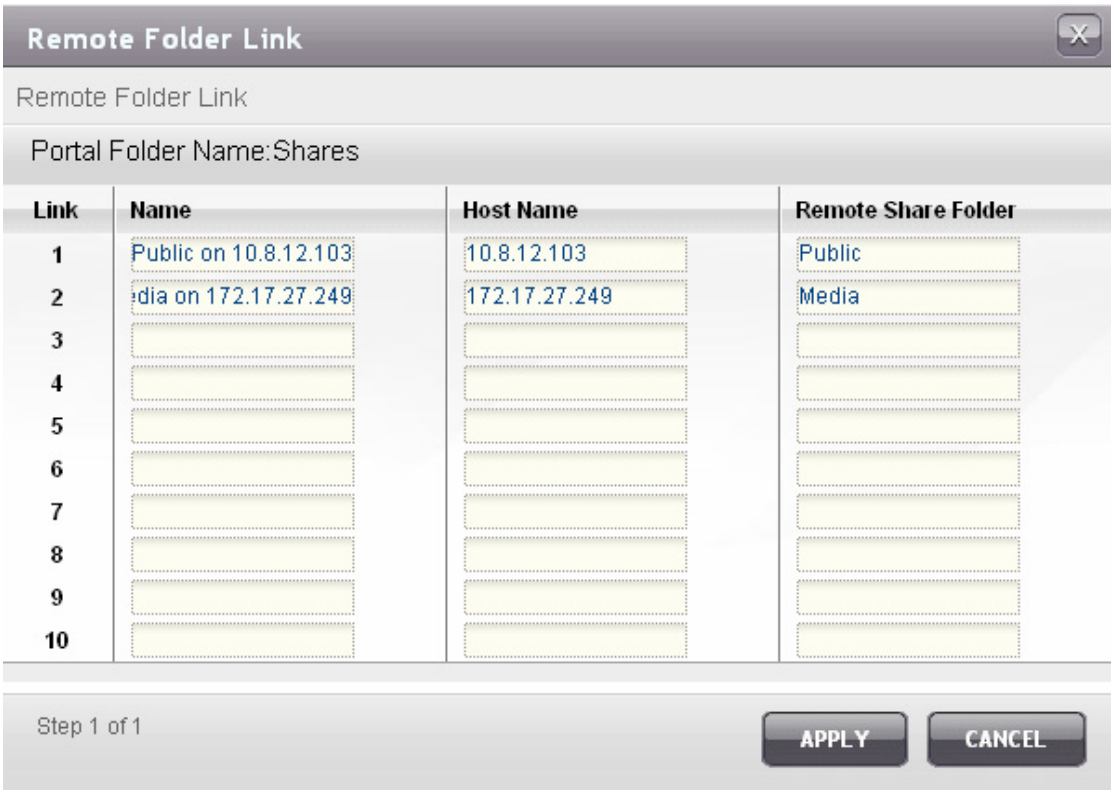
2. Click "Create A Portal Folder".

3. Enter the portal folder name. Select to hide the folder or not, and enter an optional comment for the portal folder.

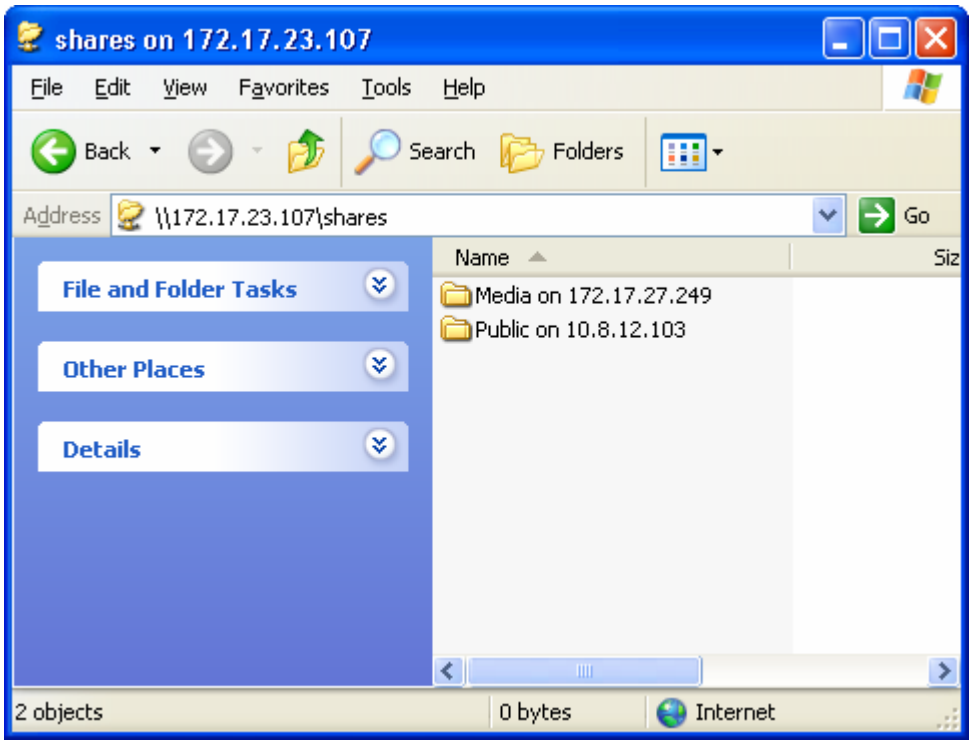


4. Click  and enter the remote folder settings. Make sure the share folders are open for public access.

Note: If there is permission control on the share folders, you need to join the NAS and the remote servers to the same AD domain.



5. Upon successful connection, you can access the remote folders through the NAS.

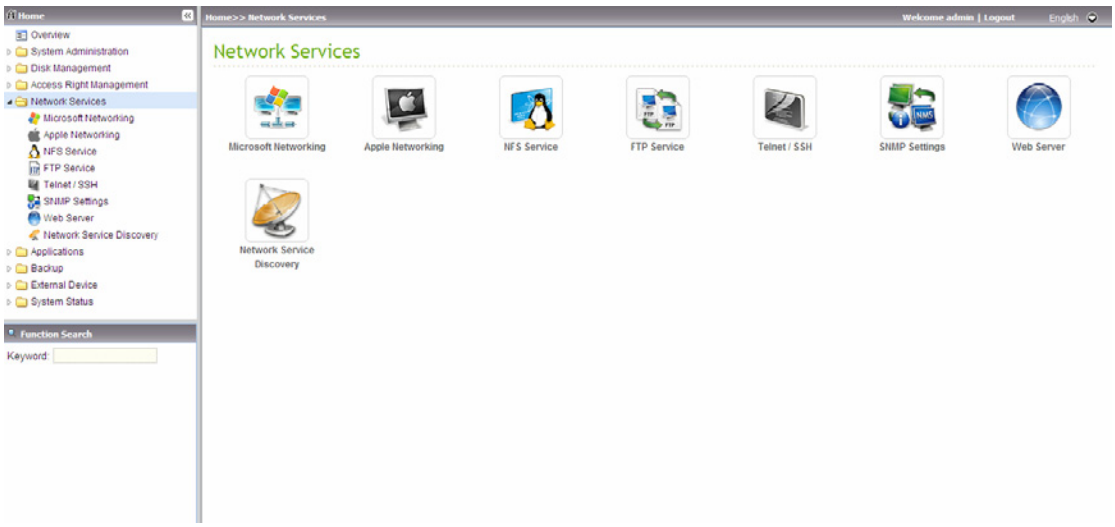


3.3.4 Quota

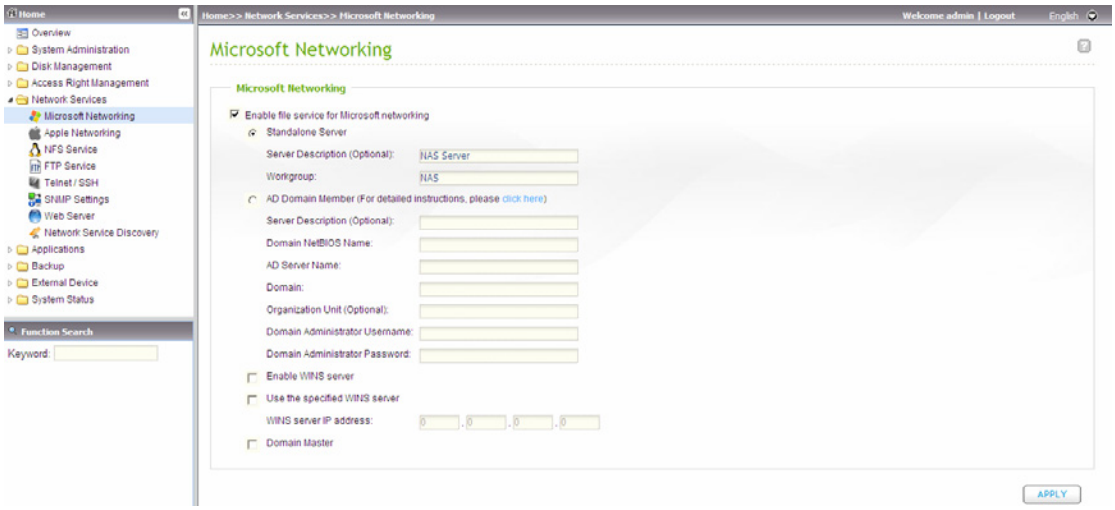
To allocate the disk volume efficiently, you can specify the quota that can be used by each user. When this function is enabled and a user has reached the disk quota, the user cannot upload any data to the server anymore. By default, no limitations are set for the users. You can modify the following two options:

- ✓ Enable quota for all users
- ✓ Quota size on each disk volume

3.4 Network Services



3.4.1 Microsoft Networking



Enable file service for Microsoft networking: If you are using Microsoft® Windows®, enable this service to access the files on the network share folders. Assign a workgroup name.

✓ **Standalone Server**

Use local users for user authentication.

✓ **AD Domain Member**

The NAS supports Windows 2003 AD (Active Directory) to provide quick and direct import of the user accounts to the existing AD server available in your

network. This function helps you to save the time and effort on creating the user accounts and passwords and lowers the IT maintenance cost by automatic configuration procedure.

- Server Description
  Describe the NAS for the users to identify the server. To use the NAS on the Microsoft Windows OS, you must enable Microsoft Network Services.
- Workgroup
  Specify the workgroup the NAS belongs to. The workgroup is a computer group unit in Microsoft Windows network for network sharing.
- AD Server Name
  Enter the name of the AD server when AD domain is selected for authentication.
- Domain Name
  The name of Microsoft domain. When you select AD domain, you must enter the domain name, the login user name, and the password.

✓ **WINS server**

If the local network has a WINS server installed, specify the IP address. The NAS will automatically register its name and IP address with WINS service. If you have a WINS server in your network and want to use this server, enter the WINS server IP.

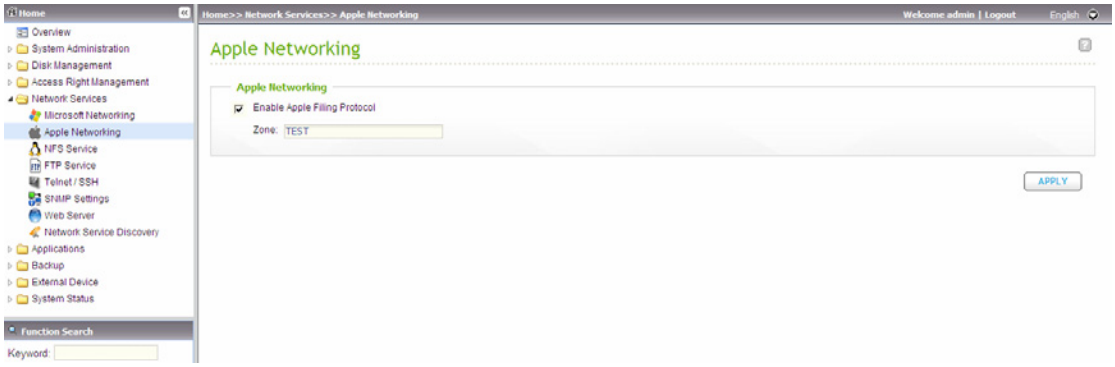
✓ **Domain Master**

There is a unique Domain Master Browser for collecting and recording resources and services available for each PC in the network or workgroup of Windows. When you find the waiting time for accessing Network Neighborhood too long, it may be caused by failure of an existing master browser, or there is no master browser in the network. If there is no master browser on your network, you can check the box Domain Master in this section to configure the NAS as the master browser to enhance the speed of accessing information on Network Neighborhood.

3.4.2 Apple Networking

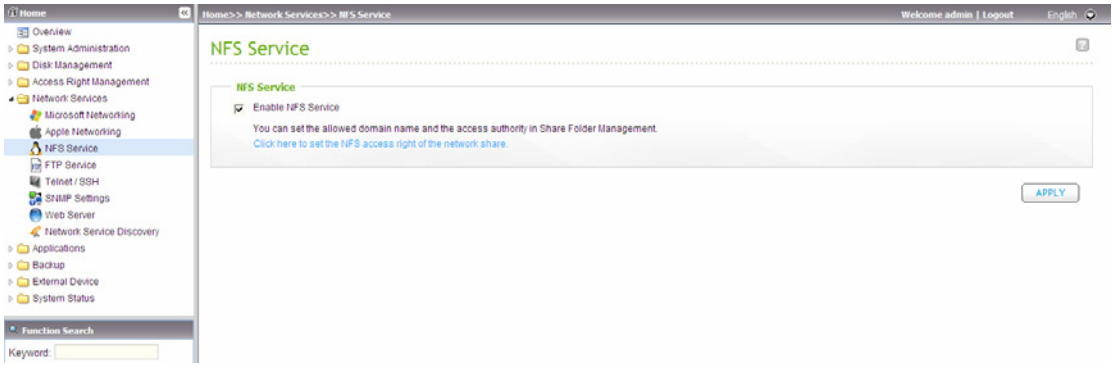
To access the NAS from Mac, enable AppleTalk Apple Filling Protocol network support.

If your AppleTalk network uses extended networks, and is assigned with multiple zones, assign a zone name to the NAS. If you do not want to assign a network zone, enter an asterisk (*) to use the default setting. This setting is disabled by default.



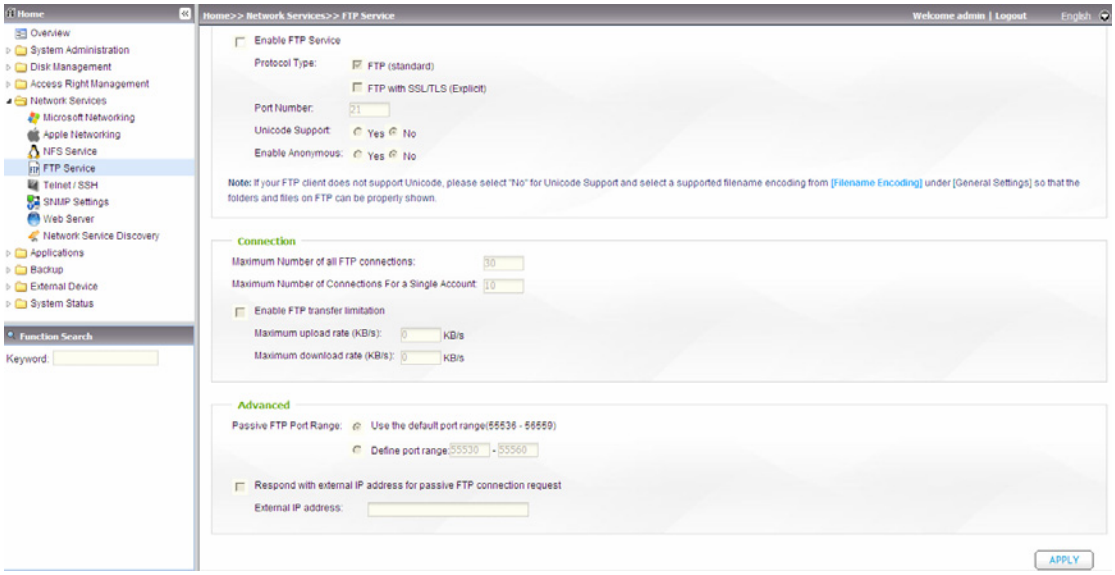
3.4.3 NFS Service

To access the NAS from Linux, enable the NFS service. For the information of connecting to the NAS via NFS on Linux, please refer to Chapter 9.



3.4.4 FTP Service

When you enable the FTP service, you can define the port number for the service and maximum number of users connected to the FTP at the same time.



To use the FTP service of the NAS, enable this function. Open an IE browser and enter ftp://[NAS IP]. Enter the user name and password to login the FTP service.

✓ **Select Protocol Type**

Select to use standard FTP connection or SSL/TLS encrypted FTP. Select the corresponding protocol type in your client FTP software to ensure successful connection.

"SFTP" requires SSH to be enabled. Only the "admin" user account can access via SFTP.

✓ **Unicode Support**

Select to enable or disable Unicode Support. The default setting is No. Since most FTP clients do not support Unicode currently, it is recommended that you disable Unicode support here and select the language the same as your OS in "General Settings" > "Language" page so that the folders and files on FTP can be properly shown. If your FTP client supports Unicode, make sure you have enabled Unicode support for both your client and the NAS.

✓ **Anonymous Login**

You can enable anonymous login to allow users to access the FTP server of the NAS anonymously. The users can access the folders and files which are

opened for public access. If this option is disabled, the users must enter an authorized user name and password to access the server.

- ✓ **Passive FTP Port Range**

  You can use the default port range (55536-56559) or define a port range larger than 1023. When using this function, please make sure you have opened the configured port range on your router or firewall.

- ✓ **FTP Transfer Limitation**

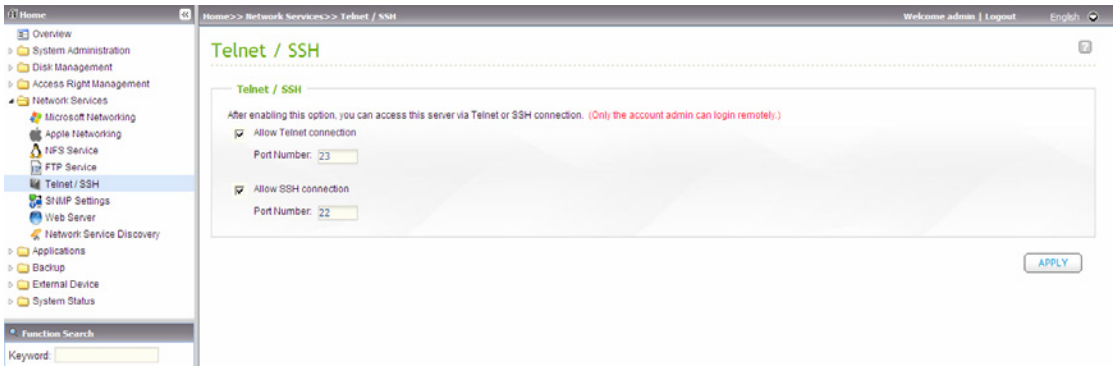
  You can configure the maximum number of FTP connections, maximum connections of a single account and the maximum upload/ download rates of a single connection.

- ✓ **Respond with external IP address for passive FTP connection request**

  When passive FTP connection is in use, the FTP server is configured under a router, and the remote computer cannot connect to the FTP server over the WAN, you can enable this function. By enabling this function, the FTP service replies the manually specified IP address or automatically detects the external IP address so that the remote computer can connect to the FTP server.

3.4.5 Telnet/SSH

After enabling this option, you can access this server via Telnet or SSH encrypted connection (only the account “admin” can login remotely). You can use certain Telnet or SSH connection clients for connection, e.g. putty. Please make sure you have opened the configured ports on your router or firewall when using this function.

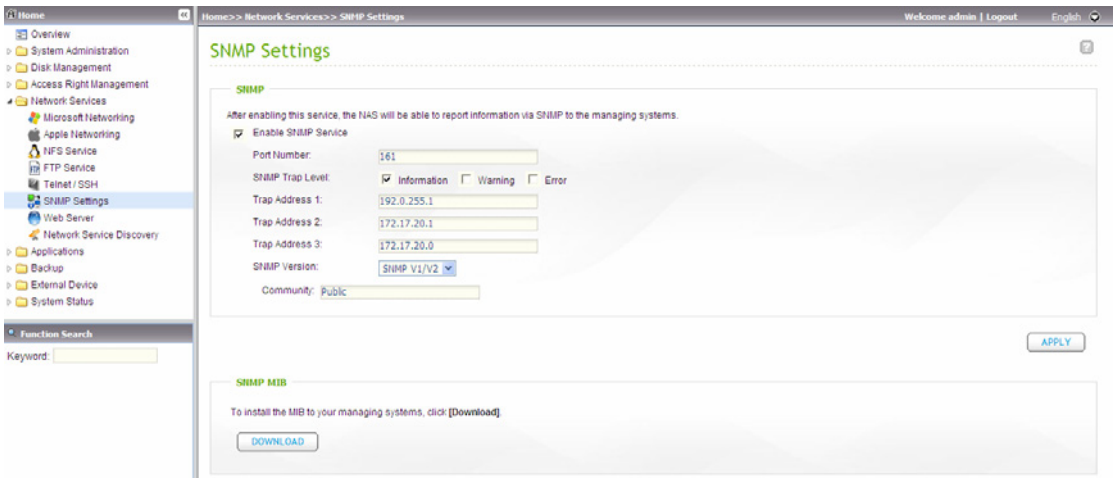


3.4.6 SNMP Settings

You can enable SNMP (Simple Network Management Protocol) service on the NAS and enter the trap address of the SNMP management stations (SNMP manager), e.g. PC with SNMP software installed. When an event, warning, or error occurs on the NAS, the NAS (as an SNMP agent) reports the real-time alert to the SNMP management stations.

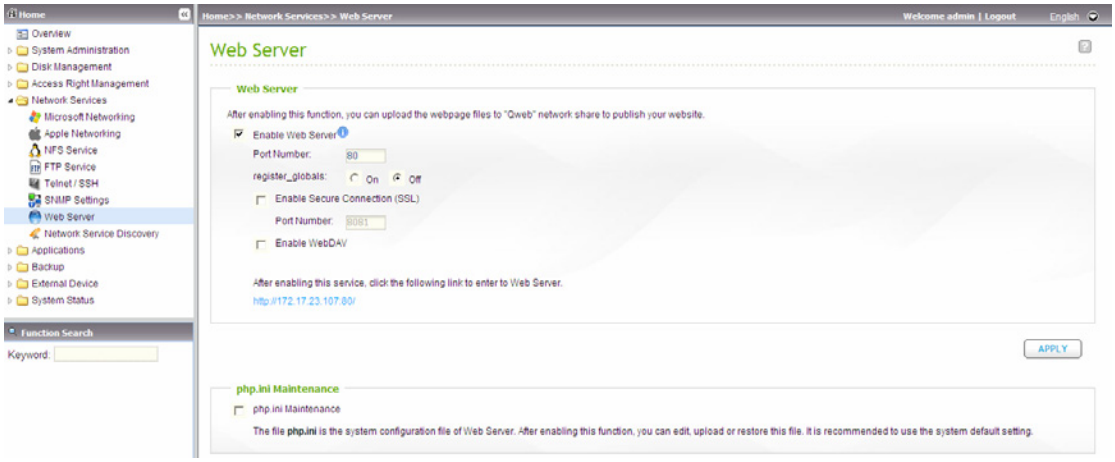
The fields are described as below:

Field	Description
SNMP Trap Level	Select the kind of information to be sent to the SNMP management stations.
Trap Address	The IP address of the SNMP manager. You can enter up to 3 trap addresses.
SNMP MIB (Management Information Base)	The MIB is a type of database in ASCII text format used to manage the NAS in the SNMP network. The SNMP manager uses the MIB to determine the values or understand the messages sent from the agent (NAS) within the network. You can download the MIB and view it with any word processor or text editor.
Community (SNMP V1/V2)	An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the NAS. The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
SNMP V3	The NAS supports SNMP version 3. You can enter the authentication and privacy settings if available.


Home
Overview
System Administration
Disk Management
Access Right Management
Network Services
Microsoft Networking
Apple Networking
NFS Service
FTP Service
Telnet / SSH
SNMP Settings
Web Server
Network Service Discovery
Applications
Backup
External Device
System Status
Function Search
Keyword:
Home>> Network Services>> SNMP Settings
Welcome admin | Logout
English
SNMP Settings
SNMP
After enabling this service, the NAS will be able to report information via SNMP to the managing systems.
Enable SNMP Service
Port Number: 161
SNMP Trap Level: Information Warning Error
Trap Address 1: 192.0.255.1
Trap Address 2: 172.17.20.1
Trap Address 3: 172.17.20.0
SNMP Version: SNMP V1/V2
Community: Public
APPLY
SNMP MIB
To install the MIB to your managing systems, click [Download]
DOWNLOAD

3.4.7 Web Server

The NAS enables you to upload web pages and manage your own website easily by Web Server. It also supports PHP and MySQL/ SQLite for you to establish an interactive website.



To use Web Server, follow the steps below.

1. Enable the service and enter the port number. The default number is 80.

2. Configure other settings:

- **Configure register_globals**

  Select to enable or disable register_globals. The setting is disabled by default. When the web program asks to enable php register_globals, please enable this option. However, for system security concerns, it is recommended to disable this option.

- **php.ini Maintenance**

  Check the box "php.ini Maintenance" to select to upload, edit or restore php.ini.

> **Note:** To use PHP mail() function, you can go to "System Administration" > "Notification" > "Configure SMTP Server" to configure the SMTP server settings.

- **Secure Connection (SSL)**
  Enter the port number for SSL connection.

3. Upload the HTML files to the share folder (Qweb/ Web) on the NAS. The file index.html, index.htm or index.php will be the home path of your web page.

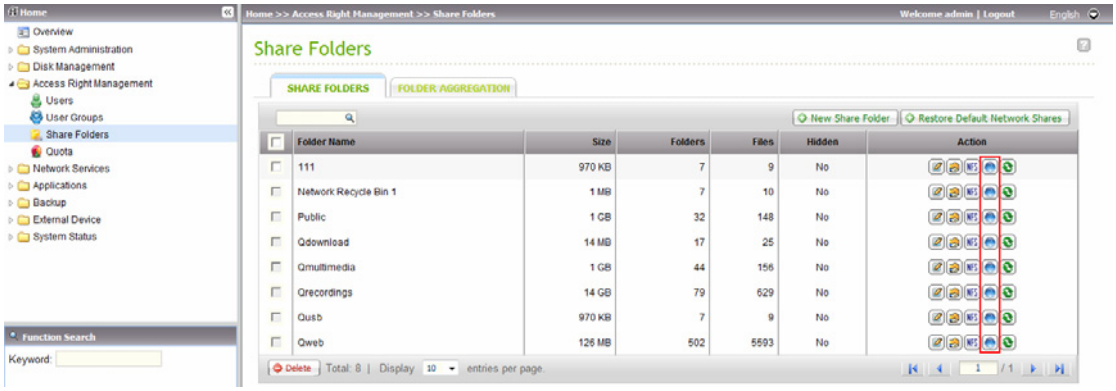
4. You can access the web page you upload by entering http://NAS IP/ in the web browser. Note that when Web Server is enabled, you have to enter http://NAS IP:8080 in your web browser to access the login page of the NAS.

3.4.7.1 WebDAV

WebDAV (Web-based Distributed Authoring and Versioning) is a set of extensions to the HTTP(S) protocol that allows the users to edit and manage files collaboratively on remote World Wide Web servers. After enabling this function, you can map the share folders of your NAS as the network drives of a remote PC over the Internet. To edit the access right settings, please go to "Access Right Management" > "Share Folders" page.

To map a share folder on the NAS as the network drive of your PC, enable WebDAV on the NAS and follow the steps below.

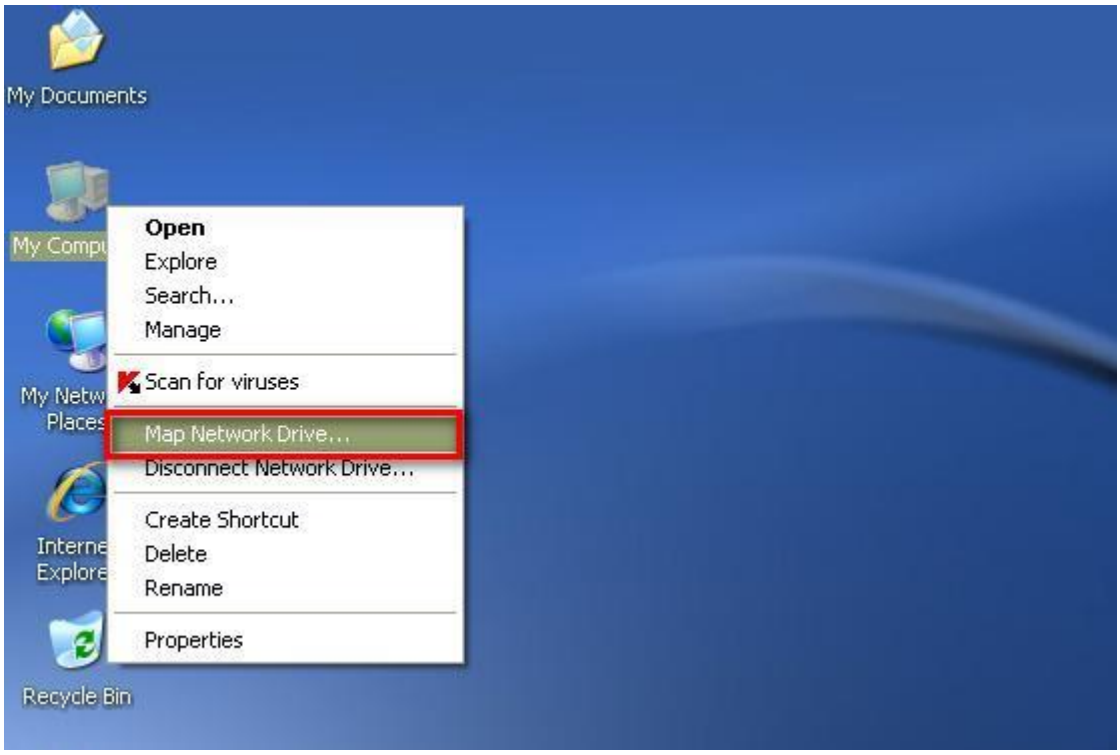
Go to "Access Right Management" > Share Folders" > "Share Folder". Click "WebDAV Access Control" button  in the "Action" column, and set up the WebDAV access right of the users to the share folders.



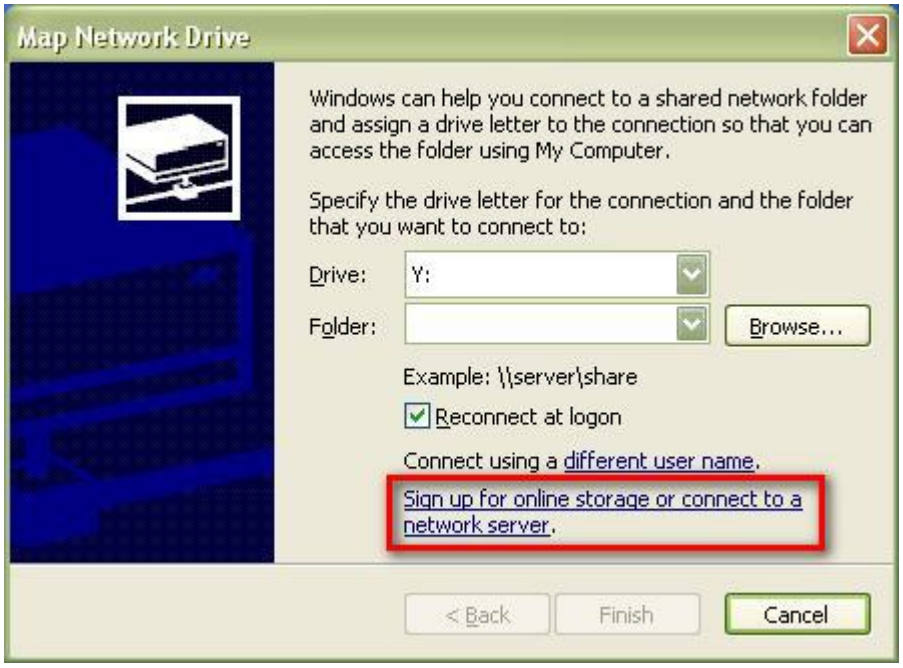
Next, mount the network share folders of the NAS as the network shares on your operating systems by WebDAV.

Windows XP:

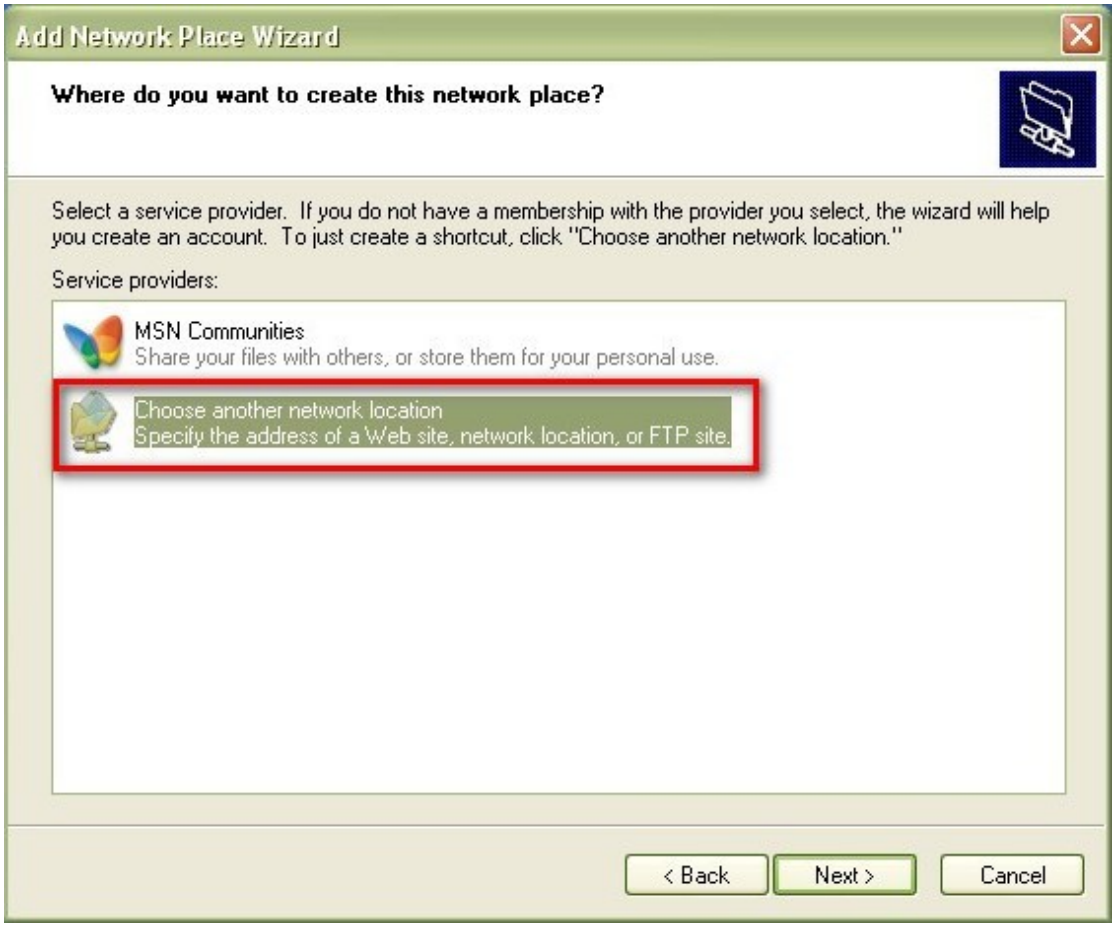
1. Right click "My Computer" and select "Map Network Drive…"



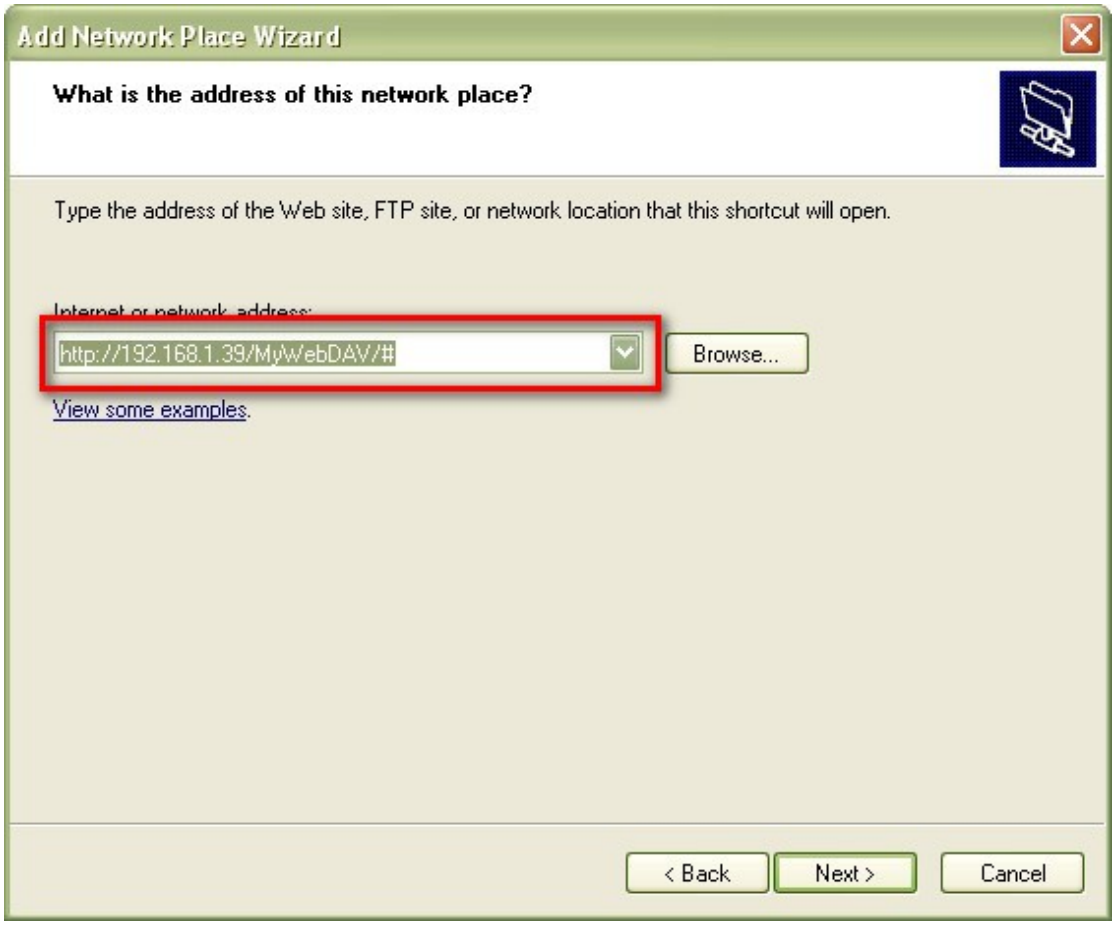
2. Click “Sign up for online storage or connect to a network server”.



3. Select “Choose another network location”.

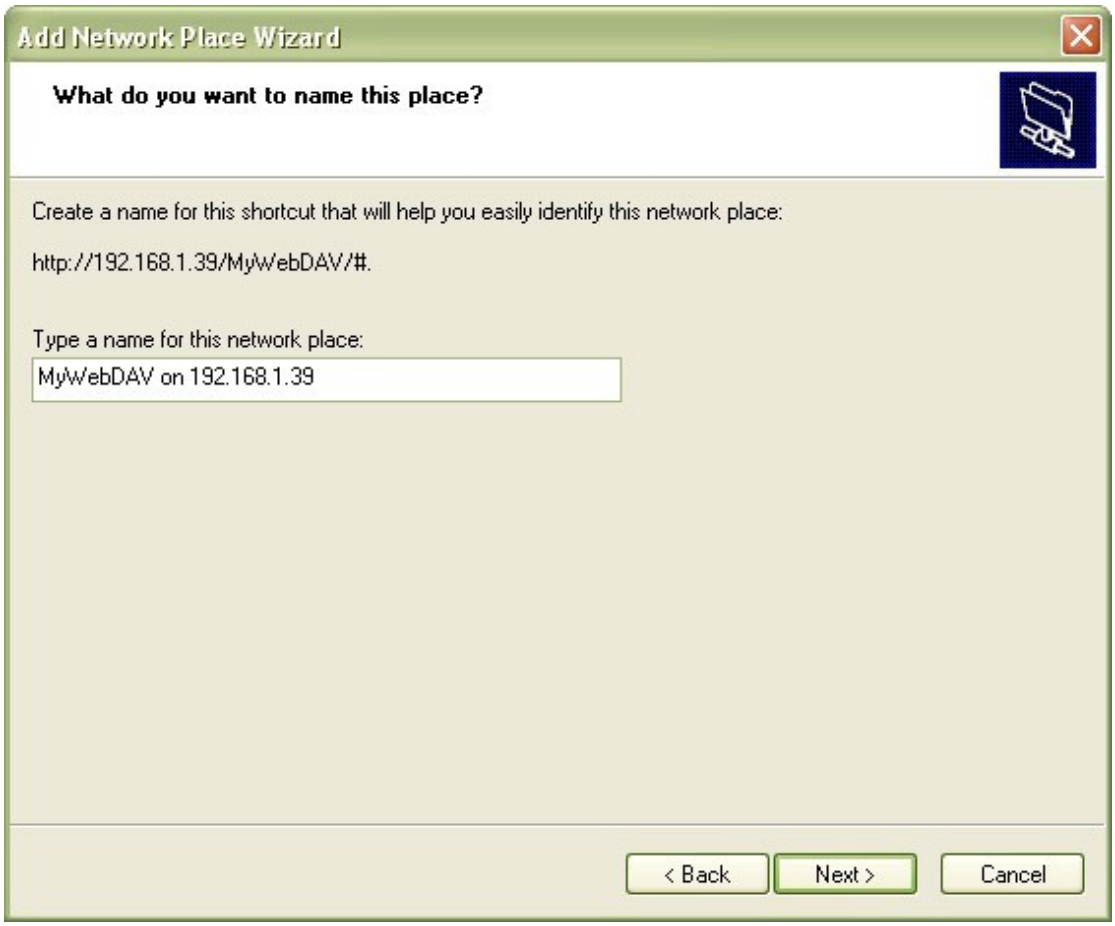


4. Enter the URL of your NAS with the share folder name. Note that you should put the "#" at the end of the URL. Click "Next".
   Format: http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME/#



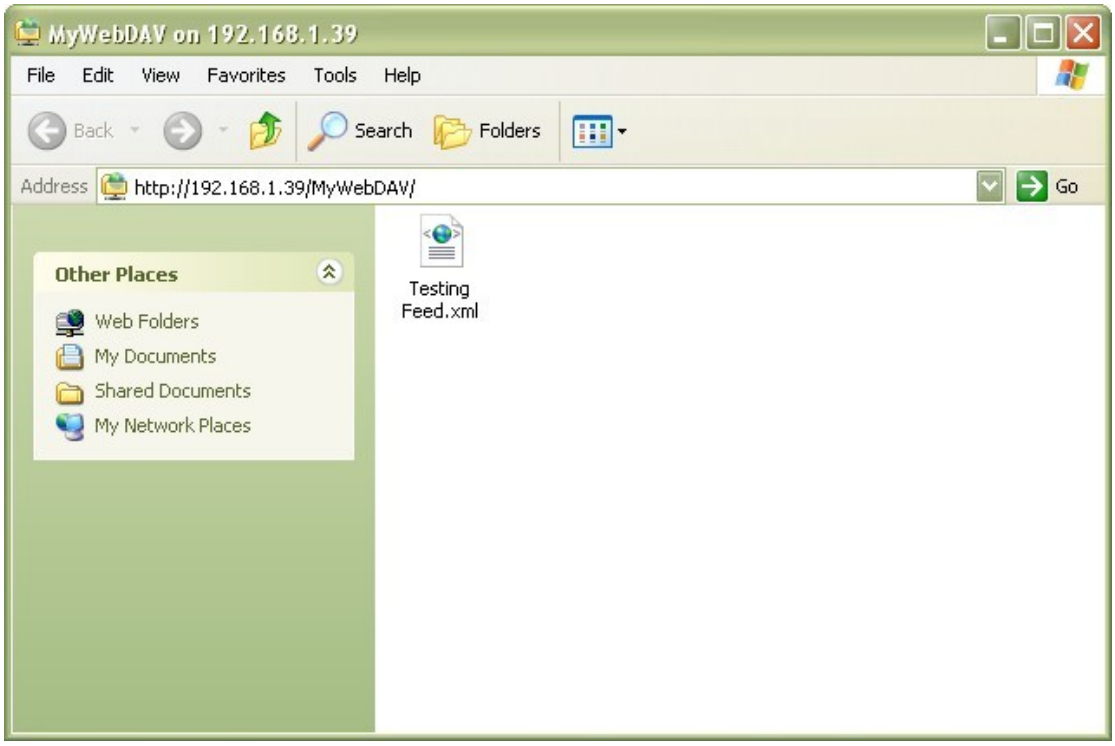
5. Enter the user name and its password which has the WebDAV privilege to access the share folder.

6. Type a name for this network place.



7. The network place has been created and is ready to be used.

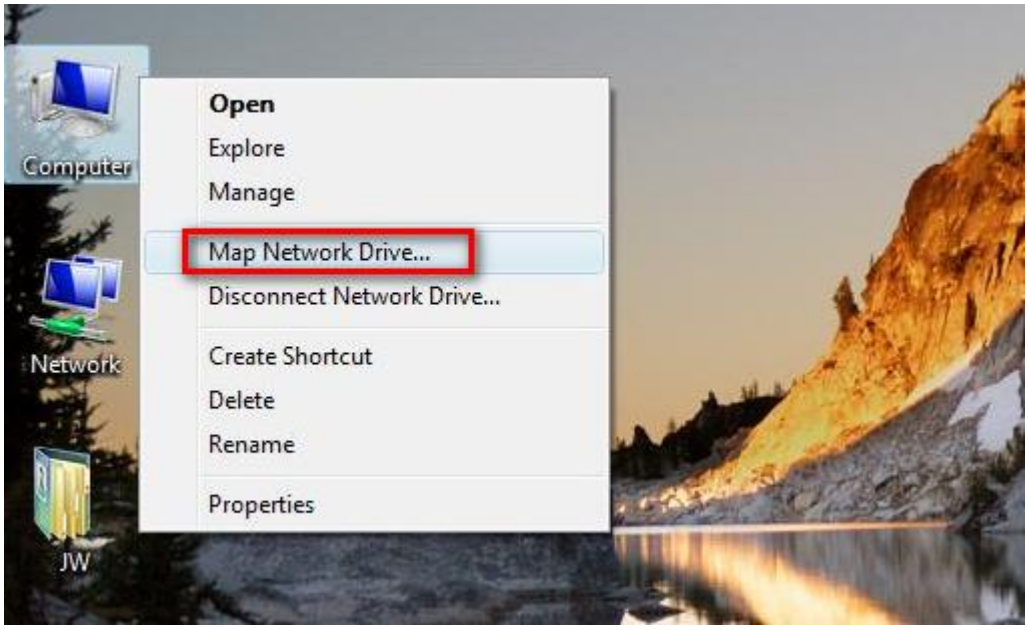
8. Now you can access this share folder anytime through WebDAV. A shortcut has also been created in “My Network Places”.



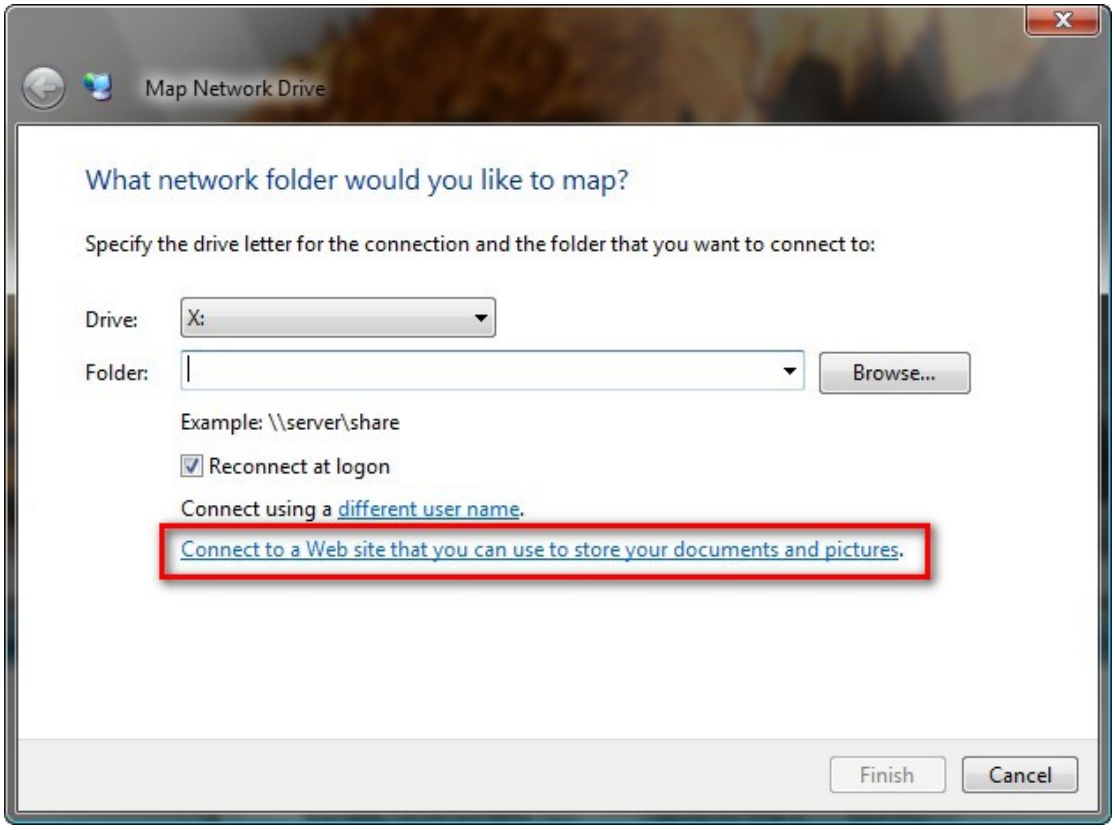
Windows Vista

If you are using Windows Vista, you might need to install the "Software Update for Web Folders (KB907306)" and this update is for 32-bit Windows OS only.
http://www.microsoft.com/downloads/details.aspx?FamilyId=17c36612-632e-4c04-9382-987622ed1d64&displaylang=en

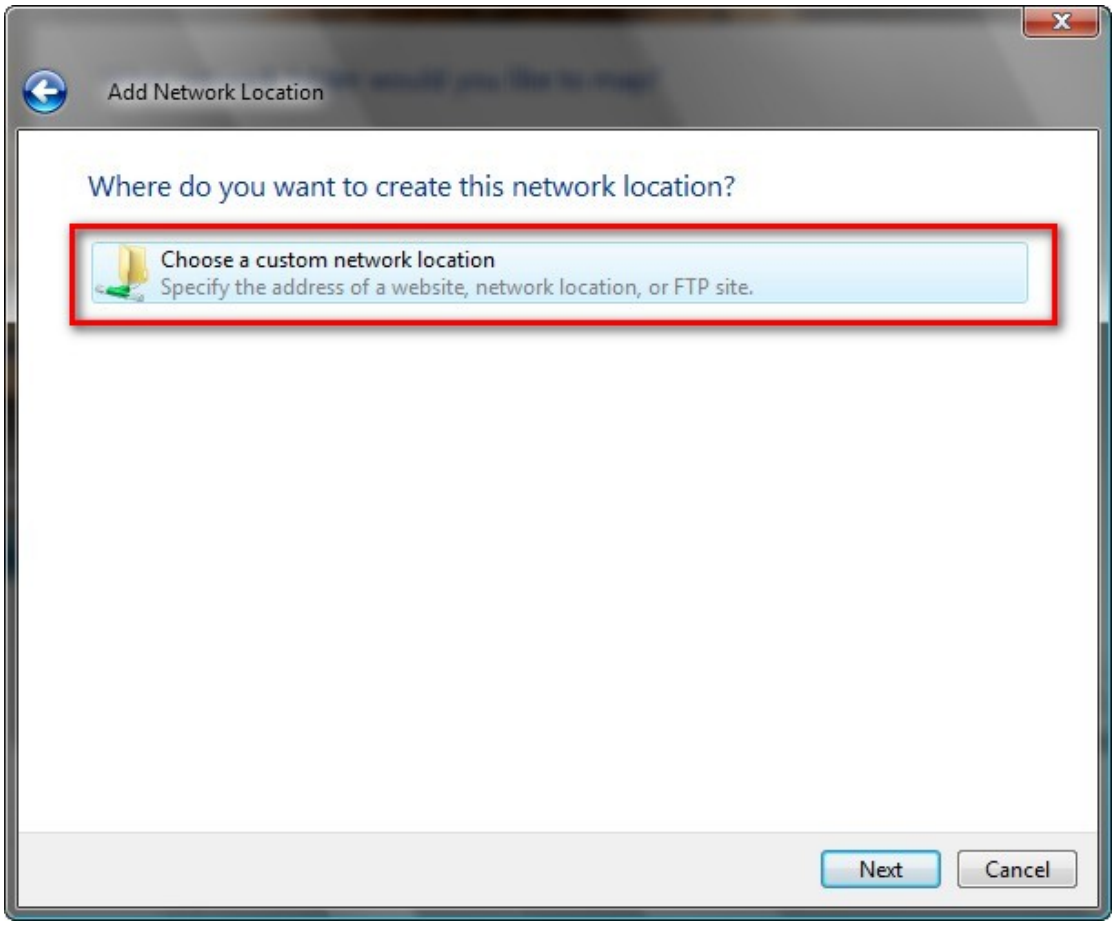
1. Right click “Computer” and select “Map Network Drive…”



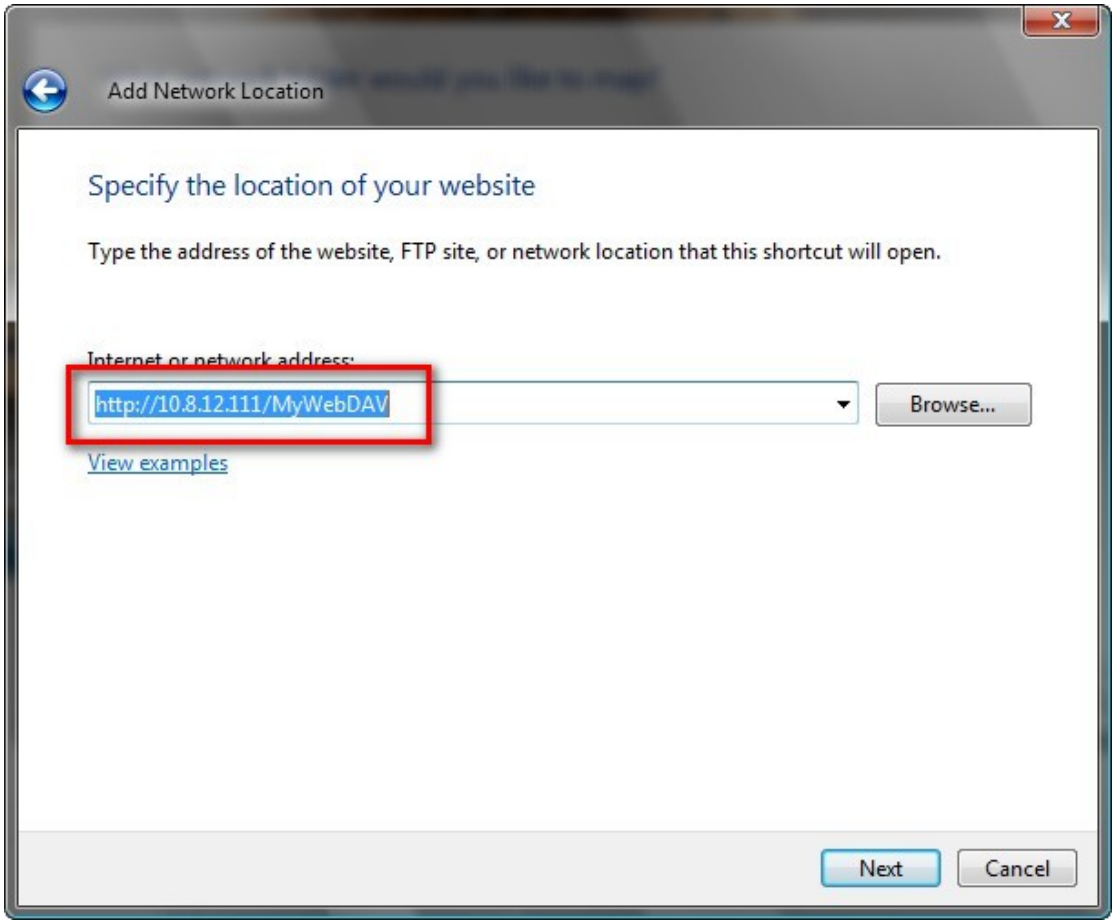
2. Click “Connect to a Web site that you can use to store your documents and pictures”.



3. Select “Choose a custom network location”.

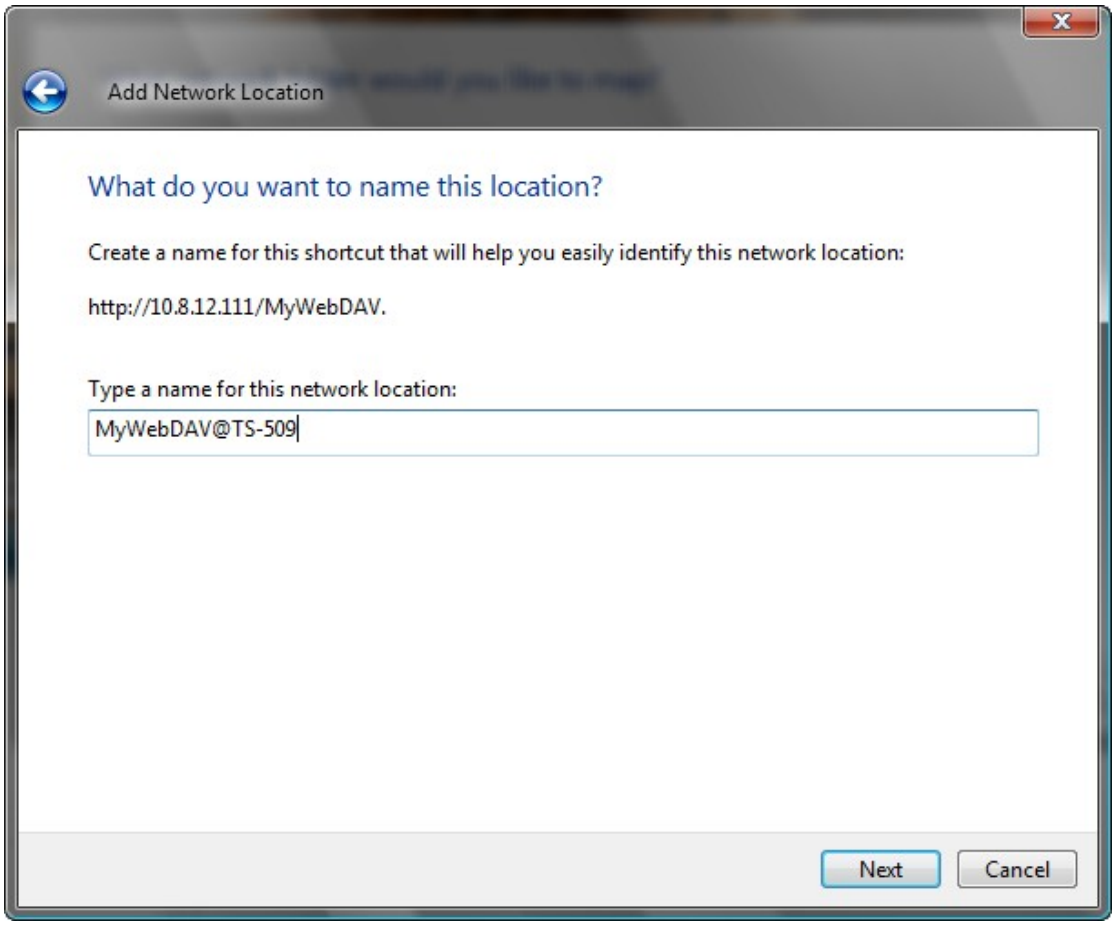


4. Enter the URL of your NAS with the share folder name.
   Format: http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME

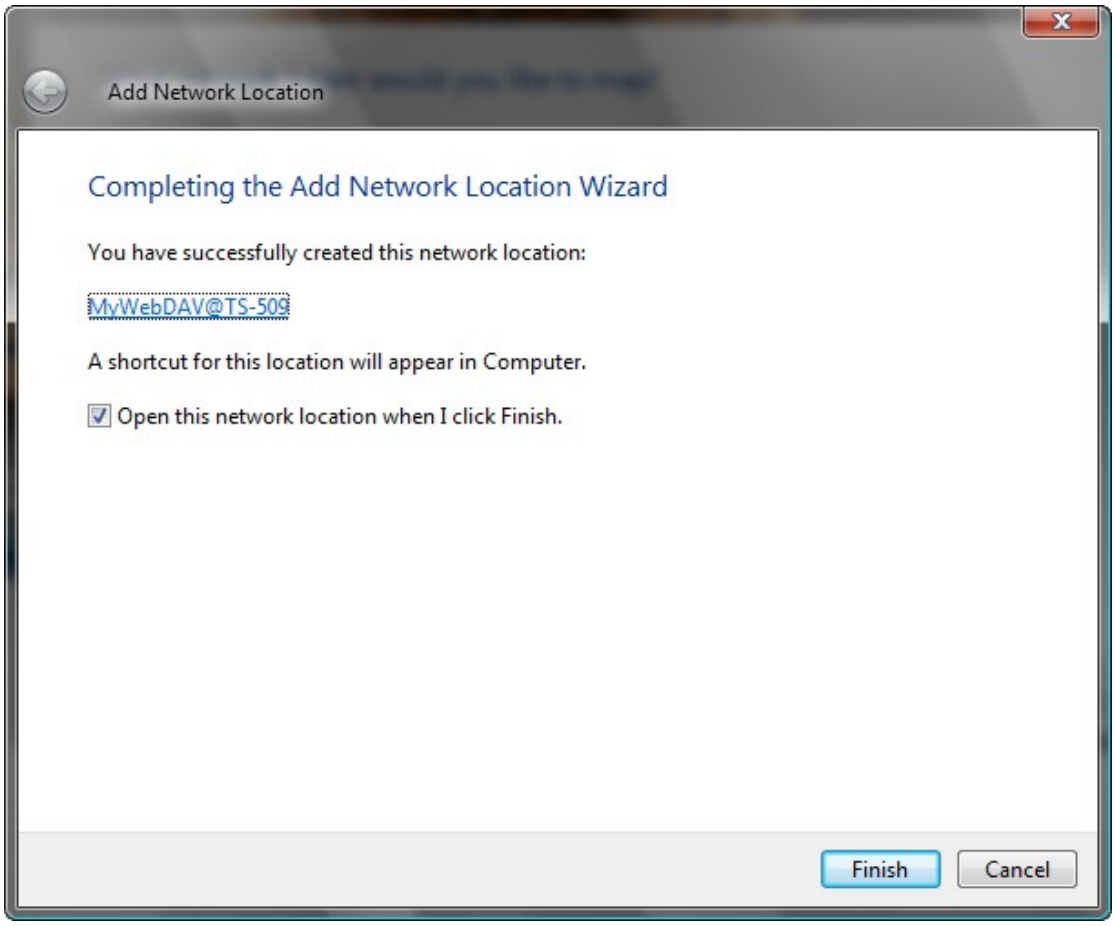


5. Enter the user name and its password which has the WebDAV privilege to access this share folder.

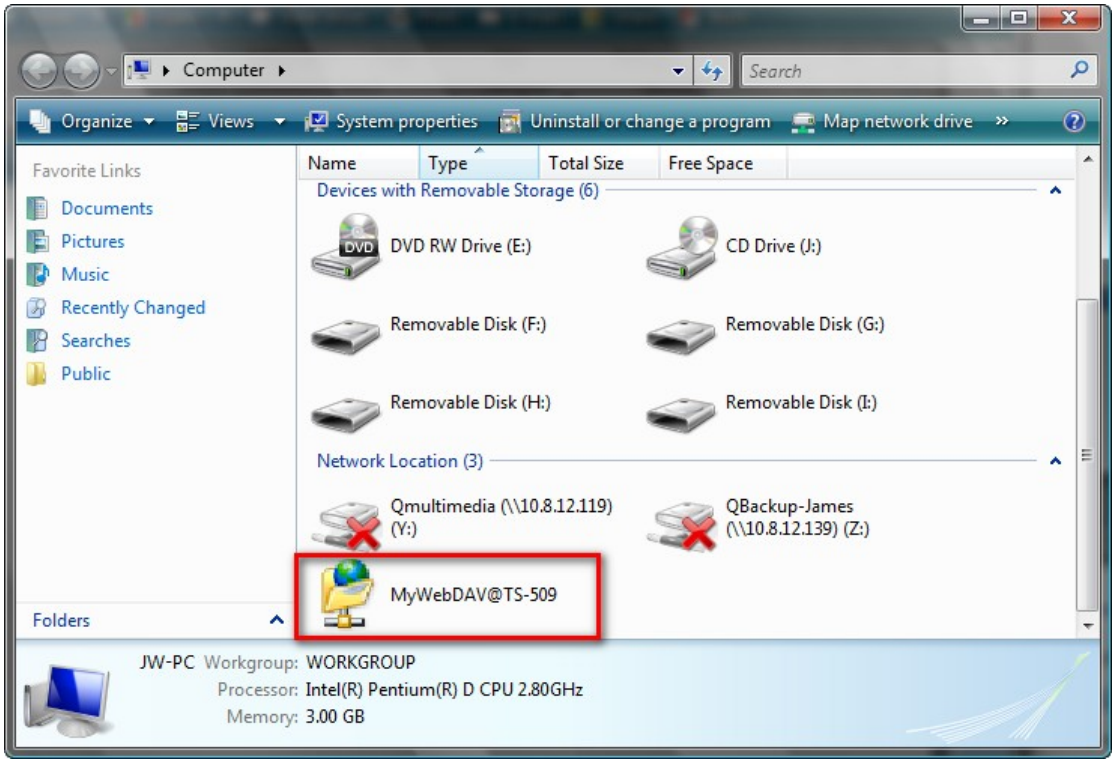
6. Type a name for this network location.



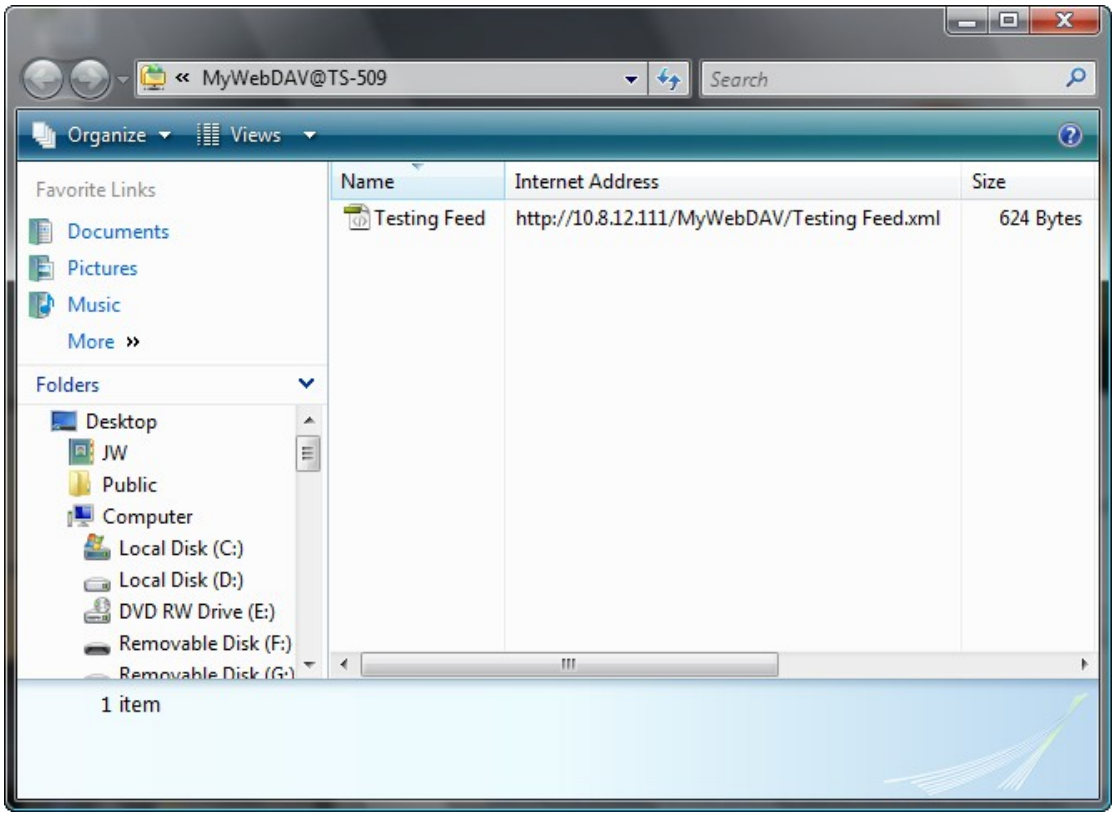
7. The Web folder has been successfully created.



8. You can locate the web folder in the "Network Location" section in "Computer".



9. You can access the share folder though this link via HTTP/WebDAV.



Mac OS X

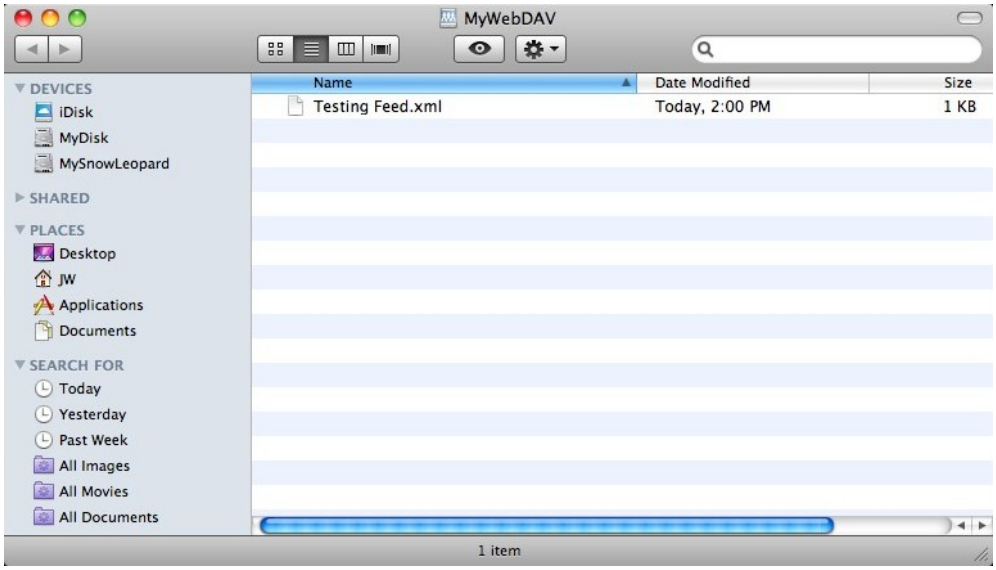
Follow the steps below to connect to your NAS via WebDAV on Mac OS X.

Client Operating System: Mac OS X Snow Leopard (10.6.1)

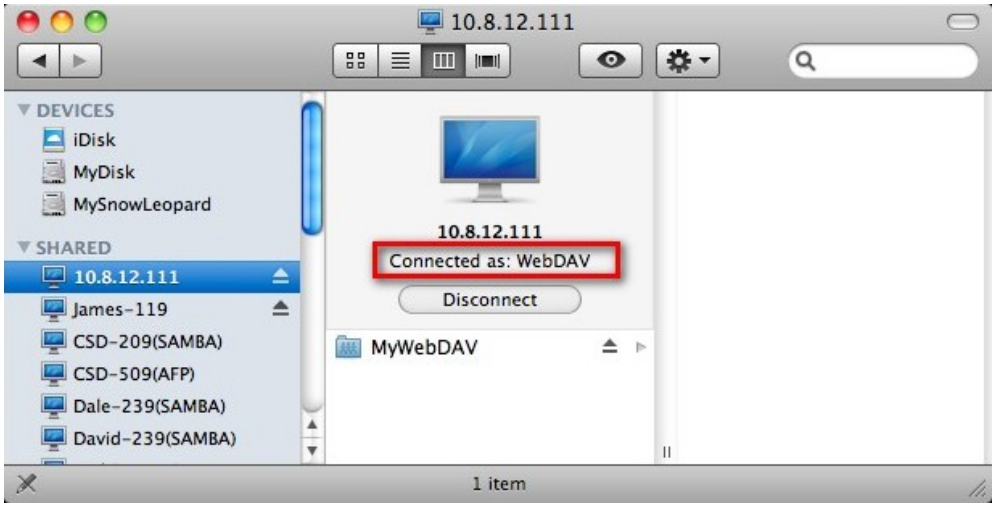
1. Open "Finder" > "Connect to Server", and enter the URL of the share folder.
   Format: http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME

2. Enter the user name and its password which has the WebDAV privilege to access this share folder.

3. You can access the share folder through this link via HTTP/WebDAV.



4. You can also find the mountpoint in the "SHARED" category in Finder and make it as one of the login items.



Please note that the instructions above are based on Mac OS X 10.6, and can be applied to 10.4 or later.

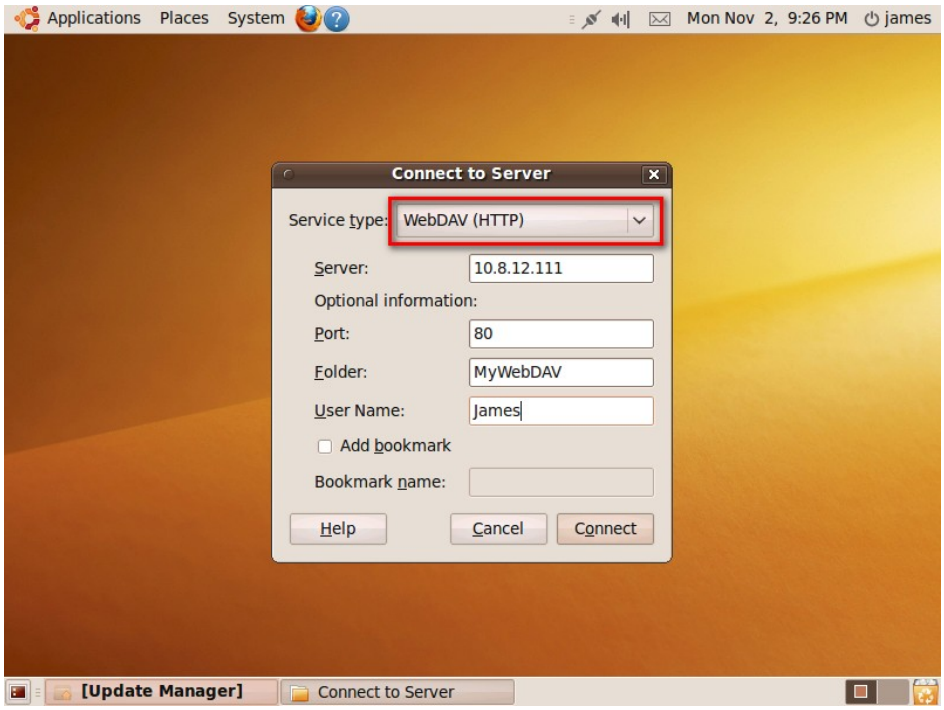
Ubuntu

Follow the steps below to connect to your NAS via WebDAV on Ubuntu.

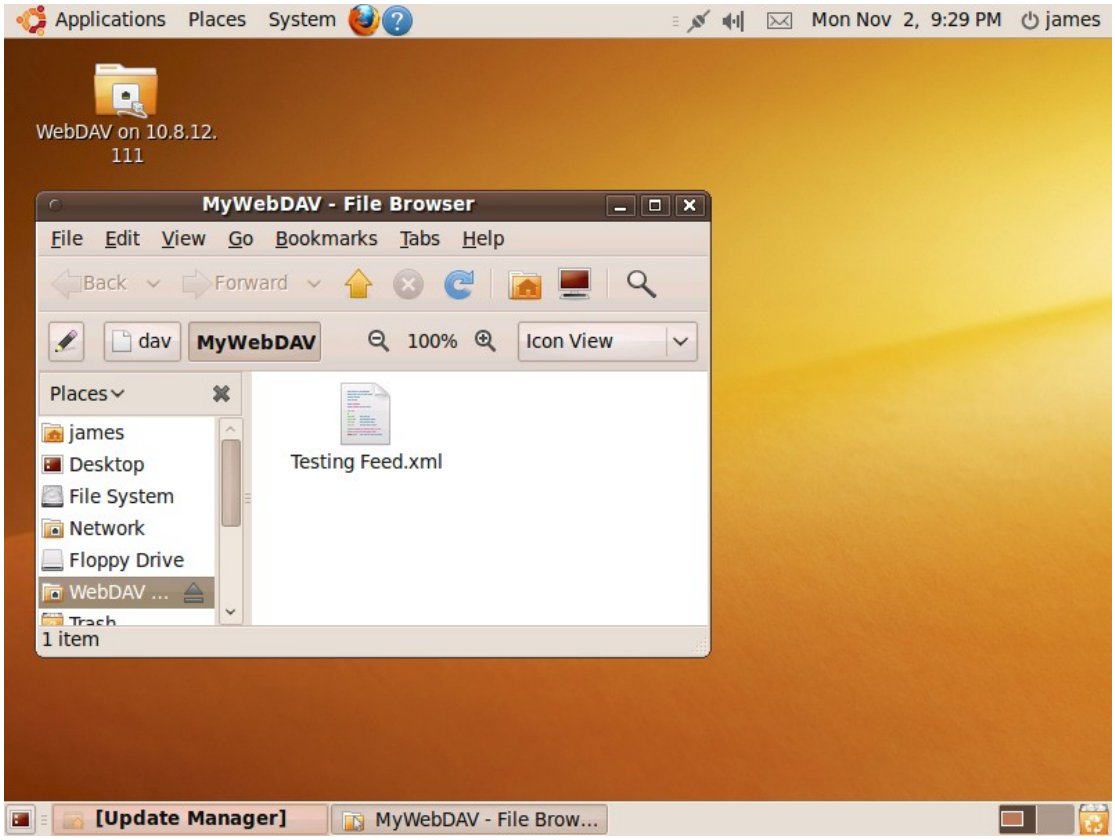
Client Operating System: Ubuntu 9.10 Desktop

1. Open “Places” > “Connect to Server…”

2. Select “WebDAV (HTTP)” or “Secure WebDAV (HTTPS)” for the Service type according to your NAS settings and enter your host information. Enter the user name and the password which has the WebDAV privilege to access this share folder. Click “Connect” to initialize the connection.



3. This WebDAV connection has been established successfully, a linked folder will be created on the desktop automatically.



MySQL Management

You may install the phpMyAdmin software and save the program files in the "Web" share folder of the NAS. You can change the folder name and access the database by entering the URL in the browser.

Note: The default user name of MySQL is "root". The password is "admin". Please change your root password immediately after logging in to the phpMyAdmin management interface.

SQLite Management

SQLiteManager is a multilingual web-based tool to manage SQLite databases and can be downloaded from http://www.sqlitemanager.org/.

Please follow the steps below or refer to the INSTALL file in the downloaded SQLiteManager-*.tar.gz? to install the SQLiteManager.

(1) Unpack your downloaded file SQLiteManager-*.tar.gz.
(2) Upload the unpacked folder **SQLiteManager-*** to **\\NAS IP\Web**.
(3) Open your web browser and go to **http://NAS IP/SQLiteManager-*/**.

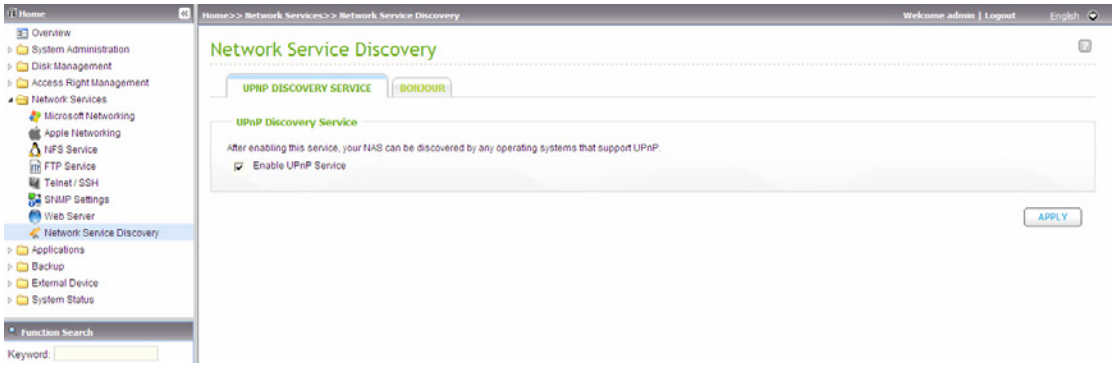
?: The symbol "*" refers to the version number of SQLiteManager.

3.4.8 Network Service Discovery

3.4.8.1 UPnP Discovery Service

When a device is added to the network, the UPnP discovery protocol allows the device to advertise its services to the control points on the network.

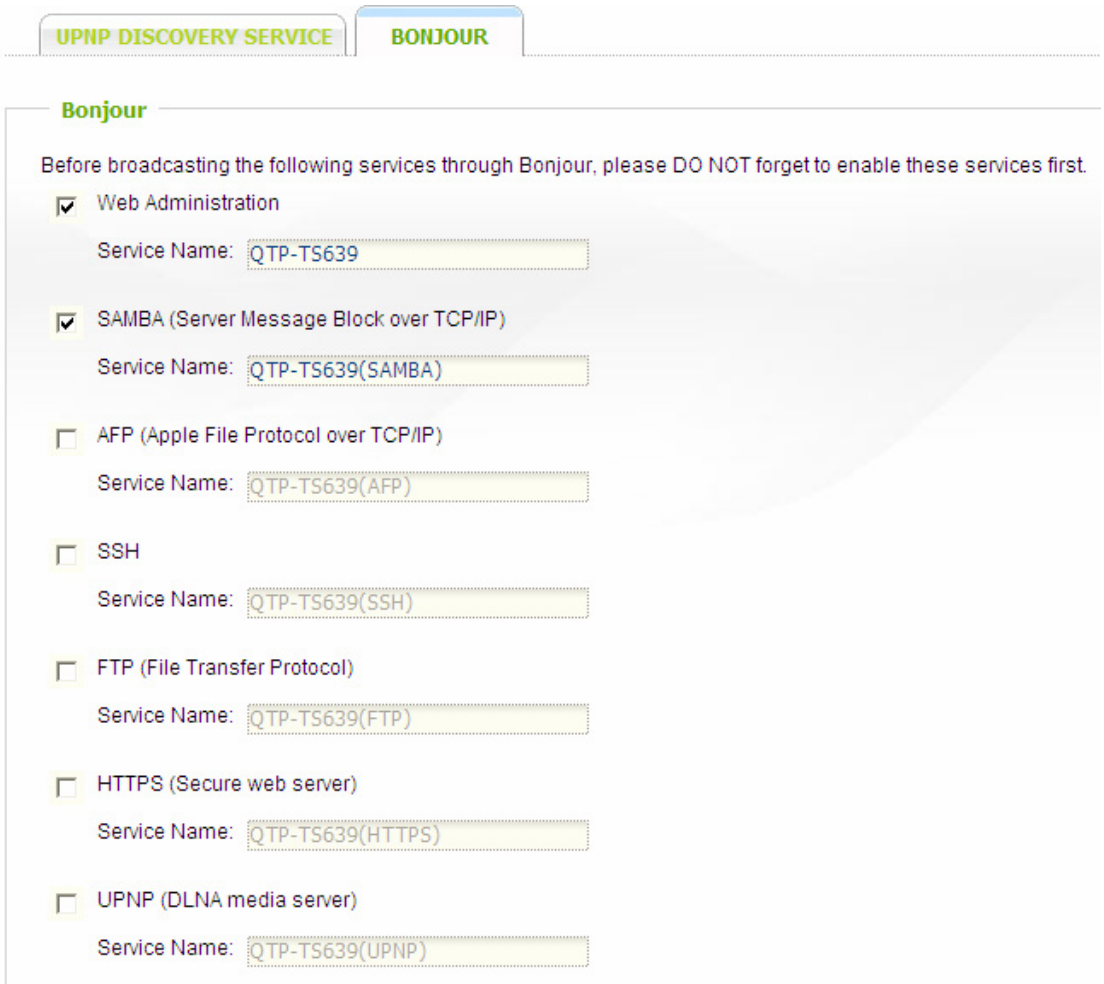
By enabling the UPnP Discovery Service, the NAS can be discovered by any operating systems that support UPnP.



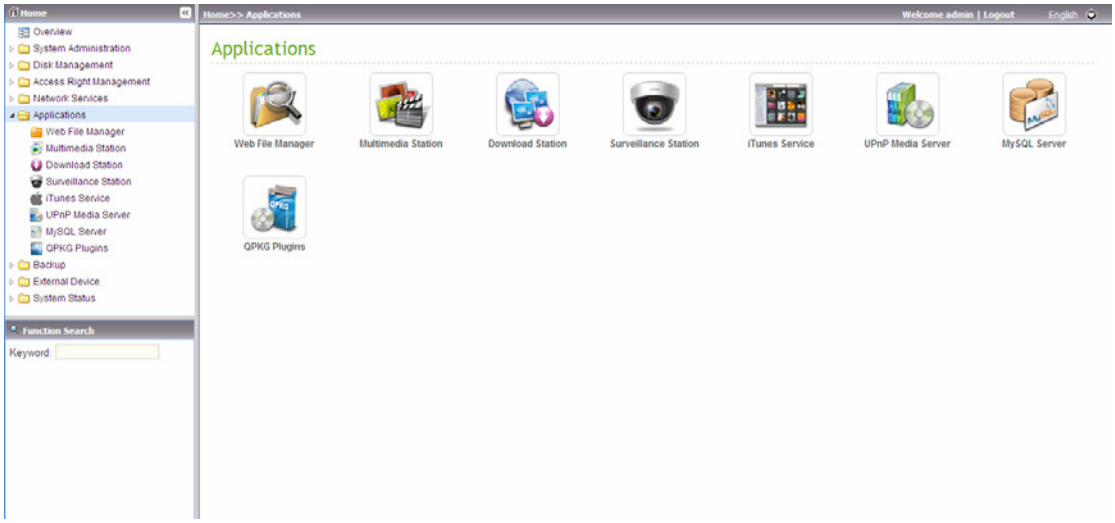
3.4.8.2 Bonjour

By broadcasting the network service(s) with Bonjour, your Mac will automatically discover the network services (e.g. FTP) which are running on the NAS without the need to enter the IP addresses or configure the DNS servers.

Note: You will have to activate each service (e.g. FTP) on its setup page, and then enable the service on the Bonjour page, so that the NAS will advertise this service with Bonjour.

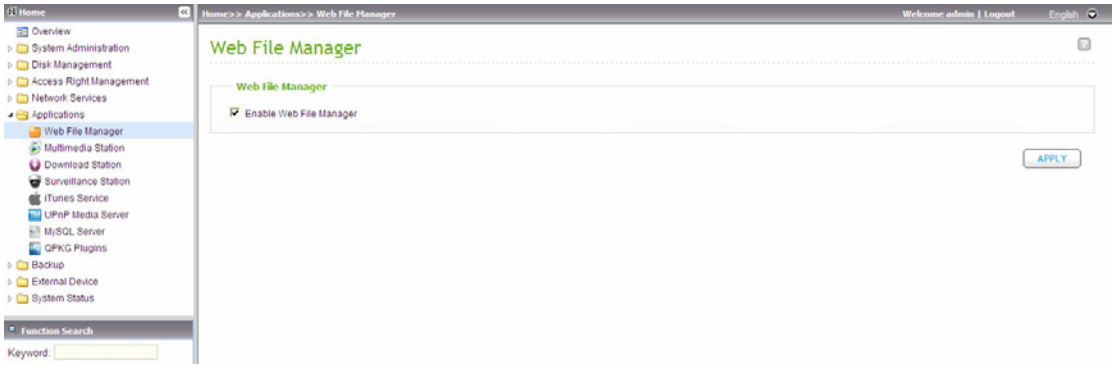


3.5 Applications



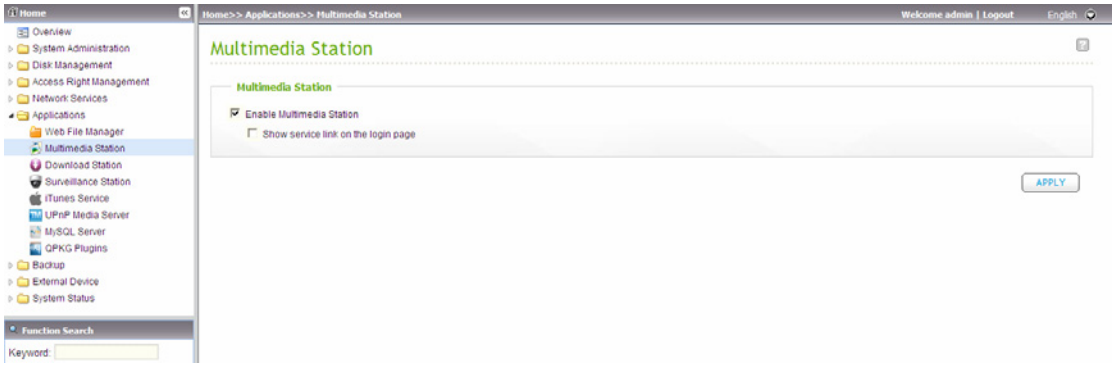
3.5.1 Web File Manager

To access the NAS via the web browser, enable Web File Manager. If the NAS is connected to the Internet and uses a valid IP address, you can access files on the server by web browser from anywhere. For more information, please refer to Chapter 6.



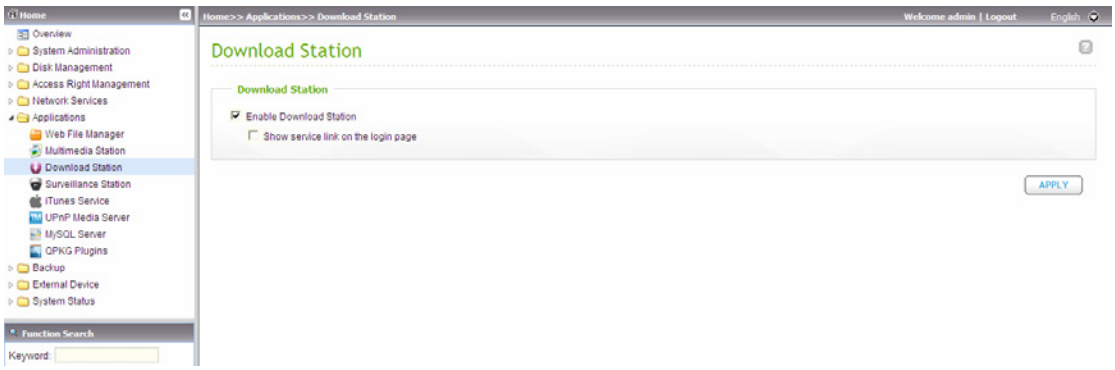
3.5.2 Multimedia Station

To share photos, music or video files on the NAS over the network, enable Multimedia Station. For further information of Multimedia Station, iTunes service and UPnP Media Server, please refer to Chapter 4.



3.5.3 Download Station

The NAS supports PC-less BT, HTTP, and FTP download. To use download function of the NAS, please enable Download Station. For further information, please refer to Chapter 5.



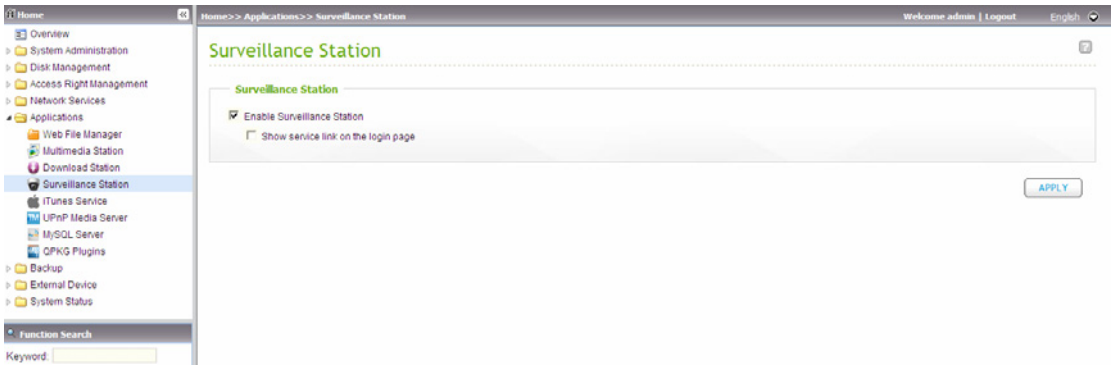
Warning: Please be warned against illegal downloading of copyrighted materials. The Download Station functionality is provided for downloading authorized files only. Downloading or distribution of unauthorized materials may result in severe civil and criminal penalty. Users are subject to the restrictions of the copyright laws and should accept all the consequences.

3.5.4 Surveillance Station

The Surveillance Station enables you to monitor and record the live video of maximum 2-4* network cameras available on the network (LAN or WAN).

*This function is applicable to some models only. Please refer to the comparison table for more details:
http://www.qnap.com/images/products/comparison/Comparison_NAS.html

Note: To use this feature on TS-x39/509/809 series, please update the system firmware with the image file enclosed in the product CD or download the latest system firmware.



Click "Surveillance Station" on the top or on the login page of NAS to access the Surveillance Station. If you login the service from the login page of the NAS, you are required to enter the user name and password.

Note: The Surveillance Station is only supported on IE browser 6.0 or later.

To set up your network surveillance system by NAS, follow the steps below:

1. Plan your home network topology
2. Set up the IP Cameras
3. Configure the camera settings on NAS
4. Configure your NAT router (for remote monitoring over the Internet)

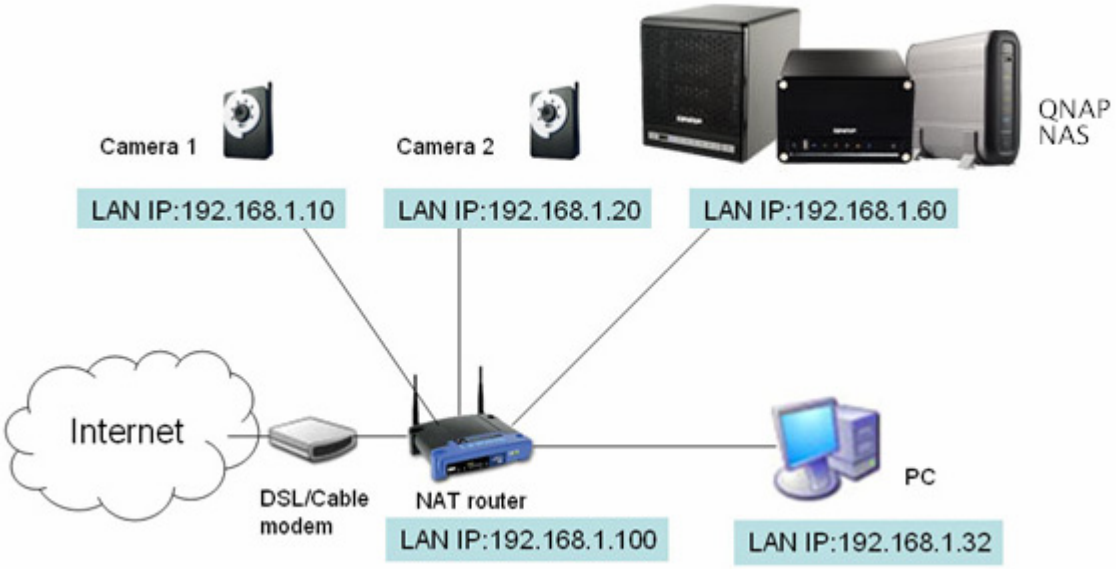
1. Plan your home network topology

Write down your plan of the home network before starting to set up the surveillance system. Consider the following when doing so:

i. The IP address of NAS
ii. The IP address of the cameras

Your computer, the NAS, and the IP cameras should be installed to the same router in LAN. Assign fixed IP addresses to the NAS and the IP cameras. For example,

- The LAN IP of the home router: 192.168.1.100
- Camera 1 IP: 192.168.1.10 (fixed IP)
- Camera 2 IP: 192.168.1.20 (fixed IP)
- NAS IP: 192.168.1.60 (fixed IP)



2. Set up the IP Cameras

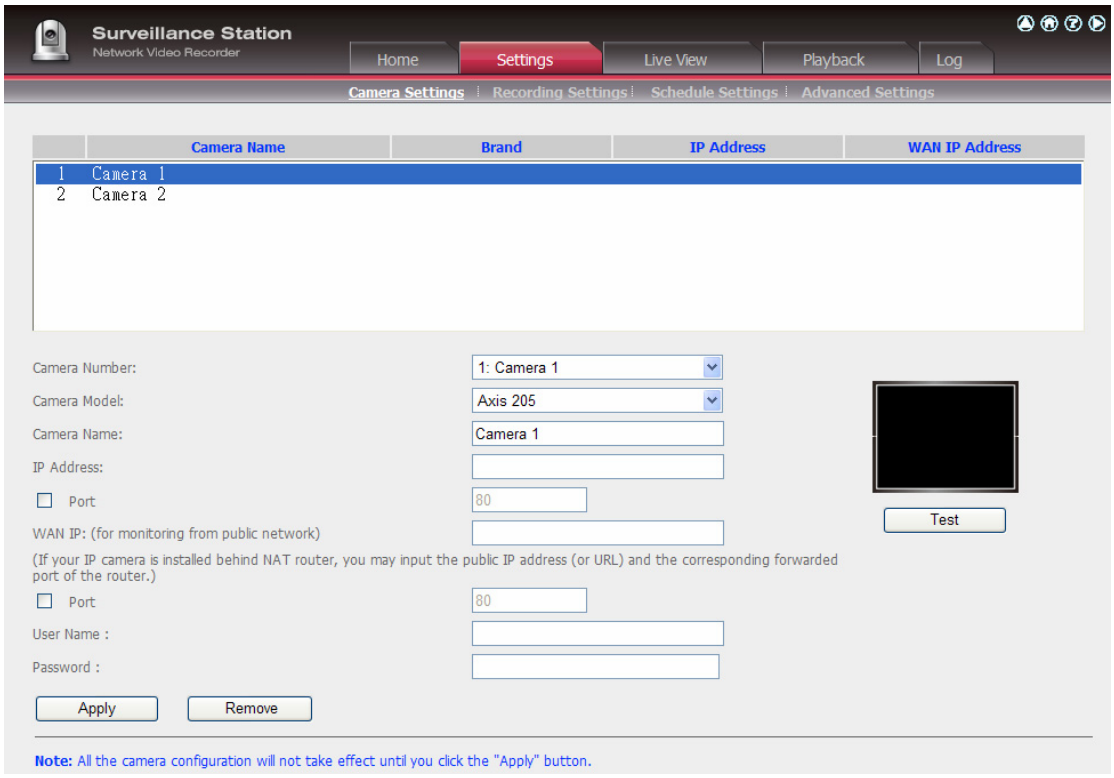
In this example, two IP cameras will be installed. Connect the IP cameras to your home network. Then set the IP address of the cameras so that they are in the same LAN as the computer. Login the configuration page of the Camera 1 by IE browser. Enter the IP address of the first camera as 192.168.1.10. The default gateway should be set as the LAN IP of the router (192.168.1.100 in this example). Then configure the IP address of the second camera as 192.168.1.20.

Some cameras provide a utility for IP configuration. You may refer to the user manual of the cameras for further details.

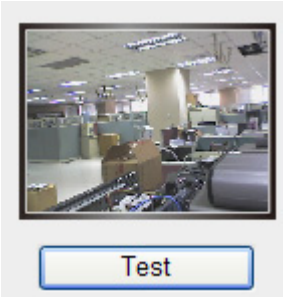
** Please refer to www.qnap.com for the supported network camera list.*

3. Configure the camera settings on NAS

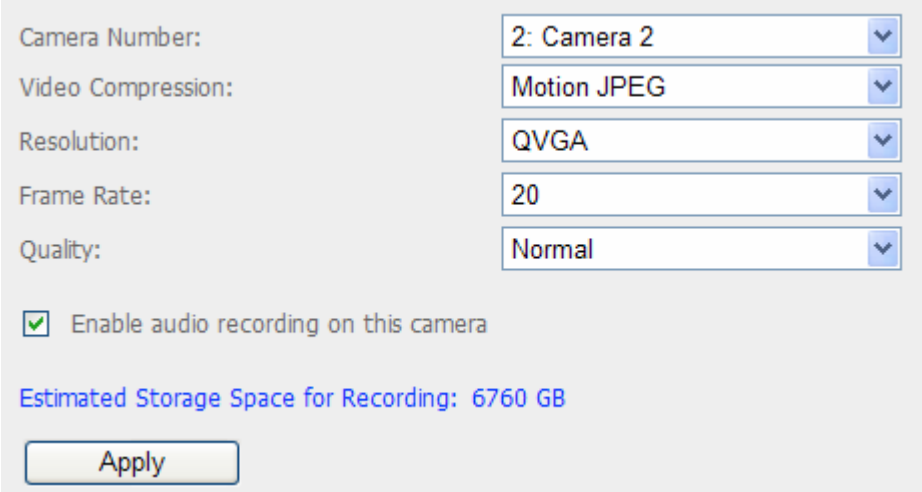
Login the Surveillance Station by IE browser to configure the IP cameras. Go to "Settings>Camera Settings" page. Enter the camera information, e.g. name, model, and IP address.



Click “Test” on the right to ensure the connection to the IP camera is successful.



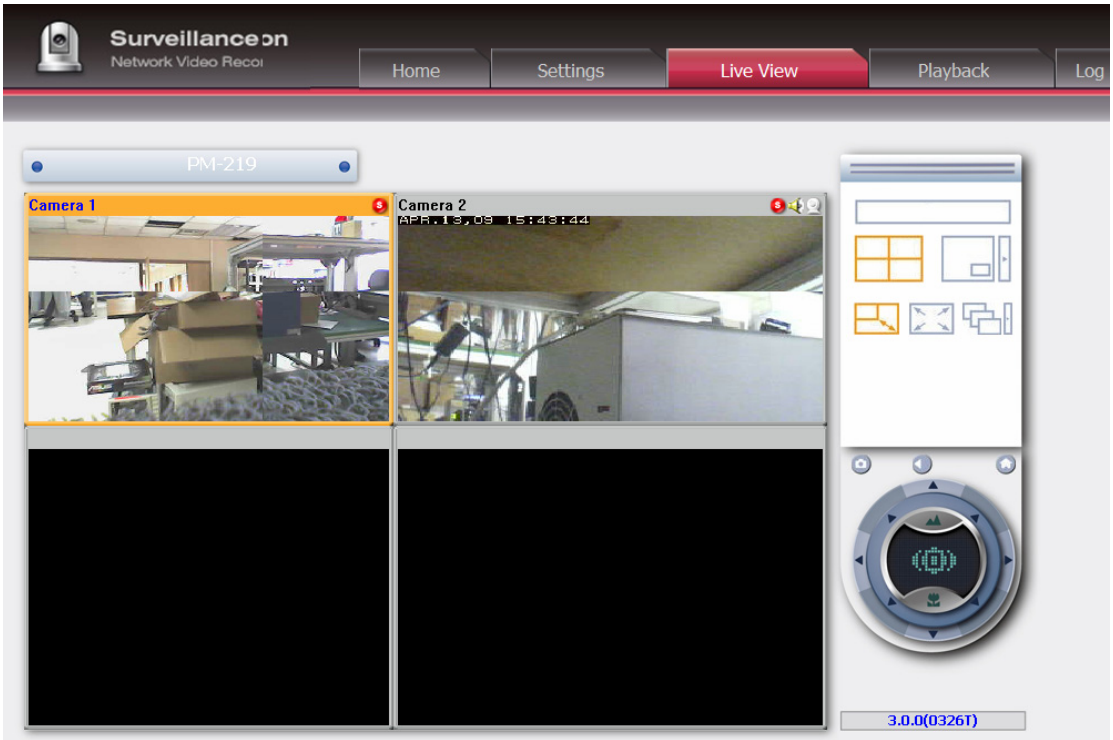
If your camera supports audio recording, you may enable the option in “Recording Settings” page. Click “Apply” to save the changes.



Configure the settings of Camera 2 following the above steps.

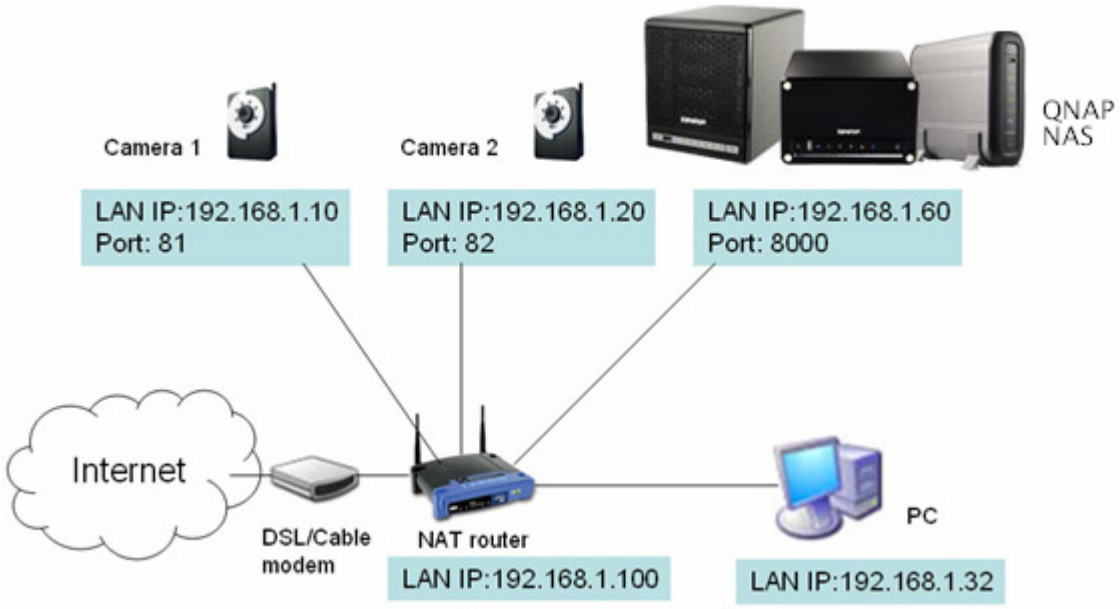
After you have added the network cameras to NAS, go to the “Live View” page. The first time you access this page by IE browser, you have to install the ActiveX control in order to view the images of Camera 1 and Camera 2. You can start to use the monitoring and recording functions of the Surveillance Station.

To use other functions of the Surveillance Station such as motion detection recording, schedule recording, and video playback, please refer to the online help.



4. Configure your NAT router (for remote monitoring over the Internet)

To view the monitoring video and access the NAS remotely, you need to change the network settings by forwarding different ports to the corresponding LAN IP on your NAT router.



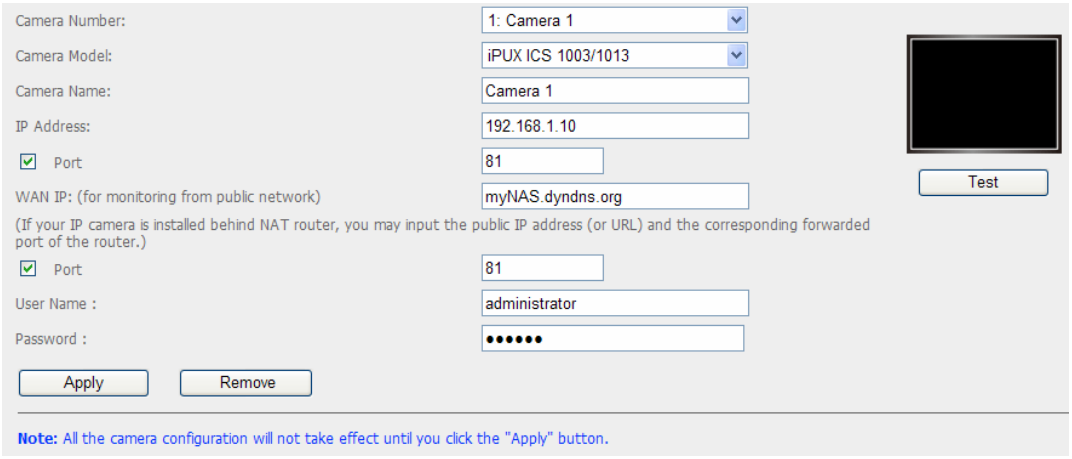
Change the port settings of NAS and IP cameras

The default HTTP port of NAS is 8080. In this example, the port is changed to 8000. Therefore, you have to access the NAS via **http://NAS IP:8000** after applying the settings.

Then login the network settings page of the IP cameras. Change the HTTP port of Camera 1 from 80 to 81. Then change the port for Camera 2 from 80 to 82.

Next, login Surveillance Station. Go to "Settings>Camera Settings". Enter the port numbers of Camera 1 and Camera 2 as 192.168.1.10 **port 81** and 192.168.1.20 **port 82** respectively. Enter the login name and password for both cameras.

Besides, enter the WAN IP address (or your domain address in public network, e.g. MyNAS.dyndns.org) and the port on the WAN side for the connection from Internet. After finishing the settings, click "Test" to ensure successful connection to the cameras.



Go to the configuration page of your router and configure the port forwarding as below:

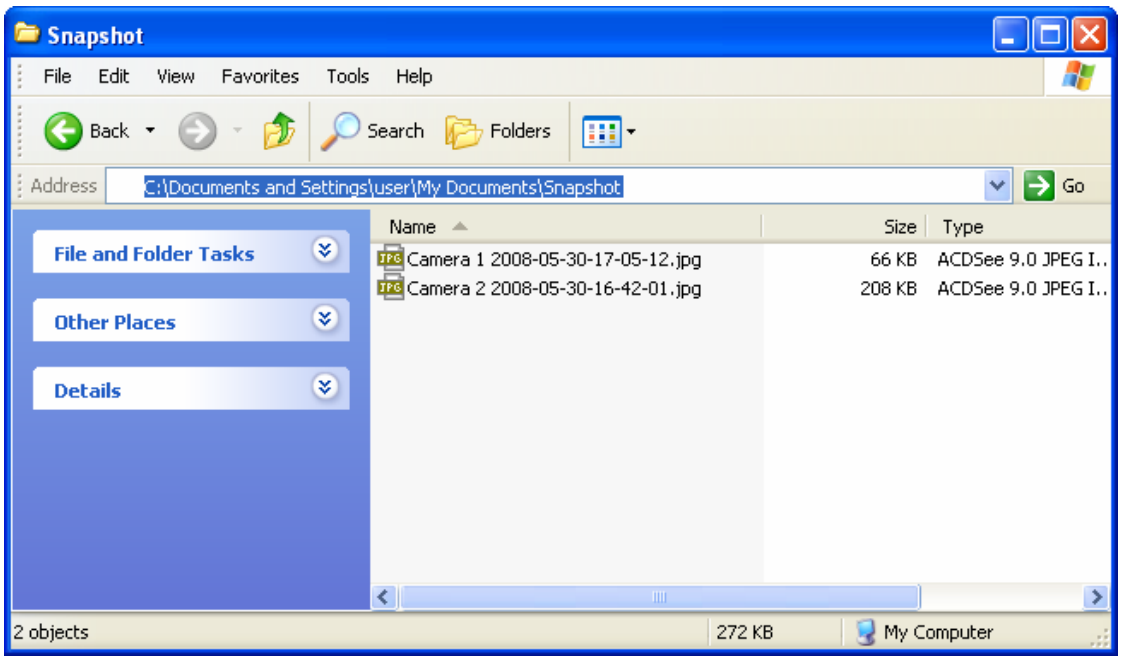
- Forward Port 8000 to NAS LAN IP: 192.168.1.60
- Forward Port 81 to Camera 1's LAN IP: 192.168.1.10
- Forward Port 82 to Camera 2's LAN IP: 192.168.1.20

Note: When you change the port settings, make sure remote access is allowed. For example, if you office network blocks port 8000, you will not be able to access your NAS from the office.

After you have configured the port forwarding and router settings, you can start to use the Surveillance Station for remote monitoring over the Internet.

Access the snapshots and video recordings of Surveillance Station

All the snapshots are saved in "My Documents" > "Snapshot" (Windows XP) in your computer. If you are using Windows 7 or Vista, the default directory is "Documents" > "Snapshot".

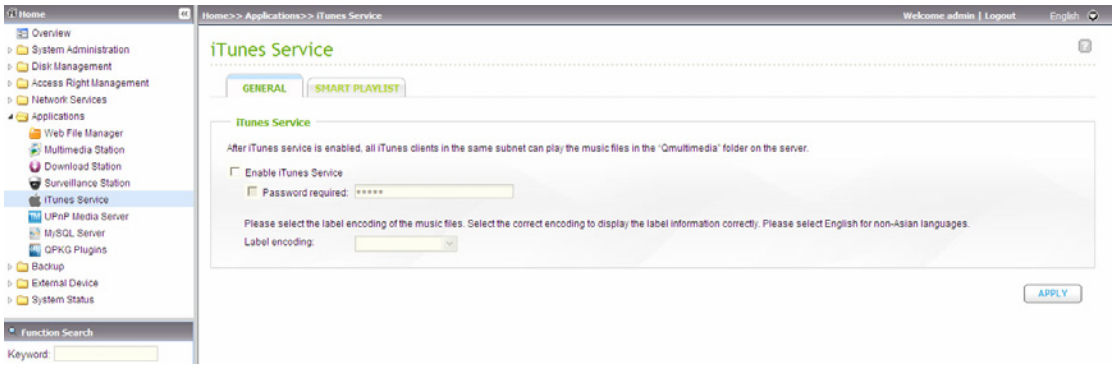


The video recordings will be saved in \\NASIP\Qrecordings or \\NASIP\Recordings. Normal recordings are saved in the folder "record_nvr" and alarm recordings are saved in the folder "record_nvr_alarm" in the network share.

3.5.5 iTunes Service

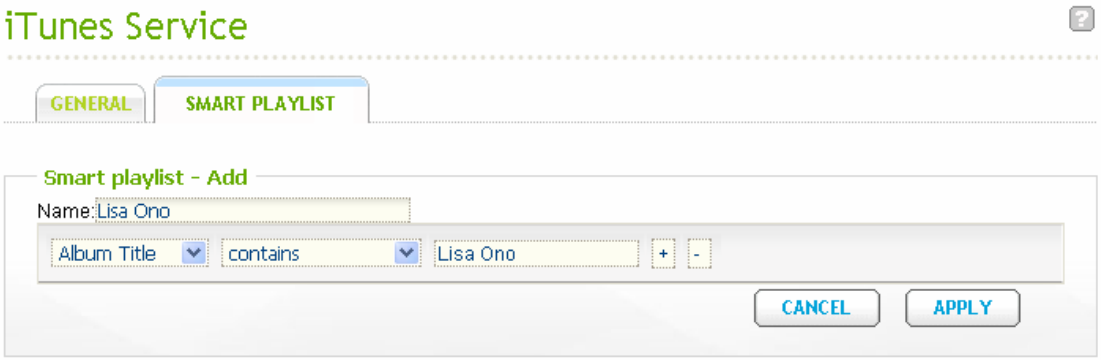
The mp3 files on Qmultimedia/ Multimedia folder of the NAS can be shared to iTunes by enabling this service. All the computers with iTunes installed on LAN are able to find, browse, and play the music files on the NAS.

To use the iTunes service, make sure you have installed the iTunes program on your computer. Enable this service. Then upload the music files to the Qmultimedia/ Multimedia folder of NAS.



Password required: To allow the users to access the data only by entering the correct password, check this option and enter the password.

Click “Smart Playlist” to enter the smart playlist page. You can define the playlist rules to categorize the songs into different playlists. If there is no song that matches the rules in the playlist, the iTunes client will not show the playlist. For detailed operation, please refer to the online help.



When you open iTunes, it detects the NAS automatically. All the songs on the Qmultimedia/ Multimedia folder will be shown.

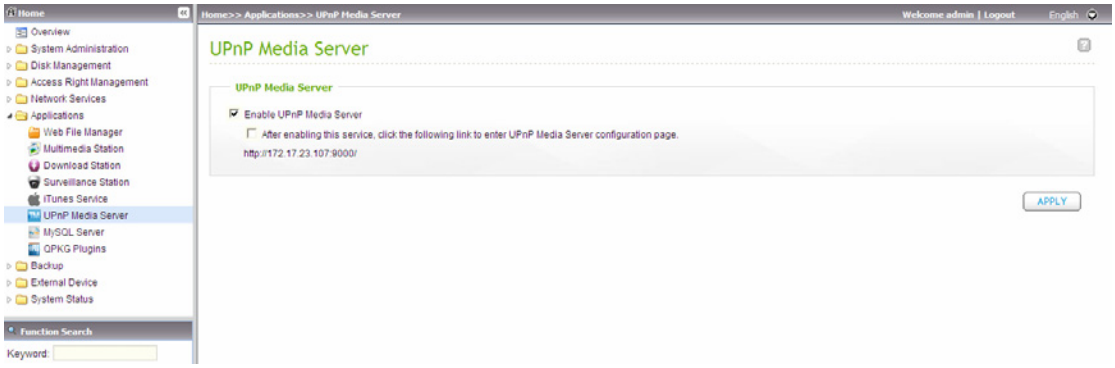
Click the triangle icon next to the NAS name. The smart playlists defined earlier will be shown. The songs are categorized accordingly. You can start to use iTunes to play the music on your NAS.

Note: You can download the latest iTunes software from official Apple website http://www.apple.com.

3.5.6 UPnP Media Server

The NAS is built-in with TwonkyMedia, DLNA compatible UPnP media server. Enable this function and the NAS will share particular music, photos, or video files to DLNA network. You can use DLNA compatible digital media players to play the multimedia files on the NAS on your TV or acoustic sound system.

To use UPnP Media Server, please enable this function and click the following link (http://NAS IP:9000/) to enter the configuration page of UPnP Media Server.



Click the link http://NAS IP:9000/. Go to "TwonkyMedia Settings" > "Basic Setup" to configure the basic server settings.

The contents on the Qmultimedia or Multimedia folder of the NAS will be shared to the digital media players by default. You can go to "Basic Setup" > "Sharing" > "Content Locations" to change the share folder or add more share folders.

After configuring the settings, you can upload mp3, photos, or video files to the specified share folders on the NAS.

Note: If you upload multimedia files to the default share folder but the files are not shown on Media Player, you can click "Rescan content directories" or "Restart server" on the Media Server configuration page.

For the online tutorial, please visit http://www.qnap.com/pro_features.asp.

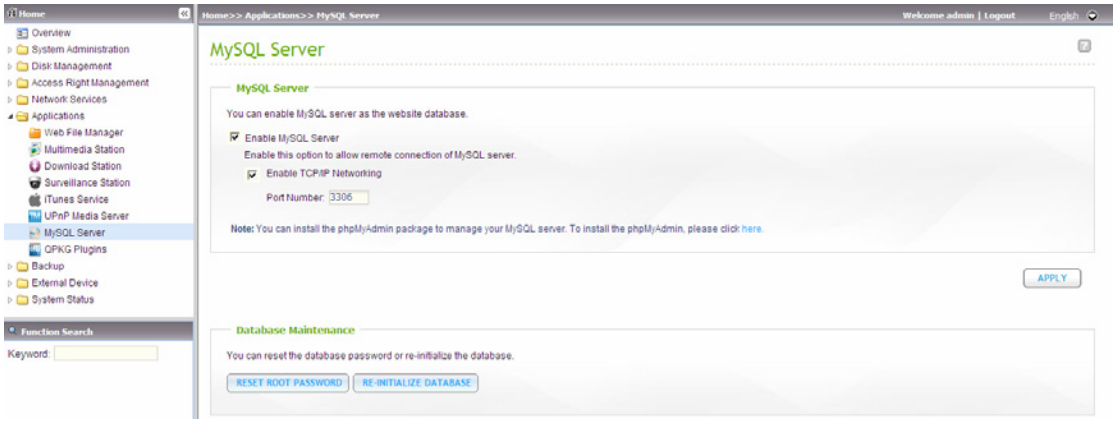
About UPnP and DLNA

Universal Plug and Play (UPnP) is a set of computer network protocols promulgated by the UPnP Forum. The purpose of UPnP is to allow devices to connect seamlessly and to simplify the implementation of networks at home and in corporate environment. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards.

The term UPnP is gleaned from Plug-and-play, a technology for dynamically attaching devices to a computer directly.

The Digital Living Network Alliance (DLNA) is an alliance of a number of consumer electronics, mobile and personal computer manufacturers. Its aim is to establish a home network in which the electronic devices from all companies are compatible with each other under an open standard. The alliance also tries to promote the idea of digital home by establishing DLNA certification standard. All DLNA certified products connected to the home network can be accessed seamlessly to enable consumers to enjoy digital life conveniently.

3.5.7 MySQL Server



Note: To use this feature on TS-x39/509/809 series, please update the system firmware with the image file enclosed in the product CD or download the latest system firmware.

You can enable MySQL Server as the website database.

Enable TCP/IP Networking

You can enable this option to configure MySQL Server of the NAS as a database server of another web server in remote site through Internet connection. When you disable this option, your MySQL Server will only be configured as local database server for the web server of the NAS.

After enabling remote connection, please assign a port for the remote connection service of MySQL server. The default port is 3306.

After the first-time installation of the NAS, a folder phpMyAdmin is created in the Qweb/ Web network folder. You can enter http://NAS IP/phpMyAdmin/ in the web browser to enter the phpMyAdmin page and manage the MySQL database.

Note:

- Please do not delete the phpMyAdmin folder. You can rename this folder but the link on the MySQL Server page will not be updated. To access the renamed folder, you can enter the link http://NAS IP/*renamed folder* in the web browser.
- The phpMyAdmin folder is created after the first-time installation. When you update the firmware, the folder remains unchanged.

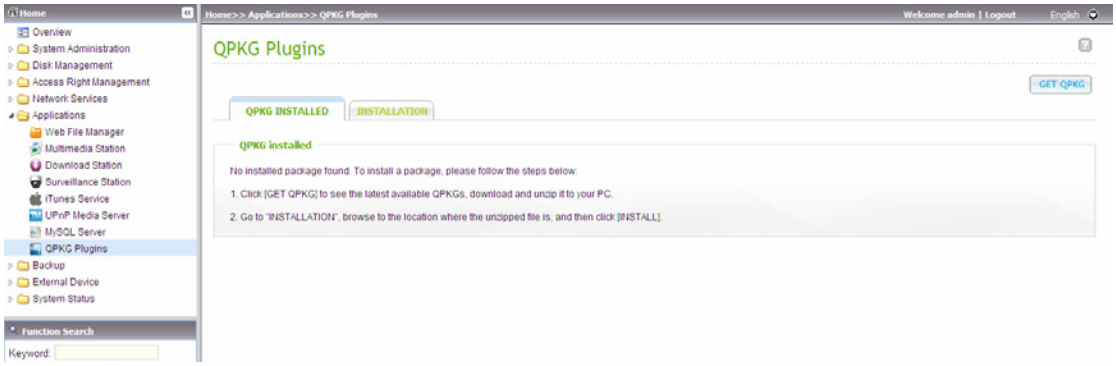
Database Maintenance

- Reset root password: Execute this function to reset the password of MySQL root as "**admin**".
- Re-initialize database: Execute this function to delete all the data on MySQL database.

For the online tutorial, please refer to http://www.qnap.com/pro_features.asp.

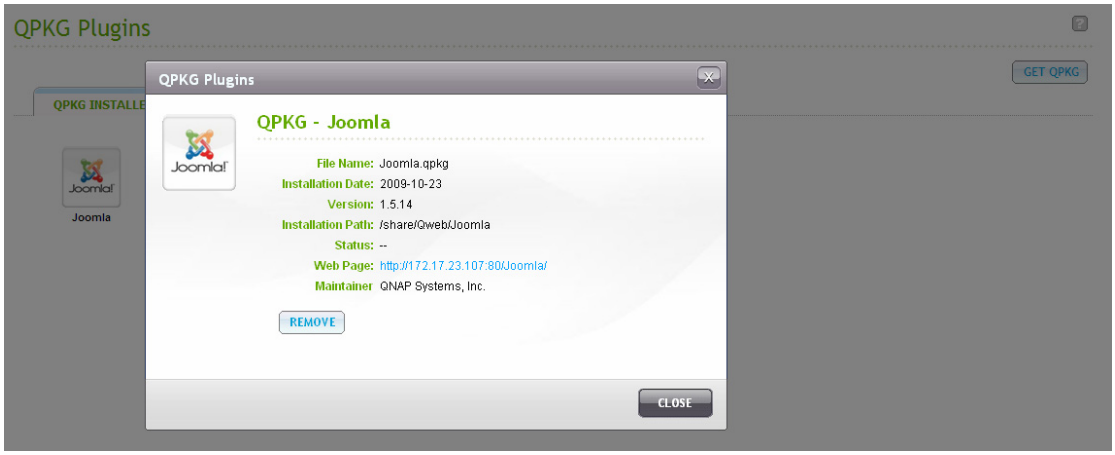
3.5.8 QPKG Plugins

You can install QPKG packages to add more functions to NAS. Click "GET QPKG".

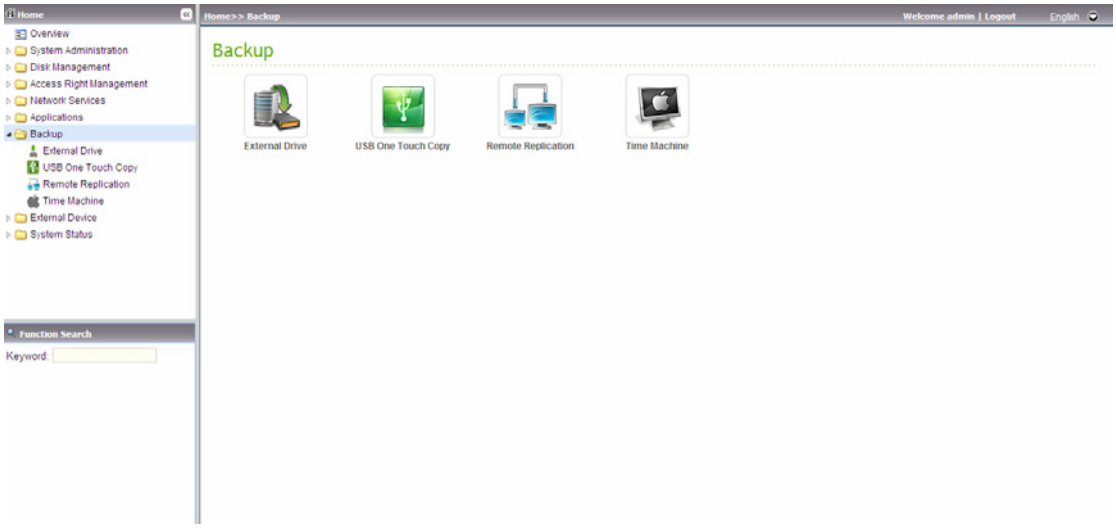


Before you install the packages, make sure the files are correct, read the instructions carefully, and back up all important data on the NAS. Download the software package you want to install on NAS to your computer.
Before installing the QPKG package, please unzip the downloaded file. To install QPKG, browse to select the correct qpkg file and click "INSTALL".

After uploading the QPKG packages, the details are shown on the QPKG page. Click the link to access the web page of the installed software package and start to configure the settings. To remove the package from the NAS, click "REMOVE".



3.6 Backup



3.6.1 External Drive

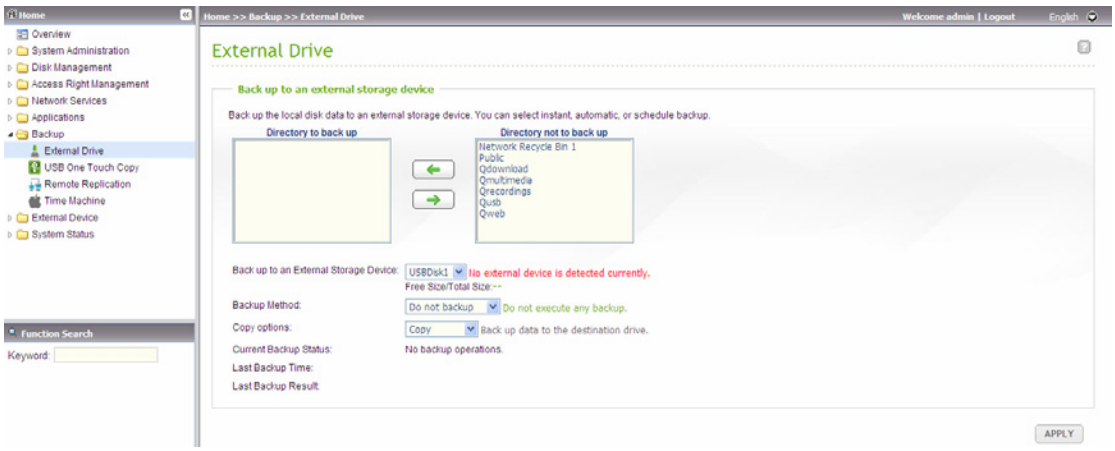
You can back up the local drive data to an external storage device. In this page, you can select to execute instant, automatic, or schedule backup methods, and configure the relevant settings.

- Backup Now: To back up data to the external storage device immediately.
- Schedule Backup: To back up data by schedule. You can select the week day and time to execute the backup.
- Auto-backup: To execute the backup automatically once the storage device is connected to the NAS.

Copy Options:

You can select "Copy" or "Synchronize" for the copy options. When "Copy" is selected, files are copied from the NAS to the external device. By selecting "Synchronize", the data on the internal drives of the NAS and the external storage device are synchronized. Any different files on the external device are deleted.

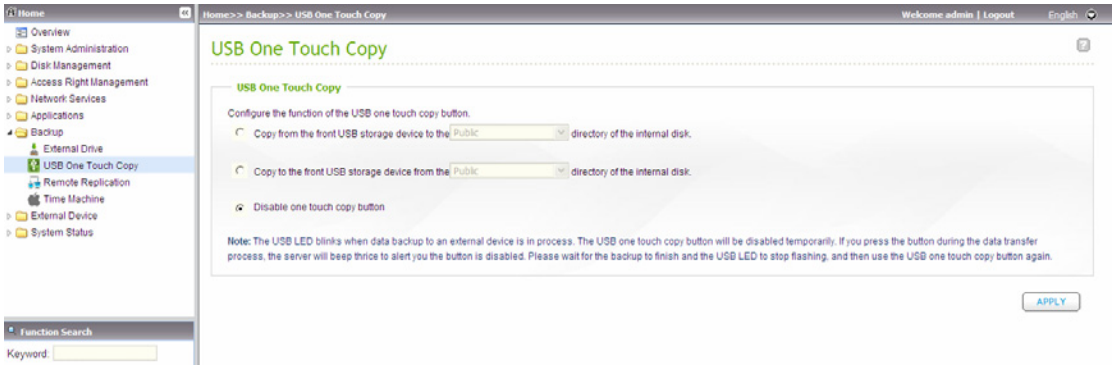
Note: In the copying and synchronizing process, if the identical files exist on both sides, the files are not copied. If there are files in the same name but different in size or modified dates on NAS and the external device, the files on the external device are overwritten.


Home
Overview
System Administration
Disk Management
Access Right Management
Network Services
Applications
Backup
External Drive
USB One Touch Copy
Remote Replication
Time Machine
External Device
System Status
Function Search
Keyword:
Home >> Backup >> External Drive
Welcome admin | Logout
English
External Drive
Back up to an external storage device
Back up the local disk data to an external storage device. You can select instant, automatic, or schedule backup.
Directory to back up
Directory not to back up
Network Recycle Bin 1
Public
Qdownload
Qmultimedia
Qrecordings
Qusb
Qweb
Back up to an External Storage Device:
USBDisk1
No external device is detected currently.
Free Size/Total Size:--
Backup Method:
Do not backup
Do not execute any backup.
Copy options:
Copy
Back up data to the destination drive.
Current Backup Status:
No backup operations.
Last Backup Time:
Last Backup Result:
APPLY

3.6.2 USB One Touch Copy

You can configure the function of the USB one touch copy button in this page. The following three functions are available:

- Copy from the front USB storage to a directory of the internal drive of the NAS.
- Copy to the front USB storage from a directory of the internal drive of the NAS.
- Disable the one touch copy button



Data Copy by the Front USB Port

The NAS supports instant data copy backup from the external USB device to the NAS or the other way round by the front one touch copy button. To use this function, follow the steps below:

1. Make sure a hard drive is installed and formatted on the NAS. The default network share Qusb/ Usb is created.
2. Turn on the NAS.
3. Configure the behavior of the Copy button on "Backup" > "USB one touch copy" page.
4. Connect the USB device, e.g. digital camera or flash, to the front USB port of the NAS.
5. Press the Copy button once. The data will be copied according to your settings on the NAS.

Note: Incremental backup is used for this feature. After the first time data backup, the NAS only copies the changed files since the last backup.

3.6.3 Remote Replication

3.6.3.1 Remote Replication

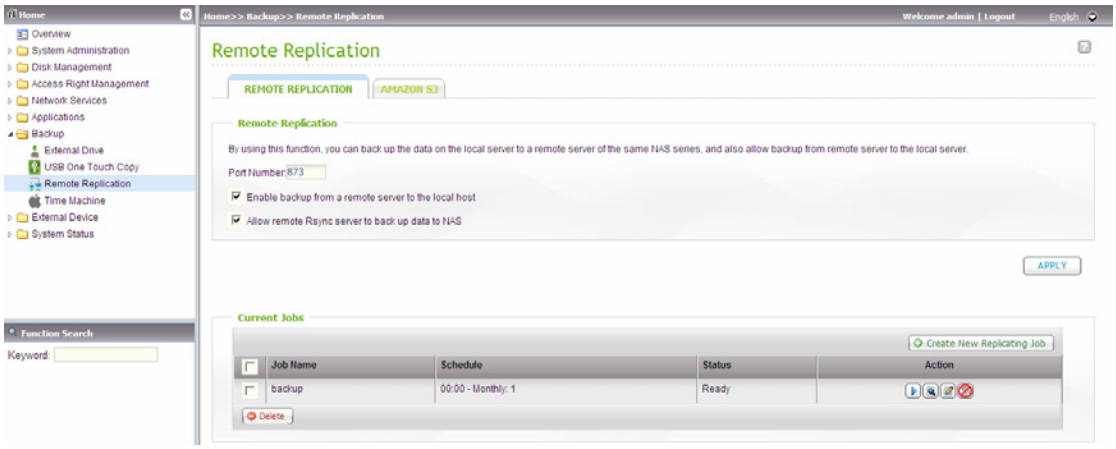
You can use this option to back up the files on the NAS to another QNAP NAS or Rsync server over LAN or the Internet.

Make sure a network share is created before creating a remote replication task.

- ✓ **Port Number:** Specify a port number for remote replication. The default port number is 873.

  Note: If this server connects to the Internet via a router, make sure the specified port for remote replication is opened on the router.

- ✓ **Enable backup from a remote server to the local host:** Check this option to allow the remote server to back up data to the local host via remote replication.
- ✓ **Allow remote Rsync server to back up data to NAS:** Enable this option to allow a remote Rsync server to back up data to the NAS by remote replication.



Follow the steps below to create a remote replication job for backup from the NAS to another QNAP NAS.

1. Click "Create New Replicating Job" to create a new task.

2. Select the server type and enter the job name.

3. Enter the IP address or domain name (if any) of the remote server, the port number of the remote server, the user name and password with write access to the remote server. Click "Test" to check if the connection is successful or not.

   Note:
   - To use remote replication, enable Microsoft Networking service, make sure the destination network share and directory have been created, and the user name and password are valid to login the destination folder.
   - The share folder name (network share or directory) is case-sensitive.

4. Enter the destination path. The share folder name (network share or directory) is case-sensitive.

5. Enter the source path. You can select to back up the whole network share and a folder in the share.

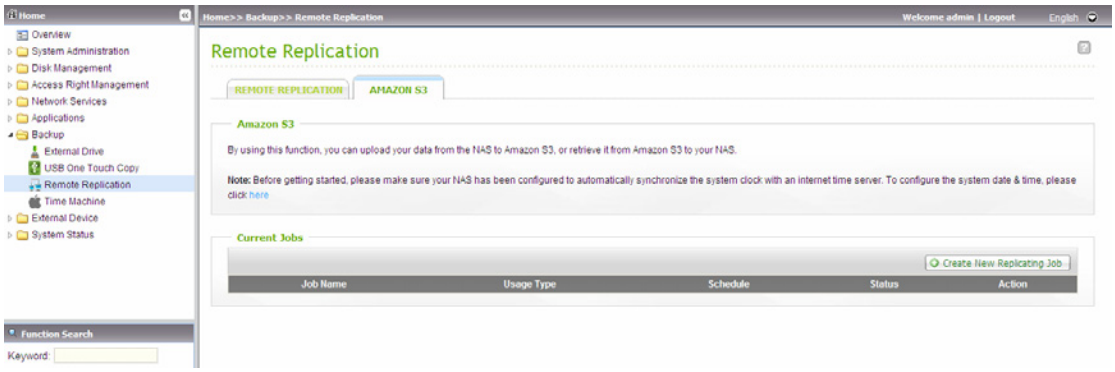
6. Define the replication schedule.

7. Set up other options for the remote replication job. Then click "Finish".

3.6.3.2 Amazon S3

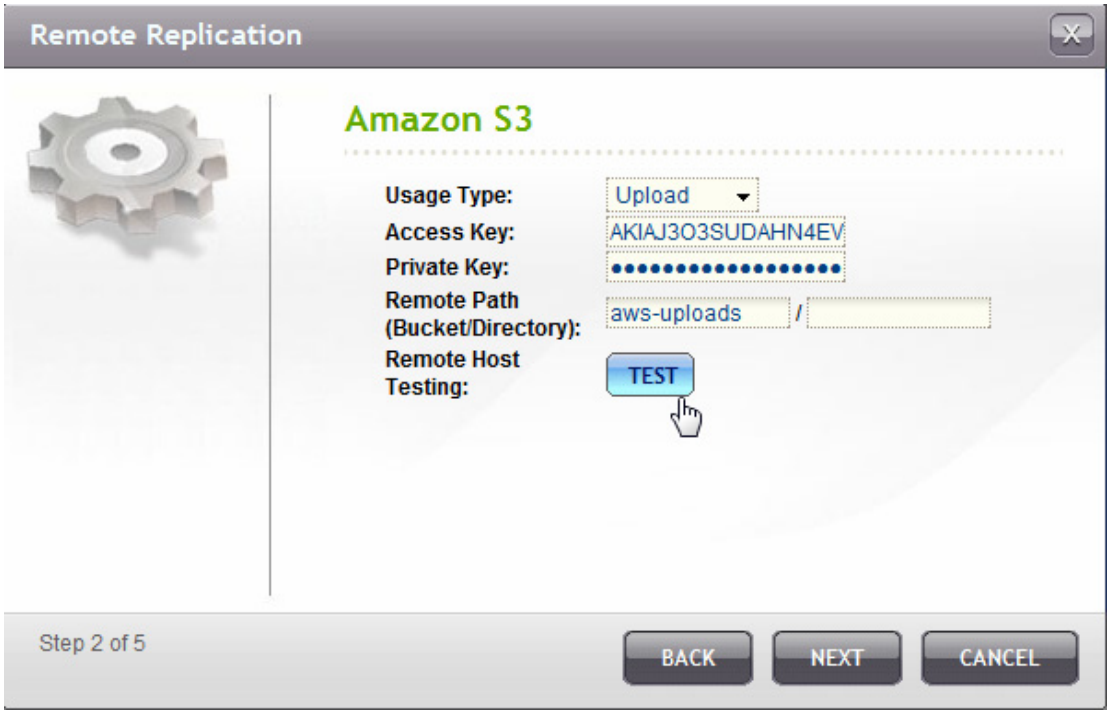
Amazon S3 (Simple Storage Service) is an online storage web service offered by AWS (Amazon Web Services). It provides a simple web services interface that can be used to store and retrieve the data from anywhere on the web. With Amazon S3, you can upload the data from your NAS to Amazon S3 or download the data from Amazon S3 to your NAS.

Note that you need to register an AWS account from http://aws.amazon.com/ and pay for the service. After signing up for an account, you need to create at least one bucket (root folder) on Amazon S3 by an Amazon S3 application. We recommend the Mozilla Firefox add-on "S3Fox" for beginners.



After setting up the Amazon S3 account, follow the steps below to back up data to or retrieve data from Amazon S3 using the NAS.

1. Click "Create New Replicating Job".
2. Enter the remote replication job name.
3. Select the usage type: "Upload" or "Download" and enter other settings. Bucket is the root directory on Amazon S3. You could do remote host testing by clicking "TEST". Other settings are optional.

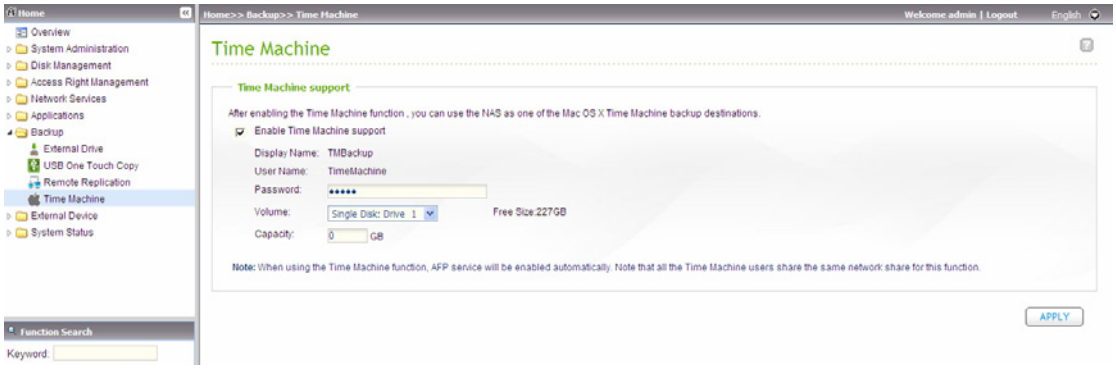


4. Specify the local directory on the NAS for replication.
5. Enter the replication schedule.
6. Click "Finish". The replication job will be executed according to your schedule.

3.6.4 Time Machine

You can enable Time Machine support to use the NAS as a backup destination of multiple Mac by the Time Machine feature on OS X.

This function is applicable to some models only. Please refer to the comparison table for more details:
http://www.qnap.com/images/products/comparison/Comparison_NAS.html



To use this function, follow the steps below.

Configure the settings on the NAS:

1. Enable Time Machine support.

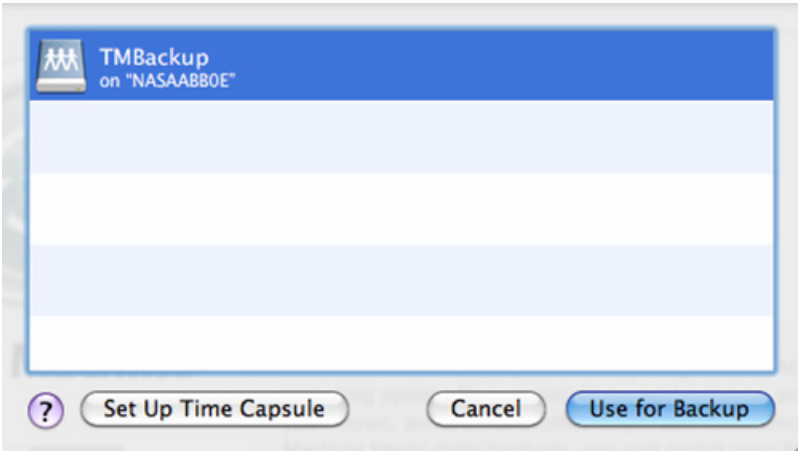
2. Enter the Time Machine password. The password is empty by default.
3. Select a volume on the NAS as the backup destination.
4. Enter the storage capacity that Time Machine backup is allowed to use.
5. Click "Apply" to save the settings.

All the Time Machine users share the same network share for this function.

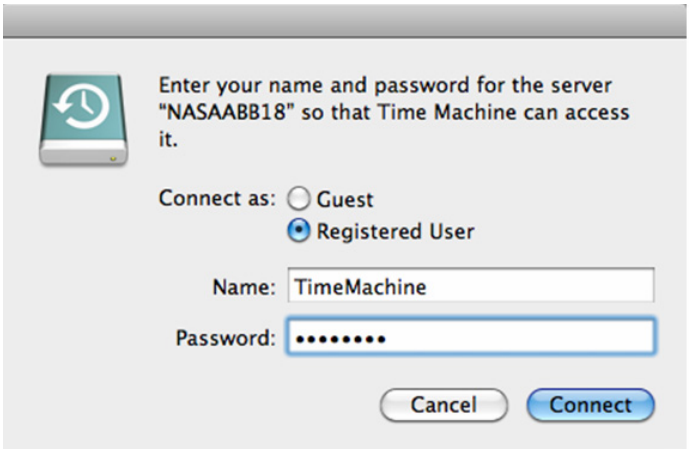
Configure the backup settings on Mac:

1. Open Time Machine on your Mac and click "Select Backup Disk".

2. Select the TMBackup on your NAS from the list and click "Use for Backup".



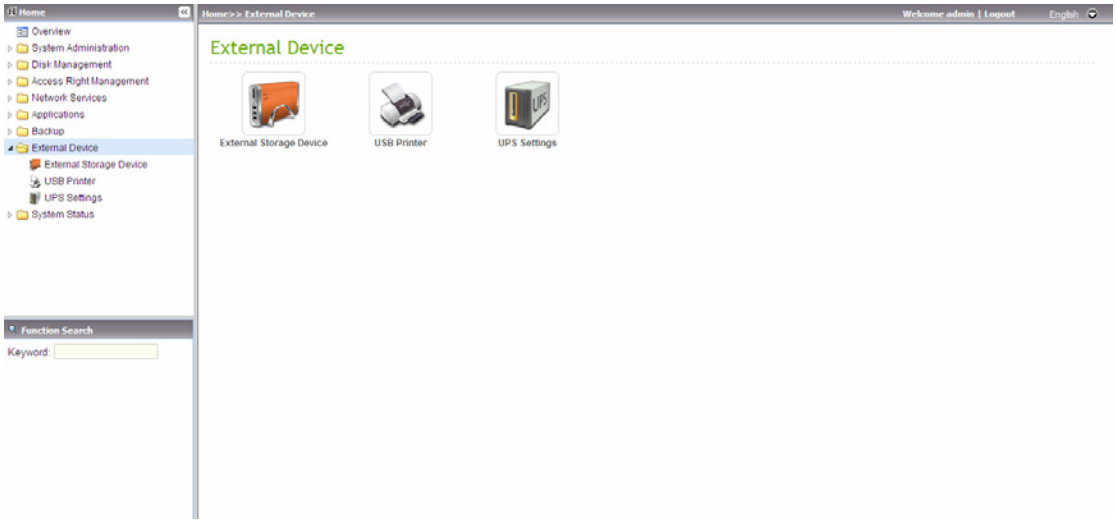
3. Enter the user name and password to access QNAP NAS. Then click "Connect".
   Registered user name: TimeMachine
   Password: The password you have configured on the NAS. The password is empty by default.



4. Upon successful connection, the Time Machine is switched "ON". The available space for backup is shown and the backup will start in 120 seconds.

The first time backup may take longer time according to the data size on Mac. To recover the data to the Mac OS, please refer to the tutorial on http://www.apple.com.

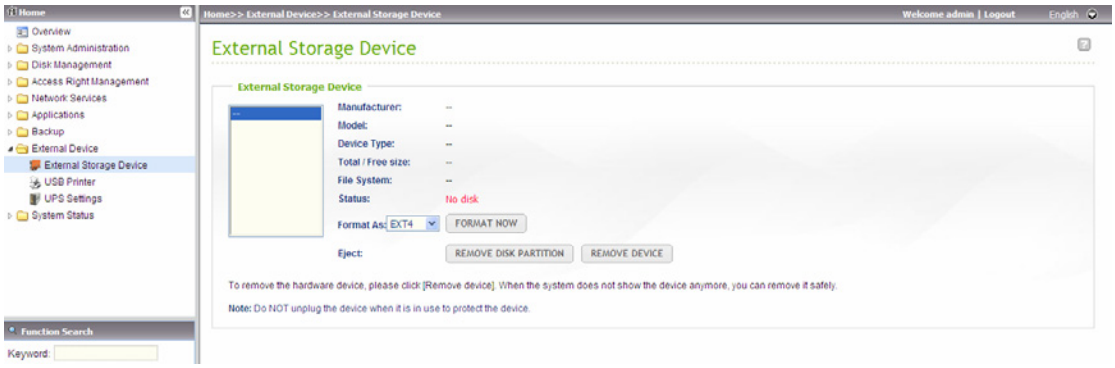
3.7 External Device



3.7.1 External Storage Device

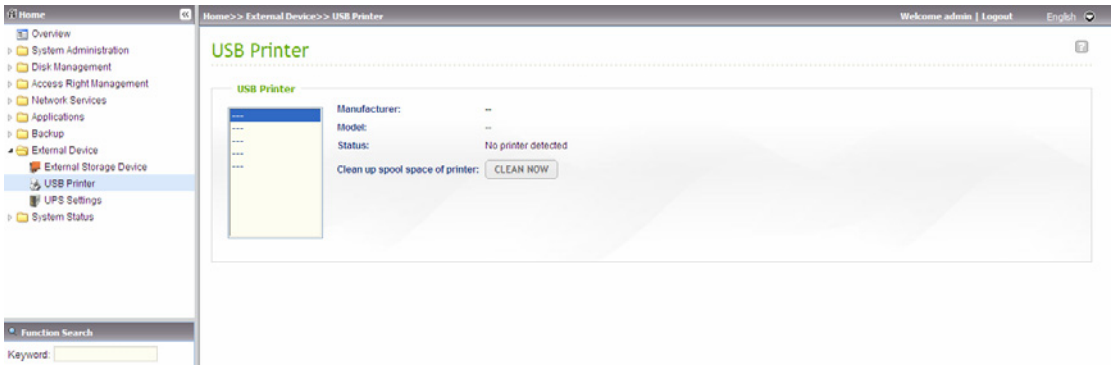
The NAS supports USB disks and thumb drives for extended storage. Connect the USB device to the USB port of the NAS, when the device is successfully detected, the details are shown on this page.

It may take tens of seconds for the NAS server to detect the external USB device successfully. Please wait patiently.



3.7.2 USB Printer

To provide printer sharing function for the network users, you can simply connect a USB printer to the USB port of the NAS. The NAS detects the printer automatically. Up to 3 printers are supported.



Note:

- Please connect a USB printer to the server after the software configuration is completed.
- The NAS does not support multifunction printer.
- For the information of supported USB printer models, please visit http://www.qnap.com.

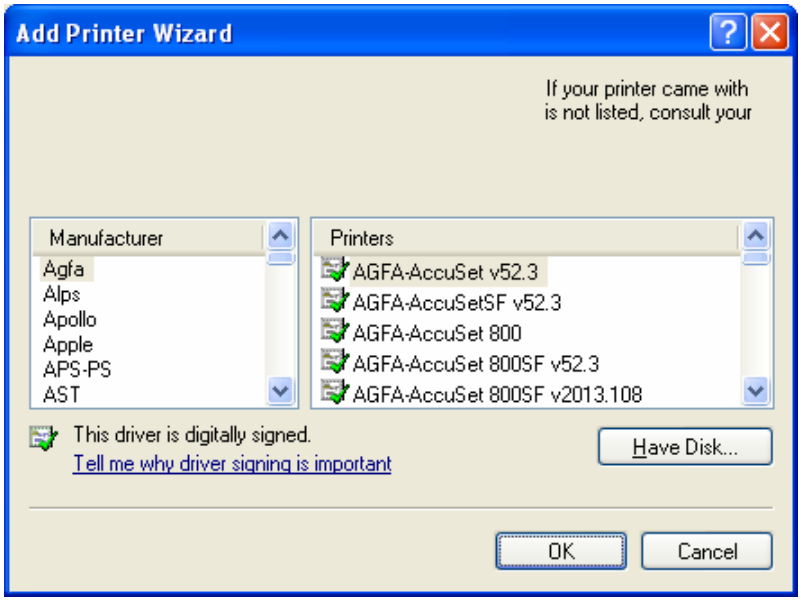
3.7.2.1 Windows XP Users

Method 1

1. Enter \\NAS IP in Windows Explorer.

2. A printer icon is shown as a network share on the server. Double click the icon.

3. Install the printer driver.



4. When finished, you can start to use the network printer service of the NAS.

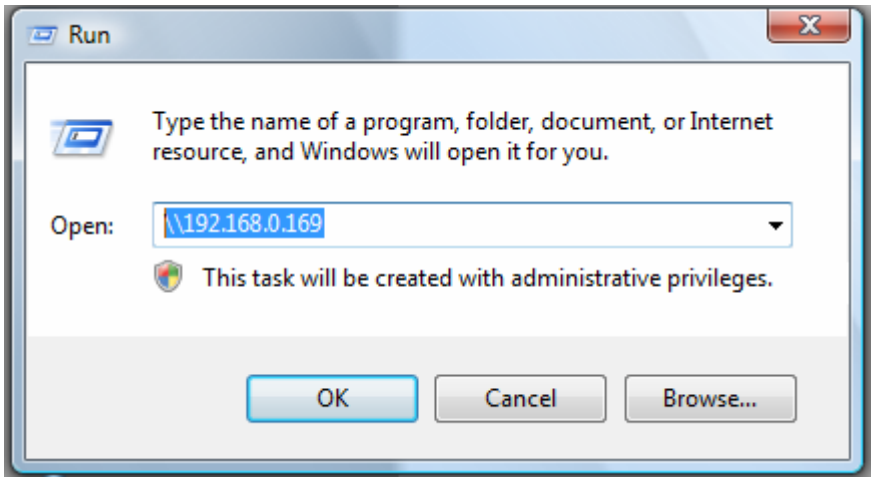
Method 2

The following configuration method has been verified on Windows XP only:

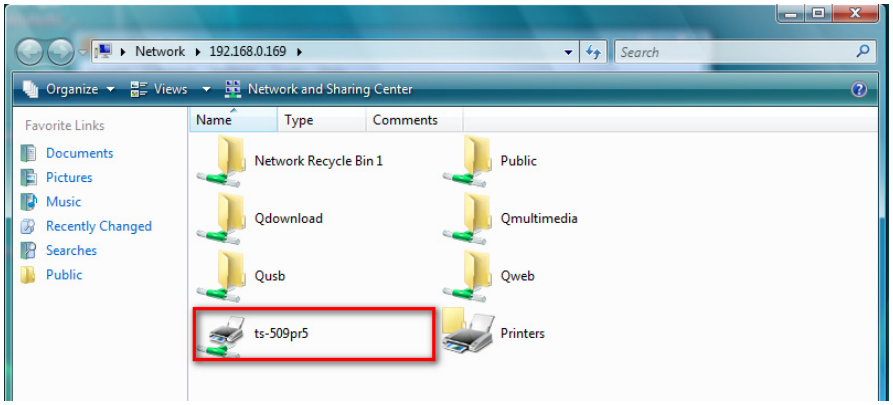
1. Open "Printers and Faxes".
2. Delete the existing network printer (if any).
3. Right click the blank area in the Printers and Faxes window. Select "Server Properties".
4. Click the "Ports" tab and delete the ports configured for the previous network printer (if any).
5. Restart your PC.
6. Open Printers and Faxes.
7. Click "Add a printer" and click "Next".
8. Select "Local printer attached to this computer". Click "Next".
9. Click "Create a new port" and select "Local Port" from the drop-down menu. Click "Next".
10. Enter the port name. The format is \\NAS IP\NAS namepr, e.g. NAS IP= 192.168.1.1, NAS name= myNAS, the link is \\192.168.1.1\myNASpr.
11. Install the printer driver.
12. Print a test page.

3.7.2.2 Windows Vista/ Windows 7 Users

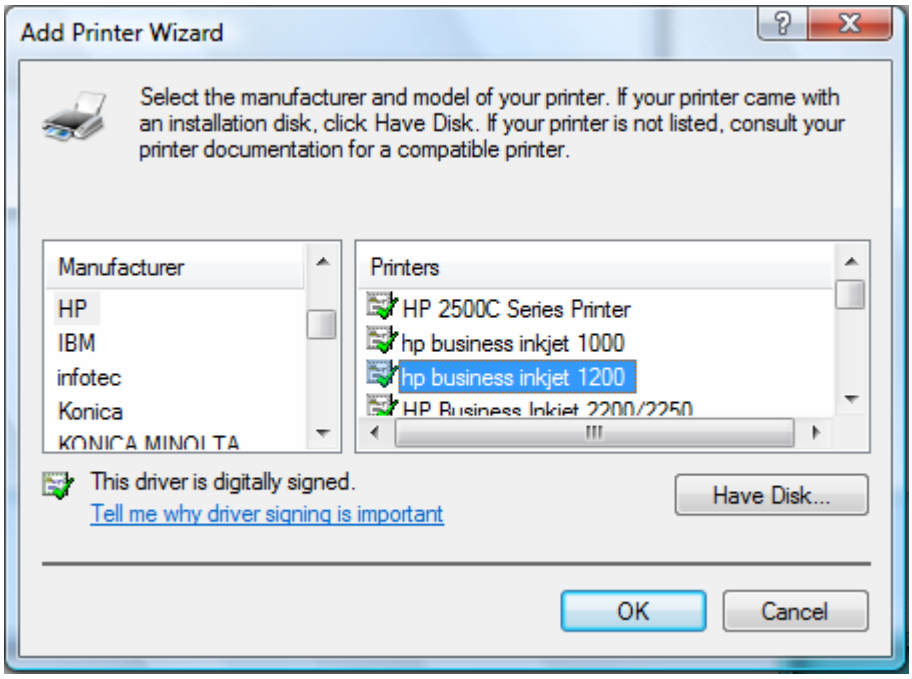
1. On the Run menu, enter \\NAS IP.



2. Find the network printer icon and double click it.



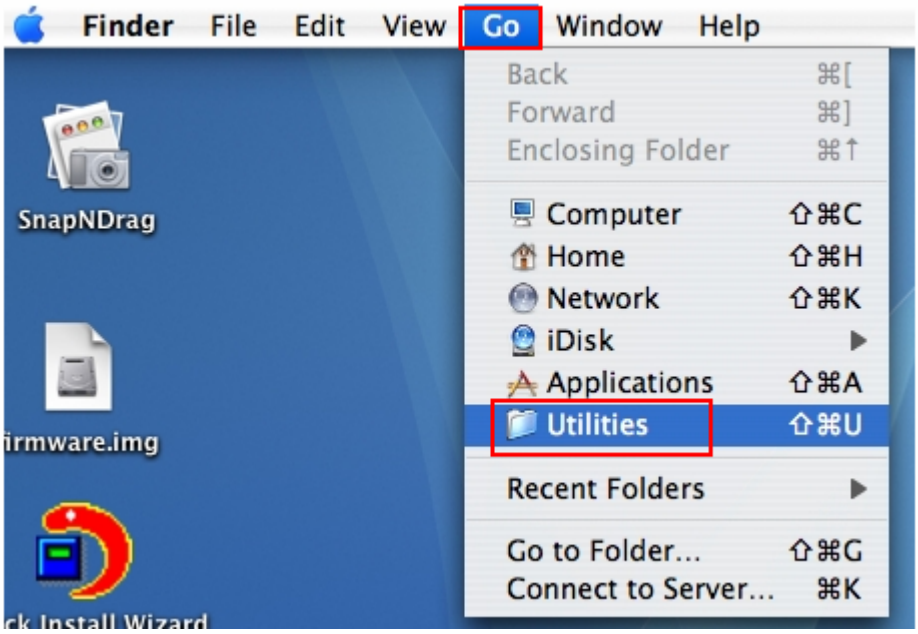
3. Install the correct printer driver.



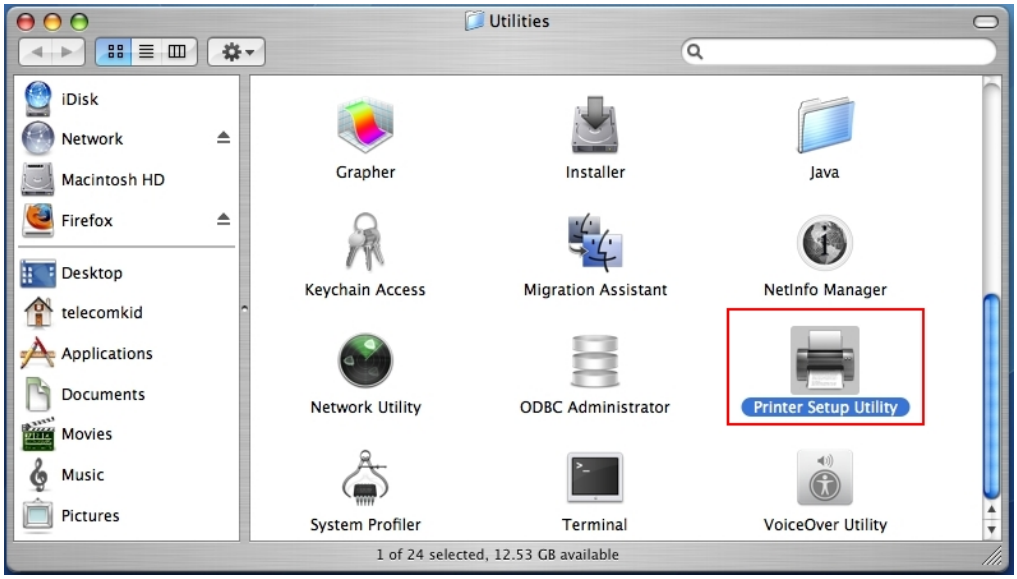
4. When finished, print a test page to verify the printer is ready to use.

3.7.2.3 Mac OS X 10.4

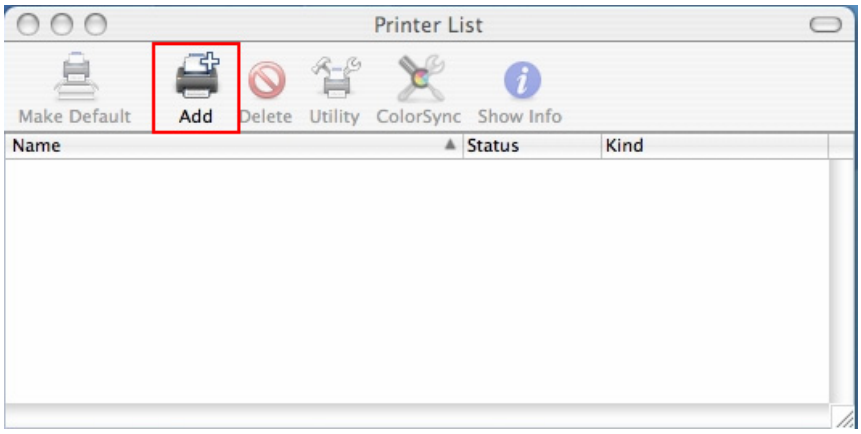
1. On the toolbar, click "Go/ Utilities".



2. Click "Printer Setup Utility".

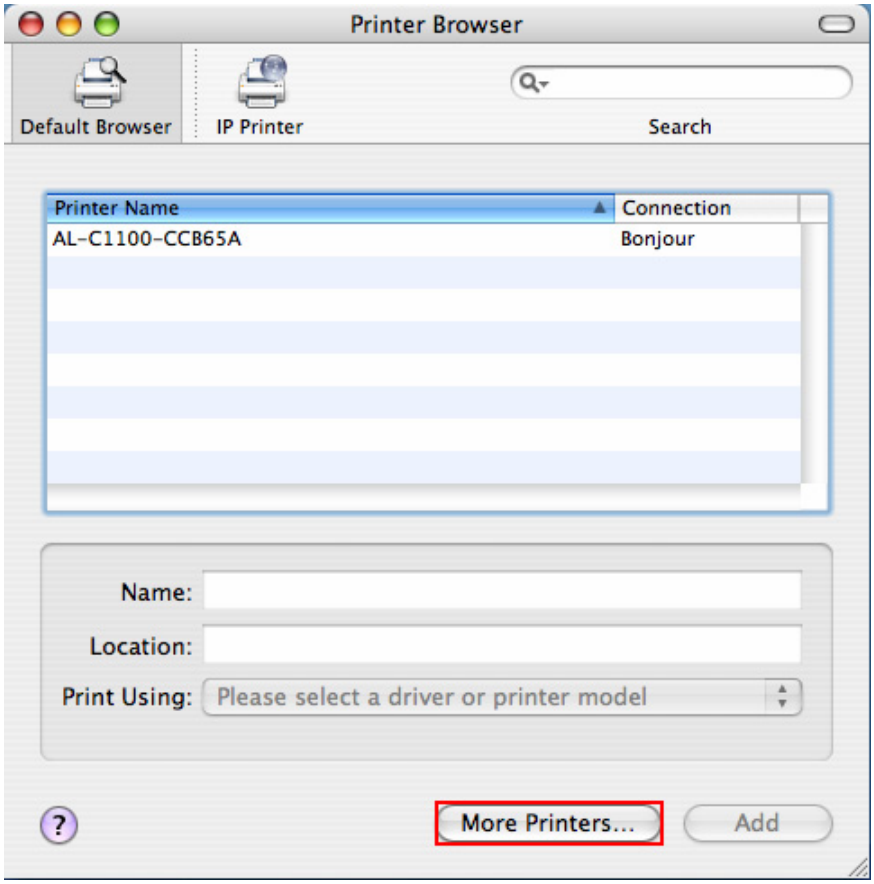


3. Click “Add”.

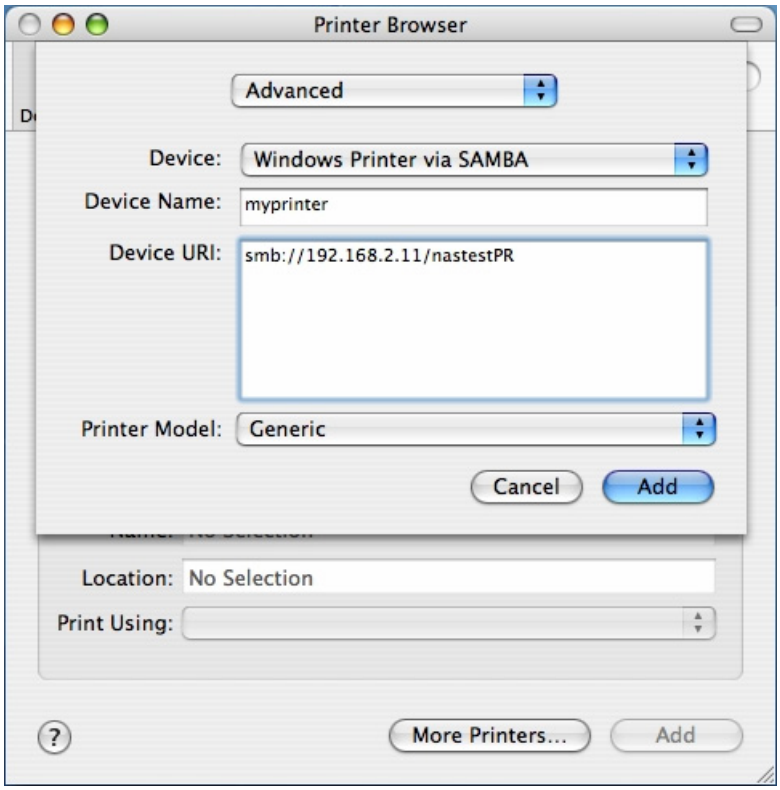


4. Press and hold the “alt” key 

on the keyboard and click “More Printers” concurrently.

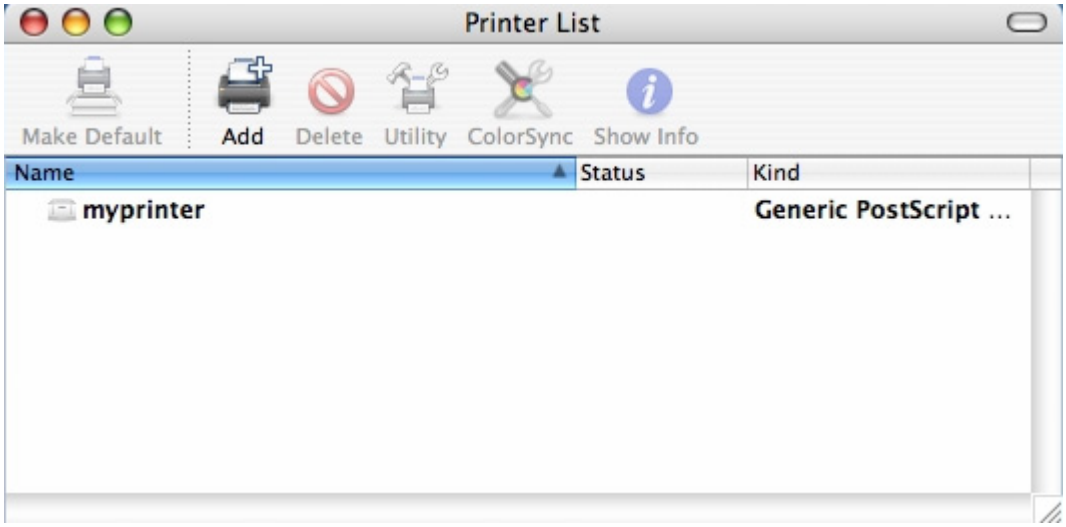


5. In the pop up window:
   a. Select “Advanced”*.
   b. Select “Windows Printer with SAMBA”.
   c. Enter the printer name.
   d. Enter the printer URI, the format is smb://NAS IP/printer name. The printer name is found on the “Device Configuration” > “USB Printer page”.
   e. Select “Generic” for Printer Model.
   f. Click “Add”.



*Note that you must hold and press the “alt” key and click “More Printers” at the same time to view the Advanced printer settings. Otherwise, this option does not appear.

6. The printer appears on the printer list. It is ready to use.

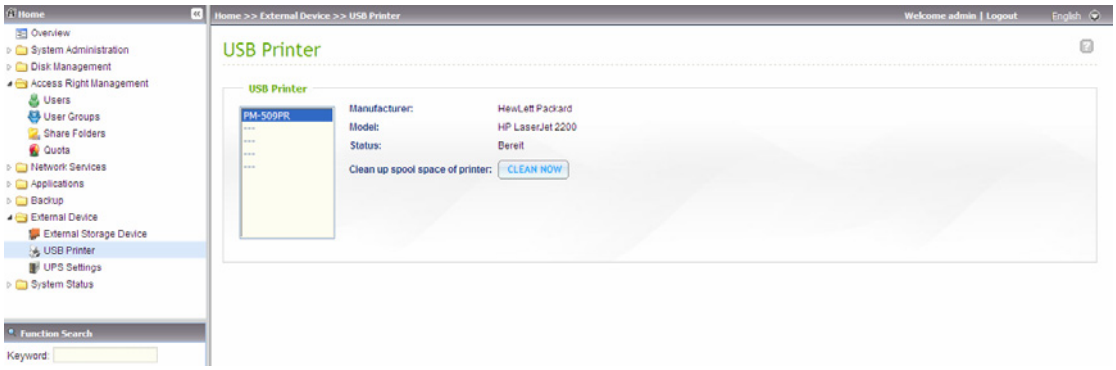


Note: The network printer service of the NAS supports Postscript printer on Mac OS only.

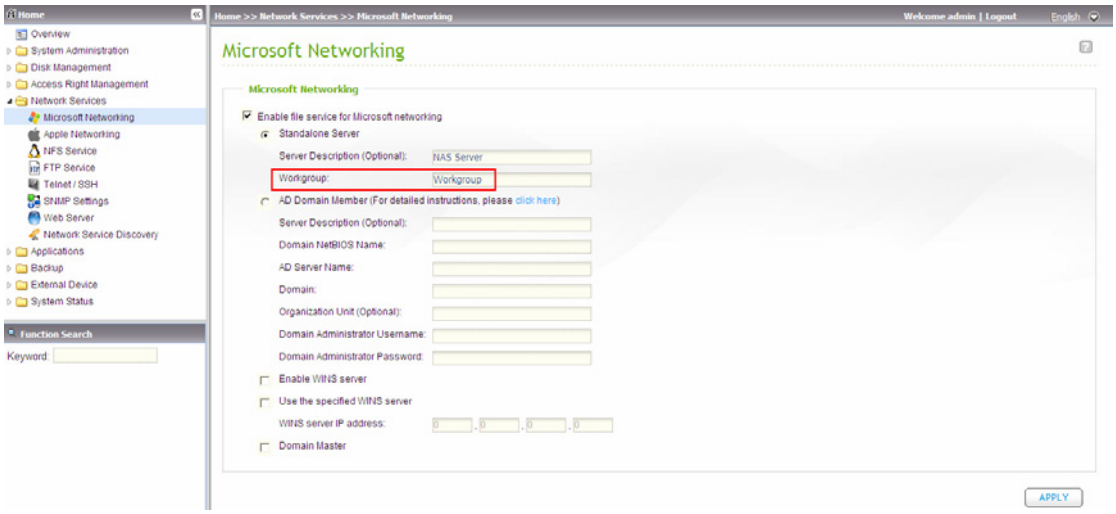
3.7.2.4 Mac OS X 10.5

If you are using Mac OS X 10.5, follow the steps below to configure the printer function of the NAS.

1. Make sure your printer is connected to the NAS and the printer information is displayed correctly on the "USB Printer" page.

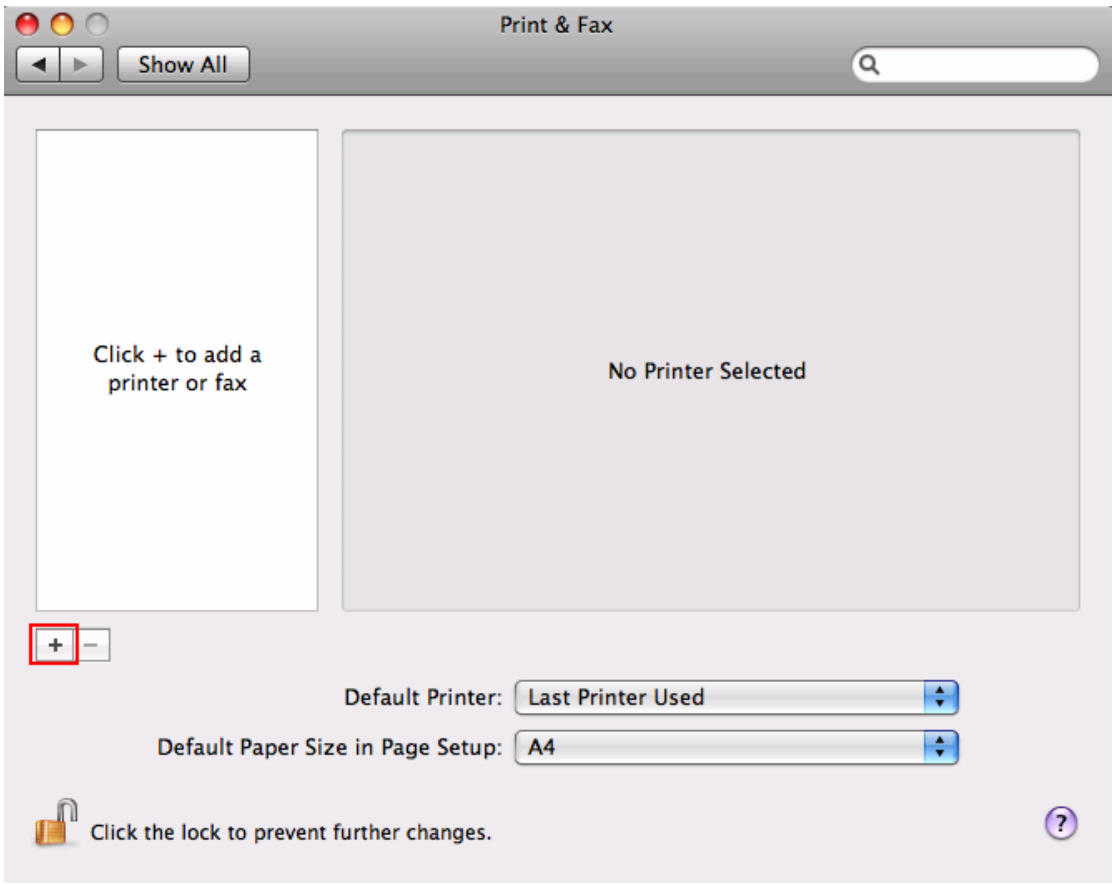


2. Go to “Network Services” > “Microsoft Networking”. Enter a workgroup name for the NAS. You will need this information later.

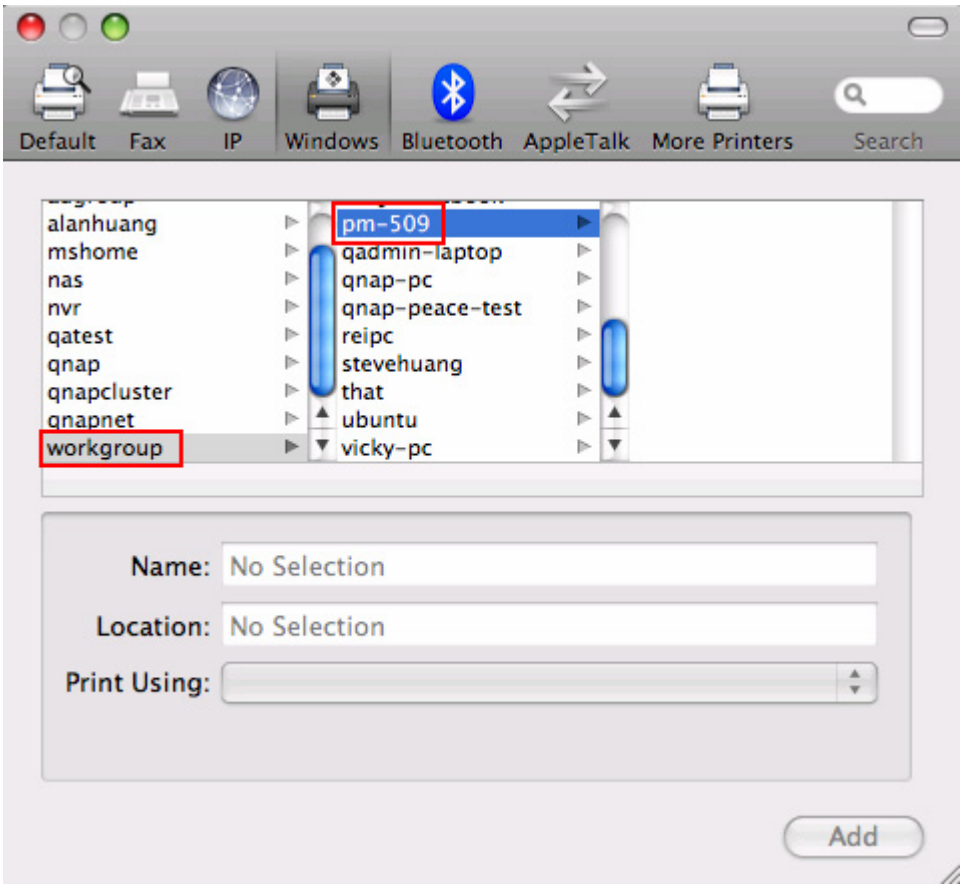


3. Go to “Print & Fax” on your Mac.

4. Click + to add a printer.

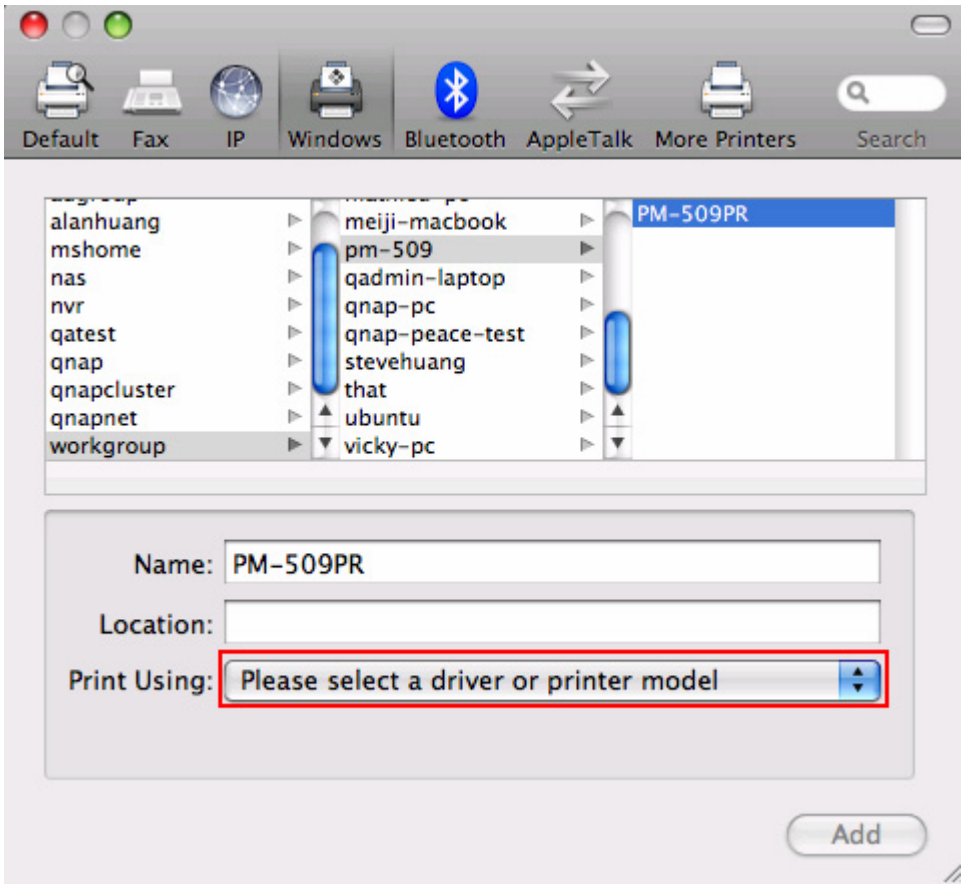


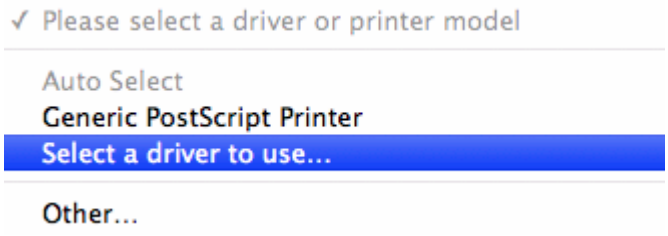
5. Select the NAS workgroup and find the printer name.



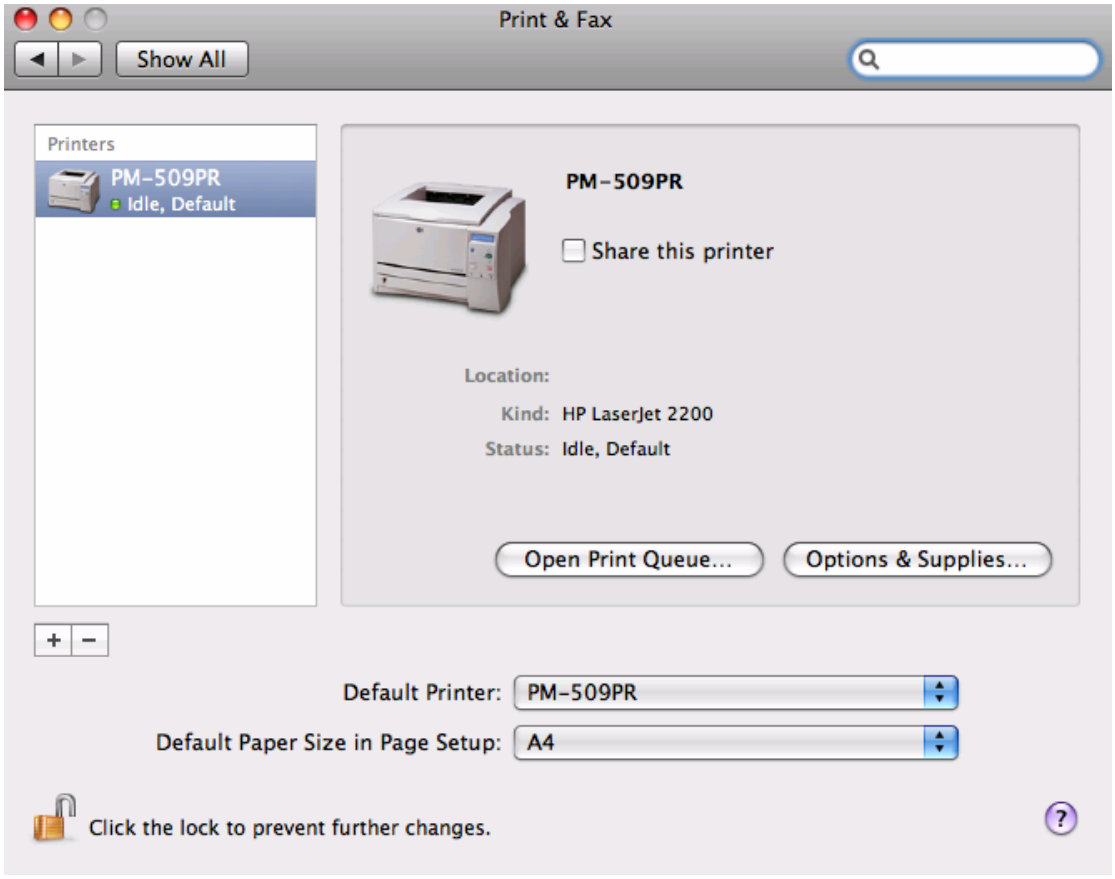
6. Enter the user name and password to access the printer server on the NAS.

7. Select the printer driver.



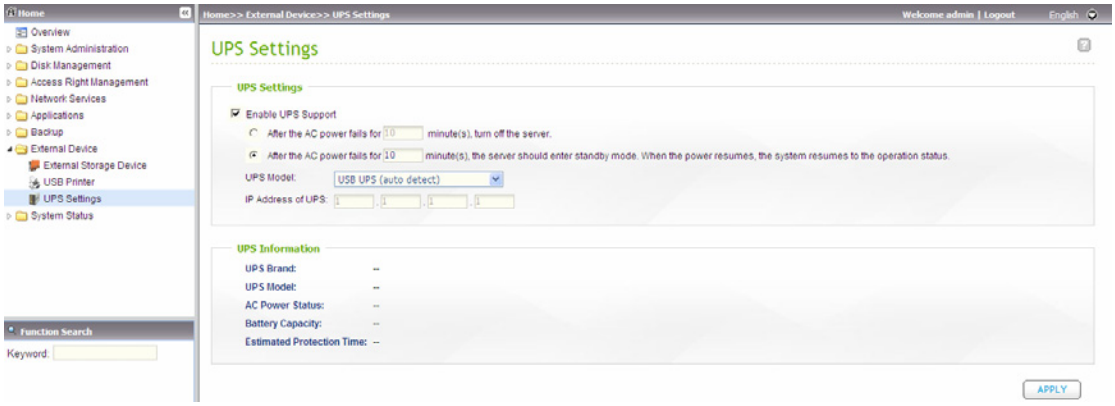


8. After installing the printer driver correctly, you can start to use the printer.



3.7.3 UPS Settings

If your UPS device provides USB interface, you can enable UPS (uninterruptible power supply) support to protect your system from abnormal system shutdown caused by power outage.



✓ **Enable UPS support**

To activate the UPS support, you can select this option. You can set the shutdown timer to turn off the system automatically after the system detects the AC power is abnormal. In general, the UPS can keep supplying the power for the system for about 5-10 minutes, depending on the maximum load of the UPS and the number of the loads connected to it. You may also configure the system to enter standby mode in case of abnormal AC power supply.

✓ **UPS Model**

Select the UPS model from the list. If the UPS model you are using is not available on the list, please contact our technical support.

✓ **IP Address of UPS**

If you have selected APC UPS with SNMP for UPS model, enter the IP address of the UPS.

Note: To allow your UPS device to send SNMP alerts to the QNAP NAS in case of power loss, you may have to enter the IP address of the NAS in the configuration page of the UPS device.

Behaviour of the UPS feature of the NAS:

In case of power loss and power recovery, the events will be logged in the "System Event Logs".

During a power loss, the NAS will wait for the specified time you enter in "UPS Settings" before going into the standby mode or powering off.

If the power is recovered before the end of the waiting time, the NAS will remain in operation and cancel its power-off or standby action. If the power does not recover after the waiting time, the NAS will power off or go into standby mode.

Once the power recovers:

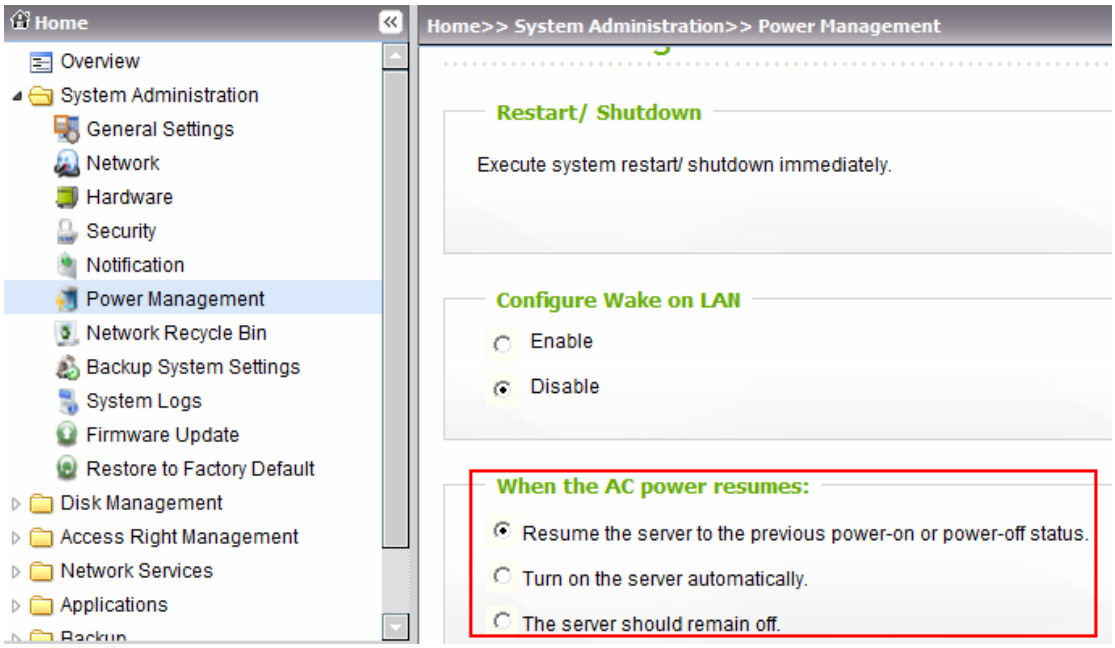
- If the NAS is in standby mode, it will resume to normal operation.
- If the NAS is powered off, it will remain off.

Comparison of the standby mode and the power-off mode

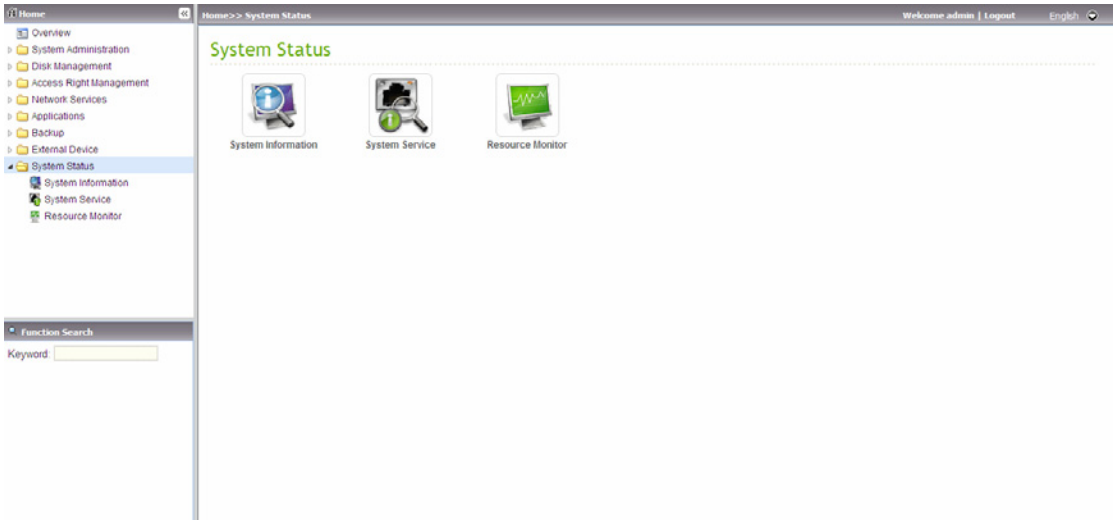
Mode	Advantage	Disadvantage
Standby mode	The NAS resumes after power recovery.	If the power outage lasts until the UPS is turned off, the NAS may suffer from abnormal shutdown.
Power-off mode	The NAS will be shut down properly.	The NAS will remain off after the power recovery. Manual power on of the server is required.

If the power recovers after the NAS has been shut down and before the UPS device is powered off, you may use the Wake on LAN feature to power on the NAS (if your NAS and UPS device both support Wake on LAN and Wake on LAN is enabled on the NAS).

If the power recovers after both the NAS and the UPS have been shut down, the NAS will react according to the settings in "System Administration" > "Power Management".

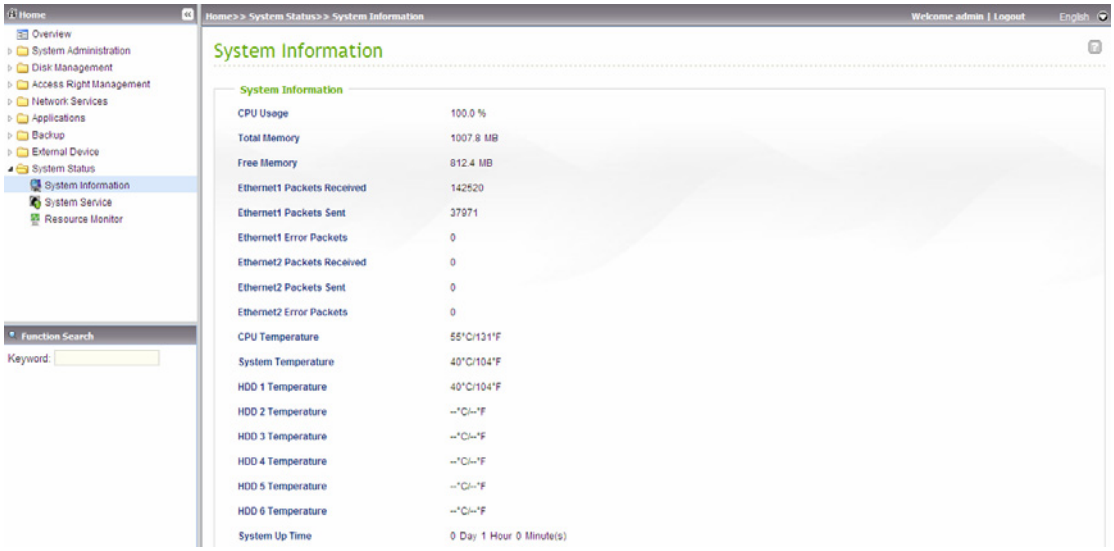

Home
Overview
System Administration
General Settings
Network
Hardware
Security
Notification
Power Management
Network Recycle Bin
Backup System Settings
System Logs
Firmware Update
Restore to Factory Default
Disk Management
Access Right Management
Network Services
Applications
Home>> System Administration>> Power Management
Restart/ Shutdown
Execute system restart/ shutdown immediately.
Configure Wake on LAN
Enable
Disable
When the AC power resumes:
Resume the server to the previous power-on or power-off status.
Turn on the server automatically.
The server should remain off.

3.8 System Status



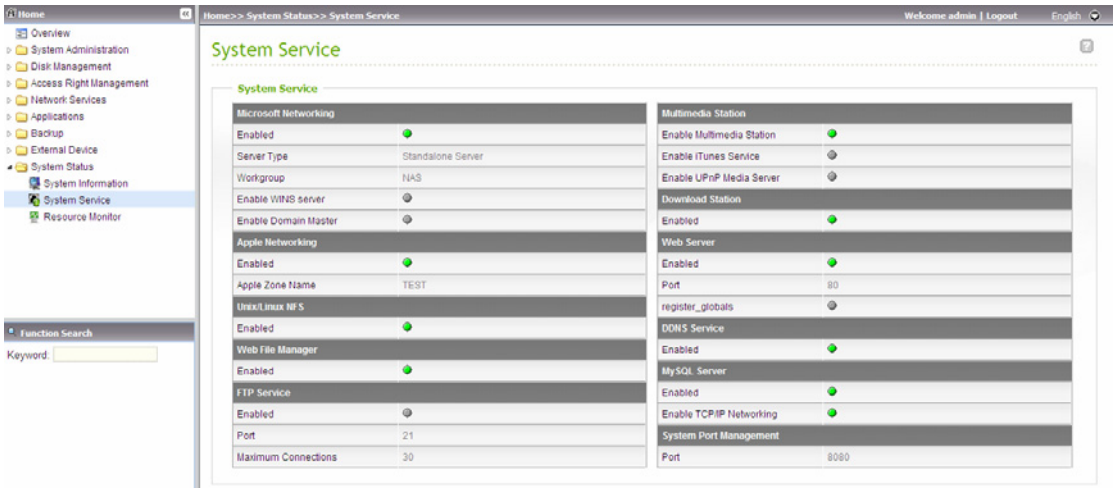
3.8.1 System Information

You can view the system information, e.g., CPU usage and memory on this page.



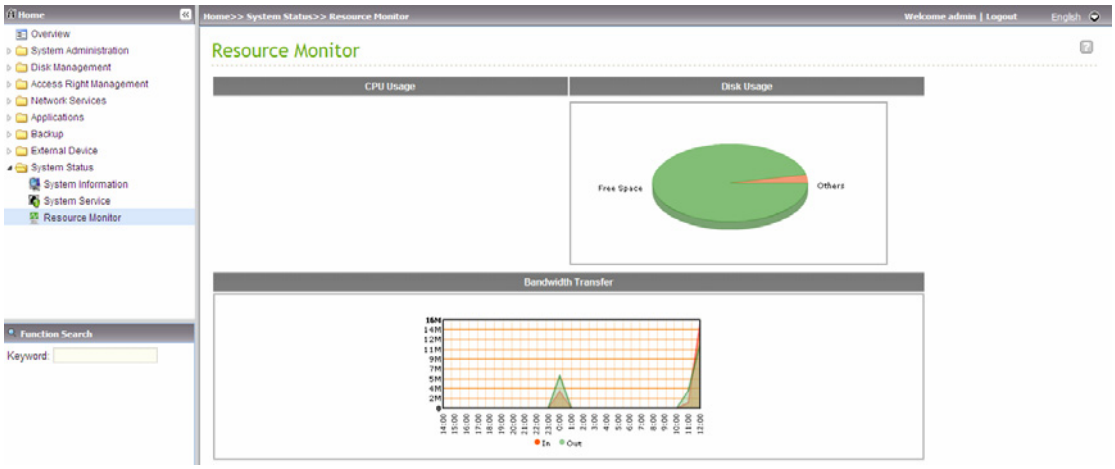
3.8.2 System Service

You can view current network settings and status of the NAS in this section.



3.8.3 Resource Monitor

You can view the CPU usage, disk usage, and bandwidth transfer statistics of the NAS on this page.

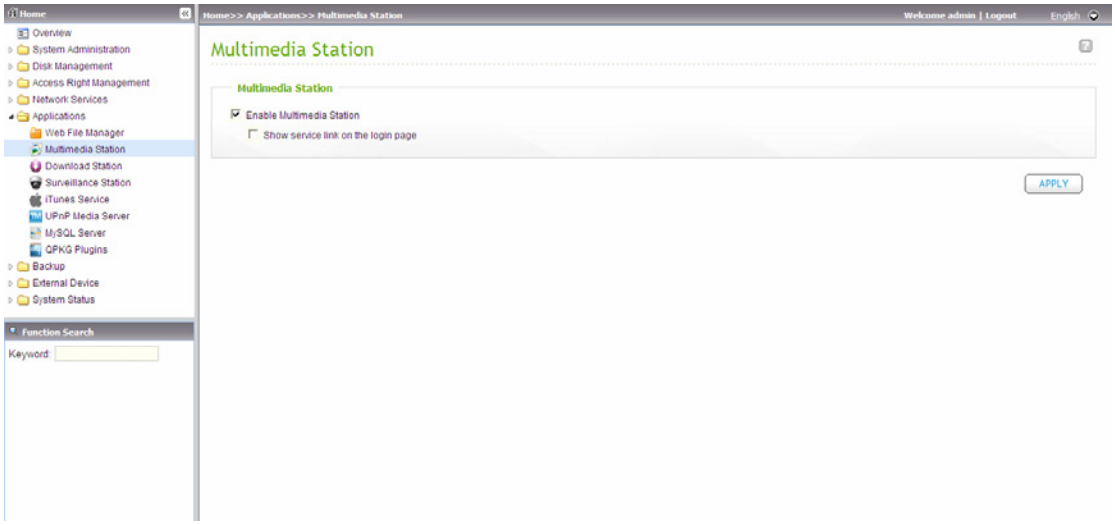


Chapter 4 Multimedia Station

The NAS provides a user-friendly web management interface for you to manage personal albums easily. You can view images and multimedia files, or browse photos by thumbnails preview.

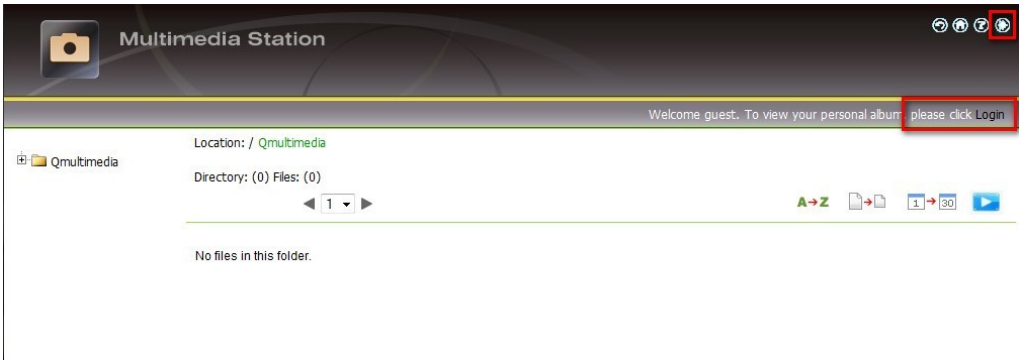
Upload photos by web administration

1. Go to "Applications" > "Multimedia Station". Enable the service.

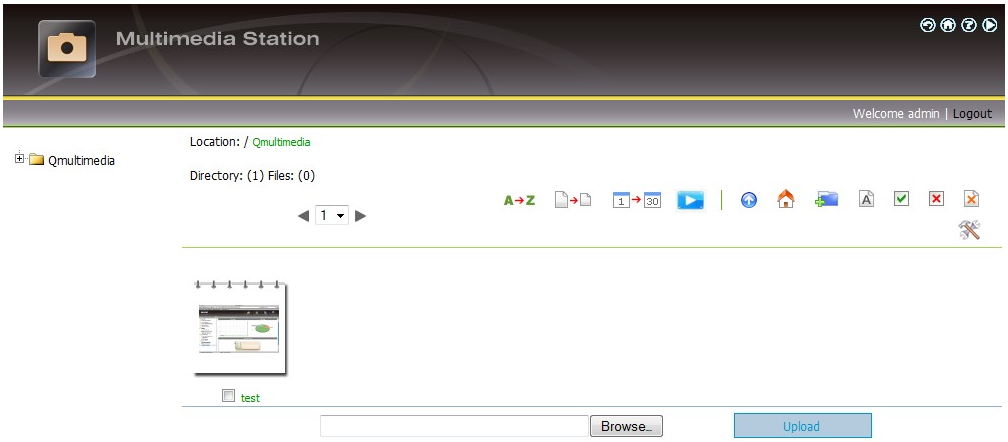


2. Click "Multimedia Station" on the top or on the login page of the NAS to access the Multimedia Station. If you login the service from the login page of the NAS, you are required to enter the user name and password.

3. Click "Login" on the top right hand corner. Login with administrator name and password to manage the Multimedia Station. You can create user accounts to allow the users to access the multimedia files.



4. Click "Browse" to select the multimedia file and then click "Upload" to upload the file to the folder.



5. You can also create folders by clicking  and upload the files to the folders.

Upload the photos to the share folder of the NAS directly

You can upload multimedia files to the NAS directly by the following steps.

1. Open the Windows Run menu. Enter \\[server name] or \\[server IP] to access share folder on the NAS.

2. Open the folder Qmultimedia/ Multimedia. Enter the user name and password to login.

3. Drag the files and folders to the folder directly. Please wait patiently when the NAS is generating thumbnails for images during uploading.

When you login Multimedia Station by web browser again, all the multimedia files will be shown.

Buttons on the Multimedia Station page

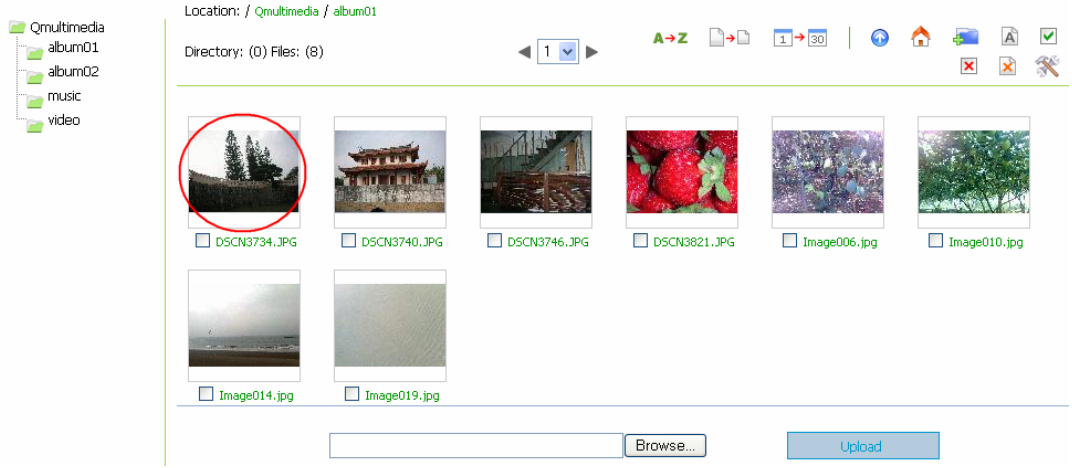
	Sort files by name
	Sort files by size
	Sort files by date
	Return to previous page
	Return to Home
	Create folder
	Rename file or folder
	Select all
	Select none
	Delete

Support file format list

Type	File format
Picture	jpg, bmp, gif
Video 	wmv, wmx, wvx, avi, mpeg, mpg, mpe, m1v, mp2, mpv2, mp2v, mpa, dvr-m, asf, asx, wpl, wm, wmx, wmd, wmz
Audio 	wma, wax, cda, wav, mp3, m3u, mid, midi, rmi, aif, aifc, aiff, au, snd
Others 	(Other formats not mentioned above)

View Photo Information

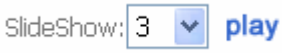
1. To view detailed information of a photo, click the thumbnail of the picture.



2. The information of the photo, e.g. file name, resolution, size, camera producer will be shown on the right. You can enter a description for the picture in the box below the photo and click "Submit". To reset the description to previously saved version, click "Reset".

Buttons Description

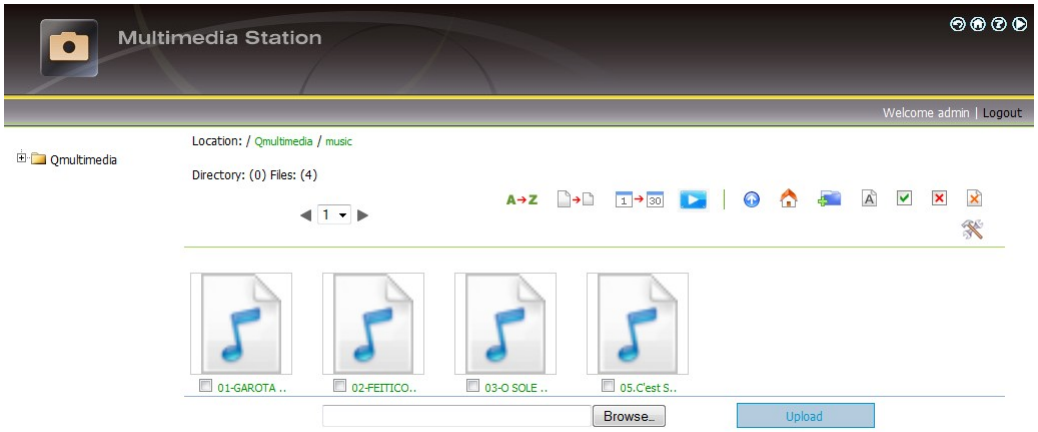
You can use the buttons on top of the photo to manage the album.

	Back to previous level
	Previous image
	Next image
	Rotate image anticlockwise
	Rotate image clockwise
	Zoom in
	Zoom out
	Play slideshow. Select the time interval in seconds. Click "play" to play slide show. To stop playing, click "stop".
	Print the image
	Save the picture
	Set the picture as album cover

Play music or video files

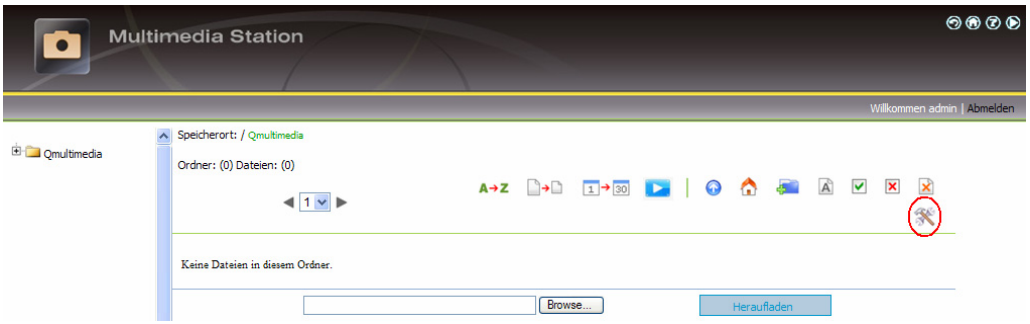
To play music or video files on the Multimedia Station, you can click the thumbnail of the file displayed on the page. The file will be played by the default music or video playing program of your PC.

*It is recommended to use Windows Media Player 10.0 or above as the default playing program.

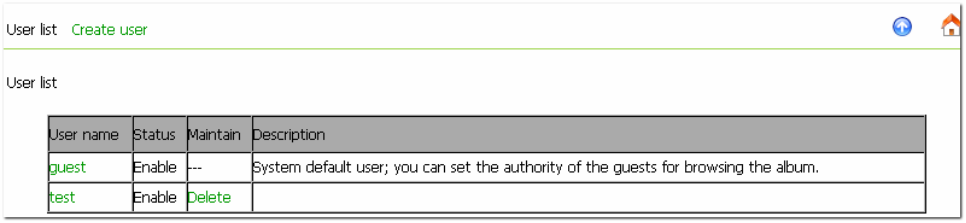


Configure album authority

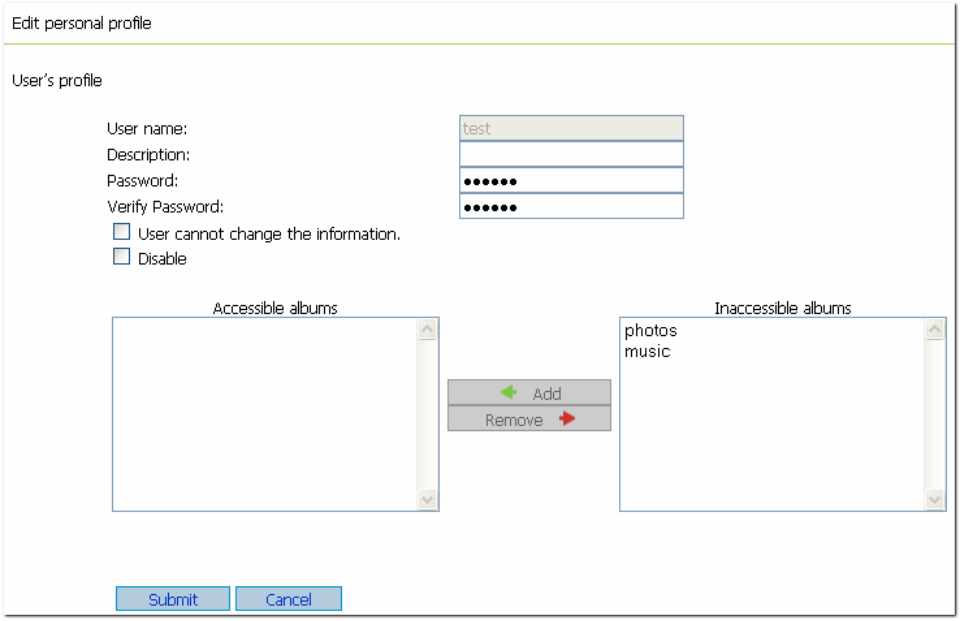
1. After logging in as administrator (admin), click  to enter the configuration page for album authority.



2. You can view, add, delete, and edit users.



3. You can edit the user profile and album access authority on this page.

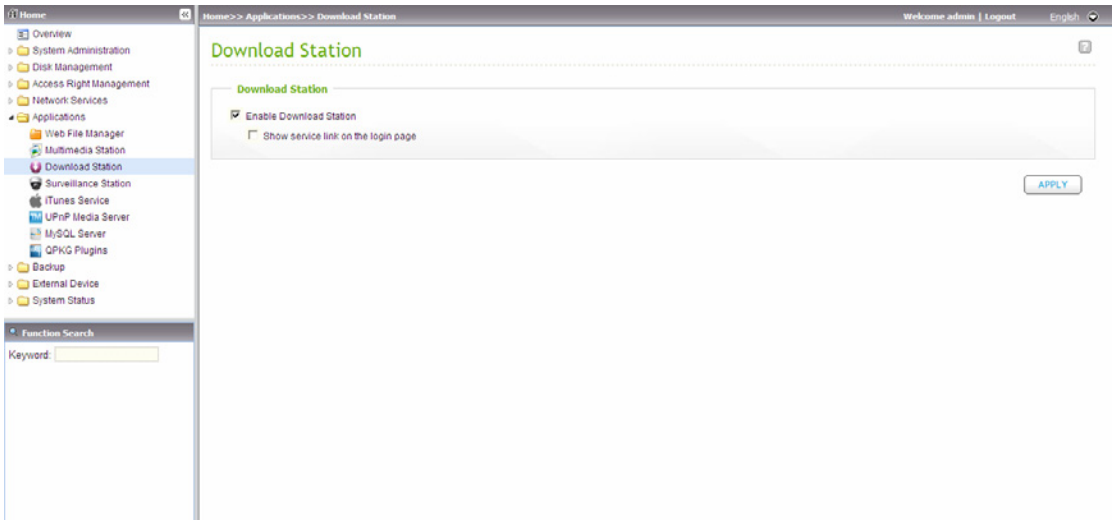


Chapter 5 Download Station

The NAS supports BT, HTTP, and FTP download. You can add download task to the NAS and let the server finish downloading independent of PC.

!	**Warning:** Please be warned against illegal downloading of copyrighted materials. The Download Station functionality is provided for downloading authorized files only. Downloading or distribution of unauthorized materials may result in severe civil and criminal penalty. Users are subject to the restrictions of the copyright laws and should accept all the consequences.

1. Go to "Applications" > "Download Station". Enable the service.

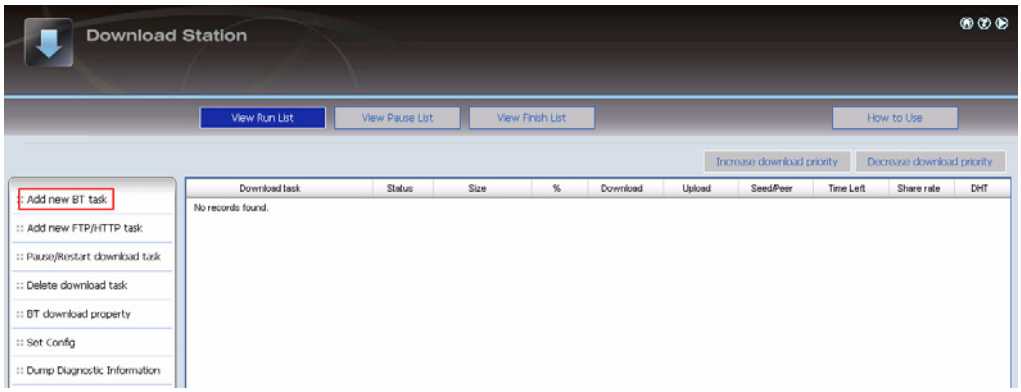


2. Click "Download Station" on the top or on the login page of NAS to access the Download Station. If you login the service from the login page of the NAS, you are required to enter the user name and password.

3. Select “Add new BT task” or “Add new FTP/HTTP task”.

(A) Add a new BT task

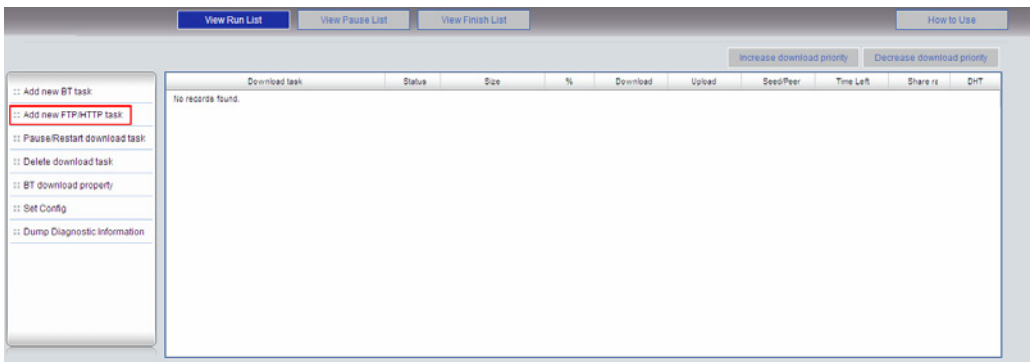
Click “Add new BT task” on the left and upload a torrent file. You can download legal torrent files by searching on the Internet. There are websites that provide legally sharing torrents e.g. www.legaltorrents.com. Please download the torrent files to your local disk and then upload them to the NAS.



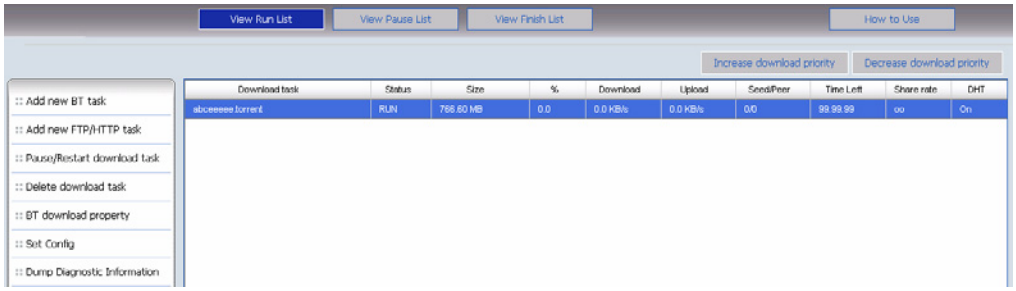
(B) Add a new FTP/HTTP task

To run an FTP download task, click “Add new FTP/HTTP task”. Enter the FTP URL of the download task and select the share folder to save the files. Enter the user name and password to login the FTP server (if necessary). Then click “OK” to start downloading.

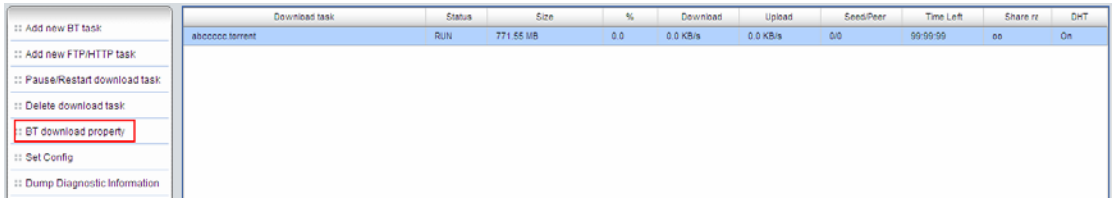
To run an HTTP download task, click “Add new FTP/HTTP task”. Enter the HTTP URL of the download task and select the share folder to save the files. Then click “OK” to start downloading.



4. After uploading a download task, the task will appear on “View Run List”.

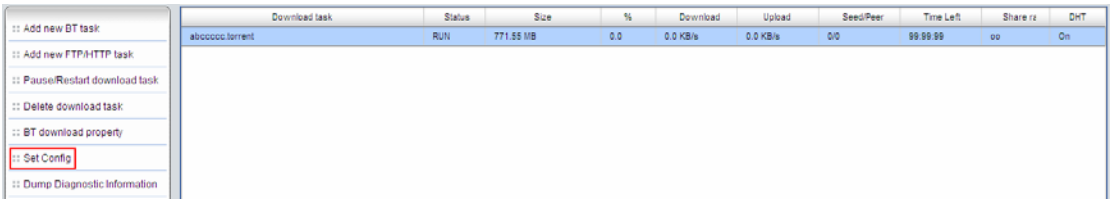


5. You can select a download task and click “BT download property” to enable or disable the DHT public network and configure the sharing time after download completes.



Note: If the sharing time (larger than 0 hr) is set for a download task, the download task will be moved to “Finish List” after download completes and the sharing time ends.

6. Click “Set Config” and enter the number of the maximum tasks you want to download at the same time (Default number: 3).
   Enter the maximum download rate (default value is 0, which means unlimited).
   Enter the maximum upload rate (default value is 0, which means unlimited).
   Enter the port range for Download Station (default range is 6881-6999).
   Check UPnP NAT port forwarding to enable automatically port forwarding on UPnP supported gateway (default is not checked).

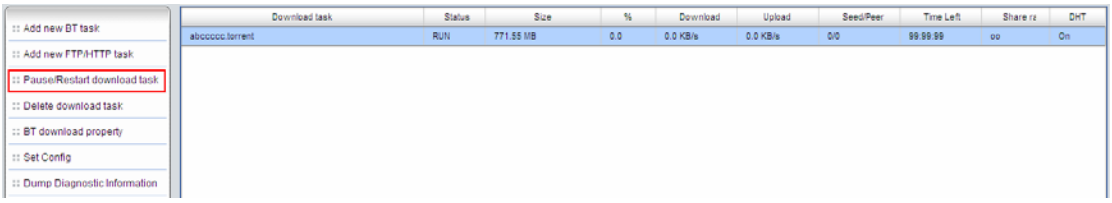


Protocol Encryption

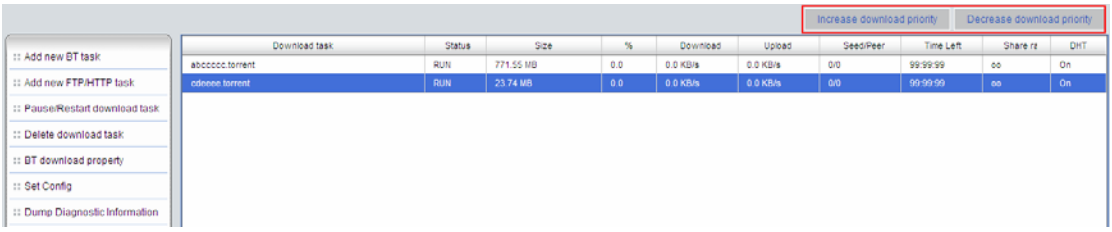
There are a number of Internet Service Providers (ISP) block or throttle BitTorrent connections for the high bandwidth it generates. By turning on “Protocol Encryption” your connections will not be distinguished by these ISPs as BitTorrent connections therefore are unable to block or throttle them and causing slow connections or even no connections. However some ISPs are starting to be able to identify these connections even if they were encrypted so users are suggested to check the Bad ISPs list on AzureusWiki and to consider switching to an ISP that does not perform BitTorrent traffic throttling or blocking.

You can set the download schedule in “Download time settings”. Select “Continuous download” to download the files continuously. To specify the download schedule, select “Daily download time” and enter start and end time. If the end time value is smaller than the start time, the end time will be treated as the time on the next day.

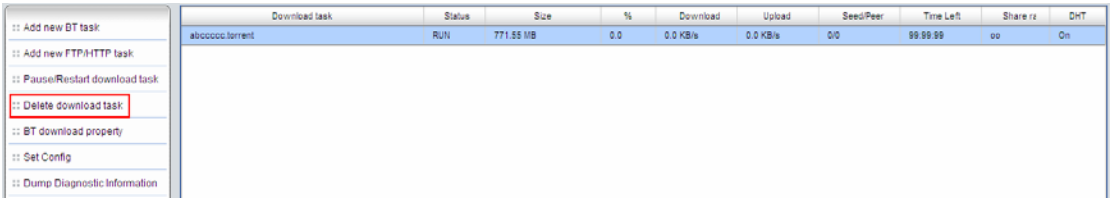
7. To pause a running download task, select the task in View Run list and click "Pause/ Restart download task". You can view tasks that are paused or finished in View Pause List and View Finish List respectively. To restart a paused task, select the task in View Pause List and click "Pause/ Restart download task".



8. You can also increase or decrease task priority by clicking "Increase download priority" and "Decrease download priority" when there are multiple download tasks.



9. To delete a running, paused, or finished task, select the task and click "Delete download task". You can select to remove the download task only and retain the downloaded files, or remove the task and downloaded files.

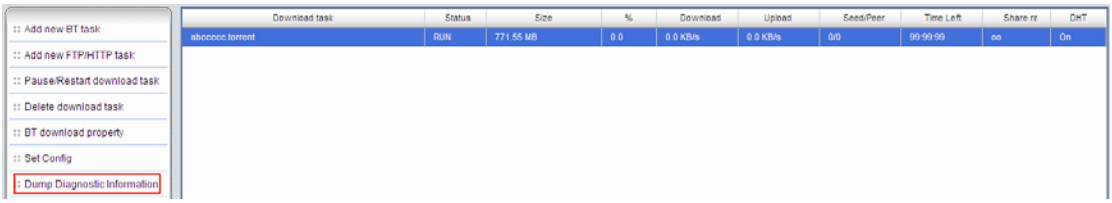


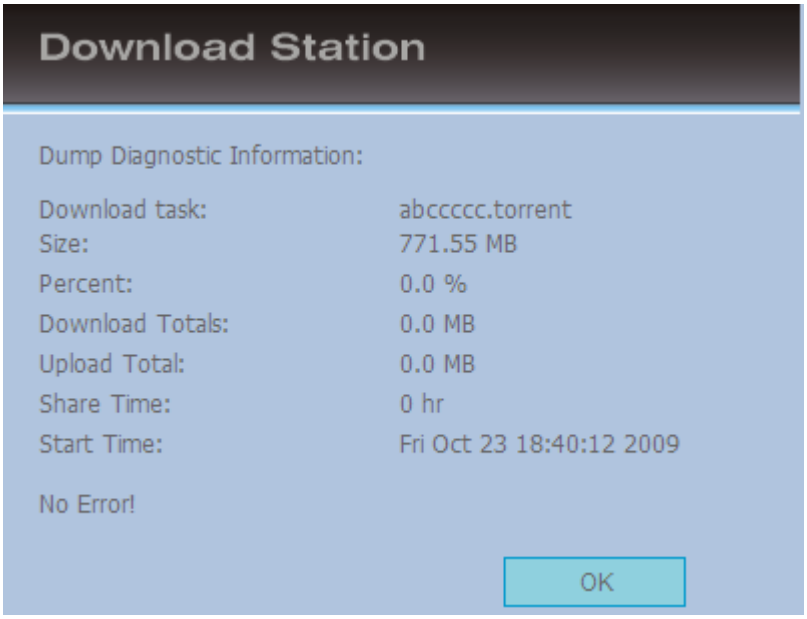
10. To logout Download Station, click  on the top right hand corner.

11. To access the folders you have downloaded, please go to the share folder Qdownload/ Download of the NAS.

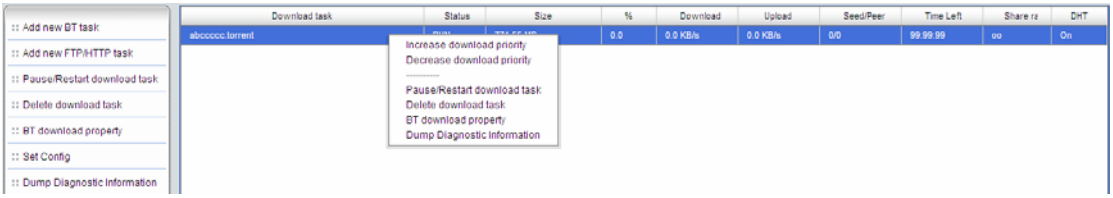
Dump Diagnostic Information

To view the diagnostic details of a download task, select a task on the list and click "Dump Diagnostic Information".





You can right click the download task to configure the download settings.



The common reasons for slow BT download rate or download error are as below:

(1) The torrent file has expired, the peers have stopped sharing this file, or there is error in the file.

(2) The NAS has configured to use fixed IP but DNS server is not configured, or DNS server fails.

(3) Set the maximum number of simultaneous downloads as 3-5 for the best download rate.

(4) The NAS is located behind NAT router. The port settings have led to slow BT download rate or no response. You may try the following means to solve the problem:

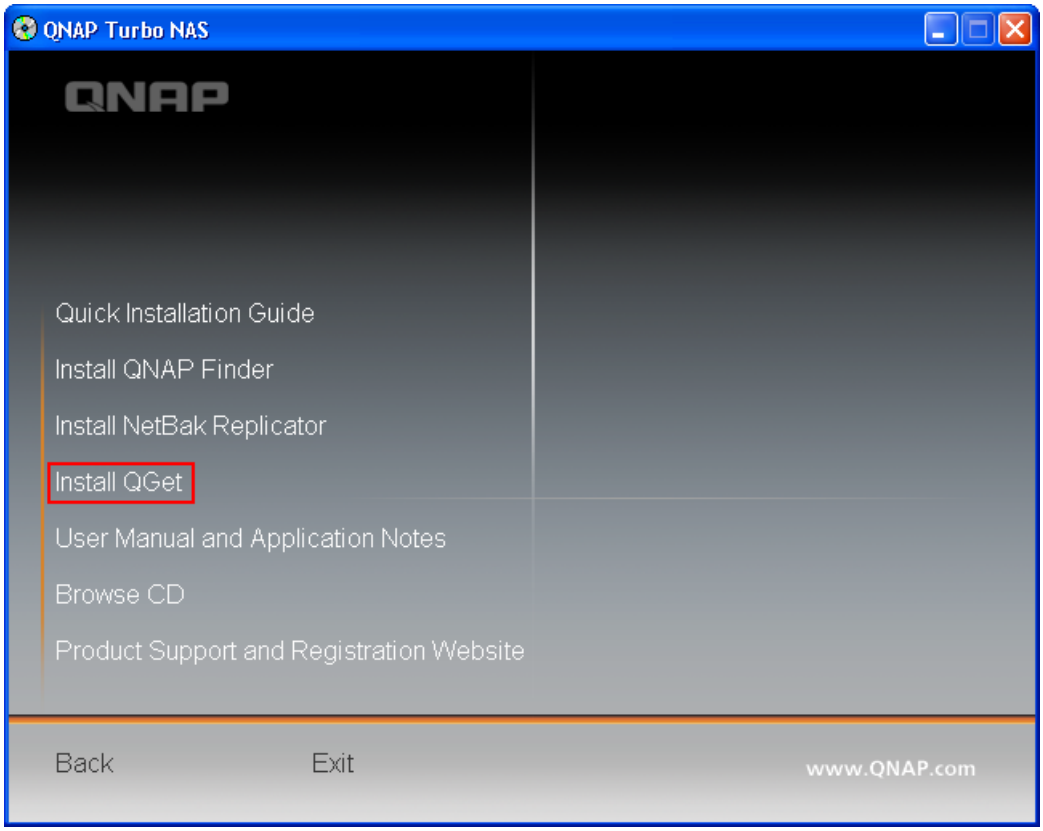
   a. Open the BitTorrent port range on NAT router manually. Forward these ports to the LAN IP of the NAS.

   b. The new NAS firmware supports UPnP NAT port forwarding. If your NAT router supports UPnP, enable this function on the NAT. Then enable UPnP NAT port forwarding of the NAS. The BT download rate should be enhanced.

5.1 Use Download Software QGet

QGet is a powerful management software for maintaining the BT, HTTP and FTP download tasks of multiple NAS servers via LAN or WAN. By using QGet, you no longer need to login the Download Station web interface of multiple servers and manage the settings one by one. Simply install QGet on any computer running Windows 2000/ XP/ Vista/ Windows 7 or Mac, you can manage the download tasks of all your NAS servers.

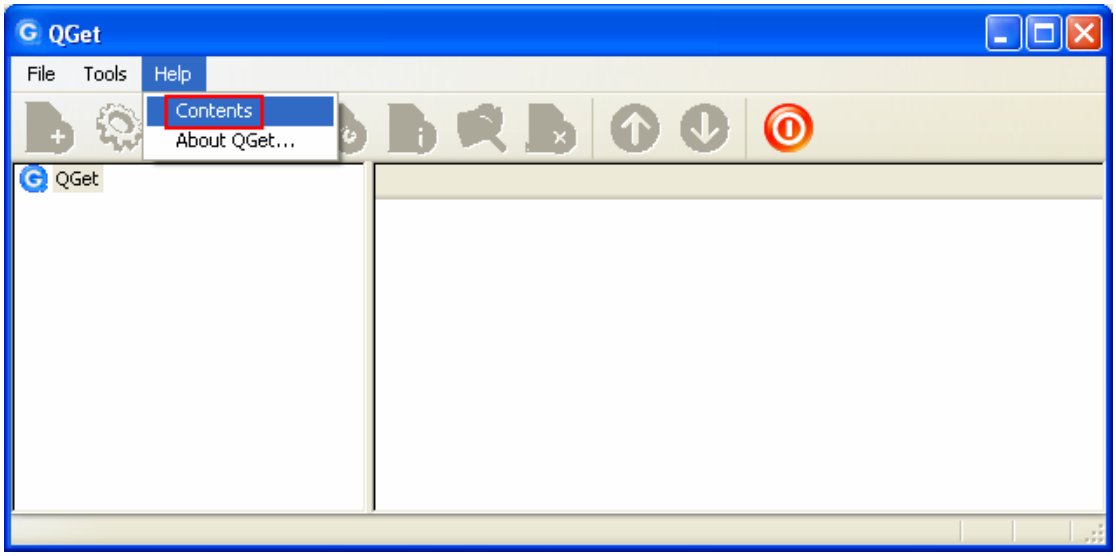
1. To use QGet, install the software from the product CD-ROM.



2. Follow the instructions to install QGet.

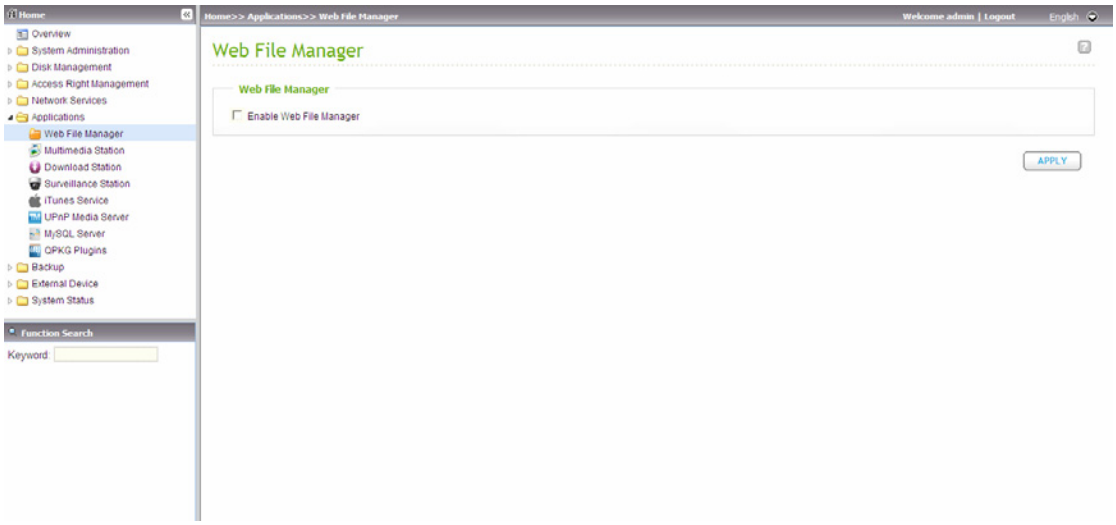
3. Run QGet from the installed location.

4. For the details of using QGet, please refer to the online help of the software.



Chapter 6 Web File Manager

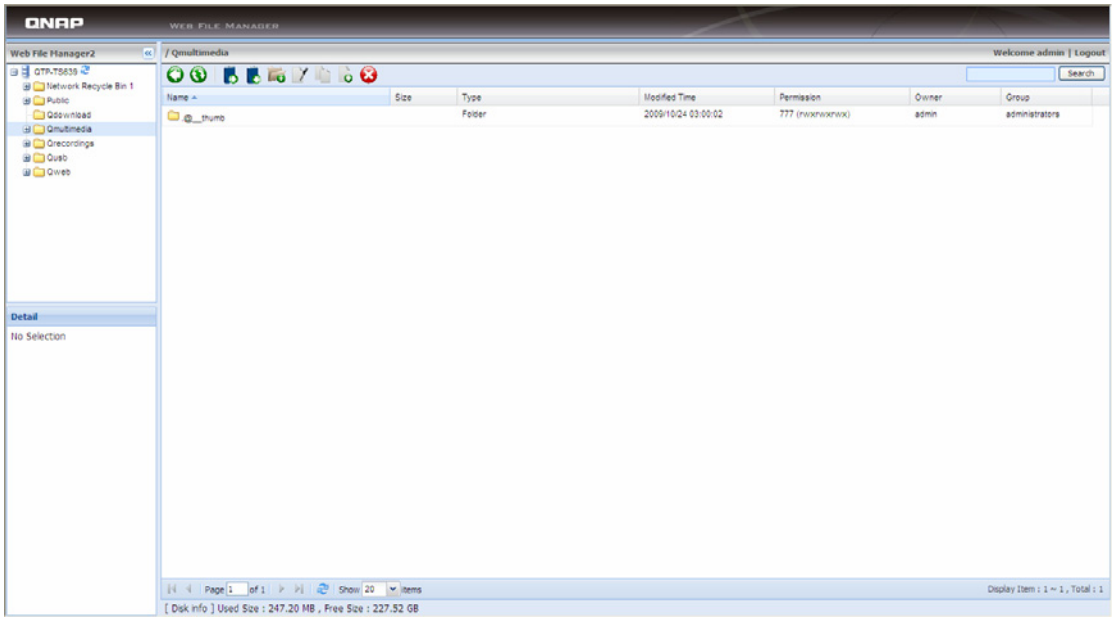
To use Web File Manager, go to “Applications” > “Web File Manager”. Enable the service.



Click “Web File Manager” on the top or on the login page of the NAS to access the Web File Manager. If you login the service from the login page of the NAS, you are required to enter the user name and password.

Note: Make sure a network share has been created before using Web File Manager.

You can organize network share folders of the NAS. With Web File Manager, you can upload, download, rename, move, copy, or delete files and folders in the network shares.



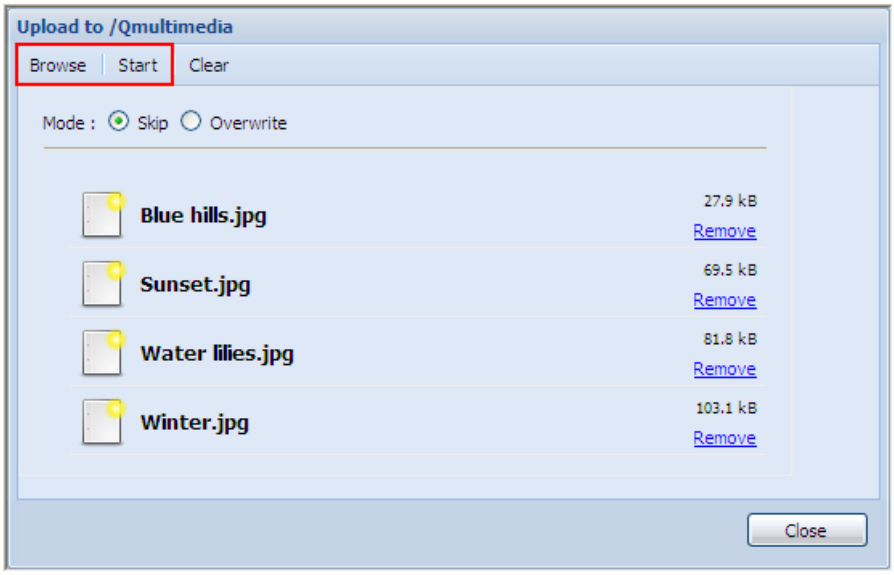
Upload file

To use this feature, please install Adobe Flash plugin for your web browser.

i. Open the folder to upload file to. Click  .

ii. Click "Browse" to select the file(s).

iii. Select to skip or overwrite existing file in the folder.



iv. Click "Start".

Download file

i. Select a file or folder to download.

ii. Right click the mouse and select "Download" or click  to download the file.

Create folder

i. Select a network share or folder in which you want to create a new folder.

ii. Click  (Create Folder).

iii. Enter the name of the new folder and click "OK".

Rename file or folder

i. Select a file or folder to rename.

ii. Click  (Rename).

iii. Enter the new file or folder name and click "OK".

Copy files or folders

i. Select the files or folders to copy.

ii. Click  (Copy).

iii. Select the destination folder.

iv. Select to skip or overwrite the existing file in the destination folder. Click "OK".

Move files or folders

i. Select the files or folders to move.

ii. Click  (Move).

iii. Select the destination folder.

iv. Select to skip or overwrite the existing file in the destination folder. Click "OK".

Delete file or folder

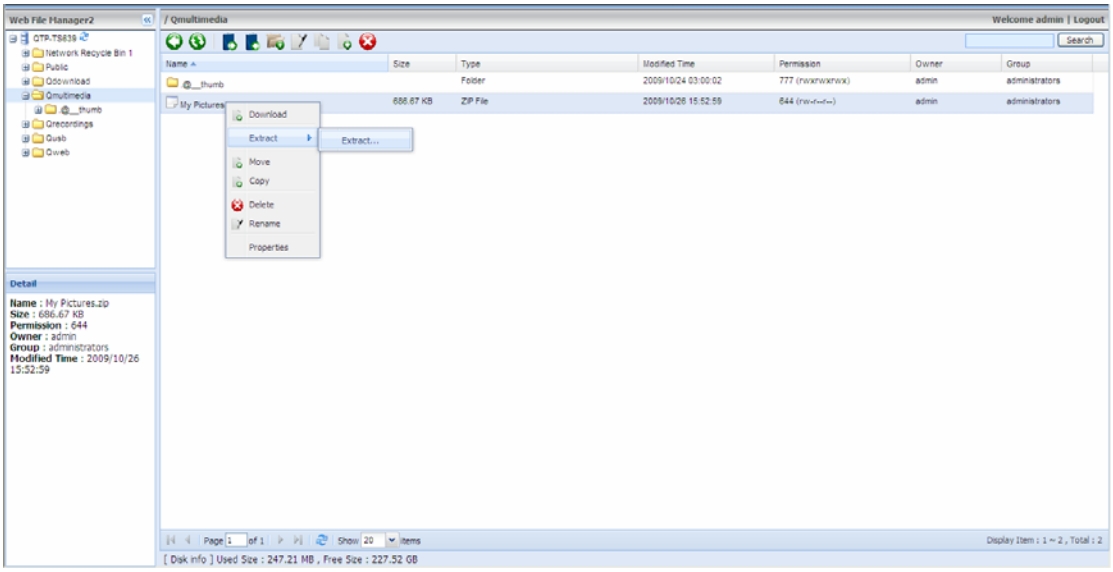
i. Select a file or folder to delete.

ii. Click  (Delete) on the toolbar.

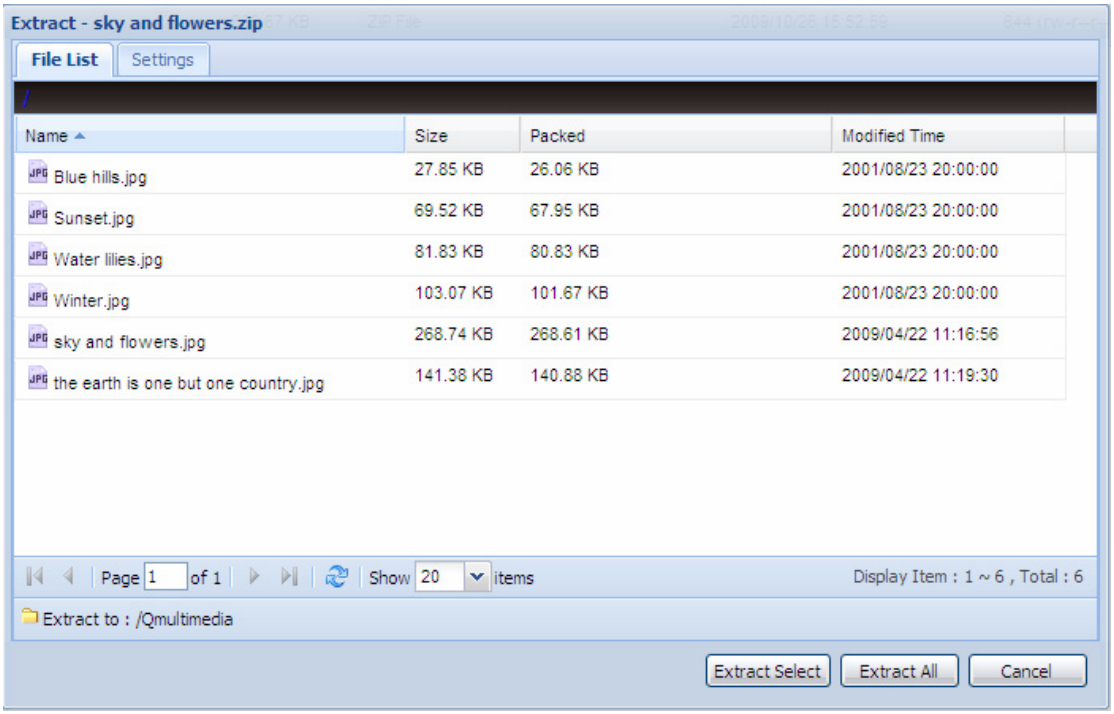
iii. Confirm to delete the file or folder.

Extract files

i. To extract a zipped file on the NAS, right click the zipped file and select "Extract".



ii. Select the files to extract and configure the extraction settings.



Chapter 7 NetBak Replicator

The NetBak Replicator is a powerful program installed in the user's system (Windows® OS only) for data backup. You can back up any files or folders on the local PC to the share folders on the NAS over LAN or WAN.

Main Functions

1. Backup

- Instant Backup
  You can select the files and folders on the local PC and back up the files to the network share folder on the NAS immediately.

- File Filter
  You can select particular file types to be excluded from backup. The system will filter all the specified file types when backing up data.

- Schedule
  You can specify a schedule for backing up the data with this option, e.g. 12:00 every day or 05:00 every Saturday.

- Monitor
  When this option is enabled, the system will upload all the files or folders to the server instantly for backup when the files or folders are modified.

2. Restore

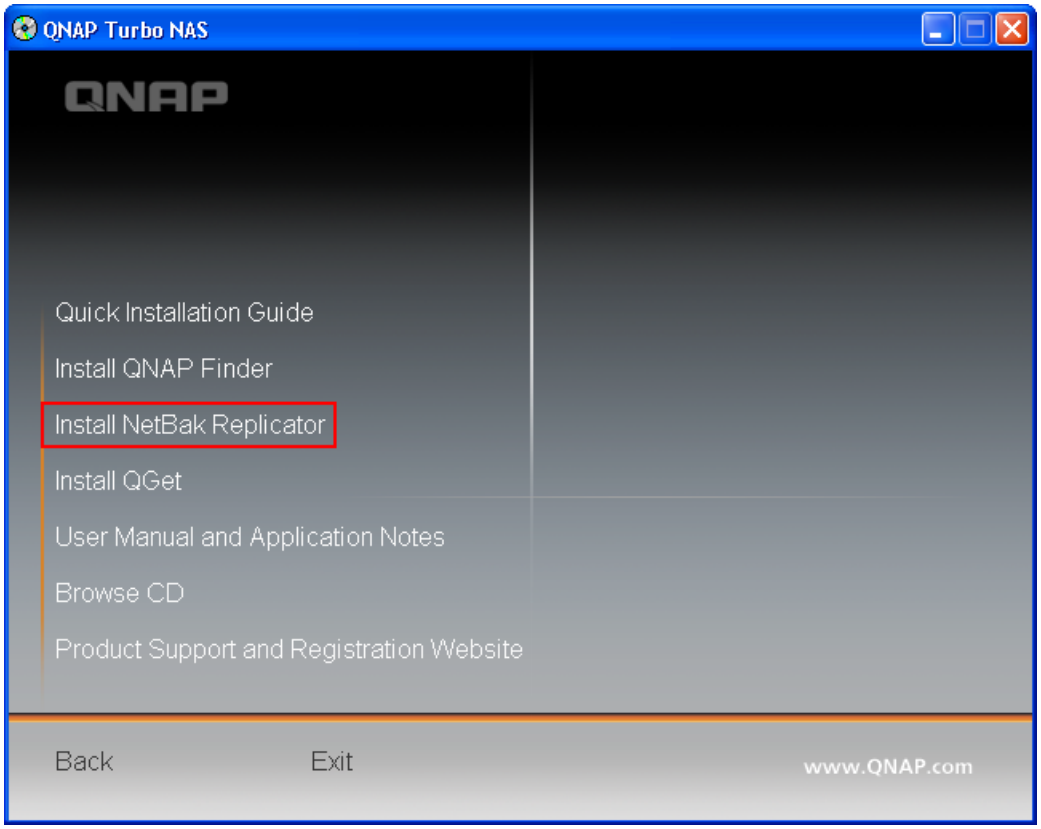
Select this option to restore the backup data to the original location of the file or to a new directory.

3. Log

Enable this option to record the events of NetBak Replicator, e.g. the time when NetBak Replicator starts and terminates.

Install NetBak Replicator

1. Run the NAS CD-ROM. Select "Install NetBak Replicator".



2. Follow the steps to install NetBak Replicator.

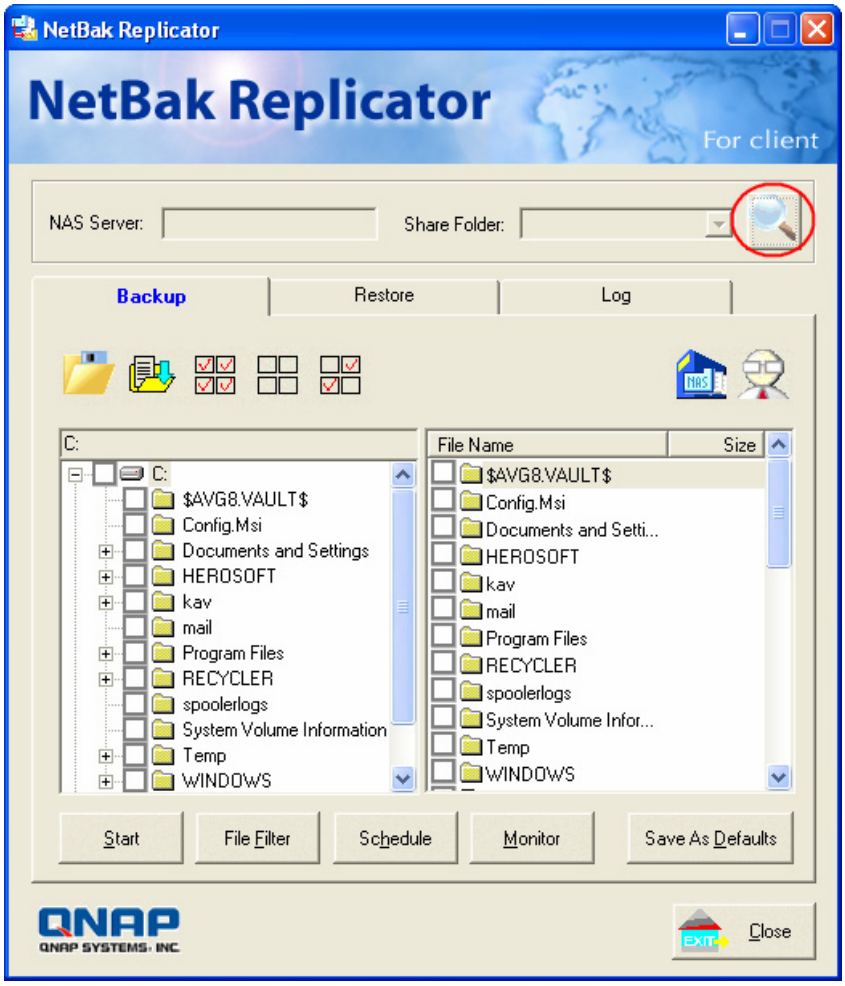
3. Upon successful installation, a shortcut icon 

will be shown on the Desktop. Double click the icon to run NetBak Replicator.

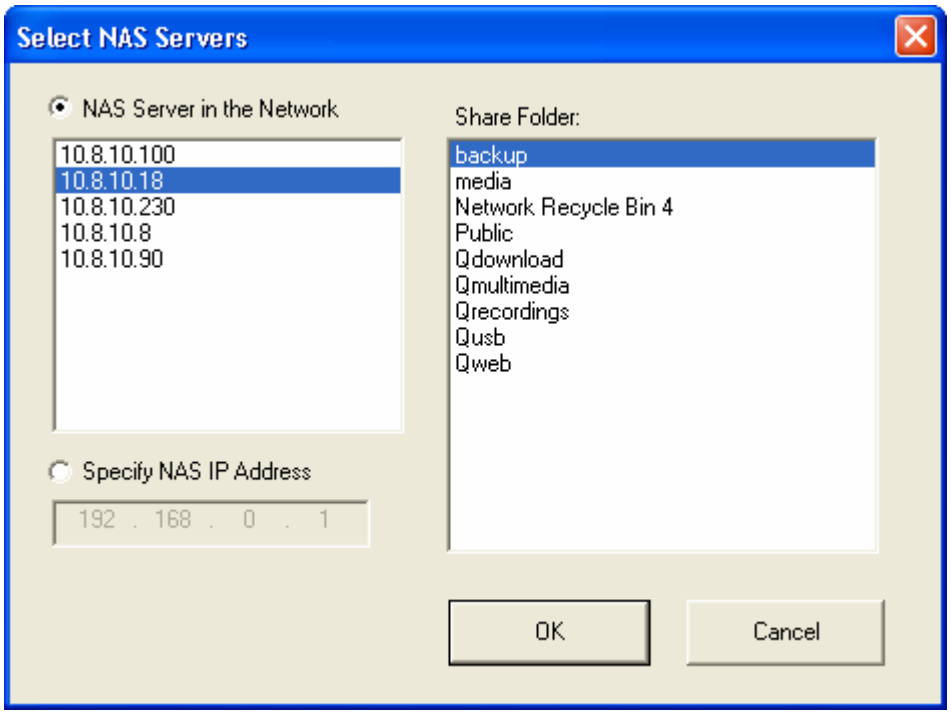
Use NetBak Replicator

1. Before using NetBak Replicator, please login the web administration page of the NAS and go to "Access Right Management" > "Share Folders" to create a share folder for backup. Make sure the share folder is open for everyone access or you login the share folder with an authorized account by NetBak Replicator.

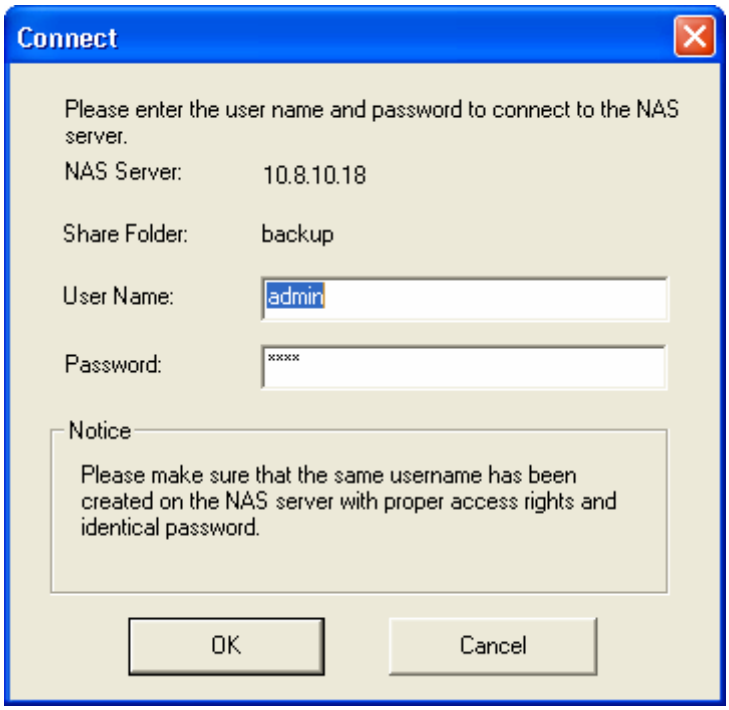
2. Run NetBak Replicator. Click  . All the NAS and their share folders on the local network will be displayed.



3. When the following window appears, all the NAS on the LAN will appear on the left list. Select a server and a share folder on the right. NetBak Replicator also supports backup over WAN, enter the IP address of the NAS for data backup directly and select a share folder. Then click "OK".



4. Enter the user name and password to login the server.



5. You can start the backup procedure upon successful connection to the NAS.

Description of Buttons on NetBak Replicator

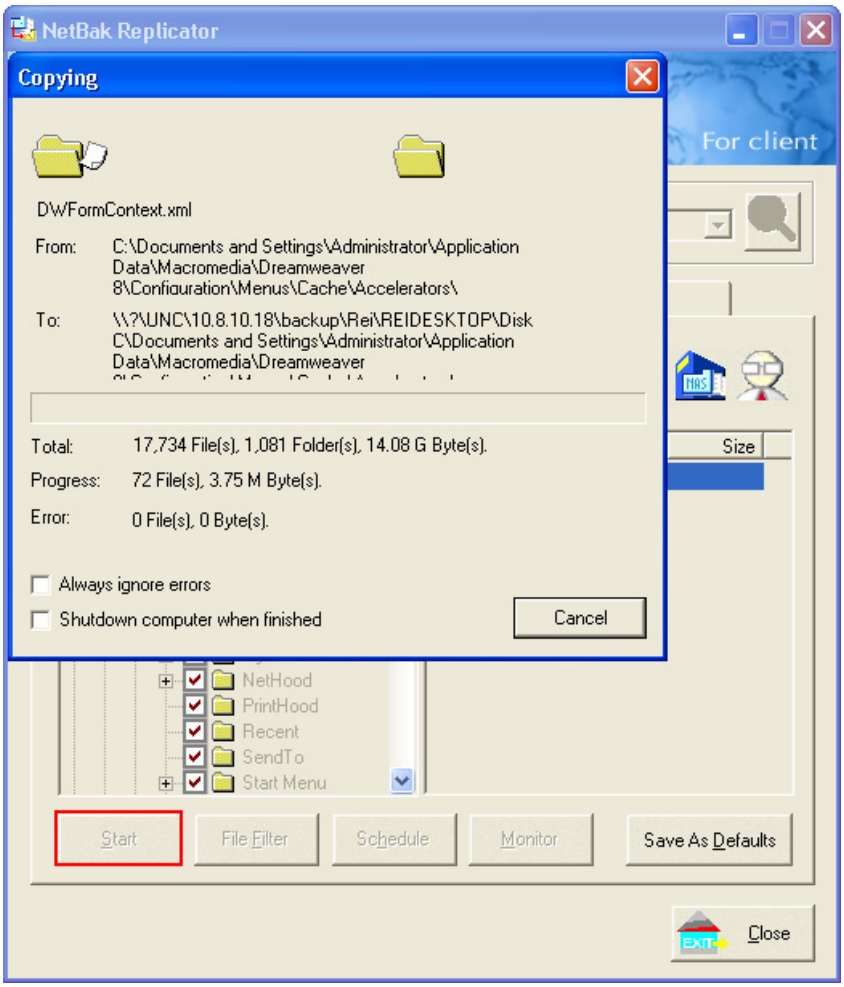
	Open Configuration: Open a previously saved NetBak Replicator configuration.
	Save Configuration: Save the settings on NetBak Replicator. The file will be named as *.rpr
	Select All: Select all the items in the window.
	Clear All: Clear the selection.
	Select My Document: Select all the folders in My Document.
	Open NAS Backup Folder: This button allows the users to find out where the files were backed up, and check or manage the archived files manually.
	Advanced Backup: Advanced Backup allows the power users to back up a single folder with more advanced options.

- **Backup**

  Select the files and folders for backup.

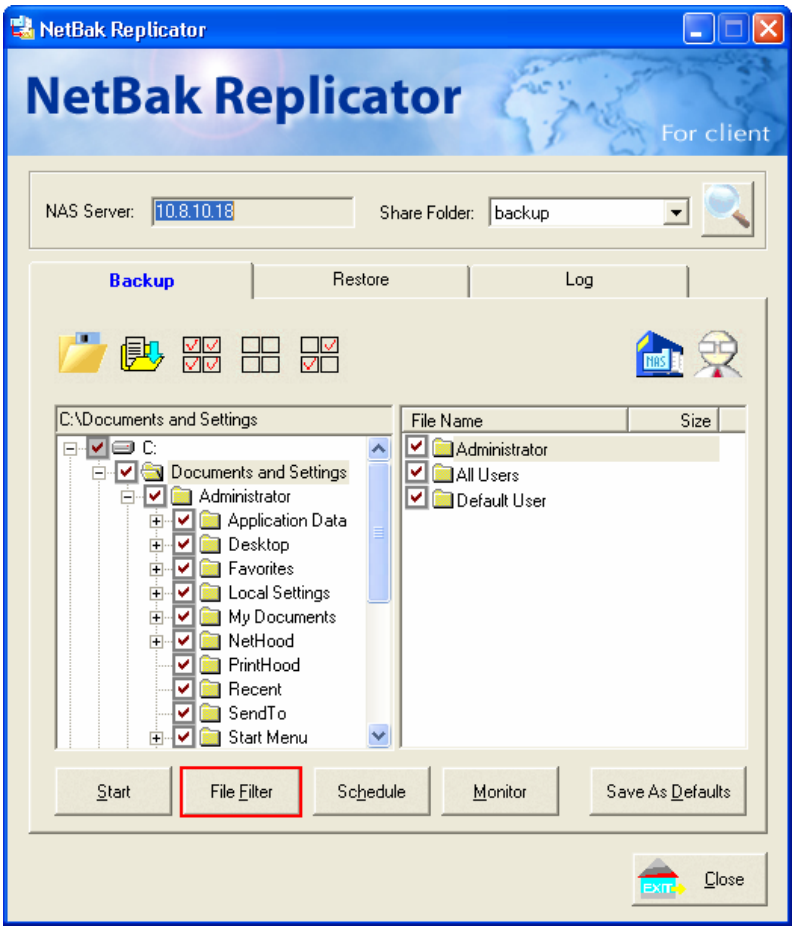
✓ Start

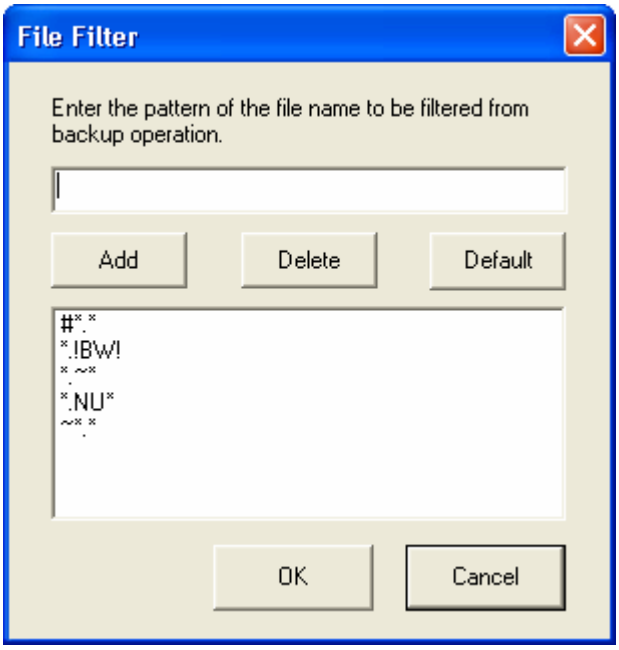
When you have selected the files for backup to the NAS, click "Start". The program will start to copy the selected files to the specified share folder on the NAS.



✓ File Filter

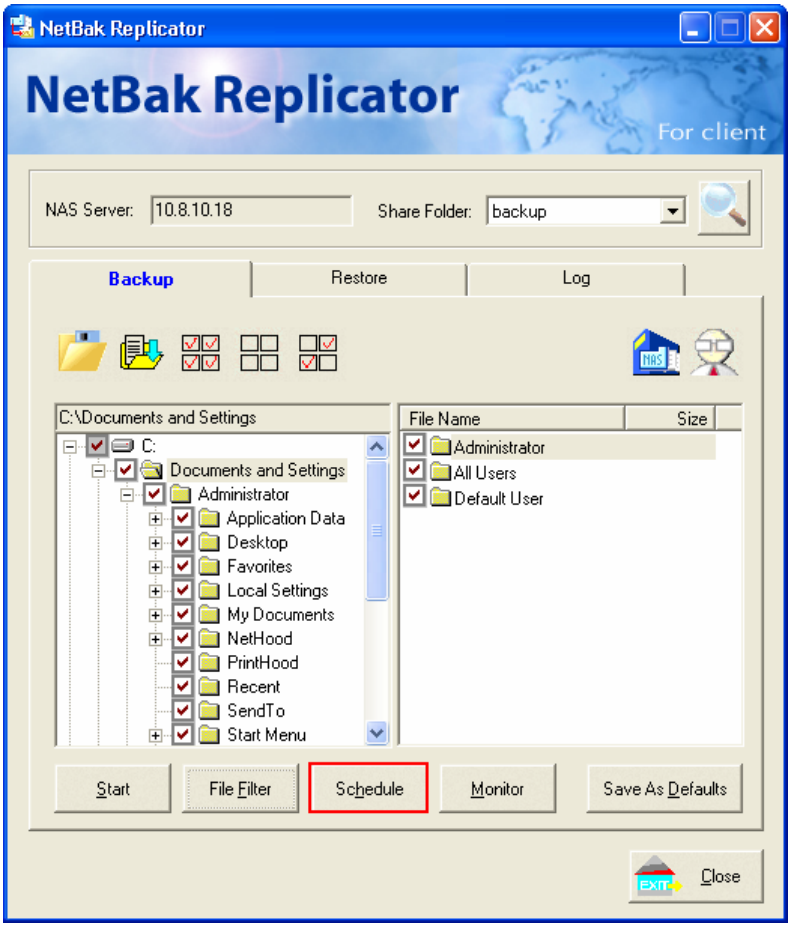
Click "File Filter" on NetBak Replicator main page to select file format to be skipped from backup. Then click "OK".

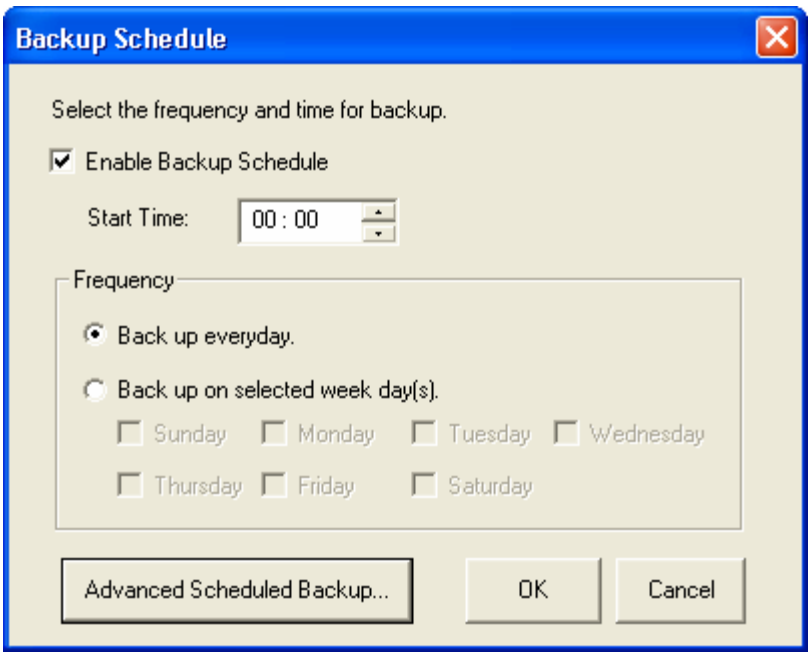




✓ Schedule

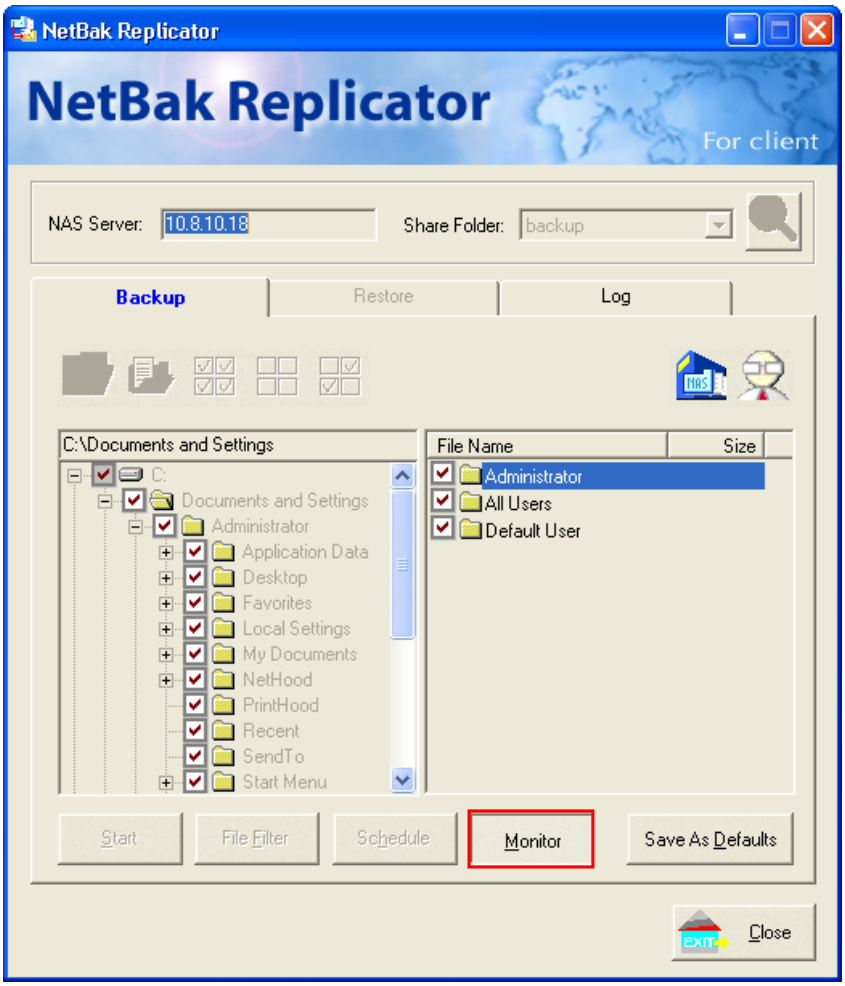
Click “Schedule” on the main page of NetBak Replicator. Then check the box “Enable Backup Schedule” and select the frequency and time for backup. Click “OK” to confirm.




Backup Schedule
Select the frequency and time for backup.
Enable Backup Schedule
Start Time:
00 : 00
Frequency
Back up everyday.
Back up on selected week day(s).
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Advanced Scheduled Backup...
OK
Cancel

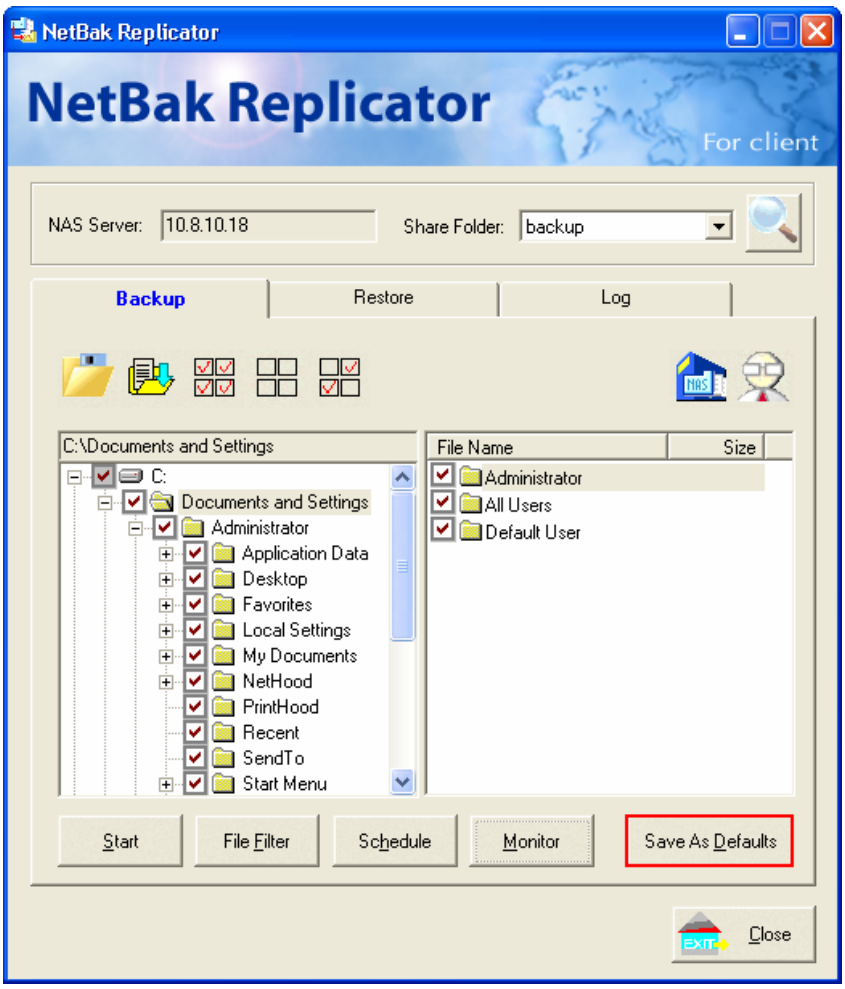
✓ Monitor

Select a folder for monitoring. When this option is enabled, the system will upload all files or folders to the server instantly for backup when the files or folders are modified. Other files will be gray and cannot be selected. Click "Monitor" again to cancel monitoring. An icon will appear on task bar of Windows® when monitoring is in process.



✓ Initialize Configuration

When using this function, NetBak Replicator will record all the current settings of the user, including whether or not the monitoring function is enabled. When the user login again, this program will load the previous recorded settings.



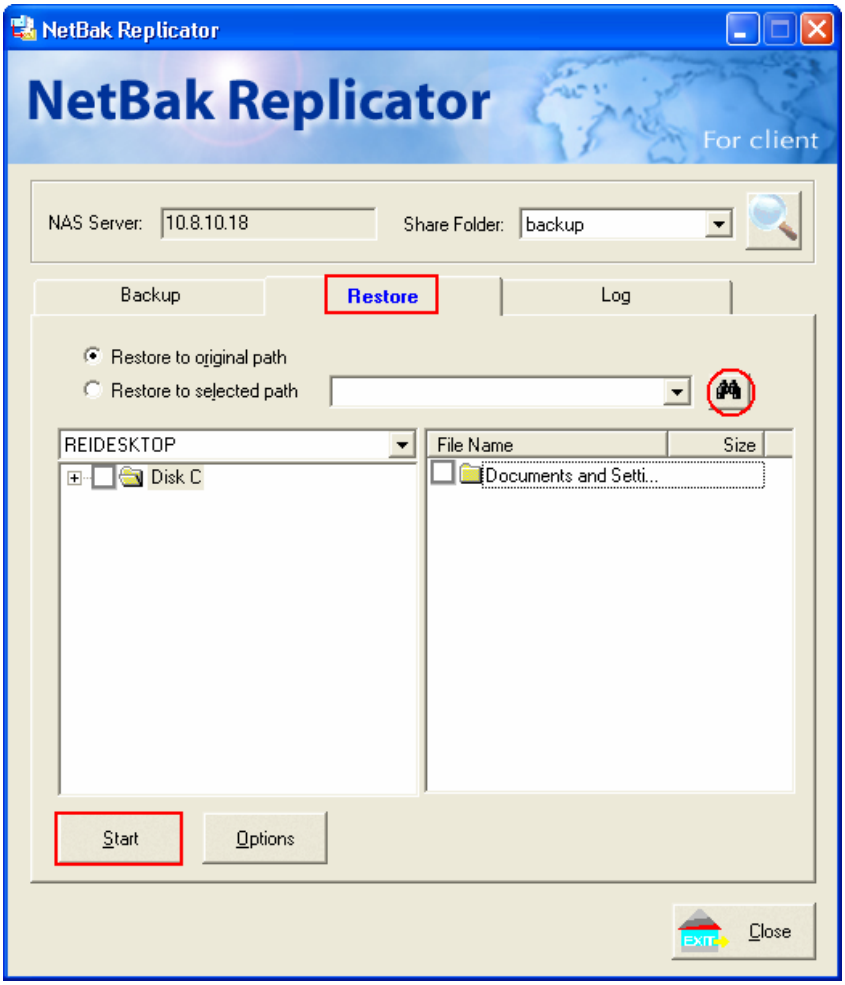
- **Restore**

  Please follow the steps below to restore files from the NAS to your PC.

  a. Restore to original position: Select the location that the data will be restored to.

  b. Select new restore position: Click  to select the directory to restore the data to or select a previously chosen location from the drop-down menu.

  c. Select the folder(s) and sub-folder(s) for data restore on the right and click "Start".



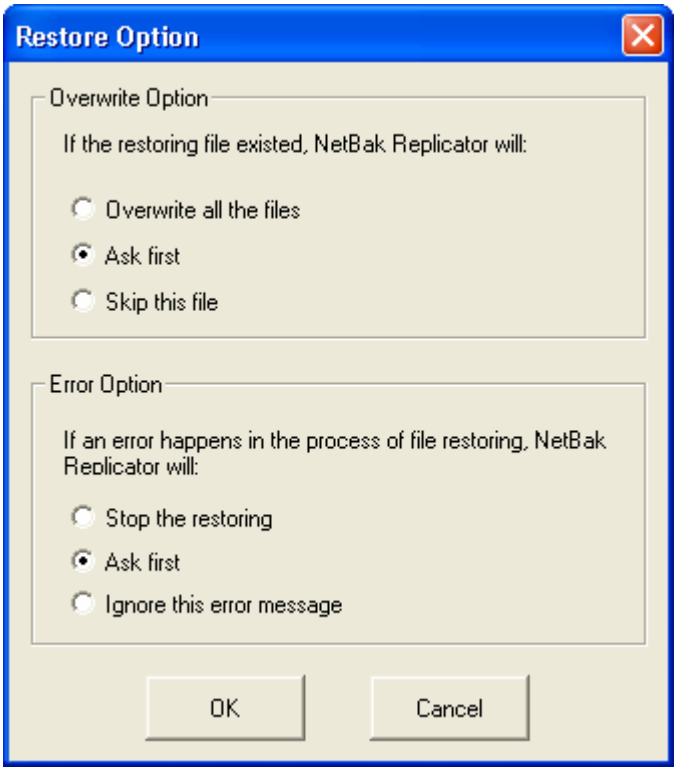
d. Option: Select recovery option and error option.

If the restoring file existed, NetBak Replicator will:

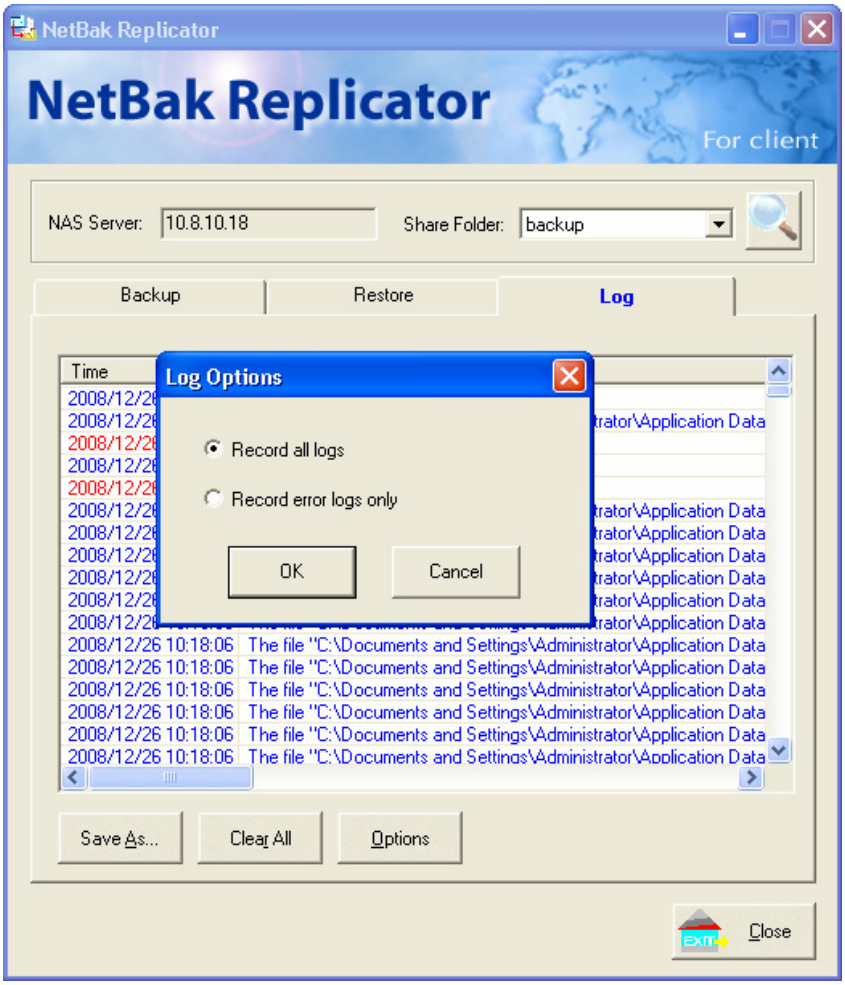
- ✓ Overwrite all the files
- ✓ Ask first
- ✓ Skip this file

If an error happens in the process of file restoring, NetBak Replicator will:

- ✓ Stop the restoring
- ✓ Ask first
- ✓ Ignore this error message



- **Log**
  a. Save As…: To save all the logs on NetBak Replicator, click this button. All the logs will be saved as text file.
  b. Clear All: Click this button to clear all the logs.
  c. Option: Select the type of logs to be recorded— "Record all logs" or "Record error logs only".



Chapter 8 Active Directory

Active Directory® is a Microsoft directory used in Windows environments to centrally store, share, and manage the information and resources on your network. It is a hierarchical data centre which centrally holds the information of the users, user groups, and the computers for secure access management.

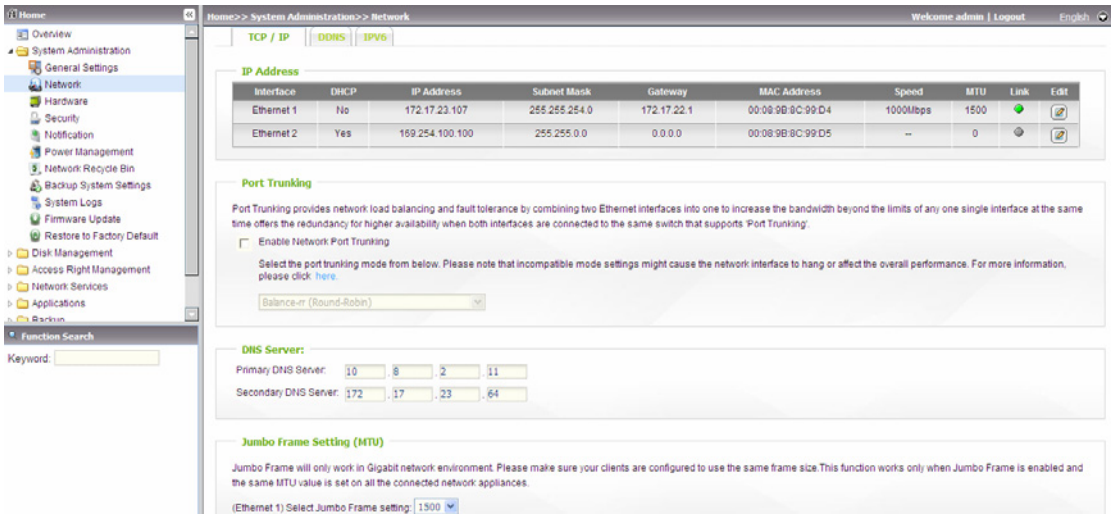
The NAS supports Active Directory (AD). By joining the NAS to the Active Directory, all the user accounts of the AD server will be imported to the NAS automatically. The AD users can use the same set of user name and password to login the NAS

Joining the QNAP NAS to Windows Server 2003/ 2008 Active Directory

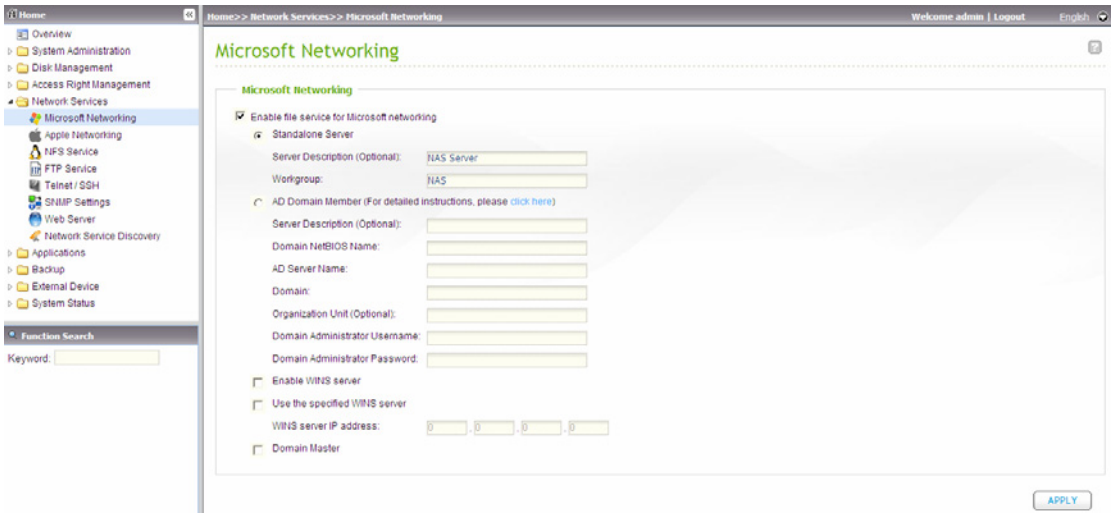
Please follow the steps below to join the QNAP NAS to the Windows Active Directory.

1. Login the NAS as an administrator. Go to "System Administration" > "General Settings" > "Date and Time". Set the date and time of the NAS, which must be consistent with the time of the AD server. The maximum time difference allowed is 5 minutes.

2. Go to "System Administration" > "Network" > "TCP/IP". Enter the IP address of the primary DNS server as the IP address of the Active Directory server.



3. Go to “Network Services” > “Microsoft Networking”. Enable AD Domain Member, and enter the AD domain information.

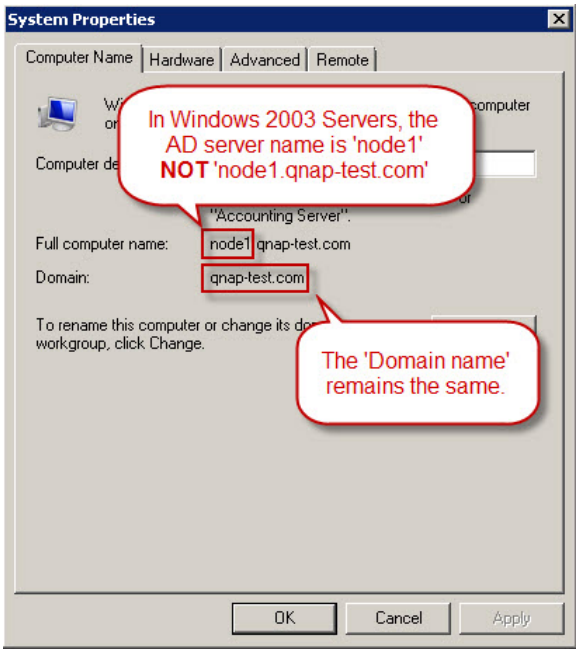


Note:

- Enter a fully qualified AD domain name, e.g. qnap-test.com
- The AD user entered here must have the administrator access right to the AD domain.
- The domain administrator password must not contain the special symbol “!”, or the NAS will fail to join the AD domain.

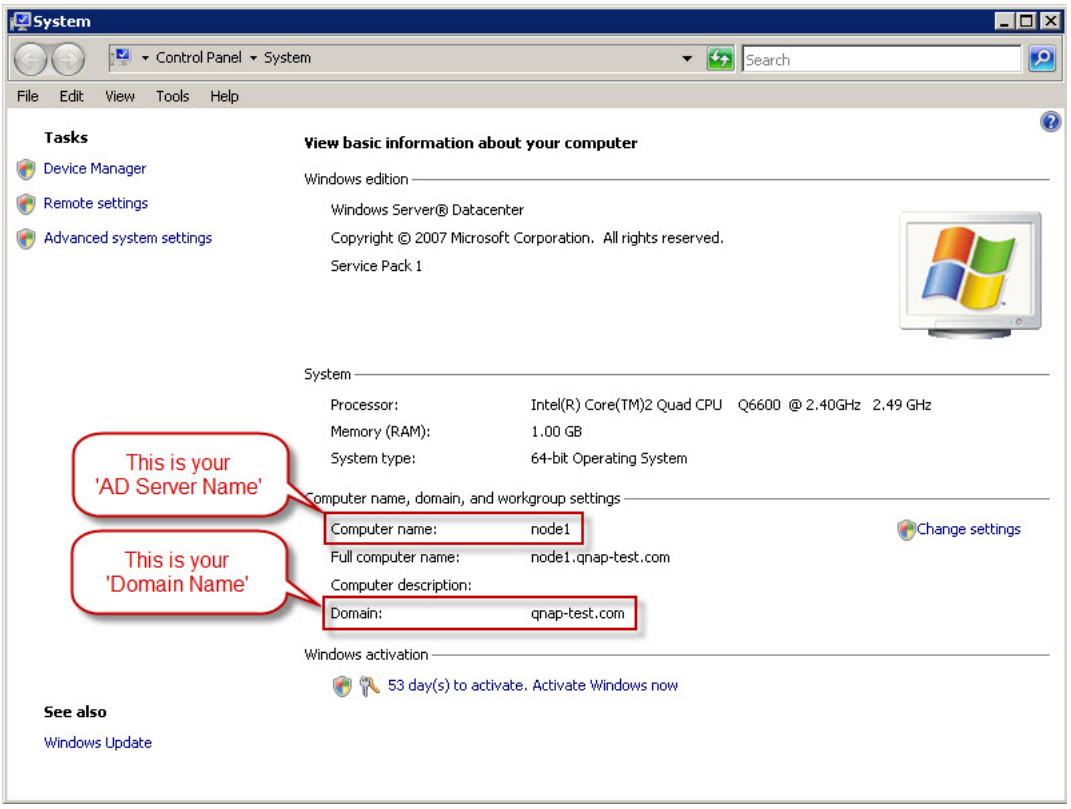
Windows 2003:

You may check the AD server name and AD domain name in "System Properties".



Windows Server 2008:

You may check the AD server name and domain name in "Control Panel" > "System".



Notes:

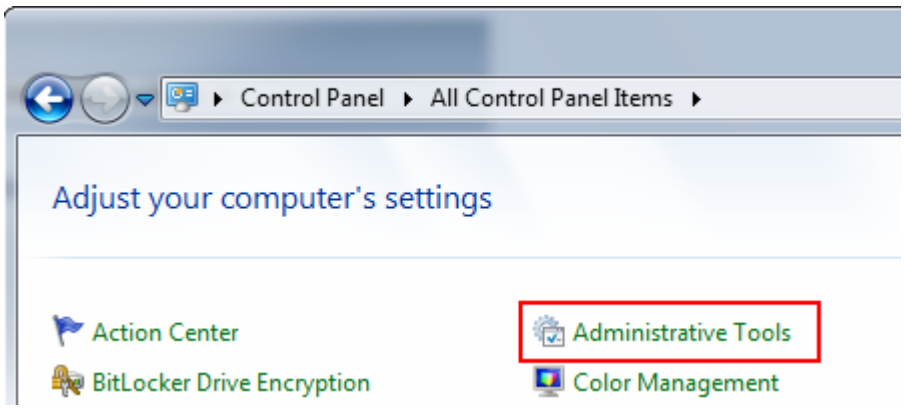
- After joining the NAS to the Active Directory, the local NAS users who have access right to the AD server should use "**NASname\username**" to login; the AD users should use their own user names to login the AD server.
- The local NAS users and the AD users (with username as domain name + username) are allowed to access the NAS (firmware version 3.2.0 and above) via AFP, FTP, Web File Manager, and WebDAV. However, if the firmware version of the NAS is earlier than 3.2.0, only local NAS users are allowed to access the NAS by Web File Manager and WebDAV.
- For TS-109/209/409/509 series Turbo NAS, if the AD domain is based on Windows 2008 Server, the NAS firmware must be updated to version 2.1.2 or later.

The step-by-step guide of joining the QNAP NAS to the Active Directory is available on http://www.qnap.com/pro_features.asp.

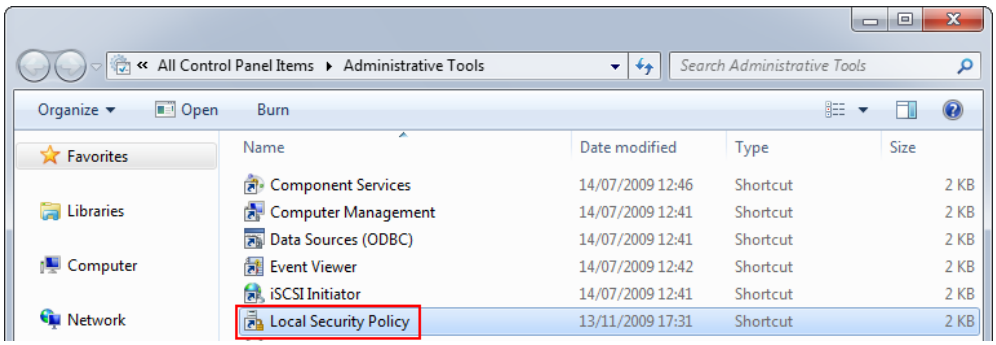
Windows 7:

If you are using a Windows 7 PC which is not a member of an Active Directory, while your NAS is an AD domain member and its firmware version is earlier than v3.2.0, please change your PC settings as shown below to allow your PC to access the NAS.

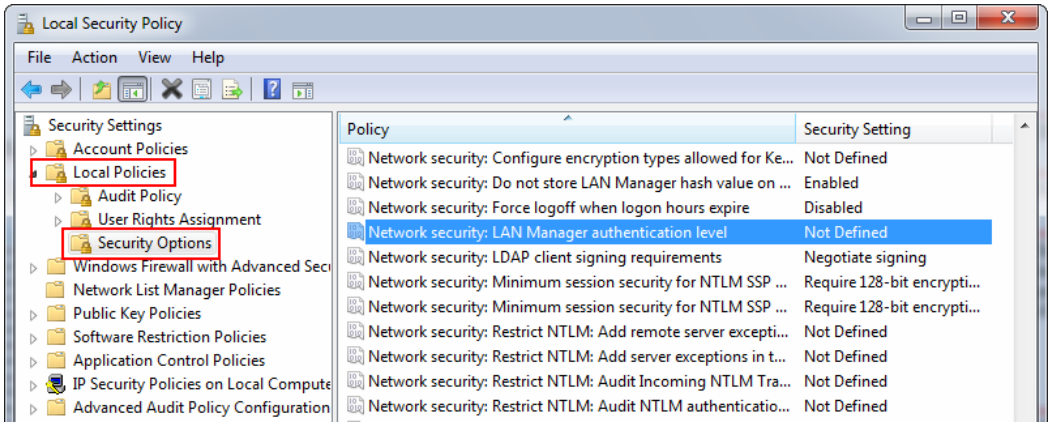
(a) Go to the "Control Panel", and click "Administrative Tools".



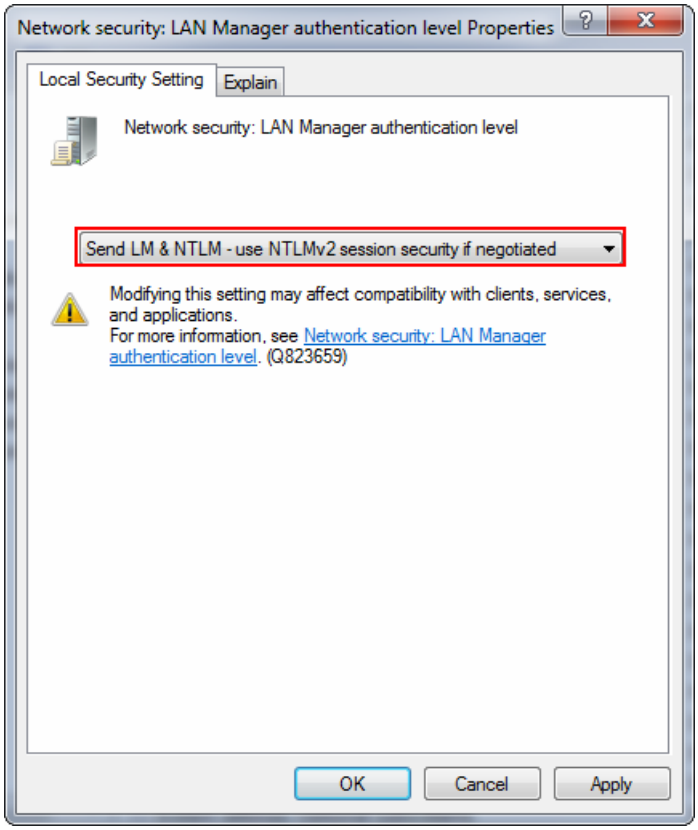
(b) Click "Local Security Policy".



(c) Go to “Local Policies” > “Security Options”. Then select “Network security: LAN Manager authentication level”.



(d) Select the “Local Security Setting” tab, and select “Send LM & NTLMv2 – use NTLMv2 session security if negotiated” from the list. Then click "OK".



Chapter 9 Access NAS via Linux OS

In addition to Microsoft and Mac OS, the NAS also supports Linux systems through the NFS service:

1. In Linux, run the following command:

   mount -t nfs <NAS IP address>:/<Network Share Name> <Directory to Mount>

   For example, if the IP address of your NAS is 192.168.0.1 and you want to link the network share folder "public" under the /mnt/pub directory, use the following command:

   mount -t nfs 192.168.0.1:/public /mnt/pub

   Note: You must login as "root" user to initiate the above command.

2. Login as the user ID you define, you can use the mounted directory to access your network share files.

Chapter 10 NAS Maintenance

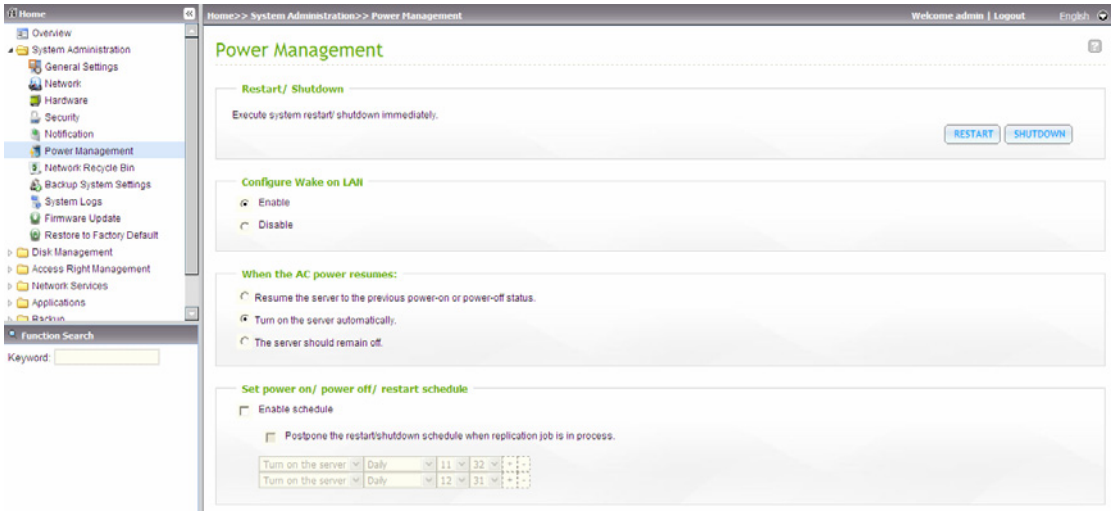
10.1 Restart/ Shut down Server

Follow the steps below to restart or shut down the NAS.

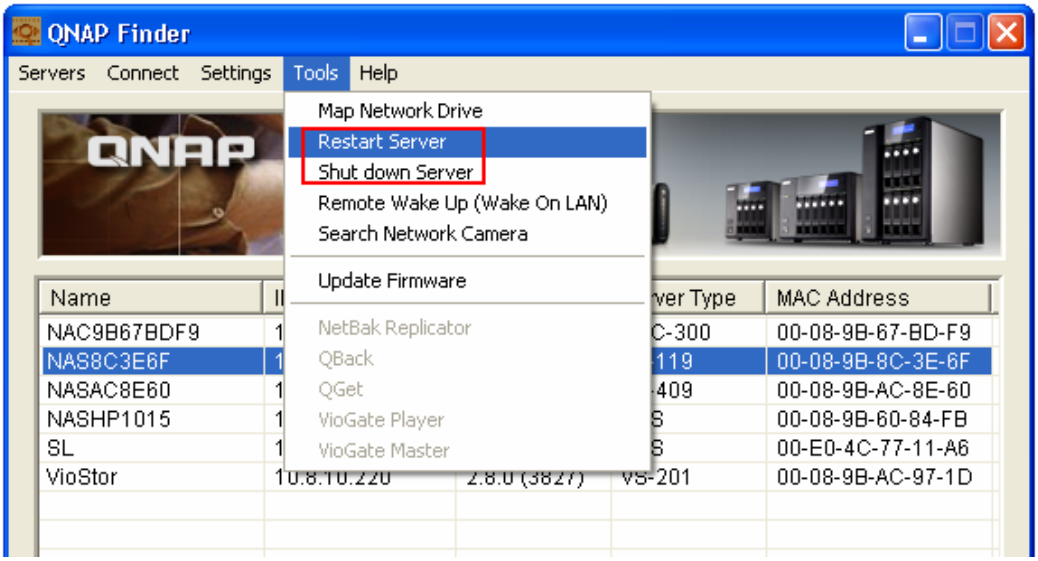
1. Login the NAS. Go to "System Administration" > "Power Management".
2. Click "Restart" to reboot the server or "Shut Down" to turn off the server.

You can also press the power button for 1.5 seconds* to turn off the NAS. To force shut down the NAS, press the power button for more than 5 seconds. The server beeps once and shuts down immediately.

*To turn off TS-109I/II, TS-109 Pro I/II, TS-209 I/II, TS-209 Pro I/II, TS-409/ TS-409 Pro/ TS-409U, press the power button for 4 seconds.

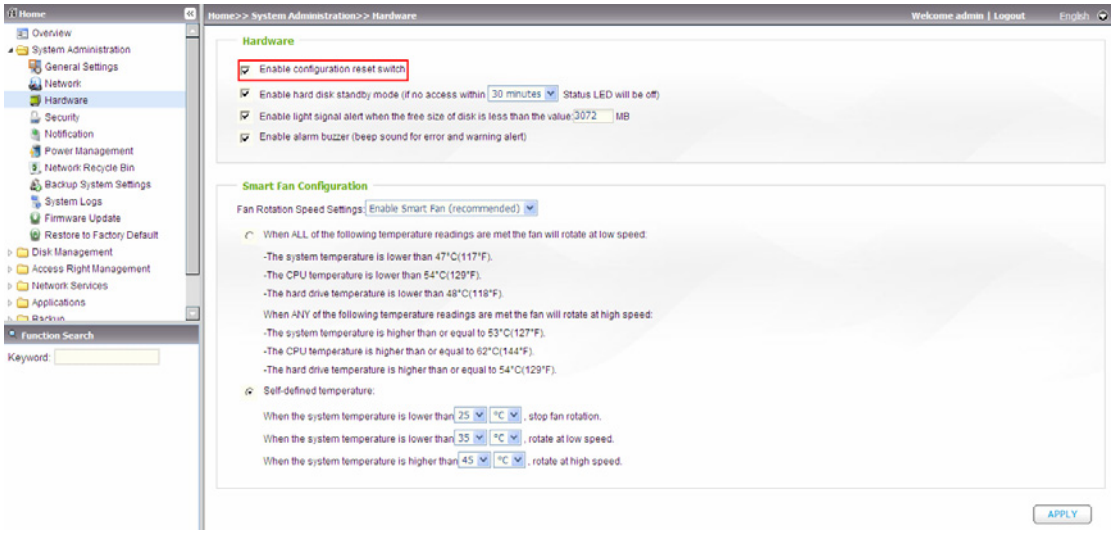


You can use the Finder to restart or shut down the server (admin access required).



10.2 Reset Administrator Password and Network Settings

Note: To reset the system by the reset button, the option "Enable configuration reset switch" in "System Administration" > "Hardware" must be activated.



System	Basic system reset (1 beep)	Advanced system reset (2 beeps)
All NAS models	Press the reset button for 3 sec	Press the reset button for 10 sec

Basic system reset (3 sec)

When you press the reset button for 3 seconds, a beep sound will be heard. The following settings are reset to default:

- System administration password: admin
- TCP/ IP configuration: Obtain IP address settings automatically via DHCP
- TCP/ IP configuration: Disable Jumbo Frame
- TCP/ IP configuration: If Port trunking is enabled (dual LAN models only), the port trunking mode will be reset to "Active Backup (Failover)".
- System Port: 8080 (system service port)
- Security Level: Low (Allow all connections)
- LCD panel password: (blank)*

* Applicable to models with LCD panel only.

Advanced system reset (10 sec)

When you press the reset button for 10 seconds, you will hear two beeps at the third and the tenth seconds. The NAS will reset all the system settings to default as it does by web-based system reset in "Administration" > "Restore to Factory Default" except all the data are reserved. The settings such as the users, user groups, and the network share folders you previously created will be cleared. To retrieve the old data after the advanced system reset, you may create the same network share folders on the NAS and the data will be accessible again.

10.3 Disk Failure or Malfunction

When you encounter disk malfunction or failure, please do the following:

1. Record the malfunction status or error messages shown in Event Logs.
2. Stop using the failed NAS and turn off the server.
3. Contact customer service for technical support.

Note: The NAS must be repaired by professional technicians, do not try to repair the server yourself.
Please back up any important files or folders to avoid potential data loss due to disk crash.

10.4 Power Outage or Abnormal Shutdown

In case of power outage or improper shutdown of the NAS, the system will resume to the state before it is shut down. If your server does not function properly after restart, please do the following:

1. If the system configuration is lost, configure the system again.
2. In the event of abnormal operation of the server, contact customer service for technical support.

10.5 System Software Abnormal Operation

When the system software does not operate properly, the NAS automatically restarts to resume normal operation. If you find the system restarts continuously, it may fail to resume normal operation. In this case, please contact the technical support immediately.

10.6 System Temperature Protection

The system shuts down automatically for hardware protection when any of the following criteria is met:

- ✓ The system temperature exceeds 70°C (158°F)
- ✓ The CPU temperature exceeds 85°C (185°F)
- ✓ The hard drive temperature exceeds 65°C (149°F)*

* Note that when the temperature of any hard drives on the NAS exceeds 65°C (149°F), the NAS waits for the standby time (configured in "System Administration" > "Hardware") and another 10 minutes and will shut down automatically. For example, if you have configured the NAS to enter the standby mode after idling for 5 minutes, the NAS shuts down automatically when the temperature of any hard drive(s) exceeds 65°C (149°F) continuously after 15 (5+10) minutes.

Chapter 11 RAID Abnormal Operation Troubleshooting

If the RAID configuration of your NAS is found abnormal or there are error messages, please try the following solutions:

Note: You must back up the important data on the NAS first to avoid any potential data loss.

1. Check that the RAID rebuilding has failed:
   a. LED: The Status LED of NAS flashes in red.
   b. On the "Disk Management" > "Volume Management" page, the status of the disk volume configuration is "In degraded mode".

2. Find out the hard drive(s) that causes the RAID rebuilding failure.
   You can go to "System Administration" > "System Logs" page to search for the following error message and find out which hard drive(s) causes the error.
   Error occurred while accessing Drive ***X***.
   Drive ***X*** has been removed.
   X refers to the number of the hard drive slot.

3. Troubleshooting

After plugging in the new hard drive (e.g., HDD 1), drive rebuilding will start. If the drive configuration fails again due to read/write error of the hard drive in the rebuilding process, identify which hard drive causes the error and follow the steps below to solve the problems.

Situation 1: The error is caused by the newly plugged in drive.

If the newly inserted drive (e.g., HDD 1) causes the rebuilding error, please unplug HDD 1 and plug in another new drive to start RAID rebuilding.

Situation 2: The error is caused by an existing drive (e.g., HDD 2) in the RAID configuration.

If the RAID configuration is RAID 1, you can do either one of the following:

a. Back up the drive data to another storage device. Then reinstall and set up the NAS.

b. Format the newly plugged in drive (e.g. HDD 1) as a single drive. Then back up the data on the NAS to this drive (HDD 1) via Web File Manager. Unplug the drive with errors (e.g., HDD 2). After that, insert a new drive to NAS to replace the fault drive, and execute RAID 1 migration.

When the RAID configuration is RAID 5 or 6: The RAID configuration is changed to degraded mode (read-only). It is recommended that you back up the data and run system installation and configuration again.

Note: When plugging in or unplugging a hard drive, please strictly adhere to the following rules to avoid abnormal system operation or data crash.

1. Plug in only one drive to NAS or unplug only one drive from NAS at one time.
2. After plugging in or unplugging a hard drive, wait for about ten seconds or longer until you hear two beeps from the NAS. Then unplug or plug in the next hard drive.

Chapter 12 Use the LCD Panel

* This section is applicable to NAS models with LCD panel only.

The NAS provides a handy LCD panel for you to perform disk configuration and view the system information.

When the NAS is started up, you will be able to view the server name and IP address:

For the first time installation, the LCD panel shows the number of hard drives detected and the IP address. You may select to configure the hard drives.

Number of hard drives detected	Default disk configuration	Available disk configuration options*
1	Single	Single
2	RAID 1	Single -> JBOD ->RAID 0 -> RAID 1
3	RAID 5	Single -> JBOD -> RAID 0 -> RAID 5
4 or above	RAID 5	Single ->JBOD -> RAID 0 -> RAID 5 -> RAID 6

*Press the "Select" button to choose the option, and press the "Enter" button to confirm.

For example, when you turn on the NAS with 5 hard drives installed, the LCD panel shows:

You can press the "Select" button to browse more options, e.g. RAID 6.
Press the "Enter" button and the following message shows. Press the "Select" button to select "Yes" to confirm.

When you execute RAID 1, RAID 5, or RAID 6 configuration, the system will initialize the hard drives, create the RAID device, format the RAID device, and mount it as a volume on the NAS. The progress will be shown on the LCD panel. When it reaches 100%, you can access the RAID volume, e.g. create share folders and upload files to the folders on the NAS. In the meantime, to make sure the stripes and blocks in all the RAID component devices are ready, the NAS will execute RAID synchronization and the progress will be shown on "Disk Management" > "Volume Management" page. The synchronization rate is around 30-60 MB/s (vary by hard drive models, system resource usage, etc.).

Note: If a member drive of the RAID configuration was lost during the synchronization, the RAID device will enter degraded mode. The volume data is still accessible. If you add a new member drive to the device, it will start to rebuild. You can check the status on the "Volume Management" page.

To encrypt the disk volume, select "Yes" when the LCD panel shows <Encrypt Volume?>. The default encryption password is "admin". To change the password, please login the web-based administration interface as an administrator and change the settings in "Device Configuration" > "Disk volume Encryption Management".

When the configuration is finished, the server name and IP address will be shown. If the NAS fails to create the disk volume, the following message will be shown.

View system information by the LCD panel

When the LCD panel shows the server name and IP address, you may press the "Enter" button to enter the Main Menu. The Main Menu consists of the following items:

1. TCP/IP
2. Physical disk
3. Volume
4. System
5. Shut down
6. Reboot
7. Password
8. Back

1. TCP/ IP

In TCP/ IP, you can view the following options:

- 1.1 LAN IP Address
- 1.2 LAN Subnet Mask
- 1.3 LAN Gateway
- 1.4 LAN PRI. DNS
- 1.5 LAN SEC. DNS
- 1.6 Enter Network Settings
  - 1.6.1 Network Settings – DHCP
  - 1.6.2 Network Settings – Static IP*
  - 1.6.3 Network Settings – BACK
- 1.7 Back to Main Menu

* In Network Settings – Static IP, you can configure the IP address, subnet mask, gateway, and DNS of LAN 1 and LAN 2.

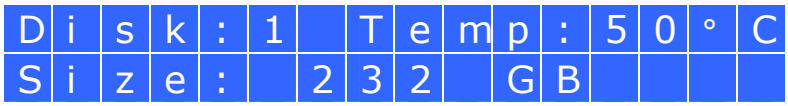
2. Physical disk

In Physical disk, you can view the following options:

2.1 Disk Info

2.2 Back to Main Menu

The disk info shows the temperature and the capacity of the hard drive.



3. Volume

This section shows the disk configuration of the NAS. The first line shows the RAID configuration and storage capacity; the second line shows the member drive number of the configuration.

If there is more than one volume, press the "Select" button to view the information. The following table shows the description of the LCD messages for RAID 5 configuration.

LCD Display	Drive configuration
RAID5+S	RAID5+spare
RAID5 (D)	RAID 5 degraded mode
RAID 5 (B)	RAID 5 rebuilding
RAID 5 (S)	RAID 5 re-synchronizing
RAID 5 (U)	RAID 5 is unmounted
RAID 5 (X)	RAID 5 non-activated

4. System

This section shows the system temperature and the rotation speed of the system fan.

5. Shut down

Use this option to turn off the NAS. Press the "Select" button to select "Yes". Then press the "Enter" button to confirm.

6. Reboot

Use this option to restart the NAS. Press the "Select" button to select "Yes". Then press the "Enter" button to confirm.

7. Password

The default password of the LCD panel is blank. Enter this option to change the password of the LCD panel. Select "Yes" to continue.

You may enter a password of maximum 8 numeric characters (0-9). When the cursor moves to "OK", press the "Enter" button. Verify the password to confirm the changes.

8. Back

Select this option to return to the main menu.

System Messages

When the NAS encounters system error, an error message will be shown on the LCD panel. Press the "Enter" button to view the message. Press the "Enter" button again to view the next message.

System Message	Description
Sys. Fan Failed	The system fan failed
Sys. Overheat	The system overheat
HDD Overheat	The hard drive overheat
CPU Overheat	The CPU overheat
Network Lost	Both LAN 1 and LAN 2 are disconnected in Failover or Load-balancing mode
LAN1 Lost	LAN 1 is disconnected
LAN2 Lost	LAN 2 is disconnected
HDD Failure	The hard drive fails
Vol1 Full	The volume is full
HDD Ejected	The hard drive is ejected
Vol1 Degraded	The volume is in degraded mode
Vol1 Unmounted	The volume is unmounted
Vol1 Nonactivate	The volume is not activated

Technical Support

QNAP provides dedicated online support and customer service via instant messenger. You can contact us by the following means:

Online Support: http://www.qnap.com/
MSN: q.support@hotmail.com
Skype: qnapskype
Forum: http://forum.qnap.com/

Technical Support in the USA and Canada:
Email: q_supportus@qnap.com
TEL: 909-595-2819 ext. 185
Address: 168 University Parkway Pomona, CA 91768-4300
Service Hours: 08:00-17:00 (GMT- 08:00 Pacific Time, Monday to Friday)

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert

copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS
0. Definitions.
“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion

requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.
The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for

which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.
All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material

outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.
No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.
You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.
You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the

requirement in section 4 to “keep intact all notices”.
c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.
A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.
You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in

accord with subsection 6b.
d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.
A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for

use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.
“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.
All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.
You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.
You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.
Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give

under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.
A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or

other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.
If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent

obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.
Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.
The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.
THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS”

WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.
If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS