QNAP Turbo NAS

Software User Manual

(Version: 3.7.0)

© 2012 QNAP Systems, Inc. All Rights Reserved.

Table of Contents

1. Notice 5

1.1 Regulatory Notice 6
1.2 Symbols in this document 7
1.3 Safety Information and Precautions 8

2. Getting Started 9

2.1 Browse the CD-ROM 14
2.2 Hard Disk Drive Compatibility List 16
2.3 Check System Status (LED and Alarm Buzzer) 17
2.4 Connect to the NAS Network Shares 20
2.5 Connect to the NAS by Web Browser 22
2.6 System Migration 28

3. System Administration 31

3.1 General Settings 32
3.2 Network 36
3.3 Service Binding 59
3.4 Hardware 61
3.5 Security 65
3.6 Notification 68
3.7 Power Management 75
3.8 Network Recycle Bin 77
3.9 Back up/Restore Settings 78
3.10 System Logs 79
3.11 Firmware Update 84
3.12 Restore to Factory Default 88

4. Disk Management 89

4.1 Volume Management 89
4.2 RAID Management 93
4.3 Hard Disk S.M.A.R.T. 119
4.4 Encrypted File System 120
4.5 iSCSI 129
4.5.1 Portal Management 129
4.5.2 Target Management 140
4.5.2.1 Connect to the iSCSI targets by Microsoft iSCSI Initiator on Windows *152*
4.5.2.2 Connect to the iSCSI targets by Xtend SAN iSCSI Initiator on Mac OS *157*
4.5.2.3 Connect to the iSCSI targets by Open-iSCSI Initiator on Ubuntu Linux *164*
4.5.3 Advanced ACL 166
4.5.4 LUN Backup 170

4.6 Virtual Disk 189

5. Access Right Management 194

5.1 Domain Security 194

5.1.1 Join the NAS to Active Directory (Windows Server 2003/2008) 196

5.1.2 Connect the NAS to an LDAP Directory 208

5.2 Users 215

5.3 User Groups 232

5.4 Share Folders 233

5.5 Quota 264

6. Network Services 265

6.1 Microsoft Networking 266

6.2 Apple Networking 270

6.3 NFS Service 273

6.4 FTP Service 276

6.5 Telnet/SSH 278

6.6 SNMP Settings 279

6.7 Web Server 281

6.7.1 Virtual Host 304

6.8 Network Service Discovery 308

7. Application Servers 310

7.1 Web File Manager 311

7.2 Multimedia Station 329

7.2.1 QMobile 361

7.3 Photo Station 385

7.4 Music Station 408

7.5 Download Station 428

7.6 Surveillance Station 450

7.7 iTunes Server 458

7.8 UPnP Media Server 461

7.9 MySQL Server 463

7.10 QPKG Center 465

7.11 Syslog Server 469

7.12 RADIUS Server 474

7.13 Backup Server 478

7.14 Antivirus 482

7.15 TFTP Server 492

7.16 VPN Service 493

7.17 LDAP Server 509

8. Backup 514

8.1 Remote Replication 514
8.2 Cloud Backup 539
8.3 Time Machine 549
8.4 External Drive 554
8.5 USB One Touch Copy 569

9. External Device 572

9.1 External Storage Device 572
9.2 USB Printer 582
9.2.1 Windows 7, Vista Users 585
9.2.2 Windows XP Users 592
9.2.3 Mac OS 10.6 594
9.2.4 Mac OS 10.5 597
9.2.5 Mac OS 10.4 602
9.2.6 Linux (Ubuntu 10.10) 607
9.3 UPS Settings 612

10. MyCloudNAS Service 617

10.1 MyCloudNAS Wizard 618
10.2 Configure MyCloudNAS 626
10.3 Auto Router Configuration 633

11. System Status 636

11.1 System Information 636
11.2 System Service 637
11.3 Resource Monitor 638

12. Use the LCD Panel 642

13. Connect to QNAP NAS from the Internet (DDNS Service) 649

14. Set up SMS, Email, and IM Alert on QNAP NAS 658

15. Set up UPnP Media Server for Media Playing 669

16. Host a Forum with phpBB on QNAP NAS 678

17. NAS Maintenance Settings 690

17.1 System Restart/Shutdown 691
17.2 System Temperature Protection 693

18. GNU GENERAL PUBLIC LICENSE 694

1. Notice

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

- The Turbo NAS is hereafter referred to as the NAS.
- This manual provides the description of all the functions of the Turbo NAS. The product you purchased may not support certain functions dedicated to specific models.

Legal Notices
All the features, functionality, and other product specifications are subject to change without prior notice or obligation. Information contained herein is subject to change without notice.

QNAP and the QNAP logo are trademarks of QNAP Systems, Inc. All other brands and product names referred to are trademarks of their respective holders.
Further, the ® or ™ symbols are not used in the text.

DISCLAIMER
In no event shall QNAP Systems, Inc. (QNAP) liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential damages resulting from the use of the product, its accompanying 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.

Back up the system periodically to avoid any potential data loss. QNAP disclaims any responsibility of all sorts of data loss or recovery.

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.

1.1 Regulatory Notice

FCC STATEMENT

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

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

The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
Shielded interface cables, if any, must be used in order to comply with the emission limits.

CE NOTICE

Class B only.

1.2 Symbols in this document

Warning	This icon indicates the instructions must be strictly followed. Failure to do so could result in injury to human body or death.
Caution	This icon indicates the action may lead to disk clearance or loss OR failure to follow the instructions could result in data damage, disk damage, or product damage.
Important	This icon indicates the information provided is important or related to legal regulations.

1.3 Safety Information and Precautions

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 the 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 normal system operation and to avoid overheat.
6. Use the flat head screws in the product package to lock the hard disk drives in the NAS when installing the hard drives 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 unsure, 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 the 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 (also known as rack mount) 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.

Warning:

- Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
- Do NOT touch the fan inside the system to avoid serious injuries.

2. Getting Started

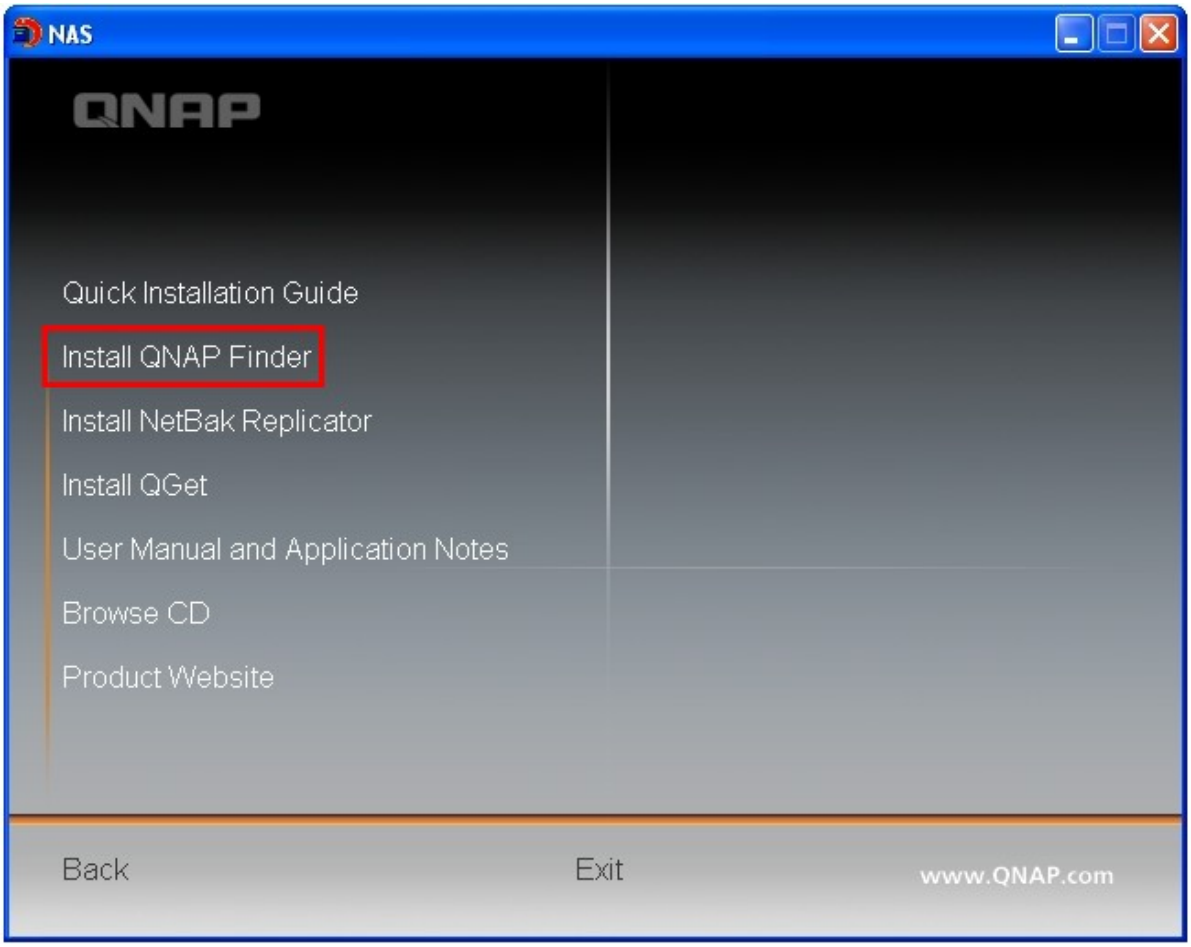
Hardware Installation

For the information of hardware installation, see the "Quick Installation Guide" (QIG) in the product package. You can also find the QIG in the product CD-ROM or QNAP website (http://www.qnap.com).

Software Installation

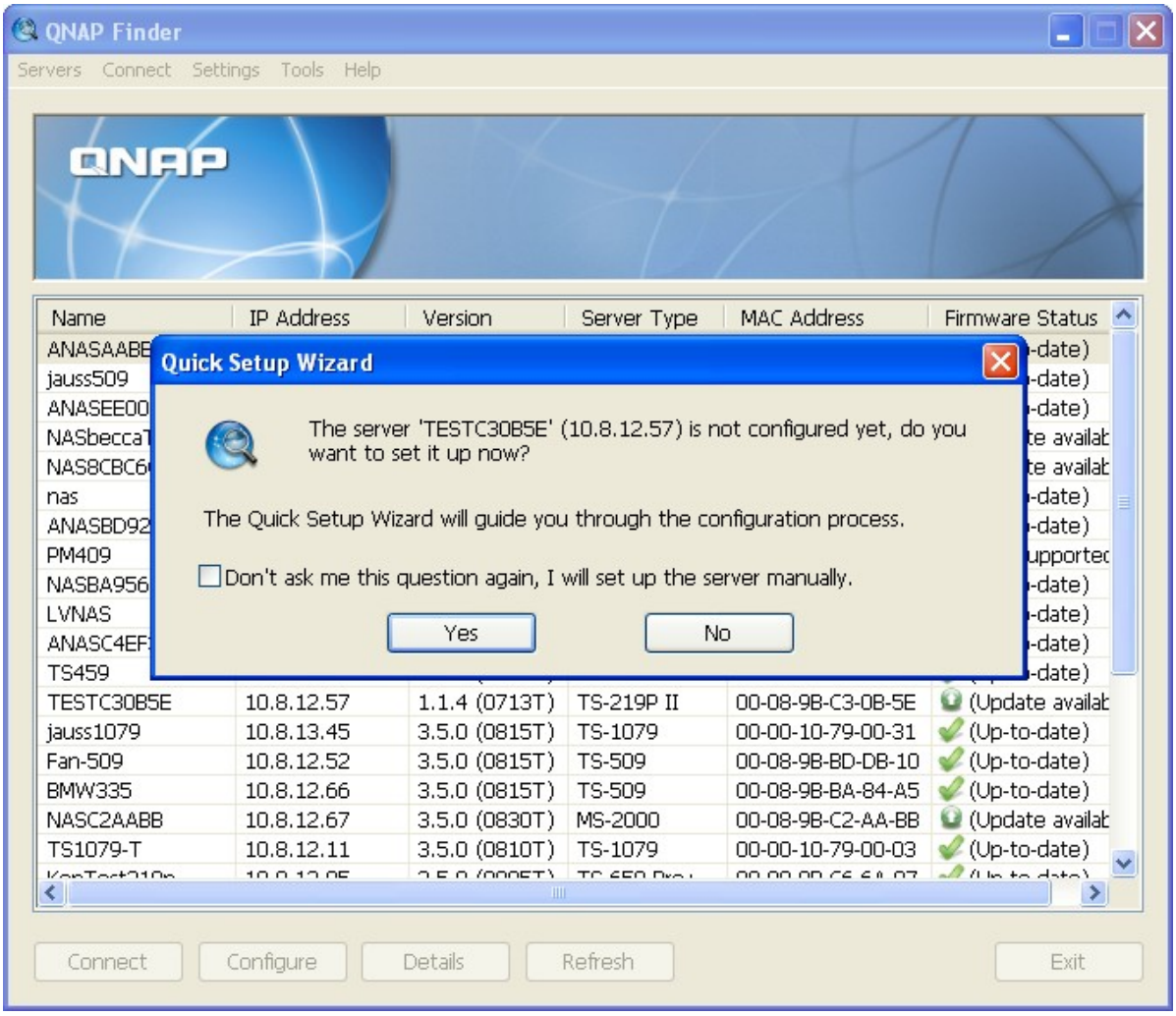
After installing the NAS hardware, proceed to the software installation. The following demonstration is based on Windows OS.

1. Install the QNAP Finder from the product CD-ROM.



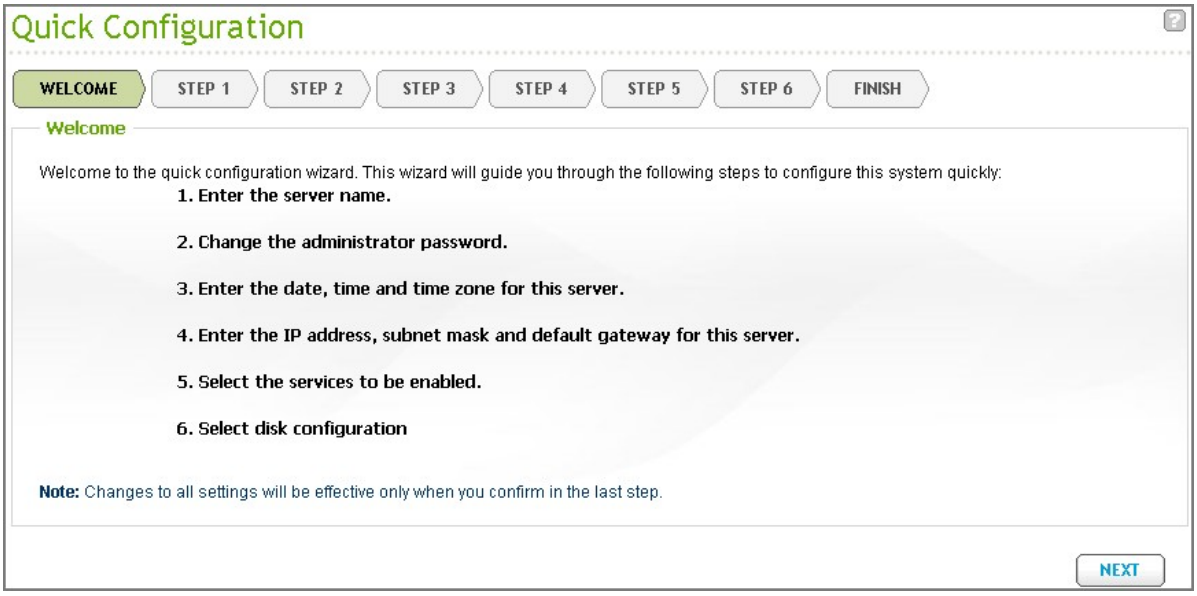
2. Run the Finder. If the Finder is blocked by your firewall, unblock the utility.

3. The Finder detects the NAS which has not been configured. Click "Yes" to perform quick setup of the NAS.

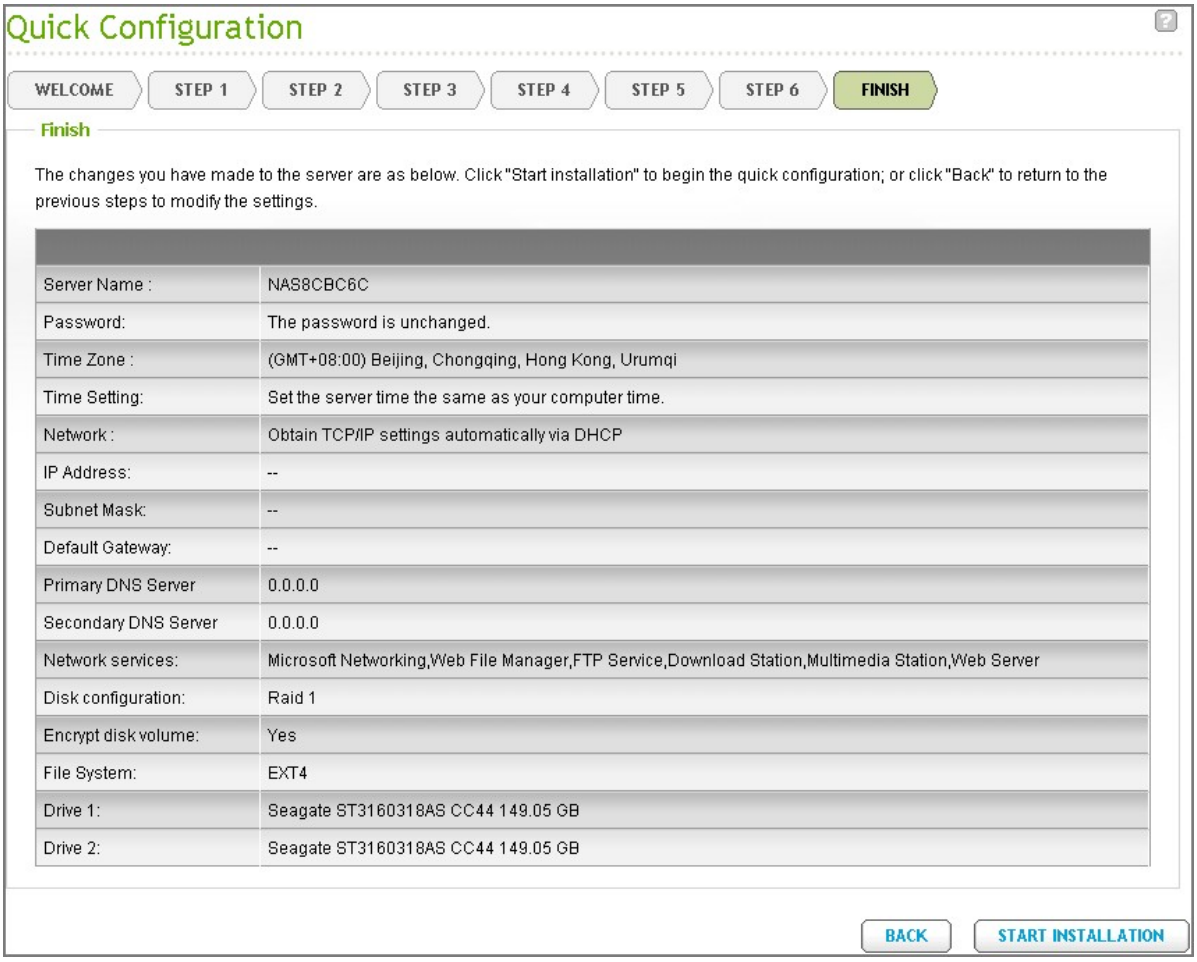


4. Click “OK” to proceed.

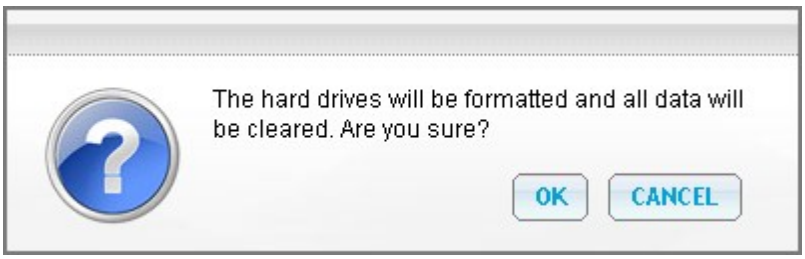
5. The default web browser will be opened. Follow the instructions to configure the NAS.



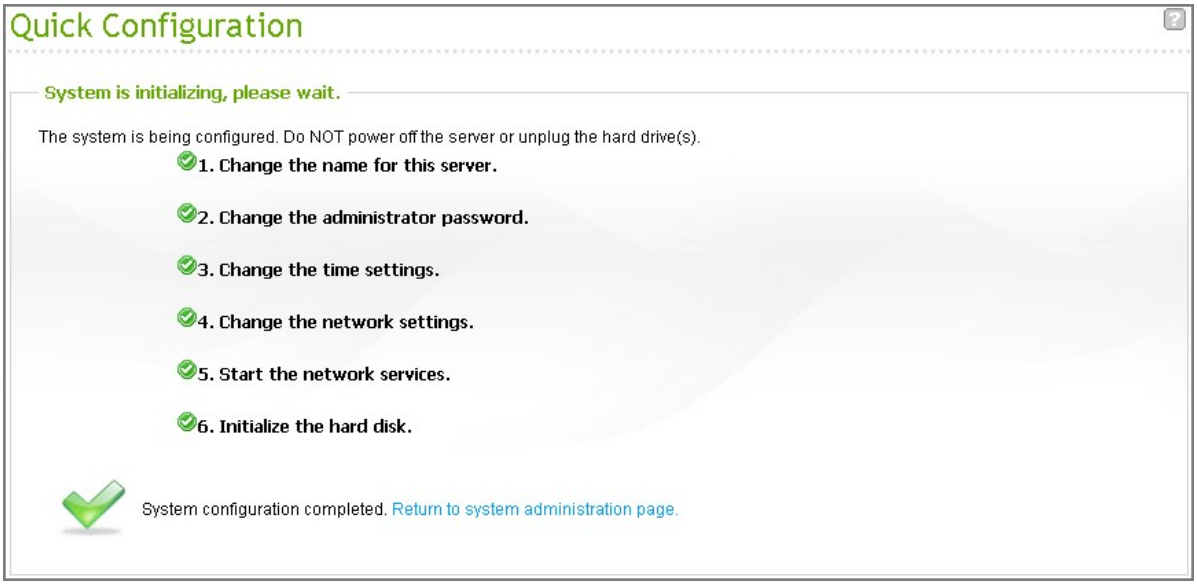
6. Click “START INSTALLATION” in the last step.



7. All the installed hard disk drives will be formatted and all the data will be cleared. Click “OK” to proceed.

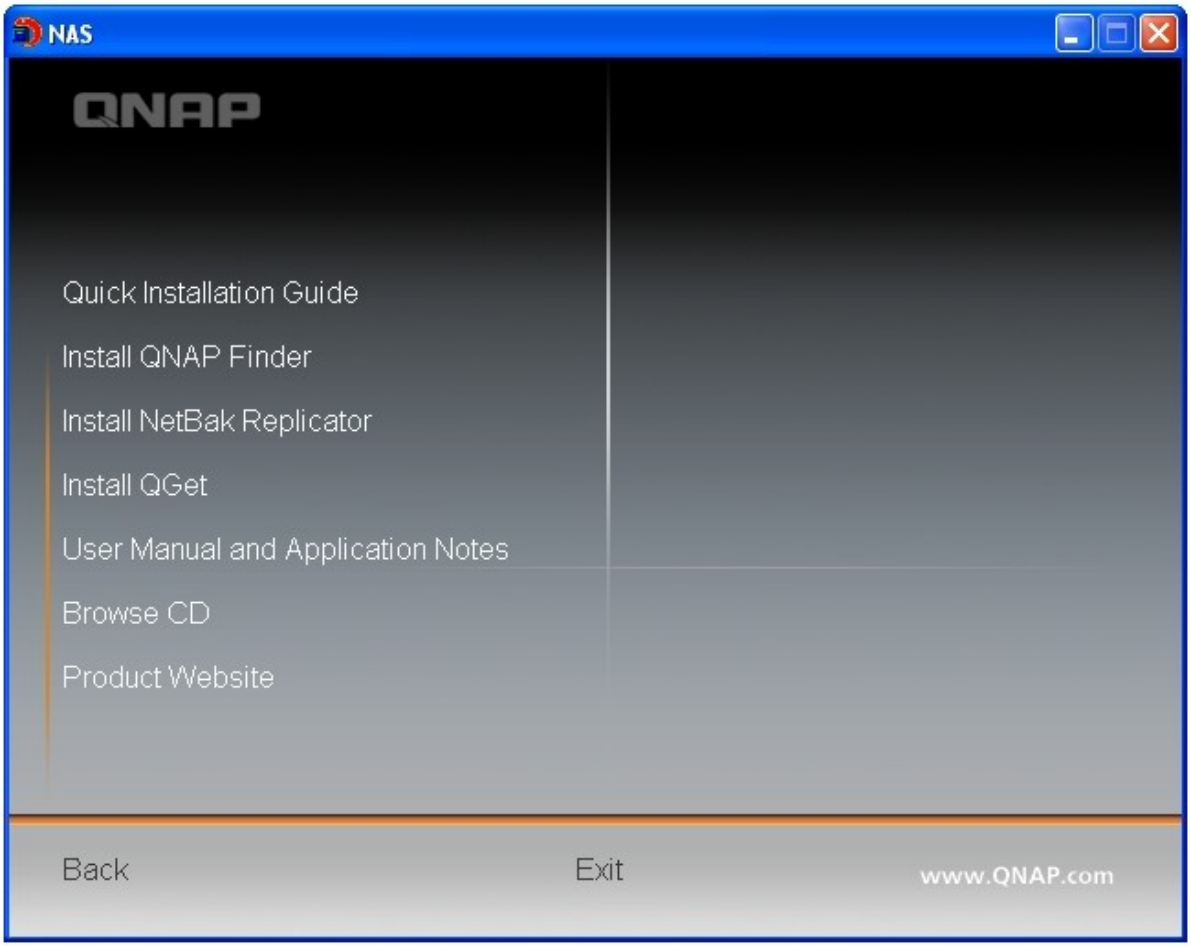


8. When finished, click "Return to system administration page" or enter the NAS IP in a web browser to connect to the web administration page of the NAS.



2.1 Browse the CD-ROM

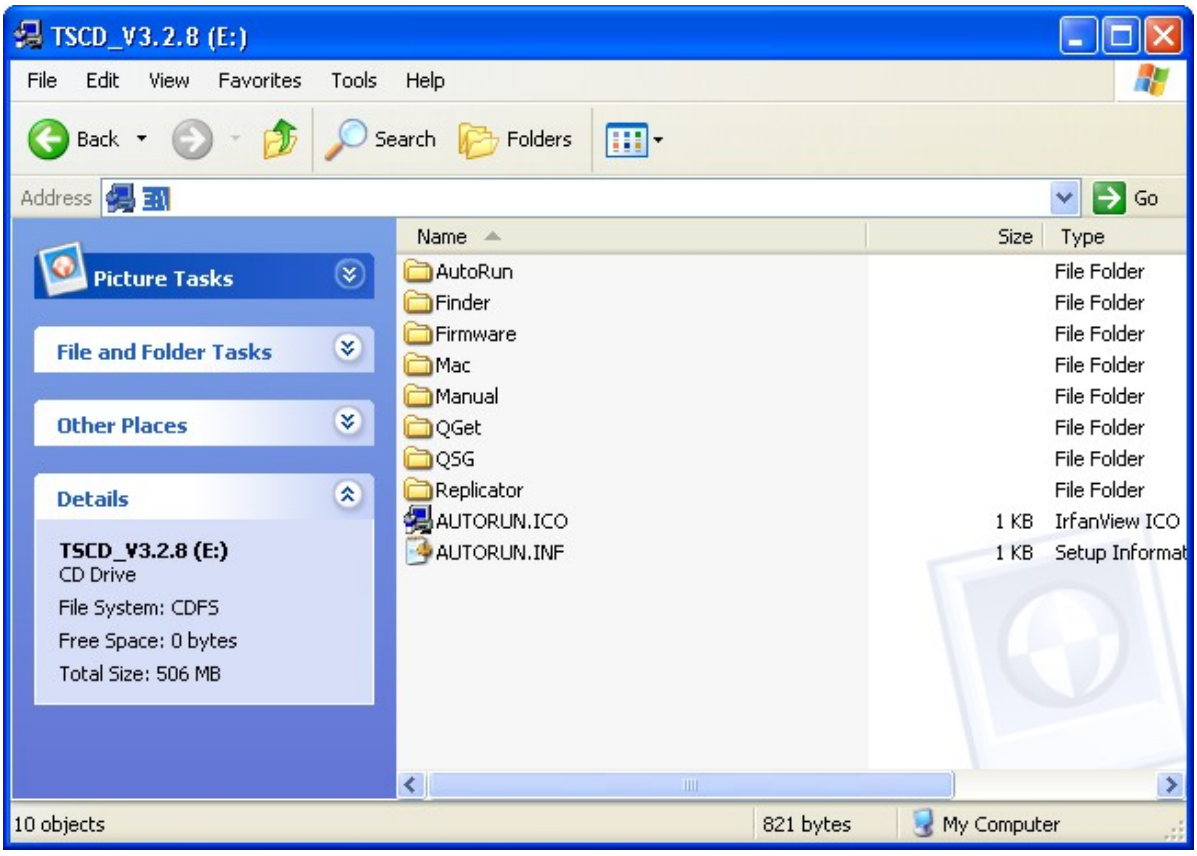
The NAS CD-ROM contains the documentation including Quick Installation Guide (QIG), user manual, application notes, and software utilities QNAP Finder, NetBak Replicator, and QGet.



Browse the CD-ROM and access the following contents:

- Finder: The setup program of the QNAP Finder (for Windows OS).
- Firmware: The firmware IMG file of the NAS model.
- Mac: The setup program of the QNAP Finder (for Mac OS).
- Manual: The Quick Installation Guide, software user manuals, and hardware manual of the Turbo NAS.
- QGet: The setup program of the QGet download utility (for Windows OS).
- QSG: View the hardware installation instructions of the NAS.
- Replicator: The setup program of NetBak Replicator (Windows utility for data backup from Windows OS to the QNAP NAS).

The above contents are also available on QNAP website (http://www.qnap.com).



2.2 Hard Disk Drive Compatibility List

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

Important: 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.

Caution: 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.

2.3 Check System Status (LED and Alarm Buzzer)

LED Display & System Status Overview

LED	Colour	LED Status	Description
System Status	Red/Green	Flashes green and red alternately every 0.5 sec	1) The hard disk drive on the NAS is being formatted. 2) The NAS is being initialized. 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 disk 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 (TS-119 does not support smart fan). 5) An error occurs when accessing (read/write) the disk data. 6) A bad sector is detected on the hard disk drive. 7) The NAS is in degraded read-only mode (2 member hard drives fail in a RAID 5 or RAID 6 configuration, the disk data can still be read). 8) (Hardware self-test error).
		Flashes red every 0.5 sec	The NAS is in degraded mode (one member hard 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 disk drive is not formatted.

LED	Colour	LED Status	Description
		Green	The NAS is ready.
		Off	All the hard disk drives on the NAS are in standby mode.
LAN	Orange	Orange	The disk data is being accessed and a read/write error occurs during the process.
		Flashes orange	The NAS is connected to the network.
10 GbE*	Green	Green	The 10GbE network expansion card is installed.
		Off	No 10GbE network expansion card is installed.
HDD	Red/Green	Flashes red	The NAS is being accessed from the network.
		Red	A hard drive read/write error occurs.
		Flashes green	The disk data is being accessed.
		Green	The hard drive can be accessed.
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	A front USB device is detected (after the device is mounted).
		Off	1) No USB device is detected. 2) The NAS has finished copying the data to or from. the USB device connected to the front USB port of the NAS.
eSATA**	Orange	Flashes	The eSATA device is being accessed.
		Off	No eSATA device can be detected.

*The 10 GbE network expansion function is only supported by the TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-1279U-RP, TS-EC879U-RP, and TS-EC1279U-RP.
**TS-210, TS-212, TS-219, TS-439U-SP/RP, TS-809 Pro, TS-809U-RP do not support eSATA port.

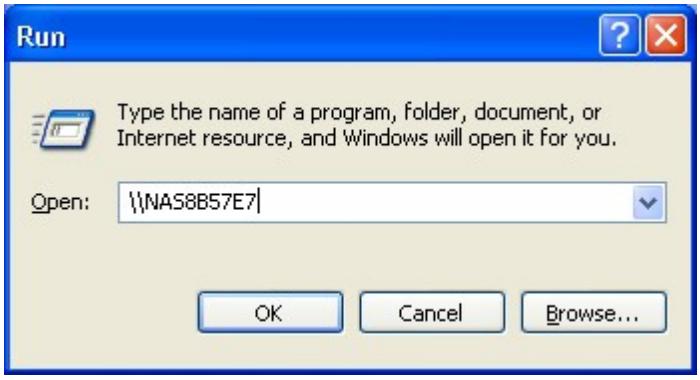
Alarm Buzzer (the alarm buzzer can be disabled in "System Tools" > "Hardware Settings")

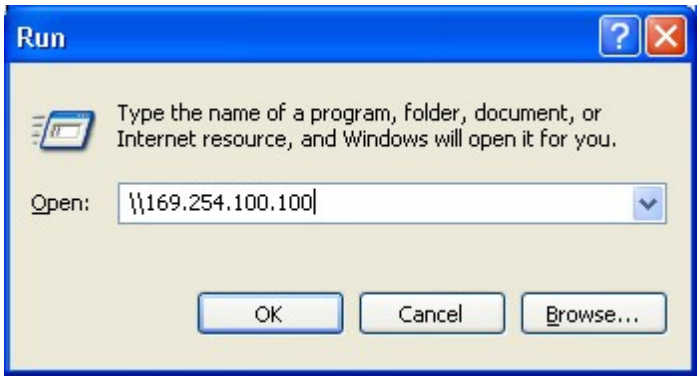
Beep sound	No. of Times	Description
Short beep (0.5 sec)	1	1) The NAS is starting up. 2) The NAS is being shut down (software shutdown). 3) The user presses the reset button to reset the NAS. 4) The system firmware has been updated.
Short beep (0.5 sec)	3	The NAS data cannot be copied to the external storage device from the front USB port.
Short beep (0.5 sec), long beep (1.5 sec)	3, every 5 min	The system fan is out of function (TS-119 does not support smart fan).
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 disk drives on the NAS are in degraded mode. 4) The user starts hard drive rebuilding.
	1	1) The NAS is turned off by force shutdown (hardware shutdown). 2) The NAS has been turned on and is ready.

2.4 Connect to the NAS Network Shares

Windows Users

1. Connect to the network shares of the NAS by the following means:
   a. Open My Network Places and find the workgroup of the NAS. If the NAS cannot be found, browse the whole network to search for the NAS. Double click the name of the NAS for connection.
   b. Use the Run function in Windows. Enter *NAS_name* or *NAS_IP*.





2. Enter the default administrator name and password.

Default user name: admin Default password: admin

3. You can upload files to the network shares.

Mac Users

1. Choose "Go" > "Connect to Server".

2. There are two ways to mount a disk:
   - AFP: type *NAS_IP* or *afp://NAS_IP*
   - SMB: type *smb://NAS_IP* or *NAS_name*

For example, 169.254.100.100 or smb://169.254.100.100

3. Click "Connect".

Linux Users

On Linux, run the following command:
mount -t nfs <NAS IP>:/<Network Share Name> <Directory to Mount>

For example, if the IP address of the NAS is 192.168.0.1, to connect to the network share "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 the "root" user to initiate the above command.

Login the NAS with the specified user ID, use the mounted directory to connect to the shared files.

2.5 Connect to the NAS by Web Browser

Connect to the NAS by web browser on Windows or Mac OS

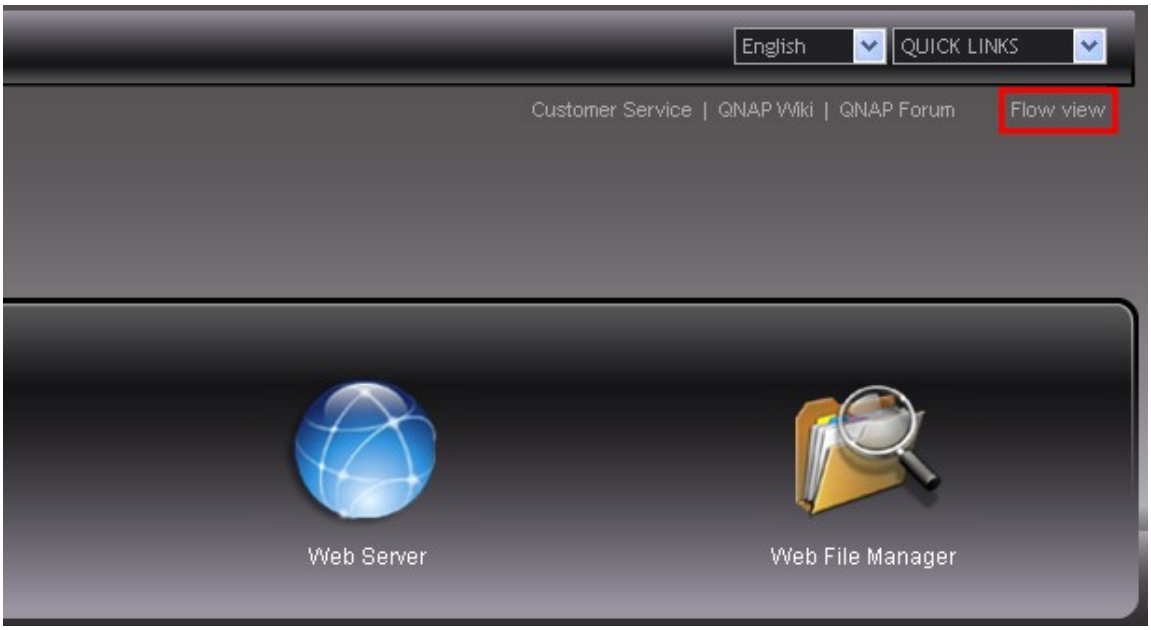
1. Connect to the web administration page of the NAS by the following methods:
   a. Use the Finder to find the NAS.
   b. Open a web browser and enter http://*NAS IP*:8080

   Note: The default NAS IP is 169.254.100.100:8080. If the NAS has been configured to use DHCP, you can use the Finder to check the IP address of the NAS. Make sure the NAS and the computer that runs the Finder are connected to the same subnet. If the NAS cannot be found, connect the NAS to the computer directly and run the Finder again.

2. Choose the display language from the drop-down menu on the login page of the NAS or after logging in the NAS.

3. Select to browse the NAS UI with the Standard view or the Flow view.

Standard view



Flow view

4. To configure the NAS, click "ADMINISTRATION". Enter the administrator name and the password.

Default user name: admin Default password: admin

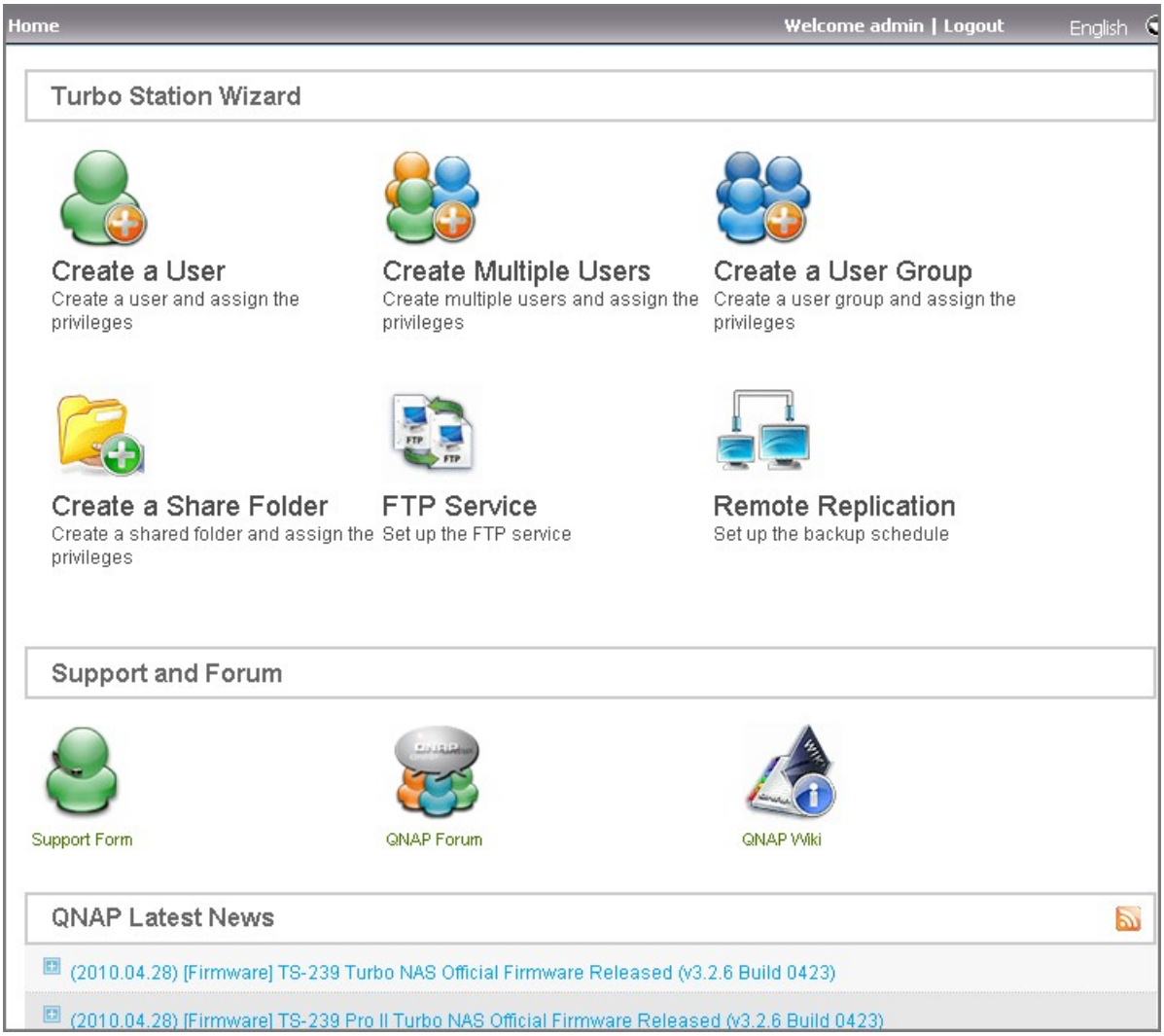
Note that if a user without administration right login the administration interface, the user can only change the login password.

5. Turn on the option "SSL login" (Secure Sockets Layer login) to allow secure connection to the NAS.

Note: If the NAS is behind an NAT gateway, to access the NAS by secure login from the Internet, the port 443 must be opened on the NAT router and forwarded to the LAN IP of the NAS.

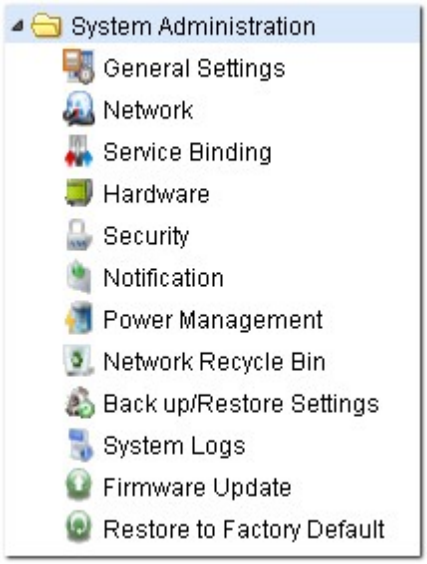
After logging in the NAS, the home page will be shown. The NAS provides several wizards for convenient setup of some features, links to QNAP technical support, forum, and Wiki*, and the latest RSS news feeds from QNAP*.

*Note that the NAS must be connected to the Internet for these features to work.



There are 8 main sections in the server administration.

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



To use the services such as Web File Manager, Download Station, Multimedia Station, and Surveillance Station, choose the services from the drop-down menu or click the icons on the login page

After logging in the NAS, click the icons on top of the page to connect to the services.

2.6 System Migration

System migration allows existing QNAP NAS users to upgrade the NAS to another new QNAP NAS model without the need to transfer the data or reconfigure the system. You only need to install the original hard disk drives on the new NAS following its original hard drive order and restart the NAS.

Due to different hardware design, the NAS will automatically check if a firmware update is required before system migration. After the migration has finished, all the settings and data will be kept and applied to the new NAS. However, the system settings of the source NAS cannot be imported to the destination NAS via "System Administration" > "Backup/Restore Settings". Configure the NAS again if the settings were lost.

The following table shows the NAS models which support system migration.

Source NAS	Destination NAS	Remarks
TS-x10, TS-x19, TS-x39, TS-509, TS-809, SS-x39, TS-x59, TS-x69, TS-x12, TS-x79	TS-x10, TS-x19, TS-x39, TS-509, TS-809, SS-x39, TS-x12	Firmware update required.
TS-x10, TS-x19, TS-x39, TS-509, TS-809, SS-x39, TS-x59, TS-x69, TS-x12, TS-x79	TS-x59, TS-x69, TS-x79	Firmware update not required.

Note:

- The destination should contain enough drive bays to house the number of hard disk drives in the disk volume of the source NAS.
- SS-x39 series supports only 2.5-inch hard disk drives.
- A NAS with encrypted disk volume cannot be migrated to a NAS which does not support file system encryption. File system encryption is not supported by TS-110, TS-119, TS-210, TS-219, TS-219P, TS-410, TS-419P, TS-410U, TS-419U, TS-119P+, TS-219P+, TS-419P+, TS-112, TS-212, TS-412, TS-419U+, TS-412U.
- The Multimedia Station, Download Station, iTunes Server, and UPnP Media Server features will be removed after migrating the non-TS-x79 models to the TS-x79 models. The network shares Multimedia/Qmultimedia, Download/Qdownload and all the downloaded files will be kept.
- The registered MyCloudNAS name on the source NAS will not be moved to the destination NAS after system migration. To use the same MyCloudNAS name on the destination NAS, change the MyCloudNAS name on the source NAS before system migration and register the same name on the destination NAS after the process.

Destination NAS	Disk volume supported for system migration
1-bay NAS	1-drive single disk volume
2-bay NAS	1 to 2-drive single disk volume, JBOD, RAID 0, 2-drive RAID 1.
4-bay NAS	1 to 4-drive single disk volume, JBOD, RAID 0, 2-drive RAID 1, 3 to 4-drive RAID 5, 4-drive RAID 6, 4-drive RAID 10.
5-bay NAS	1 to 5-drive single disk volume, JBOD, RAID 0, 2-drive RAID 1, 3 to 5-drive RAID 5, 4 to 5-drive RAID 6, 4-drive RAID 10.
6-bay NAS	1 to 6-drive single disk volume, JBOD, RAID 0, 2-drive RAID 1, 3 to 6-drive RAID 5, 4 to 6-drive RAID 6, 4-drive or 6-drive RAID 10.
8-bay NAS	1 to 8-drive single disk volume, JBOD, RAID 0, 2-drive RAID 1, 3 to 8-drive RAID 5, 4 to 8-drive RAID 6, 4-drive, 6-drive, or 8-drive RAID 10.

Follow the steps below to perform system migration.

> **Caution:** To avoid system damage or serious injuries, the system migration procedure should be performed by an authorized server manager or IT administrator.

1. Turn off the source NAS and unplug the hard drives.
2. Remove the hard drives from the old trays and install them to the hard drive trays of the new NAS.
3. Plug the hard drives to the destination NAS (new model). Make sure the hard drives are installed in the original order.
4. Follow the instructions of the Quick Installation Guide (QIG) to connect the power supply and network cable(s) of the new NAS.
5. Turn on the new NAS. Login the web administration interface as an administrator (default login: admin; password: admin).
6. If you are informed to update the firmware of the new NAS, follow the instructions to download and install the firmware.
7. Click "Start Migrating". The NAS will restart after system migration. All the data and settings will be retained.

Some system settings will be removed after system migration due to different system design. Configure the following settings again on the new NAS.

- Windows AD
- Some QPKGs need to be resintalled (e.g. XDove)

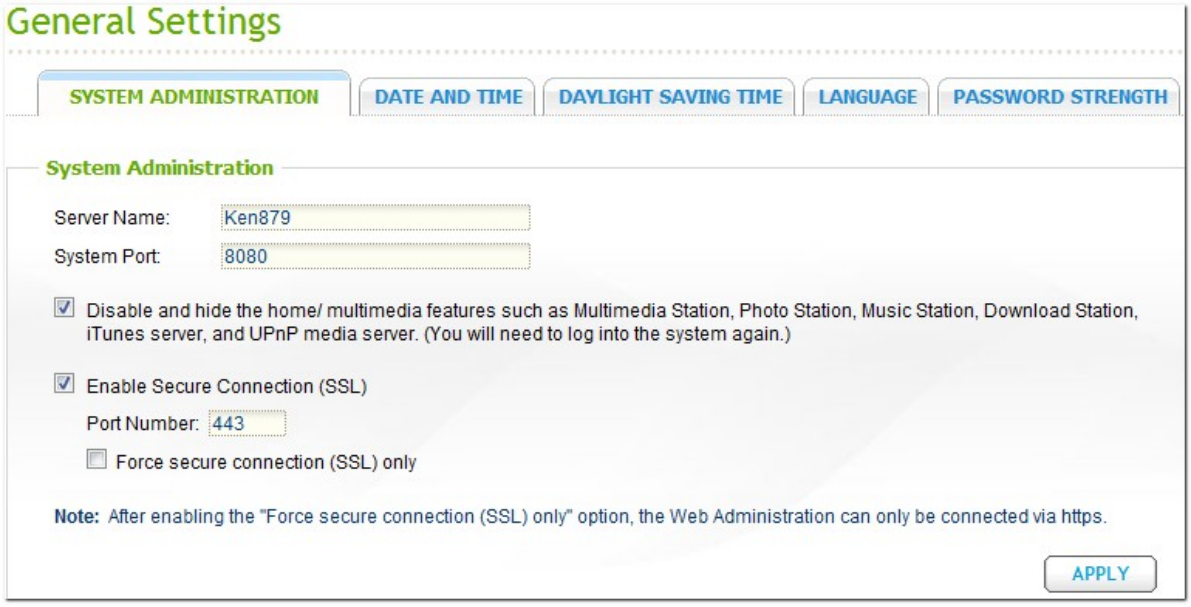
3. System Administration

General Settings 32
Network 36
Service Binding 59
Hardware 61
Security 65
Notification 68
Power Management 75
Network Recycle Bin 77
Backup/Restore Settings 78
System Logs 79
Firmware Update 84
Restore to Factory Default 88

3.1 General Settings

System Administration

Enter the name of the NAS. The NAS name supports maximum 14 characters and can be a combination of the alphabets (a-z, A-Z), numbers (0-9), and dash (-). Space ( ), period (.), or pure number are not allowed.



The home/multimedia features such as Multimedia Station, Photo Station, Music Station, Download Station, iTunes server, and UPnP media server are hidden for the TS-x79 series by default. Select to enable and show or disable and hidden these features. Users are required to re-login the NAS after changing this setting.

Enter a port number 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. If you are not sure about this setting, use the default port number.

Enable Secure Connection (SSL)

To allow the users to connect the NAS by HTTPS, turn on secure connection (SSL) and enter the port number. If the option "Force secure connection (SSL) only" is turned on, the users can only connect to the web administration page by HTTPS connection.

Date and Time

Adjust the date, time, and time zone according to the location of the NAS . If the settings are incorrect, the following problems may occur:

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

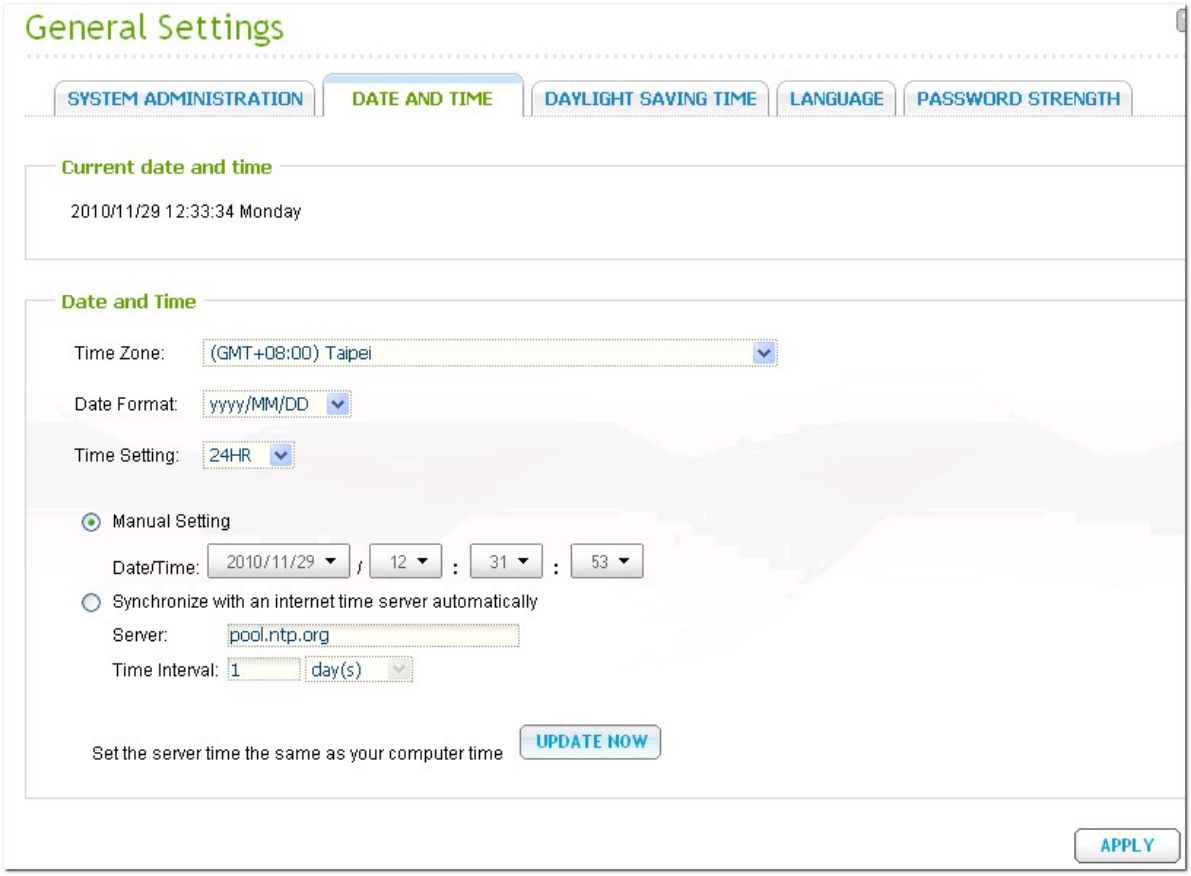
Set the server time the same as your computer time

To synchronize the time of the NAS with the computer time, click "Update now" next to this option.

Synchronize with an Internet time server automatically

Turn on this option to synchronize the date and time of the NAS automatically with an NTP (Network Time Protocol) server. Enter the IP address or domain name of the NTP server, for example, time.nist.gov, time.windows.com. Then enter the time interval for synchronization. This option can be used only when the NAS is connected to the Internet.

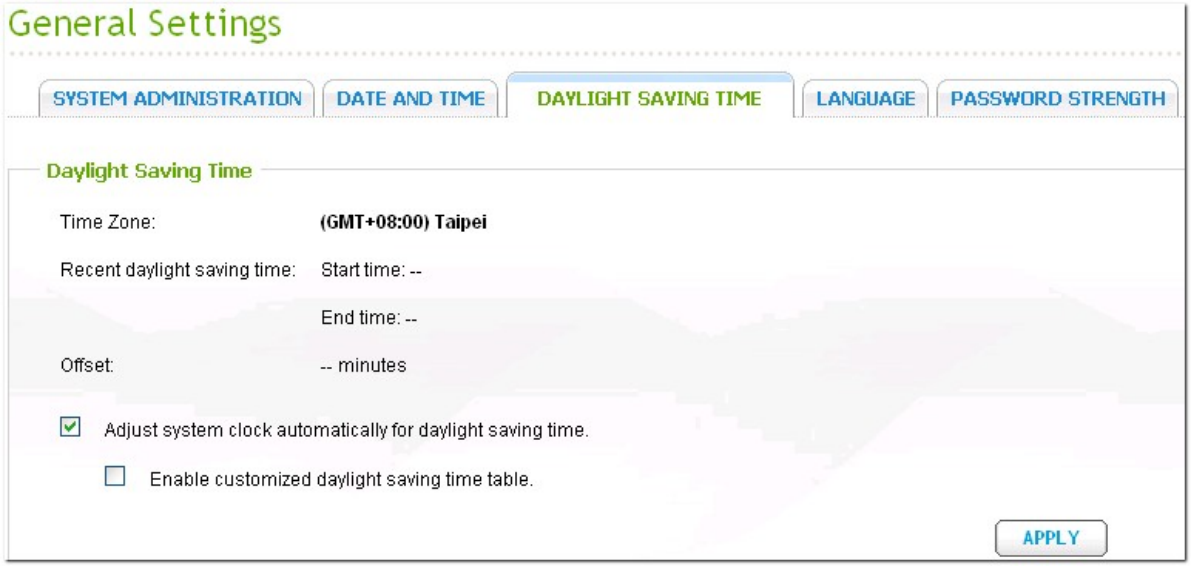
Note: The first time synchronization may take several minutes to complete.



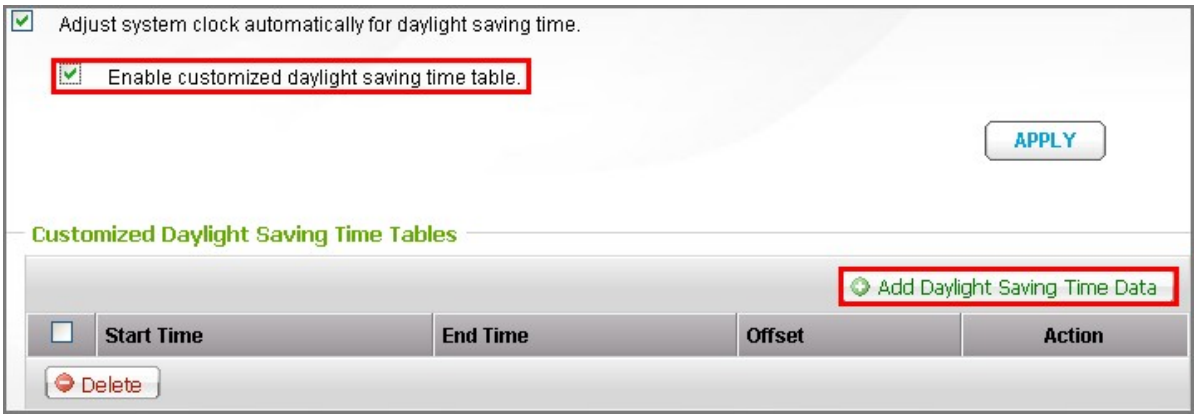
Daylight Saving Time

If your region adopts daylight saving time (DST), turn on the option "Adjust system clock automatically for daylight saving time". Click "Apply". The latest DST schedule of the time zone specified 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.



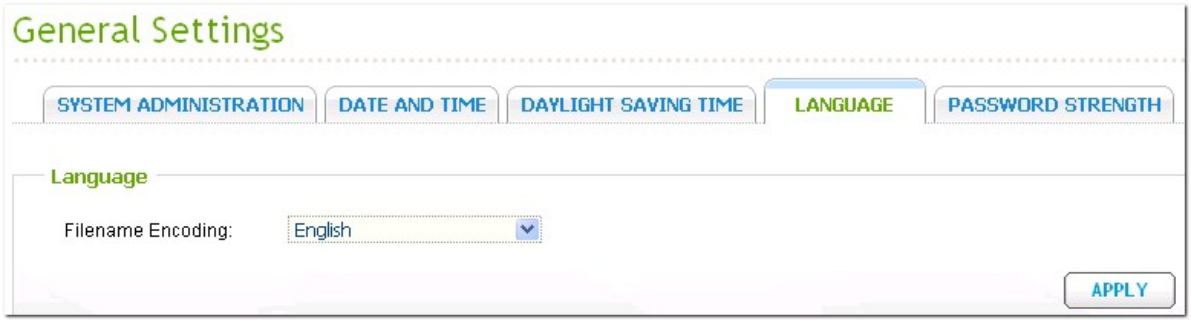
To enter the daylight saving time table manually, select the option "Enable customized daylight saving time table". Click "Add Daylight Saving Time Data" and enter the daylight saving time schedule. Then click "Apply" to save the settings.



Language

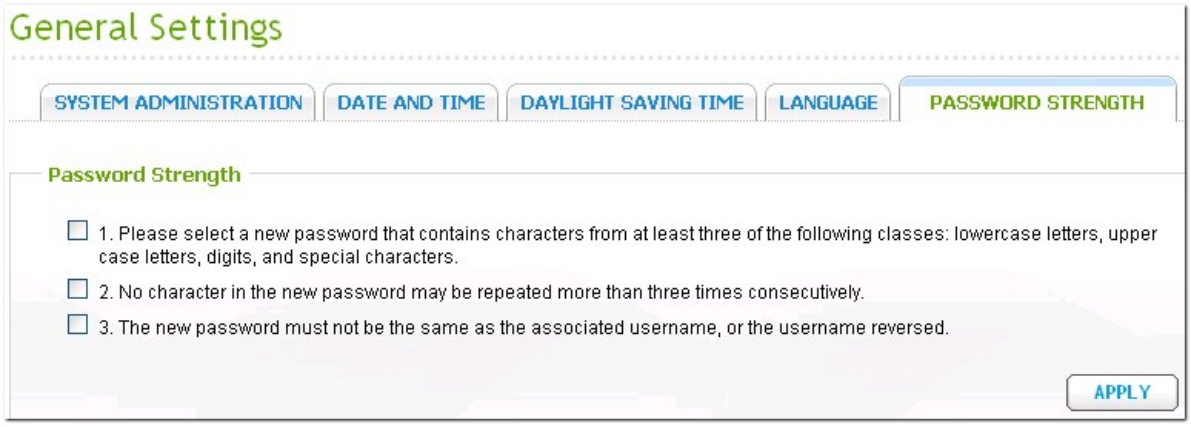
Select the language the NAS uses to display the files and directories.

Note: All the files and directories on the NAS will be created using Unicode encoding. If the FTP clients or the PC OS does not support Unicode, select the language which is the same as the OS language in order to view the files and directories on the NAS properly.



Password Strength

Specify the password rules. After applying the setting, the NAS will automatically check the validity of the password.



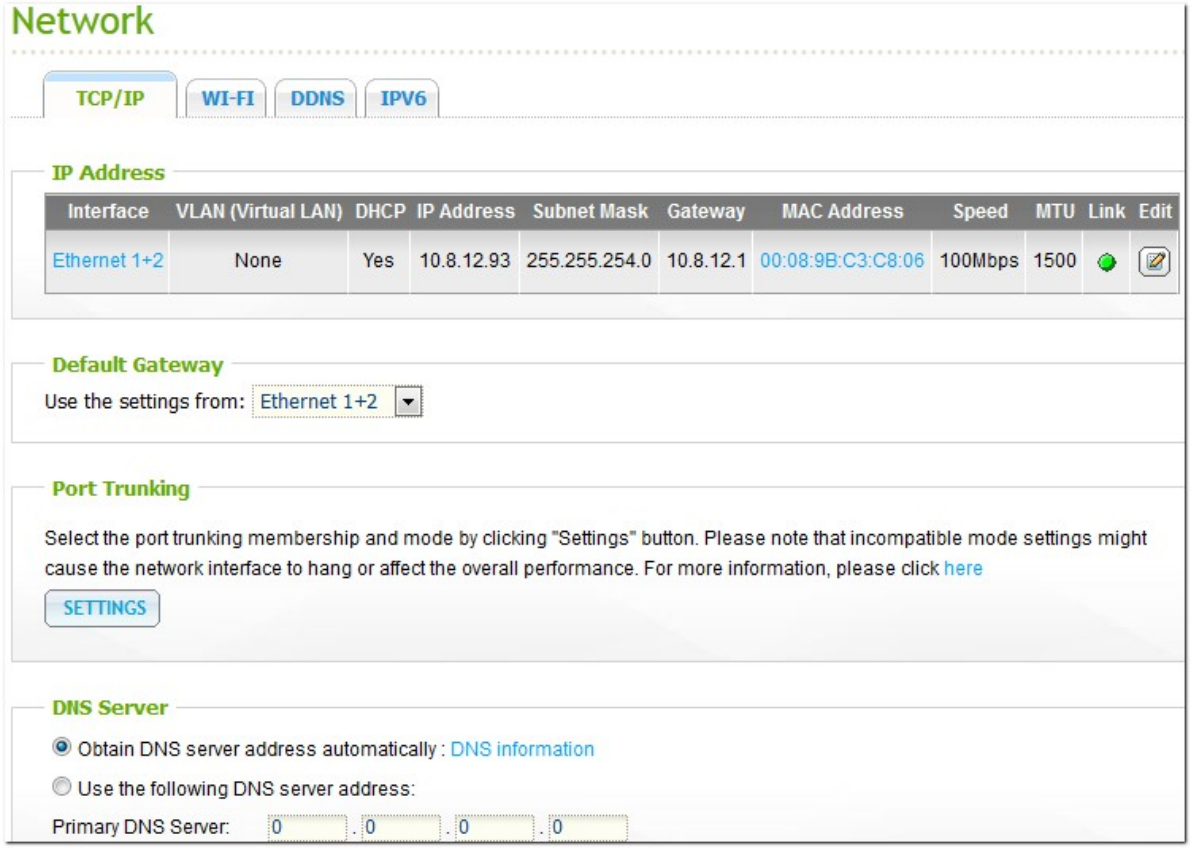
3.2 Network

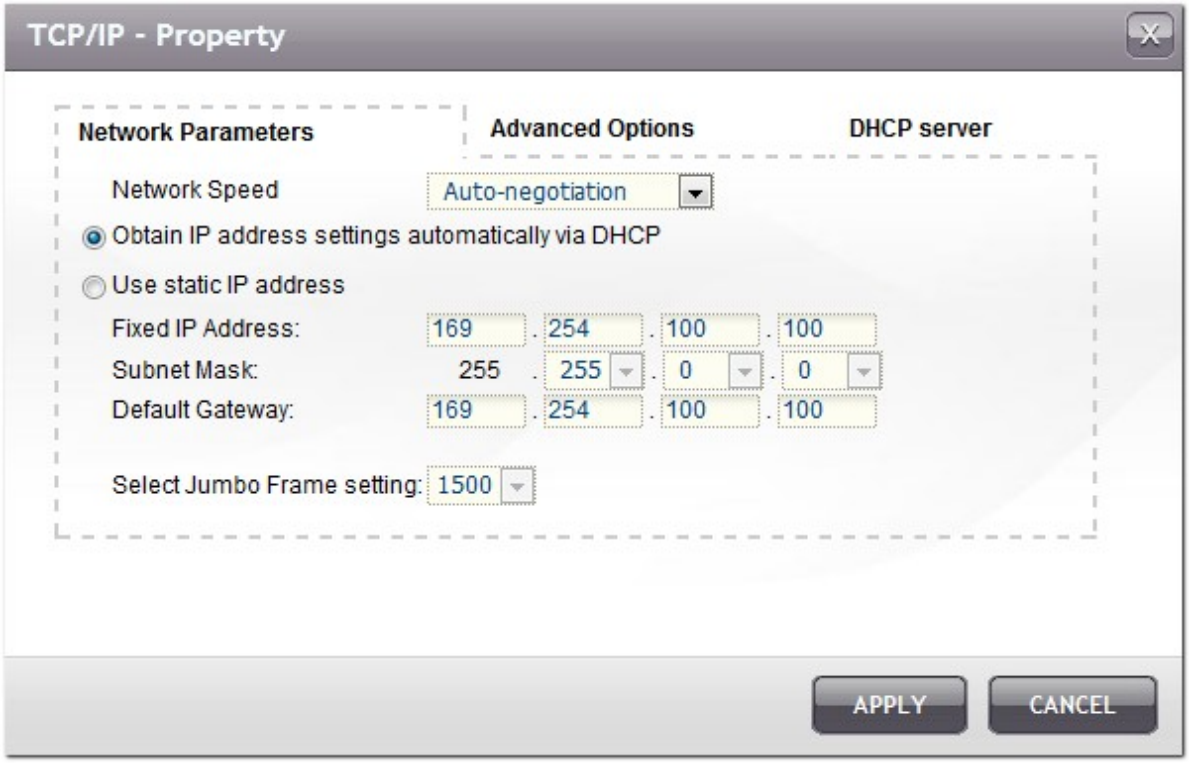
TCP/IP

(i) IP Address

Configure the TCP/IP settings of the NAS on this page. Click the Edit button ( ) to edit the network settings. For the NAS with two LAN ports, users can connect both network interfaces to two different switches and configure the TCP/IP settings. The NAS will acquire two IP addresses which allow access from two different subnets. This is known as multi-IP settings*. When using the Finder to detect the NAS IP, the IP of the Ethernet 1 will be shown in LAN 1 only and the IP of the Ethernet 2 will be shown in LAN 2 only. To use port trunking mode for dual LAN connection, see section (iii).

* TS-110, TS-119, TS-210, TS-219, TS-219P, TS-119P+, TS-219P+, TS-112, TS-212 provide one Giga LAN port only therefore do not support dual LAN configuration or port trunking.





On the TCP/IP Property page, configure the following settings:

Network Speed
Select the network transfer rate according to the network environment to which the NAS is connected. Select auto negotiation and the NAS will adjust the transfer rate automatically.

Obtain the IP address settings automatically via DHCP
If the network supports DHCP, select this option and the NAS will obtain the IP address and network settings automatically.

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

Jumbo Frame Settings (MTU)

This feature is not supported by TS-509 Pro, TS-809 Pro, and TS-809U-RP.

"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 the network appliances support

Jumbo Frame setting, select the appropriate MTU value for the 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.

DHCP Server

A DHCP (Dynamic Host Configuration Protocol) server assigns IP addresses to the clients on a network. Select "Enable DHCP Server" to set the NAS a DHCP server if there is none on the local network where the NAS locates.

Note:

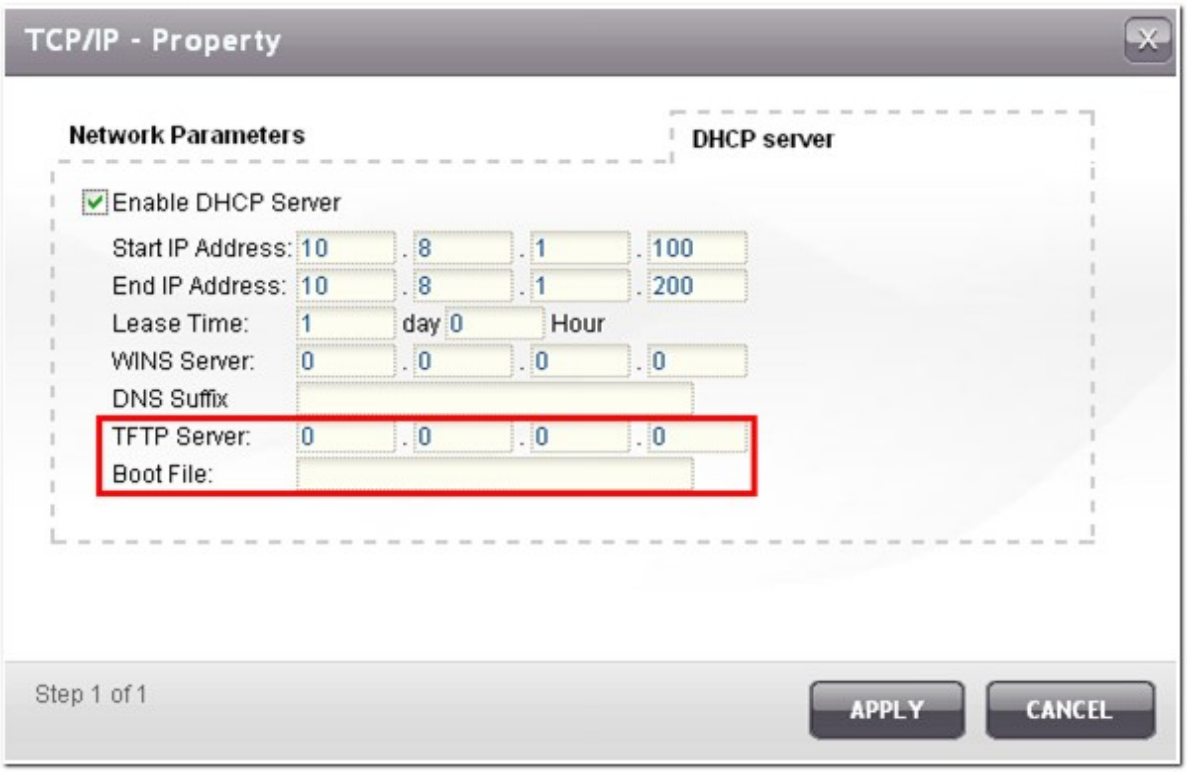
- Do not enable DHCP server if there is one the local network to avoid IP address conflicts or network access errors.
- The DHCP server option is available to Ethernet 1 only when both LAN ports of a dual LAN NAS are connected to the network and configured as standalone IP settings.

Start IP, End IP, Lease Time: Set the range of IP addresses allocated by the NAS to the DHCP clients and the lease time. The lease time refers to the time that an IP address is leased to the clients. During that time, the IP will be reserved to the assigned client. When the lease time expires, the IP can be assigned to another client.

WINS Server (optional): WINS (Windows Internet Naming Service) resolves Windows network computer names (NetBIOS names) to IP addresses, allowing Windows computers on a network to easily find and communicate with each other. Enter the IP address of the WINS server on the network if available.

DNS Suffix (optional): The DNS suffix is used for resolution of unqualified or incomplete host names.

TFTP Server & Boot File (optional): The NAS supports PXE booting of network devices. Enter the IP address of the TFTP server and the boot file (including directory on the TFTP server and file name). For remote booting of the devices, enter the public IP address of the TFTP server.

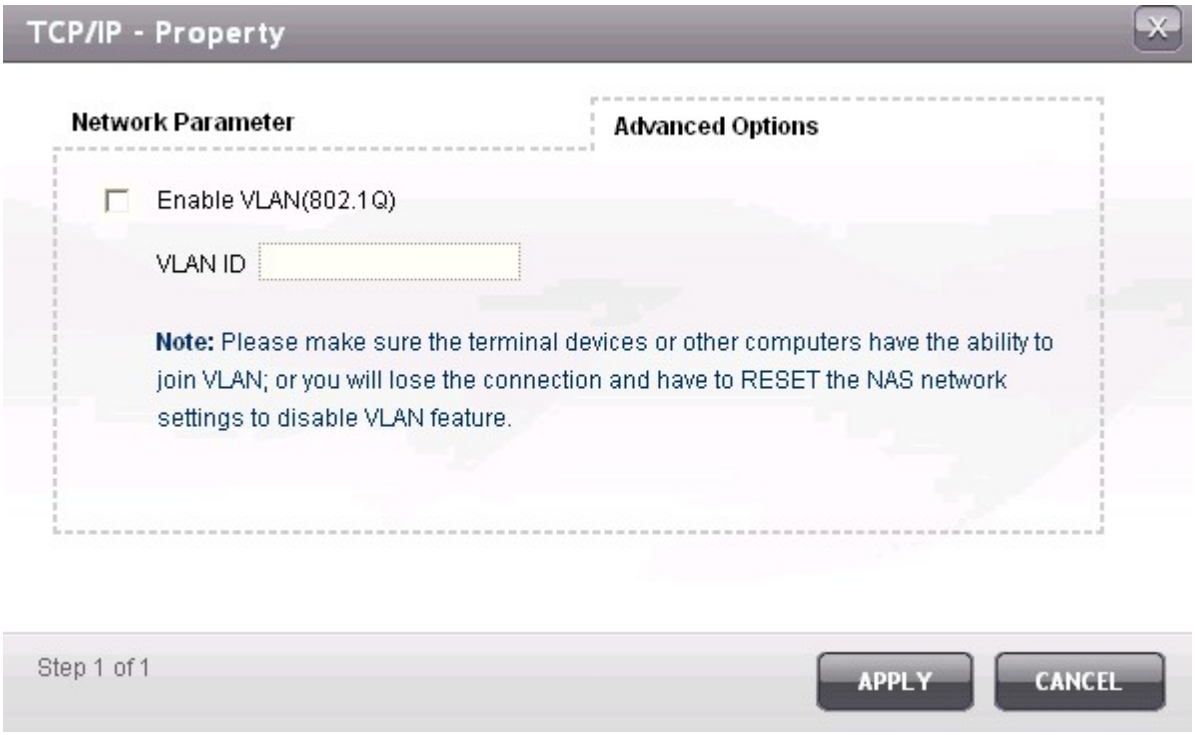

TCP/IP - Property
Network Parameters
DHCP server
Enable DHCP Server
Start IP Address: 10 . 8 . 1 . 100
End IP Address: 10 . 8 . 1 . 200
Lease Time: 1 day 0 Hour
WINS Server: 0 . 0 . 0 . 0
DNS Suffix
TFTP Server: 0 . 0 . 0 . 0
Boot File:
Step 1 of 1
APPLY
CANCEL

Advanced Options

A Virtual LAN (VLAN) is a group of hosts which communicate as if they were attached to the same broadcast domain even if they were located in different physical locations. The NAS can be joined to a VLAN and configured as a backup storage of other devices on the same VLAN.

To join the NAS to a VLAN, select "Enable VLAN" and enter the VLAN ID (a value between 0 and 4094). Please keep the VLAN ID safe and make sure the client devices are able to join the VLAN. If you forgot the VLAN ID and were not able to connect to the NAS, you would need to press the reset button of the NAS to reset the network settings. Once the NAS is reset, the VLAN feature will be disabled. If the NAS supports two Gigabit LAN ports and only one network interface is configured to enable VLAN, you may also connect to the NAS via the other network interface.

Note: The VLAN feature is supported by Intel-based NAS models only. Please visit http://www.qnap.com for details.



(ii) Default Gateway

Select the gateway settings to use if both LAN ports have been connected to the network (dual LAN NAS models only).

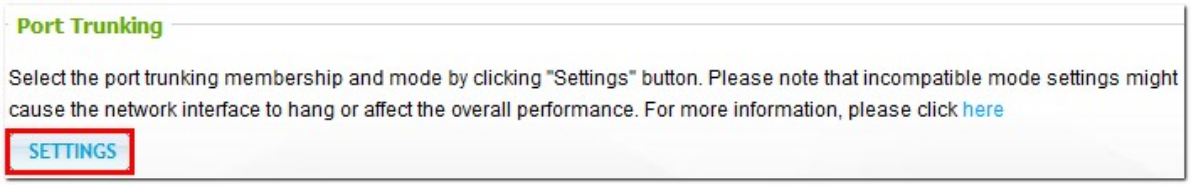
(iii) Port Trunking

Applicable to NAS models with two or more LAN ports only.

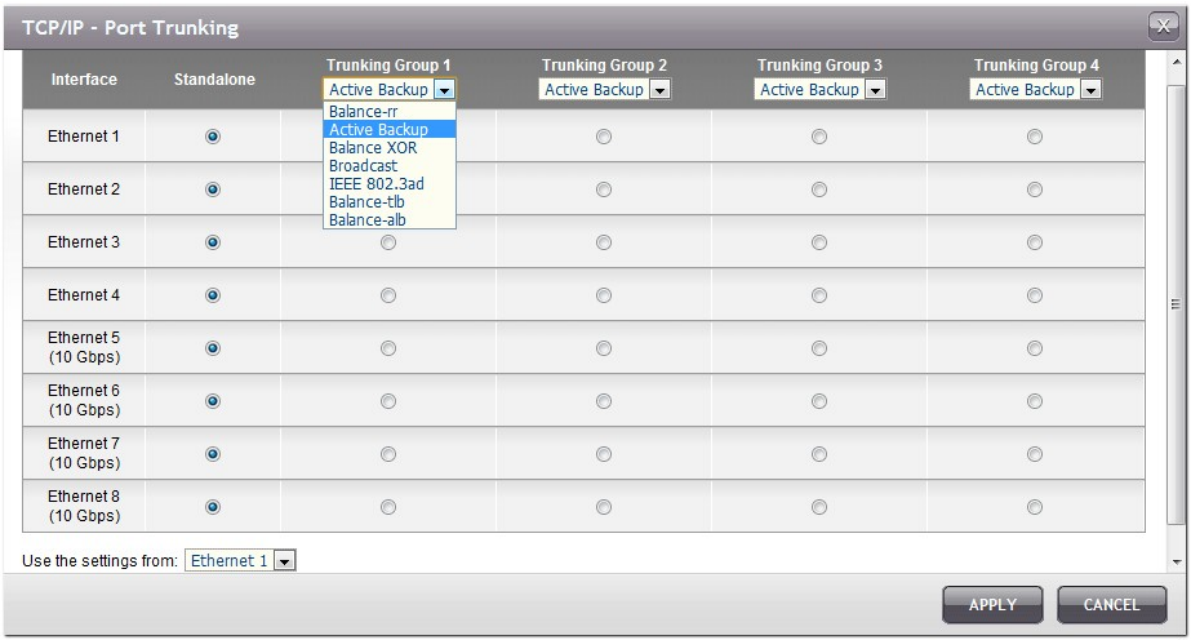
The NAS supports port trunking which combines two Ethernet interfaces into one to increase the bandwidth and offers load balancing and fault tolerance (also known as failover). Load balancing is a feature which distributes the workload evenly across two Ethernet interfaces for higher redundancy. Failover is the capability to switch over to a standby network interface (also known as the slave interface) when the primary network interface (also known as the master interface) does not correspond correctly to maintain high availability.

To use port trunking on the NAS, make sure at least two LAN ports of the NAS have been connected to the same switch and the settings described in sections (i) and (ii) have been configured.
Follow the steps below to configure port trunking on the NAS:

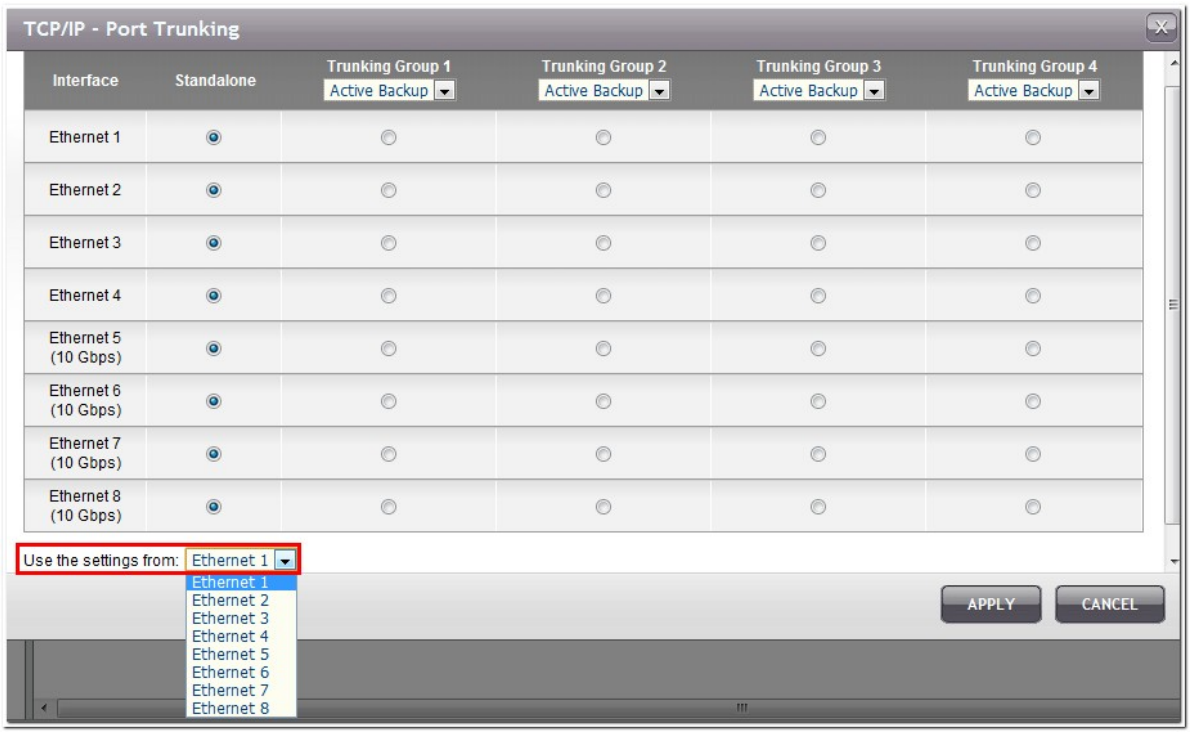
1. Click "Settings".



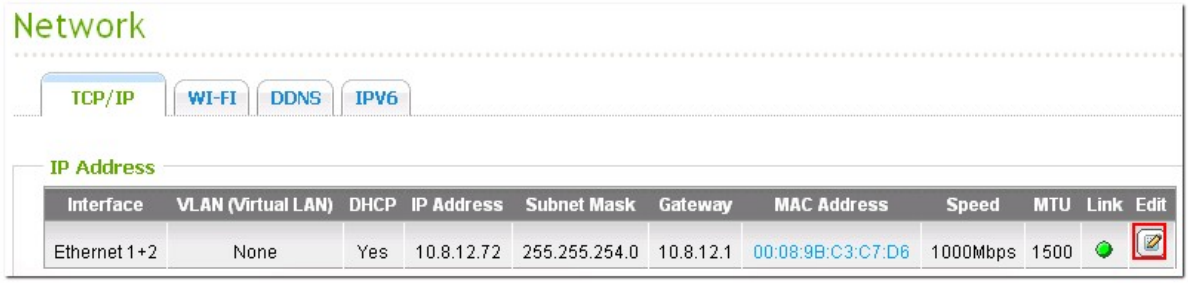
2. Select the network interfaces for a trunking group (Ethernet 1+2, Ethernet 3+4, Ethernet 5+6, or Ethernet 7+8). Choose a port trunking mode from the drop-down menu. The default option is Active Backup (Failover).



3. Select a port trunking group to use. Click "Apply".


TCP/IP - Port Trunking
Interface
Standalone
Trunking Group 1
Active Backup
Trunking Group 2
Active Backup
Trunking Group 3
Active Backup
Trunking Group 4
Active Backup
Ethernet 1
Ethernet 2
Ethernet 3
Ethernet 4
Ethernet 5 (10 Gbps)
Ethernet 6 (10 Gbps)
Ethernet 7 (10 Gbps)
Ethernet 8 (10 Gbps)
Use the settings from:
Ethernet 1
Ethernet 1
Ethernet 2
Ethernet 3
Ethernet 4
Ethernet 5
Ethernet 6
Ethernet 7
Ethernet 8
APPLY
CANCEL

4. Click the Edit button under "IP Address" to edit the network settings.



Note: Make sure the Ethernet interfaces are connected to the correct switch and the switch has been configured to support the port trunking mode selected on the NAS.

The port trunking options available on the NAS:

Field	Description	Switch Required
Balance-rr (Round-Robin)	Round-Robin mode is good for general purpose load balancing between two Ethernet interfaces. This mode transmits packets in sequential order from the first available slave through the last. Balance-rr provides load balancing and fault tolerance.	Supports static trunking. Make sure static trunking is enabled on the switch.
Active Backup	Active Backup uses only one Ethernet interface. It switches to the second Ethernet interface if the first Ethernet interface does not work properly. Only one interface in the bond is active. The bond's MAC address is only visible externally on one port (network adapter) to avoid confusing the switch. Active Backup mode provides fault tolerance.	General switches
Balance XOR	Balance XOR balances traffic by splitting up outgoing packets between the Ethernet interfaces, using the same one for each specific destination when possible. It transmits based on the selected transmit hash policy. The default policy is a simple slave count operating on Layer 2 where the source MAC address is coupled with destination MAC address. Alternate transmit policies may be selected via the xmit_hash_policy option. Balance XOR mode provides load balancing and fault tolerance.	Supports static trunking. Make sure static trunking is enabled on the switch.
Broadcast	Broadcast sends traffic on both network interfaces. This mode provides fault tolerance.	Supports static trunking. Make sure static trunking is enabled on the switch.
IEEE 802.3ad (Dynamic Link Aggregation)	Dynamic Link Aggregation uses a complex algorithm to aggregate adapters by speed and duplex settings. It utilizes all slaves in the active aggregator according to the 802.3ad specification. Dynamic Link Aggregation mode provides load balancing and fault tolerance but requires a switch that supports IEEE 802.3ad with LACP mode properly configured.	Supports 802.3ad LACP
Balance-tlb (Adaptive Transmit Load Balancing)	Balance-tlb uses channel bonding that does not require any special switch. The outgoing traffic is distributed according to the current load on each Ethernet interface (computed relative to the speed). Incoming traffic is received by the current Ethernet interface. If the receiving Ethernet interface fails, the other slave takes over the MAC address of the failed receiving slave. Balance-tlb mode provides load balancing and fault tolerance.	General switches

Balance-alb (Adaptive Load Balancing)	Balance-alb is similar to balance-tlb but also attempts to redistribute incoming (receive load balancing) for IPV4 traffic. This setup does not require any special switch support or configuration. The receive load balancing is achieved by ARP negotiation sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the Ethernet interfaces in the bond such that different peers use different hardware address for the server. This mode provides load balancing and fault tolerance.	General switches

(iv) 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:

- Please contact the 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, for example, BT download, enter at least one DNS server IP for proper URL connection. Otherwise, the function may not work properly.
- If you select to obtain the IP address by DHCP, there is no need to configure the primary and the secondary DNS servers. In this case, enter "0.0.0.0".

Wi-Fi

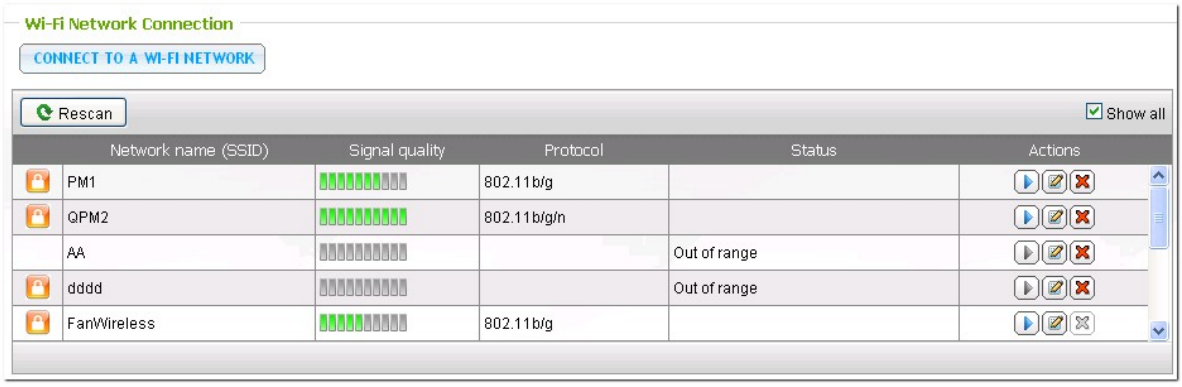
To connect the NAS to a Wi-Fi network, plug in a wireless dongle into a USB port of the NAS. The NAS will detect a list of wireless access points. You can connect the NAS to the Wi-Fi network in two ways.

Note:

- The wireless connection performance depends on many factors such as the adapter model, the USB adapter's performance, and the network environment. For higher connection performance, you are recommended to use wired connection.
- The system supports only one USB Wi-Fi dongle at a time.

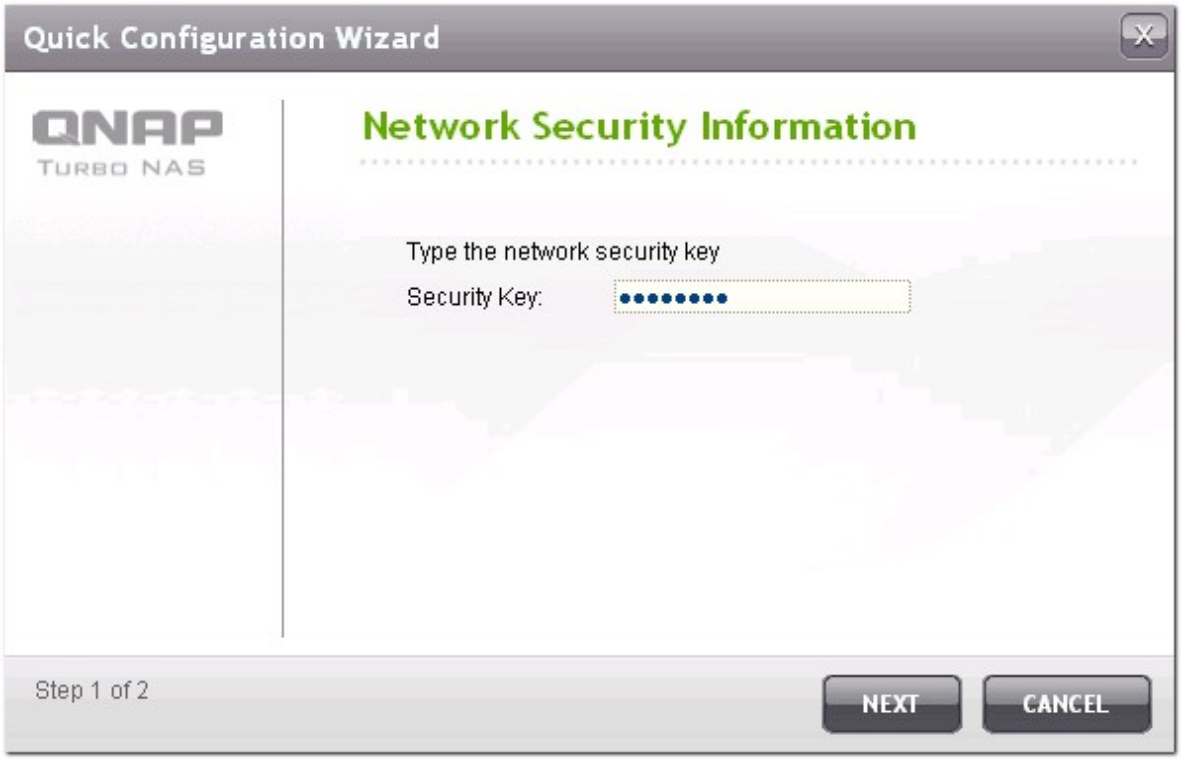
1. Connect to an existing Wi-Fi network:

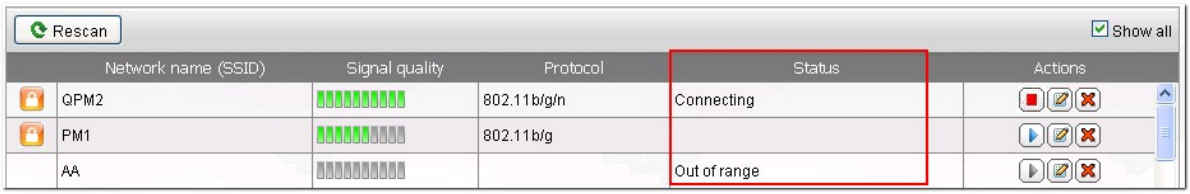
A list of Wi-Fi access points with signal strength are displayed on the "Wi-Fi Network Connection" panel.



Icons and Options	Description
Rescan	To search for the Wi-Fi networks in range.
(Secured network)	This icon shows that the Wi-Fi network requires a network key; enter the key to connect to the network.
(Connect)	To connect to Wi-Fi network. If a security key is required, you will be prompted to enter the key.
(Edit)	To edit the connection information. You may also select to connect to the Wi-Fi network automatically when it is in range.
(Disconnect)	To disconnect from the Wi-Fi network.
(Remove)	To delete the Wi-Fi network profile from the panel.
Show all	Select this option to display all the available Wi-Fi networks. Unselect this option to show only the configured network profiles.

Click “Rescan” to search for available Wi-Fi networks in range. Select a Wi-Fi network to connect to and click the Connect button ( ). Enter the security key if it is a security-key enabled network. Click “Next” and the NAS will attempt to connect to the wireless network.



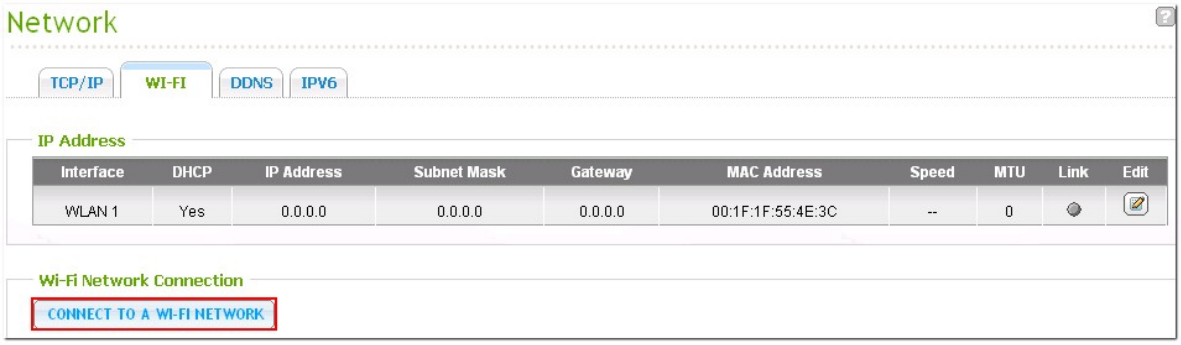


You can view the status of the configured network profiles.

Message	Description
Connected	The NAS is currently connected to the Wi-Fi network.
Connecting	The NAS is trying to connect to the Wi-Fi network.
Out of range or hidden SSID	The wireless signal is not available or the SSID is not broadcast.
Failed to get IP	The NAS is connected to the Wi-Fi network but could not get an IP address from the DHCP server. Please check the router settings.
Association failed	The NAS cannot connect to the Wi-Fi network. Please check the router settings.
Incorrect key	The security key entered is incorrect.
Auto connect	Automatically connect to the Wi-Fi network if it is in range. The auto connection function is not supported if the SSID of the Wi-Fi network is not broadcast.

2. Manually connect to a Wi-Fi network:

To manually connect to a Wi-Fi network that does not broadcast its SSID (network name), click "CONNECT TO A Wi-Fi NETWORK".



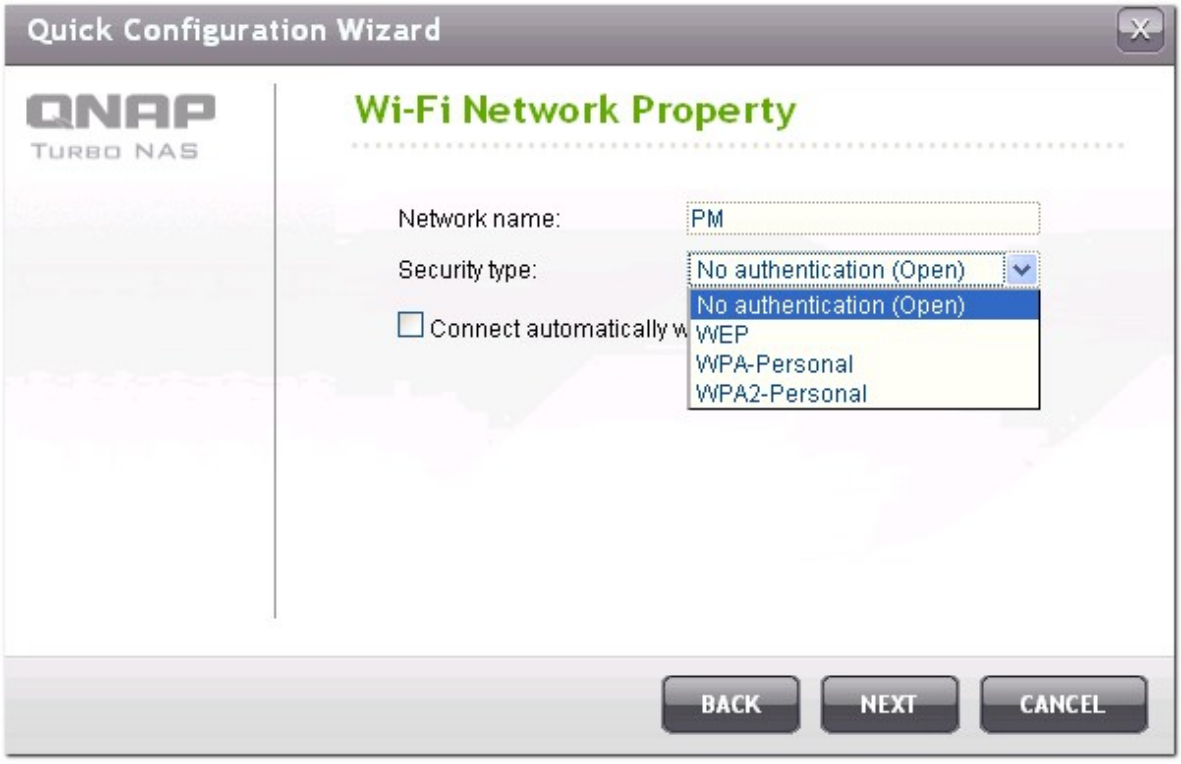
You can choose to connect to an ad hoc network in which you can connect to any wireless devices without the need for an access point.

Enter the network name (SSID) of the wireless network and select the security type.

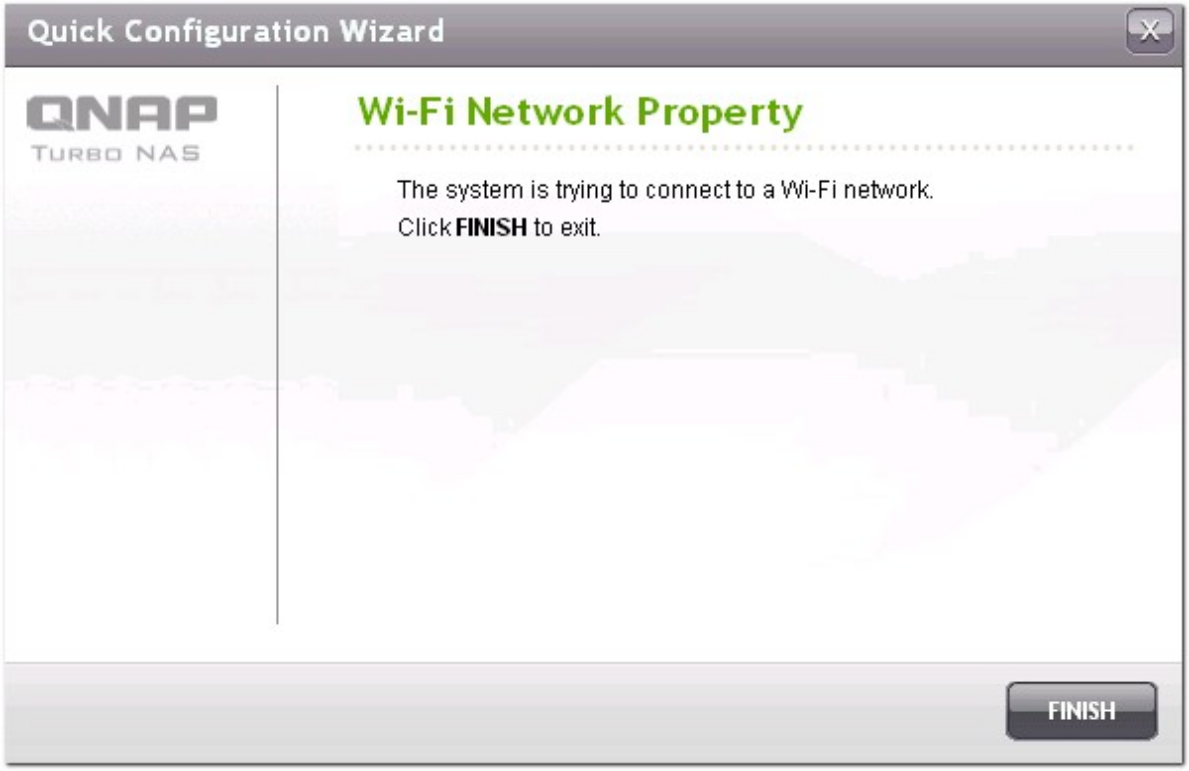
- No authentication (Open): No security key required.
- WEP: Enter up to 4 WEP keys and choose 1 key to be used for authentication.
- WPA-Personal: Choose either the AES or TKIP encryption type and enter the encryption key.
- WPA2-Personal: Enter a security key.

Note:

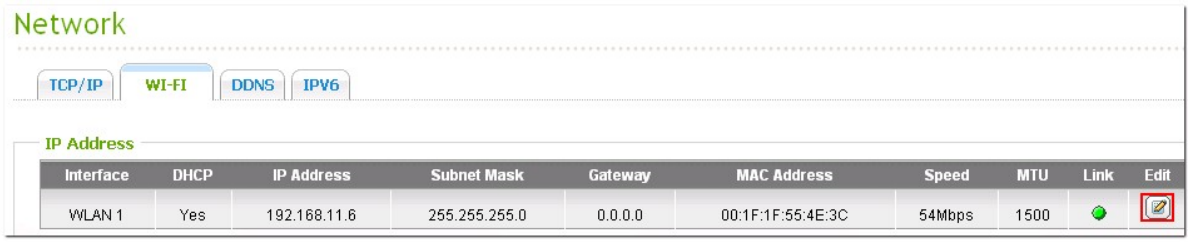
- The WEP key must be exactly 5 or 13 ASCII characters; or exactly 10 or 26 hexadecimal characters (0-9 and A-F).
- If you have trouble connecting to an encrypted wireless network, check the wireless router/AP settings and change the transfer rate from "N-only" mode to "B/G/N mixed" or similar settings.
- Users of Windows 7 with WPA2 encryption cannot establish ad-hoc connection with the NAS. Please change to use WEP encryption on Windows 7.
- A fixed IP address is required for the wireless interface in order to establish an ad-hoc connection.



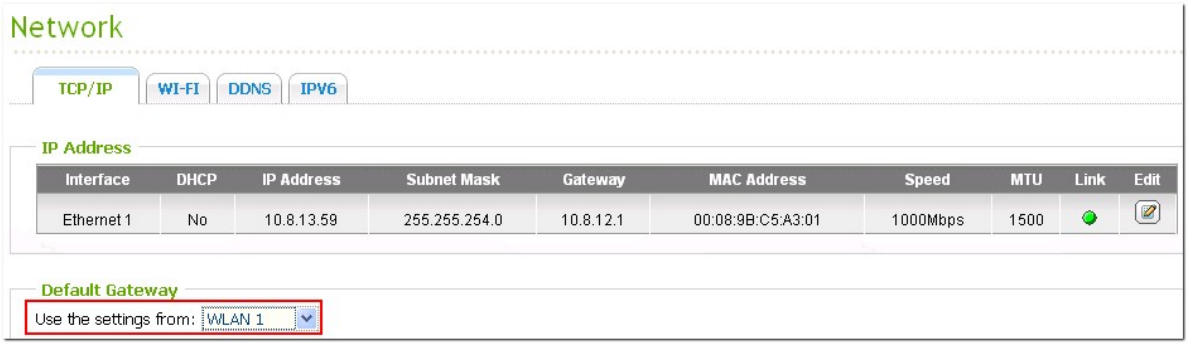
Click "Finish" after the NAS has added the Wi-Fi network.



To edit the IP address settings, click the Edit button . You can select to obtain the IP address automatically by DHCP or configure a fixed IP address.



If the Wi-Fi connection is the only connection between the NAS and the router/AP, you must select "WLAN1" as the default gateway in "Network" > "TCP/IP" page. Otherwise, the NAS will not be able to connect to the Internet or communicate with another network.

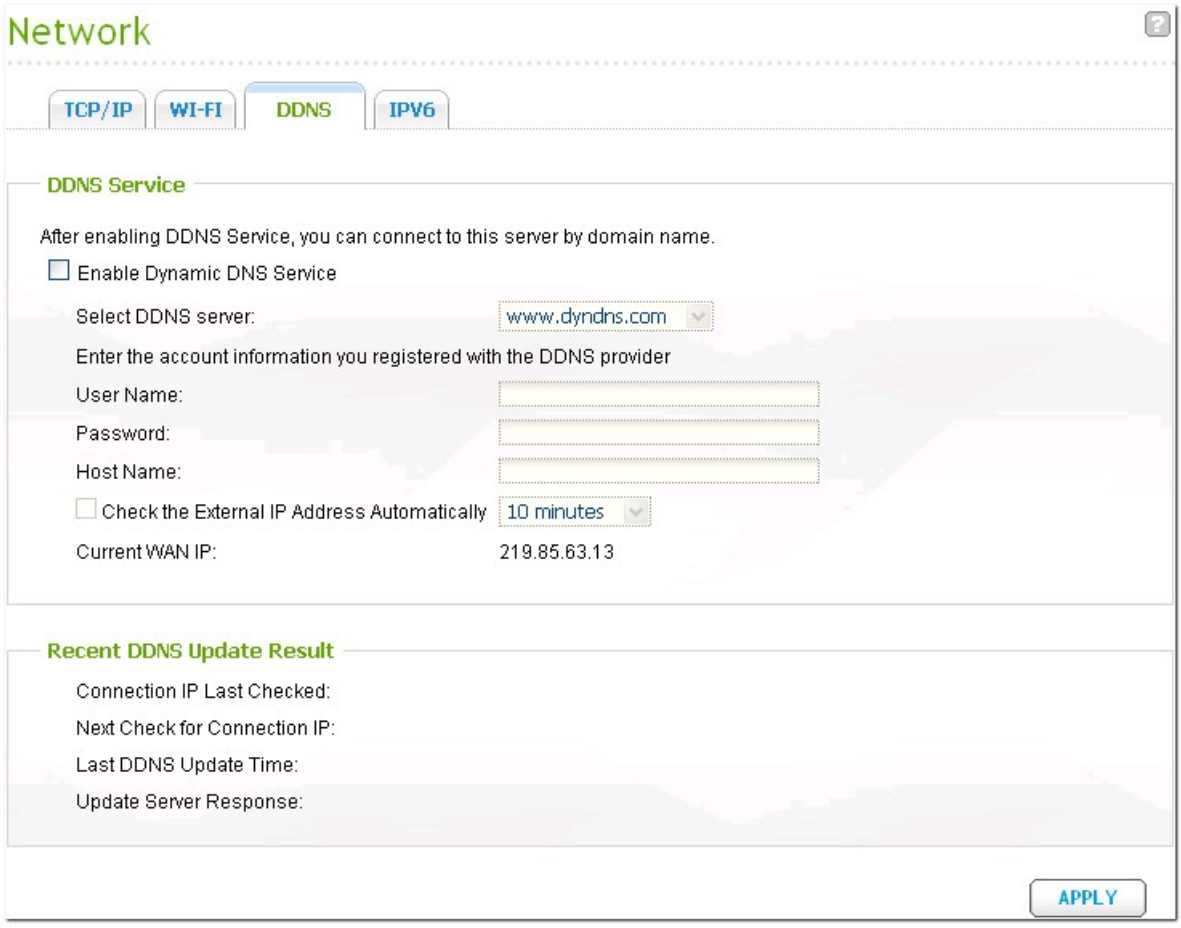


DDNS

To allow remote access to the NAS using a domain name instead of a dynamic IP address, enable the DDNS service.

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

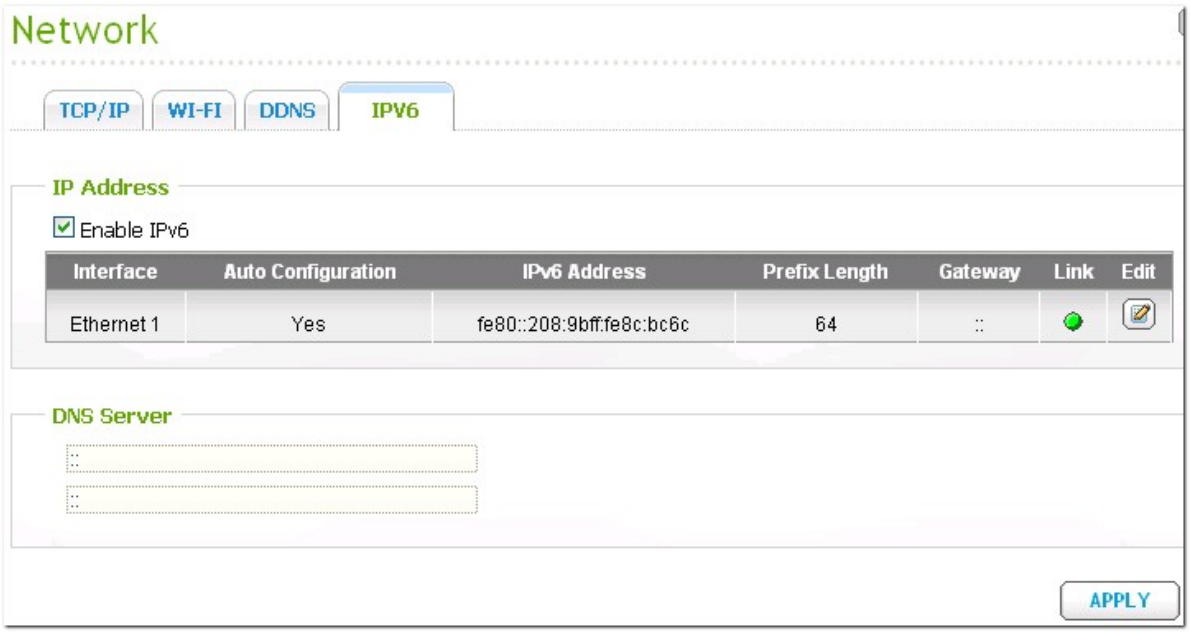
For the information of setting up the DDNS and port forwarding on the NAS, see here 649.



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 NAS services which support IPv6 include:

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



To use this function, select the option "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 the Edit button to edit the settings.

IPv6 Auto Configuration

If an IPv6 enabled router is available 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.

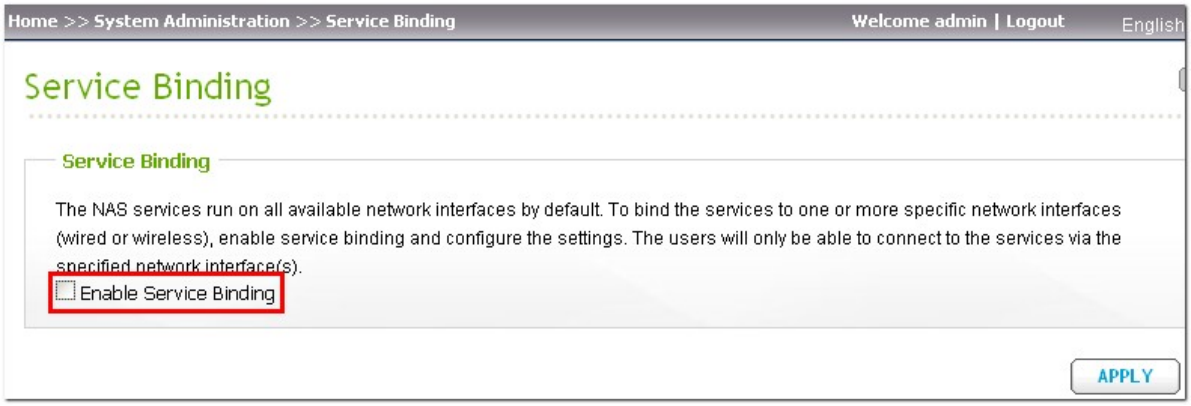
IPv6 DNS server

Enter the preferred DNS server in the upper field and the alternate DNS server in the lower field. Contact the ISP or network administrator for the information. If IPv6 auto configuration is selected, leave the fields as "::".

3.3 Service Binding

Note: The service binding feature is only available for the NAS with more than one network interfaces (wired and wireless).

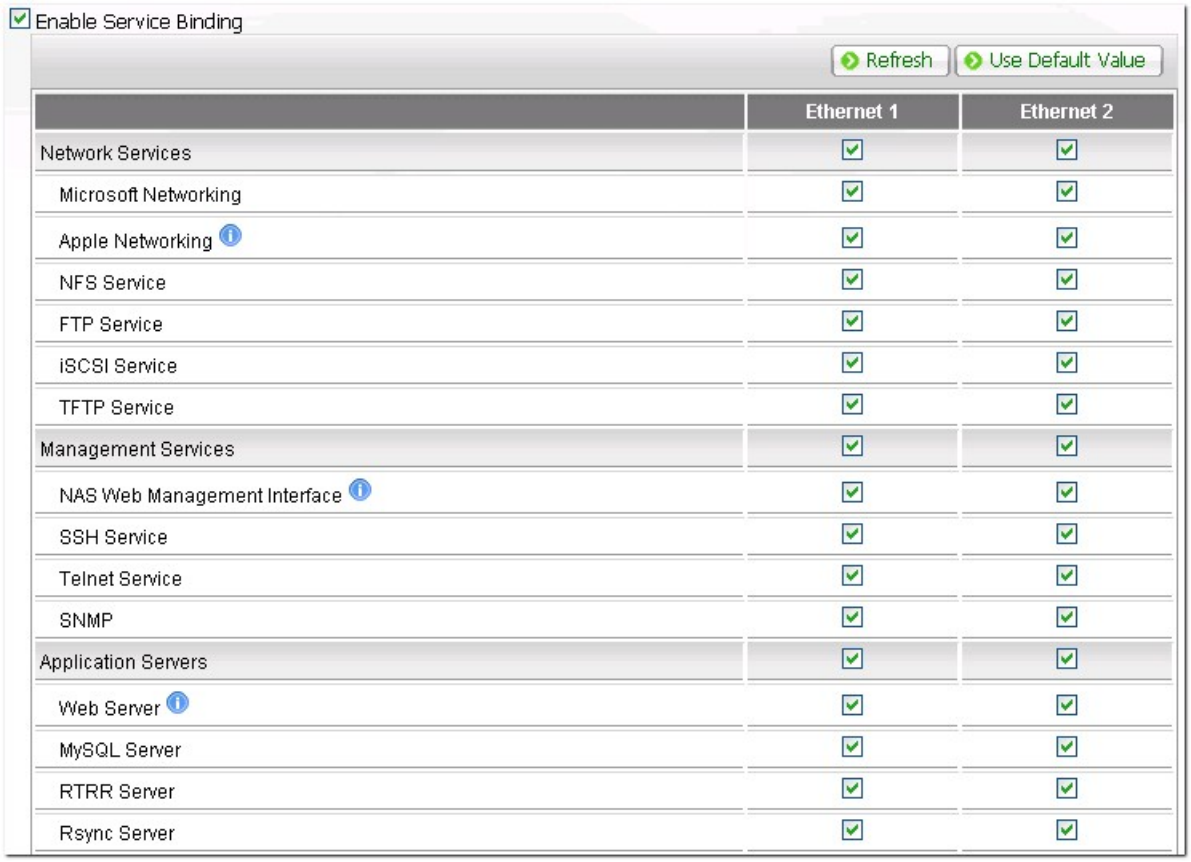
The NAS services run on all available network interfaces by default. To bind the services to one or more specific network interfaces (wired or wireless), enable service binding.



The available network interfaces on the NAS will be shown. All the NAS services run on all network interfaces by default. Select at least one network interface that each service should be bound to. Then click "Apply". The users will only be able to connect to the services via the specified network interface (s).

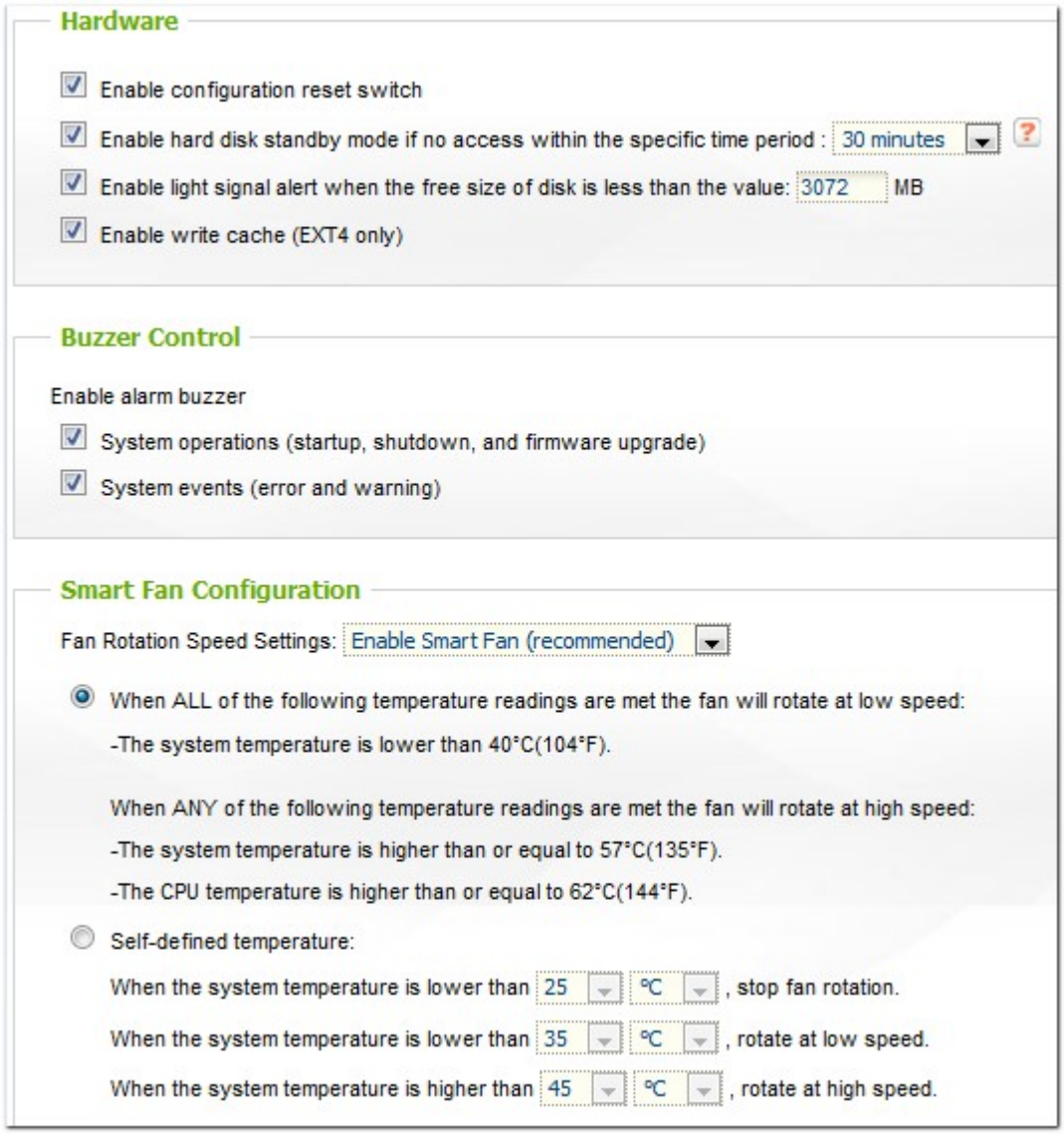
If the settings cannot be applied, click "Refresh" to list the current network interfaces on the NAS and configure service binding again.

Note: After applying the service binding settings, the connection of the currently online users will be kept even if they were not connecting to the services via the specified network interface(s). The specified network interface(s) will be used for the next connected session.



3.4 Hardware

Configure the hardware functions of the NAS.



Enable configuration reset switch

When this function is turned on, you can press the reset button for 3 seconds to reset the administrator password and the system settings to default. The disk data will be retained.

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)

After pressing the reset button for 3 seconds, a beep sound will be heard. The following settings will be 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)*.
- VLAN will be disabled.
- Service binding: All NAS services run on all available network interfaces.

*This feature is only provided by the NAS models with LCD panels. Please visit http://www.qnap.com for details.

Advanced system reset (10 sec)

After pressing 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 the 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 shares previously created will be cleared. To retrieve the old data after advanced system reset, create the same network shares on the NAS and the data will be accessible again.

Enable hard disk standby mode

This option allows the hard drives on the NAS to enter standby mode if there is no disk 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 option is turned on and the free space of the SATA hard drive is less than the value. The valid range of the value is 1-51200 MB.

Enable write cache (EXT4 only)

If the disk volume of the NAS is formatted as EXT4, turn on this option for higher write performance. Note that an unexpected system shutdown may lead to incomplete data transfer when data write is in process. This option will be turned off when any of the following services is enabled: Download Station, MySQL service, user quota, and Surveillance Station. You are recommended to turn this option off if the NAS is set as a shared storage in a virtualized or clustered environment.

Enable alarm buzzer

Turn on this option to allow the alarm buzzer to beep when certain system operations (startup, shutdown, or firmware upgrade) are executed or system events (error or warning) occur.

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 will be automatically adjusted when the NAS 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 warning alert for redundant power supply on the web-based interface:

If two power supply units (PSU) are installed on the NAS and connected to the power sockets, both PSU will supply the power to the NAS (applied to 1U and 2U models). Turn on the redundant power supply mode in "System Administration" > "Hardware" to receive warning alert for the redundant power supply. The NAS will sound and record the error messages in "System Logs" when the PSU is plugged out or does not correspond correctly.

If only one PSU is installed on the NAS, do NOT enable this option.

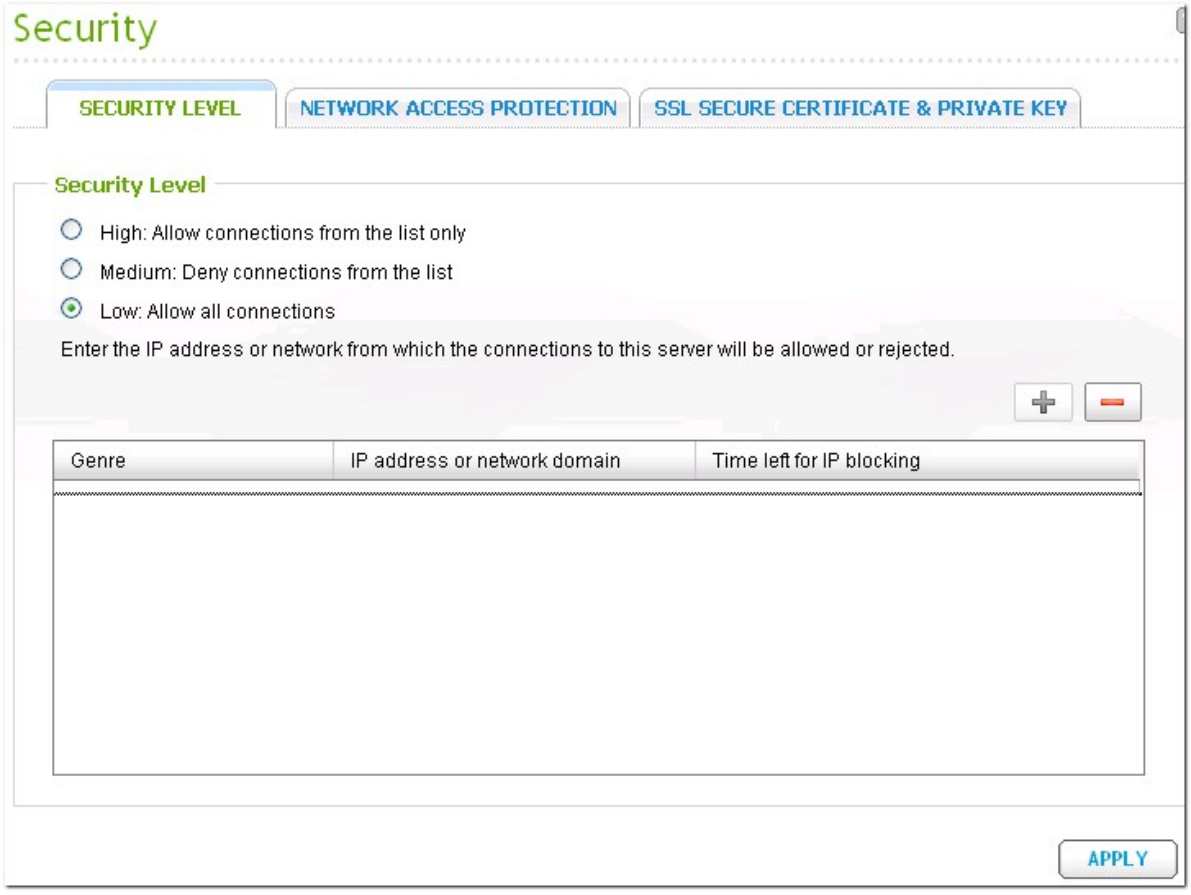
* This function is disabled by default.

3.5 Security

Security Level

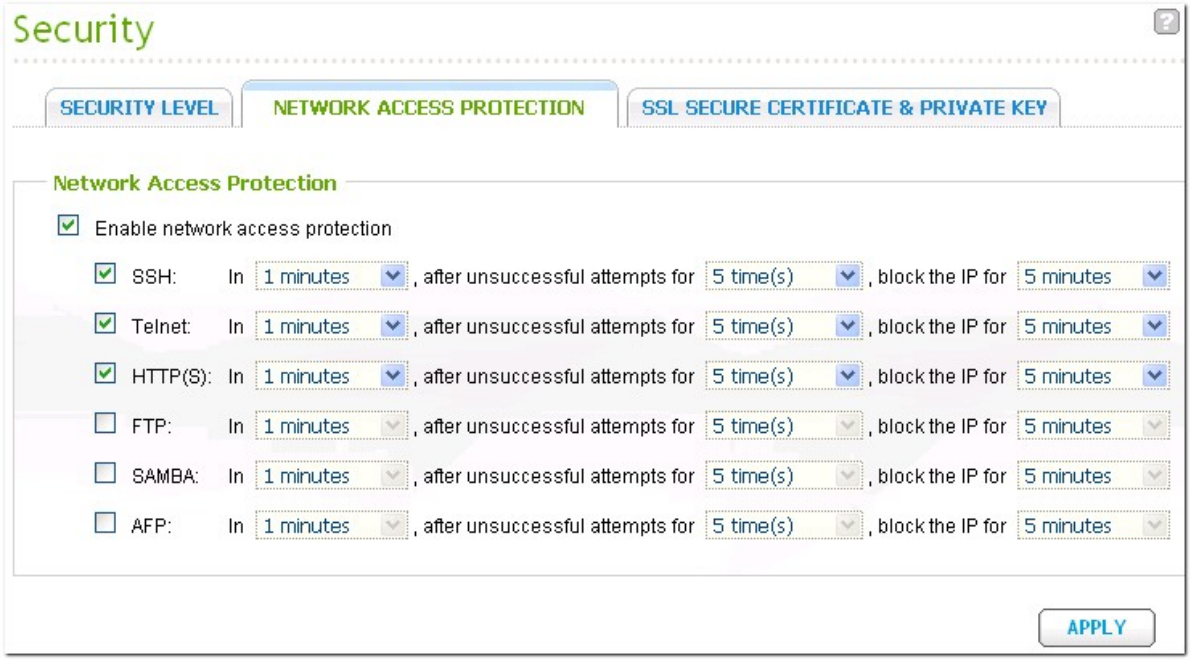
Specify the IP address or the network domain from which the connections to the NAS are allowed or denied. When the connection of a host server is denied, all the protocols of that server are not allowed to connect to the NAS.

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



Network Access Protection

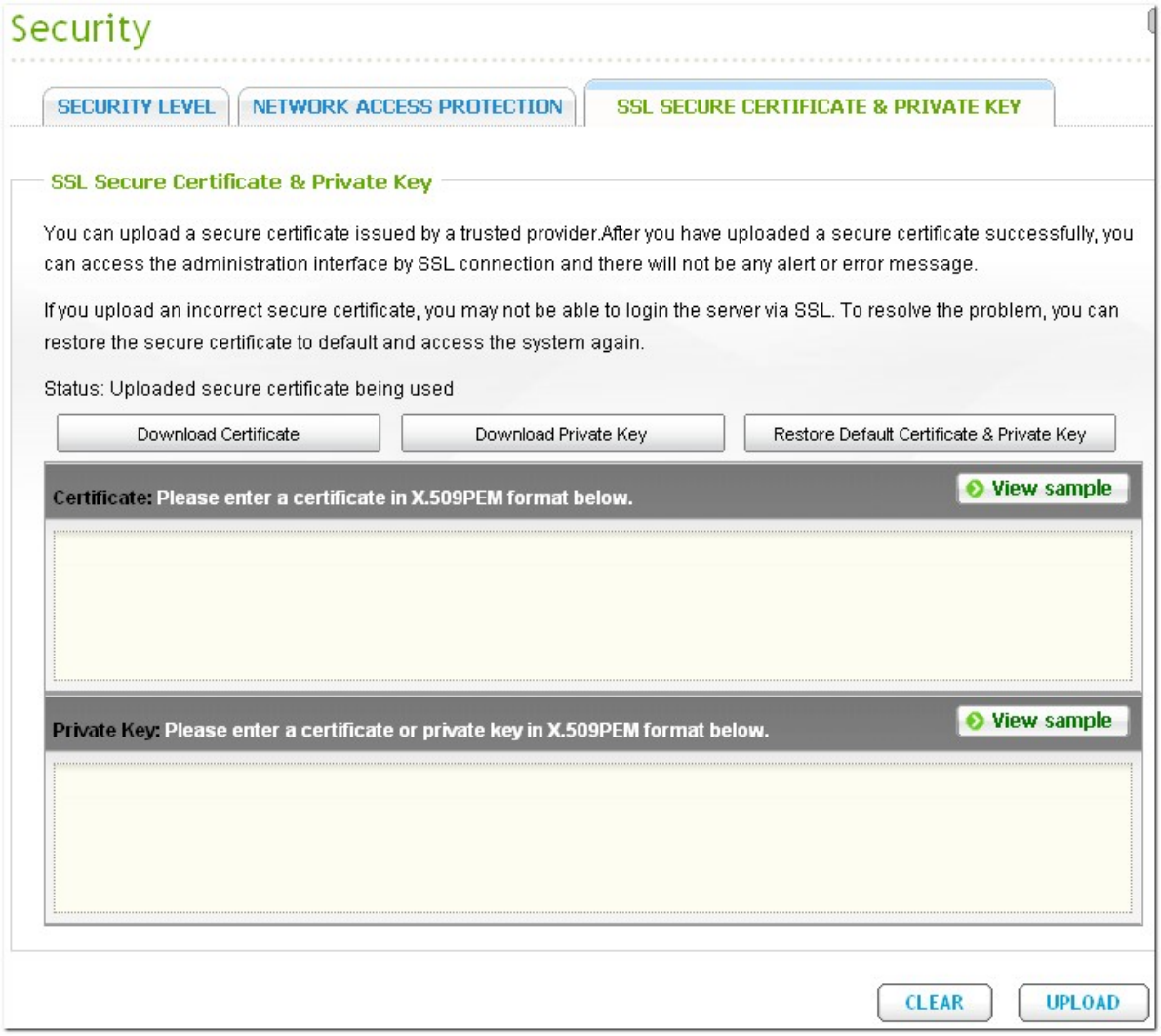
The network access protection enhances system security and prevents unwanted intrusion. You can block an IP for a certain period of time or forever if the IP fails to login the NAS from a particular connection method.



Import SSL Secure Certificate

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

- Download Certificate: To download the secure certificate which is currently in use.
- Download Private Key: To download the private key which is currently in use.
- Restore Default Certificate & Private Key: To restore the secure certificate and private key to system default. The secure certificate and private key in use will be overwritten.

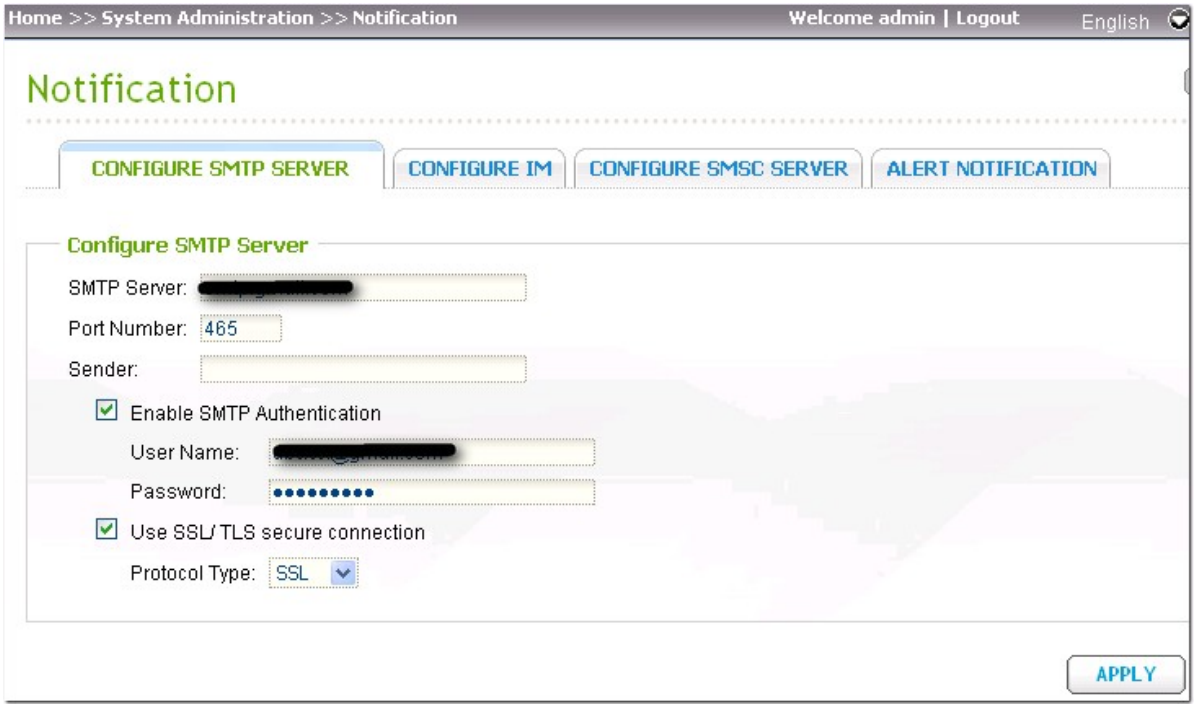


3.6 Notification

Configure SMTP Server

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

- SMTP Server: Enter the SMTP server name, for example, 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: When this function is turned on, the system will request the authentication of the mail server before a message is sent.
- User Name and Password: Enter the login information of the email account.
- Use SSL/TLS secure connection: If the SMTP server supports this function, turn it on.



Configure IM

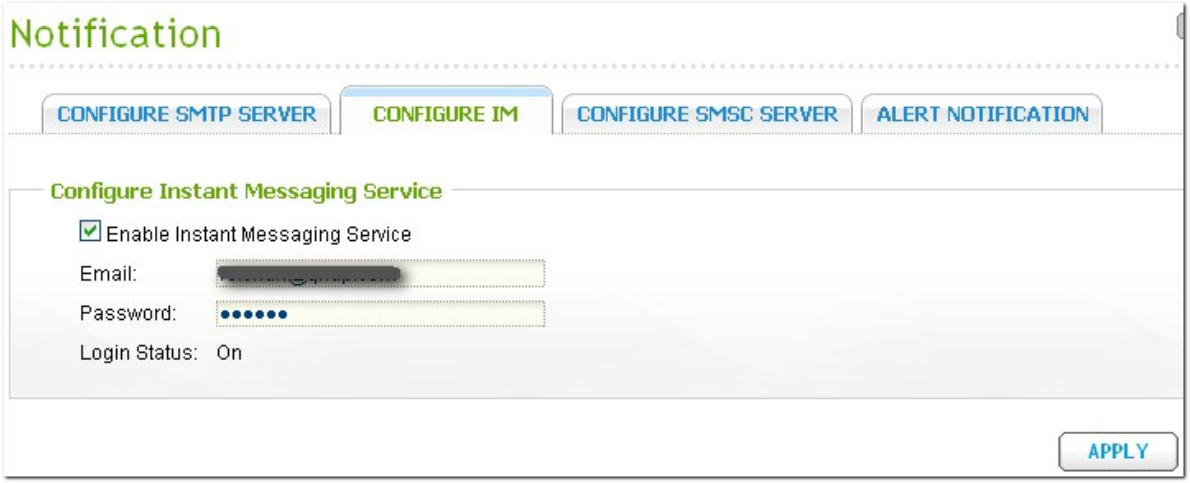
The NAS supports instant messaging (IM) service to allow multiple authorized Windows Live Messenger contacts to receive instant system error or warning messages and enter commands in the Windows Live Messenger conversation to inquire real-time system information from the NAS.

Note:

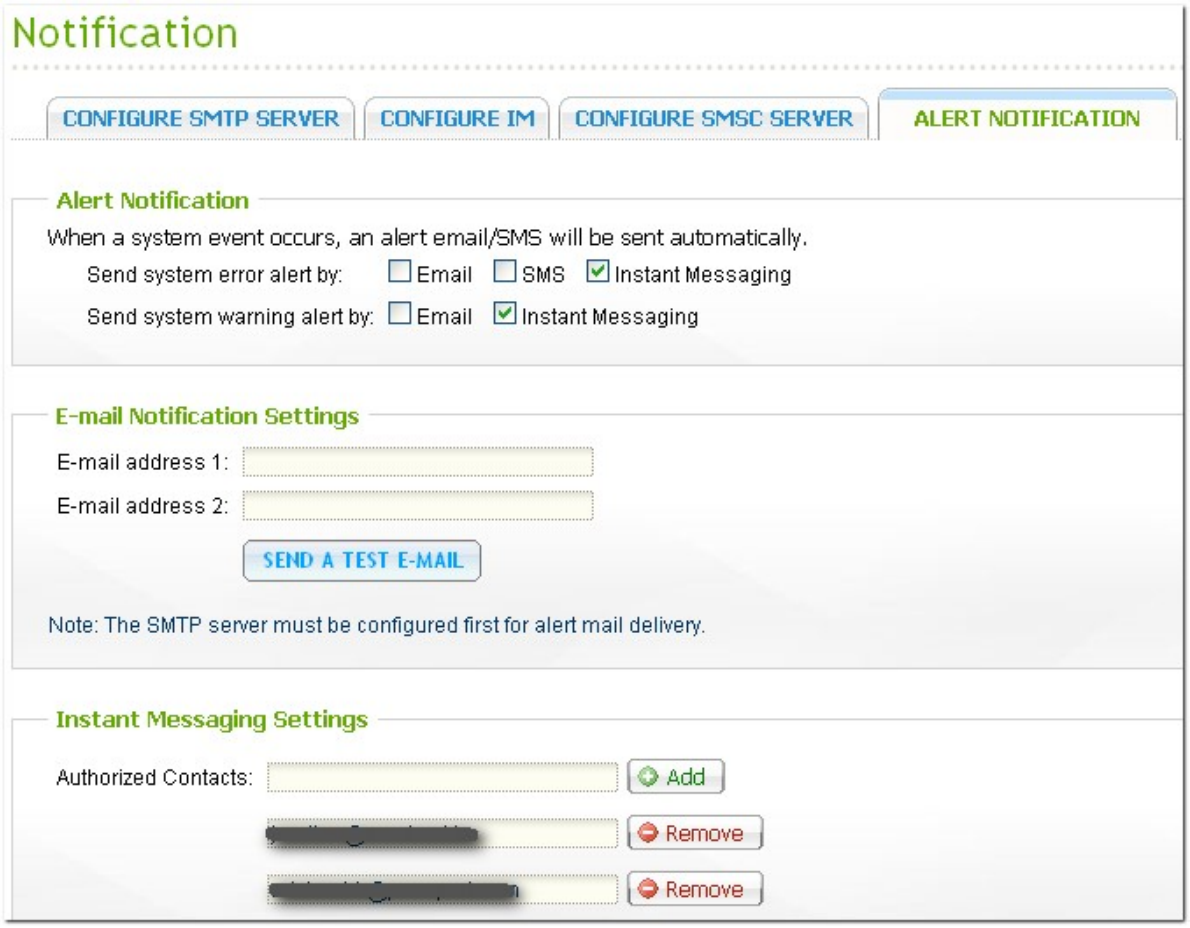
- To use this feature, the NAS must be connected to the Internet.
- The NAS supports Windows Live Messenger 2009 or above.
- Register a dedicated Windows Live Messenger account for the NAS. One Windows Live Messenger account can only be used by one NAS.

To use this feature, follow the steps below:

1. Sign up a Windows Live ID for the NAS from https://signup.live.com/.
2. Download Windows Live Messenger for your Windows OS from http://explore.live.com/. The NAS supports Windows Live Messenger 2009 or above.
3. Login the Windows Live Messenger account registered in Step 1. Add the authorized contacts (up to 10) to interact with the NAS. Make sure these contacts have also added the Messenger account of the NAS.
4. Go to "Notification" > "Configure IM" and enter the login information registered in Step 1. Click "Apply". The login status will be shown as "On".



5. Go to “Notification” > “Alert Notification”. Enable alert notification by Instant Messaging and enter the authorized contacts (up to 10) under “Instant Messaging Settings”. Click “Apply”.



6. Login an authorized Windows Live Messenger account and interact with the NAS via Windows Live Messenger. The NAS will send instant error or warning alerts (English only) to the authorized contacts when events occur.

The authorized Windows Live Messenger contacts can enter the following command to inquire real-time system information from the NAS. The information is available in English only.

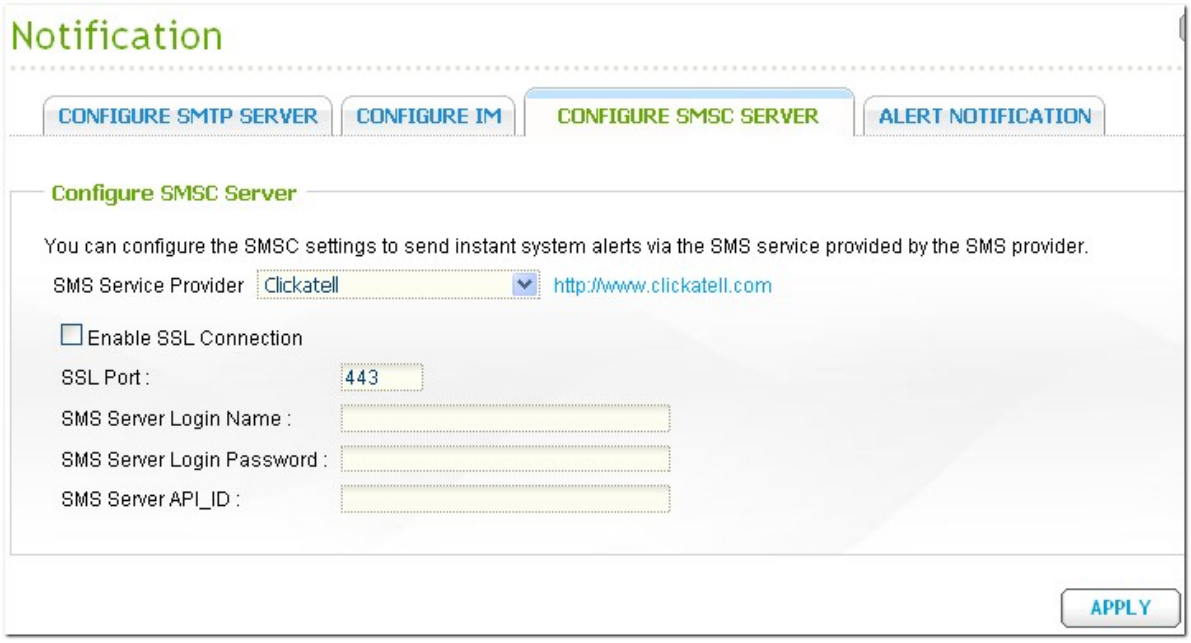
Command	Description
help	A list of command options will be shown.
info-cpu	Inquire the current CPU temperature.
info-sys	Inquire the current system temperature and fan speed.
info-model	Inquire the NAS model number.
info-hd	Inquire the number of hard disks on the NAS.
info-hd-[hd#]	Inquire the current temperature and S.M.A.R.T. status of a hard disk. For example, info-hd-1.
info-vol	Inquire the number of disks volumes on the NAS.
info-vol-[vol#]	Inquire the information of a disk volume. For example, info-vol-1.

Configure SMS Server

Configure the SMS server settings to send SMS messages to the specified phone number(s) from the NAS. The default SMS service provider is Clickatell. You can add your own SMS service provider by selecting "Add SMS Provider" from the drop-down menu.

When "Add SMS service provider" is selected, enter the name of the SMS provider and the URL template text.

Note: The URL template text must follow the standard of the SMS service provider to receive the SMS alert properly.



Alert Notification

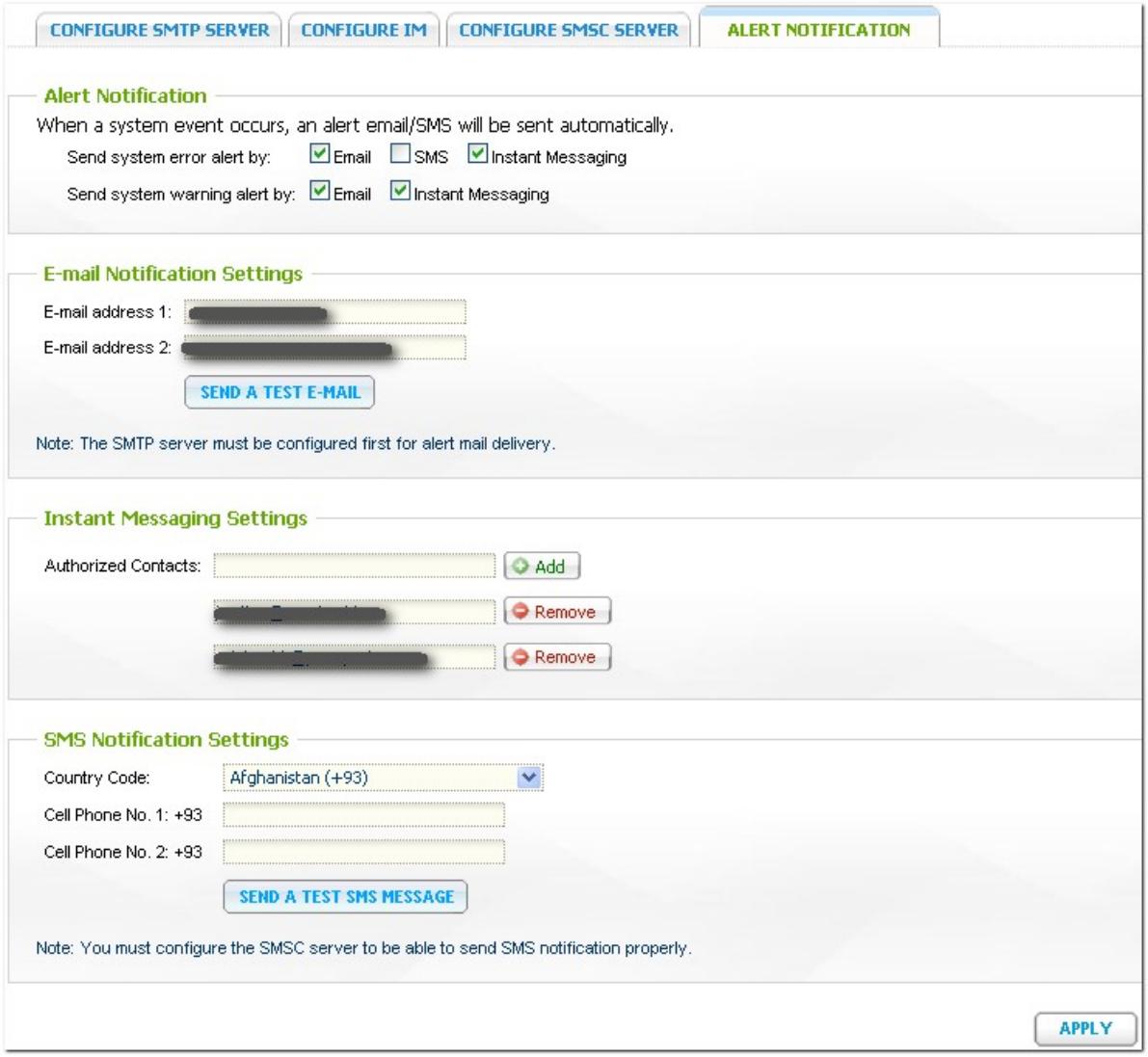
Select the type of instant alert the NAS will send to the designated users when system events (warning/ error) occur.

Email Notification Settings
Specify the email addresses (maximum 2) to receive instant system alert from the NAS.

Instant Messaging Settings
Specify the Windows Live Messenger contacts (maximum 10) who are allowed to receive instant system alert from the NAS and inquire real-time system information from the NAS via Windows Live Messenger.

The Windows Live Messenger contacts must first be added to the Windows Live Messenger account of the NAS specified in "Notification" > "Configure IM".

SMS Notification Settings
Specify the cell phone numbers (maximum 2) to receive instant system alert from the NAS.


CONFIGURE SMTP SERVER
CONFIGURE IM
CONFIGURE SMSC SERVER
ALERT NOTIFICATION
Alert Notification
When a system event occurs, an alert email/SMS will be sent automatically.
Send system error alert by: Email SMS Instant Messaging
Send system warning alert by: Email Instant Messaging
E-mail Notification Settings
E-mail address 1:
E-mail address 2:
SEND A TEST E-MAIL
Note: The SMTP server must be configured first for alert mail delivery.
Instant Messaging Settings
Authorized Contacts:
Add
Remove
Remove
SMS Notification Settings
Country Code: Afghanistan (+93)
Cell Phone No. 1: +93
Cell Phone No. 2: +93
SEND A TEST SMS MESSAGE
Note: You must configure the SMSC server to be able to send SMS notification properly.
APPLY

3.7 Power Management

You can restart or shut down the NAS, specify the behaviour of the NAS after a power recovery, and set the schedule for automatic system power on/off/restart on this page.

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

Turn on 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 NAS will ignore the running replication job and execute scheduled system restart or shutdown.

EuP Mode Configuration
EuP (also Energy-using Products) is a European Union (EU) directive designed to improve the energy efficiency of electrical devices, reduce use of hazardous substances, increase ease of product recycling, and improve environment-friendliness of the product.

When EuP is enabled, the following settings will be affected so that the NAS maintains low power consumption (less than 1W) when the NAS is powered off:

- Wake on LAN: Disabled.
- AC power resumption: The NAS will remain off after the power restores from an outage.
- Scheduled power on, off, restart settings: Disabled.

When EuP is disabled, the power consumption of the NAS is slightly higher than 1W when the NAS is powered off. EuP is disabled by default so that you can use the functions Wake on LAN, AC power resumption, and power schedule settings properly.

This feature is only supported by certain NAS models, please visit http://www.qnap.com for details.

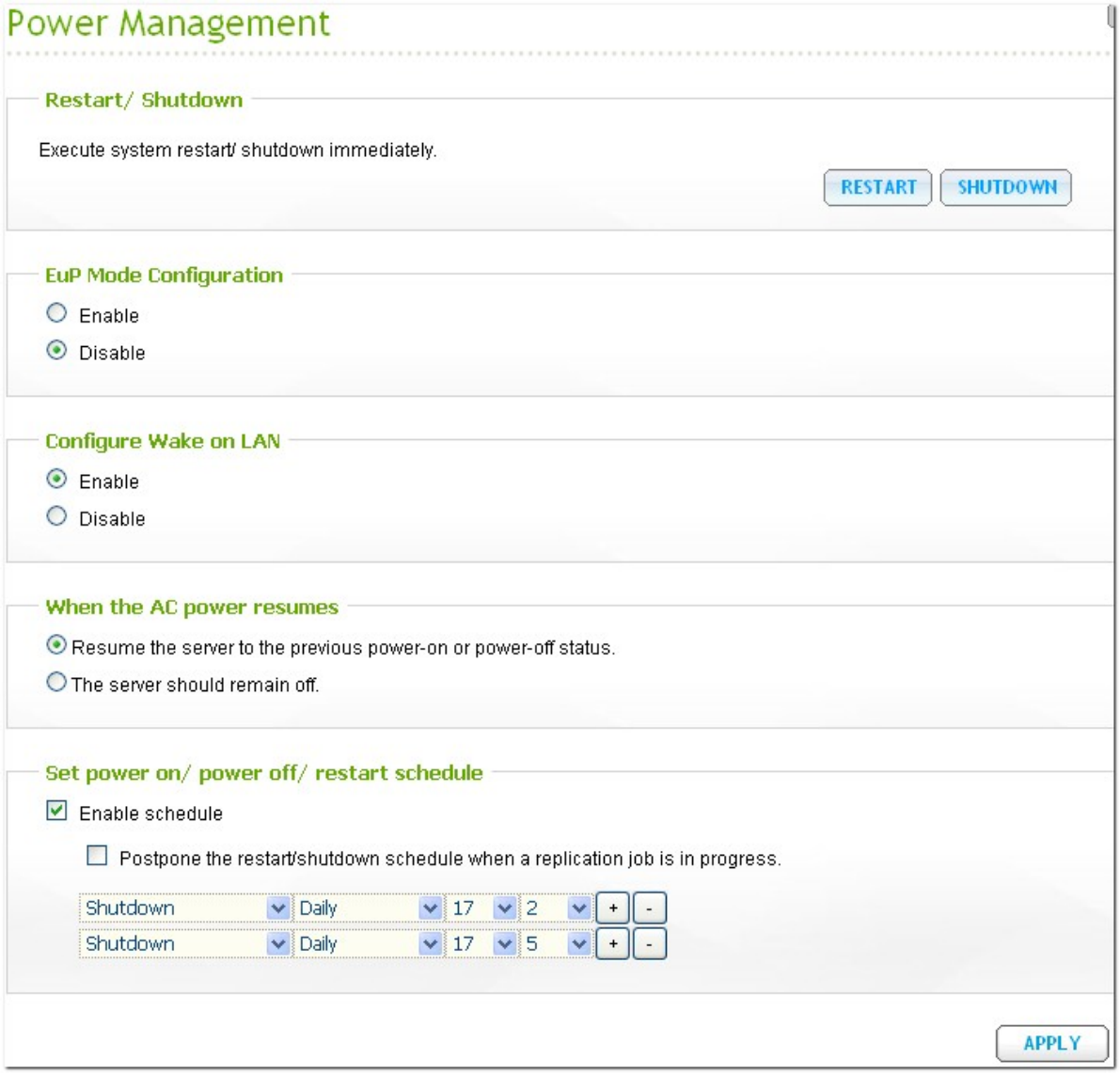
Wake on LAN
Turn on this option to allow the users to power on the NAS remotely by Wake on LAN. Note that if the power connection is physically removed (in other words, the power cable is unplugged) when the NAS is turned off, Wake on LAN will not function whether or not the power supply is reconnected afterwards.

This feature is only supported by certain NAS models, please visit http://www.qnap.com for details.

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

Specify the schedule 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.



3.8 Network Recycle Bin

Network Recycle Bin

The Network Recycle Bin keeps the deleted files on the NAS. Enable this feature and specify the number of days (1-9999) to keep the deleted files. You may also specify the file extensions to be excluded from the bin. Click "Apply". The NAS will create a network share "Network Recycle Bin" automatically.

Note that this feature only supports file deletion via Samba and AFP.

Empty Network Recycle Bin

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

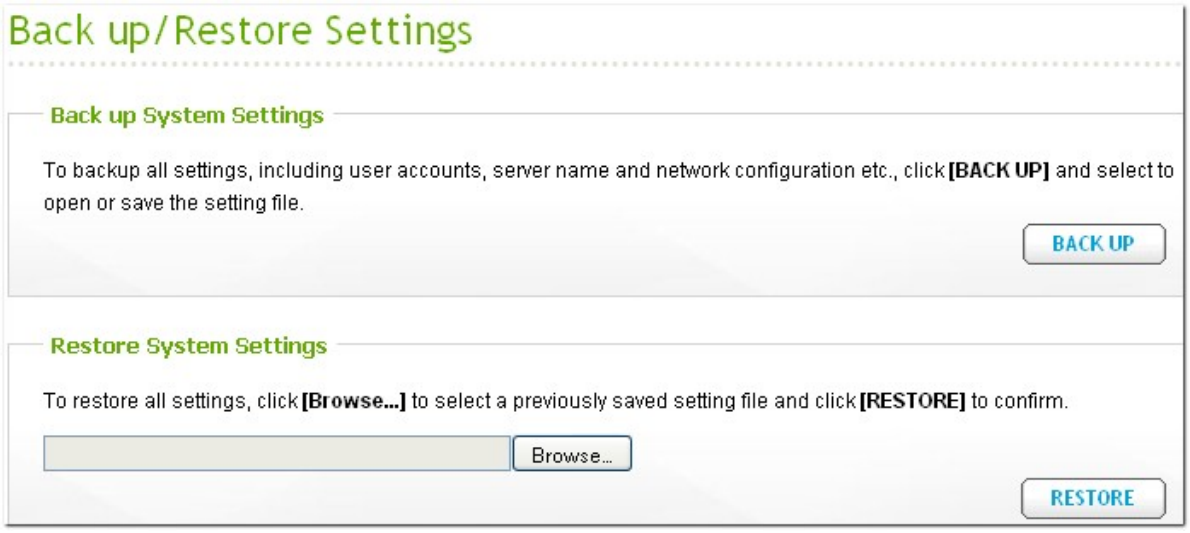
3.9 Back up/Restore Settings

Back up System Settings

To back up all the settings, including the user accounts, server name, network configuration and so on, click "Backup" and select to open or save the setting file.

Restore System Settings

To restore all the settings, click "Browse" to select a previously saved setting file and click "Restore".

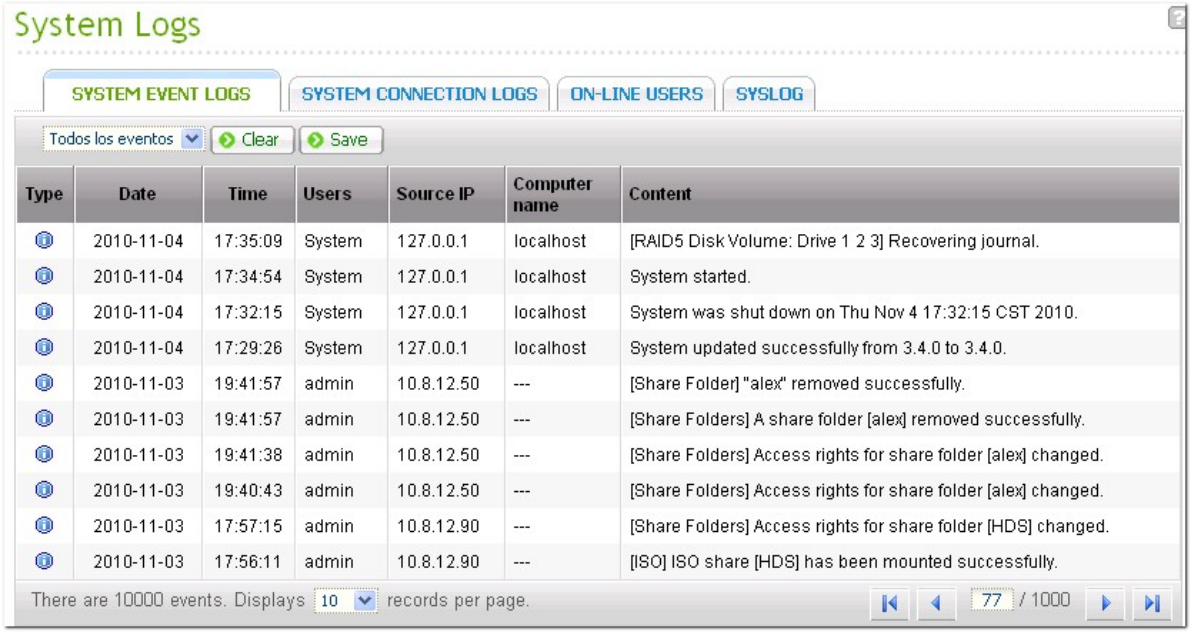


3.10 System Logs

System Event Logs

The NAS can store 10,000 recent event logs, including warning, error, and information messages. If the NAS does not function correctly, refer to the event logs for troubleshooting.

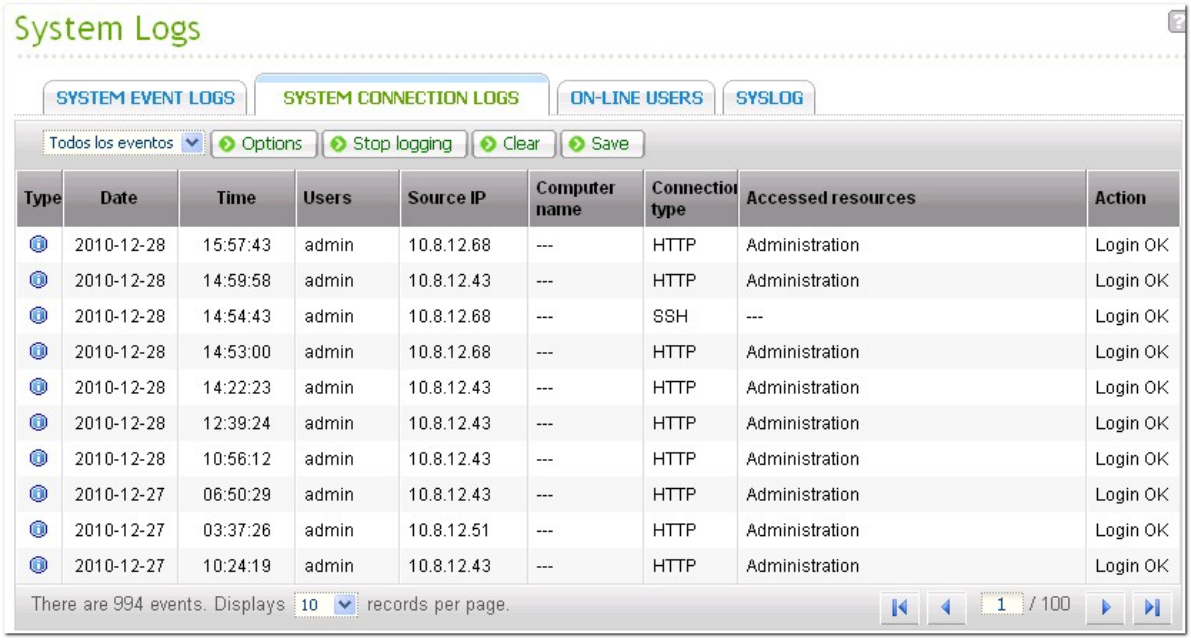
Tip: Right click a log and delete the record. To clear all the logs, click "Clear".



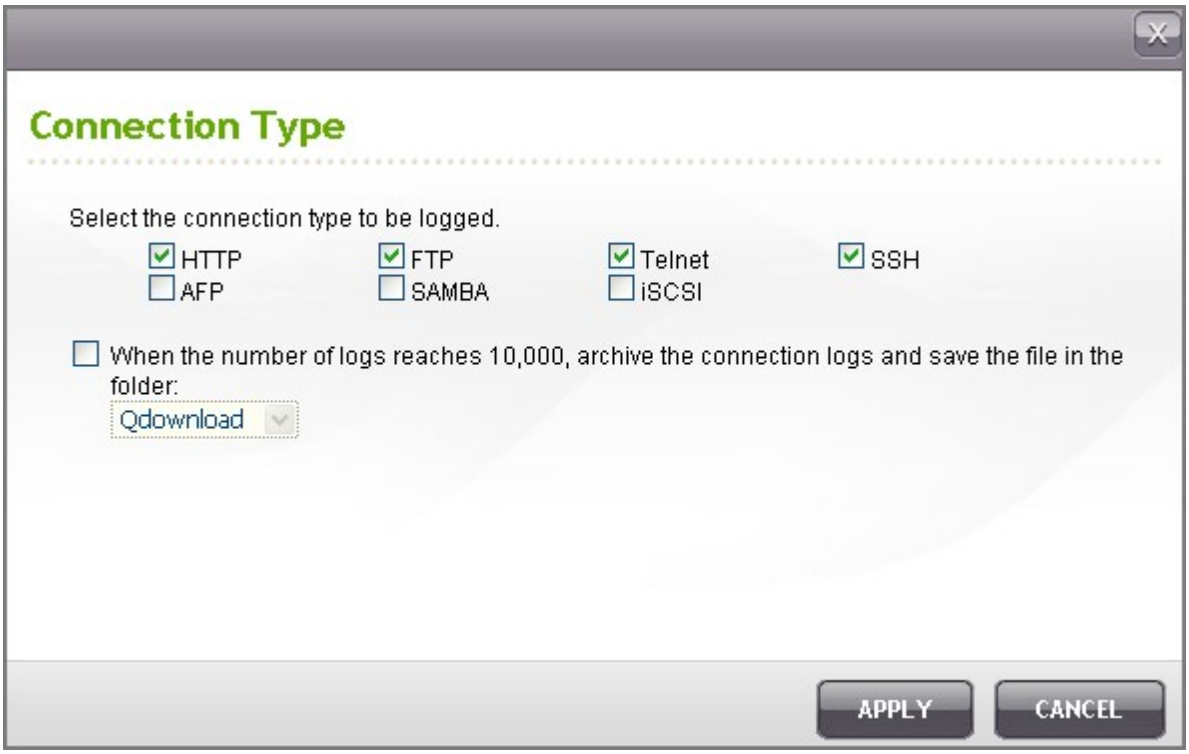
System Connection Logs

The NAS supports recording 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 when this feature is turned on.

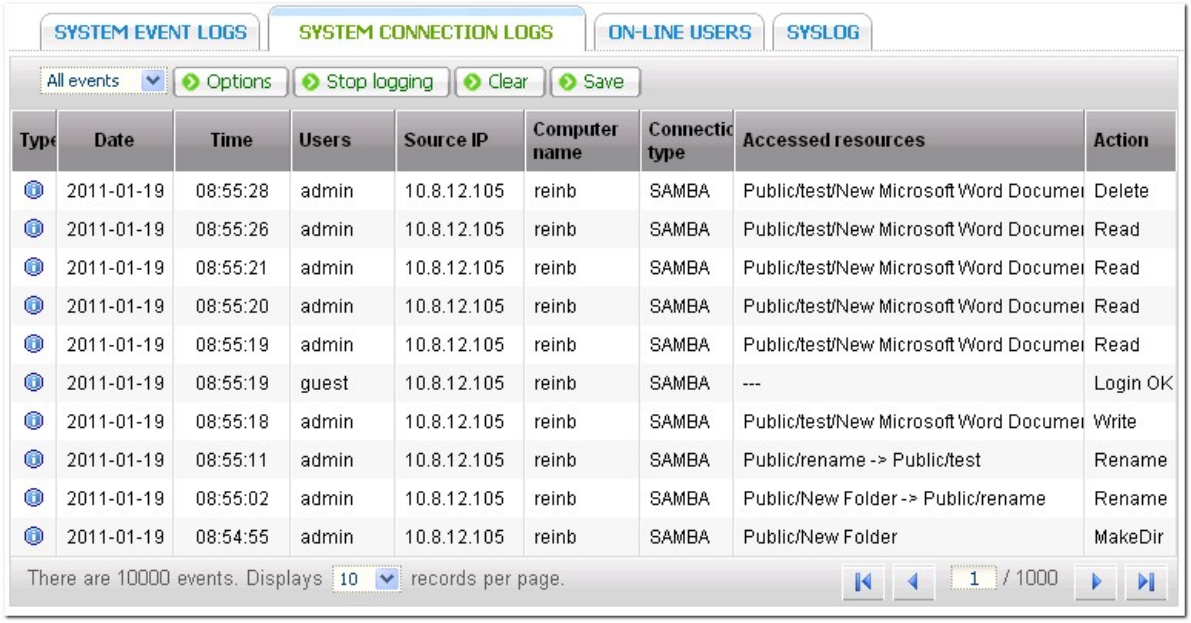
Tip: Right click a log and select to delete the record or block the IP and select how long the IP should be blocked. To clear all the logs, click "Clear".



Archive logs: Turn on this option to archive the connection logs. The NAS generates a CSV file automatically and saves it to a specified folder when the number of logs reaches the upper limit.



The file-level access logs are available on this page. The NAS will record the logs when users access, create, delete, move, or rename any files or folders via the connection type specified in "Options". To disable this feature, click "Stop logging".

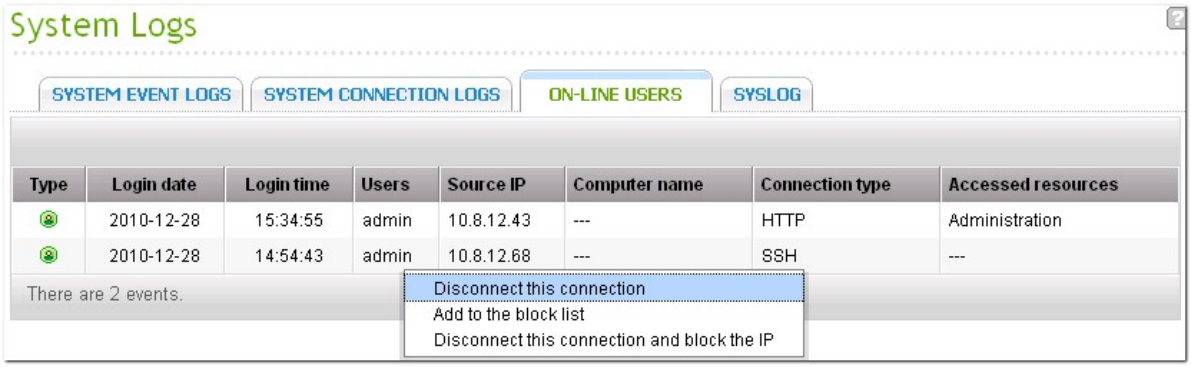


Type	Date	Time	Users	Source IP	Computer name	Connection type	Accessed resources	Action
	2011-01-19	08:55:28	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documer	Delete
	2011-01-19	08:55:26	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documer	Read
	2011-01-19	08:55:21	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documer	Read
	2011-01-19	08:55:20	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documer	Read
	2011-01-19	08:55:19	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documer	Read
	2011-01-19	08:55:19	guest	10.8.12.105	reinb	SAMBA	---	Login OK
	2011-01-19	08:55:18	admin	10.8.12.105	reinb	SAMBA	Public/test/New Microsoft Word Documer	Write
	2011-01-19	08:55:11	admin	10.8.12.105	reinb	SAMBA	Public/rename -> Public/test	Rename
	2011-01-19	08:55:02	admin	10.8.12.105	reinb	SAMBA	Public/New Folder -> Public/rename	Rename
	2011-01-19	08:54:55	admin	10.8.12.105	reinb	SAMBA	Public/New Folder	MakeDir

On-line Users

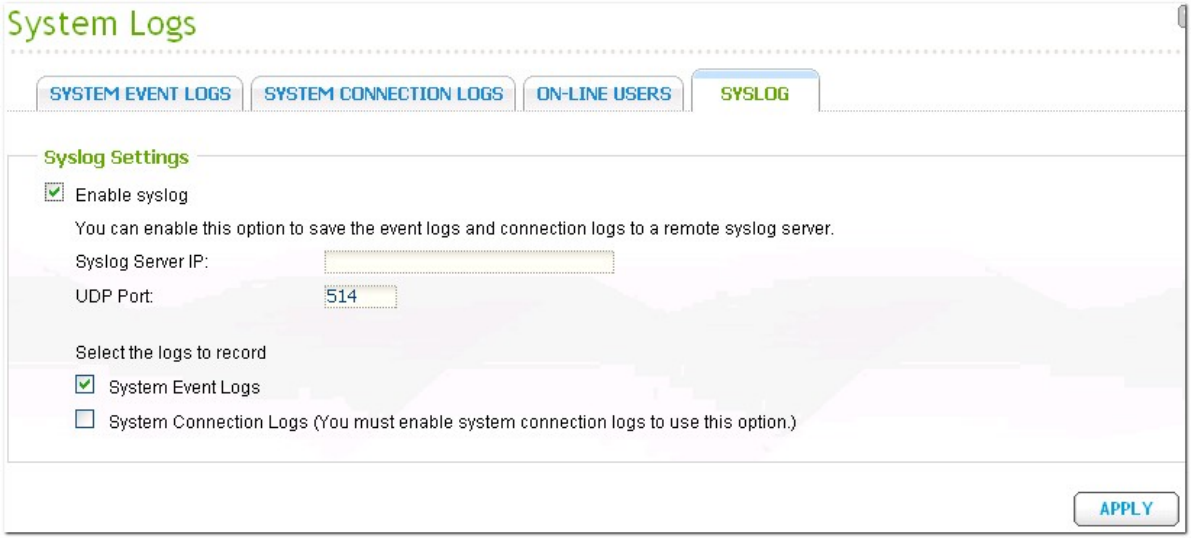
The information of the on-line users connecting to the NAS by networking services is shown on this page.

Tip: Right click a log and disconnect the IP connection and block the IP.



Syslog

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

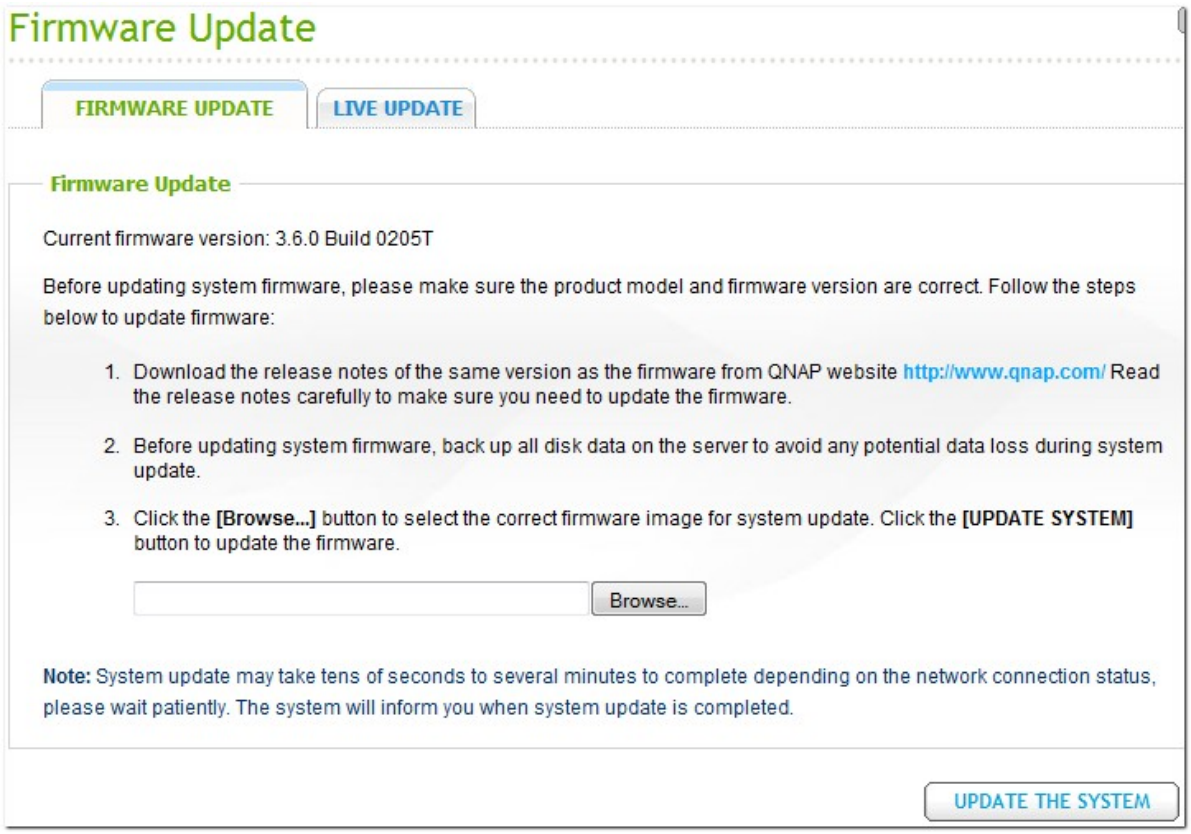


When converting the connection logs into a CSV file, the connection type and action will be number coded. Please refer to the table below for the code meaning.

Connection type codes	Action codes
0 - UNKNOWN	0 - UNKNOWN
1 - SAMBA	1 - DEL
2 - FTP	2 - READ
3 - HTTP	3 - WRITE
4 - NFS	4 - OPEN
5 - AFP	5 - MKDIR
6 - TELNET	6 - NFSMOUNT_SUCC
7 - SSH	7 - NFSMOUNT_FAIL
8 - ISCSI	8 - RENAME
	9 - LOGIN_FAIL
	10 - LOGIN_SUCC
	11 - LOGOUT
	12 - NFSUMOUNT
	13 - COPY
	14 - MOVE
	15 - ADD

3.11 Firmware Update

Update Firmware by Web Administration Page



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

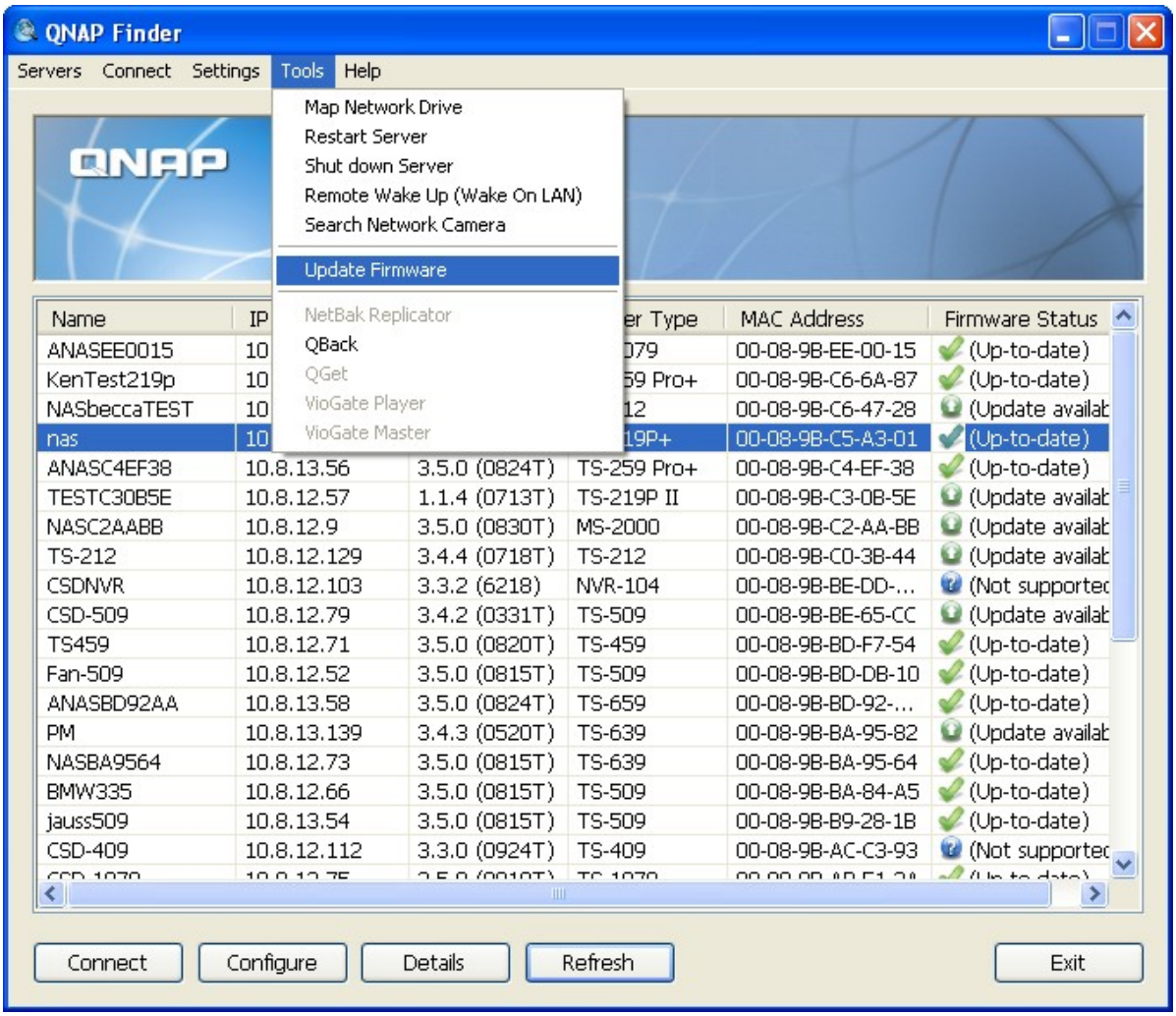
Before updating the system firmware, make sure the product model and firmware version are correct. Follow the steps below to update firmware:

1. Download the release notes of the firmware from the QNAP website http://www.qnap.com. Read the release notes carefully to make sure it is required to update the firmware.
2. Download the NAS firmware and unzip the IMG file to the computer.
3. Before updating the system firmware, back up all the disk data on the NAS to avoid any potential data loss during the system update.
4. Click "Browse" to select the correct firmware image for the 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 NAS will inform you when the system update has completed.

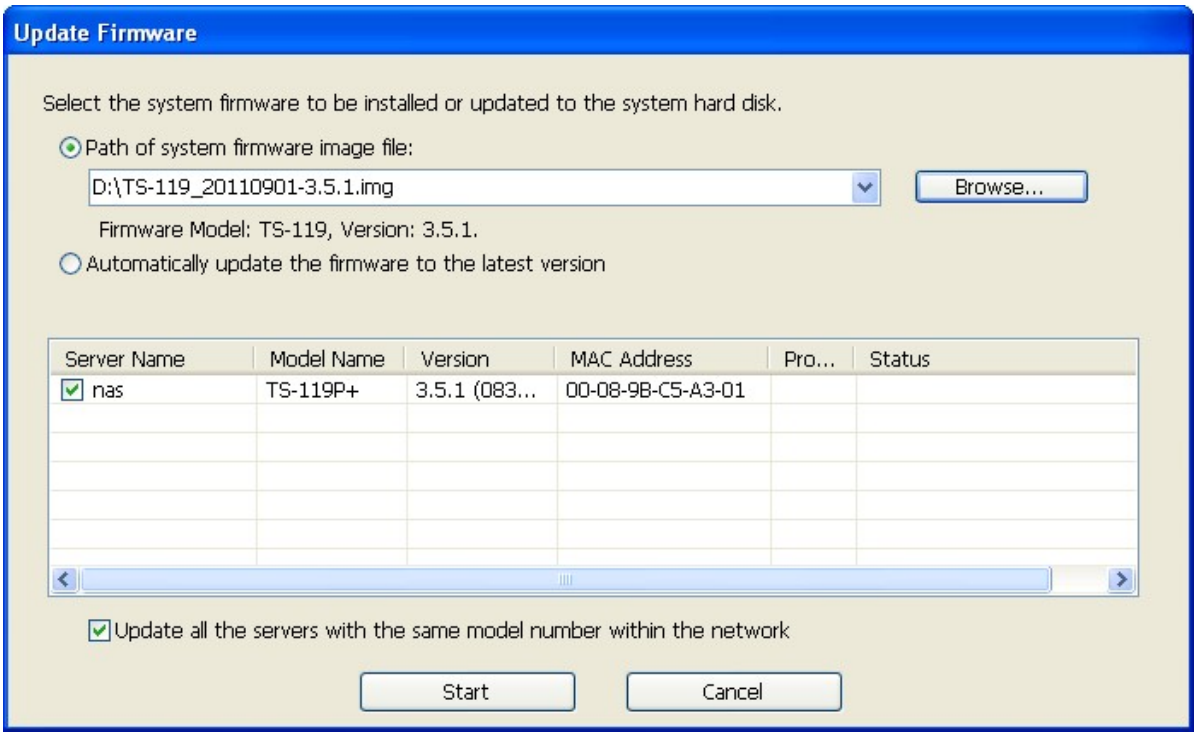
Update Firmware by Finder

The NAS firmware can be updated by the QNAP Finder. Select a NAS model and choose "Update Firmware" from the "Tools" menu.



Login the NAS as an administrator.

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



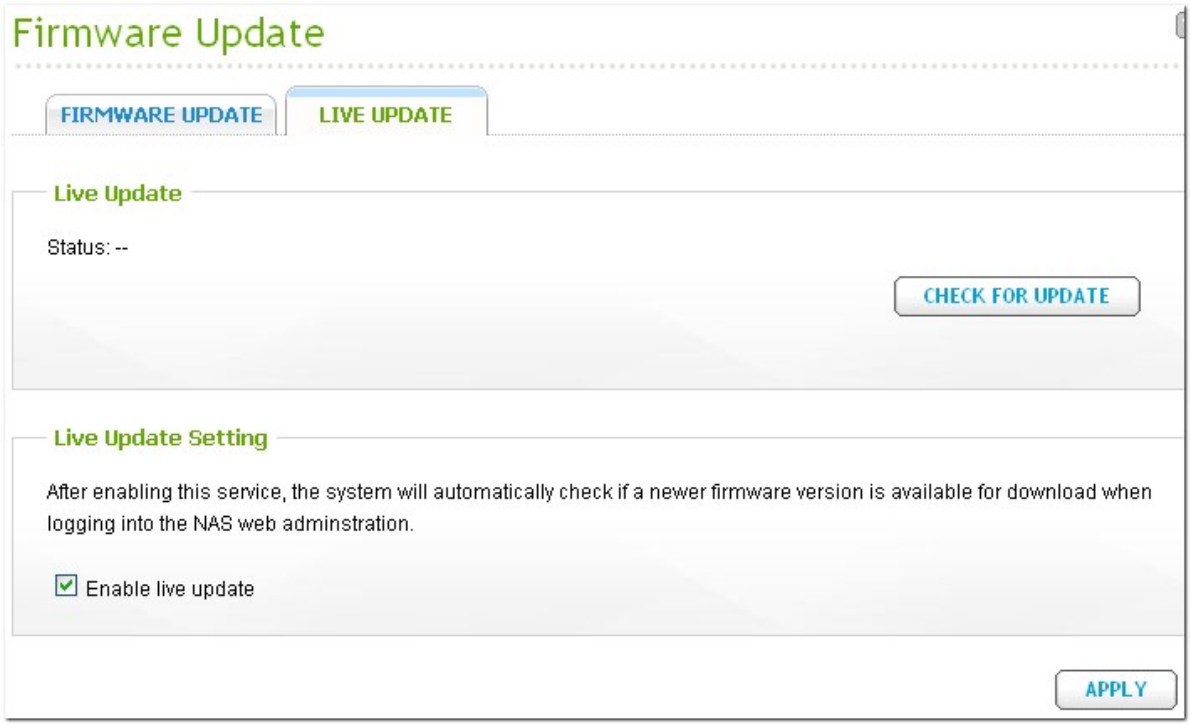
Note: The NAS servers of the same model on the same LAN can be updated by the Finder at the same time. Administrator access is required for system update.

Live Update

Select "Enable live update" to allow the NAS to automatically check if a new firmware version is available for download from the Internet. If a new firmware is found, you will be notified after logging in the NAS as an administrator.

Click "CHECK FOR UPDATE" to check if any firmware update is available.

Note that the NAS must be connected to the Internet for these features to work.



3.12 Restore to Factory Default

To reset all the system settings to default, click "RESET" and then click "OK".

Caution: When "RESET" is pressed on this page, all the disk data, user accounts, network shares, and system settings will be cleared and restored to default. Always back up all the important data and system settings before resetting the NAS.

To reset the NAS by the reset button, see "System Administration" > "Hardware" 61.

4. Disk Management

Volume Management 89
RAID Management 93
Hard Disk SMART 119
Encrypted File System 120
iSCSI 129
Virtual Disk 189

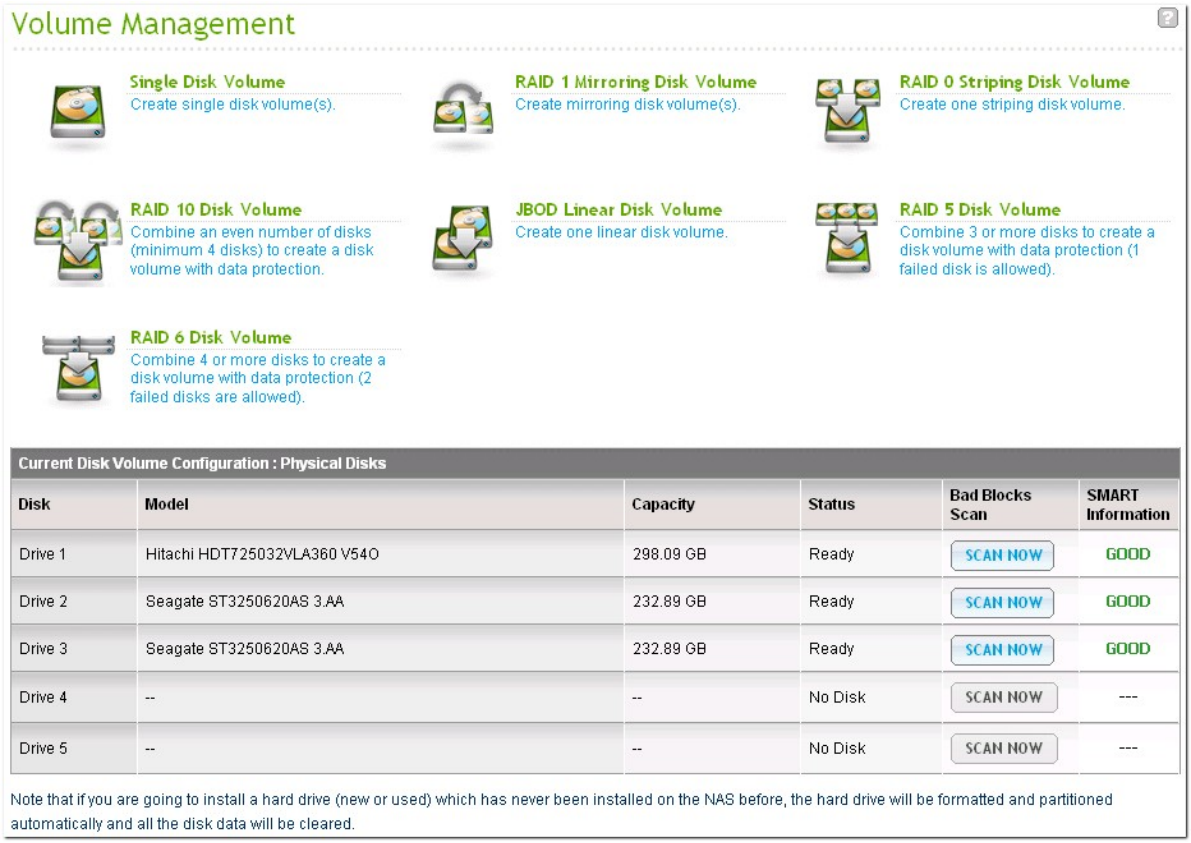
4.1 Volume Management

This page shows the model, size, and current status of the hard drives on the NAS. You can format and check the hard drives, and scan the bad blocks on the hard drives. When the hard drives have been formatted, the NAS will create the following default network shares:

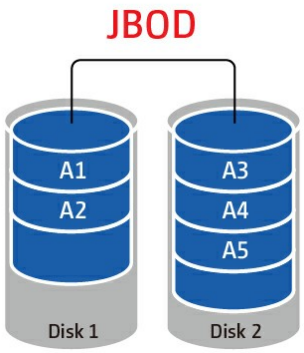
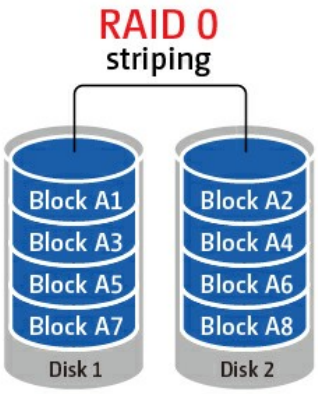
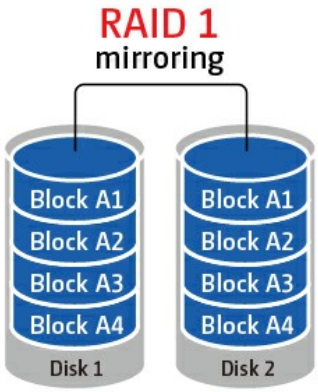
- Public: The default network share for file sharing by everyone.
- Qdownload/Download*: The network share for Download Station.
- Qmultimedia/Multimedia*: The network share for Multimedia Station.
- Qusb/Usb*: The network share for data copy function using the USB ports.
- Qweb/Web*: The network share for Web Server.
- Qrecordings/Recordings*: The network share for Surveillance Station.

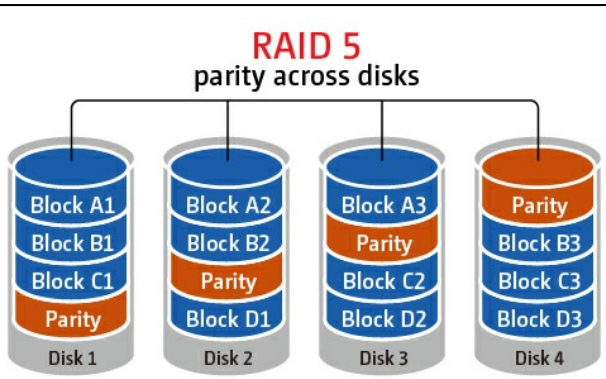
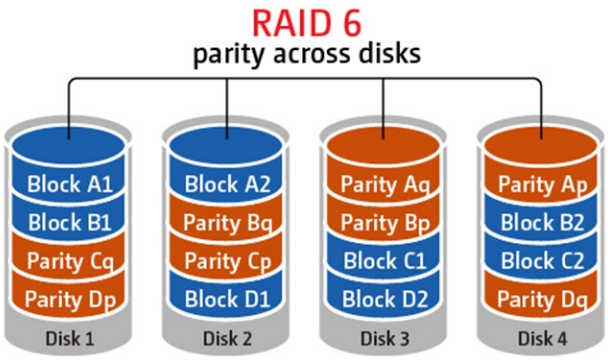
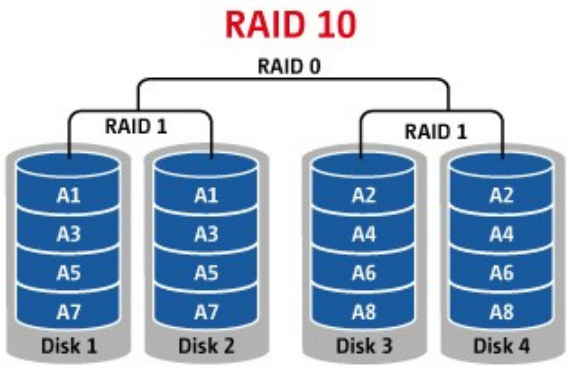
*The default network shares of the TS-x59 and TS-x69 Turbo NAS series are Public, Download, Multimedia, Usb, Web, and Recordings.

Note: The default network shares of the NAS 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-drive models or above
RAID 5, RAID 6, RAID 5+hot spare	4-drive models or above
RAID 6+hot spare	5-drive models or above
RAID 10	4-drive models or above
RAID 10+hot spare	5-drive models or above

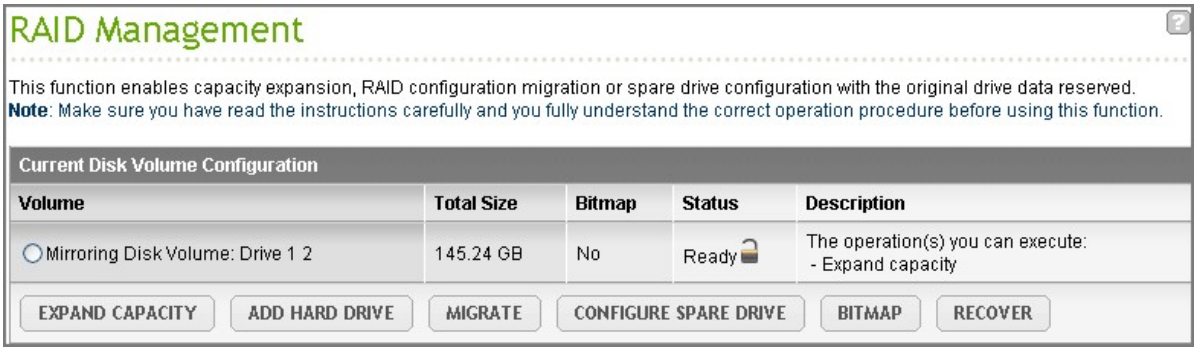
Single Disk Volume Each hard drive is used as a standalone disk. If a hard drive is damaged, all the data will be lost.	
JBOD (Just a bunch of disks) JBOD is a collection of hard drives that does not offer any RAID protection. The data are written to the physical disks sequentially. The total storage capacity is equal to the sum of the capacity of all member hard drives.	
RAID 0 Striping Disk Volume RAID 0 (striping disk) combines 2 or more hard drives into one larger volume. The data is written to the hard drive without any parity information and no redundancy is offered. The total storage capacity of a RAID 0 disk volume is equal to the sum of the capacity of all member hard drives.	
RAID 1 Mirroring Disk Volume RAID 1 duplicates the data between two hard drives to provide disk mirroring. To create a RAID 1 array, a minimum of 2 hard drives are required. The storage capacity of a RAID 1 disk volume is equal to the size of the smallest hard drive.	

RAID 5 Disk Volume The data are striped across all the hard drives in a RAID 5 array. The parity information is distributed and stored across each hard drive. If a member hard drive fails, the array enters degraded mode. After installing a new hard 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 drives are required. The storage capacity of a RAID 5 array is equal to (N-1) * (size of smallest hard drive). N is the number of hard drives in the array.	
RAID 6 Disk Volume The data are striped across all the hard 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 hard drives. To create a RAID 6 disk volume, a minimum of 4 hard drives are required. The storage capacity of a RAID 6 array is equal to (N-2) * (size of smallest hard drive). N is the number of hard drives in the array.	
RAID 10 Disk Volume RAID 10 combines four or more disks in a way that protects data against loss of non-adjacent disks. It provides security by mirroring all data on a secondary set of disks while using striping across each set of disks to speed up data transfers. RAID 10 requires an even number of hard drives (minimum 4 hard drives). The storage capacity of RAID 10 disk volume is equal to (size of the smallest capacity disk in the array) * N/2. N is the number of hard drives in the volume.	

4.2 RAID Management

*Online RAID capacity expansion, online RAID level migration, and RAID recovery are not supported by one-bay NAS models, TS-210, and TS-212.

You can perform online RAID capacity expansion (RAID 1, 5, 6, 10) and online RAID level migration (single disk, RAID 1, 5, 10), add a hard drive member to a RAID 5, 6, or 10 configuration, configure a spare hard drive (RAID 5, 6, 10) with the data retained, enable Bitmap, and recover a RAID configuration on this page.
To expand the storage capacity of a RAID 10 volume, you can perform online RAID capacity expansion or add an even number of hard disk drives to the volume.

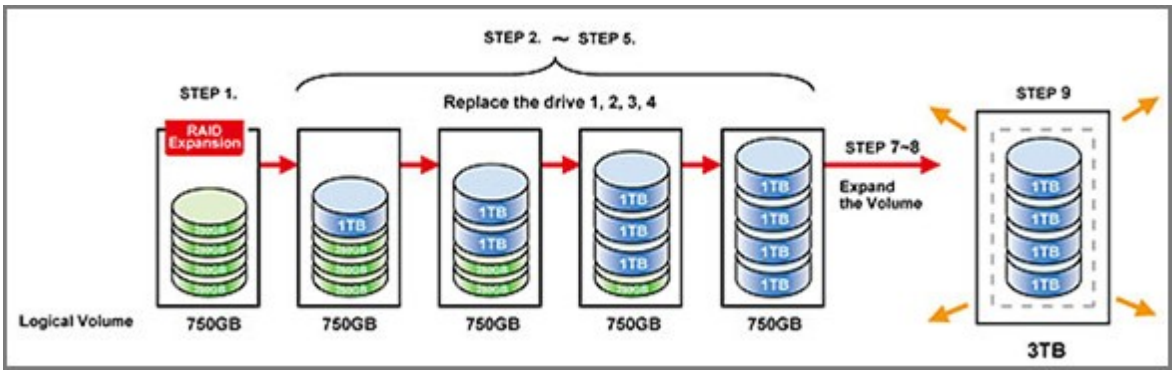


Expand Capacity (Online RAID Capacity Expansion)

Scenario

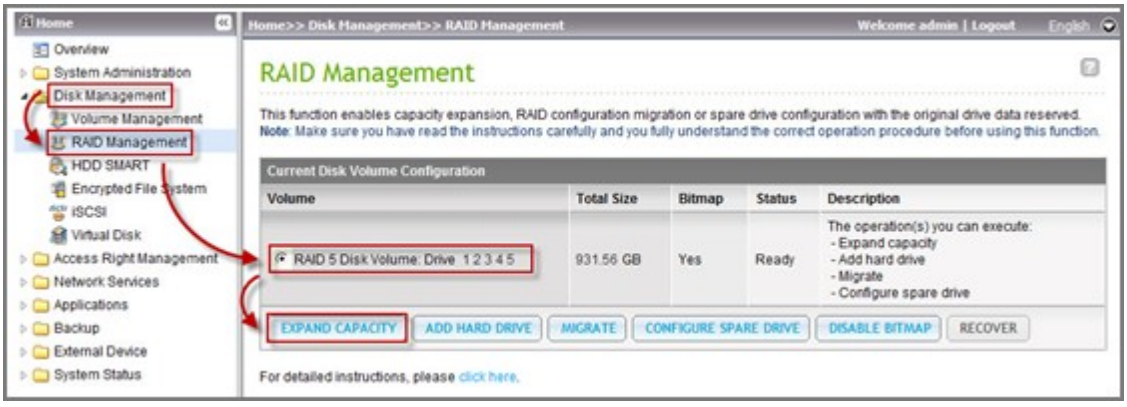
You bought four 250GB hard drives for initial setup of a TS-509 Pro NAS and configured RAID 5 disk configuration with the four hard drives.

A half year later, the data size of the department has largely increased to 1.5TB. In other words, the storage capacity of the NAS is running out of use. At the same time, the price of 1TB hard drives has dropped to a large extent.

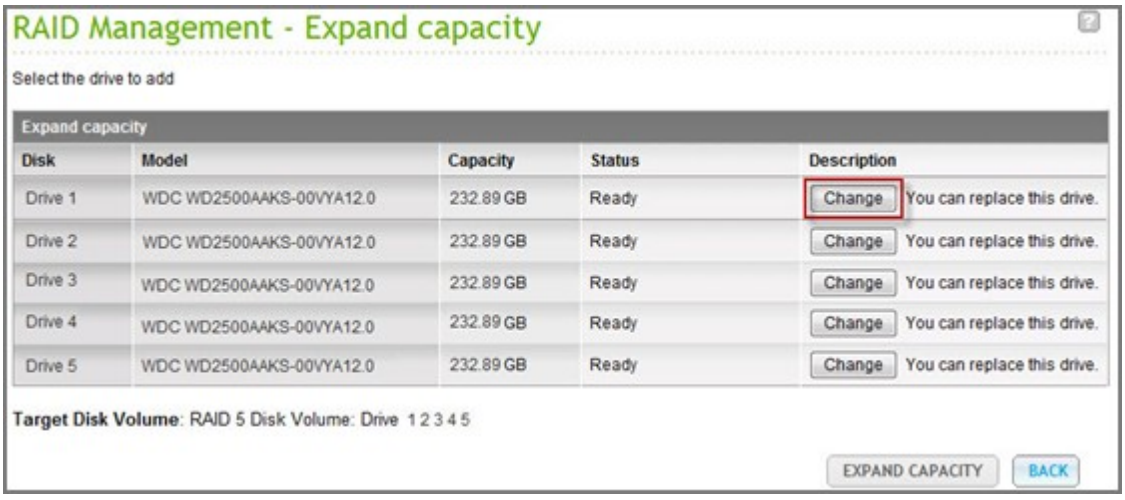


Operation procedure

In “Disk Management” > “RAID Management”, select the disk volume for expansion and click “EXPAND CAPACITY”.



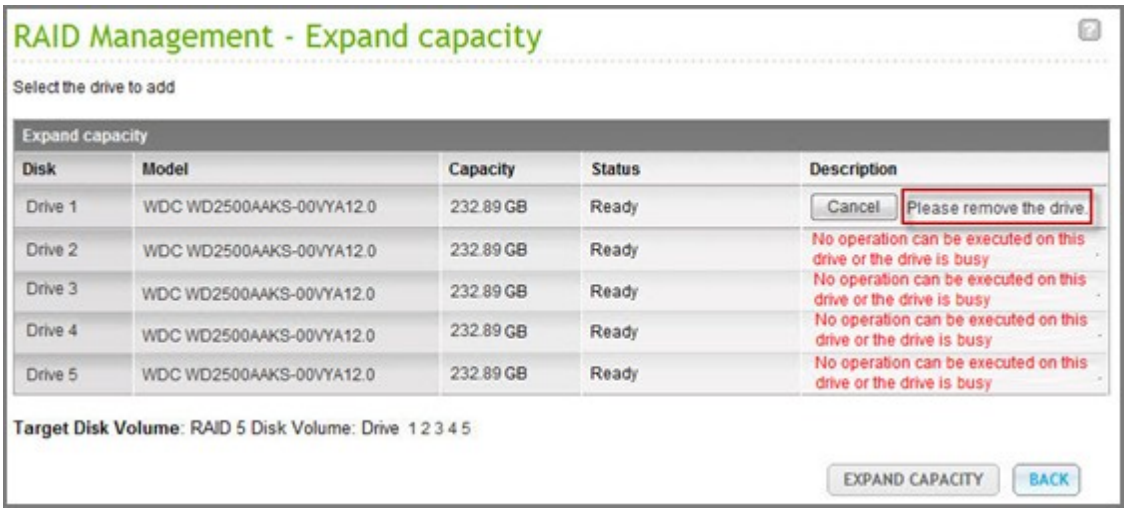
Click “Change” for the first hard drive to be replaced. Follow the instructions to proceed.



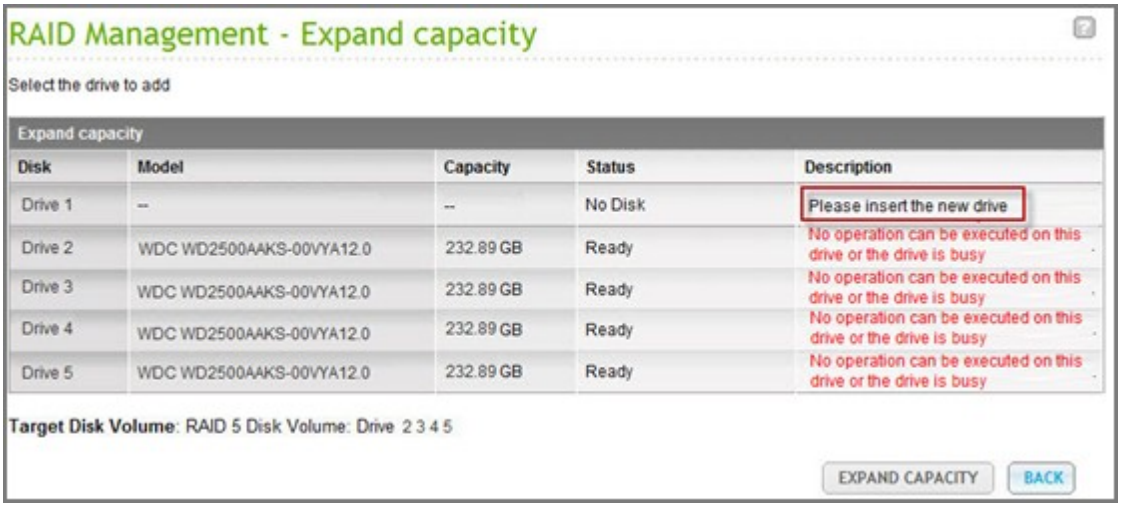
Tip: After replacing the hard drive, the description field shows “You can replace this drive”. This means you can replace the hard drive to a larger one or skip this step if the hard drives have been replaced already.

Caution: When the hard drive synchronization is in process, do NOT turn off the NAS or plug in or unplug the hard disk drives.

When the description displays “Please remove this drive”, remove the hard drive from the NAS. Wait for the NAS to beep twice after removing the hard drive.



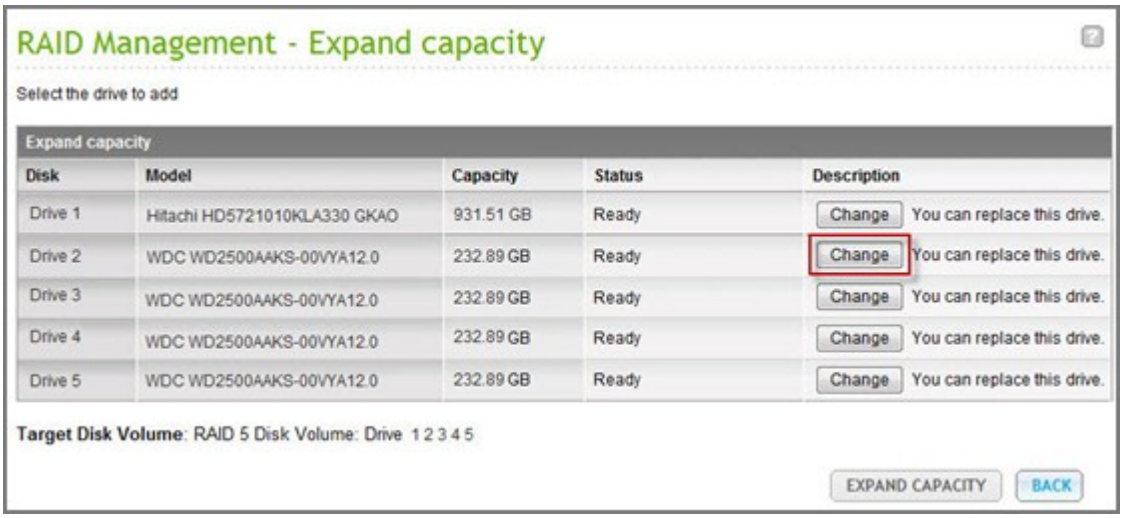
When the description displays “Please insert the new drive”, plug in the new hard drive to the drive slot.



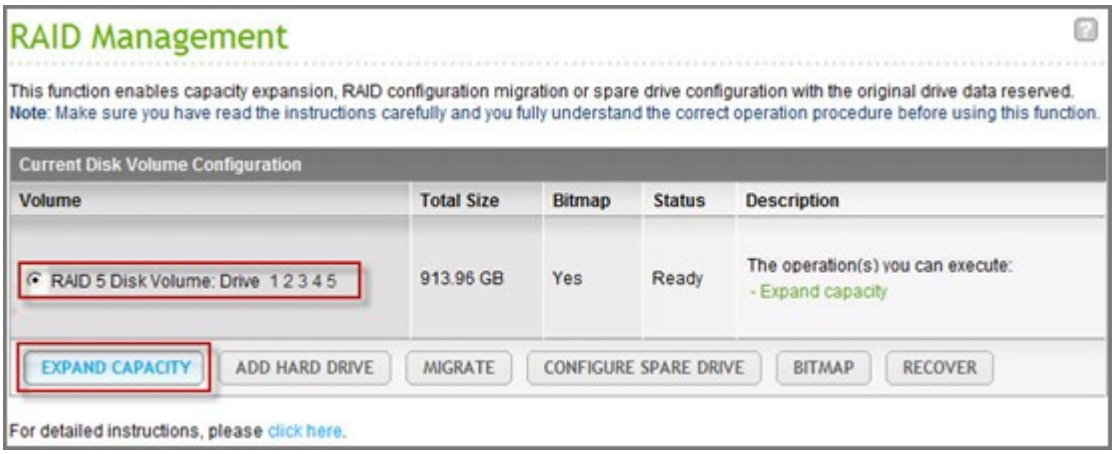
After plugging in the hard drive, wait for the NAS to beep. The system will start rebuilding.

Status	Description
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy
Rebuilding... (0%)	No operation can be executed on this drive or the drive is busy

After rebuilding has completed, repeat the steps above to replace other hard drives.

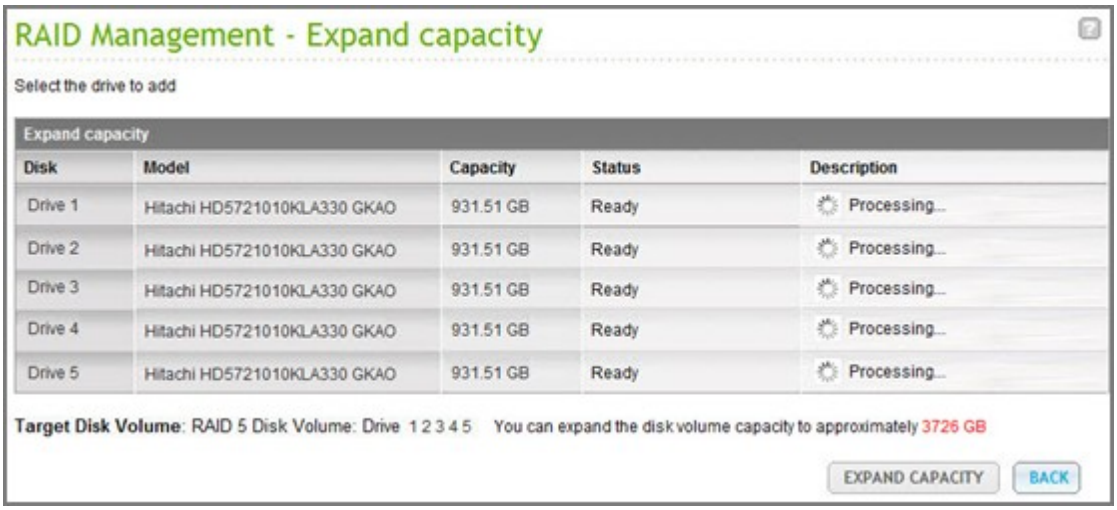


After changing the hard drives and disk rebuilding has completed, click "EXPAND CAPACITY" to execute RAID capacity expansion.

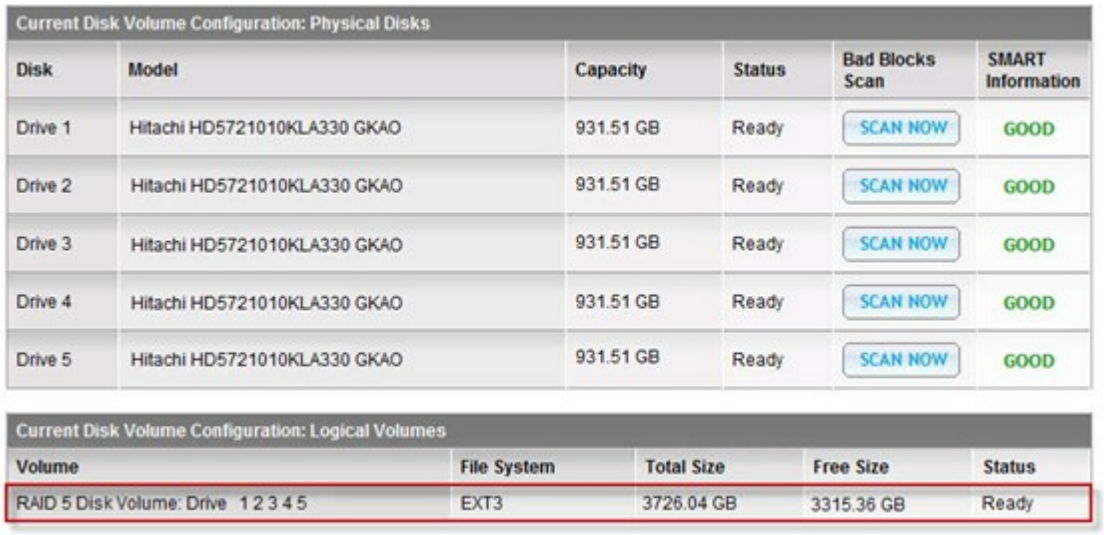


Click "OK" to proceed.

The NAS beeps and starts to expand the capacity.



The process may take from hours to tens of hours to finish depending on the drive size. Please wait patiently for the process to finish. Do NOT turn off the power of the NAS.



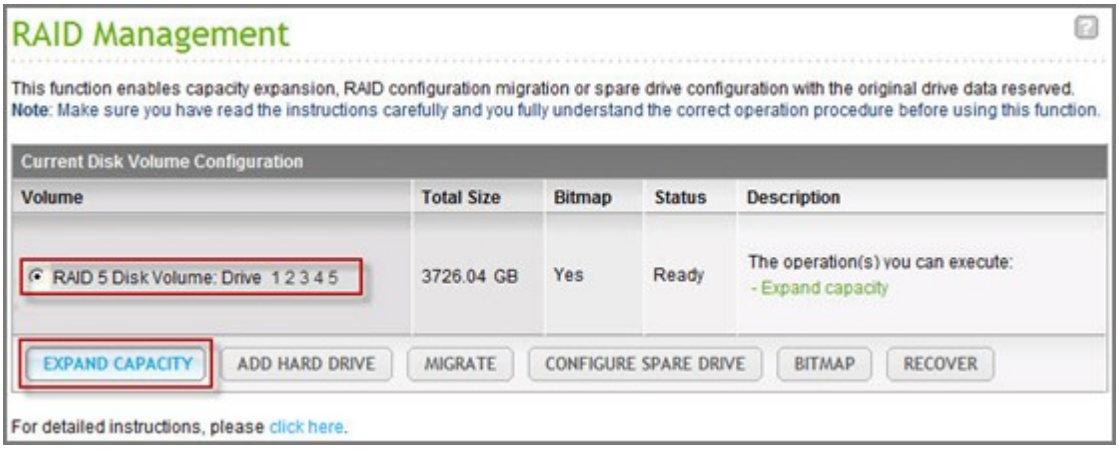
Current Disk Volume Configuration: Physical Disks

Disk	Model	Capacity	Status	Bad Blocks Scan	SMART Information
Drive 1	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 3	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 4	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 5	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD

Current Disk Volume Configuration: Logical Volumes

Volume	File System	Total Size	Free Size	Status
RAID 5 Disk Volume: Drive 1 2 3 4 5	EXT3	3726.04 GB	3315.36 GB	Ready

After RAID capacity expansion has finished, the new capacity is shown and the status is "Ready". You can start to use the NAS. (In the example you have 3.7TB logical volume.)



Tip: If the description still shows "You can replace this hard drive" and the status of the drive volume says "Ready", it means the RAID volume is still expandable.

Migrate (Online RAID Level Migration)

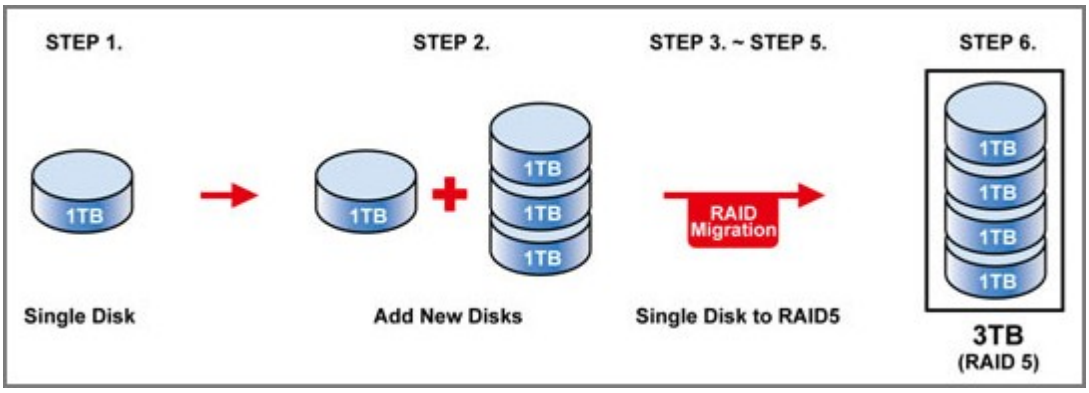
During the initial setup of the TS-509 Pro, you bought a 1TB hard drive and configured it as single disk. The TS-509 Pro is used as a file server for data sharing among the departments.

After a half year, more and more important data are saved on the TS-509 Pro. There is a rising concern for hard drive damage and data loss. Therefore, you planned to upgrade the disk configuration to RAID 5.

You can install one hard drive for setting up the TS-509 Pro and upgrade the RAID level of the NAS with online RAID level migration in the future. The migration process can be done without turning off the NAS. All the data will be retained.

You can do the following with online RAID level migration:

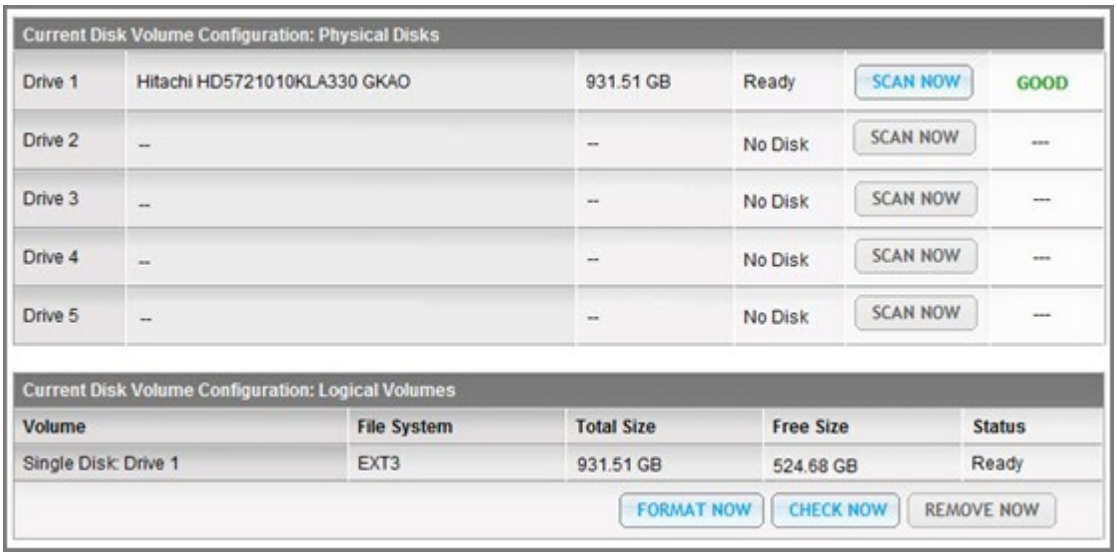
- Migrate the system from single disk to RAID 1, RAID 5, RAID 6 or RAID 10
- Migrate the system from RAID 1 to RAID 5, RAID 6 or RAID 10
- Migrate the system from RAID 5 with 3 hard drives to RAID 6



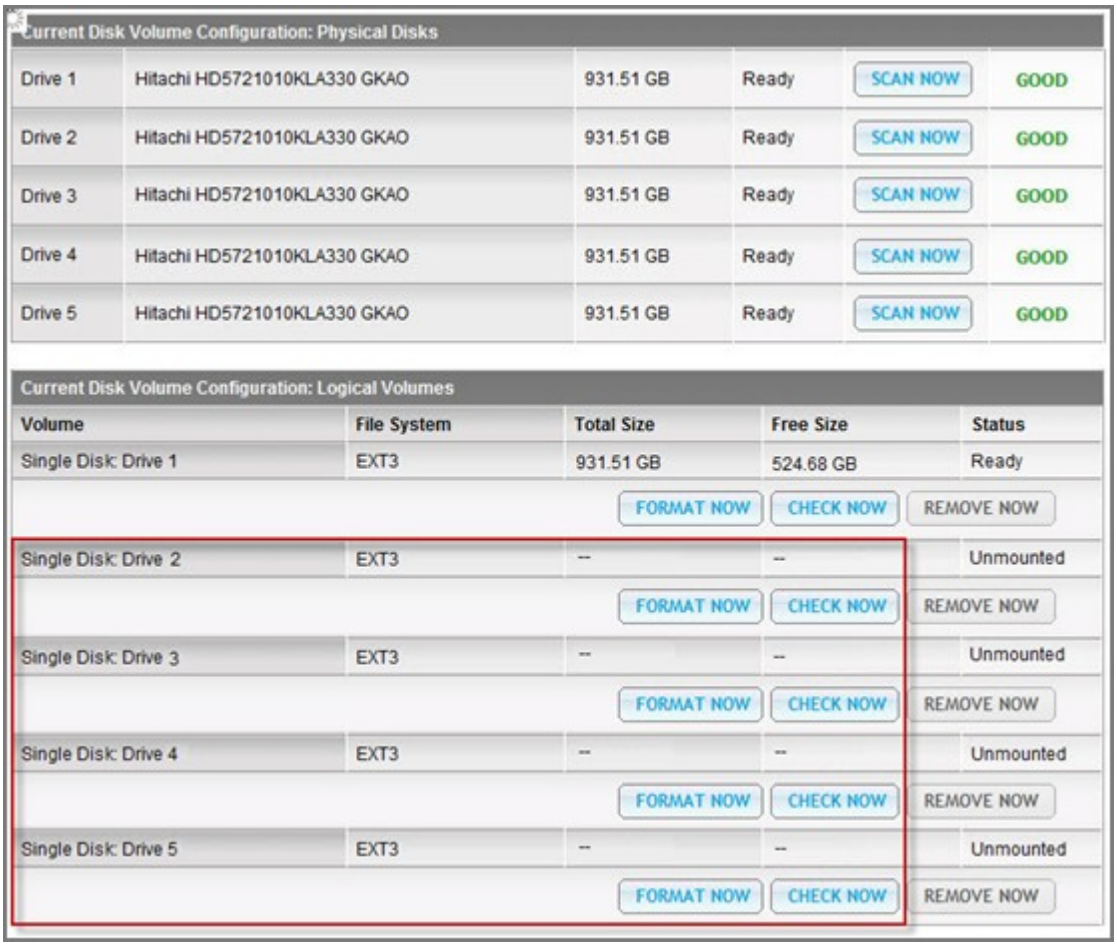
You need to:

- Prepare a hard drive of the same or larger capacity as an existing drive in the RAID configuration.
- Execute RAID level migration (migrate the system from single disk mode to RAID 5 with 4 hard drives).

Go to “Disk Management” > “Volume Management”. The current disk volume configuration displayed on the page is single disk (the capacity is 1TB).



Plug in the new 1TB hard drives to drive slots 2, 3, 4 and 5 of NAS. The NAS will detect the new hard drives. The status of the new hard drives is "Unmounted".



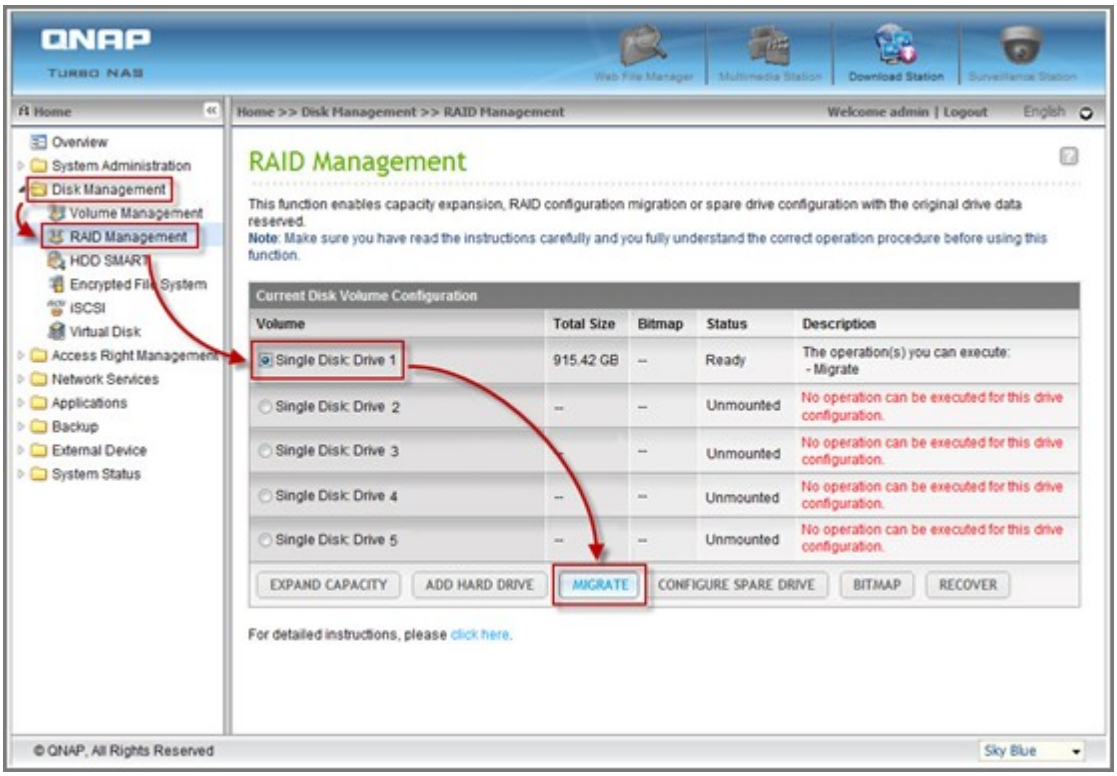
Current Disk Volume Configuration: Physical Disks

Drive 1	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 3	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 4	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 5	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD

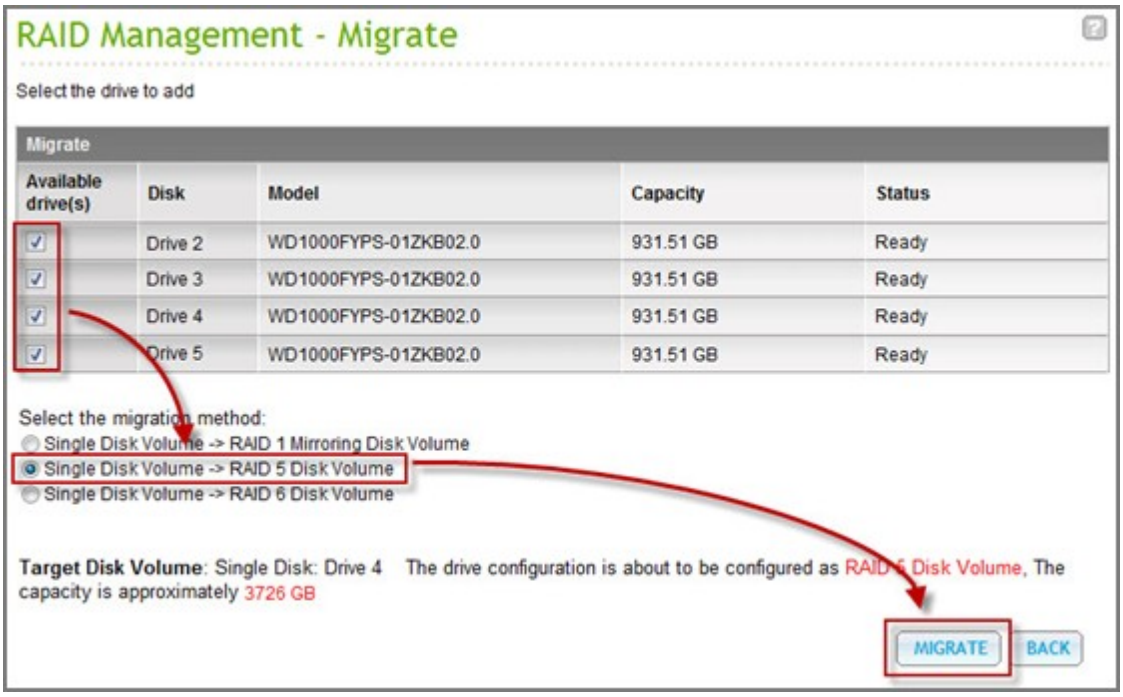
Current Disk Volume Configuration: Logical Volumes

Volume	File System	Total Size	Free Size	Status	
Single Disk: Drive 1	EXT3	931.51 GB	524.68 GB	Ready	
		FORMAT NOW	CHECK NOW	REMOVE NOW	
Single Disk: Drive 2	EXT3	--	--	Unmounted	
		FORMAT NOW	CHECK NOW	REMOVE NOW	
Single Disk: Drive 3	EXT3	--	--	Unmounted	
		FORMAT NOW	CHECK NOW	REMOVE NOW	
Single Disk: Drive 4	EXT3	--	--	Unmounted	
		FORMAT NOW	CHECK NOW	REMOVE NOW	
Single Disk: Drive 5	EXT3	--	--	Unmounted	
		FORMAT NOW	CHECK NOW	REMOVE NOW	

Go to “Disk Management” > “RAID Management”, select the drive configuration for migration and click “Migrate”.

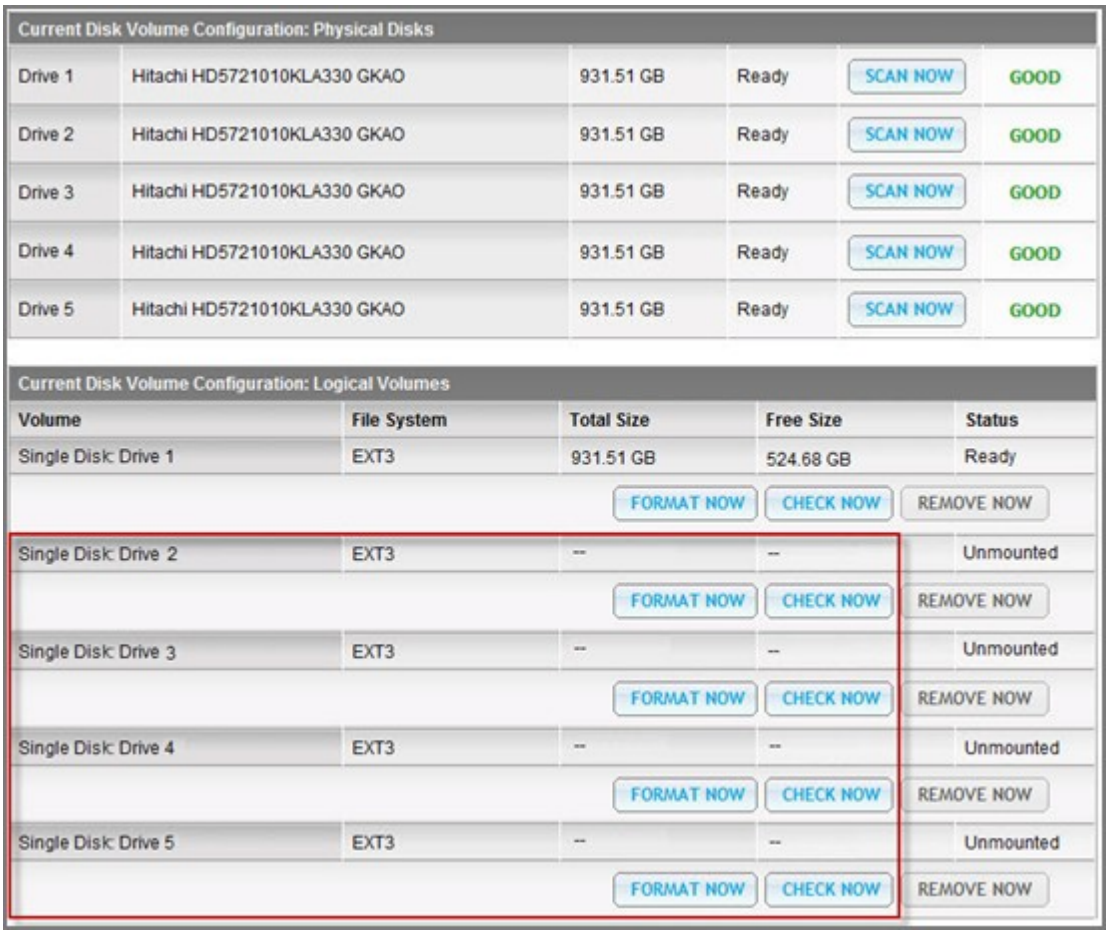


Select one or more available drives and the migration method. The drive capacity after migration is shown. Click “Migrate”.



Note that all the data on the selected hard drive will be cleared. Click “OK” to confirm.

When migration is in process, the required time and total drive capacity after migration are shown in the description field.



Current Disk Volume Configuration: Physical Disks

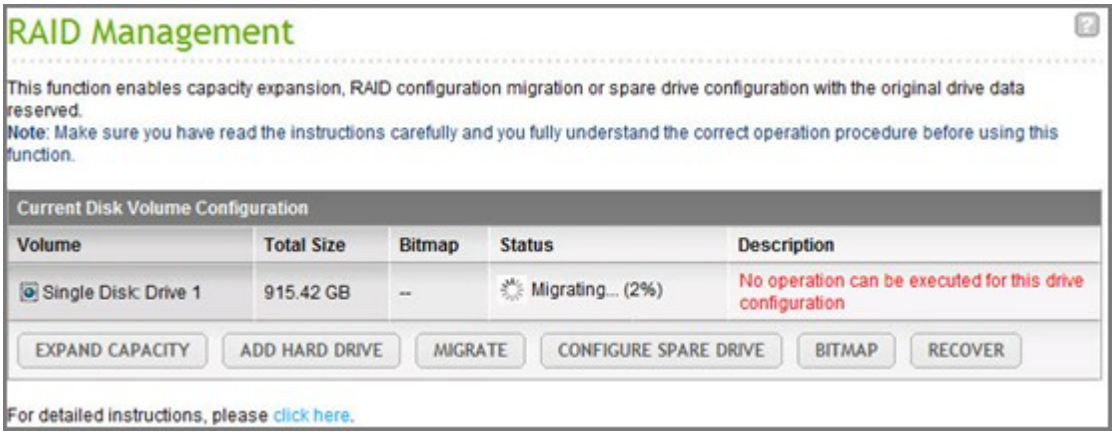
Drive 1	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 2	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 3	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 4	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD
Drive 5	Hitachi HD5721010KLA330 GKAO	931.51 GB	Ready	SCAN NOW	GOOD

Current Disk Volume Configuration: Logical Volumes

Volume	File System	Total Size	Free Size	Status	
Single Disk: Drive 1	EXT3	931.51 GB	524.68 GB	Ready	
			FORMAT NOW	CHECK NOW	REMOVE NOW
Single Disk: Drive 2	EXT3	--	--	Unmounted	
			FORMAT NOW	CHECK NOW	REMOVE NOW
Single Disk: Drive 3	EXT3	--	--	Unmounted	
			FORMAT NOW	CHECK NOW	REMOVE NOW
Single Disk: Drive 4	EXT3	--	--	Unmounted	
			FORMAT NOW	CHECK NOW	REMOVE NOW
Single Disk: Drive 5	EXT3	--	--	Unmounted	
			FORMAT NOW	CHECK NOW	REMOVE NOW

The NAS will enter "Read only" mode when migration is in process during 11%–49% to assure the data of the RAID configuration will be consistent after RAID migration completes.

After migration completes, the new drive configuration (RAID 5) is shown and the status is Ready. You can start to use the new drive configuration.



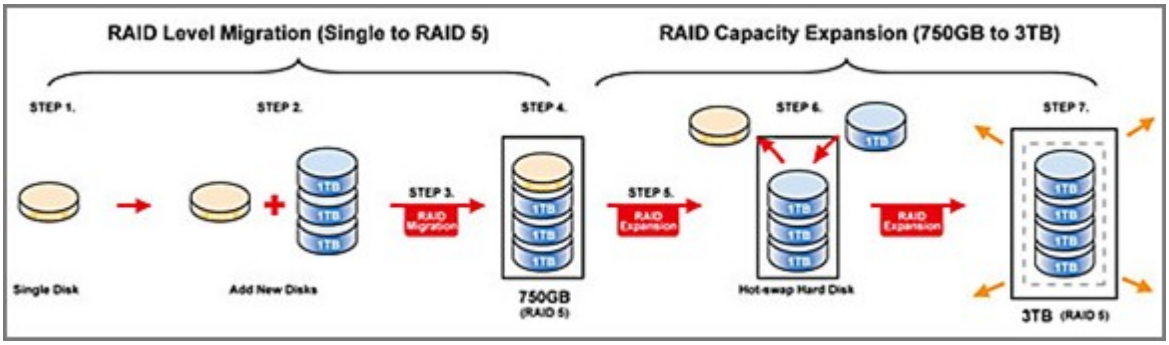
The process may take from hours to tens of hours to finish depending on the hard drive size. You can connect to the web page of the NAS to check the status later.

Use Online RAID Capacity Expansion and Online RAID Level Migration

Scenario

You had a tight schedule to set up a file server and an FTP server. However, you had only one 250GB hard drive. Therefore, you set up the TS-509 Pro with the single disk configuration.

The original plan was to set up a 3TB RAID 5 network data centre with the TS-509 Pro.
You now plan to upgrade the disk configuration of the TS-509 Pro to RAID 5 and expand the total storage capacity to 3TB with all the original data retained after the hard drives are purchased.



Execute online RAID level migration to migrate the system from single disk to RAID 5. The total storage capacity will be 750GB, RAID 5 (with one 250GB hard drive and three 1TB hard drives, the disk usage will be 250GB*4 for RAID 5). You can refer to the previous step for the operation procedure.

Execute online RAID capacity expansion to replace the 250GB hard drive with a new 1TB hard drive, and then expand the logical volume from 750GB to 3TB of RAID 5. You can refer to the previous step for the operation procedure.

Add a hard drive

Follow the steps below to add a hard drive member to a RAID 5 or RAID 6 disk configuration.

1. Make sure the status of the RAID 5 or RAID 6 configuration is "Ready".
2. Install a hard drive on the NAS. If you have a hard drive which has already been formatted as single disk volume on the NAS, you can add this hard drive to the RAID 5 or RAID 6 configuration. You are recommended to use hard disk drives of the same storage capacity for the RAID configuration.
3. Select the RAID 5 or RAID 6 configuration on the "RAID Management" page and click "ADD HARD DRIVE".
4. Select the new hard drive member. The total drive capacity after adding the drive will be shown. Click "ADD HARD DRIVE".
5. All the data on the new hard drive member will be deleted during this process. The data on the original RAID 5 or RAID 6 configuration will be retained. Click "OK". The NAS will beep twice.

To add hard drives member to a RAID 10 disk volume, repeat the above steps. Note that you need to add an even number of hard disk drives to a RAID 10 volume. The storage capacity of the RAID 10 volume will increase upon successful configuration.

This process may take a few hours to tens of hours to complete depending on the number and the size of the hard drive. Please wait patiently for the process to finish. Do NOT turn off the NAS during this process. You can use a RAID configuration of larger capacity after the process.

Configure Spare Drive

You can add a spare drive to or remove a spare drive from a RAID 5, 6, or 10 configuration.

Follow the steps below to use this feature.

1. Make sure the status of the RAID 5, 6, 10 configuration is "Ready".
2. Install a hard drive on the NAS. If you have a hard drive which has already been formatted as single disk volume on the NAS, you can configure this hard drive as the spare drive. You are recommended to use hard disk drives of the same storage capacity for the RAID configuration.
3. Select the RAID volume and click "CONFIGURE SPARE DRIVE".
4. To add a spare drive to the selected configuration, select the hard drive and click "CONFIGURE SPARE DRIVE". To remove a spare drive, unselect the spare drive and click "CONFIGURE SPARE DRIVE".
5. All the data on the selected hard drive will be deleted. Click "OK" to proceed.

The original data on the RAID 5, 6, or 10 disk volume will be retained. After the configuration completes, the status of the disk volume will become "Ready".

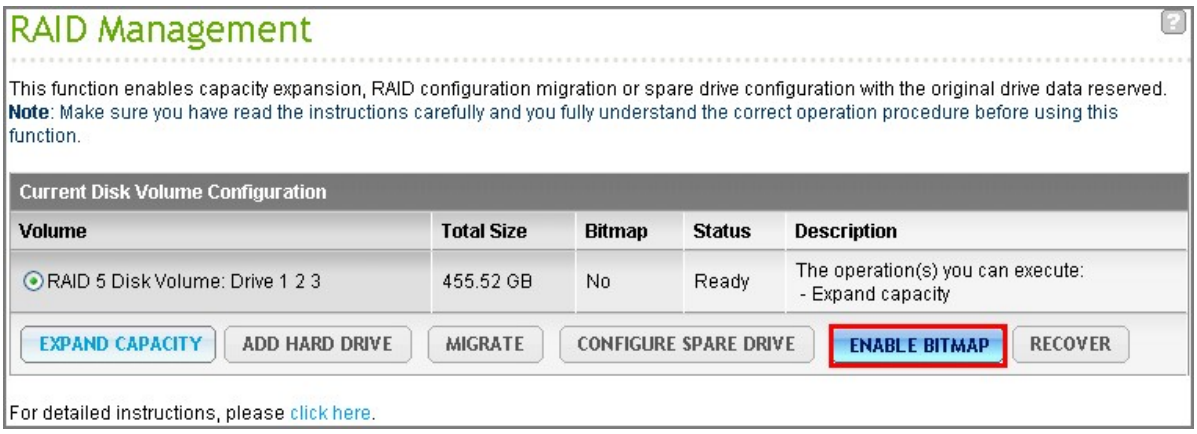
A hot spare drive must be removed from the disk volume before executing the following action:

- Online RAID capacity expansion
- Online RAID level migration
- Adding a hard drive member to a RAID 5, RAID 6 or RAID 10 volume

Bitmap

Bitmap improves the time for RAID rebuilding after an unexpected error, or removing or re-adding a member hard drive of the RAID configuration. If an array has a bitmap, the member hard drive can be removed and re-added and only blocks changes since the removal (as recorded in the bitmap) will be re-synchronized. To use this feature, select a RAID 1, 5, or 6 disk volume and click "ENABLE BITMAP".

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



Recover (RAID Recovery)

RAID Recovery: When the NAS is configured as RAID 1, RAID 5, or RAID 6 and any number of hard drives is uplugged from the NAS 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 hard drive members are disconnected or unplugged, you can plug in the same hard drives into the same drive slots and use this function to recover the volume status from "Not active" to "Normal". The disk volume can be used normally after successful recovery.

Disk volume	Supports RAID recovery	Maximum number of disk removal allowed
Single	No	-
JBOD	Yes	1 or more
RAID 0	Yes	1 or more
RAID 1	Yes	1 or 2
RAID 5	Yes	2 or more
RAID 6	Yes	3 or more
RAID 10	No	-

Note:

- After recovering a RAID 1, RAID 5 or RAID 6 disk volume from not active to degraded mode by the RAID recovery, you can read or write the volume normally. The volume status will be recovered to normal after synchronization.
- If the disconnected drive member is damaged, the RAID recovery function will not work.

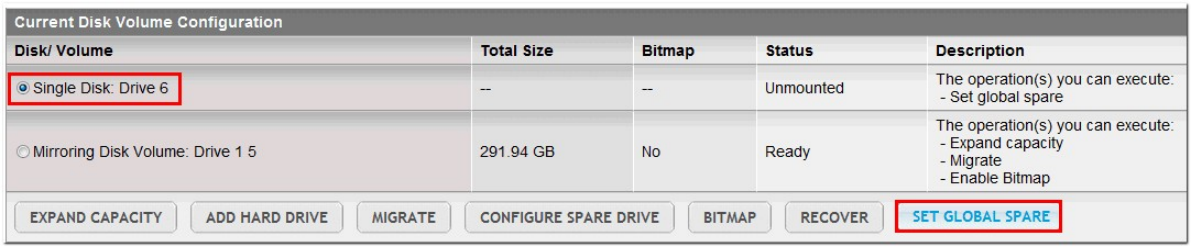
	Standard RAID 5	QNAP RAID 5	Standard RAID 6	QNAP RAID 6
Degraded mode	N-1	N-1	N-1 & N-2	N-1 & N-2
Read Only Protection (for immediate data backup & hard drive replacement)	N/A	N-1, bad blocks found in the surviving hard drives of the array.	N/A	N-2, bad blocks found in the surviving hard drives of the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

N = Number of hard disk drives in the array

Set/Cancel Global Spare

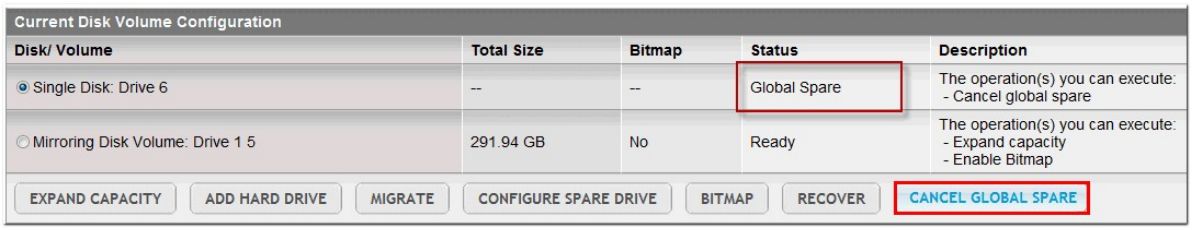
A global spare drive replaces a failed hard drive in any RAID 1, 5, 6, 10 disk volumes on the NAS automatically. When the same global spare drive is shared by multiple RAID volumes on the NAS, the spare drive will replace the first failed drive in a RAID volume.

To set a disk drive as a global spare drive, select the single disk volume and click "Set Global Spare". **All the disk data will be cleared on the hard drive.**



Note: The capacity of the global spare drive must be equal to or larger than that of a member drive of a RAID disk volume.

To cancel a global spare drive, select the drive and click "Cancel Spare Drive".



Further information about RAID management of the NAS:

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

Original Disk Configuration * No. of Hard Disk Drives	No. of New Hard Disk Drives	Action	New Disk Configuration * No. of Hard Disk Drives
RAID 5 * 3	1	Add hard drive member	RAID 5 * 4
RAID 5 * 3	2	Add hard drive member	RAID 5 * 5
RAID 5 * 3	3	Add hard drive member	RAID 5 * 6
RAID 5 * 3	4	Add hard drive member	RAID 5 * 7
RAID 5 * 3	5	Add hard drive member	RAID 5 * 8
RAID 5 * 4	1	Add hard drive member	RAID 5 * 5
RAID 5 * 4	2	Add hard drive member	RAID 5 * 6
RAID 5 * 4	3	Add hard drive member	RAID 5 * 7
RAID 5 * 4	4	Add hard drive member	RAID 5 * 8
RAID 5 * 5	1	Add hard drive member	RAID 5 * 6
RAID 5 * 5	2	Add hard drive member	RAID 5 * 7
RAID 5 * 5	3	Add hard drive member	RAID 5 * 8
RAID 5 * 6	1	Add hard drive member	RAID 5 * 7
RAID 5 * 6	2	Add hard drive member	RAID 5 * 8
RAID 5 * 7	1	Add hard drive member	RAID 5 * 8
RAID 6 * 4	1	Add hard drive member	RAID 6 * 5
RAID 6 * 4	2	Add hard drive member	RAID 6 * 6
RAID 6 * 4	3	Add hard drive member	RAID 6 * 7
RAID 6 * 4	4	Add hard drive member	RAID 6 * 8
RAID 6 * 5	1	Add hard drive member	RAID 6 * 6
RAID 6 * 5	2	Add hard drive member	RAID 6 * 7
RAID 6 * 5	3	Add hard drive member	RAID 6 * 8

RAID 6 * 6	1	Add hard drive member	RAID 6 * 7
RAID 6 * 6	2	Add hard drive member	RAID 6 * 8
RAID 6 * 7	1	Add hard drive member	RAID 6 * 8
RAID 10 * 4	2	Add hard drive member	RAID 10 * 6
RAID 10 * 4	4	Add hard drive member	RAID 10 * 8
RAID 10 * 6	2	Add hard drive member	RAID 10 * 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
RAID 10 * 4	1	Online RAID capacity expansion	RAID 10 * 4

RAID 10 * 6	1	Online RAID capacity expansion	RAID 10 * 6
RAID 10 * 8	1	Online RAID capacity expansion	RAID 10 * 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
Single * 1	3	Online RAID level migration	RAID 10 * 4
Single * 1	5	Online RAID level migration	RAID 10 * 6
Single * 1	7	Online RAID level migration	RAID 10 * 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 1 * 2	2	Online RAID level migration	RAID 10 * 4
RAID 1 * 2	4	Online RAID level migration	RAID 10 * 6
RAID 1 * 2	6	Online RAID level migration	RAID 10 * 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

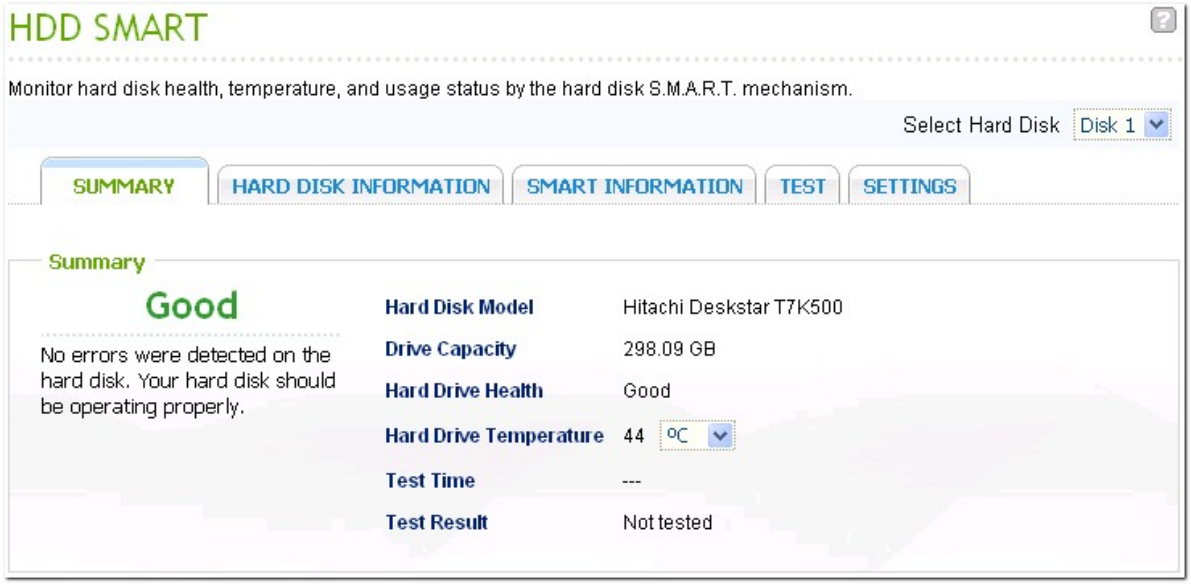
RAID 5 * 3	4	Online RAID level migration	RAID 6 * 7
RAID 5 * 3	5	Online RAID level migration	RAID 6 * 8

4.3 Hard Disk S.M.A.R.T.

Monitor the hard disk drives (HDD) health, temperature, and the usage status by HDD S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology).

The following information of each hard drive on the NAS is available.

Field	Description
Summary	Display the hard drive S.M.A.R.T. summary and the latest test result.
Hard disk information	Display the hard drive details, for example, model, serial number, HDD capacity.
SMART information	Display the hard drive S.M.A.R.T. information. Any items that the values are lower than the threshold are regarded as abnormal.
Test	Perform quick or complete hard drive S.M.A.R.T. test.
Settings	Configure temperature alarm. When the hard drive temperature is over the preset values, the NAS records the error logs. You can also set the quick and complete test schedule. The latest test result is shown on the Summary page.



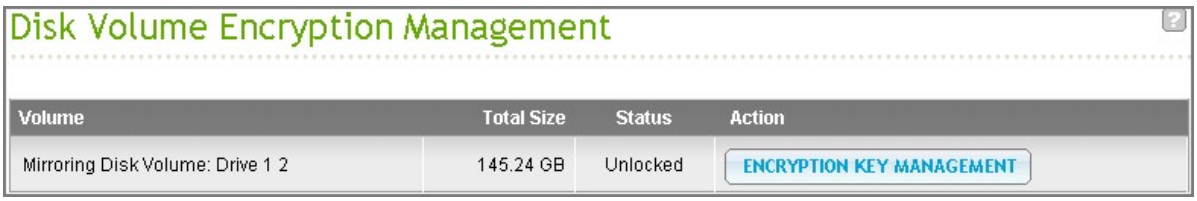
4.4 Encrypted File System

This feature is not supported by TS-110, TS-119, TS-210, TS-219, TS-219P, TS-410, TS-419P, TS-410U, TS-419U, TS-119P+, TS-219P+, TS-419P+, TS-112, TS-212, TS-412, TS-419U+, TS-412U.

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: Upload the encryption file to the NAS to unlock the disk volume. The key can be downloaded from "Encryption Key Management" page after the disk volume has been unlocked successfully.

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



How to use the data encryption feature on QNAP Turbo NAS

The disk volumes on the NAS can be encrypted with 256-bit AES encryption for data breach protection. The encrypted disk volumes can only be mounted for normal read/write access with the authorized password. The encryption feature protects the confidential data from unauthorized access even if the hard drives or the entire NAS were stolen.

About AES encryption:
In cryptography, the Advanced Encryption Standard (AES) is an encryption standard adopted by the U. S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256 […]. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide. (Source: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

The AES volume-based encryption is applicable only to specific QNAP NAS models.
Please refer to the comparison table at: http://www.qnap.com/images/products/comparison/Comparison_NAS.html

Before you start
Please beware of the following before using the data encryption feature of the NAS.

- The encryption feature of the NAS is volume-based. A volume can be a single disk, a JBOD configuration, or a RAID array.
- Select whether or not to encrypt a disk volume before it is created on the NAS. In other words, you will not be able to encrypt a volume after it has been created unless the disk volume is initialized. Note that initializing a disk volume will clear all the disk data.
- The encryption on the disk volume cannot be removed without initialization. To remove the encryption on the disk volume, you have to initialize the disk volume and all the data will be cleared.
- Keep the encryption password or key safe. If you forgot the password or lost the encryption key, the data cannot be accessed anymore.
- Before you start, read the instructions carefully and strictly adhere to the instructions.

Activate disk volume encryption on the NAS

Encrypt the disk volume during the NAS installation

Follow the instructions of the Quick Installation Guide (QIG) to initialize the NAS by the web-based interface. In Step 6 of the quick configuration, select "Yes" for the "Encrypt disk volume" option.

Note: You can execute disk volume encryption by the LCD panel (if available) of the NAS. Please refer to the QIG for the instructions.

Once you have selected to encrypt the disk volume, the encryption settings will appear.

Enter an encryption password, which will be used to unlock the encrypted volume. The encryption password must be 8-16 characters long and cannot contain spaces ( ). Try to select a long password which combines alphabets and numbers.

- Use Default Value: Select to use the default encryption password "admin".
- Save Encryption Key: Save the encryption key on the NAS (this option can be changed later).
  - If checked: The NAS will unlock the encrypted disk volume automatically using the saved password when it starts up.
  - If not checked: The encrypted disk volume is locked when the NAS starts up. You have to login the NAS as an administrator and enter the encryption password to unlock the disk volume.

Then proceed to the next step and finish the NAS installation.

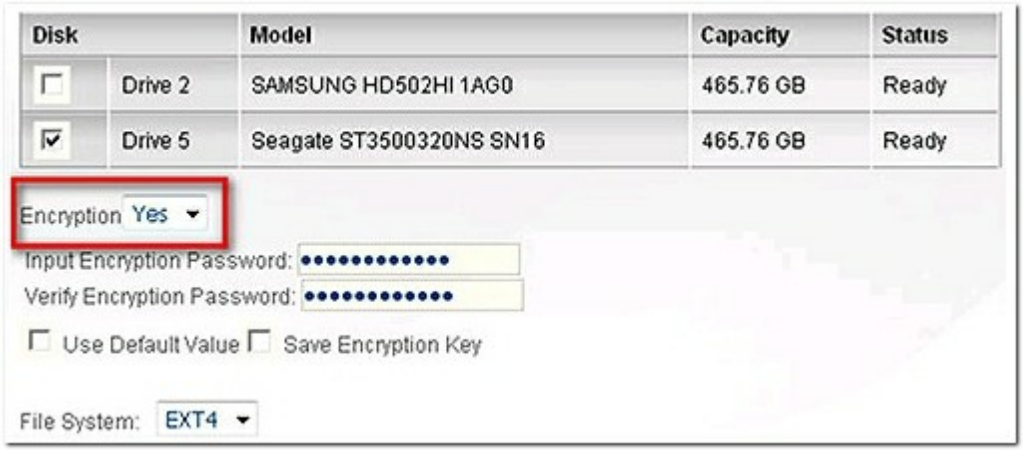
Create a new encrypted disk volume with new hard drives

If the NAS has been installed, to create a new encrypted disk volume by installing new hard drives on the NAS, follow the steps below.

1. Install the new hard drive(s) on the NAS.
2. Login the NAS as an administrator. Go to "Disk Management" > "Volume Management".
3. Select the disk volume you want to configure according to the number of new hard drives installed.

4. Select the hard drive(s) for creating the disk volume. In this example, we select to create a single drive. The procedure applies also to a RAID configuration.

5. Select "Yes" for the "Encryption" option and enter the encryption settings.



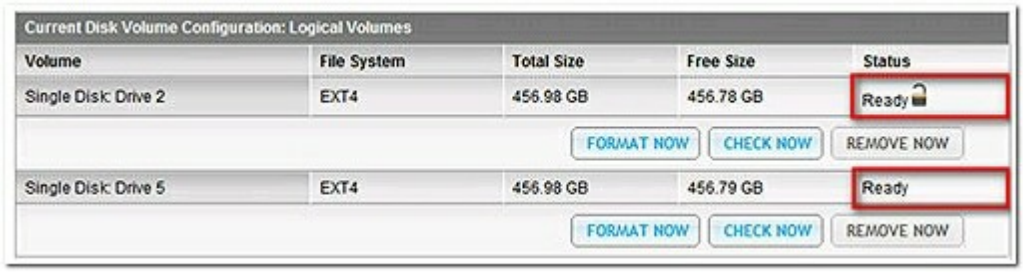
6. Then click "CREATE" to create the new encrypted volume. Note that all the data on the selected drives will be DELETED! Please back up the data before creating the encrypted volume.

You have created a encrypted disk volume on the NAS.

Verify that disk volume is encrypted

To verify the disk volume is encrypted, login the NAS as an administrator. Go to "Disk Management" > "Volume Management".

You will be able to see the encrypted disk volume, with a lock icon in the Status column.
The lock will be open if the encrypted volume has been unlocked. A disk volume without the lock icon in the Status column is not encrypted.

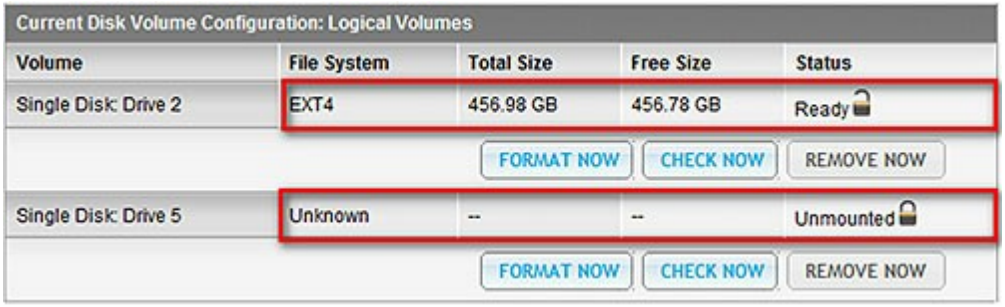


Behavior of an encrypted volume upon system reboot

In this example, we have two encrypted disk volumes on the NAS.

The first volume (Single Disk Drive 2) has been created with the option "Save Encryption Key" enabled. The second volume (Single Disk Drive 5) has been created with the option "Save Encryption Key" disabled.

After restarting the NAS, check the volume status. The first drive has been unlocked and mounted but the second drive is locked. Since the encryption key is not saved on the second disk volume, you have to manually enter the encryption password to unlock it.



- Saving the key on the NAS will protect you only if your hard drives are stolen. However, there is a risk of data breach if the entire NAS is stolen as the data is accessible after restarting the NAS.
- If you select not to save the encryption key on the NAS, your NAS will be protected against data breach even if the entire NAS were stolen. The disadvantage is that you have to unlock the disk volume manually on each system restart.

Encryption key management: new password, save encryption key, export encryption key

To manage the encryption key settings, login the NAS as an administrator and go to "Disk Management" > "Encrypted File System".

Click "ENCRYPTION KEY MANAGEMENT" on the "Action" column of an unlocked disk volume.

You can perform the following actions:

- Change the encryption key
- Save the encryption key on the NAS
- Download the encryption key file

- Change the encryption key:
  Input your old encryption password and input the new password. (Note that after the password is changed, any previously exported keys will not be working anymore. You have to download the new encryption key if necessary, see below).
- Save Encryption Key:
  Save the encryption key on the NAS for automatic unlocking and mounting the encrypted disk volume when the NAS restarts.
- Download Encryption Key File:
  Input the encryption password to download the encryption key file. Downloading the encryption key file will allow you to save the encryption key in a file. The file is also encrypted and can be used to unlock a volume, without knowing the real password (see "unlock a disk volume manually" below). Please save the encryption key file in a secure place!

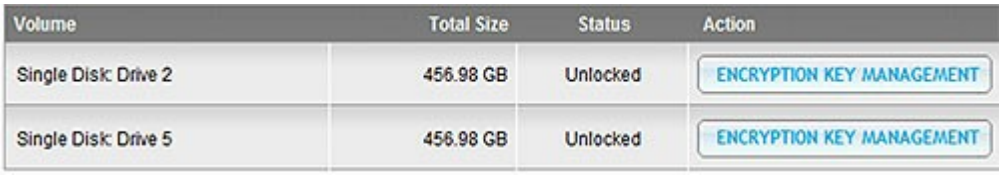
Unlock a disk volume manually

To unlock a volume, login the NAS as an administrator. Go to "Disk Management" > "Encrypted File System".

You will be able to see your encrypted volumes and their status: locked or unlocked.

To unlock your volume, you can either input the encryption password, or use the encryption key file that has been exported previously.

If the encryption password or the key file is correct, the volume will be unlocked and become available.



4.5 iSCSI

Portal Management 129
Target Management 140
Advanced ACL 166
LUN Backup 170

4.5.1 Portal Management

The NAS supports built-in iSCSI (Internet Small Computer System Interface) service for server clustering and virtualized environments.

iSCSI Configuration

The NAS supports built-in iSCSI service. To use this function, follow the steps below:

1. Install an iSCSI initiator on the computer (Windows PC, Mac, or Linux).
2. Enable iSCSI Target Service on the NAS and create an iSCSI target.
3. Run the iSCSI initiator and connect to the iSCSI target (NAS).
4. After successful logon, format the iSCSI target (disk volume). You can start to use the disk volume on the NAS as a virtual drive on the computer.

In between the relationship of your computer and the storage device, the computer is called an initiator because it initiates the connection to the device, which is called a target.

Note: It is suggested NOT to connect to the same iSCSI target with two different clients (iSCSI initiators) at the same time, because this may lead to data damage or disk damage.

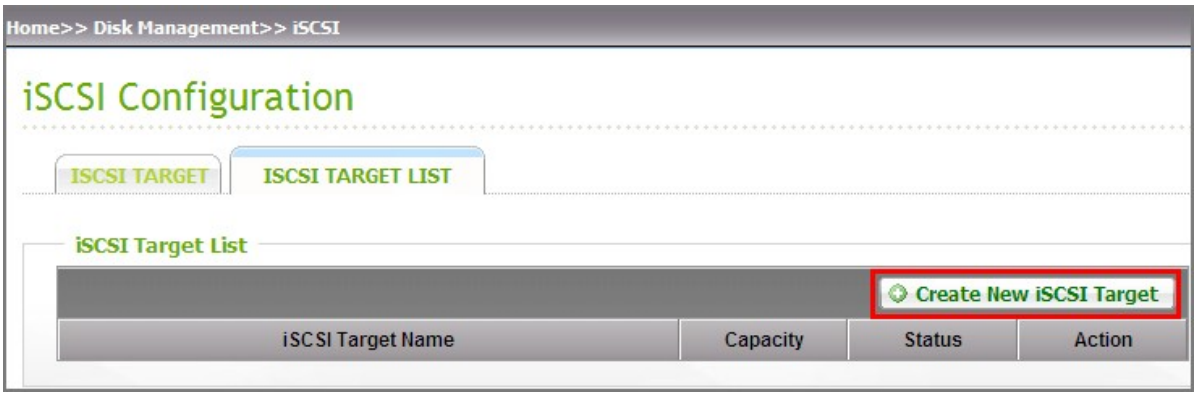
The description below applies to non Intel-based NAS models running firmware **prior to** version 3.3.0 and Intel-based NAS models running firmware **prior to** version 3.2.0 only. If your NAS models are not listed, please visit http://www.qnap.com for details.

Intel-based NAS	TS-x39 series, TS-x59 series, TS-x69 series, TS-509, TS-809, TS-809 Pro, TS-809U-RP, SS-439 Pro, SS-839 Pro, TS-x59 Pro+, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP
Non Intel-based NAS	TS-109, TS-209, TS-409, TS-409U, TS-x10, TS-x12, TS-x19 series

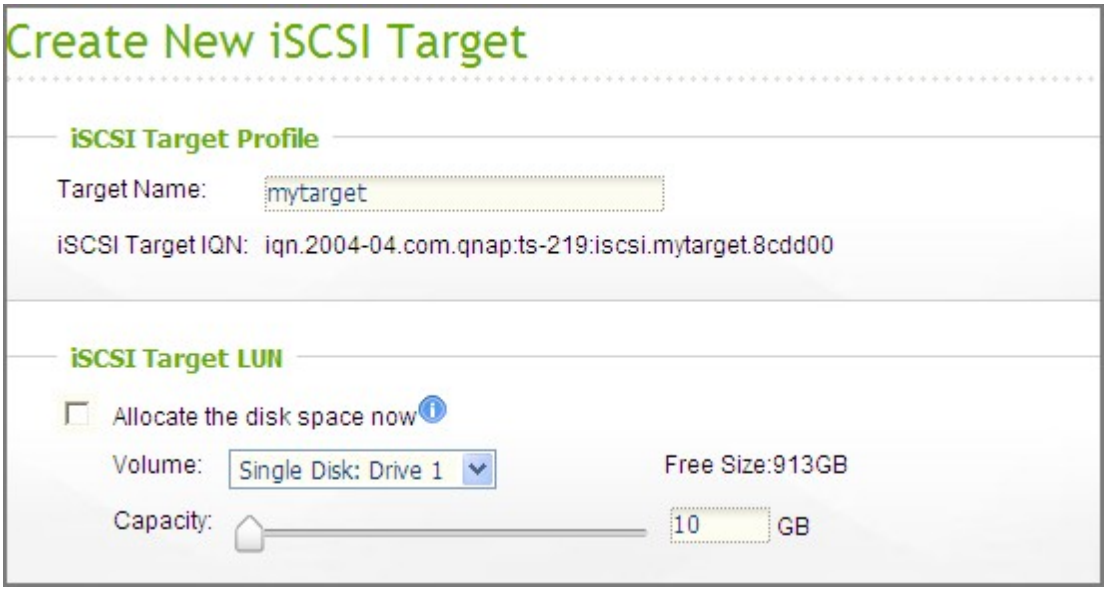
Follow the steps below to create iSCSI targets and LUN on the NAS.

A logical unit number (LUN) will be created for each iSCSI target you create. A maximum of 4 targets and 4 LUNs can be created.

1. Under the tab "iSCSI TARGET LIST", click "Create New iSCSI Target".



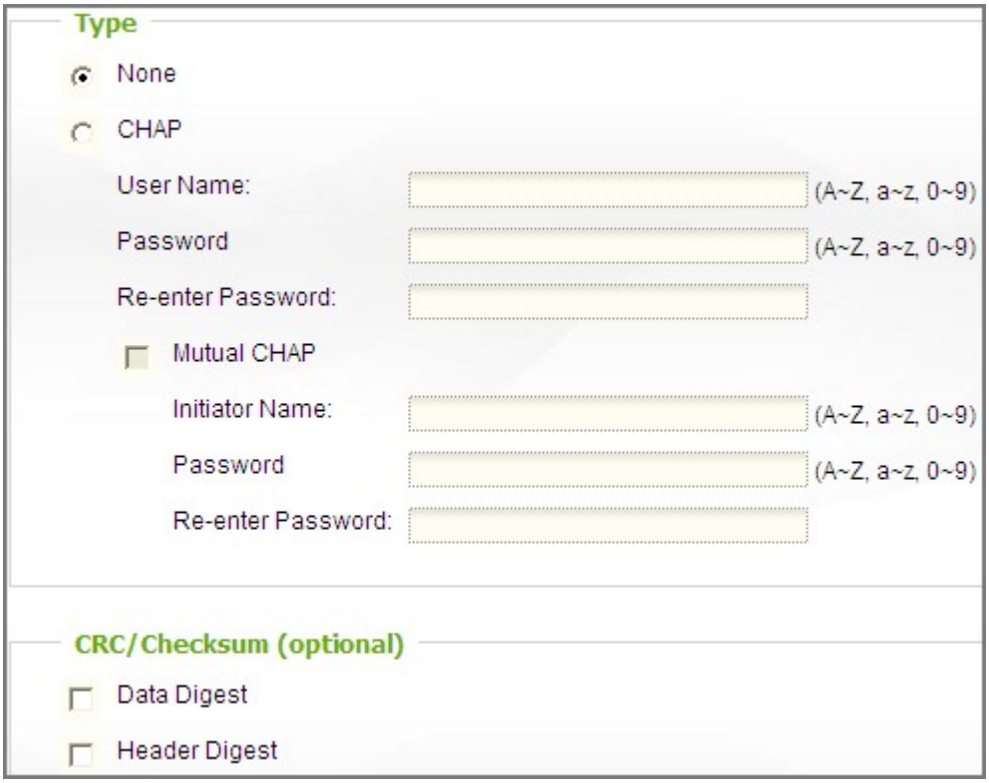
2. Enter the target name. Specify the volume on which the iSCSI target will be created on and the size of the target, also whether or not to pre-allocate the disk space.



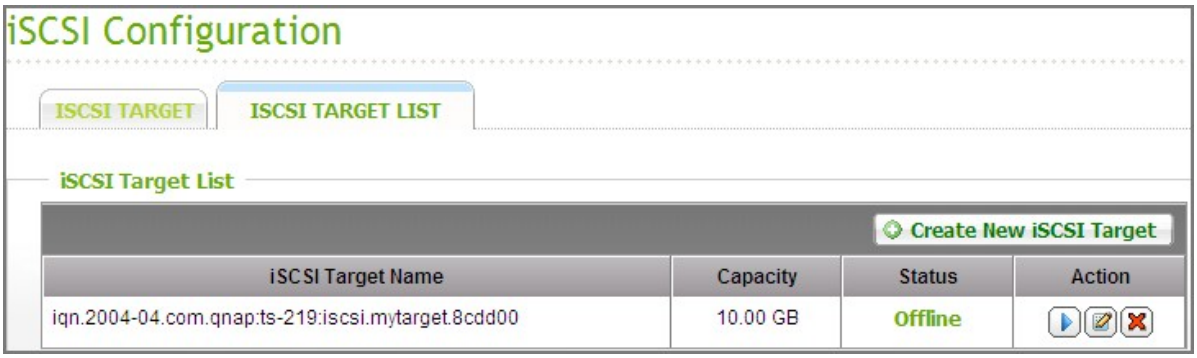
3. Enter the CHAP authentication settings (optional) if the NAS is located on a public or untrusted network. If you enter the user name and password settings under "CHAP" only, only the iSCSI target authenticates the initiator. In other words, the initiators have to enter the user name and password to connect to the target.

Mutual CHAP: Turn on 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



4. Upon successful creation the iSCSI target will be shown on the iSCSI Target List.



5. Select the option "Enable iSCSI Target Service" under the tab "iSCSI TARGET" and click "Apply". The iSCSI target will become ready.

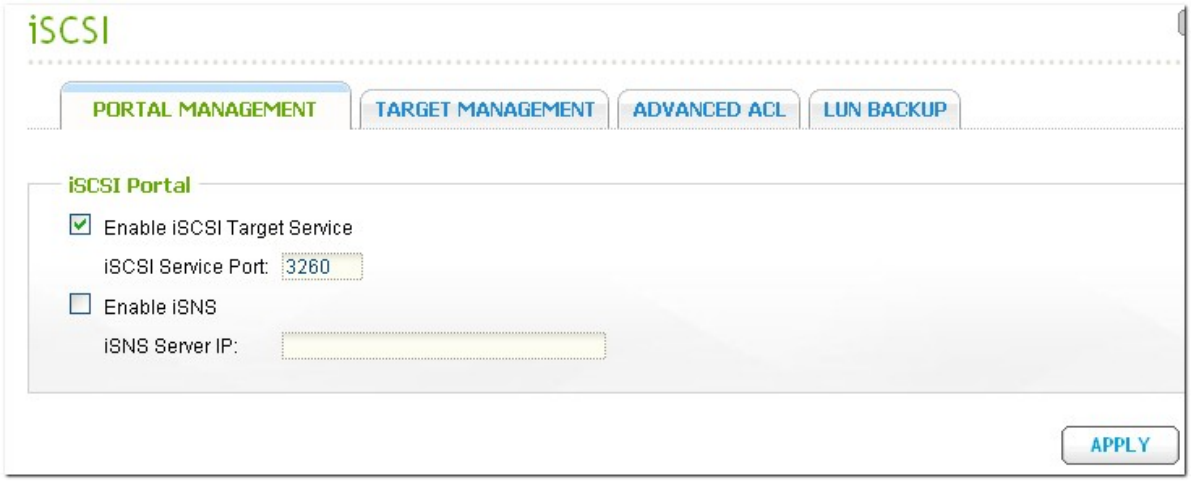
iSCSI Quick Configuration Wizard

The description below applies to non Intel-based NAS models running firmware version 3.3.0 **or later** and Intel-based NAS models running firmware version 3.2.0 **or later** only.

A maximum of 256 iSCSI targets and LUNs can be created. For example, if you create 100 targets on the NAS, the maximum number of LUNs you can create is 156. Multiple LUNs can be created for each target. However, the maximum number of concurrent connections to the iSCSI targets supported by the NAS varies depending on the network infrastructure and the application performance. Too many concurrent connections may slow down the performance of the NAS.

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

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



2. Go to the "Target Management" tab and 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 LUN (Logical unit number). Click "OK".

3. 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 and 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: 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 as the storage capacity of the NAS can be expanded by online RAID capacity expansion.
- Instant Allocation: Allocate the disk space to the LUN instantly. This option guarantees the disk space assigned to the LUN but may take more time to create the LUN.

Enter the name of the LUN 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.

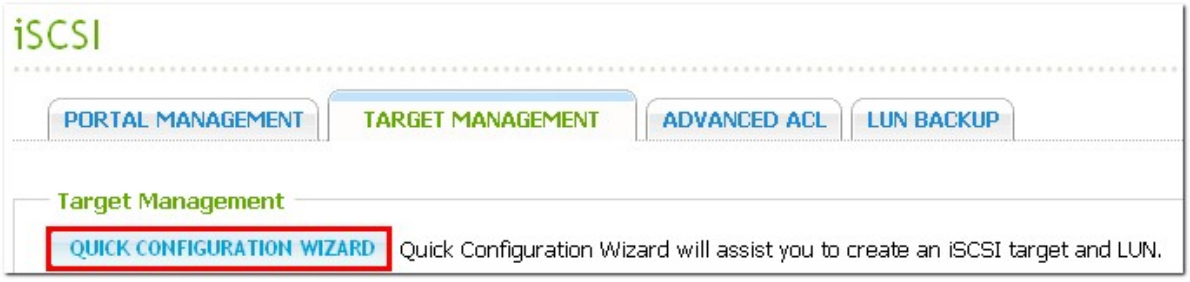
4.5.2 Target Management

Create iSCSI targets

The description below applies to non Intel-based NAS models running firmware version 3.3.0 **or later** and Intel-based NAS models running firmware version 3.2.0 **or later** only.

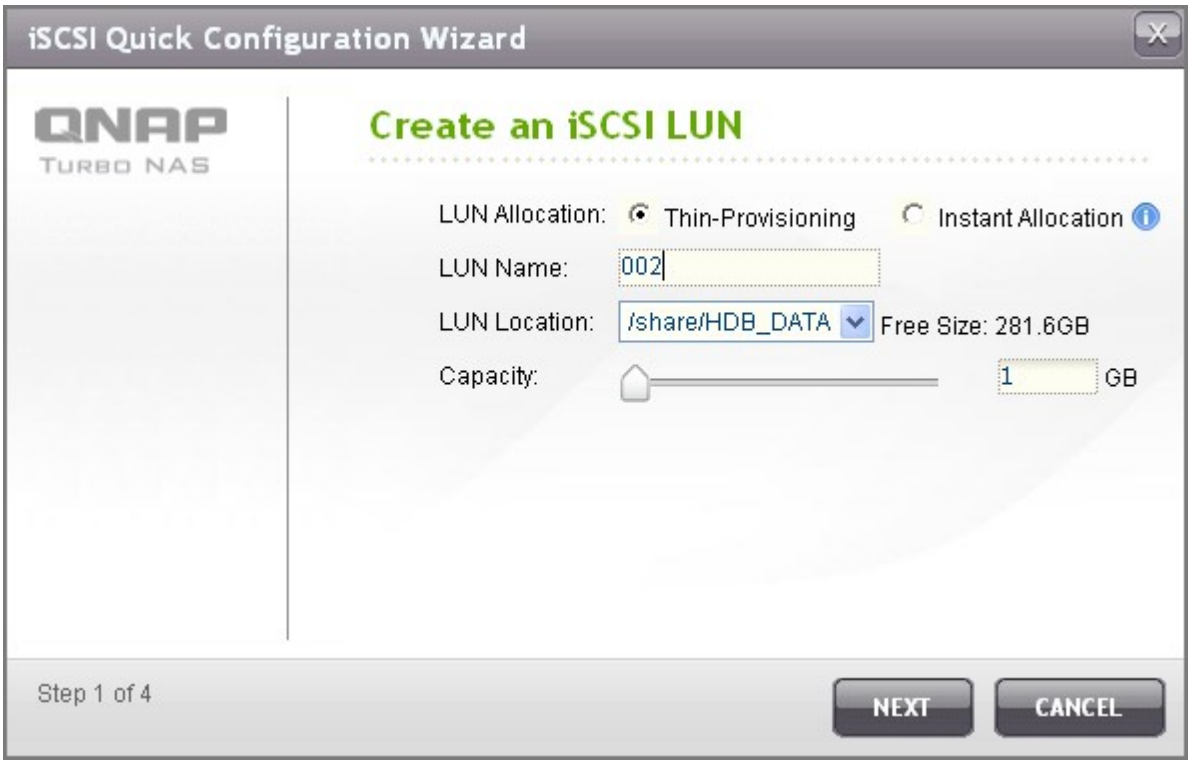
You can create multiple LUNs for an iSCSI target. Follow the steps below to create more LUNs for an iSCSI target.

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

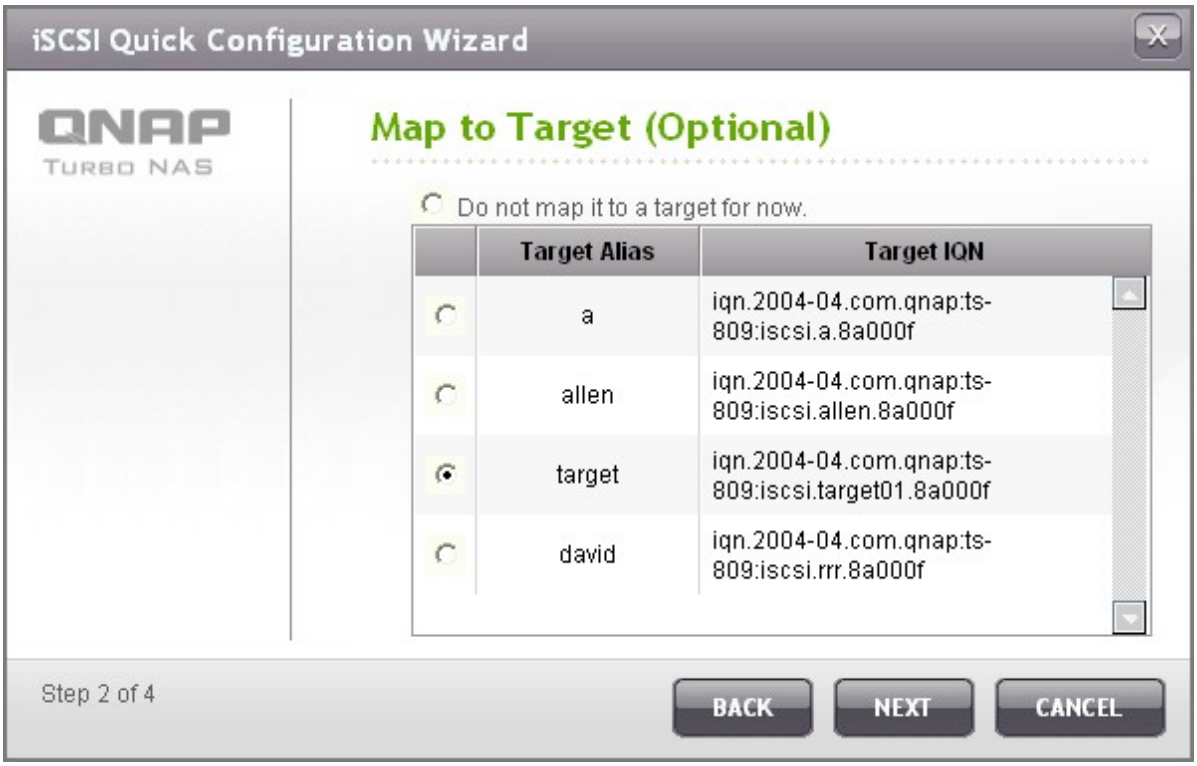


2. Select "iSCSI LUN only" and click "Next".

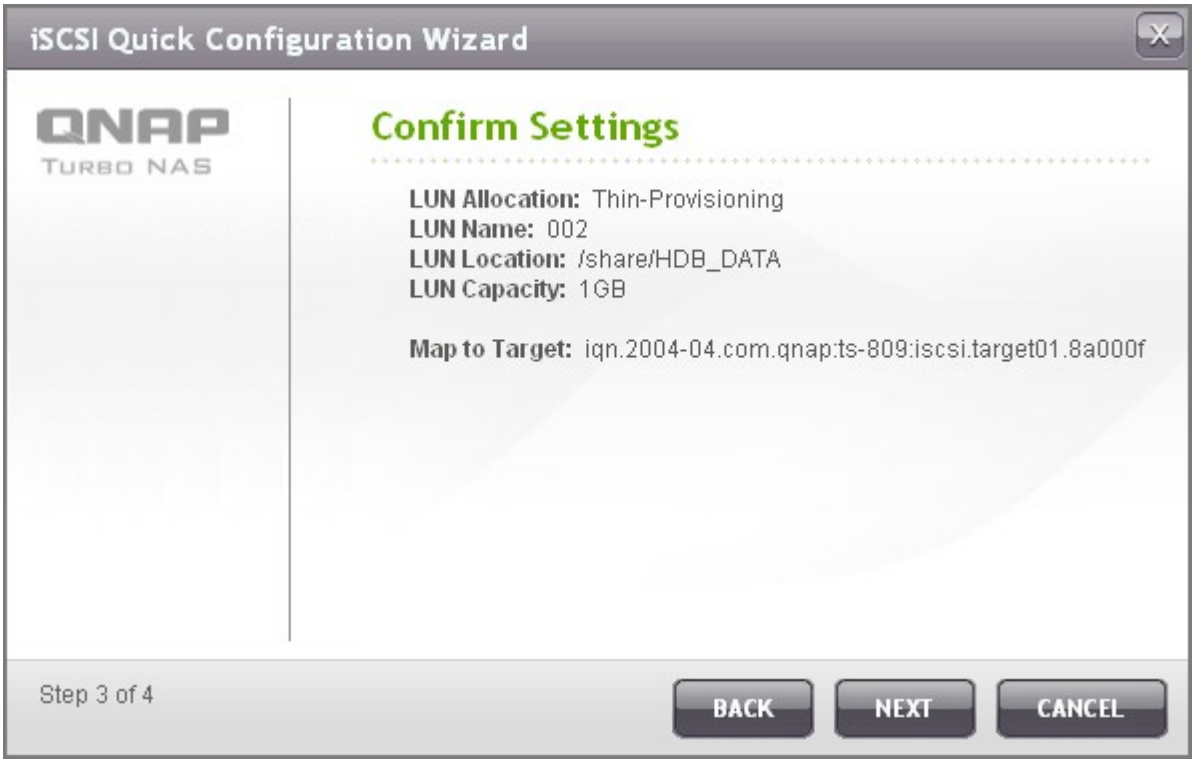
3. Select the allocation method. Enter the name of the LUN, select the LUN directory, and specify the capacity for the LUN. Click “Next”.



4. Select the target to map the LUN to (optional step).

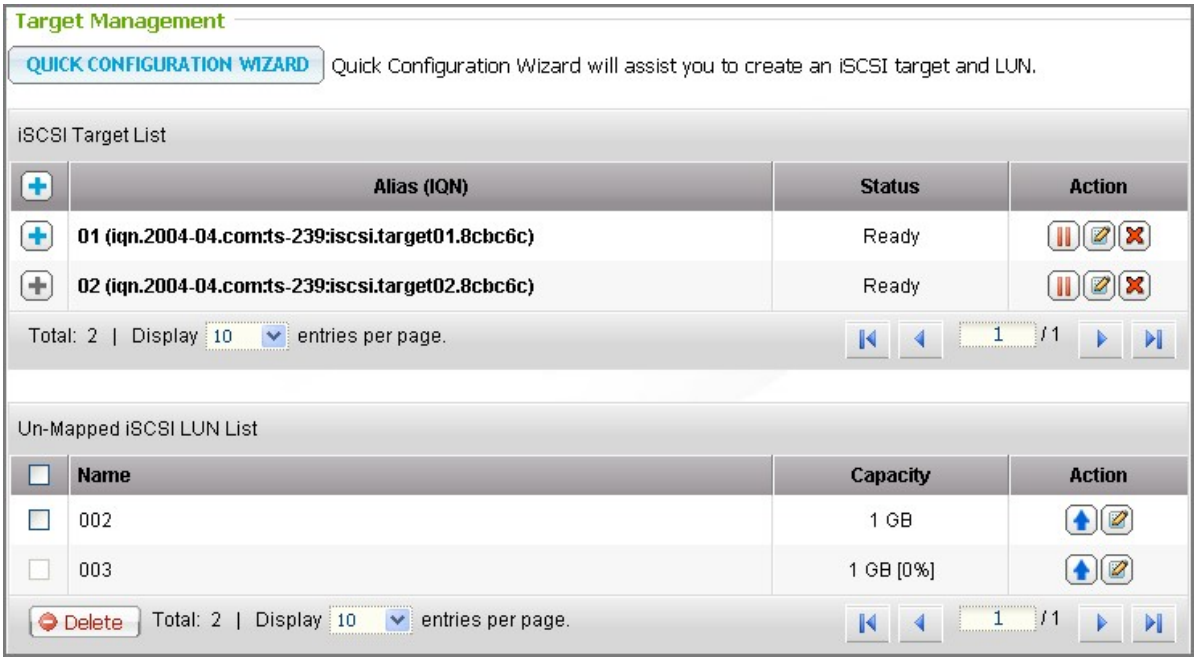


5. Confirm the settings and click “Next”.



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.

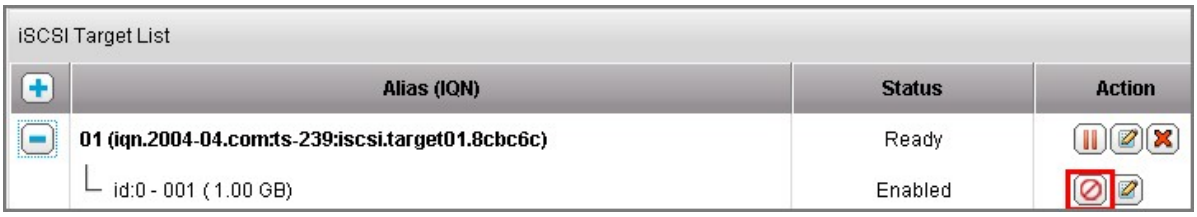
Button	Description
	Deactivate a ready or connected target. Note that the connection from the initiators will be removed.
	Activate an offline target.
	Modify the target settings: target alias, CHAP information, and checksum settings. Modify the LUN settings: LUN allocation, name, disk volume directory, 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 LUN mapping

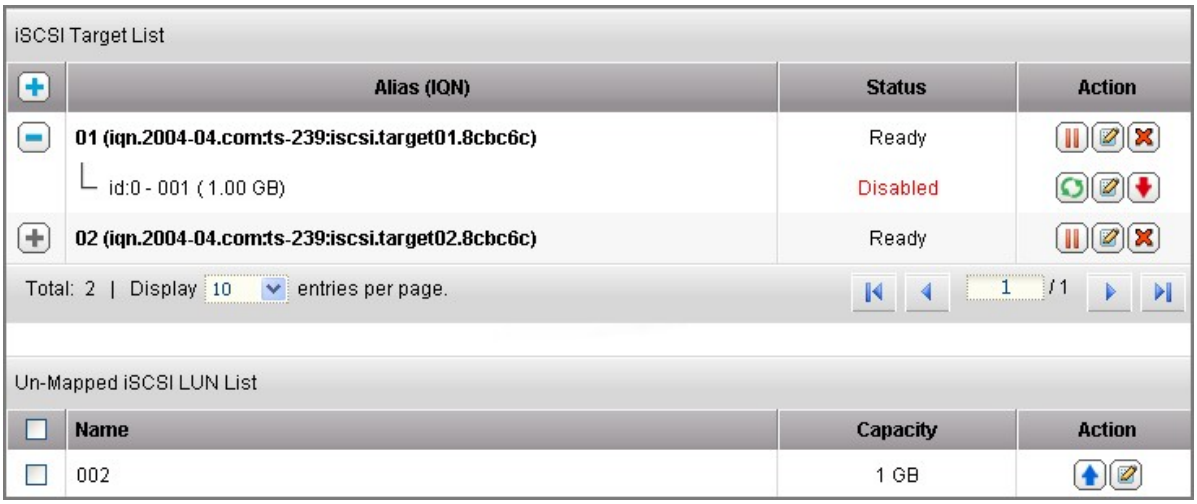
The description below applies to non Intel-based NAS models running firmware version 3.3.0 **or later** and Intel-based NAS models running firmware version 3.2.0 **or later** only.

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

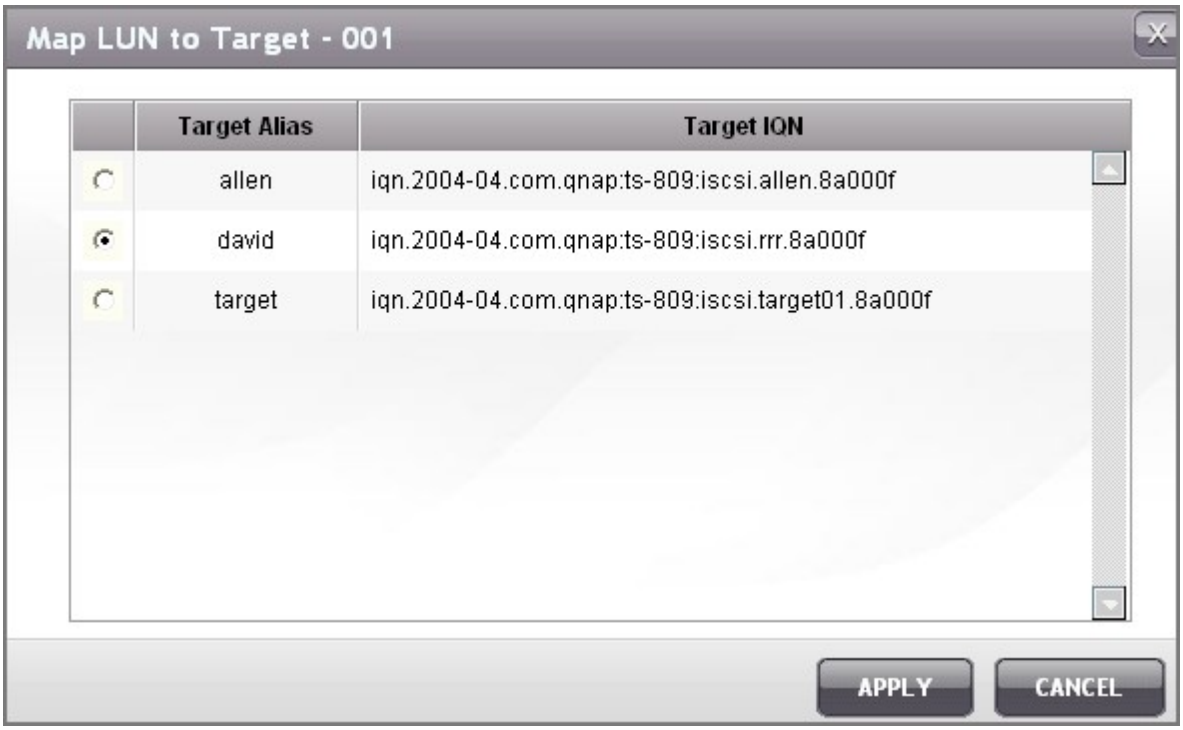
1. Select an iSCSI LUN to unmap from an iSCSI target and click (Disable).



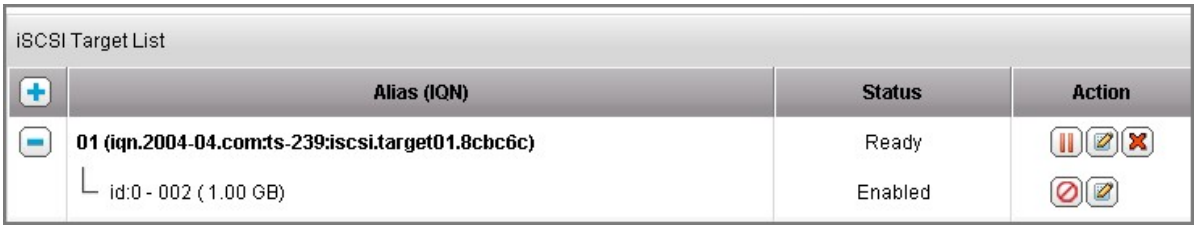
2. Next, click (Unmap) to unmap the LUN. The LUN will appear on the Un-Mapped iSCSI LUN List. Click (Map) to map the LUN to another target.



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



4. The LUN is mapped to the target.

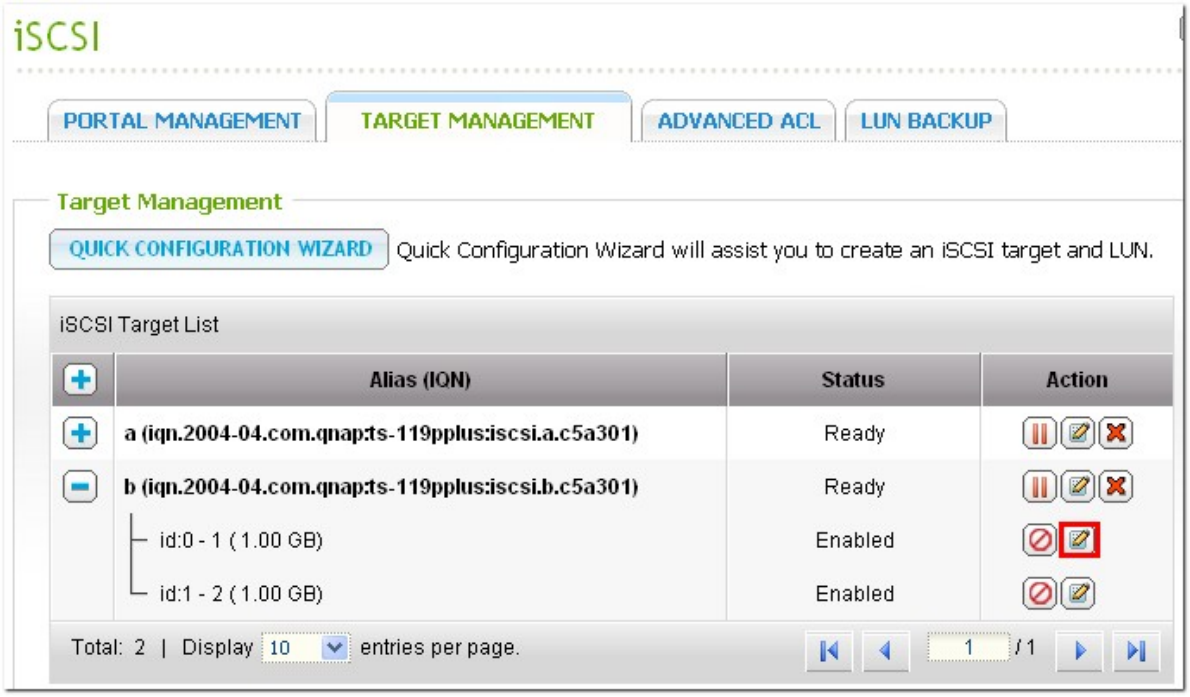


After creating the iSCSI targets and LUN on the NAS, you can use the iSCSI initiator installed on your computer (Windows PC, Mac, or Linux) to connect to the iSCSI targets and LUN and use the disk volumes as the virtual drives on your computer.

iSCSI LUN capacity expansion

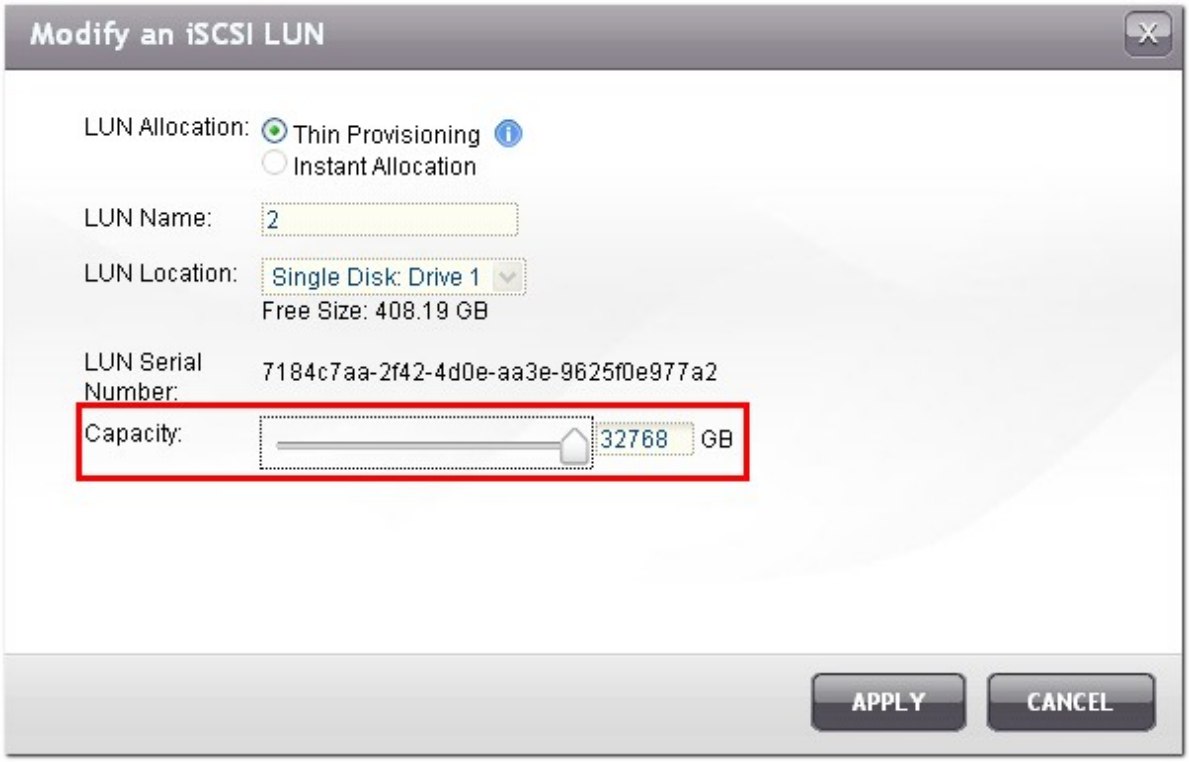
The NAS supports expanding the capacity of an iSCSI LUN. To do so, follow the steps below.

1. Locate an iSCSI LUN on the iSCSI target list in "iSCSI" > "Target Management". Click .



2. Use the slide bar to specify the capacity of the LUN or enter the capacity in the field. Note that the LUN capacity can be increased many times up to the maximum limit but cannot be decreased.

Type of LUN allocation	**Maximum LUN capacity**
Thin Provisioning	32TB
Instant Allocation	Free size available on the disk volume



3. Click "Apply" to save the settings.

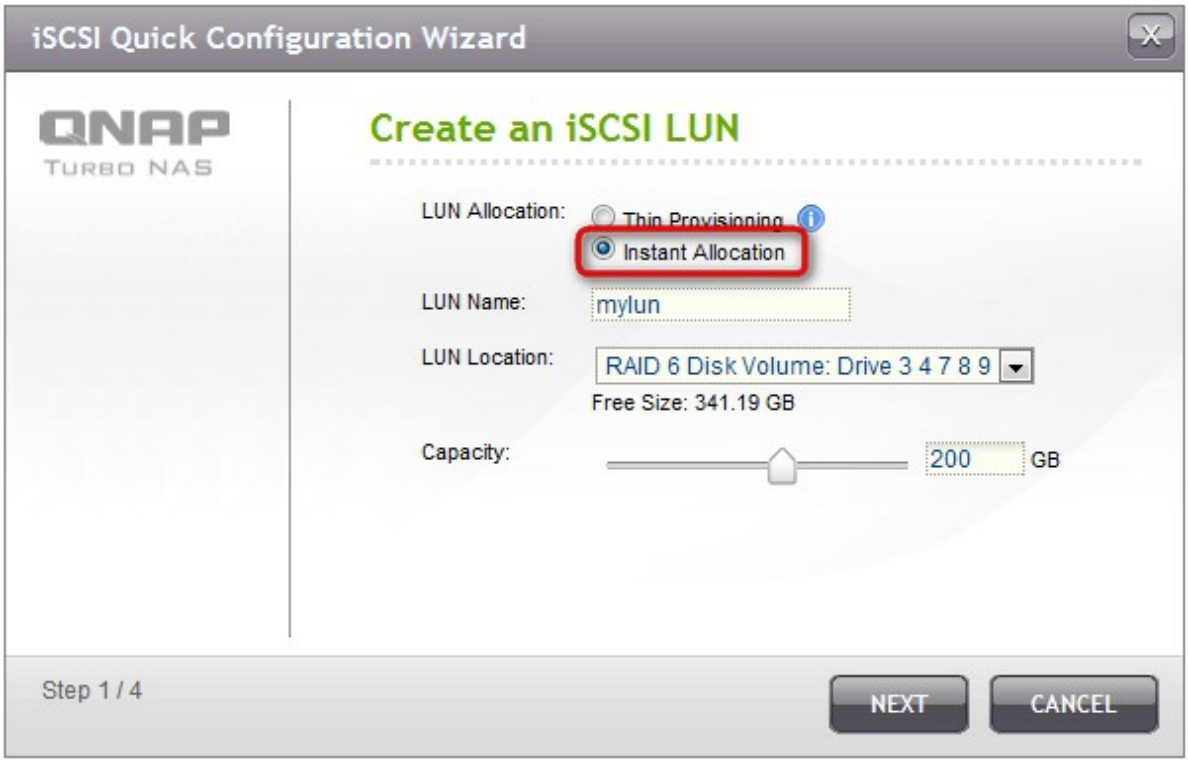
Note: An iSCSI LUN must be mapped to an iSCSI target before increasing the capacity.

Optimize iSCSI performance

In the environments that require high performance storage, such as virtualization, users are recommended to do the following to optimize the iSCSI and NAS hard disks performance:

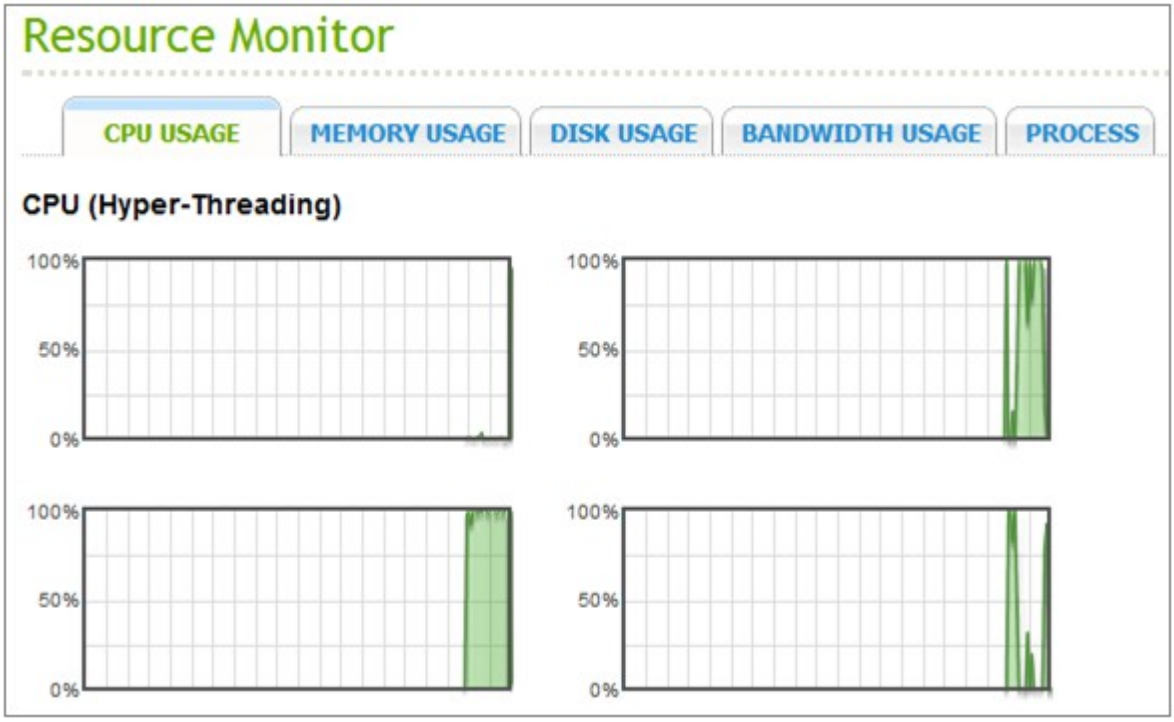
Use instant allocation

When creating an iSCSI LUN, select "Instant Allocation" to achieve slightly higher iSCSI performance. However, the benefits of thin provisioning will be lost.



Create multiple LUNs

Create multiple LUNs according to the processor number of the NAS. The information can be checked in "System Status" > "Resource Monitor". If the NAS has four processors, it is advised to create four or more LUNs to optimize the iSCSI performance.



Use different LUNs for heavy load applications

Spread the applications such as database and virtual machines that need high Read/Write performance on different LUNs. For example, if there are two virtual machines which read and write data intensively on the LUNs, it is recommended to create two LUNs on the NAS so that the VM workloads can be efficiently distributed.

4.5.2.1 Connect to the iSCSI targets by Microsoft iSCSI Initiator on Windows

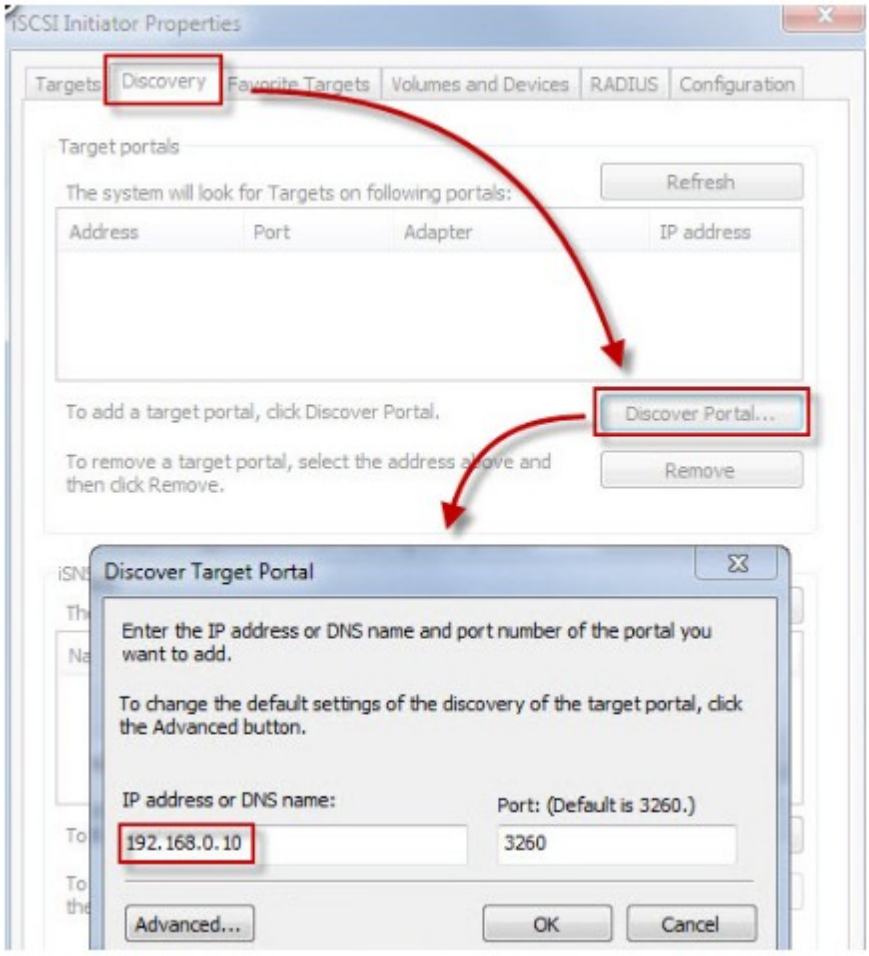
---

Before you start to use the iSCSI target service, make sure you have created an iSCSI target with a LUN on the NAS and installed the correct iSCSI initiator for your OS.

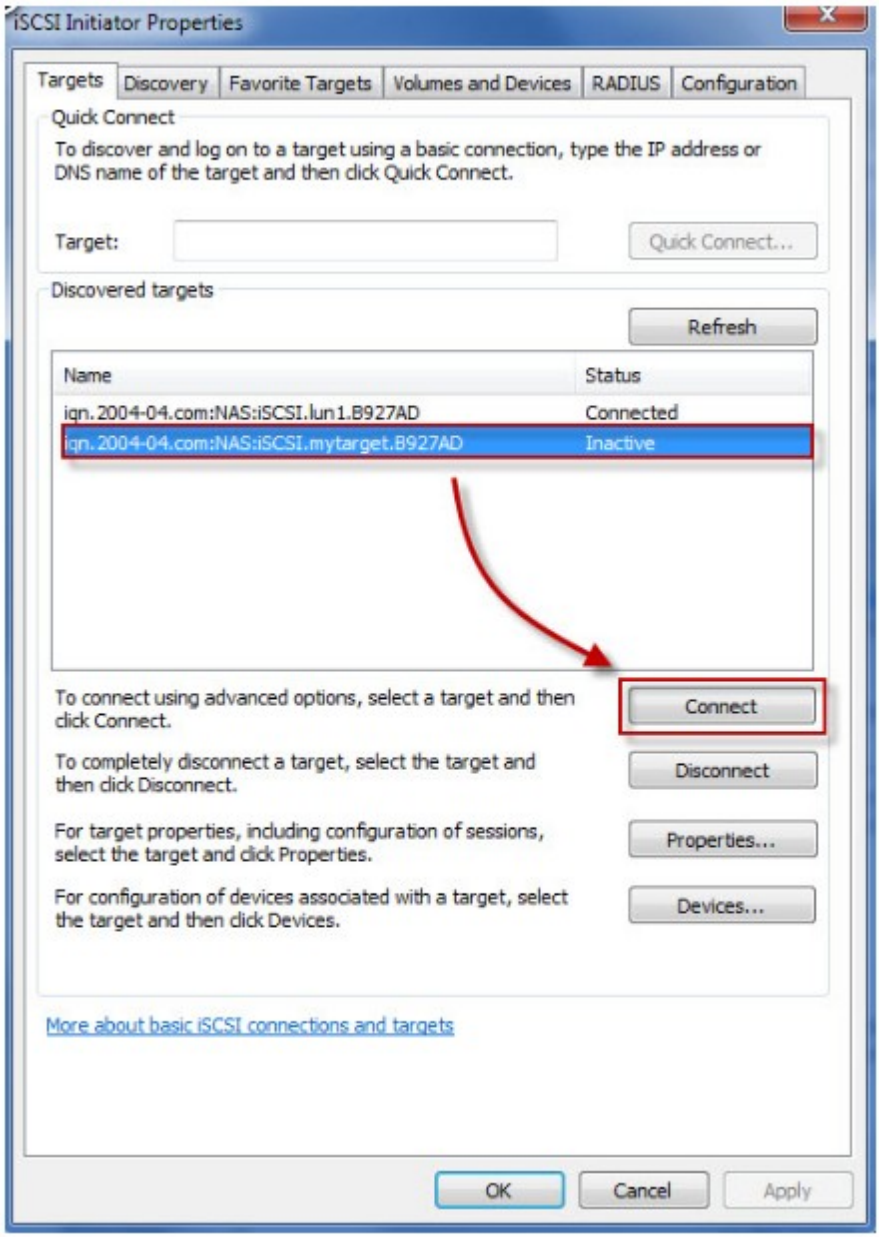
iSCSI initiator on Windows

Microsoft iSCSI Software Initiator v2.07 is an official application for Windows OS 2003, XP, and 2000 to allow users to implement an external iSCSI storage array over the network. If you are using Windows Vista or Windows Server 2008, Microsoft iSCSI Software Initiator is included. For more information and the download location, visit:
http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en

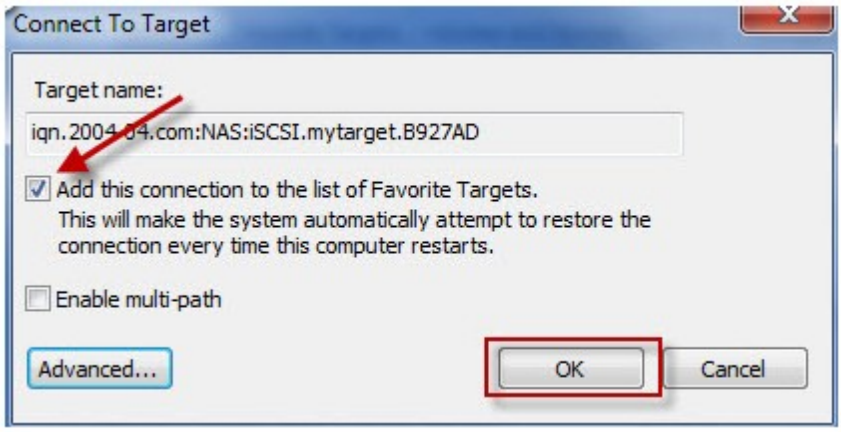
Start iSCSI initiator from "Control Panel" > "Administrative Tools". Under the "Discovery" tab click "Add Portal". Enter the NAS IP and the port number for the iSCSI service.



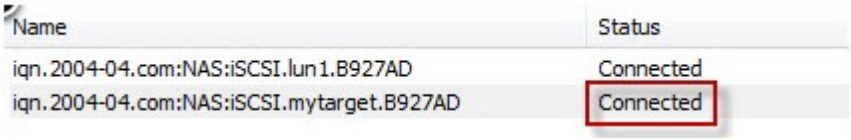
The available iSCSI targets and their status will then be shown under the "Targets" tab. Select the target you wish to connect then click "Connect".



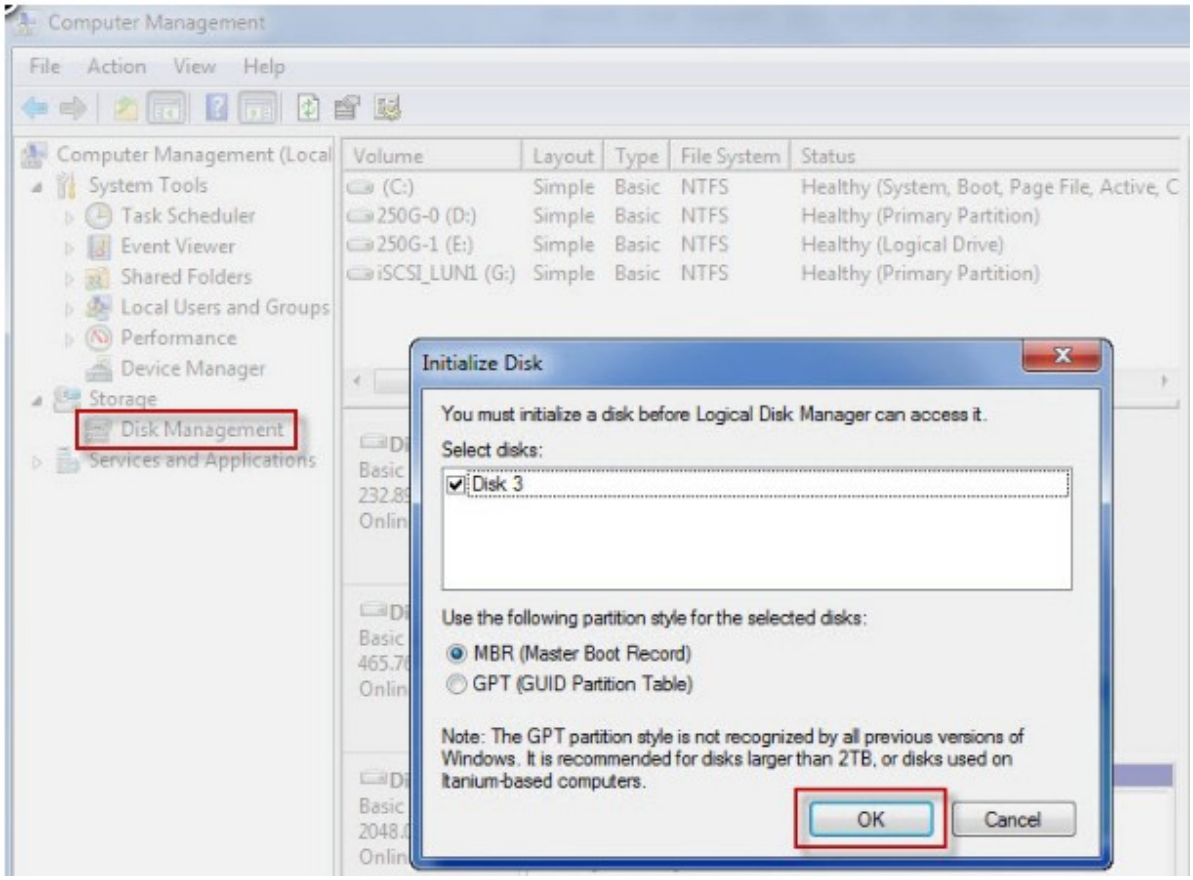
You may click "Advanced" to specify the logon information if you have configured the authentication otherwise simply click "OK" to continue.



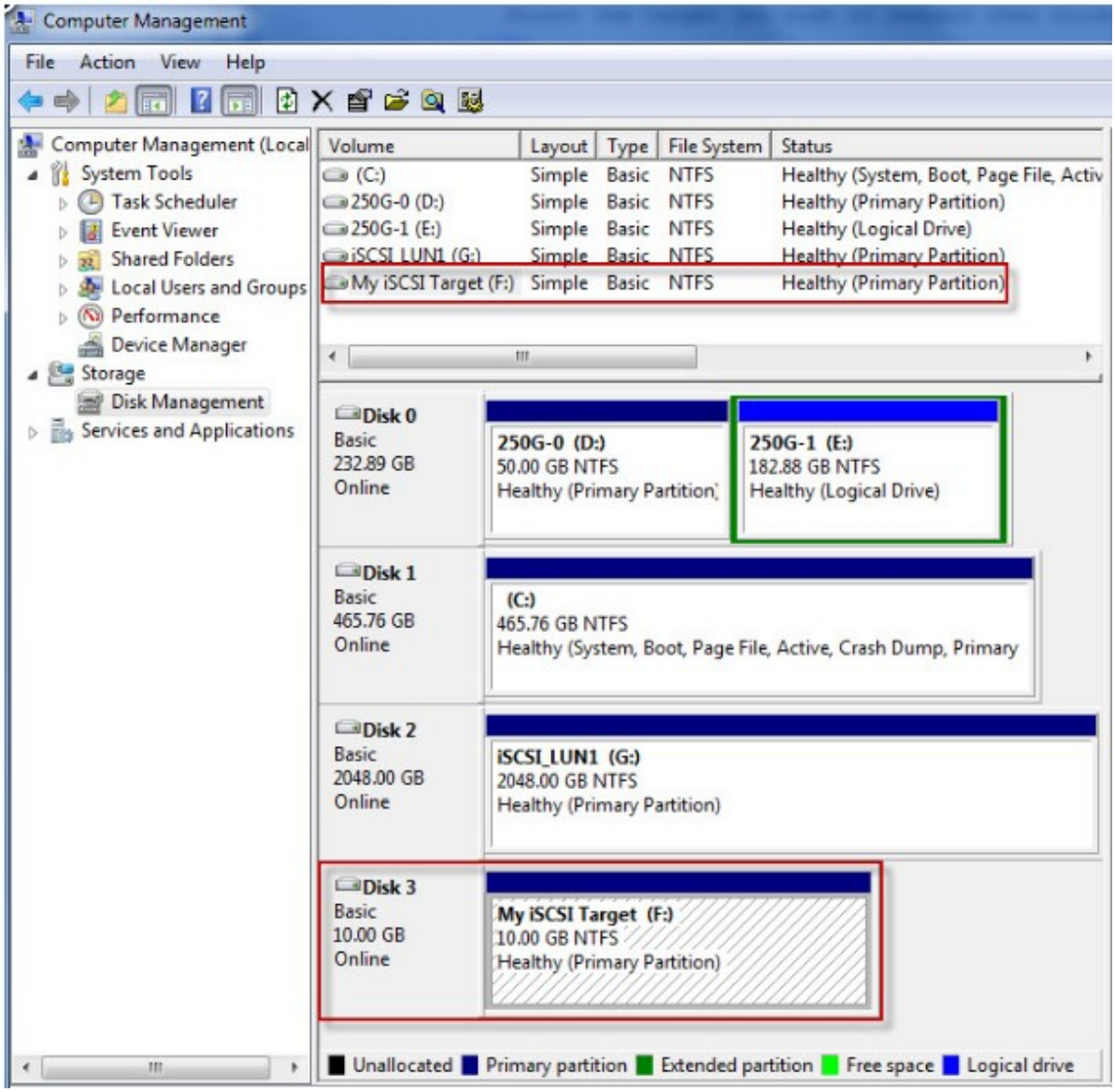
Upon successful logon, the status of the target now shows "Connected".



After the target has been connected Windows will detect its presence and treat it as if a new hard disk drive has been added which needs to be initialized and formatted before we can use it. Right click "My Computer" > "Manage" to open the "Computer Management" window then go to "Disk Management" and a window should pop up automatically asking whether you want to initialize the newly found hard drive. Click "OK" then format this drive as normally you would when adding a new disk.



After disk initialization and formatting, the new drive is attached to your PC. You can now use this iSCSI target as a regular disk partition.



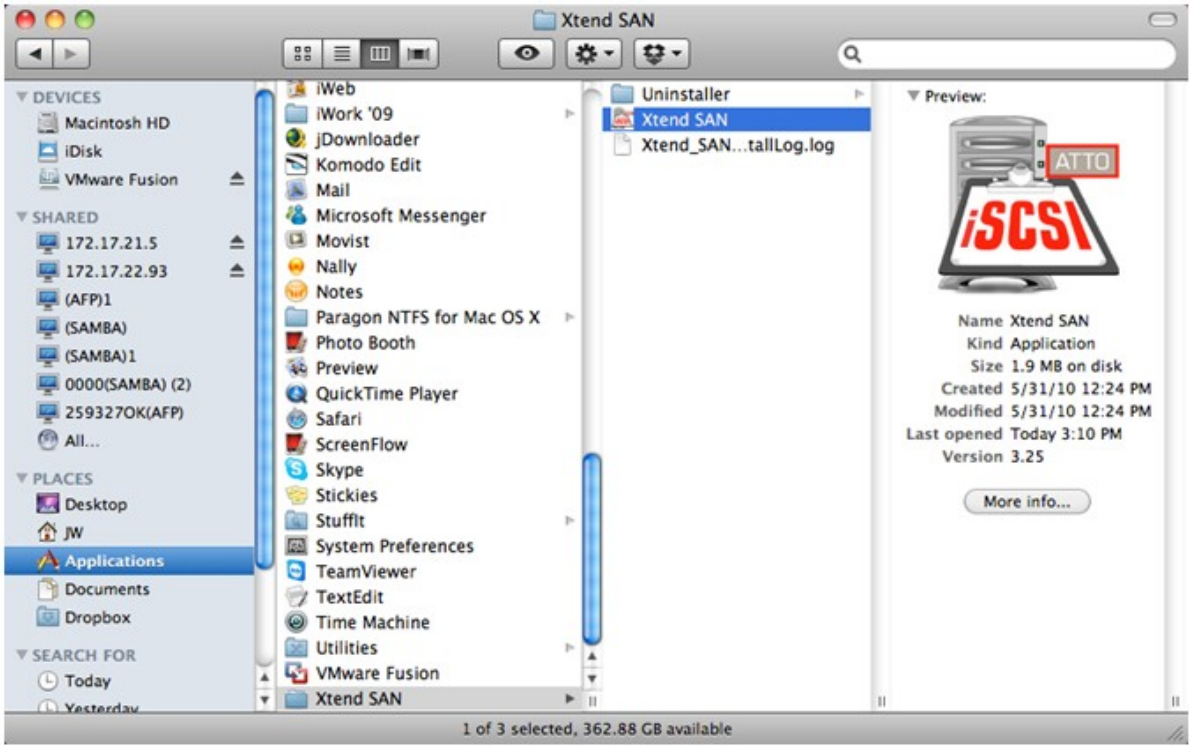
4.5.2.2 Connect to the iSCSI targets by Xtend SAN iSCSI Initiator on Mac OS

This section shows you how to use Xtend SAN iSCSI Initiator on Mac OS to add the iSCSI target (QNAP NAS) as an extra partition. Before you start to use the iSCSI target service, make sure you have created an iSCSI target with a LUN on the NAS and installed the correct iSCSI initiator for your OS.

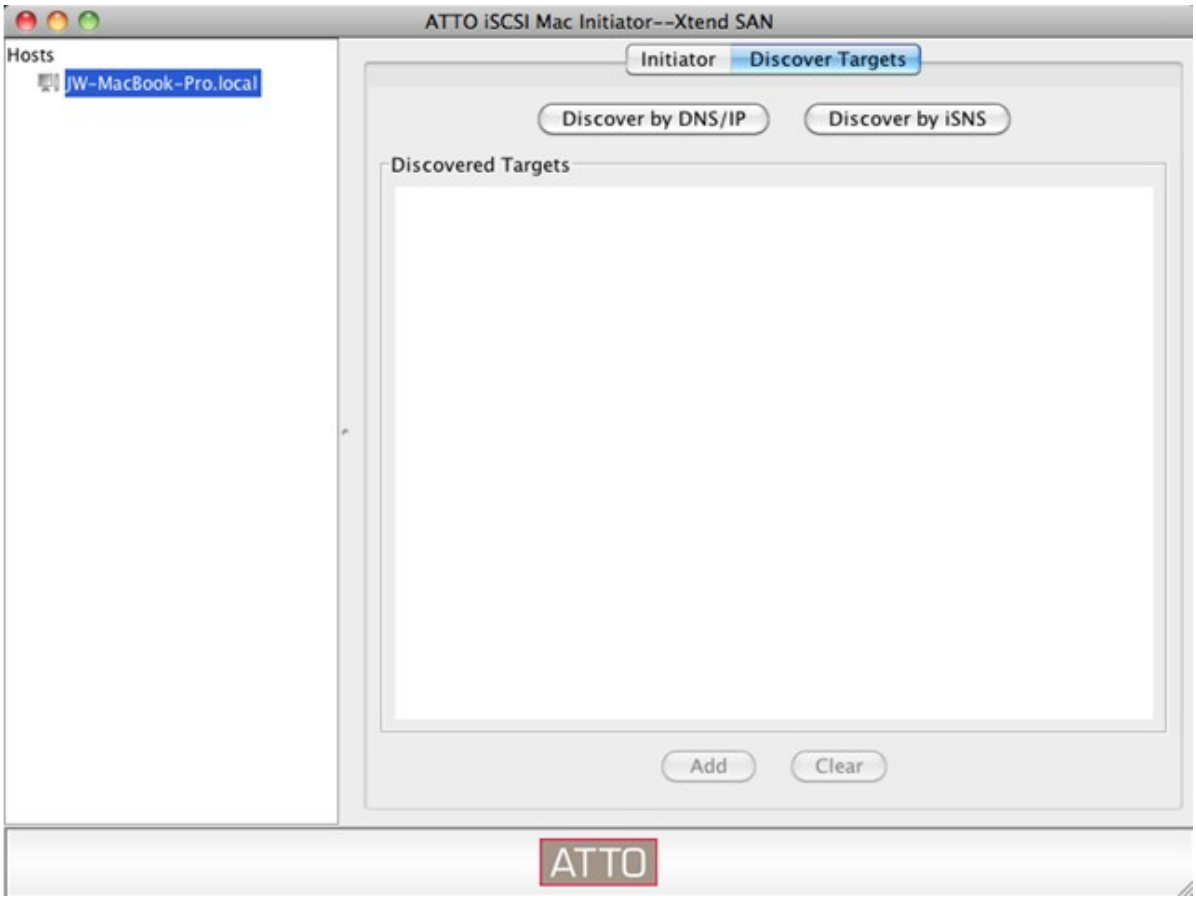
About Xtend SAN iSCSI initiator

ATTO's Xtend SAN iSCSI Initiator for Mac OS X allows Mac users to utilize and benefit from iSCSI. It is compatible with Mac OS X 10.4.x to 10.6.x. For more information, please visit: http://www.attotech.com/products/product.php?sku=INIT-MAC0-001

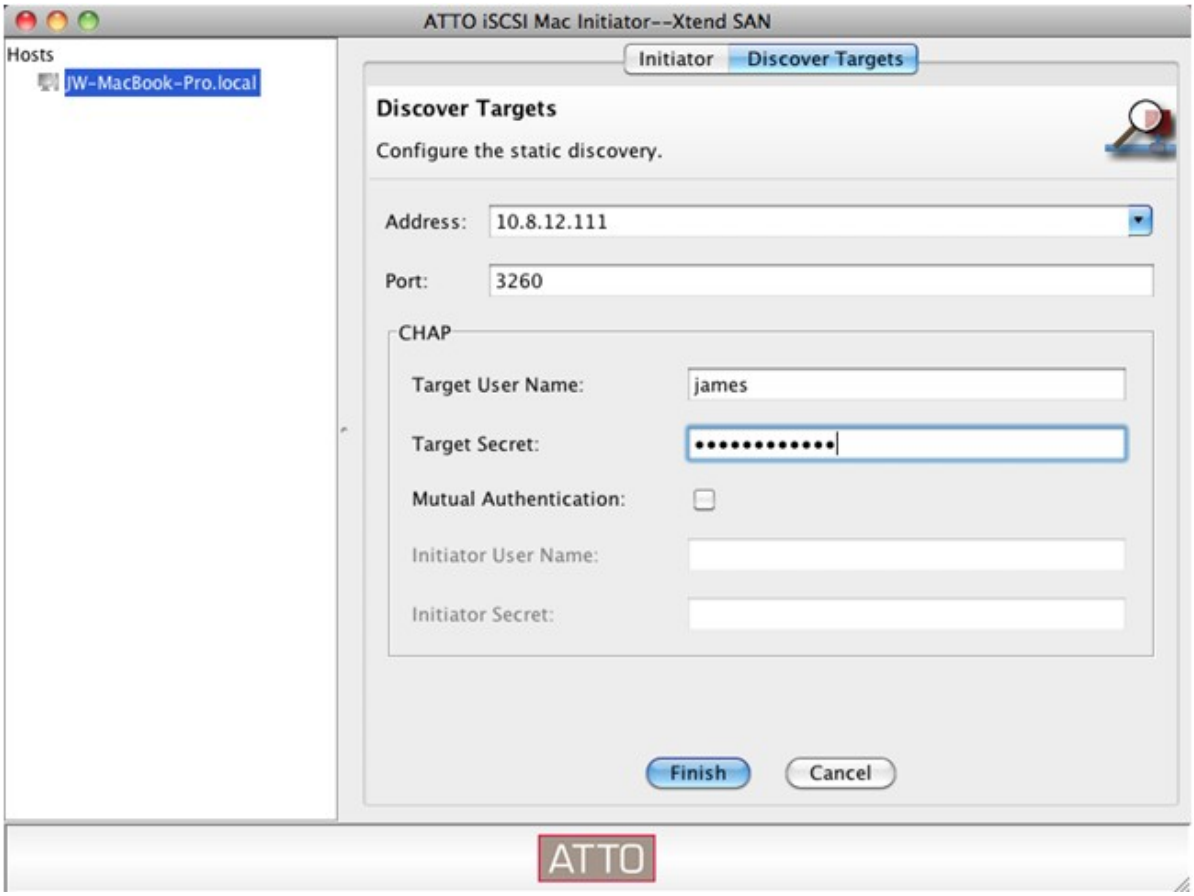
After installing Xtend SAN iSCSI initiator, you can find it in "Applications".



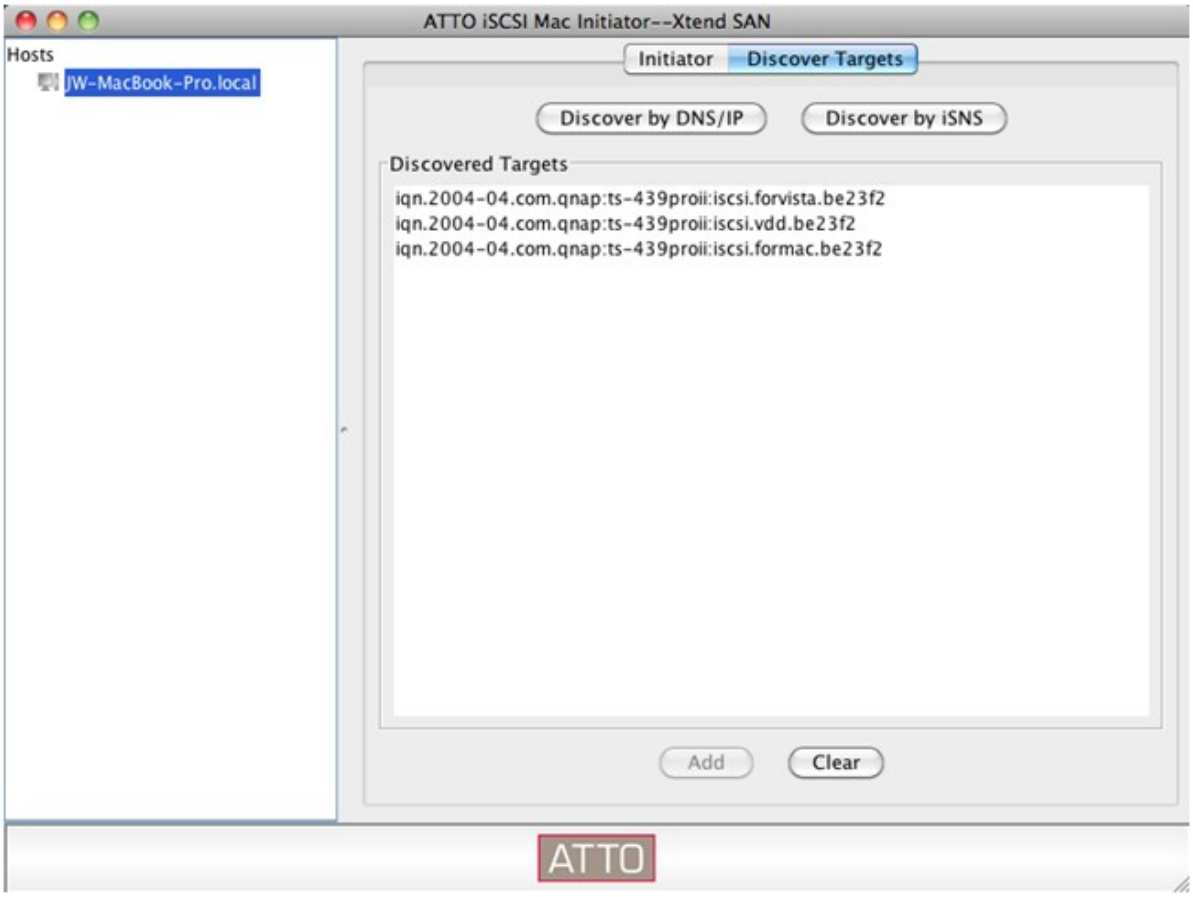
Click the "Discover Targets" tab, you can either choose "Discover by DNS/IP" or "Discover by iSNS" according to the network topology. In this example, we will use the IP address to discover the iSCSI targets.



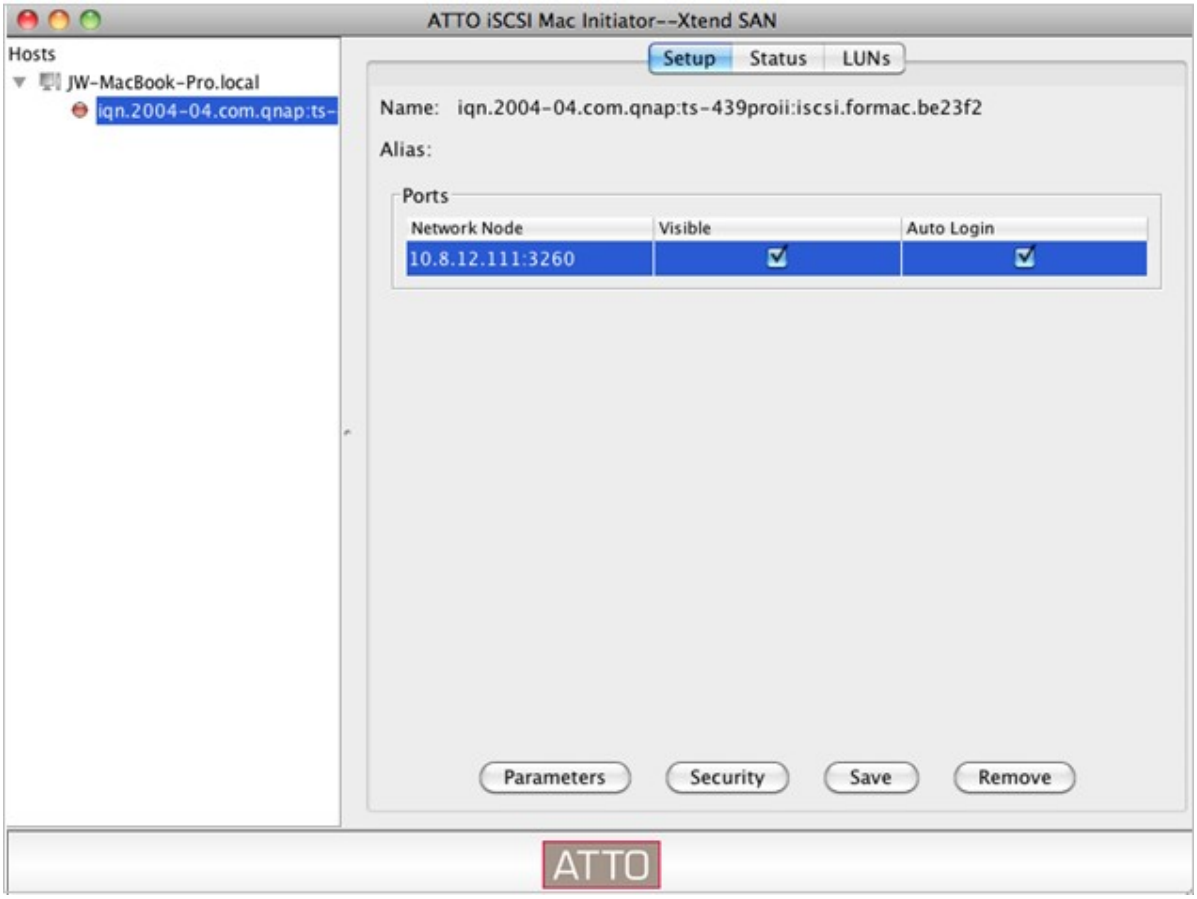
Follow the screen instructions and enter the server address, iSCSI target port number (default: 3260), and CHAP information (if applicable). Click “Finish” to retrieve the target list after all the data have been entered correctly.



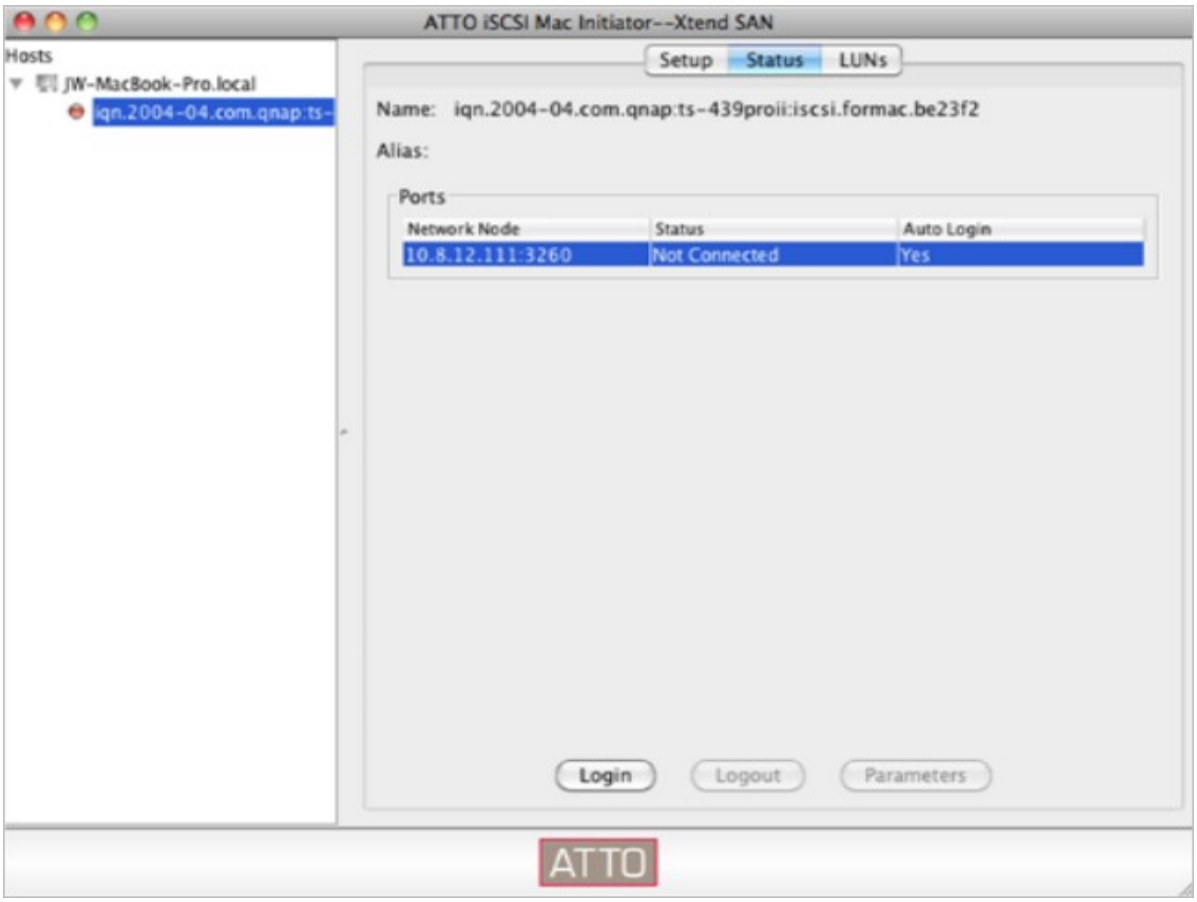
All the available iSCSI targets on the NAS will be shown. Select the target you would like to connect and click "Add".



You can configure the connection properties of the selected iSCSI target in the “Setup” tab.



Click the “Status” tab, select the target to connect. Then click “Login” to proceed.



The first time you logon to the iSCSI target, a popup message will be shown to remind you the disk is not initialized. Click "Initialize…" to format the disk. You can also open the "Disk Utilities" application to do the initialization.

You can now use the iSCSI target as an external drive on your Mac.

4.5.2.3 Connect to the iSCSI targets by Open-iSCSI Initiator on Ubuntu Linux

---

This section shows you how to use Linux Open-iSCSI Initiator on Ubuntu to add the iSCSI target (QNAP NAS) as an extra partition. Before you start to use the iSCSI target service, make sure you have created an iSCSI target with a LUN on the NAS and installed the correct iSCSI initiator for your OS.

About Linux Open-iSCSI Initiator
The Linux Open-iSCSI Initiator is a built-in package in Ubuntu 8.04 LTS (or later). You can connect to an iSCSI volume at a shell prompt with just a few commands. More information about Ubuntu is available at http://www.ubuntu.com and for information and download location of Open-iSCSI, please visit: http://www.open-iscsi.org

Before you start
Install the open-iscsi package. The package is also known as the Linux Open-iSCSI Initiator.

```
# sudo apt-get install open-iscsi
```

Now follow the steps below to connect to an iSCSI target (QNAP NAS) with Linux Open-iSCSI Initiator. You may need to modify the iscsid.conf for CHAP logon information, such as node.session.auth. username & node.session.auth.password.

```
# vi /etc/iscsi/iscsid.conf
```

Save and close the file, then restart the open-iscsi service.

```
# /etc/init.d/open-iscsi restart
```

Discover the iSCSI targets on a specific host (the QNAP NAS in this example), for example, 10.8.12.31 with default port 3260.

```
# iscsiadm -m discovery -t sendtargets -p 10.8.12.31:3260
```

Check the available iSCSI node(s) to connect.

```
# iscsiadm -m node
```

** You can delete the node(s) you do not want to connect to when the service is on with the following command:

```
# iscsiadm -m node --op delete --targetname THE_TARGET_IQN
```

Restart open-iscsi to login all the available nodes.

```
# /etc/init.d/open-iscsi restart
```

You should be able to see the login message as below:
Login session [iface: default, target: iqn.2004-04.com:NAS:iSCSI.ForUbuntu.B9281B, portal: 10.8.12.31,3260] [OK]

Check the device status with dmesg.

```
# dmesg | tail
```

Enter the following command to create a partition, /dev/sdb is the device name.

```
# fdisk /dev/sdb
```

Format the partition.

```
# mkfs.ext3 /dev/sdb1
```

Mount the file system.

```
# mkdir /mnt/iscsi
```

```
# mount /dev/sdb1 /mnt/iscsi/
```

You can test the I/O speed using the following command.

```
# hdparm -tT /dev/sdb1
```

Below are some “iscsiadm” related commands.

Discover the targets on the host:

```
# iscsiadm -m discovery --type sendtargets --portal HOST_IP
```

Login a target:

```
# iscsiadm –m node --targetname THE_TARGET_IQN --login
```

Logout a target:

```
# iscsiadm –m node --targetname THE_TARGET_IQN --logout
```

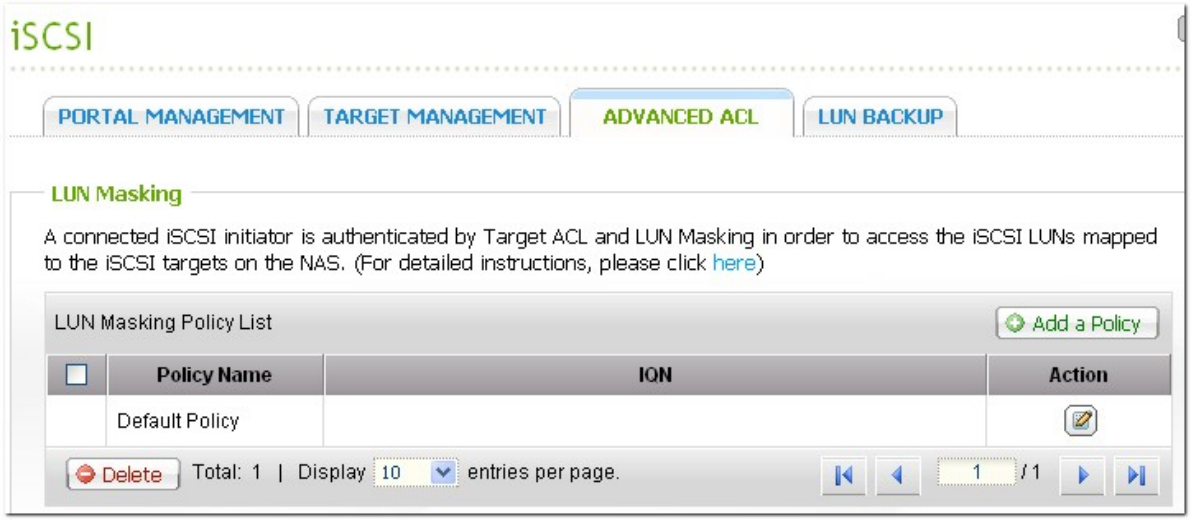
Delete a Target:

```
# iscsiadm –m node --op delete --targetname THE_TARGET_IQN
```

4.5.3 Advanced ACL

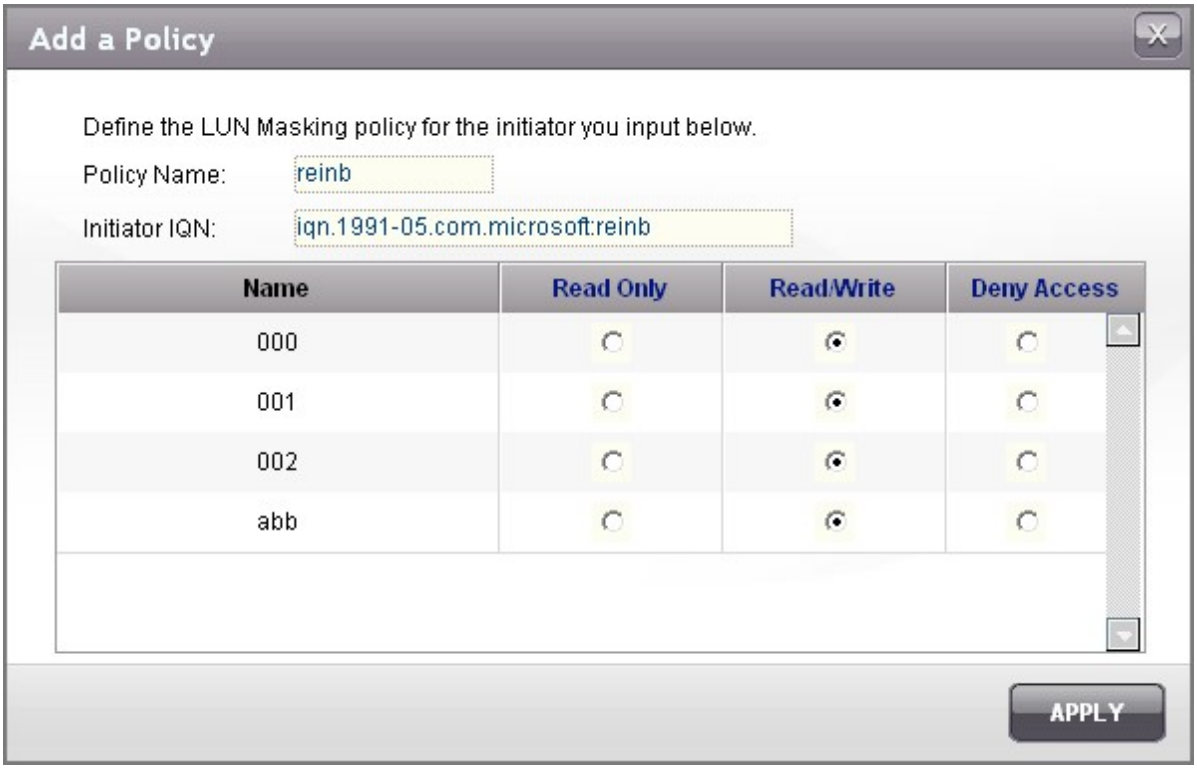
The description below applies to non Intel-based NAS models running firmware version 3.3.0 **or later** and Intel-based NAS models running firmware version 3.2.0 **or later** only.

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" under "ADVANCED ACL".



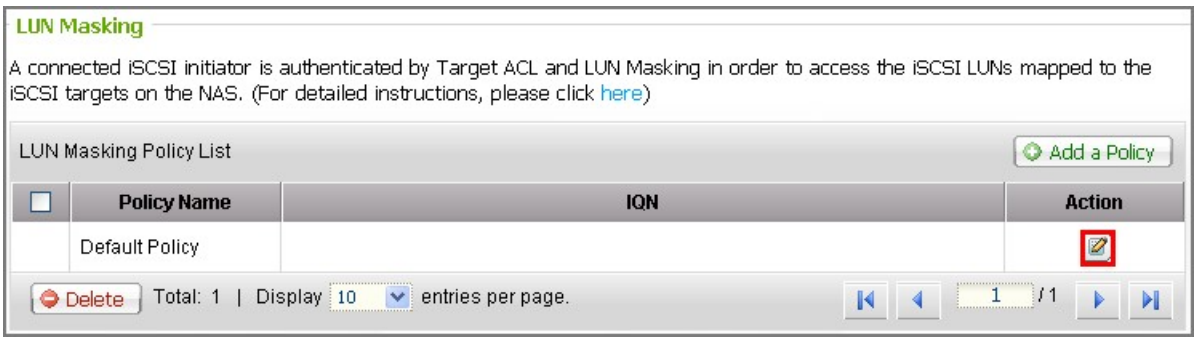
Enter the policy name, the initiator IQN, and assign the access right for each LUN created on the NAS.

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



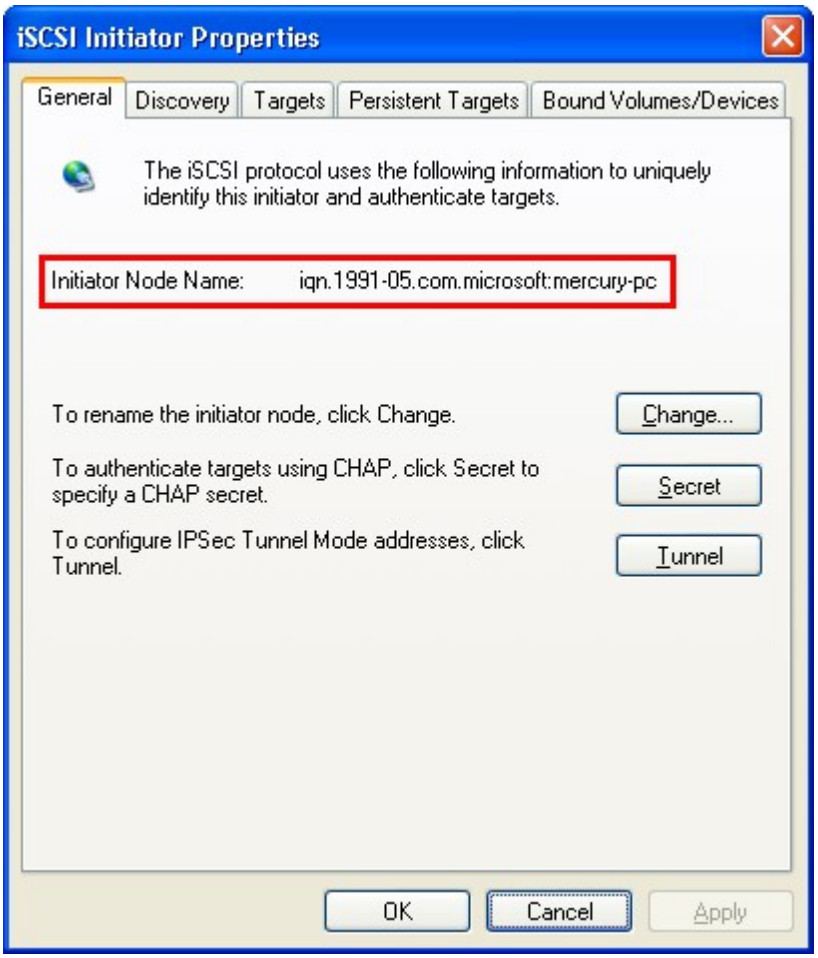
If no LUN masking policy is specified for a connected iSCSI initiator, the default policy will be applied. The system default policy allows read and write access from all the connected iSCSI initiators. You can click (Edit) on the LUN masking list to edit the default policy.

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



Hint: How do I find the initiator IQN?

Start Microsoft iSCSI initiator and click “General”. You can find the IQN of the initiator as shown below.



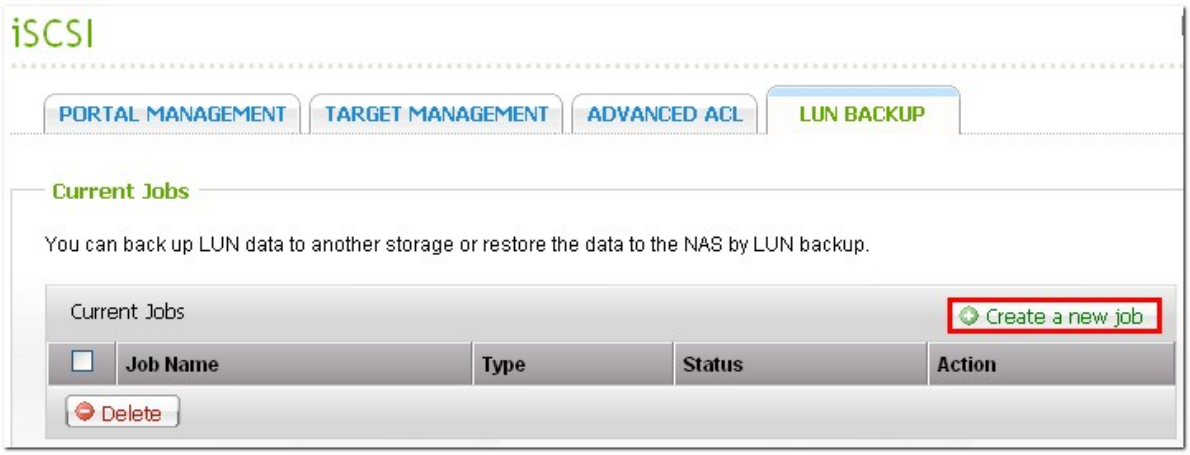
4.5.4 LUN Backup

The NAS supports backing up iSCSI LUNs to different storage locations (Windows, Linux, or local network shares), restoring the LUNs to the NAS, or creating a LUN snapshot and mapping it to an iSCSI target.

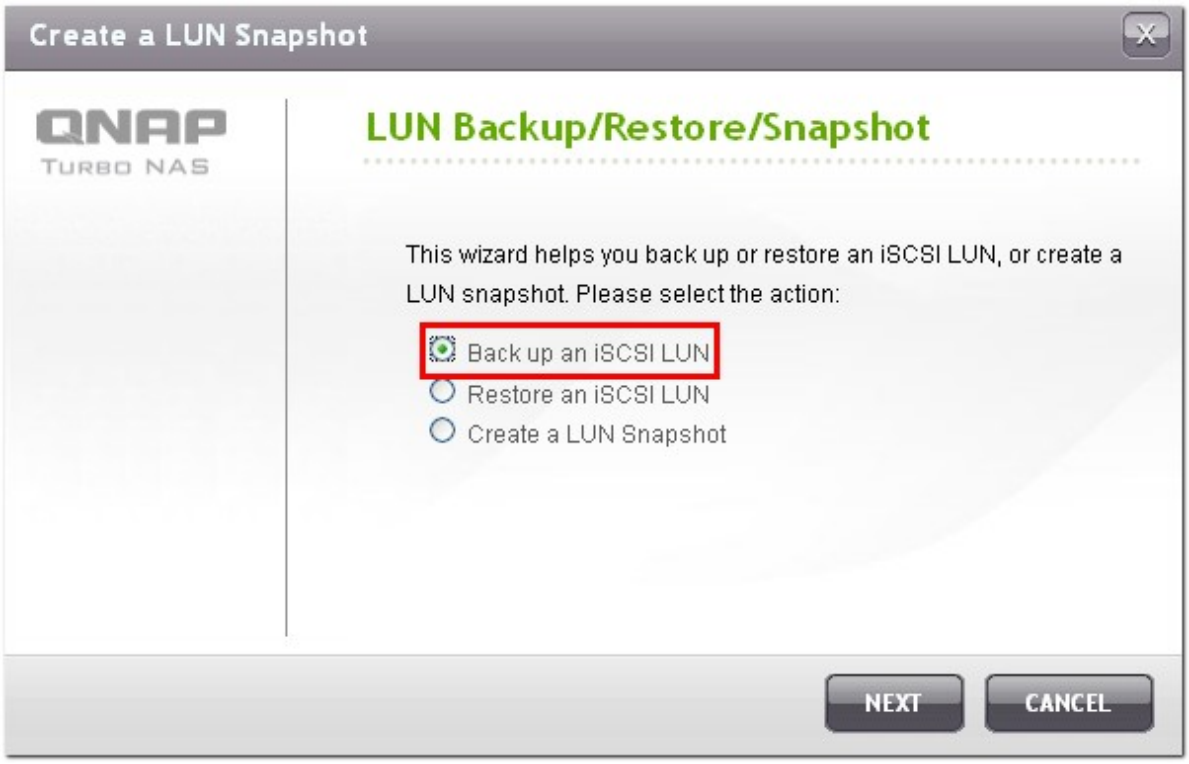
Back up an iSCSI LUN

Before backing up an iSCSI LUN, make sure at least one iSCSI LUN has been created on the NAS. To create iSCSI targets and LUN, go to "Disk Management" > "iSCSI" > "Target Management".

1. Go to "Disk Management" > "iSCSI" > "LUN Backup". Click "Create a new job".



2. Select "Back up an iSCSI LUN" and click "Next".

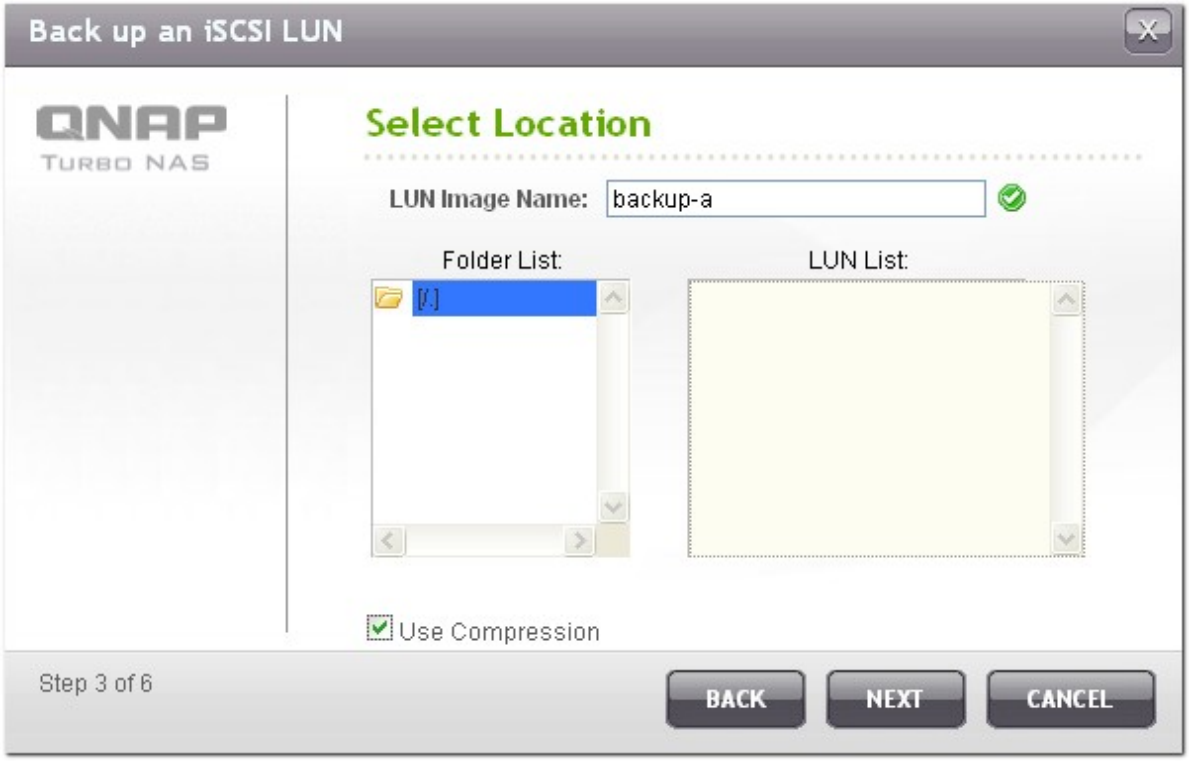


3. Select the source LUN for backup. If an online LUN is selected, the NAS will create a point-in-time snapshot for the LUN automatically.

4. Specify the destination where the LUN will be backed up to. The NAS supports LUN backup to a Linux share (NFS), a Windows share (CIFS/SMB), and a local folder on the NAS. Click "Test" to test the connection to the specified path. Then click "Next".

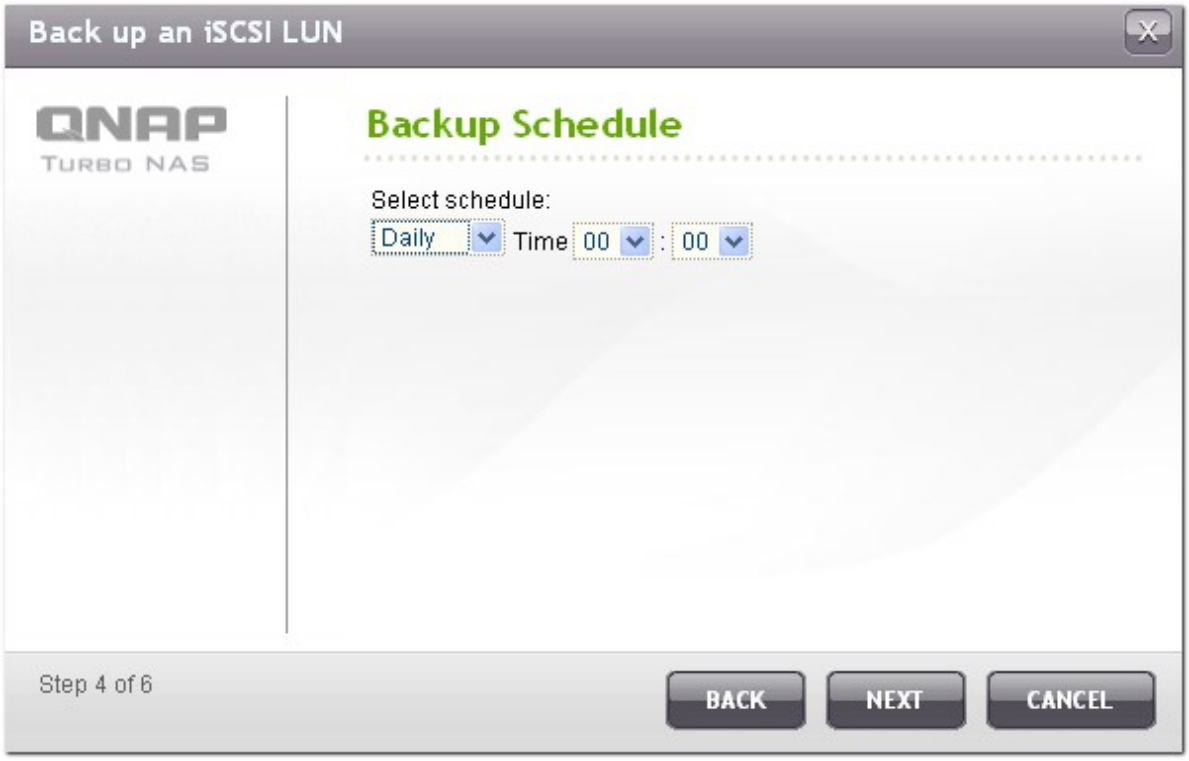
5. Enter a name of the backup LUN image or use the one generated by the NAS. Select the subfolder where the image file will be stored. Select to use compression* or not. Click "Next".

*Use Compression: When this option is enabled, more CPU resources of the NAS will be consumed but the size of the backup LUN can be reduced. The backup time may vary depending on the size of the iSCSI LUN.

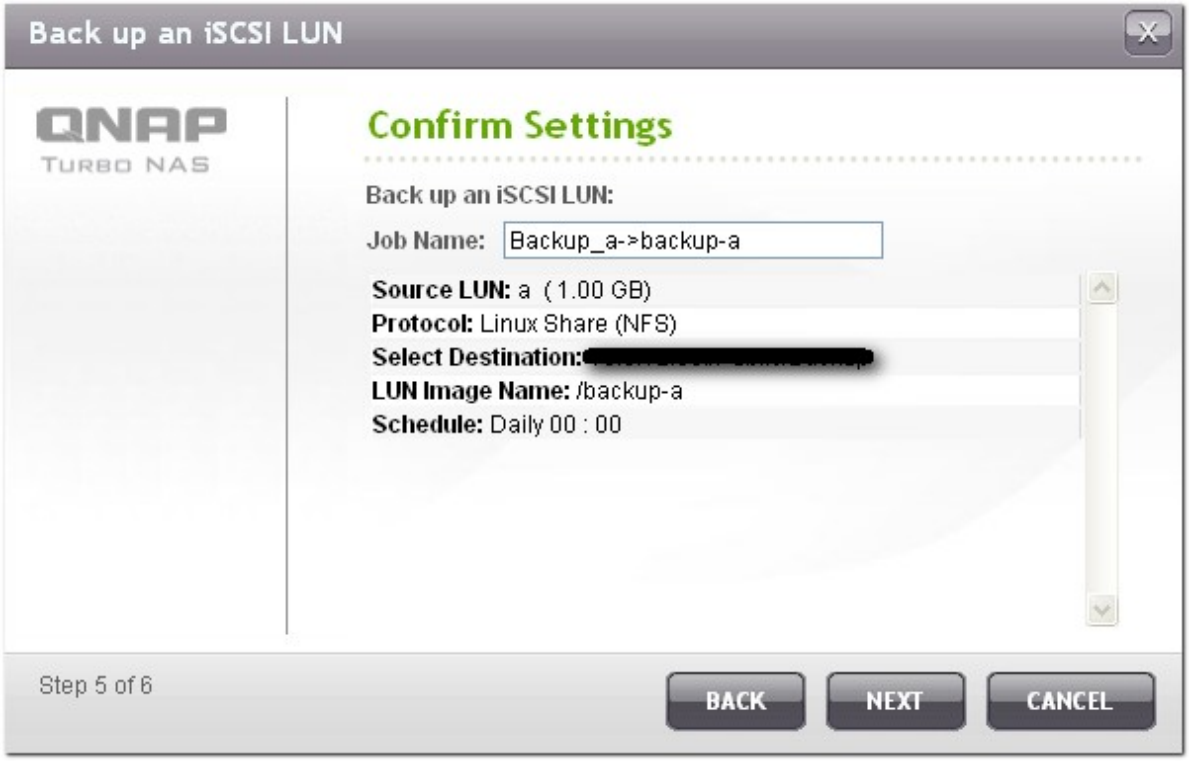


6. Specify the backup schedule. The options available are:
   - Now
   - Hourly
   - Daily
   - Weekly
   - Monthly

Click "Next".



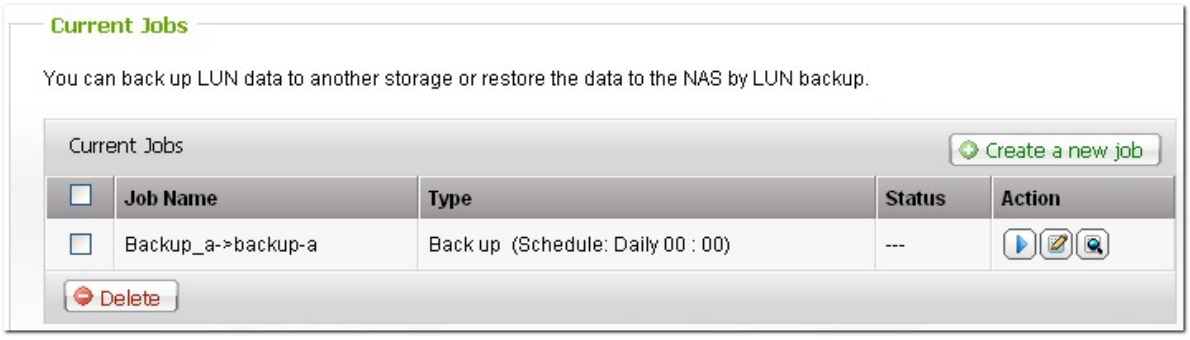
7. The settings will be shown. Enter a name for the job or use the one generated by the NAS. Click "Next".



8. Click "Finish" to exit.

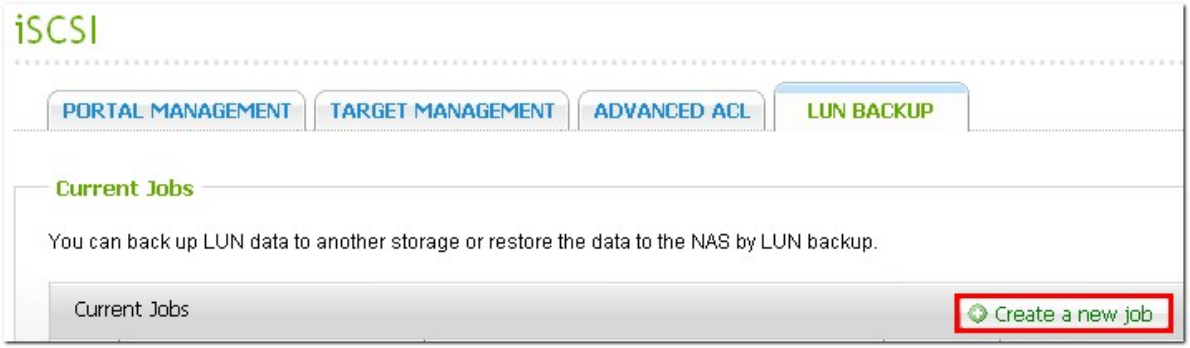
9. The backup job is shown on the list.

Button	Description
	Start the job immediately.
	Stop the running job.
	Edit the job settings.
	View the job status and logs.

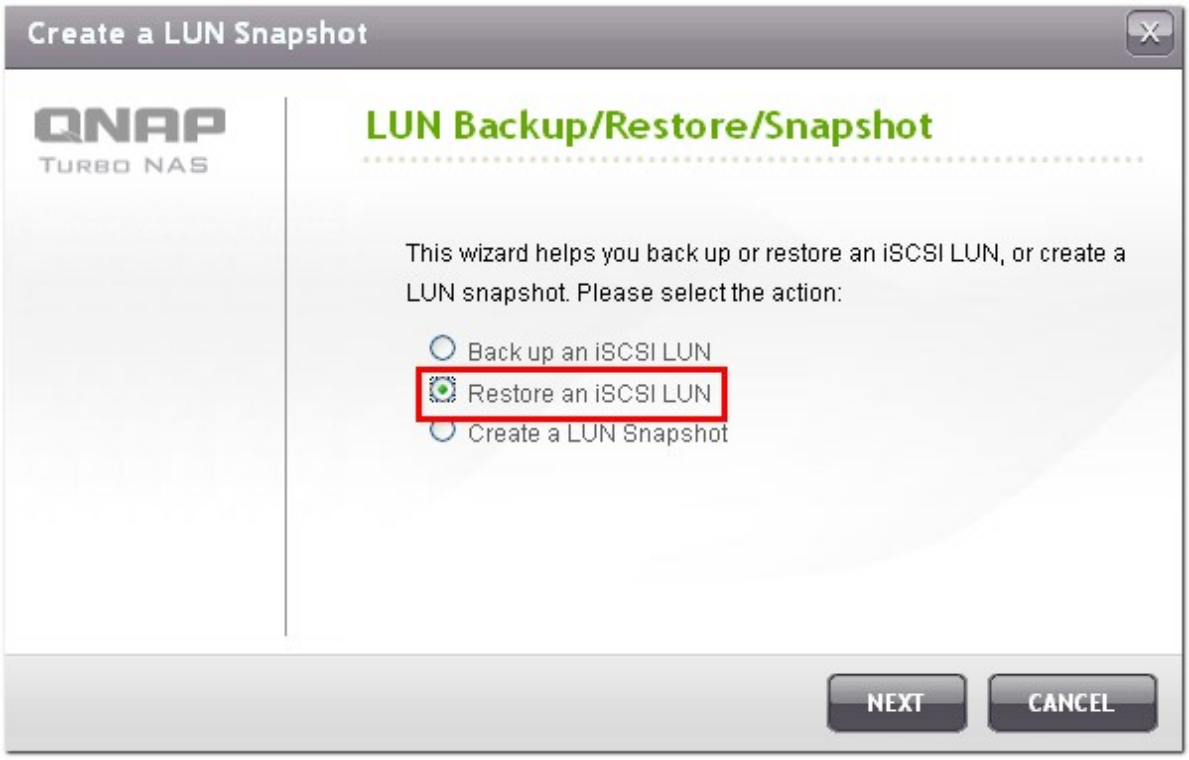


Restore an iSCSI LUN

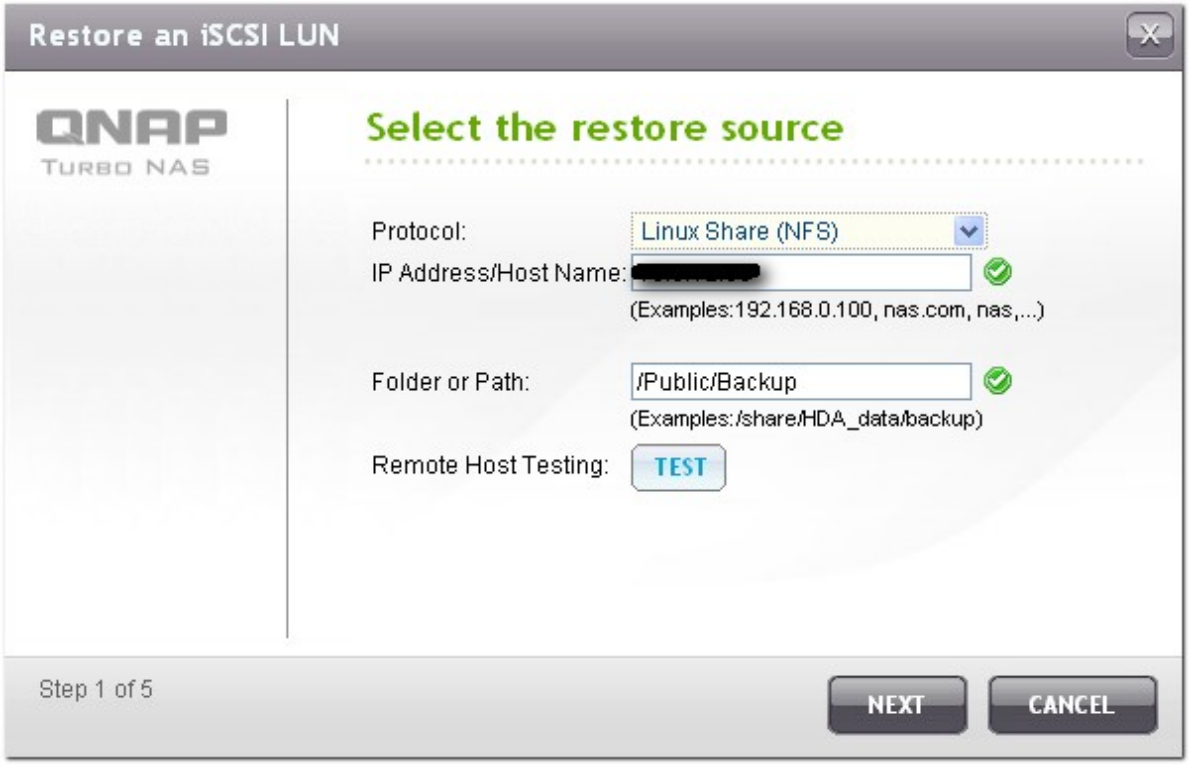
1. To restore an iSCSI LUN to the NAS, go to "Disk Management" > "iSCSI" > "LUN Backup". Click "Create a new job".



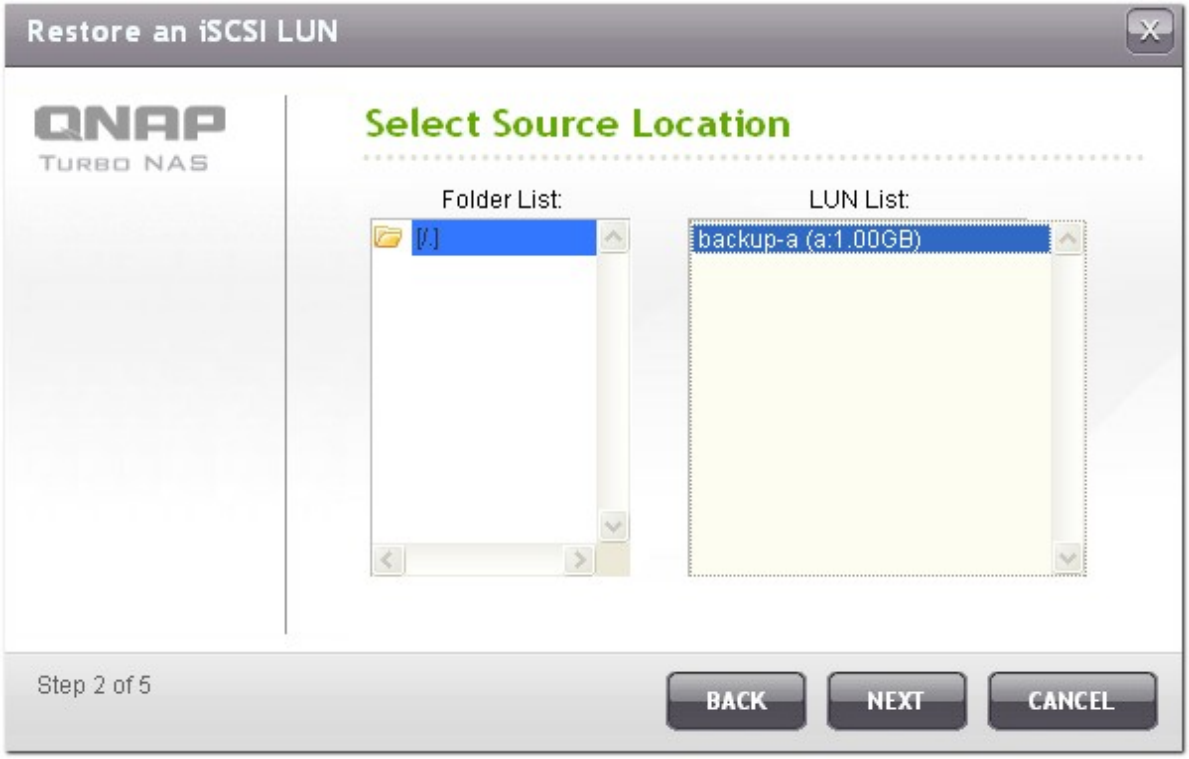
2. Select "Restore an iSCSI LUN" and click "Next".



3. Specify the protocol, IP address/host name, and folder/path of the restore source. Click "Test" to test the connection. Then click "Next".



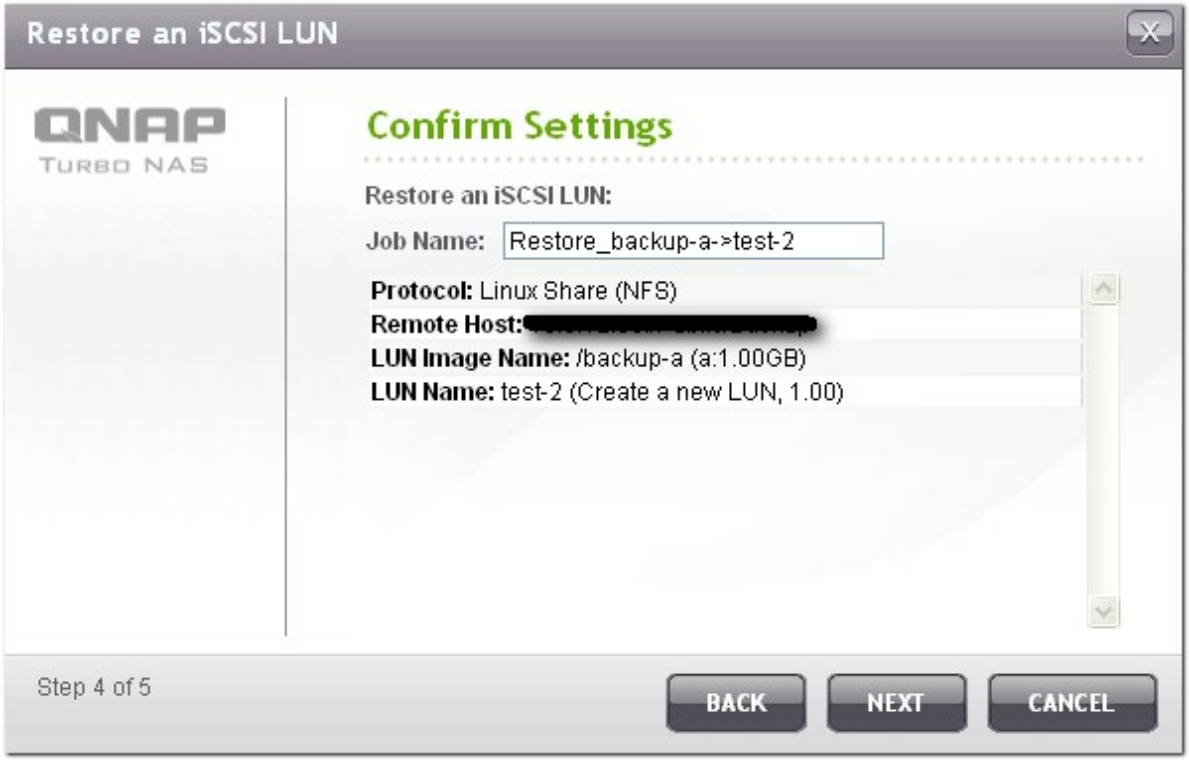
4. Browse and select the LUN image file. Click "Next".



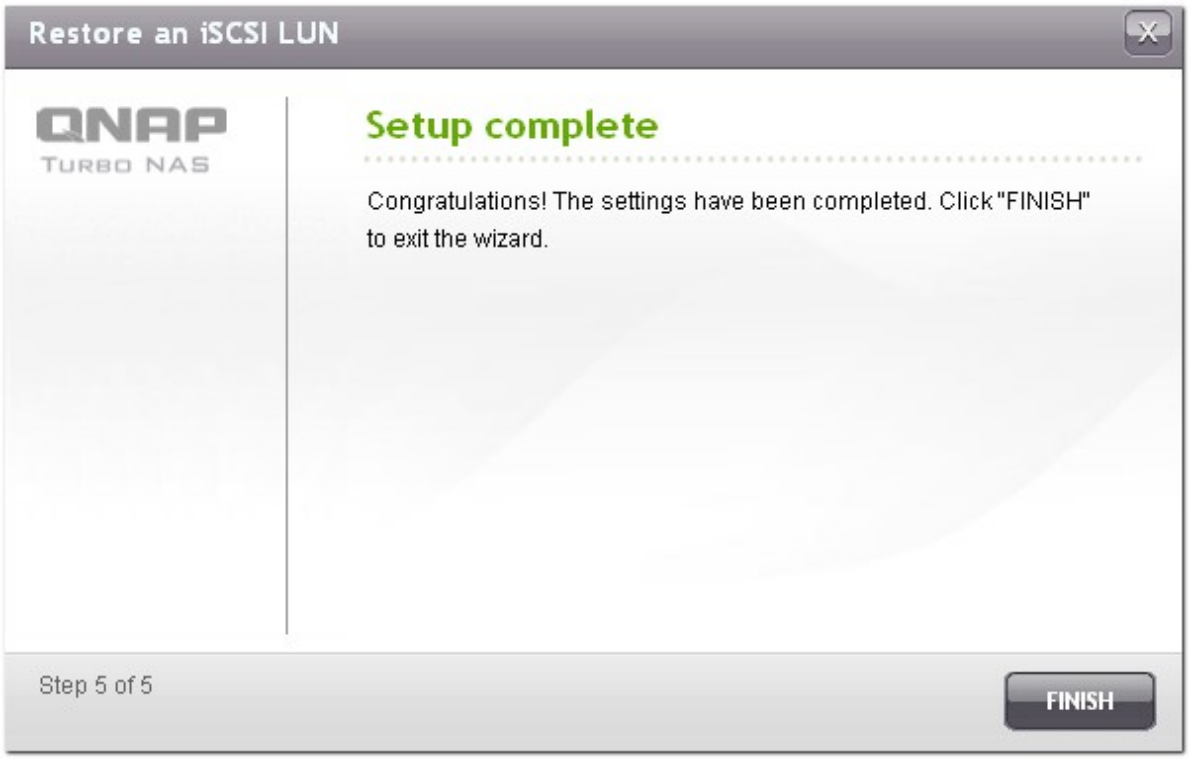
5. Select the destination.
   - Overwrite existing LUN: Restore the iSCSI LUN and overwrite the existing LUN on the NAS. All the data on the original LUN will be overwritten.
   - Create a new LUN: Restore the iSCSI LUN to the NAS as a new LUN. Enter the name and select the location of the new LUN.

Click “Next”.

6. The settings will be shown. Enter a name for the job or use the one generated by the NAS. Click "Next".

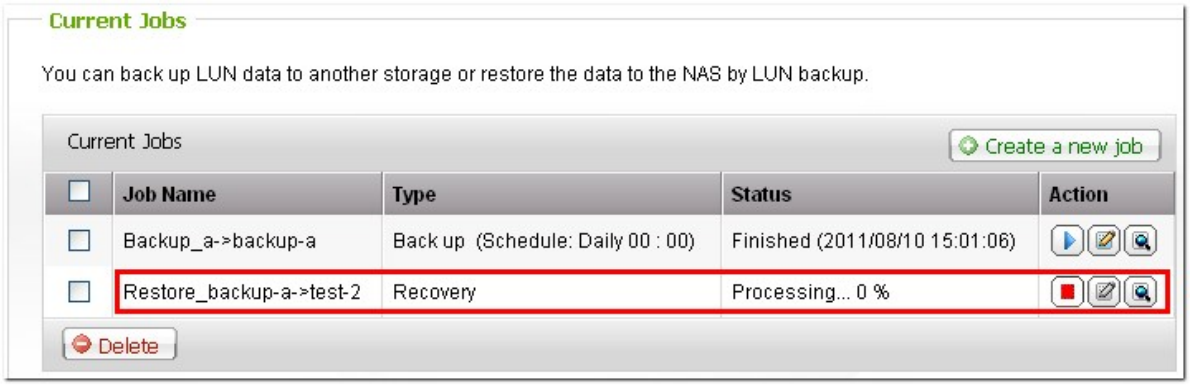


7. Click "Finish" to exit.



8. The restore job will be executed immediately.

Button	Description
	Stop the running job.
	Edit the job settings.
	View the job status and logs.



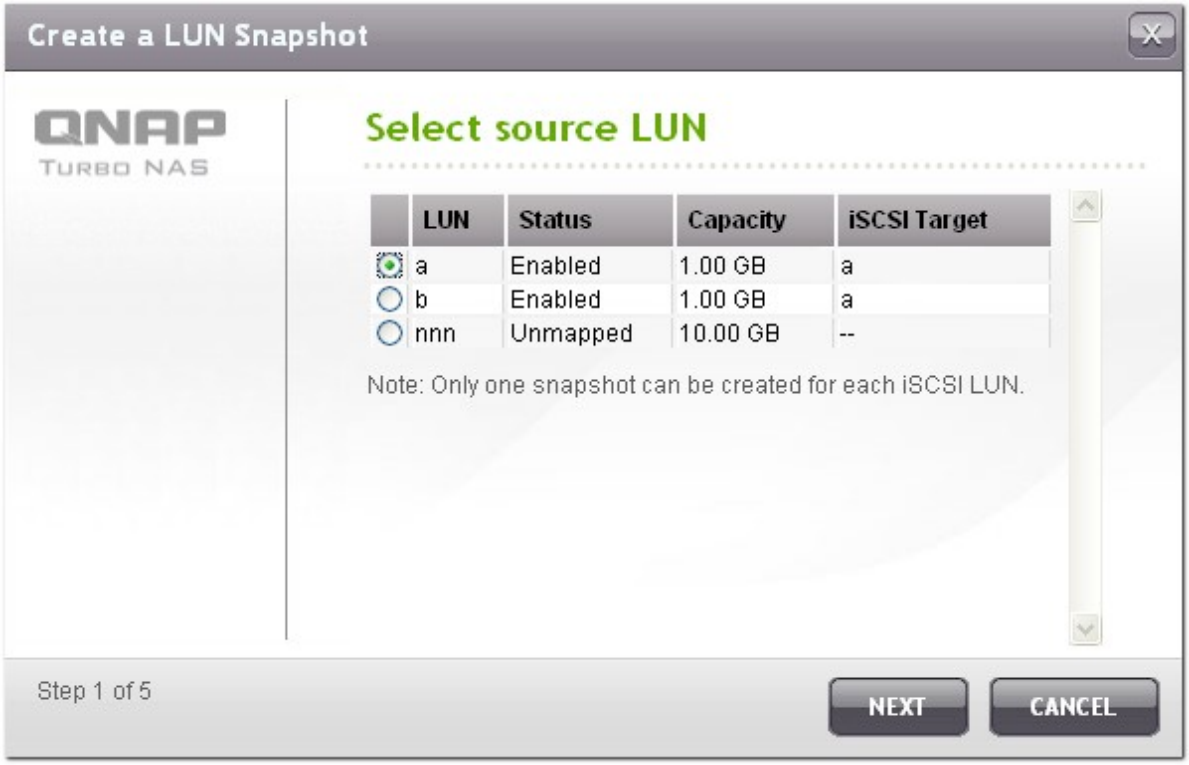
Create an iSCSI LUN Snapshot

Before creating an iSCSI LUN snapshot, make sure at least one iSCSI LUN and one iSCSI target has been created on the NAS. To create iSCSI targets and LUN, go to "Disk Management" > "iSCSI" > "Target Management".

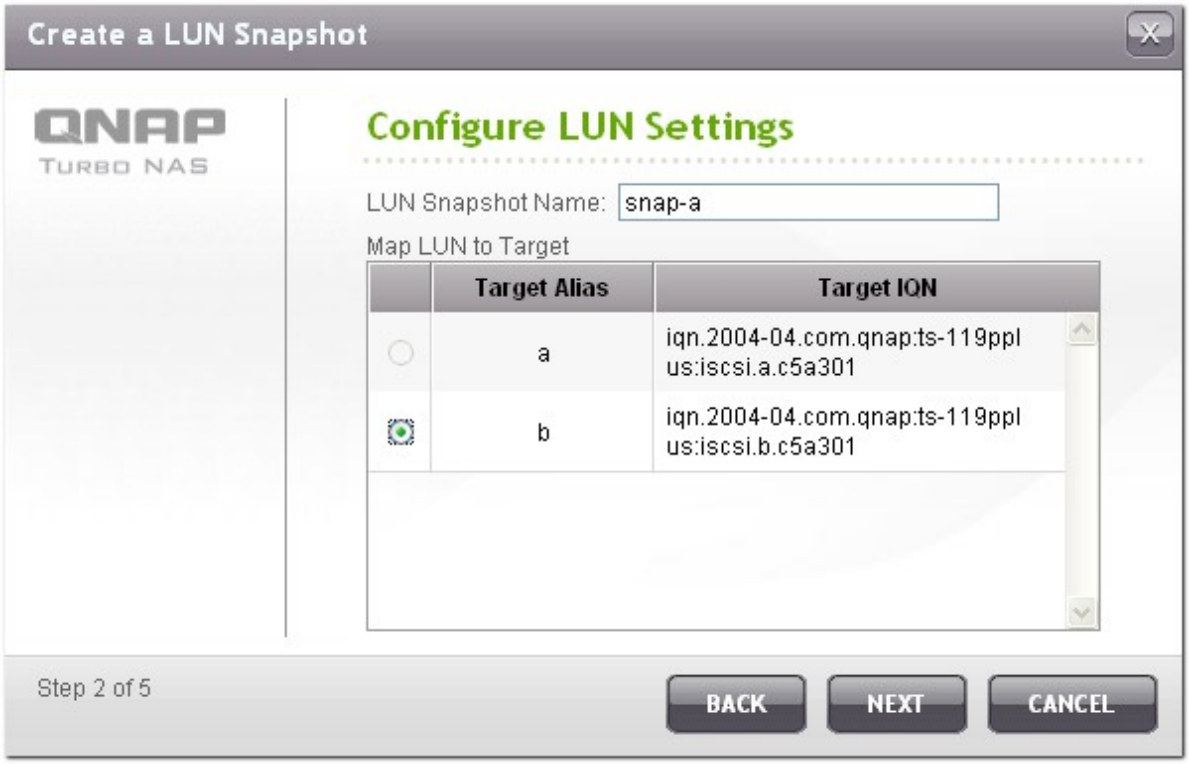
1. To create an iSCSI LUN snapshot, go to "Disk Management" > "iSCSI" > "LUN Backup". Click "Create a new job".

2. Select "Create a LUN Snapshot" and click "Next".

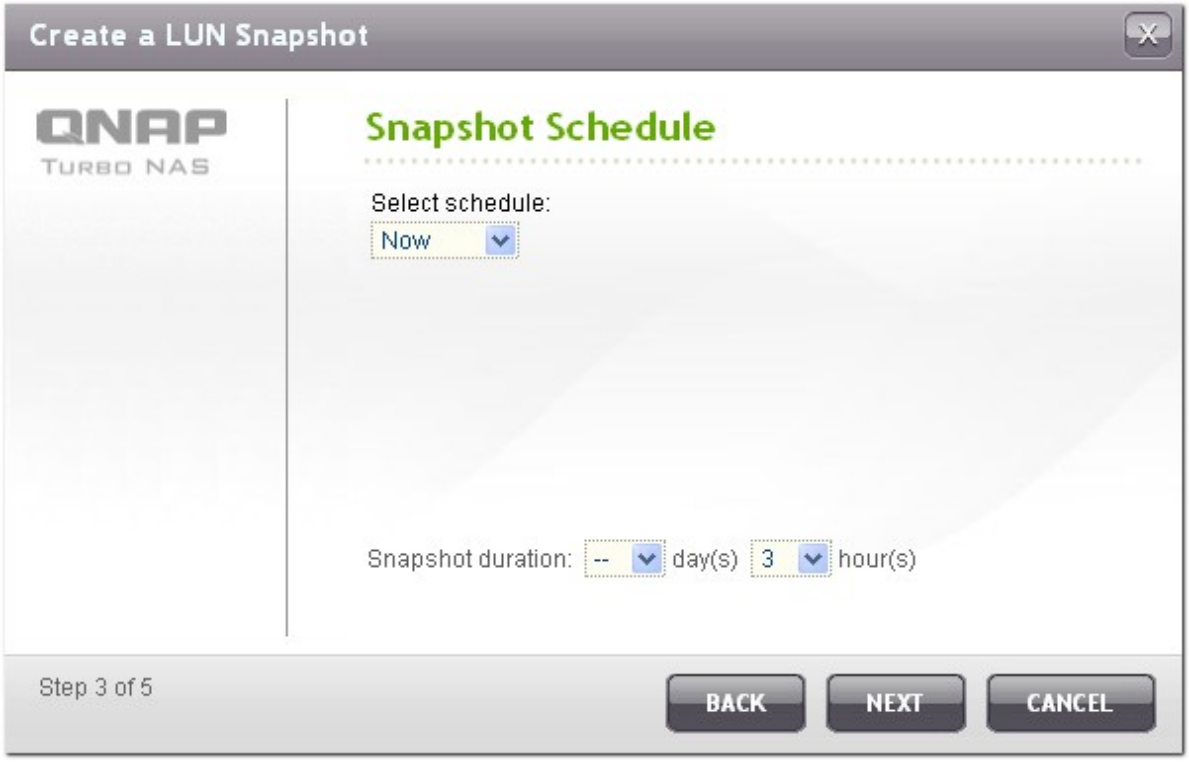
3. Select an iSCSI LUN on the NAS. Only one snapshot can be created for each iSCSI LUN. Click "Next".



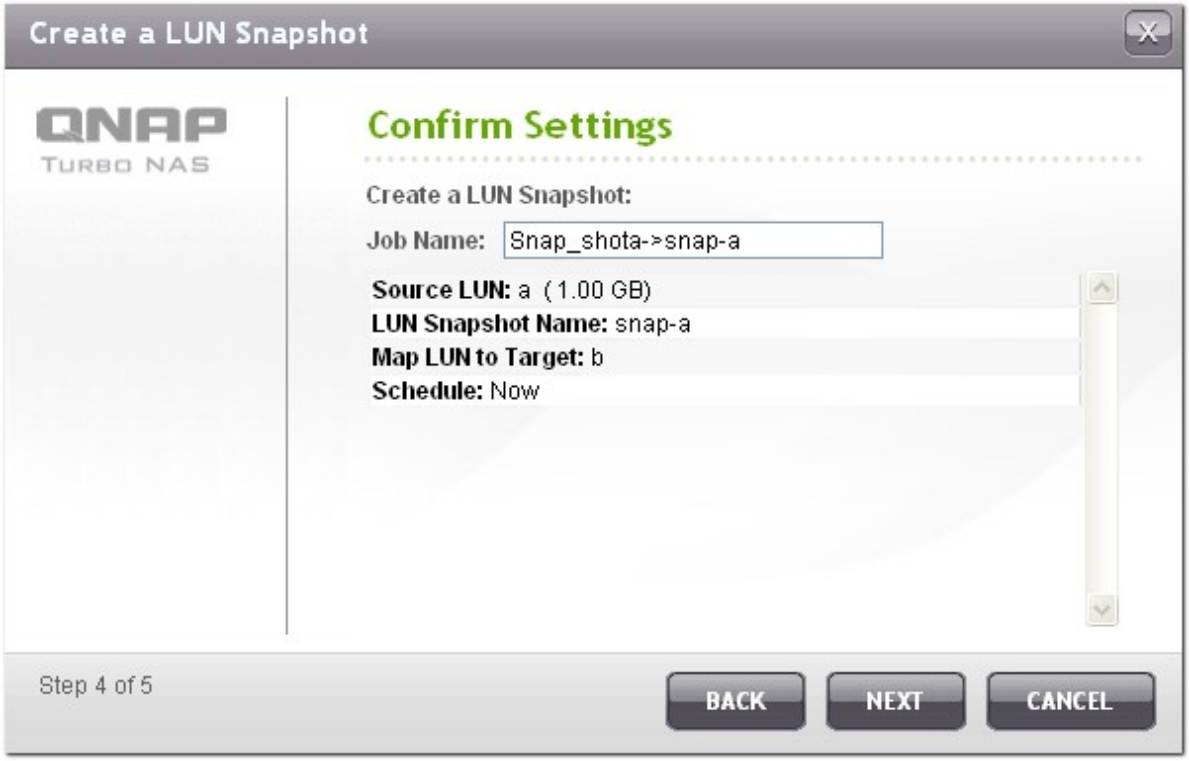
4. Enter a name for the LUN snapshot or use the one generated by the NAS. Select an iSCSI target where the LUN snapshot is mapped to. Click "Next". The LUN snapshot must be mapped to another iSCSI target different from the original one.



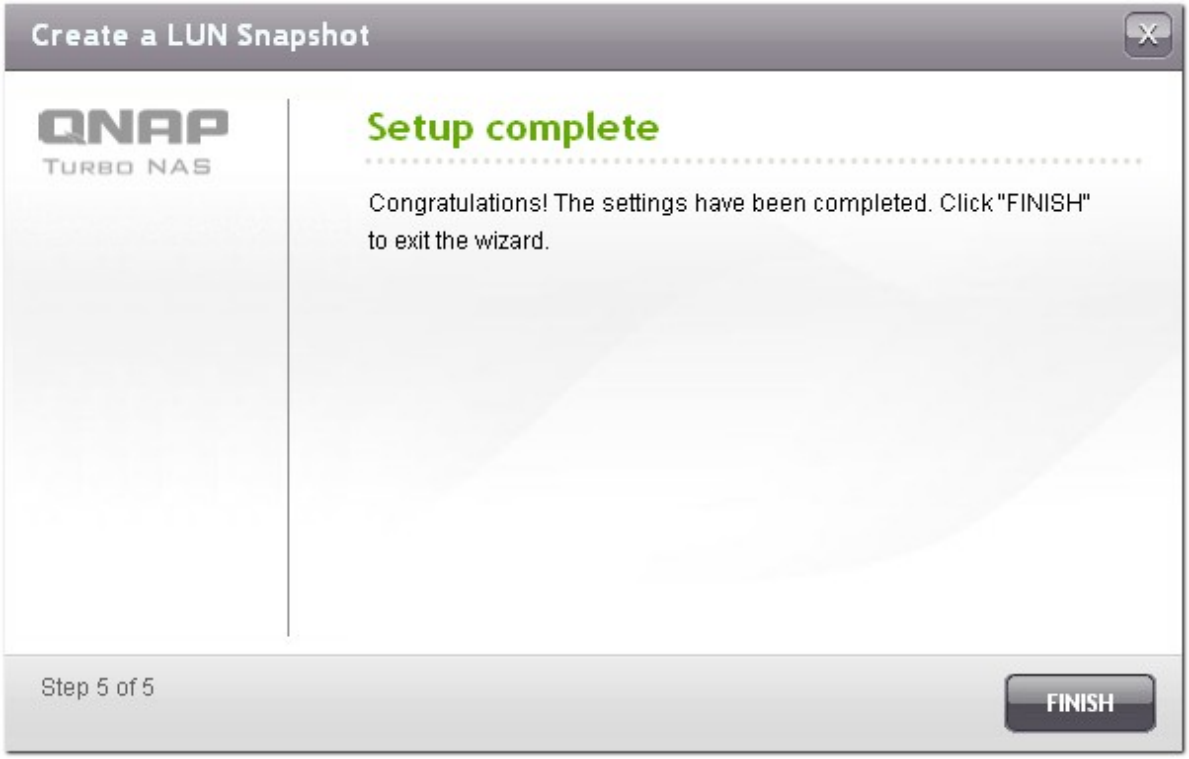
5. Specify the snapshot schedule and the snapshot duration. The snapshot will be removed automatically when the snapshot duration is reached.



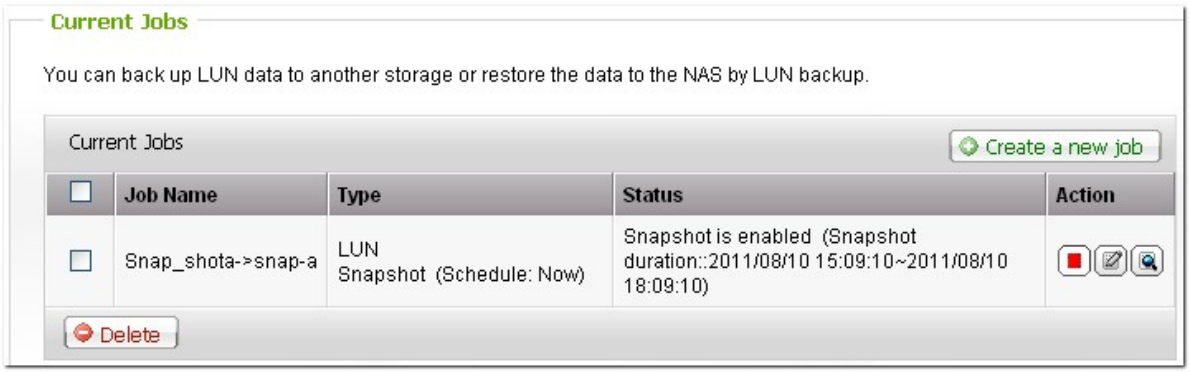
6. The settings will be shown. Enter a name for the job or use the one generated by the NAS. Click "Next".



7. Click “Finish” to exit.

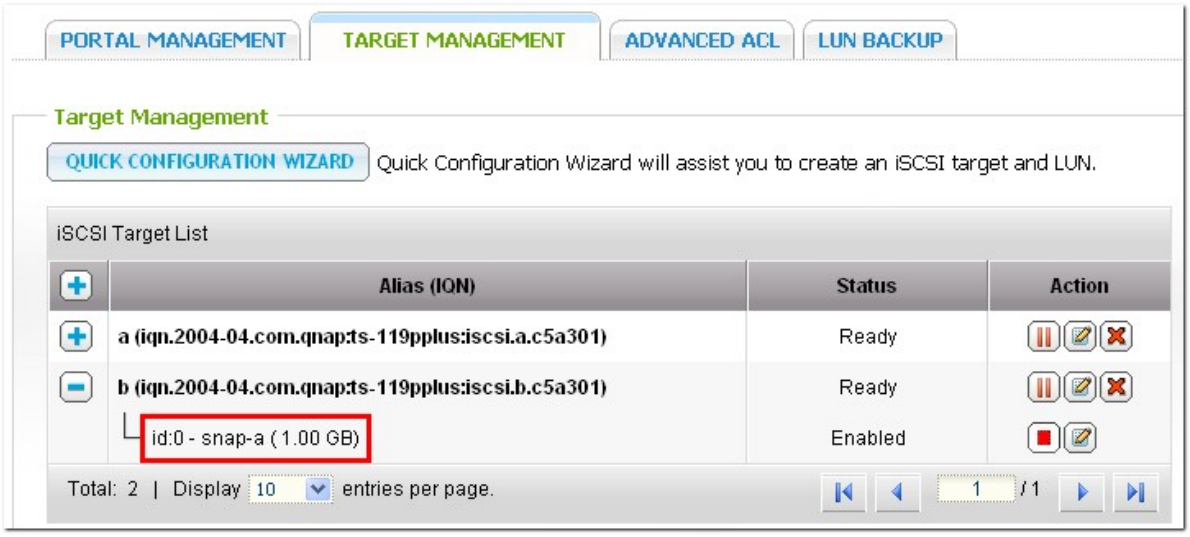


8. The snapshot will be created immediately. The status and duration will be shown on the list.



9. Go to "iSCSI" > "Target Management", the snapshot LUN will be shown in the iSCSI Target List. Use iSCSI initiator software to connect to the iSCSI target and access the point-in-time data on the snapshot LUN. For the information of connecting to the iSCSI targets on QNAP NAS, please refer to http://www.qnap.com/pro_application.asp?ap_id=135.

Note: The source LUN and snapshot LUN cannot be mounted on the same NAS on certain operating systems such as Windows 7 and Windows 2008 R2. Please mount the LUN to different NAS servers in such case.



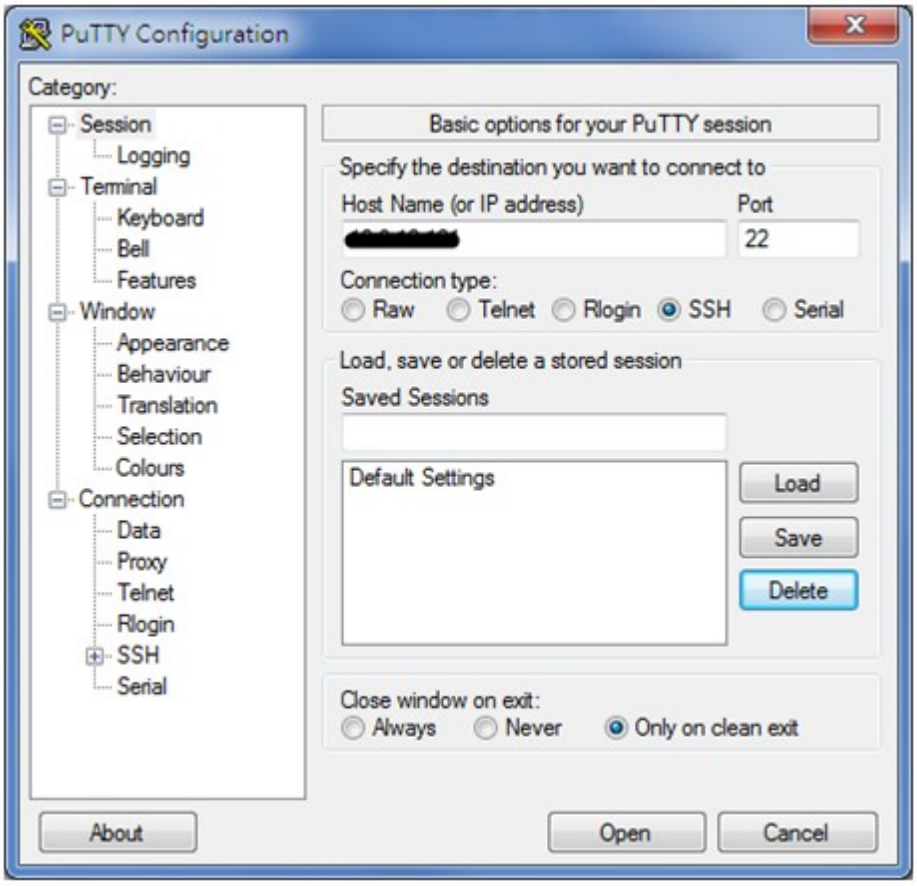
Manage LUN Backup/Restore/Snapshot by Command Line

QNAP NAS users can execute or stop the iSCSI LUN backup, restore, or snapshot jobs on the NAS by command line. Follow the instructions below to use this feature.

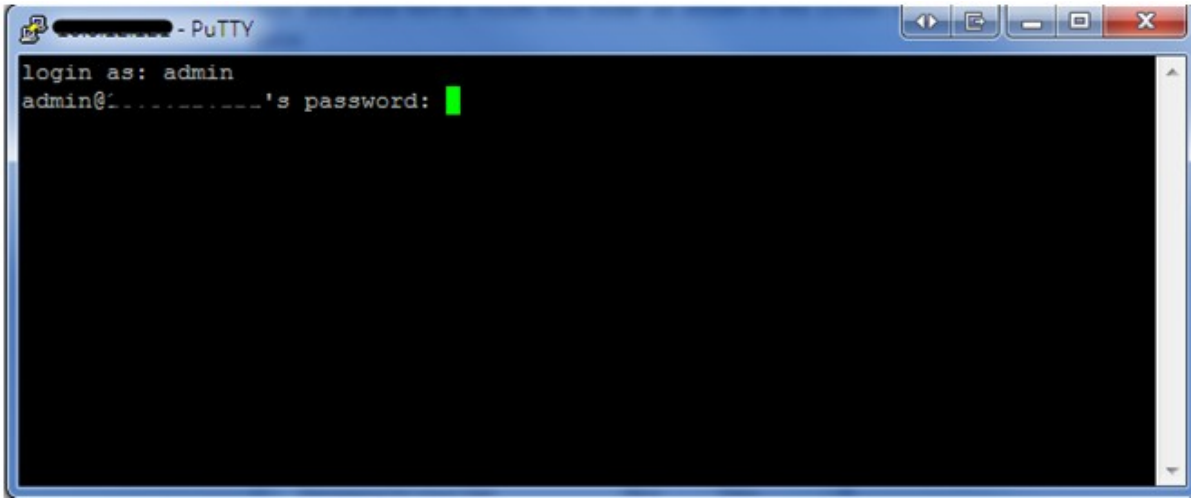
> **Note:** The following instructions should only be operated by IT administrators who are familiar with command line.

1. First make sure the iSCSI LUN backup, restore, or snapshot jobs have been created on the NAS in "Disk Management" > "iSCSI" > "LUN Backup".

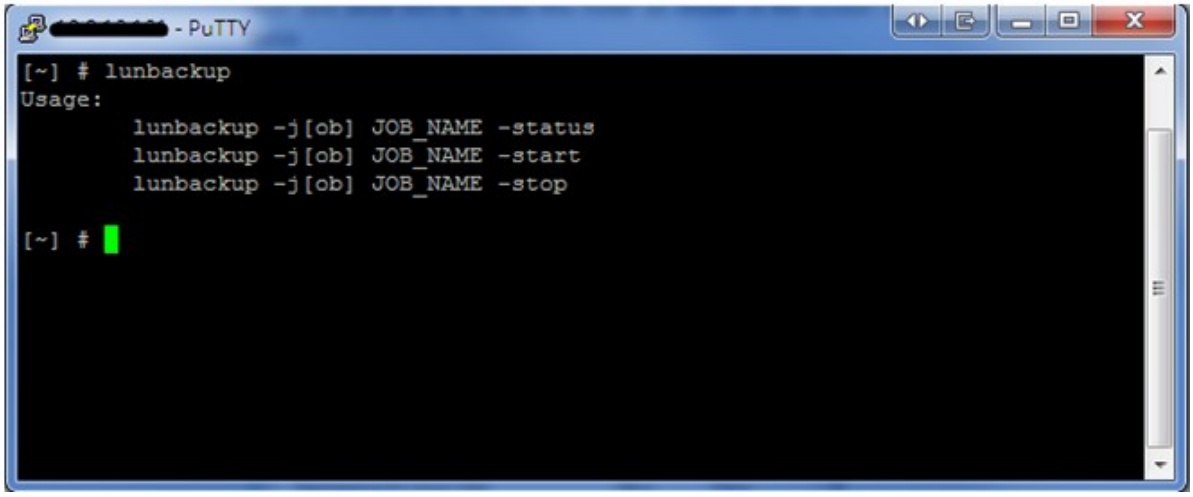
2. Connect to the NAS by an SSH utility such as Putty.



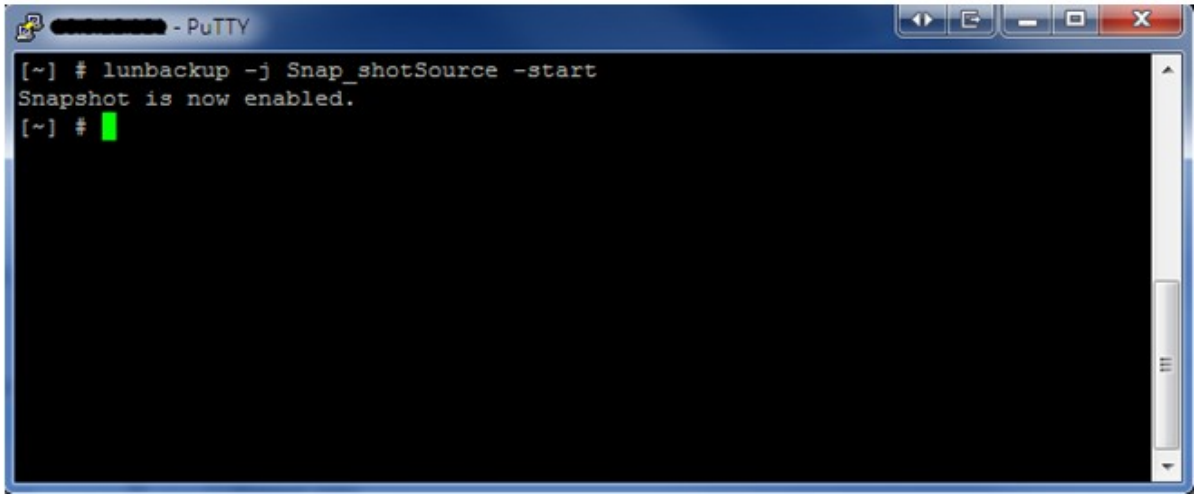
3. Login the NAS as an administrator.



4. Input the command "lunbackup". The command usage description will be shown.



5. Use the lunbackup command to start or stop an iSCSI LUN backup, restore, or snapshot job on the NAS.

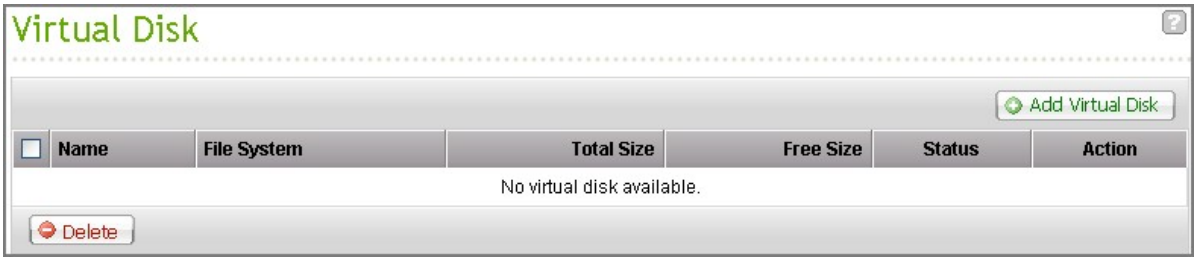


4.6 Virtual Disk

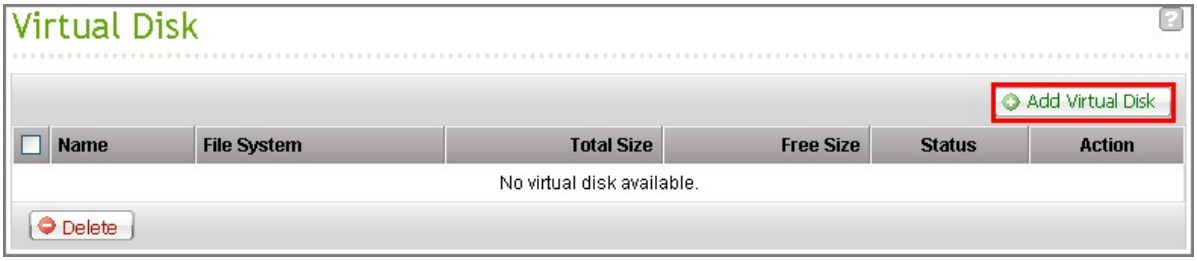
You can use this function to add the iSCSI targets of other QNAP NAS or storage servers to the NAS as the virtual disks for storage capacity expansion. The NAS supports maximum 8 virtual disks.

Note:

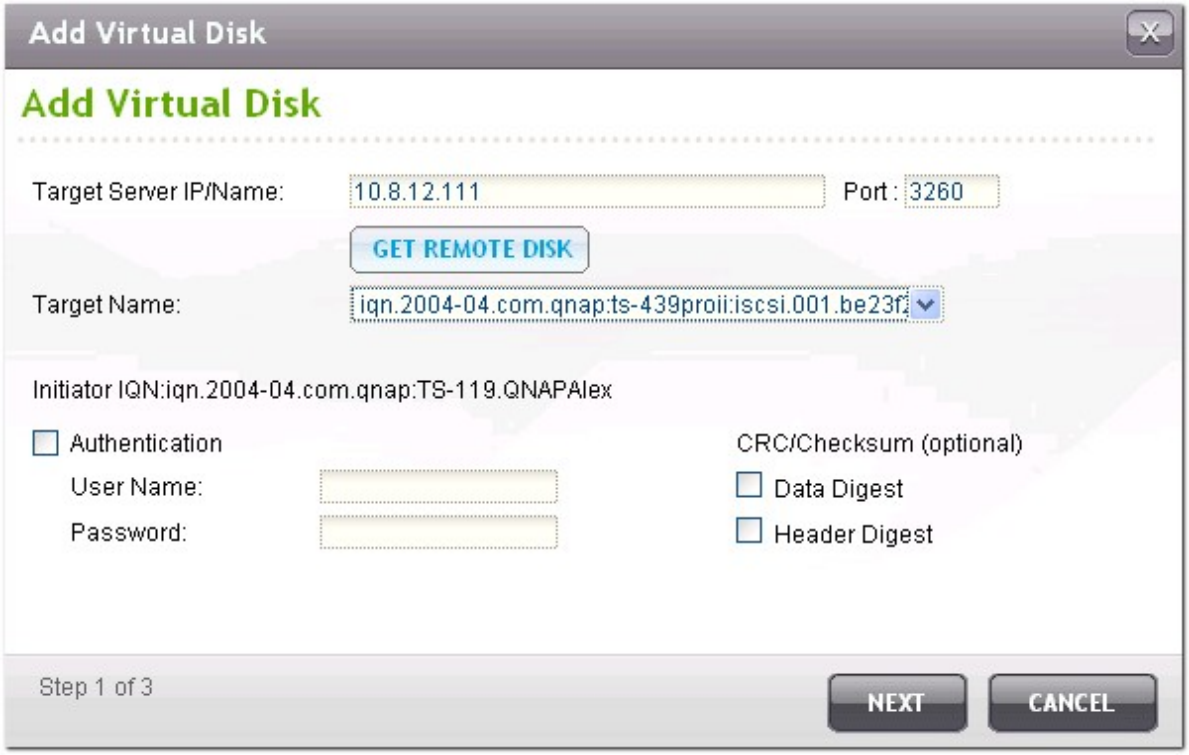
- The maximum size of a virtual disk the NAS supports is 16TB.
- When the virtual disk (iSCSI target) was disconnected, the virtual disk will disappear on the NAS interface and the NAS will try to connect to the target in two minutes. If the target cannot be connected after two minutes, the status of the virtual disk will become "Disconnected".



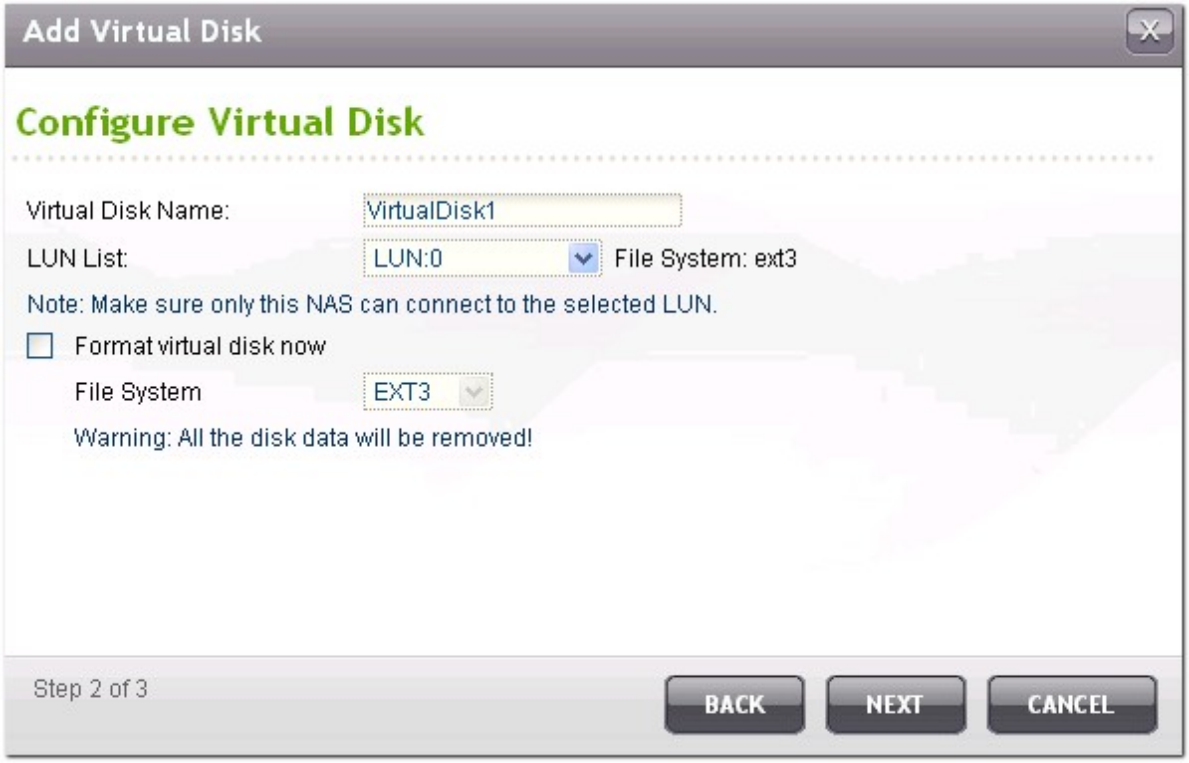
To add a virtual disk to the NAS, make sure an iSCSI target has been created. Click "Add Virtual Disk".



Enter the target server IP and port number (default: 3260). Click "Get Remote Disk". Select a target from the target list. If authentication is required, enter the user name and the password. You may select 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. Then, click "Next".

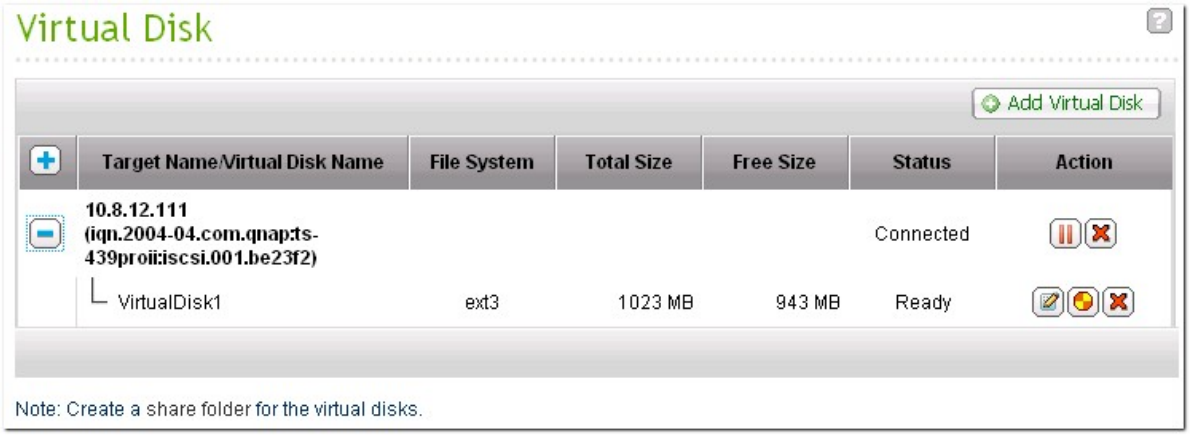


Enter a name for the virtual disk. If the target is mapped with multiple LUNs, select a LUN from the list. Make sure only this NAS can connect to the LUN. The NAS supports mounting EXT3, EXT4, FAT32, NTFS, HFS+ file systems. If the file system of the LUN is "Unknown", select "Format virtual disk now" and the file system. You can format the virtual disk as EXT3, EXT4, FAT 32, NTFS, or HFS+. By selecting "Format virtual disk now", the data on the LUN will be removed.



Click "Finish" to exit the wizard.

The storage capacity of your NAS has been expanded by the virtual disk. You can go to "Access Right Management" > "Share Folders" to create new share folders on the virtual disk.



Icon	Description
(Edit)	To edit a virtual disk name or the authentication information of an iSCSI target.
(Connect)	To connect to an iSCSI target.
(Disconnect)	To disconnect an iSCSI target.
(Format)	To format a virtual disk as EXT3, EXT 4, FAT 32, NTFS, or HFS+ file system.
(Delete)	To delete a virtual disk or an iSCSI target.

5. Access Right Management

Domain Security 194
Users 215
User Groups 232
Share Folders 235
Quota 264

5.1 Domain Security

The NAS supports user authentication by local access right management, Microsoft Active Directory (Windows Server 2003/2008), and Lightweight Directory Access Protocol (LDAP) directory. By joining the NAS to an Active Directory or a LDAP directory, the AD or LDAP users can access the NAS using their own accounts without extra user account setup on the NAS.

No domain security
Only the local users can access the NAS.

Active Directory authentication (domain members)
Join the NAS to an Active Directory. The domain users can be authenticated by the NAS. After joining the NAS to an AD domain, both the local NAS users and AD users can access the NAS via the following protocols/services:

- Samba (Microsoft Networking)
- AFP
- FTP
- Web File Manager
- WebDAV

LDAP authentication
Connect the NAS to an LDAP directory. The LDAP users can be authenticated by the NAS. After connecting the NAS to an LDAP directory, either the local NAS users or the LDAP users can be authenticated to access the NAS via Samba (Microsoft Networking). Both the local NAS users and LDAP users can access the NAS via the following protocols/services:

- AFP
- FTP
- Web File Manager

Home >> Access Right Management >> Domain Security
Welcome admin | Logout
English
Domain Security
Domain Security for File Services
No domain security (local users only)
Active Directory authentication (domain member)
LDAP authentication
APPLY

5.1.1 Join the NAS to Active Directory (Windows Server 2003/2008)

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

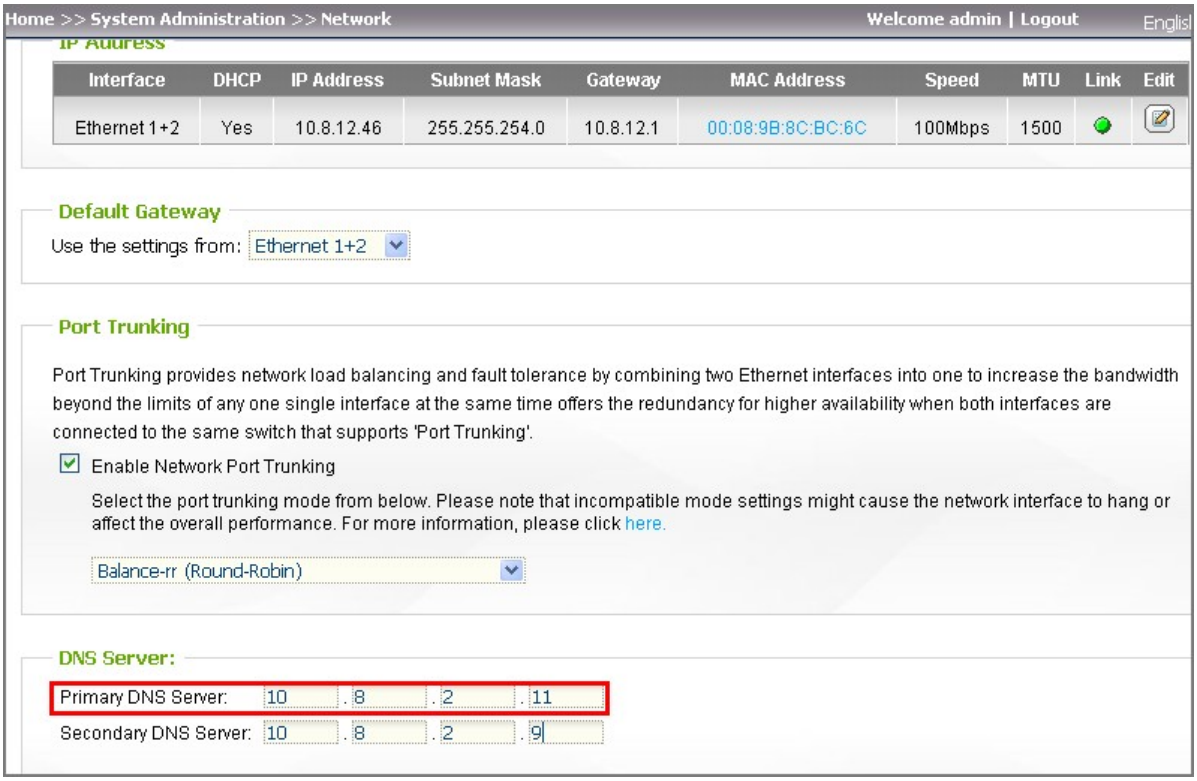
The NAS supports Active Directory (AD). By joining the NAS to the Active Directory, all the user accounts of the AD server will be imported to the NAS automatically. The AD users can use the same set of user name and password to login the NAS

If you are using Active Directory with Windows Server 2008 R2, you must update the NAS firmware to V3.2.0 or above to join the NAS to the AD.

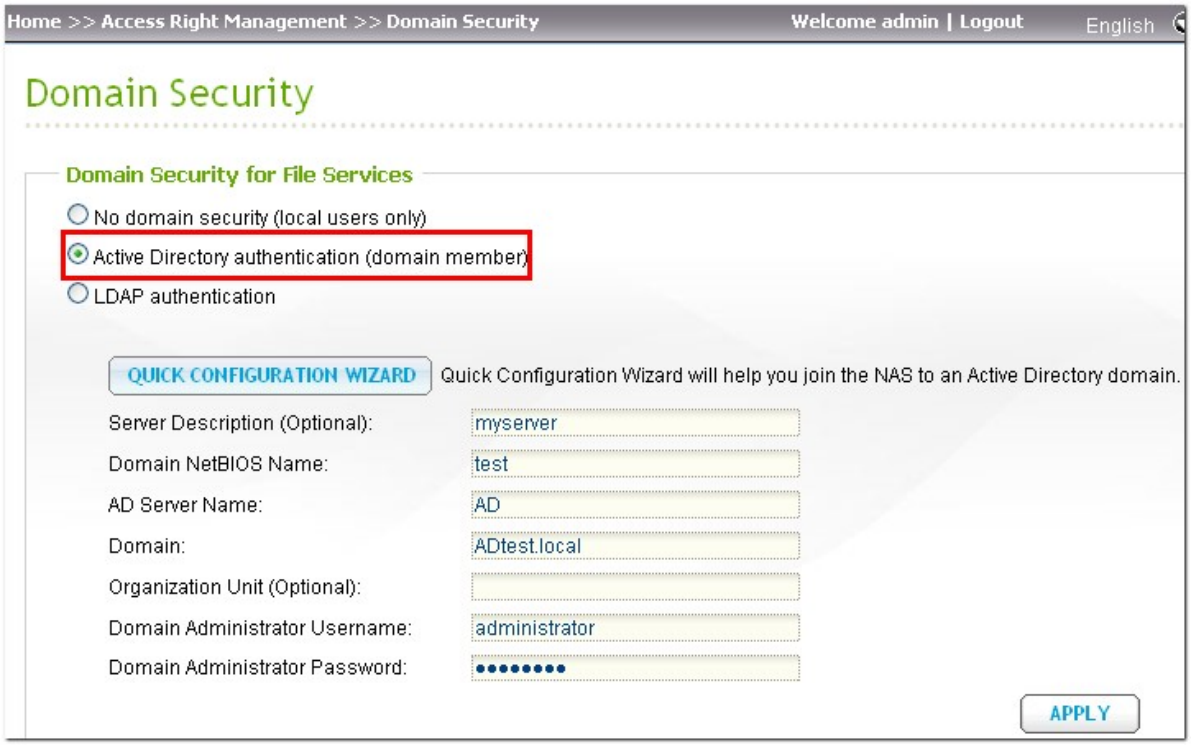
Follow the steps below to join the QNAP NAS to the Windows Active Directory.

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". Set the IP of the primary DNS server as the IP of the Active Directory server that contains the DNS service. It must be the IP of the DNS server that is used for your Active Directory. If you use an external DNS server, you will not be able to join the domain.



3. Go to “Access Right Management” > “Domain Security”. Enable “Active Directory authentication (domain member)”, and enter the AD domain information.



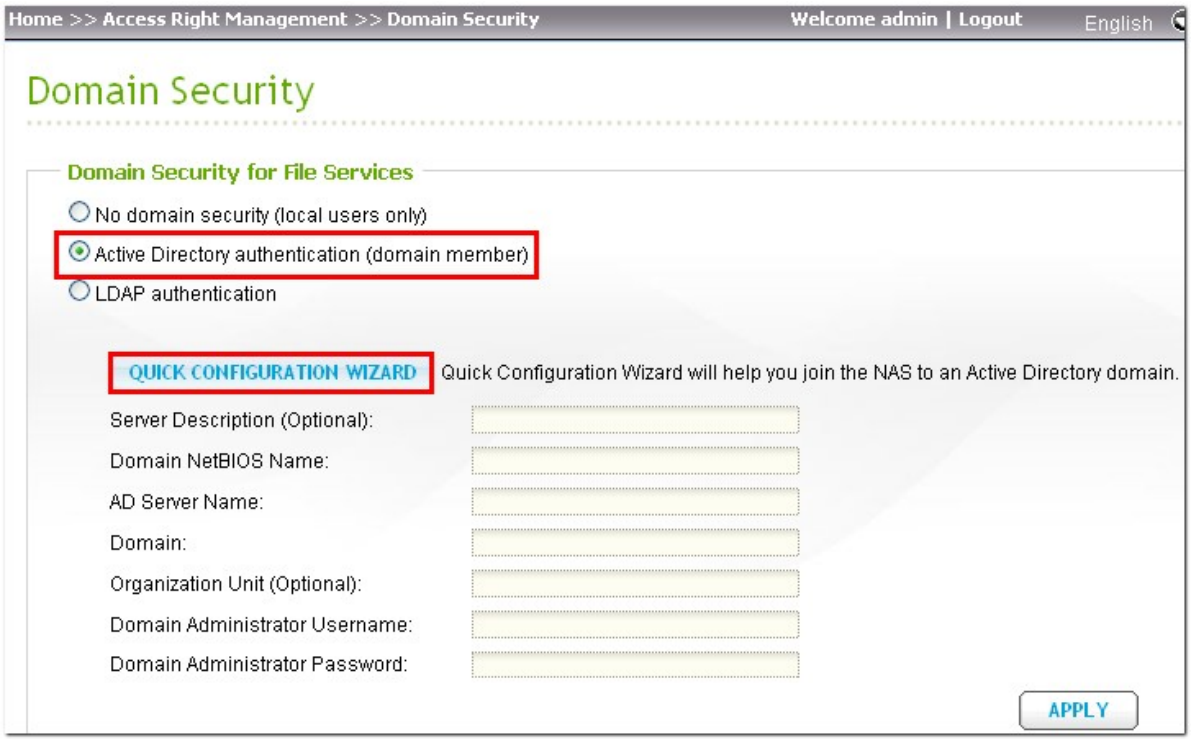
Note:

- Enter a fully qualified AD domain name, for example, qnap-test.com
- The AD user entered here must have the administrator access right to the AD domain.
- WINS Support: If you are using a WINS server on the network and the workstation is configured to use that WINS server for name resolution, you must set up the WINS server IP on the NAS (use the specified WINS server).

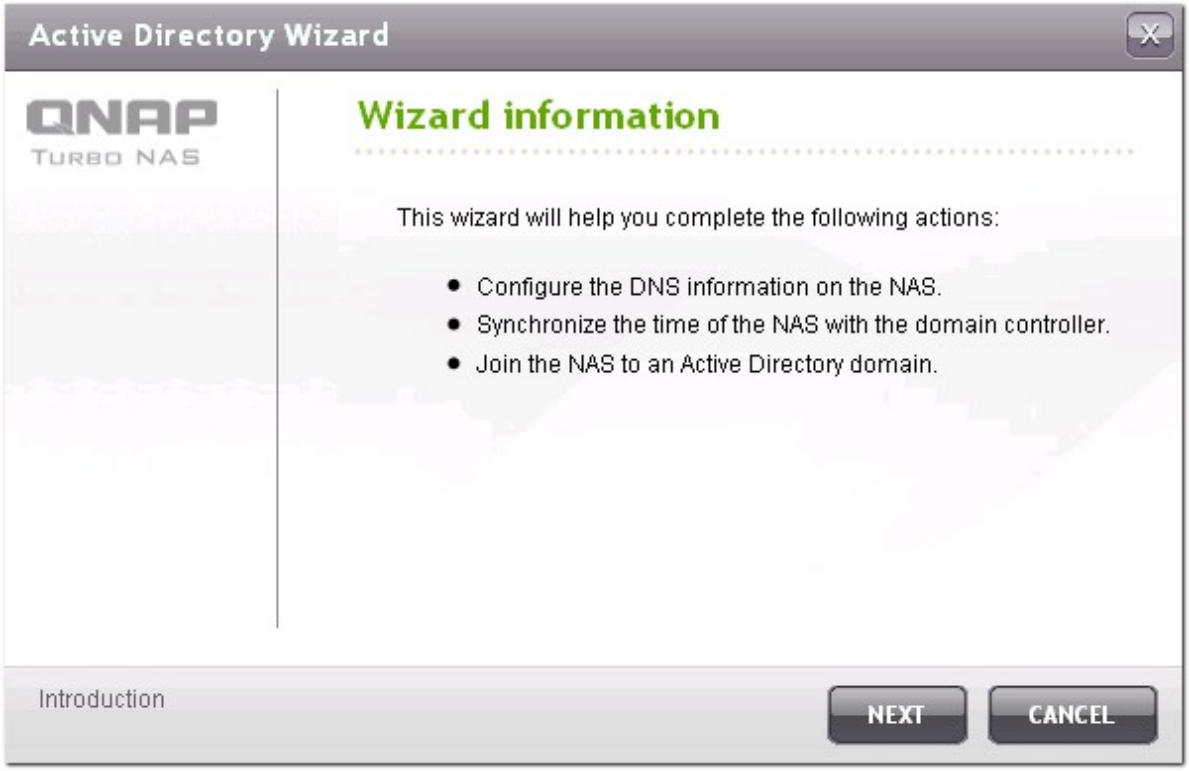
Join the NAS to Active Directory (AD) by Quick Configuration Wizard

To join the NAS to an AD domain by the Quick Configuration Wizard, follow the steps below.

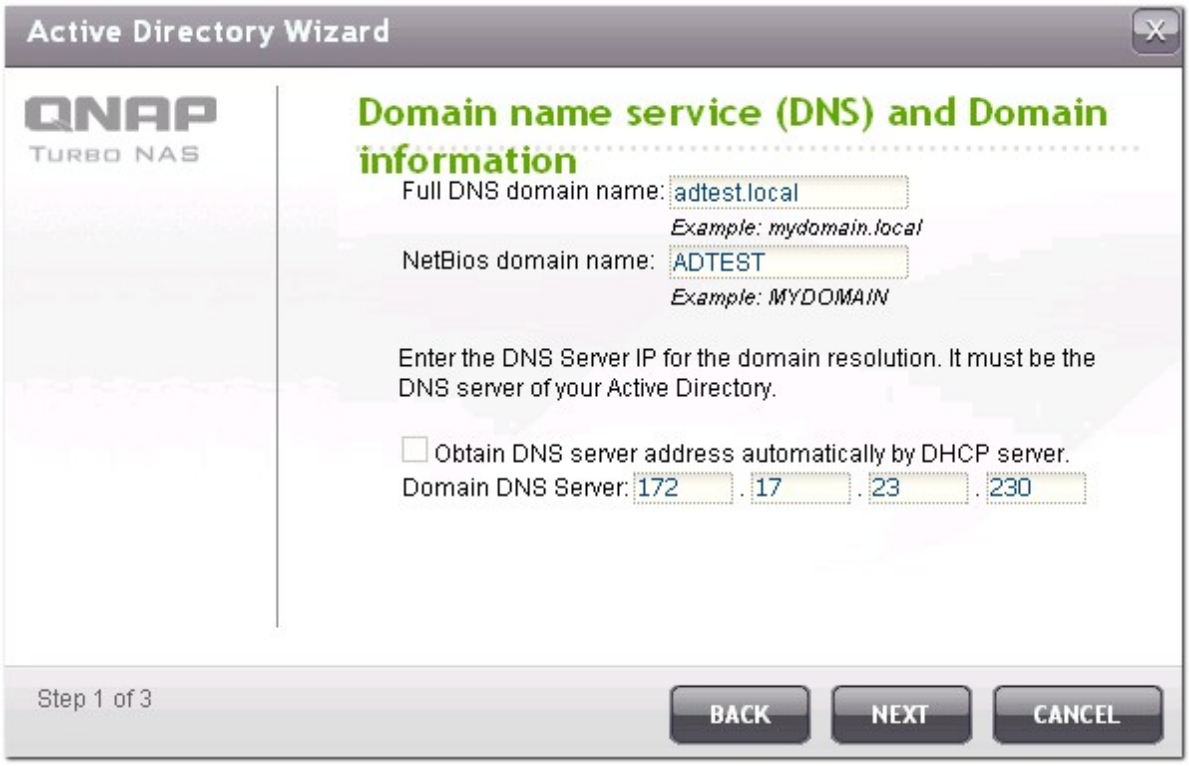
1. Go to "Access Right Management" > "Domain Security". Select "Active Directory authentication (domain member)" and click "Quick Configuration Wizard".



2. Read the introduction of the wizard. Click “Next”.

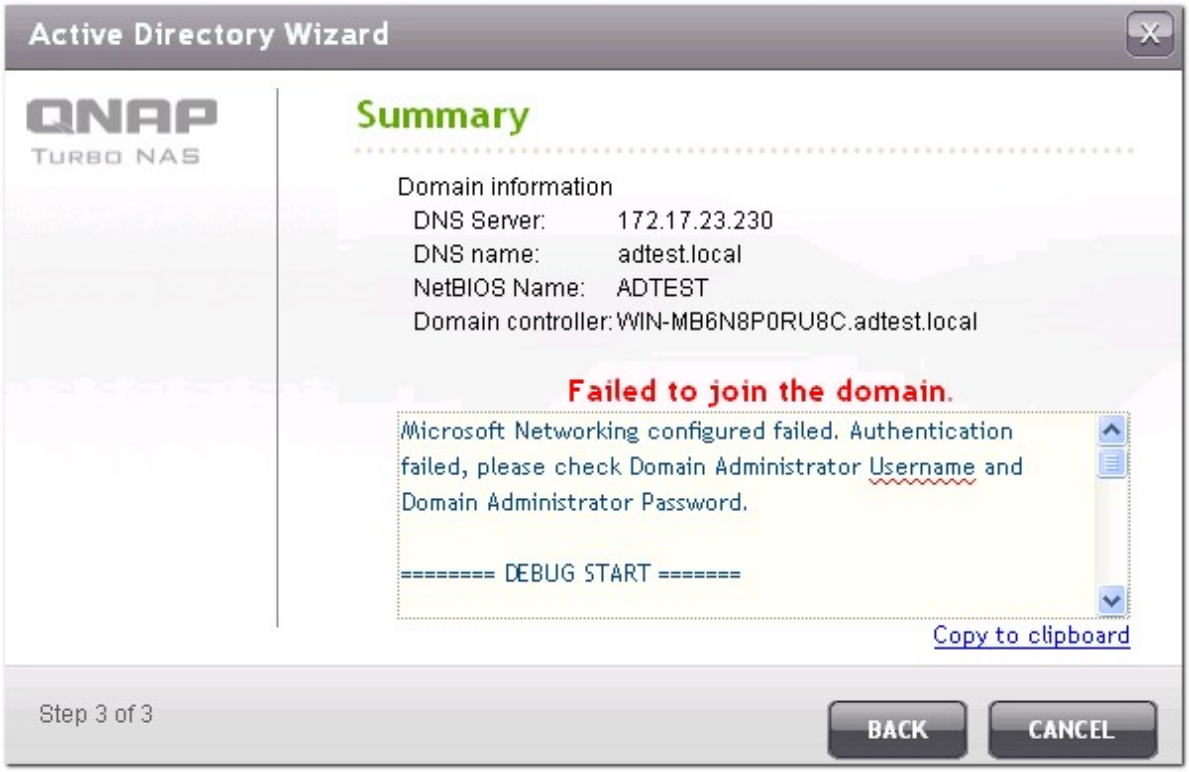


3. Enter the domain name of the domain name service (DNS). The NetBIOS name will be generated automatically when you type the domain name. Specify the DNS server IP for domain resolution. The IP must be the same as the DNS server of your Active Directory. Click "Next".

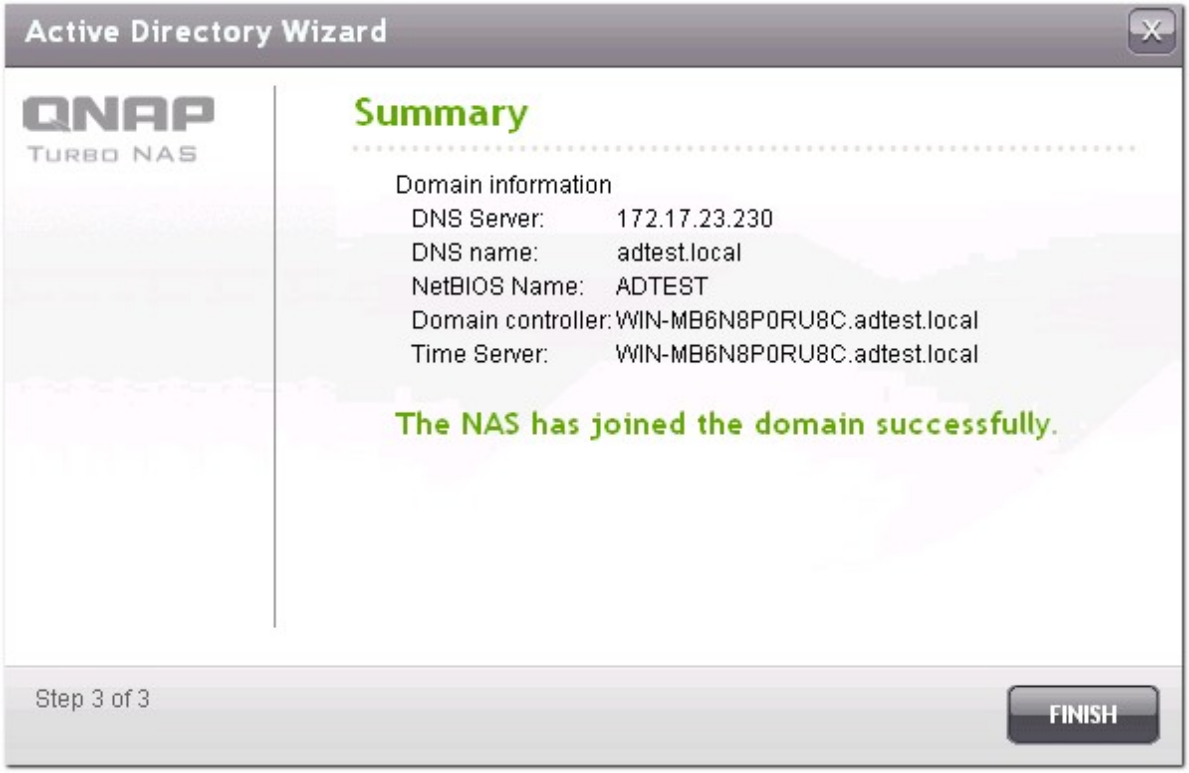


4. Select a domain controller from the drop-down menu. The domain controller is responsible for time synchronization between the NAS and the domain server and user authentication. Enter the domain administrator name and password. Click "JOIN".

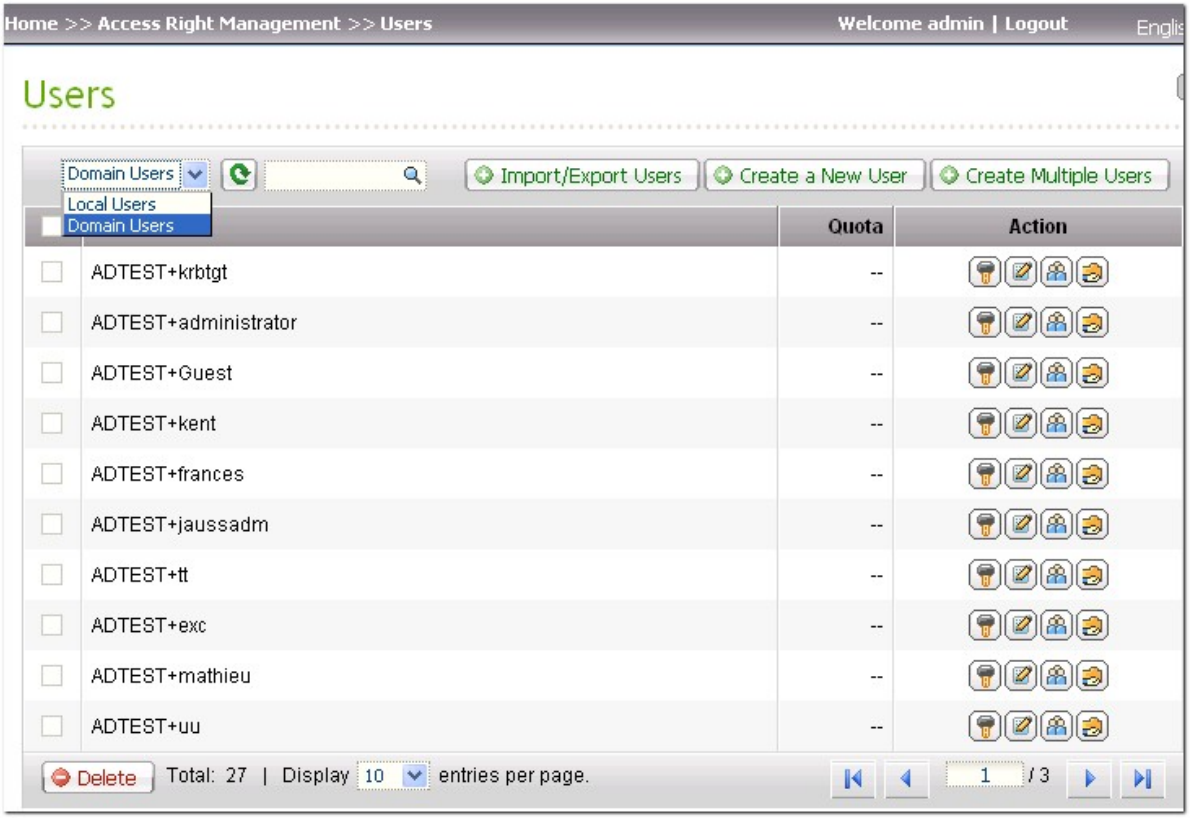
5. If you failed to join the NAS to the domain, you could copy the error logs or go back to modify the settings.



6. Upon successful login to the domain server, the NAS has joined to the domain. Click "Finish" to exit the wizard.

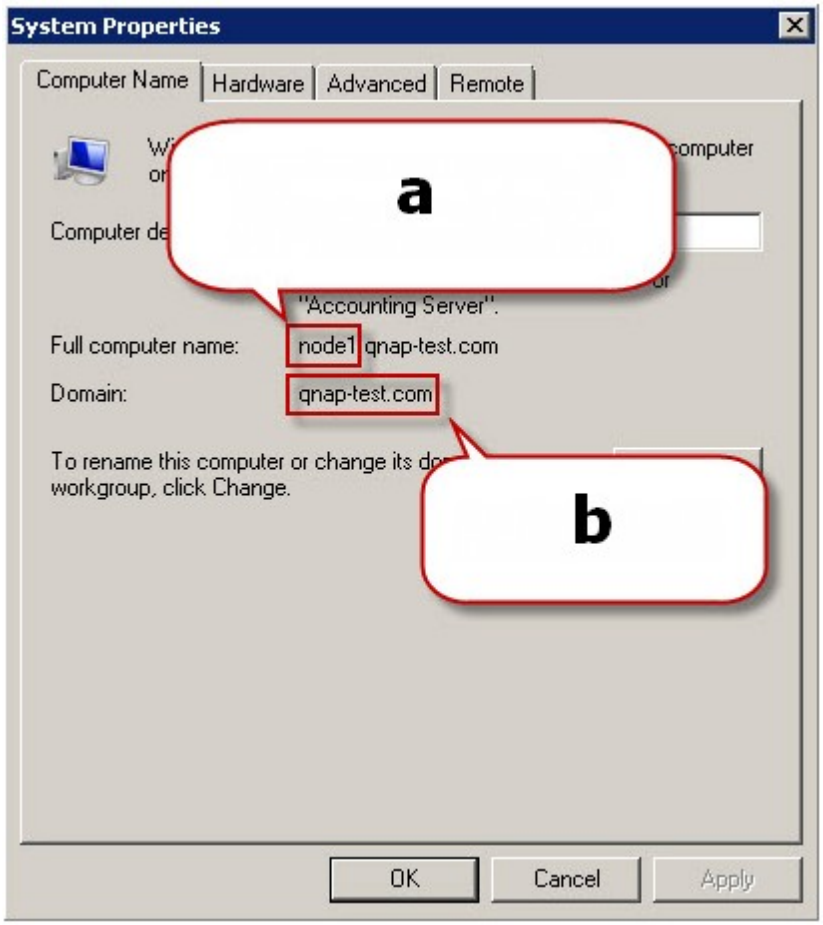


7. Go to "Access Right Management" > "Users" or "User Groups" to load the domain users or user groups to the NAS.



Windows 2003

The AD server name and AD domain name can be checked in "System Properties".



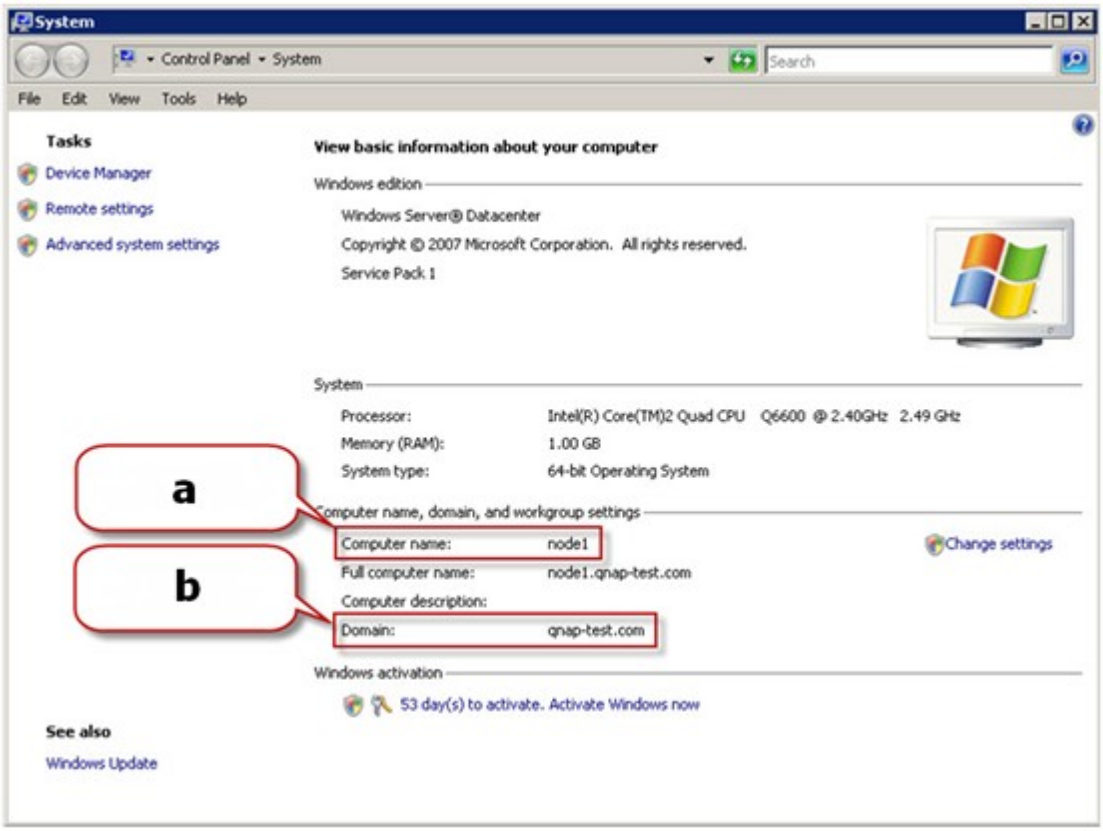
a. In Windows 2003 servers, the AD server name is "node1" NOT "node1.qnap-test.com".
b. The domain name remains the same.

Windows Server 2008

Check the AD server name and domain name in "Control Panel" > "System".

a. This is the AD server name.

b. This is the domain name.



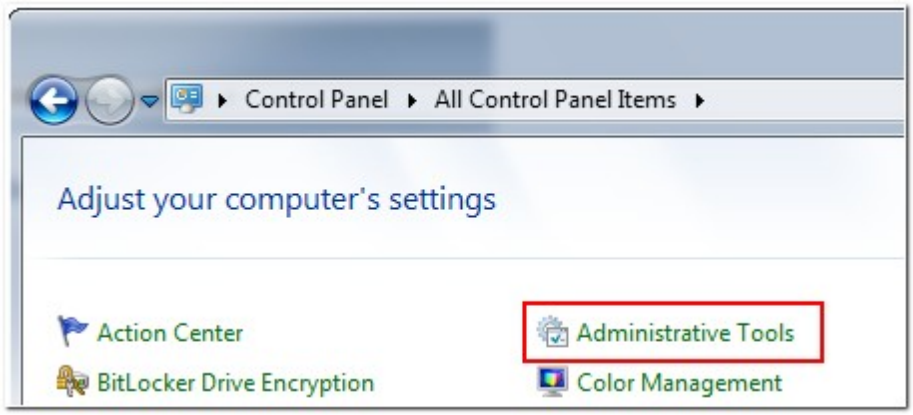
Note:

- 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 login the NAS (firmware version 3.2.0 or above) via AFP, FTP, Web File Manager, and WebDAV. However, if the firmware version of the NAS is earlier than 3.2.0, only the local NAS users are allowed to login the NAS by Web File Manager and WebDAV.
- For TS-109/209/409/509 series NAS, if the AD domain is based on Windows 2008 Server, the NAS firmware must be updated to version 2.1.2 or above.

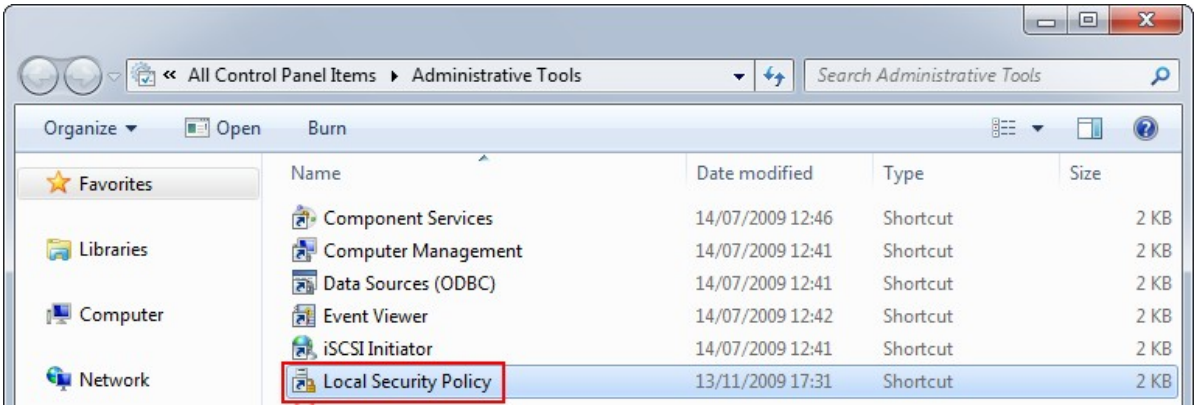
Windows 7

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, change your PC settings as shown below to allow your PC to connect to the NAS.

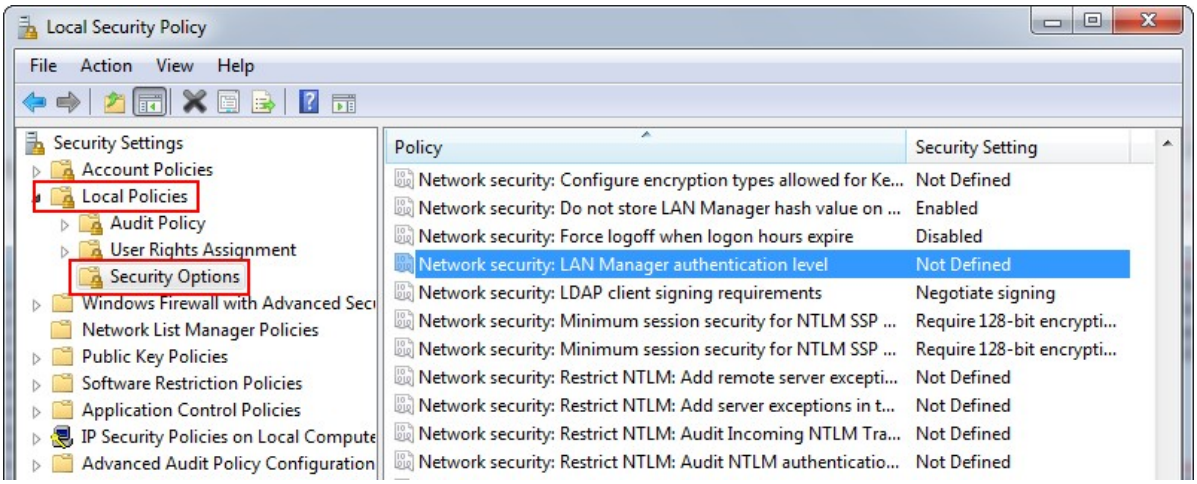
a. Go to "Control Panel" > "Administrative Tools".



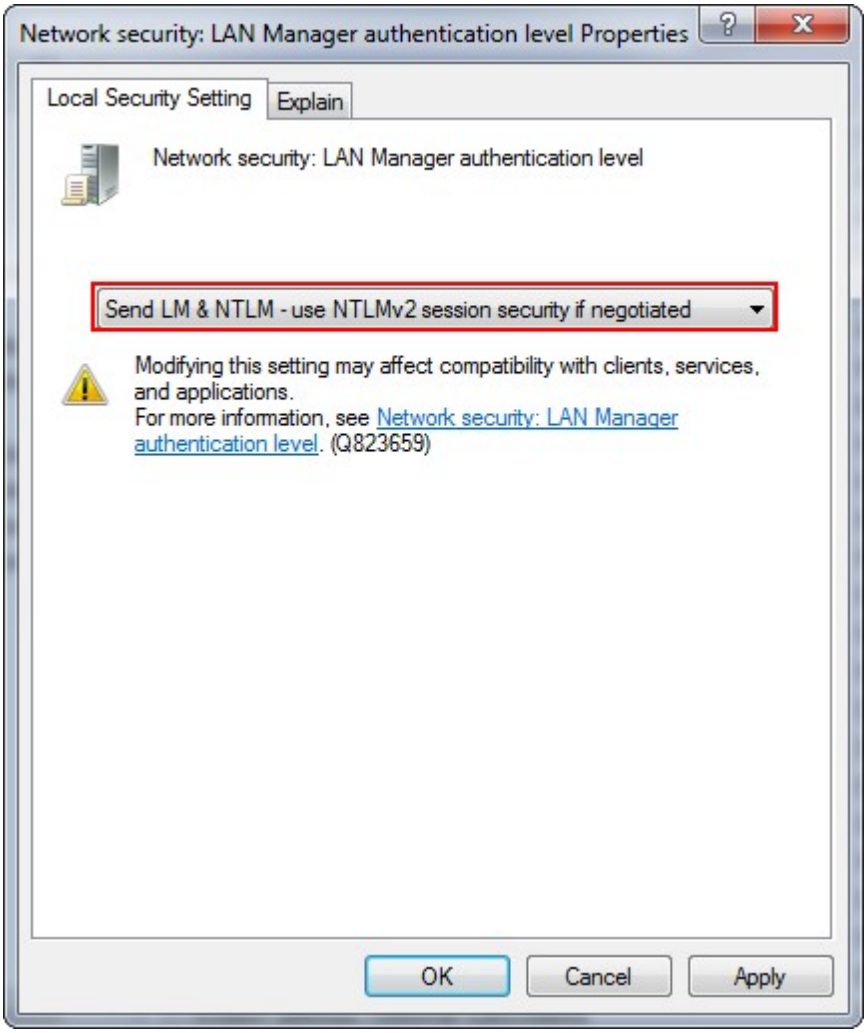
b. Click "Local Security Policy".



c. Go to “Local Policies” > “Security Options”. 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”.



Verify the settings

To verify that the NAS has been joined to the Active Directory successfully, go to "Access Right Management" > "Users" and "User Groups". A list of users and user groups will be shown on the "Domain Users" and "Domain Groups" lists respectively.

If you have created new users or user groups in the domain, you can click the reload button next to "Domain Users" drop-down menu in "Access Right Management" > "Users" or "Domain Groups" drop-down menu in "Access Right Management" > "User Groups". This will reload the user and user group lists from the Active Directory to the NAS. The user permission settings will be synchronized in real time with the domain controller.

5.1.2 Connect the NAS to an LDAP Directory

LDAP stands for Lightweight Directory Access Protocol. It is a directory that can store the information of all the users and groups in a centralized server. Using LDAP, the administrator can manage the users in the LDAP directory and allow the users to connect to multiple NAS servers with the same username and password.

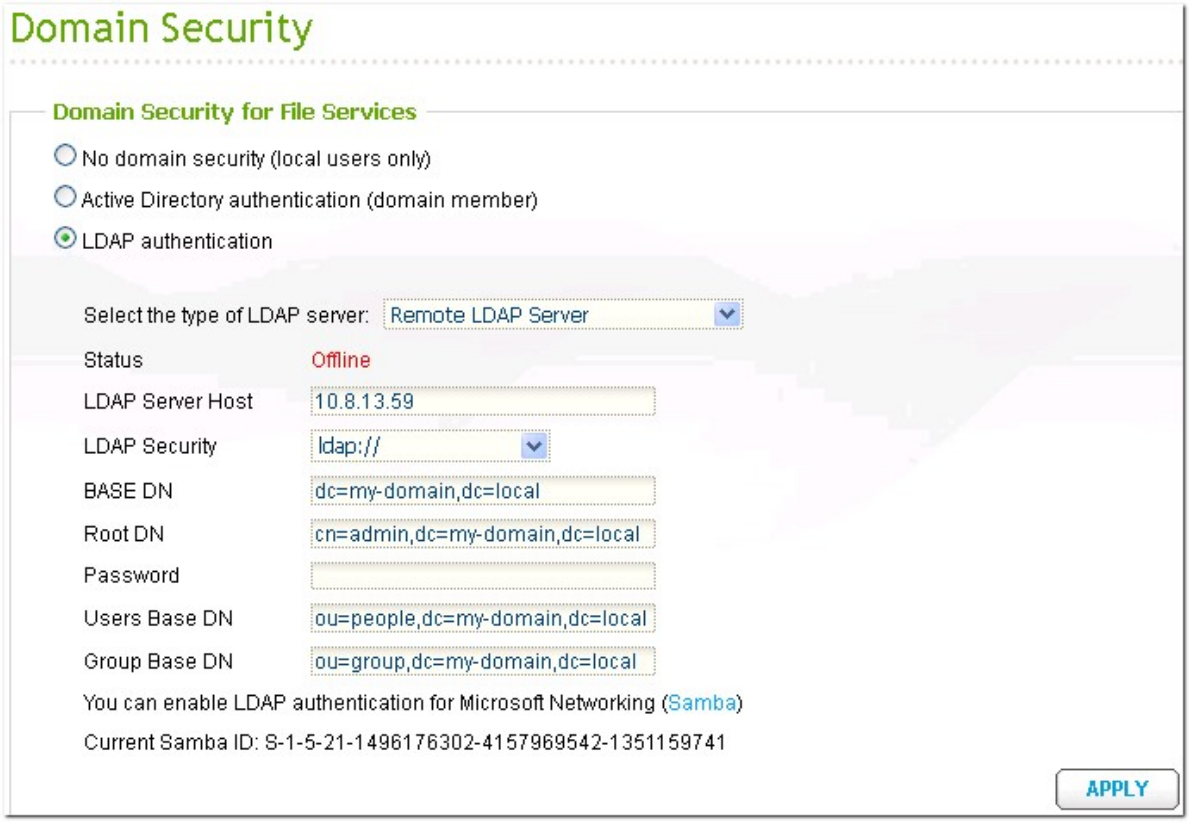
This feature is intended for administrator and users who have some knowledge about Linux servers, LDAP servers, and Samba. An LDAP server which is up and running is required when using the LDAP feature of the QNAP NAS.

Required information/settings:

- The LDAP server connection and authentication information
- The LDAP structure, where the users and groups are stored
- The LDAP server security settings

Follow the steps below to connect the QNAP NAS to an LDAP directory.

1. Login the web interface of the NAS as an administrator.
2. Go to "Access Right Management" > "Domain Security". By default, the option "No domain security" is enabled. That means only the local NAS users can connect to the NAS.
3. Select "LDAP authentication" and complete the settings.

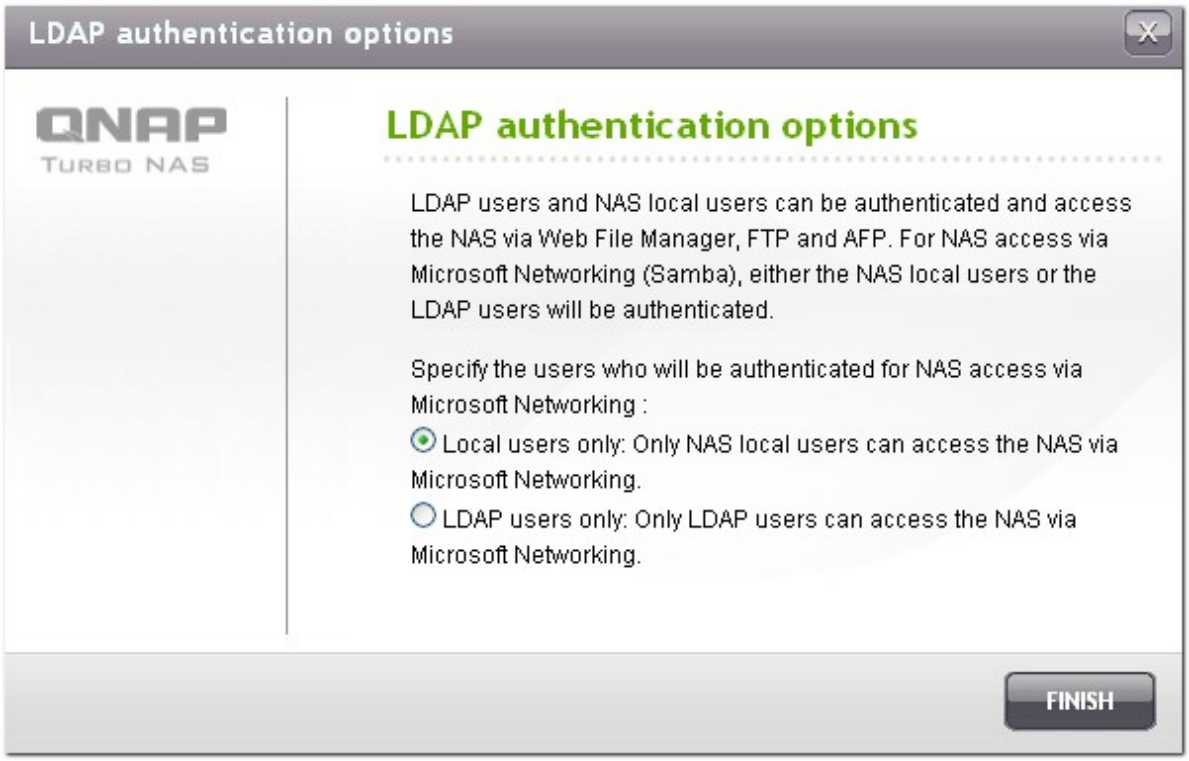


- LDAP Server Host: The host name or IP address of the LDAP server.
- LDAP Security: Specify how the NAS will communicate with the LDAP server:
  - ldap:// = Use a standard LDAP connection (default port: 389).
  - ldap:// (ldap + SSL) = Use an encrypted connection with SSL (default port: 686). This is usually used by older version of LDAP servers.
  - ldap:// (ldap + TLS) = Use an encrypted connection with TLS (default port: 389). This is usually used by newer version of LDAP servers
- BASE DN: The LDAP domain. For example: dc=mydomain,dc=local
- Root DN: The LDAP root user. For example cn=admin, dc=mydomain,dc=local
- Password: The root user password.
- Users Base DN: The organization unit (OU) in which users are stored. For example: ou=people, dc=mydomain,dc=local
- Groups Base DN: The organization unit (OU) in which groups are stored. For example ou=group, dc=mydomain,dc=local

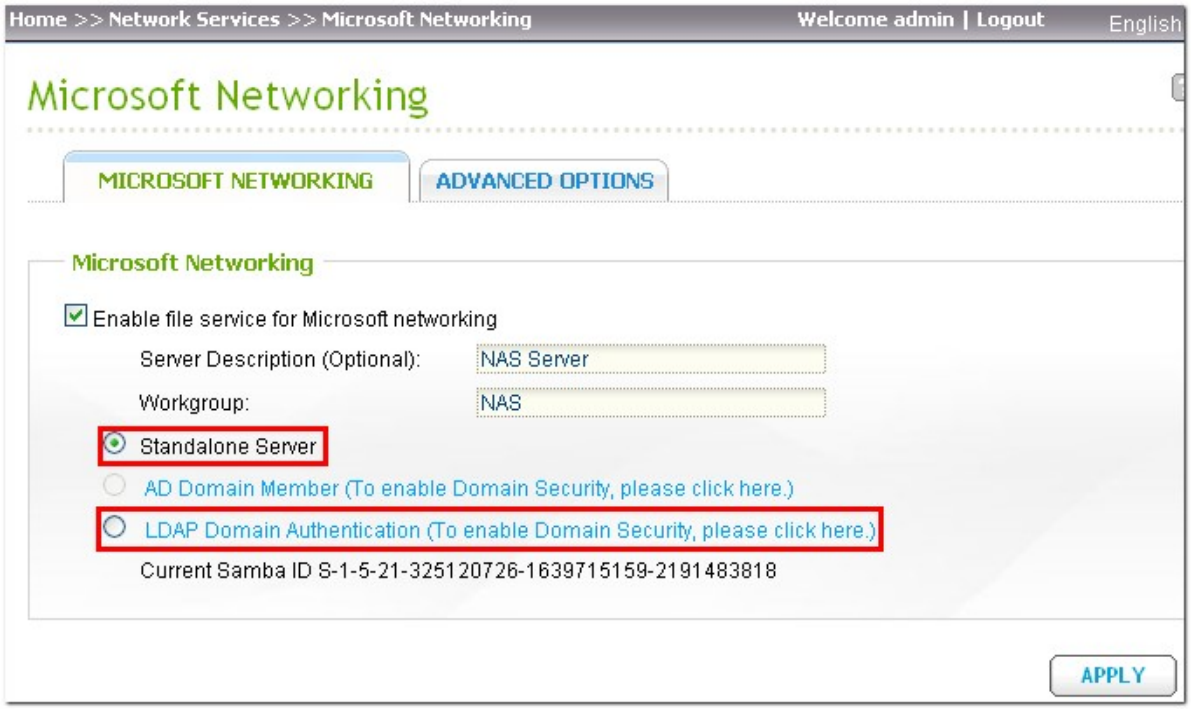
4. Click "Apply" to save the settings. Upon successful configuration, the NAS will be able to connect to the LDAP server.

5. Configure LDAP authentication options.
   - If Microsoft Networking has been enabled (Network Services > Microsoft Networking) when applying the LDAP settings, specify the users who can access the NAS via Microsoft Networking (Samba).
     - Local users only: Only the local NAS users can access the NAS via Microsoft Networking.
     - LDAP users only: Only the LDAP users can access the NAS via Microsoft Networking.

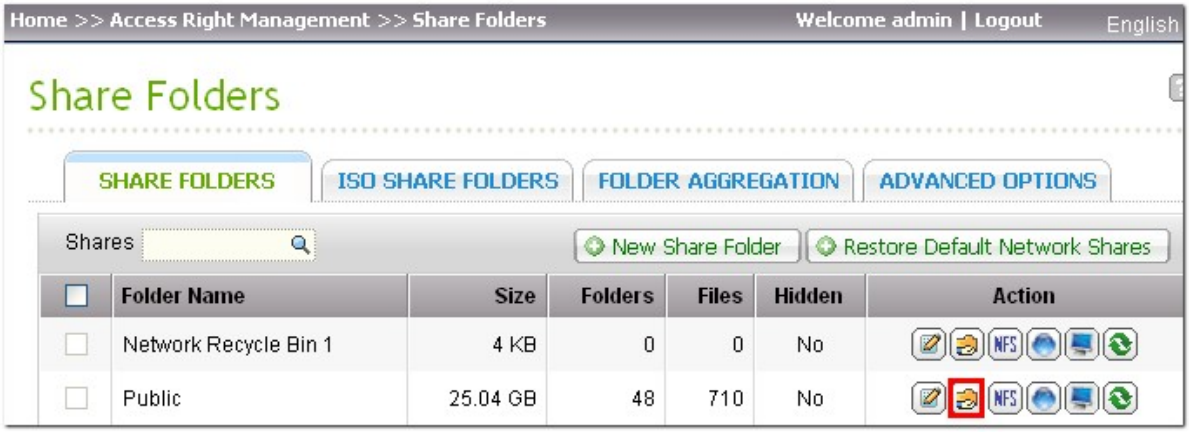
Note: Both the LDAP users and local NAS users can access the NAS via Web File Manager, FTP, and AFP.

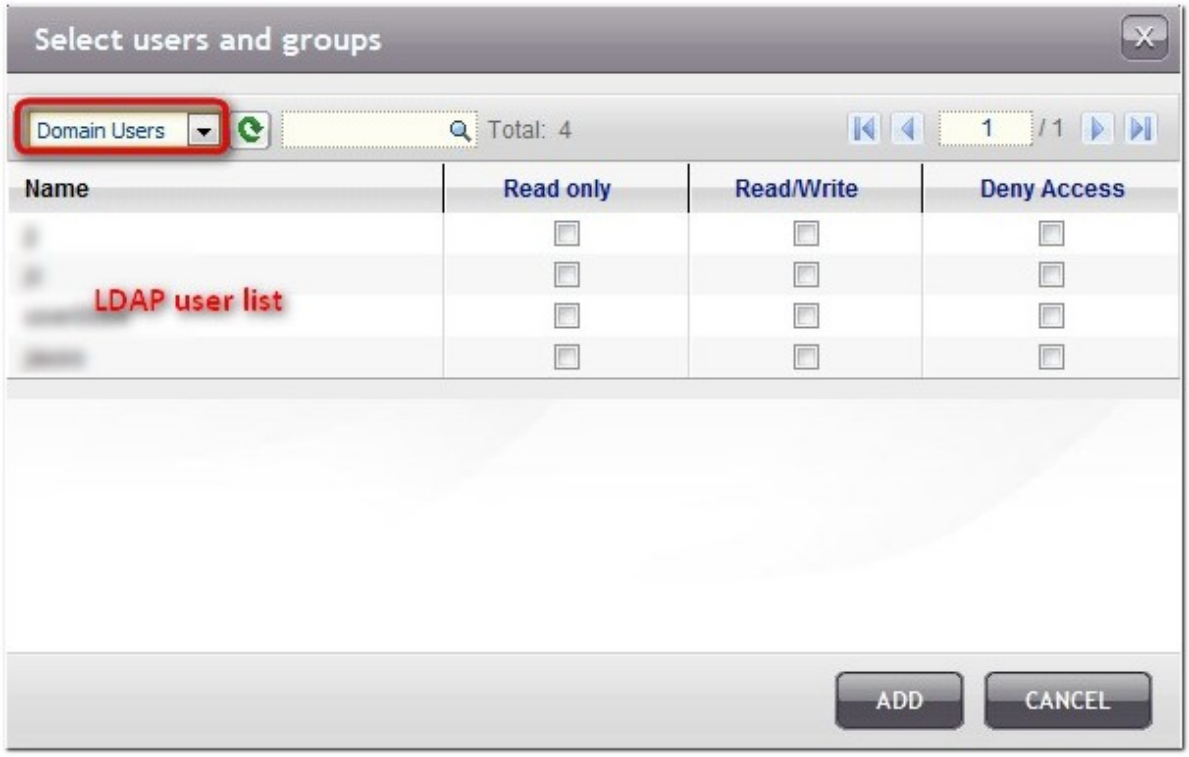


- If Microsoft Networking is enabled after the NAS has already been connected to the LDAP server, select the authentication type for Microsoft Networking.
  - Standalone Server: Only local NAS users can access the NAS via Microsoft Networking.
  - LDAP Domain Authentication: Only LDAP users can access the NAS via Microsoft Networking.



6. When the NAS is connected to an LDAP server, the administrator can:
   - Go to "Access Right Management" > "Users" and select "Domain Users" from the drop-down menu. The LDAP users list will be shown.
   - Go to "Access Right Management" > "User Groups" and select "Domain Groups" from the drop-down menu. The LDAP groups will be shown.
   - Specify the folder permissions of the LDAP domain users or groups in "Access Right Management" > "Shared Folders" > "Folder Permissions" .





Technical requirements of LDAP authentication with Microsoft Networking:

Required items to authenticate the LDAP users on Microsoft Networking (Samba):

1. a third party software to synchronize the password between LDAP and Samba in the LDAP server.
2. importing the Samba schema to the LDAP directory.

1) Third-party software:

Some software are available and allow management of the LDAP users, including Samba password. For example:

- LDAP Account Manager (LAM), with a Web-based interface, available at: http://www.ldap-account-manager.org/
- smbldap-tools (command line tool)
- webmin-ldap-useradmin - LDAP user administration module for Webmin.

2) Samba schema:

To import the samba schema to the LDAP server, please refer to the documentation or FAQ of the LDAP server.
The samba.schema file is required and can be found in the directory examples/LDAP in the Samba source distribution.

Example for open-ldap in the Linux server where the LDAP server is running (it can be different depending on the Linux distribution):

Copy the samba schema:

```
zcat /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz > /etc/ldap/schema/samba.schema
```

Edit /etc/ldap/slapd.conf (openldap server configuration file) and make sure the following lines are present in the file:

```
include /etc/ldap/schema/samba.schema

include /etc/ldap/schema/cosine.schema

include /etc/ldap/schema/inetorgperson.schema

include /etc/ldap/schema/nis.schema
```

Configuration examples:

The following are some configuration examples. They are not mandatory and need to be adapted to match the LDAP server configuration:

1. Linux OpenLDAP Server

Base DN: dc=qnap,dc=com
Root DN: cn=admin,dc=qnap,dc=com
Users Base DN: ou=people,dc=qnap,dc=com
Groups Base DN: ou=group,dc=qnap,dc=com

2. Mac Open Directory Server

Base DN: dc=macserver,dc=qnap,dc=com
Root DN: uid=root,cn=users,dc=macserver,dc=qnap,dc=com
Users Base DN: cn=users,dc=macserver,dc=qnap,dc=com
Groups Base DN: cn=groups,dc=macserver,dc=qnap,dc=com

5.2 Users

The NAS has created the following users by default:

- admin
  The administrator "admin" has full access to system administration and all network shares. It 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 is "guest".
- anonymous
  This is a built-in user and will not be shown on the "User Management" page. When you connect to the server by FTP, you can use this name to login.

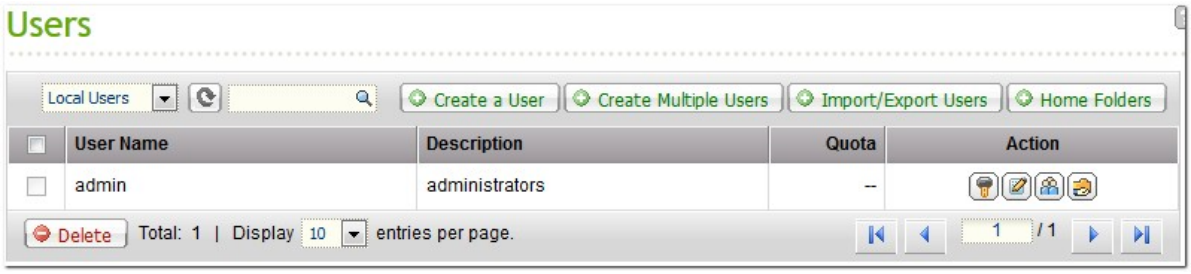
The number of users you can create on the NAS varies according to the NAS models. If your NAS models are not listed, please visit http://www.qnap.com for details.

Maximum number of users	**NAS models**
1,024	TS-110, TS-210
2,048	TS-112, TS-119, TS-119P+, TS-212, TS-219P+, TS-410, TS-239 Pro II+, TS-259 Pro+
4,096	TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP

The following information is required to create a new user:

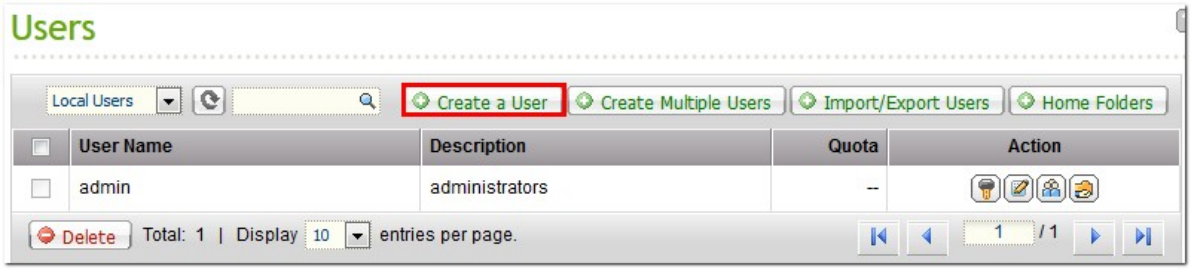
- User name
  The user name must not exceed 32 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean. The invalid characters are listed below:
  " / \ [ ] : ; | = , + * ? < > ` '

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

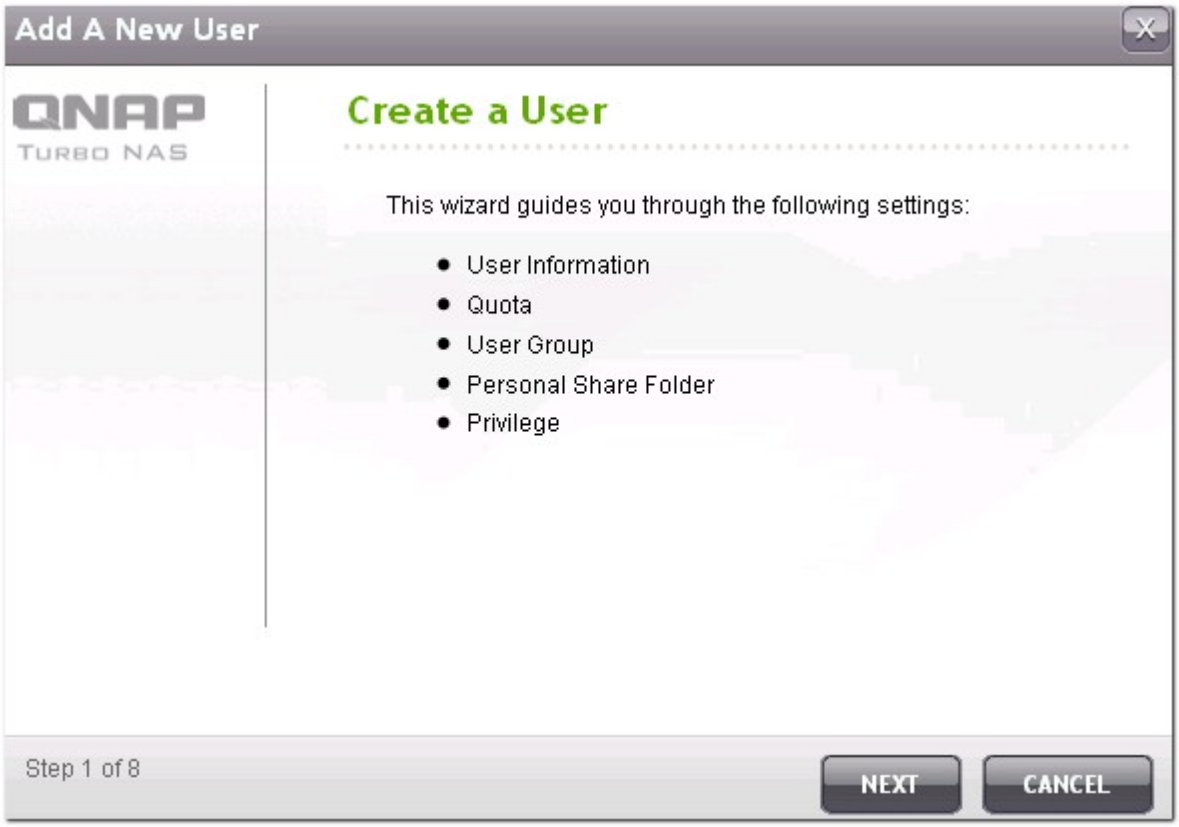


Create a User

To create a user on the NAS, click "Create a User".

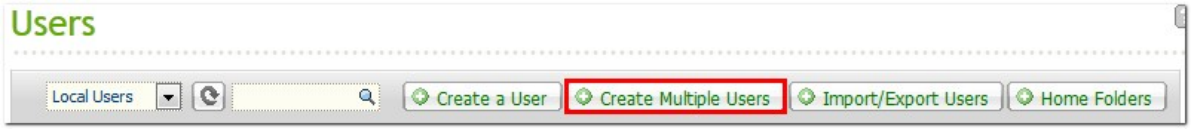


Follow the instructions of the wizard to complete the details.



Create Multiple Users

1. To create multiple users on the NAS, click "Create Multiple Users".



2. Click "Next".

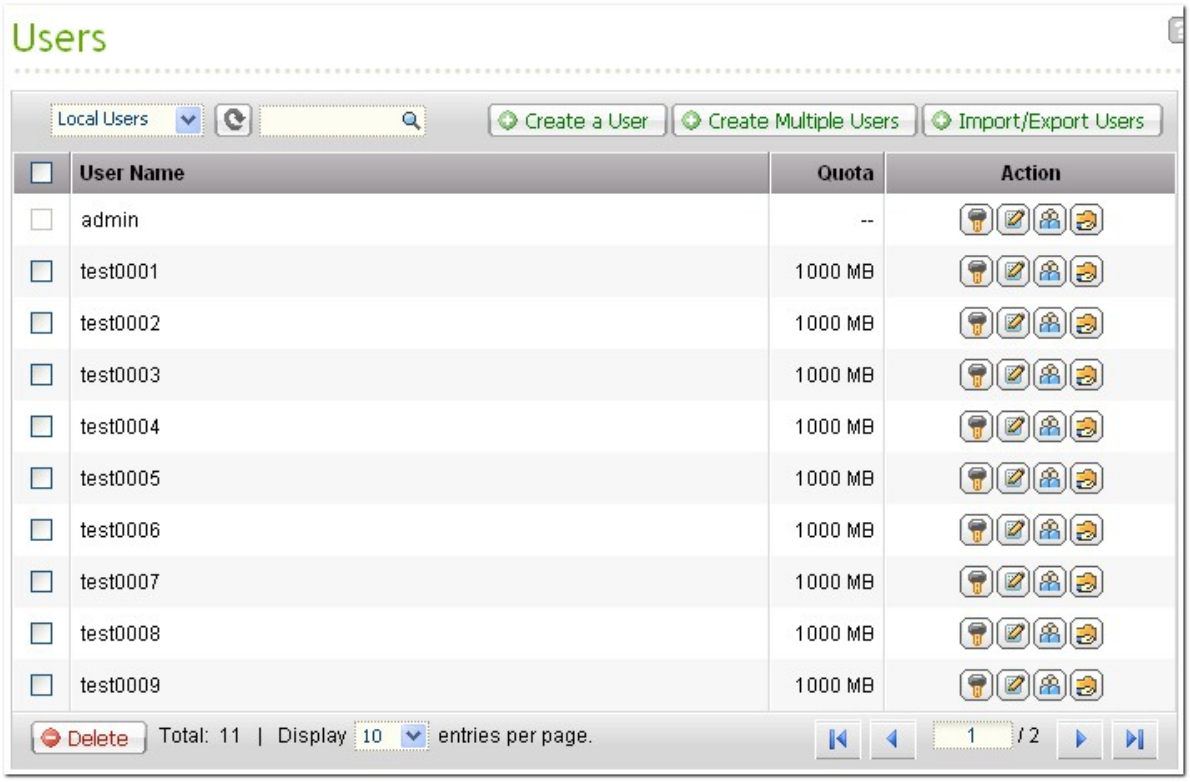
3. Enter the name prefix, e.g. test. Enter the start number for the user name, e.g. 0001 and the number of users to be created, e.g. 10. The NAS creates ten users named test0001, test0002, test0003…test0010. The password entered here is the same for all the new users.

4. Select to create a private network share for each user or not. The network share will be named after the user name. If a network share of the same name has already existed, the NAS will not create the folder.

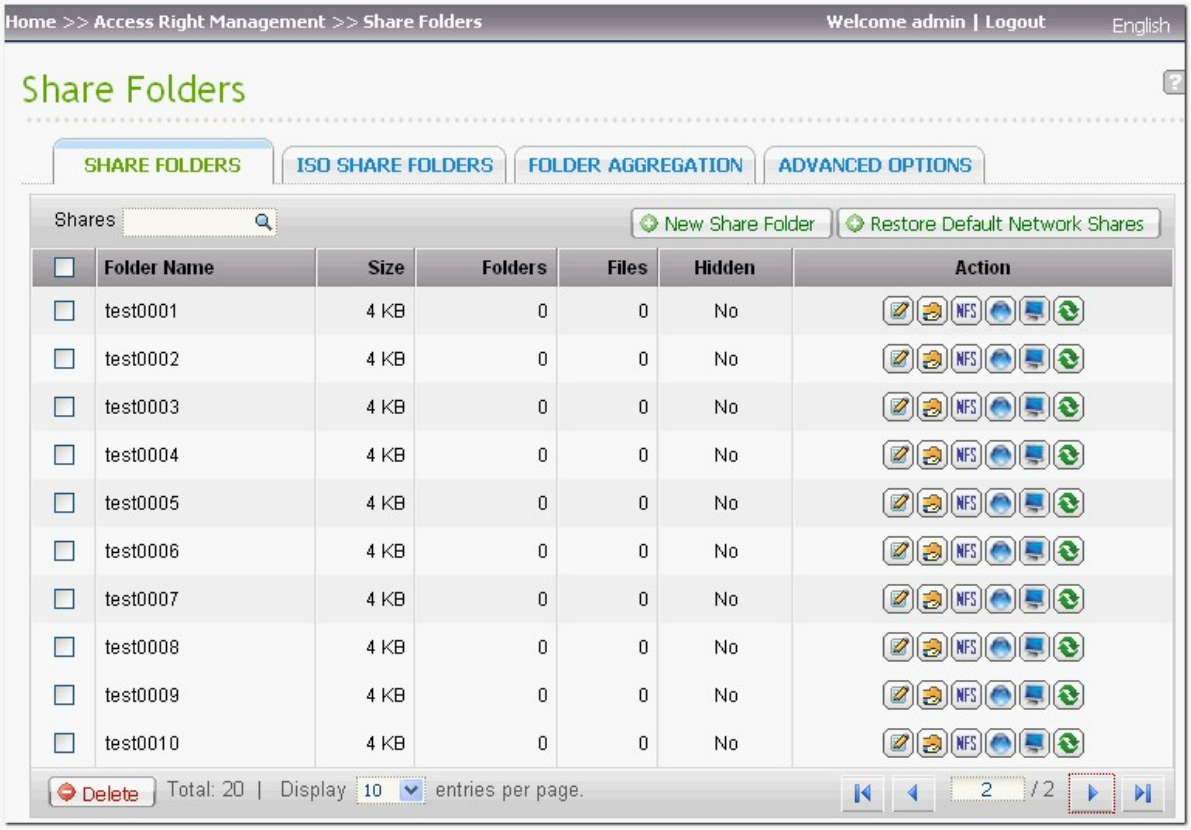
5. Specify the folder settings.

6. You can view the new users created in the last step. Click "Finish" to exit the wizard.

7. Check that the users have been created.



8. Check that the network shares have been created for the users.



Import/Export Users

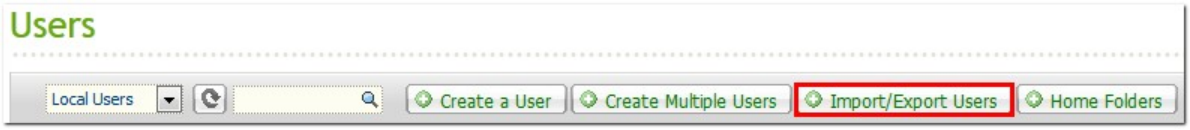
You can import users to or export users from the NAS with this function.

> **Note:** The password rules (if applicable) will not be applied when importing the users.

Export users

Follow the steps below to export users from the NAS:

1. Click "Import/Export Users".



2. Select the option "Export user and user group settings".

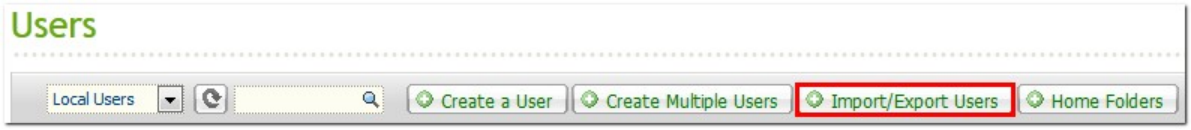
3. Click “Next” to download and save the account setting file (*.bin). The file can be imported to another NAS for account setup.

Note that the quota settings can be exported only when the quota function is enabled in “Access Right Management” > “Quota”.

Import users

Before you import users to the NAS, make sure you have backed up the original users settings by exporting the users. Follow the steps below to import users to the NAS:

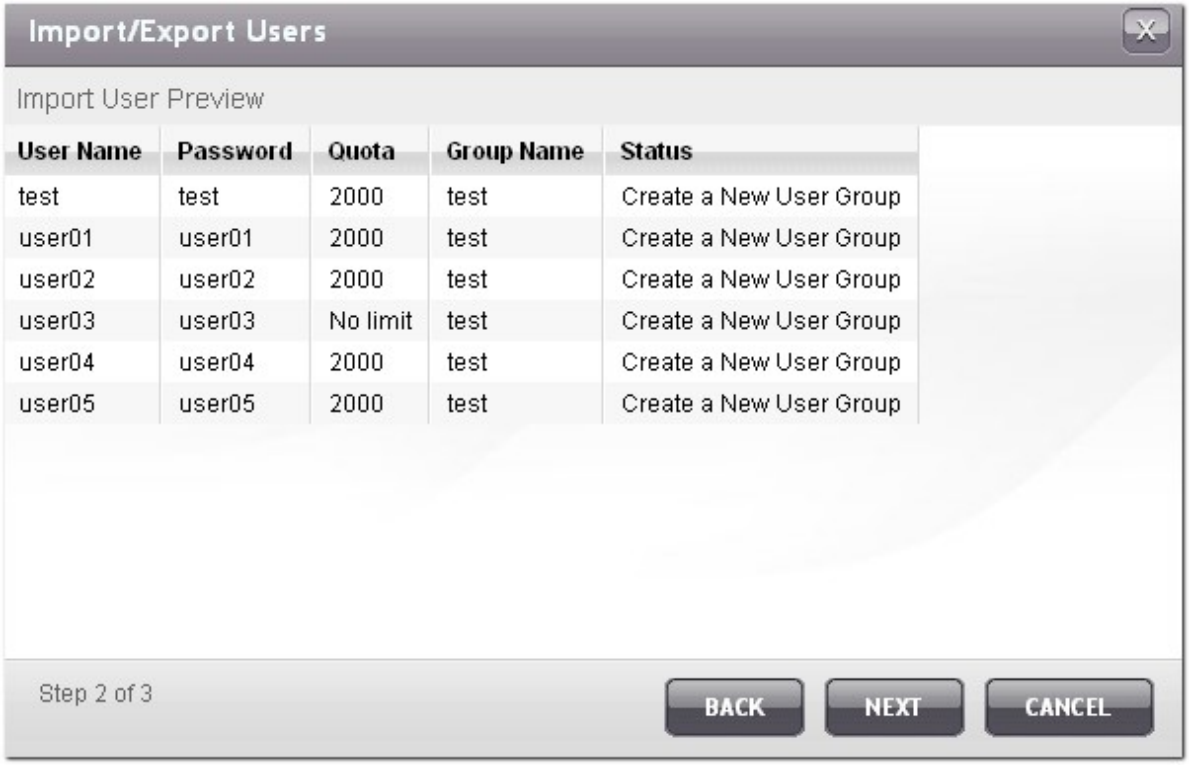
1. Click "Import/Export Users".



2. Select "Import user and user group settings". Select the option "Overwrite duplicate users" to overwrite existing users on the NAS.

3. Click "Browse" and select the file (*.txt, *.csv, *.bin) which contains the users information. Click "Next" to import the users.

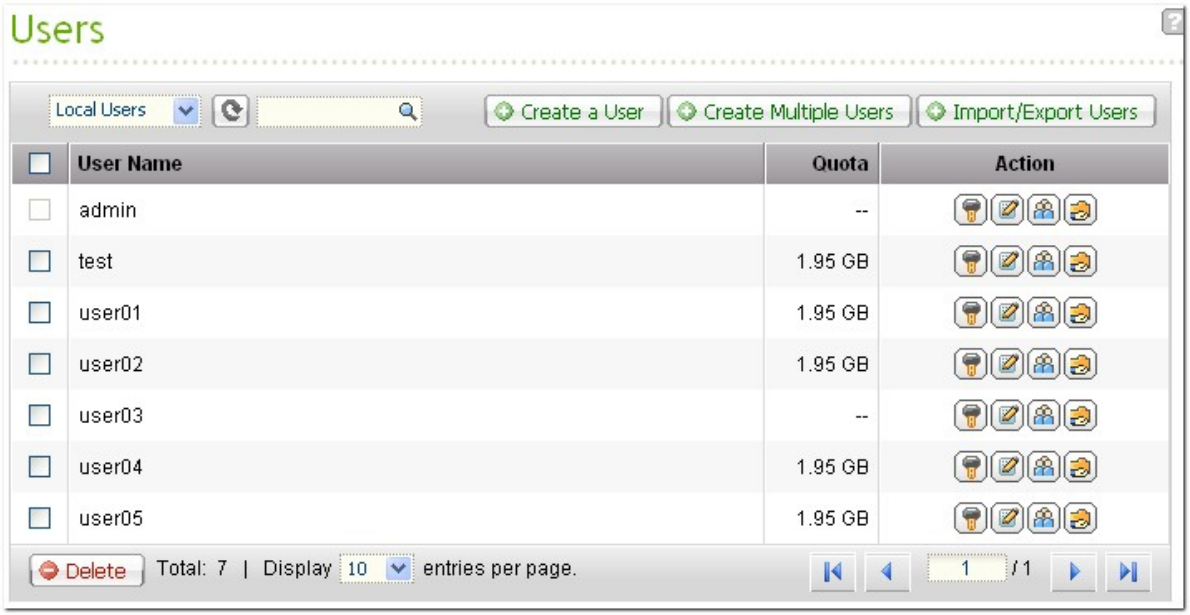
4. A list of imported users will be displayed. Any users with abnormal status, highlighted in red, will be skipped. Note that this step will not be shown if you import users by a BIN file.



5. Click "Next" to create the user accounts.

6. Click "Finish" after the users have been created.

7. The imported user accounts will be shown.

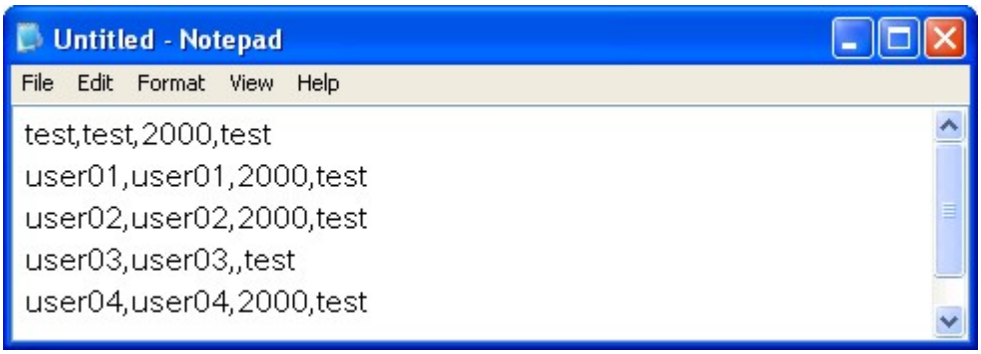


The NAS supports importing user accounts from TXT, CSV or BIN files. To create a list of user accounts with these file types, follow the steps below.

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

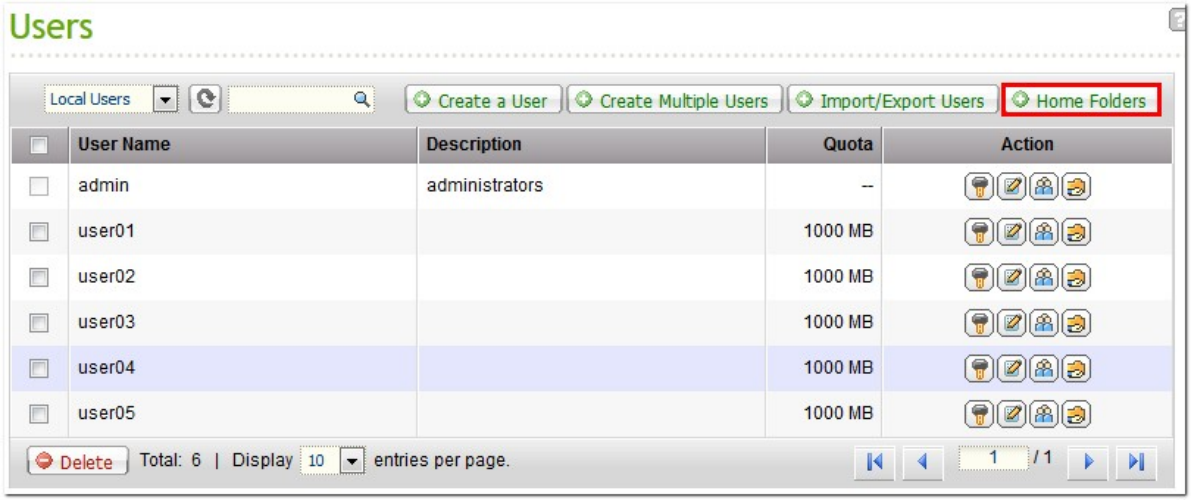
BIN (Exported from the NAS)

The BIN file is exported from a QNAP NAS. It contains information including user name, password, quota, and user group. The quota setting can be exported only when the quota function is enabled in "Access Right Management" > "Quota".

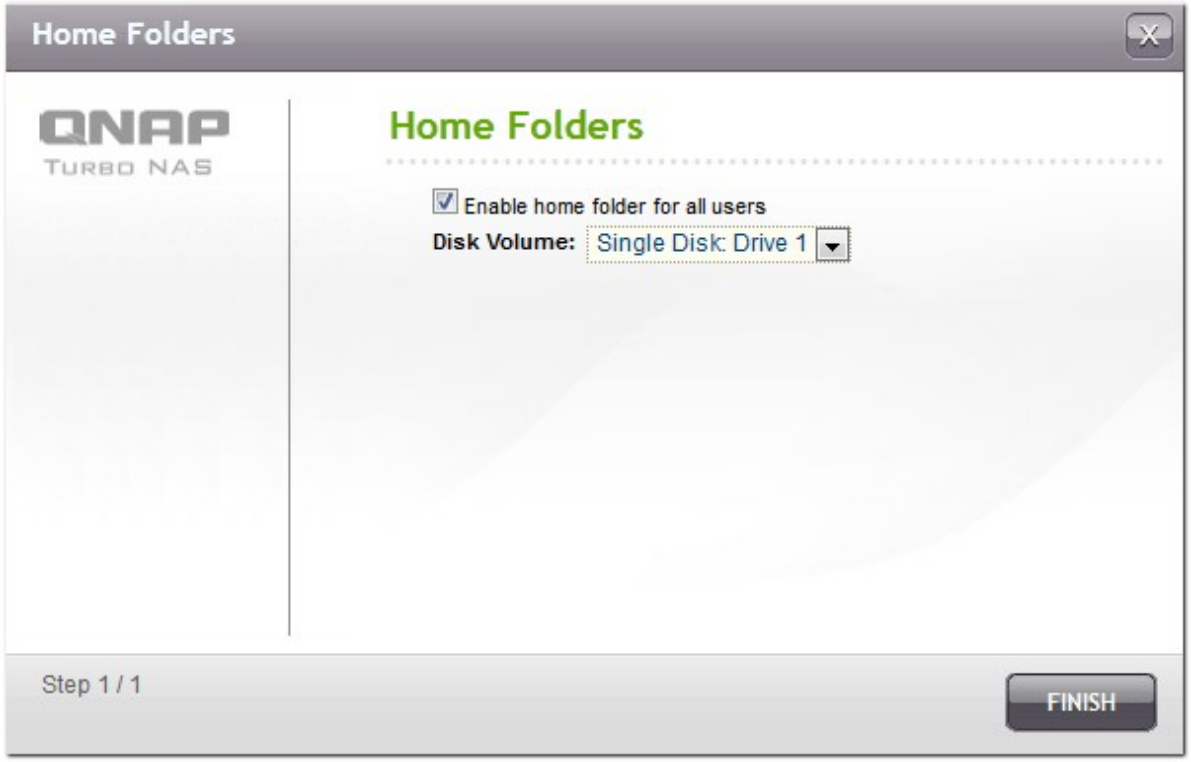
Home Folders

Enable Home Folders to create a personal folder to each local and domain user on the NAS. Users can access their folders "home" via Microsoft networking, FTP, AFP, and Web File Manager. All the home folders are located in the network share "Homes", which can only be accessed by "admin" by default.

To use this feature, click "Home Folders".



Select "Enable home folder for all users" and the disk volume where the home folders will be created in. Click "Finish".



5.3 User Groups

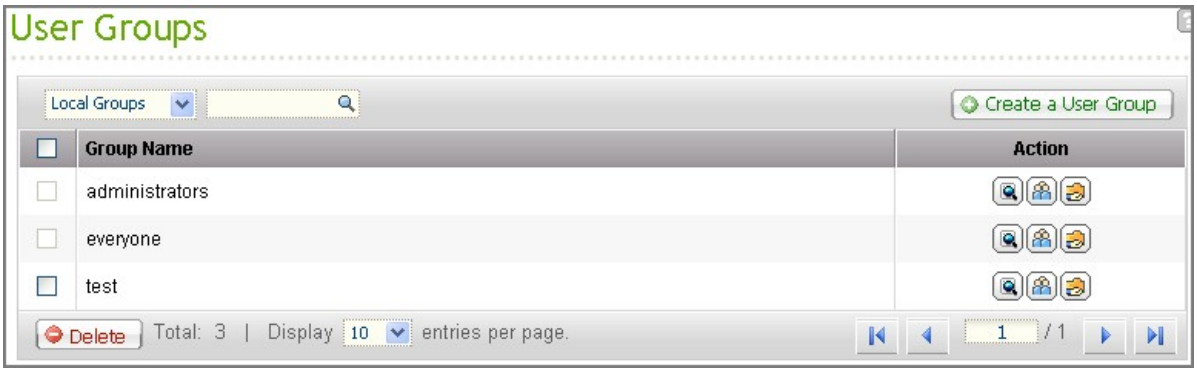
A user group is a collection of users with the same access right to the files or folders. The NAS has created the following user groups by default:

- administrators
  All the members in this group have the administration right of the NAS. This group cannot be deleted.
- everyone
  All the registered users belong to everyone group. This group cannot be deleted.

The number of user groups you can create on the NAS varies according to the NAS models. If your NAS models are not listed, please visit http://www.qnap.com for details.

Maximum number of user groups	NAS models
128	TS-110, TS-210
256	TS-112, TS-119, TS-119P+, TS-212, TS-219P+, TS-410, TS-239 Pro II+, TS-259 Pro+
512	TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP

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



5.4 Share Folders

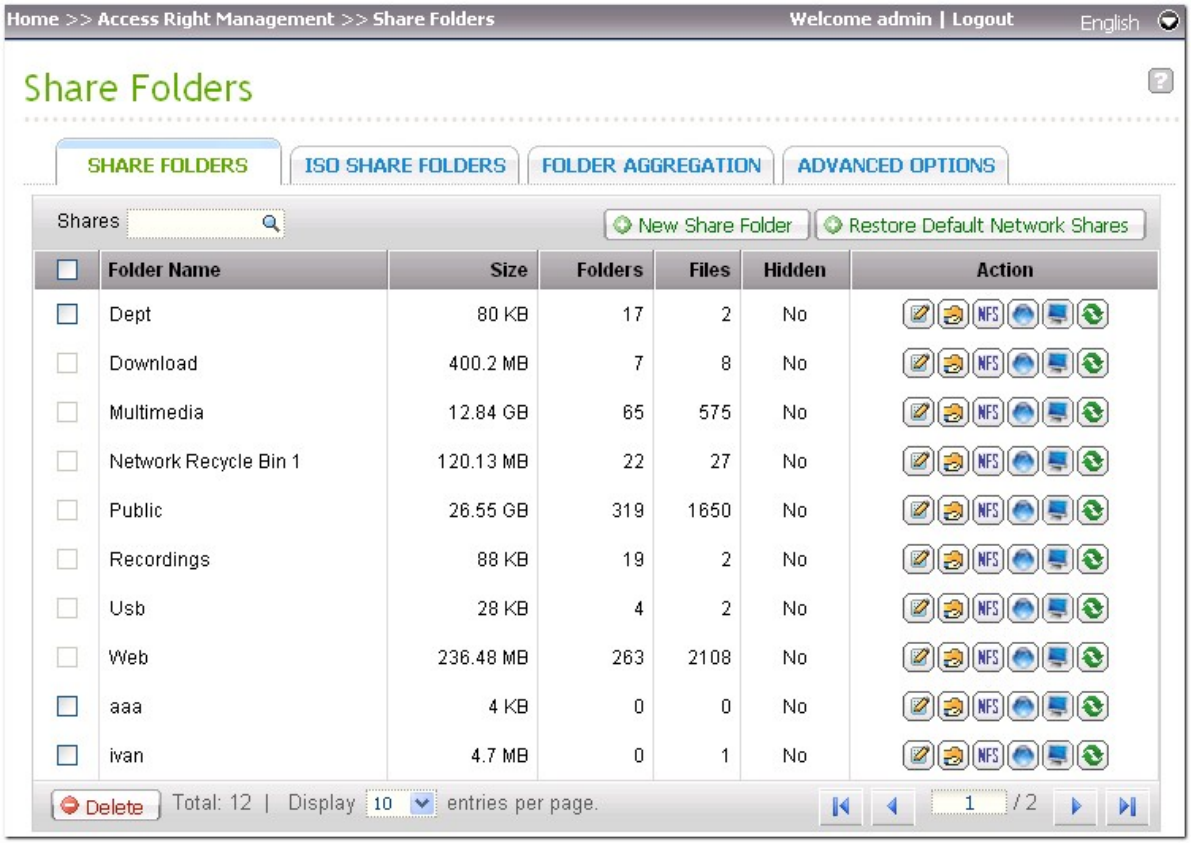
Share Folders

You can create multiple network shares on the NAS and specify the access rights of the users and user groups to the shares.

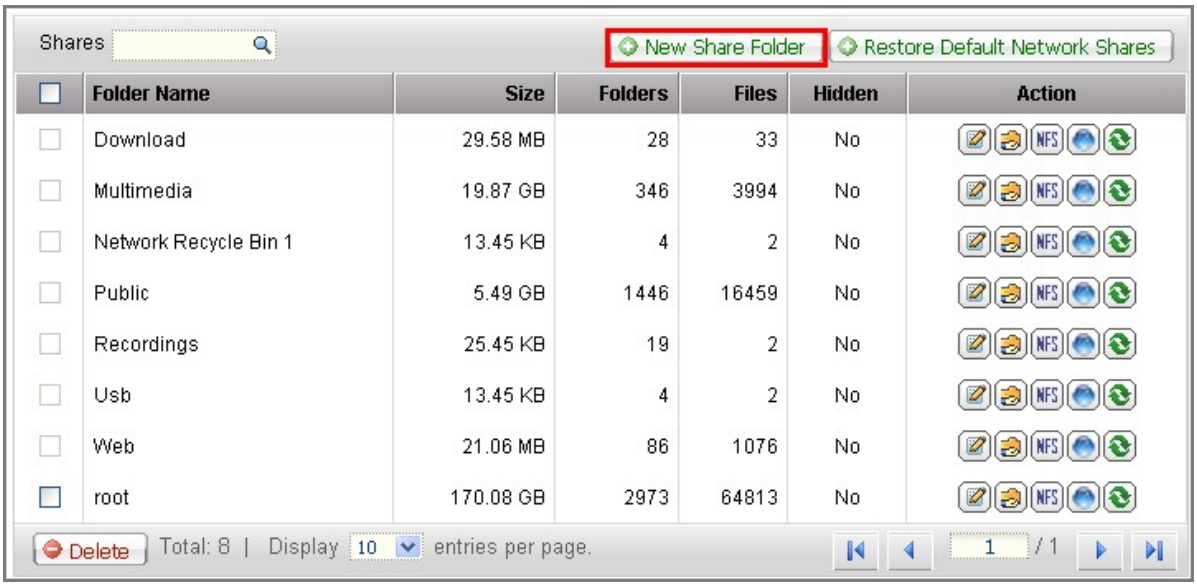
The number of network shares you can create on the NAS varies according to the NAS models. If your NAS models are not listed, please visit http://www.qnap.com for details.

Maximum number of network shares	NAS models
256	TS-110, TS-210, TS-112, TS-119, TS-119P+, TS-212, TS-219P+, TS-410, TS-239 Pro II+, TS-259 Pro+
512	TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP

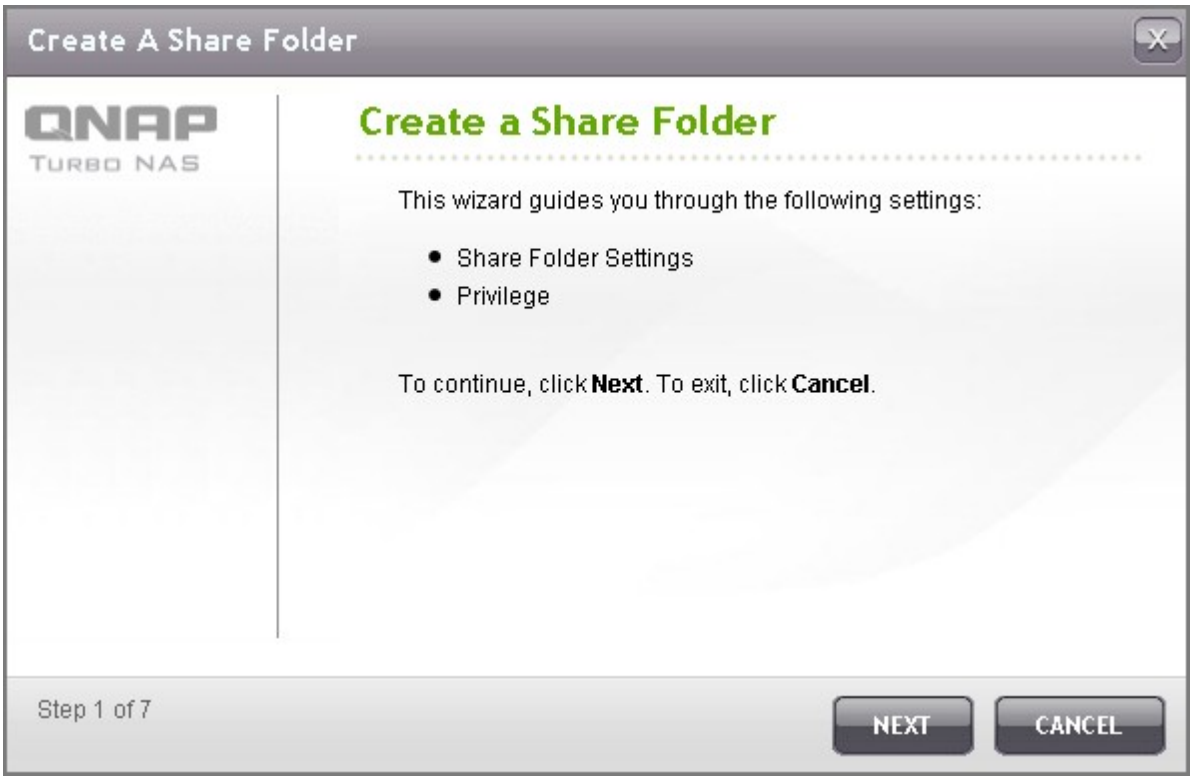
On the folder list, you can view the current data size, number of sub-folders and files created in the network share, and the folder status (hidden or not).



1. To create a network share, click “New Share Folder”.



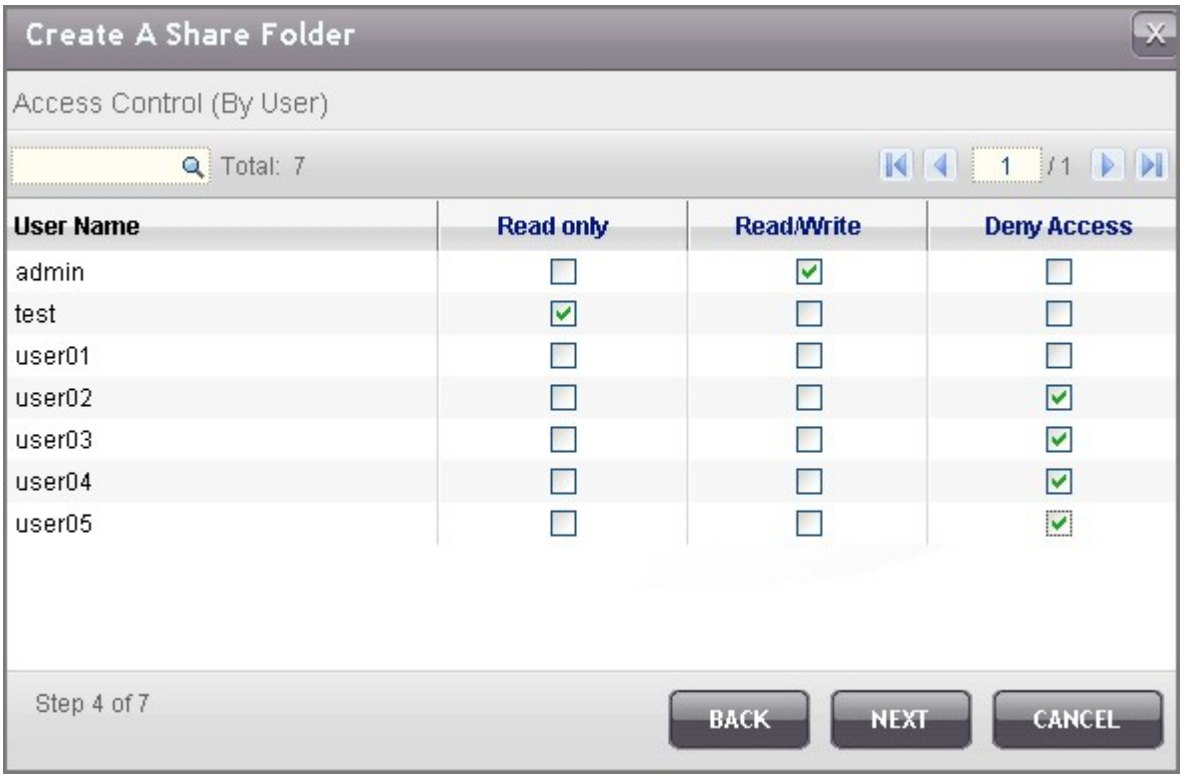
2. Click “Next”.



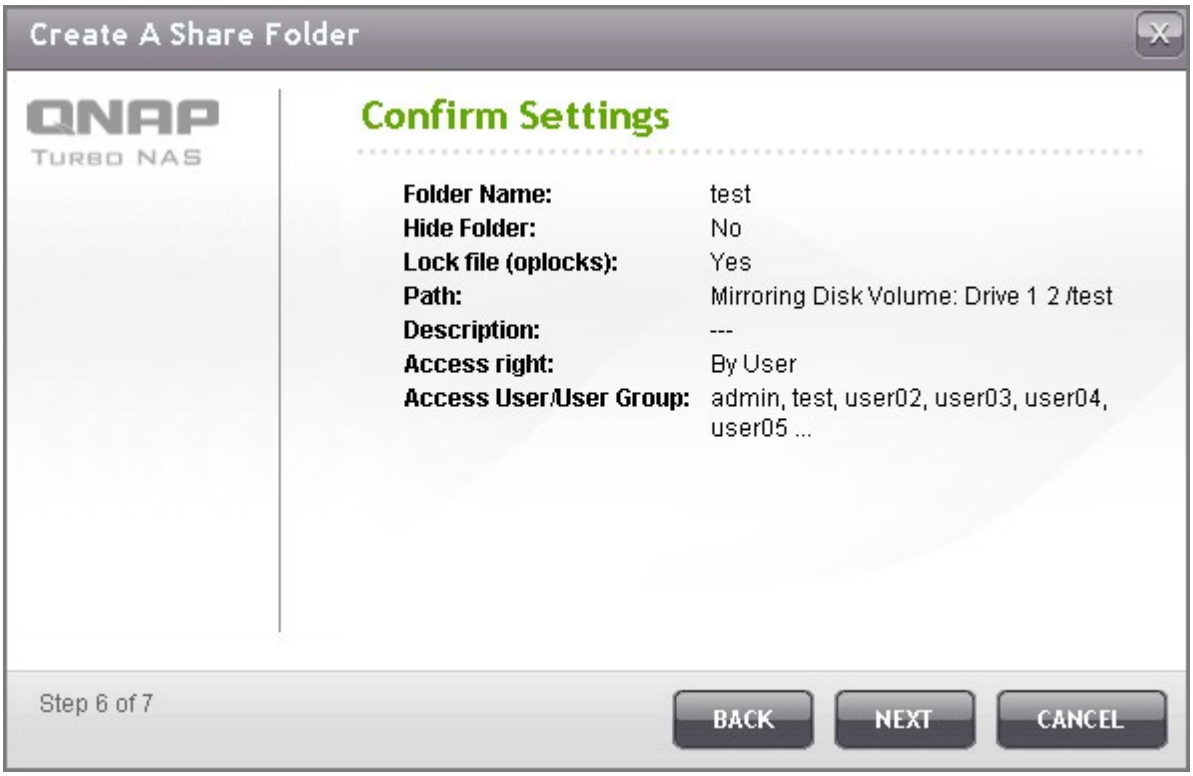
3. Enter the folder settings.
   - Folder name: Enter the share name. The share name does not support " / \ [ ] : ; | = , + * ? < > ` '
   - Hide Folder: Select to hide the network share or not in Microsoft Networking. When a network share is hidden, you have to enter the complete directory \\NAS_IP\share_name to access the share.
   - Lock file (oplocks): Opportunistic locking is a Windows mechanism for the client to place an opportunistic lock (oplock) on a file residing on a server in order to cache the data locally for improved performance. Oplocks is enabled by default for everyday usage. For networks that require multiple users concurrently accessing the same file such as a database, oplocks should be disabled.
   - Path: Specify the path of the network share or select to let the NAS specify the path automatically.
   - Description: Enter an optional description of the network share.

4. Select the way you want to specify the access right to the folder and specify the guest access right.

5. If you select to specify the access right by user or user group, you can select to grant read only, read/write, or deny access to the users or user groups.

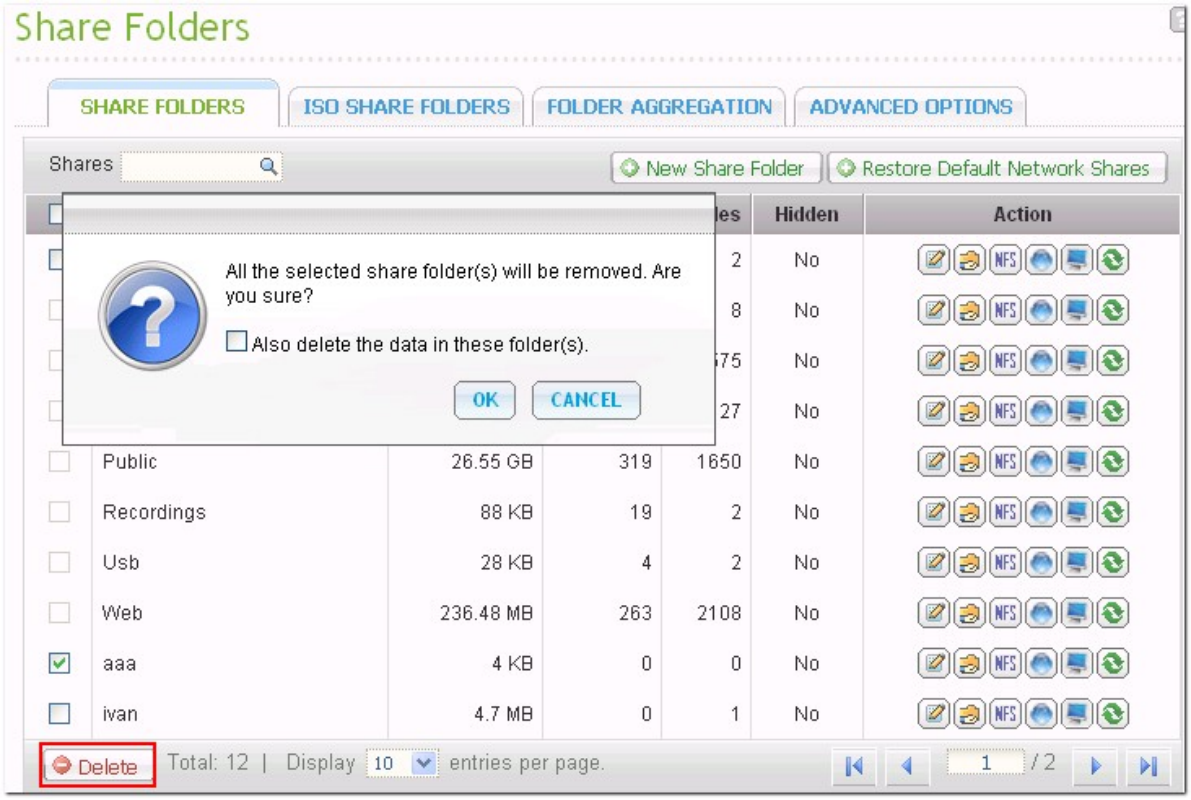


6. Confirm the settings and click “Next”.



7. Click "Finish" to complete the setup.

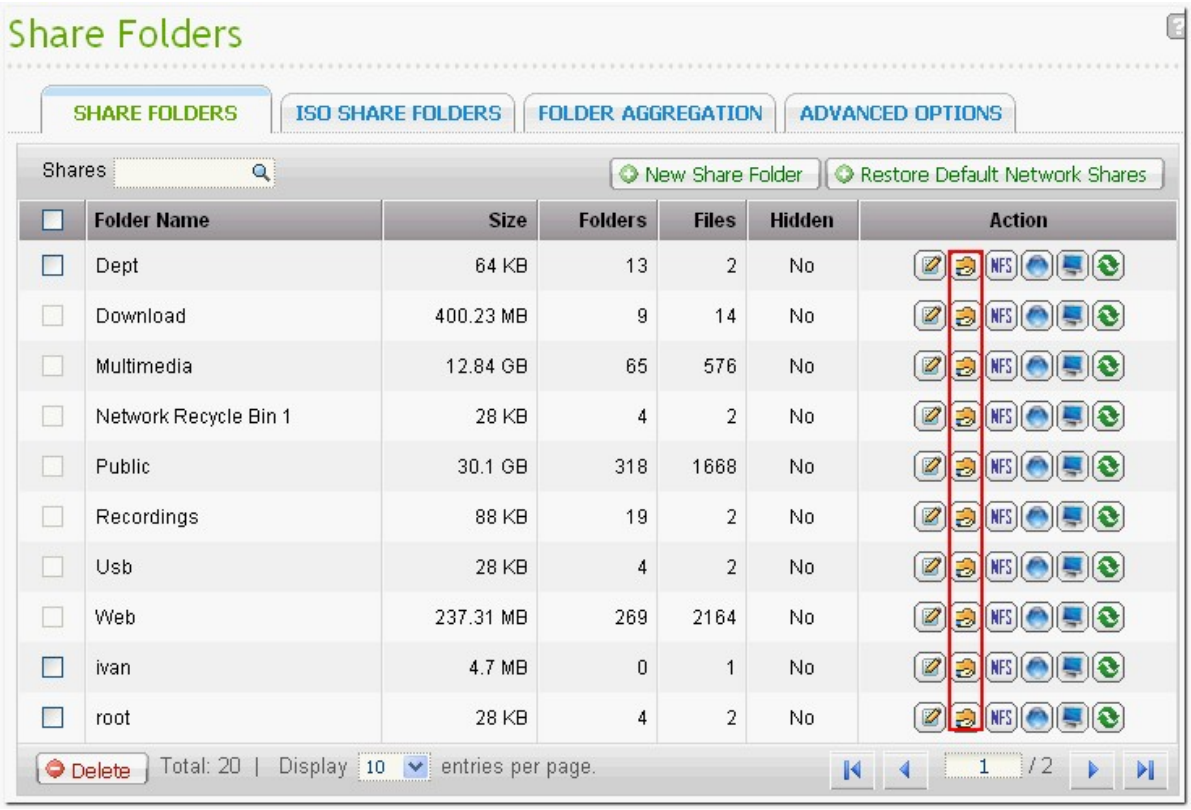
To delete a network share, select the folder checkbox and click "Delete". You can select the option "Also delete the data in these folder(s)" to delete the folder and the files in it. If you select not to delete the folder data, the data will be retained in the NAS. You can create a network share of the same name again to access the data.



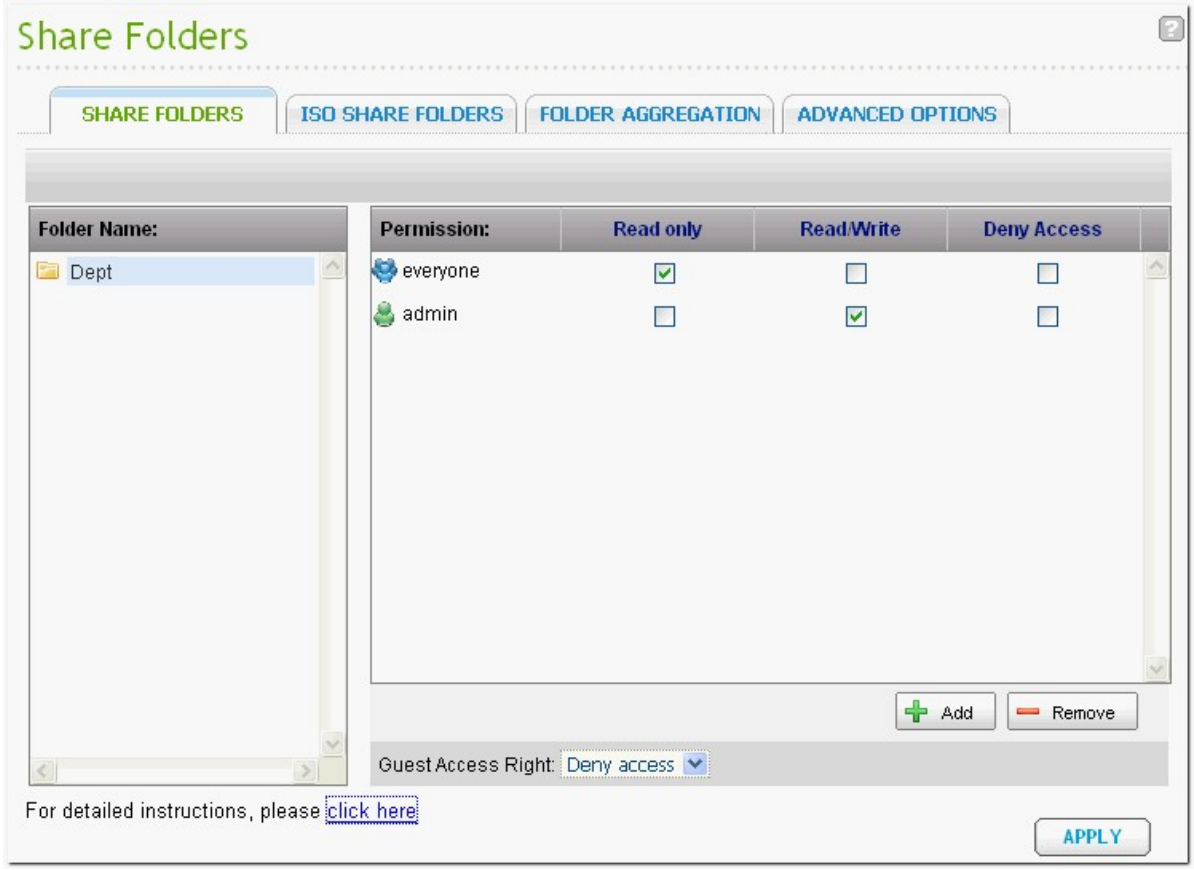
Icon	Description
(Folder property)	Edit the folder property. Select to hide or show the network share, enable or disable oplocks, folder path, comment, and enable or disable write-only access on FTP connection.
(Folder permissions)	Edit folder permissions and subfolder permissions.
(NFS access control)	Specify NFS access right to the network share. An asterisk (*) means all connections.
(WebDAV access control)	Specify WebDAV access right to the network share.
(Microsoft Networking host access control)	Enter the host names or IP addresses which are allowed to connect to the network share via Microsoft Networking. Note that a user still needs a correct login name and password to access the share via Microsoft Networking.
(Refresh)	Refresh the network share details.

Folder Permissions

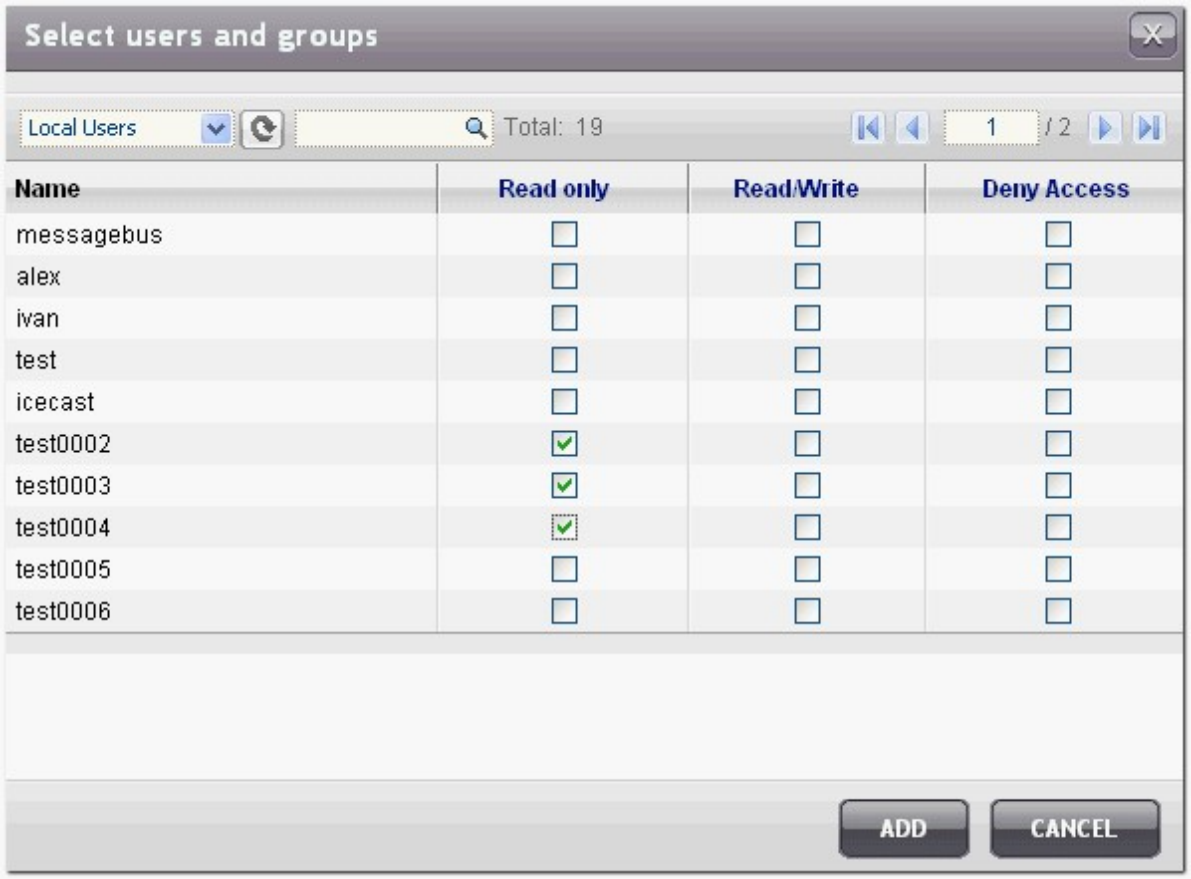
Configure folder and subfolder permissions on the NAS. To edit basic folder permissions, locate a folder name in “Access Right Management” > “Share Folders” and click .



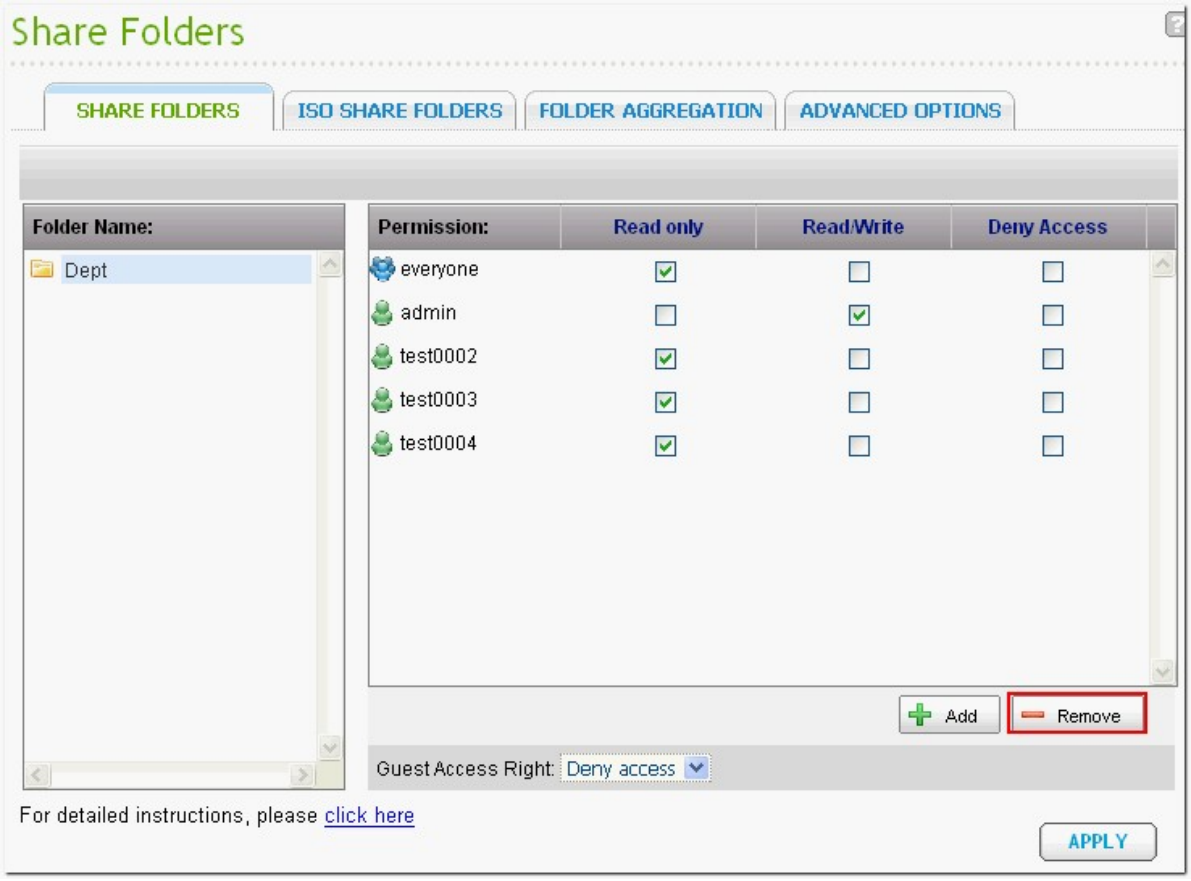
The folder name will be shown on the left and the users with configured access rights are shown in the panel. You can also specify the guest access right at the bottom of the panel.



Click "+ Add" to select more users and user groups and specify their access rights to the folder. Click "ADD" to confirm.



Click "– Remove" to remove any configured permissions. You can select multiple items by holding the Ctrl key and left clicking the mouse. Click "Apply" to save the settings.

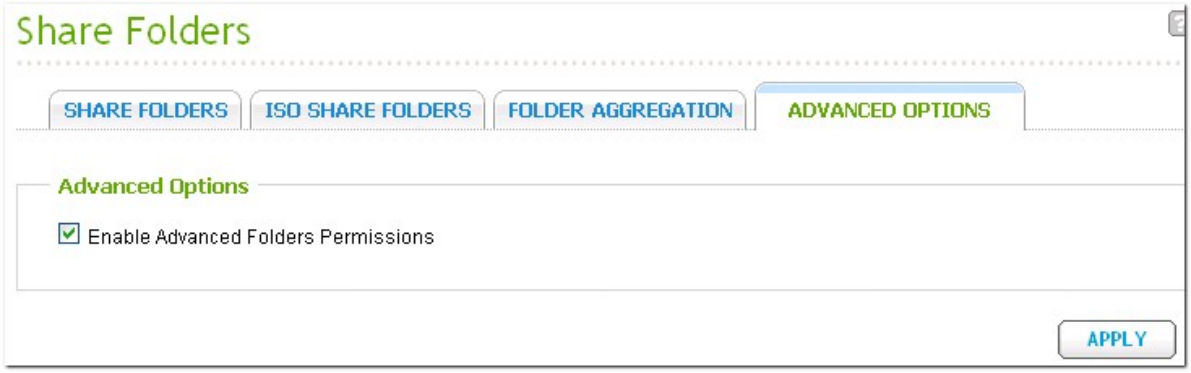


Subfolder Permissions

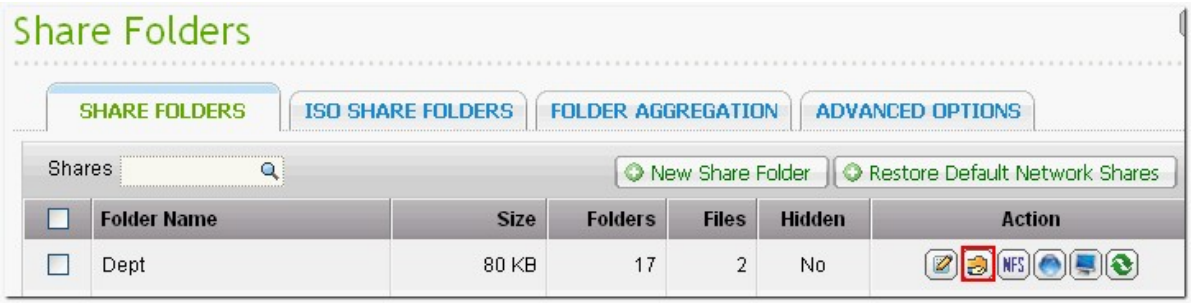
The NAS supports subfolder permissions for secure management of the folders and subfolders. You can specify read, read/write, and deny access of individual user to each folder and subfolder.

To configure subfolder permissions, go to "Access Right Management" > "Share Folders" > "Advanced Options" tab. Select "Enable Advanced Folder Permissions" and click "Apply".

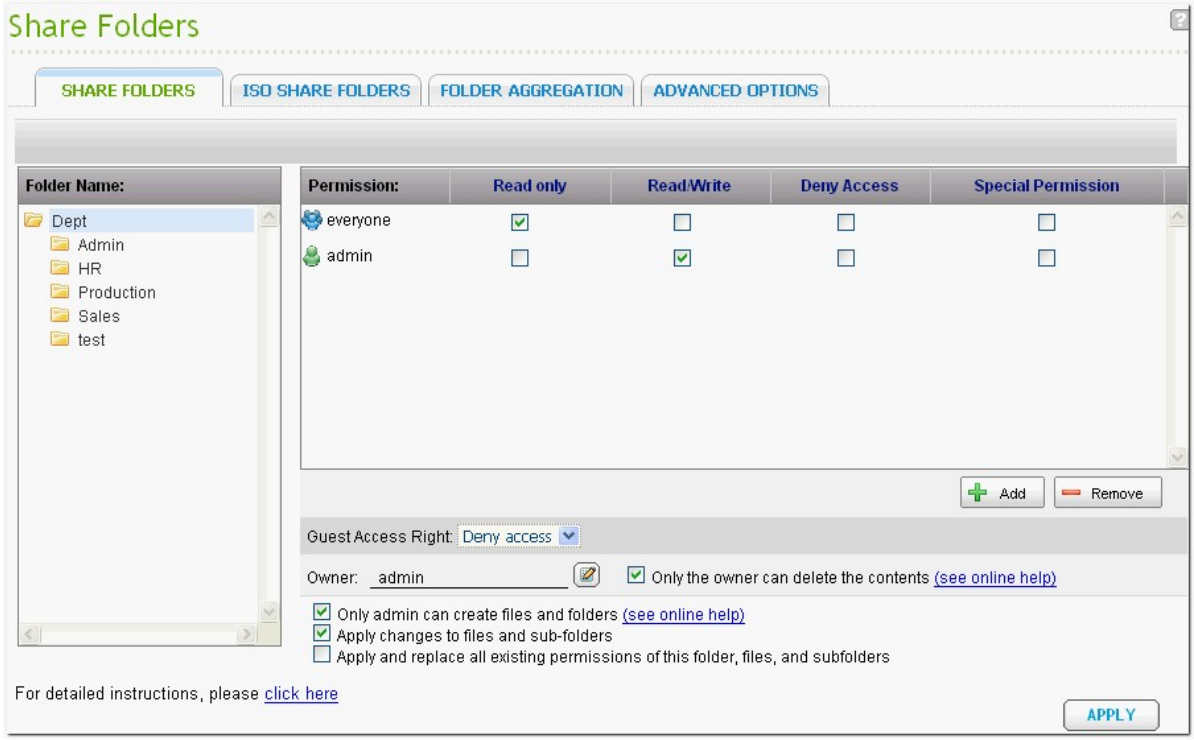
> **Note:** You can create maximum 230 permission entries for each folder when Advanced Folder Permission is enabled.



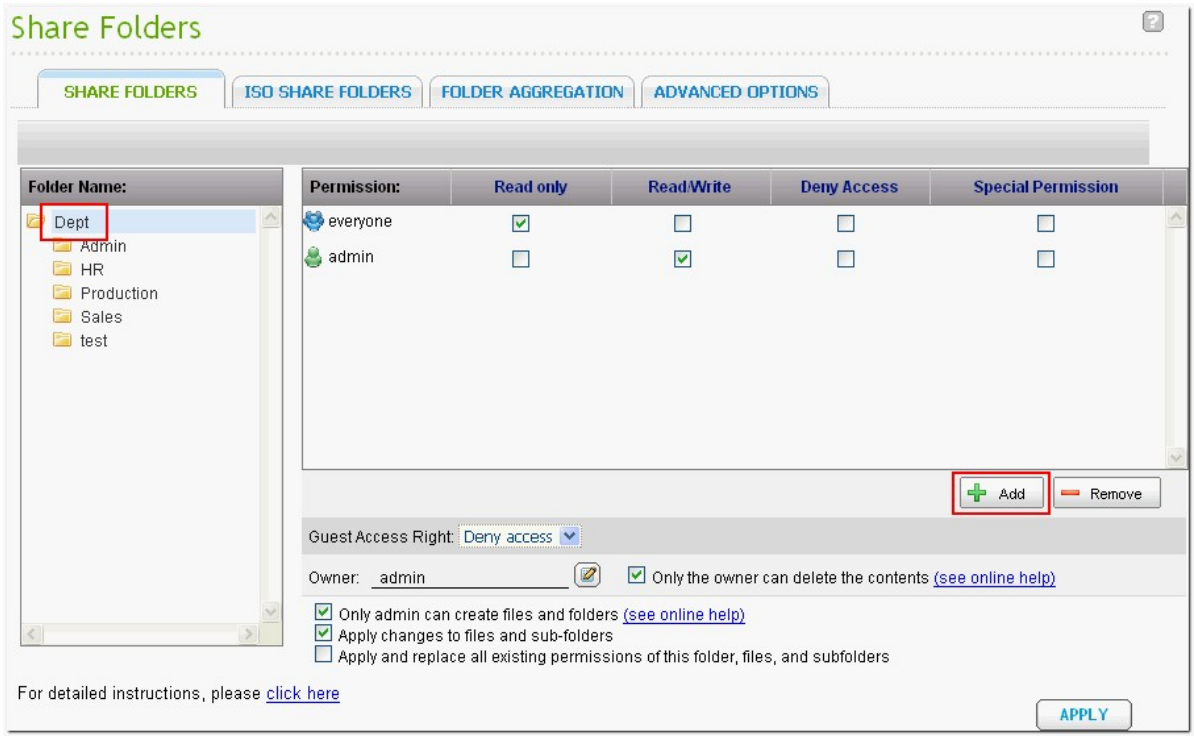
Go to "Access Right Management" > "Share Folders" > "Share Folders" tab. Select a root folder, for example Dept, and click .



The network share name and its first-level subfolders are shown on the left. The users with configured access rights are shown in the panel, with special permission below. Double click the first-level subfolders to view the second-level subfolders.



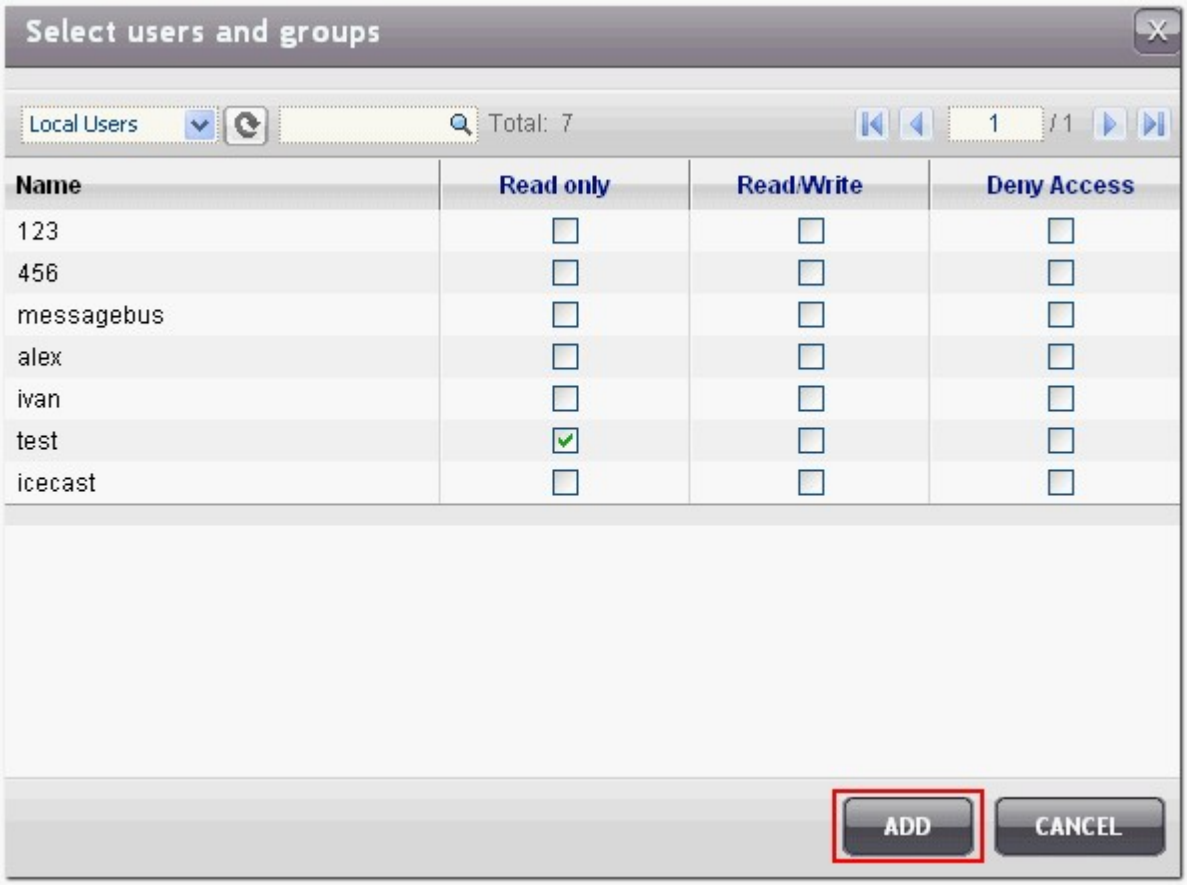
Select the root folder (Dept). Click "+ Add" to specify read only, read/write, or deny access for the users and user groups.



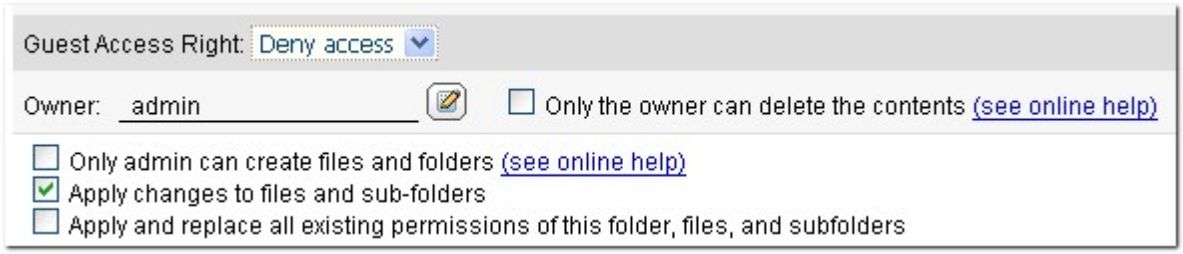
Note:

- If you have specified "deny access" for a user on the root folder, the user will not be allowed to access the folder and subfolders even if you select read/write access to the subfolders.
- If you have specified "read only access" for a user on the root folder, the user will have read only access to all the subfolders even if you select read/write access to the subfolders.
- To specify read only permission on the root folder and read/write permission on the subfolders, you must set read/write permission on the root folder and use the option "Only admin can create files and folders" (to be explained later).

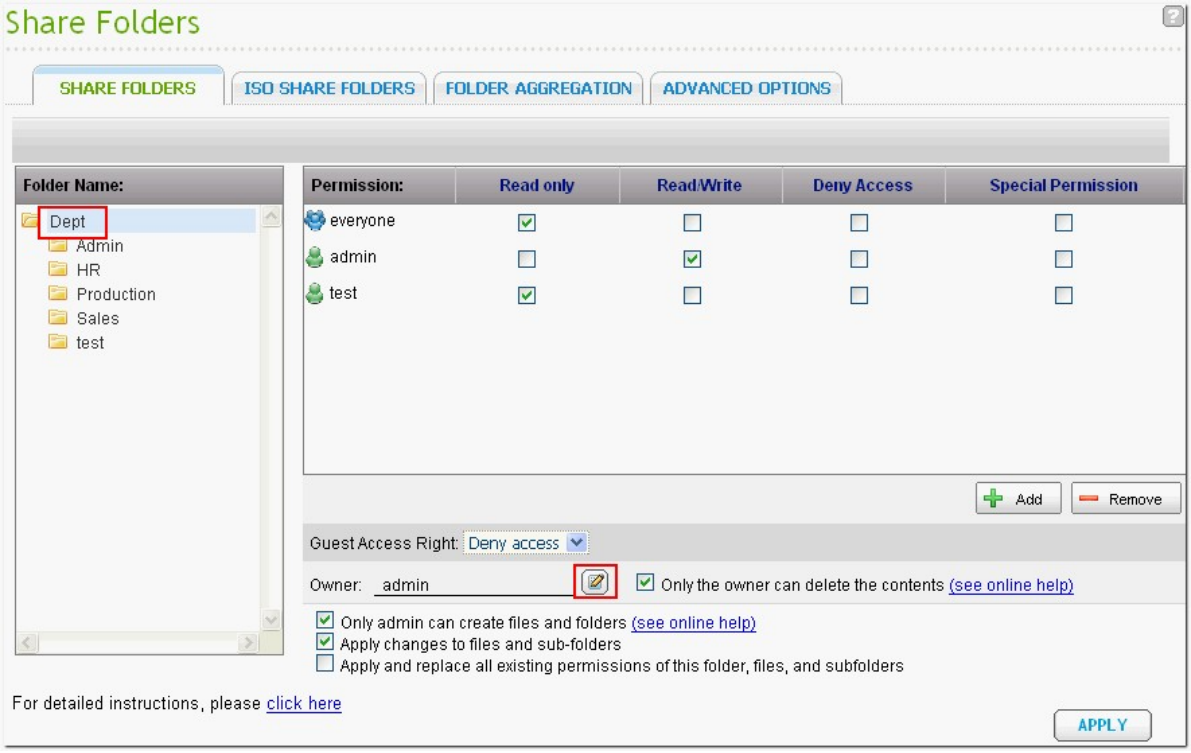
Click "ADD" when you have finished the settings.



Specify other permissions settings below the folder permissions panel.

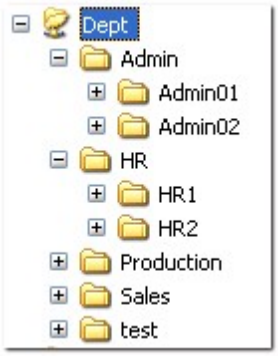


- Guest Access Right: Specify to grant full or read only access or deny guest access.
- Owner: Specify the owner of the folder. By default, the folder owner is the creator. To change the folder owner, click .



Select a user from the list or search a user name. Then click "Set".

- Only the owner can delete the contents
  When you apply this option to a folder, e.g. Dept, only the folder owner can delete the first-level subfolders and files. Users who are not the owner but possess read/write permission to the folder cannot delete the folders Admin, HR, Production, Sales, and test in this example. This option does not apply to the subfolders of the selected folder even if the options "Apply changes to files and subfolders" and "Apply and replace all existing permissions of this folder, files, and subfolders" are selected.



- Only admin can create files and folders: This option is only available for root folders. Select this option to allow admin to create first-level subfolders and files in the selected folder only. For example, in the folder "Dept", only admin can create files and subfolders Admin, HR, Production, and so on. Other users with read/write access to Dept can only create files and folders in the second and lower-level subfolders such as Admin01, Admin02, HR1, and HR2.

- Apply changes to files and subfolders: Apply permissions settings except owner protection and root folder write protection settings to all the files and subfolders within the selected folder. These settings include new users, deleted users, modified permissions, and folder owner. The options "Only the owner can delete the contents" and "Only admin can create files and folders" will not be applied to subfolders.

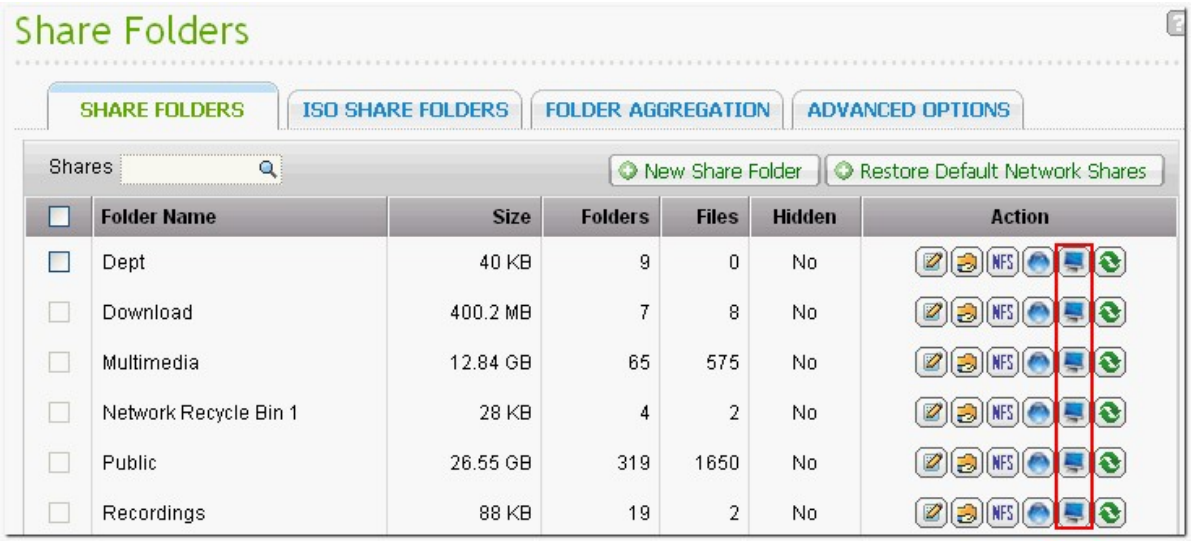
- Apply and replace all existing permissions of this folder, files, and subfolders: Select this option to override all previously configured permissions of the selected folder and its files and subfolders except owner protection and root folder write protection settings. The options "Only the owner can delete the contents" and "Only admin can create files and folders" will not be applied to subfolders.

- Special Permission: This option is only available for root folders. Select this option and choose between "Read only" or "Read/Write" to allow a user to access to all the contents of a folder irrespectively of the pre-configured permissions. A user with special permission will be identified as "admin" when he/she connects to the folder via Microsoft Networking. If you have granted special permission with "Read/Write" access to the user, the user will have full access and is able to configure the folder permissions on Windows. Note that all the files created by this user belong to "admin". Since "admin" does not have quota limit on the NAS, the number and size of the files created by users with special permission will not be limited by their pre-configured quota settings. This option should be used for administrative and backup tasks only.

After changing the permissions, click "Apply" and then "YES" to confirm.

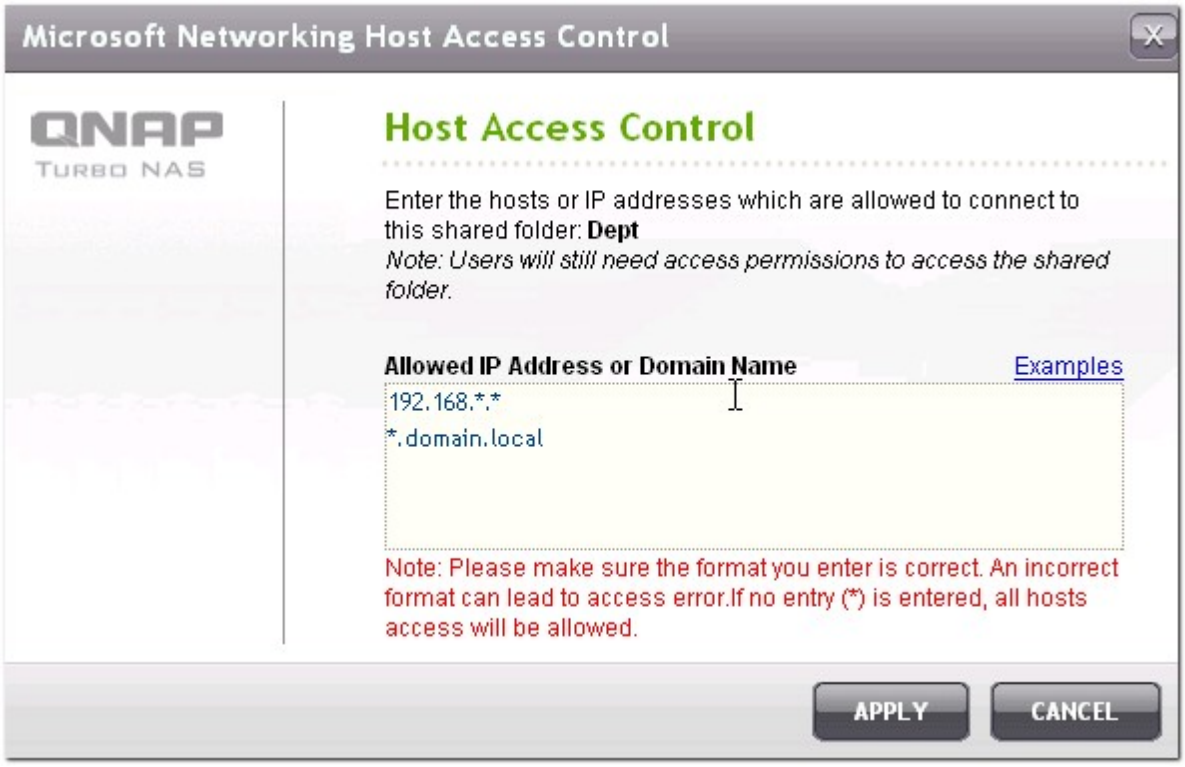
Microsoft Networking Host Access Control

The NAS folders can be accessed via Samba connection (Windows) by default. You can specify the IP addresses and hosts which are allowed to access the NAS via Microsoft Networking. Click to edit the host access control of a folder.



A wizard will be shown. Enter the allowed IP addresses and host names. For example:

IP address	192.168.12.12 192.168.*.*
Host name	dnsname.domain.local *.domain.local



Wildcard characters

You can enter wildcard characters in an IP address or host name entry to represent unknown characters.

Asterisk (*)

Use an asterisk (*) as a substitute for zero or more characters. For example, if you enter *.domain.local, the following items are included:

a.domain.local

cde.domain.local

test.domain.local

Question mark (?)

Use a question mark (?) as a substitute for only one character. For example, test?.domain.local includes the following:

test1.domain.local

test2.domain.local

testa.domain.local

When you use wildcard characters in a valid host name, dot (.) is included in wildcard characters. For example, when you enter *.example.com, "one.example.com" and "one.two.example.com" are included.

ISO Share Folders

You can mount the ISO image files on the NAS as ISO shares and access the contents without disc burning. The NAS supports mounting up to 256 ISO shares.

*TS-110, TS-119, TS-210, TS-219, TS-219P, TS-410, TS-119P+, TS-219P+, TS-112, TS-212 support maximum 256 network shares only (including 6 default network shares). The maximum number of ISO image files supported by these models is less than 256 (256 minus 6 default shares minus number of network recycle bin folders).

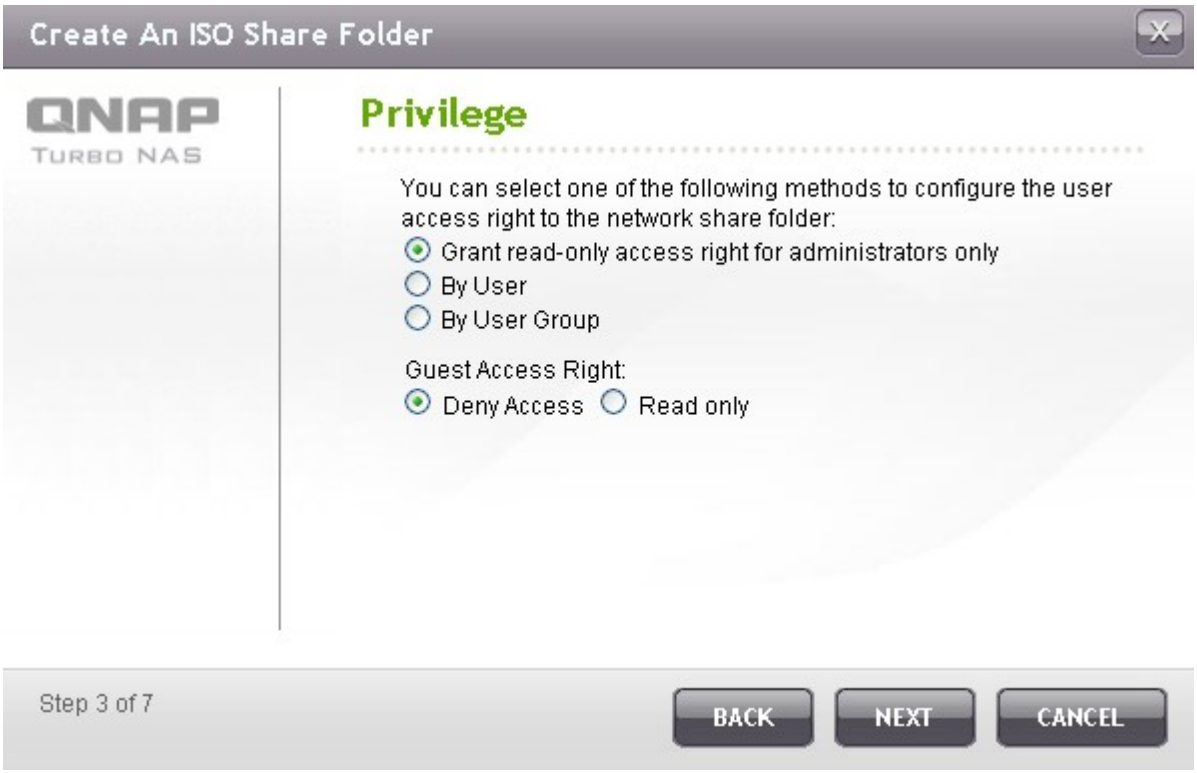
Follow the steps below to mount an ISO file on the NAS by the web interface.

1. Login the NAS as an administrator. Go to "Share Folders" > "ISO SHARE FOLDERS". Click "Mount An ISO File".

2. Select an ISO image file on the NAS. Click "Next".

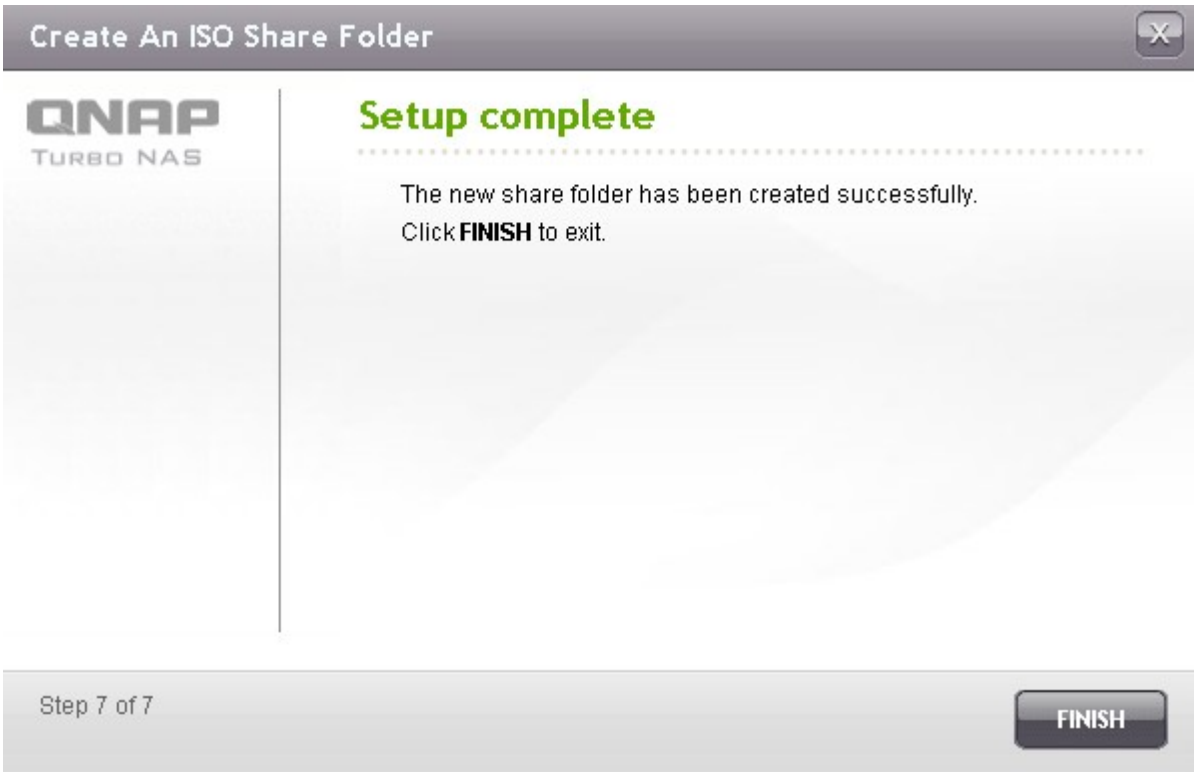
3. The image file will be mounted as a network share of the NAS. Enter the folder name.

4. Specify the access rights of the NAS users or user groups to the network share. You can also select "Deny Access" or "Read only" for the guest access right. Click "Next".

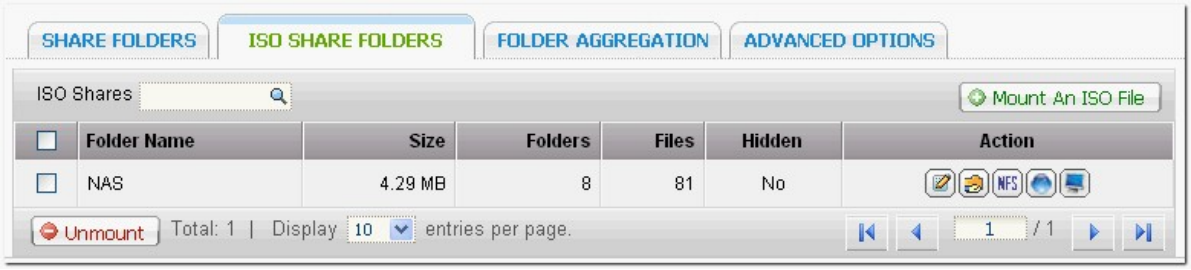


5. Confirm the settings and click “Next”.

6. Click “Finish”.



7. After mounting the image file, you can specify the access rights of the users over different network protocols such as SMB, AFP, NFS, and WebDAV by clicking the icons in the "Action" column.



The NAS supports mounting ISO image files by Web File Manager, see here 311 for more information.

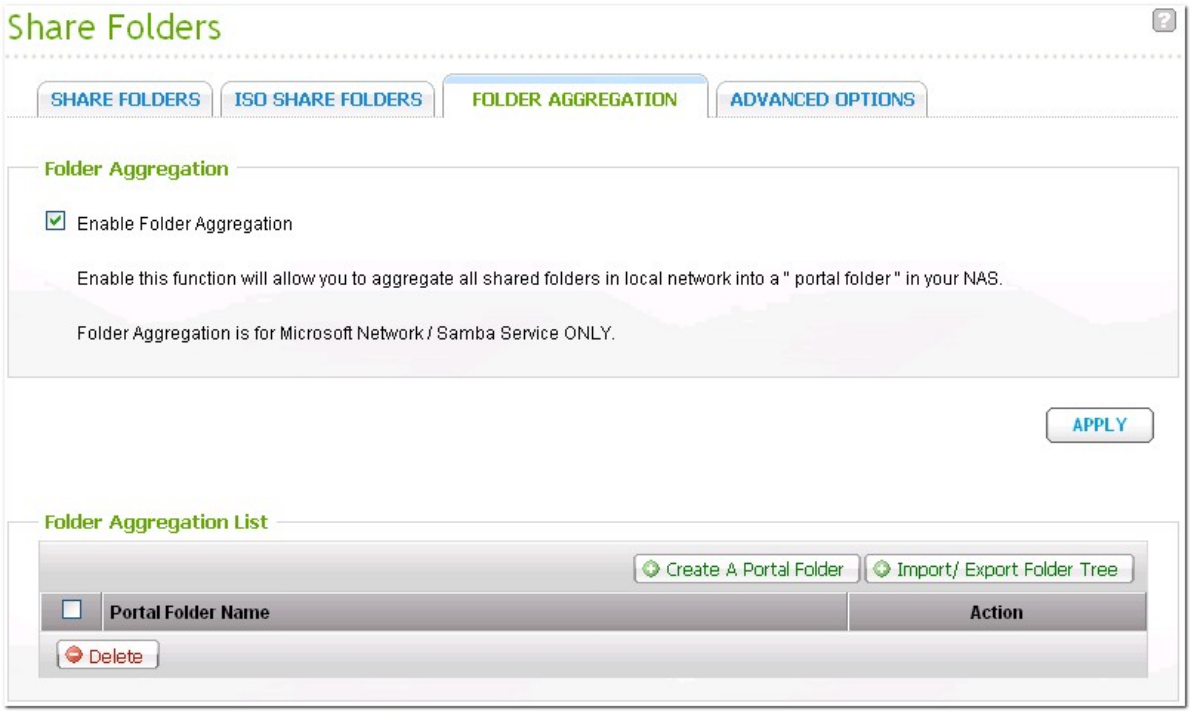
Folder Aggregation

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

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

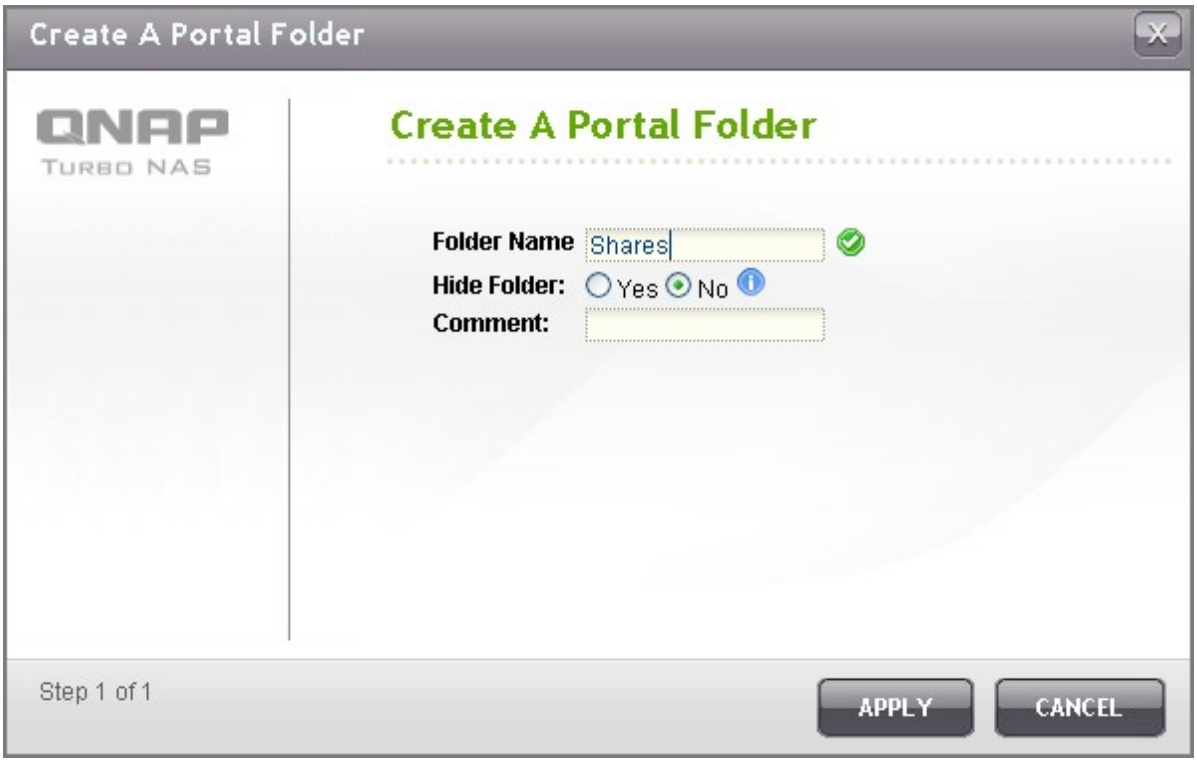
To use this function, follow the steps below.

1. Enable folder aggregation.



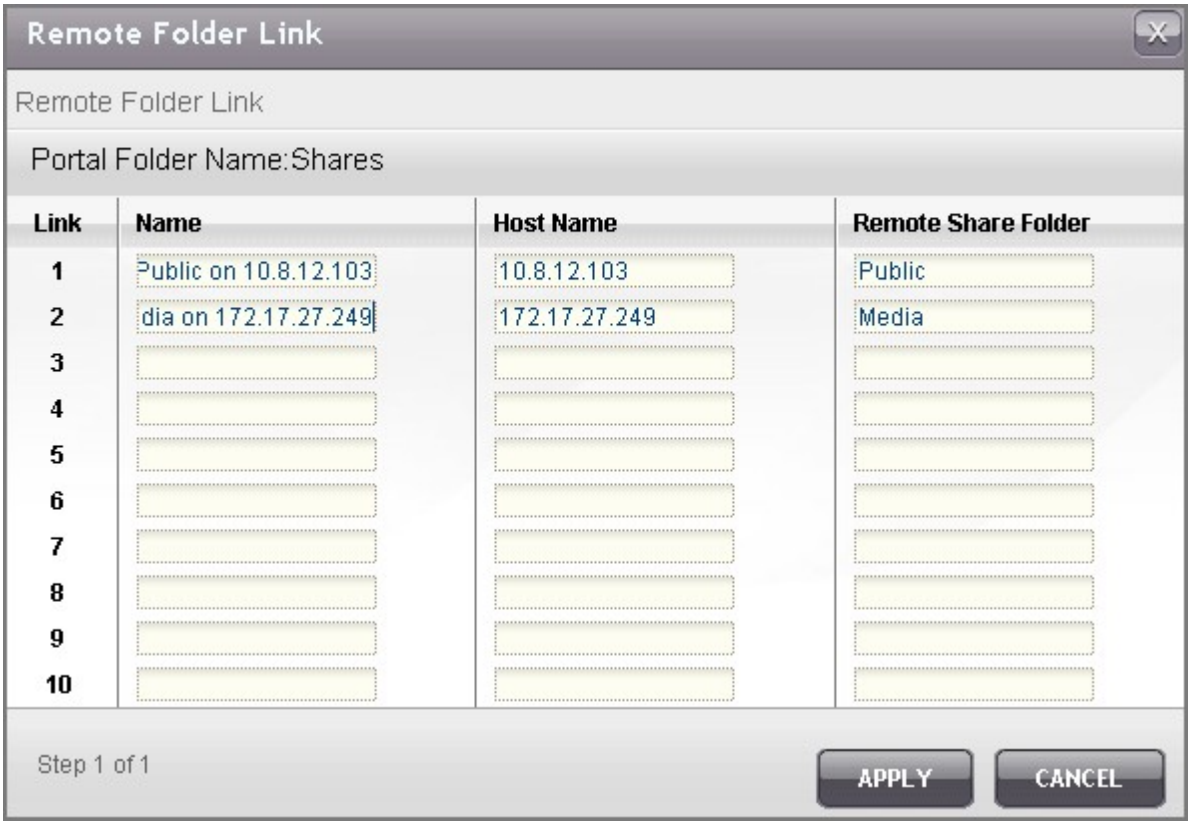
2. Click "Create A Portal Folder".

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

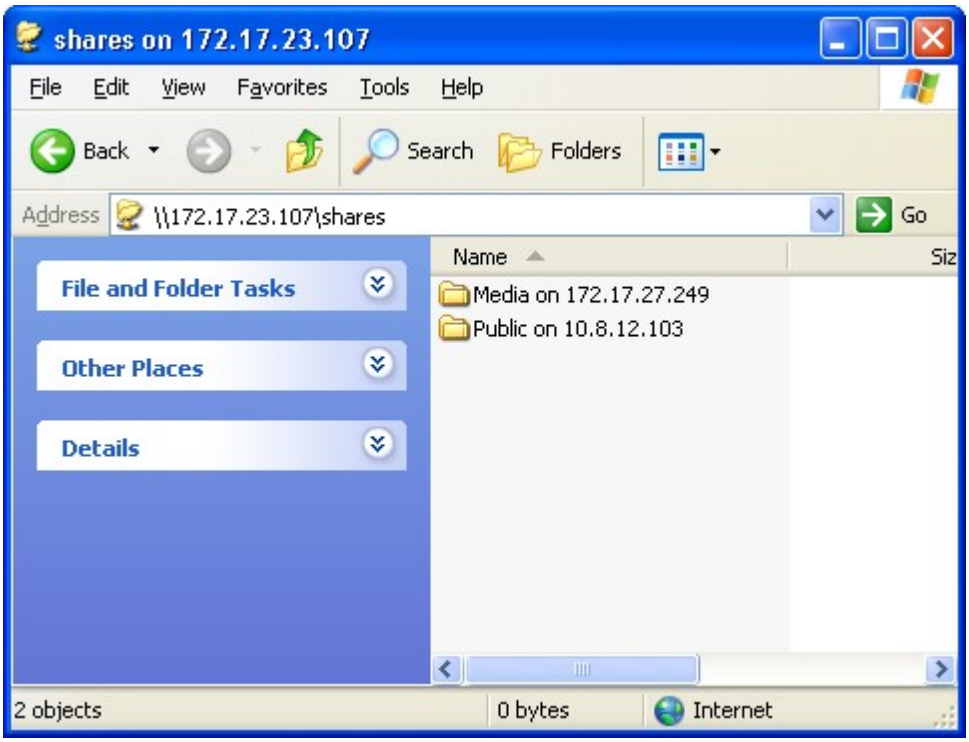


4. Click (Link Configuration) and enter the remote folder settings. Make sure the folders are open for public access.

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

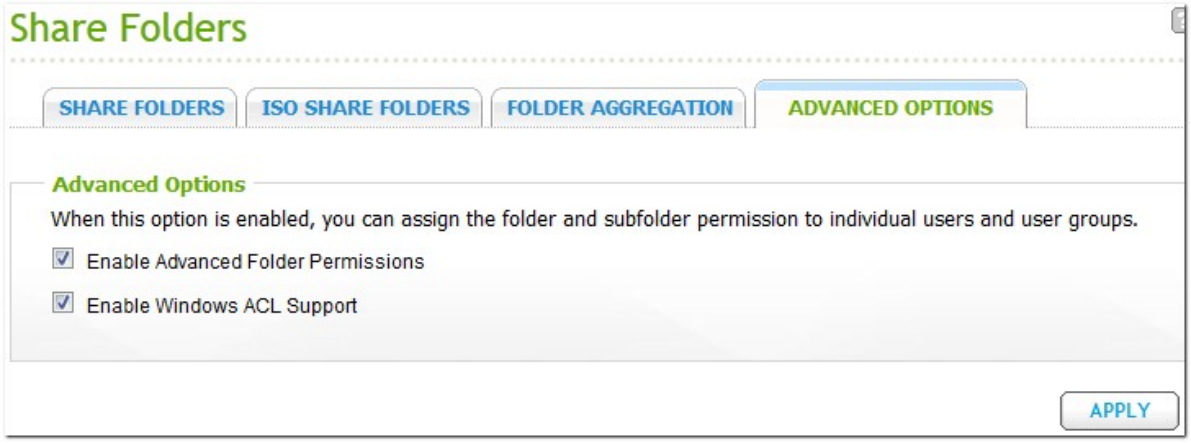


5. Upon successful connection, you can connect to the remote folders through the NAS.



Advanced Options

"Advanced Folder Permissions" and "Windows ACL" provide subfolder and file level permissions control. They can be enabled independently or together.



Protocols	Permission	Options	How to Configure
Advanced Folder Permissions	FTP, AFP, Web File Manager, Samba	3 (Read, Read & Write, Deny)	NAS web UI
Windows ACL	Samba	13 (NTFS permissions)	Windows File Explorer
Both	FTP, AFP, Web File Manager, Samba	Please see the application note (http://www.qnap.com/index.php?lang=en&sn=4686) for more details.	Windows File Explorer

Advanced Folder Permissions

Use "Advanced Folder Permissions" to configure subfolder permissions directly from the NAS UI. There is no depth limitation for the subfolder permissions. However, it is highly recommended to change the permissions only on the first or second level of the subfolders. When "Advanced Folder Permissions" is enabled, click the "Folder Permissions" icon under the "Share Folders" tab to configure the subfolder permission settings. See "Share Folders" > "Folder Permission"231 of this section for details.

Windows ACL

Use "Windows ACL" to configure the subfolder and file level permissions from Windows File Explorer. All Windows Permissions are supported. For detailed Windows ACL behavior, please refer to standard NTFS permissions: http://www.ntfs.com/#ntfs_permiss

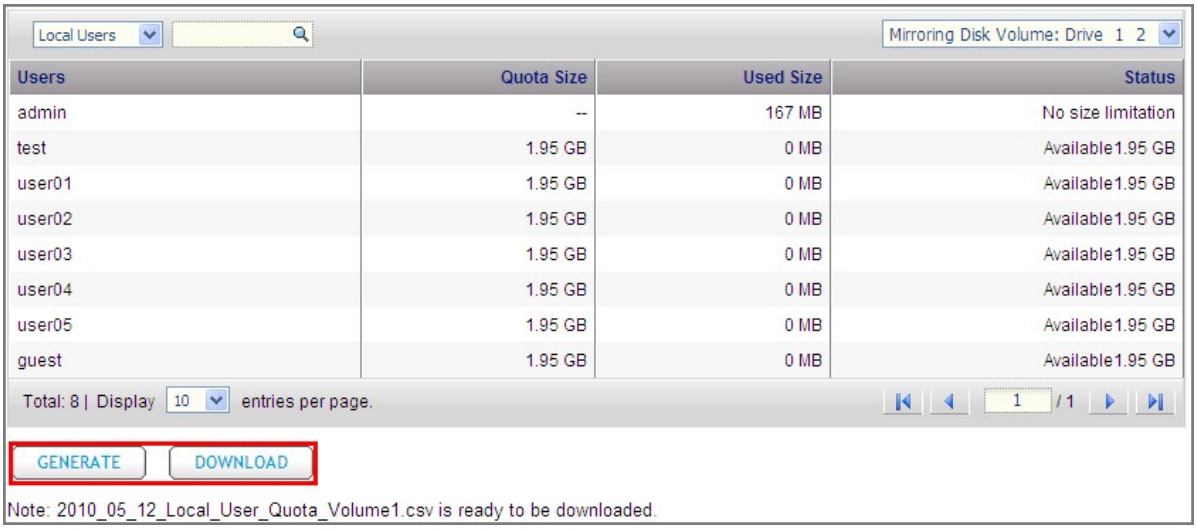
- To assign subfolder and file permissions to a user or a user group, full control share-level permissions must be granted to the user or user group.
- When Windows ACL is enabled while "Advanced Folder Permissions" are disabled, subfolder and file permissions will have effect only when accessing the NAS from Windows File Explorer. Users connecting to the NAS via FTP, AFP, or Web File Manager will only have share-level permissions.
- When Windows ACL and Advanced Folder Permissions are both enabled, users cannot configure Advanced Folder Permissions from the NAS UI. The permissions (Read only, Read/Write, and Deny) of Advanced Folder Permissions for AFP, Web File Manager, and FTP will automatically follow Windows ACL configuration.

5.5 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 options:

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

After applying the changes, the quota settings will be shown. Click "GENERATE" to generate a quota settings file in CSV format. After the file has been generated, click "DOWNLOAD" to save it to your specified location.



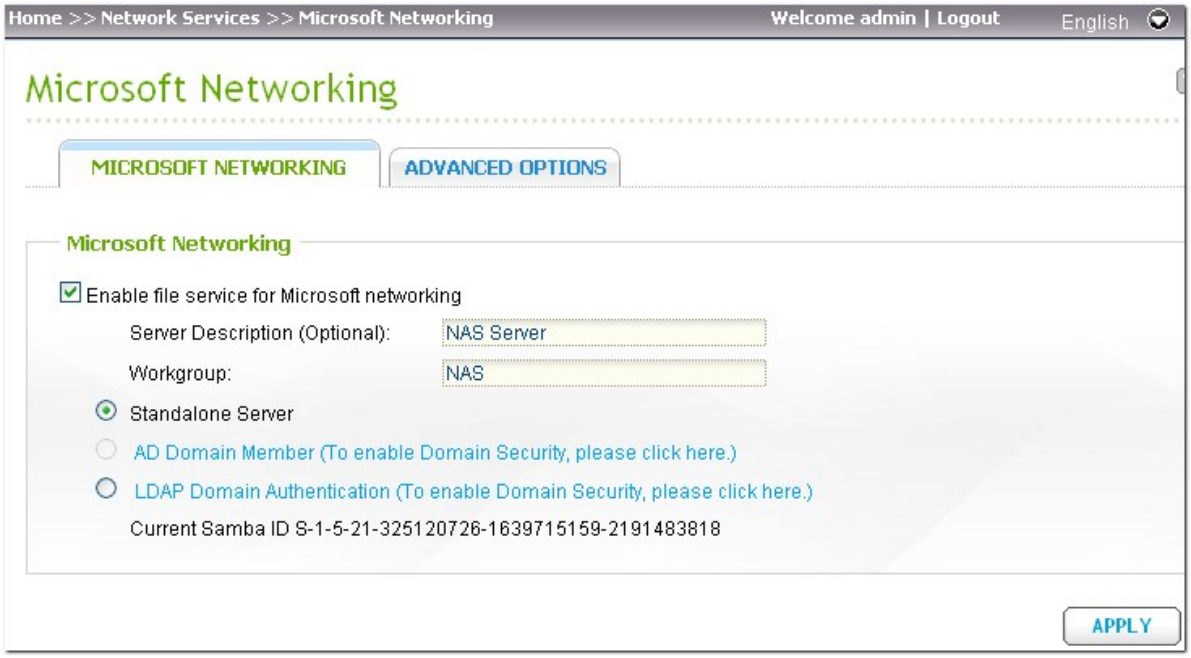
6. Network Services

Microsoft Networking 266
Apple Networking 270
NFS Service 273
FTP Service 276
Telnet/SSH 278
SNMP Settings 279
Web Server 281
Network Service Discovery 308

6.1 Microsoft Networking

Microsoft Networking

To allow access to the NAS on Microsoft Windows Network, enable file service for Microsoft networking. Specify also how the users will be authenticated.



Standalone Server

Use local users for authentication. The NAS will use the local user accounts information (created in "Access Right Management" > "Users") to authenticate the users who access the NAS.

- Server Description (optional): Describe the NAS so that the users can easily identify the server on Microsoft Network.
- Workgroup: Specify the workgroup to which the NAS belongs. A workgroup name supports up to 15 characters but cannot contain:
  " + = / \ : | * ? < > ; [ ] % , `

AD Domain Member

Use Microsoft Active Directory (AD) to authenticate the users. To use this option, enable Active Directory authentication in "Access Right Management" > "Domain Security" and join the NAS to an Active Directory.

LDAP Domain Authentication

Use Lightweight Directory Access Protocol (LDAP) directory to authenticate the users. To use this option, enable LDAP authentication and specify the settings in "Access Right Management" > "Domain Security". When this option is enabled, you need to select either the local NAS users or the LDAP users can access the NAS via Microsoft Networking.

Advanced Options

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 on your network and want to use this server, enter the WINS server IP. Do not turn on this option if you are not sure about the settings.

Local Domain Master

A Domain Master Browser is responsible for collecting and recording resources and services available for each PC on the network or a workgroup of Windows. When you find the waiting time for connecting to the Network Neighborhood/My Network Places too long, it may be caused by failure of an existing master browser or a missing master browser on the network. If there is no master browser on your network, select the option "Domain Master" to configure the NAS as the master browser. Do not turn on this option if you are not sure about the settings.

Allow only NTLMv2 authentication

NTLMv2 stands for NT LAN Manager version 2. When this option is turned on, login to the shared folders by Microsoft Networking will be allowed only with NTLMv2 authentication. If the option is turned off, NTLM (NT LAN Manager) will be used by default and NTLMv2 can be negotiated by the client. The default setting is disabled.

Name resolution priority

You can select to use DNS server or WINS server to resolve client host names from IP addresses. When you set up your NAS to use a WINS server or to be a WINS server, you can choose to use DNS or WINS first for name resolution. When WINS is enabled, the default setting is "Try WINS then DNS". Otherwise, DNS will be used for name resolution by default.

Login style: DOMAIN\USERNAME instead of DOMAIN+USERNAME for FTP, AFP, and Web File Manager
In an Active Directory environment, the default login formats for the domain users are:
Windows shares: domain\username
FTP: domain+username
Web File Manager: domain+username
AFP: domain+username

When you turn on this option, the users can use the same login name format (domain\username) to connect to the NAS via AFP, FTP, and Web File Manager.

Automatically register in DNS: When this option is turned on and the NAS is joined to an Active Directory, the NAS will register itself automatically in the domain DNS server. This will create a DNS host entry for the NAS in the DNS server. If the NAS IP is changed, the NAS will automatically update the new IP in the DNS server.

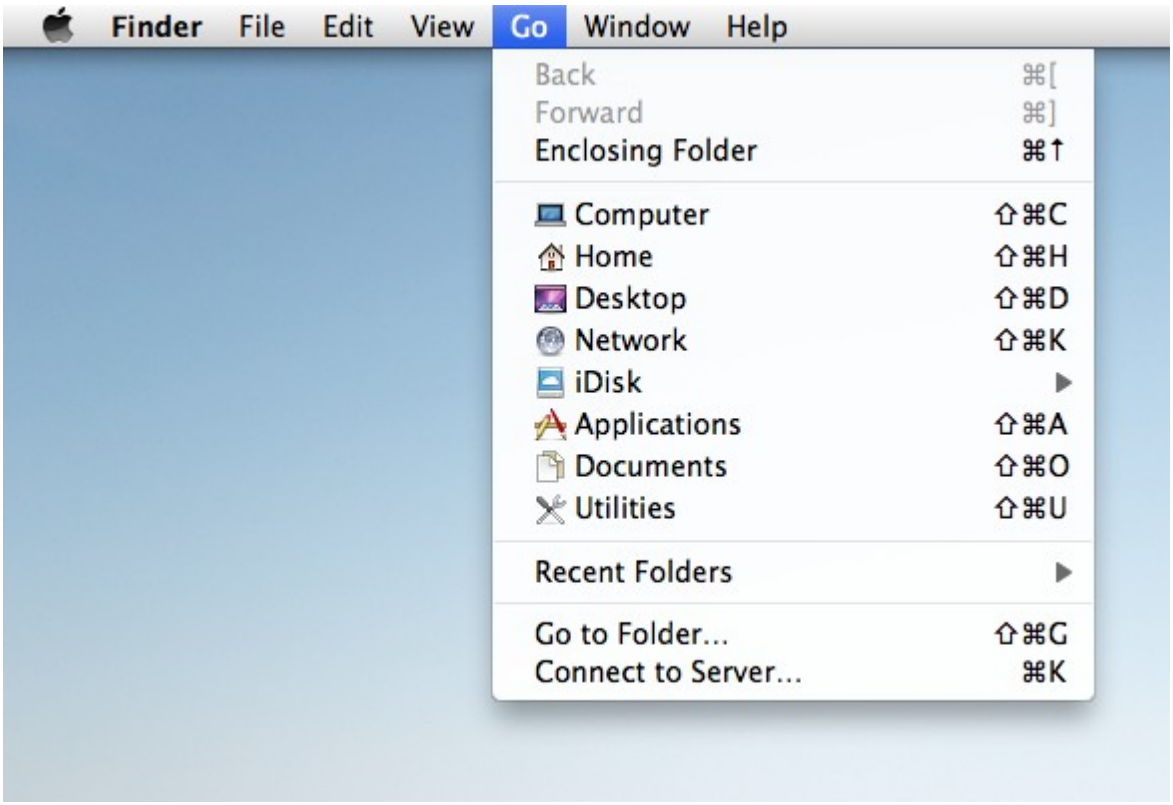
Enable trusted domains: Select this option to load the users from trusted Active Directory domains and specify their access permissions to the NAS in "Access Right Management" > "Share Folders". (The domain trusts are set up in Active Directory only, not on the NAS.)

6.2 Apple Networking

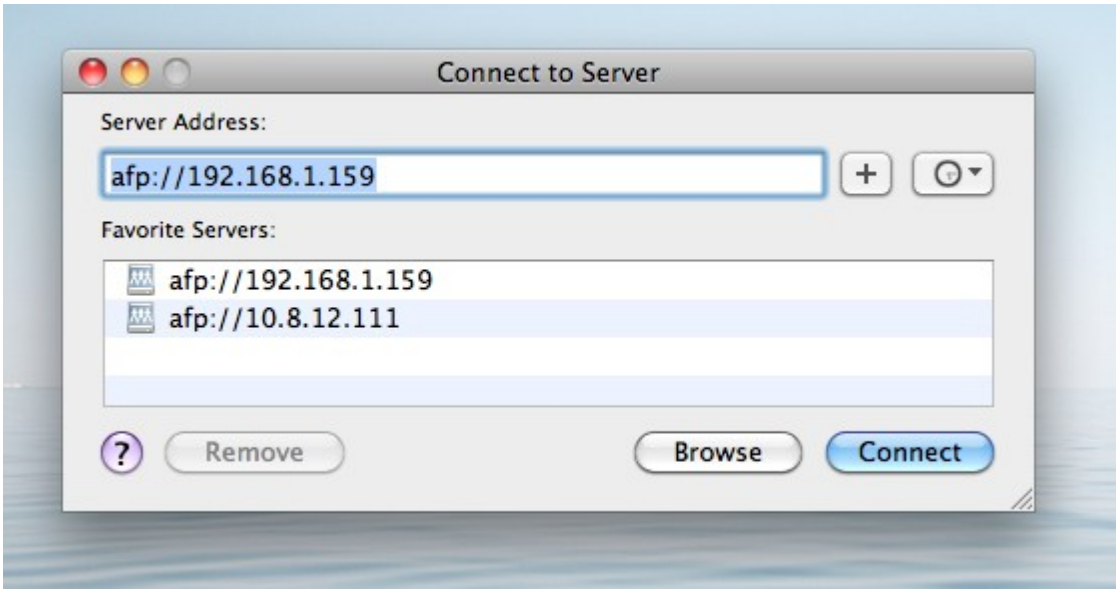
To connect to the NAS from Mac, enable Apple Filing Protocol. If the AppleTalk network uses extended networks and is assigned with multiple zones, assign a zone name to the NAS. Enter an asterisk (*) to use the default setting. This setting is disabled by default.

To allow access to the NAS from Mac OS X 10.7 Lion, enable "DHX2 authentication support". Click "Apply" to save the settings.

You can use the Finder to connect to a shared folder from Mac. Go to "Go" > "Connect to Server", or simply use the default keyboard shortcut "Command+k".



Enter the connection information in the "Server Address" field, such as "afp://*YOUR_NAS_IP_OR_HOSTNAME*". Here are some examples:
afp://10.8.12.111
afp://NAS-559
smb://192.168.1.159

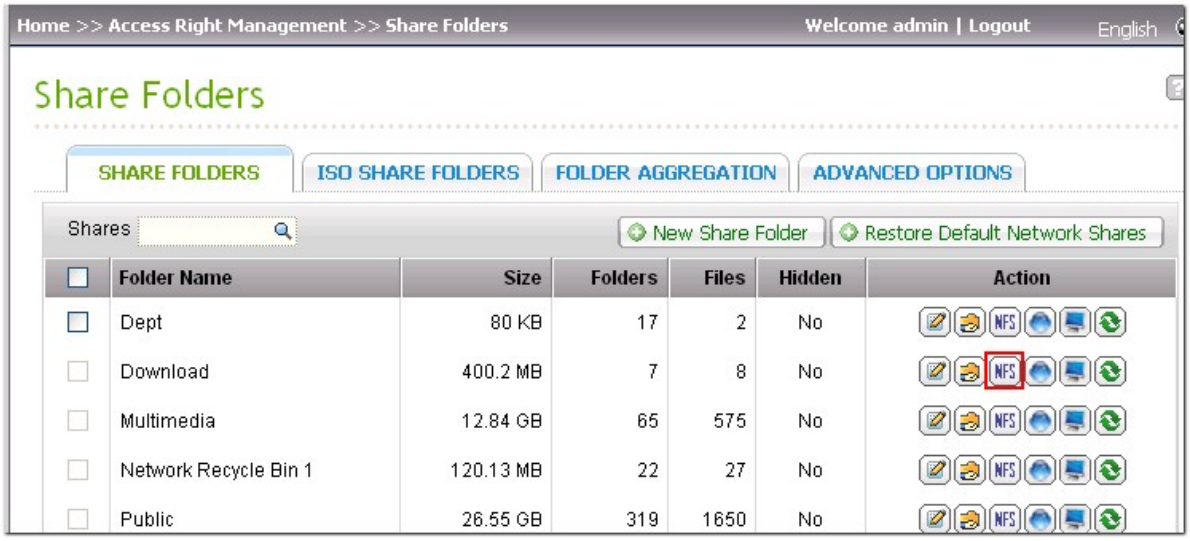


Note: Mac OS X supports both Apple Filing Protocol and Microsoft Networking. To connect to the NAS via Apple Filing Protocol, the server address should start with "afp://". To connect to the NAS via Microsoft Networking, please use "smb://".

6.3 NFS Service

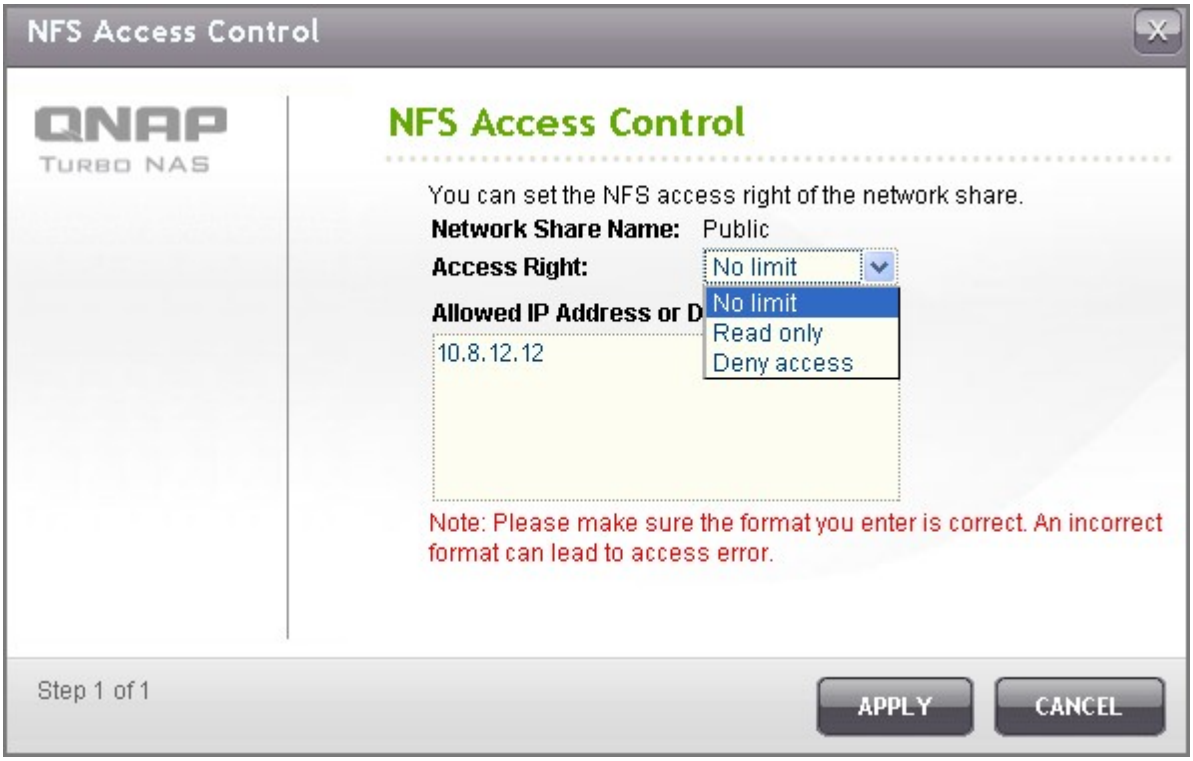
To connect to the NAS from Linux, enable NFS service.

To configure the NFS access right to the network shares on the NAS, go to "Access Right Management" > "Share Folders". Click the NFS button on the "Action" column.



Specify the access right to the network share. If you select "No limit" or "Read only", you can specify the IP address or domains that are allowed to connect to the folder by NFS.

- No limit: Allow users to create, read, write, and delete files or folders in the network share and any subdirectories.
- Read only: Allow users to read files in the network share and any subdirectories but they are not allowed to write, create, or delete any files.
- Deny access: Deny all access to the network share.



Connect to the NAS by NFS

On Linux, run the following command:
mount -t nfs <NAS IP>:/<Network Share Name> <Directory to Mount>

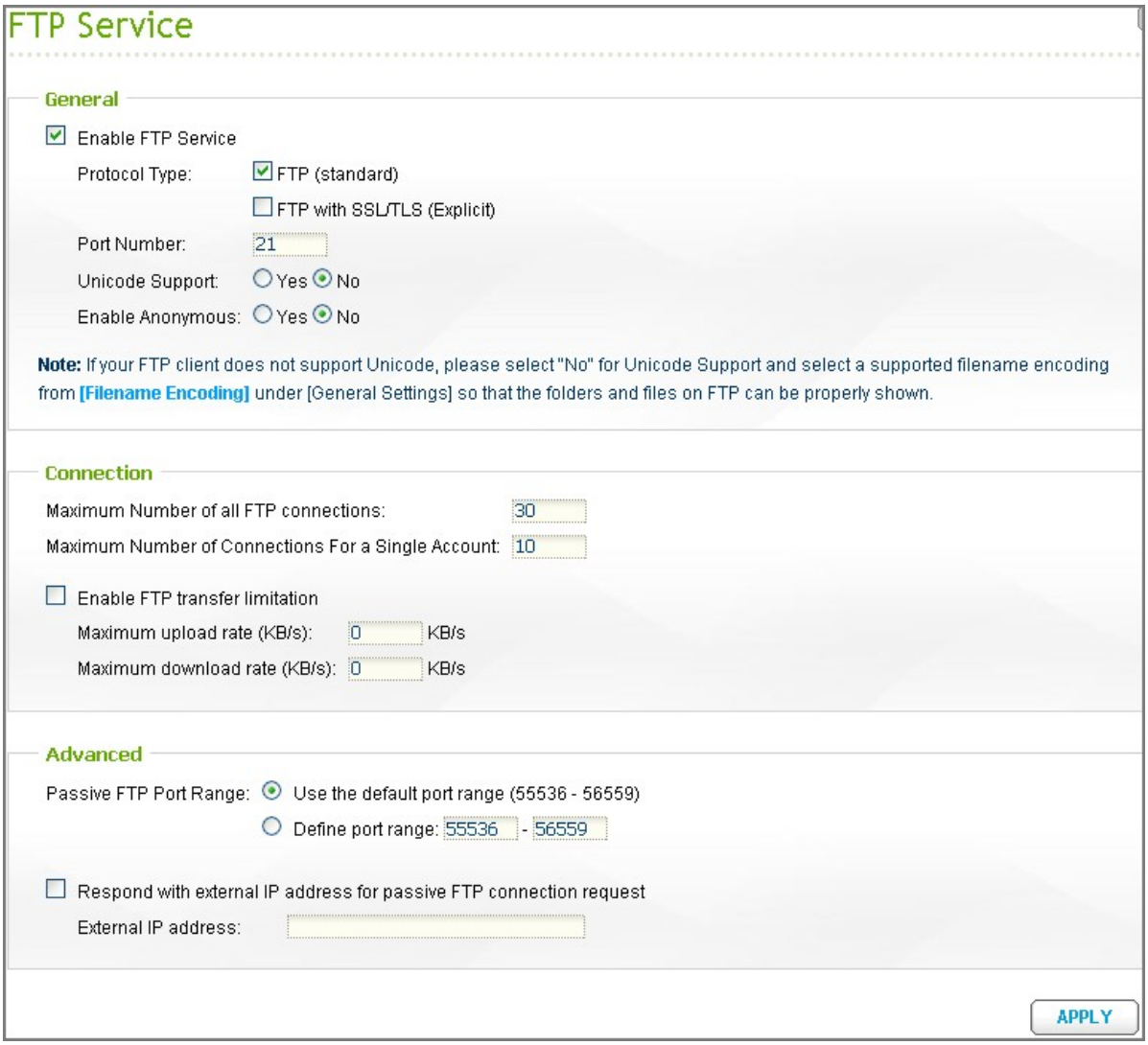
For example, if the IP address of your NAS is 192.168.0.1 and you want to link the network share "public" under the /mnt/pub directory, use the following command:
mount -t nfs 192.168.0.1:/public /mnt/pub

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

Login as the user ID you define, you can use the mounted directory to connect to your shared files.

6.4 FTP Service

When you turn on FTP service, you can specify the port number and the maximum number of users that are allowed to connect to the NAS by 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 the password to login the FTP service.

Protocol Type

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

Unicode Support

Turn on or off the Unicode support. The default setting is No. If your FTP client does not support Unicode, you are recommended to turn off this option and select the language you specify in "General Settings" > "Language" so that the file and folder names can be correctly shown. If your FTP client supports Unicode, enable Unicode support for both your client and the NAS.

Anonymous Login

You can turn on this option to allow anonymous access to the NAS by FTP. The users can connect to the files and folders which are open for public access. If this option is turned off, the users must enter an authorized user name and password to connect to the server.

Passive FTP Port Range

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

FTP Transfer Limitation

Specify the maximum number of FTP connections, maximum connections of a single user 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 (NAS) is behind a router, and a remote computer cannot connect to the FTP server over the WAN, enable this function. When this option is turned on, the NAS replies the IP address you specify or automatically detects the external IP address so that the remote computer is able to connect to the FTP server.

6.5 Telnet/SSH

Turn on this option to connect to the NAS by Telnet or SSH encrypted connection (only the "admin" account can login remotely). Use Telnet or SSH connection clients, for example, putty for connection. Make sure the specified ports have been opened on the router or firewall.

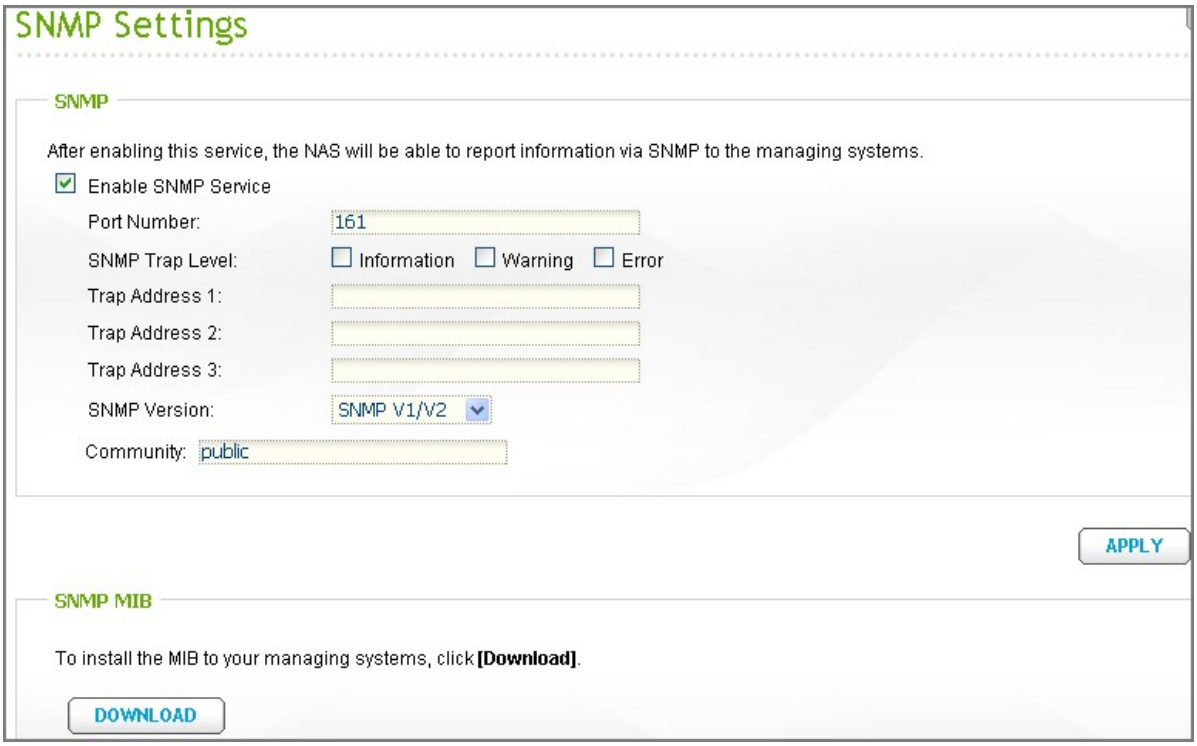
To use SFTP (known as SSH File Transfer Protocol or Secure File Transfer Protocol), make sure the option "Allow SSH connection" has been turned on.

6.6 SNMP Settings

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

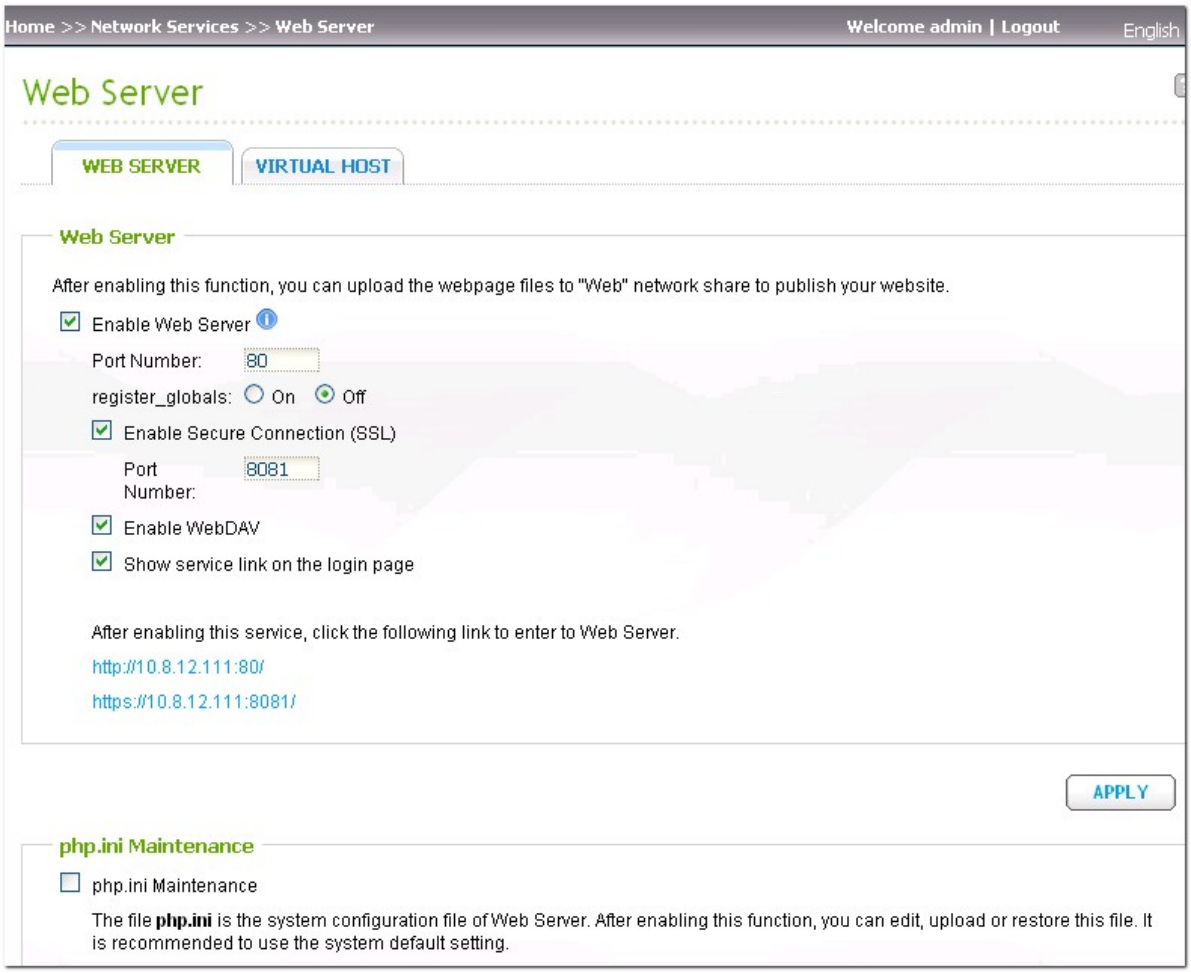
The fields are described as below:

Field	Description
SNMP Trap Level	Select the information to be sent to the SNMP management stations.
Trap Address	The IP address of the SNMP manager. Specify maximum 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. Specify the authentication and privacy settings if available.


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:
Trap Address 2:
Trap Address 3:
SNMP Version:
SNMP V1/V2
Community:
public
APPLY
SNMP MIB
To install the MIB to your managing systems, click [Download].
DOWNLOAD

6.7 Web Server

The NAS supports Web Server for web sites creation and management. It also supports Joomla!, PHP and MySQL/SQLite 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 prompts you to enable php register_globals, enable this option. However, for system security concern, it is recommended to turn this option off.
   - php.ini Maintenance
     Select the option "php.ini Maintenance" and choose to upload, edit or restore php.ini.

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

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

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

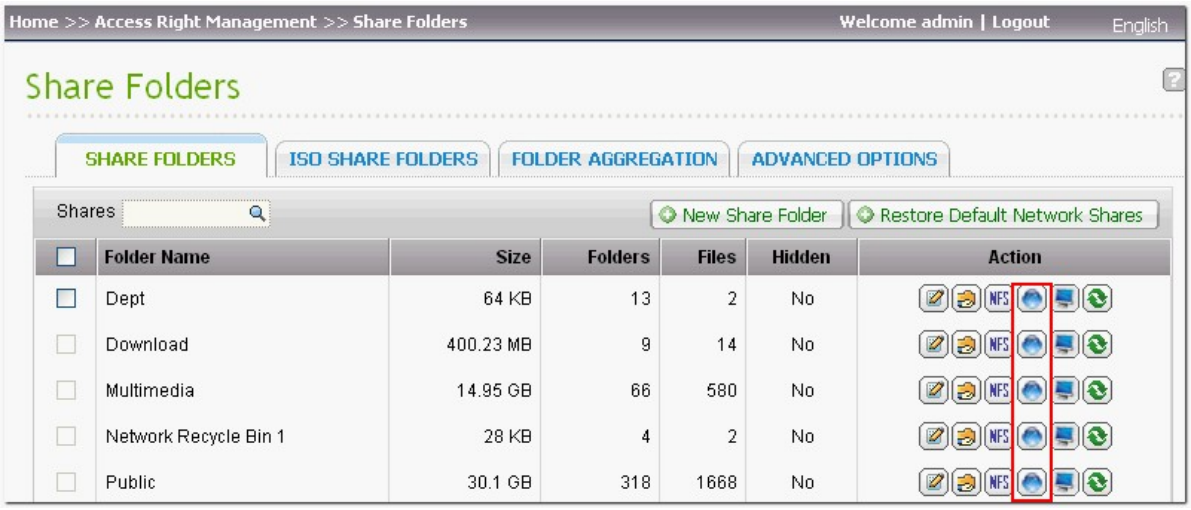
4. You can access the web page you upload by entering http://NAS IP/ in the web browser. Note that when Web Server is enabled, you have to enter http://NAS IP:8080 in your web browser to access the login page of the NAS.

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 the files collaboratively on the remote World Wide Web servers. After turning on this function, you can map the network shares of your NAS as the network drives of a remote PC over the Internet. To edit the access right settings, go to "Access Right Management" > "Share Folders" page.

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

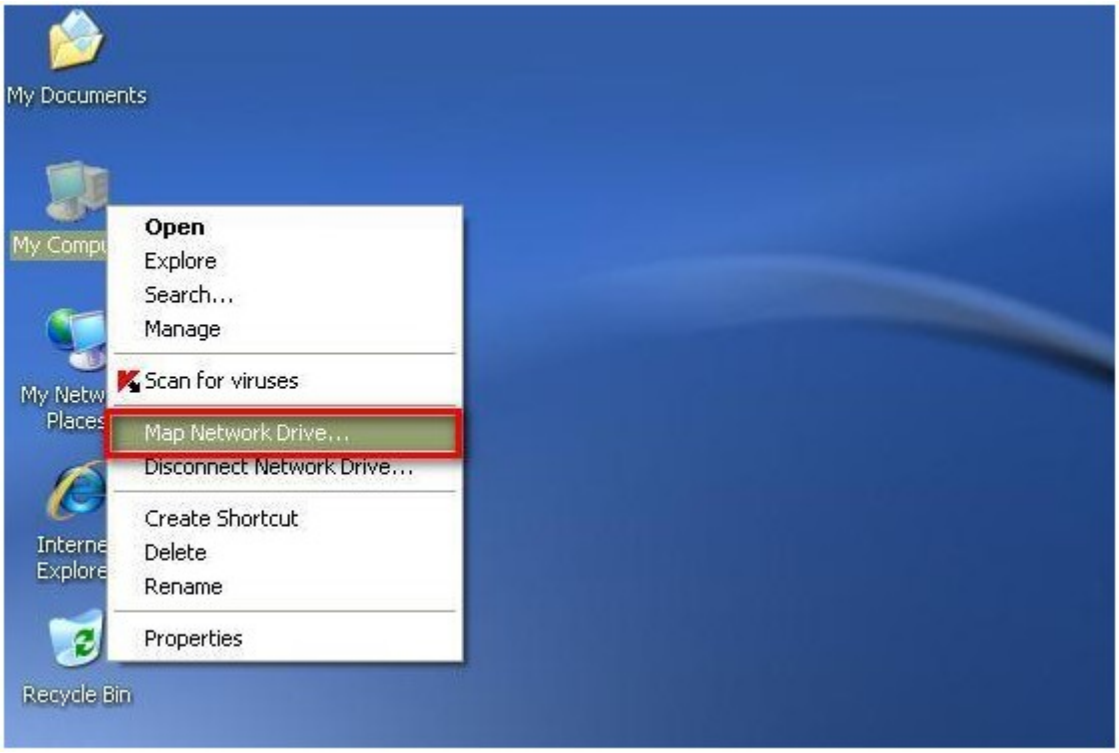
Go to "Access Right Management" > "Share Folders" > "Share Folder". Click the "WebDAV Access Control" button in the "Action" column, and set the WebDAV access right of the users to the network shares.



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

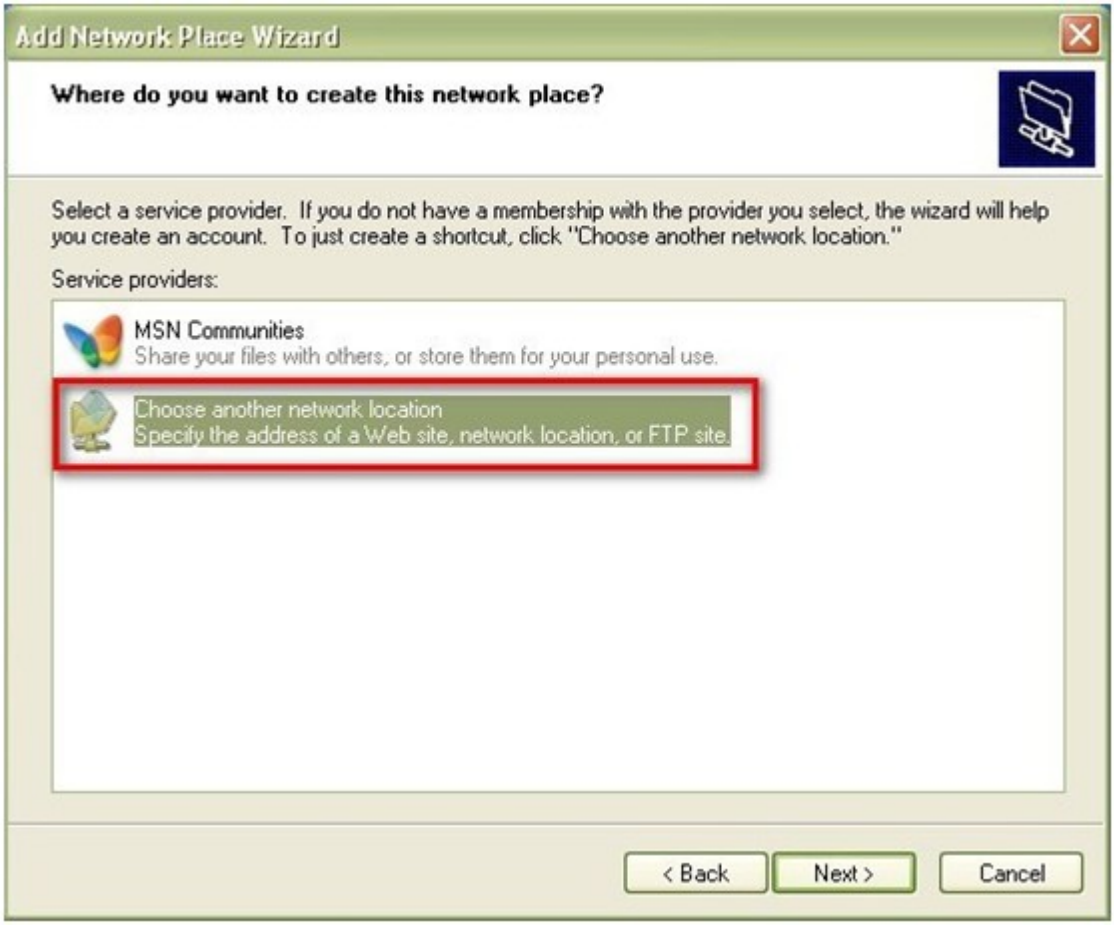
Windows XP:

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



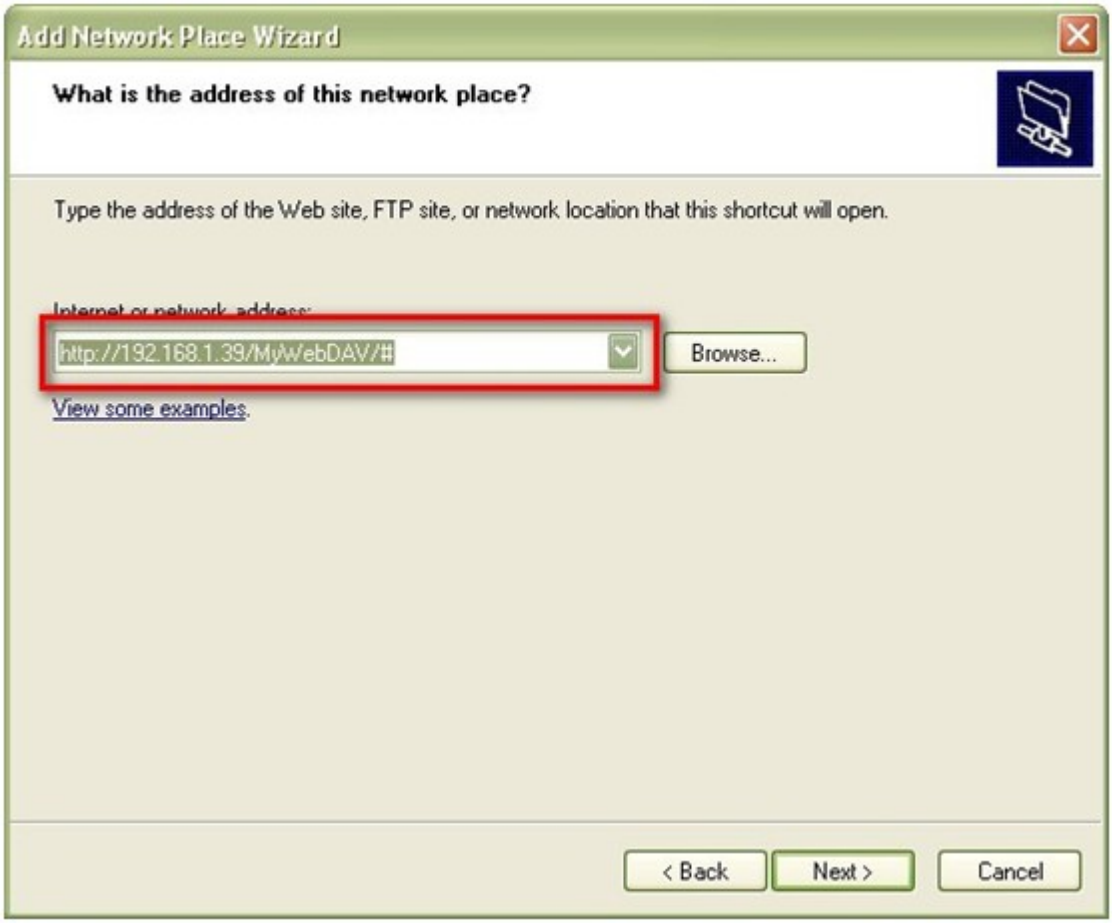
2. Click "Sign up for online storage or connect to a network server".

3. Select “Choose another network location”.



4. Enter the URL of your NAS with the folder name. Note that you should put a "#" key at the end of the URL. Click "Next".

Format: http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME/#

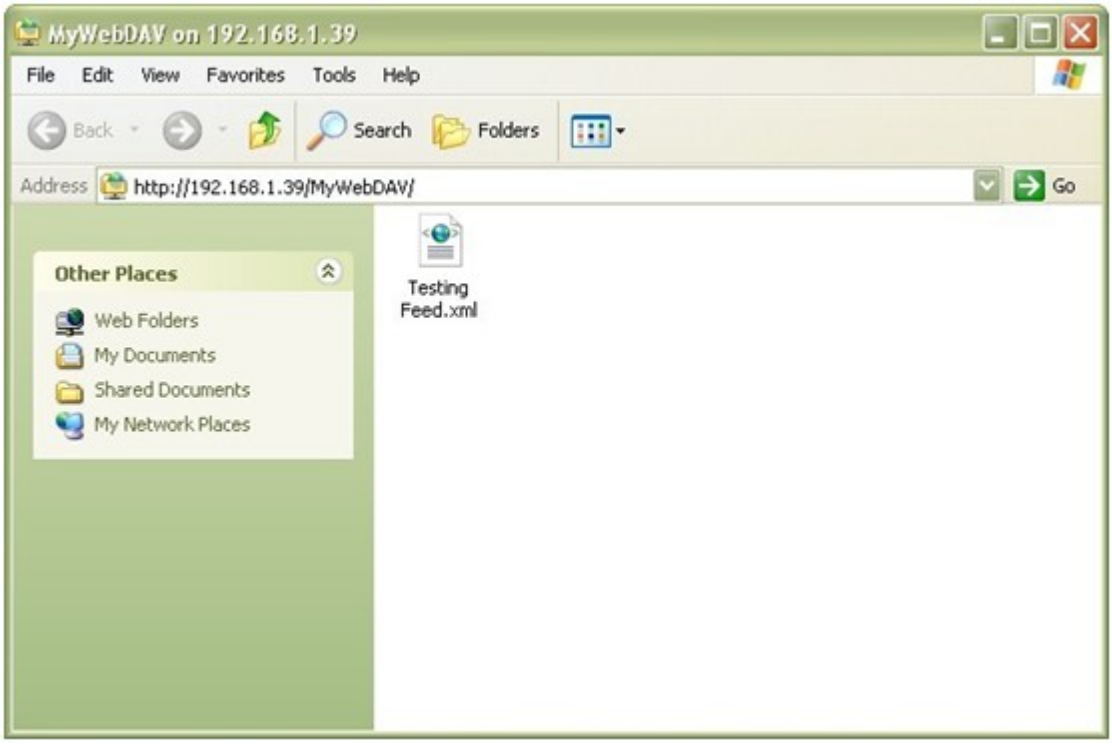


5. Enter the user name and password which has the WebDAV access right to connect to the folder.

6. Type a name for this network place.

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

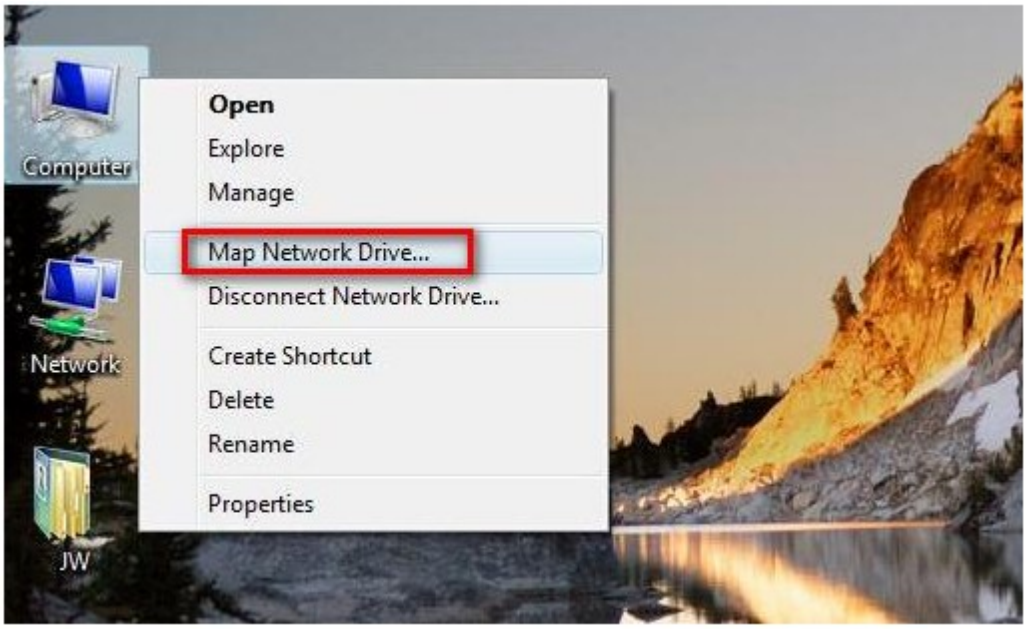
8. Now you can connect to this folder anytime through WebDAV. A shortcut has also been created in "My Network Places".



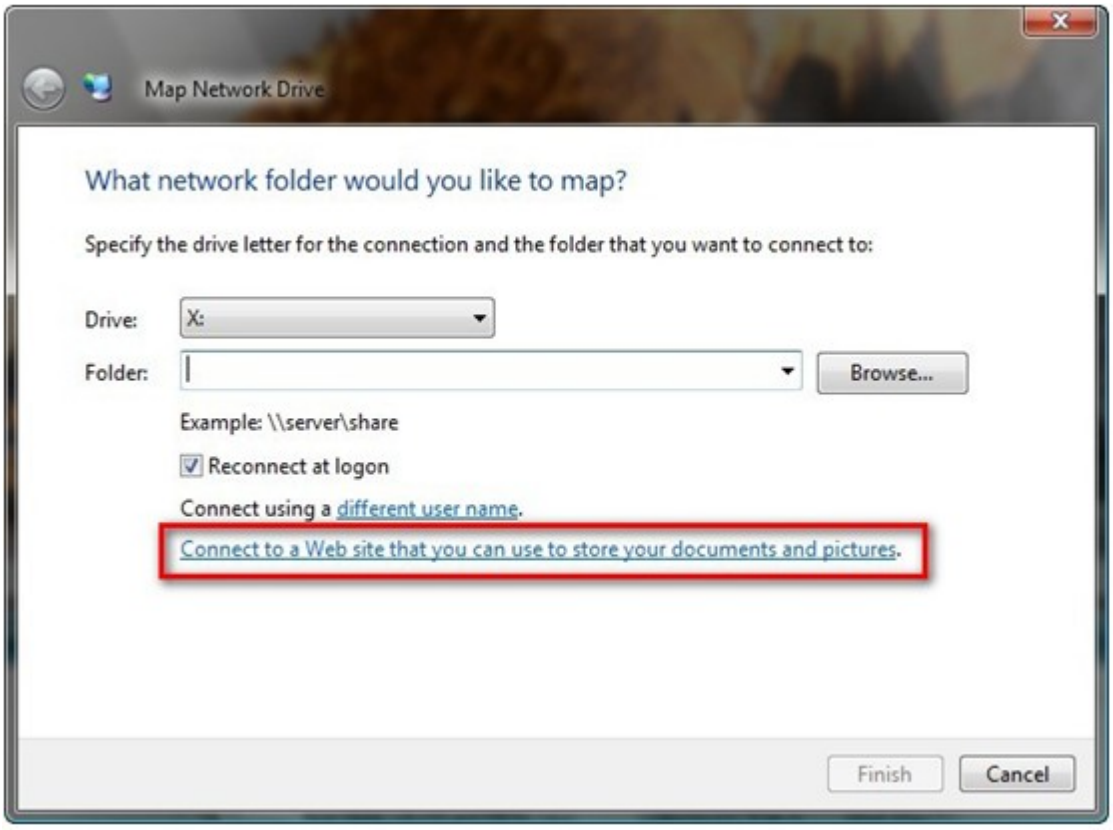
Windows Vista

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

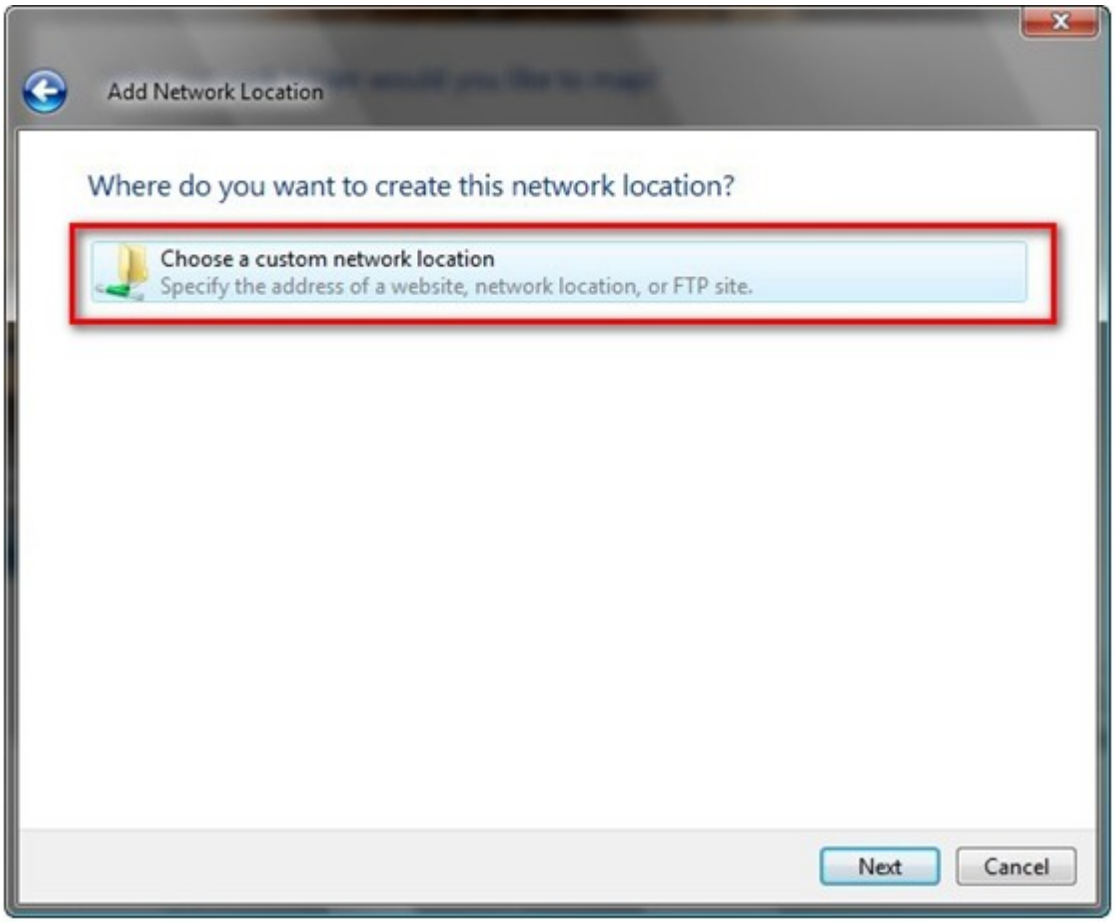
1. Right click "Computer" and select "Map Network Drive…"



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

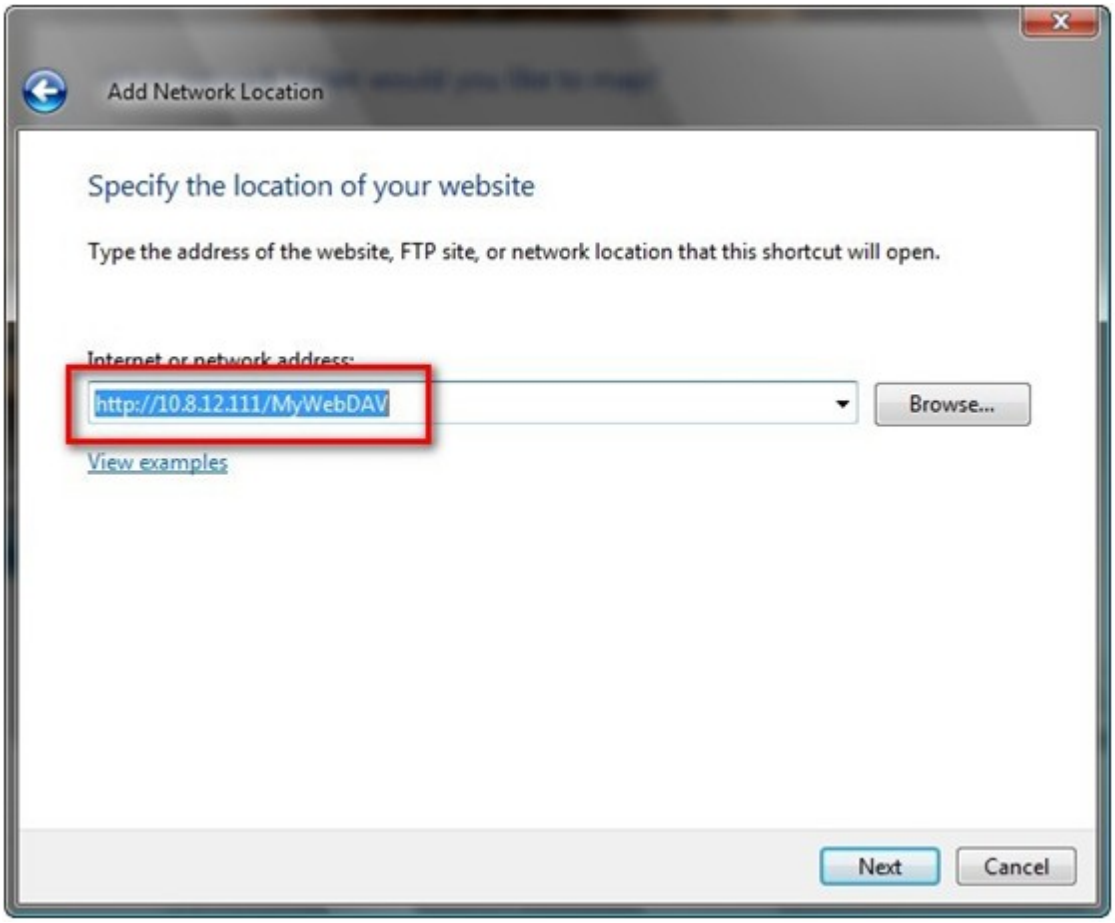


3. Select “Choose a custom network location”.



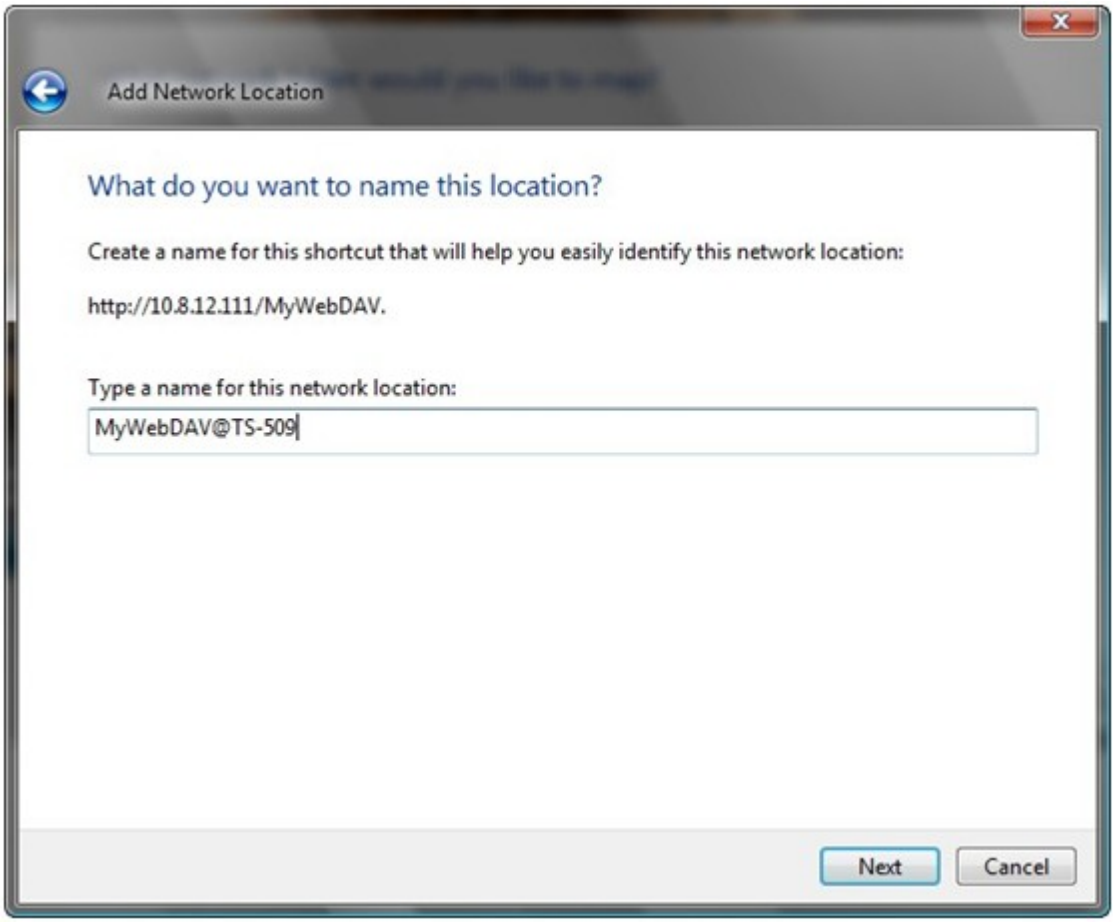
4. Enter the URL of your NAS with the folder name.

Format: http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME

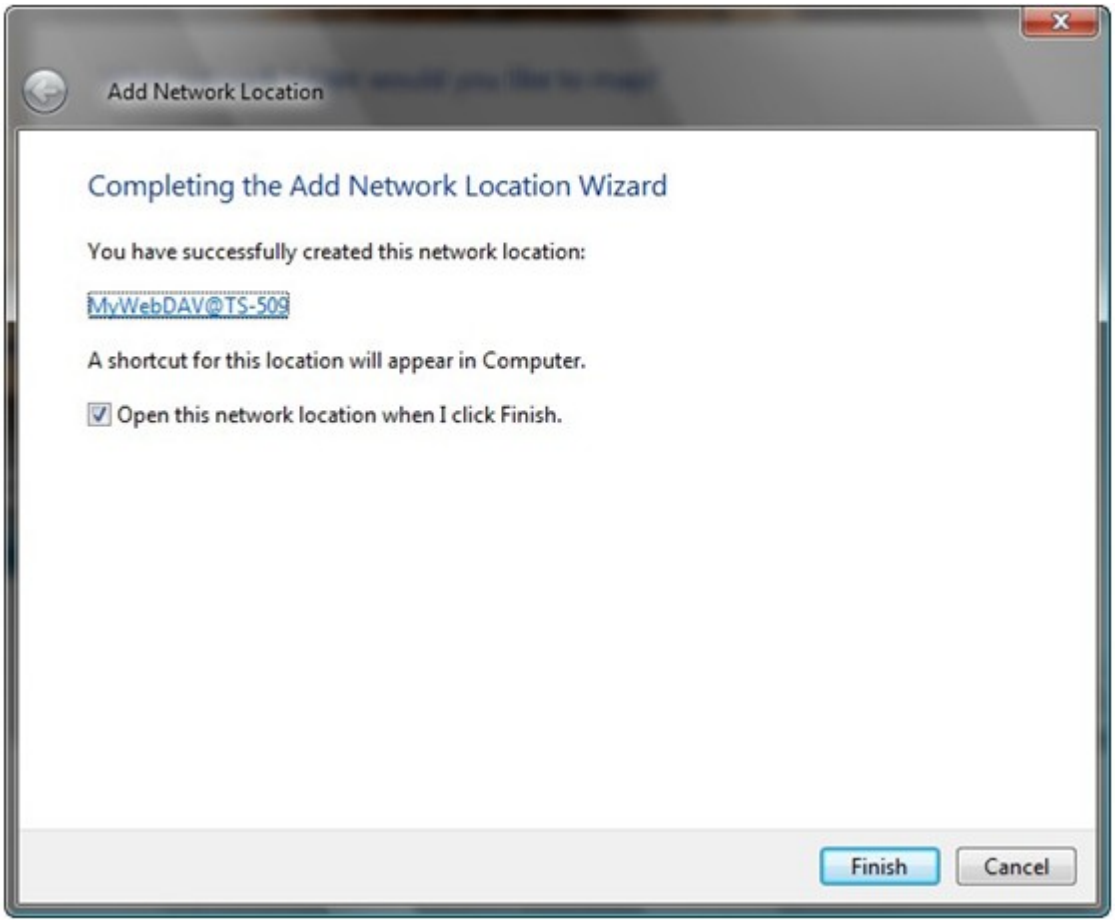


5. Enter the user name and password which has the WebDAV access right to connect to this folder.

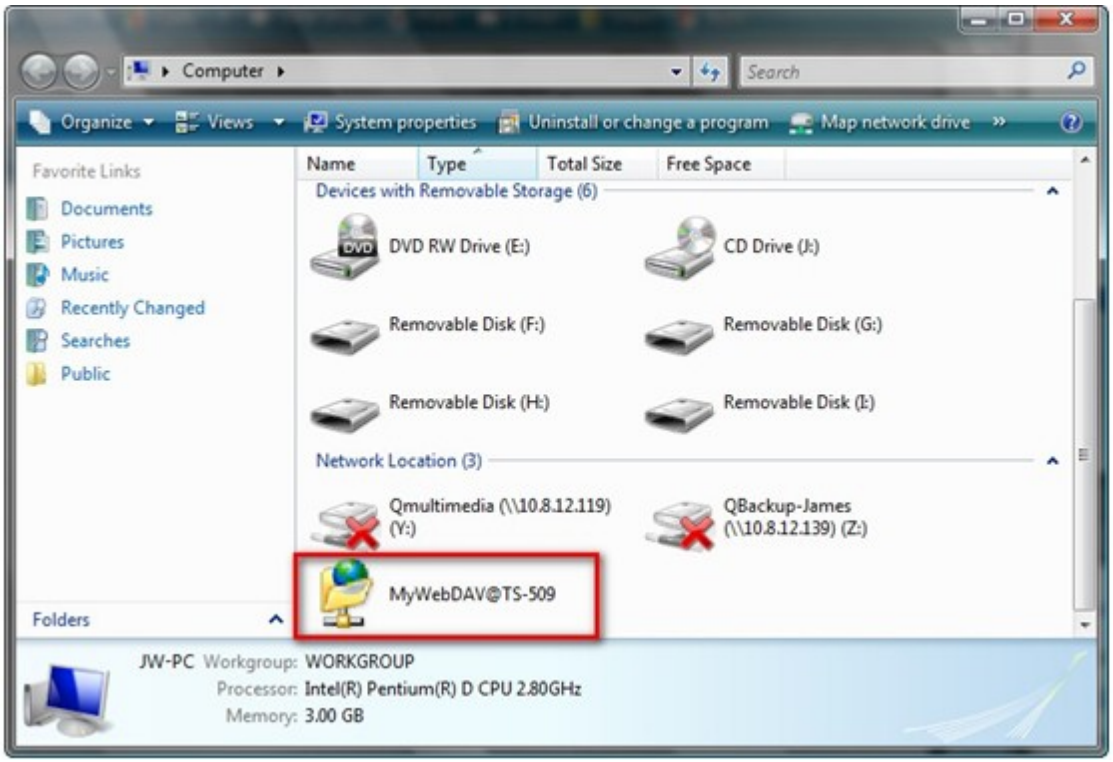
6. Type a name for this network location.



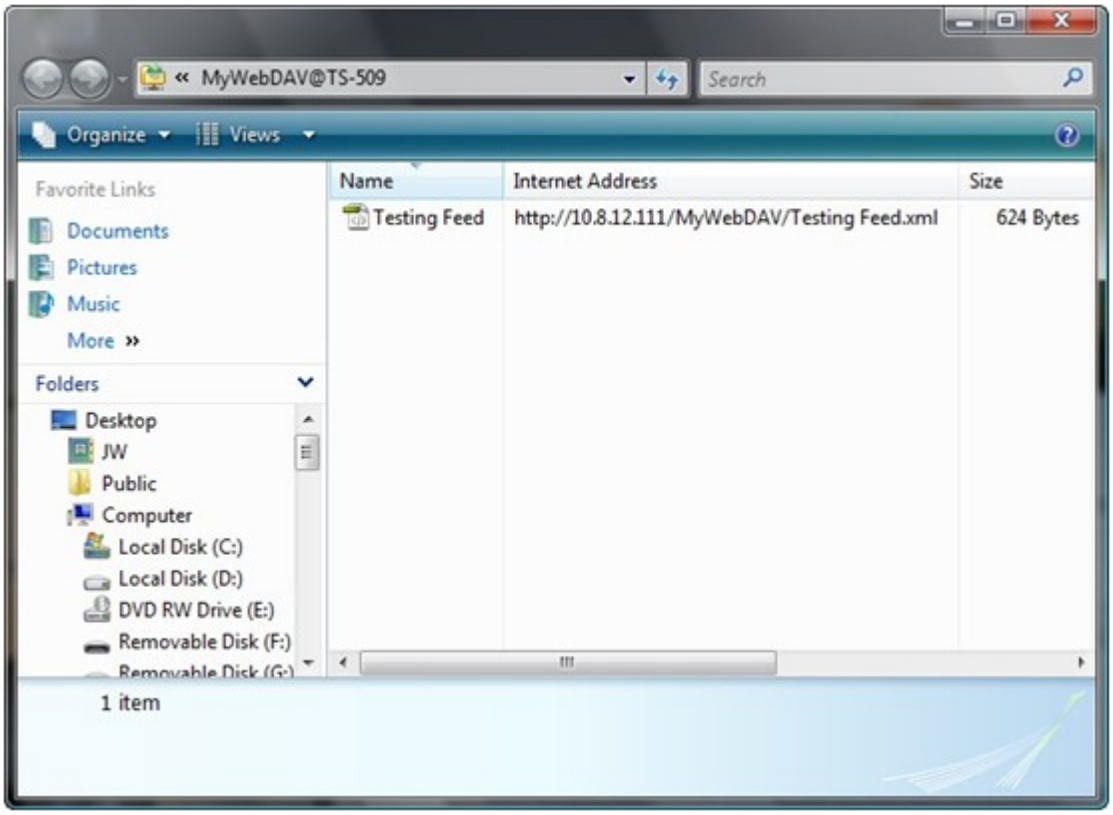
7. The Web folder has been successfully created.



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



9. You can connect to the folder though this link via HTTP/WebDAV.



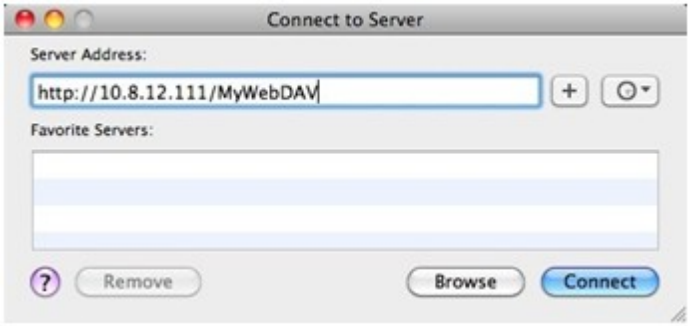
Mac OS X

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)

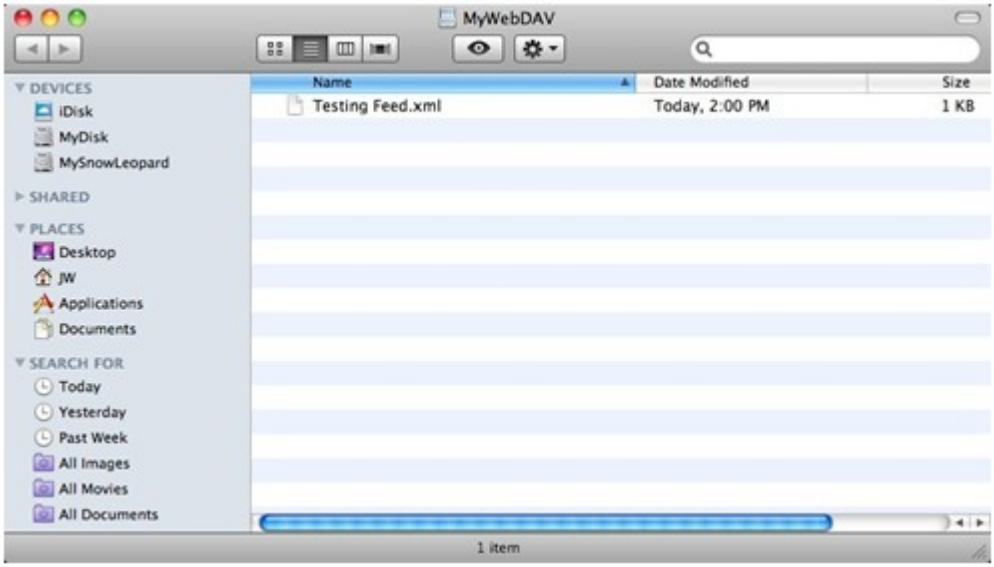
1. Open “Finder” > “Connect to Server”, and enter the URL of the folder.

Format: http://NAS_IP_or_HOST_NAME/SHARE_FOLDER_NAME

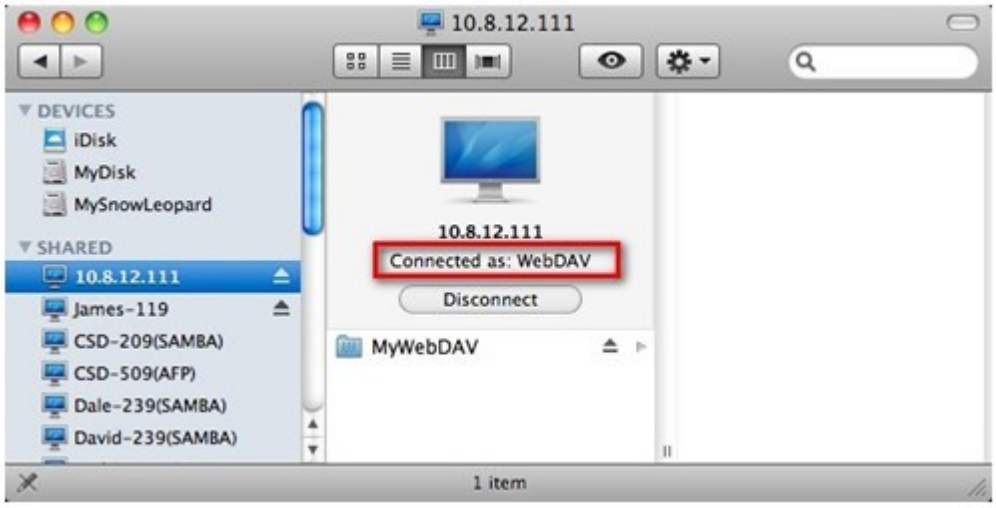


2. Enter the user name and password which has the WebDAV access right to connect to this folder.

3. You can connect to the folder through this link via HTTP/WebDAV.



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



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

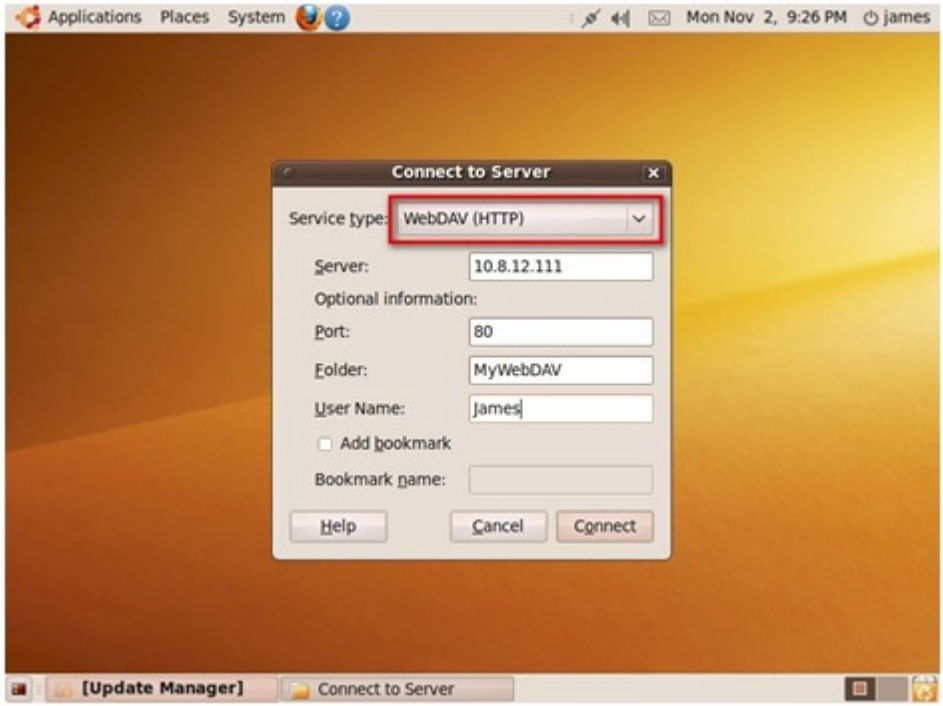
Ubuntu

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

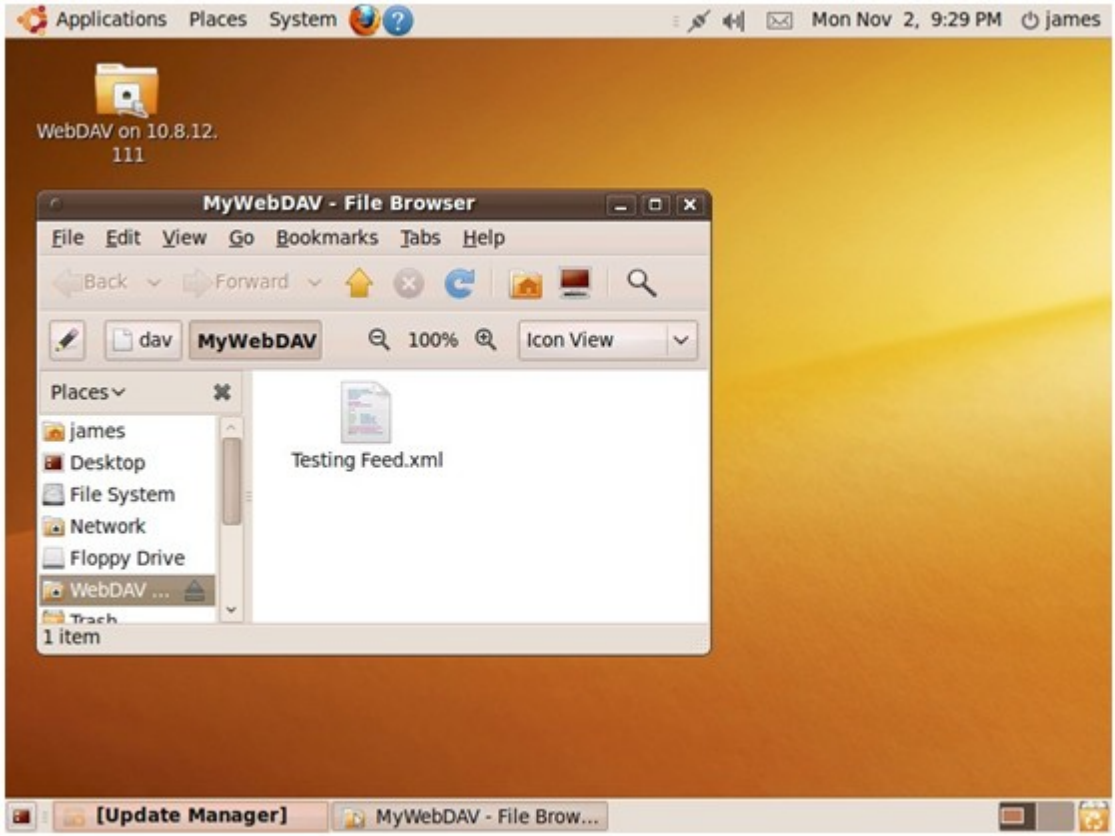
Client Operating System: Ubuntu 9.10 Desktop

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 password which has the WebDAV access right to connect to this 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

Install phpMyAdmin software and save the program files in the Web or Qweb share of the NAS. You can change the folder name and connect to 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

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

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

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

6.7.1 Virtual Host

Virtual host is a web server technique that provides the capability to host more than one domain (website) on one physical host offers a cost-effective solution for personal and small business with such need. You can host multiple websites (maximum 32) on the NAS with this feature.

In this tutorial we will use the information provided in the table below as the reference guide.

Host name	WAN/LAN IP and port	Document root	Demo web application
site1.mysite.com	WAN IP: 111.222.333.444 LAN IP: 10.8.12.45 (NAS) Port: 80 (NAS)	/Qweb/site1_mysite	Joomla!
site2.mysite.com		/Qweb/site2_mysite	WordPress
www.mysite2.com		/Qweb/www_mysite2	phpBB3

Before you start, make sure you have checked the following items:

- Web Server

  Enable Web Server in "Network Services" > "Web Server".
- DNS records

  The host name must point to the WAN IP of your NAS and you can normally configure this from your DNS service providers.
- Port forwarding

  If the web server listens on port 80 you need to configure port forwarding on your router to allow inbound traffic from port 80 to the LAN IP (10.8.12.45) of your NAS.
- SSL certificate import

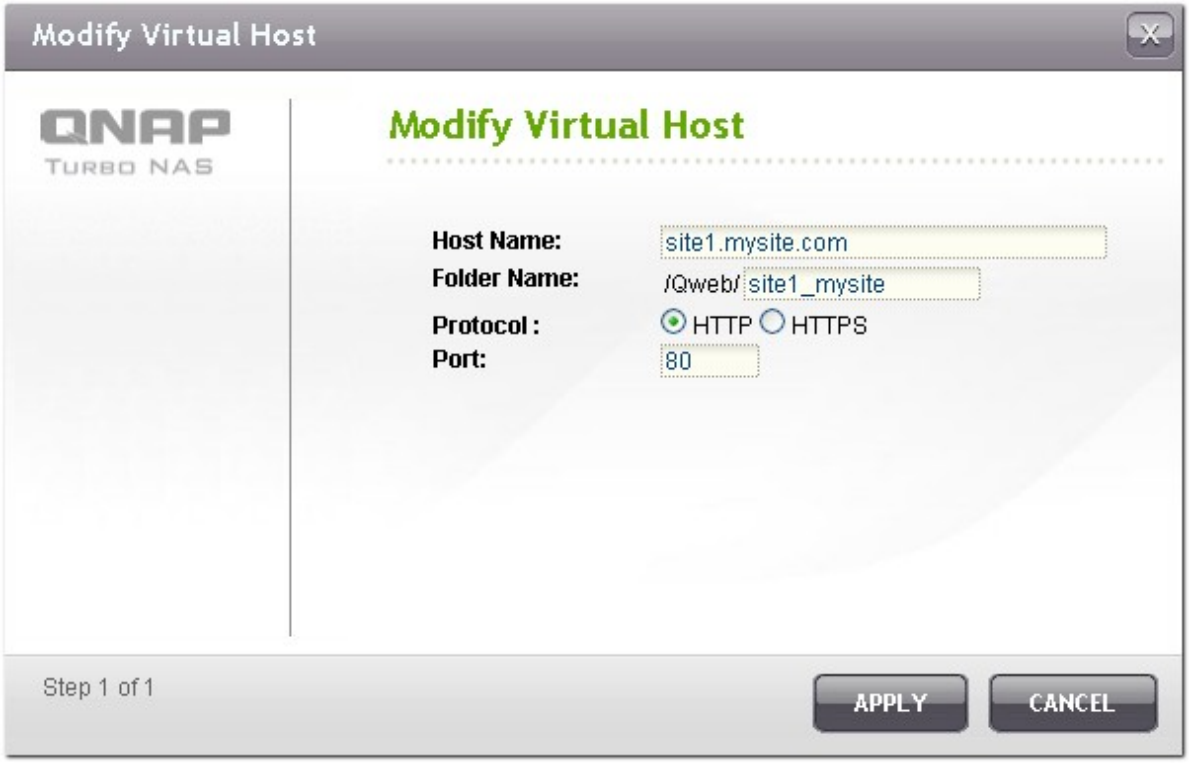
  If you are going to enable SSL connection for the website and intend to use your own trusted SSL certificates you may import the certificate from within the administration backend under "System Administration" > "Security" > "Import SSL Secure Certificate".

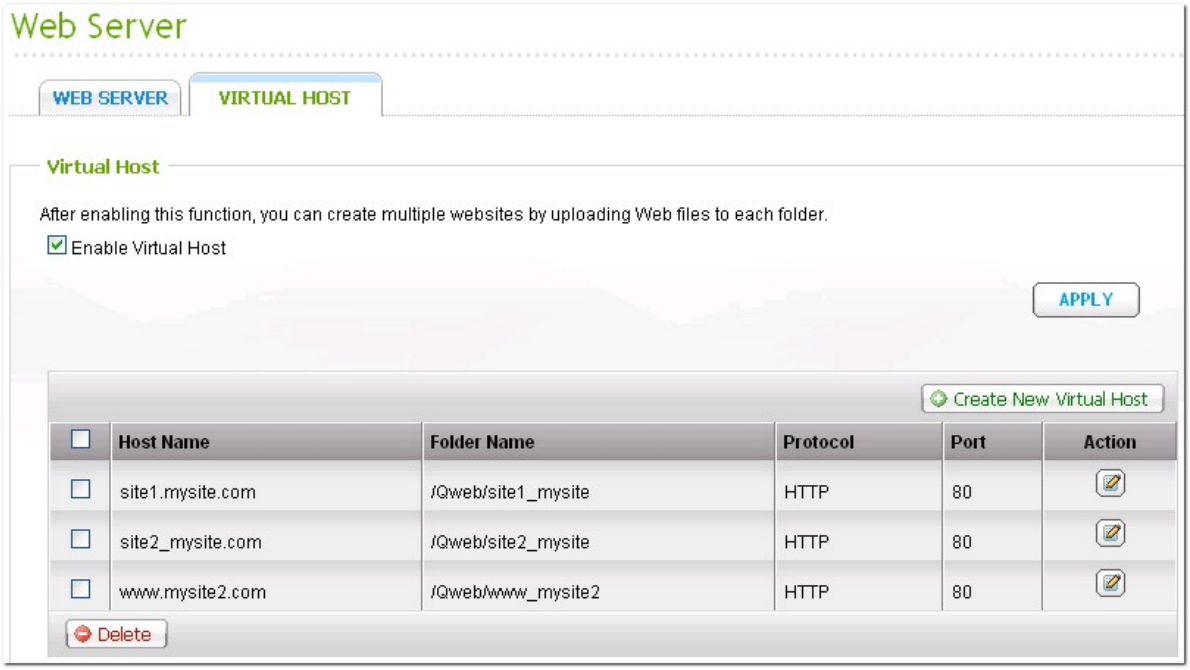
Follow the steps below to use virtual host.

1. Select "Enable Virtual Host" and click "Apply".
2. Click "Create New Virtual Host".

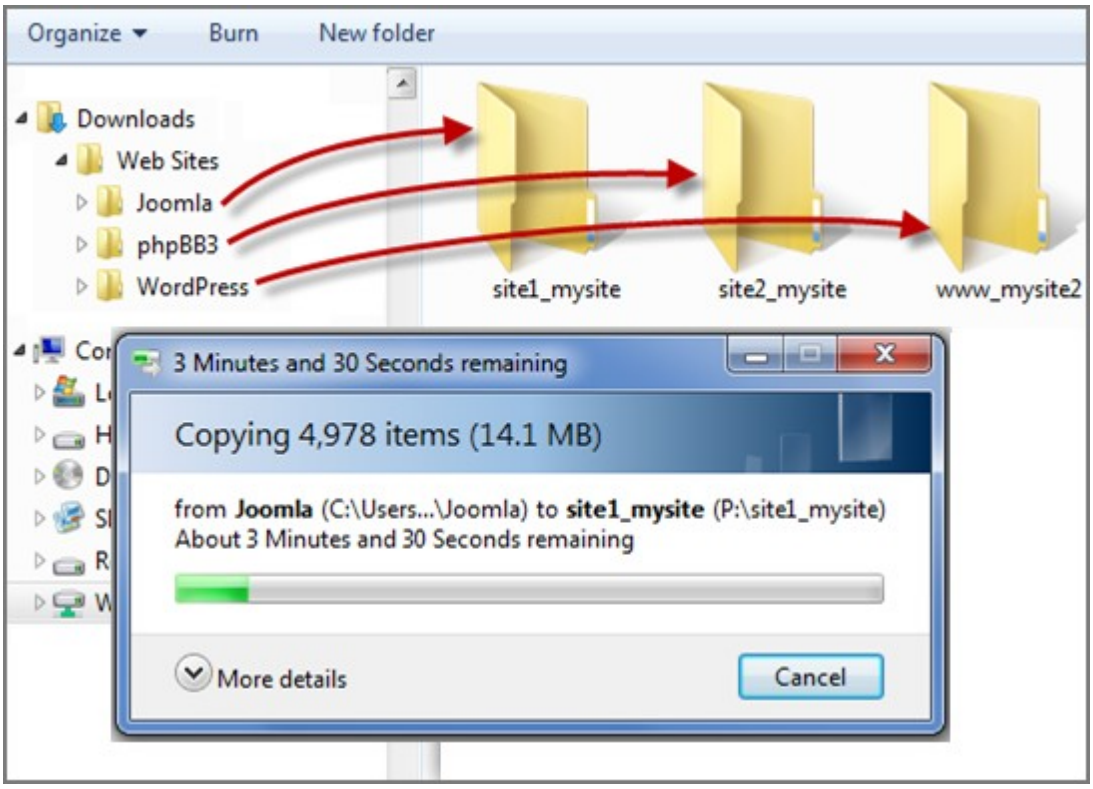
3. Enter the host name and specify the folder (under Web or Qweb) where the web files will be uploaded to.
4. Specify the protocol (HTTP or HTTPS) for connection. If you select HTTPS, make sure the option "Enable Secure Connection (SSL)" in Web Server has been turned on.
5. Specify the port number for connection.
6. Click "Apply".

7. Continue to enter the information for the rest of the sites you want to host on the NAS.





8. Create a folder for each website (site1_mysite, site2_mysite, and www_mysite2) and start transferring the website files to the corresponding folders.



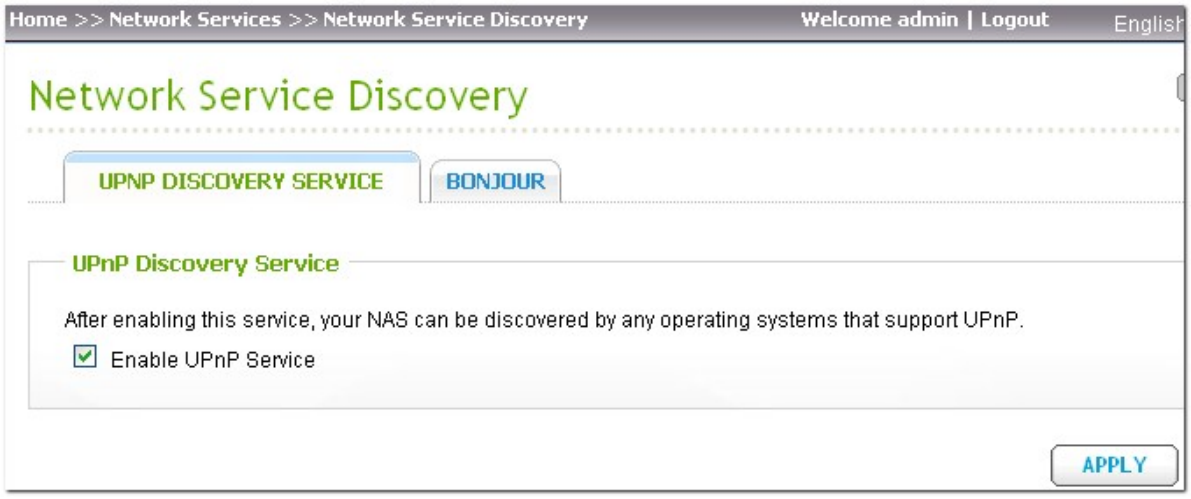
Once the files transfers complete point your web browser to the websites by http://NAS_host_name or https://NAS_host_name according to your settings. In this example, the URLs are:
http://site1.mysite.com
http://site2.mysite.com
http://www.mysite2.com

You should see the Joomla!, phpBB3, and WordPress web pages respectively.

6.8 Network Service Discovery

UPnP Discovery Service

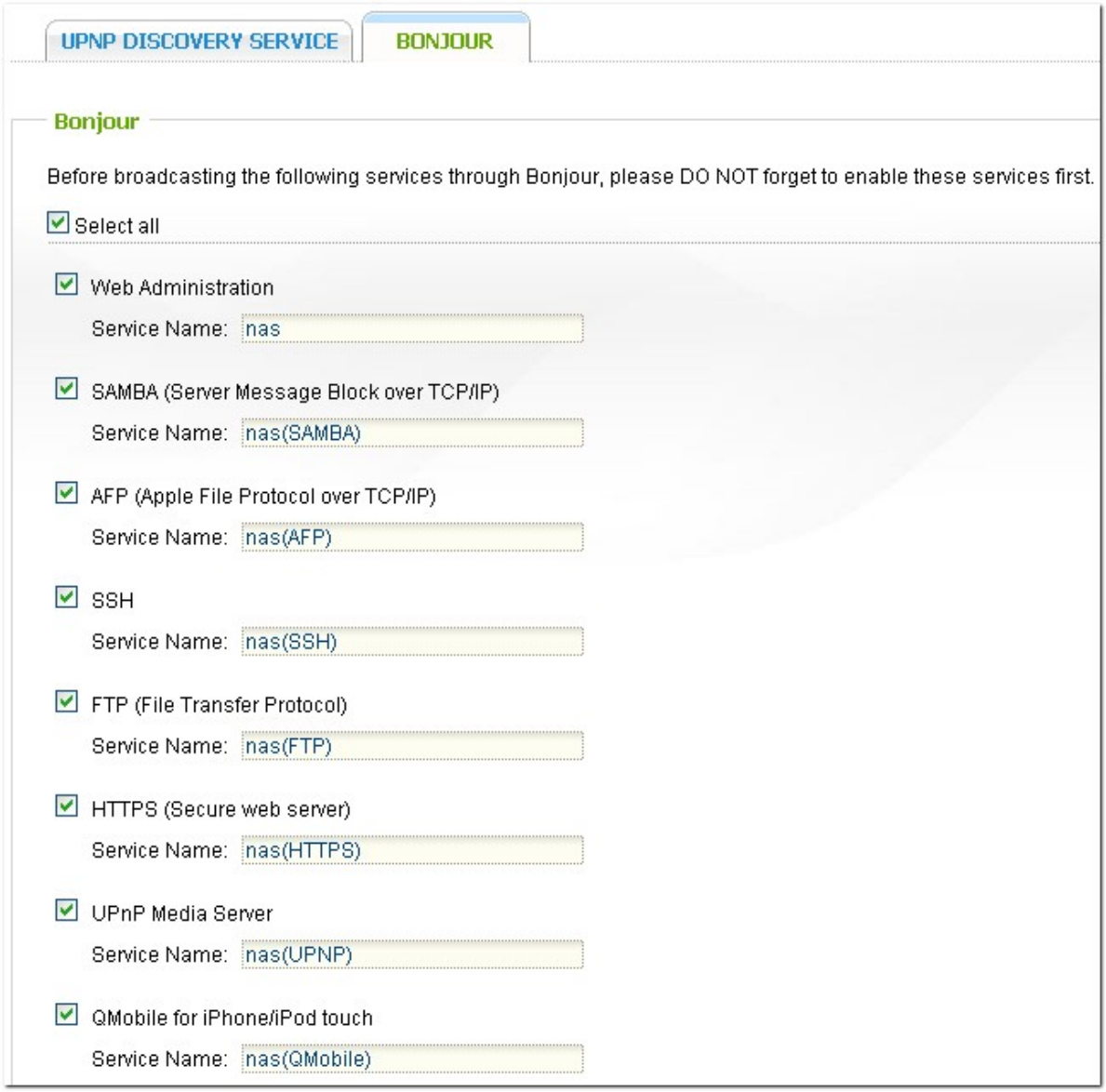
When a UPnP device is added to the network, the UPnP discovery protocol allows the device to advertise its services to the control points on the network.
By enabling UPnP Discovery Service, the NAS can be discovered by any operating systems that support UPnP.



Bonjour

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

Note: You have to activate the services on their setup pages and then turn them on in this section so that the NAS will advertise this service with Bonjour.



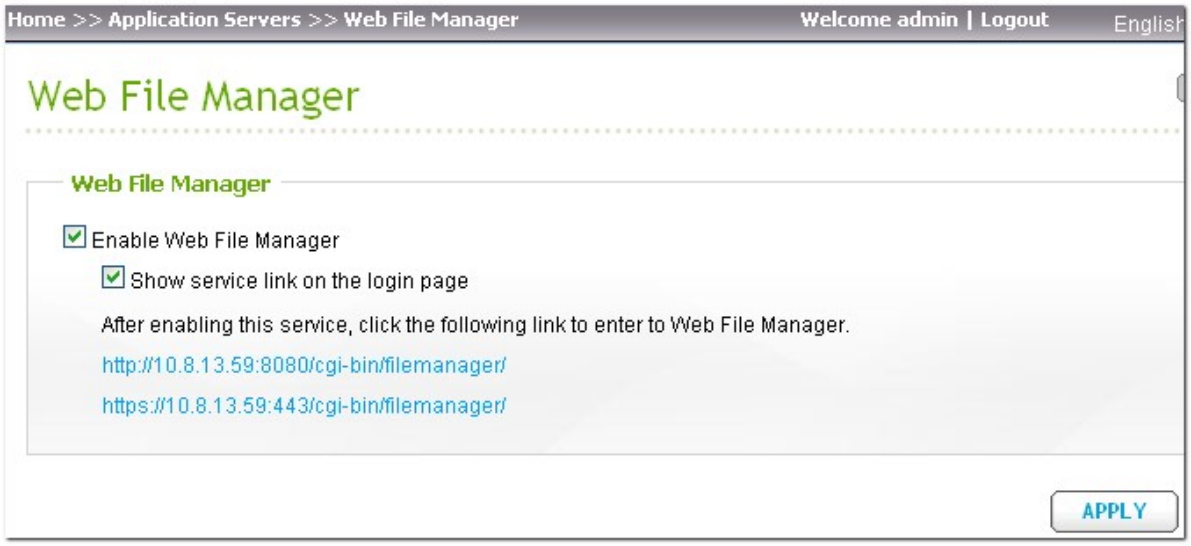
7. Application Servers

Web File Manager 311
Multimedia Station 329
Photo Station 385
Music Station 408
Download Station 428
Surveillance Station 450
iTunes Server 458
UPnP Media Server 461
MySQL Server 463
QPKG Center 465
Syslog Server 469
RADIUS Server 474
Backup Server 478
Antivirus 482
TFTP Server 492
VPN Service 493
LDAP Server 509

7.1 Web File Manager

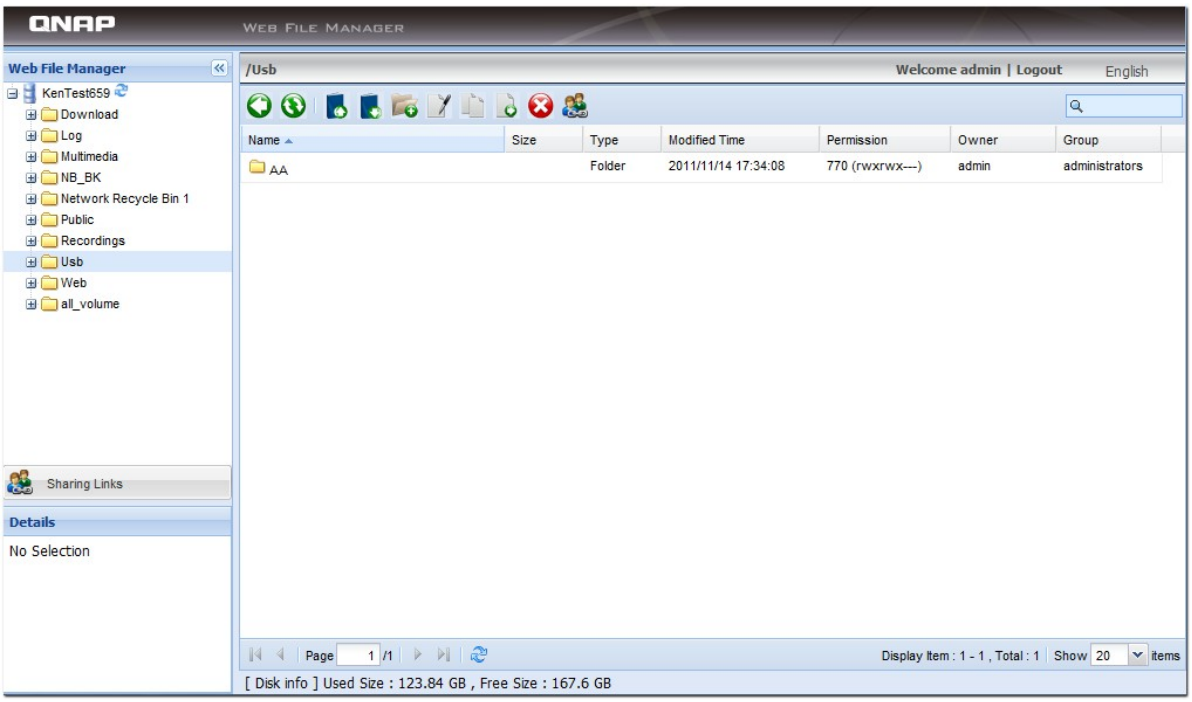
To connect to the files on the NAS by a web browser, enable Web File Manager. If the NAS is connected to the Internet and uses a valid IP address, you can connect to the NAS by web browser from anywhere.

To use Web File Manager, go to "Application Servers" > "Web File Manager". Enable the service.



Click "Web File Manager" on the top or on the login page of the NAS to connect to 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.

With Web File Manager, you can upload, download, rename, move, copy, or delete the files and folder on the NAS.

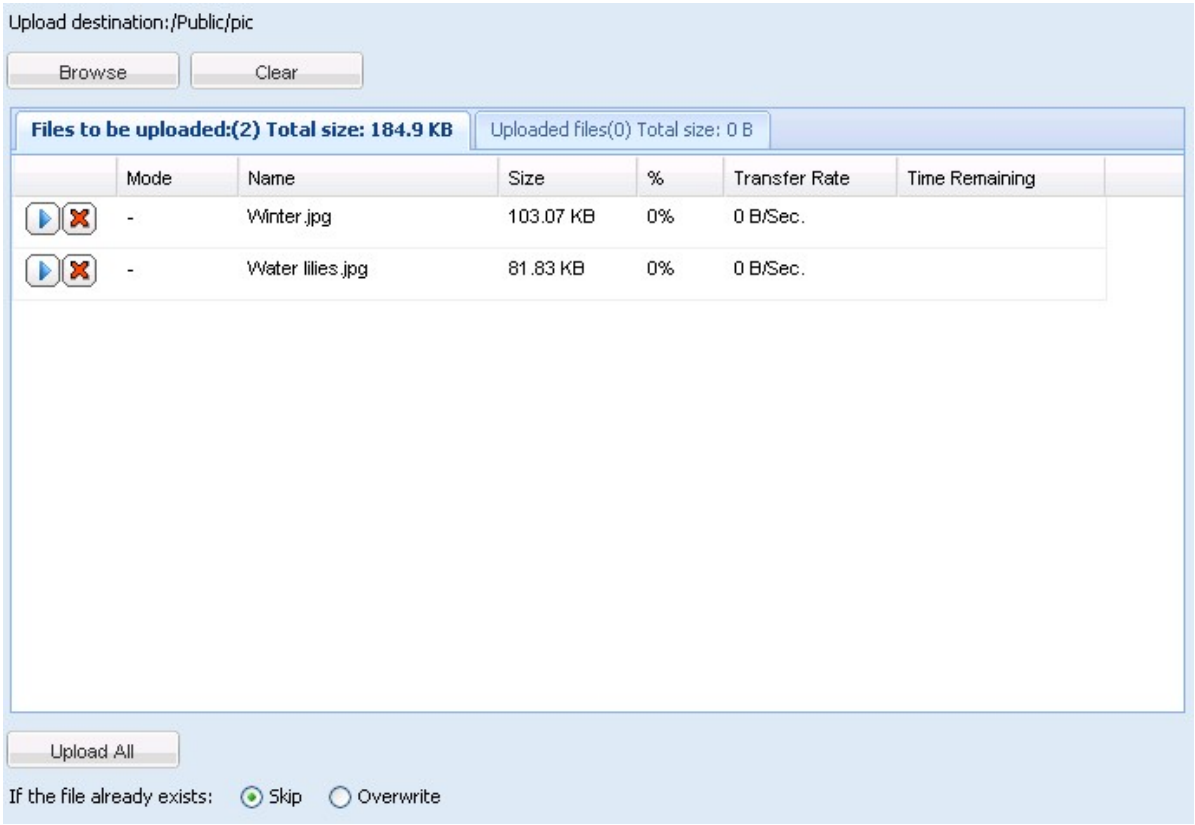


Upload files

Note: The maximum size of a file that can be uploaded to the NAS by Web File Manager is 2GB.

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

i. Select a folder and click .
ii. Click "Browse" to select the file(s).
iii. Select to skip or overwrite the existing file(s) in the folder.
iv. Click to upload a file or "Upload All" to upload all the selected files.



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

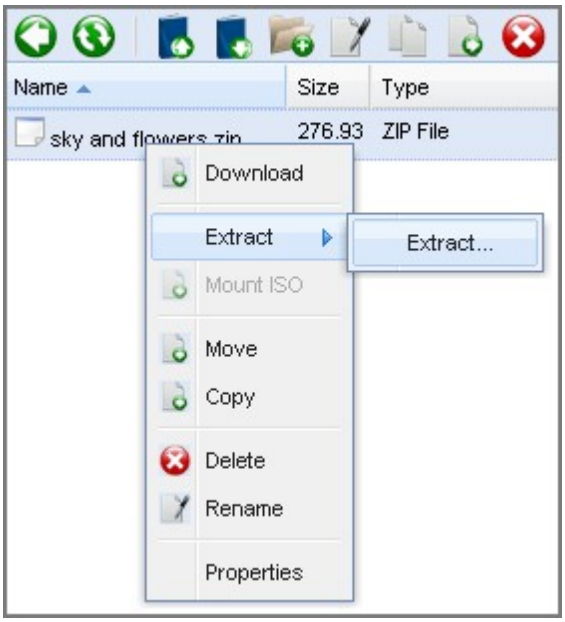
i. Select a file or folder to delete.

ii. Click (Delete) on the toolbar.

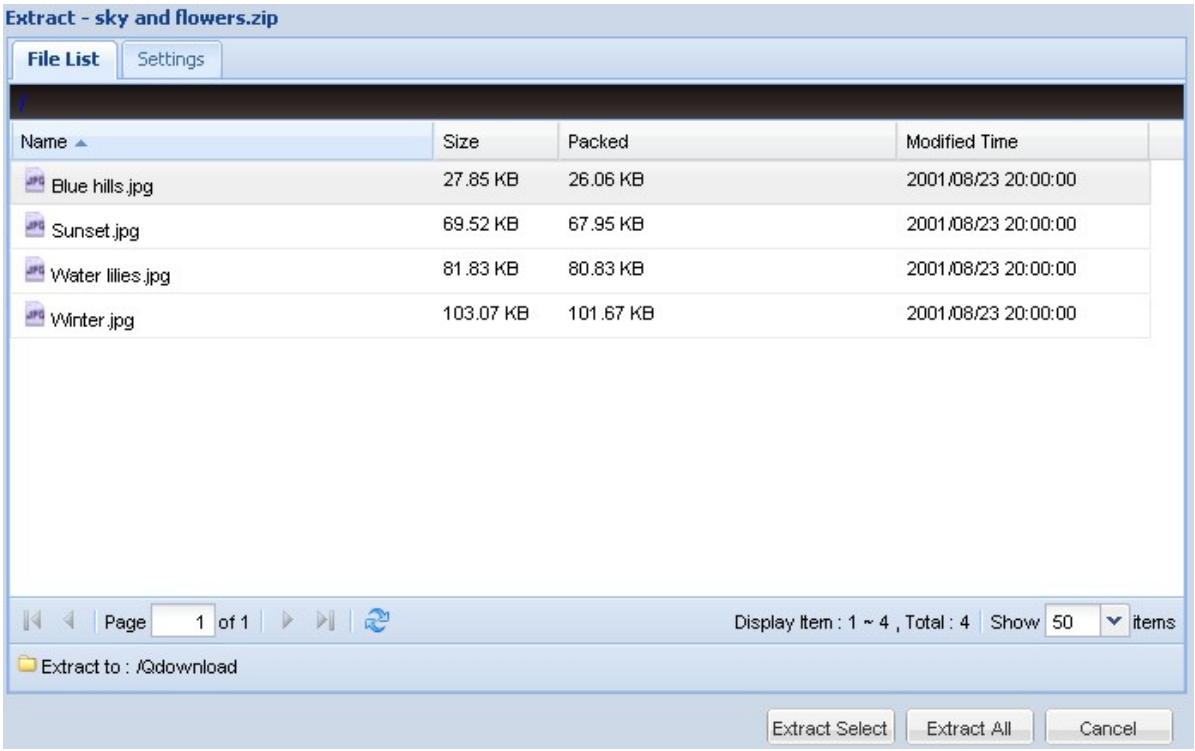
iii. Confirm to delete the file or folder.

Extract files

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

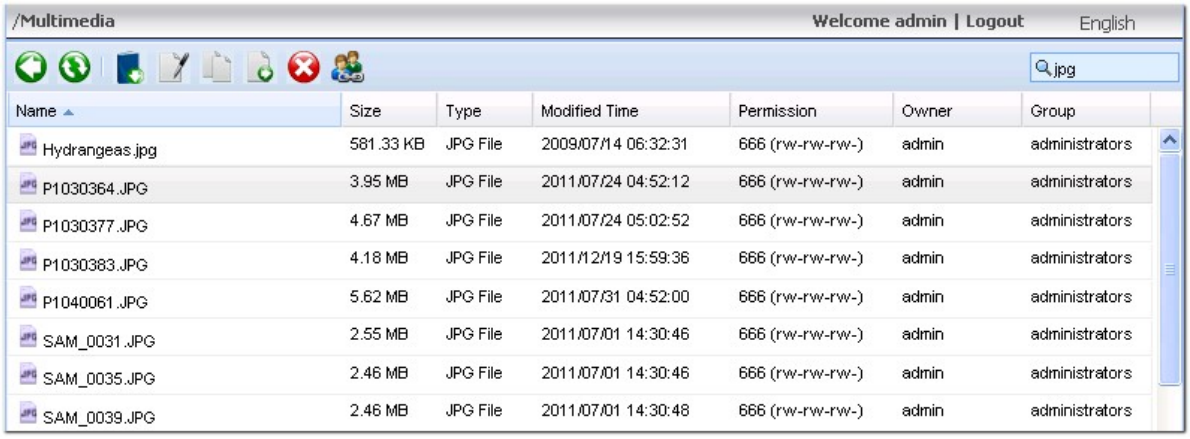


ii. Select the files to extract and configure the extraction settings.



Files/Folders Search

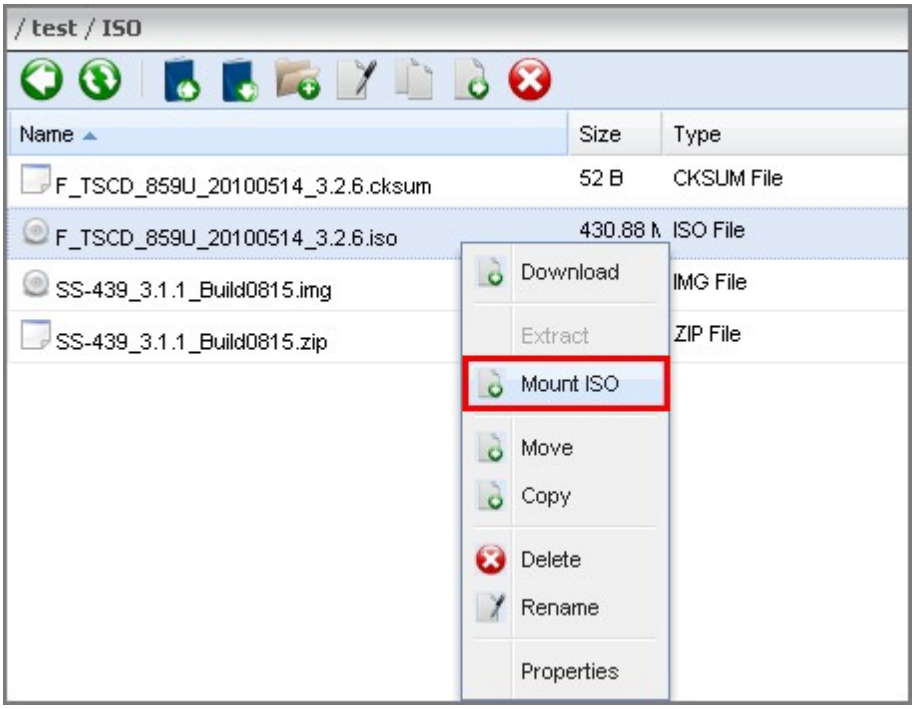
Web File Manager supports smart search of files, sub-folders, and folders on the NAS. You can search a file or folder by all or part of the file or folder name, or by the file extension, for example, AVI, MP3.



Mount ISO Shares

To mount an ISO file on the NAS as a network share, follow the steps below.

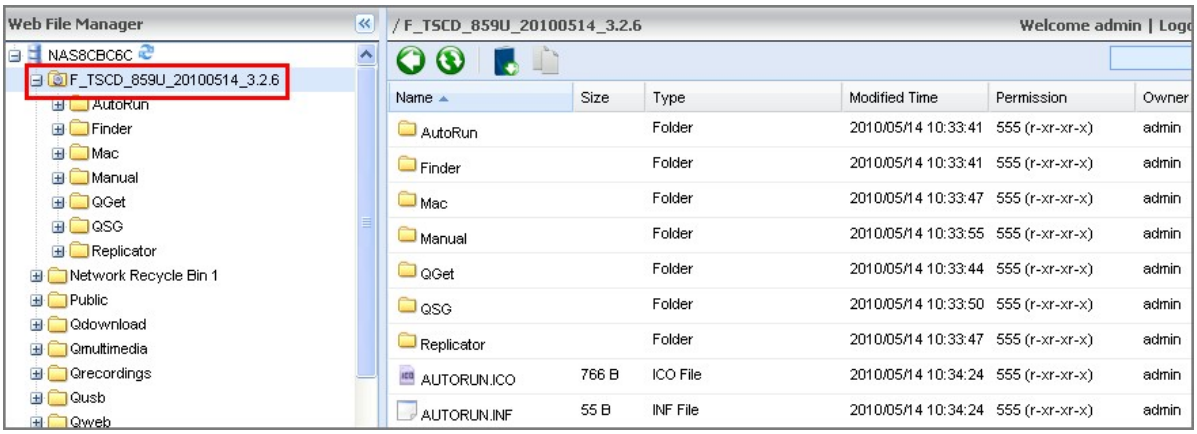
Locate the ISO file on the NAS. Right click the file and select "Mount ISO".



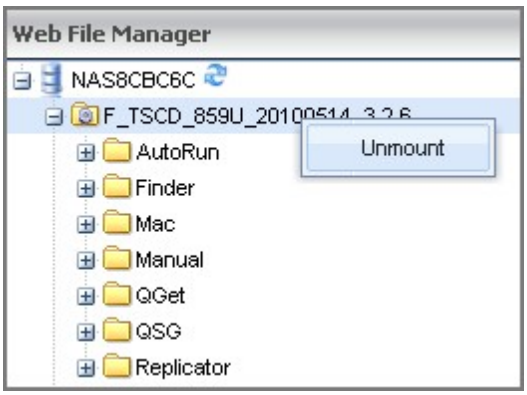
Enter the share name and click "OK".

Click "OK" to confirm.

The ISO share will appear on the folder list. You can access the contents of the ISO image file. You can login the NAS web interface with an administrator account and specify the access rights of the users in "Access Right Management" > "Share Folders" > "ISO Share Folders".

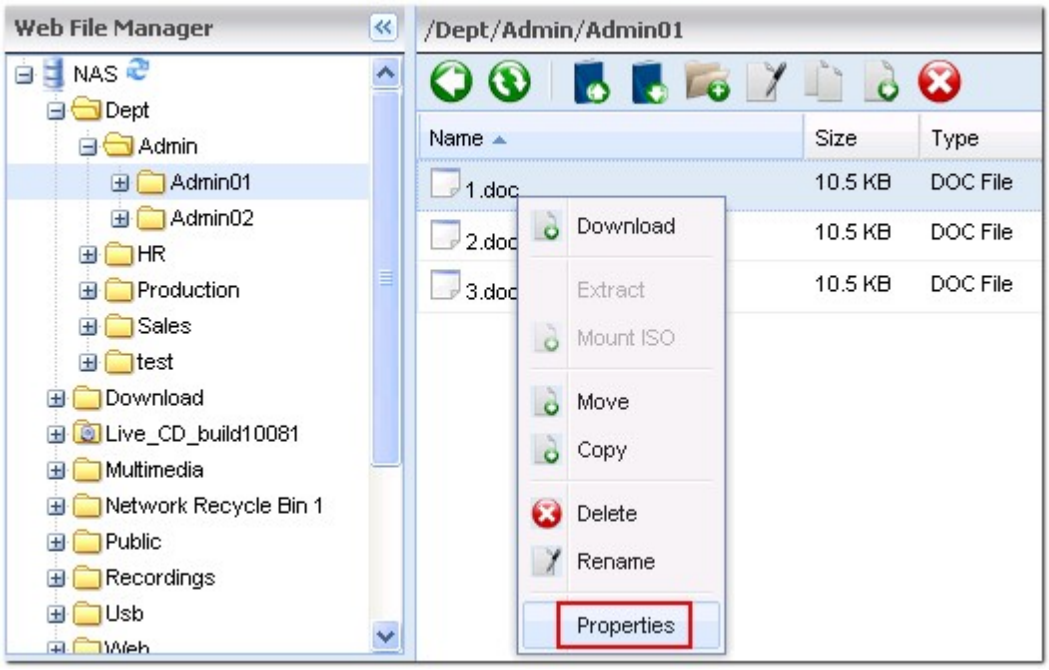


To unmount the share, right click the folder name and select "Unmount". Click "Yes" to confirm and then click "OK" to unmount.



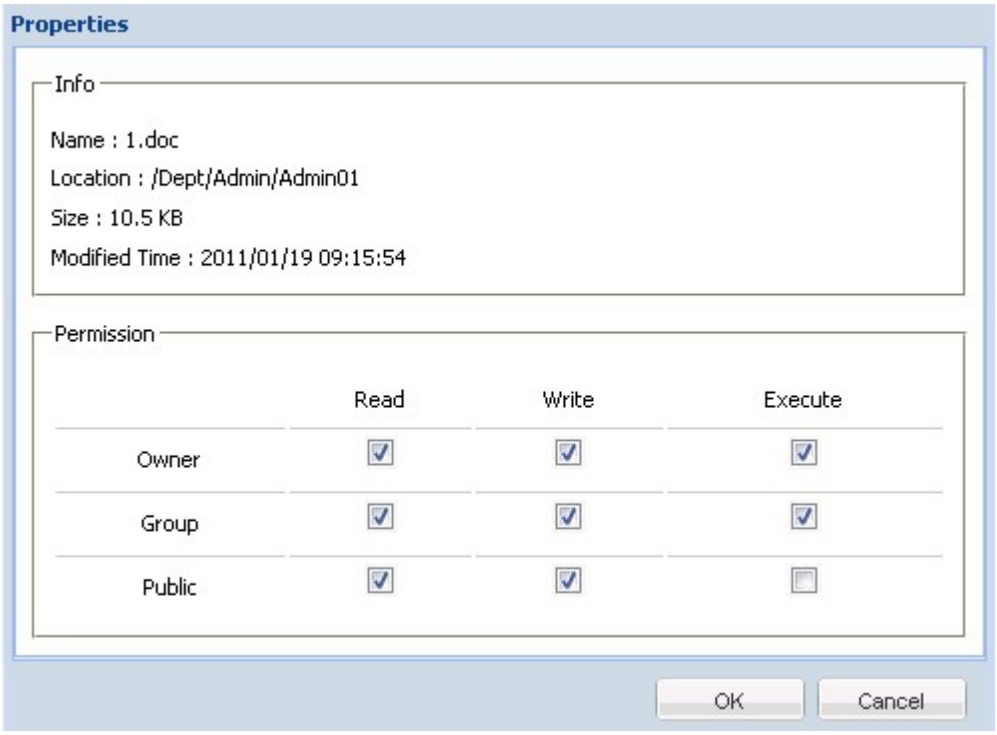
File/Folder Level Permissions

You can set file or folder level permissions on the NAS by Web File Manager. Right click a file or folder and select “Properties”.

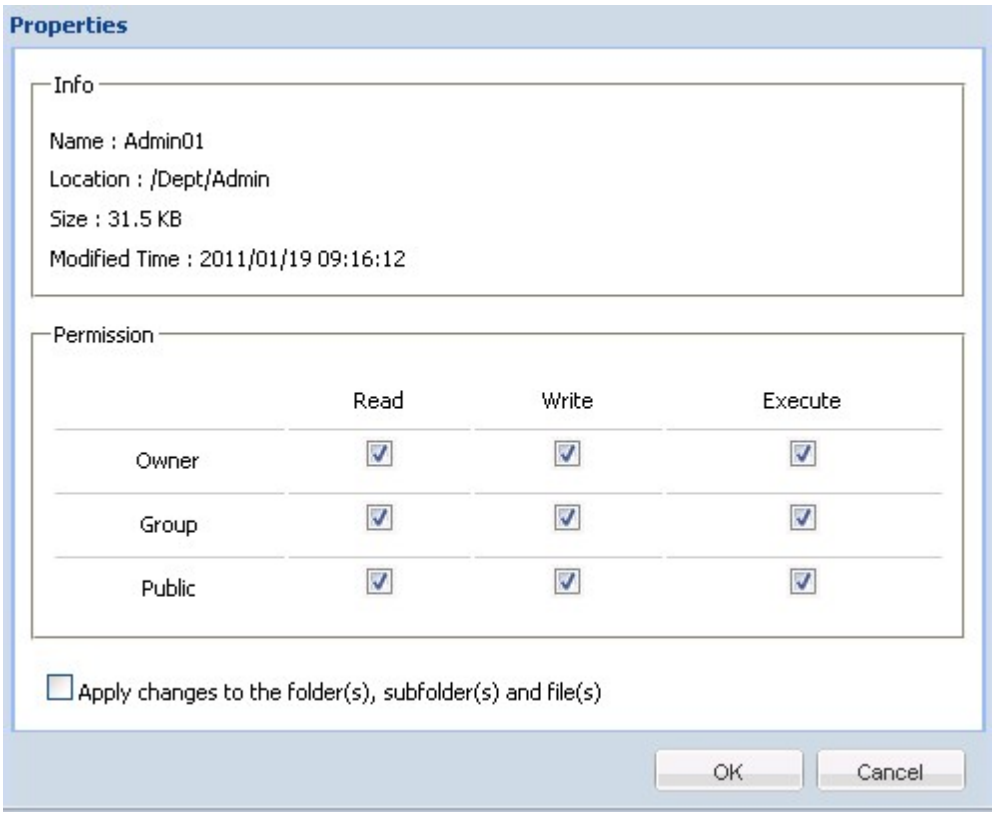


If the “Advanced Folder Permissions” option is disabled in “Access Right Management” > “Share Folder” > “Advanced Options”, the following settings will be shown. Define the Read, Write, and Execute access rights for Owner, Group, and Public.

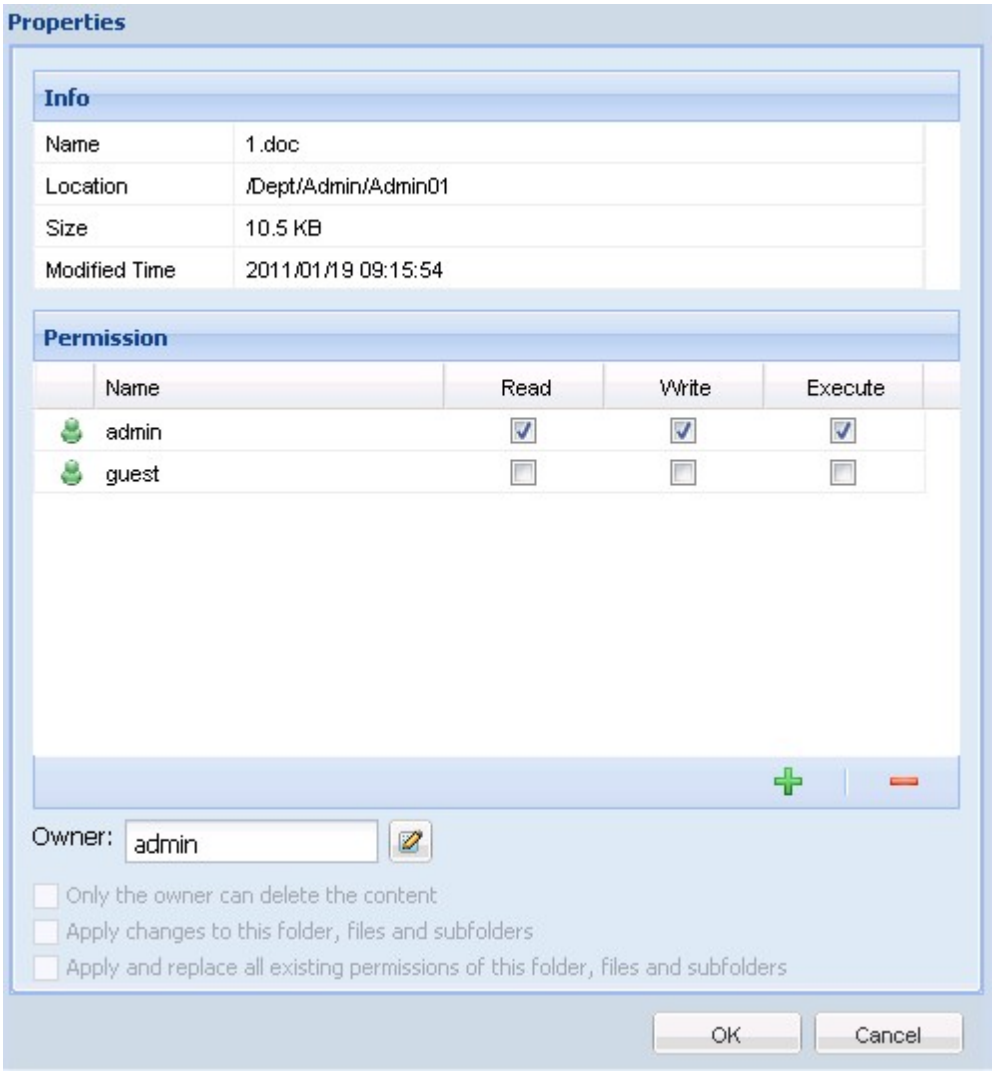
- Owner: Owner of file or folder.
- Group: Group owner of the file or folder.
- Public: Any other (local or domain member) users who are not the owner or a member of the group owner.



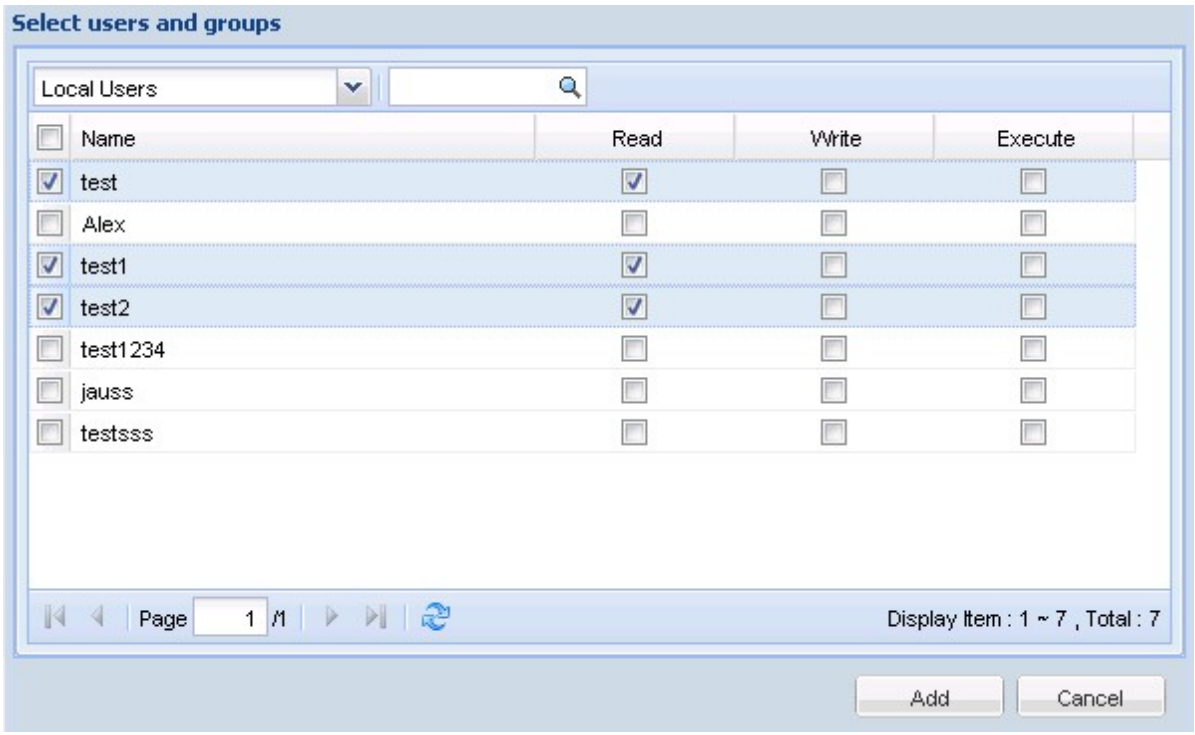
If a folder is selected, you can choose "Apply changes to folder(s), subfolder(s) and file(s)" to apply the settings to all the files and subfolders within the selected folder. Click "OK" to confirm.



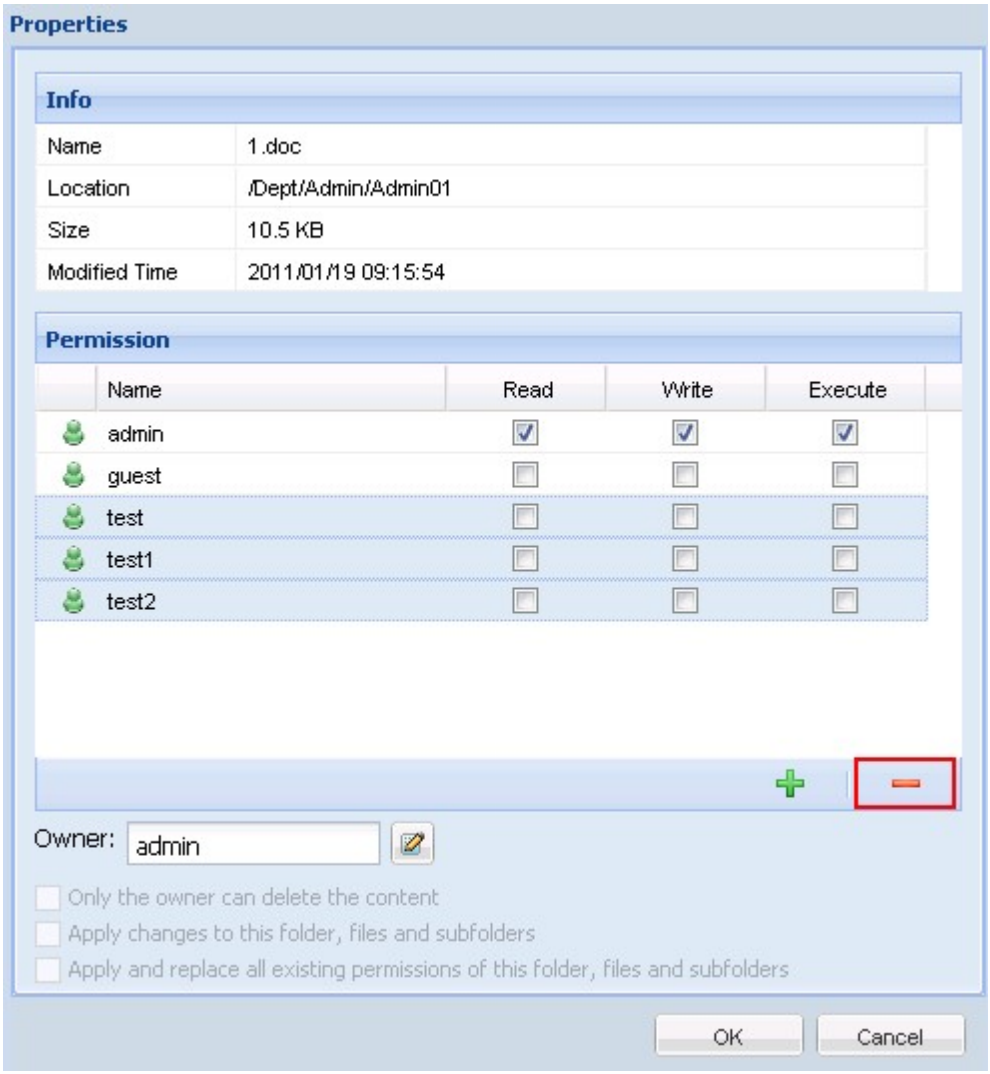
If the “Advanced Folder Permissions” option is enabled in “Access Right Management” > “Share Folder” > “Advanced Options”, you will be able to specify the file and folder permissions by users and user groups. Click .



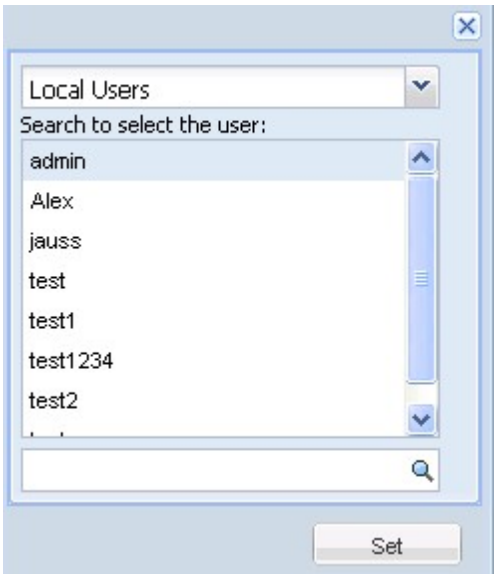
Select the users and user groups and specify the Read, Write, Execute rights. Click “Add”.



To remove the permissions on the list, select the user(s) or user group(s) and click .

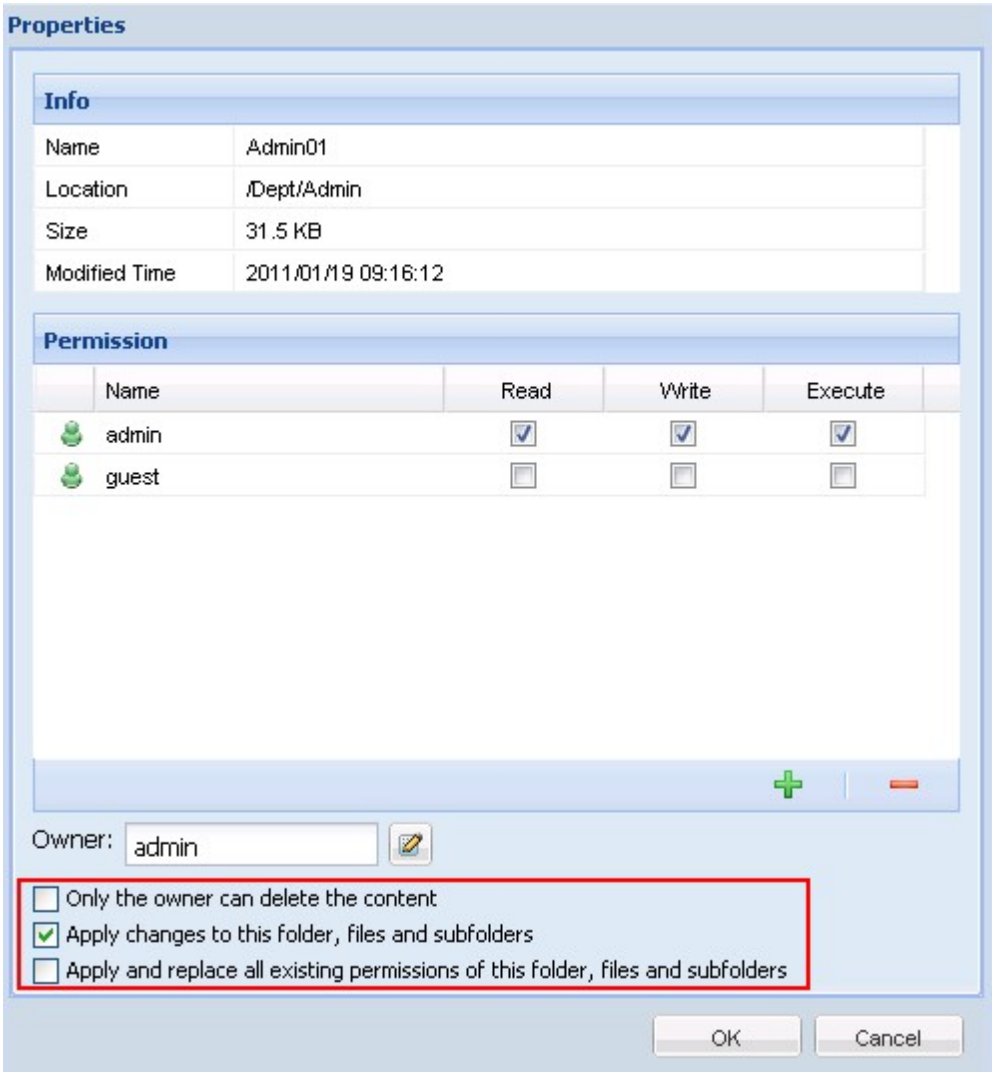


You can also define the file and folder owner by clicking . Select a user from the list or search a user name. Then click “Set”.



The following options are available for folder permission settings. You are recommended to configure folder permissions and subfolder permissions in "Access Right Management" > "Share Folders"233.

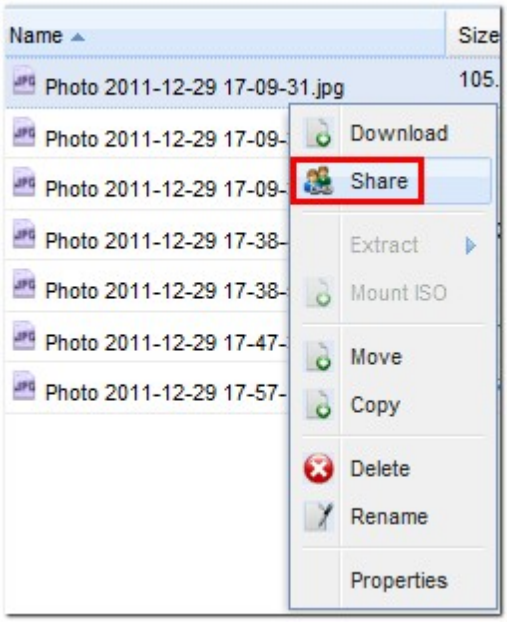
- Only the owner can delete the contents: When you apply this option to a folder, the first-level subfolders and files can be deleted only by their owner.
- Apply changes to files and subfolders: Apply changed permissions settings except owner protection to all the files and subfolders within the selected folder. The option "Only the owner can delete the contents" will not be applied to subfolders.
- Apply and replace all existing permissions of this folder, files, and subfolders: Select this option to override all previously configured permissions of the selected folder and its files and subfolders except owner protection. The option "Only the owner can delete the contents" will not be applied to subfolders.



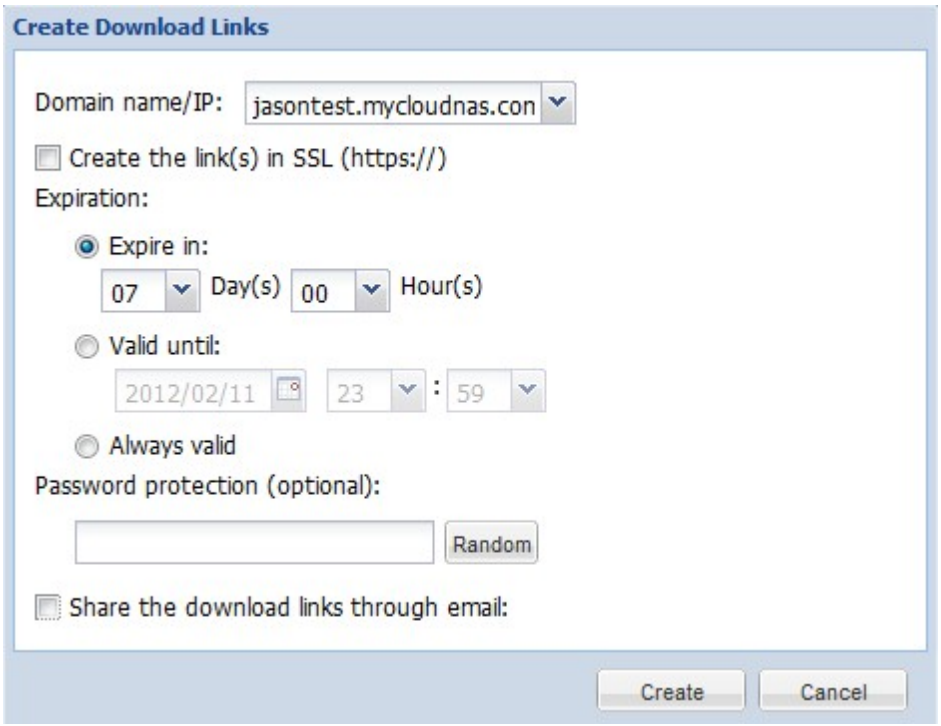
Share Files

Note: This feature can only be used by admin.

To share the files on the NAS by Web File Manager, select the files and click or right click the file (s) and select "Share".

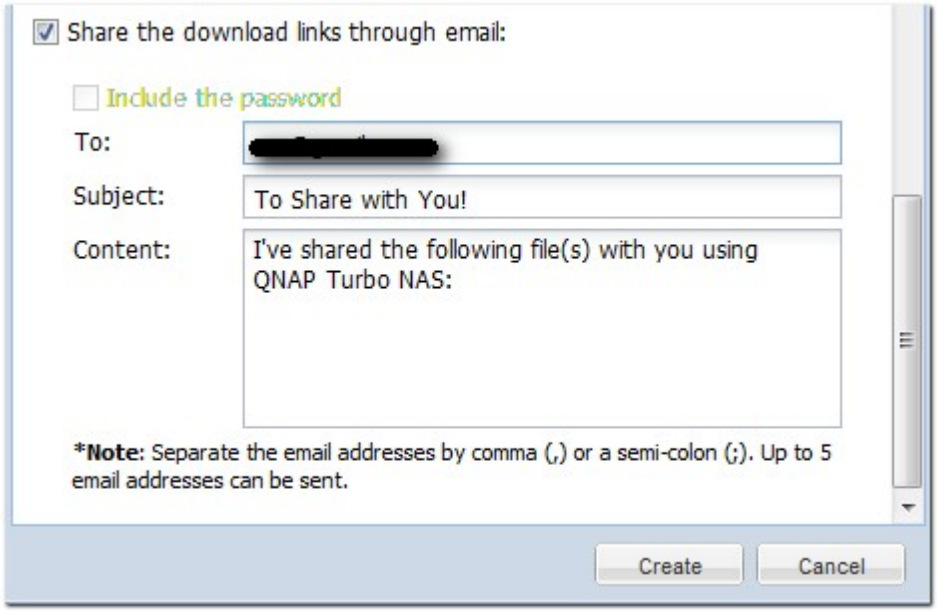


Select the IP or domain name of the NAS. Select to create the link(s) in SSL (optional) and specify the expiration settings and enter a password (optional).

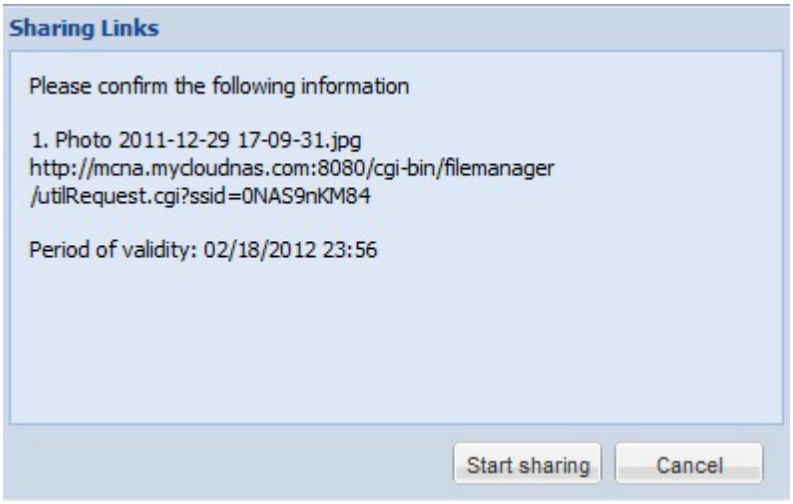


To share the links by emails, select "Share the download links through email" and enter the contents. Click "Create".

Note: To use this function, the mail server settings must be properly configured in "System Administration" > "Notification" > "Configure SMTP Server".



Confirm the information and click "Start Sharing".



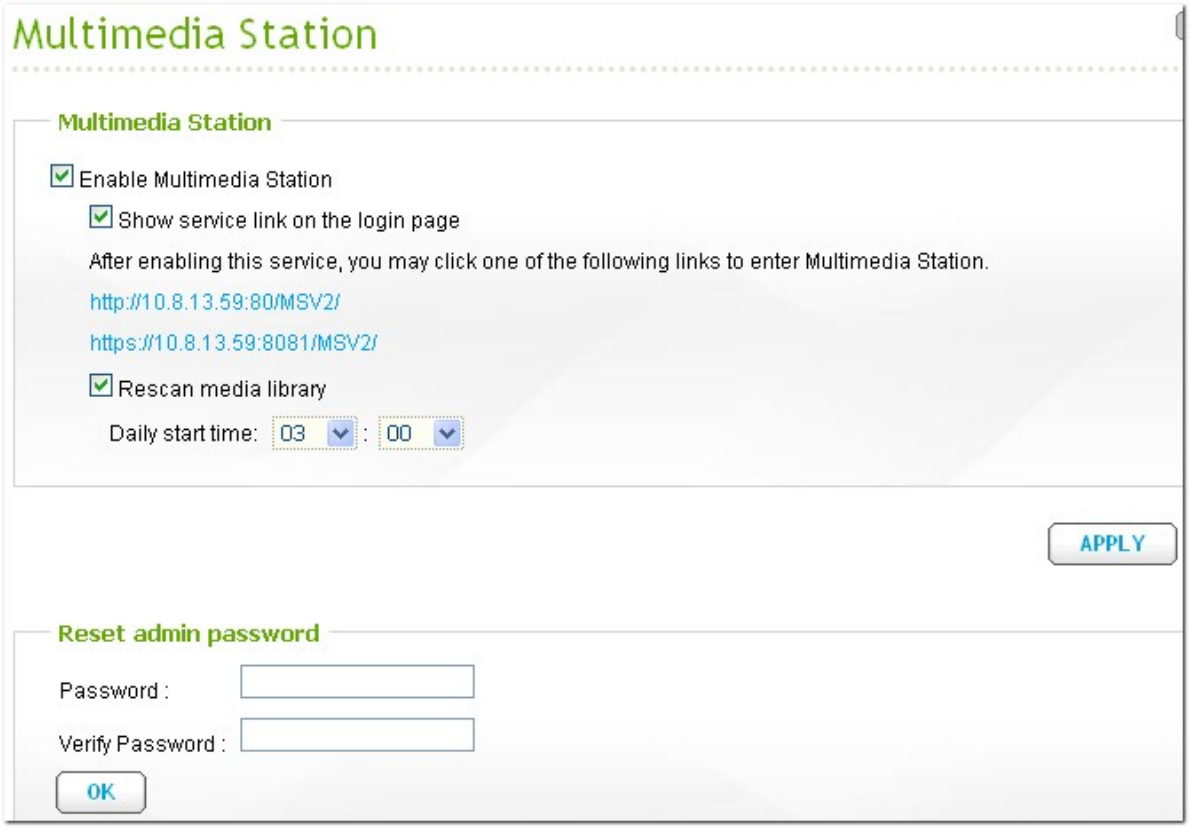
7.2 Multimedia Station

Multimedia Station is a web-based application which lets you view your photos, play music, and videos on the NAS by a web browser. You can also share the multimedia files with your friends and publish photos to popular social networking sites such as Facebook, Plurk, Twitter, Blogger, and so on.

To use Multimedia Station, follow the steps below.

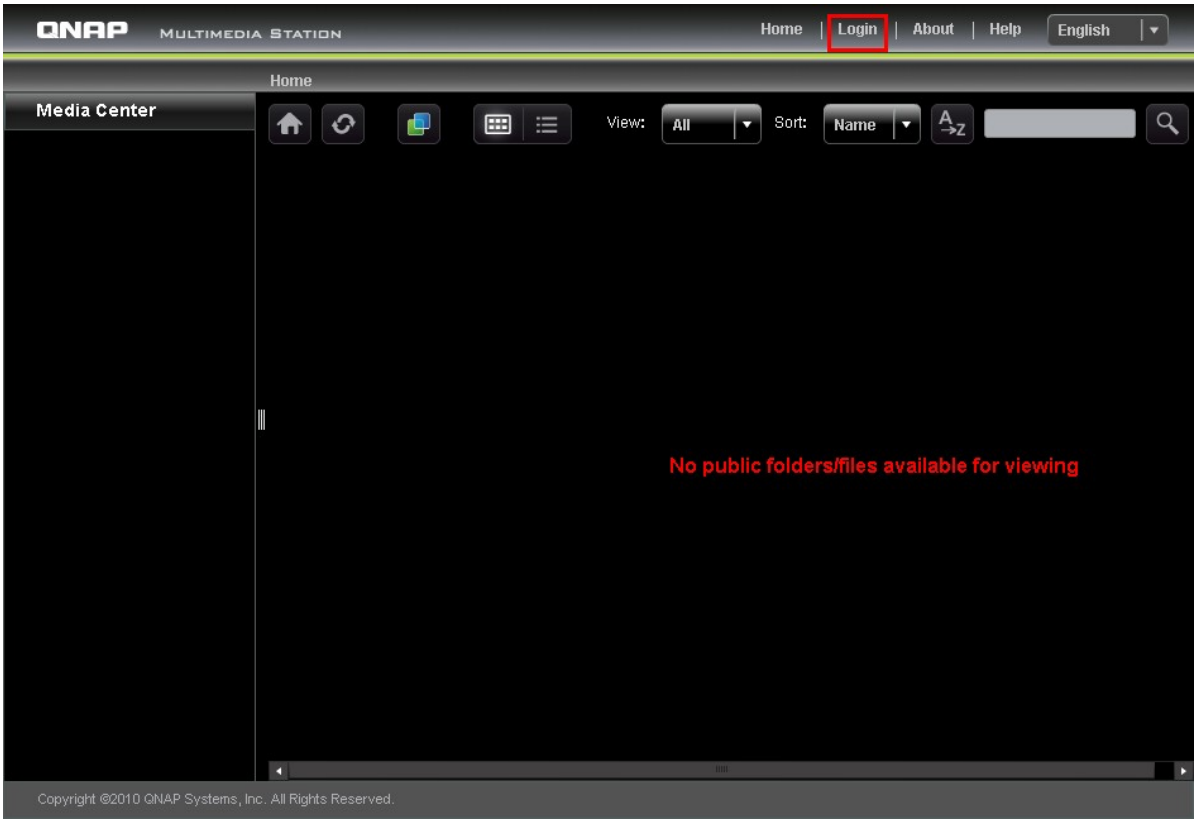
1. Go to "Network Services" > "Web Server". Turn on the web server feature. To allow access to Multimedia Station by HTTPS, turn on the option "Enable Secure Connection (SSL)".

2. Go to "Application Servers" > "Multimedia Station". Enable the service. Next, go to the web page of Multimedia Station by http://NAS_IP:80/MSV2/ or https://NAS_IP:8081/MSV2/ (secure connection). The port number may be different according to your own settings.

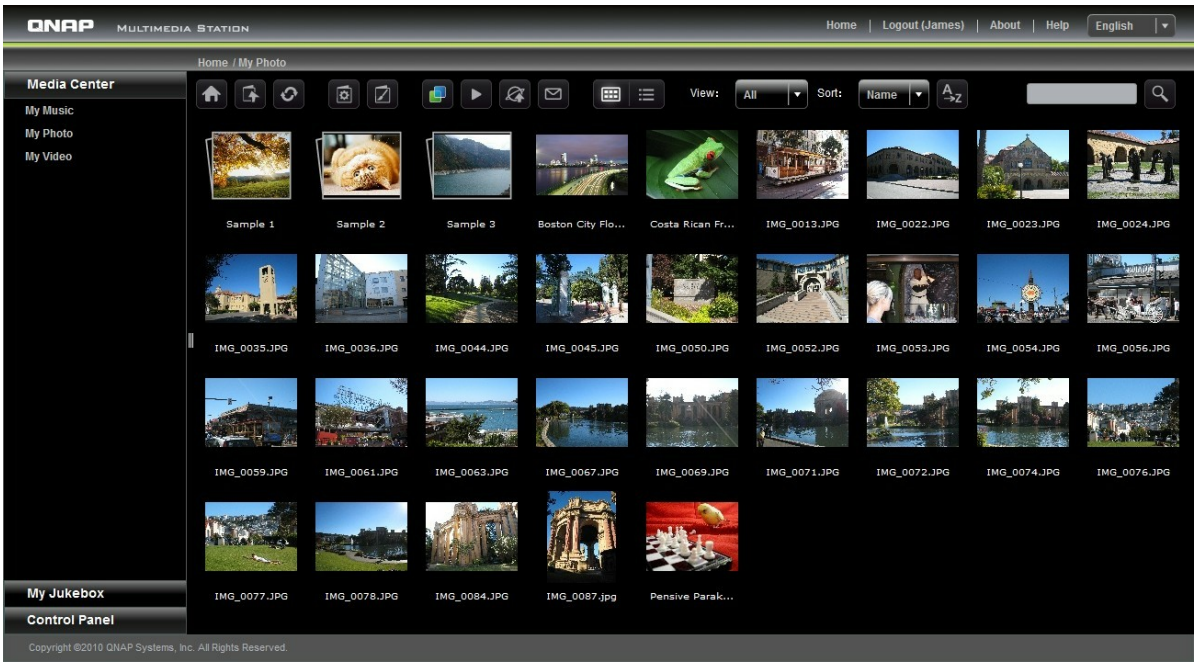


3. The first time you connect to Multimedia Station, enter a new password for the “admin” account. Then click “Submit”. If you have created user accounts for the previous version of Multimedia Station, you may select “Keep existing user accounts” to reserve the user accounts. Note that the user accounts (including admin) of Multimedia Station are different from the system user accounts on the NAS. For security concern, you are highly suggested to set a different password for admin. The password must be 1 to 16 characters long. It can only contain A-Z, a-z, 0-9, -, !, @, #, $, %, _.

4. When the page of Multimedia Station is shown, click "Login". Enter the user name with access right to this service and the password. If you login as the administrator (admin), you can create new users and configure other advanced settings.



Multimedia Station consists of Media Center, My Jukebox, and Control Panel.



Media Center

The folders and multimedia files of the default network share (Qmultimedia/Multimedia) of Multimedia Station are shown in Media Center. You can view or play the multimedia contents (images, videos, and audio files) on the NAS on the web browser over LAN or WAN.

Supported file format

Type	File format
Audio	MP3
Image	JPG/JPEG, GIF, PNG (Animation will not be shown for animated GIF files)
Video	Playback: FLV, MPEG-4 Video (H.264 + AAC) Transcode: AVI, MP4, M4V, MPG, MPEG, RM, RMVB, WMV (Files will be converted to FLV)

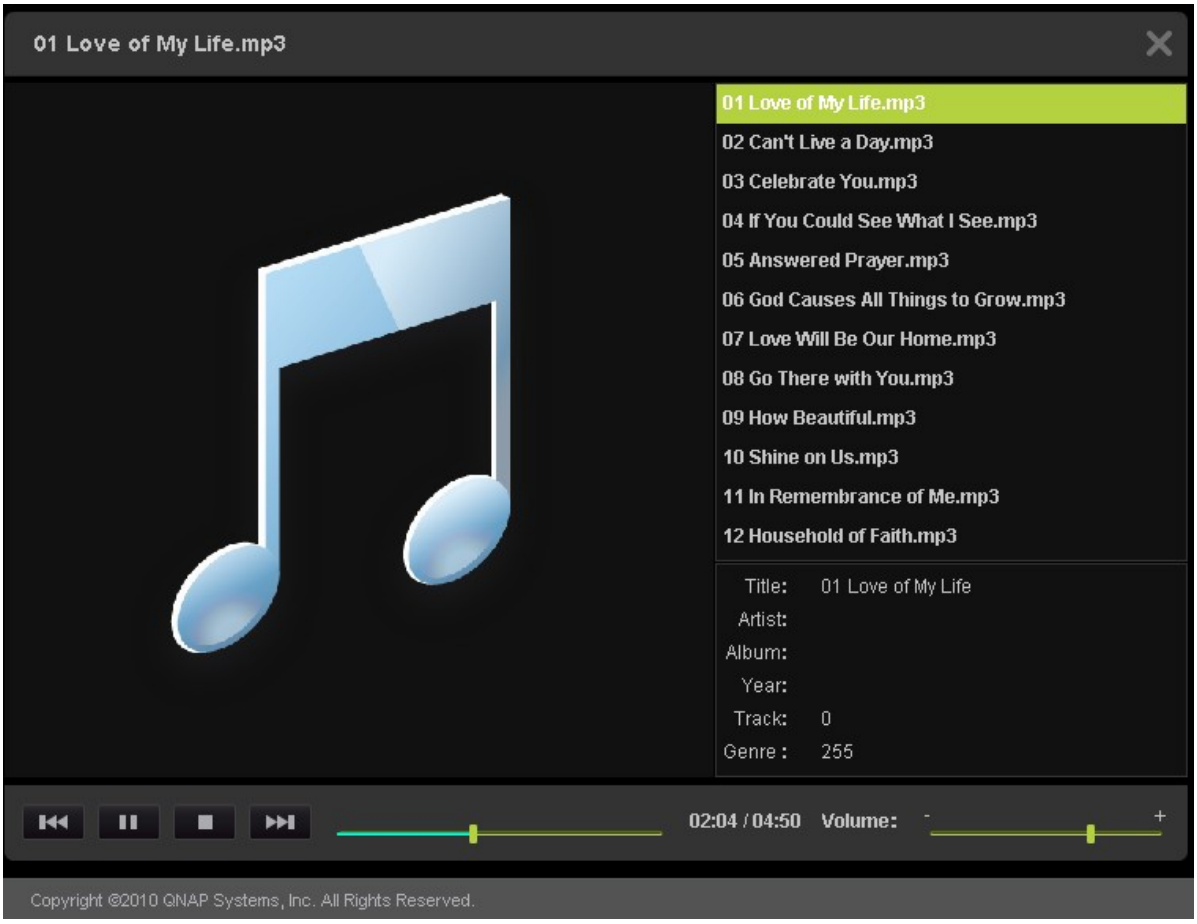
Icon	Description
	Home Return to the home directory of Multimedia Station.
	Parent Directory Return to the parent directory.
	Refresh Refresh current directory.
	Manage Album* You can: 1. Create new album under the current directory and 2. Add new files to this album by copying or uploading files to this directory.
	Set Album Cover* You can set up the album cover for each album/directory by specifying one photo in this album/directory.
	Cooliris Browse your photos in 3-dimensional way with Cooliris. You need to install the Cooliris plug-in for your browser first.
	Slide Show Start slide show. You can set up the photo frame, background music, and animation in the slide show mode.
	Publish* Publish the chosen photos (max. 5 photos) to popular social networking sites. It now supports: Twitter, Facebook, MySpace, Plurk, Windows Live, and Blogger. Note that the album must be set to public (Control Panel > Set Folder Public) before it can be published, and Multimedia Station must be accessible from the Internet. It is suggested to set up the DDNS for the NAS before using this feature.
	E-mail* Send photos (max. 5 photos) to friends by e-mails. Note that you have to set up the SMTP server in the NAS administration console before using this feature.
	Thumbnails You can browse the files in thumbnail view. This is the default view in Multimedia Station.
	Details

	You can browse the files in detailed view. It supports the following functions: Open, Rename, Delete, Download, and Full Image View.
	Sort You can choose to sort files alphabetically in ascending or descending order.
	Search You can search files by this function. Note that it only supports search within the current directory.

*Options that can be operated by administrators only.

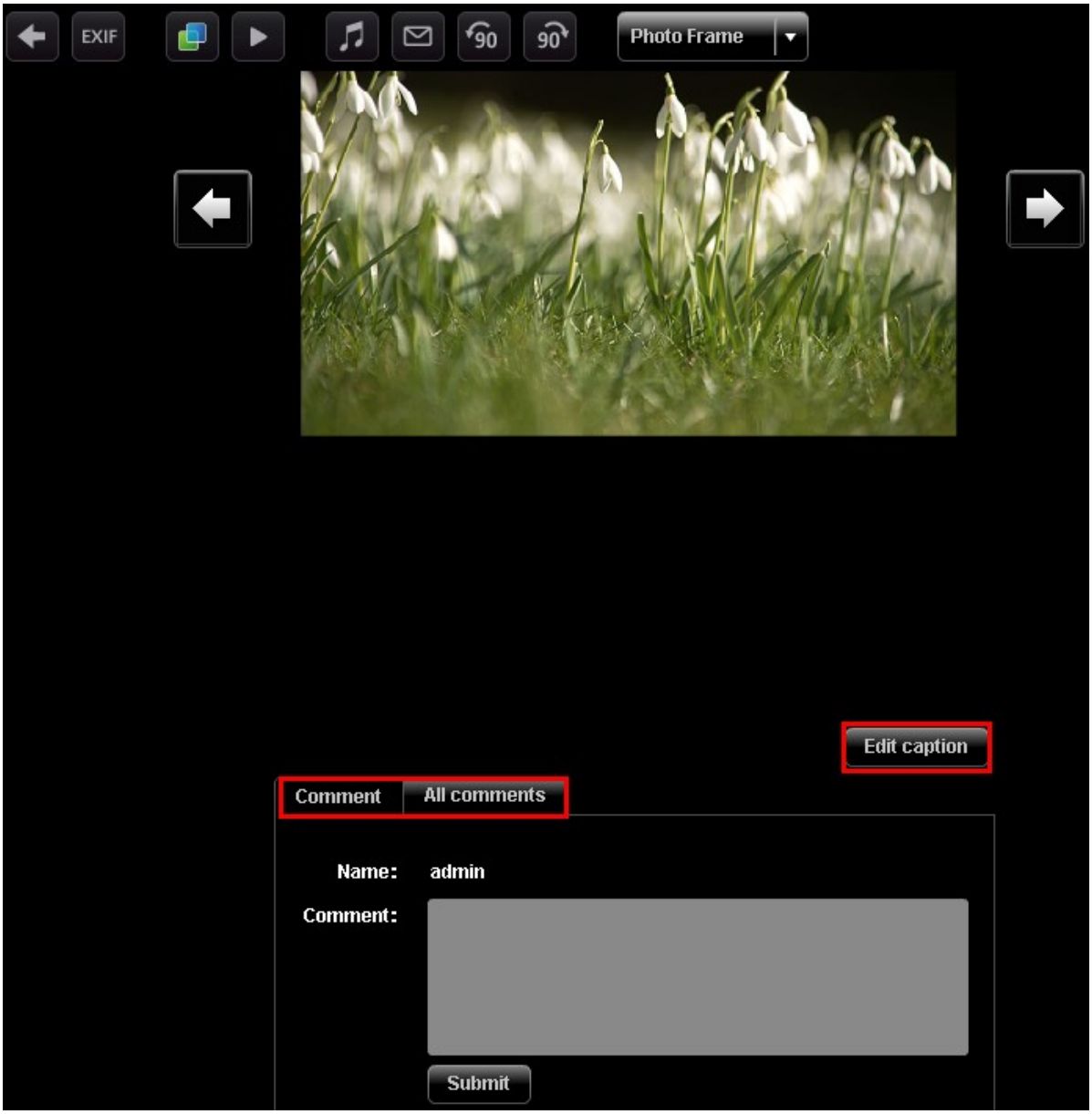
Play music

The NAS supports playing music files on the web browser. Simply click a file (MP3) on the web page, the NAS will start playing it. If you click a music file in a folder, all other supported music files in the folder will also be shown in the playlist and played. Click "X" to exit the playback page.



View image files

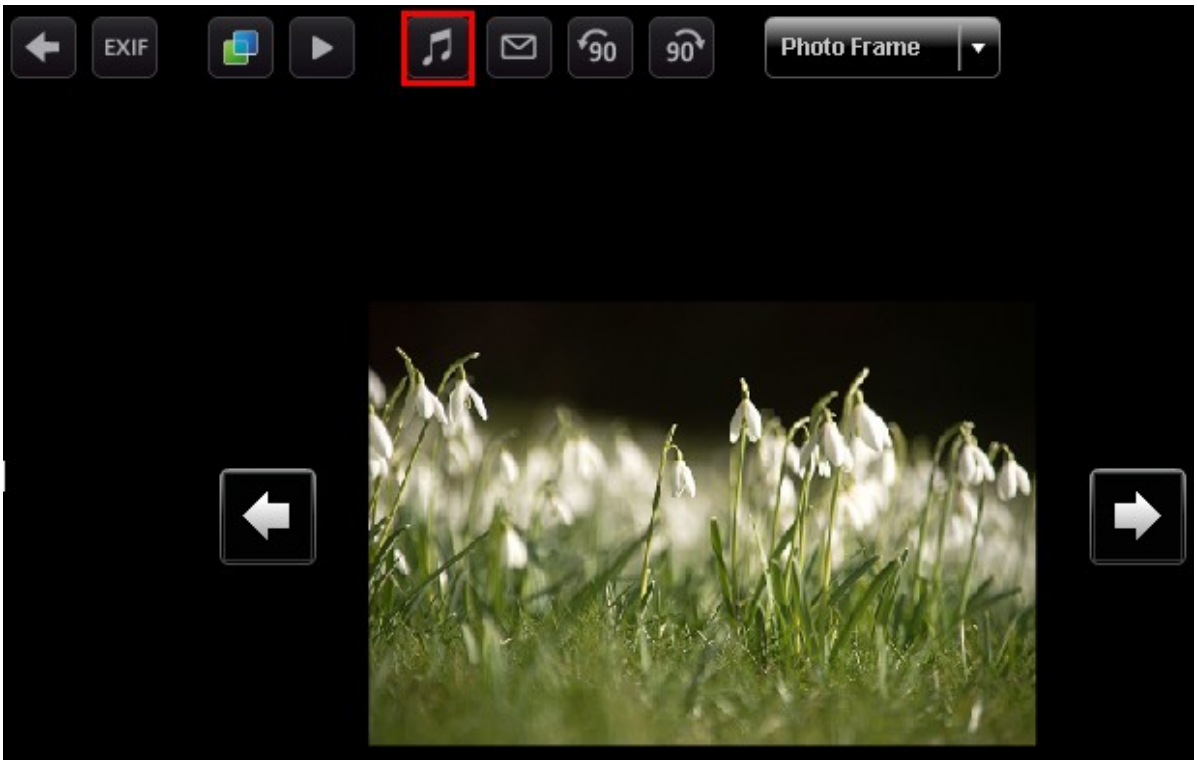
When viewing an image file, you can click “EXIF” to view the detailed information such as file name, size, date, and aperture. To add a caption for the file, click “Edit caption” and enter the description. The description must not exceed 512 characters.
You can also submit your comments on the image file and view the comments from other users on “All comments”. Each comment cannot exceed 128 characters.



Set background music

To set the background music of an image file or a folder of image files, make sure you have created a playlist in "Control Panel" > "Playlist Editor" (to be introduced later) in Multimedia Station.

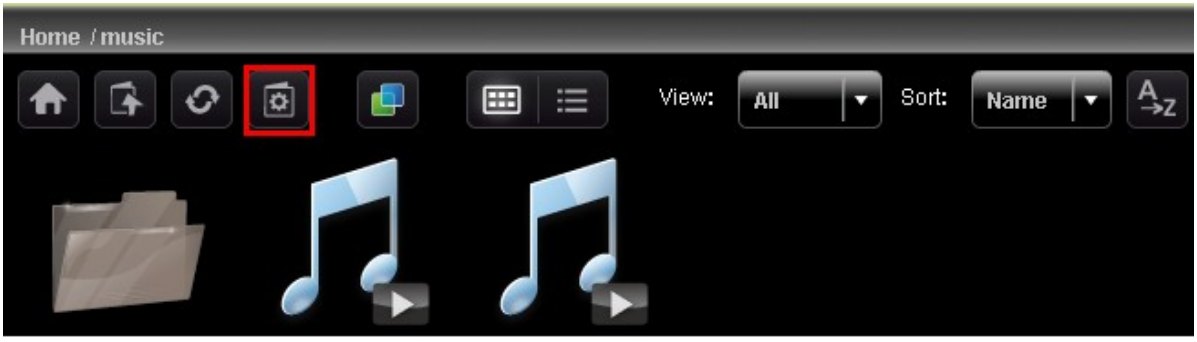
Open an image file in Media Center and click .



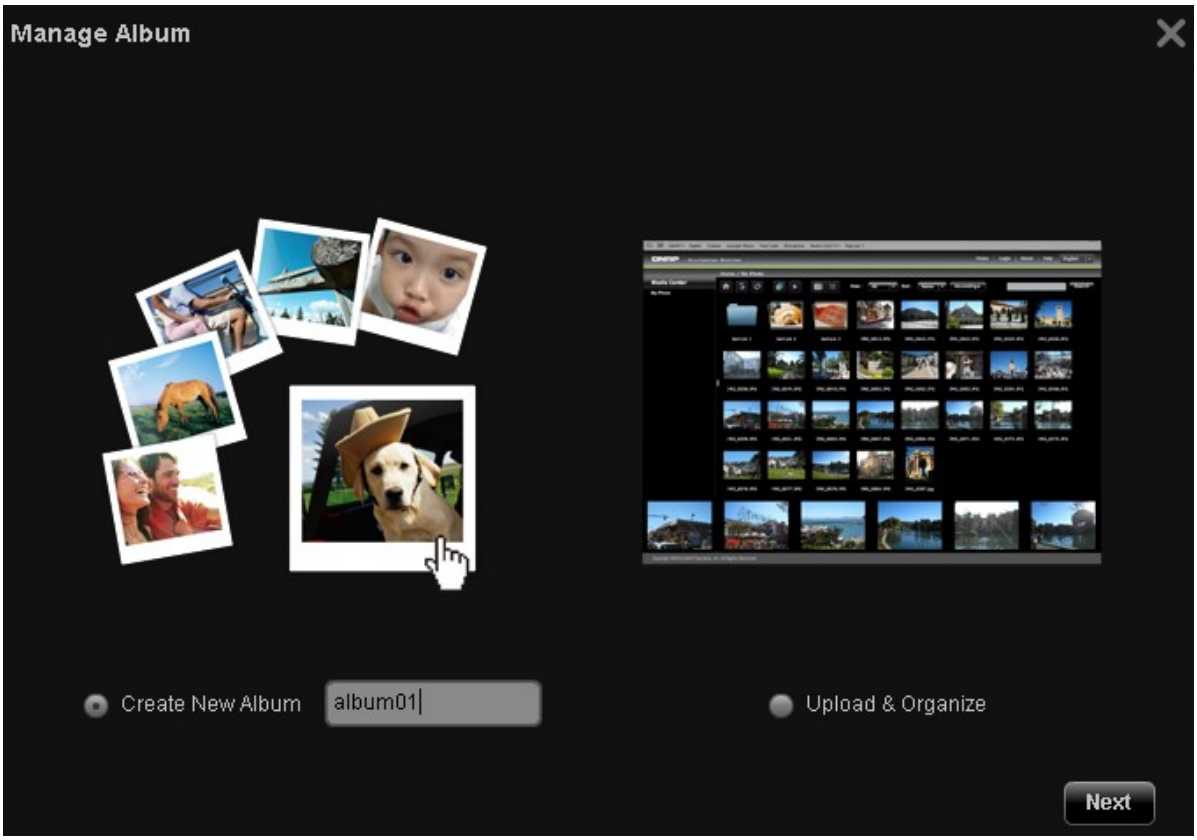
Select the playlist and click “Save”. To remove the background music, you can select “No music”.

Create album

To create an album (folder) by the web-based interface on Multimedia Station, locate the directory in Media Center. Click (Create Album).

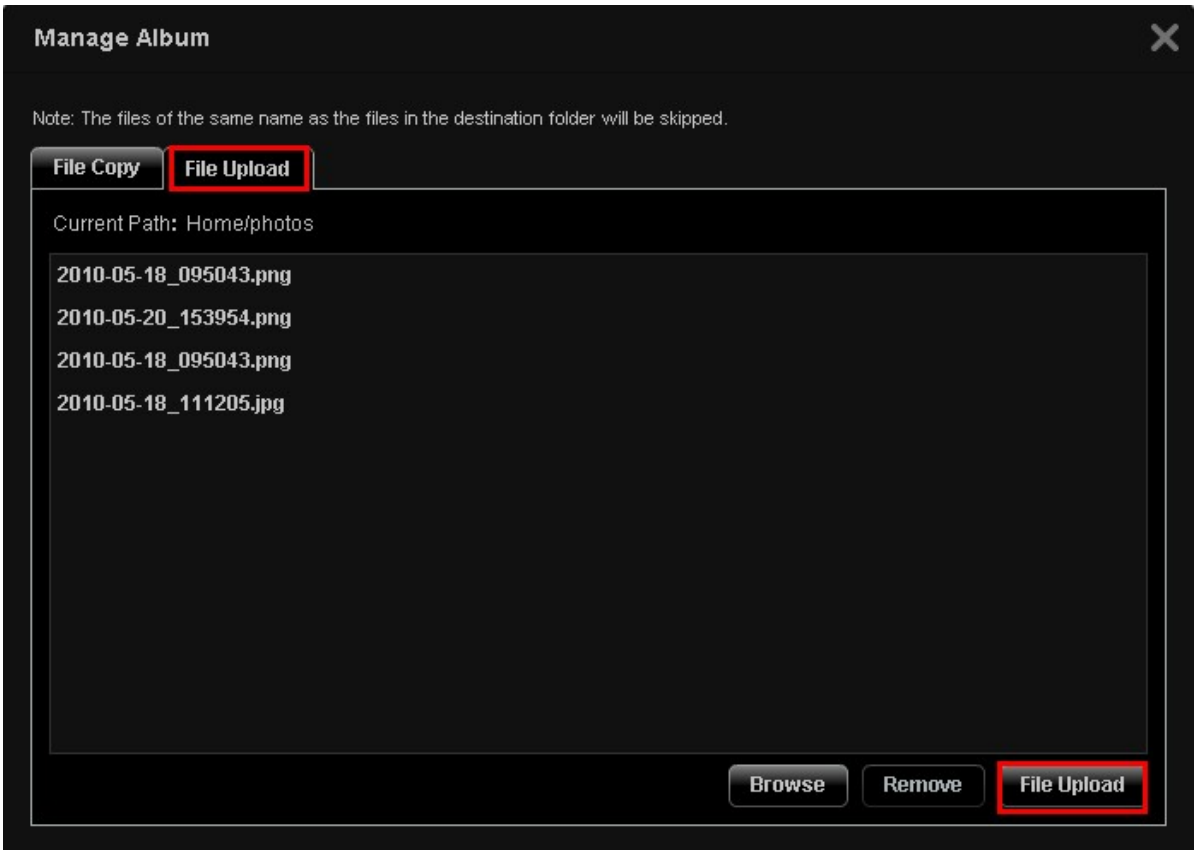


Select “Create New Album” and enter the album name. Click “Next”.
The album name must be 1 to 64 characters long, and cannot contain | \ : ? " < > *



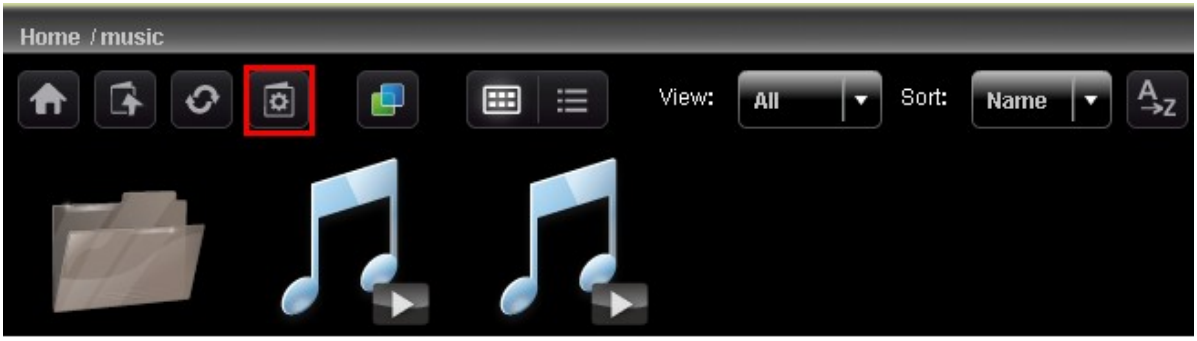
To copy the files from other location in Media center to the album, select "File Copy", choose the files to copy and click >. Then click "File Copy" to start copying the files.

To upload files to the album, click “Browse” to select the files and click “File Upload”.

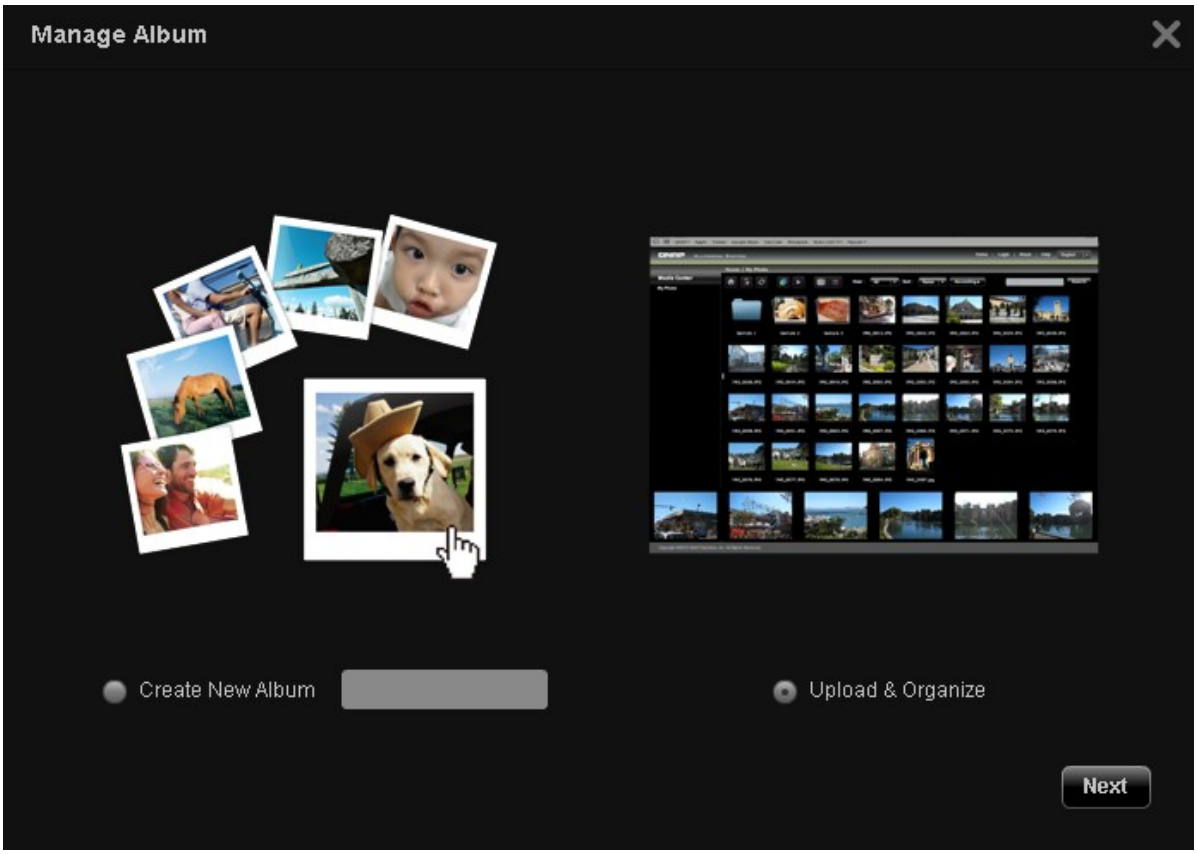


Manage album

To manage an album (folder) by the web-based interface on Multimedia Station, locate the directory in Media Center. Click (Create Album).

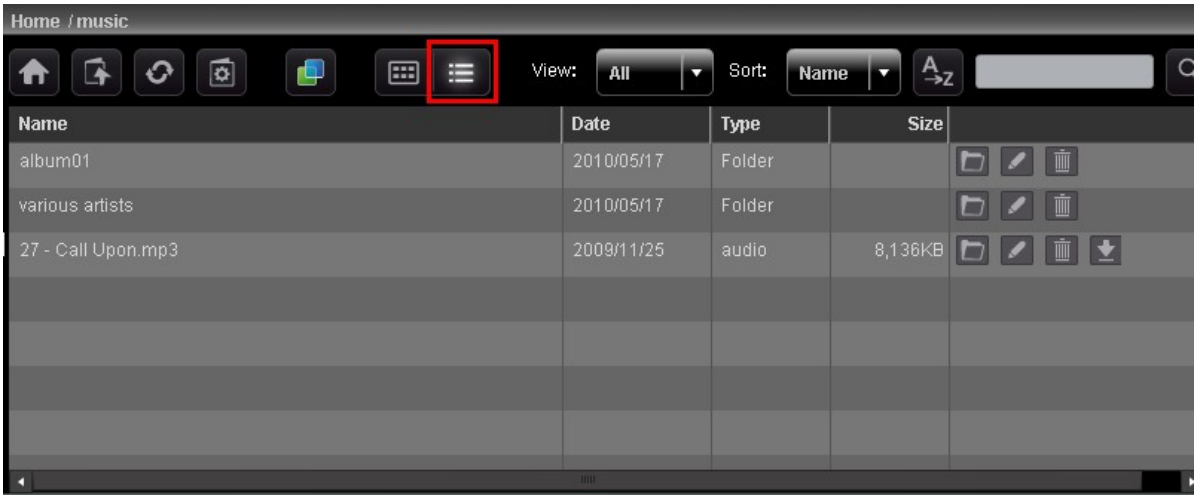


Select “Upload & Organize” and click “Next”.



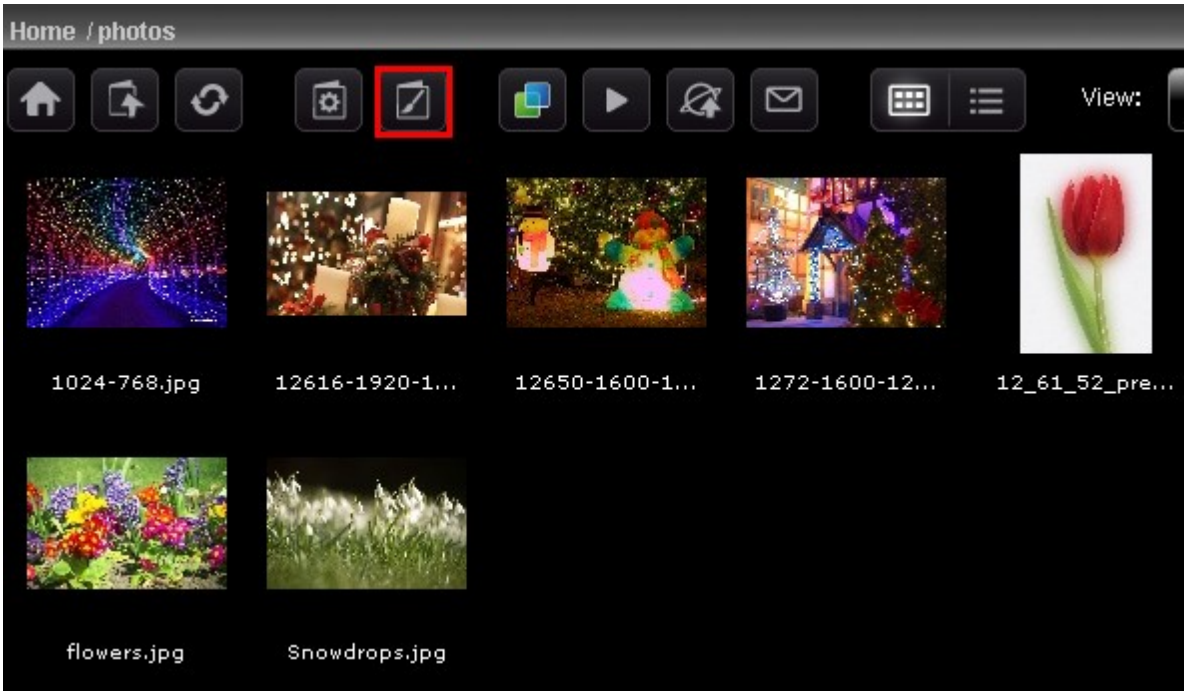
To copy the files from other location in Media center to the album, select "File Copy", choose the files to copy and click >. Then click "File Copy" to start copying the files. To upload files to the album, click "Browse" to select the files and click "File Upload".

You can click to browse the multimedia contents in details and click the icons to open, rename, delete, or download the files or folders.



Set album cover

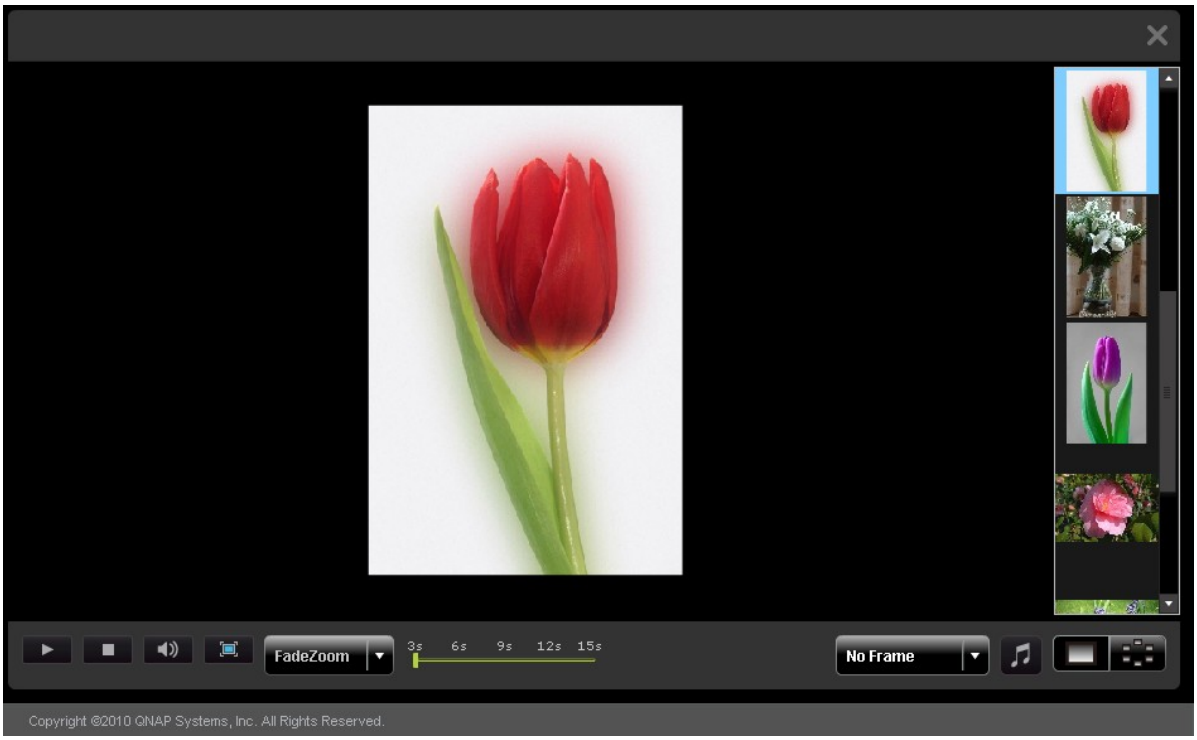
To set an image file as the album cover, click .



Select the image file and click “Save”.

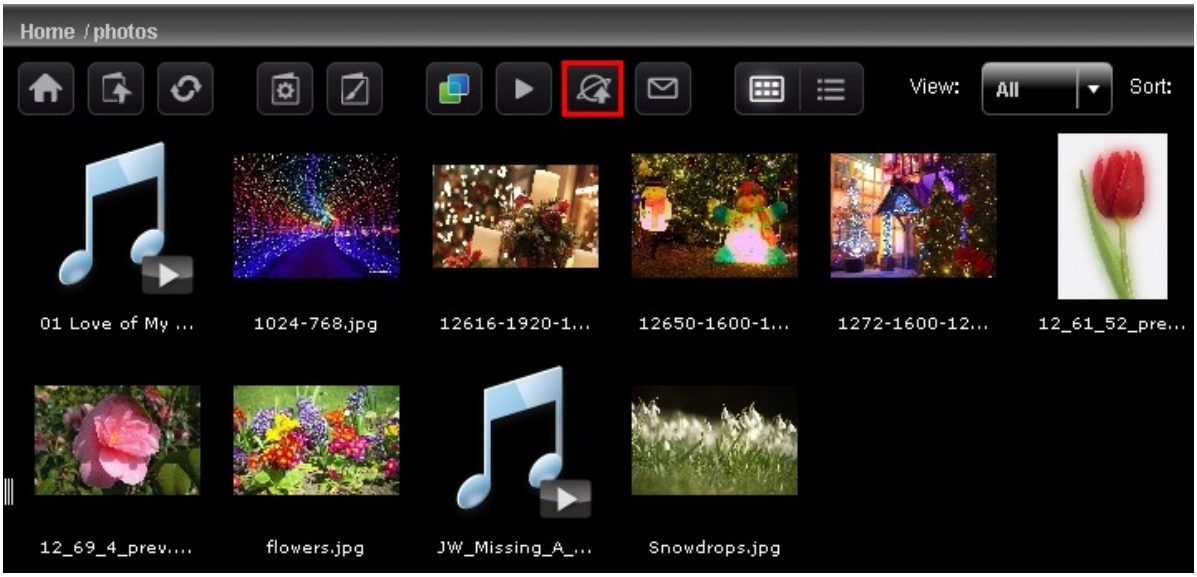
Slide Show

Click to view multiple image files in slide show. Select the playback speed (3s/6s/9s/15s) and the slide show effect (for full screen display) from the drop-down menu. You can also select the photo frame for displaying the image file. To view the image files in 3-dimensional (3D) display, click .



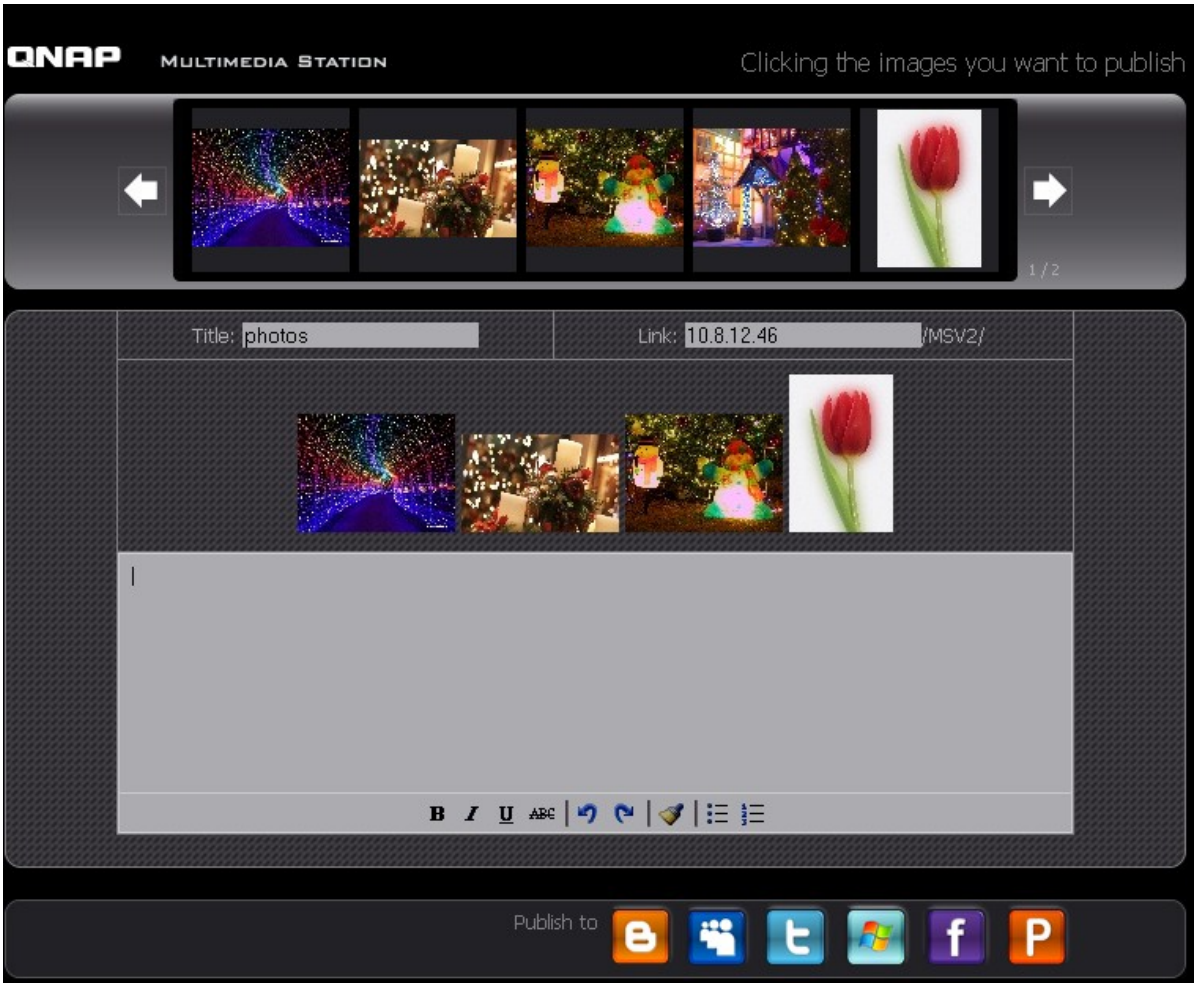
Publish image files

You can publish the image files on Multimedia Station to social networking sites such as Facebook and Twitter. Click .



Select the image files to publish. You can publish maximum 5 photos at a time. Enter the title and description. Then select the website to publish the files to and enter the login information of the website. Note that the album must be set to public (Control Panel > Set Folder Public) before it can be published, and Multimedia Station must be accessible from the Internet. It is suggested to set up the DDNS for the NAS before using this feature.

Field	Limitation
Title	Maximum number of characters: 256
Link (the IP address or host name of the NAS)	Support alphanumeric characters, dot (.), and slash (/) only Maximum number of characters: 256
Description	Maximum number of characters: 1024



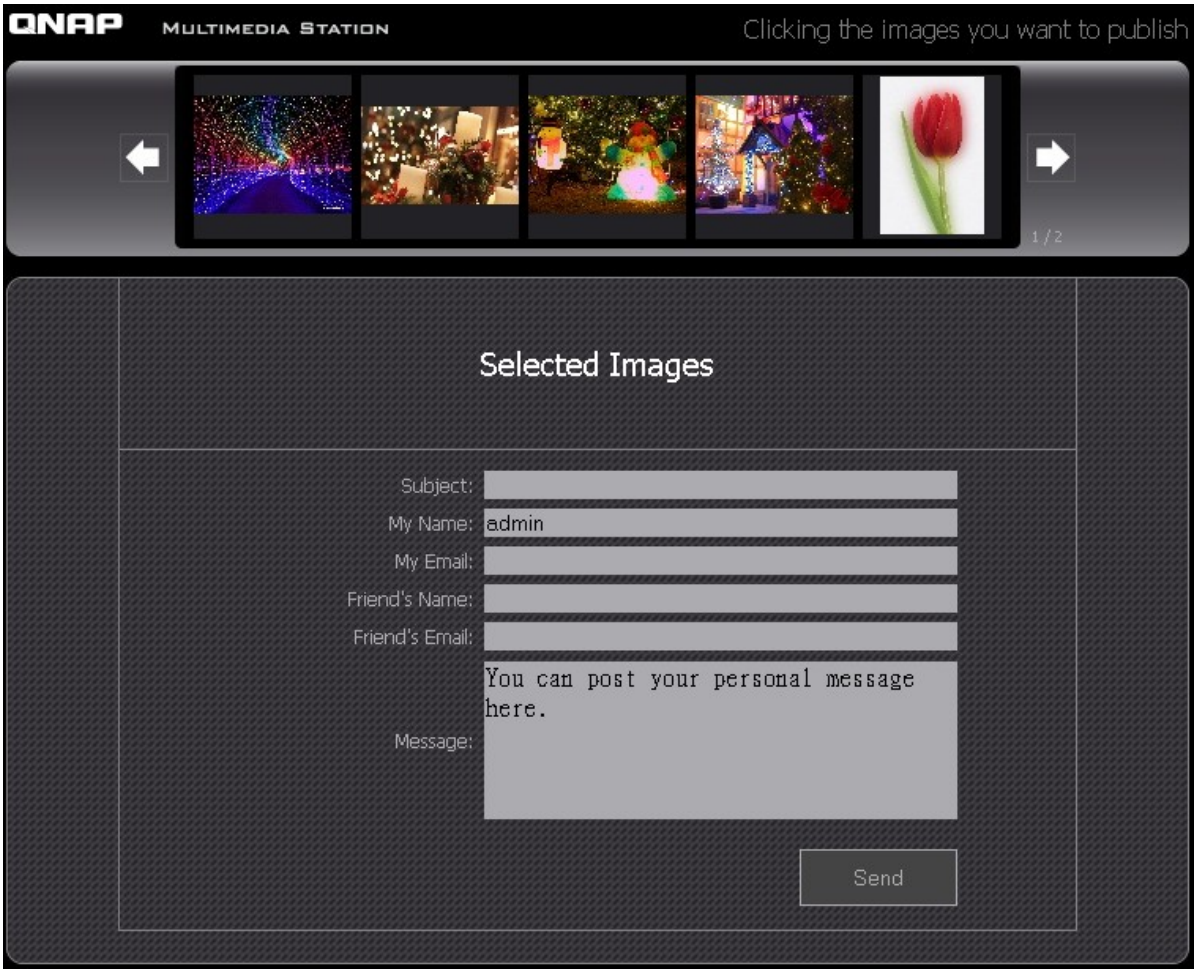
Email image files

To email the image files, make sure SMTP server settings have been correctly configured on the NAS.

Click .

Enter the information and click "Send".

Field	Limitation
Subject	Maximum number of characters: 128
My Name	The name only supports alphabets (A-Z and a-z), numbers (0-9), dash (-), and underscore (_)
My Email	Maximum number of characters: 128
Friend's Name	Maximum number of characters: 128
Friend's Email	Maximum number of characters: 128
Message	Maximum number of characters: 1024



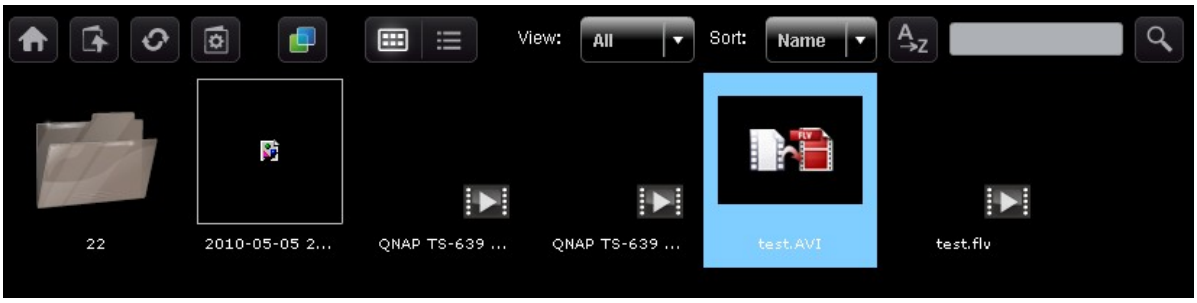
Play video

The NAS supports playing video files on the web browser. Simply click a video file on the web page, the NAS will start playing it. If you click a video file in a folder, all other supported video files in the folder will also be shown in the playlist and played. Click "X" to exit the playback page.

Transcode video

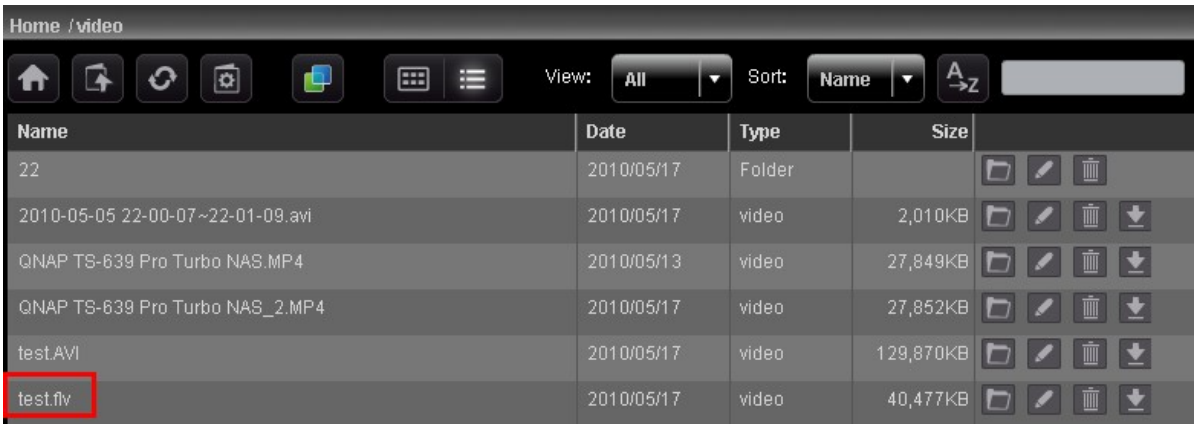
If the video files are in AVI, M4V, MPG/MPEG, RM/RMVB, WMV formats, you need to transcode the file in order to play it on Multimedia Station properly. A video file which can be transcoded is shown with an icon like below in thumbnail view.

Click the icon and confirm to perform video transcoding. Wait patiently when transcoding is in process.



The video will be converted to FLV format. You can then play it on your web browser. Only administrators are allowed to transcode a video.

QNAP does not guarantee all video formats or codecs are supported. You are highly recommended to convert the video files into the formats that Multimedia Station supports before uploading the files to the NAS.



My Jukebox

You can create playlists of music files and play them in My Jukebox. The album art and its information will be read from the ID3 tag automatically if applicable.

To create or edit your own playlist for My Jukebox, go to “Control Panel” > “Playlist Editor”. Note that only the administrators can edit the playlists. The playlists in My Jukebox will be shared with all the users of Multimedia Station.

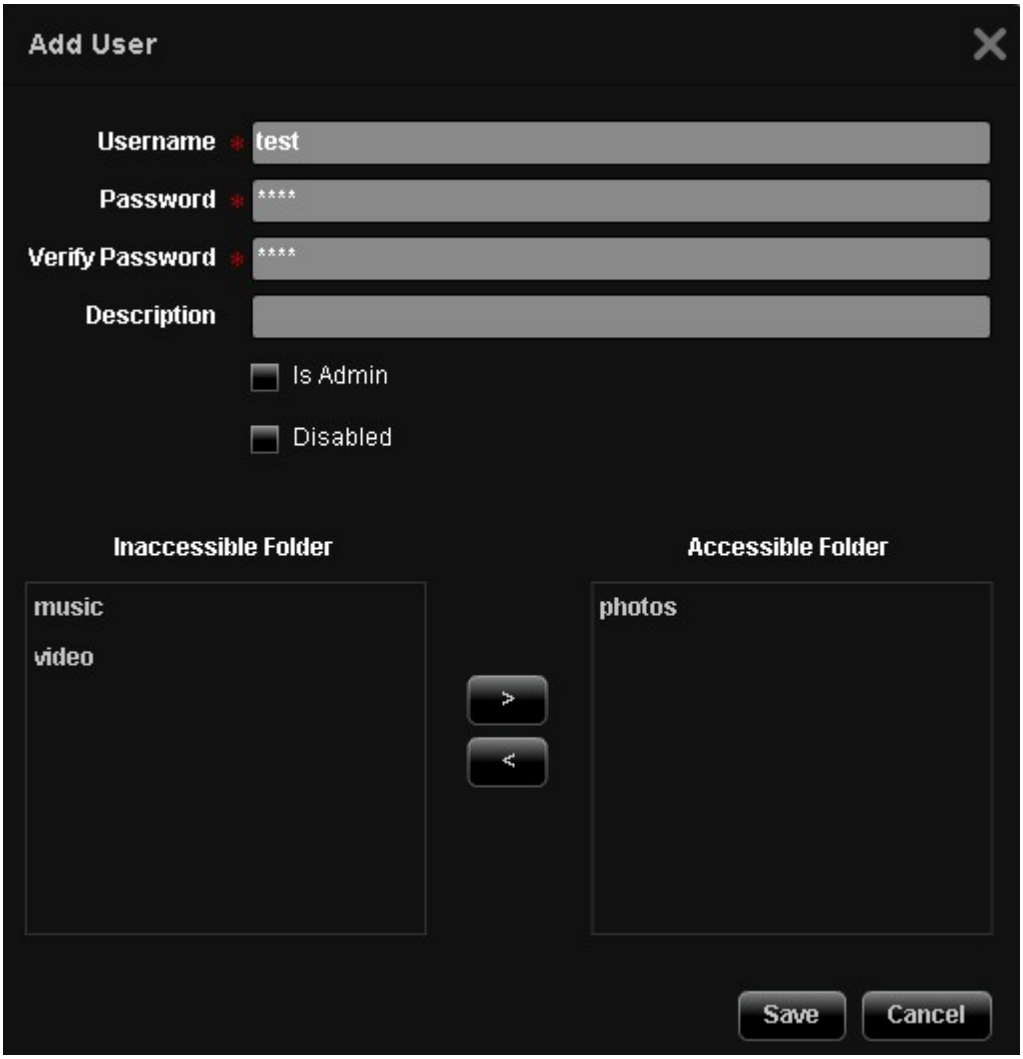
Control Panel

User Management

You can create multiple user accounts on Multimedia Station. Note that the user accounts created here are different from the system accounts you create on NAS (Access Right Management > Users). Click "Add User" to create a user. The maximum number of users Multimedia Station supports is 128, including "admin".

Enter the user information. The user name only supports alphabets (A-Z and a-z), numbers (0-9), dash (-), and underscore (_). The user name cannot exceed 32 characters.

Specify whether or not the user is an administrator and the folders that the user can or cannot access. Click "Save". Note that the password must be 1 to 16 characters long. It can only contain A-Z, a-z, 0-9, -, !, @, #, $, %, _.



The users are shown on the list. You can edit the user information, delete the user, or change the login password. Note that the default account "admin" cannot be deleted.

Change Password

You can change the administrator password in this section. The password must be 1 to 16 characters long. The password can only contain A-Z, a-z, 0-9, -, !, @, #, $, %, _.

Playlist Editor

To create a playlist, enter Playlist Editor. Select an existing playlist from the drop down menu or click "Add" to create a playlist.

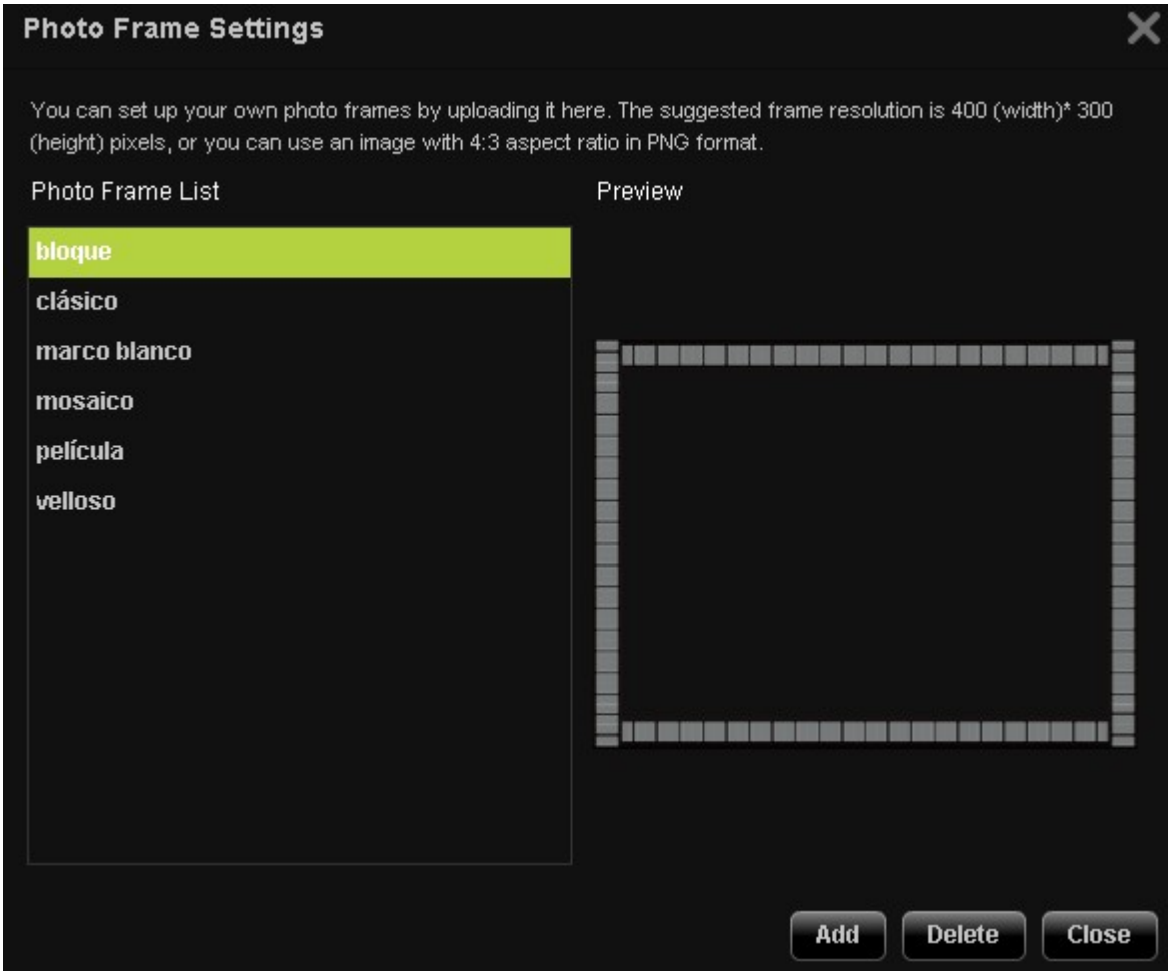
Next, select the music files from the left column (folders on Multimedia Station) and click > to add the files to the playlist. Click "Save" and then "Close".

After creating the playlist, you can play it in My Jukebox.

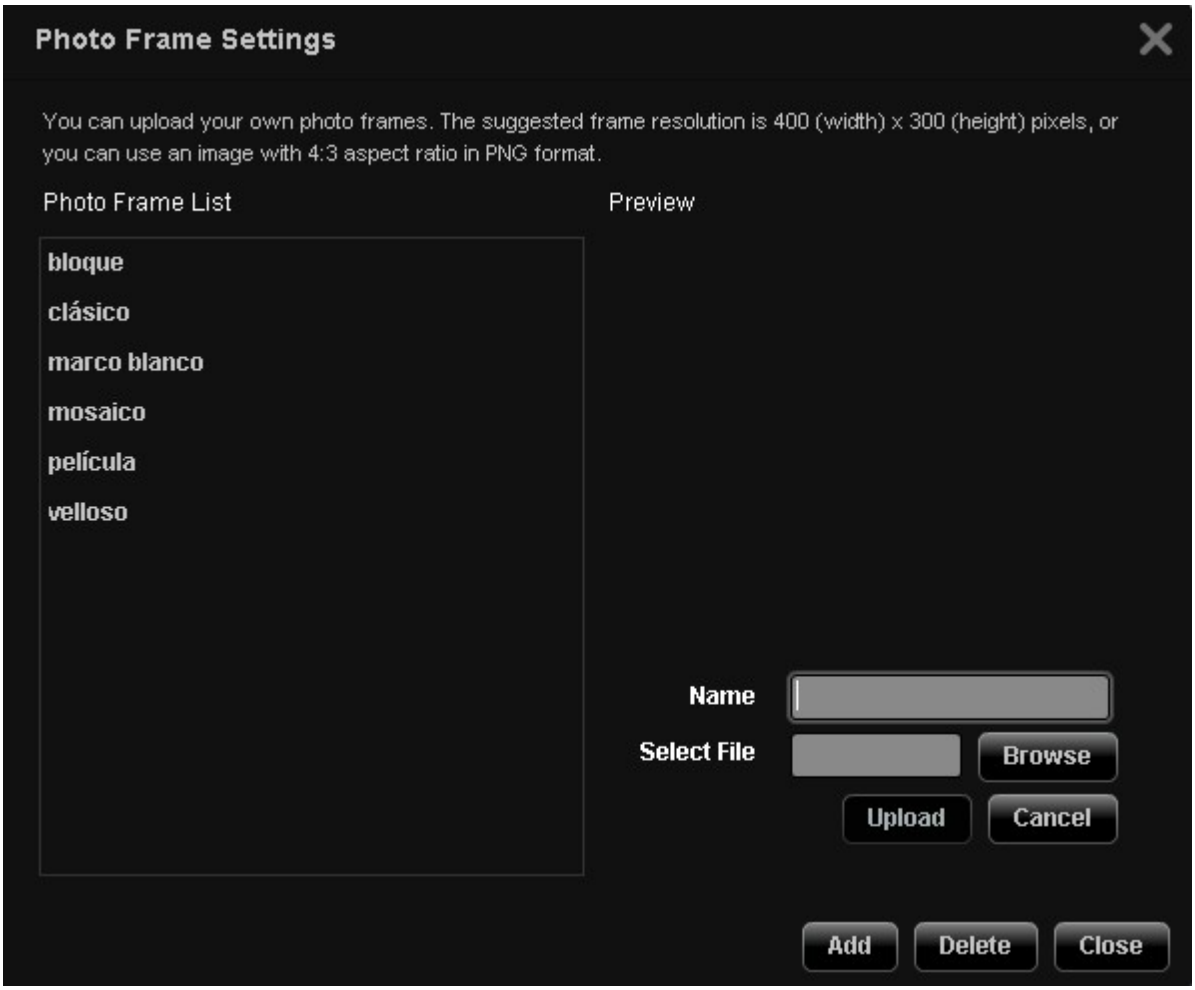
Maximum number of characters in a playlist	24
Maximum number of songs in a playlist	512
Maximum number of playlists	128

Photo Frame Settings

You can upload your photo frames for viewing the image files. The suggested resolution is 400 (width) x 300 (height) pixels, or you can use an image with 4:3 aspect ratio. The supported format is PNG. To add a photo frame, click "Add" and upload the file.

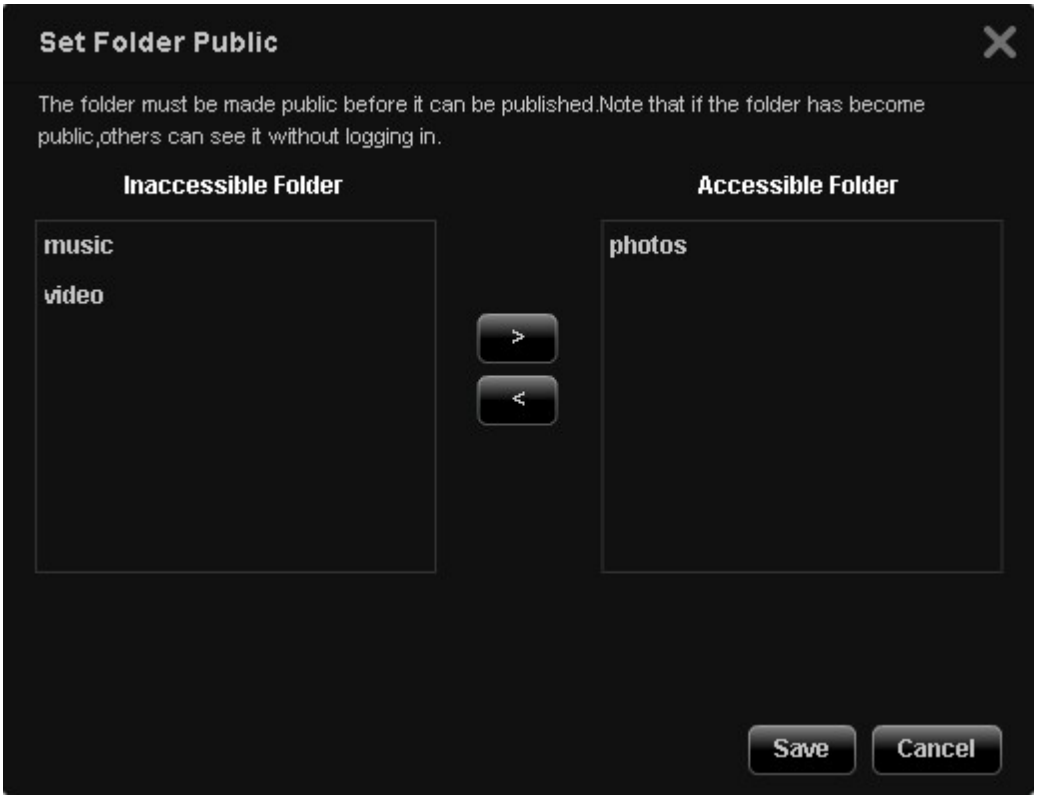


The name of a photo frame must be 1 to 16 characters long. The maximum number of photo frames Multimedia Station supports is 64 (including the system default photo frames). Note that the system default photo frames cannot be deleted.



Set Folder Public

To publish the image files to the Web, you have to make the folder public. Select the folder to allow public access and click >. Then click "Save". Note that the public folders will be seen and accessed by anyone without logging in Multimedia Station.



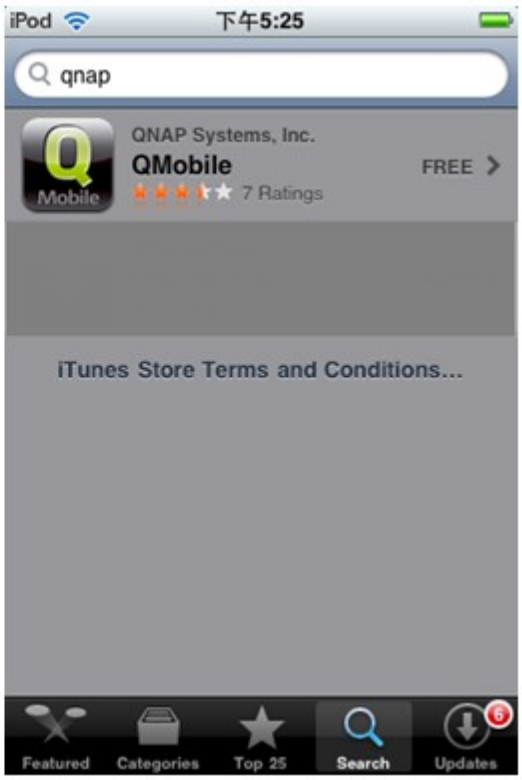
7.2.1 QMobile

QMobile is an application for you to use your handheld devices, such as iPhone, iPod touch, iPad, and Android phones, to stream music, digital pictures, and videos from your QNAP NAS servers and play the files directly on your devices from anywhere. As long as you have Internet access, you may access all the contents on the NAS remotely.

Note: QMobile is applicable to QNAP Turbo NAS running firmware version 3.3.0 or later. Make sure you have enabled Multimedia Station and Web Server, and configured the shared contents to allow QMobile to access the multimedia files on the QNAP NAS. (The user accounts created on the NAS and Multimedia Station are independent of one another. Please access Multimedia Station with an authorized user account.)

Install QMobile

Download QMobile from App Store (iPhone) or Android Market (Android phones).

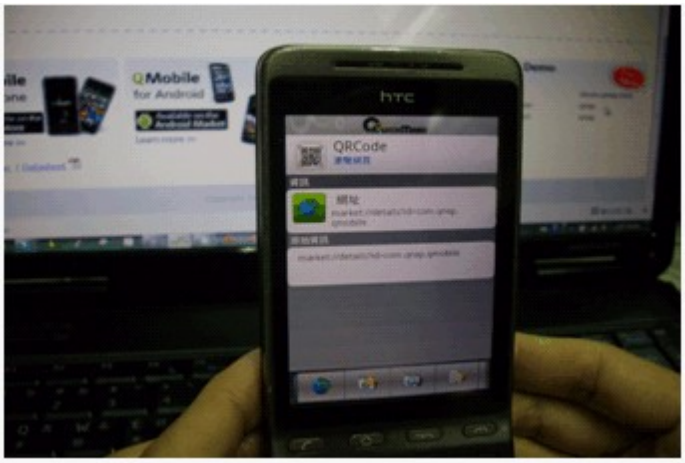


Android phone users may also get the download link of QMobile by taking a picture of the QR-code from the website below:

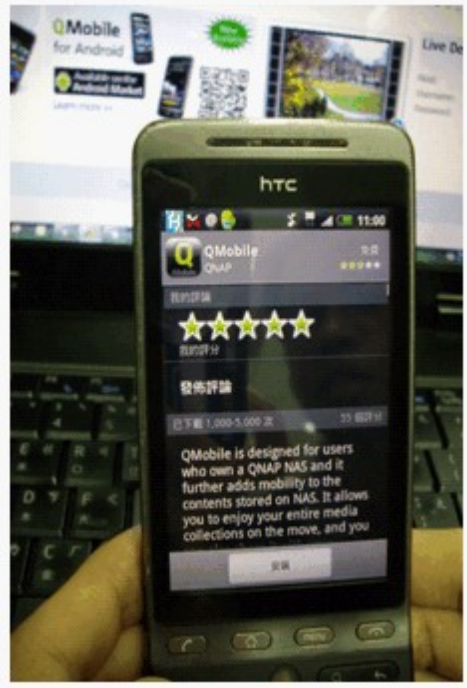
1. http://www.qnap.com/QMobile/Default.aspx?lang=eng
2. http://www.doubletwist.com/apps/android/qmobile/-6558955796410604679/

Take a picture of the QR-code.

Get the download link automatically from the QR-code.



Download QMobile to your Android phone.



After installation, QMobile will be shown on the screen.

Configure the NAS settings on your handheld devices

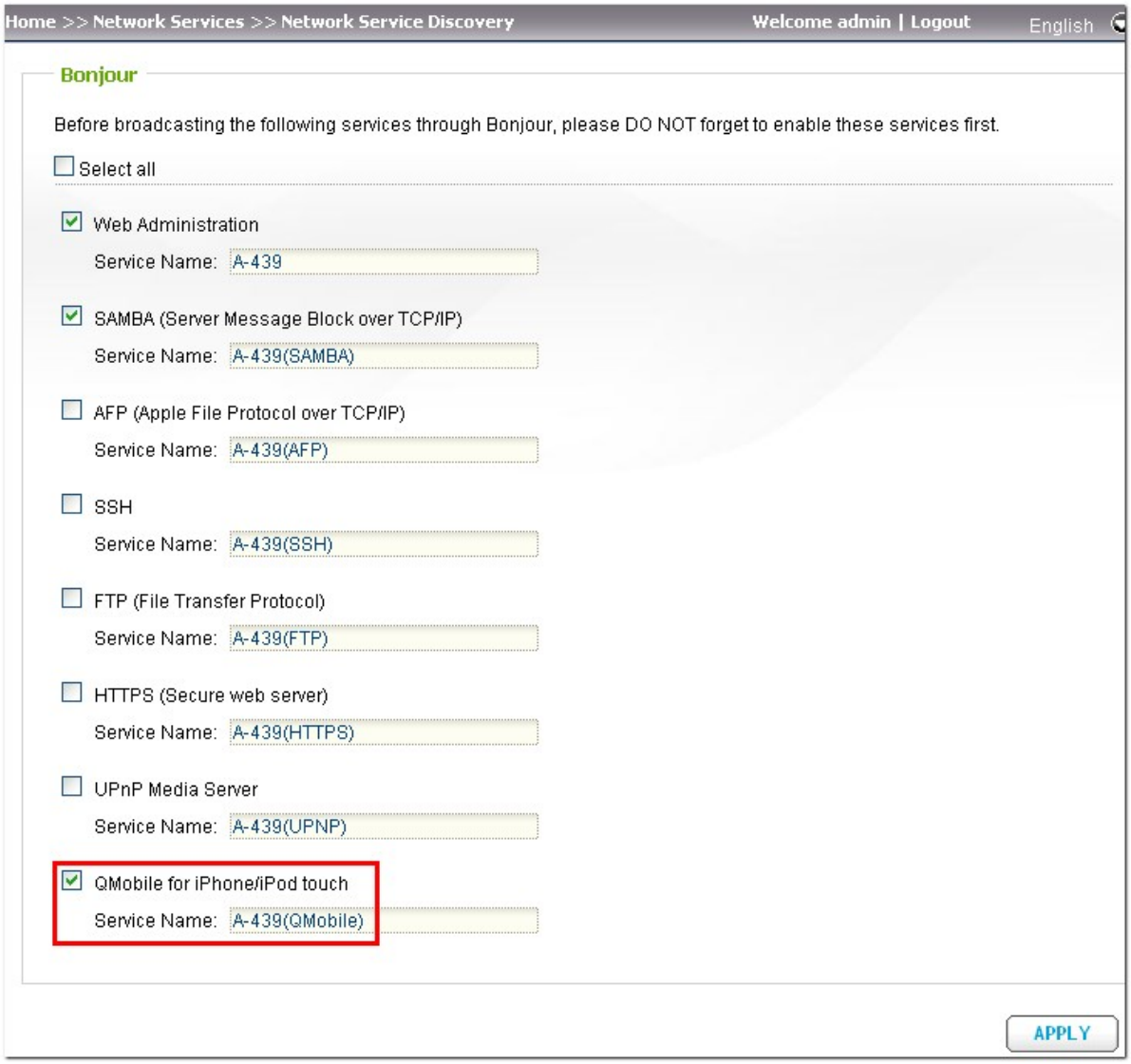
Launch QMobile App and add a QNAP NAS. You can add the NAS to QMobile by "Automatic Discovery" or "Add Server Manually".

Automatic Discovery

Note:

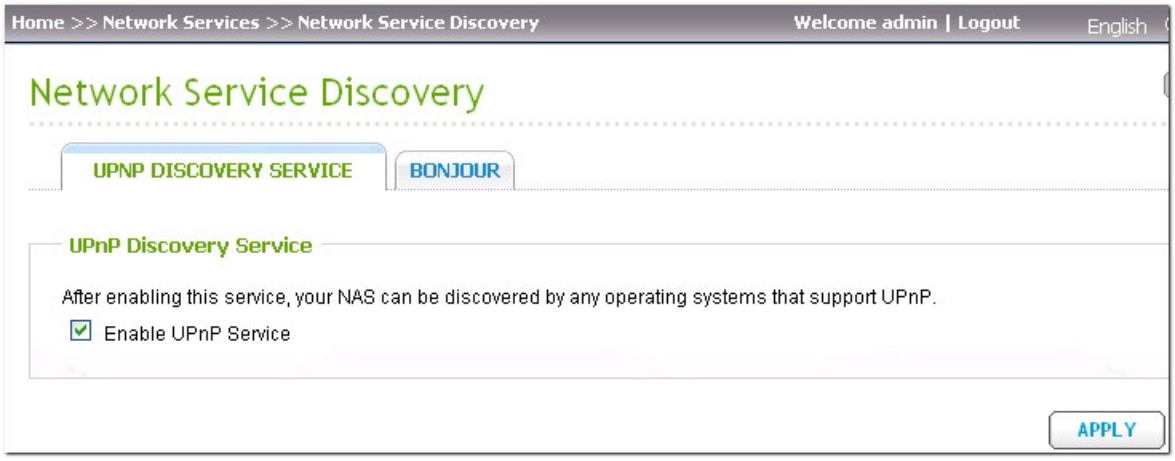
1. For iPhone users

This feature is only available after you have enabled "QMobile for iPhone/iPod touch" on the NAS under "Network Services" > "Network Service Discovery" > "Bonjour".

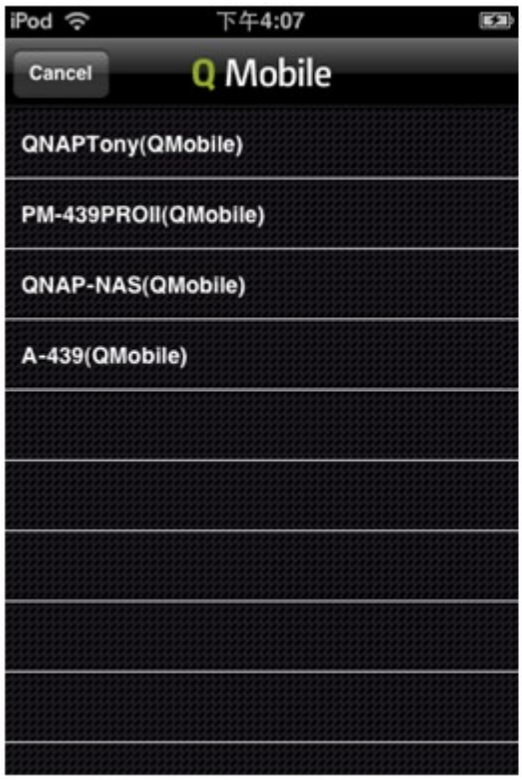


2. For Android devices

This feature is only available after you have enabled "Enable UPnP Service" on the NAS under "Network Services" > "Network Service Discovery" > "UPnP Discovery Service".



QMobile will find all the NAS servers which have enabled Bonjour/UPnP on the local network. Select the NAS and login with your user name and password.



Add Server Manually

Enter the name, host/IP, user name and password of the NAS.

Select the NAS you wish to connect. To delete a NAS from QMobile, swipe the NAS name and tap "Delete".

Use QMobile to manage your media center on the NAS

1. Media Center

You may view and play the multimedia files saved on Multimedia Station of your NAS.
Note: QMobile can only play the file formats supported by your handheld devices.

Connect to the NAS and tap the Media Center icon.

You can browse the multimedia files under "Qmultimedia/Multimedia" default network share or you may choose the specific photo, music or video files by tapping the corresponding icon at the bottom.

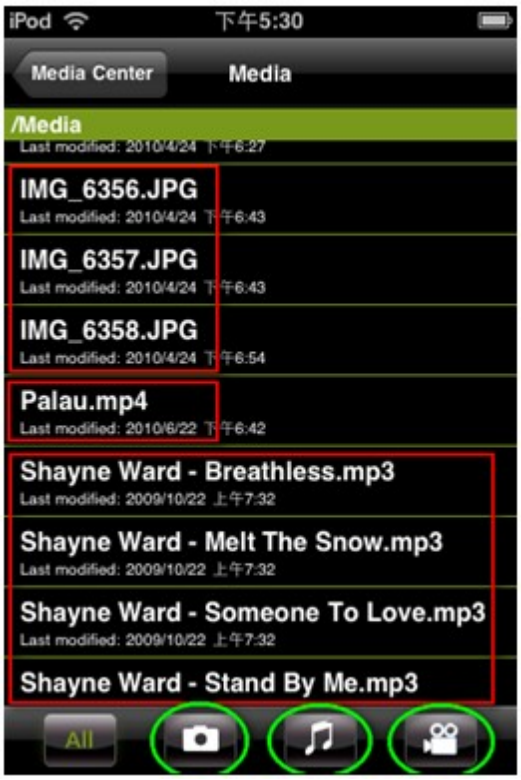
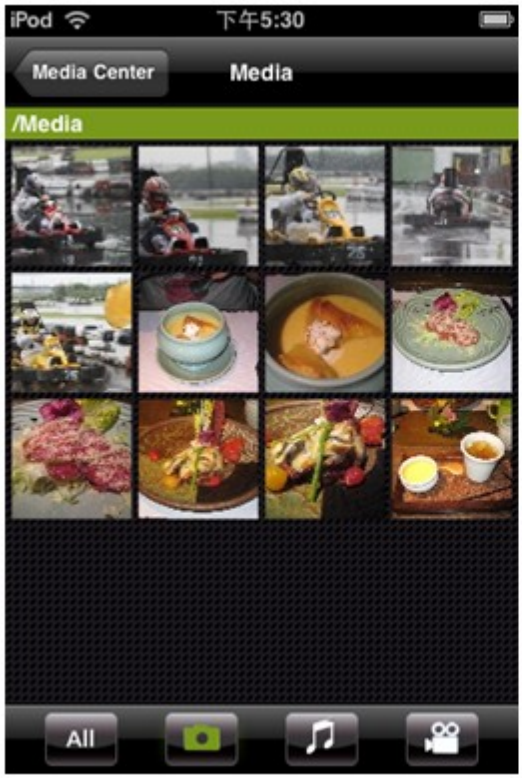
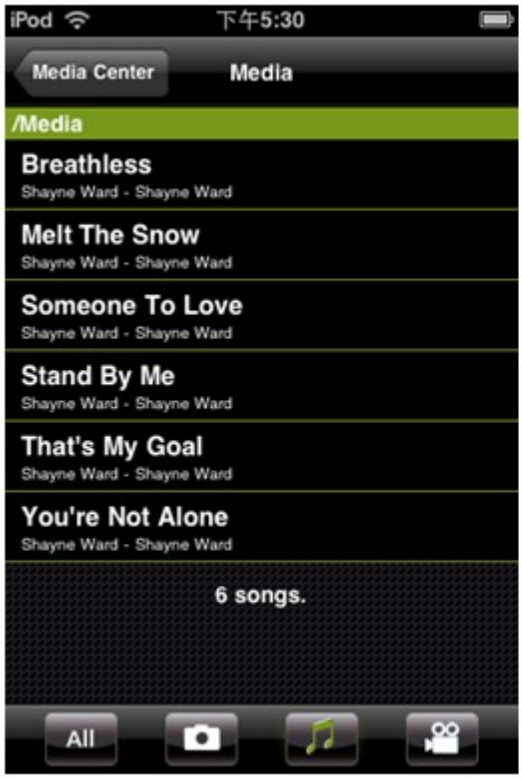


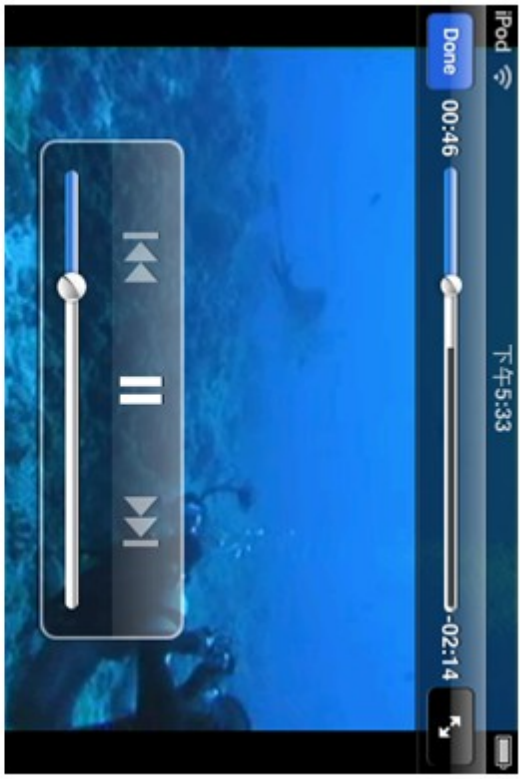
Photo view



Music view



Video view



2. Upload Photos to NAS

You may upload photos on your handheld devices to the NAS directly through QMobile. Select the file source by tapping and select the file destination of the NAS by tapping .

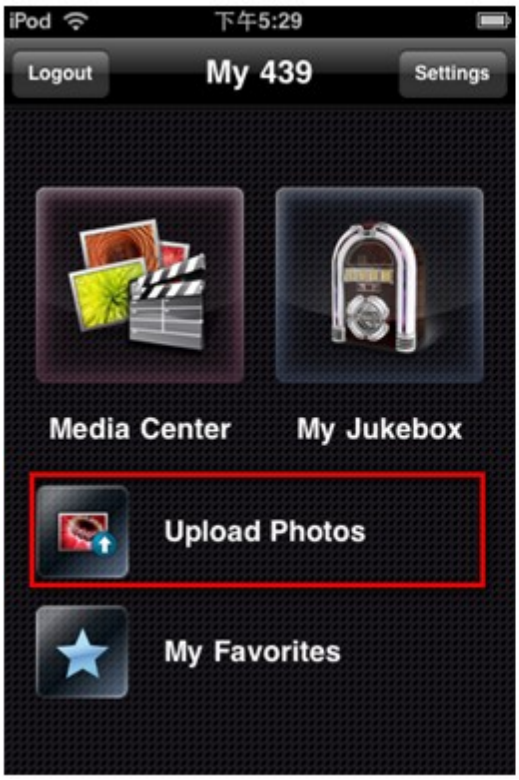
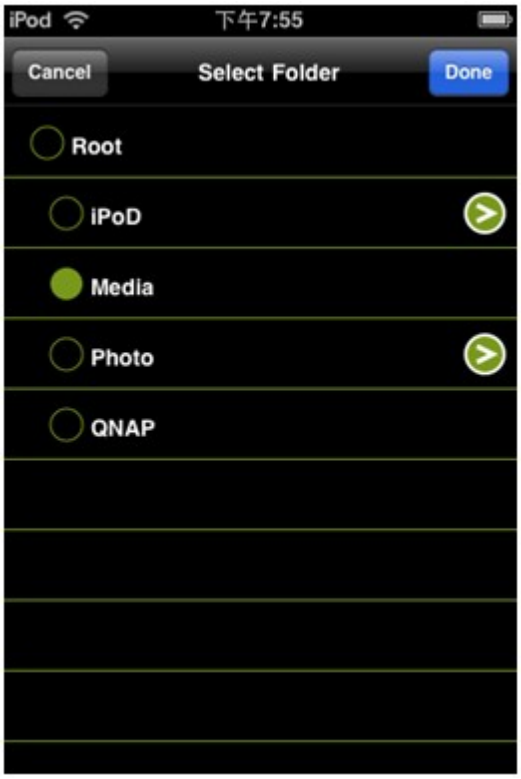


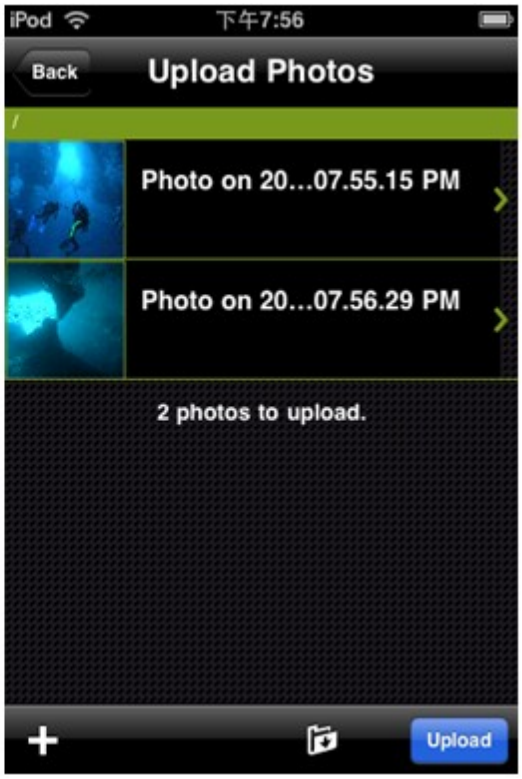
Photo Source: Choose the photos from your handheld devices.
Photo destination: Choose the root folder ("Qmultimedia/Multimedia" folder of NAS) or the sub-folder to save the photos.

(Photo source)



(Photo destination)

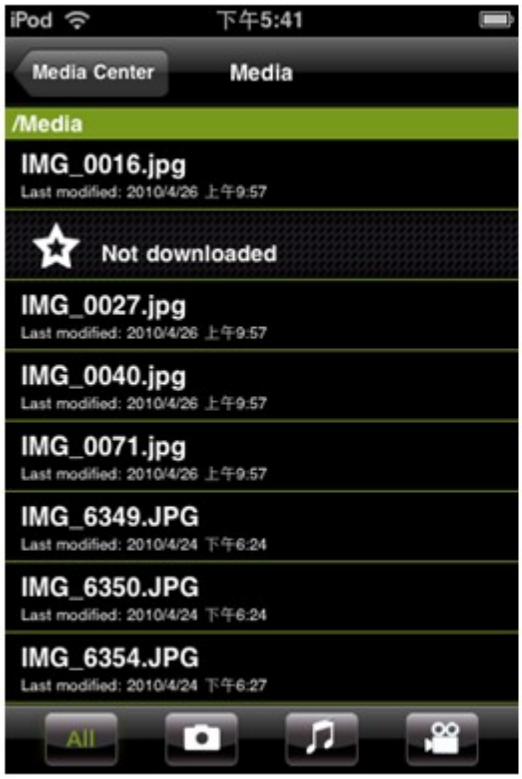
Select the photos and tap the “Upload” icon to upload the photos to the NAS.

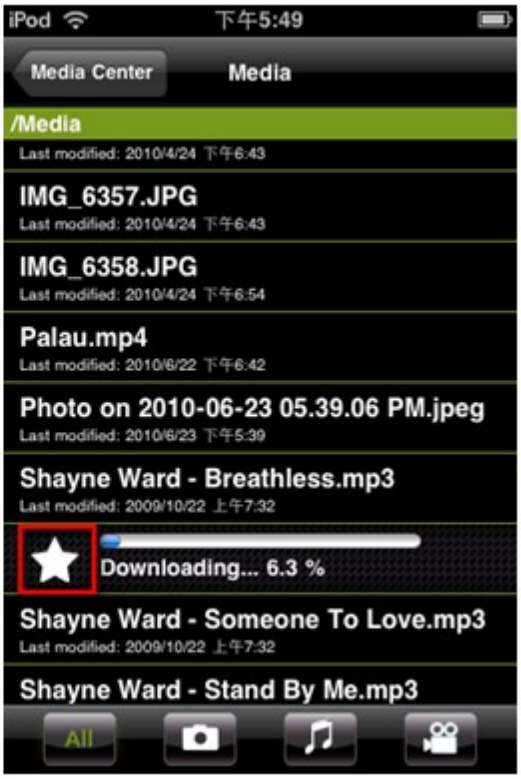


3. My Favorites

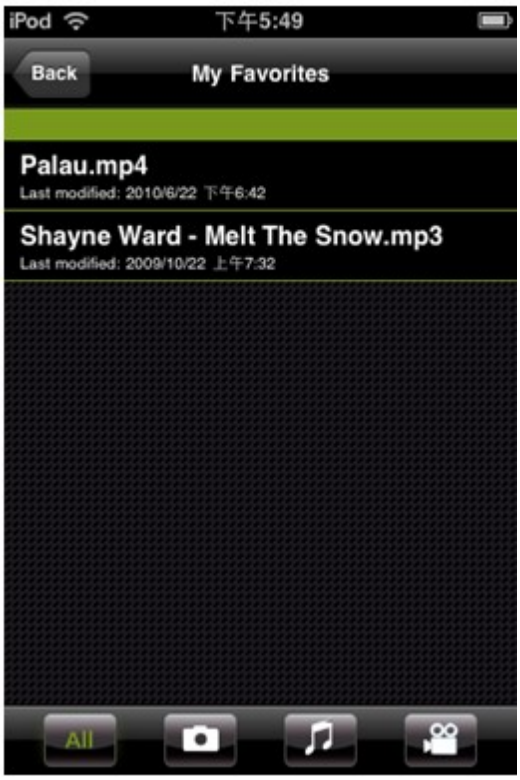
You may download the multimedia files from the NAS to your handheld devices under “My Favorites” and play them offline.

From Media Center, swipe the file and tap the star sign to start to download it.
(Files that have never been downloaded will be shown as “Not downloaded”.)





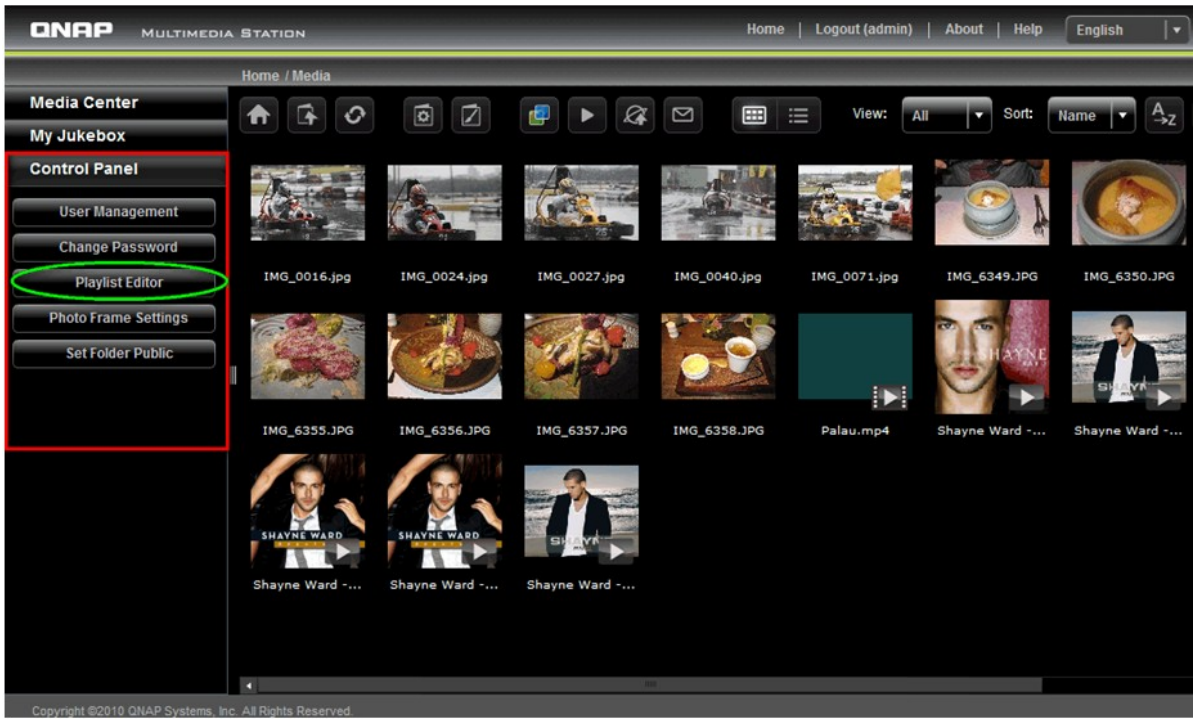
Downloaded files will be shown in “My Favorites”. QMobile will check if the source of the downloaded files have been updated or deleted from the NAS upon every new connection to the NAS. You can select to synchronize the changes with the NAS.



4. My Jukebox

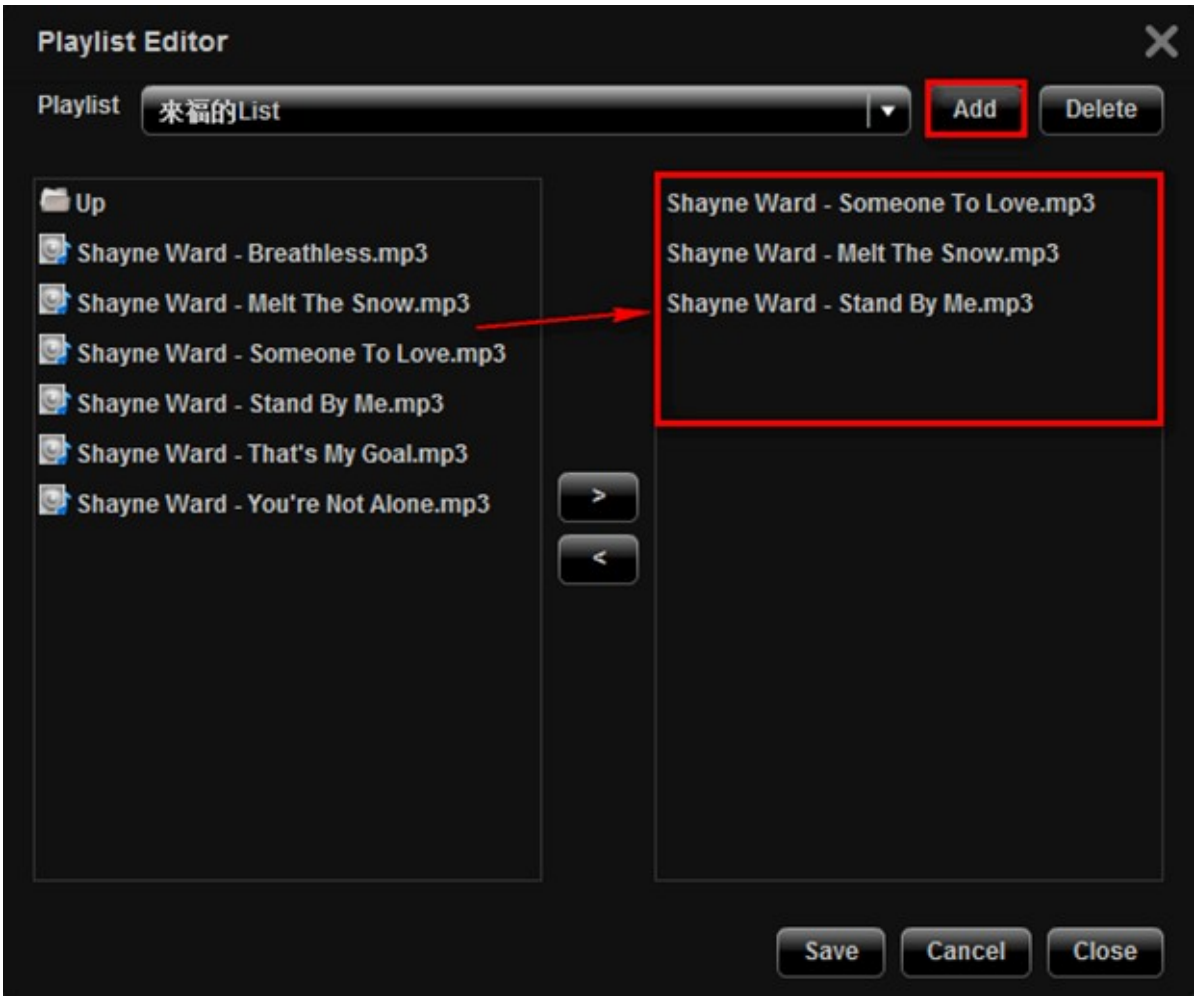
You may view, stream and play the playlists configured on Multimedia Station.

Login Multimedia Station as an administrator. Select "Control Panel" > "Playlist Editor".

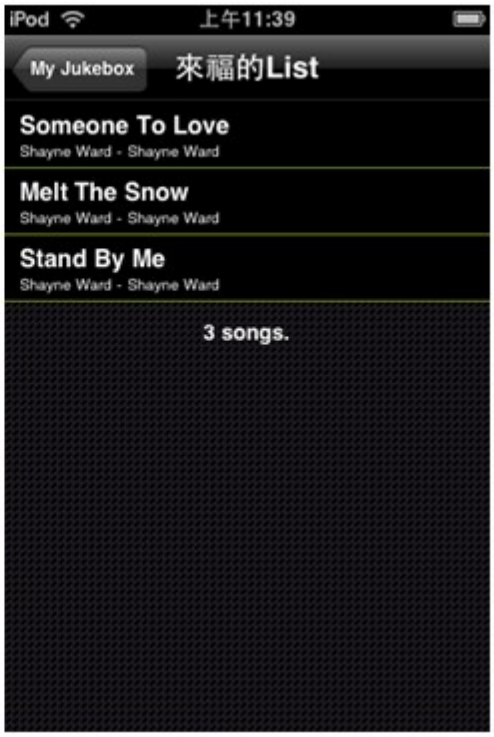


Click “Add” to create a Playlist. Enter the playlist name and click “Save”.

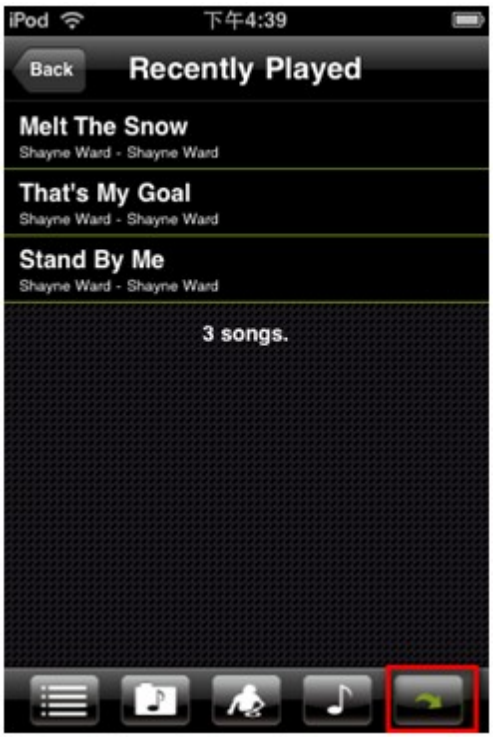
Select the playlist from the drop-down menu and then choose the music files to add to the playlist and click ">". Click "Save" to save the playlist.



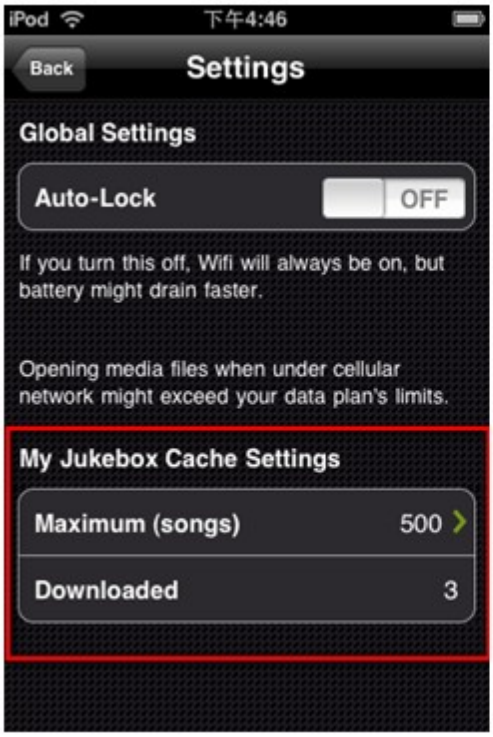
You can play the playlists created on the NAS by “My Jukebox” on your handheld devices.



Once the audio file has been streamed completely, it will be saved in the cache in “Recently Played”.



You can edit the cache settings under “Settings”.



7.3 Photo Station

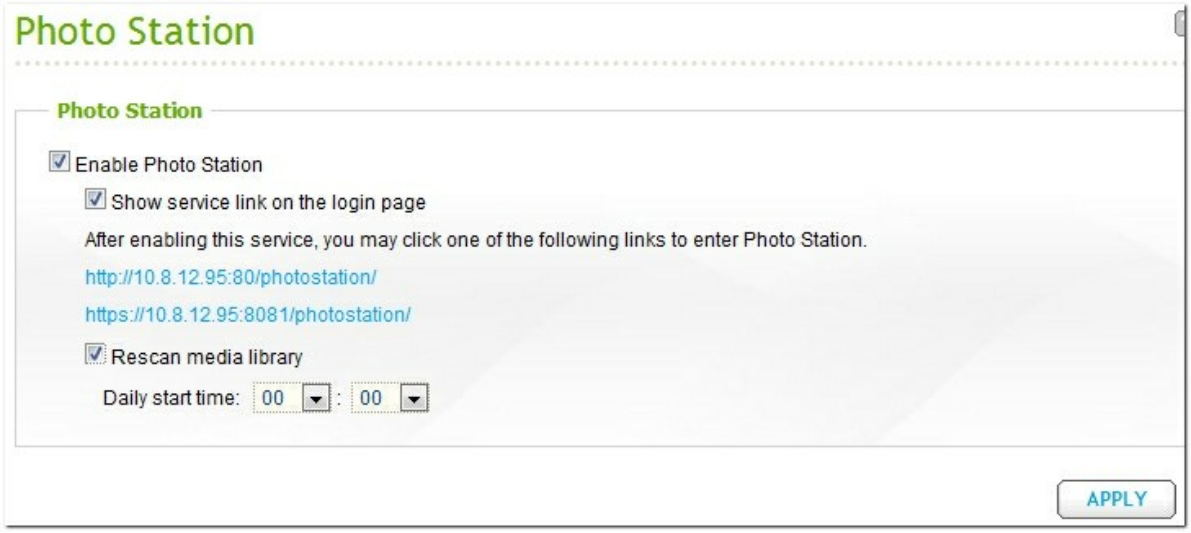
Photo Station is a web album for organizing and sharing your photos and videos on the Internet.

Requirements:

- Enable Web Server and Multimedia Station of the NAS. Photo Station utilizes the media library of Multimedia Station. When enabling Photo Station, Multimedia Station (if disabled) will be enabled automatically.
- Adobe Flash Player 9 or above.

To use Photo Station, do the following.

1. Login the NAS as "admin". Go to "Application Servers" > "Photo Station" and enable this feature. Enable the option "Rescan media library" and specify the time for the NAS to scan the media library daily. The NAS will generate thumbnails, retrieve media information and transcode videos for the newly added files at the specified time every day.



2. Upload photos and video files to Qmultimedia or Multimedia folder of the NAS.

Photo Station supports the following file format:

Images	BMP (Intel-based NAS only), GIF, PNG, JPG, and JPEG
Video	FLV and H.264 (AAC)

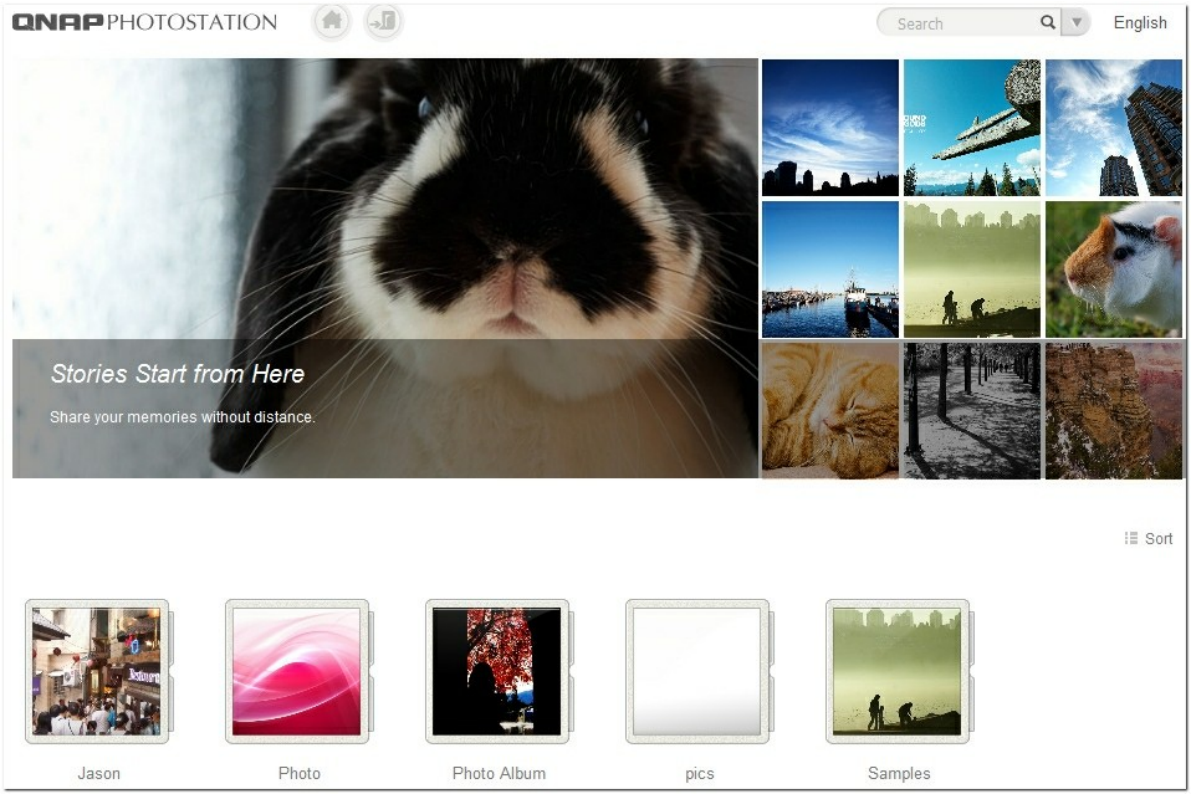
Tips on file upload:

- The maximum size of an image file is 32MB.
- The maximum size of multiple files that can be uploaded at a time is 2GB.

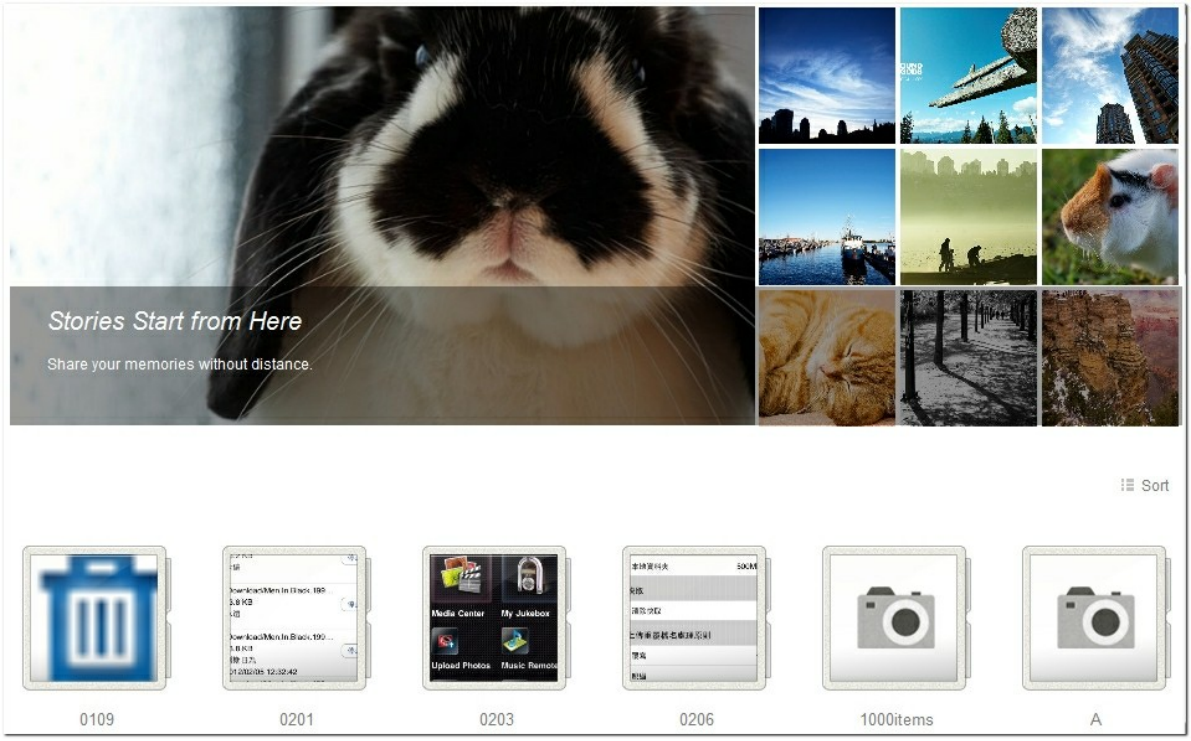
3. Go to the login page of Photo Station. To do this, click the Photo Station icon on the login page of the NAS or the link on "Application Servers" > "Photo Station", or enter http://NAS IP/photostation in a web browser (Internet Explorer, Mozilla Firefox, or Google Chrome).

4. The banner and description of Photo Station are shown on the upper section of the login page. Below the banner are the public albums. Select the display language from the drop-down menu on the top right hand corner.

5. Click and enter the user name and password to login Photo Station. The admin login credentials are the same as that of the NAS web administration.



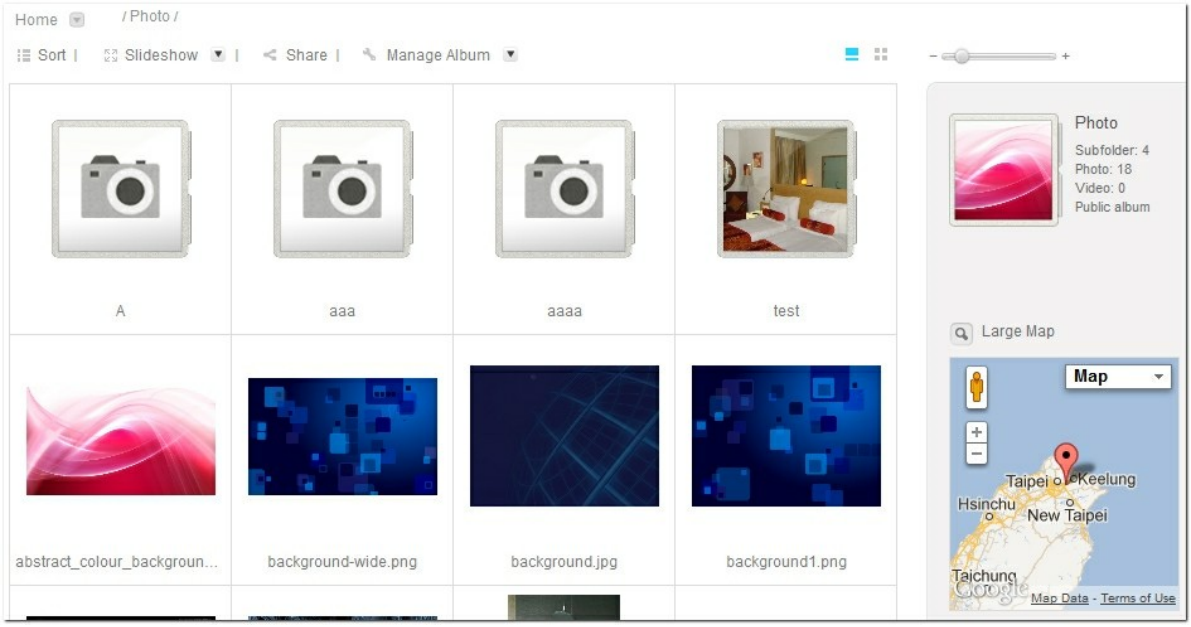
Upon successful logon, all the folders (albums) in Photo Station will be shown.



Icon	Description
	Go to the home page of Photo Station. Only folders on Qmultimedia/Multimedia folder will be shown.
	Logout.
	Go to the Settings page.
	Search for the folders, photos, or videos under the current directory. Click the triangle icon for advanced search.
	Sort the contents by file name, size, file created date, or photo taken date in ascending or descending alphabetical order.

1. View an album (folder)

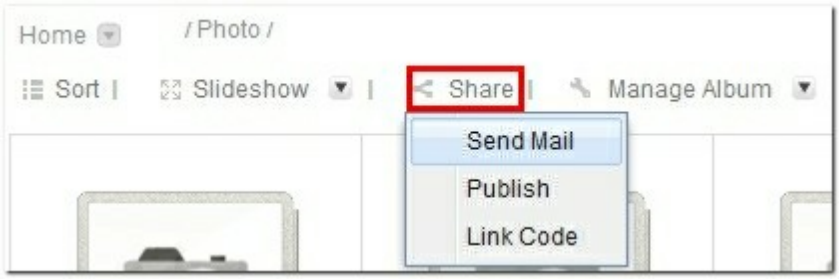
When browsing an album (a folder), the subfolders and supported images and video files will be shown.



Icon/Option	Description
Home	Go to the page where all the folders and files in Photo Station (Qmultimedia/ Multimedia folder) are listed.
/Directory/	Quick link to the directories within an album (folder).
Sort	Sort the contents by file name, size, file created date, or photo taken date in ascending or descending alphabetical order.
Slideshow	View the photos in slideshow. Click the triangle icon to select the display mode, speed, and playlist (background music). The playlists can be created and edited in Music Station ("Application Servers" > Music Station").
Share	Share the contents with others by email, publishing to social networks, or link code.
Manage Album	Add an album or upload/copy files to an existing album.
	Adjust the thumbnail size.
	Select to view the contents in Thumbnails or Photo Wall. The name of the image or video file will only be shown in Thumbnails view.

2. Share photos and video files

The images on Photo Station can be shared on the Internet by email, publishing to social networks, or link code. Click "Share" and select an option.

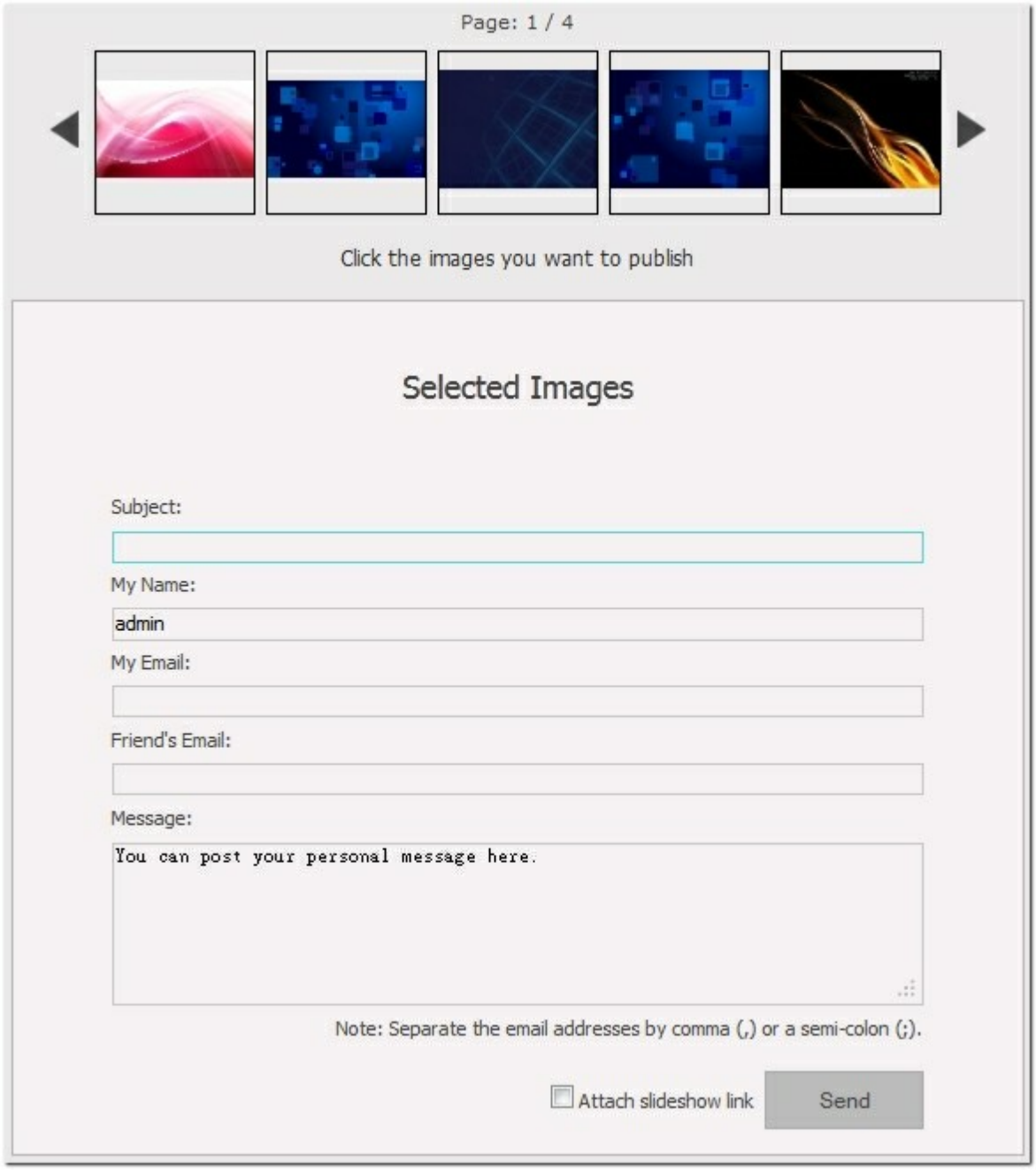


2.1 Send Mail

Select up to five images to send to your friends by email. Enter the subject (max 128 characters), sender's name (max 128 characters) and email, recipient's name (max 128 characters) and email, and message (max 1024 characters). Select "Attach slideshow link of current album" to attach the link of the album slideshow in the email. Click "Send".

Note:

- To use this function, the mail server settings must be properly configured in "System Administration" > "Notification" > "Configure SMTP Server".
- The album must be made public in "Settings" > "Set Folder Public" before sharing the images.


Page: 1 / 4
Click the images you want to publish
Selected Images
Subject:
My Name:
admin
My Email:
Friend's Email:
Message:
You can post your personal message here.
Note: Separate the email addresses by comma (,) or a semi-colon (;).
Attach slideshow link
Send

2.2 Publish

Select up to five images to publish to social networks: Twitter, Facebook, MySpace, Plurk, or Blogger. Enter the title (max 256 characters) and message (max 1024 characters), and specify the URL. Click the social network icon and enter the login information to publish the images.

Note:

- The album must be made public in "Settings" > "Set Folder Public" before sharing the images.
- Photo Station must be accessible on the Internet. It is suggested to set up the DDNS ("System Administration" > "Network") or MyCloudNAS service on the NAS.

2.3 Link Code

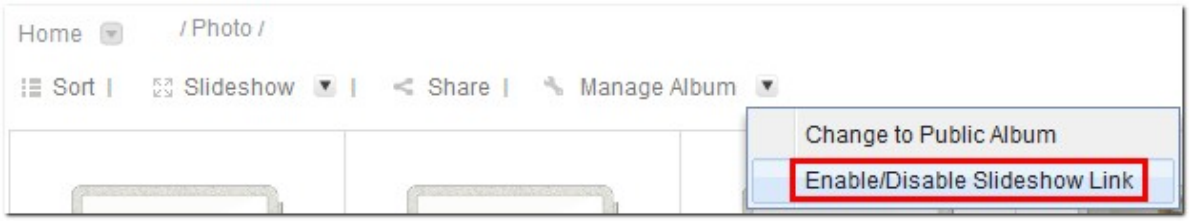
Copy the link of an album slideshow to publish the contents to any social networks, emails, or forums.

Note:

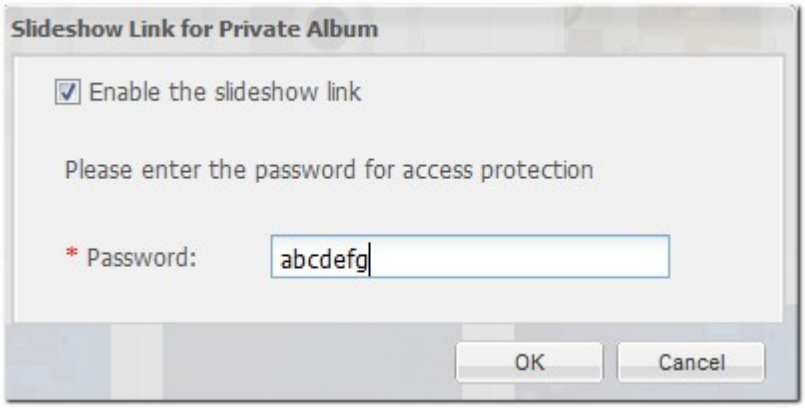
- The album must be made public in "Settings" > "Set Folder Public" before sharing the images.
- Photo Station must be accessible on the Internet. It is suggested to set up the DDNS or MyCloudNAS service on the NAS.

Share Private Albums

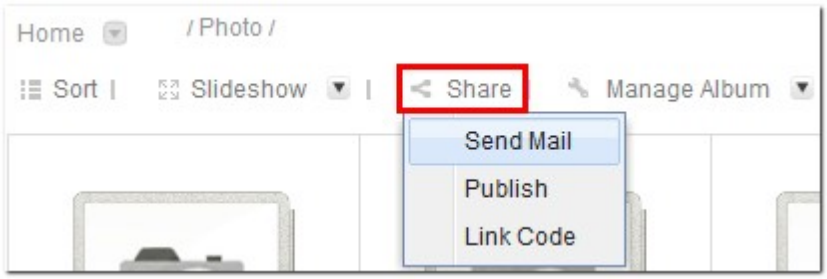
Click ▼and select "Enable/Disable Slideshow Link".



Enable slideshow link and enter an access password for the slideshow link.



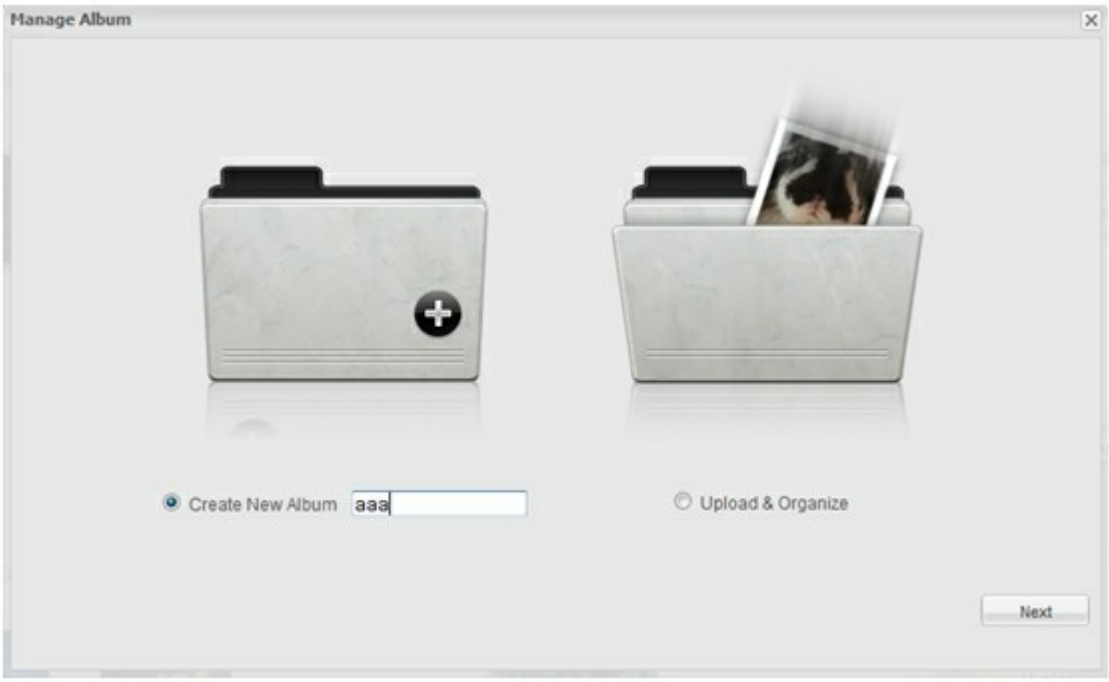
Click "Share" to share the album by email or link code.



3. Create an album

To create an album in a folder, click “Manage Album”.

Select “Create an Album” and enter the album name. Click “Next”.

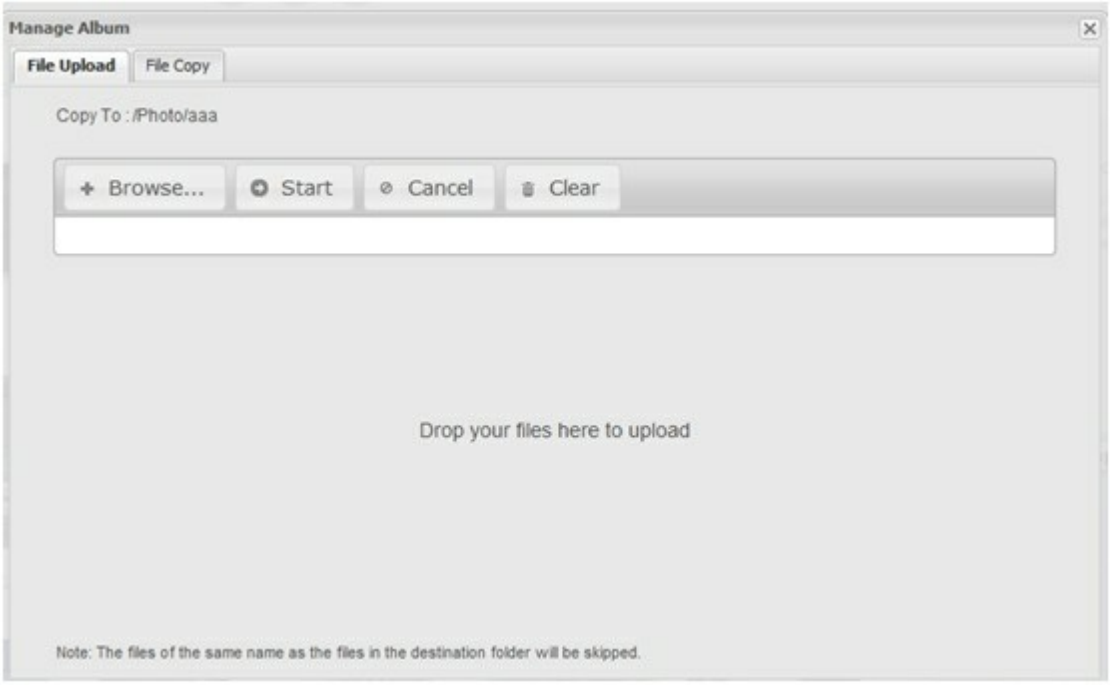


3.1 File upload

Under the "File Upload" tab, browse the images or video files and click "Start" to upload the files. Mozilla Firefox or Google Chrome users can drag and drop to upload files to the album. If a file of the same name exists in the album, the action will be skipped.

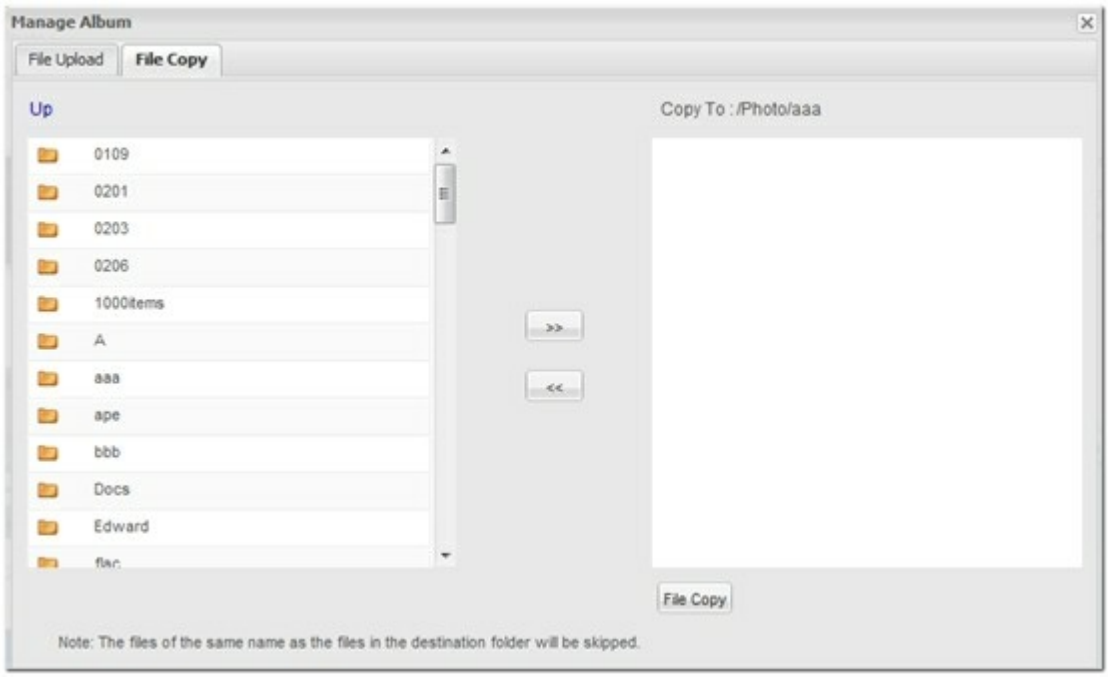
Note:

- The maximum size of an image file supported is 32MB.
- The maximum size of multiple files that can be uploaded at a time is 2GB.



3.2 File copy

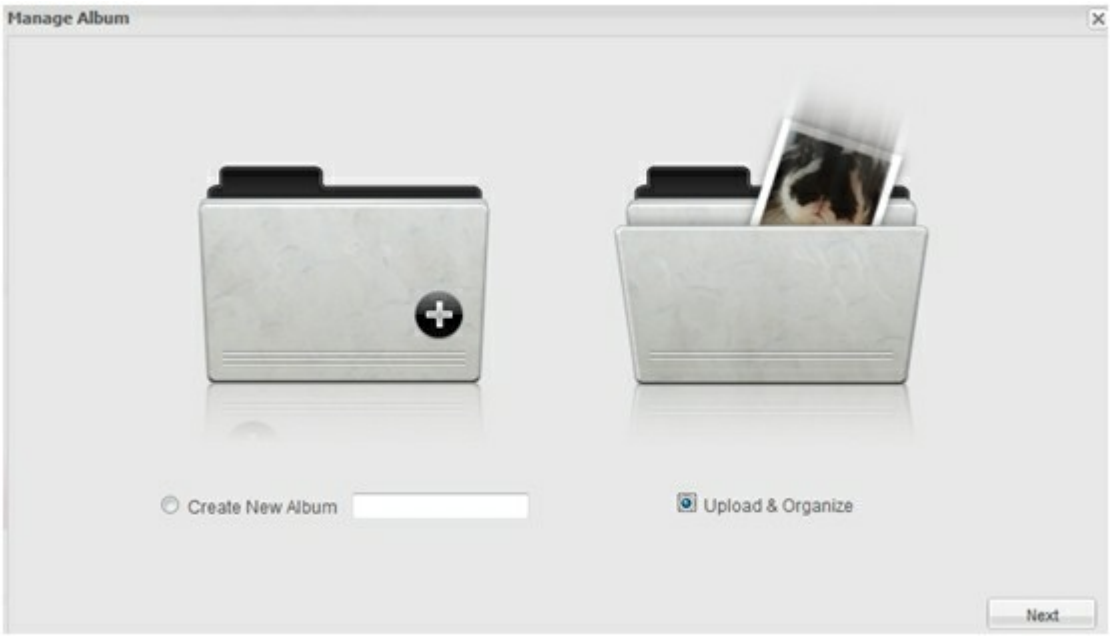
To copy the images or video files from a folder on Photo Station to the selected album, select the folder and files under the "File Copy" tab and click >>. Then click "File Copy". If a file of the same name exists in the album, the action will be skipped.



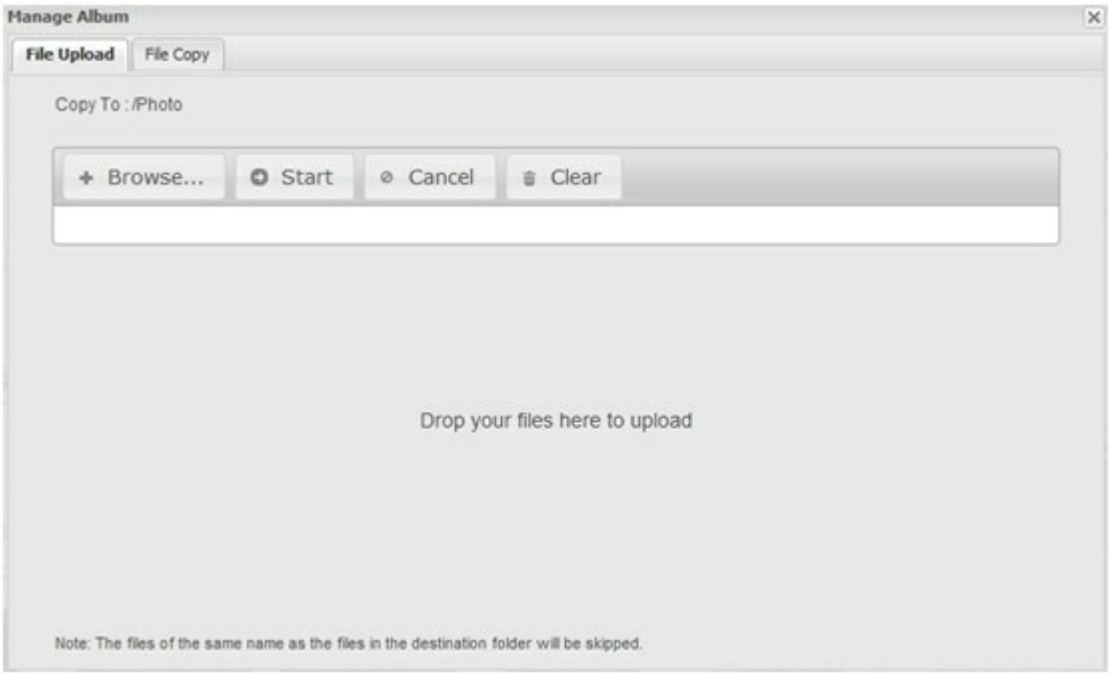
4. Edit an album

To upload or copy files to an existing album on Photo Station, click "Manage Album".

Select "Upload & Organize". Click "Next".



Select to upload files or copy files from existing albums to the album.



5. View a photo

Photo Station supports the following options for viewing an image file.

Icon/Option	Description
Link Code	Copy the links of an image in different sizes for publishing on the Internet.
Slideshow	View the images in an album in slideshow. Click the triangle icon to select the display mode, speed, and playlist (background music). The playlists can be created and edited in Music Station ("Application Servers" > Music Station").
Download	Download an image.
EXIF	View the EXIF information of an image.
Edit (Pixlr Editor)	Edit the image online by Pixlr Editor.
	Rotate an image 90° anticlockwise.
	Rotate an image 90° clockwise.
	Set an image as the album cover.
	View the original size of an image.
File name	Click to edit the file name of an image. Click "Submit" to save the changes.
Description	Enter a description (max 512 characters) for an image.
Add Comment	Click to comment (max 128 characters) on an image.
Comment	Click to view all the comments on an image.

Home / Photo /

Link Code | Slideshow | Download | EXIF | Edit (Pixlr Editor)

8 / 18

IMAG0154.jpg

Click here to edit the description

Add Comment

admin

Comment

Submit

Comment

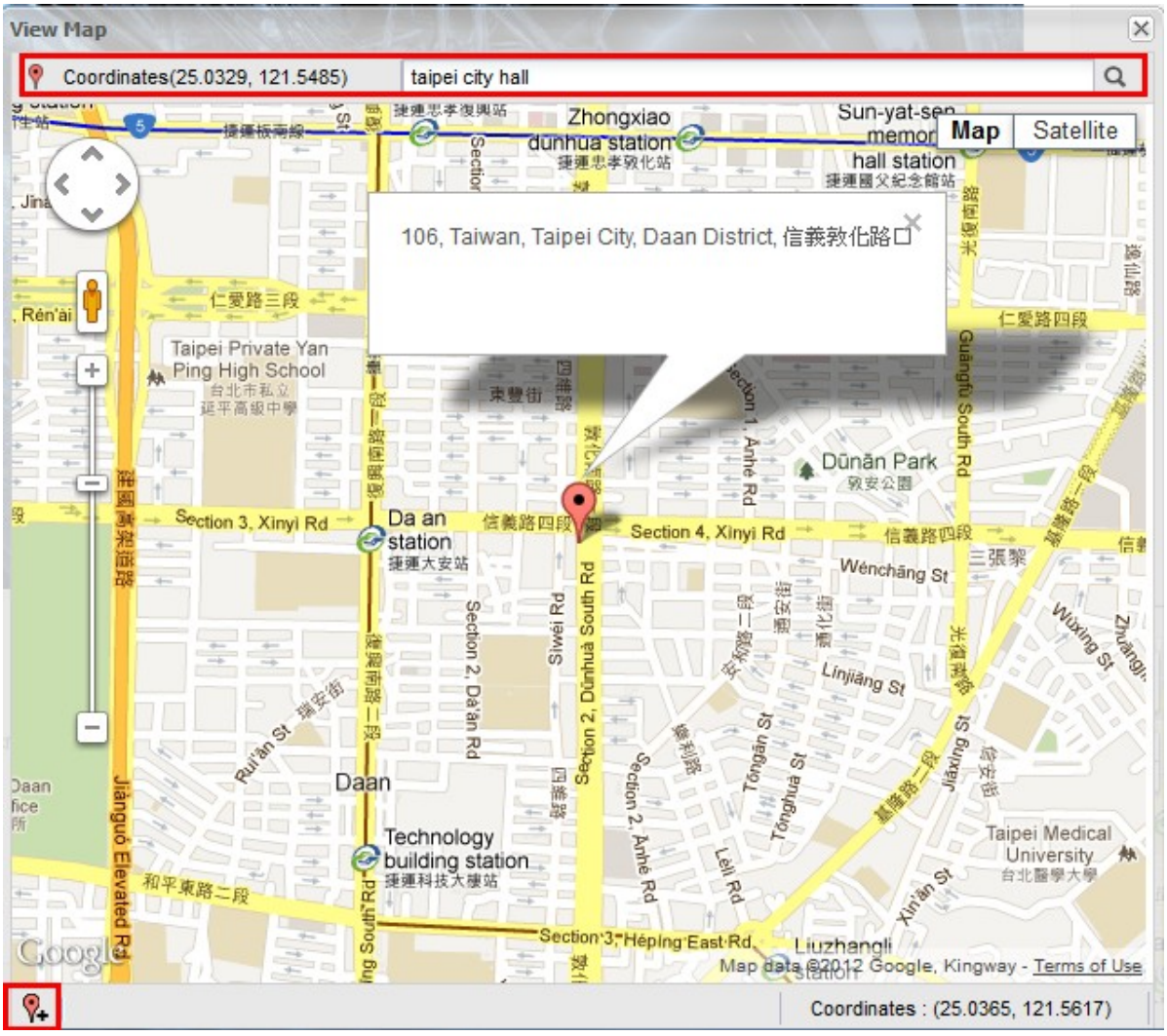
Large Map

Geotag this photo

Geotag photos

To geotag a photo with Google Maps, click

. Search a spot on the map. Right click the spot and select "Set Coordinates" or click at the bottom left corner and click a spot on the map.

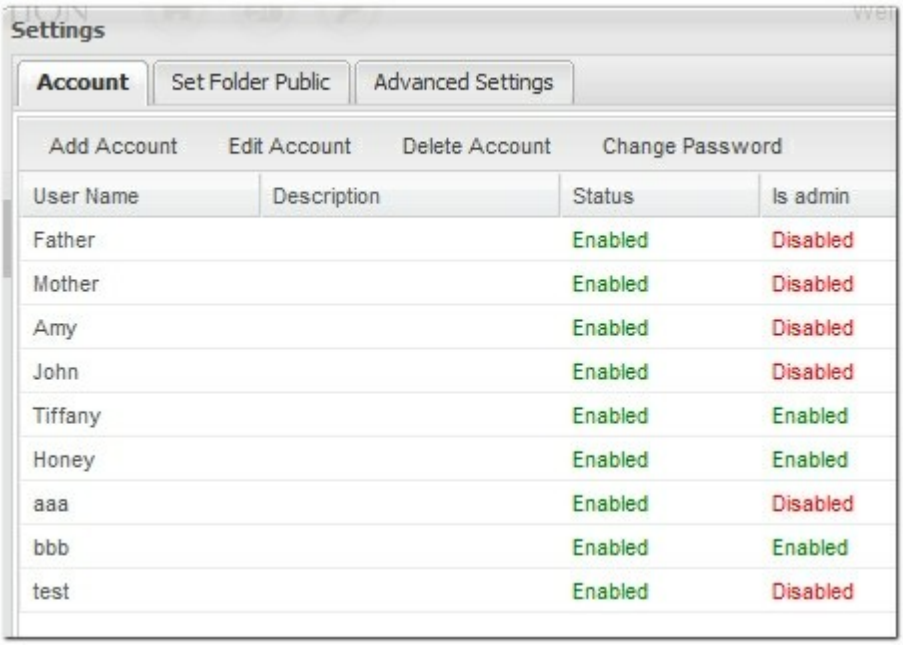


6. View a video

Click a video to view it by the web browser. To download the file, click “Download”.

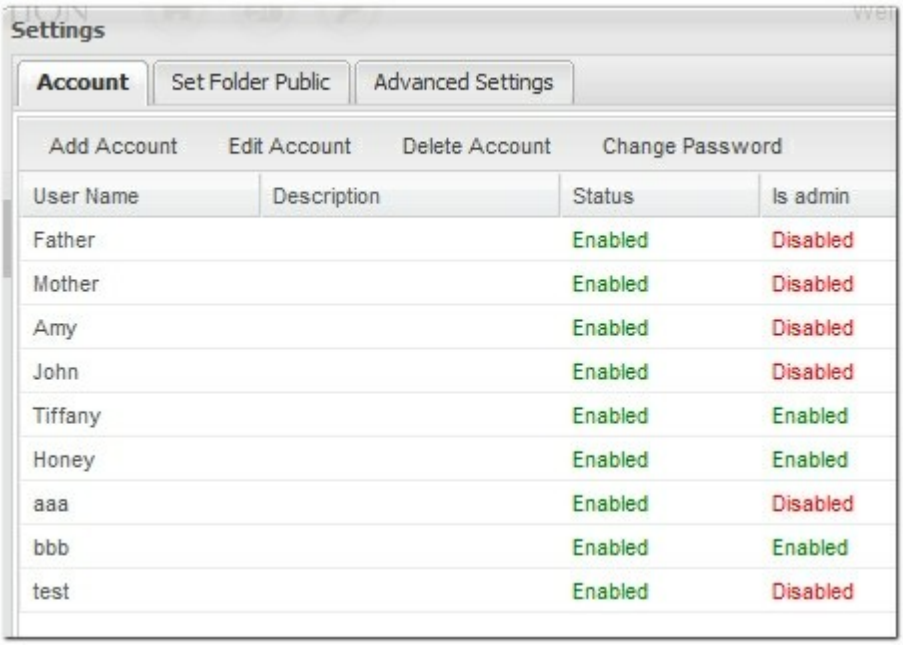
7. Settings

Click to enter the Settings page.



7.1 Account

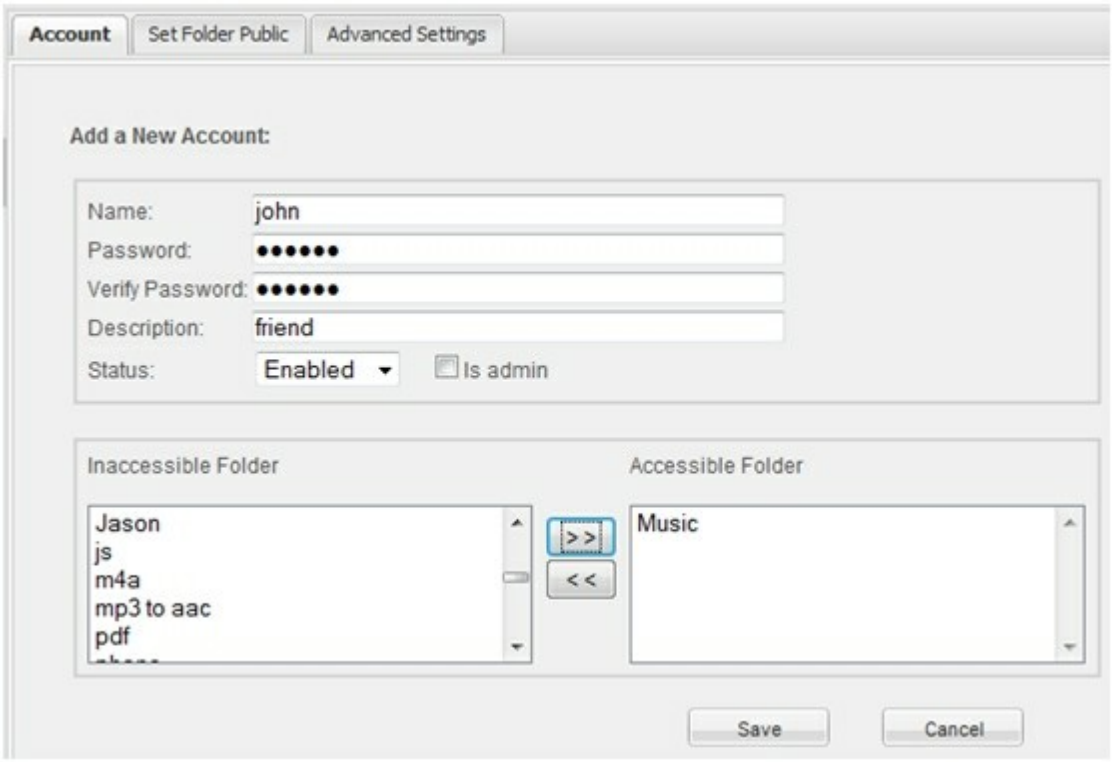
To create a user, click "Add Account" under the "Account" tab.



Enter the user name (max 32 characters), password (1-16 characters), and description (max 512 characters). Select the user status (enabled or disabled) and specify if the user is an administrator. Then select the folder(s) that the user is allowed to access by adding them to the accessible folder list. Click "Save".

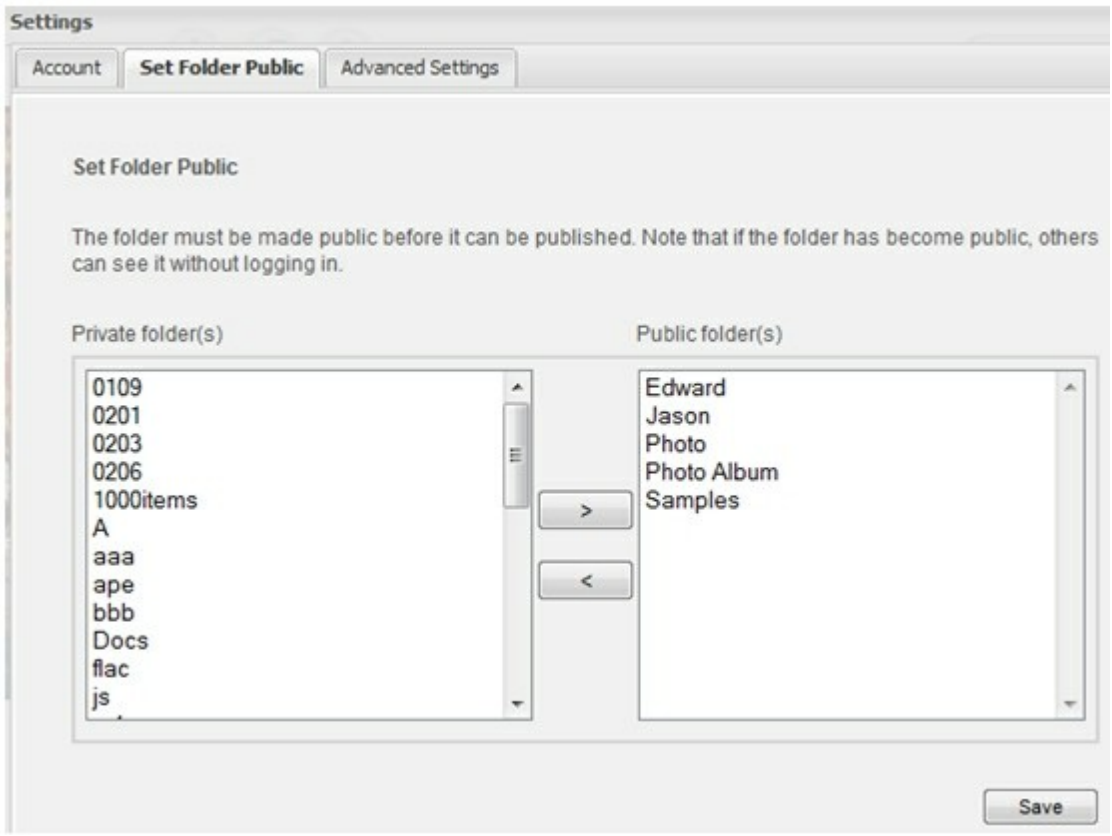
Note:

- The user name only supports A-Z, a-z, 0-9, dash (-), and underscore (_).
- The password only supports A-Z, a-z, 0-9, -, !, @, #, $, %, _.

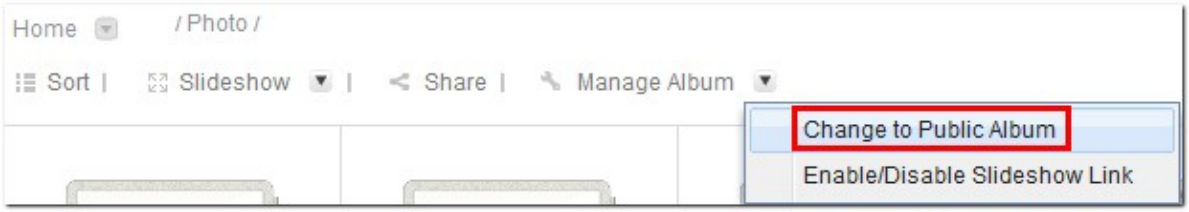


7.2 Set folder public

All the folders in Photo Station are for private viewing by default. Select the folder(s) to be published for public access. Private folders can only be accessed by authorized Photo Station users. Click "Save" to save the changes.

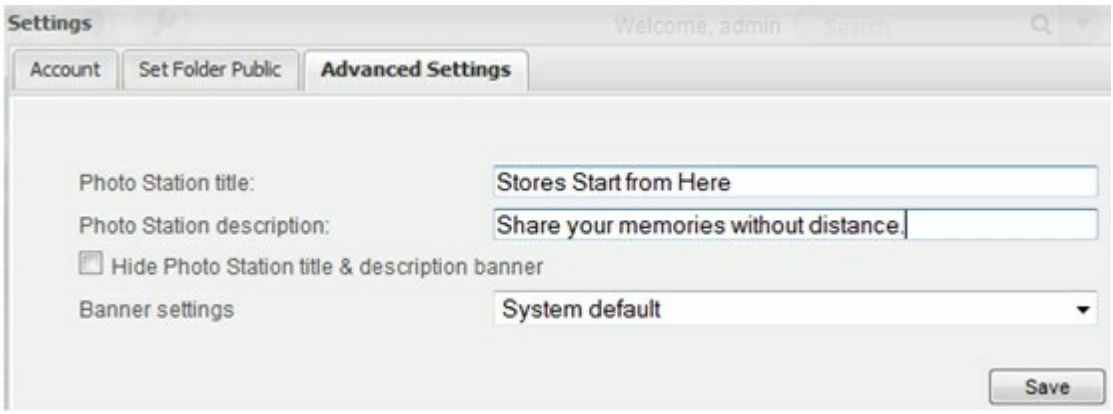


An album can also be changed to public or private by clicking ▾.



7.3 Advanced settings

Customize the banner of Photo Station on the home page in "Advanced Settings".



1. Enter the title (max 35 characters) and description (max 120 characters) of Photo Station or select to hide the information.

2. Select the banner settings. When 2x2, 3x3, or 4x4 photo wall banner is selected, click "Browse" to choose a public album.

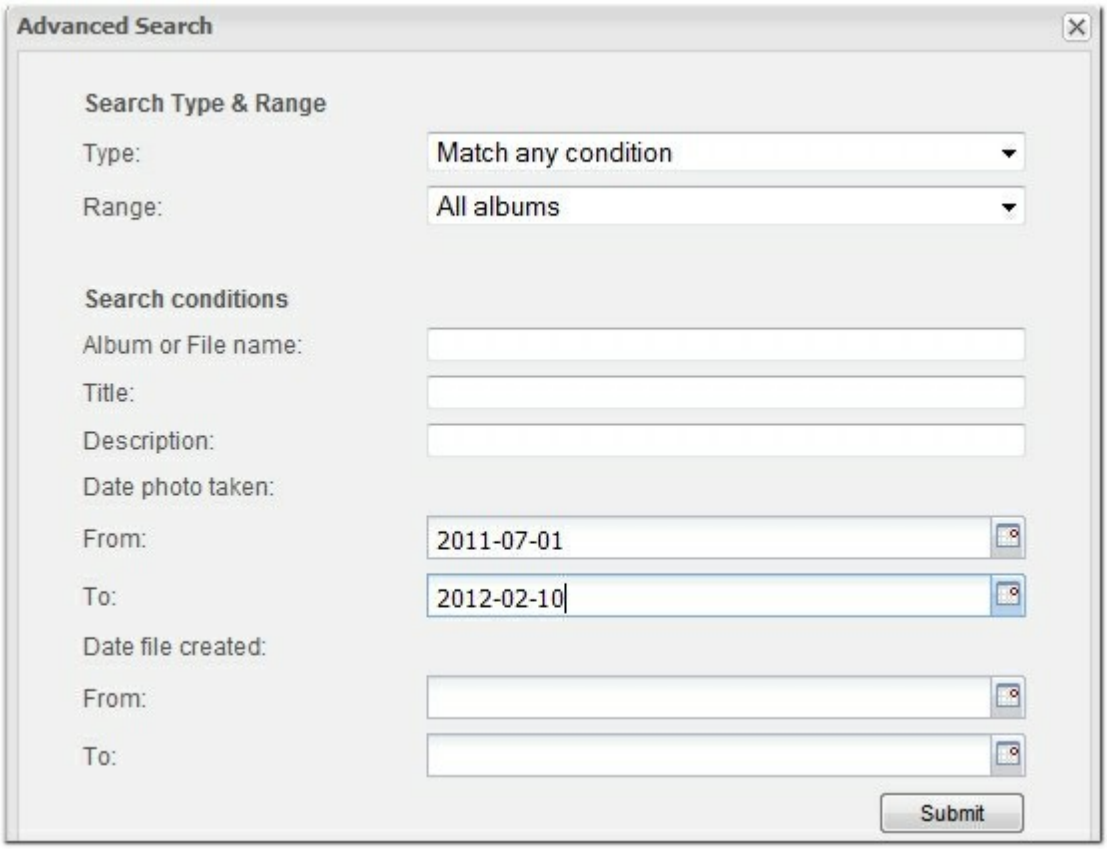
3. Click "Select".

4. The photos in the public album will be shown at the bottom. Select a block of the banner (highlighted in red) and choose an image file. Empty blocks will be shown with system default images. Click "Save" to save the changes.

8. Advanced search

Advanced search offers more options for searching a folder (album) and a file (photo or video). Click the triangle icon next to the search box to enter the advanced search page.

Enter the search criteria and click “Submit”.



7.4 Music Station

Music Station is a web-based application for playing the music files on the NAS or media server, and Internet radio by remote streaming via a web browser or by local playback via a USB speaker or USB soundcard connected to the NAS. Music alarms can also be set with local playback.

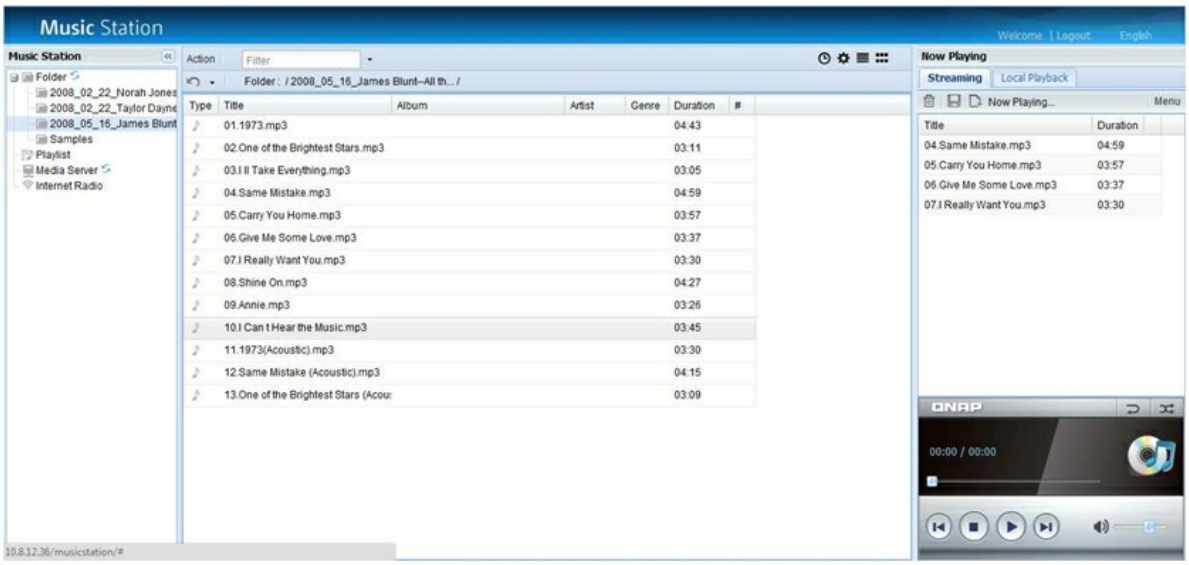
Follow the steps below to enable Music Station and prepare the music files for playback.

1. Login the NAS as admin. Go to "Application Servers" > "Music Station" and enable this feature.

2. Upload music files to the folder "Multimedia" or "Qmultimedia" of the NAS. The folders uploaded to Music Station are for private viewing by default and can only be managed by the administrator or authorized admin groups.

3. Login Music Station as an administrator for management. The admin login information of Music Station is the same as that of the NAS web administration.

Note: Music Station uses the same user account information as Multimedia Station. To create users for Music Station, login Multimedia Station as admin and create the accounts in "Control Panel" > "User Management".



A. Music Sources

The music files available for playback are shown on the left panel. The items are described below:

1. Folder: The folders and supported music files on Multimedia or Qmultimedia folder of the NAS are shown. Click "Folder" to load or refresh the list.

> **Note:** Music Station only supports audio files in MP3, MP4, OGG, WAV, AIFF, AU, FLAC, M4A, APE format.

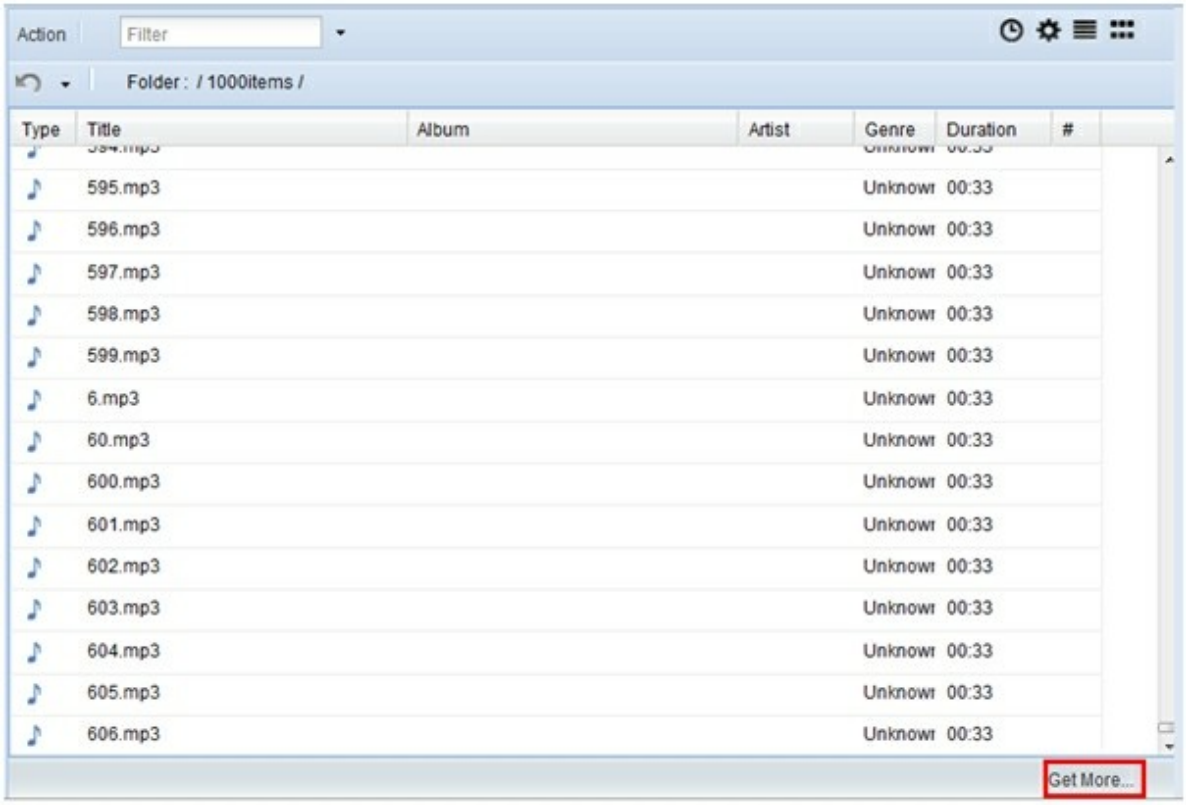
2. Playlist: The playlists available on Music Station. Each playlist can contain 512 items, including music files on the NAS or media server and Internet radio. Maximum128 playlists are supported.

3. Media server: Click "Media Server" and the NAS will search for all available DLNA media servers on the local network automatically. Only the music files supported will be displayed.

4. Internet radio: Links of Internet radio stations. Maximum 1024 items are supported. Note that the type of the radio stations must be MP3.

Display more than 600 items in a folder

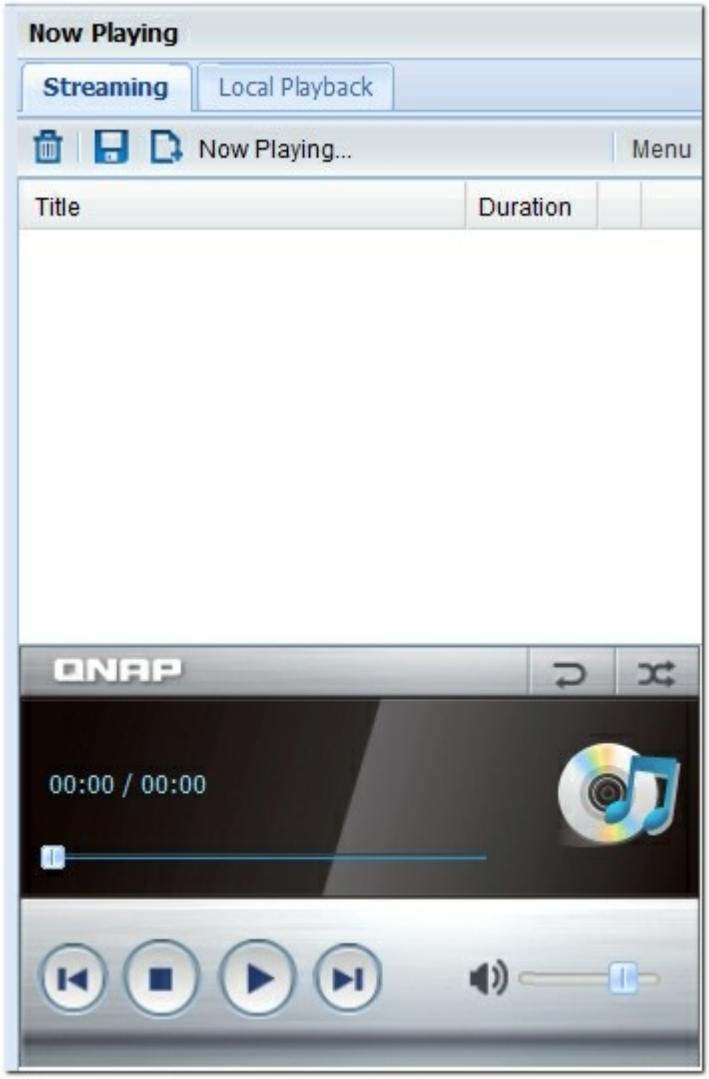
If a folder contains more than 600 items, Music Station will display the first 600 items alphabetically. Click "Get more" at the bottom right of the UI to load the next 500 items.



B. Music Playing

The “Now Playing” panel on the right provides two playing modes:

1. Streaming (music playback by a web browser)
2. Local playback (music playback by a USB speaker or soundcard connected to the NAS)



Player

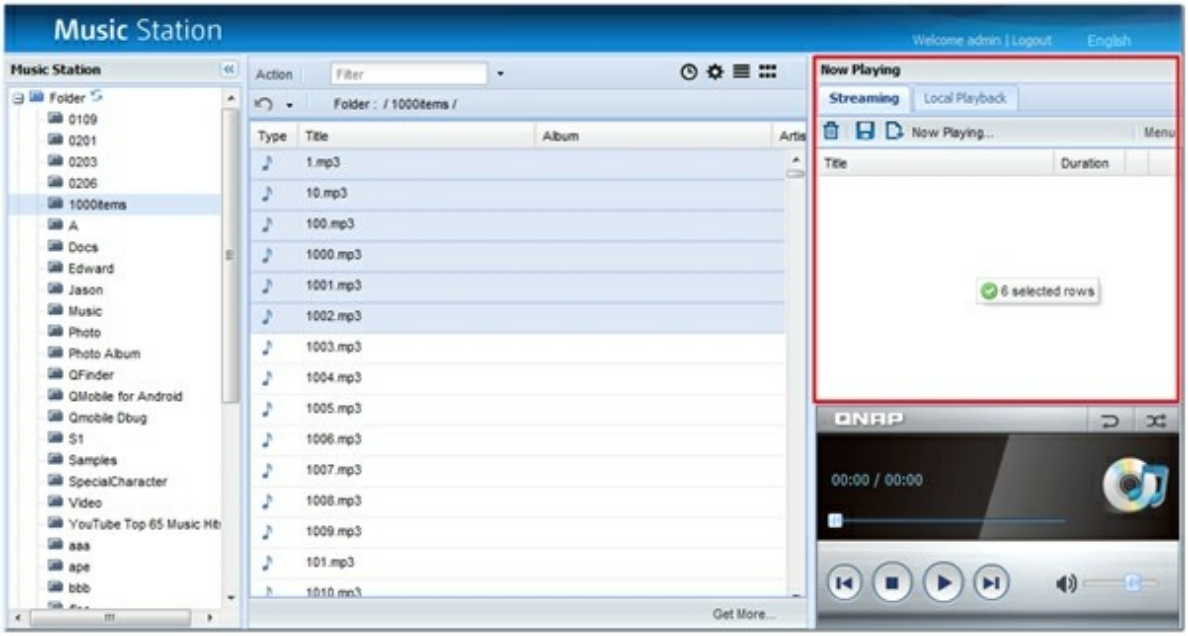
Icon	Description
	Repeat the current playlist.
	Rearrange the item order in the playlist.
	Play.
	Pause.
	Stop.
	Play the previous item.
	Play the next item.
	Adjust the volume.

Play music files

1. Browse the contents in “Folder”, “Playlist”, “Media Server”, or “Internet Radio.
2. Double click a file name to add the file to now playing list and play it immediately or right click one or multiple files and click “Add Selected Entries to Playlist”.

Or

1. Click to show the contents in Details view.
2. Drag and drop one or multiple files to the playlist under “Now Playing”.



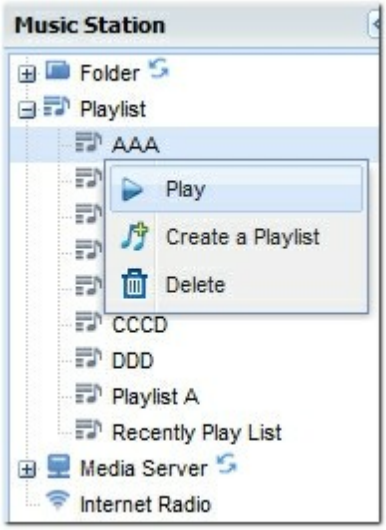
Play a folder

Right click a folder and select "Add Selected Entries to Playlist" or drag and drop the folder to "Now Playing".

> **Note:** If a folder contains more than 100 music files, only the first 100 files will be added to the playlist.

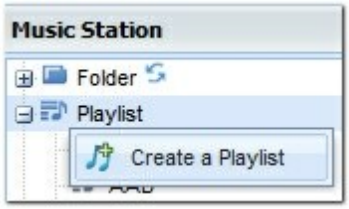
Play a playlist

1. Browse the entries under "Playlist".
2. Right click a playlist and select "Play".



Create a playlist

1. Right click "Playlist" and select "Create a Playlist".



2. Enter the playlist name (max 24 characters) and click "OK".

Or

1. Click under "Now Playing".
2. Add files or folders to the playlist.
3. Click or "Menu" > "Save" and enter the playlist name.
4. Click "OK".

Note: Up to 128 playlists are supported. Each can contain maximum 512 items.

Edit a playlist

1. Drag and drop a playlist from the left panel to "Now Playing".
2. Add files or folders to the playlist, arrange the item order or remove the items.
3. Click or "Menu" > "Save" to save the changes or click "Menu" > "Save as" to save the playlist as a new one.

Arrange item order in a playlist

1. Drag and drop a playlist to "Now Playing".
2. Drag and drop to rearrange the items.
3. Click to save the changes.

Add an Internet radio station

1. Right click “Internet Radio”.
2. Click “Add an Internet Radio”.
3. Enter the name (max 512 characters), URL (max 1024 characters), and description (max 512 characters).
4. Click “OK”.

> **Note:** The type of Internet radio stations must be MP3.

Edit an Internet radio station

1. Right click an Internet radio station.
2. Click “Edit Internet Radio Settings”.
3. Edit the contents and click “OK” to save the changes.

Remove an Internet radio station

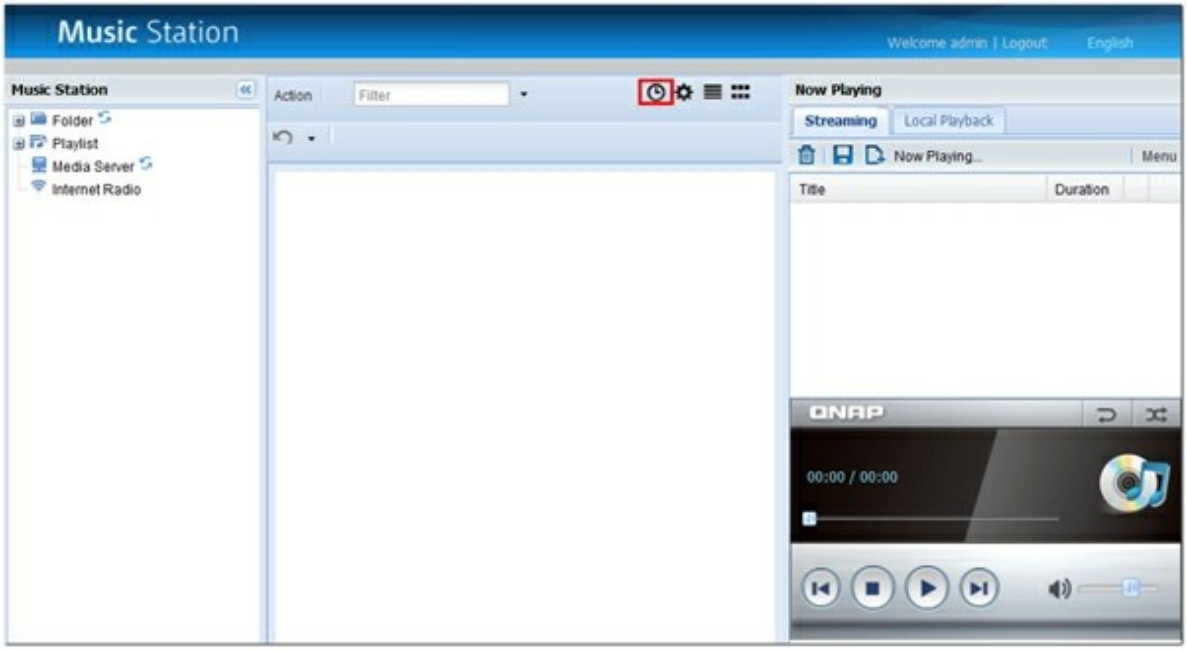
1. Right click an Internet radio station.
2. Click “Remove”.

C. Music Alarm

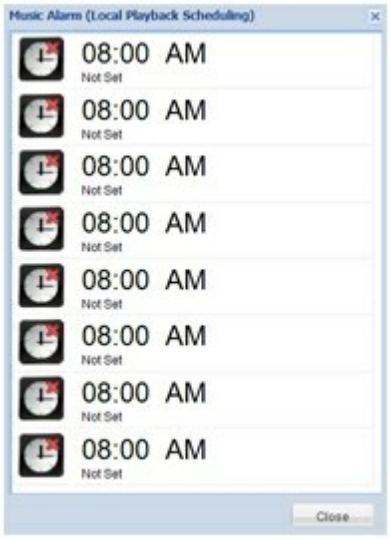
Music Station supports setting music alarm in local playback mode. To use this function, a USB speaker or USB soundcard must be connected to the NAS.

Set music alarm

1. Click .

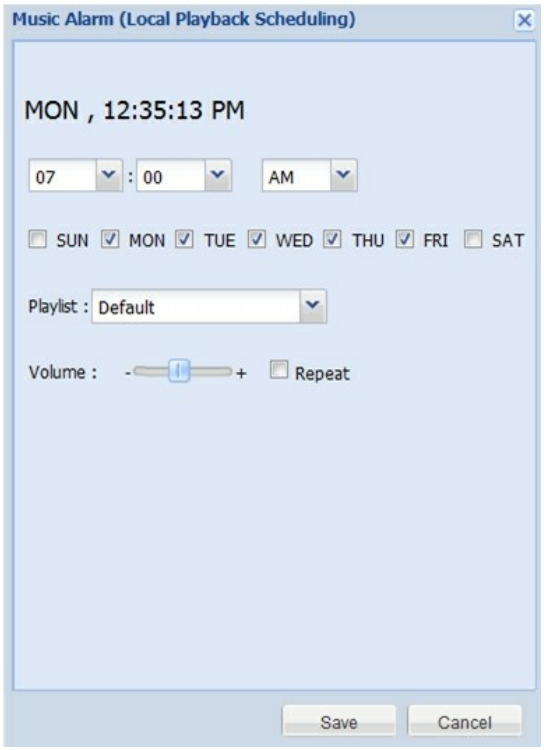


2. Click a schedule.



3. Set up the alarm schedule.
4. Select to use the default alarm or a playlist on Music Station.
5. Adjust the alarm volume.
6. Select "Repeat" to play the playlist repeatedly when the alarm is on.

7. Click “Save”.


Music Alarm (Local Playback Scheduling)
MON , 12:35:13 PM
07
00
AM
SUN MON TUE WED THU FRI SAT
Playlist : Default
Volume :
Repeat
Save
Cancel

Enable/Disable music alarm

Icon	Description
	Alarm is enabled.
	Alarm is disabled.

Click the icons to enable or disable the alarm.

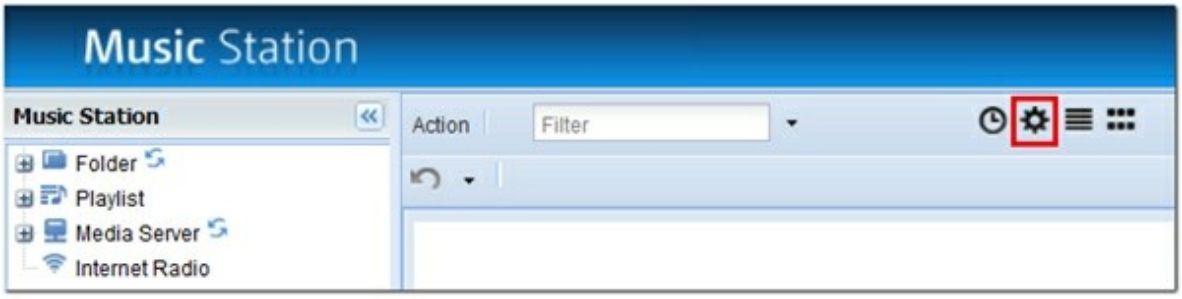
Stop music alarm

To stop the music alarm, press the one touch copy button on the front of the NAS or click the Stop button on the UI of local playback mode.

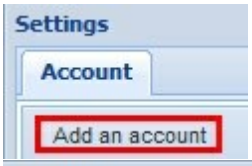
D. Account and Access Management

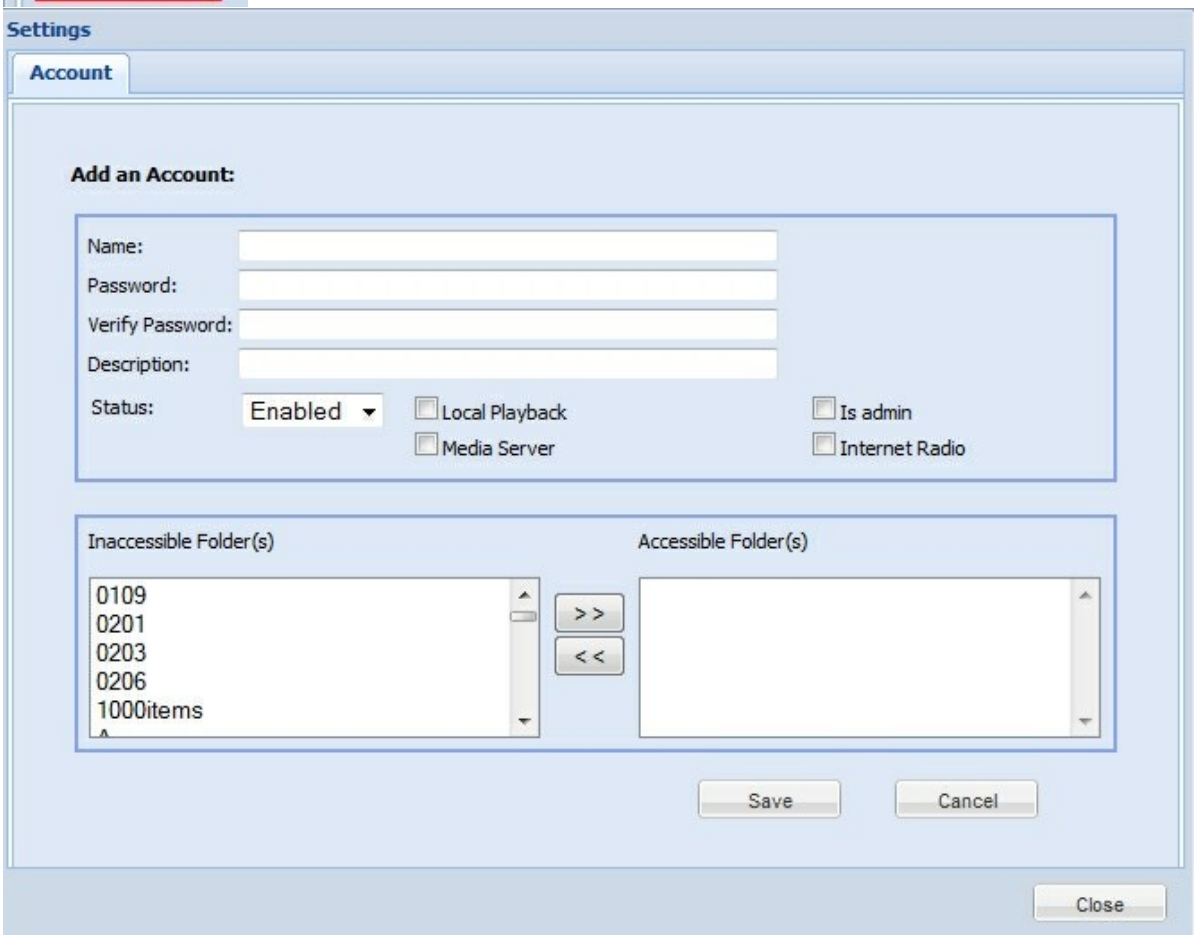
Create an account

1. Click .



2. Click "Add an account".





3. Enter the user name (max 32 characters), password (max 16 characters), and description (max 512 characters). Only alphabets (A-Z and a-z), numbers (0-9), dash (-), and underscore (_) are supported.

4. Enable or disable the account and grant the privileges.
   - Local Playback: Allow the user to play the music files via local playback.
   - Is admin: Allow the user to manage the playlist and configure the music alarms.
   - Media Server: Allow users to access Media Server contents.
   - Internet Radio: Allow users to access the Internet radio stations. If a user is granted both admin and Internet radio access, the user will be able to edit the Internet radio contents.

5. Select the folder(s) the user is allowed to access.

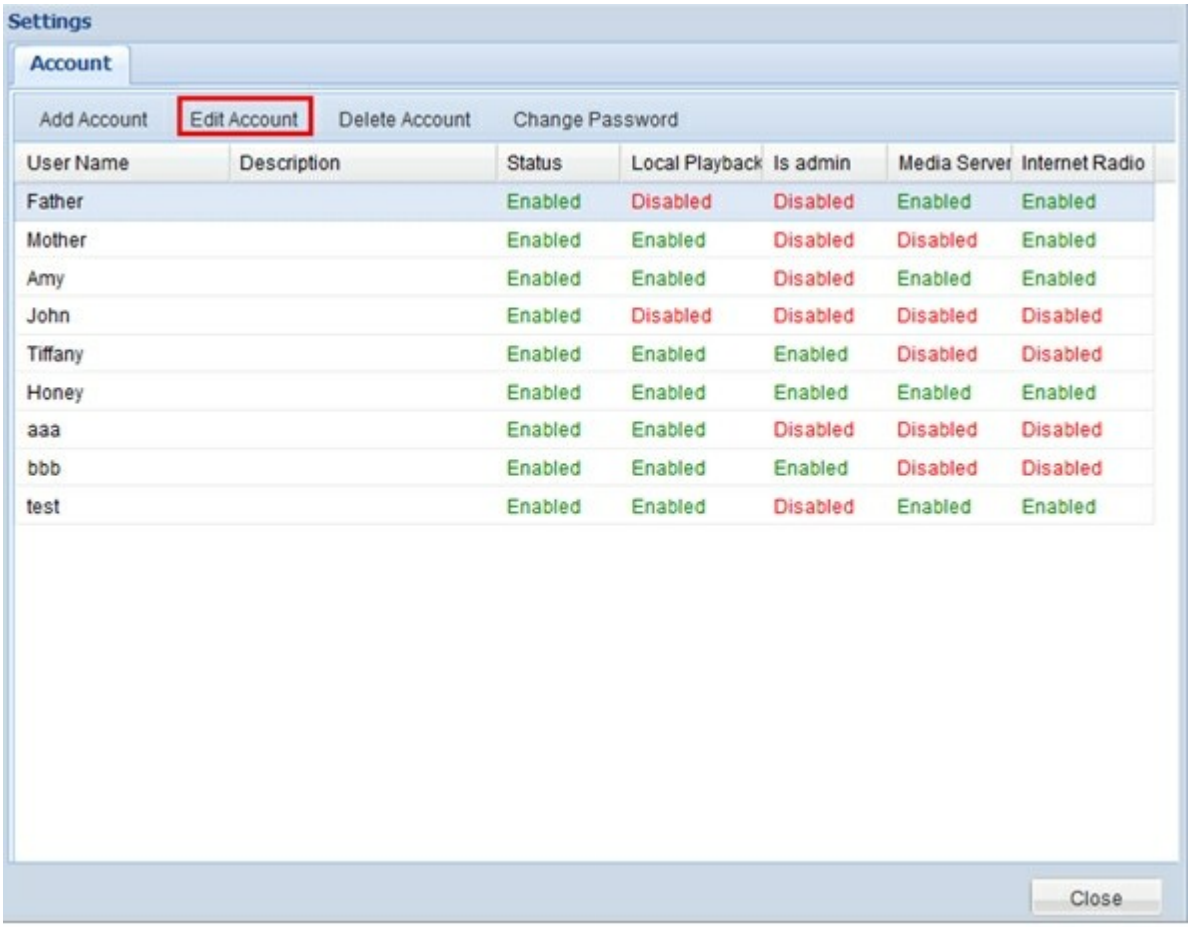
6. Click "Save".

Note:

- The total number of users supported by Multimedia Station, Music Station, and Photo Station is 1024 at maximum, including "admin".
- Users can only view the playlists and music files in inaccessible folders but are unable to play them.

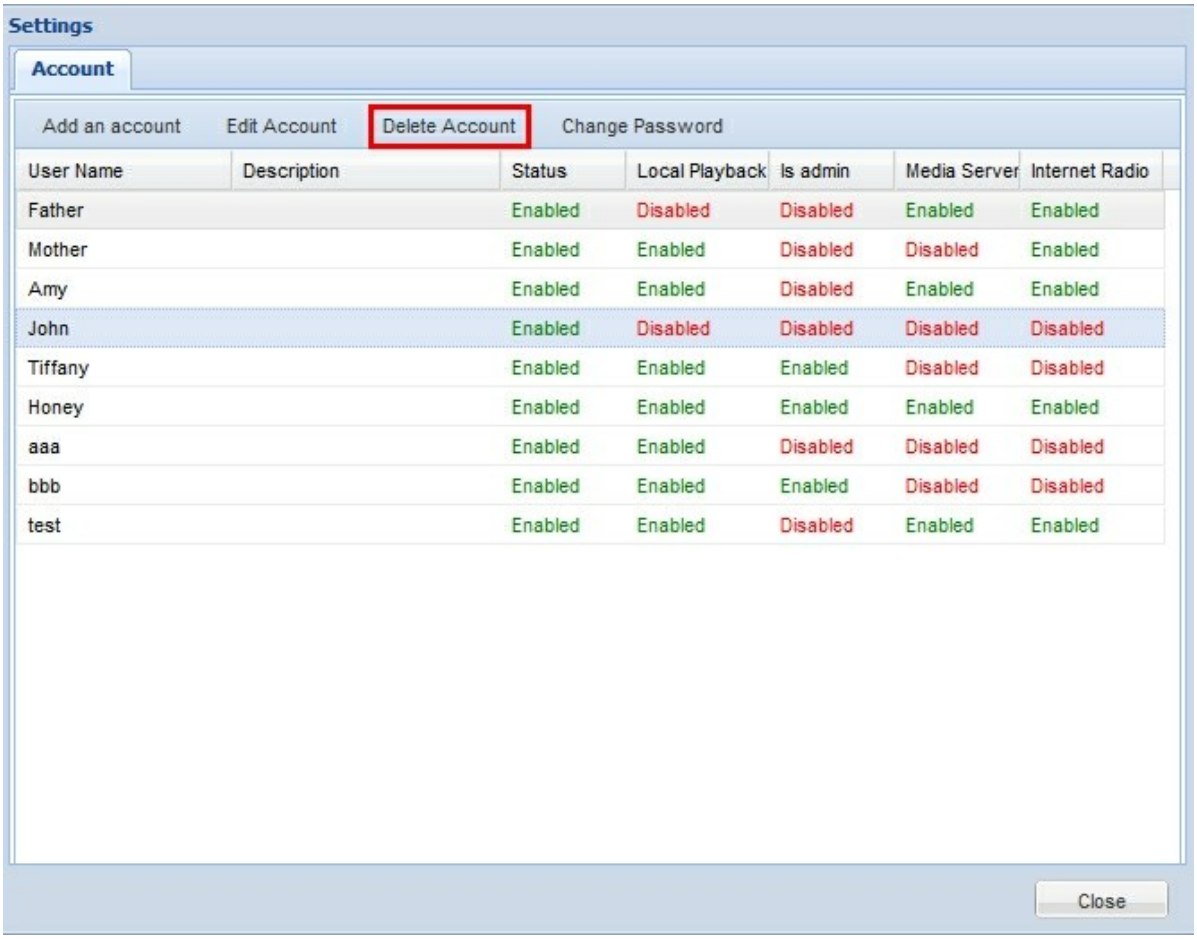
Edit an account

1. Click .
2. Select an account.
3. Click "Edit Account".
4. Edit the settings and click "Save".



Delete an account

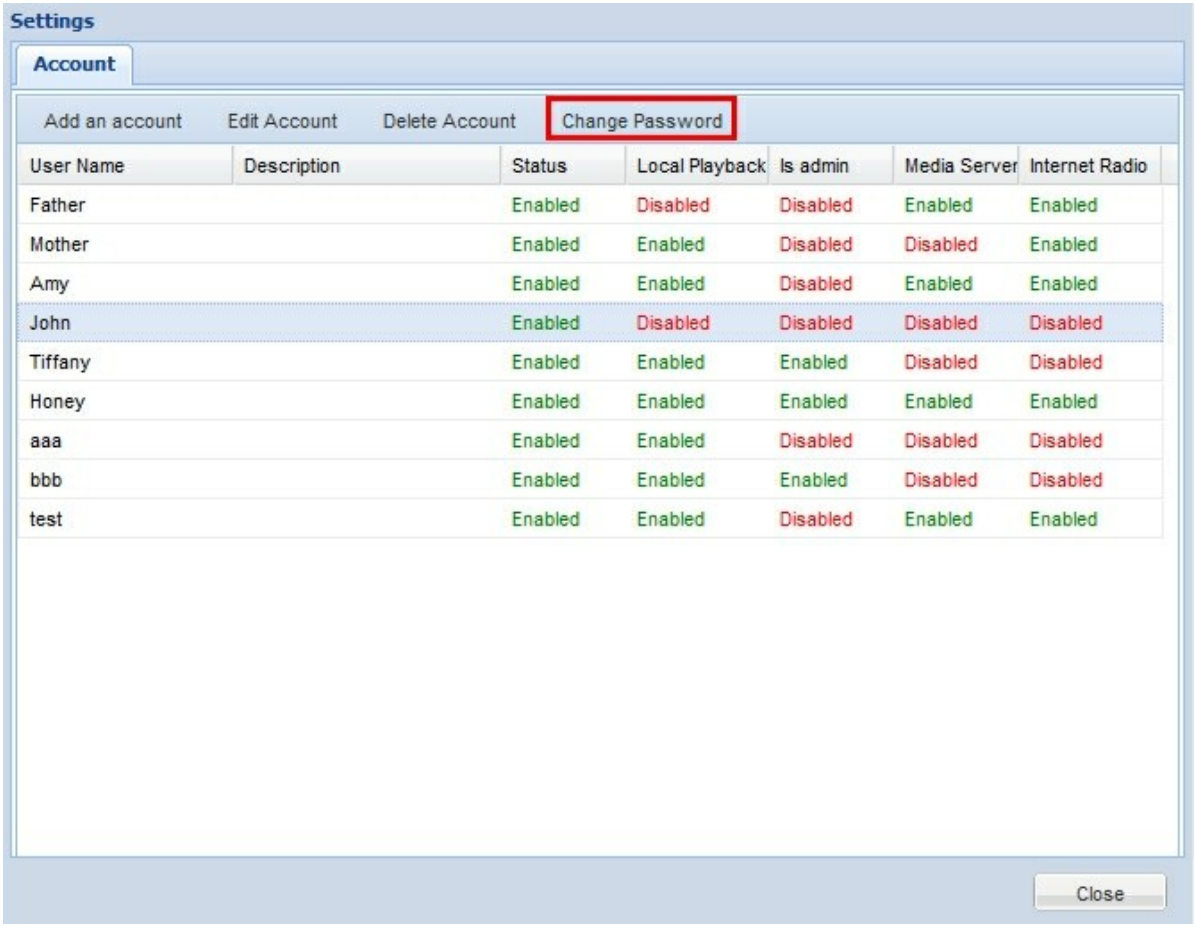
1. Click .
2. Select an account.
3. Click "Delete Account".



4. Click "OK" to confirm.

Change password

1. Click .
2. Select an account.
3. Click "Change Password".



4. Enter the new password and click "Change Password".

7.5 Download Station

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

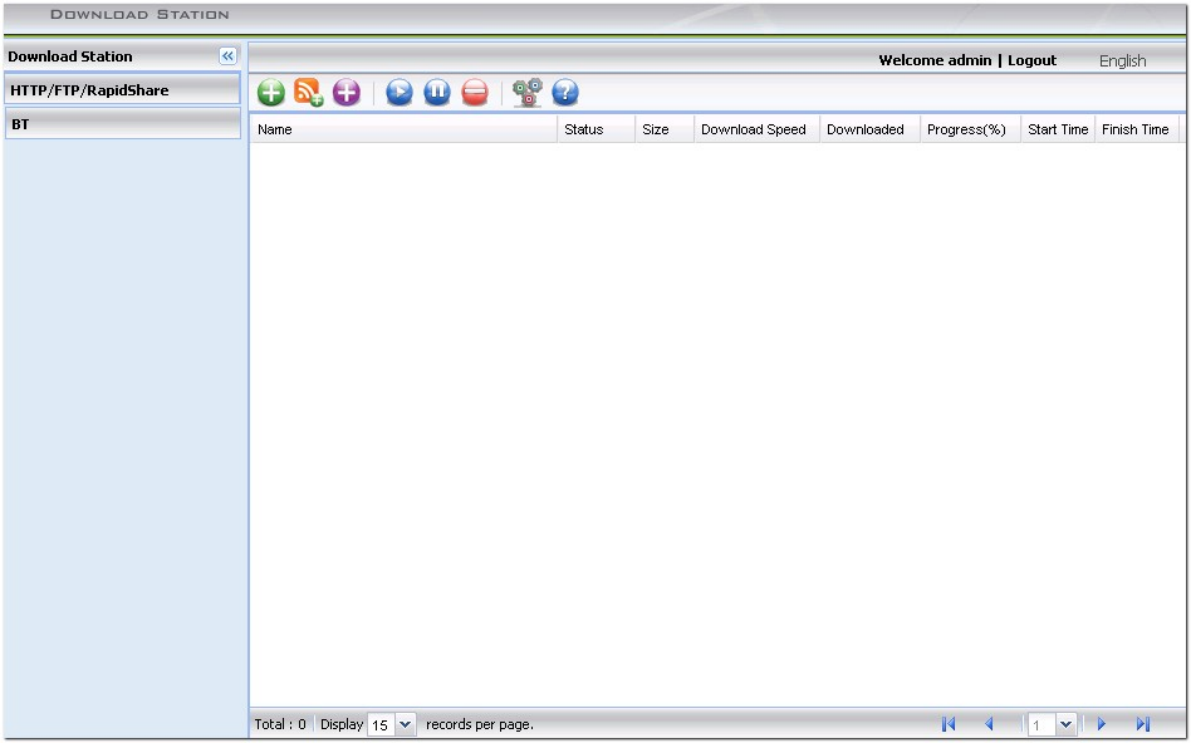
Important: Please be warned against illegal downloading of copyrighted materials. The Download Station functionality is provided for downloading authorized files only. Downloading or distribution of unauthorized materials may result in severe civil and criminal penalty. Users are subject to the restrictions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

Note:

- By updating the NAS firmware from version 3.3.x or below to version 3.4.0 or above, Download Station will be upgraded from v1 to v2. All the tasks in Run, Pause, and Finish lists will be stopped and cleared. The downloaded files will remain.
- Download Station v2 is only compatible with QGet 2.0 or later.

1. Go to "Application Servers" > "Download Station". Enable the service.

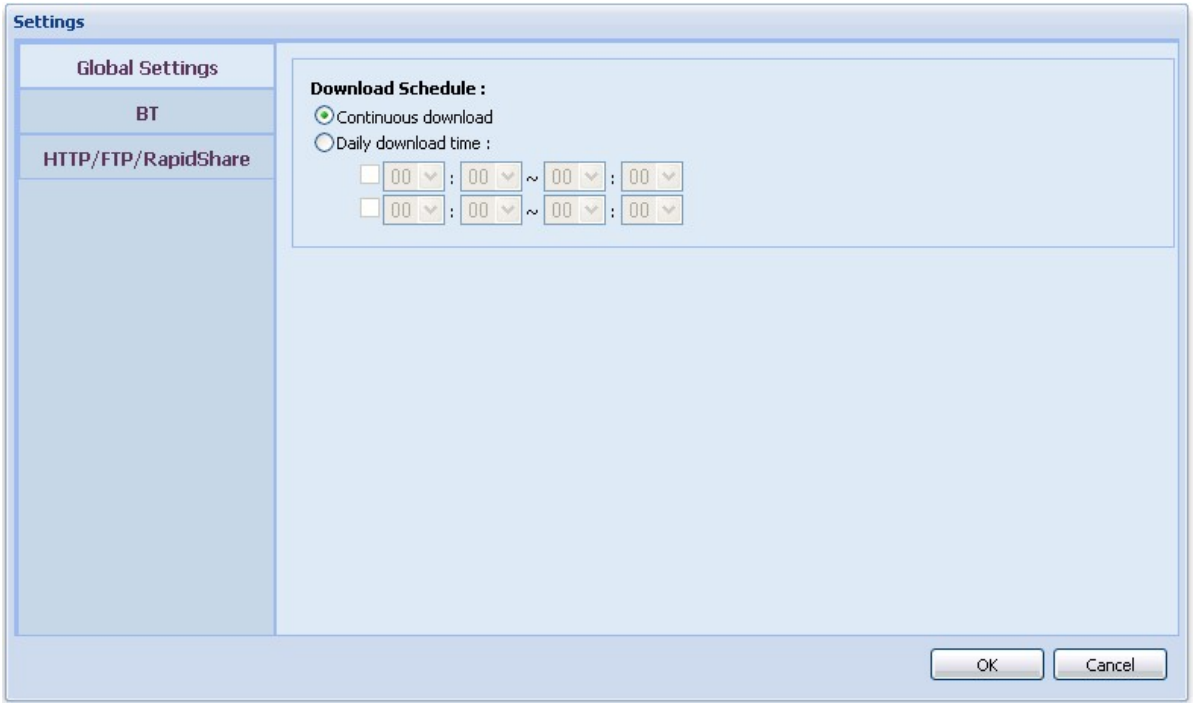
2. Click "Download Station" on the top or on the login page of the NAS to connect to the Download Station. If you login the service from the login page of the NAS, you are required to enter the user name and password.



Before you start to download files, click to configure the download settings.

Global Settings

Select continuous download or specify the download schedule for the task.

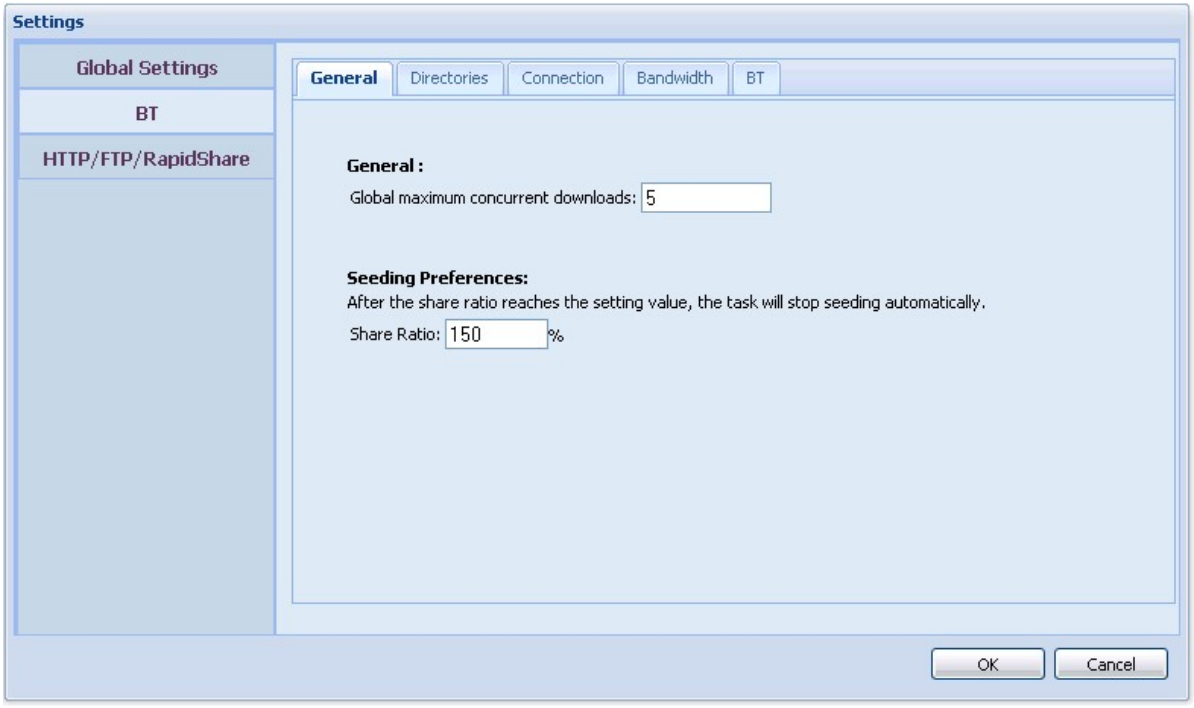


BT Settings

1. General:

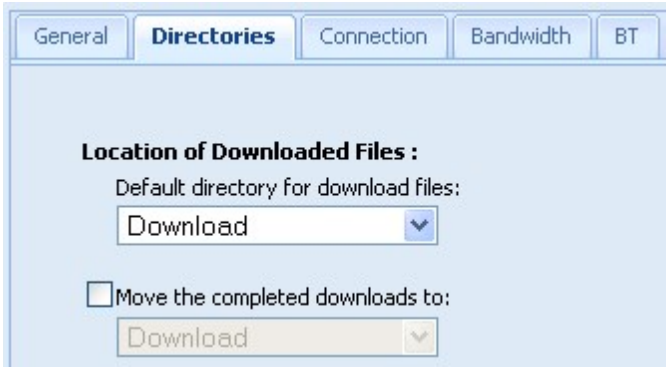
Specify the maximum number of concurrent BT downloads allowed for the NAS and the share ratio. The share ratio is calculated by dividing the amount of uploaded data by the amount of downloaded data. When the ratio has reached its limit, uploading will stop automatically.

NAS models	Maximum number of concurrent downloads
Intel-based NAS	30
ARM-based (Non Intel-based) NAS	10



2. Directories

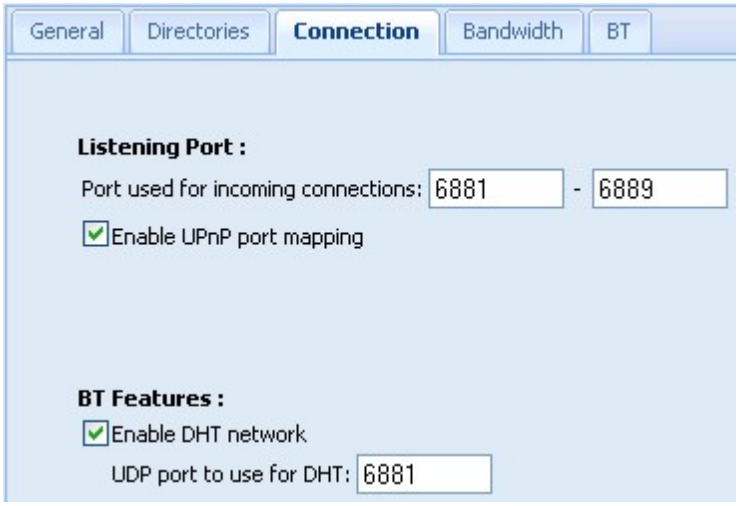
Select the default folder for saving the downloaded files. You can also specify a folder to which the completed downloaded files will be moved to.



3. Connection

Specify the ports for BT download. The default port numbers are 6881-6889. Select UPnP port mapping to enable automatically port mapping on UPnP supported gateway.

Enable DHT network: To allow the NAS to download the files even no trackers of the torrent can be connected, enable DHT (Distributed Hash Table) network and specify the UDP port number for DHT.

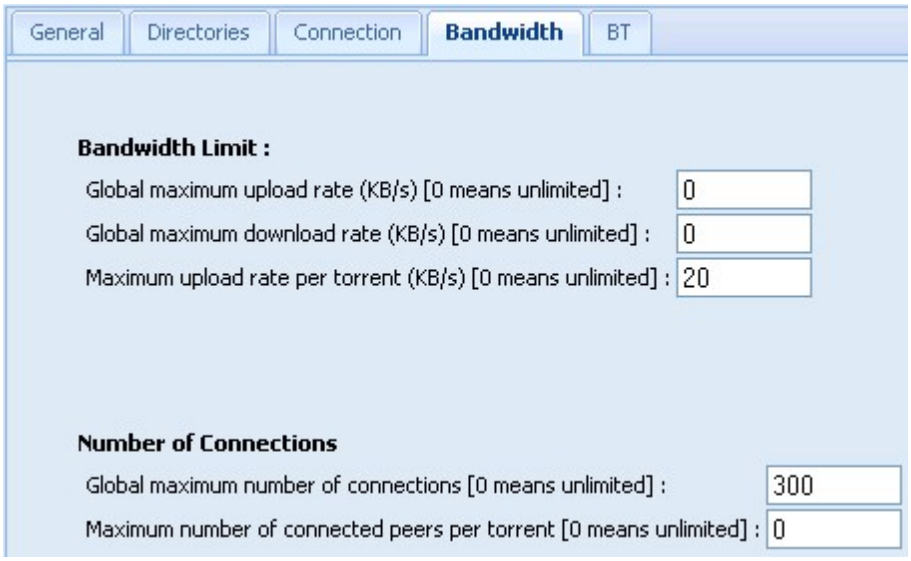


4. Bandwidth

Specify the maximum upload and download rate for all BT download tasks. 0 means no limit.

Global maximum number of connections: This refers to the maximum number of allowed connections to the torrent.

Maximum number of connected peers per torrent: This refers to the maximum number of allowed peers to connect to a torrent.



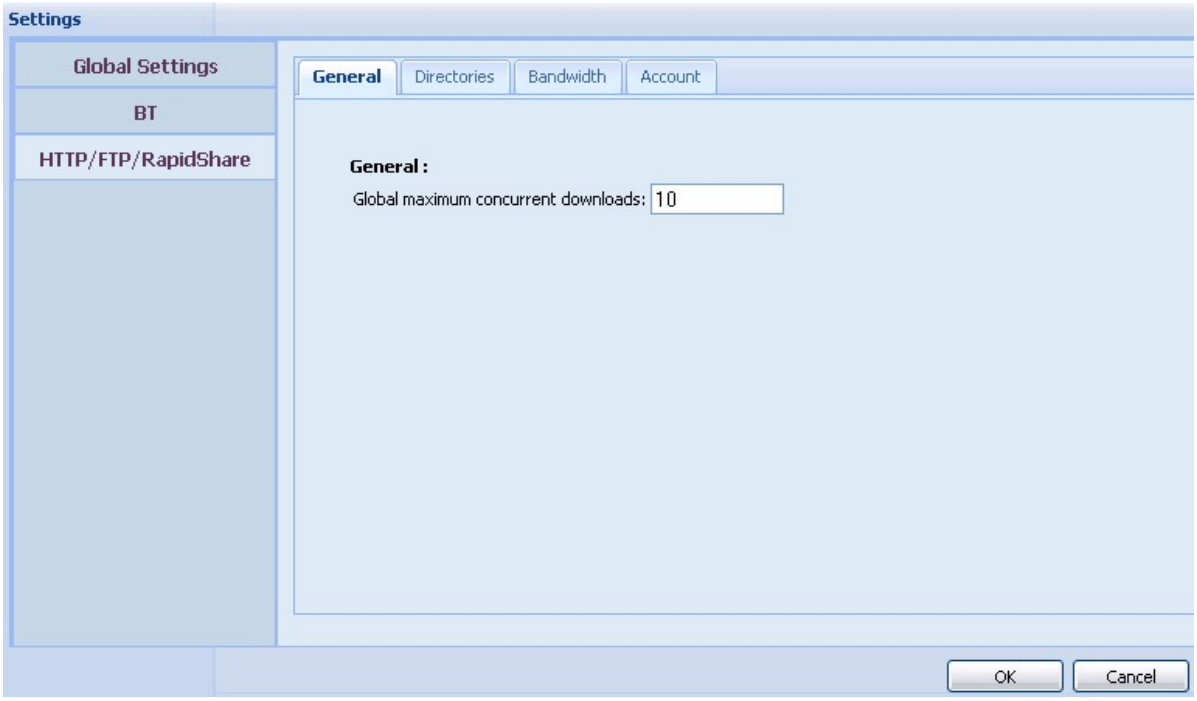
5. BT

Protocol encryption: Enable this option for encrypted data transfer.

HTTP, FTP, RapidShare Settings

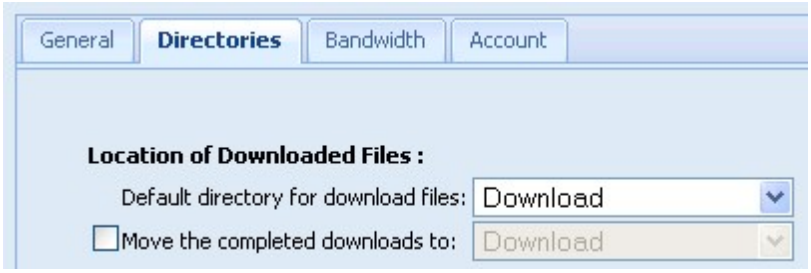
1. General:
Specify the maximum number of concurrent HTTP, FTP, and RapidShare downloads allowed for the NAS. Click "OK" to save the changes.

NAS models	Maximum number of concurrent downloads
Intel-based NAS	30
ARM-based (Non Intel-based) NAS	10



2. Directories

Select the default folder for saving the downloaded files. You can also specify a folder to which the completed downloaded files will be moved to. Click "OK" to save the changes.

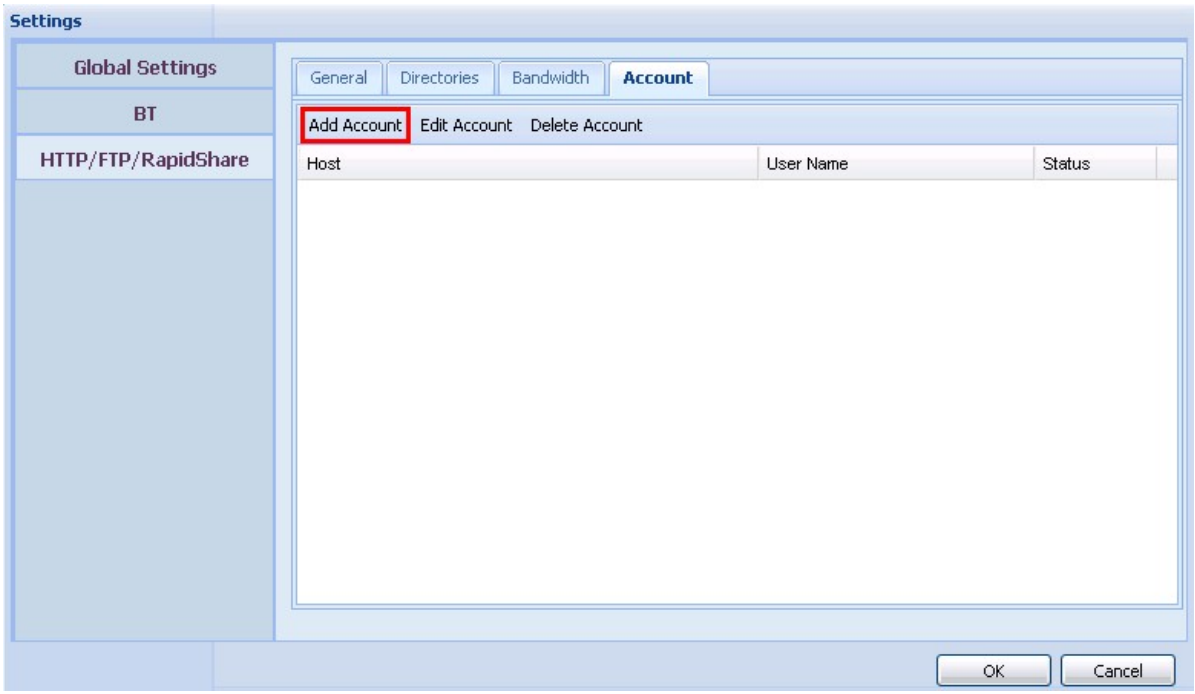


3. Bandwidth

Specify the maximum download rate of a single HTTP, FTP, or RapidShare download. 0 means no limit. Click "OK" to save the changes.

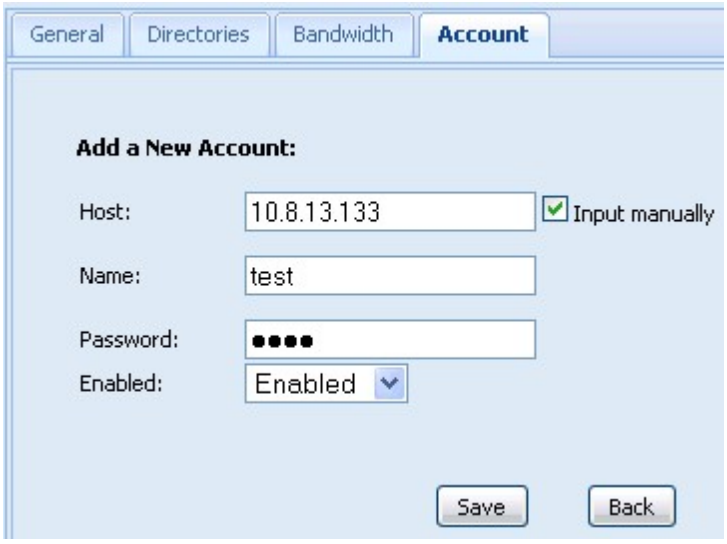
4. Account

You can save the login information of maximum 64 HTTP, FTP, and RapidShare accounts. To add login information, click “Add Account”.

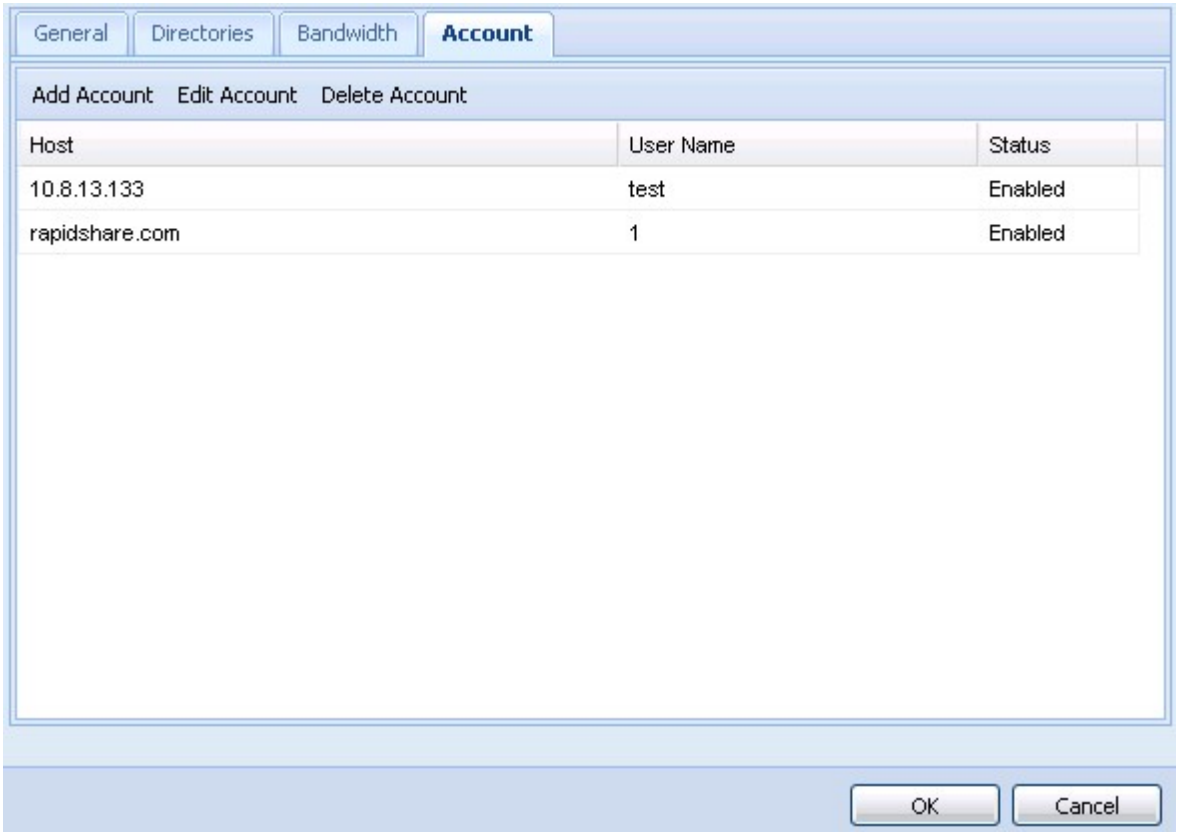


The default host is rapidshare.com. To enter the login information for an HTTP or FTP server, select “Input manually”.

Enter the host name or IP, user name and password. To allow the login information to appear for account selection when configuring HTTP, FTP, or RapidShare download, select "Enabled" from the drop-down menu. Click "Save" to confirm or "Back" to cancel.

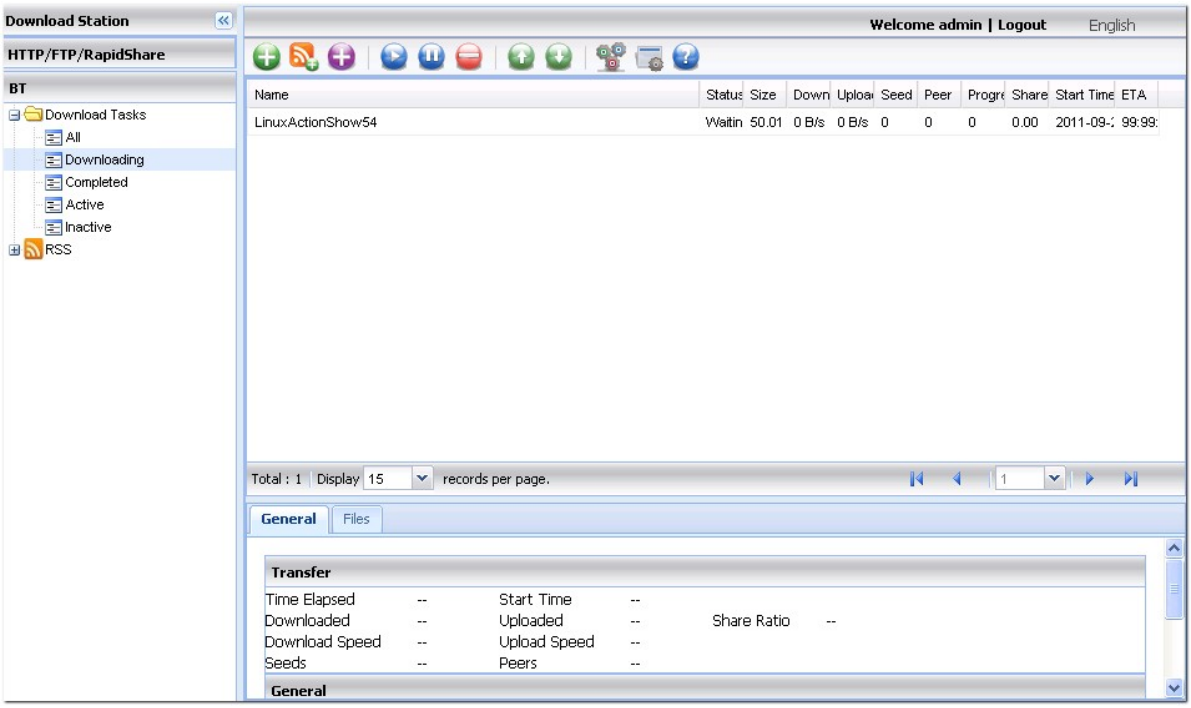


To edit the settings of an account, select an entry on the list and click "Edit Account". To delete an account, select an entry on the list and click "Delete Account". Click "OK" to save the changes to General, Directories, and Bandwidth.

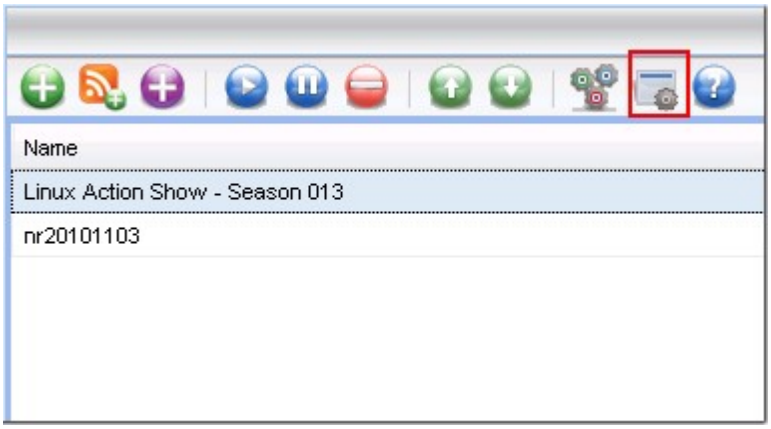


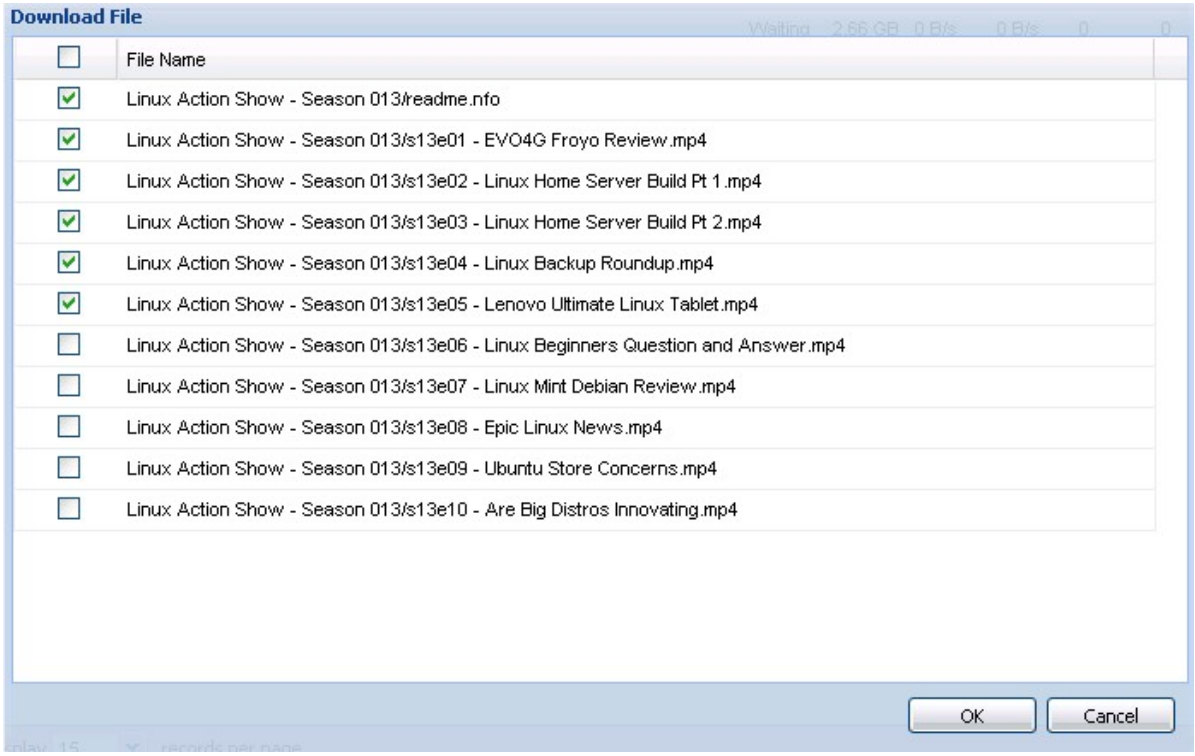
BT Download

To download a file by BT, click . Browse and select a torrent file and click "OK". The download task will be shown under "BT" > "Download Tasks" > "All" or "Downloading". You can view the details and the download status of the task.

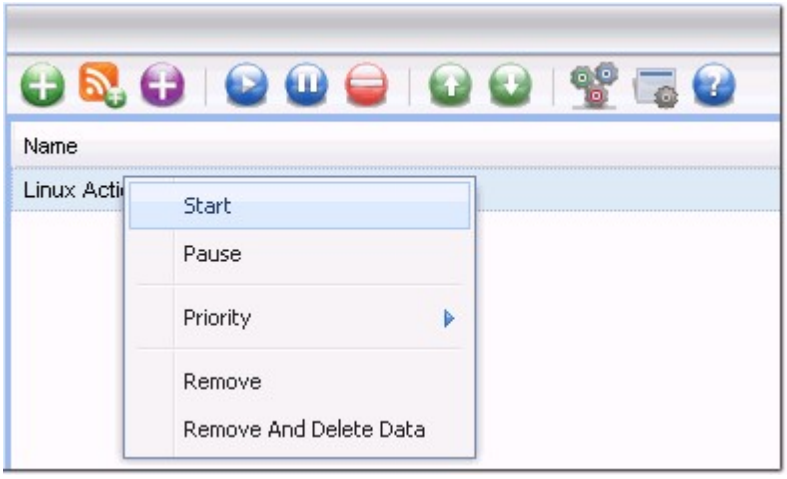


You can select particular files to download from a torrent file. Select a download task on the list. Click and select the files to download.





You can view the download tasks and right click a task to start, pause, prioritize, or remove a task. To remove a download task and all its downloaded data, select "Remove and Delete Data".

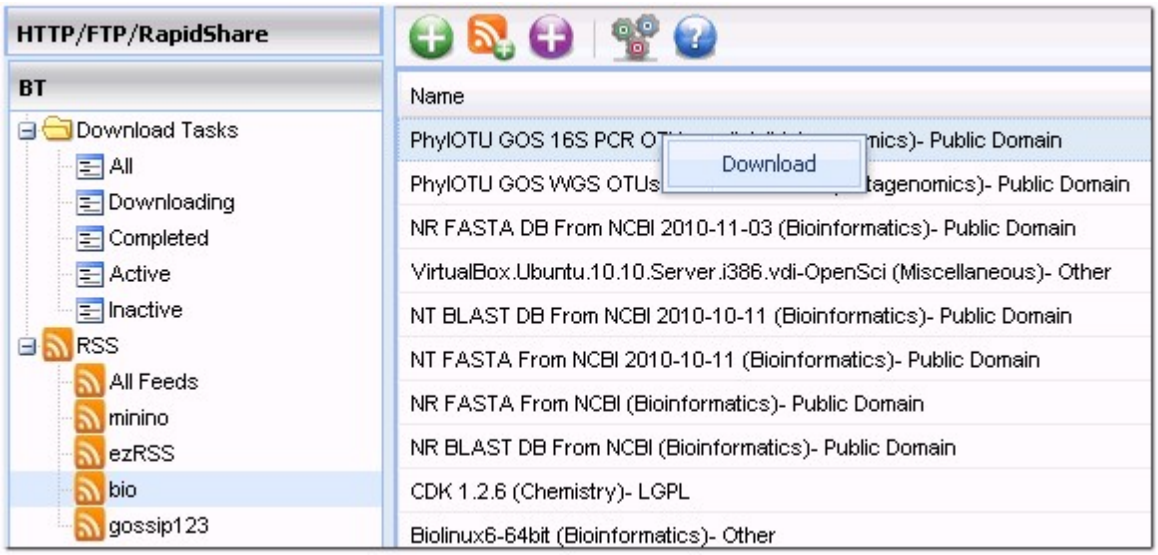


RSS Feed

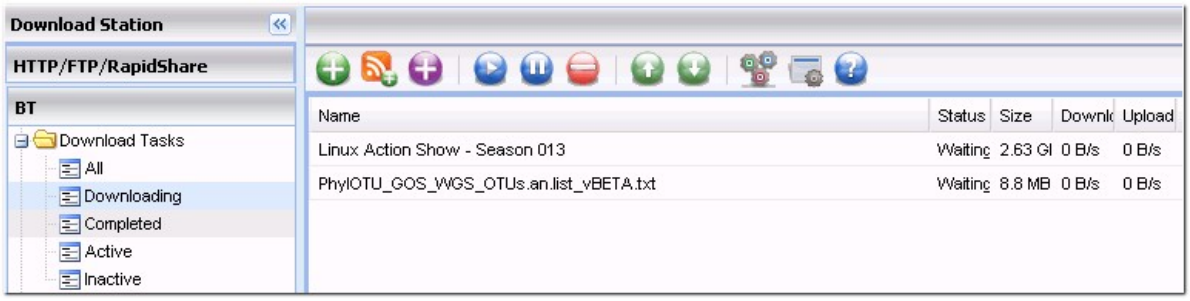
You can subscribe to RSS feeds by Download Station and download the torrent files in the feeds. Click to add an RSS feed.

Enter the URL and the label.

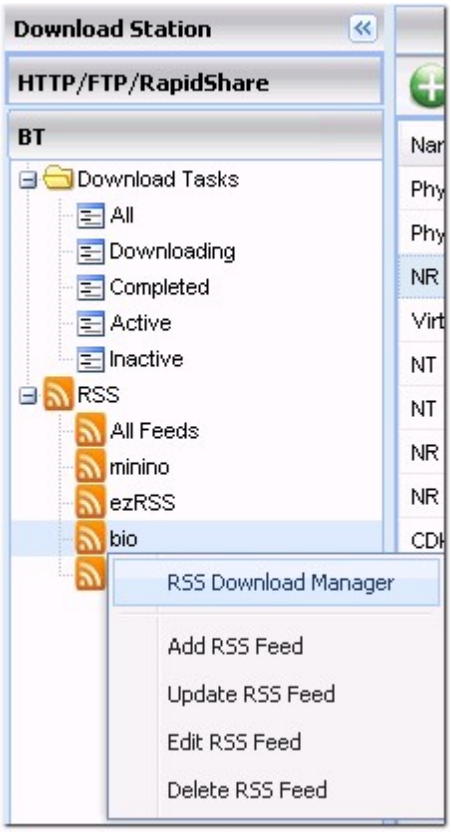
You can view the RSS feeds by expanding "BT" > "RSS" on the left panel of Download Station. To download a torrent file from an RSS feed, right click the feed and select "Download".



The NAS will start to download the file automatically. You can view the download status in BT download.



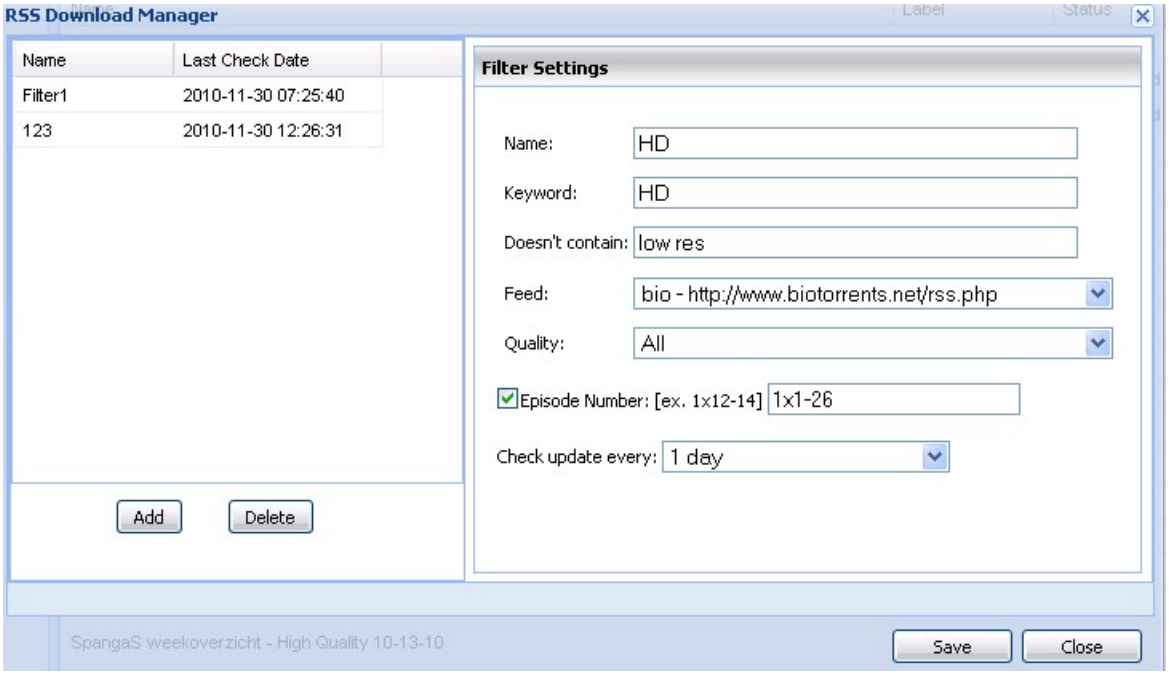
To manage the RSS feeds subscription, right click an RSS feed label. You can open RSS Download Manager, add, update, edit, or delete an RSS feed.



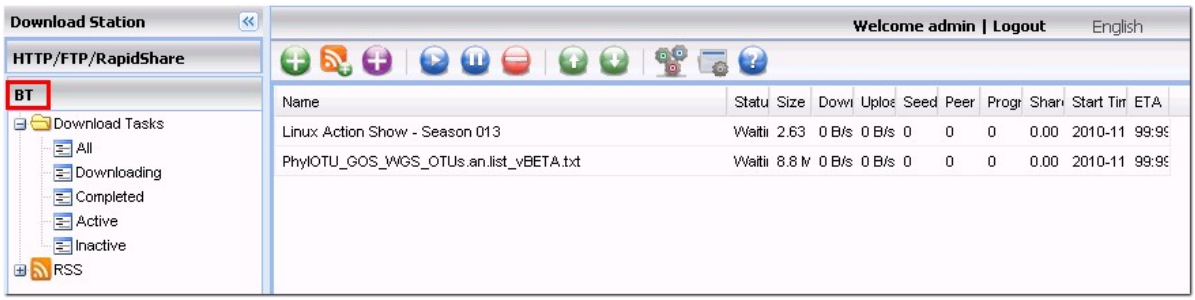
RSS Download Manager

You can use RSS Download Manager to create and manage filters to download particular torrent files for BT Download.

1. To add a filter, click "Add".
2. Enter the filter name and specify the keyword to include and exclude.
3. Select the RSS feed to apply the filter settings.
4. You may also specify the quality of the video torrent files (leave it as "All" if you do not need this function or the torrent file is not a video).
5. Episode number: Select this option to specify particular episodes or a serial of episodes of a drama work. For example, to download episodes 1-26 of season 1 of a TV program, enter 1x1-26. To download only episode 1 of season 1, enter 1x1.
6. Select the time interval for automatic update of the RSS feeds. The NAS will update the RSS feeds and check if any new contents that match the filters are available.
7. Click "Save" to save the filter or "Close" to cancel or exit.
8. To delete a filter, select the filter from the list and click "Delete".



You can view the status of all BT download tasks by clicking "BT" on the left column.

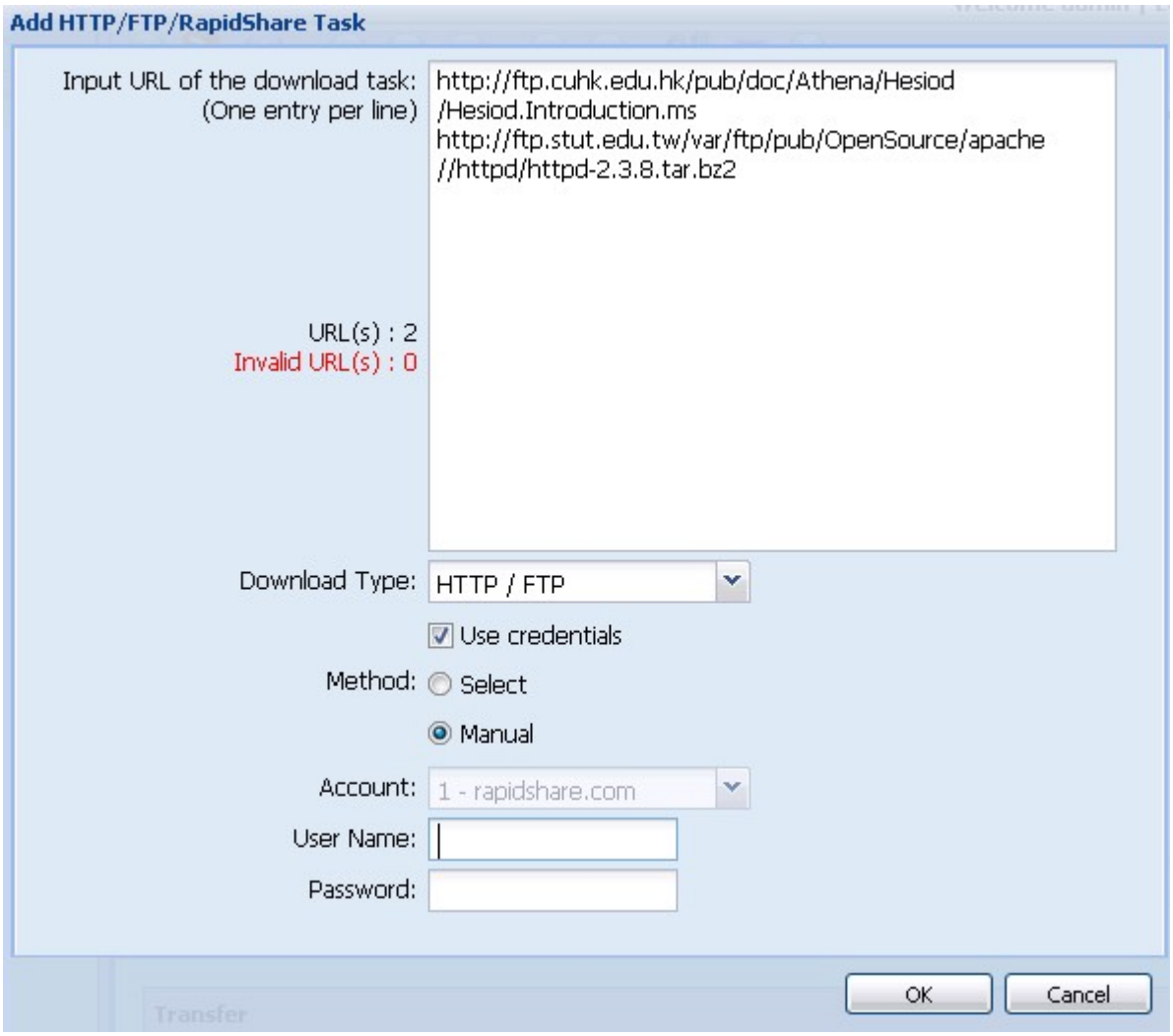


HTTP, FTP, RapidShare, Magnet Download

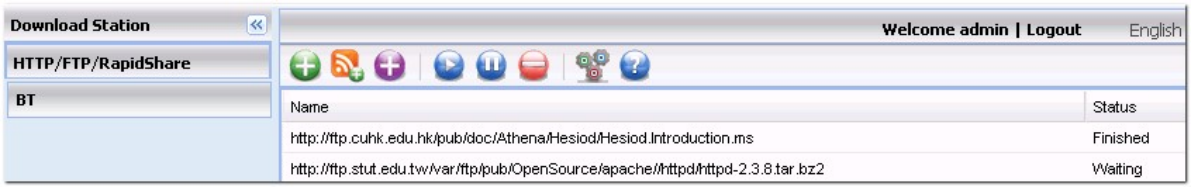
To add an HTTP, FTP, RapidShare, or Magnet download task, click .

Enter the URL of the download task (one entry per line). Then select the download type: HTTP/FTP, RapidShare, or Magnet Link. If a user name and password is required to access the file, select "Use credentials" and select a pre-configured account (Settings > HTTP/FTP/RapidShare > Account) or enter a user name and password. Then click "OK". The NAS will download the files automatically.

> **Note:** You can only enter maximum 30 entries at one time.



You can view the status of the download tasks by clicking “HTTP/FTP/RapidShare” on the left column.



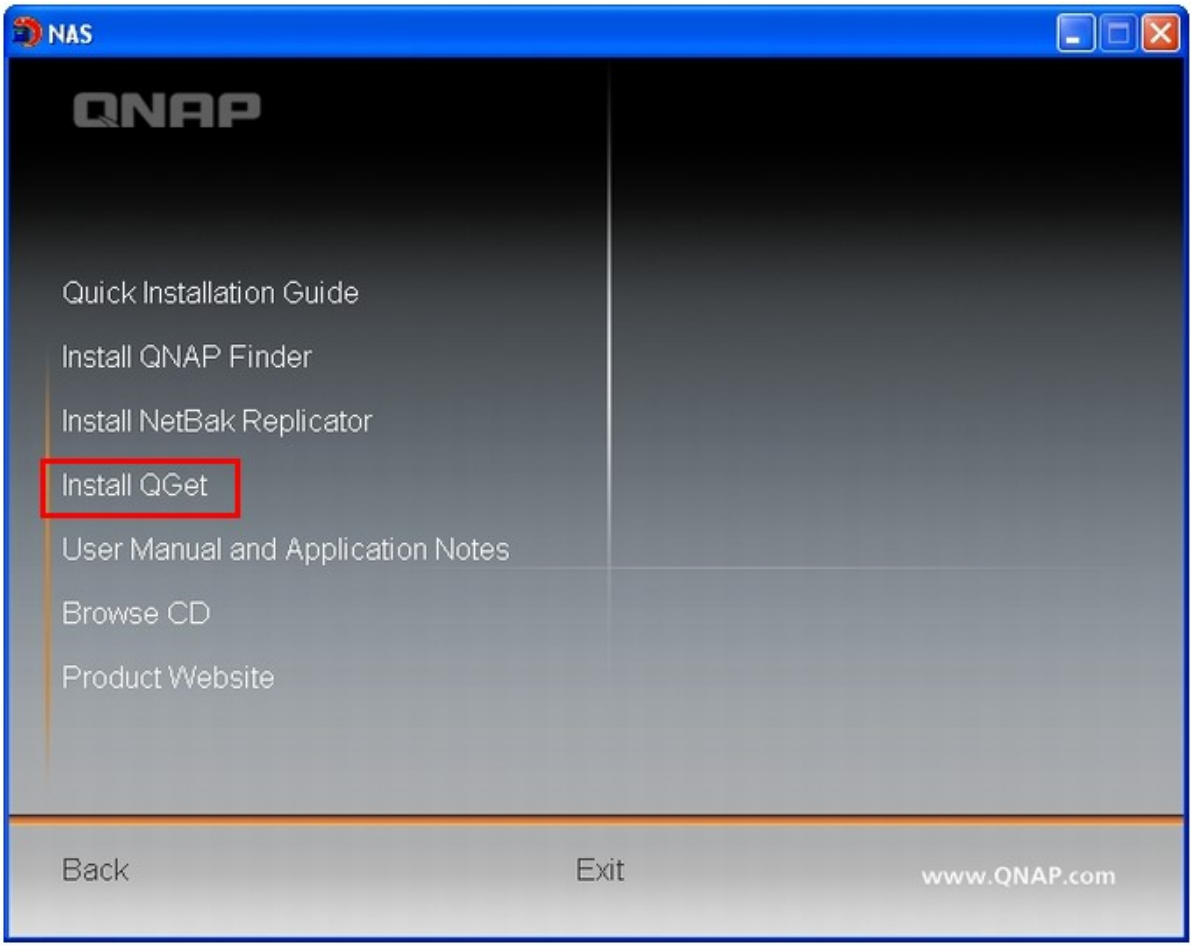
The common reasons for slow BT download rate or download error are as below:

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 BT 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.

Use Download Software QGet

QGet is a utility to manage the download tasks on multiple NAS servers over LAN or the Internet. You can install the software on multiple PCs or Macs; no license is required. QGet is compatible with Download Station v1 and v2.

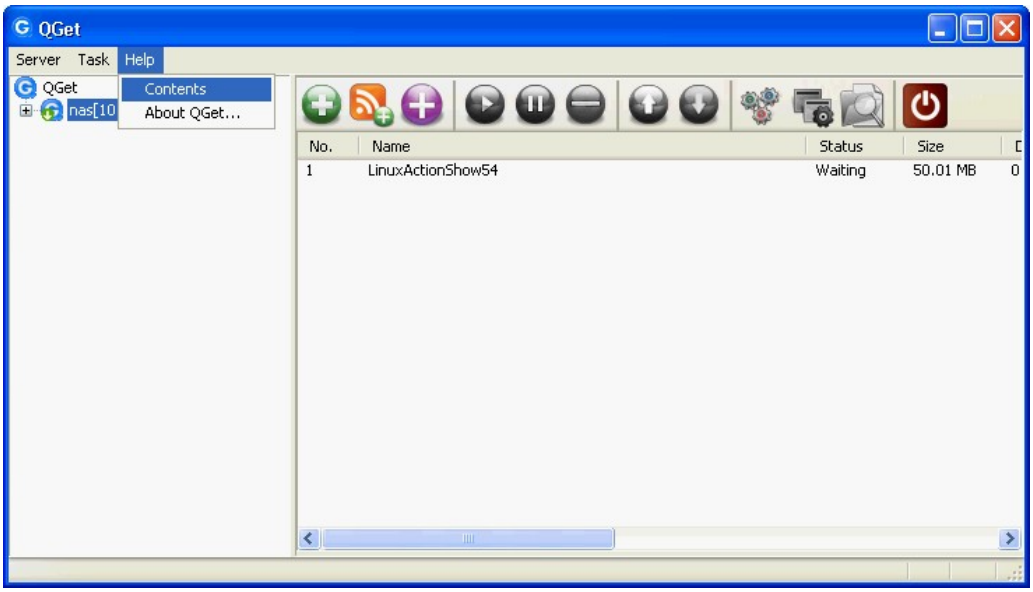
1. Install QGet from the product CD-ROM disc.



2. Follow the instructions to install QGet.

3. Run QGet from the installed location.

4. You can use QGet to manage the download tasks on multiple NAS servers as if you were using the web-based Download Station. For the introduction and button description of QGet, see the online help in "Help" > "Contents".



Note: Download Station v2 is only compatible with QGet 2.0 or later.

7.6 Surveillance Station

You monitor and record the live video of maximum 2-4 IP cameras available on the network (LAN or WAN) with Surveillance Station. If your NAS models are not listed, please visit http://www.qnap.com for details.

Maximum number of IP cameras	NAS models
2	TS-110, TS-210, TS-112, TS-119, TS-119P+, TS-210, TS-212, TS-219P+, TS-239 Pro II+, TS-259 Pro+
4	TS-410, TS-412, TS-419P+, TS-410U, TS-419U, TS-412U, TS-419U+, SS-439 Pro, SS-839 Pro, TS-439 Pro II+, TS-459U-RP/SP, TS-459U-RP+/SP+, TS-459 Pro+, TS-459 Pro II, TS-559 Pro+, TS-559 Pro II, TS-659 Pro+, TS-659 Pro II, TS-859 Pro+, TS-859U-RP, TS-859U-RP+, TS-809 Pro, TS-809U-RP, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP

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 the NAS to connect to 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 the NAS, follow the steps below:

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

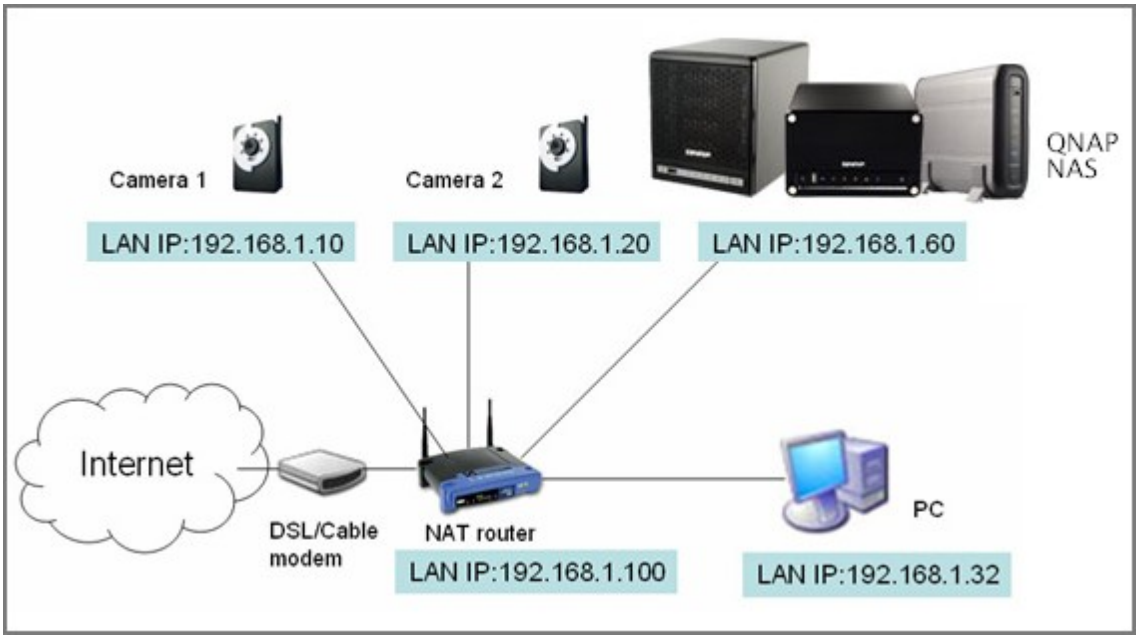
Plan your home network topology

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

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

Your computer, the NAS, and the IP cameras should be connected to the same router on the 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)



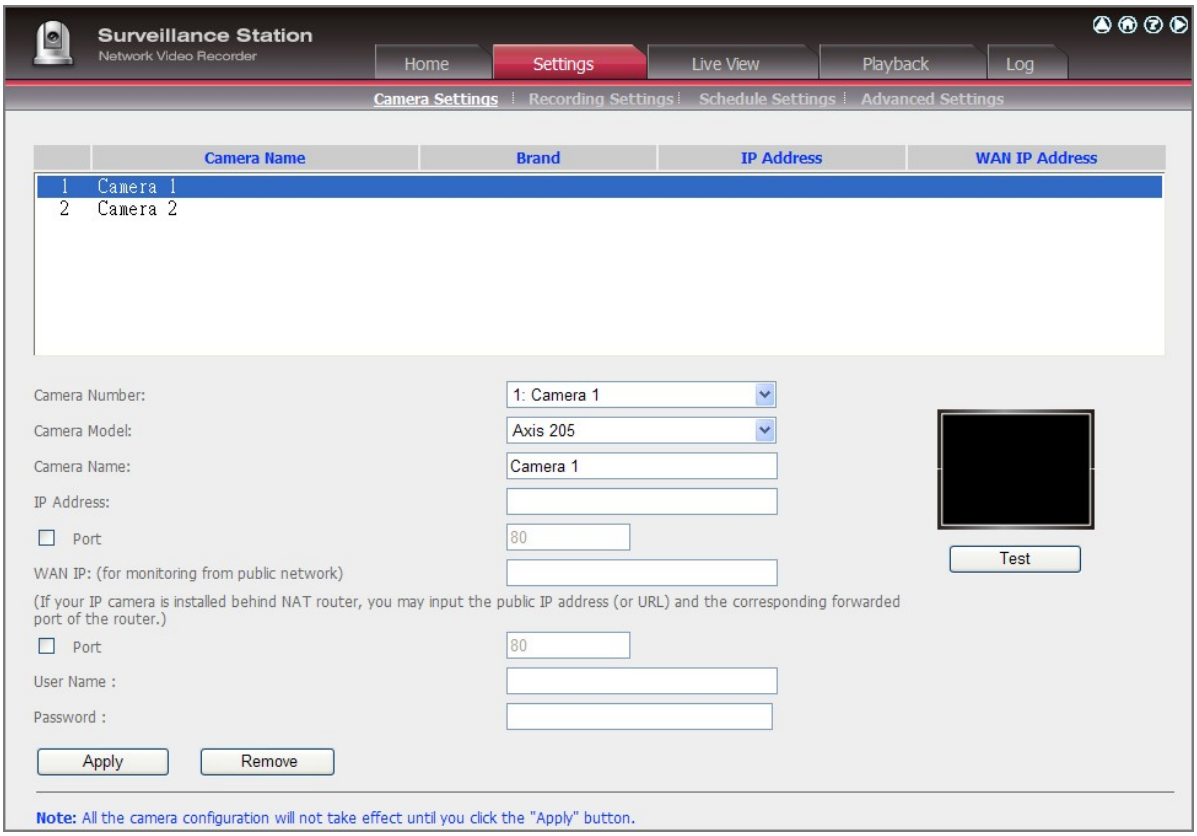
Set up the IP cameras

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 IP 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 IP camera as 192.168.1.20.
Some IP cameras provide a utility for IP configuration. You may refer to the user manual of the cameras for further details.

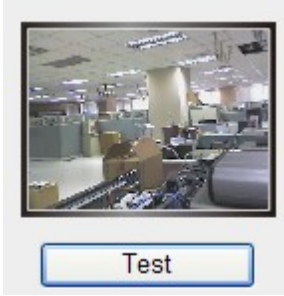
* Please refer to http://www.qnap.com for the supported network camera list.

Configure the camera settings on the NAS

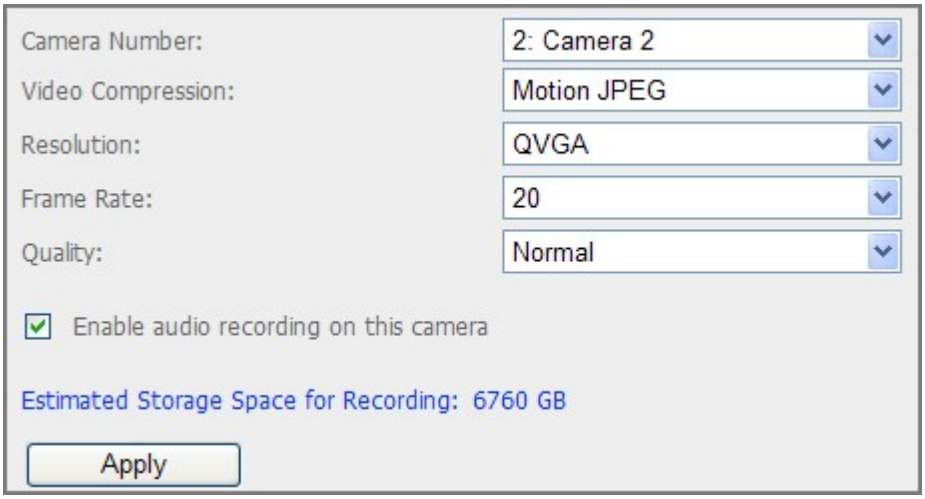
Login the Surveillance Station by the IE browser to configure the IP cameras. Go to "Settings" > "Camera Settings". Enter the IP camera information, for example, name, model, and IP address.



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



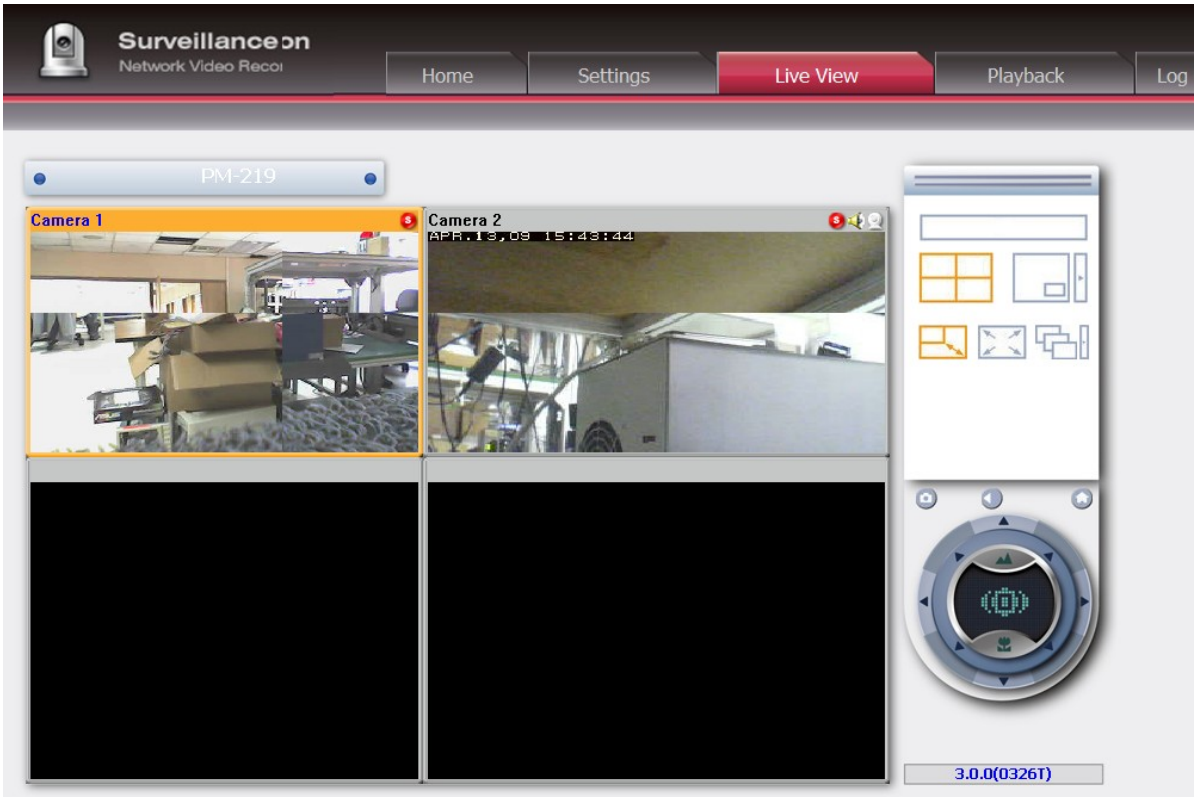
If your IP camera supports audio recording, you may enable the option on the “Recording Settings” page. Click “Apply” to save the changes.



Configure the settings of IP camera 2 following the above steps.

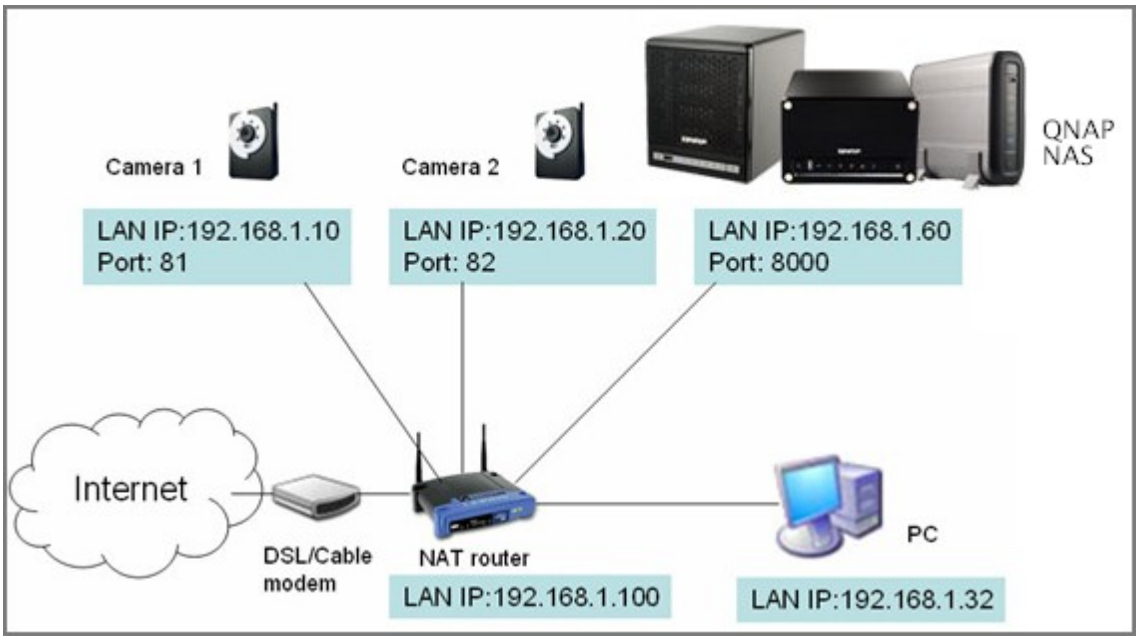
After you have added the network cameras to the NAS, go to the "Live View" page. The first time you connect to this page by the IE browser, you have to install the ActiveX control in order to view the images of IP camera 1 and IP camera 2. You can start to use the monitoring and recording functions of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

To use other functions such as motion detection recording, scheduled recording, and video playback, see the online help.



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

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



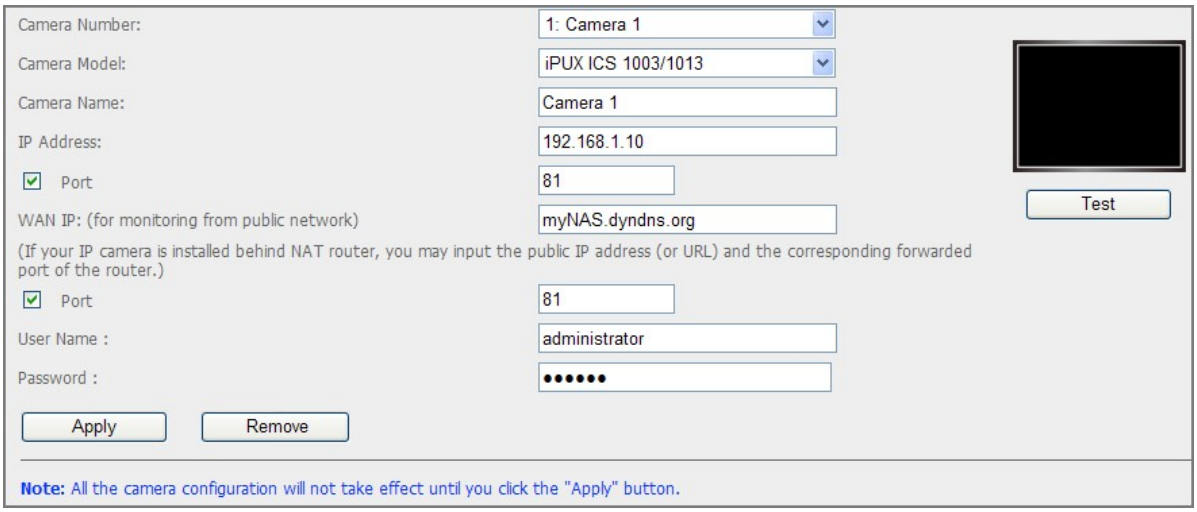
Change the port settings of the NAS and the IP cameras

The default HTTP port of NAS is 8080. In this example, the port is changed to 8000. Therefore, you have to connect to 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 IP camera 1 from 80 to 81. Then change the port of IP camera 2 from 80 to 82.

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

Besides, enter the WAN IP address (or your domain address on the public network, for example, MyNAS.dyndns.org) and the port on the WAN for the connection from the Internet. After finishing the settings, click "Test" to verify the connection.



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

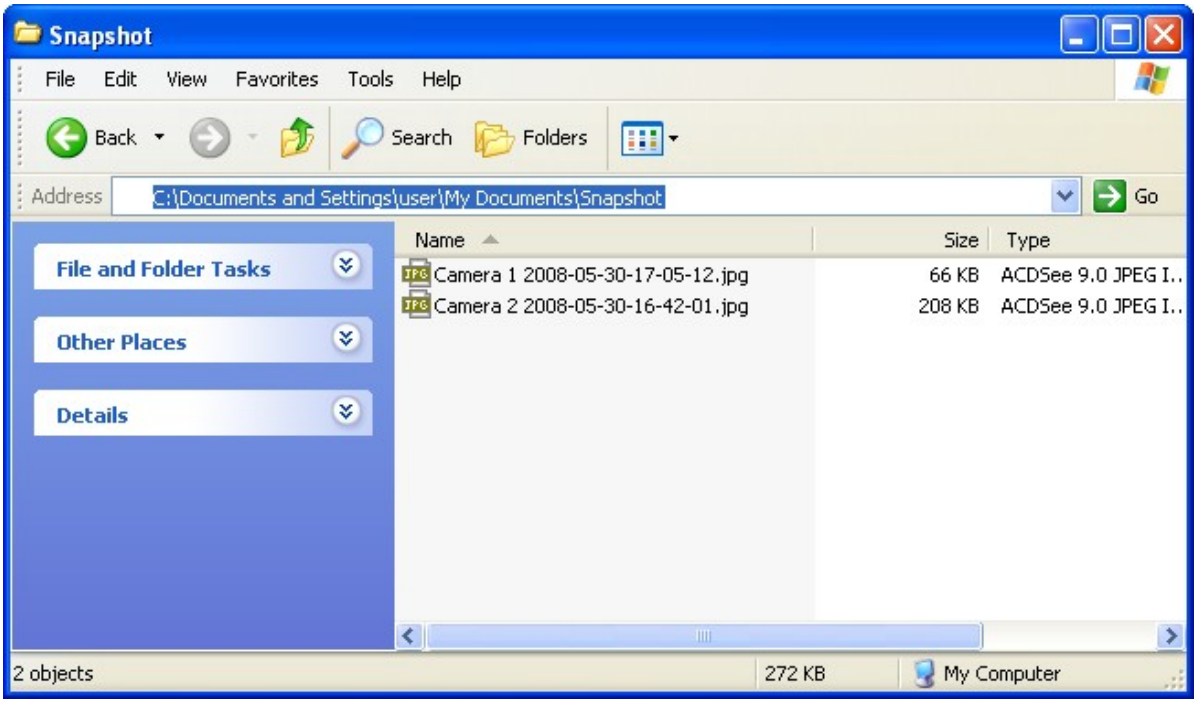
- Forward port 8000 to the LAN IP of the NAS: 192.168.1.60
- Forward port 81 to the LAN IP of IP camera 1: 192.168.1.10
- Forward port 82 to the LAN IP of IP camera 2: 192.168.1.20

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

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

Connect to 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".

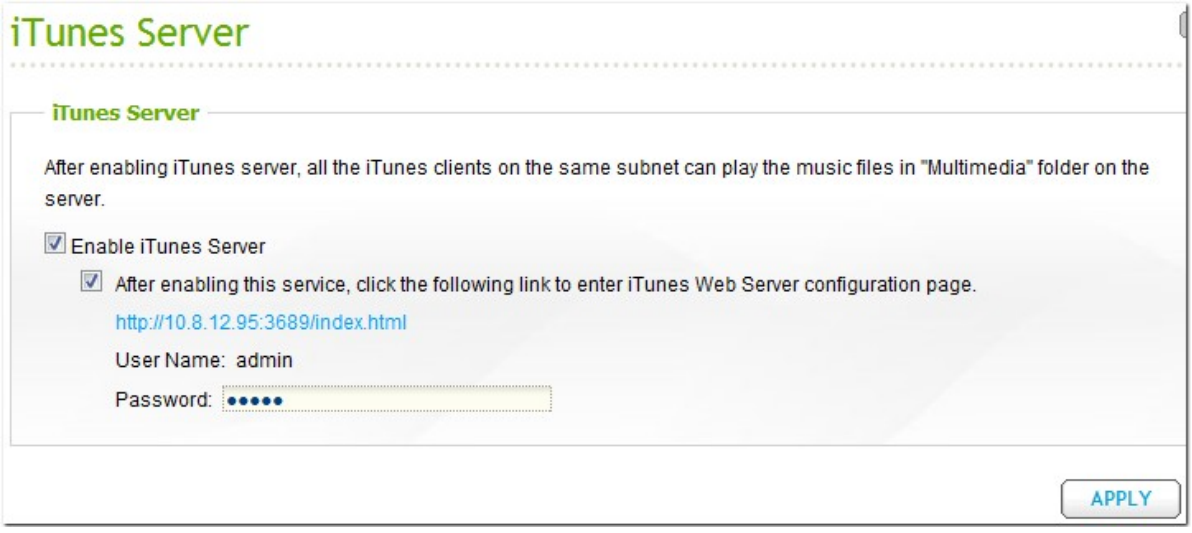


The video recordings will be saved in \\NASIP\Qrecordings or \\NASIP\Recordings. The general recordings are saved in the folder "record_nvr" and the alarm recordings are saved in the folder "record_nvr_alarm".

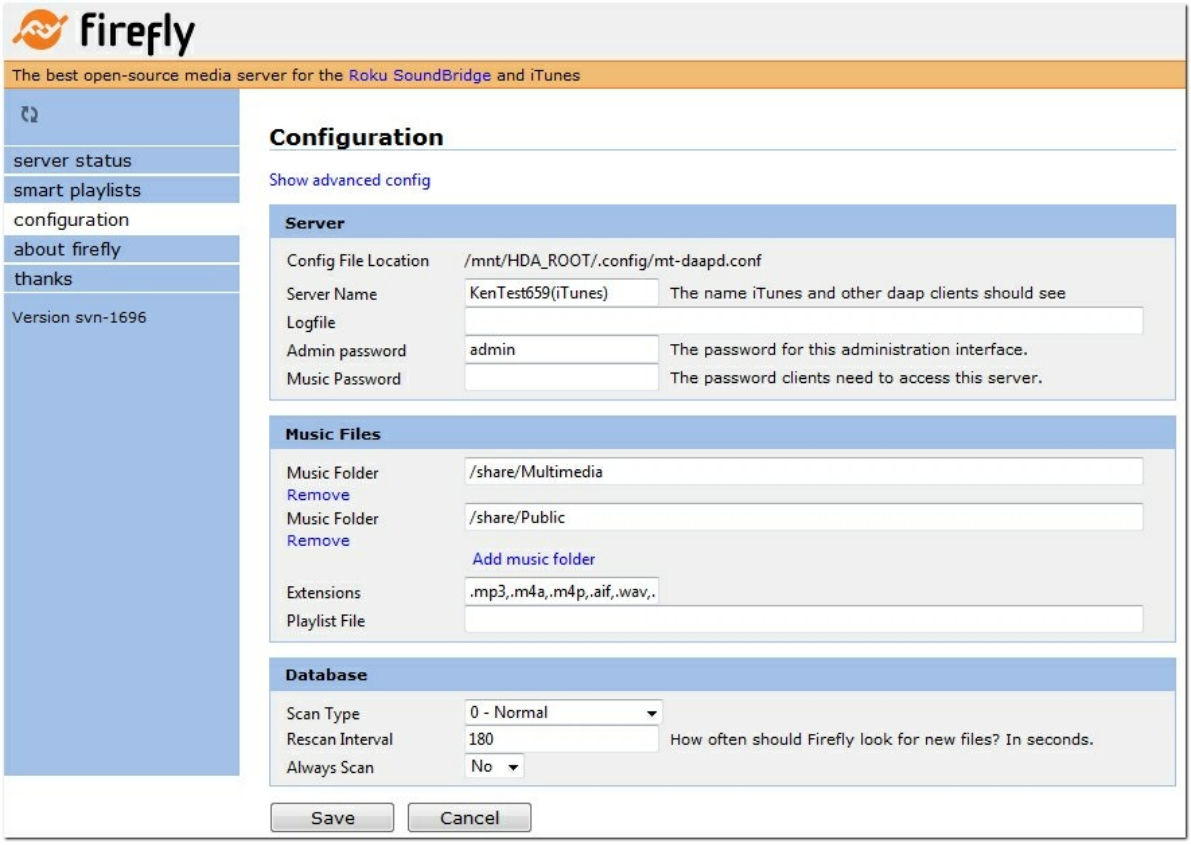
7.7 iTunes Server

The MP3 files on the Qmultimedia/Multimedia folder of the NAS can be shared to iTunes by this service. All the computers with iTunes installed on LAN are able to find, browse, and play the shared music files on the NAS.

To use iTunes server, install iTunes (www.apple.com/itunes/) on your computer. Enable this feature and then upload the music files to the Qmultimedia/Multimedia folder of the NAS.



To configure the iTunes server settings and add smart playlists, login the web page of iTunes server: http://NAS-IP:3689/index.html



Connect the PC and the NAS to the same LAN and run iTunes on the PC. Find the NAS name under "SHARED" and start to play the music files or playlists.

7.8 UPnP Media Server

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

After configuring the settings, you can upload MP3, photos, or video files to the specified folders on the NAS.

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

For the information of setting up the UPnP media server of the NAS for media playing, see here 669.

About UPnP

Universal Plug and Play (UPnP) is a set of computer network protocols promulgated by the UPnP Forum. The purpose of UPnP is to allow the devices to connect seamlessly and to simplify the implementation of the networks at home and in the 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.

7.9 MySQL Server

Note: To use this feature on the 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 from http://www.qnap.com.

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, 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.

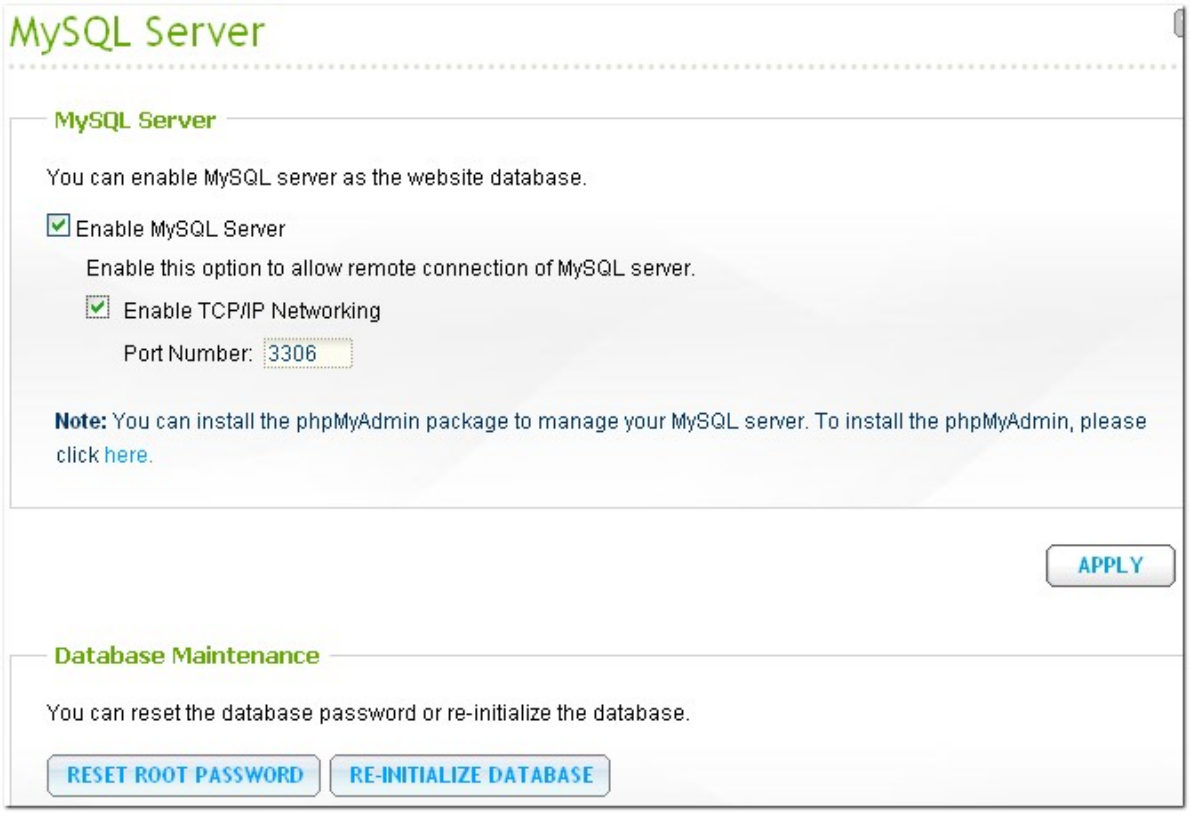
Note:

- Do not delete the phpMyAdmin folder. You can rename this folder but the link on the MySQL server page will not be updated. To connect to 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 information of hosting a phpBB forum on the NAS, see here[678].

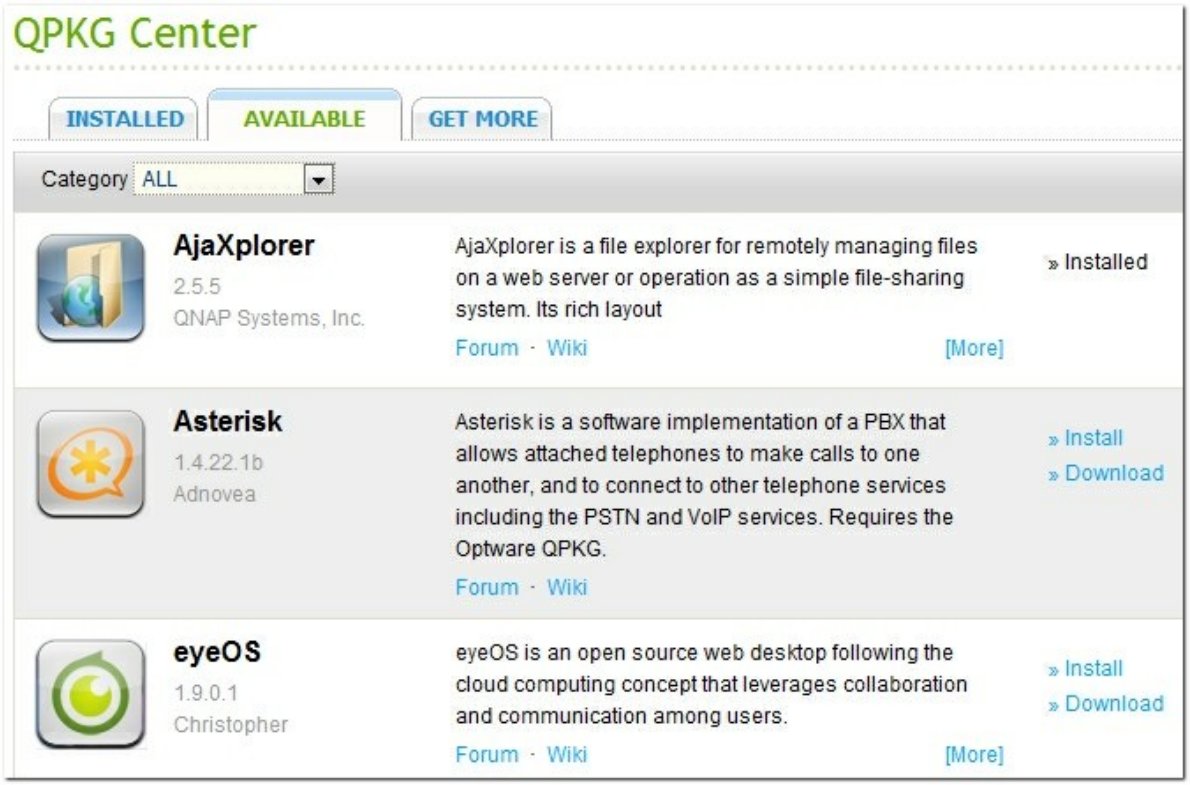


7.10 QPKG Center

The QPKG center is a management platform for installing third party software add-ons on the NAS. Go to "QPKG Center" > "Available" to browse the add-ons. Click "Install" to install them.

Note:

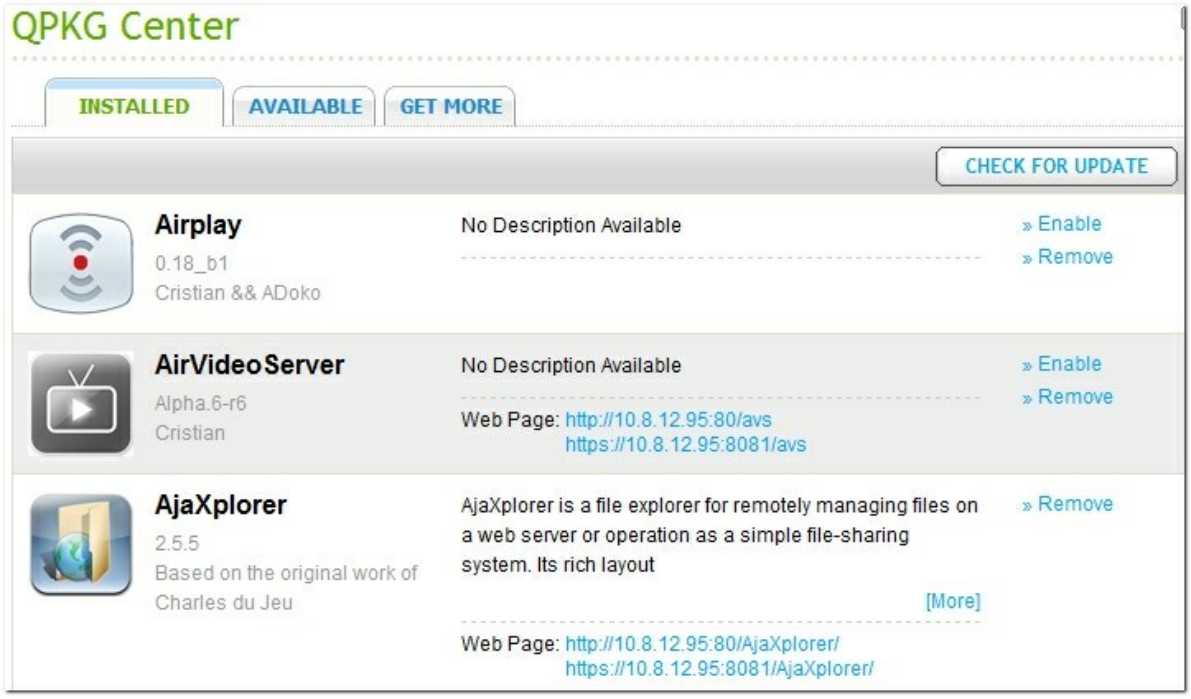
- Make sure the NAS is connected to the Internet.
- QNAP is not responsible for troubleshooting any issues caused by the open source software/add-ons. Users are recommended to participate in the discussion in the QNAP community forum or contact the original creators of the open source software for the solutions.



The selected add-ons and installation progress will be shown.

Note: When installing a QPKG add-on which requires a prerequisite QPKG, the prerequisite add-on will be added to the installation queue automatically prior to the dependent add-on.

Go to the "Installed" tab to view and enable, disable, or remove the installed add-ons. Click "Check for update" to check for the available updated version of the add-ons. Click the download link to install the updates (if any).



Offline Installation

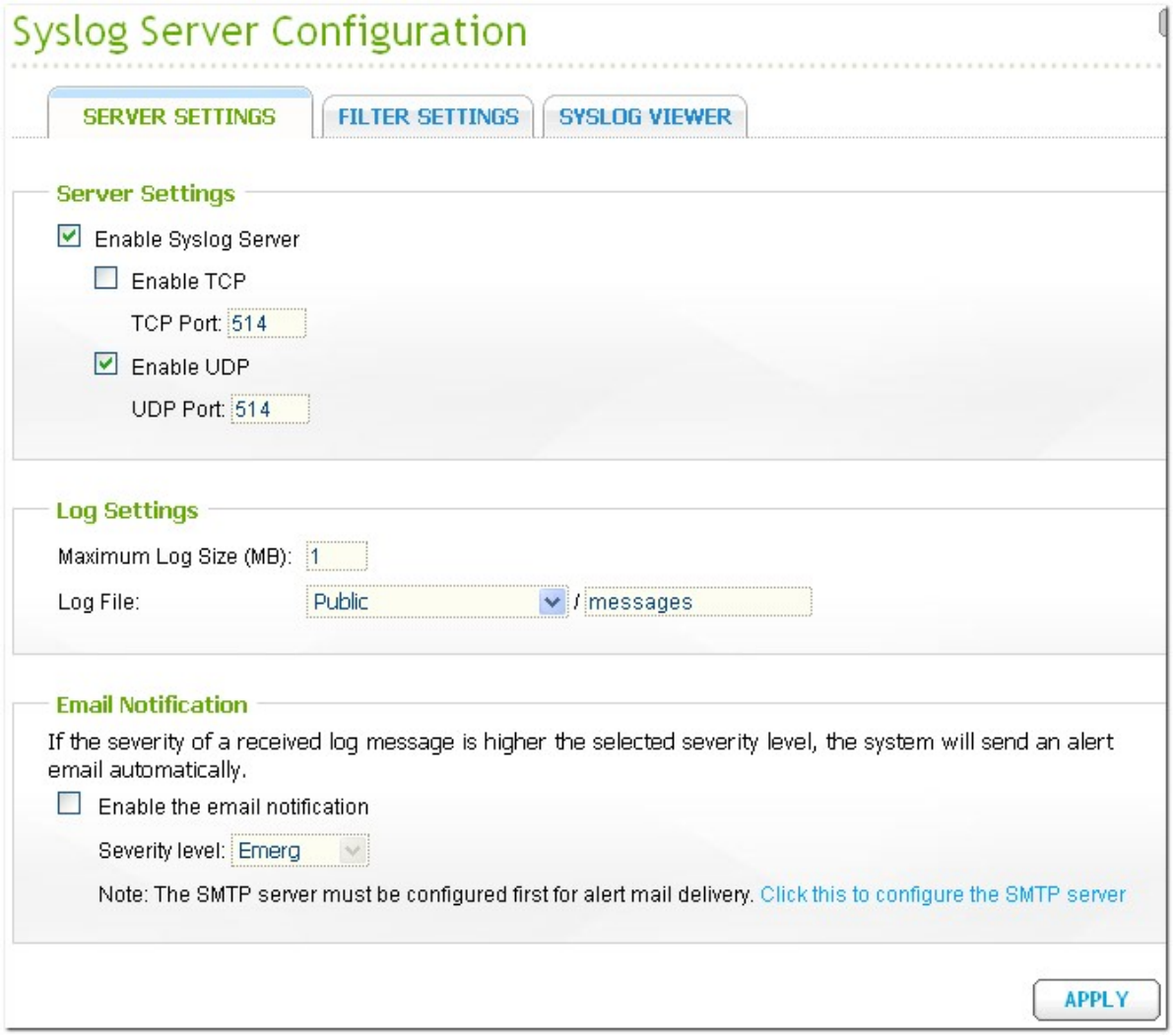
To install QPKG add-ons when the NAS is offline or beta add-ons that are not officially available on QNAP QPKG server, users can download the QPKG files from QNAP website (http://www.qnap.com/QPKG.asp) or forum (http://forum.qnap.com/), unzip the files, and install the add-ons manually in "QPKG Center" > "Get More".

7.11 Syslog Server

Server Settings

To configure the NAS as a Syslog server and allow it to receive syslog messages from the clients, enable Syslog Server. Select the protocols (TCP and/or UDP) the NAS uses to receive syslog messages. Specify the port numbers if necessary or use the default port number 514. Click "Apply" to save the settings. After enabling the NAS as a syslog server, enter the NAS IP as the syslog server IP on the syslog clients to receive the syslog messages from them.

Log Settings:
Specify the maximum log size (1-100 MB) of the syslog messages, the location (NAS network share) to which the logs will be saved, and the file name. Once the logs have reached the maximum size, the log file will be automatically archived and renamed with the archive date as MyLogFile_yyyy_mm_dd, for example MyLogFile_2011_12_31. If multiple log files are archived on the same day, the file will be named as MyLogFile_yyyy_mm_dd.[number]. For example, MyLogFile_2011_12_31.1, MyLogFile_2011_12_31.2, and so on. Click "Apply" to save the settings.



Email Notification:

The NAS supports sending email alert to dedicated email addresses (maximum 2, configured in "System Administration" > "Notification" > "Alert Notification") when the severity of the received syslog messages match the specified level. To use this feature, configure the SMTP server settings in "System Administration" > "Notification" > "Configure SMTP Server". Next, enable email notification and select the severity level in "Application Servers" > "Syslog Server" > "Server Settings". Click "Apply" to save the settings.

Severity	Level (smallest number the highest)	Description
Emerg	0	Emergency: the system is unusable. Alert emails will be sent when syslog messages of levels 0-4 are received.
Alert	1	Alert: immediate action required. Alert emails will be sent when syslog messages of levels 1-4 are received.
Crit	2	Critical: critical conditions. Alert emails will be sent when syslog messages of levels 2-4 are received.
Err	3	Error: error conditions. Alert emails will be sent when syslog messages of levels 3-4 are received.
Warning	4	Warning: warning conditions. Alert emails will be sent when syslog messages of level 4 are received.

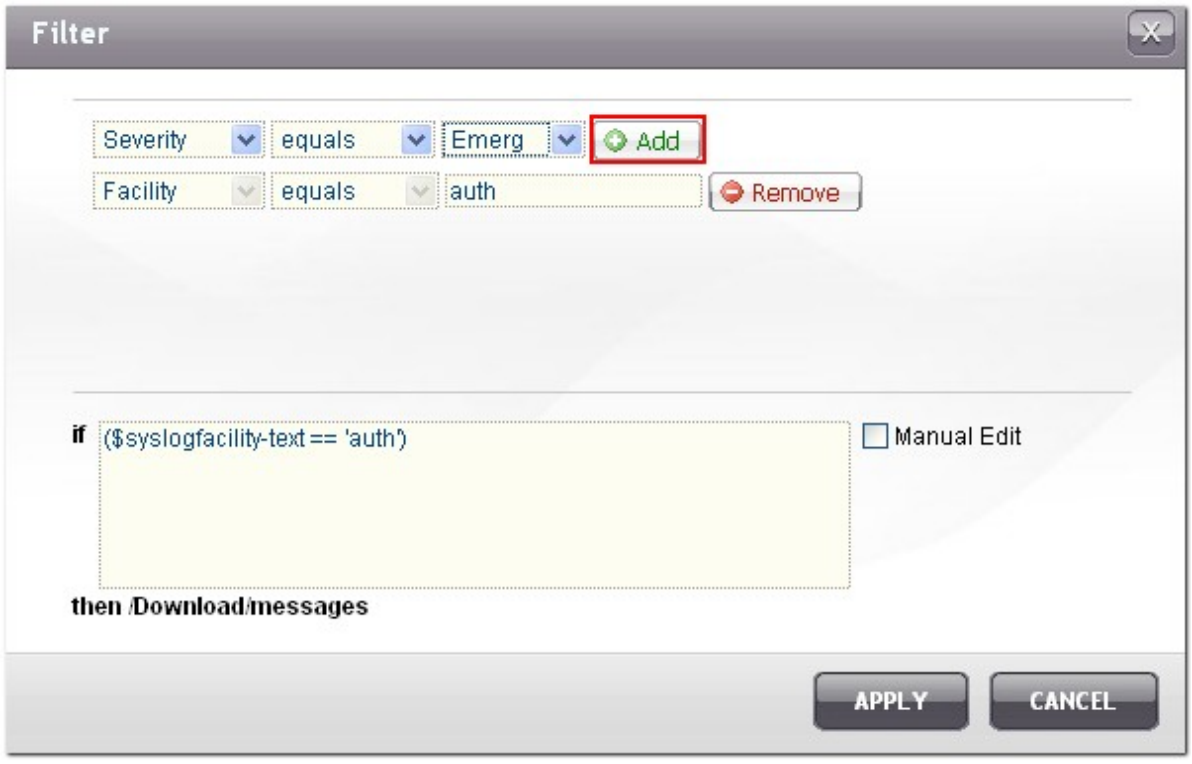
Filter Settings

This feature should only be operated by system administrators who are familiar with syslog filters.

Follow the steps below to create syslog filters for the NAS to receive syslog messages that match the criteria.

1. Click "Add a New Filter".

2. Define the filter settings and click "Add". To edit the filters or add the filters manually, click "Manual Edit" and modify the contents in the dialog. Click "Apply" to save the filter.

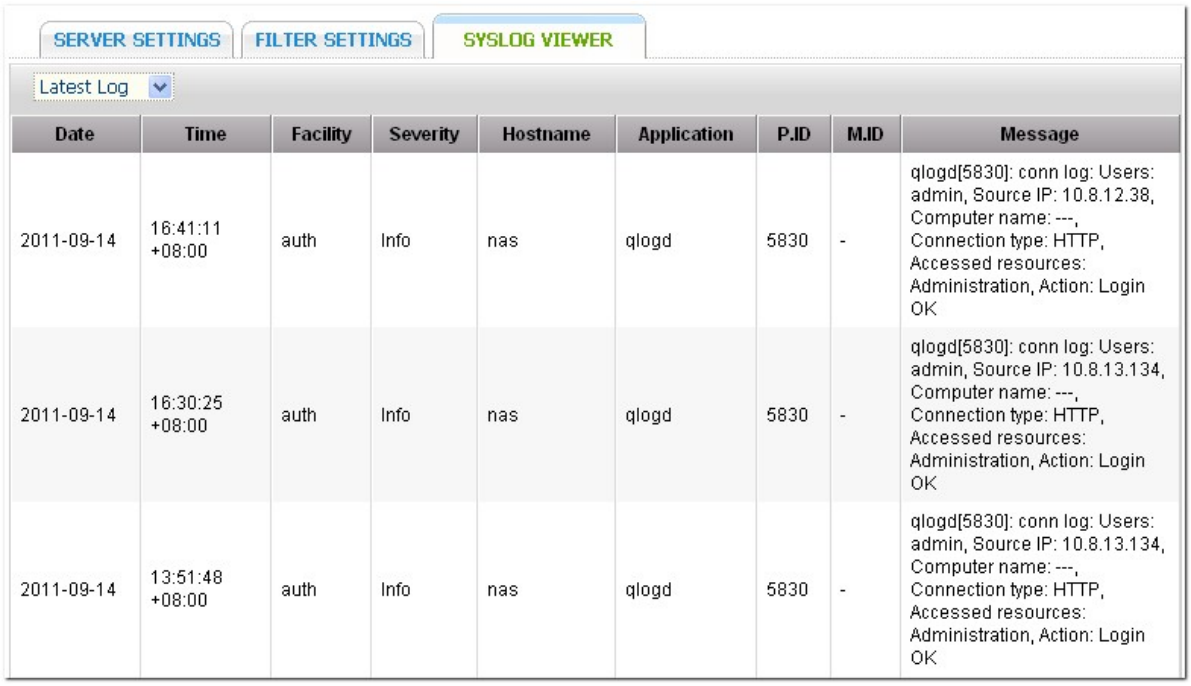


3. The filters will be shown on the list. The NAS will only receive the syslog messages that match the filters which are in use.

Button	Description
	Enable a filter
	Disable a filter
	Edit the filter settings
Delete	Delete one or more filters

Syslog Viewer

Use the web-based syslog viewer to view the available syslog messages on the NAS. Select to view the latest logs or the logs in a particular archived file. The log files can be accessed on the directory configured in “Syslog Server” > “Server Settings” > “Log Settings”.



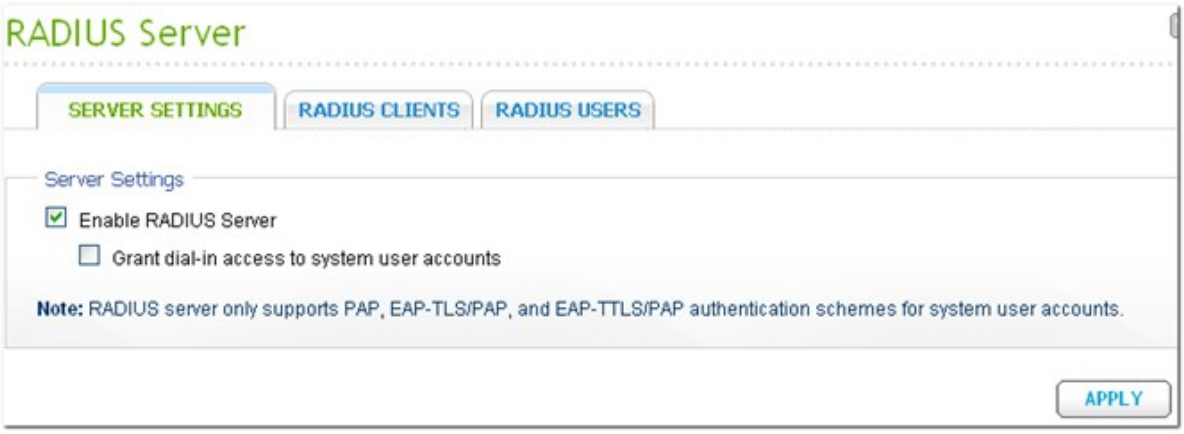
Date	Time	Facility	Severity	Hostname	Application	P.ID	M.ID	Message
2011-09-14	16:41:11 +08:00	auth	Info	nas	qlogd	5830	-	qlogd[5830]: conn log: Users: admin, Source IP: 10.8.12.38, Computer name: ---, Connection type: HTTP, Accessed resources: Administration, Action: Login OK
2011-09-14	16:30:25 +08:00	auth	Info	nas	qlogd	5830	-	qlogd[5830]: conn log: Users: admin, Source IP: 10.8.13.134, Computer name: ---, Connection type: HTTP, Accessed resources: Administration, Action: Login OK
2011-09-14	13:51:48 +08:00	auth	Info	nas	qlogd	5830	-	qlogd[5830]: conn log: Users: admin, Source IP: 10.8.13.134, Computer name: ---, Connection type: HTTP, Accessed resources: Administration, Action: Login OK

7.12 RADIUS Server

The NAS can be configured as a RADIUS (Remote Authentication Dial In User Service) server to provide centralized authentication, authorization, accounting management for computers to connect and use a network service.

To use this feature, follow the steps below:

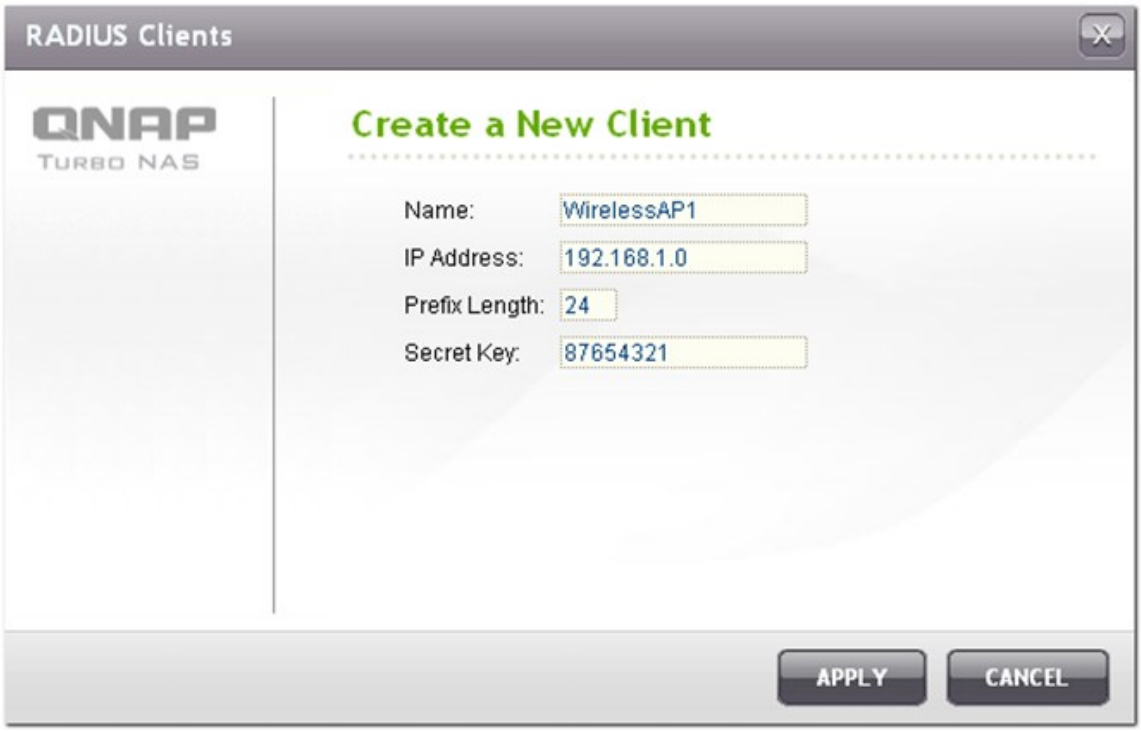
1. Enable RADIUS Server on the NAS in "RADIUS Server" > "Server Settings". Click "Apply".



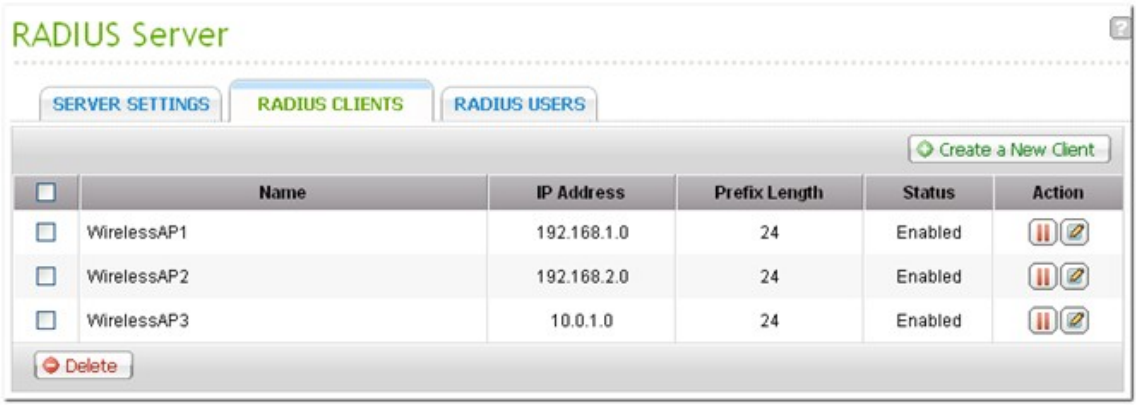
2. Add RADIUS clients, such as Wi-Fi access points and VPN, on the NAS in "RADIUS Server" > "RADIUS Clients". Up to 10 RADIUS clients are supported.

   a. Click "Create a New Client".

b. Enter the client information and click “Apply”.

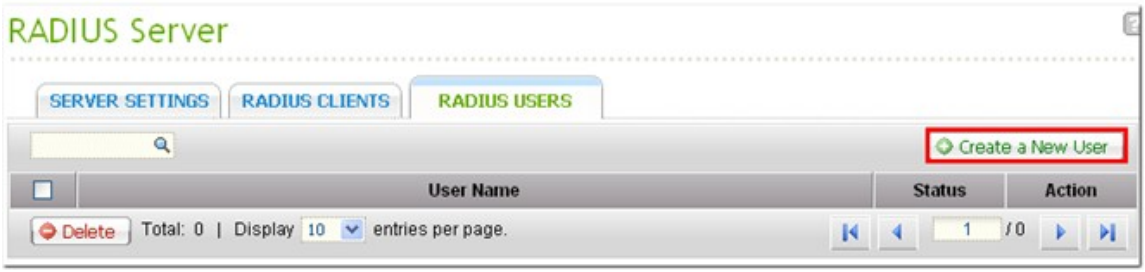


c. The clients are shown on the list.

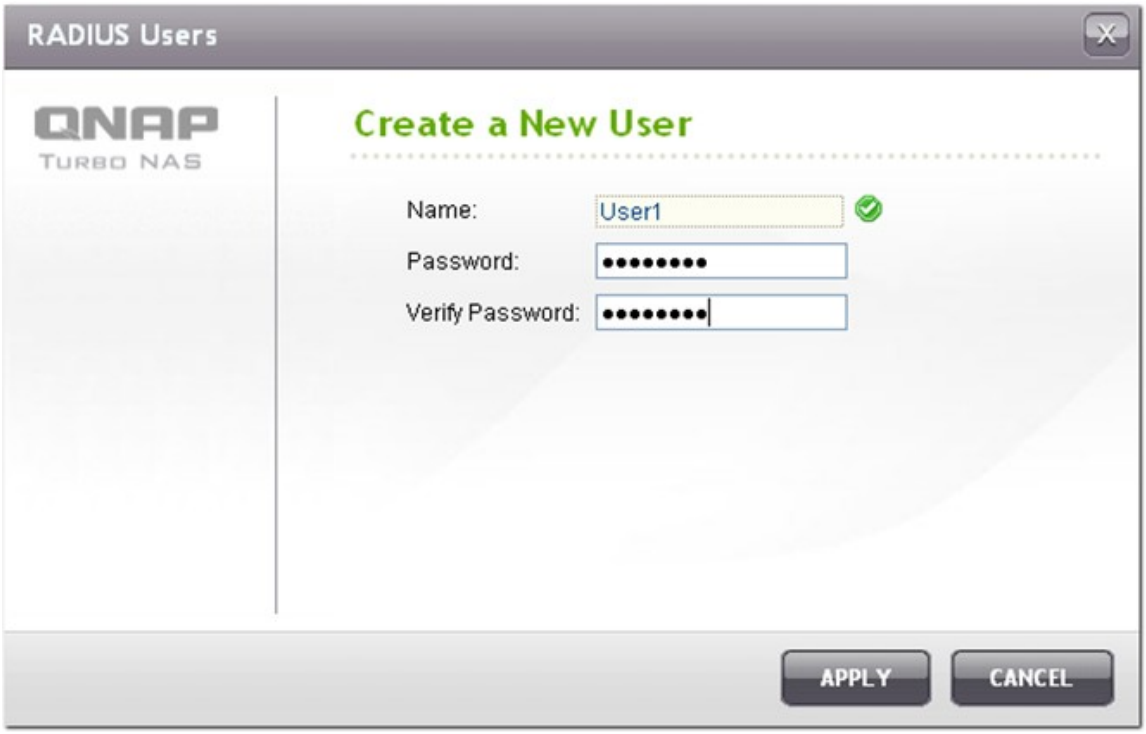


3. Create RADIUS users and their password in "RADIUS Server" > "RADIUS Users". The users will be authenticated when trying to access the network through the RADIUS clients. The maximum number of RADIUS users the NAS supports is the same as the maximum number of local NAS users supported. See http://docs.qnap.com/nas/en/index.html?users.htm for details.

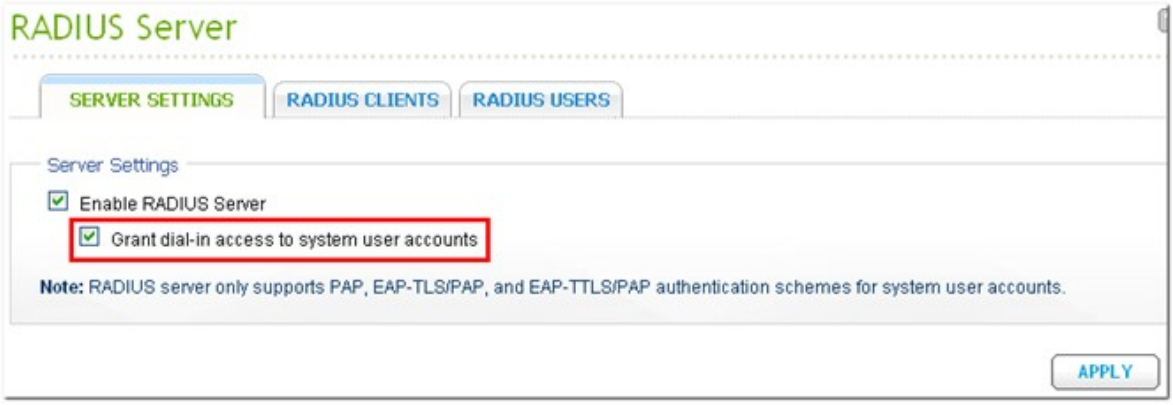
   a. Click "Create a New User".



   b. Enter the user name and password. The user name supports alphabets (a-z and A-Z) and numbers (0-9) only. The password must be 8-32 characters (a-z, A-Z, and 0-9 only). Click "Apply".



4. Specify to grant dial-in access to local NAS users. Enable this option to allow the local NAS users to access the network services through the RADIUS clients using their NAS login name and password. Click “Apply”.



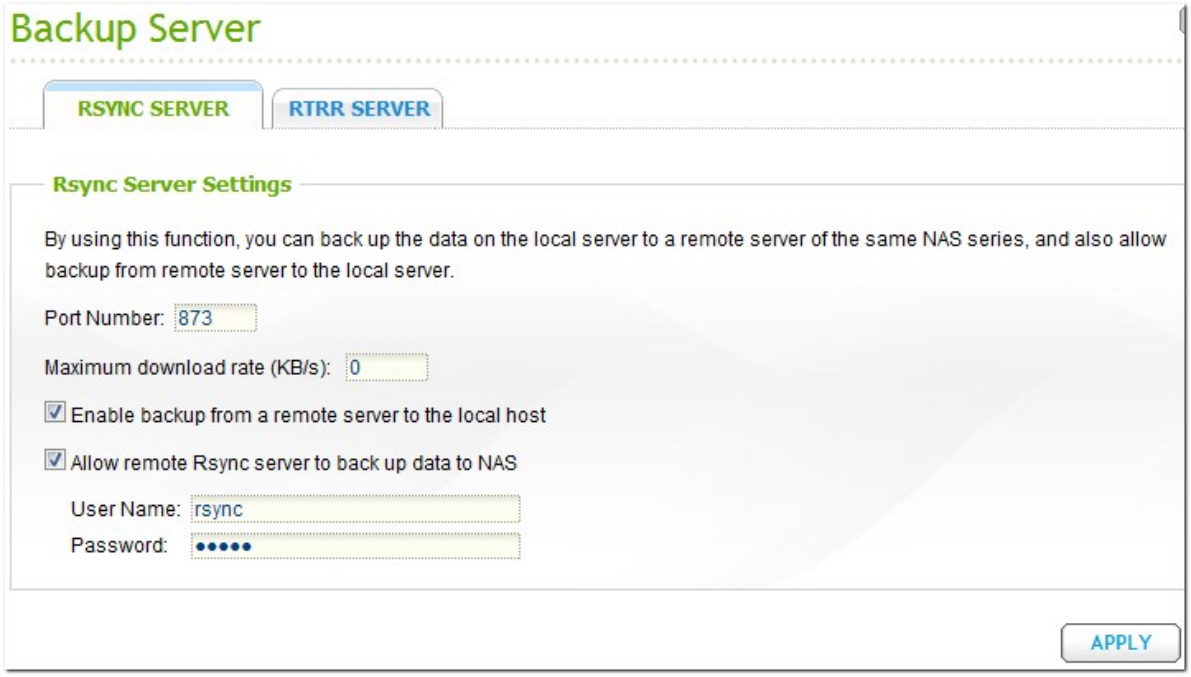
Note: The RADIUS server only supports PAP, EAP-TLS/PAP, and EAP-TTLS/PAP authentication for local NAS user accounts.

7.13 Backup Server

Rsync Server

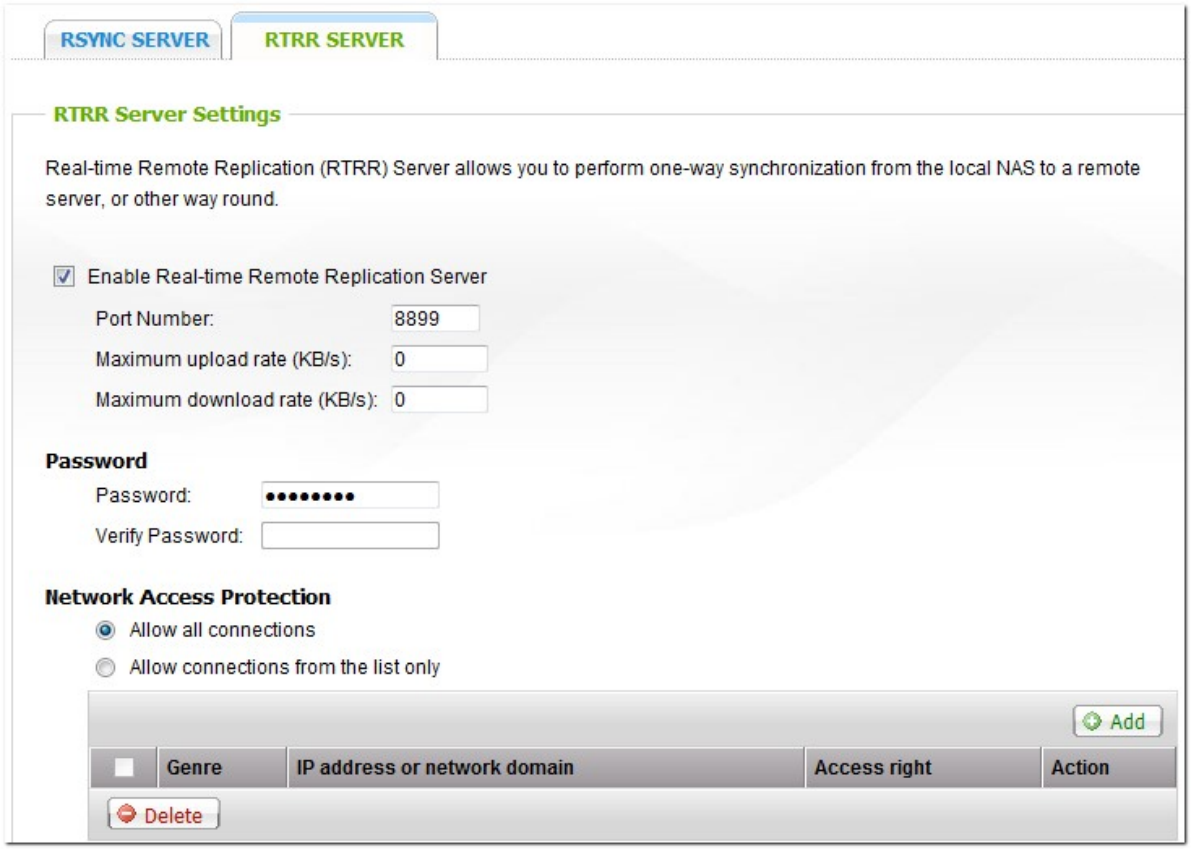
Enable Rsync server to configure the NAS as a backup server for data backup from a remote Rsync server or NAS server. The default port number for remote replication via Rsync is 873. Specify the maximum download rate for bandwidth control. 0 means unlimited.

- Enable backup from a remote server to the local host: Select this option to allow data backup from a remote server (NAS) to the local server (NAS).
- Allow remote Rsync server to back up data to the NAS: Select this option to allow data backup from an Rsync server to the local server (NAS). Enter the user name and password to authenticate the Rsync server which attempts to back up data to the NAS.

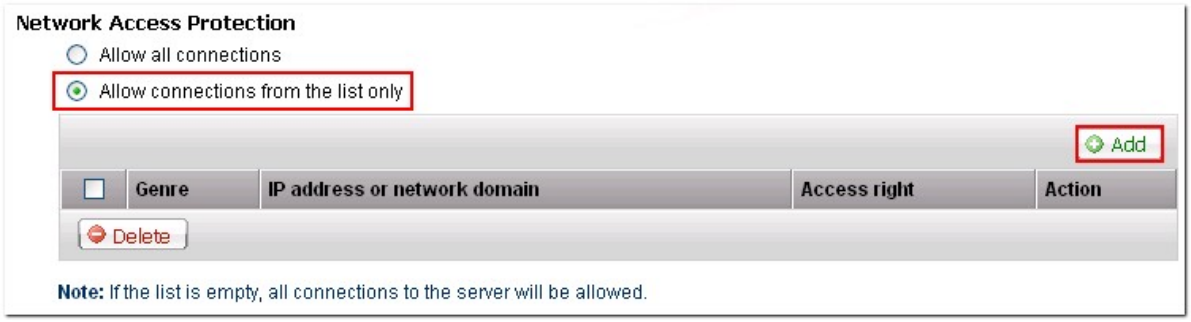


RTRR Server

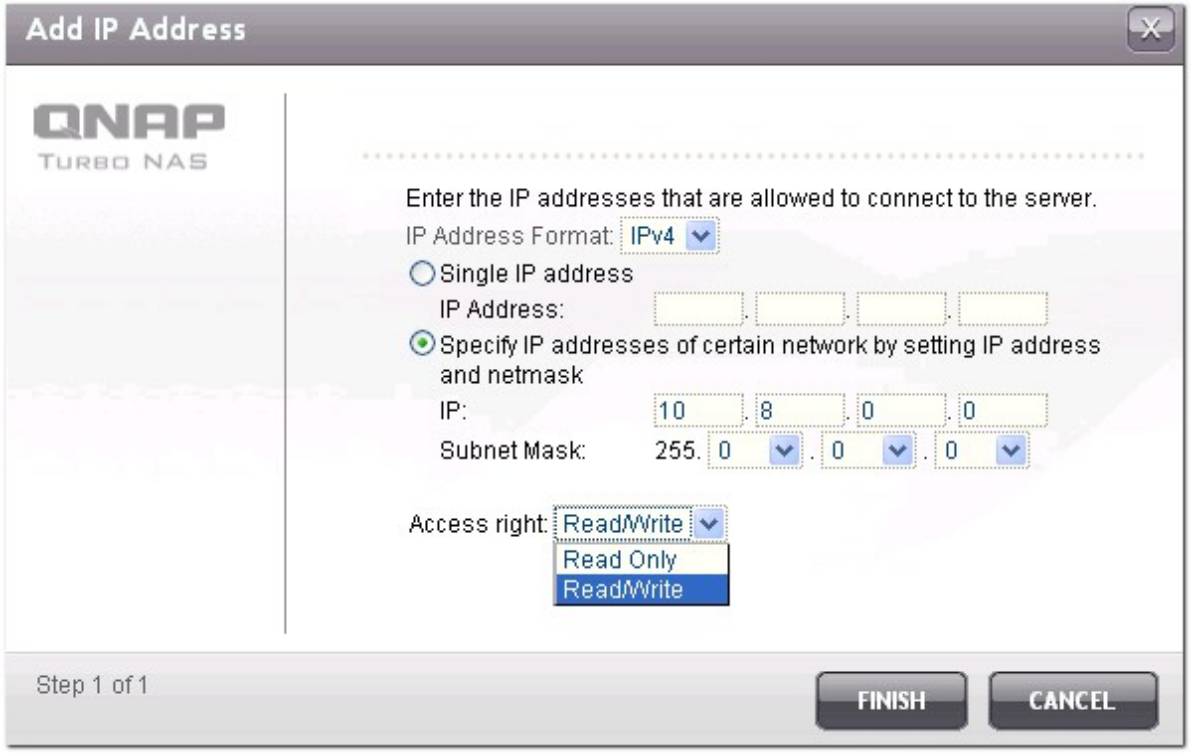
To allow real-time or schedule data replication from a remote server to the local NAS, select "Enable Real-time Remote Replication Server". You can specify the port number for remote replication. The default port number is 8899. Specify the maximum upload and download rate for bandwidth control. 0 means unlimited. To allow only authenticated access to back up data to the local NAS, specify the access password. The client server will be prompted to enter the password to back up data to the NAS via RTRR.



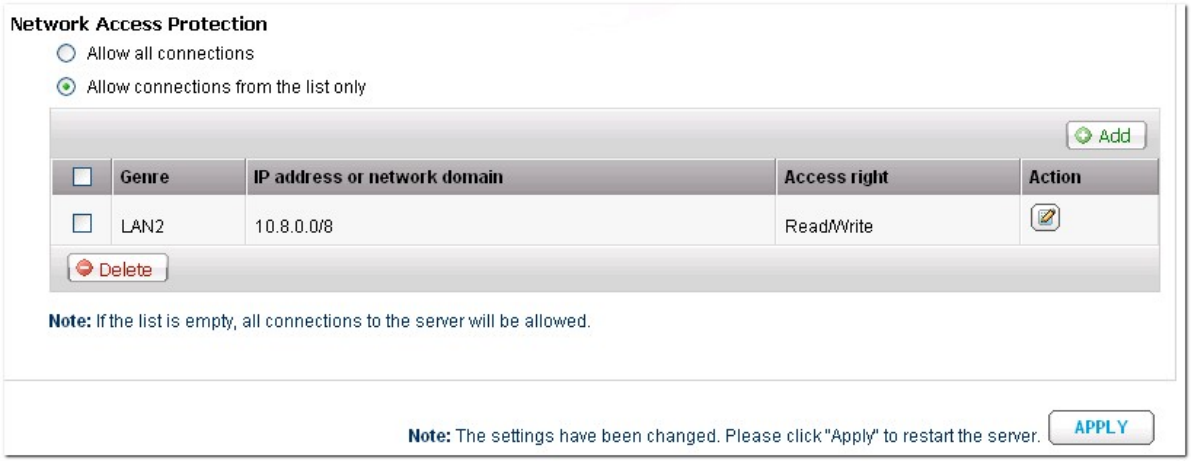
You can specify the IP addresses or host names which are allowed to access the NAS for remote replication. **Up to 10 rules can be configured.** To allow all connections, select "Allow all connections". To specify the IP addresses or host names, select "Allow connections from the list only" and click "Add".



Enter an IP address or specify a range of IP addresses by entering the IP and subnet mask. Select the access right "Read Only" or "Read/Write". By selecting "Read/Write", the client server is allowed to delete the files on the local NAS. Click "Finish" to exit.



After saving the access rule, click “Apply” and the NAS will restart to apply the settings.



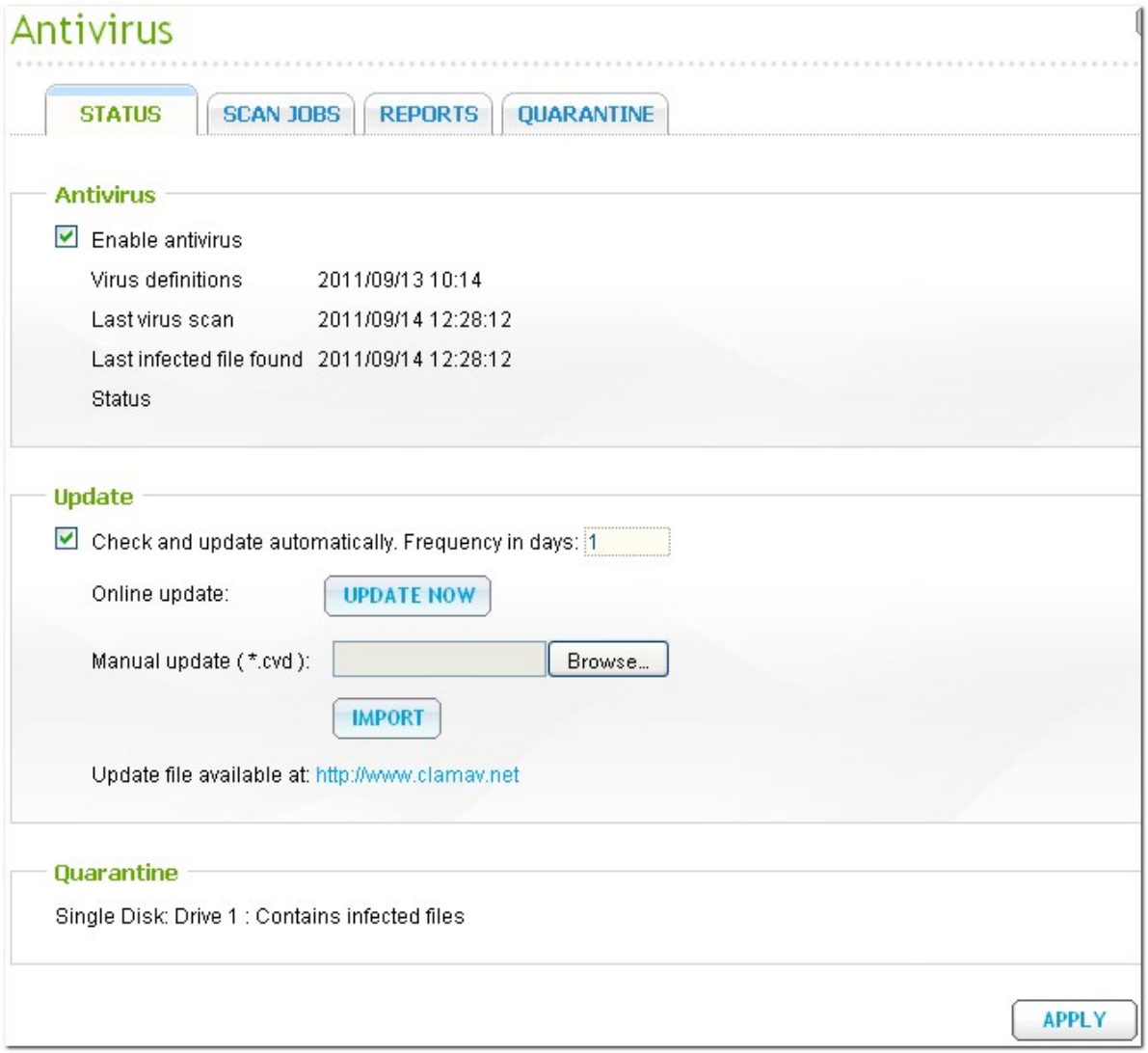
7.14 Antivirus

Status

Use the antivirus feature to scan the NAS manually or on recurring schedule and delete, quarantine, or report files infected by viruses, malware, Trojans, and other malicious threats. To use this feature, select "Enable antivirus" and click "Apply".

Update:
Select "Check and update automatically" and specify the interval in days to update the antivirus definitions automatically. Click "Update Now" next to online update to update the antivirus definitions immediately. Users can also download the update files from http://www.clamav.net and update the antivirus definitions manually.
The NAS must be connected to the Internet to use this feature.

Quarantine:
View the quarantine information of the disk volumes on the NAS. For the details, go to "Application Servers" > "Antivirus" > "Quarantine".


Antivirus
STATUS
SCAN JOBS
REPORTS
QUARANTINE
Antivirus
Enable antivirus
Virus definitions 2011/09/13 10:14
Last virus scan 2011/09/14 12:28:12
Last infected file found 2011/09/14 12:28:12
Status
Update
Check and update automatically. Frequency in days: 1
Online update:
UPDATE NOW
Manual update (*.cvd):
Browse...
IMPORT
Update file available at: http://www.clamav.net
Quarantine
Single Disk: Drive 1 : Contains infected files
APPLY

Scan Jobs

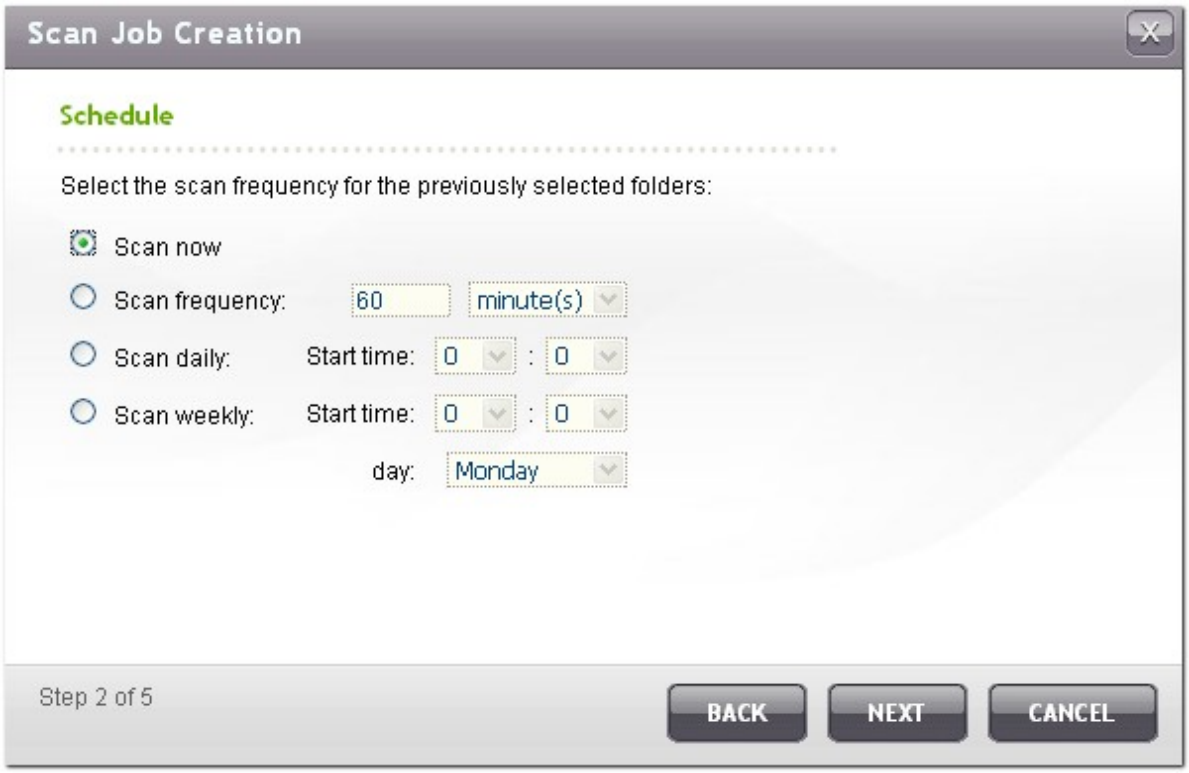
The NAS supports manual and scheduled scanning of all or specific network shares. Up to 64 schedules can be created and maximum 5 scan jobs can run concurrently. To create a scan job, follow the steps below.

1. Go to "Application Servers" > "Antivirus" > "Scan Jobs". Click "New Scan Job".

2. Enter the job name and select the network shares to scan. To scan a specific network share, select the share and click "Add".

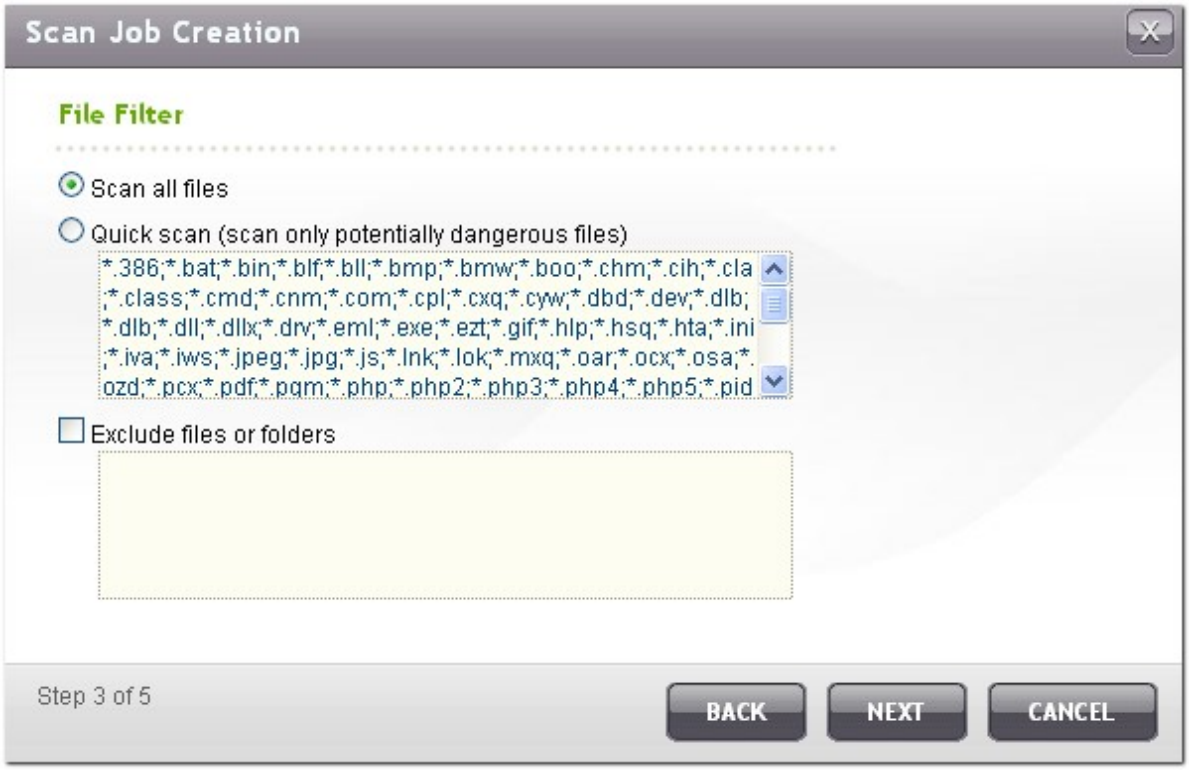
3. Multiple network shares can be selected. To remove a network share, click next to the share name. Click "Next".

4. Define the schedule for the scan job. Click "Next".



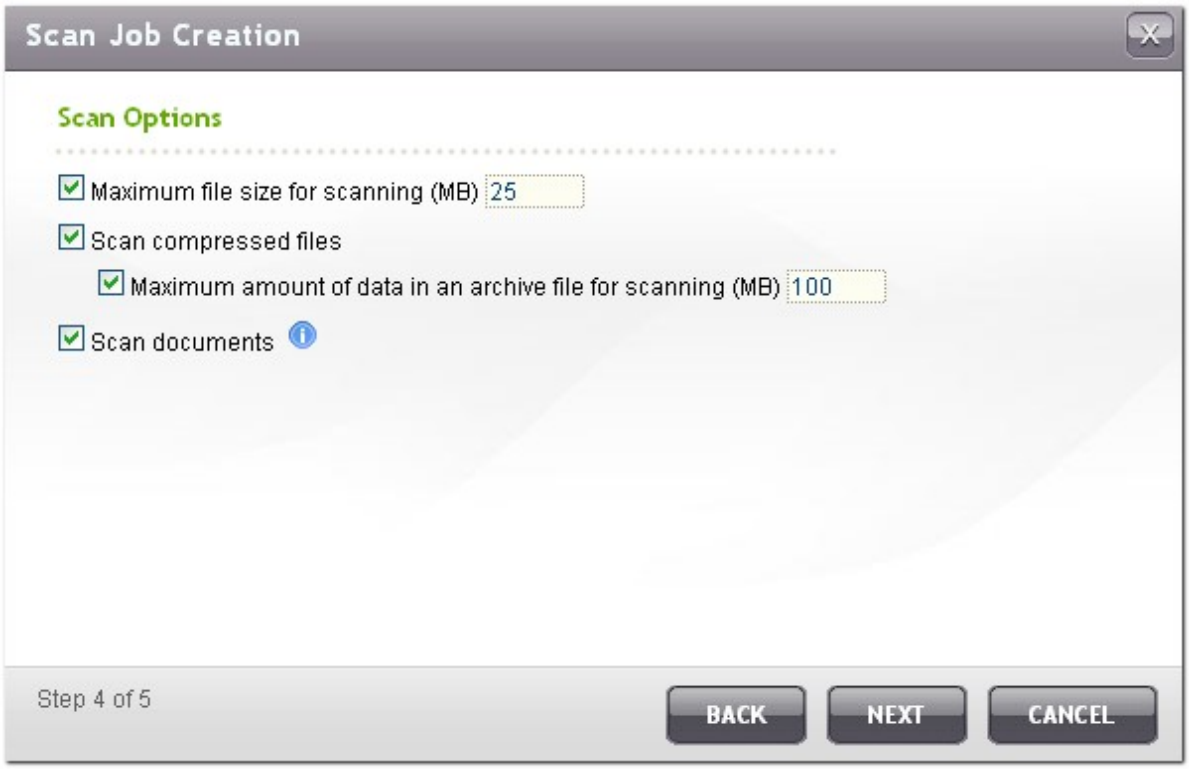
5. Select to scan all the files in the network share(s) or quick scan to scan only potentially dangerous files. Select "Exclude files or folders" and specify a file, a folder, or a file extension to be excluded from the virus scan. Separate each entry by a space in the same line or enter one entry per line. For example:

/Public/testfile.txt
/Download
*.log
*.exe *.com
*.txt
Click "Next".



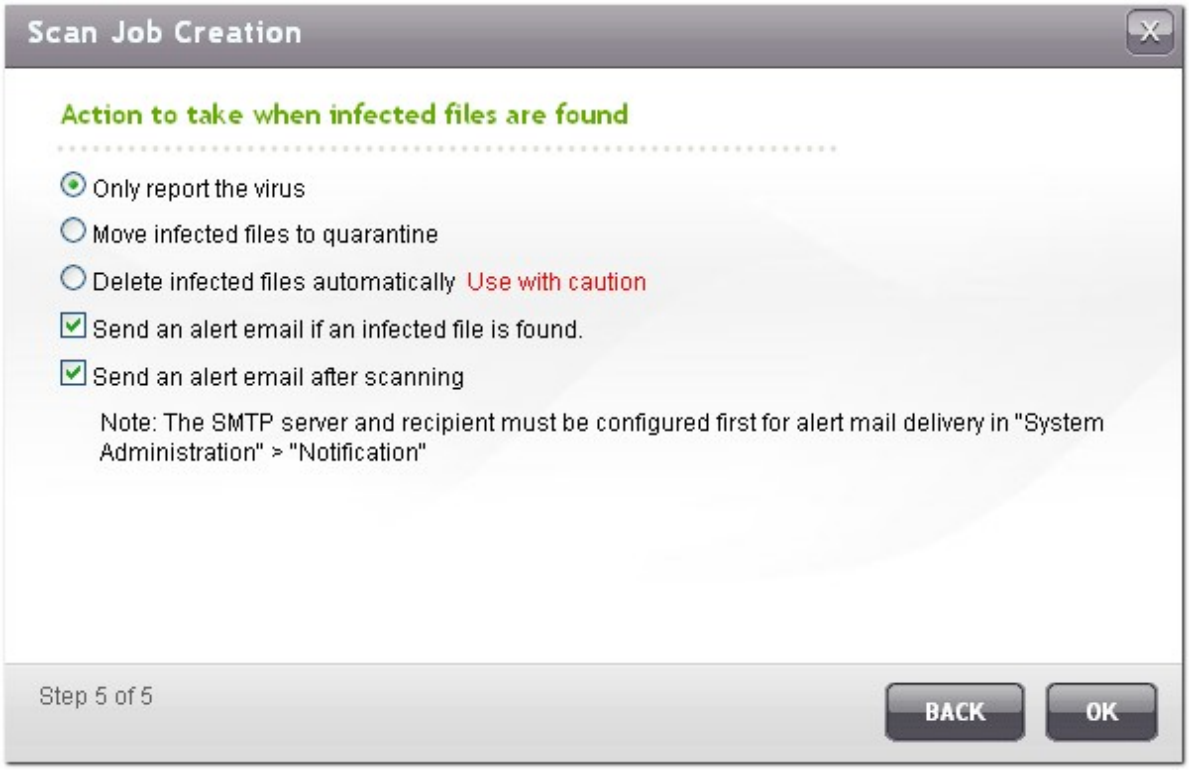
6. Enable other scan options:
    - Specify the maximum file size (1-4096 MB) allowed for scanning.
    - To scan compressed files in the network share(s), enable "Scan compressed files". Specify the maximum amount of data (1-4096 MB) in an archive file for scanning if applicable.
    - To scan MS Office and Mac Office files, RTF, PDF, and HTML files, select "Scan documents".

Click "Next".



7. Specify the actions to take when infected files are found.
    - Only report the virus: The virus scan reports are recorded under the “Reports” tab. No actions will be done to the infected files.
    - Move infected files to quarantine: The infected files will be quarantined and cannot be accessed from the original network shares. Users can view the virus scan reports under the “Reports” tab and delete/restore the infected files under the “Quarantine” tab.
    - Delete infected files automatically: The infected files will be deleted and cannot be recovered.

To receive an alert email when an infected file is found or after scanning has completed, configure the SMTP server settings in “System Administration” > “Notification” > “Configure SMTP Server”. Click “OK” to create the scan job.



8. The scan job will run according to the specified schedule.

Button	Description
	Run the scan job now.
	Stop the scan job.
	Edit the scan job settings.
	Download the last virus scan summary. The file can be opened by a text editor, such as WordPad.
	Delete the scan job.

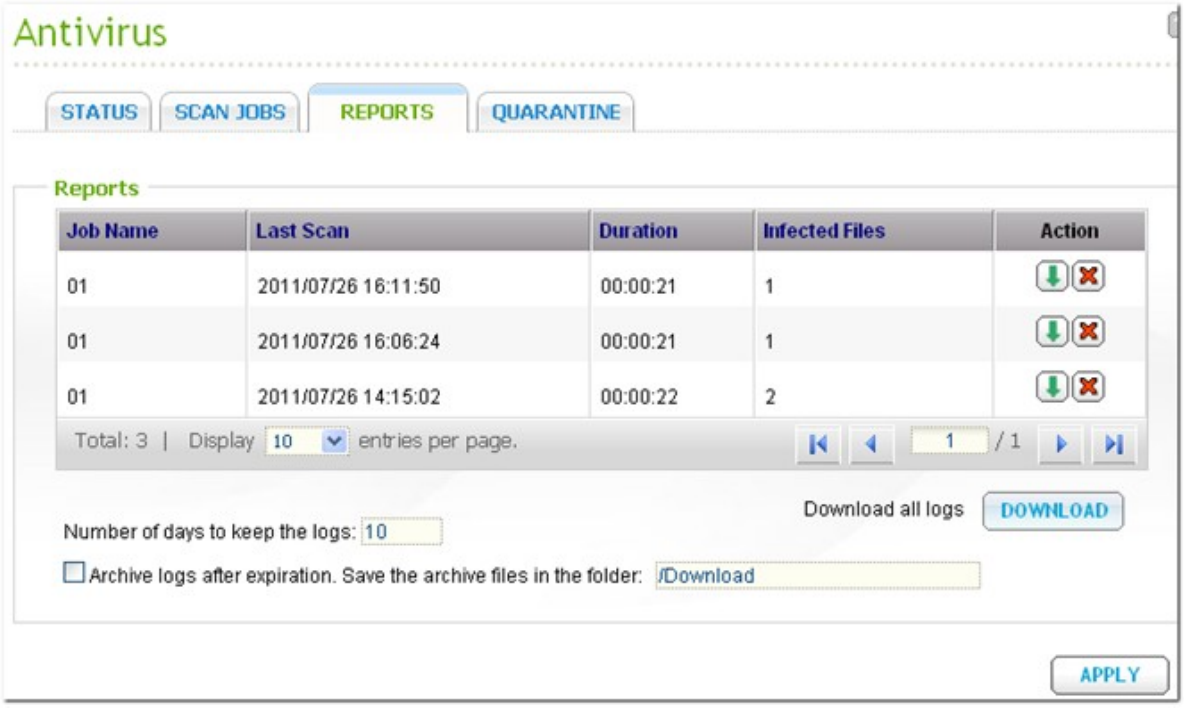
Reports

View or download the reports of the latest scan jobs on the NAS.

Button	Description
	Download the virus scan report. The file can be opened by a text editor, such as WordPad.
	Delete an entry on the list.
DOWNLOAD	Download all the virus scan logs on the list as a zip file.

Report options

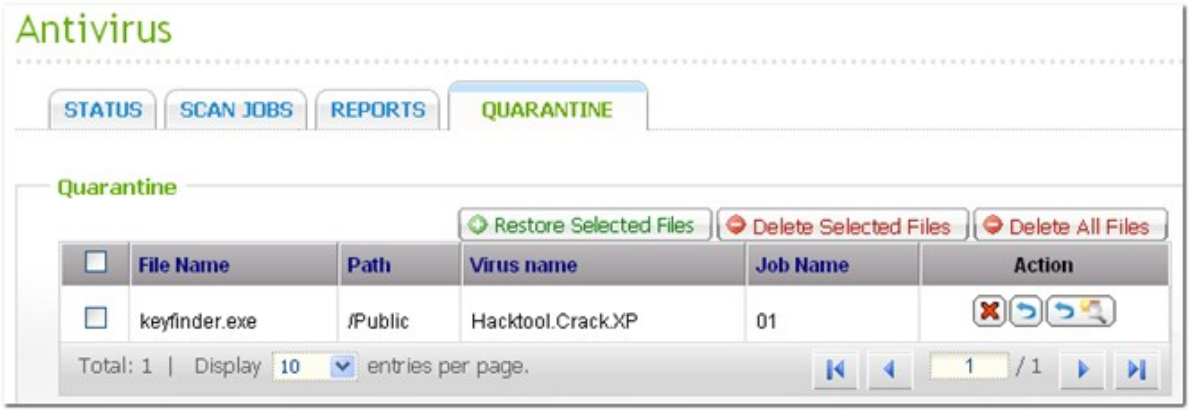
- Specify the number of days (1-999) to keep the logs
- Enable the option "Archive logs after expiration" and specify the network share to save the logs once the number of days to keep the logs has been reached. Click "Apply" to save the changes.



Quarantine

This page shows the quarantined files on the NAS. Users can manually delete or restore the quarantined files, or restore and add the files to the exclude list.

Button	Description
	Delete an infected file. The file cannot be recovered.
	Restore an infected file to its original network share.
	Restore an infected file and add the file into the exclude list (scan filter).
Restore Selected Files	Restore multiple files on the list.
Delete Selected Files	Delete multiple files on the list. The files cannot be recovered.
Delete All Files	Delete all the files on the list. The files cannot be recovered.

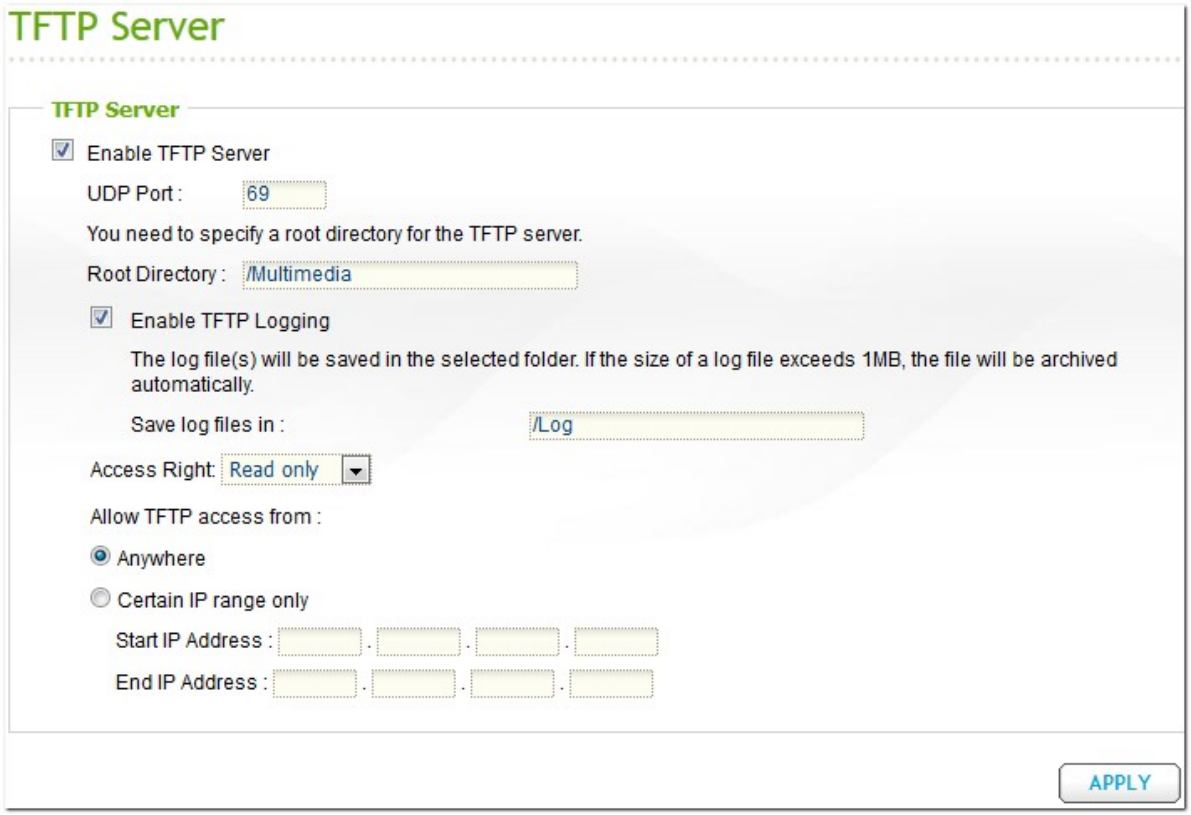


7.15 TFTP Server

Configure the NAS as a TFTP (Trivial File Transfer Protocol) server for configuration management of network devices and remote network booting of computers for system imaging or recovery. TFTP is a file transfer protocol with the functionality of a very basic form of FTP. TFTP does not provide user authentication and cannot be connected by a standard FTP client.

Follow the steps below to use this feature:

1. Select "Enable TFTP Server".
2. The default UDP port for file transfer is 69. Change the port number only when necessary.
3. Specify a folder on the NAS as the root directory of the TFTP server.
4. Enable TFTP Logging: Enable this option and specify the directory to save the TFTP log file (opentftpd.log). It is recommended to view the log file by Microsoft Excel or WordPad on Windows OS or by TextEdit on Mac OS.
5. Assign read only or full access to the clients.
6. Restrict the TFTP client access by specifying the IP address range or select "Anywhere" to allow any TFTP client access.
7. Click "Apply".



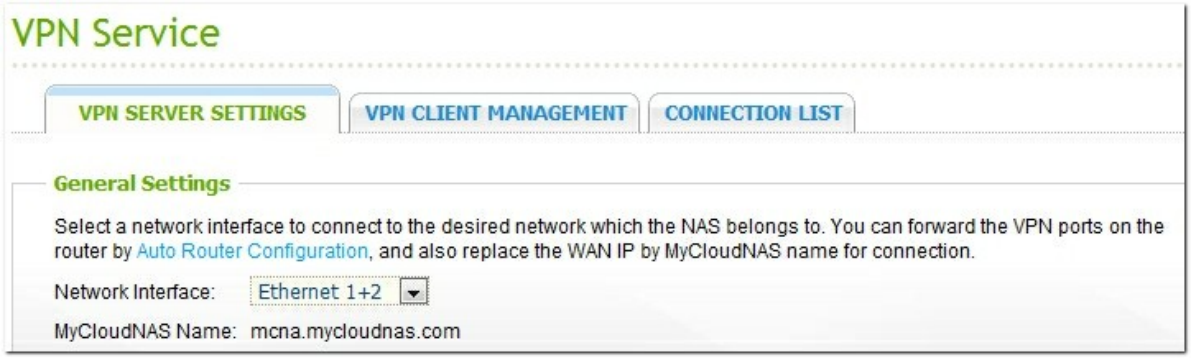
7.16 VPN Service

The NAS supports Virtual Private Network (VPN) service for users to access the NAS and resources on a private network from the Internet. Follow the instructions below for the first time setup of the VPN service on the NAS.

1. Select a network interface to connect
2. Enable PPTP or OpenVPN service
3. Configure port forwarding by auto router configuration
4. Register MyCloudNAS service
5. Add VPN users
6. Connect to the private network by a VPN client

1. Select a network interface to connect

Login the NAS as "admin" and go to "Application Servers" > "VPN Service" > "VPN Server Settings". Under "General Settings", select a network interface to connect to the desired network which the NAS belongs to.



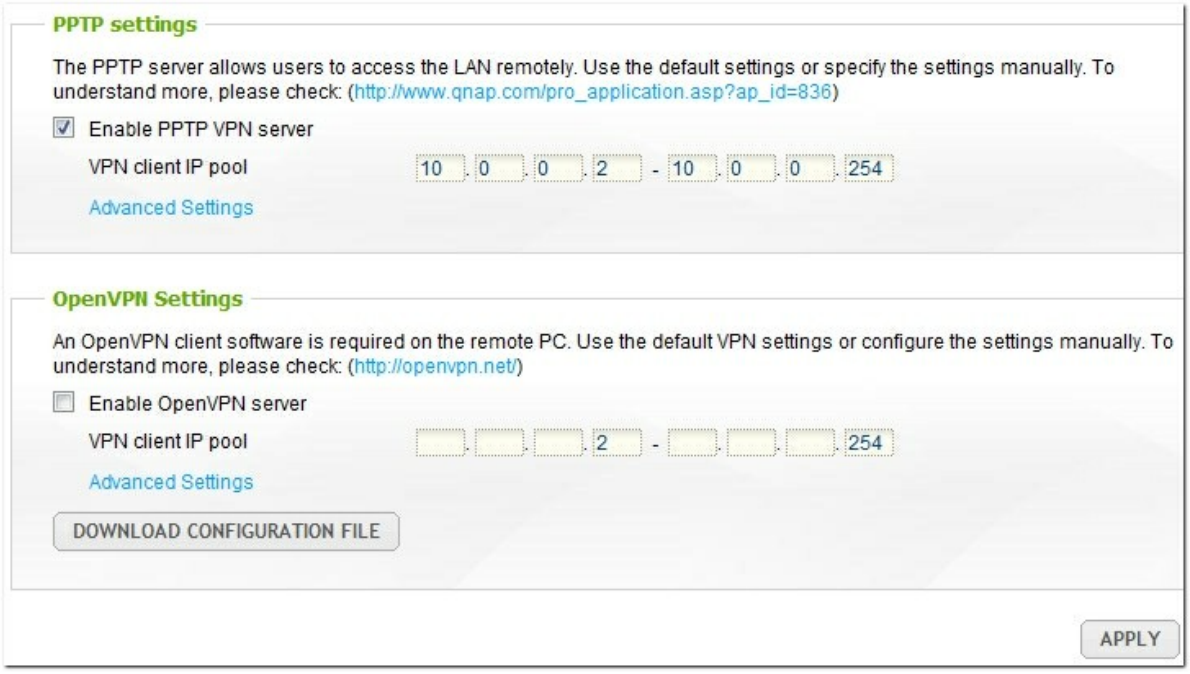
2. Enable PPTP or OpenVPN service

The NAS supports PPTP and OpenVPN for VPN connection. Select either one option and configure the settings.

PPTP: Point-to-Point Tunneling Protocol (PPTP) is one of the most commonly used methods for VPN connection. It is natively supported by Windows, Mac, Linux, Android, and iPhone.

OpenVPN: OpenVPN is an open source VPN solution which utilizes SSL encryption for secure connection. To connect to the OpenVPN server, OpenVPN client must be installed on your PC. Click "Download Configuration File" to download the VPN client settings, certificate/key and installation guide from the NAS and upload the files to the OpenVPN client.

Note: Upload the configuration file to the OpenVPN client every time the OpenVPN settings, MyCloudNAS name, or the secure certificate is changed.



3. Configure port forwarding by auto router configuration

The NAS supports auto port forwarding for UPnP (Universal Plug-and-Play network protocol) routers. Go to "MyCloudNAS Service" > "Auto Router Configuration" to enable UPnP port forwarding and open the ports of the PPTP or OpenVPN service on the router.

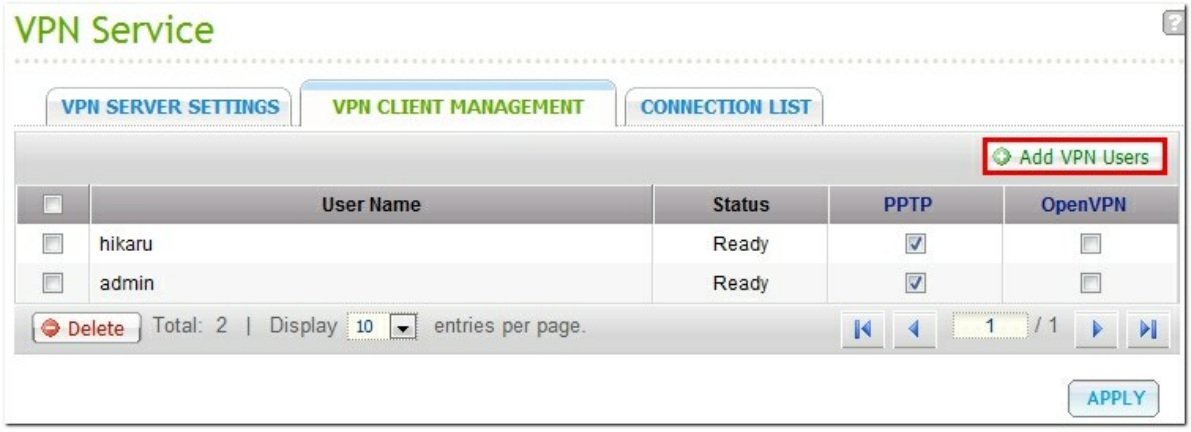
Note: To connect to the PPTP server on the Internet, the PPTP passthrough options on some routers have to be opened. PPTP uses only port TCP-1723; forward this port manually if your router doe not support UPnP.

4. Register MyCloudNAS service

You can connect to the NAS by WAN IP or MyCloudNAS name. To enable MyCloudNAS service, go to "MyCloudNAS Service" > "Configure MyCloudNAS". For more information, see http://www.qnap.com/pro_application.asp?ap_id=637

5. Add VPN users

Go to "Application Servers" > "VPN Service" > "VPN Client Management", click "Add VPN Users". The local NAS users will be listed. Select the users who are allowed to use the VPN service and their connection method (PPTP, OpenVPN, or both). Click "Add".



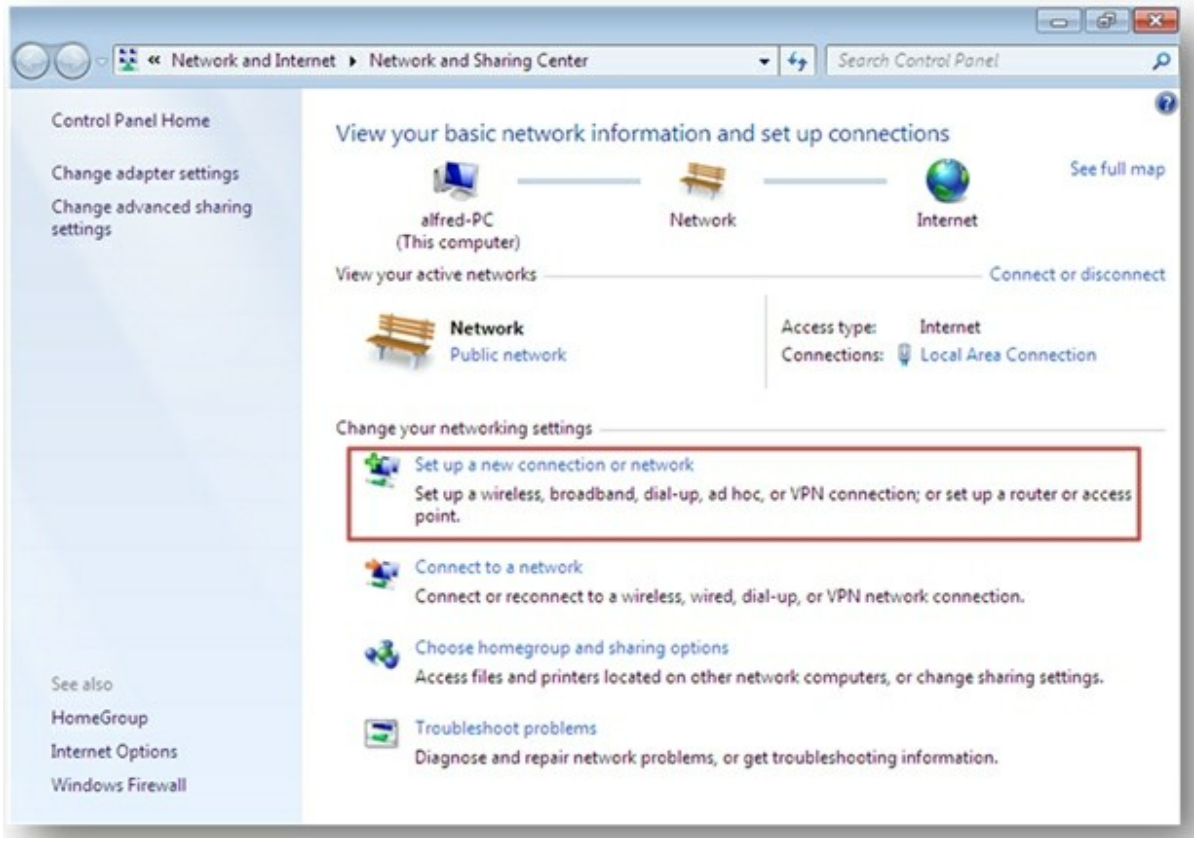
Select users and their privileges
Create a User
Total: 3
1 / 1
User Name
PPTP
OpenVPN
bbb
jason
rr
Step 1 / 1
ADD
CANCEL

6. Connect to the private network by a VPN client

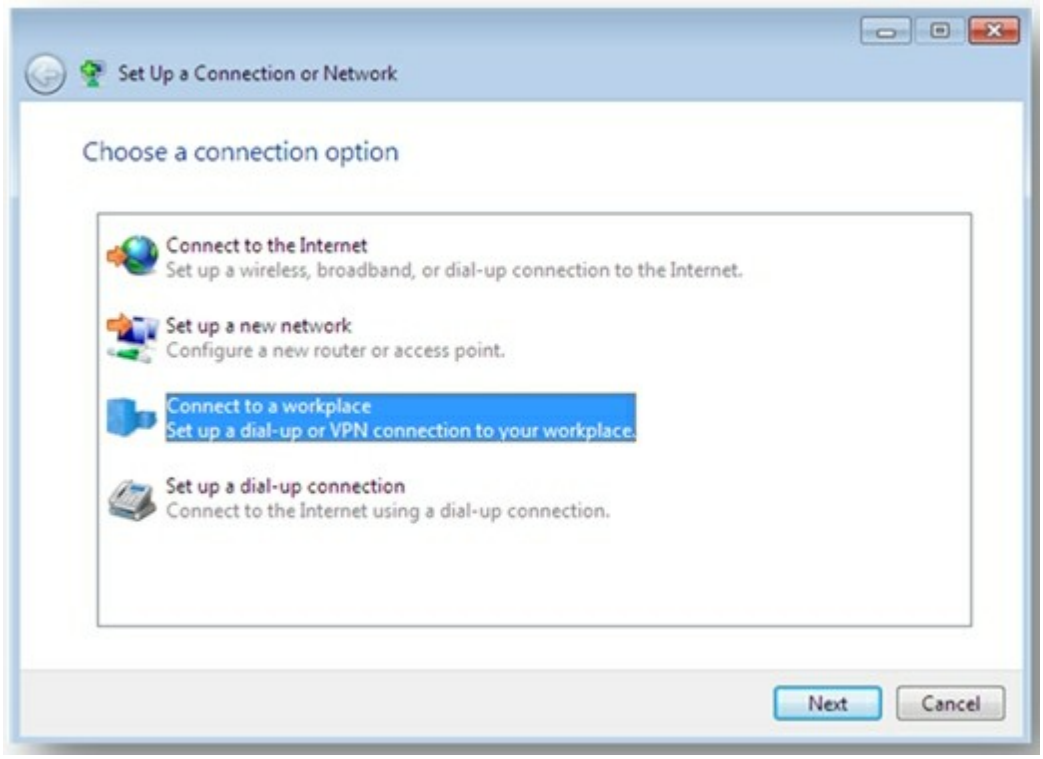
Now you can use your VPN client to connect to the NAS via the VPN service.

PPTP on Windows 7

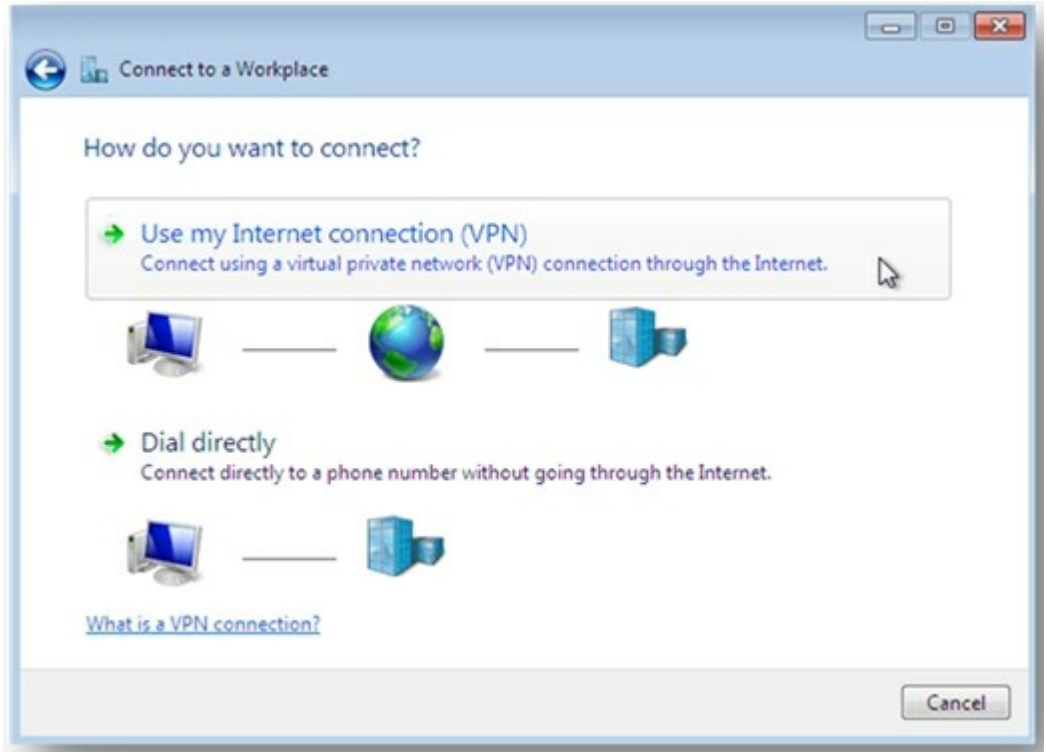
1. Go to "Control Panel" > "Network and Sharing Center". Select "Set up a new connection or network".



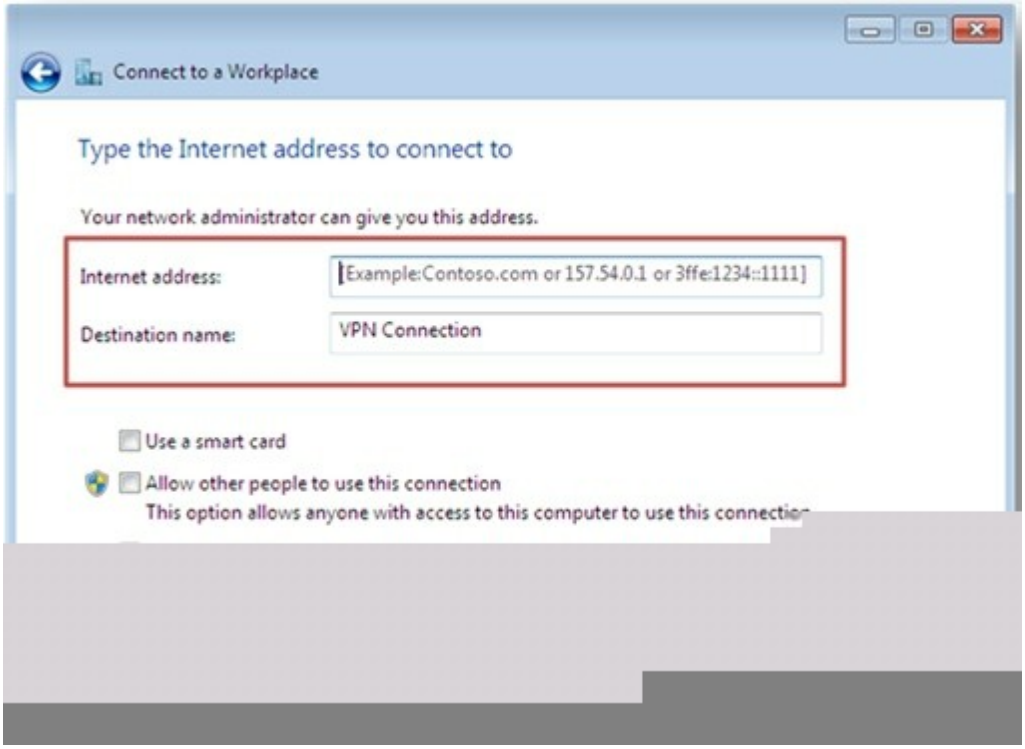
2. Select “Connect to a workplace” and click “Next”.



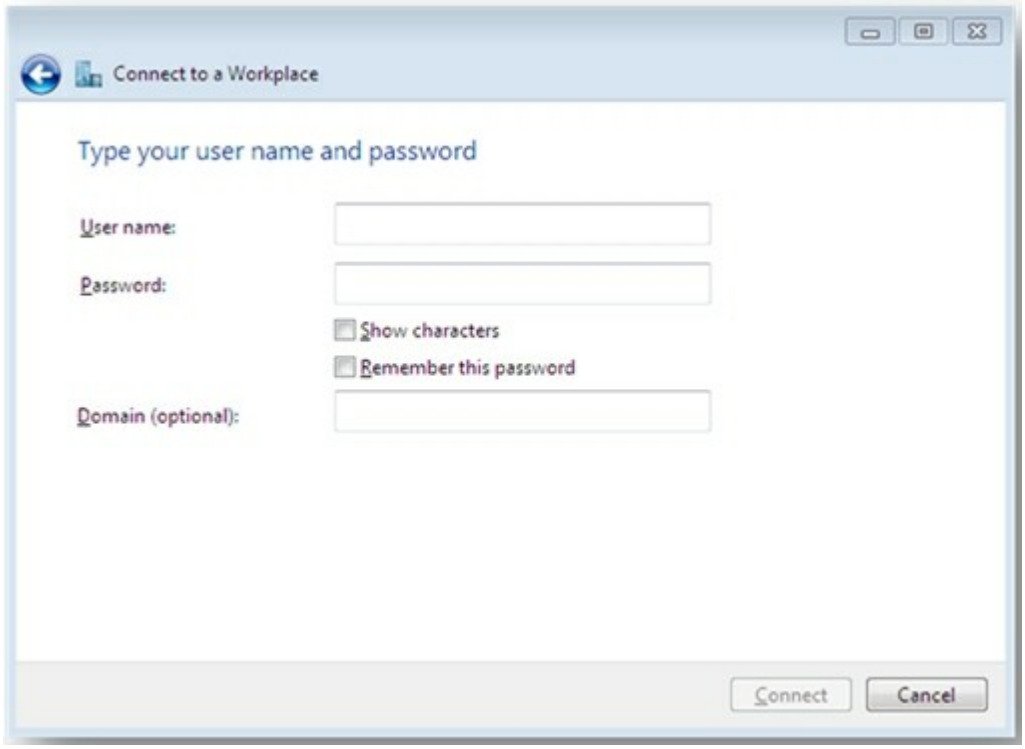
3. Select “Use my Internet connection (VPN)”.



4. Enter the MyCloudNAS name or the WAN IP of the NAS and enter a name of the connection. Then click “Next”.



5. Enter your user name and password which is added from the NAS for VPN access. Click “Connect”.

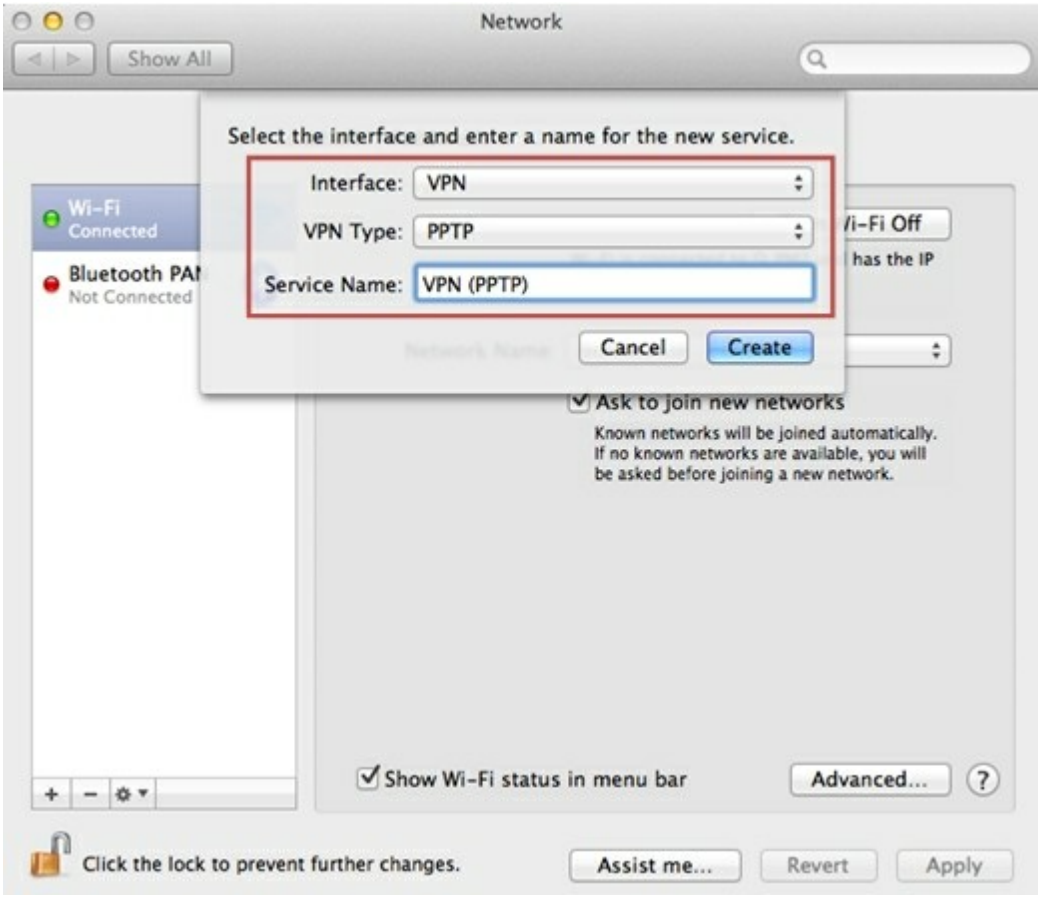


PPTP on Mac OS X 10.7

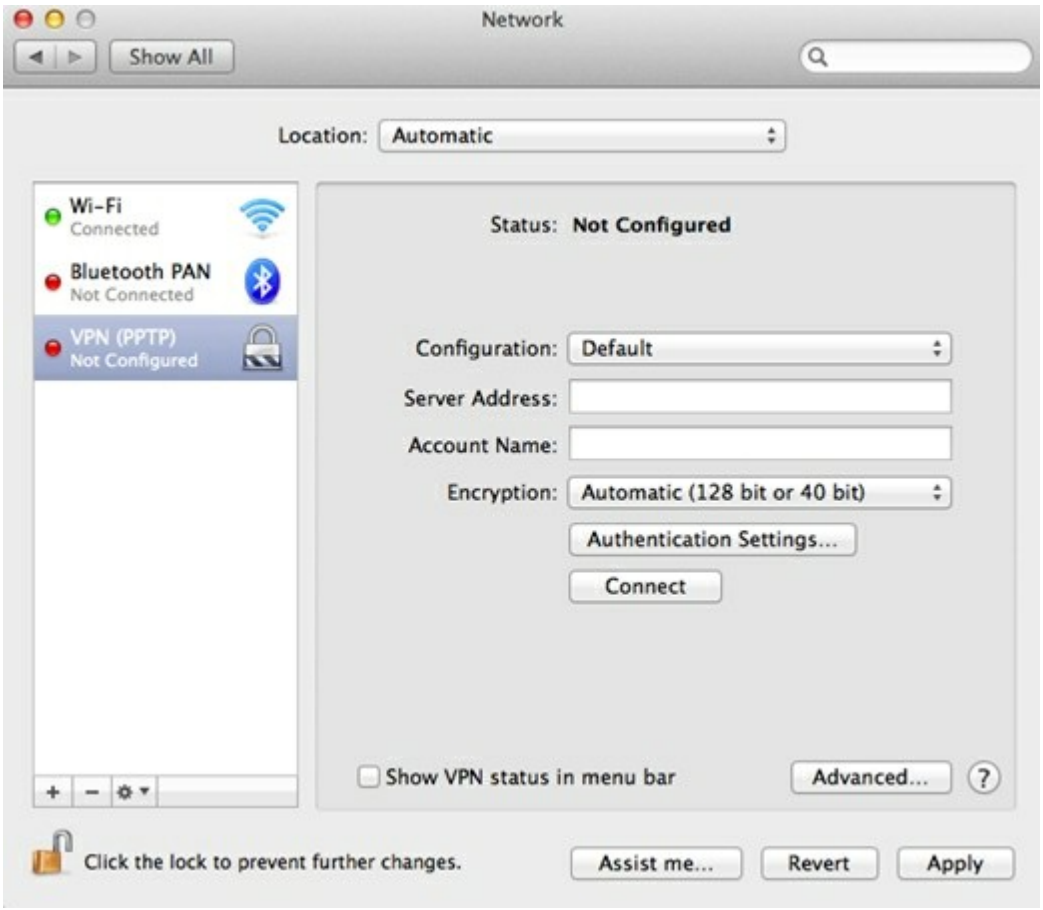
1. Choose “Apple menu” > “System Preferences”, and click “Network”.

2. Click “Add (+)” at the bottom of the list, and choose “VPN” as the interface.

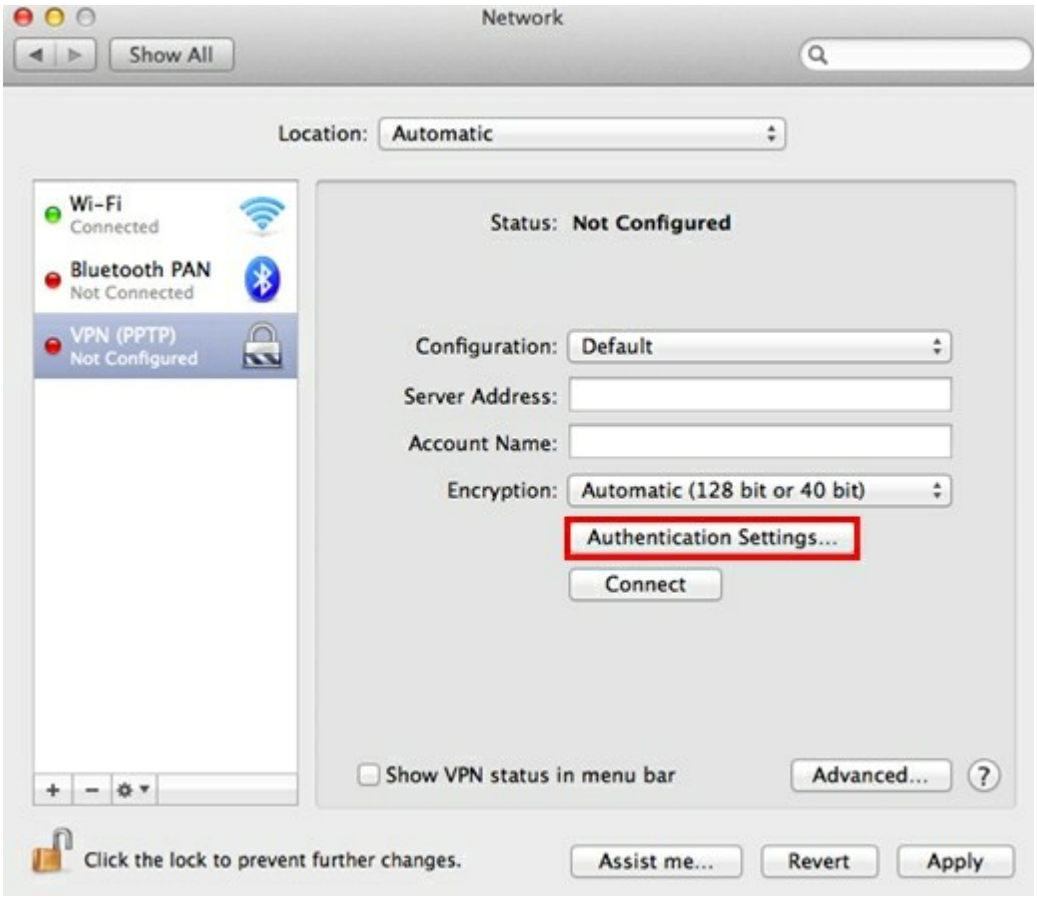
3. Choose the VPN type according to the settings of the NAS to connect. Enter the service name.



4. In “Server Address”, enter the MyCloudNAS name or the WAN IP of the NAS. In “Account Name”, enter your user name which is added from the NAS.


Network
Show All
Location: Automatic
Wi-Fi
Connected
Bluetooth PAN
Not Connected
VPN (PPTP)
Not Configured
Status: Not Configured
Configuration: Default
Server Address:
Account Name:
Encryption: Automatic (128 bit or 40 bit)
Authentication Settings...
Connect
Show VPN status in menu bar
Advanced...
Click the lock to prevent further changes.
Assist me...
Revert
Apply

5. Click “Authentication Settings”, and enter the user authentication information given by the network administrator.



6. After entering the user authentication information, click “OK”, and then click “Connect”.

PPTP on iOS 5

1. Go to “Settings” > “General” > “Network”, select “VPN”.

2. Select “Add VPN Configuration”.

3. Select “PPTP”, and enter the Description, Server, Account, and Password for the connection.

4. Return to “Settings” > “General” > “Network” > “VPN”, and enable “VPN”.

OpenVPN on Windows

1. Download OpenVPN from http://openvpn.net/index.php/open-source/downloads.html
2. Install OpenVPN client on Windows. The default installation directory is C:\Program Files\OpenVPN.
3. Run OpenVPN GUI as administrator.
4. Download OpenVPN configuration file and certificate from the NAS ("Application Servers" > "VPN Service" > "VPN Server Settings" > "OpenVPN Settings").
5. Edit openvpn.ovpn and replace "OPENVPN_SERVER_IP" with the OpenVPN server IP.
6. Put "ca.crt" and "openvpn.ovpn" into the configuration folder under OpenVPN configuration subdirectory (C:\Program Files\OpenVPN\config).

Note: If the OpenVPN client is running on Windows 7, add the firewall rules in the advanced settings of OpenVPN.

OpenVPN on Linux

1. Download OpenVPN from http://openvpn.net/index.php/open-source/downloads.html
2. Install OpenVPN client on Linux.
3. Download OpenVPN configuration file and certificate from the NAS (“Application Servers” > “VPN Service” > “VPN Server Settings” > “OpenVPN Settings”).
4. Edit openvpn.ovpn and replace “OPENVPN_SERVER_IP” with OpenVPN server IP.
5. Put “ca.crt” and “openvpn.ovpn” into the configuration folder under OpenVPN configuration subdirectory.
6. Run OpenVPN.

OpenVPN on Mac

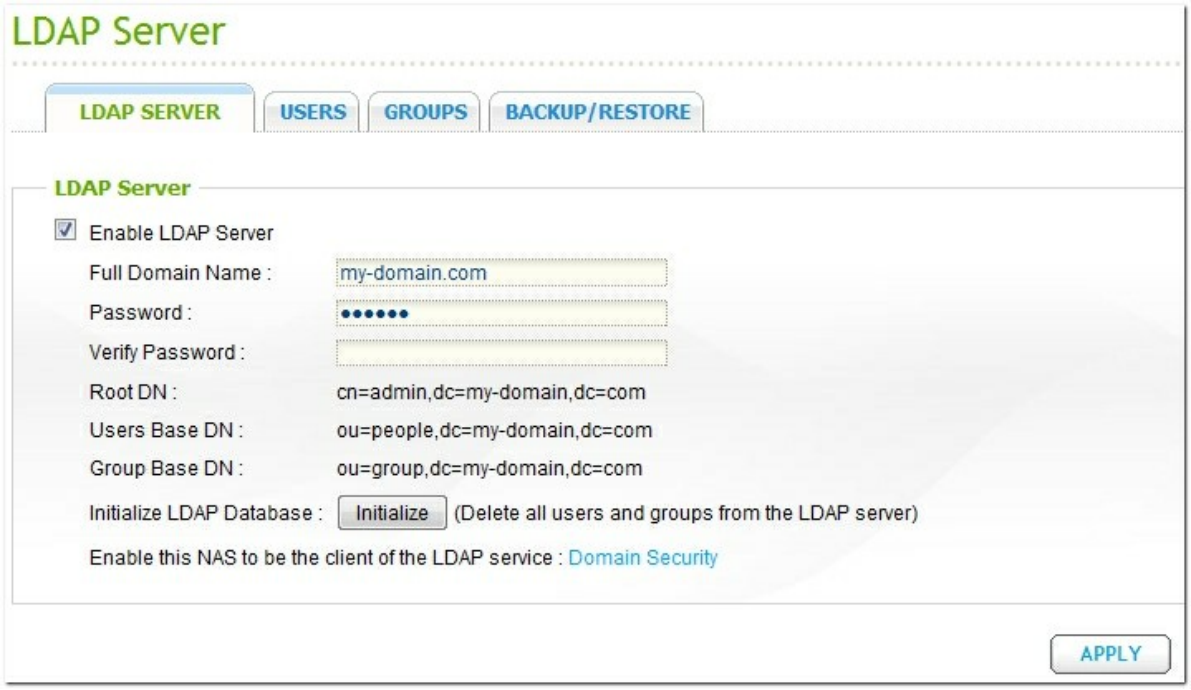
1. Download the disk image of OpenVPN client from http://code.google.com/p/tunnelblick/
2. Launch Tunnelblick.
3. Download OpenVPN configuration file and certificate from the NAS (“Application Servers” > “VPN Service” > “VPN Server Settings” > “OpenVPN Settings”).
4. Edit openvpn.ovpn and replace OPENVPN_SERVER_IP (alfred.myqnapnas.com) with OpenVPN server IP.
5. Put “ca.crt” and “openvpn.ovpn” into the configuration folder under OpenVPN configuration subdirectory.
6. Run OpenVPN.

7.17 LDAP Server

The LDAP server of the NAS allows the administrator to create users to access multiple NAS servers with the same user name and password. Follow the instructions below to configure the LDAP server.

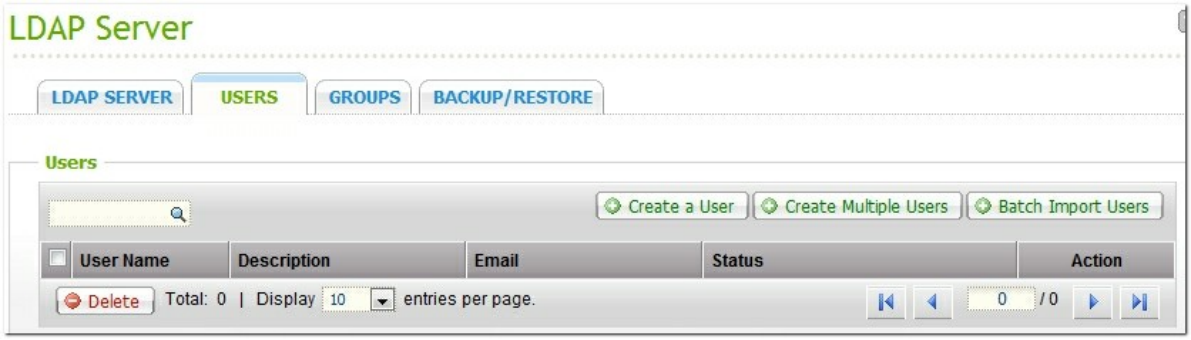
Enable LDAP Server

Login the NAS as "admin". Go to "Application Servers" > "LDAP Server" and enable LDAP server. Enter the full LDAP domain name and the password for the LDAP server, then click "Apply".



Create LDAP Users

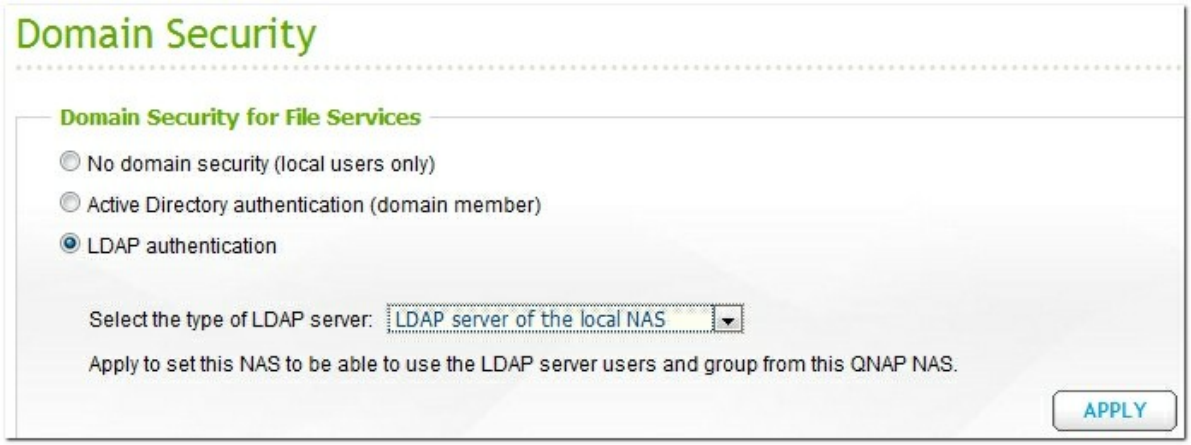
Under the "Users" tab, click "Create a User" or "Create Multiple Users" or "Batch Import Users". Follow the instructions of the wizard to create the LDAP users.



Once you have created the LDAP users, the NAS can be joined to the domain. You can set the permissions of the LDAP users and allow them to be authenticated by the NAS.

Join a NAS to LDAP Domain

To allow the LDAP users to connect to the NAS, join the NAS to the LDAP domain. Go to "Access Right Management" > "Domain Security". Select "LDAP authentication" and choose "LDAP server of local NAS" as the server type. Then click "Apply".



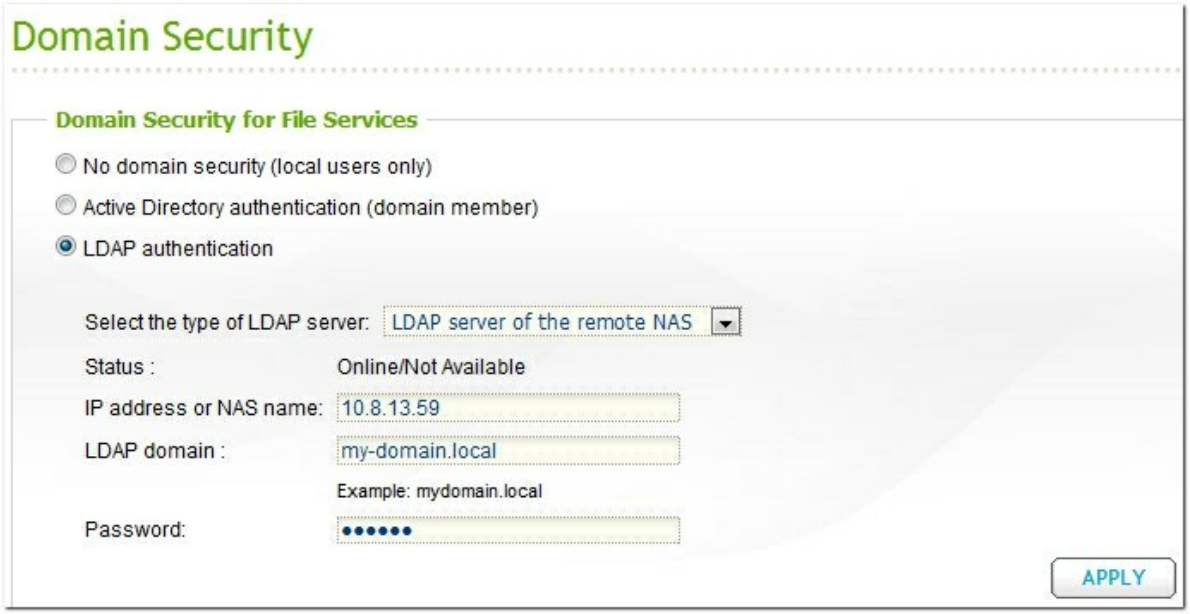
The NAS is now a client of the LDAP server. To view the domain users or groups, go to "Access Right Management" > "Users" or "User Groups", then select "Domain Users" or "Domain Groups". You can also set the folder permission for the domain users or groups.

Join a Second NAS to LDAP Domain

You can join multiple NAS servers to the same LDAP domain and allow the LDAP users to connect to the NAS servers using the same login credentials.

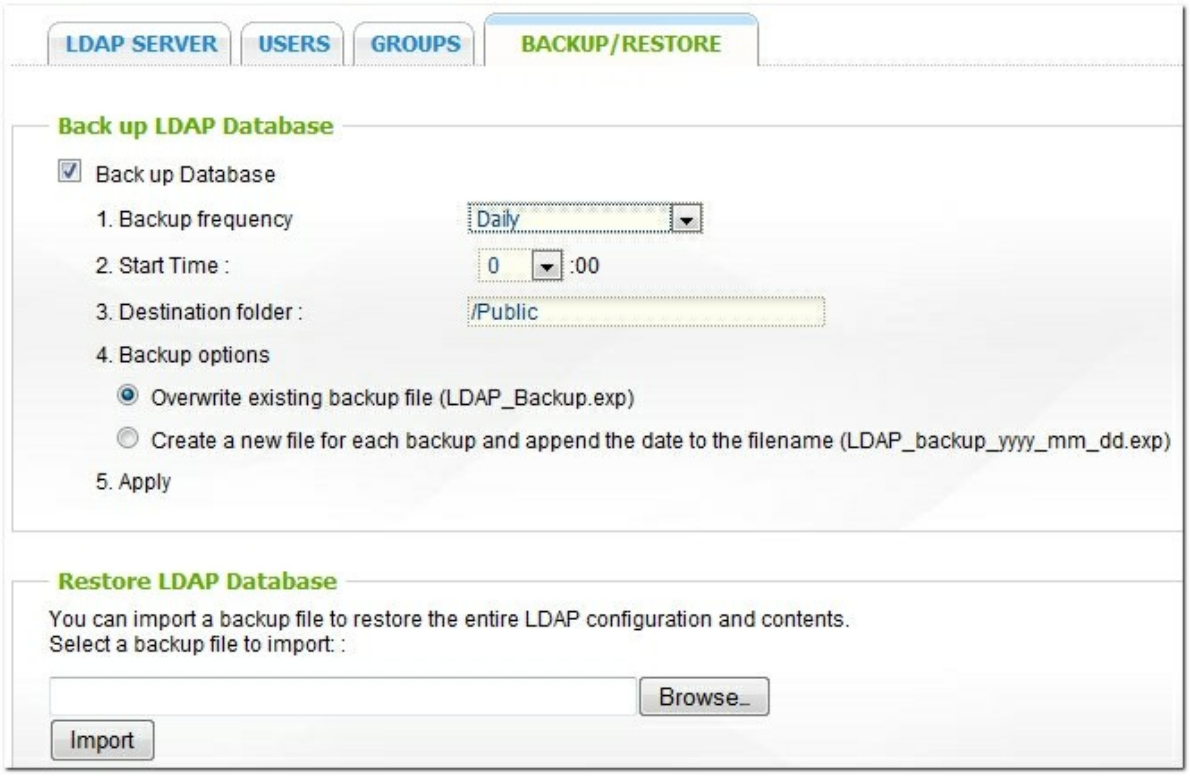
To join another NAS to the LDAP domain, login the NAS and go to "Access Right Management" > "Domain Security". Select "LDAP authentication" and then "LDAP server of a remote NAS" as the server type.

Enter the DNS name or IP address of the remote NAS, the name of the LDAP domain that you created previously, and enter the LDAP server password. Click "Apply".



Back up/Restore LDAP Database

To back up the LDAP database on the NAS, select "Back up Database" and specify the backup frequency, destination folder on the NAS and other options. To restore an LDAP database, browse to select the *.exp file and click "Import". Click "Apply" to apply the settings.



8. Backup

Remote Replication 514
Cloud Backup 539
Time Machine 549
External Drive 554
USB One Touch Copy 569

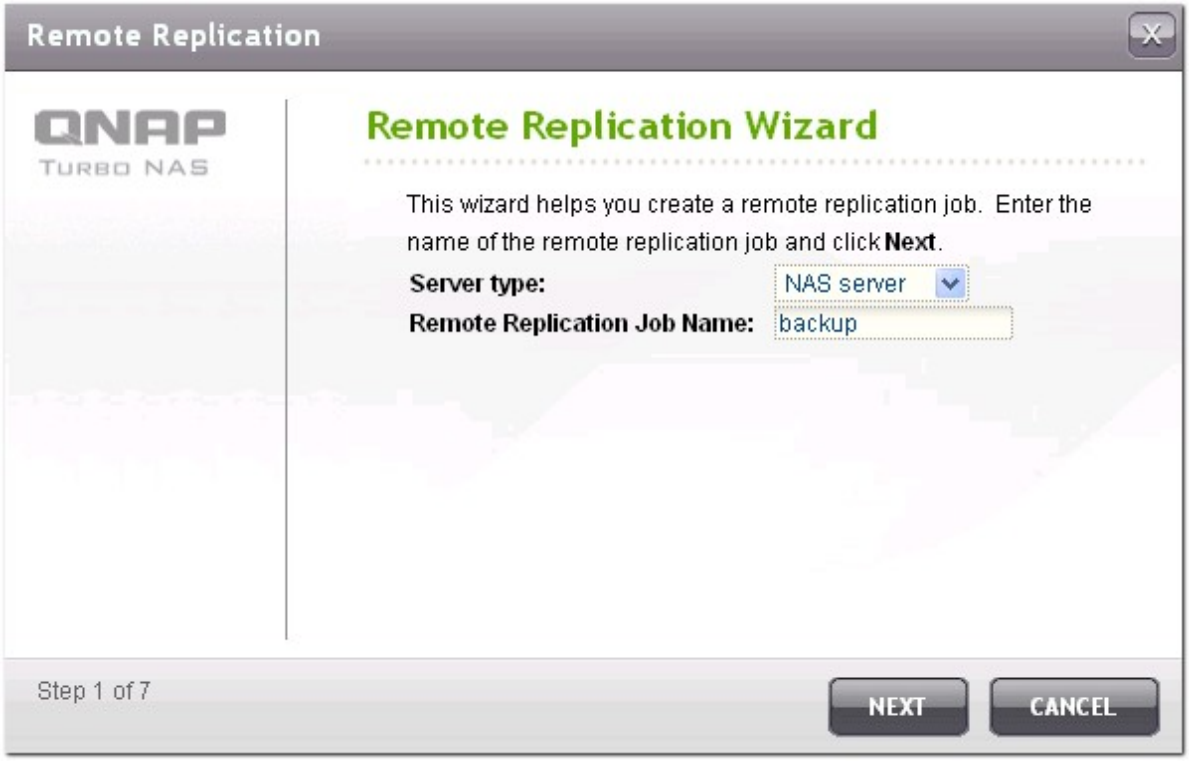
8.1 Remote Replication

Rsync Replication

The NAS data can be backed up to a remote NAS or Rsync server by Rsync remote replication. If the backup destination is a NAS, go to "Application Servers" > "Backup Server" > "Rsync Server" and enable the remote NAS as an Rsync backup server.

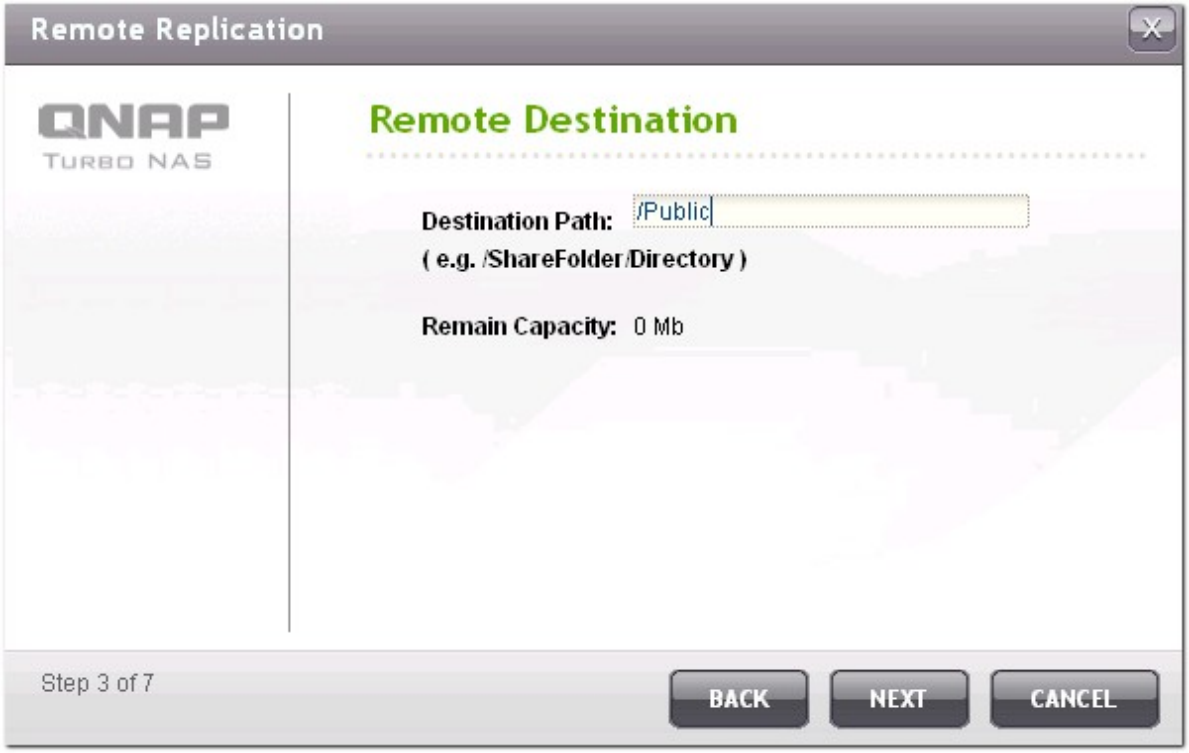
1. To create a replication job, click "Create a Replication Job".

2. Specify the server type, NAS or Rsync server, of the remote server. Enter a job name. Click "Next".



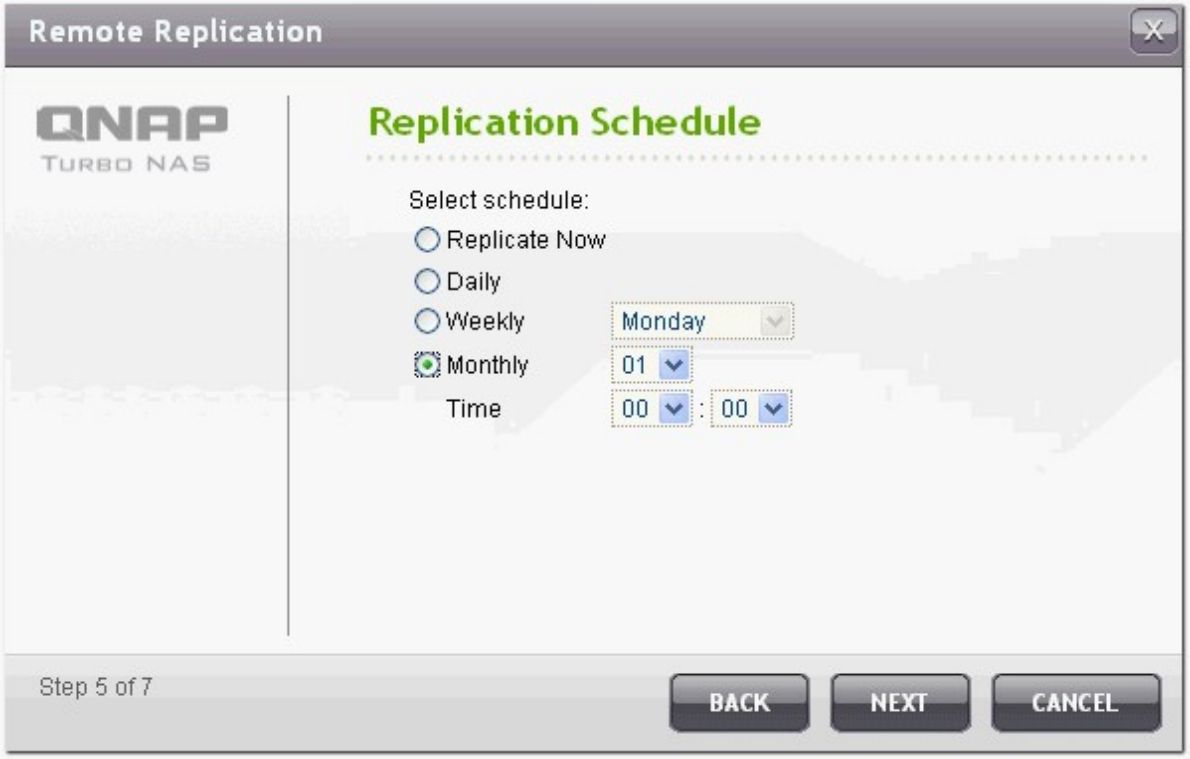
3. Enter the IP address, port number, user name and password to login the remote server. The default port number is 873. Note that the login user name must have read/write access to the remote server and sufficient quota limit on the server. Click "TEST" to verify the connection. Then click "Next".

4. Specify the destination folder, where the data will be replicated to.

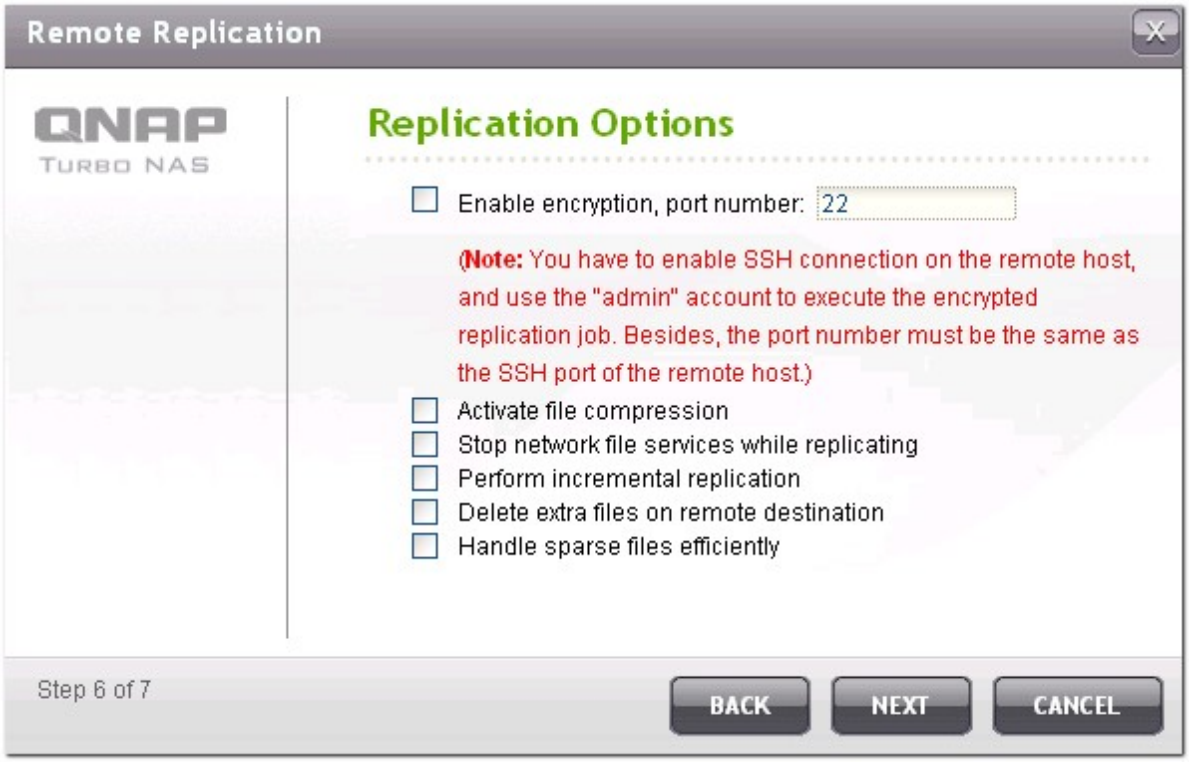


5. Specify the local folder, where the data will be replicated from.

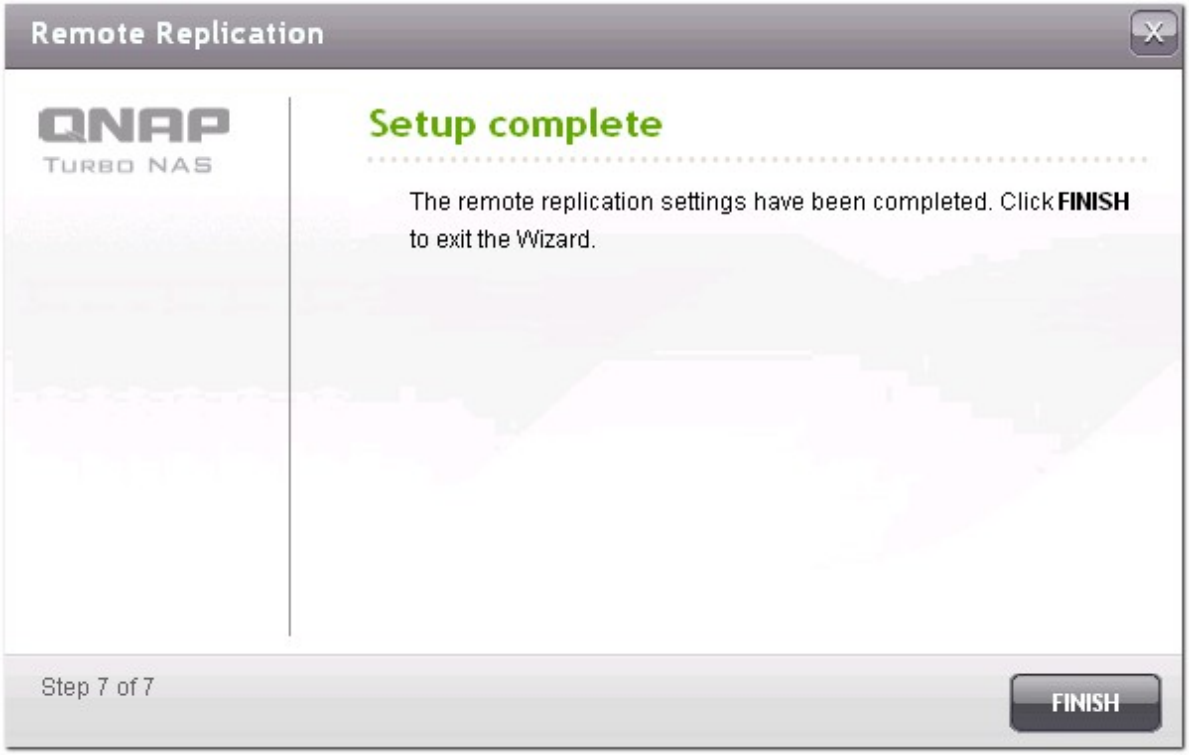
6. Select to replicate the data immediately or specify the backup schedule.

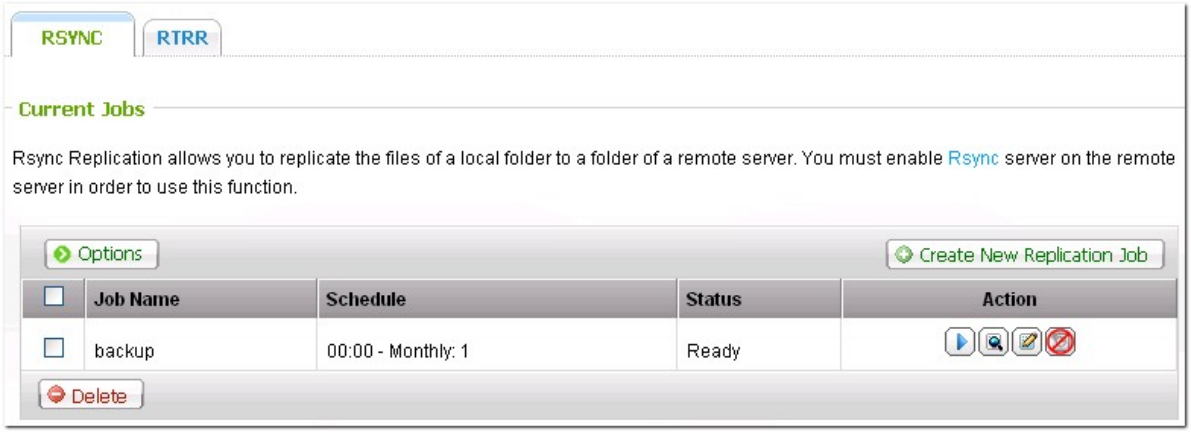


7. Specify other options for the remote replication job.
   - Enable encryption: Select this option to execute encrypted remote replication. Note that you must turn on "Allow SSH connection" in "Network Services > "Telnet/SSH" and specify the same port number for SSH and encrypted remote replication.
   - Activate file compression: Turn on this option to allow file compression during the data transfer process. This option is recommended for low bandwidth environment or remote replication over WAN.
   - Stop network file services while replicating: Stop all connections to the NAS via Samba (SMB), AFP, and FTP when remote replication is in process.
   - Perform incremental replication: When this option is turned on, after the first-time replication, the NAS will only back up the files that have been changed since the last backup. The files of the same name, size, and modified time will not be copied again. You are recommended to turn on this option for the replication job which will be executed for more than once in order to shorten the backup time.
   - Delete extra files on remote destination: Select the option to synchronize the source data with the destination data (one-way synchronization). Extra files on the destination will be deleted. Source data will remain unchanged.
   - Handle sparse files efficiently: A sparse file is a type of computer file that contains large blocks of zero-byte data. Turn on this option may reduce the time required for remote replication.



8. Click "Finish". The job will be executed according to your schedule. Note that the job is recursive. Do not turn off the local NAS and the remote server when remote replication is running.



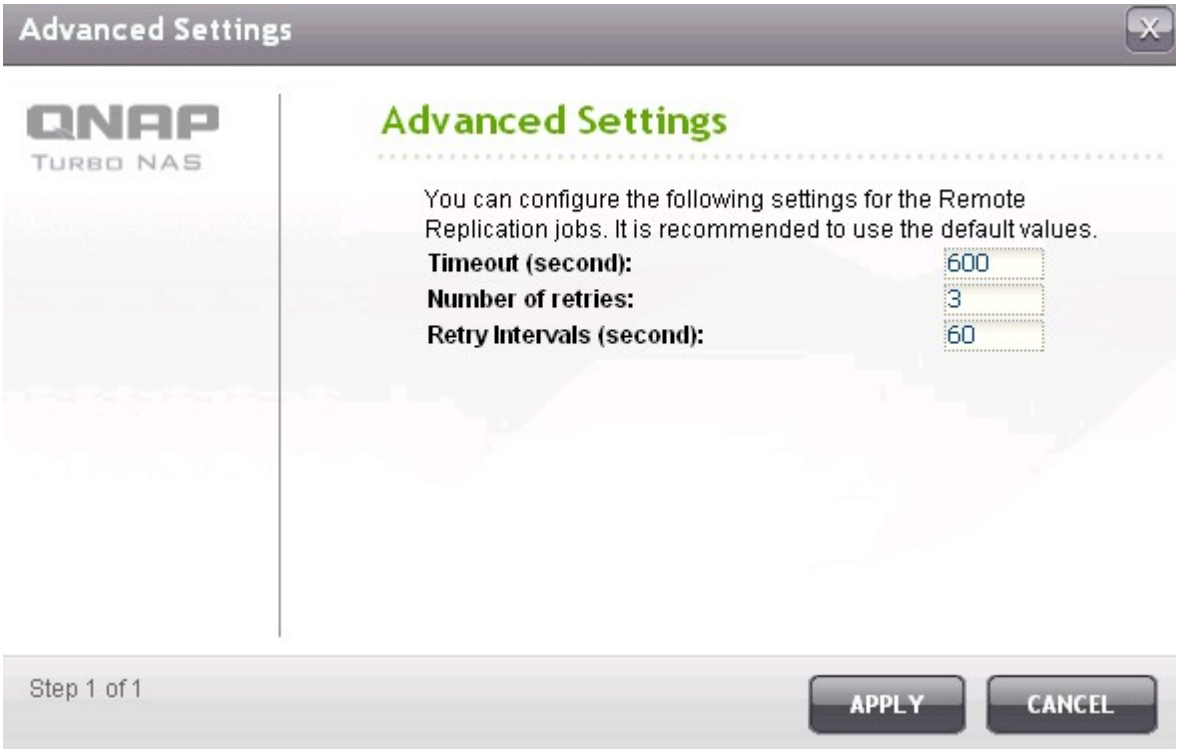


Icon	Description
	Start a replication job immediately.
	Stop a running replication job.
	View Rsync logs (replication results).
	Edit a replication job.
	Disable replication schedule.
	Enable replication schedule.

To configure the timeout and retry settings of the replications jobs, click "Options".

- Timeout (second): Specify a timeout value for each replication job. This is the maximum number of seconds to wait until a replication job is cancelled if no data has been received.
- Number of retries: Specify the number of times the NAS should try to execute a replication job should it fail.
- Retry intervals (second): Specify the number of seconds to wait in between each retry.

For example, if you entered 600 seconds for timeout, 3 retries, and 60 seconds for retry intervals, a replication job will timeout in 600 seconds if no data is received. The NAS will wait for 60 seconds and try to execute the job a second time. If the job timed out again, the NAS wait for another 60 seconds and retry for a third time.



How to back up all the shares on a disk volume by remote replication (rsync)?

To back up all the shares on a disk volume by remote replication (rsync), create a network share (for example, root) as the root directory which contains all the folders in the same volume, and specify the path to "/". Then create a remote replication job to copy this share (root). All the folders and subfolders will be replicated.

RTRR Replication

Real-time Remote Replication (RTRR) provides real-time or scheduled data replication between the local NAS and a remote NAS, an FTP server, or an external drive, or replication between two local folders. In real-time mode, the source folder will be monitored and any files that are new, changed, and renamed will be replicated to the target folder immediately. In scheduled mode, the source folder will be replicated to the target folder according to the pre-defined schedule.

If the backup destination is a NAS, you must first enable RTRR server ("Application Servers" > "Backup Server" > "RTRR Server") or FTP service ("Network Services > "FTP Service") on the remote NAS.

NAS models	**Firmware**	**Maximum number of replication jobs supported**
Intel-based NAS	Prior to v3.5.0	64*
	v3.5.0 or above	32*
ARM-based (Non Intel-based) NAS	Prior to v3.5.0	RTRR replication not supported.
	v3.5.0 or above	8*

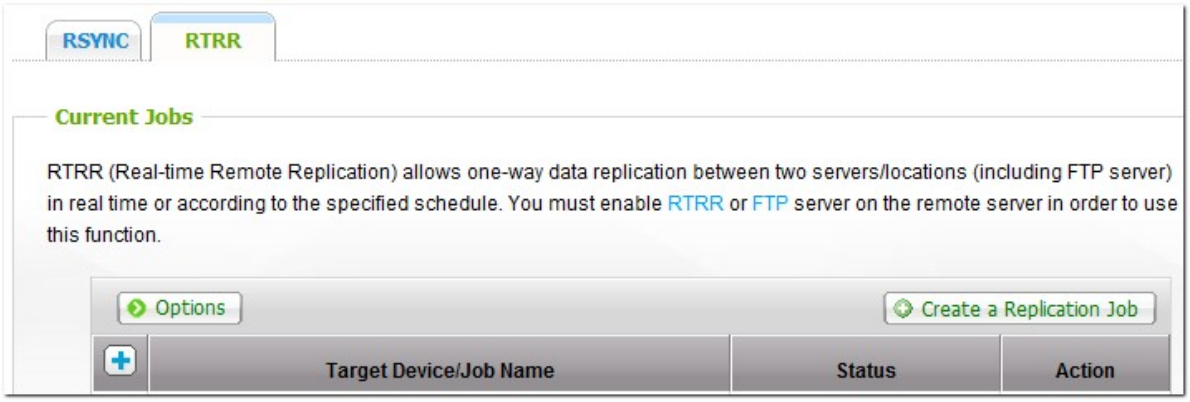
*Each job supports maximum 5 folder pairs.

If your NAS models are not listed below, please visit http://www.qnap.com for details.

Intel-based NAS	TS-x39 series, TS-x59 series, TS-x69 series, TS-509, TS-809, TS-809 Pro, TS-809U-RP, SS-439 Pro, SS-839 Pro, TS-x59 Pro+, TS-879 Pro, TS-1079 Pro, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP
ARM-based (Non Intel-based) NAS	TS-x10, TS-x12, TS-x19 series

Follow the steps below to create a replication job.

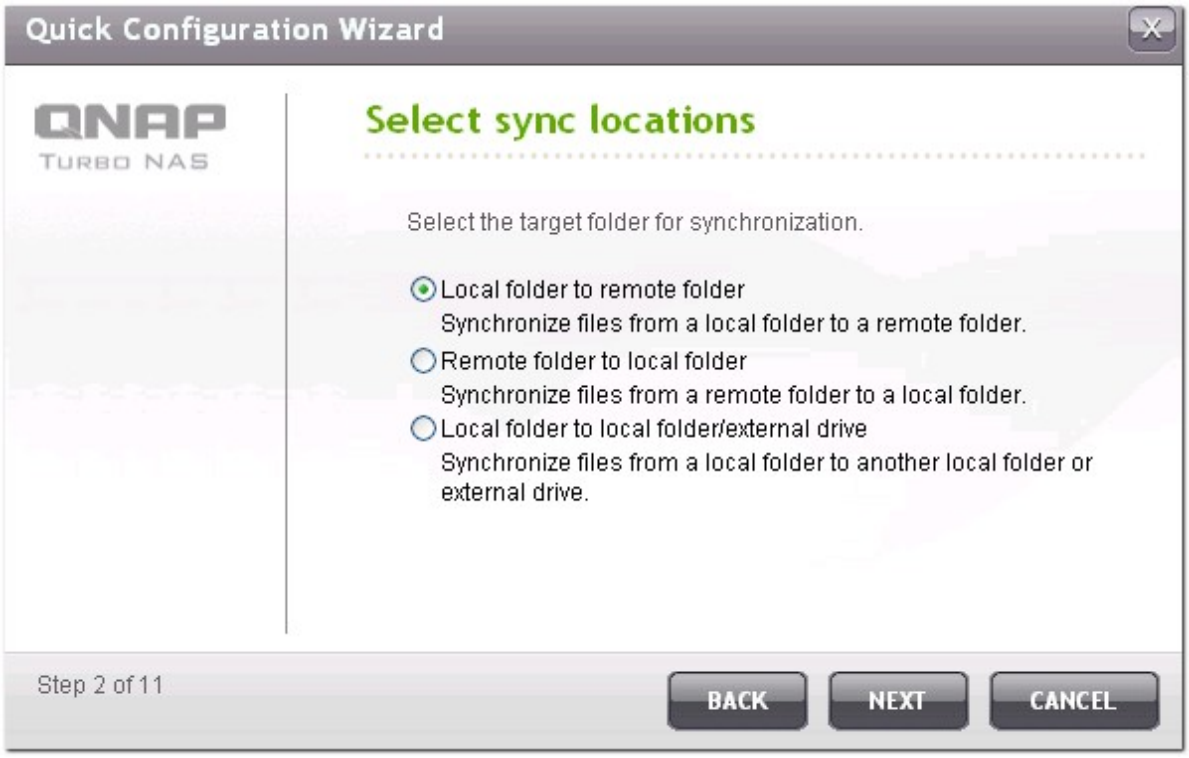
1. To create a real-time or scheduled remote replication, click “Create a Replication Job”.



2. When the wizard shows up, click “Next”.

3. Select the sync locations. Make sure the destination device has been formatted and folders have been created. The NAS supports:
   - Synchronize data from a local folder to a remote folder (NAS or FTP server)
   - Synchronize data from a remote folder (NAS or FTP server) to a local folder
   - Synchronize data from a local folder to another local folder or an external drive

Click "Next".



4. Enter the IP address or host name. Select the server type (FTP server or NAS server with RTRR service enabled).

Remote replication to FTP server:

Specify the port number and if you want to enable FTP with SSL/TLS (Explicit) for encrypted data transfer. If the FTP server is behind a firewall, enable passive mode. Enter the user name and password with read/write access to the server. Click "Next".

Remote replication to NAS with RTRR service:

Enter the IP address of the RTRR service-enabled server. Specify the connection port and select whether or not to enable secure connection. The default port number for remote replication via RTRR is 8899. Enter the password for RTRR connection. Click "Next".

5. Select the folder pair for data synchronization.

Note: If a folder or its parent folder or child folder has been selected as the source or destination in a folder pair of a replication job, you cannot select the folder as the source or destination of another folder pair of the same job.

6. Select "Add More Folder Pairs" to add more folder pairs for backup.

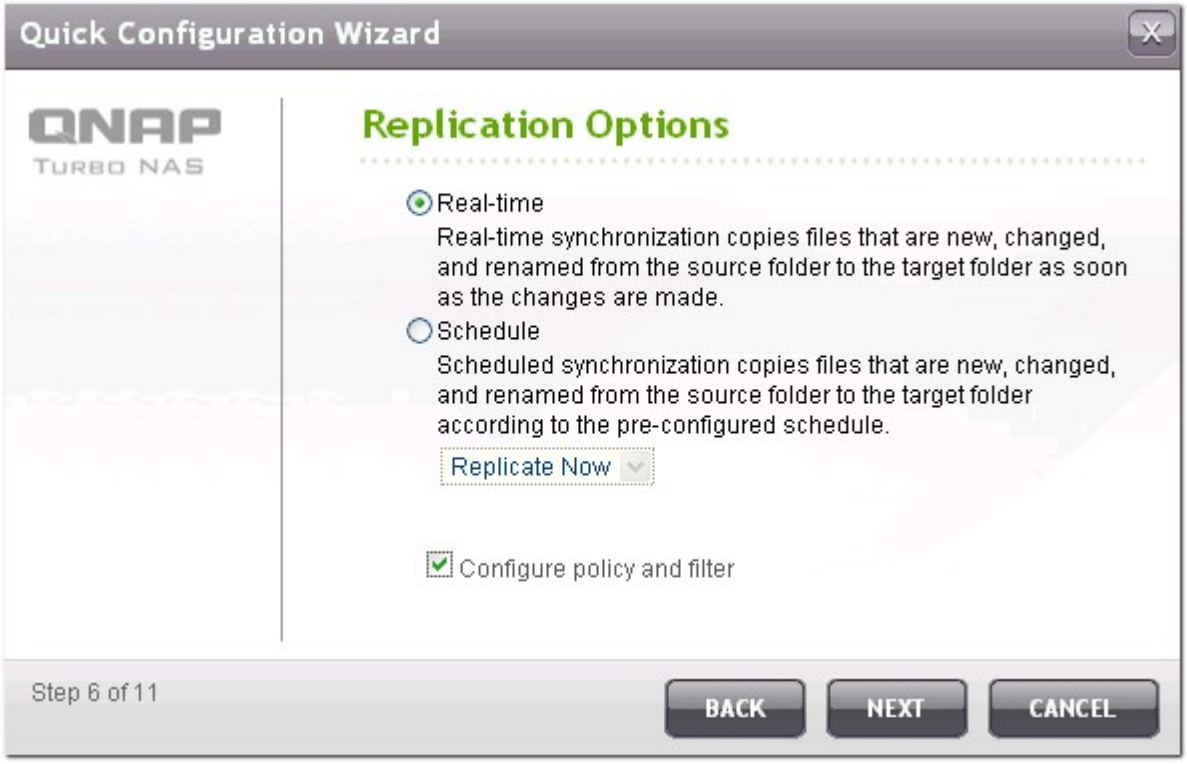
Each sync job supports maximum 5 folder pairs. Select the folder pairs and click "ADD". Click "Next".

7. Choose between real-time and scheduled synchronization. Real-time synchronization copies files that are new, changed, and renamed from the source folder to the target folder as soon as the changes are made after the first-time backup.

Note: RTRR does not support bi-directional synchronization in the current version. The folder pair cannot be synchronized between two NAS servers in real-time mode. To synchronize the data between the folder pair of two NAS servers, please use scheduled backup.

Scheduled synchronization copies files from the source folder to the target folder according to the pre-configured schedule. The options are:

- Replicate Now: Replicate data immediately.
- Periodically: Enter the time interval in hour and minute that the backup should be executed. The minimum time interval is 5 minutes.
- Hourly: Specify the minute when an hourly backup should be executed, e.g. enter 01 to execute backup each first minute of every hour, 1:01, 2:01, 3:01...
- Daily: Specify the time when a daily backup should be executed, e.g. 02:02 every day.
- Weekly: Select a day of the week and the time when a weekly backup should be executed.
- Monthly: Select a day of the month and the time when a monthly backup should be executed.

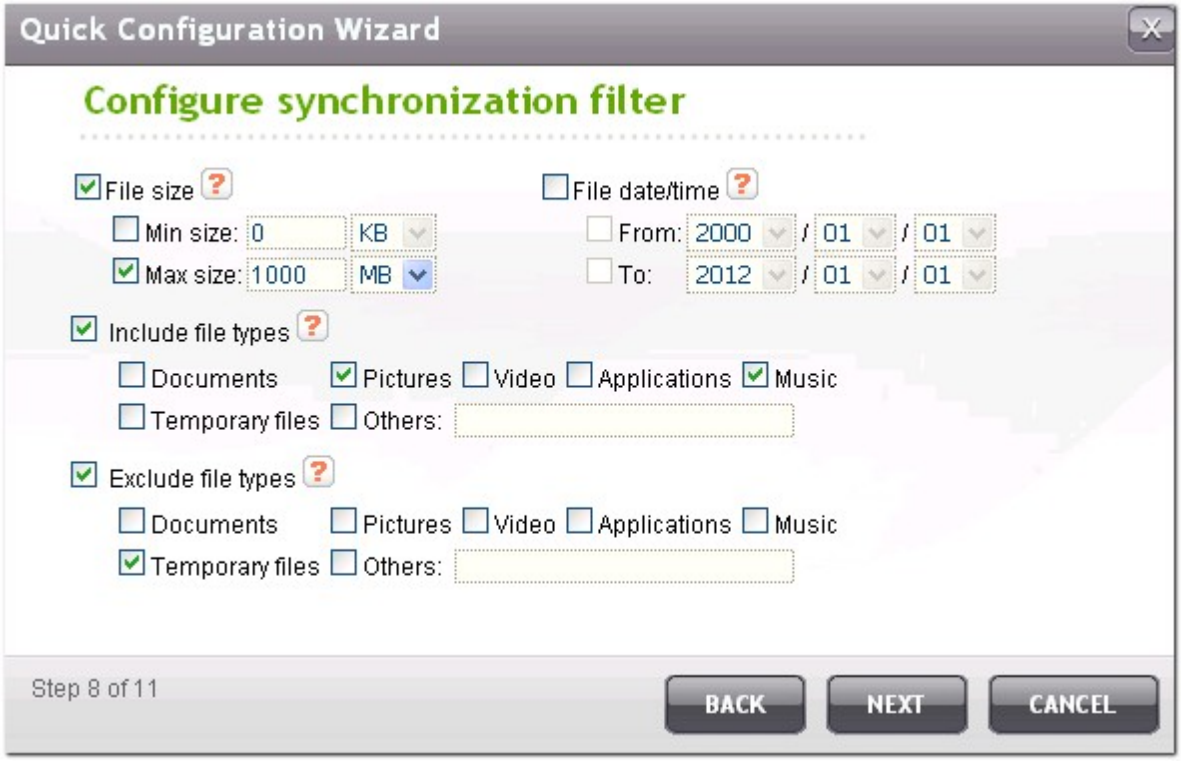


8. To configure synchronization policy, select "Configure policy and filter" and click "Next".

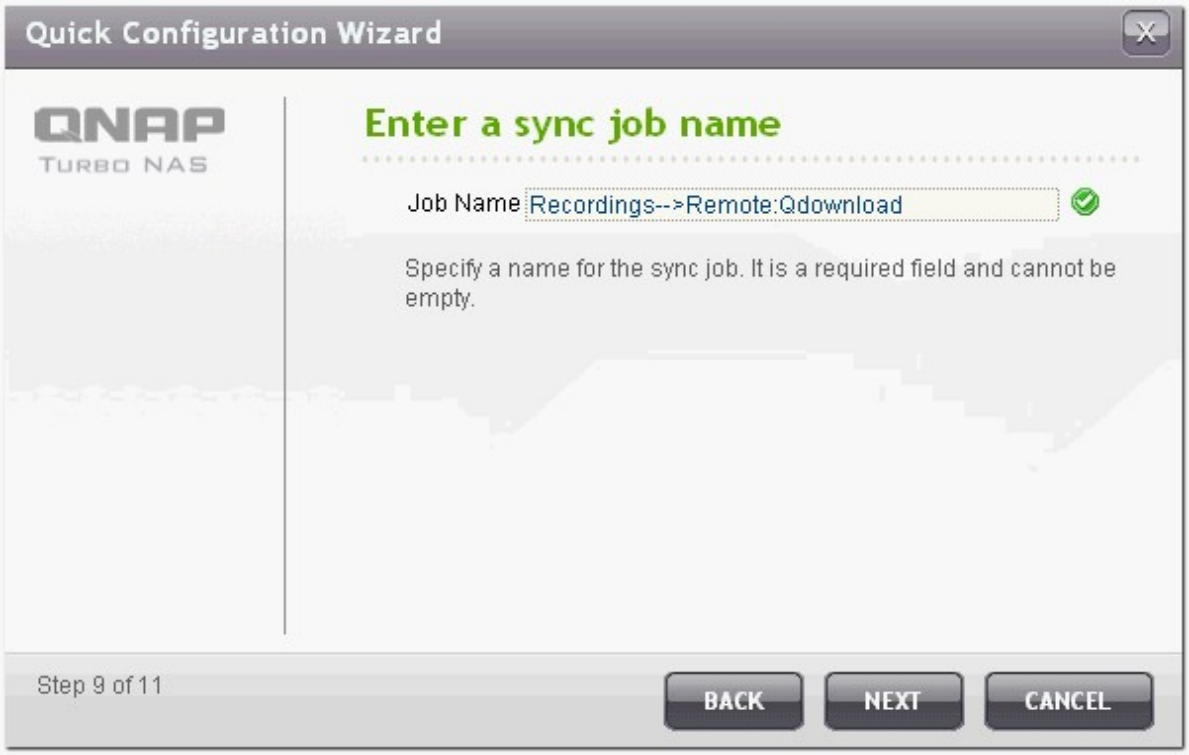
Select whether or not to enable the following options:

- Delete extra files: Delete extra files in the target folder. Deletions made on the source folder will be repeated on the target folder. This option is not available for real-time synchronization.
- Detect sparse files: Select this option to ignore files of null data.
- Check file contents: Specify to examine file contents, date, size, and name to determine if two files are identical. This option is not available for real-time synchronization.
- Compress files during transmissions: Specify whether or not the files should be compressed for sync operations. Note that more CPU resources will be consumed.
- Ignore symbolic links: Select this option to ignore symbolic links in the pair folder.
- Extended attributes: Select this option to keep the information in extended attributes.
- Timeout and retry settings: Specify the timeout period and retry settings if a sync operation fails.

9. Specify the file size, file types to include/exclude, and file date/time to filter data synchronization.
   - File size: Specify the minimum and maximum size of the files to be replicated.
   - Include file types: Specify the file types to be replicated.
   - Exclude file types: Specify the file types to be excluded for replication.
   - File date/time: Specify the date and time of the files to be replicated.

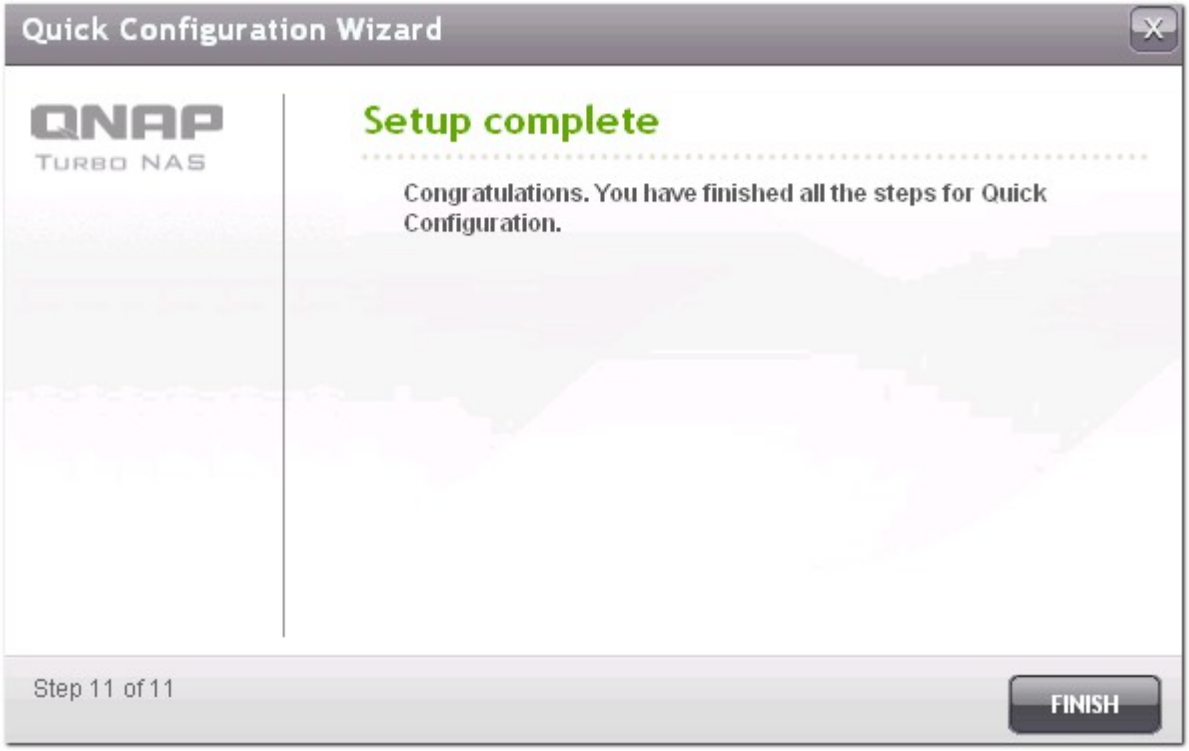


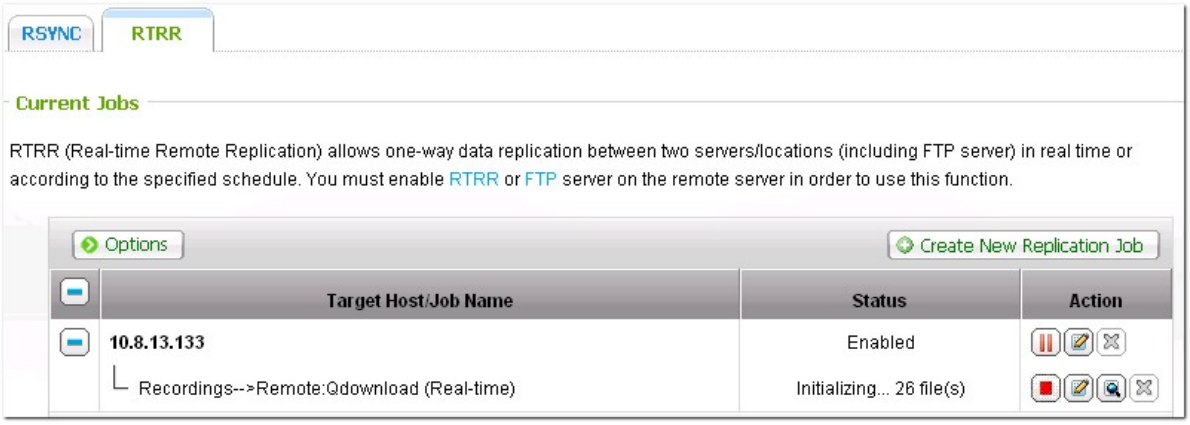
10. Enter a job name. Click “Next”.



11. Confirm the settings and click “Next”.

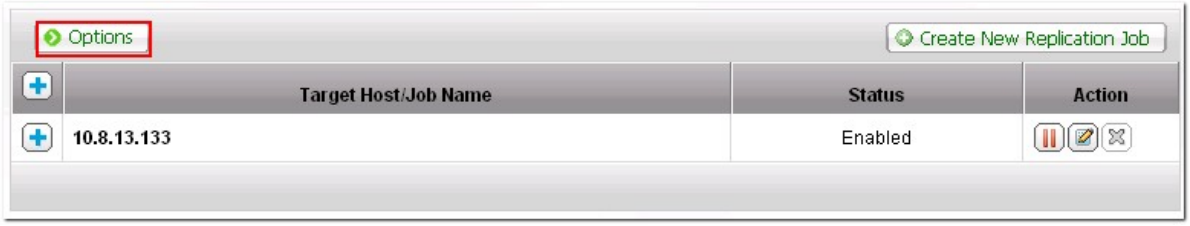
12. Click “Finish” to exit the wizard.



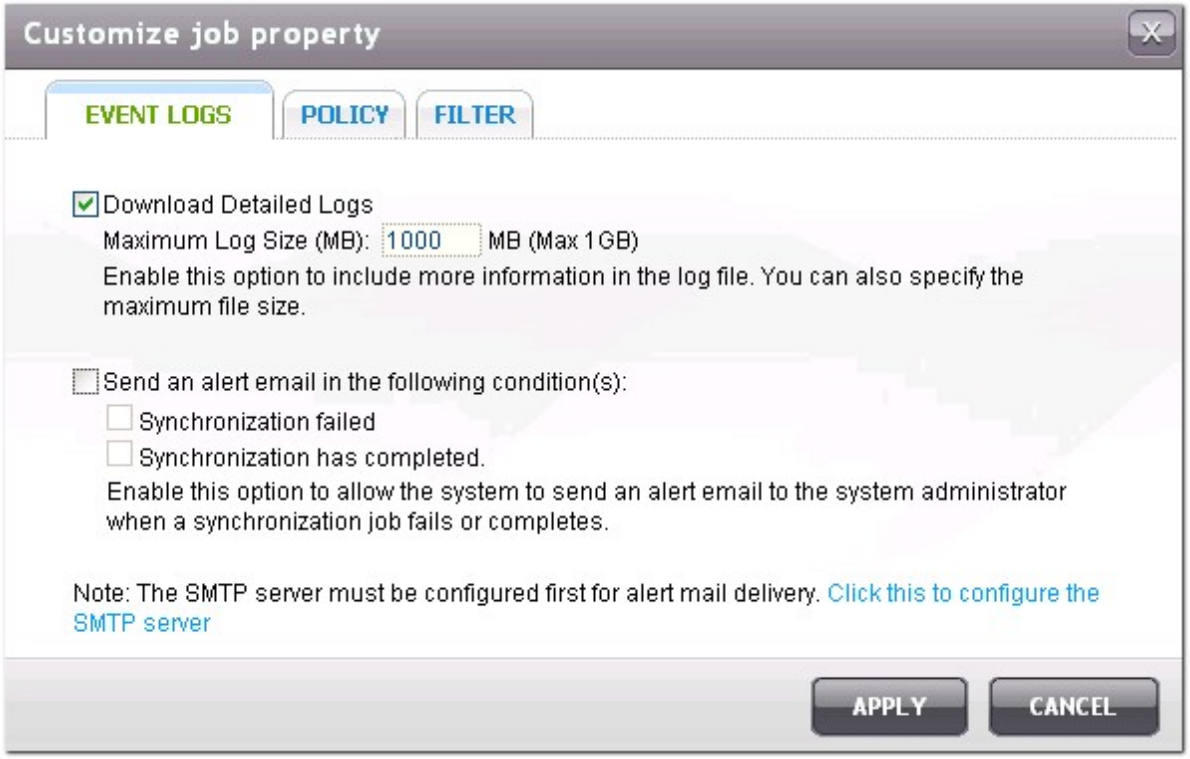


Icon	Description
	• Enable connection to a remote server. • Start a replication job.
	Stop connection to a remote server or external drive.
	Stop a replication job.
	View job status and logs; download logs.
	• Edit the connection settings of a remote server. • Edit the settings of a replication job.
	• Delete connection settings to a remote server. • Delete a replication job. This button is available only after a replication job is stopped or the connection to the remote server is stopped.

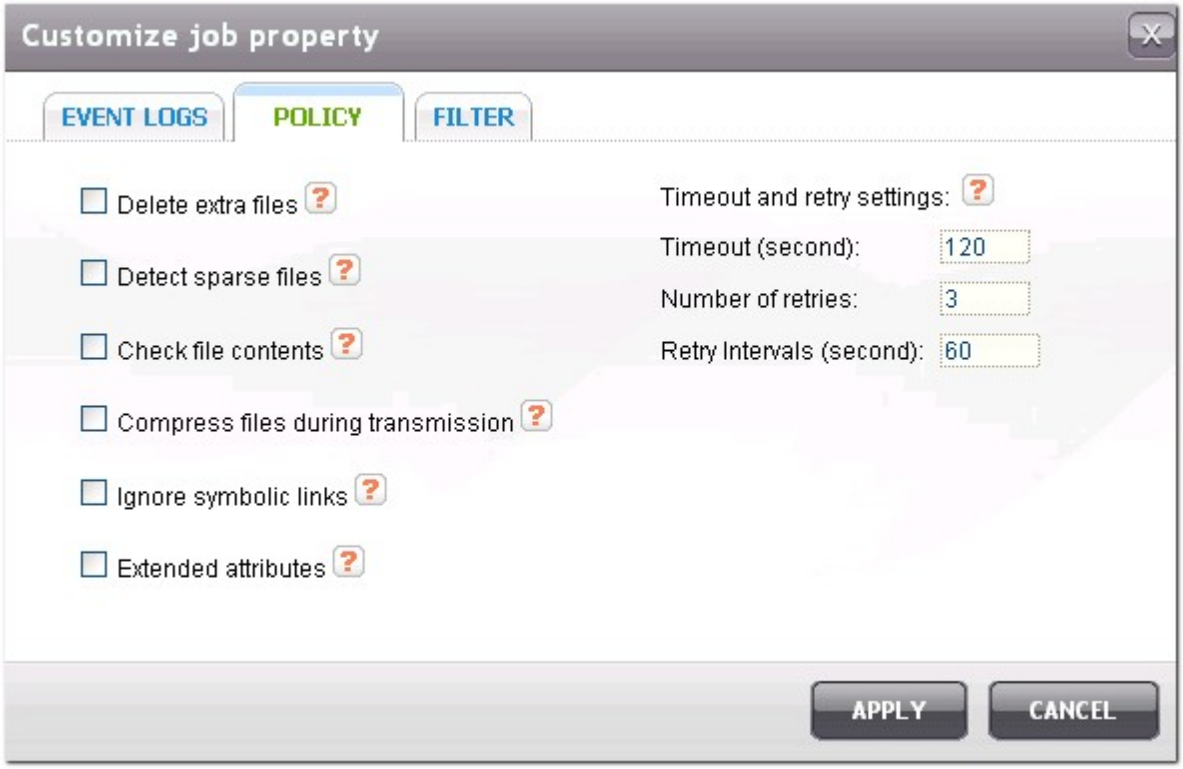
To edit the replication job properties, click "Options".



Under "Event Logs" you can select to enable "Download Detailed Logs" and specify the maximum file size of the log file. You can also select to send an email alert when synchronization fails or completes. Note that the SMTP server settings must be properly set up on the NAS ("System Administration" > "Notification").



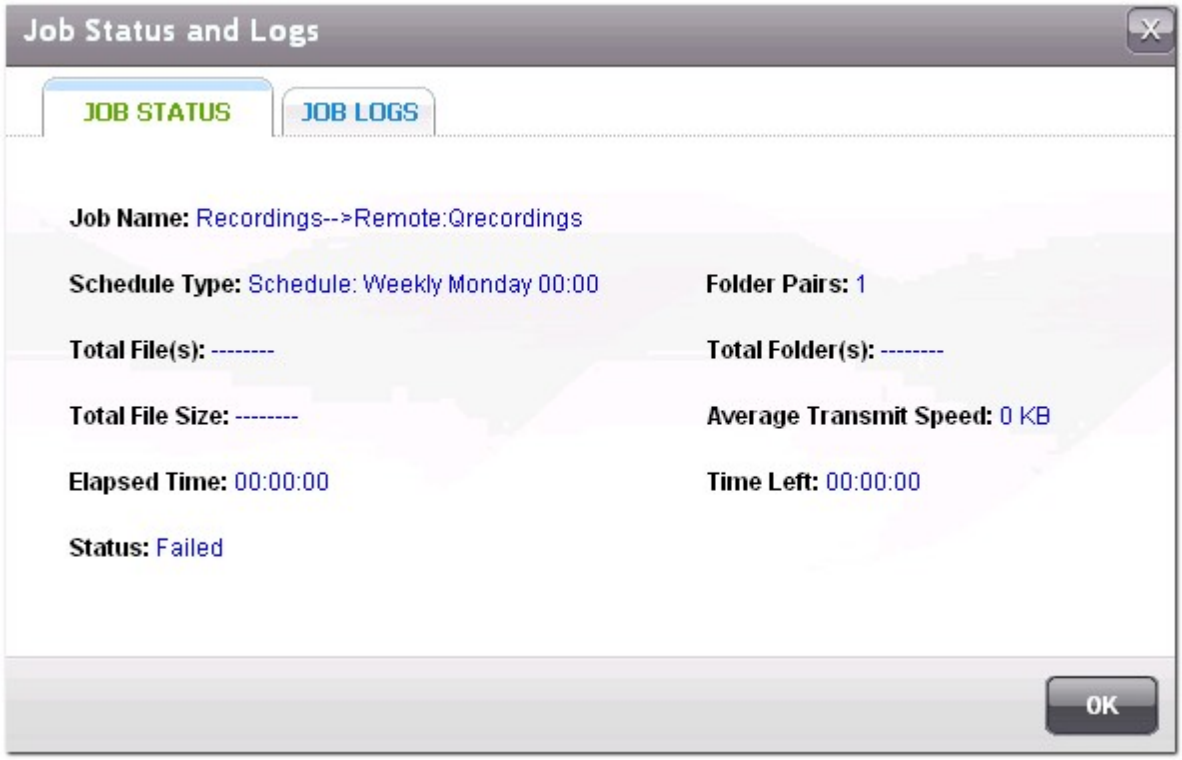
Specify the replication policy in “Policy” and filter settings in “Filter”. These will become the default settings for all RTRR replication jobs.



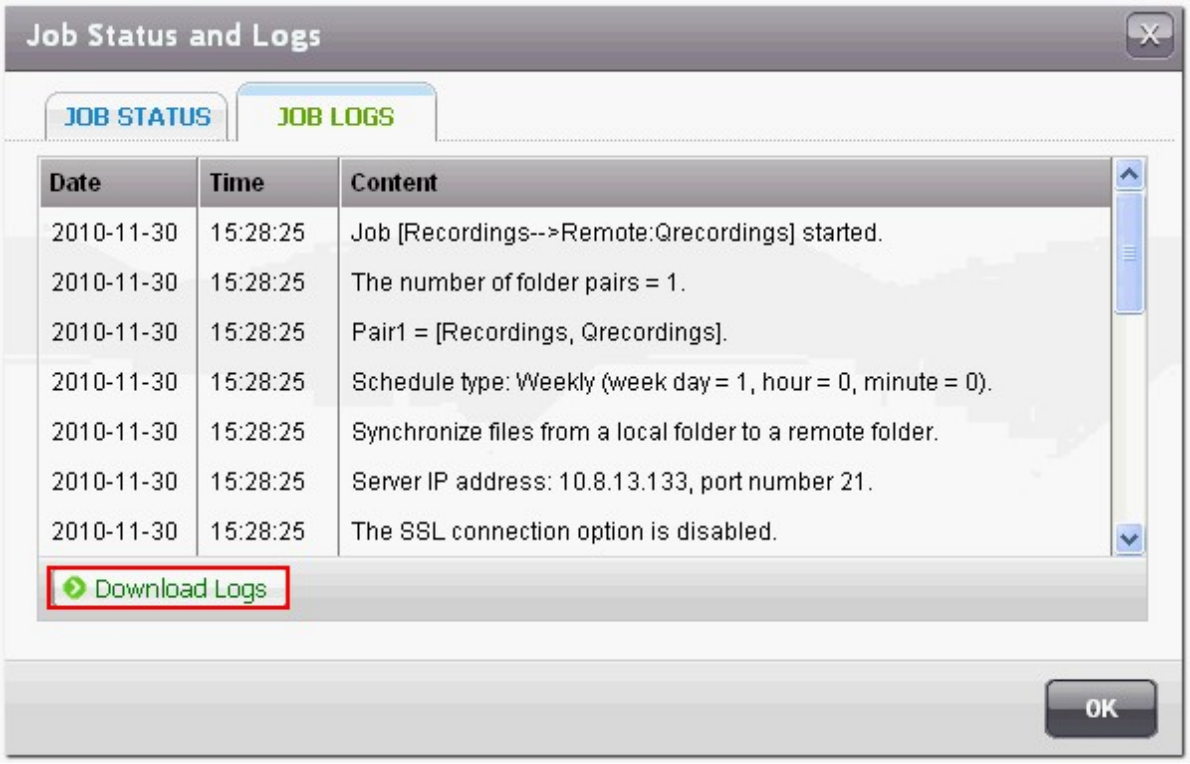
Download replication job logs:

To view the status and logs of a replication job, click .

You can view the details of a replication job.



You can view the job logs or download the logs by clicking "Download Logs". The log file can be opened by Microsoft Excel or other text editor software. Note that this button is only available after you have enabled "Download Detailed Logs" in "Options" > "Event Logs" and executed the replication job once.

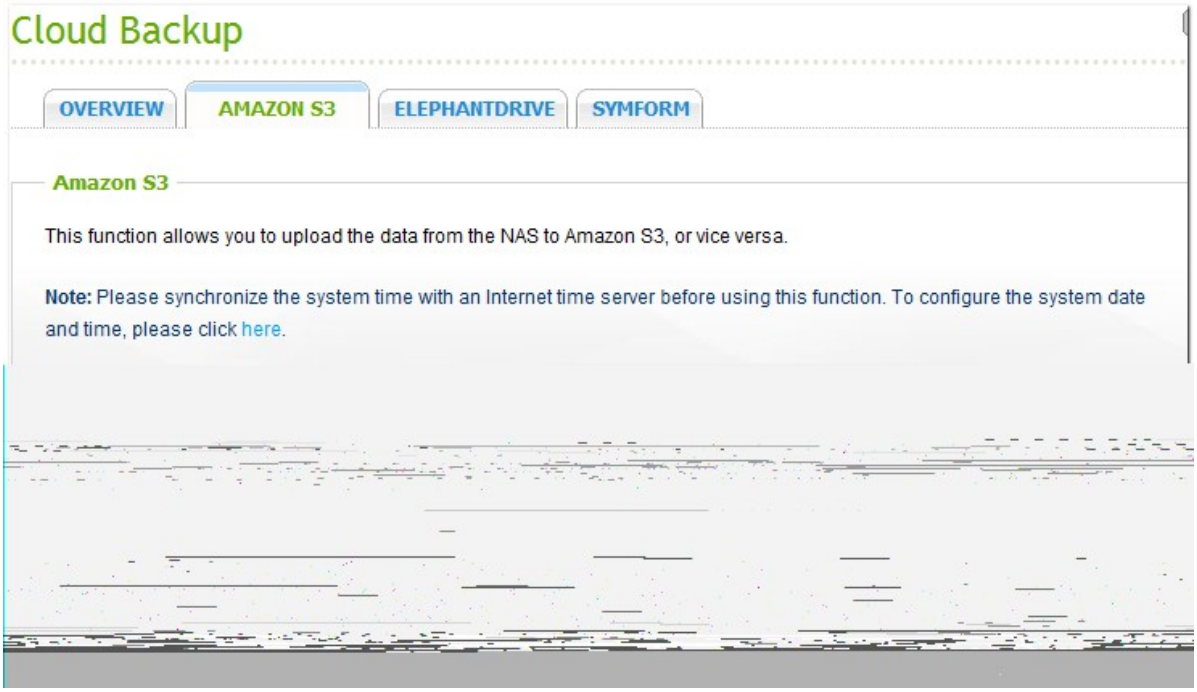


8.2 Cloud Backup

Amazon S3

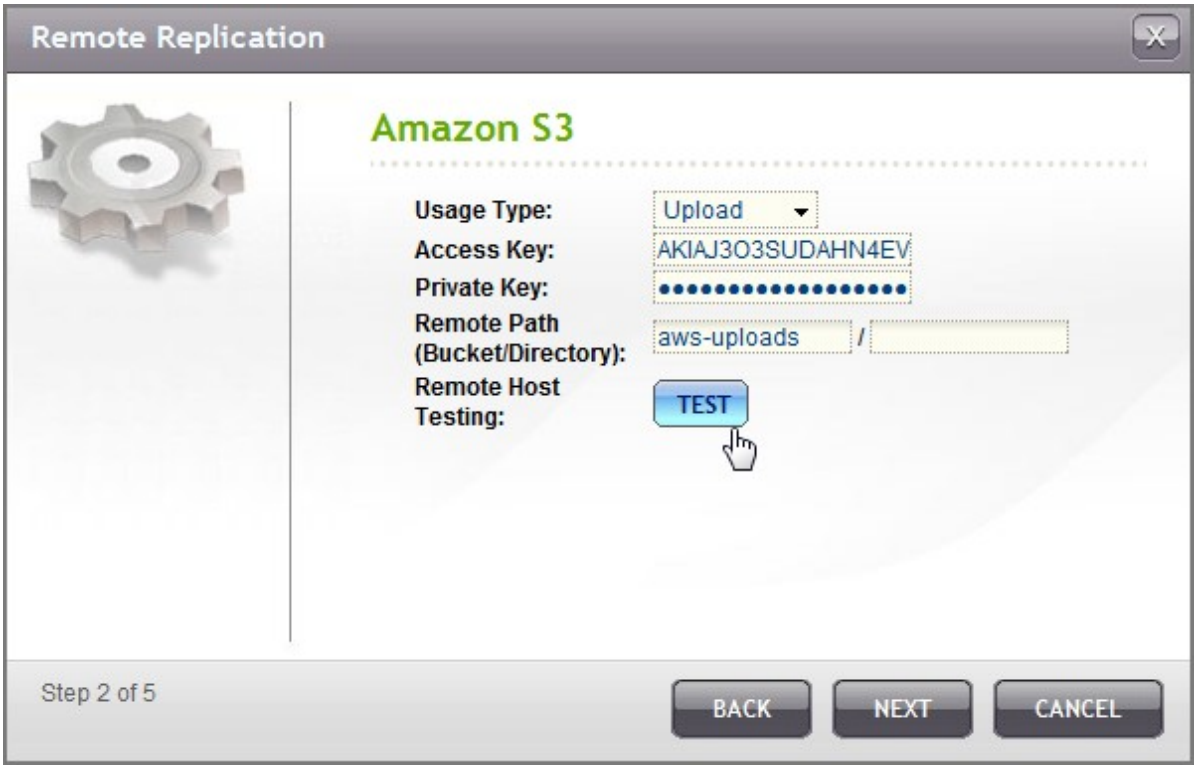
Amazon S3 (Simple Storage Service) is an online storage web service offered by AWS (Amazon Web Services). It provides a simple web services interface that can be used to store and retrieve the data from anywhere on the web. With Amazon S3, you can upload the data from your NAS to Amazon S3 or download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

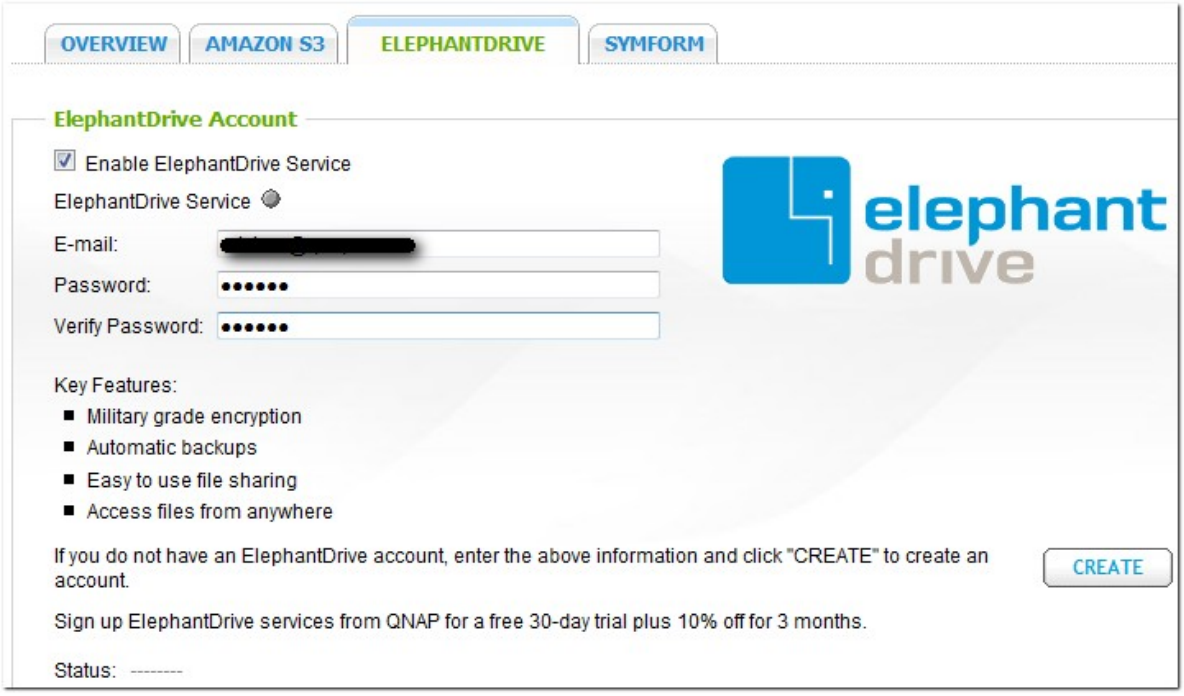
1. Click "Create a Replication Job".
2. Enter the remote replication job name.
3. Select the usage type: "Upload" or "Download" and enter other settings. A bucket is the root directory on Amazon S3. You can test the connection to the remote host testing by clicking "TEST". Other settings are optional.



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.

ElephantDrive

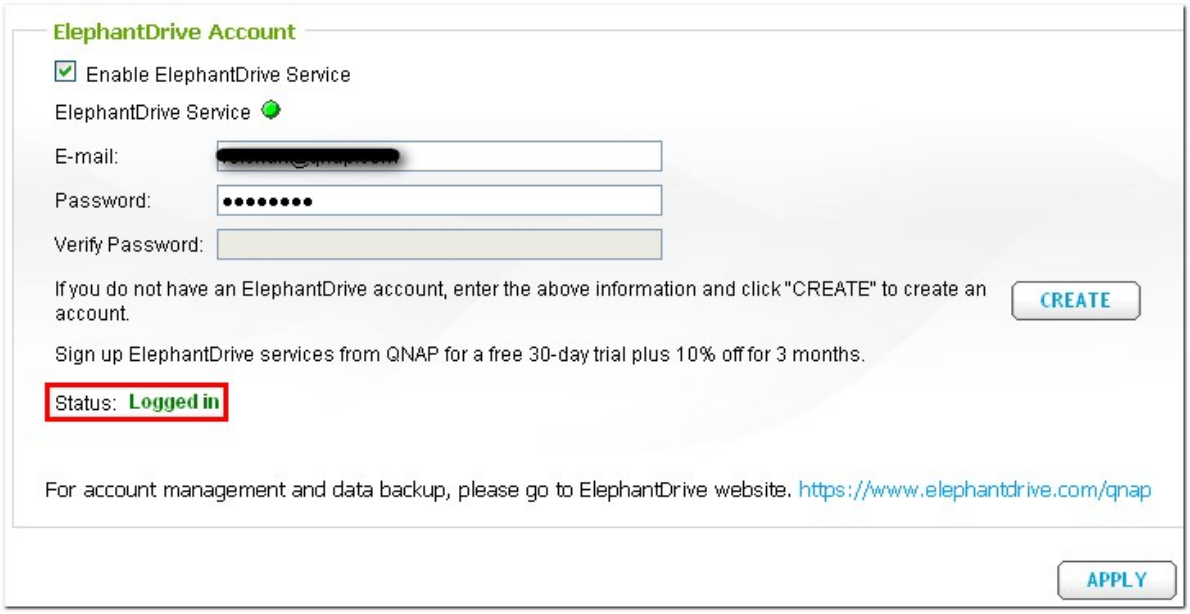
To use ElephantDrive Service, select "Enable ElephantDrive Service". Enter your email and password for the ElephantDrive service. If you do not have an account, enter the information and click "Create".



Click "OK" to confirm.

After creating an account, click “Apply”. The NAS will help you login the ElephantDrive service.

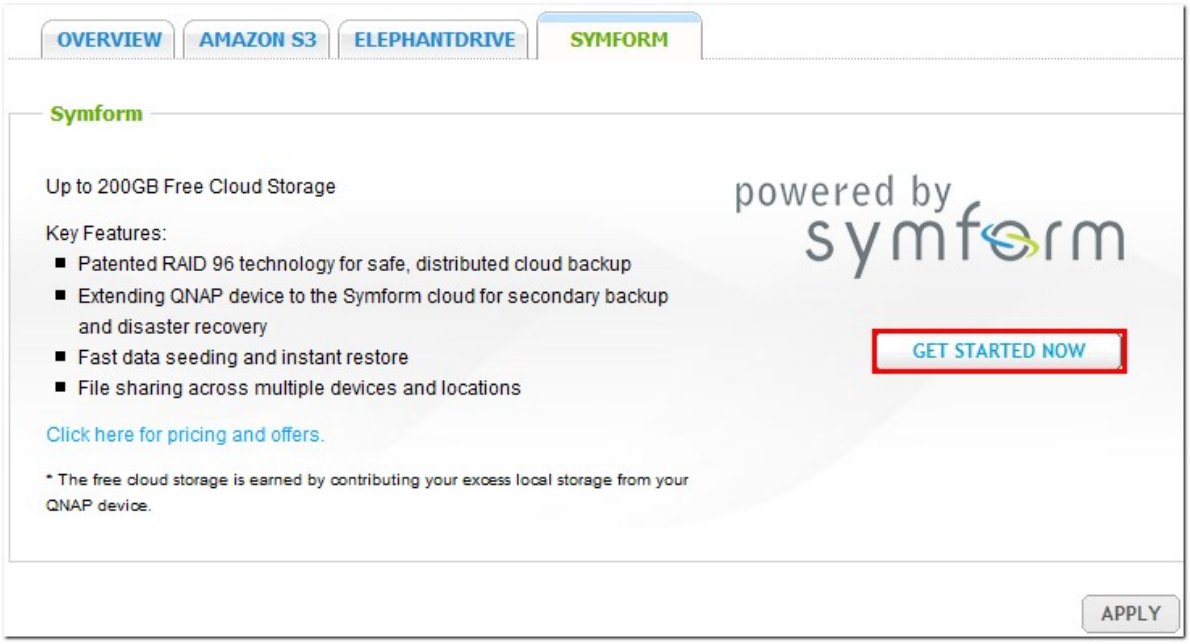
After you have logged in ElephantDrive service on the NAS, you can go to ElephantDrive website (http://www.elephantdrive.com/qnap) and manage the backup.



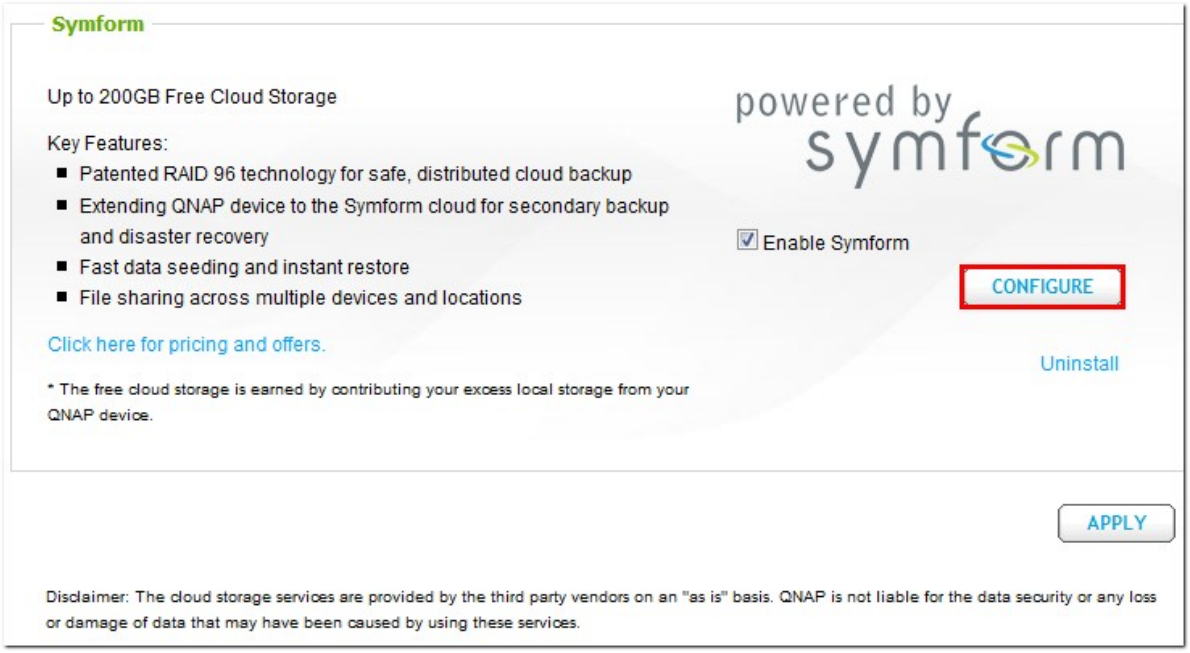
Login your ElephantDrive account. You can manage the backup and restore jobs on the website (https://www.elephantdrive.com/qnap).

Symform

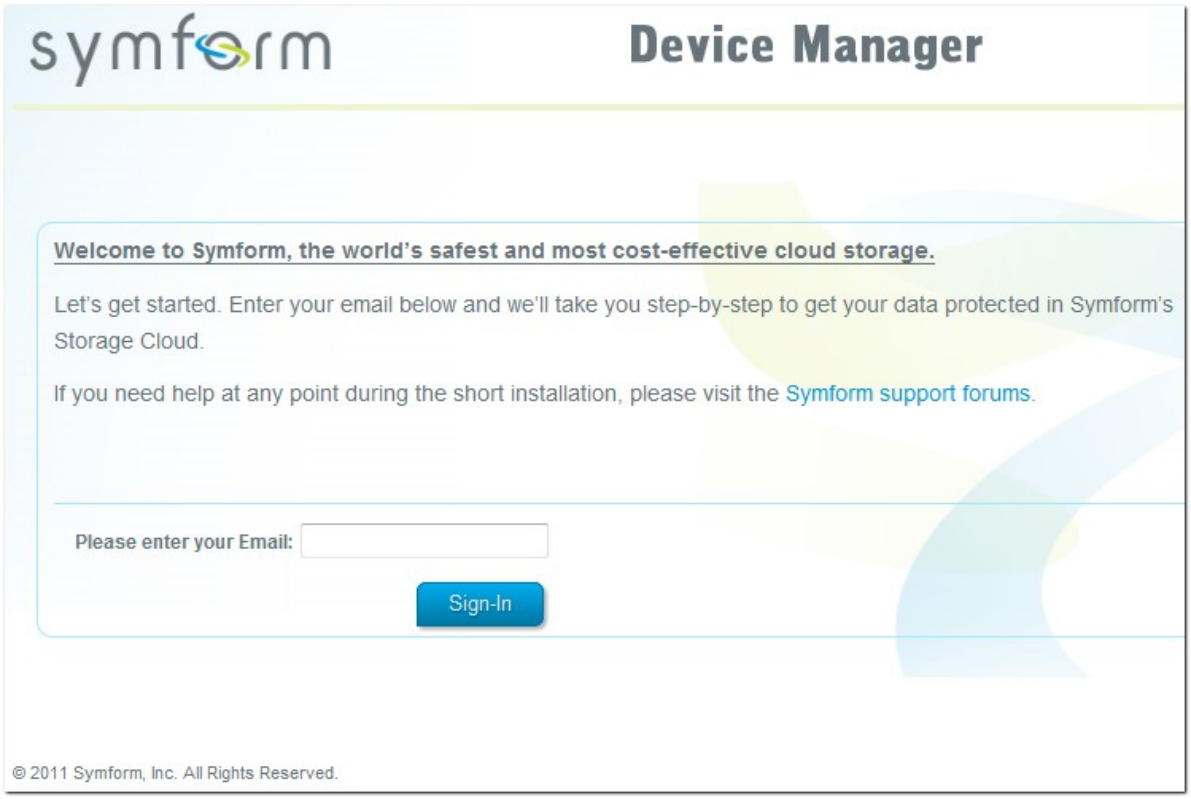
To use Symform cloud backup, go to "Backup > Cloud Backup > Symform". Click "Get Started Now" to install Symform. The NAS will download, verify, and install the package automatically.



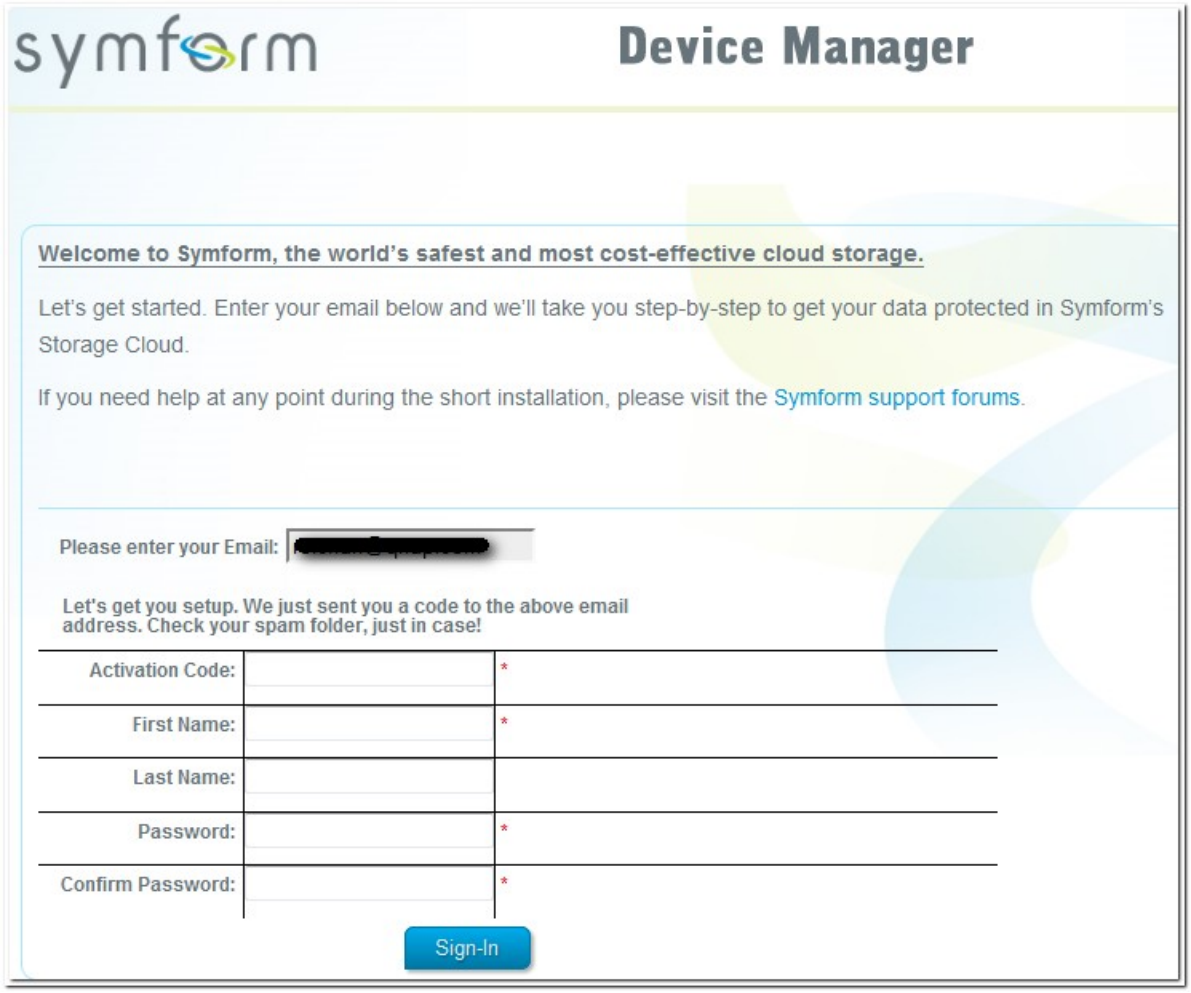
Click "Configure".



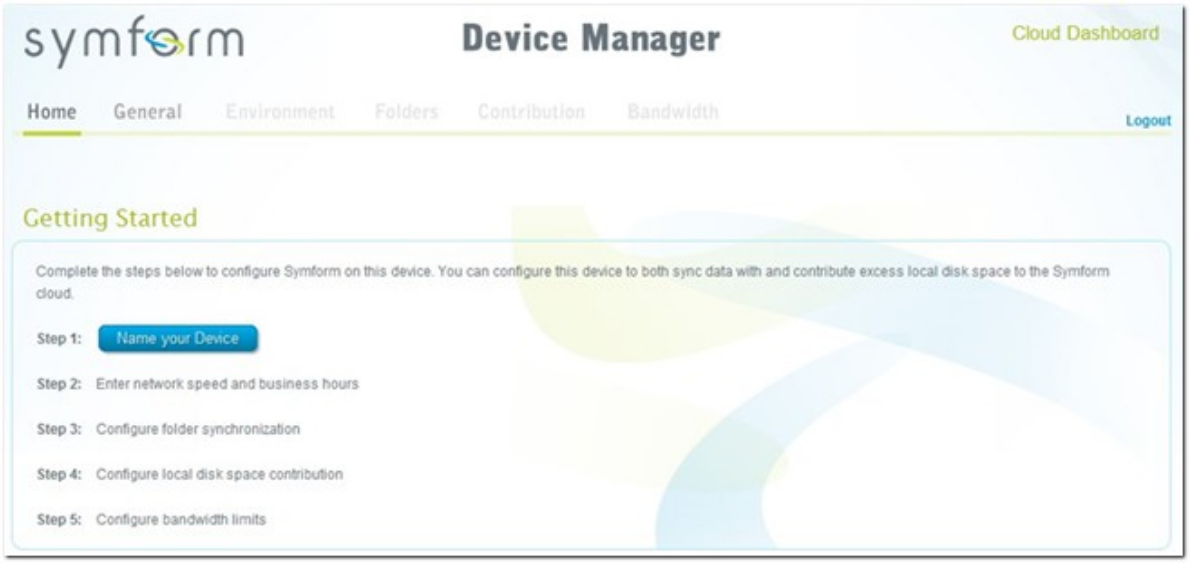
Enter your email address and click "Sign-In" to activate Symform on the NAS. An activation code will be sent to this address.



Check your email to get the activation code and finish the setup.


symform
Device Manager
Welcome to Symform, the world's safest and most cost-effective cloud storage.
Let's get started. Enter your email below and we'll take you step-by-step to get your data protected in Symform's Storage Cloud.
If you need help at any point during the short installation, please visit the Symform support forums.
Please enter your Email:
Let's get you setup. We just sent you a code to the above email address. Check your spam folder, just in case!
Activation Code:
First Name:
Last Name:
Password:
Confirm Password:
Sign-In

Configure Symform according to the instructions.



When done, the folders chosen during the setup will be backed up to Symform Storage Cloud.

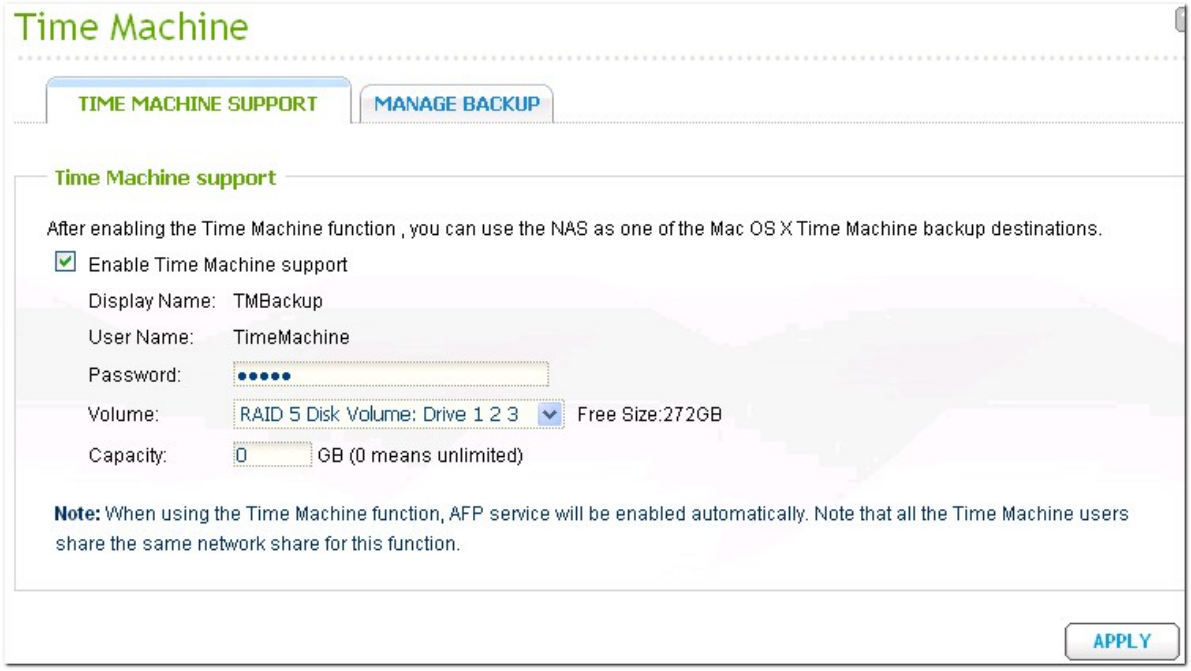
After Symform is activated, you will be able to see the device configuration. Click "Cloud Dashboard" to have access to Symform Cloud Dashboard and check the status of all the devices that are running Symform Storage Cloud.

Note about Symform service:

- Web administration interface TCP port: 59234
- Contribution TCP port: Defined randomly during Symform setup and can be changed if necessary.
- All TCP outbound ports are mandatory.
- The hard drive standby function of the NAS may not work when contribution is in use, because Symform service always reads and writes data on the hard drives.
- Symform with contribution requires network bandwidth. If contribution is enabled, there will always be communication between the NAS and Symform Cloud. This may cause network utilization and the bandwidth can be limited as needed.

8.3 Time Machine

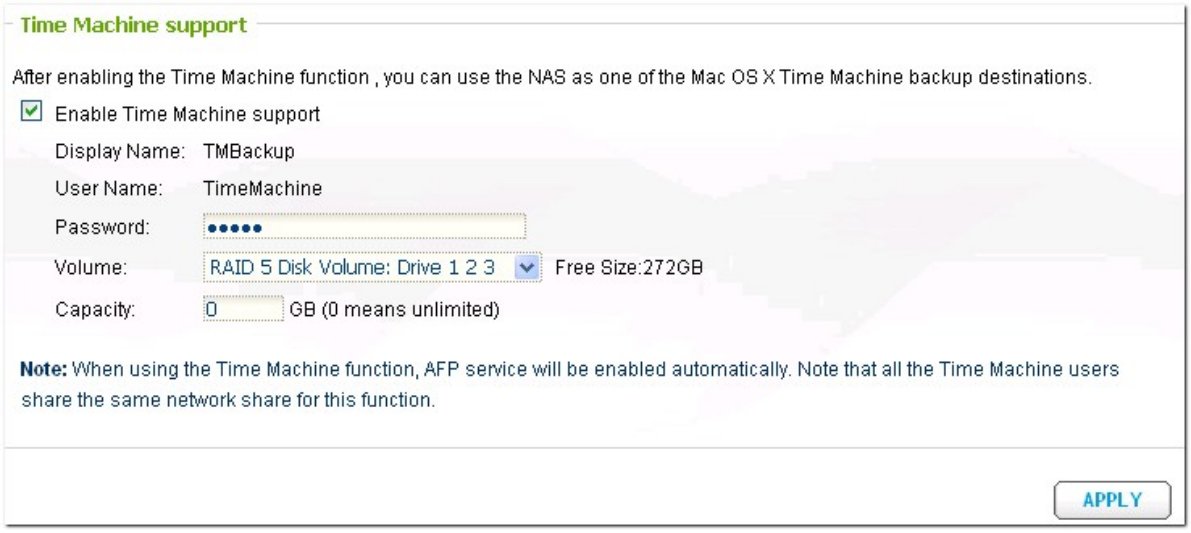
You can enable Time Machine support to use the NAS as a backup destination of multiple Mac by the Time Machine feature on OS X.



To use this function, follow the steps below.

Configure the settings on the NAS:

1. Enable Time Machine support.



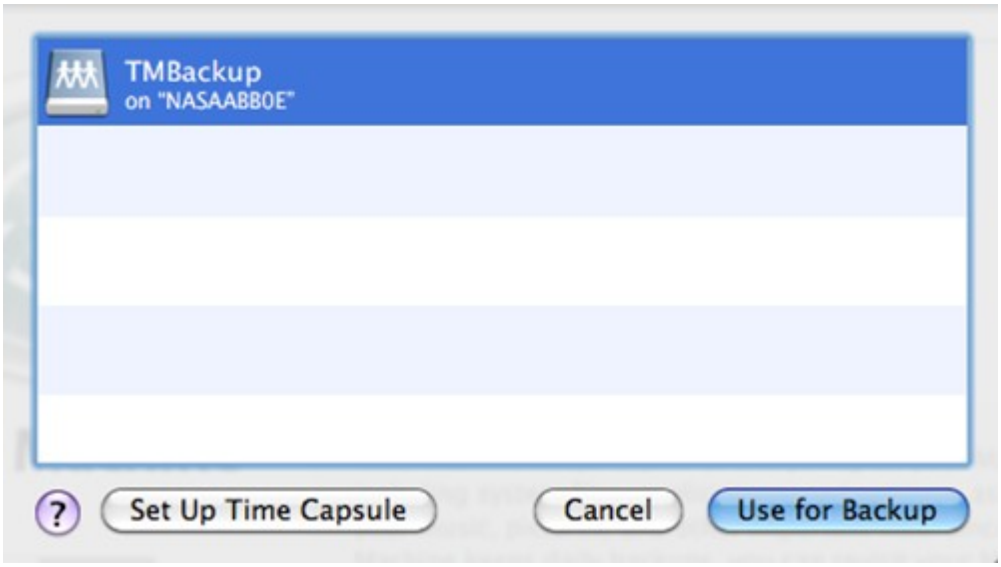
2. Enter the Time Machine password. The password is empty by default.
3. Select a volume on the NAS as the backup destination.
4. Enter the storage capacity that Time Machine backup is allowed to use. The maximum value is 4095GB. To specify a larger capacity, please enter 0 (unlimited).
5. Click "Apply" 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”.

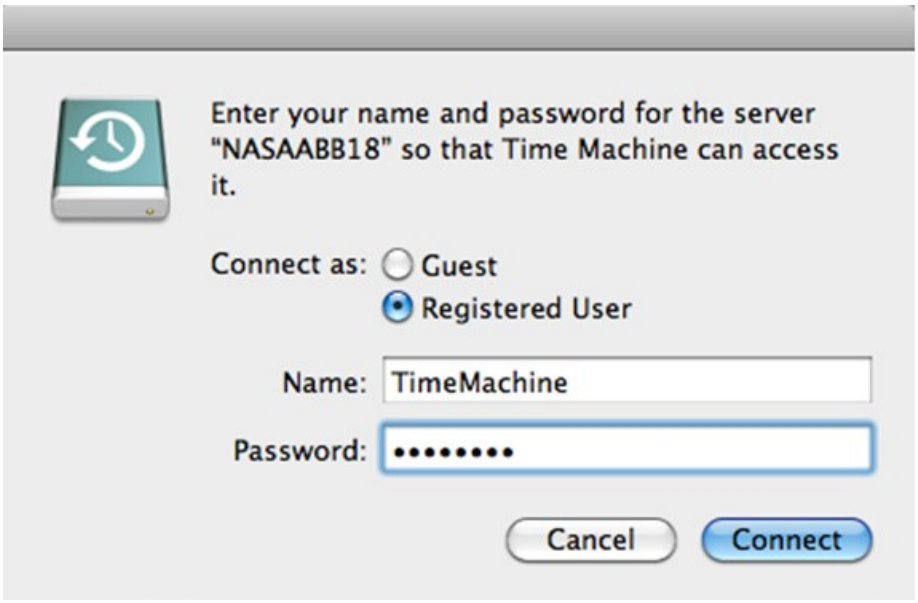
2. Select the TMBackup on your NAS from the list and click “Use for Backup”.



3. Enter the user name and password to login the QNAP NAS. Then click "Connect".

Registered user name: TimeMachine

Password: The password you have configured on the NAS. It is empty by default.

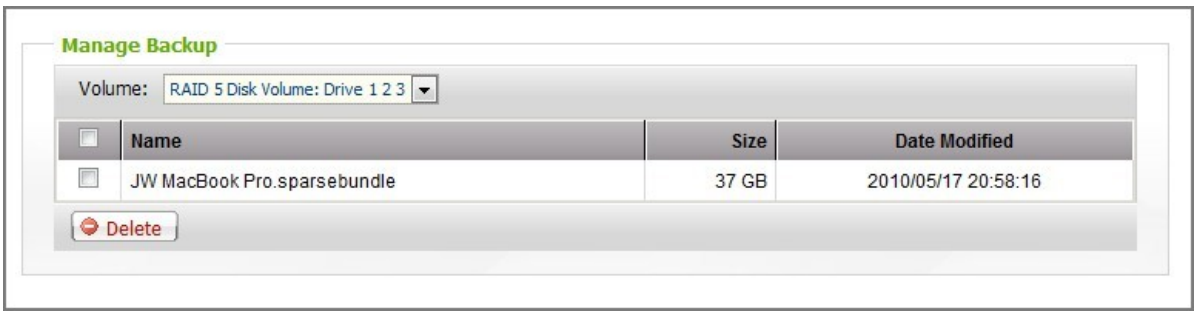


4. Upon successful connection, the Time Machine is switched "ON". The available space for backup is shown and the backup will start in 120 seconds.

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

Manage Backup

You can manage the existing backup on this page.



Volume: Display Time Machine backup tasks stored in the volume.
Name: The name of the Time Machine backup (the sparse bundle disk image which was created by Time Machine).
Size: Size of this Time Machine backup.
Date Modified: Last modified date of this Time Machine backup.
Delete: Delete the selected Time Machine backup.

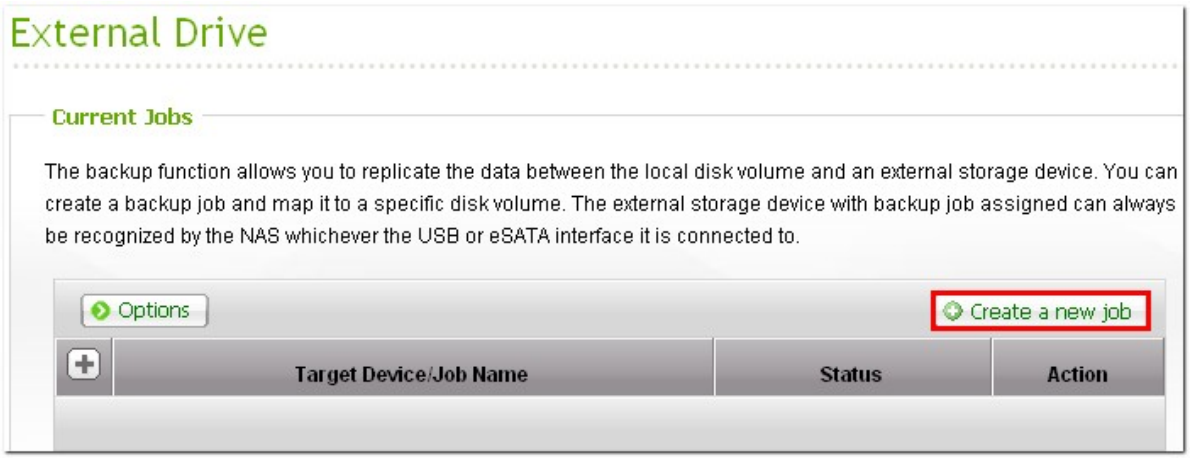
8.4 External Drive

The NAS supports real-time and scheduled data backup between the internal disks volumes on the NAS and external USB/eSATA storage devices. To use this feature, follow the steps below.

Note: If an external storage device is encrypted by the NAS, make sure it is unlocked in "External Device" > "External Storage Device" before creating any backup jobs.

1. Connect one or more external storage devices to the USB or eSATA (if available) interfaces of the NAS.

2. Click "Create a new job".



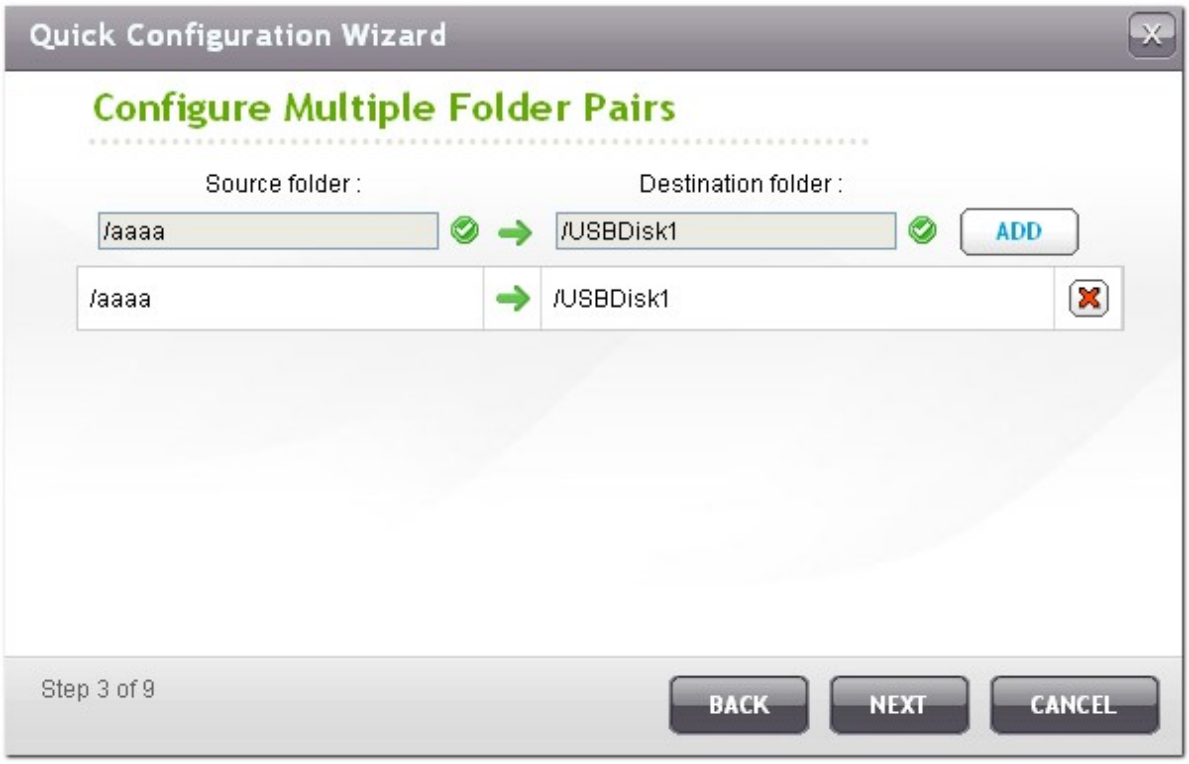
3. When the wizard is shown, read the instructions carefully and click “Next”.

4. Select the backup locations.
   a. Select an external disk volume* from the drop-down menu. The NAS supports EXT3, EXT4, FAT, NTFS, and HFS+ file systems. The general information of the storage device will be shown.
   b. Select "Map this backup job to the volume ID only" to map the backup job to this particular external storage device. The NAS will recognize the device and execute the backup job according to the settings automatically every time it is connected to the NAS via any USB/ eSATA interface.
   c. Select to back up the data from local disk volume to the external storage or vice versa.
   d. Click "Next".

*Multiple partitions on the external storage device will be recognized as individual disk volumes.

5. Select the source and destination folders for backup. Then click "Add". Up to 5 folder pairs can be created. Click "Next".

Note: If a folder or its parent folder or child folder has been selected as the source or destination in a folder pair of a backup job, the same folder cannot be selected as the source or destination of another folder pair of the same backup job.

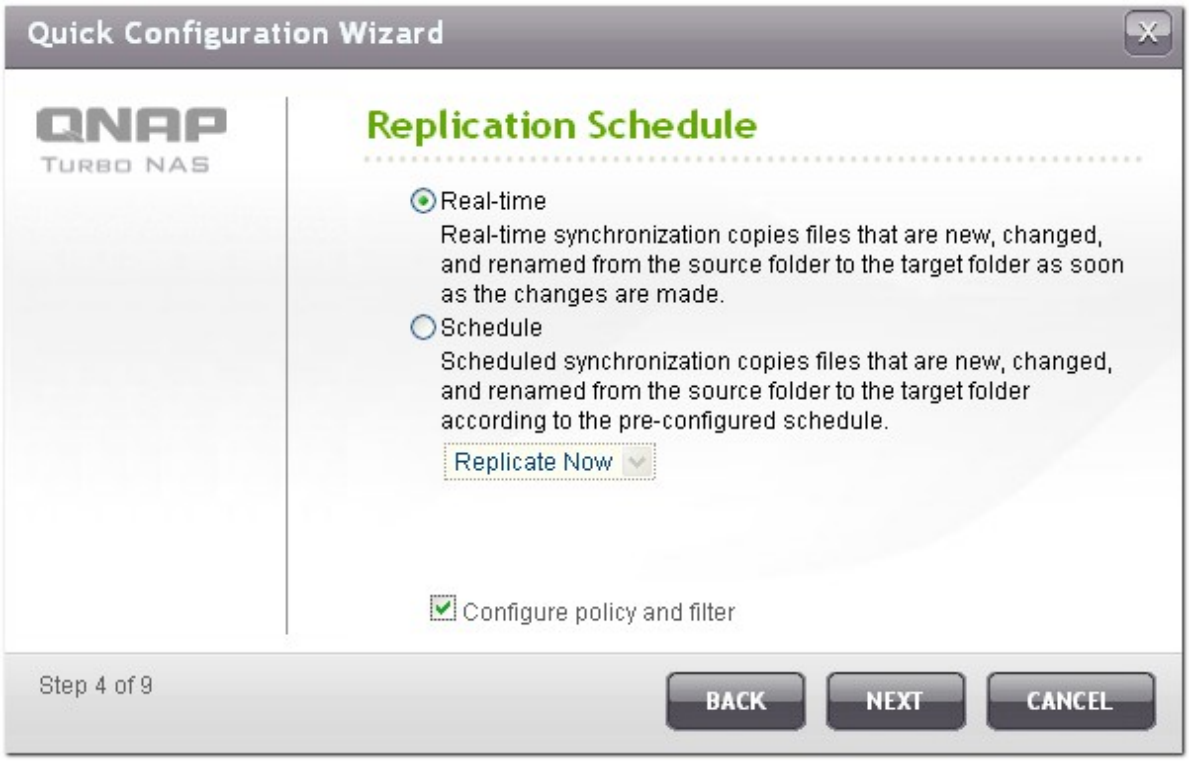


6. Choose between real-time and scheduled backup. Real-time backup copies files that are new, changed, and renamed from the source folder to the target folder as soon as the changes are made after the first-time backup.

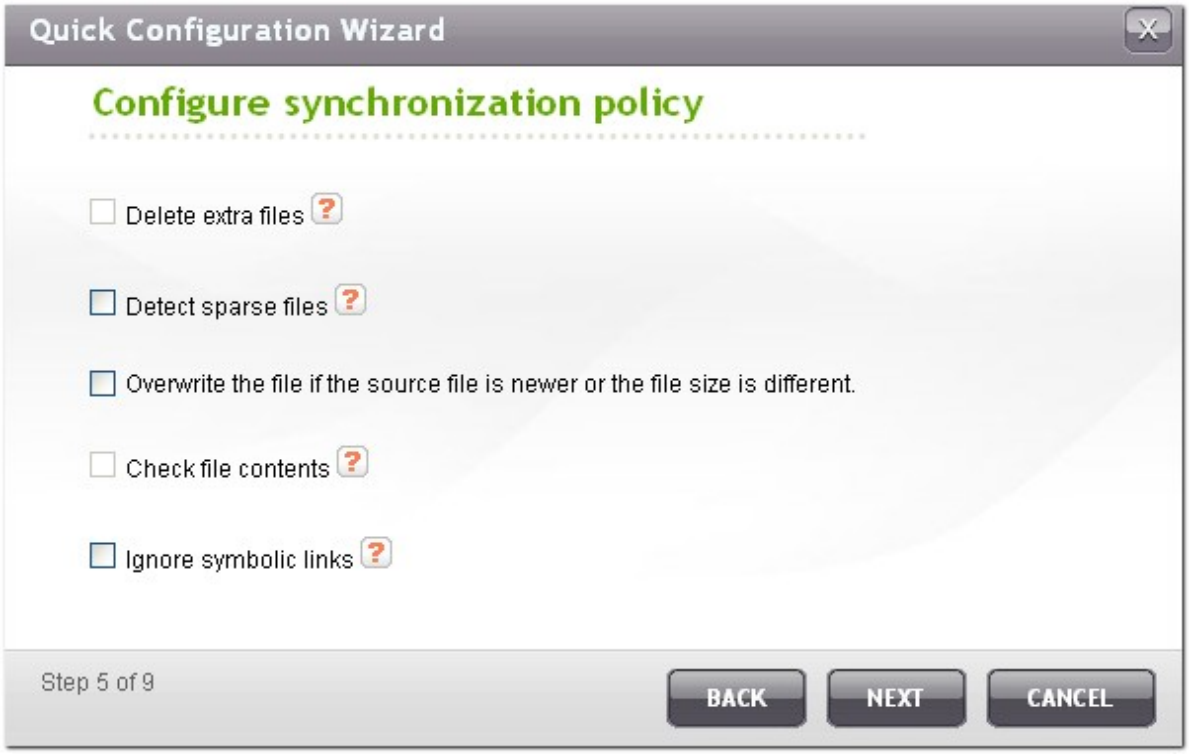
   Scheduled backup copies files from the source folder to the target folder according to the schedule. The options are:

   - Replicate Now: Copy the data immediately.
   - Periodically: Enter the time interval in hour and minute that the backup job should be executed. The minimum time interval is 5 minutes.
   - Hourly: Select the minute when an hourly backup should be executed, e.g. select 01 to execute the backup job every first minute of an hour, 1:01, 2:01, 3:01...
   - Daily: Specify the time when a daily backup should be executed, e.g. 02:02 every day.
   - Weekly: Select a day of the week and the time when a weekly backup should be executed.
   - Monthly: Select a day of the month and the time when a monthly backup should be executed.
   - Auto-Backup: Execute data backup automatically every time the device is connected and detected by the NAS.

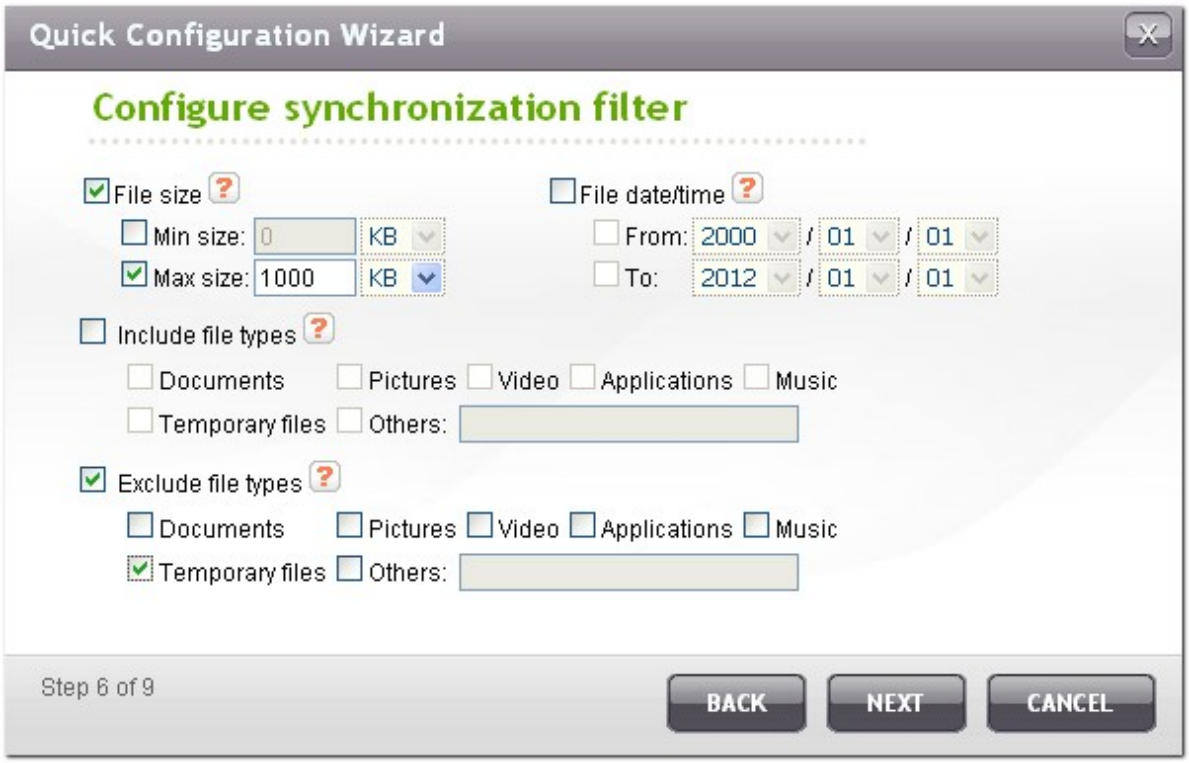
To configure the backup policy and filter settings, select "Configure policy and filter". Click "Next".



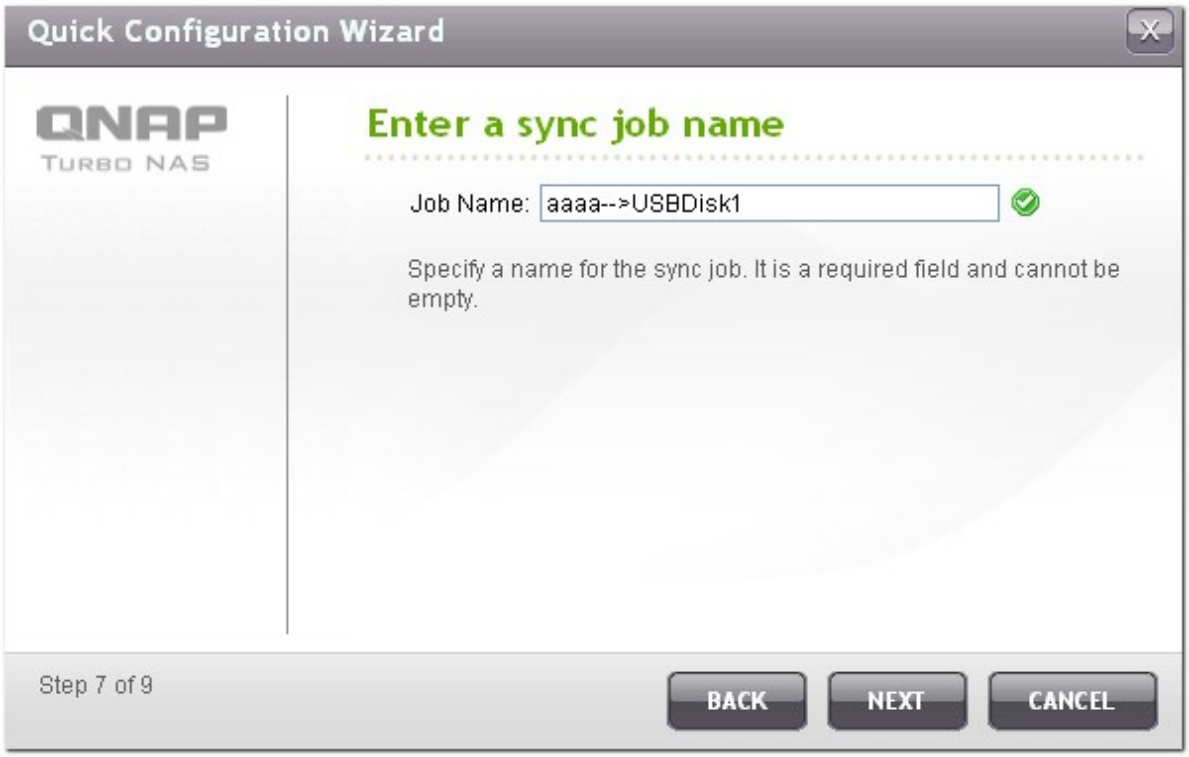
7. Select whether or not to enable the following options:
   - Delete extra files: Delete extra files in the target folder. Deletions made on the source folder will be repeated on the target folder. This option is not available for real-time data backup.
   - Detect sparse files: Select this option to ignore files of null data.
   - Overwrite the file if the source file is newer or the file size is different ·
   - Check file contents: Examine the file contents, date, size, and name to determine if two files are identical. This option is not available for real-time data backup.
   - Ignore symbolic links: Select this option to ignore symbolic links in the pair folder.



8. Create filters for the backup job.
   - File size: Specify the minimum and maximum size of the files to be copied.
   - File date/time: Specify the date and time of the files to be copied.
   - Include file types: Specify the file types to be copied.
   - Exclude file types: Specify the file types to be excluded for data copy.

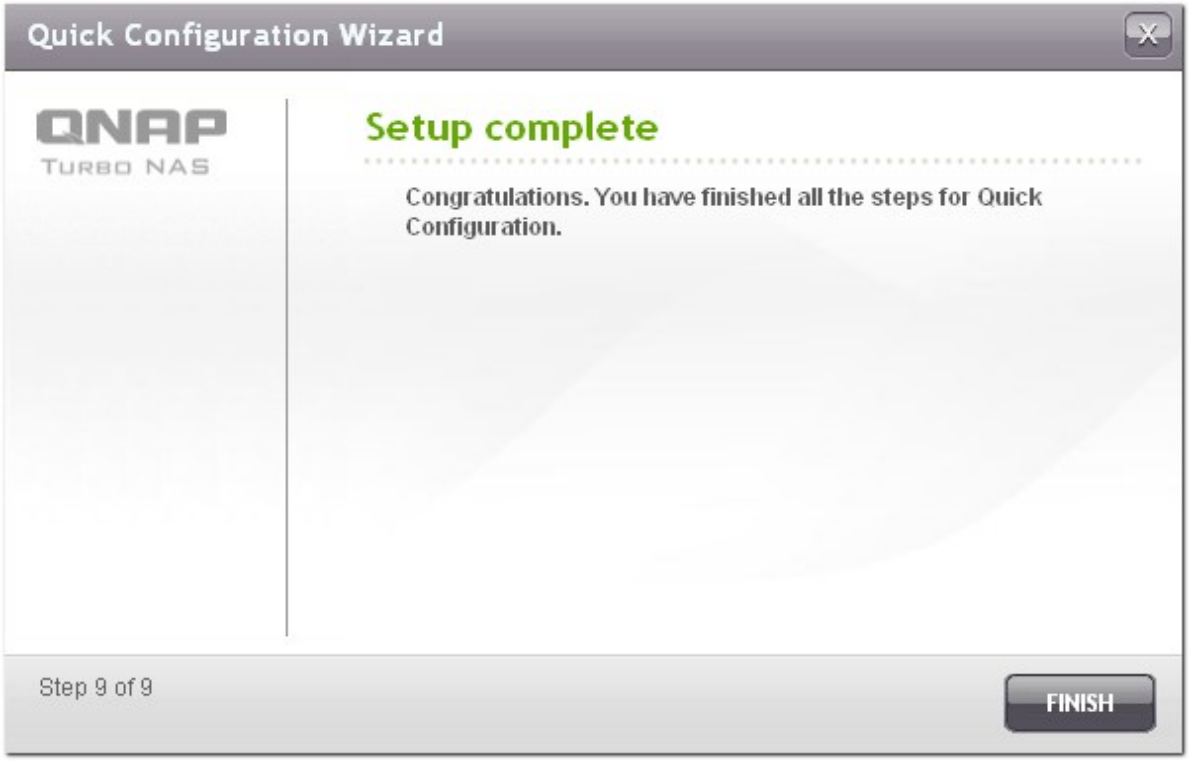


9. Enter a name for the backup job. A job name supports up to 63 characters; it cannot start or end with a space. Click "Next".

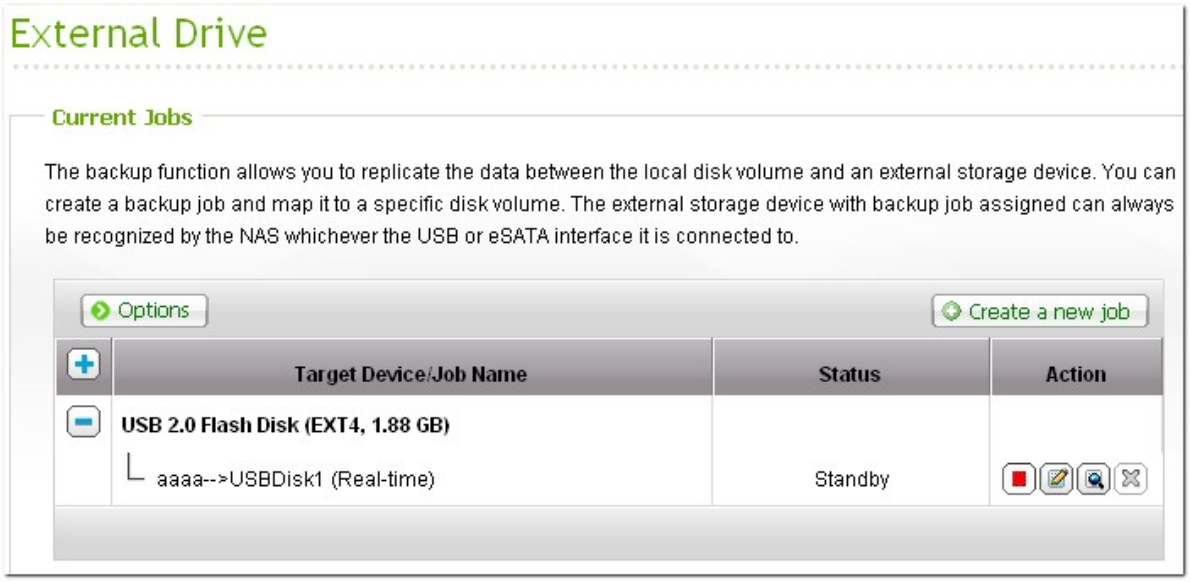


10. Confirm the settings and click "Next".

11. Click "Finish" to exit the wizard.

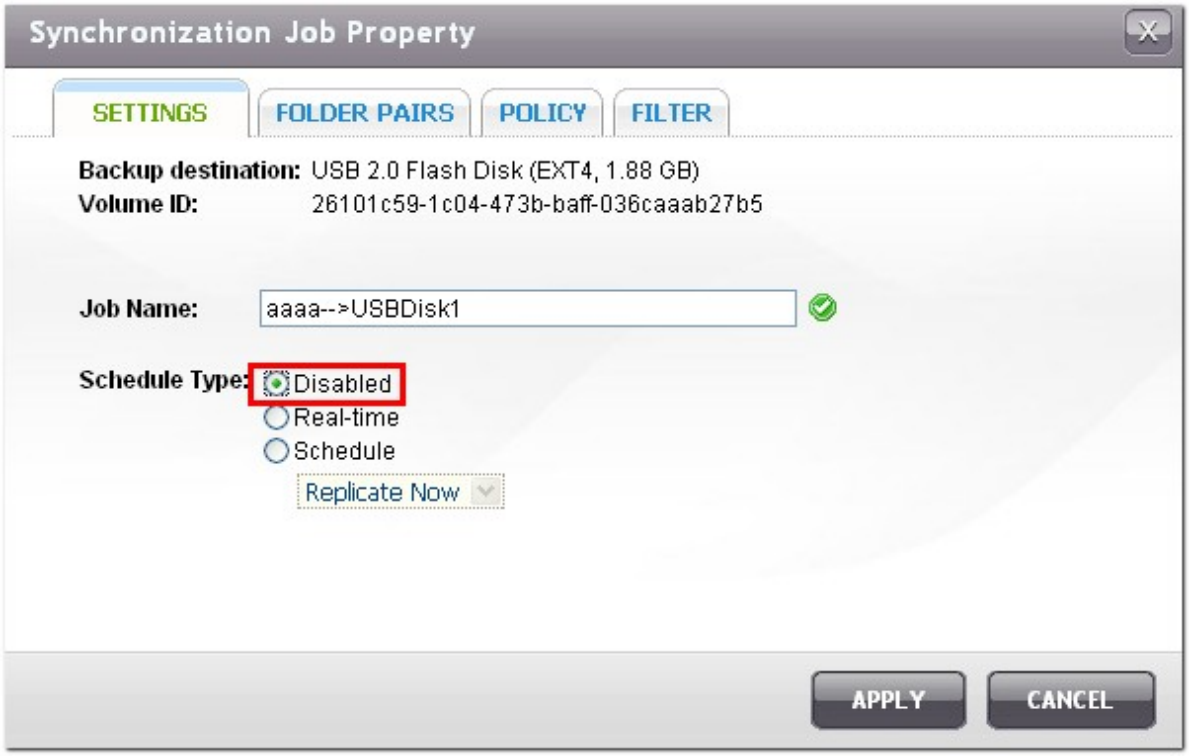


12. The backup job and the status will be shown on the list.



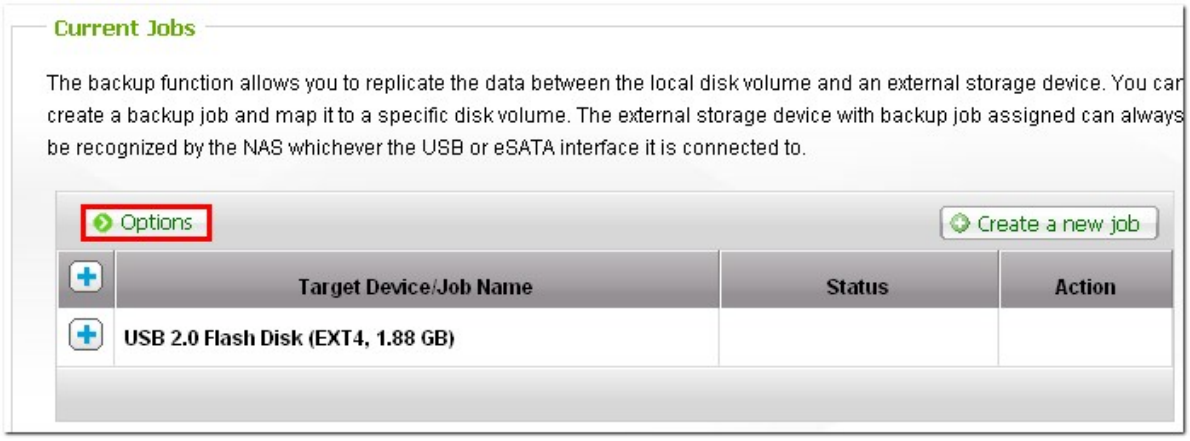
Button	Description
	Start a backup job.
	Stop a backup job.
	Edit the settings of a backup job.
	View the job status and logs. Download the logs of a backup job.
	Delete a backup job. This button is available only after a backup job is stopped.

To disable the backup schedule of a backup job, click and select "Disabled" under "Settings" > "Schedule Type" and click "Apply".

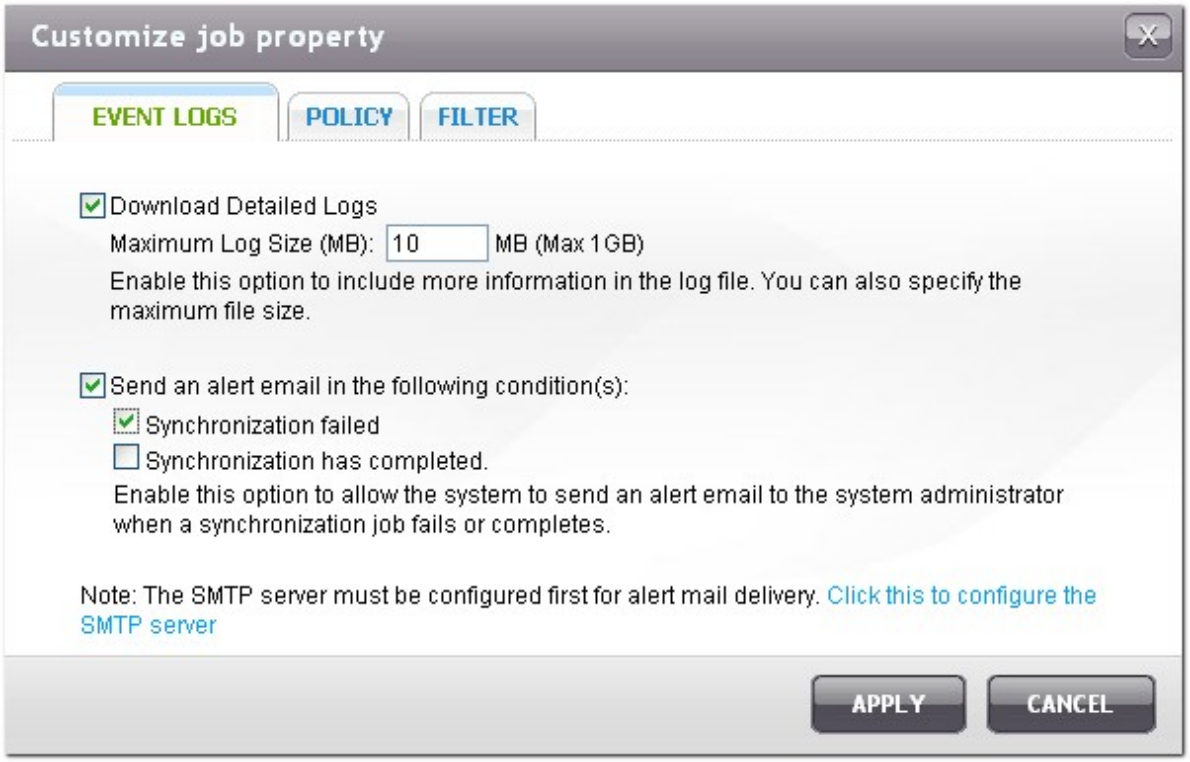


Default Backup Job Settings

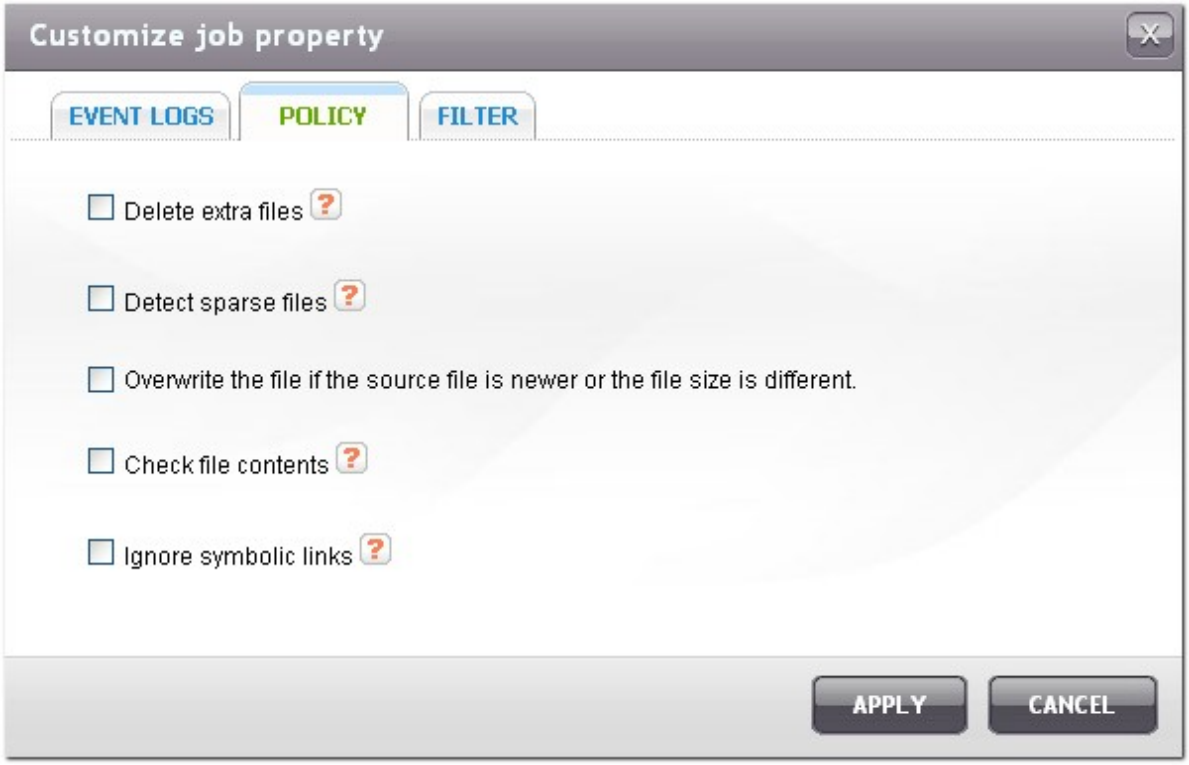
To edit the default backup job properties, click "Options".

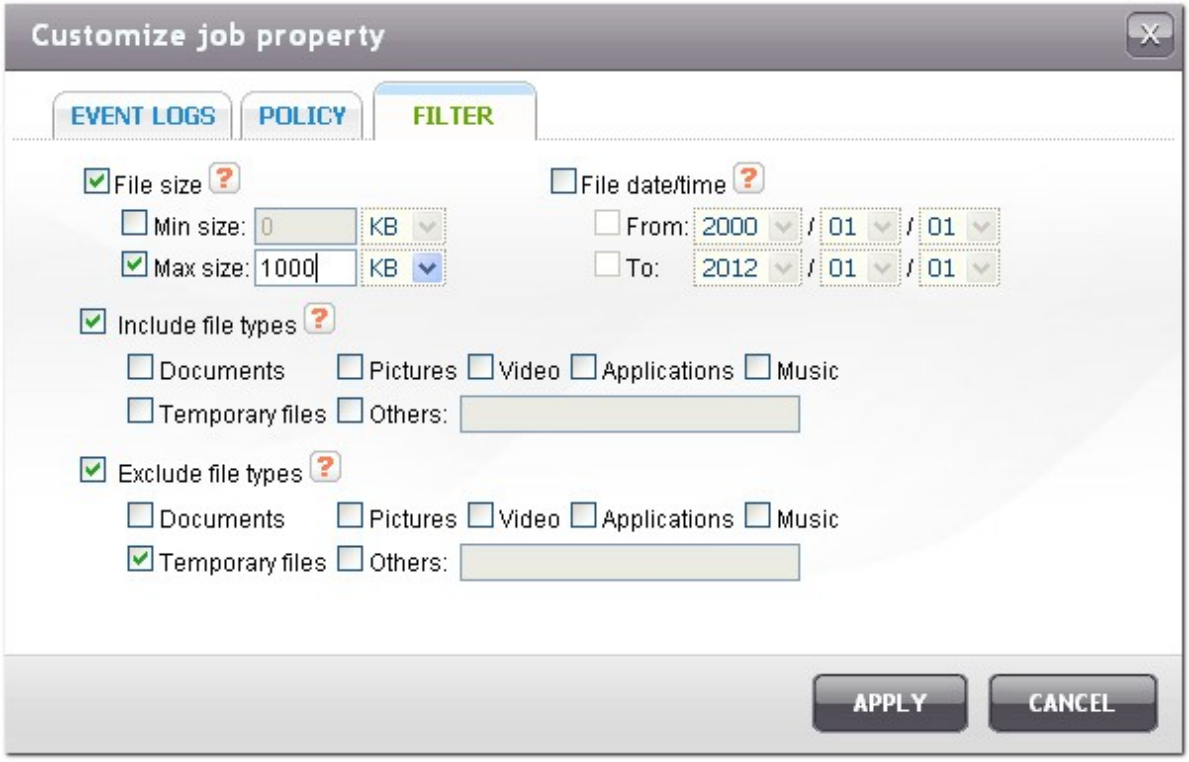


Under "Event Logs" you can select to enable "Download Detailed Logs" and specify the maximum file size of the log file. Select to send an email alert when a backup job fails or completes. Note that the SMTP server settings must be properly set up in "System Administration" > "Notification".



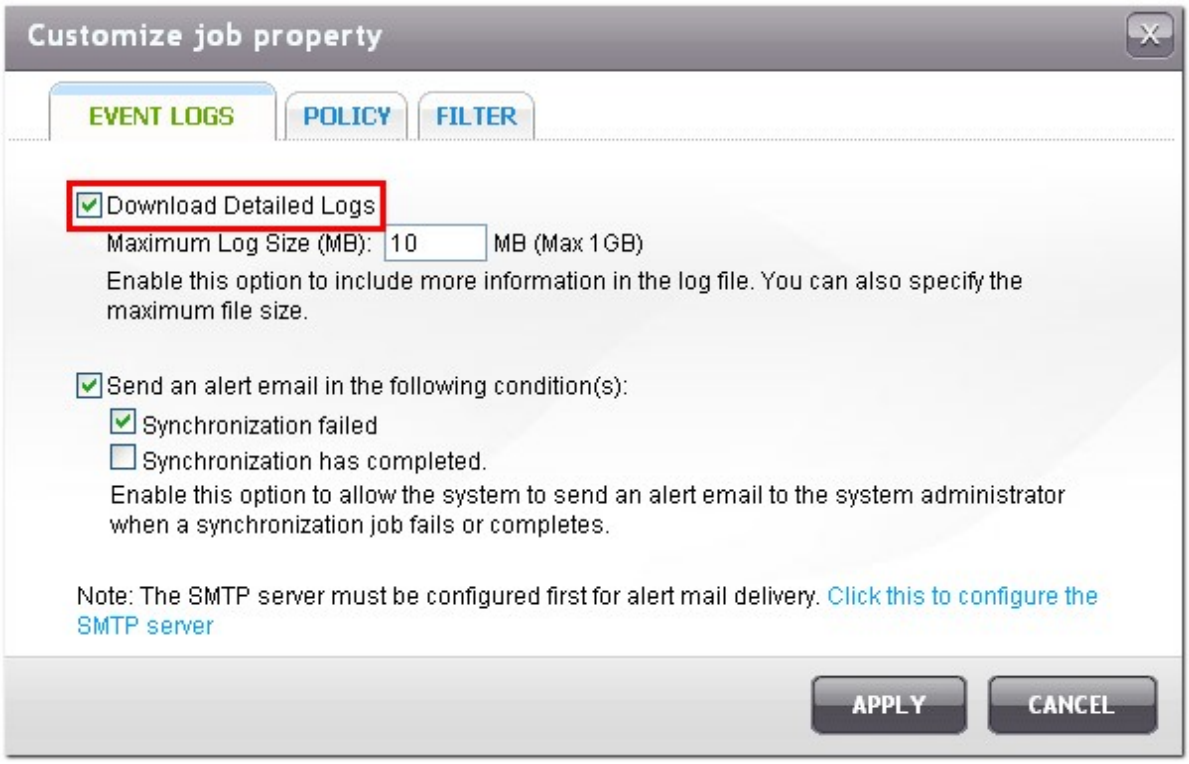
Specify the backup policy in “Policy” and filter settings in “Filter”. These will become the default settings for all the backup jobs.





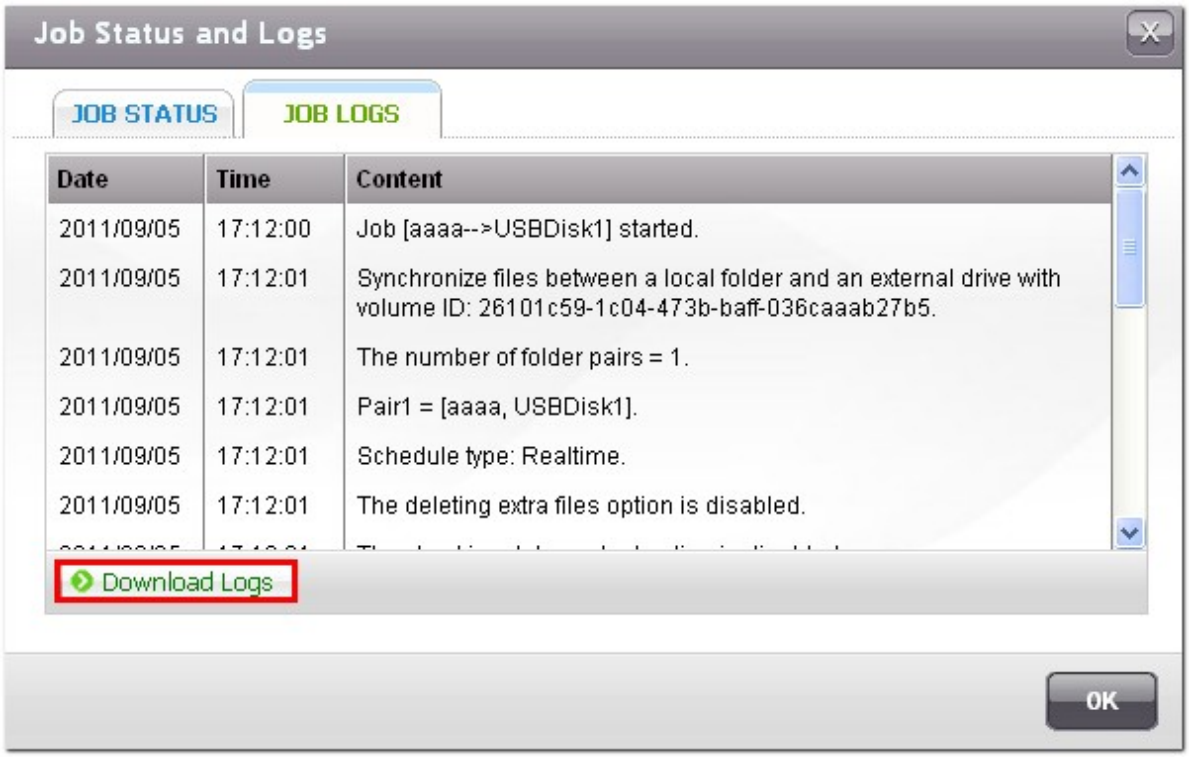
Download Backup Logs

1. To download the logs of a backup job, make sure the option "Download Detailed Logs" in "Options" > "Event Logs" has been enabled.



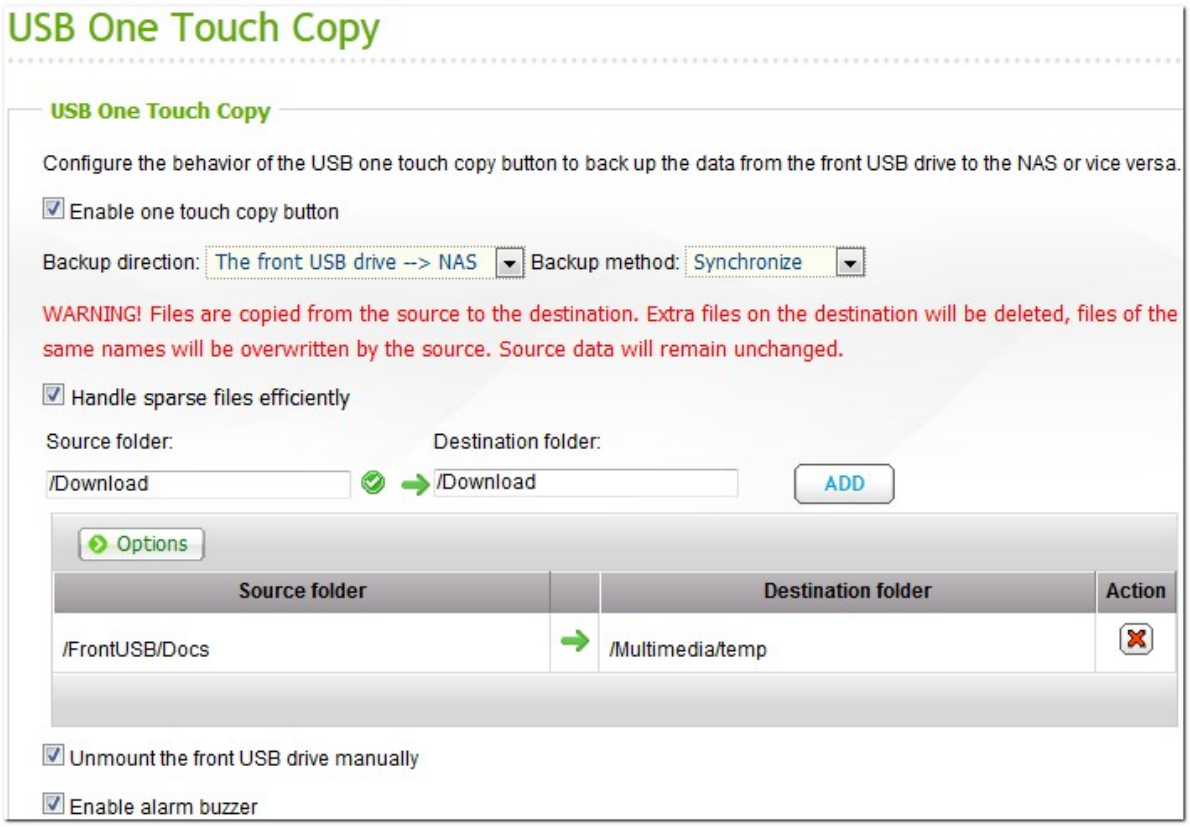
2. Click in "Action" column of a backup job.

3. Go to "Job Logs" and click "Download Logs". The log file can be opened by Microsoft Excel or any other text editor software. Note that this button is only available after you have enabled "Download Detailed Logs" in "Options" > "Event Logs" and executed the backup job once.



8.5 USB One Touch Copy

Enable the USB one touch copy button to back up data from the front USB drive to the NAS or vice versa. This feature is not supported by TS-809U-RP, TS-879U-RP, TS-EC879U-RP, TS-1279U-RP, TS-EC1279U-RP.



Backup direction: From the front USB drive to the NAS or vice versa.
Backup method:

- Create directory: A new directory will be created on the destination and the source data will be copied to this directory. The new directory will be named as the backup date (YYYYMMDD). If there are two or more backups on the same day, the directory will be named with YYYYMMDD-1, YYYYMMDD-2... and so on.
- Copy: Back up data to the destination share. If the same file exists, the destination file will be overwritten.
- Synchronize: Back up data to the destination share and clear the redundant files. If the same file exists, the destination file will be overwritten.

Note: If there are multiple partitions on the source storage device, a new folder will be created for each partition on the destination as the backup folder. The backup folder will be named with the backup date and the partition number, *YYYYMMDD*-1 for partition 1, *YYYYMMDD*-2 for partition 2... and so on. If the source storage device contains only one partition, the backup folder will be named as *YYYYMMDD* only.

Handle sparse files efficiently: A sparse file is a type of computer file that contains large blocks of zero-byte data. Turn on this option may reduce the time required for backup.
Source and destination folders: Specify the folder pairs for backup and click "Add". Maximum 9 folder pairs can be added.
Options: Click "Options" to set up notification of the backup jobs by email, SMS, or instant messaging (IM).
Unmount the front USB drive manually: When enabled, users can press the Copy button for about 8–10 seconds until the USB LED light turns off and remove the front USB drive from the NAS.
Enable the alarm buzzer:

- One short beep: Backup has started.
- Two short beeps: The front USB drive is being unmounted.

Data copy by 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 has been created.
2. Turn on the NAS.
3. Configure the behaviour of the Copy button on "Backup" > "USB one touch copy" page.
4. Connect the USB device, for example, 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.

Caution: Files are copied from the source to the destination. Extra files on the destination will be deleted; files of the same names will be overwritten by the source. Source data will remain unchanged.

9. External Device

External Storage Device 572
USB Printer 582
UPS Settings 612

9.1 External Storage Device

The NAS supports external USB and eSATA storage devices* for storage expansion. Connect the external storage device to a USB or an eSATA interface of the NAS, when the device is successfully detected, the details will be shown on this page.

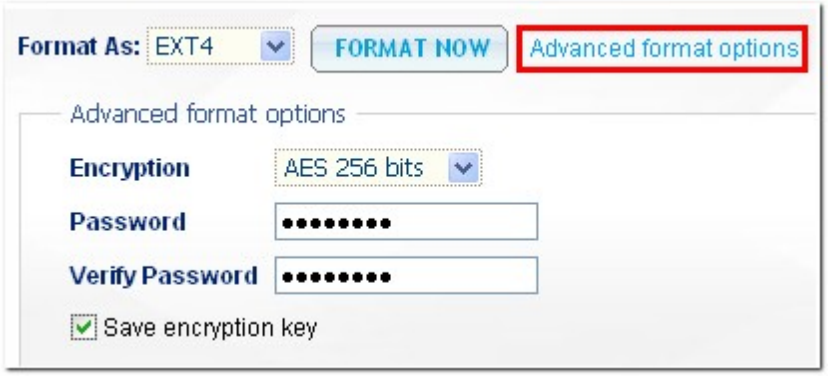
*The number of USB and eSATA interfaces supported varies by models. Please refer to http://www.qnap.com for details.

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

The external storage device can be formatted as FAT32, NTFS, EXT3, or HFS+ (Mac only) file system. Select the option from the drop-down menu next to "Format As".

Advanced format options:

The NAS supports external drive encryption. To encrypt an external storage device, click "Advanced format options". Select the encryption method: AES 128-, 192- or 256-bit and enter the password (8-16 characters). Select "Save encryption key" to save the password in a hidden location on a hard drive of the NAS. The NAS will unlock the encrypted external storage device automatically every time the device is connected.



Click "Format Now". All the data will be cleared. The device will be "Ready" after disk initialization.

Encryption management

If an external storage device is encrypted by the NAS, the button "Encryption Management" will appear. Click this button to manage the encryption password/key, or lock or unlock the device.

Lock the device

Note: The external storage device cannot be locked if a real-time or scheduled backup job is running on the device. To disable the backup job, go to "Backup" > "External Drive".

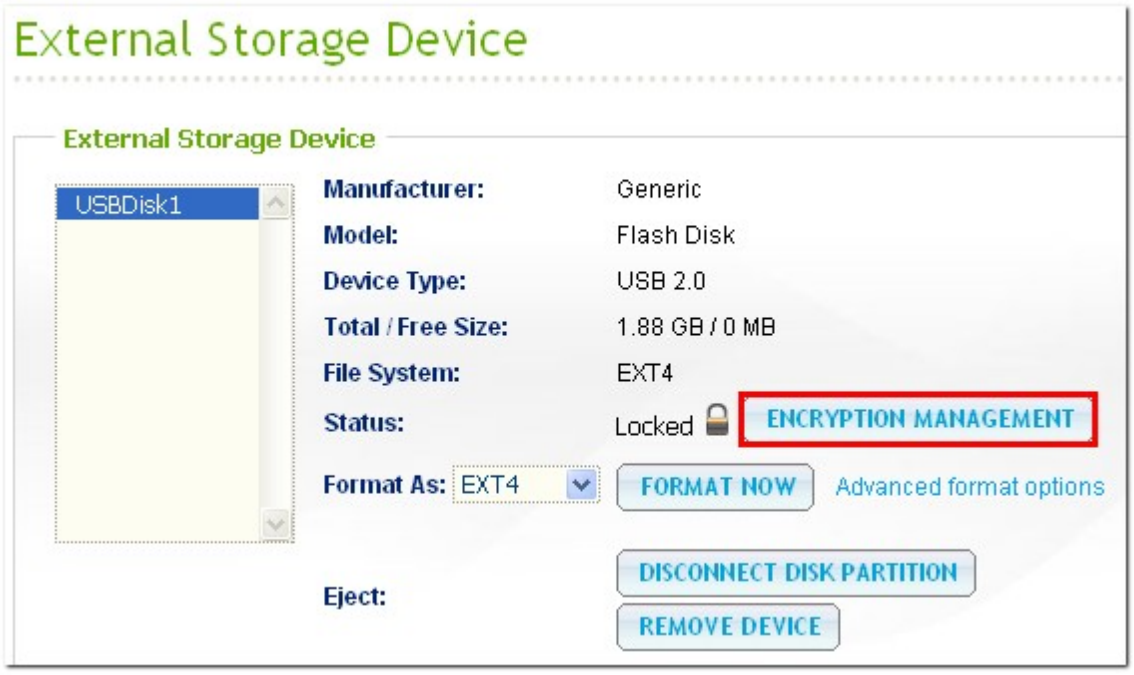
1. To lock an encrypted external storage device, click "Encryption Management".

2. Select "Lock this device" and click "Next".

3. Click “Finish” to lock the device.

Unlock the device

1. To unlock an encrypted external storage device, click "Encryption Management".



2. Select "Unlock this device". Click "Next".

3. Enter the encryption password or upload the key file. Select "Save encryption key" to save the password in a hidden location on a hard drive of the NAS. The NAS will unlock the encrypted external storage device automatically every time the device is connected. Click "Finish".

Manage the encryption key

1. To change an encryption password or download an encryption key file, click "Encryption Management".

2. Select "Manage encryption key". Click "Next".

3. Select to change the encryption password or download the encryption key file to the local PC. Click "Finish".

Disk usage settings for 1-drive models

Select one of the following settings for an external storage device connected to a 1-drive NAS:

- Data sharing: Use the external drive for storage expansion of the NAS.
- Q-RAID 1: Configure the external drive and a local hard drive on the NAS as Q-RAID 1. Q-RAID 1 enables one-way data synchronization from the NAS to the external storage device but does not offer any RAID redundancy. **Note that the external drive will be formatted when Q-RAID 1 is executed.**

After Q-RAID 1 has been executed once, the NAS data will be automatically copied to the external storage device whenever it is connected to the NAS.

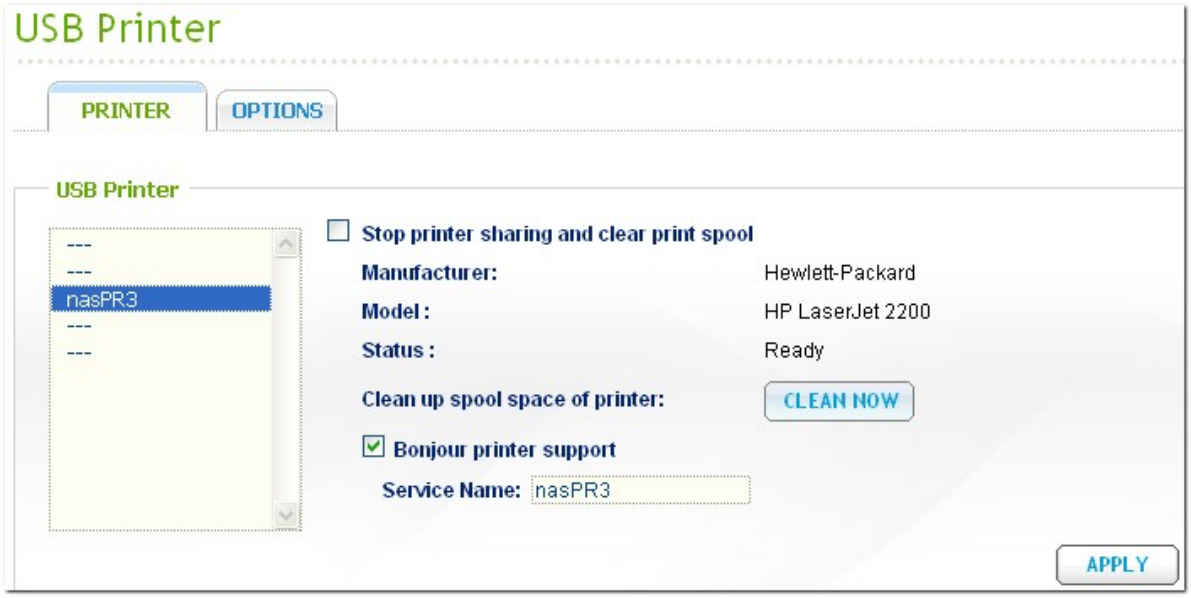
Note:

- Only one external hard disk can be set as Q-RAID 1 at one time.
- It is recommended to use an external storage device of the same capacity as the internal hard drive of the NAS. If the storage capacity of the external storage device is too small to synchronize with the internal hard drive, the device can only be used for data sharing.

9.2 USB Printer

The NAS supports network printing sharing service over local network and the Internet in Windows, Mac, and Linux (Ubuntu) environments. Up to 3 USB printers are supported.

To share a USB printer by NAS, connect the printer to a USB port of the NAS. The printer will be detected automatically and the printer's information will be shown.



Note:

- Please connect a USB printer to the NAS after the software configuration is completed.
- The NAS does not support multifunction printer.
- The file name display on the printer job table is only available for printer jobs sent via IPP (Internet Printing Protocol) connection.
- For the information of the supported USB printer models, please visit http://www.qnap.com

Stop printer sharing and clear print spool
Select this option to temporarily disable the selected printer for print sharing. All the data in the printer spool will also be cleared.

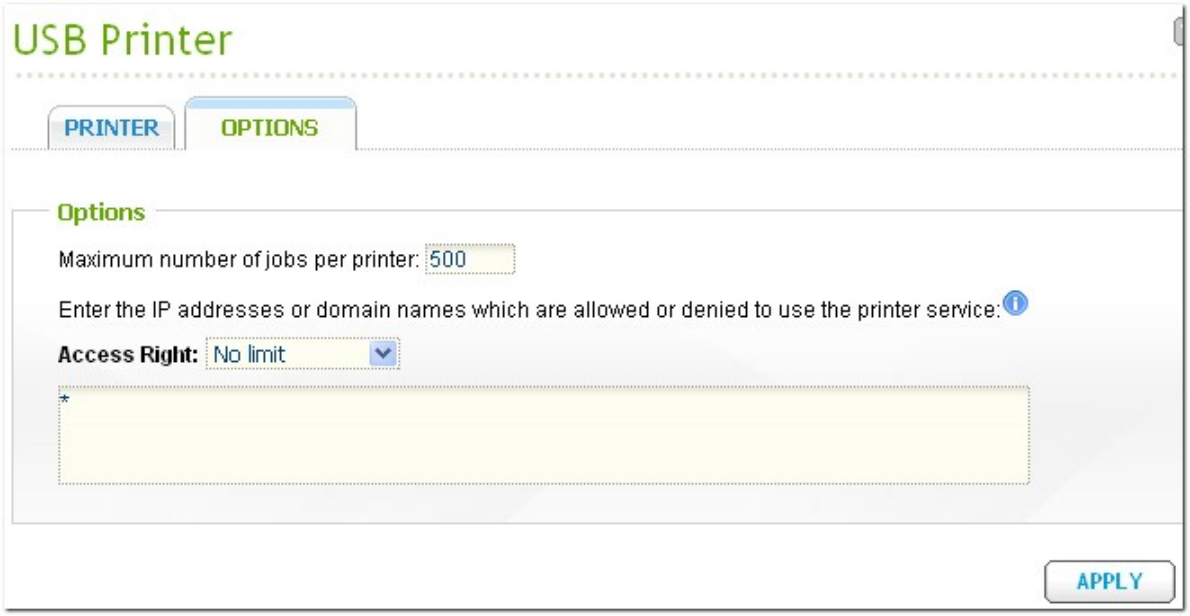
Clean up spool space of printer

Click "Clean Now" to clean up the data saved in the printer spool.

Bonjour printer support

Select this option to broadcast printing service to Mac users via Bonjour. Enter a service name, which allows the printer to be found by Bonjour. The name can only contain "a-z", "A-Z", "0-9", dot (.), comma (,) and dash (-).

You can configure other printer options in the "Options" tab.



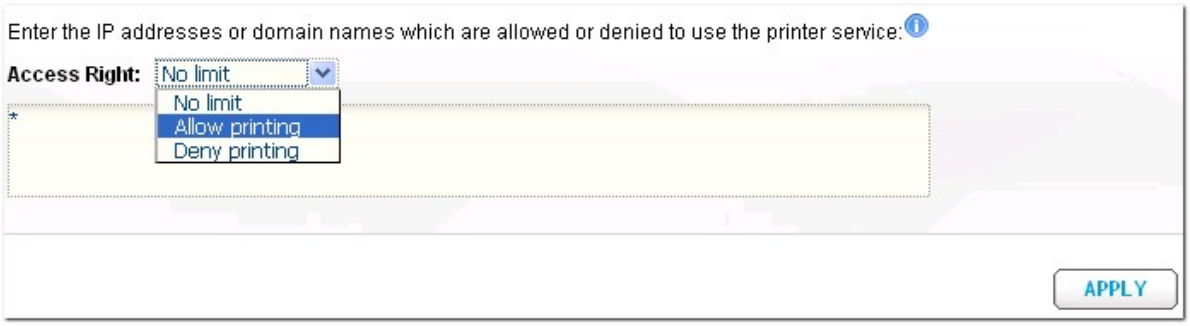
Maximum printer jobs per printer

Specify the maximum number of printer jobs for a printer. A printer supports maximum 1,000 printer jobs. The oldest printer job will be overwritten by the newest one if the printer has reached the maximum number of printer jobs.

Enter IP addresses or domain names to allow or deny printing access

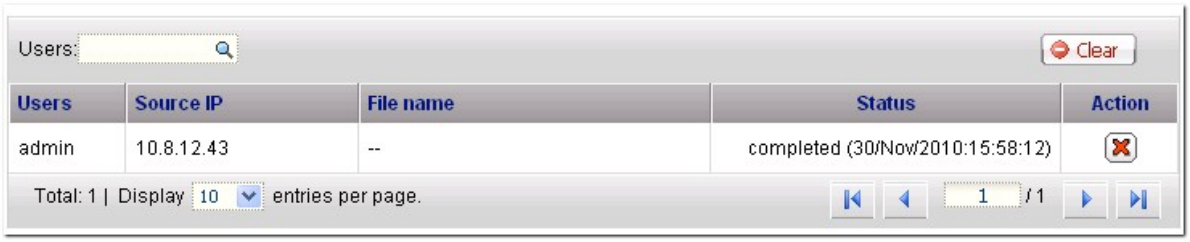
To allow or deny particular IP addresses or domain names to use the printing service of the NAS, select "Allow printing" or "Deny printing" and enter the IP address(es) or domain name(s). An asterisk (*) denotes all connections. To allow all users to use the printer, select "No limit". Click "Apply" to save the settings.

Note: This feature only works for printing service configured via IPP and Bonjour, but not Samba.



Pause, resume, or delete printer jobs

You can pause or cancel ongoing or pending jobs, resume paused jobs, or delete completed or pending jobs.



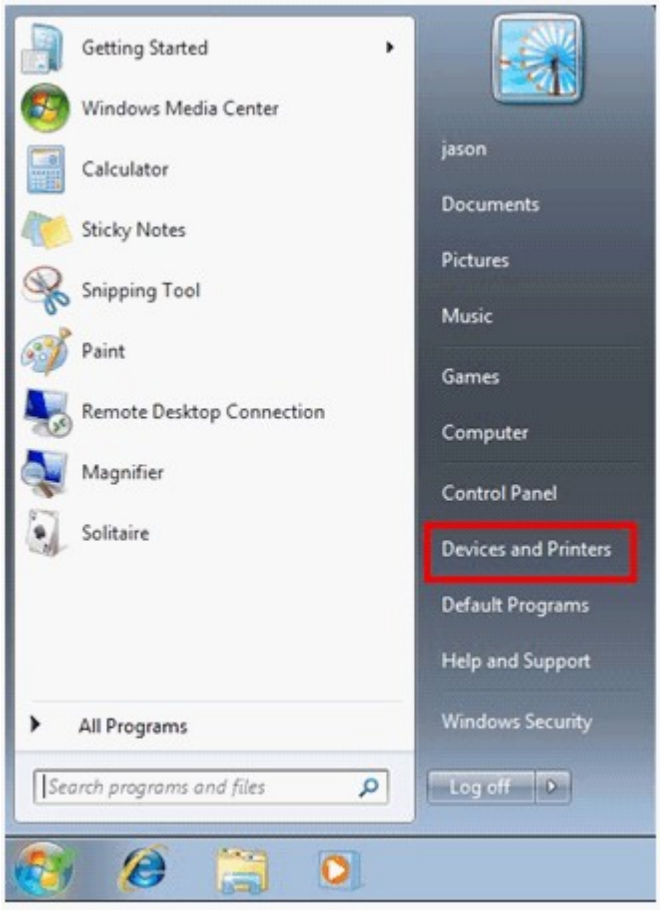
Note: Do NOT restart the NAS or update the system firmware when printing is in process or there are queued jobs. Otherwise all the queued jobs will be cancelled and removed.

9.2.1 Windows 7, Vista Users

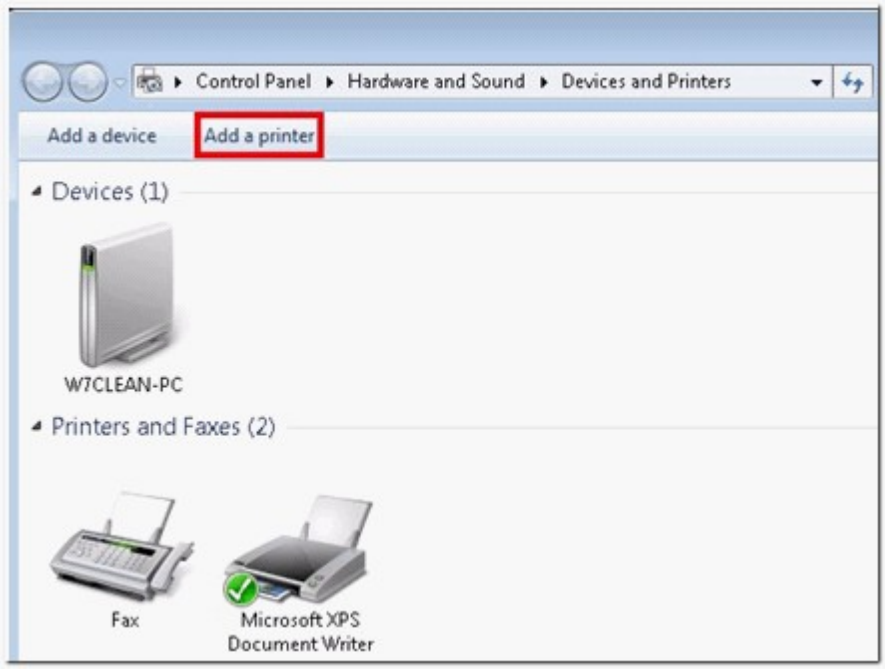
The following description applies to Windows 7.

Follow the steps below to set up your printer connection.

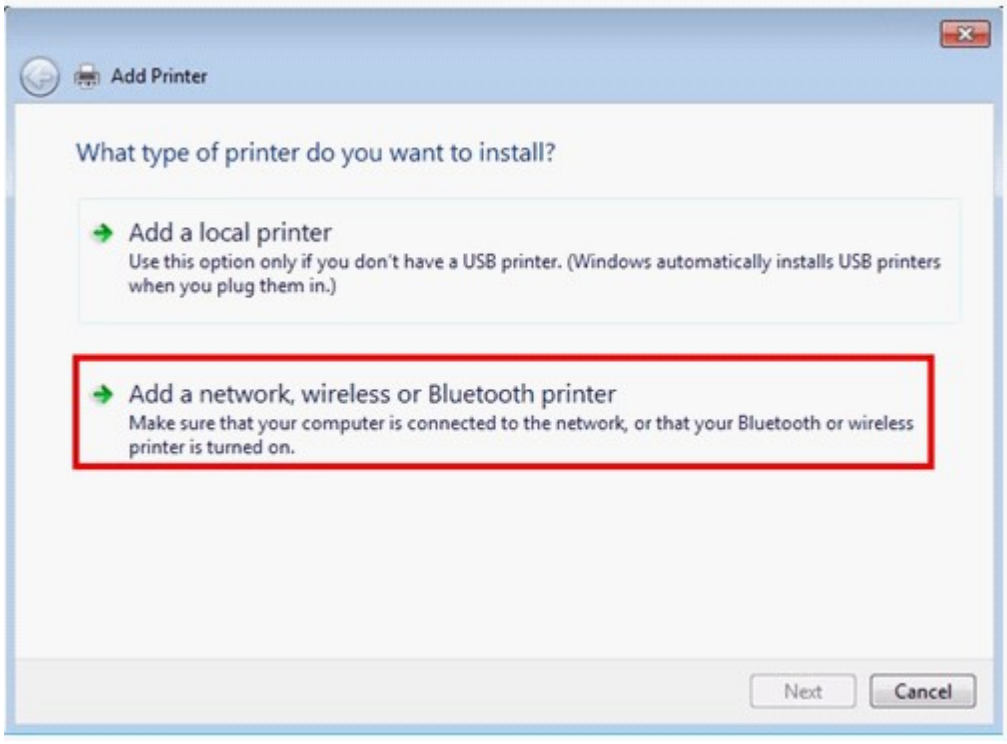
1. Go to Devices and Printers.



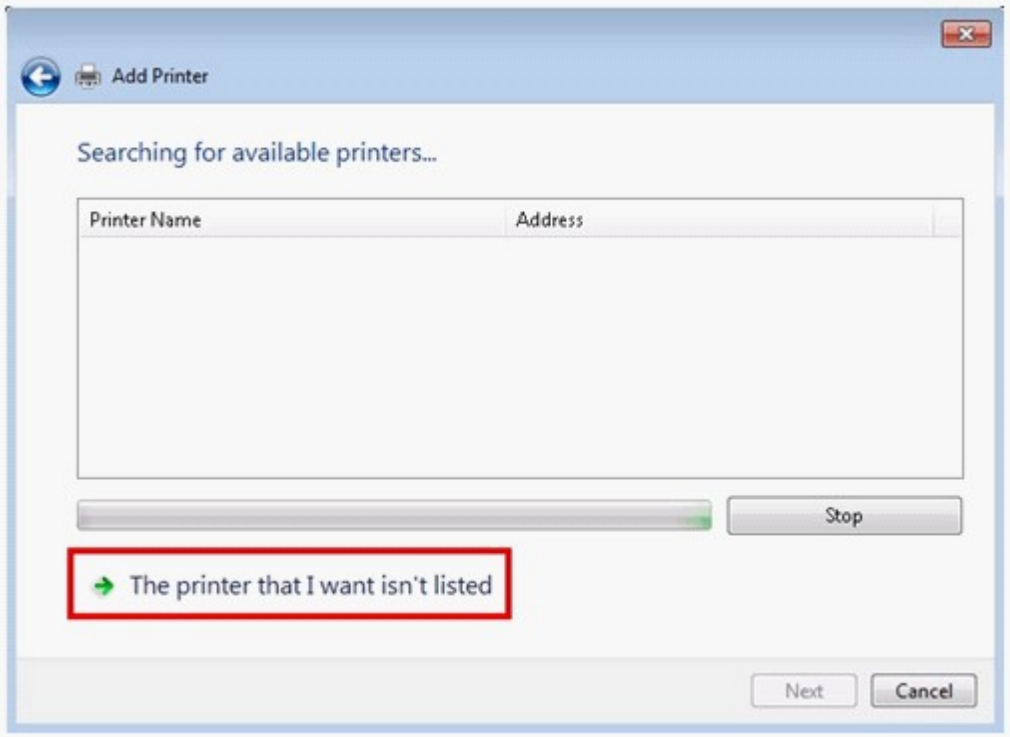
2. Click “Add a printer”.



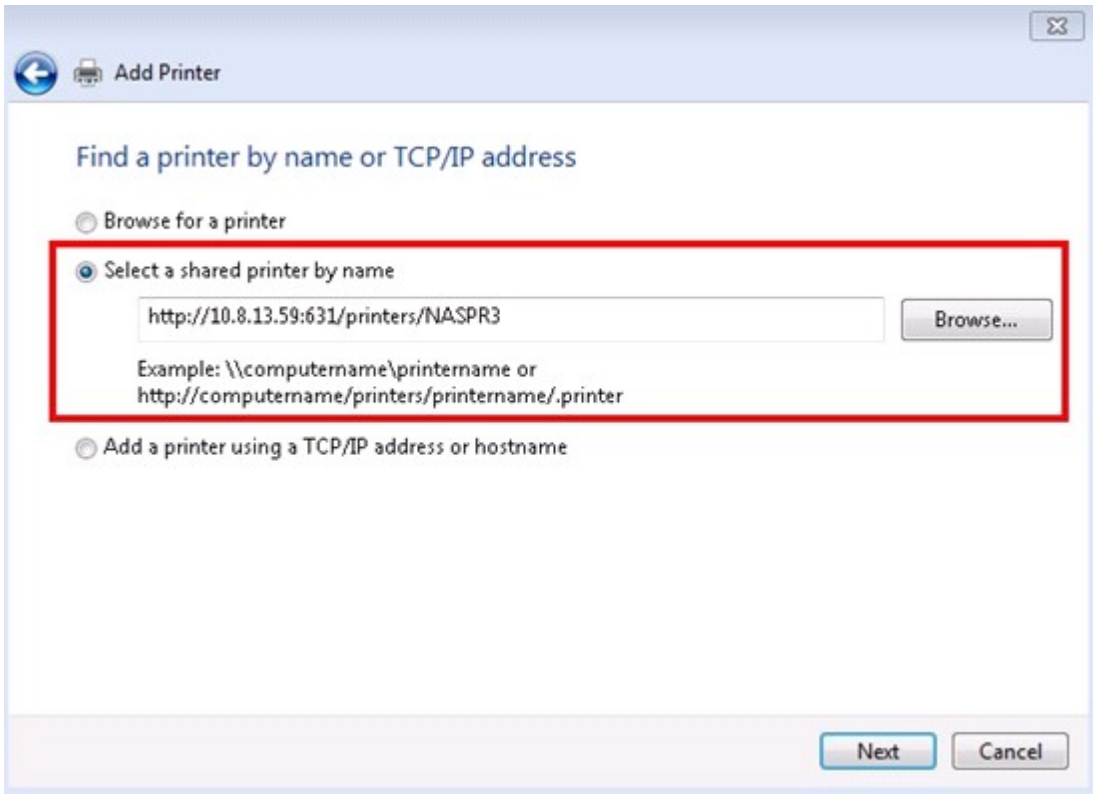
3. In the Add printer wizard, click “Add a network, wireless or Bluetooth printer”.



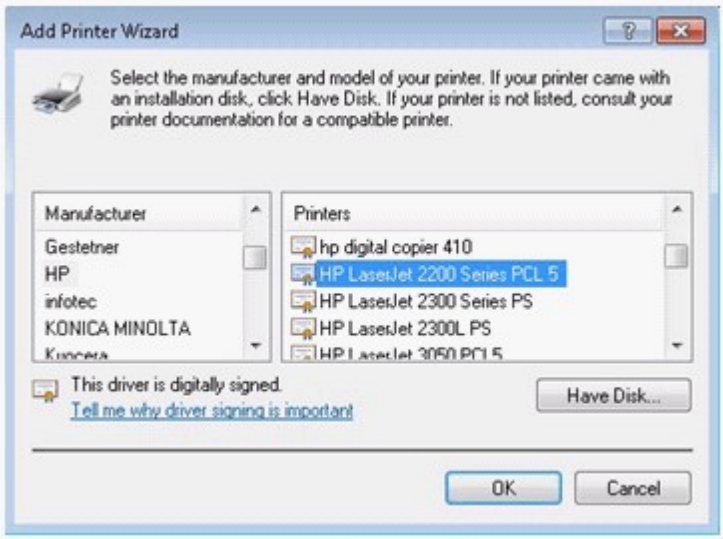
4. While Windows is searching for available network printers, click "The printer that I want isn't listed".



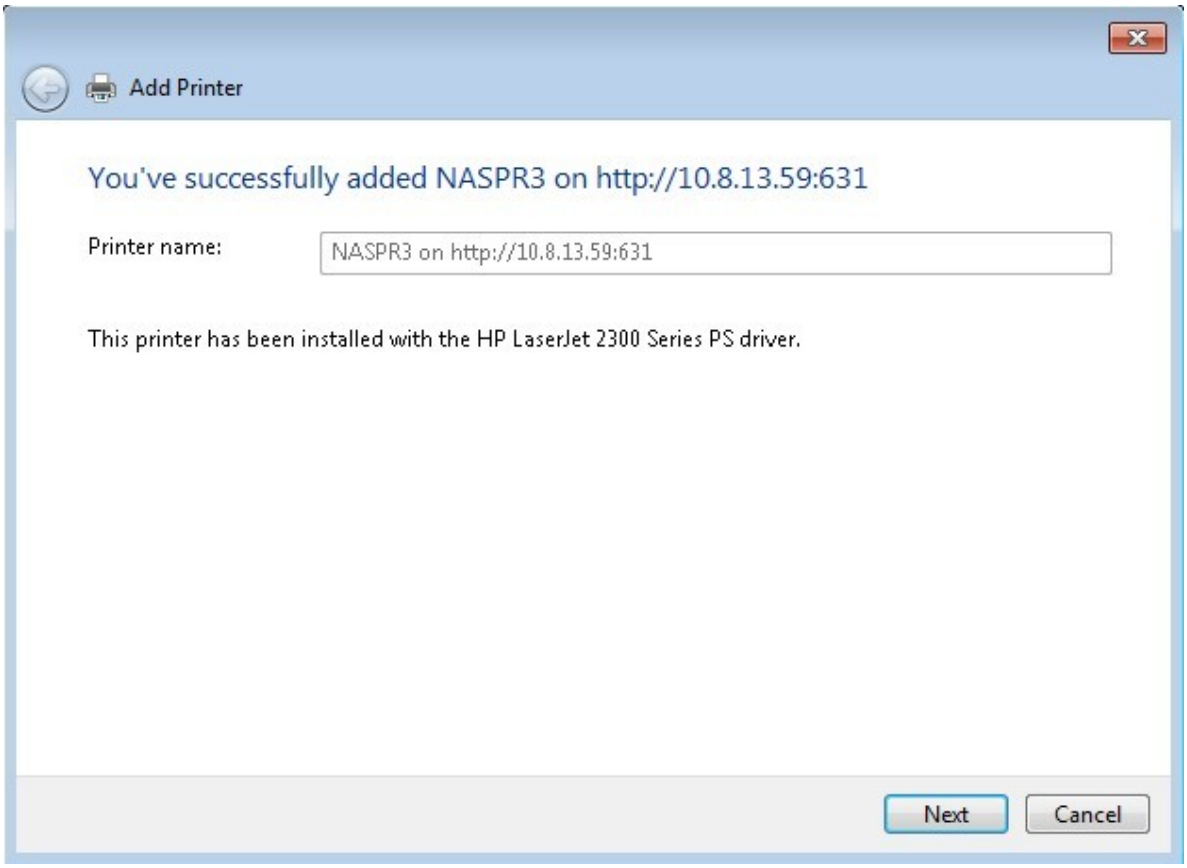
5. Click "Select a shared printer by name", and then enter the address of the network printer. The address is in the following format – http://NAS_IP:631/printers/ServernamePR, where the NAS_IP can also be a domain name address if you want to print remotely. For example, http://10.8.13.59:631/printers/NASPR3



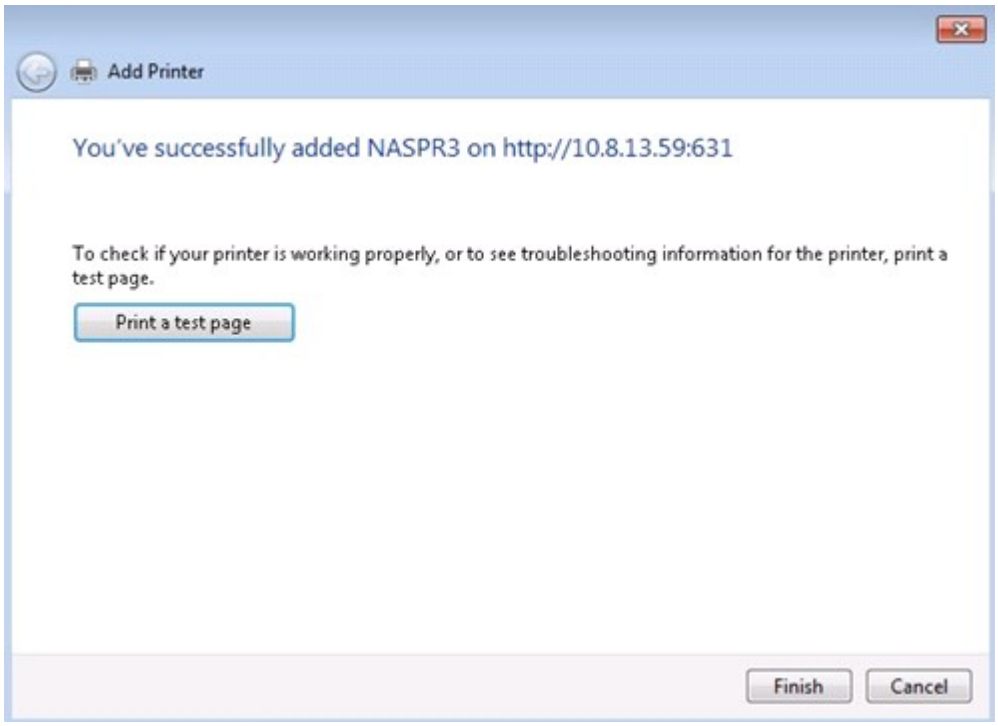
6. The wizard will prompt you for the correct printer driver. You may also download the latest printer driver from the manufacturer's website if it is not built-into Windows operating system.



7. After installing the correct printer driver, the wizard shows the address and driver of the new network printer.



8. You may also set the network printer as the default printer or print a test page. Click "Finish" to exit the wizard.

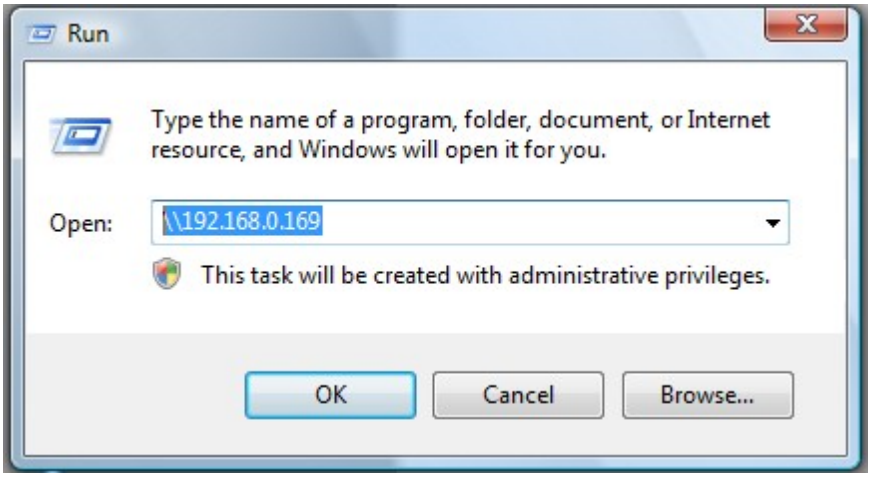


9. The new network printer is now available for printing.

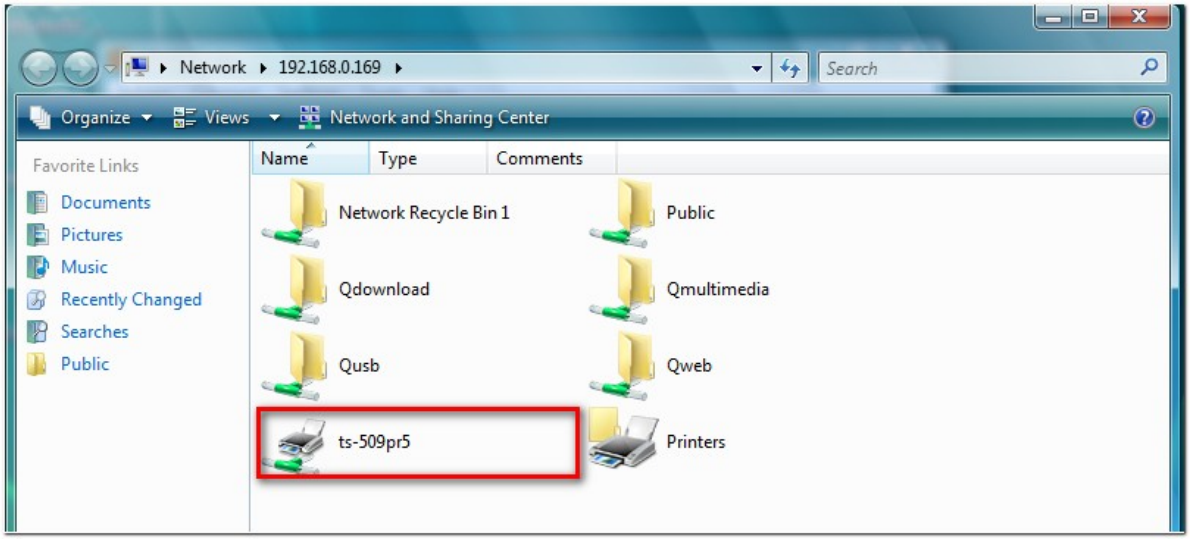
The following description applies to Windows 7 and Vista OS.

Follow the steps below to set up your printer connection.

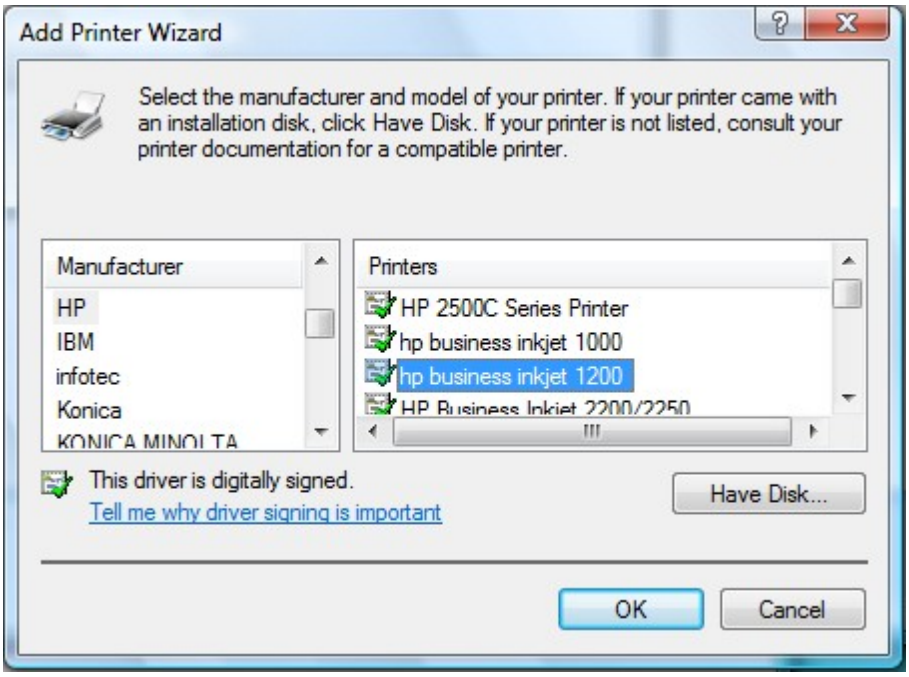
1. On the Run menu, enter \\NAS IP.



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.

9.2.2 Windows XP Users

Follow the steps below to set up your printer connection.

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

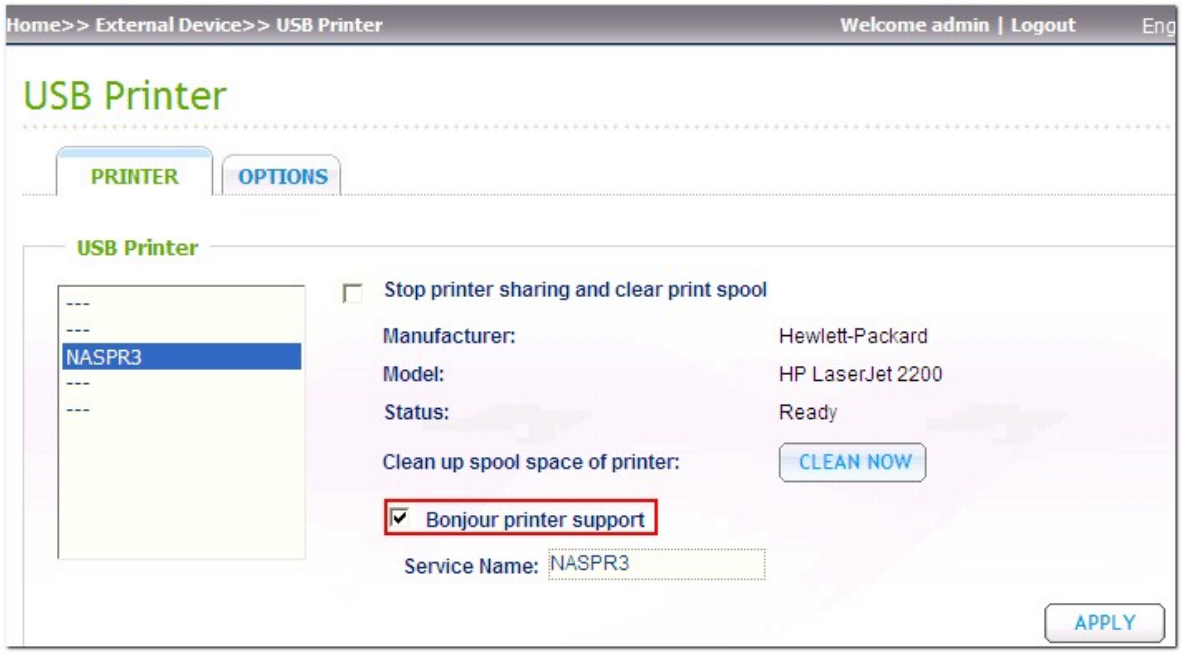
The following configuration method has been verified on Windows XP only:

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, for example, 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.

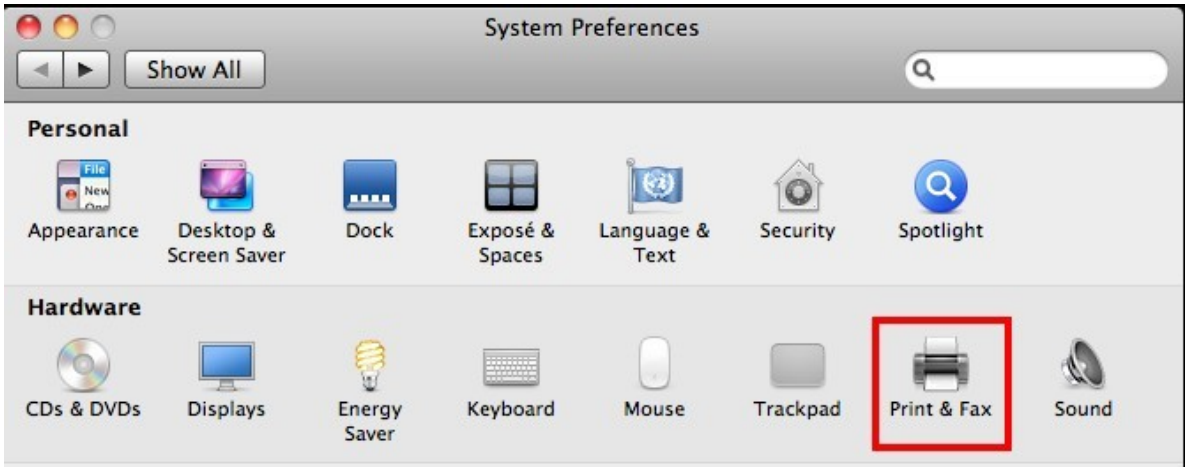
9.2.3 Mac OS 10.6

If you are using Mac OS 10.6, follow the steps below to configure the printer function of the NAS.

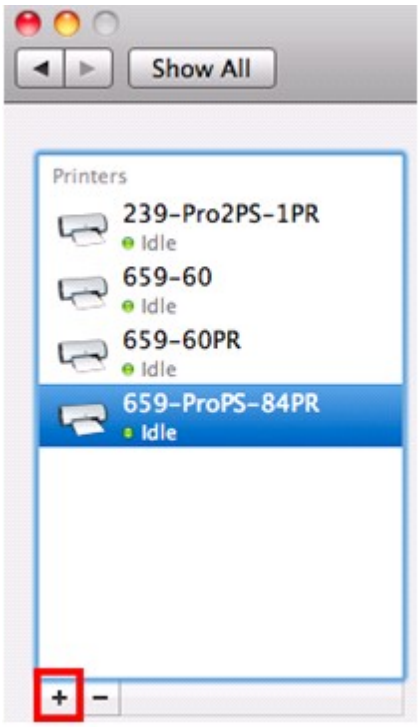
1. First make sure the Bonjour printer support is enabled on the NAS in "External Device" > "USB Printer". You may change the Service Name to better represent the printer.



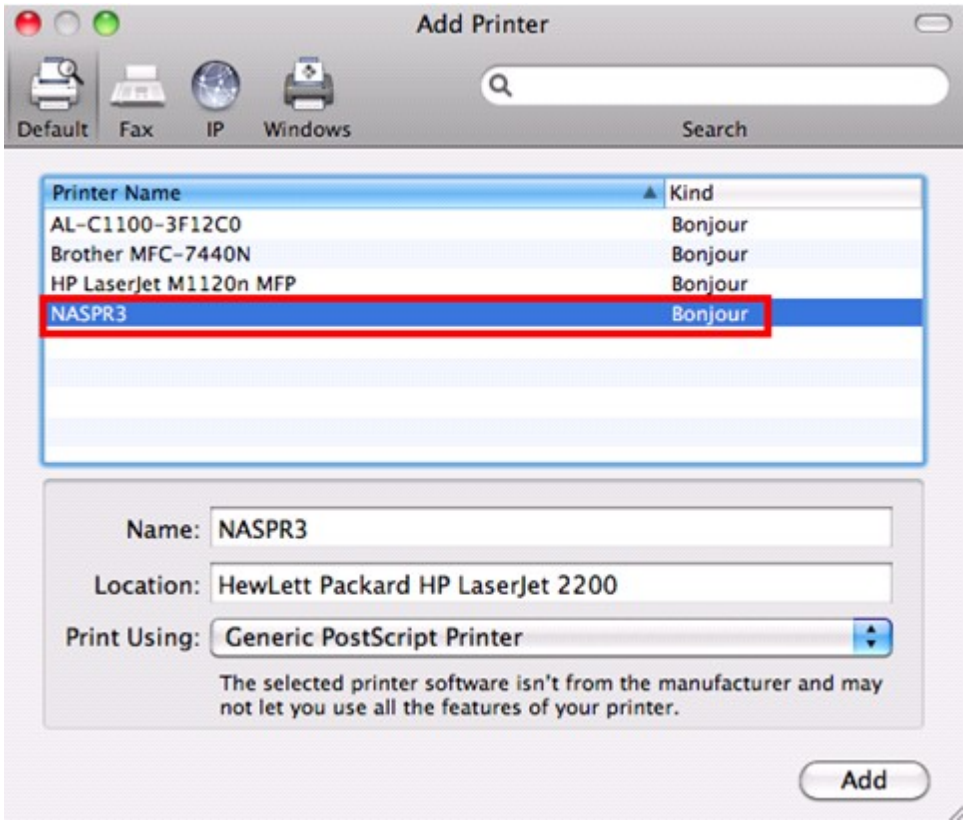
2. On your Mac, go to "System Preferences", and then click "Print & Fax".



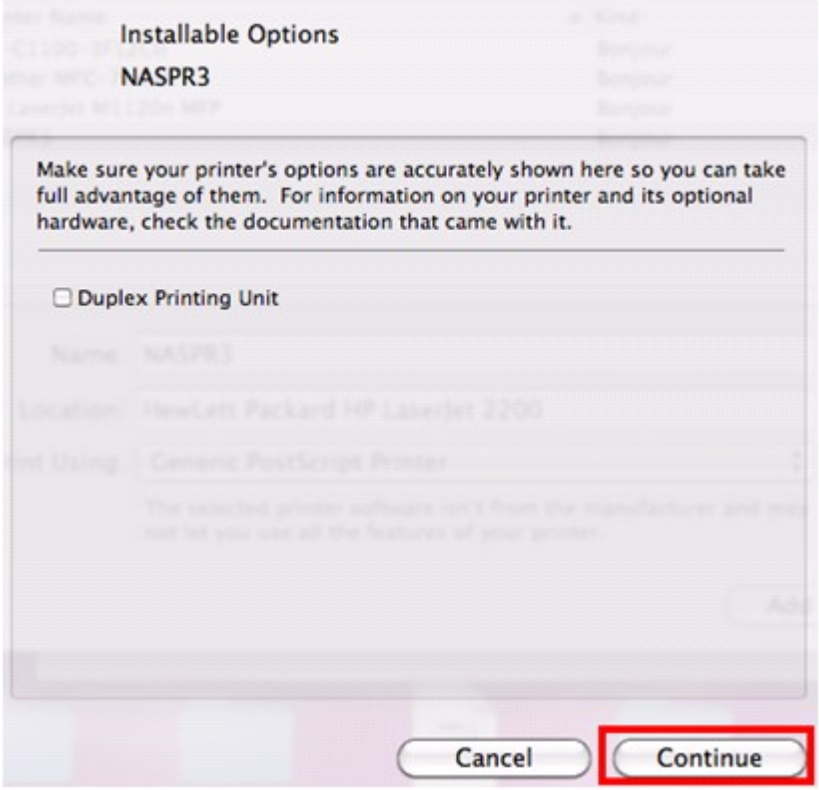
3. In the Print & Fax window, click + to add a printer.



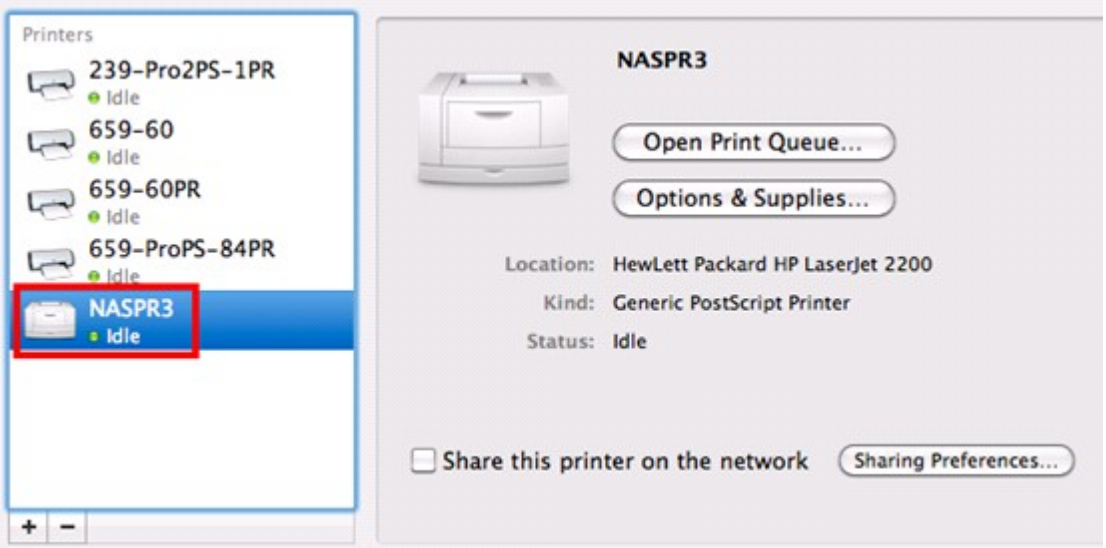
4. The USB network printer will be listed via Bonjour. Select the default printer driver or you may download and install the latest one from the printer manufacturer"s website. Click "Add" to add this printer.



5. Additional options may be available for your printer. Click “Continue”.



6. The new network printer is now available for printing.

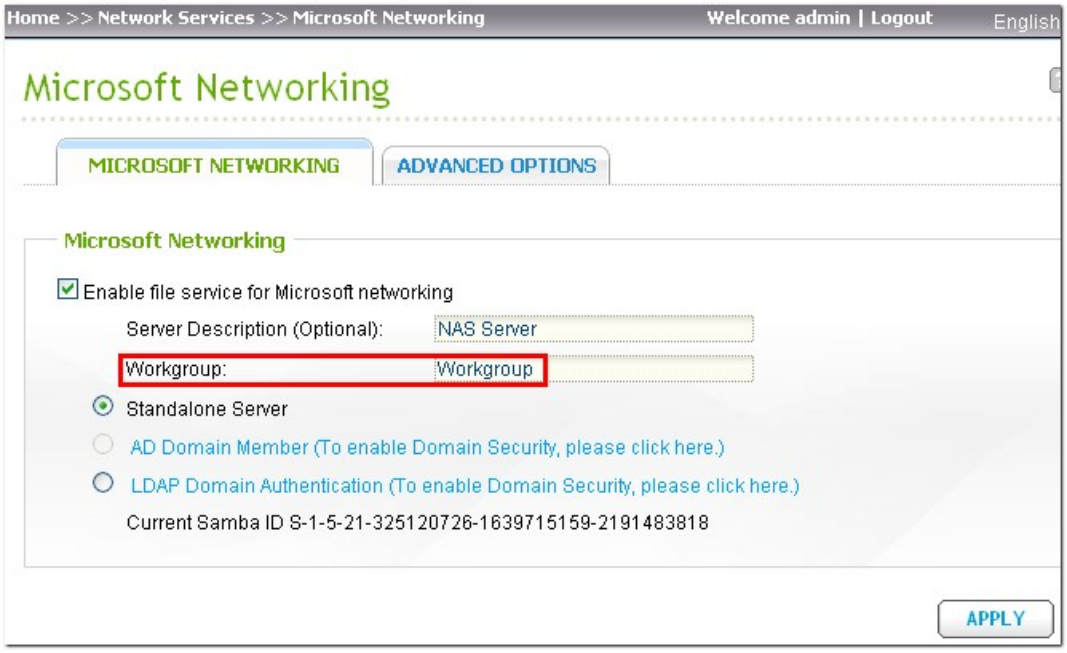


9.2.4 Mac OS 10.5

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

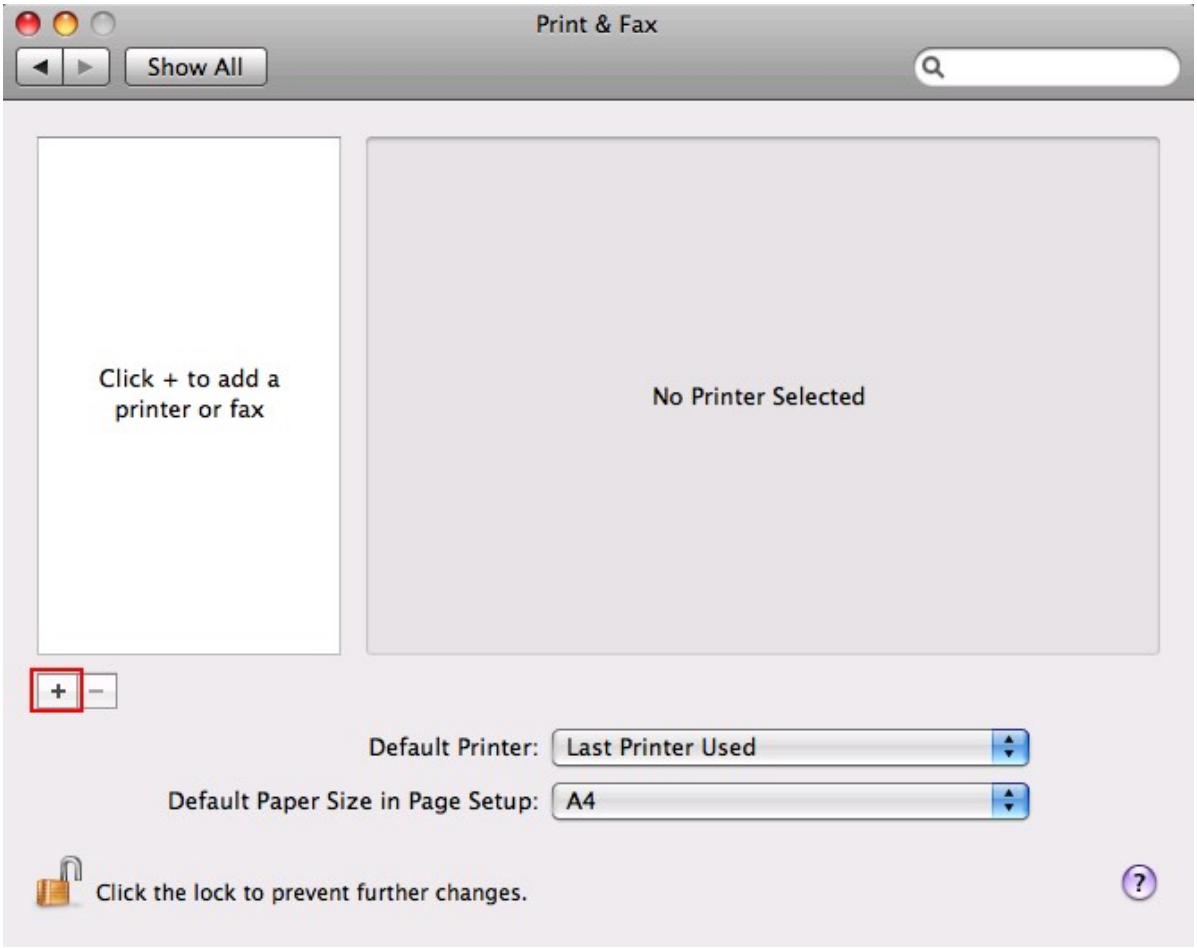
1. Make sure your printer is connected to the NAS and the printer information is displayed correctly on the "USB Printer" page.

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

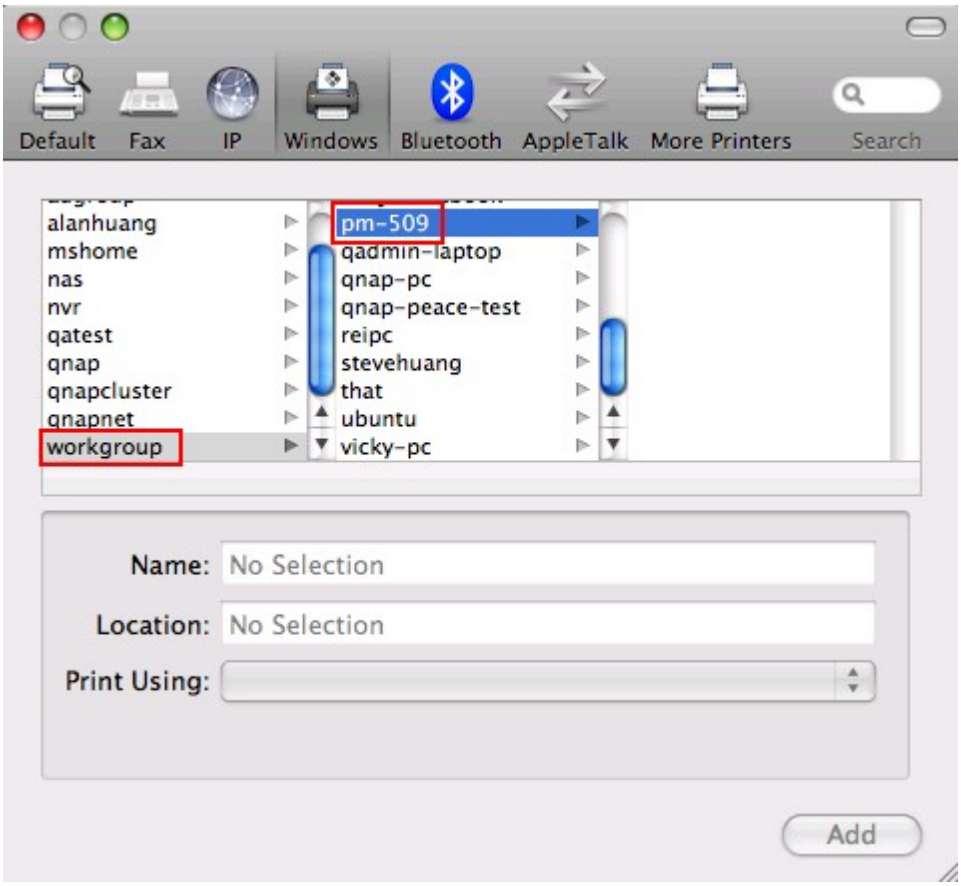


3. Go to "Print & Fax" on your Mac.

4. Click + to add a printer.

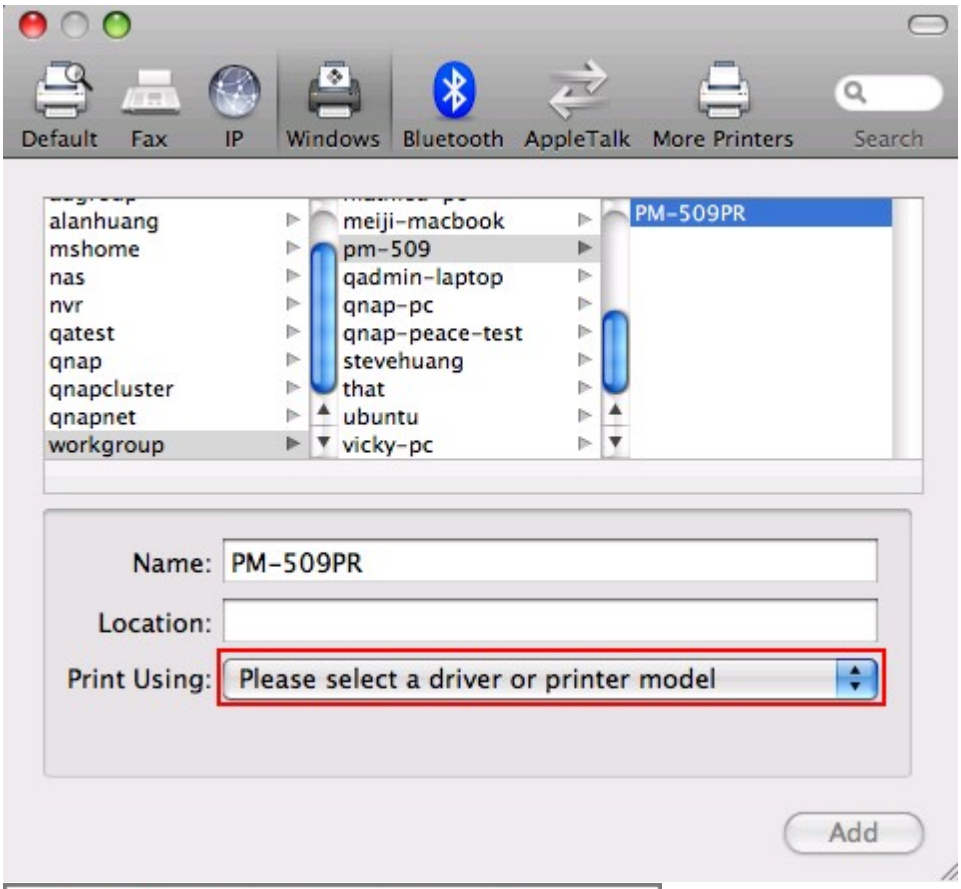


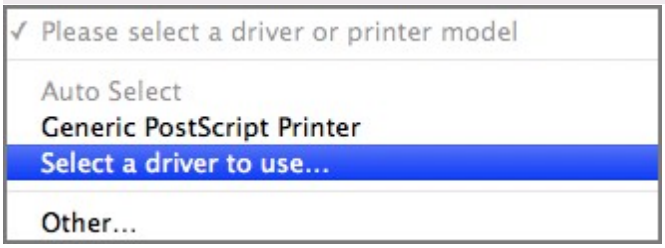
5. Select the NAS workgroup and find the printer name.



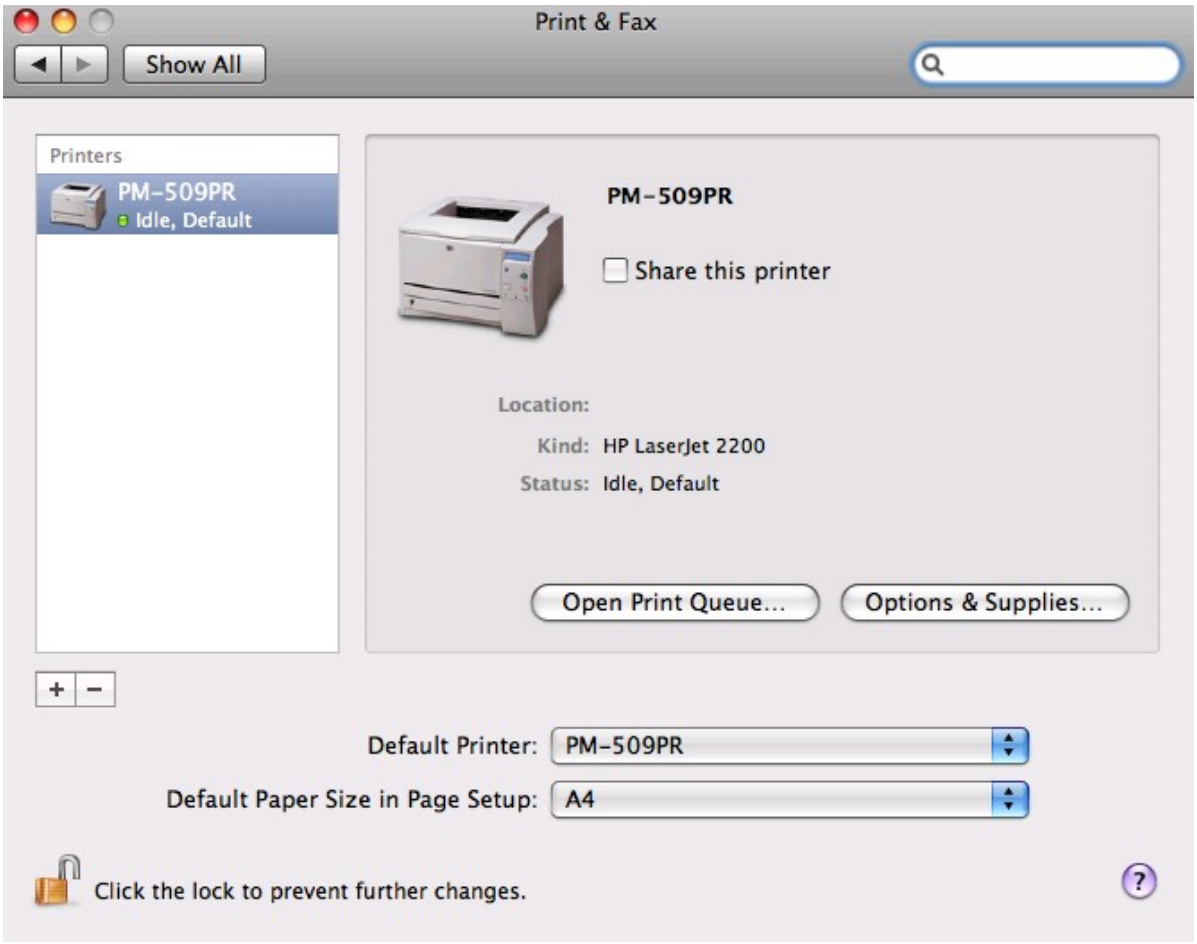
6. Enter the user name and password to login the printer server on the NAS.

7. Select the printer driver.





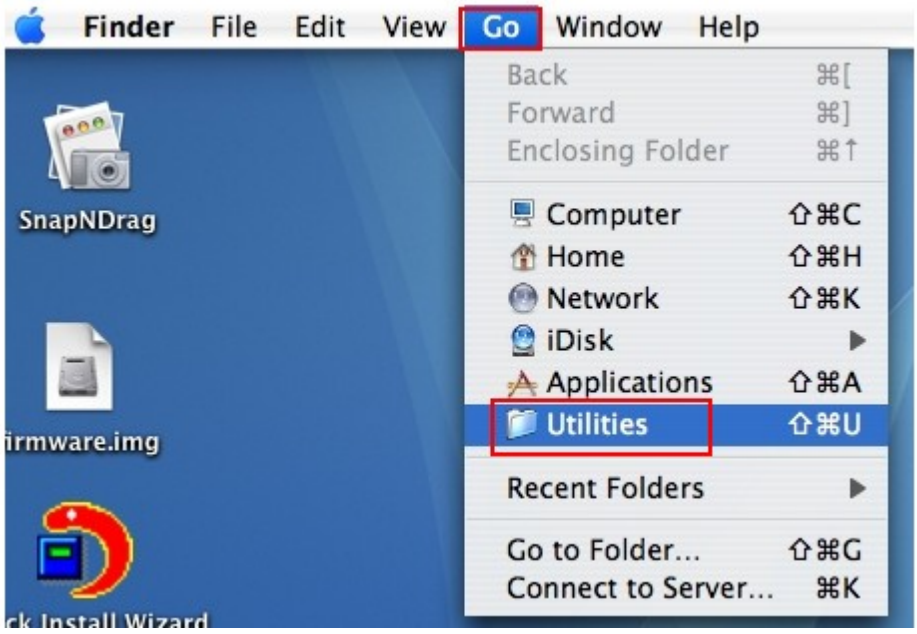
8. After installing the printer driver correctly, you can start to use the printer.



9.2.5 Mac OS 10.4

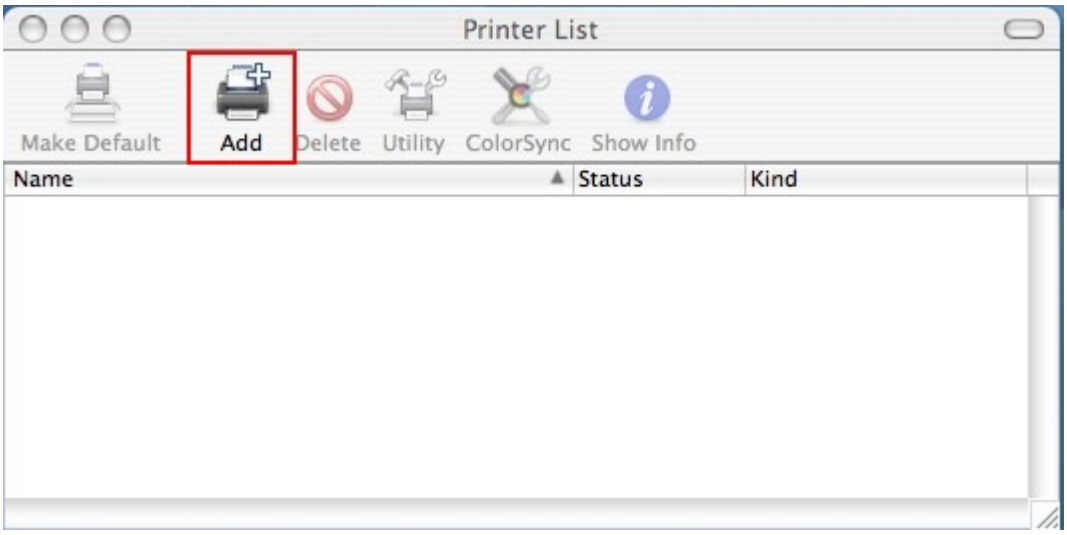
If you are using Mac OS 10.4, follow the steps below to configure the printer function of the NAS.

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



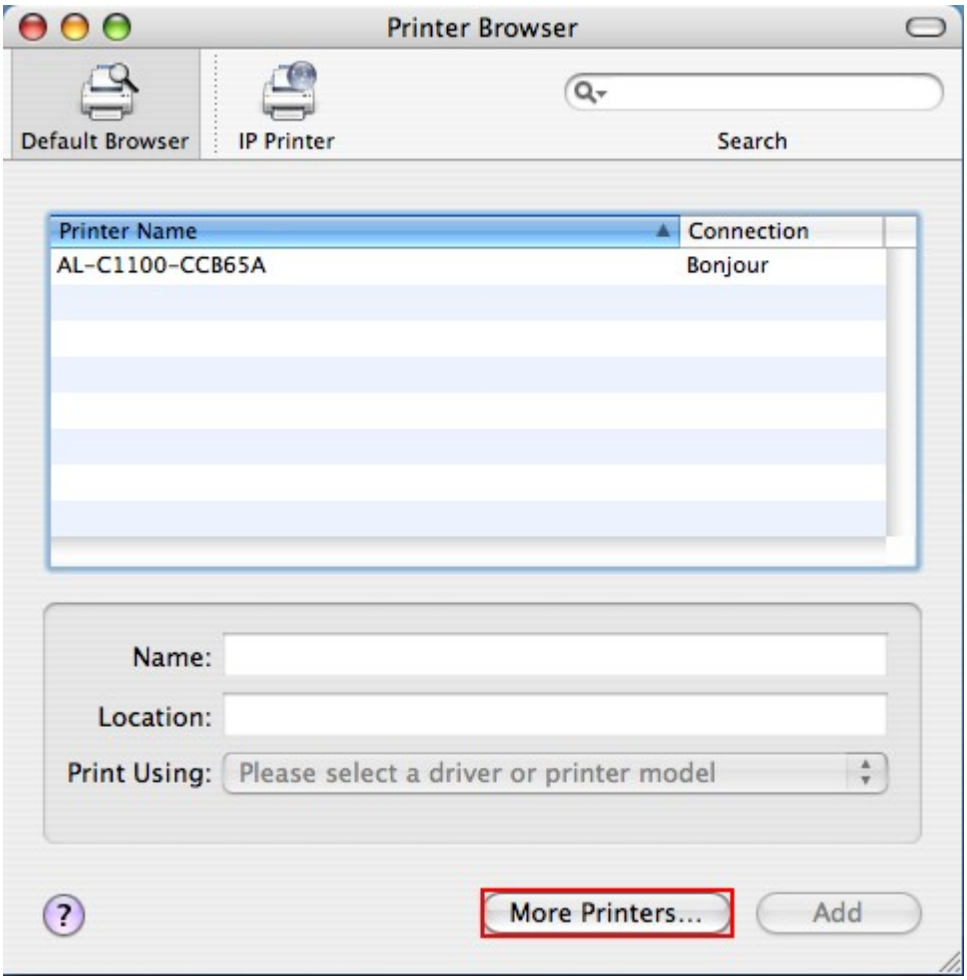
2. Click "Printer Setup Utility".

3. Click “Add”.

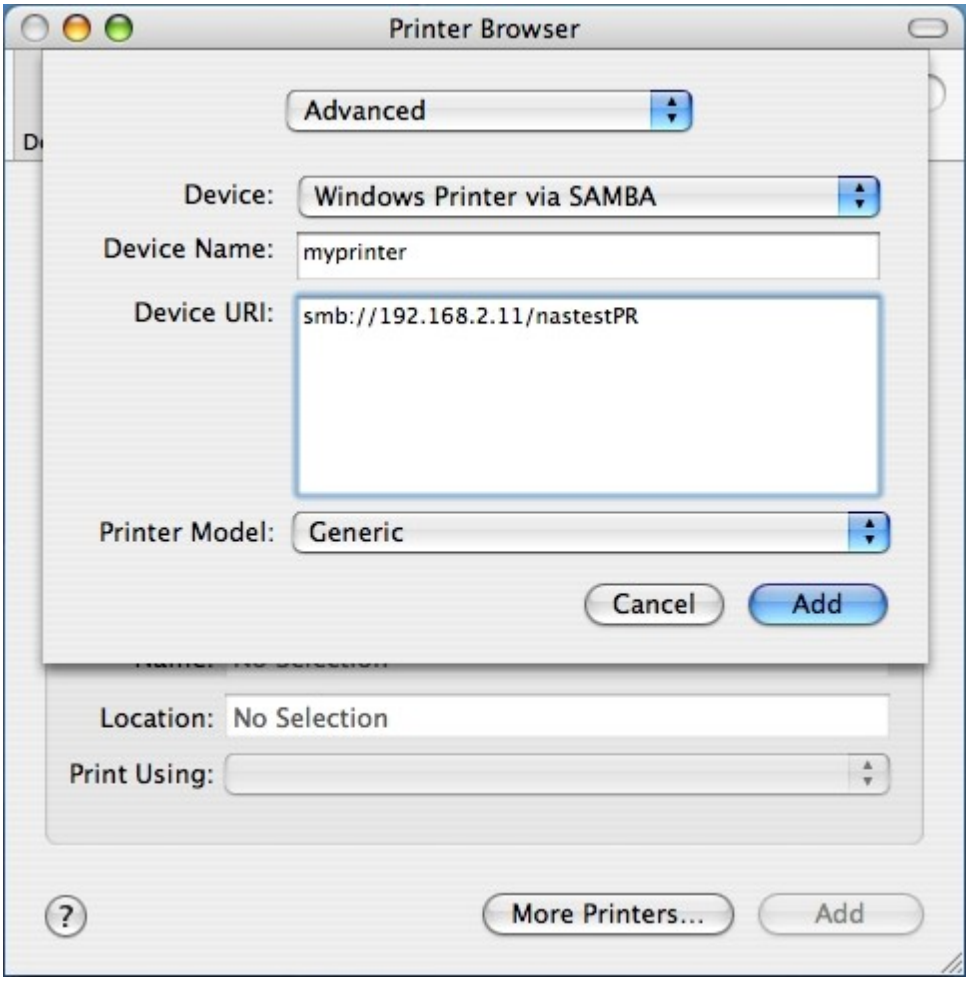

Printer List
Make Default
Add
Delete
Utility
ColorSync
Show Info
Name
Status
Kind

4. Press and hold the “alt” key

on the keyboard and click “More Printers” concurrently.

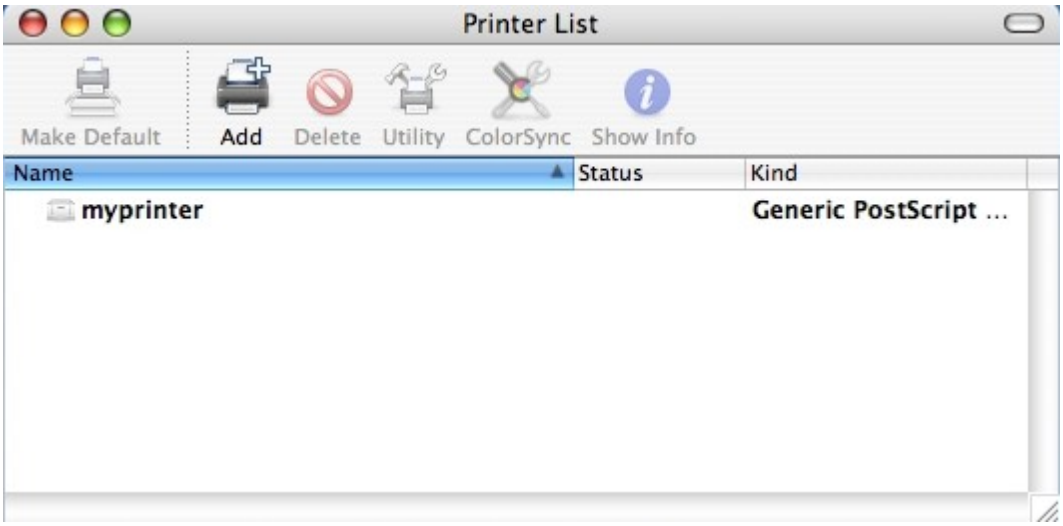


5. In the pop up window:
   a. Select "Advanced"*.
   b. Select "Windows Printer with SAMBA".
   c. Enter the printer name.
   d. Enter the printer URI, the format is smb://NAS IP/printer name. The printer name is found on the "Device Configuration" > "USB Printer page".
   e. Select "Generic" for Printer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



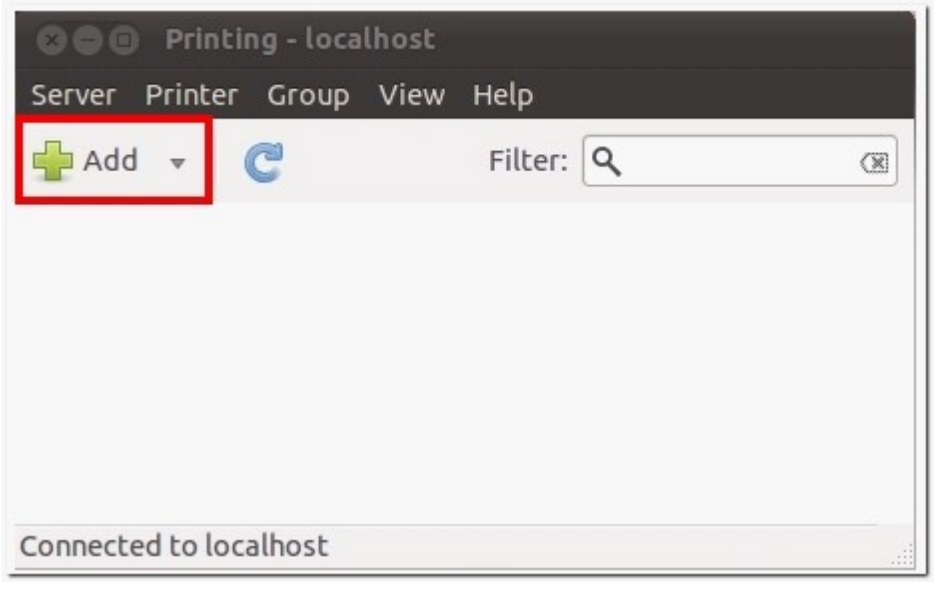
Note: The network printer service of the NAS supports Postscript printer on Mac OS only.

9.2.6 Linux (Ubuntu 10.10)

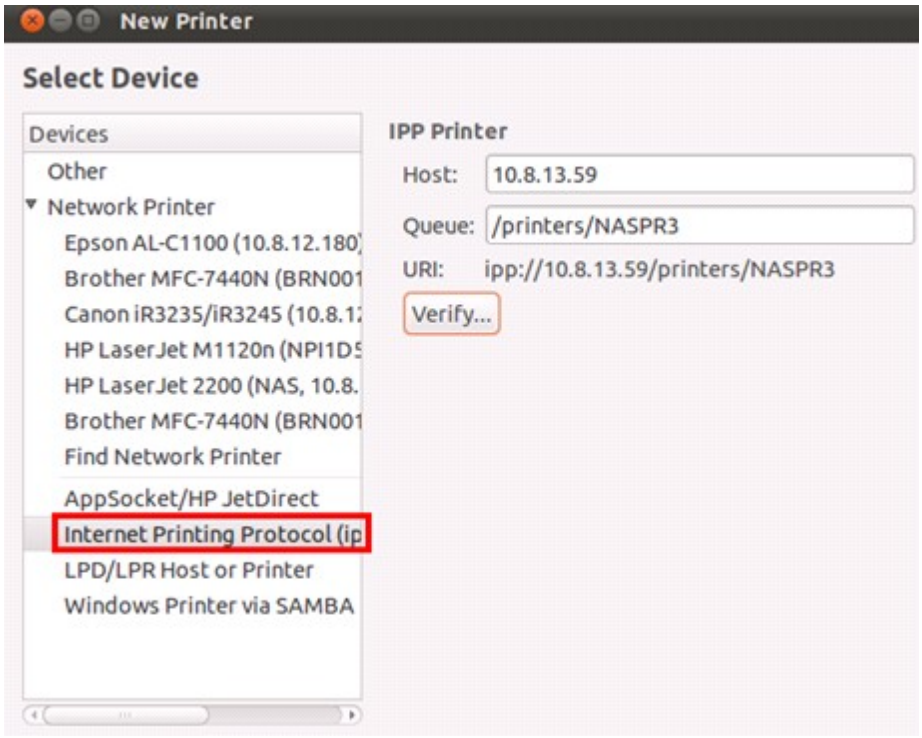
If you are using Linux (Ubuntu 10.10), follow the steps below to configure the printer function of the NAS.

1. Click the "System" tab, choose "Administration". Then select "Printing".

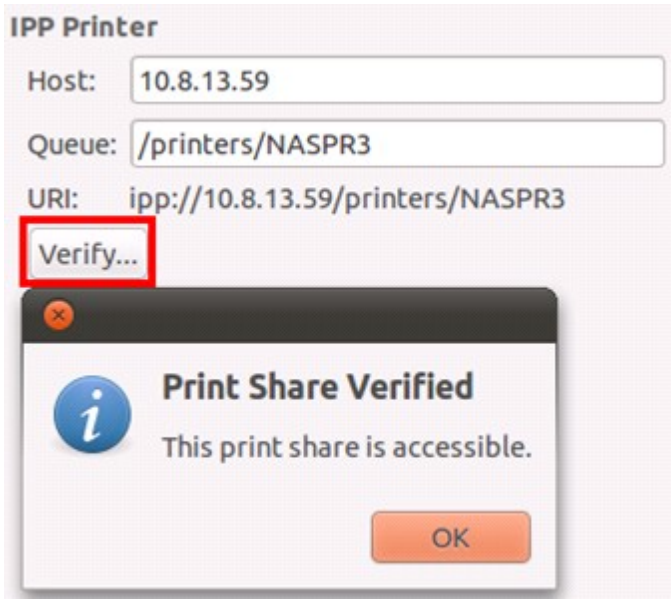
2. Click "Add" to add a printer.



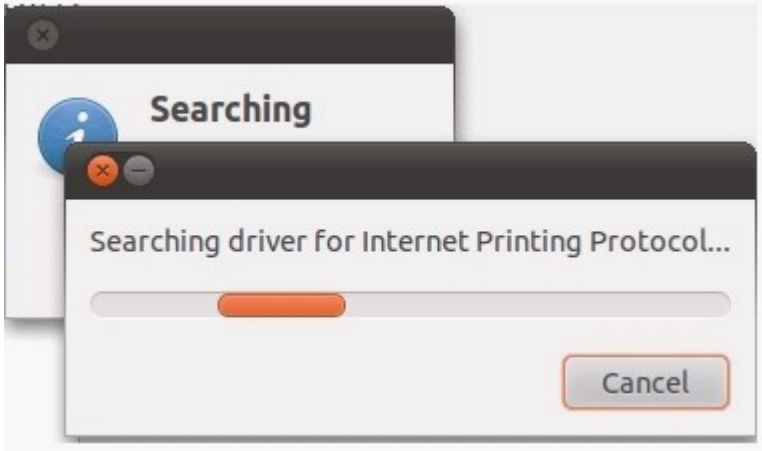
3. Click “Network Printer”, and then select “Internet Printing Protocol (ipp)”. Enter the NAS IP address in “Host”. “/printers” is already present. Enter the printer name after “printers/” in the field “Queue”.



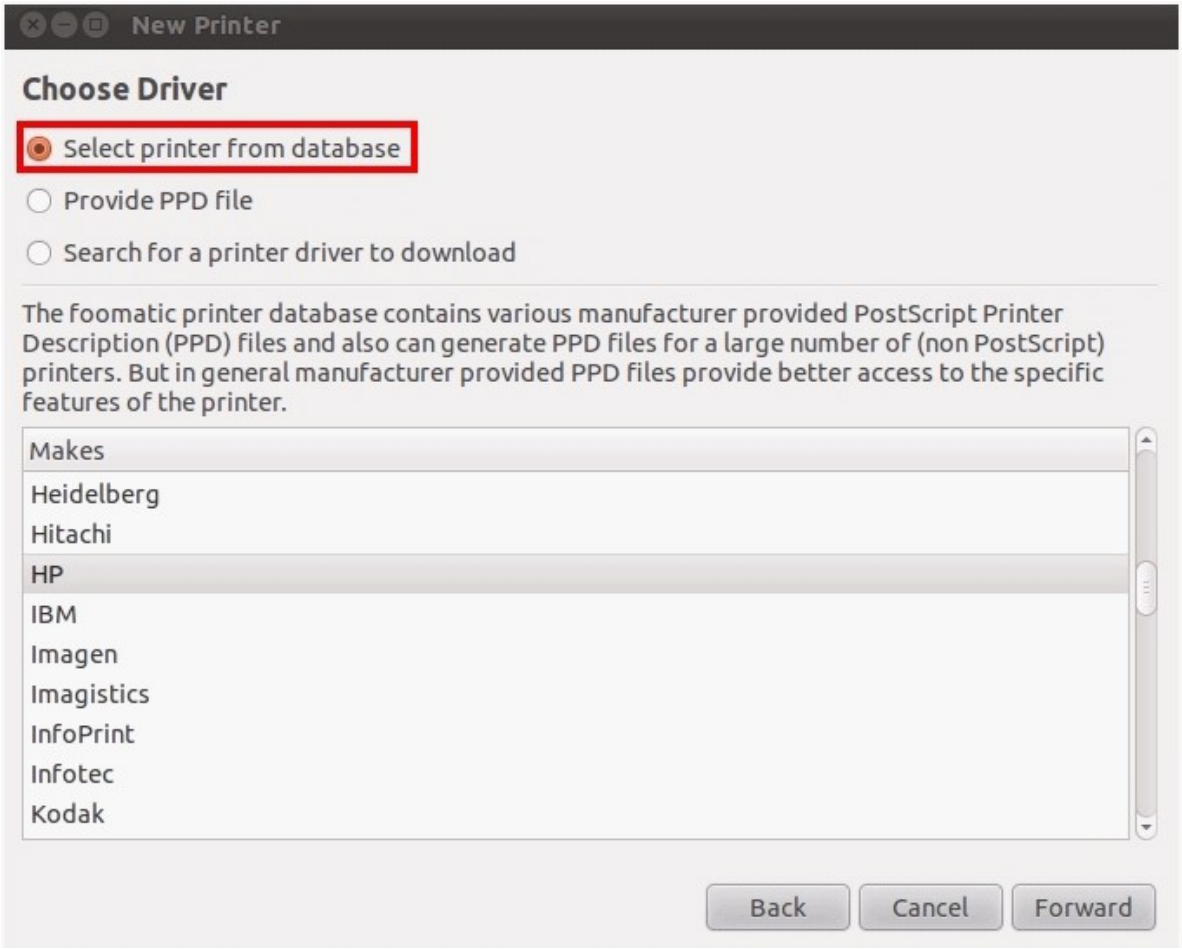
4. Before you continue, you may click “Verify” to test the printer connection.



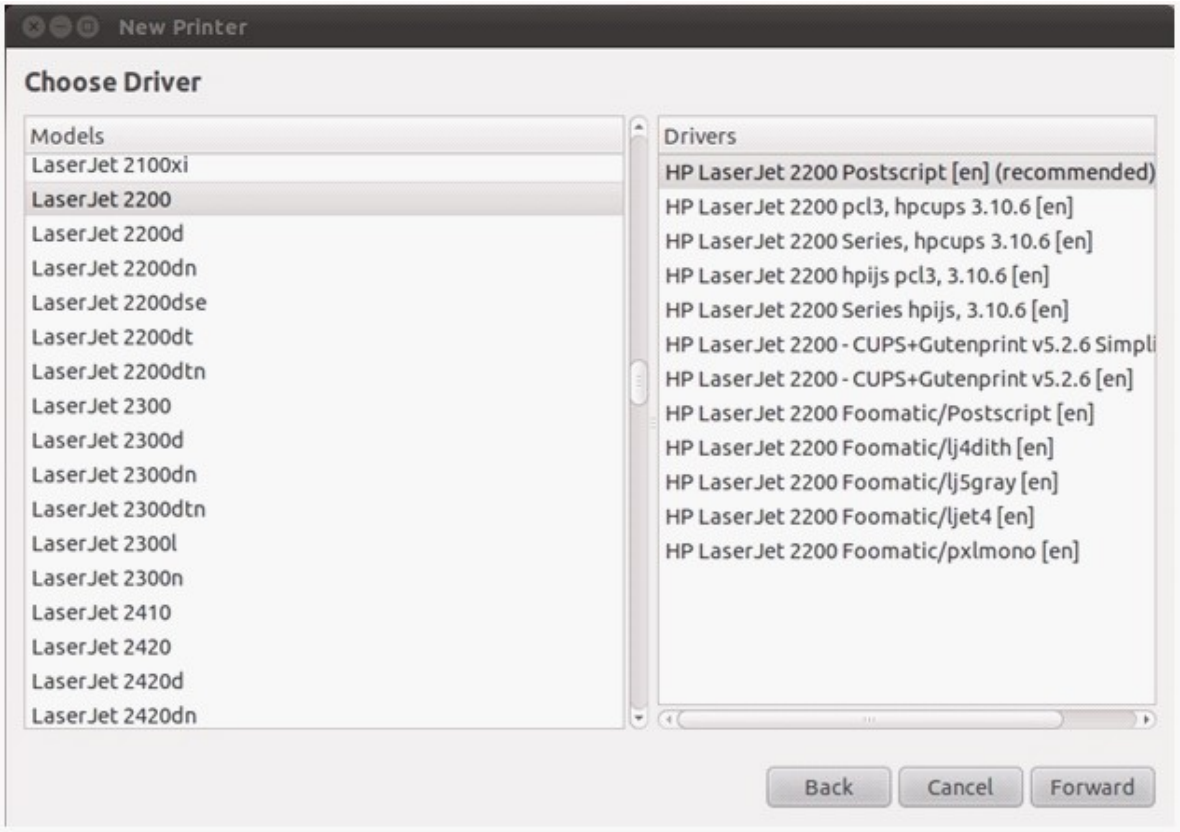
5. The operating system starts to search for the possible driver list.



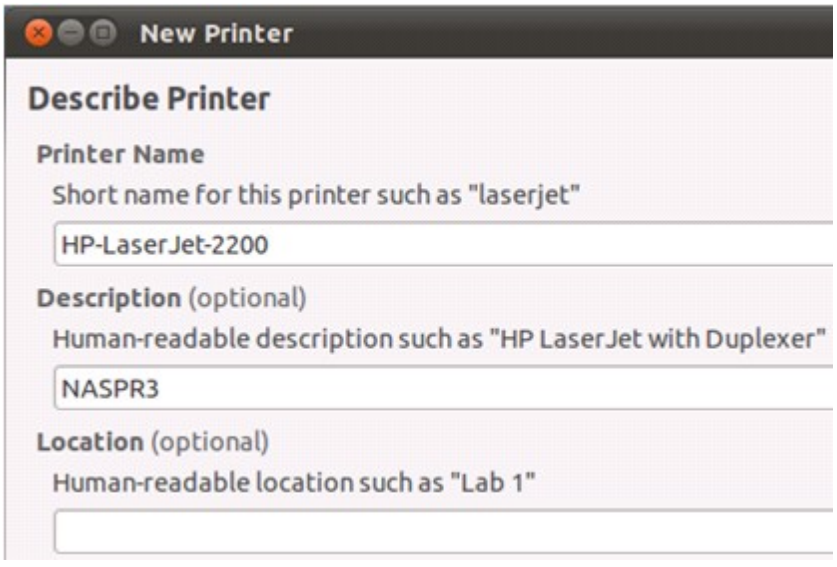
6. Select the printer driver from the built-in database, or search online.



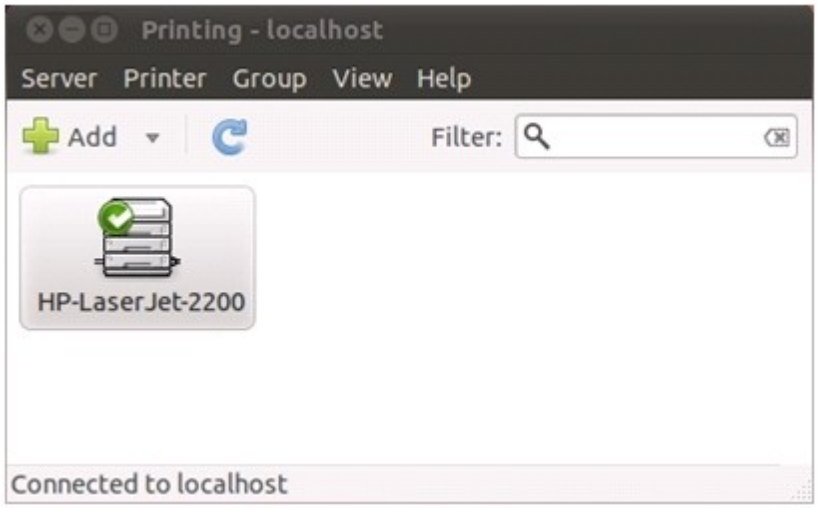
7. Choose the correct printer model and driver. Depending on the printer, some additional printer options may be available in the next step.



8. You can rename this printer or enter additional information. Click "Apply" to exit and finish.

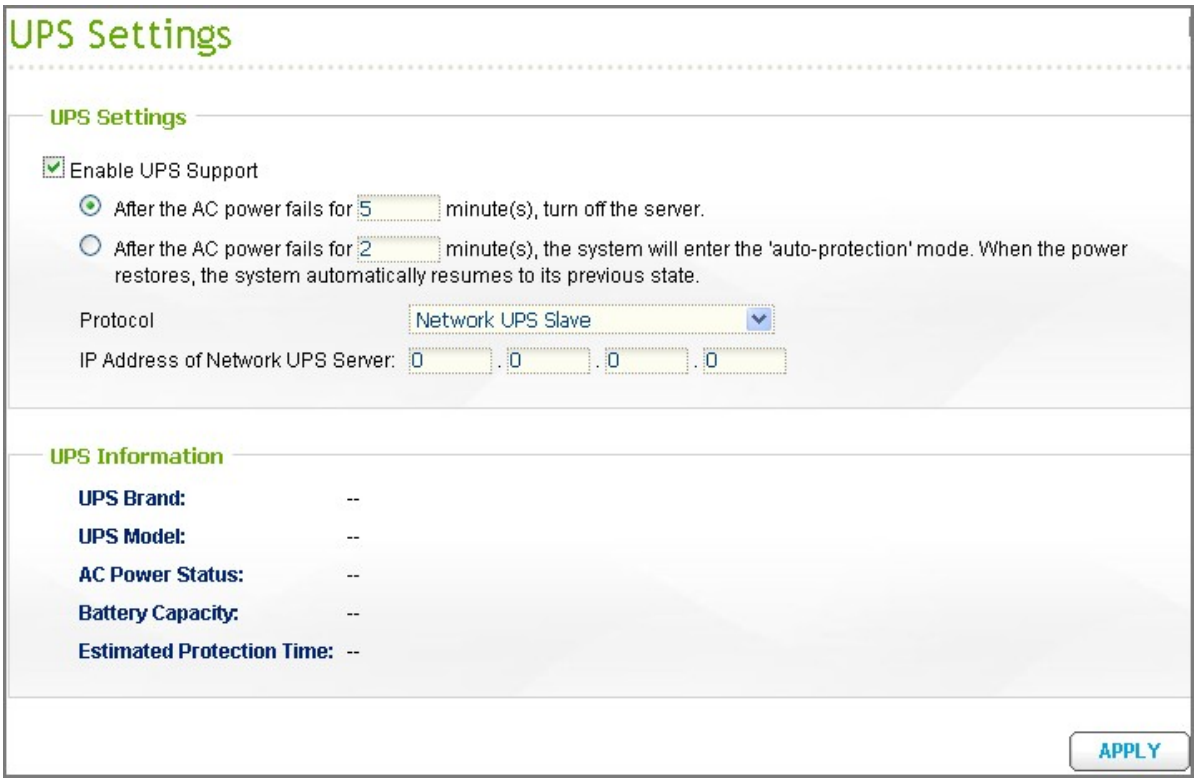


9. The network printer is now available for printing.



9.3 UPS Settings

By enabling the UPS (Uninterruptible Power Supply) support, you can protect your NAS from abnormal system shutdown caused by power disruption. In the event of a power failure the NAS will shut down automatically or enter auto-protection mode by probing the power status of the connected UPS unit.



Standalone mode - USB

To operate under USB standalone mode, follow the steps below:

1. Plug in the USB cable on the UPS to the NAS.
2. Select the option "Enable UPS Support".
3. Choose between whether the NAS will shut down or enter auto-protection mode after AC power fails. Specify the time in minutes that the NAS should wait before executing the option you have selected. After the NAS enters auto-protection mode, the NAS resumes the previous operation status when the power restores.
4. Click "Apply" to confirm.

Standalone mode - SNMP

To operate under SNMP standalone mode, follow the steps below:

1. Make sure the NAS is connected to the same physical network as the SNMP-based UPS.
2. Select the option "Enable UPS Support".
3. Choose between whether the NAS will shut down or enter auto-protection mode after AC power fails. Specify the time in minutes that the NAS should wait before executing the option you have selected. After the NAS enters auto-protection mode, the NAS resumes the previous operation status when the power restores.
4. Select "SNMP" from the "Protocol" drop down menu.
5. Enter the IP address of the SNMP-based UPS.
6. Click "Apply" to confirm.

Network master mode

A network UPS master is responsible for communicating with network UPS slaves on the same physical network about critical power status. To set up your NAS with UPS as network master mode, plug in the USB cable on the UPS to the NAS and follow the steps below:

1. Make sure the NAS is connected to the same physical network as the network UPS slaves.
2. Select the option "Enable UPS Support".
3. Choose between whether the NAS will shut down or enter auto-protection mode after AC power fails. Specify the time in minutes that the NAS should wait before executing the option you have selected. After the NAS enters auto-protection mode, the NAS resumes the previous operation status when the power restores.
4. Click "Enable network UPS master". This option appears only when your NAS is connected to the UPS by a USB cable.
5. Enter the "IP address" of other network UPS slaves to be notified in the event of power failure.
6. Click "Apply" to confirm and continue the setup for the NAS systems which operate in network slave mode below.

Network slave mode

A network UPS slave communicates with network UPS master to receive the UPS status. To set up your NAS with UPS as network slave mode, follow the steps below:

1. Make sure the NAS is connected to the same physical network as the network UPS master.
2. Select the option "Enable UPS Support".
3. Choose between whether the NAS will shut down or enter auto-protection mode after AC power fails. Specify the time in minutes that the NAS should wait before executing the option you have selected. After the NAS enters auto-protection mode, the NAS resumes the previous operation status when the power restores.
4. Select "USB slave mode" from the "Protocol" drop down menu.
5. Enter the IP address of the network UPS master.
6. Click "Apply" to confirm.

Note: To allow the 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 the "UPS Settings" before powering off or entering auto-protection mode.
If the power restores before the end of the waiting time, the NAS will remain in operation and cancel its power-off or auto-protection action.

Once the power restores:

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

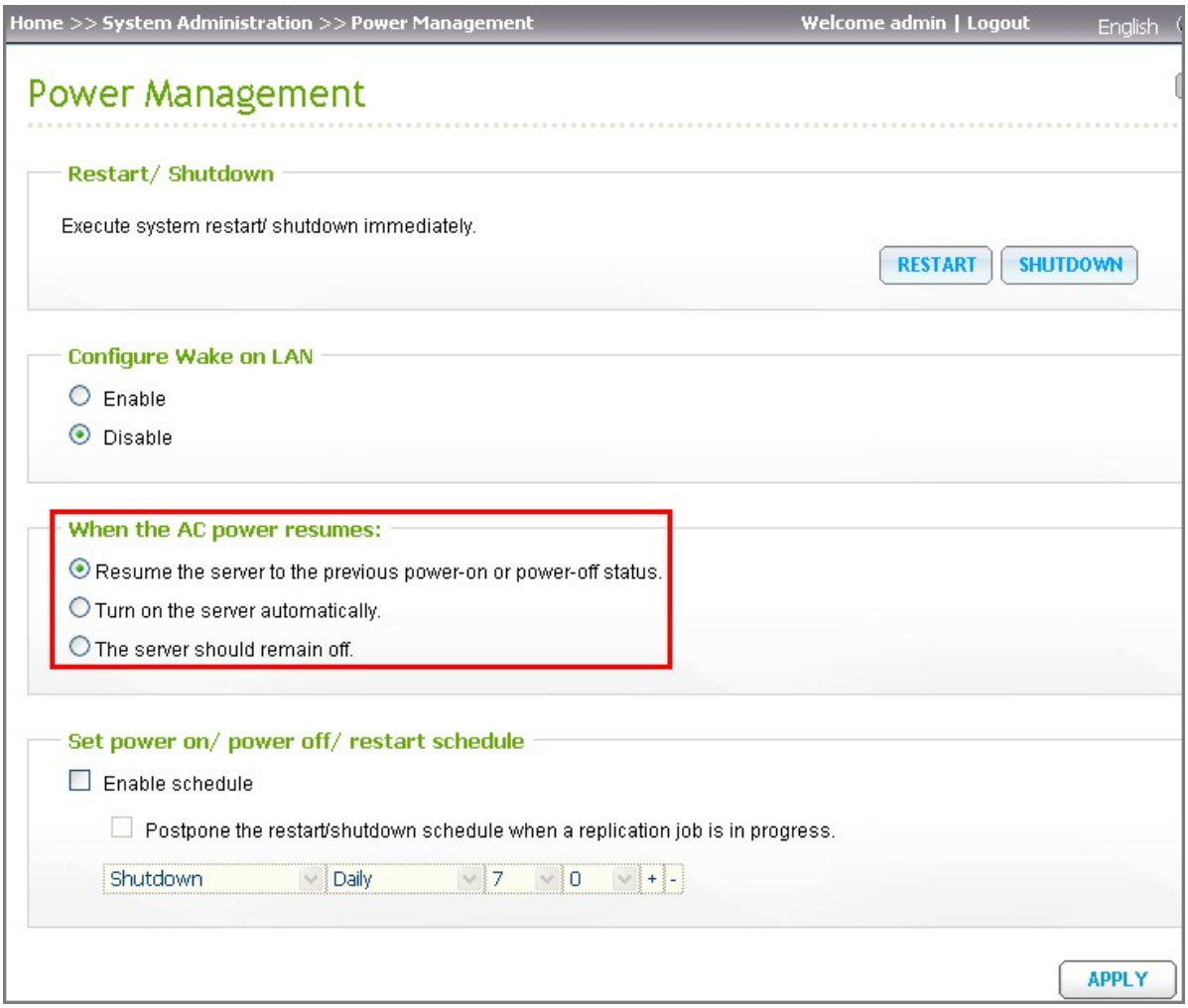
Difference between auto-protection mode and power-off mode

Mode	Advantage	Disadvantage
Auto-protection 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 NAS is required.

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

*This feature is not supported by TS-110, TS-119, TS-210, TS-219, TS-219P, TS-410, TS-419P, TS-410U, TS-419U, TS-112, TS-212, TS-412, TS-412U. Please visit http://www.qnap.com for details.

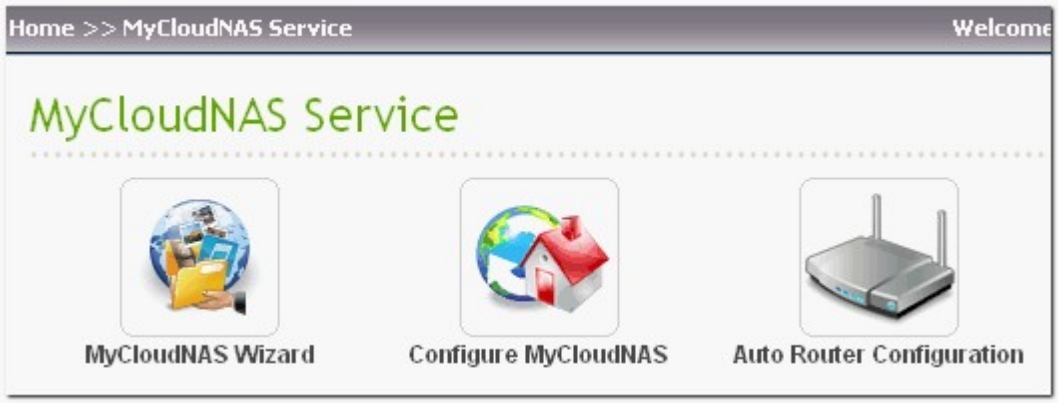
If the power restores after both the NAS and the UPS have been shut down, the NAS will react according to the settings in "System Administration" > "Power Management".


Home >> 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 a replication job is in progress.
Shutdown
Daily
7
0
+
-
APPLY

10. MyCloudNAS Service

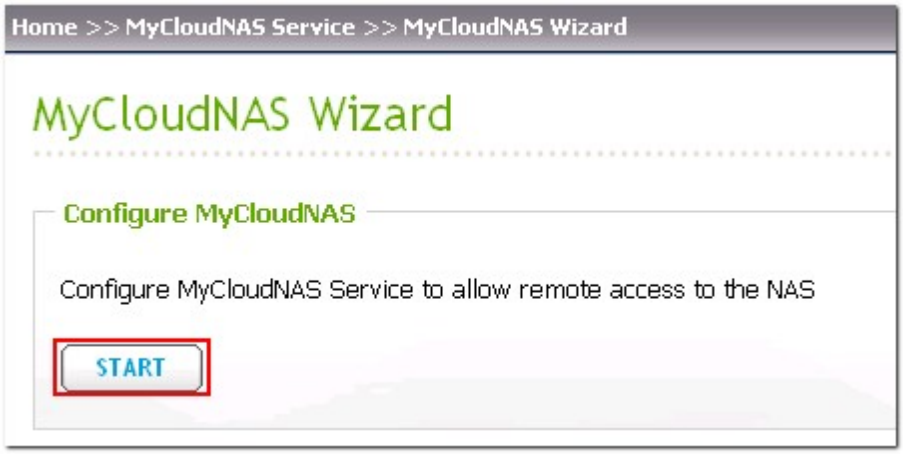
MyCloudNAS Service is a function which provides host name registration, mapping of the dynamic NAS IP to a domain name, and auto port mapping of UPnP router on the local network. Use MyCloudNAS Wizard to register a unique host name for the NAS, configure automatic port forwarding on the UPnP router, and publish NAS services for remote access over the Internet.

To use MyCloudNAS Service, make sure the NAS has been connected to a UPnP router and the Internet.



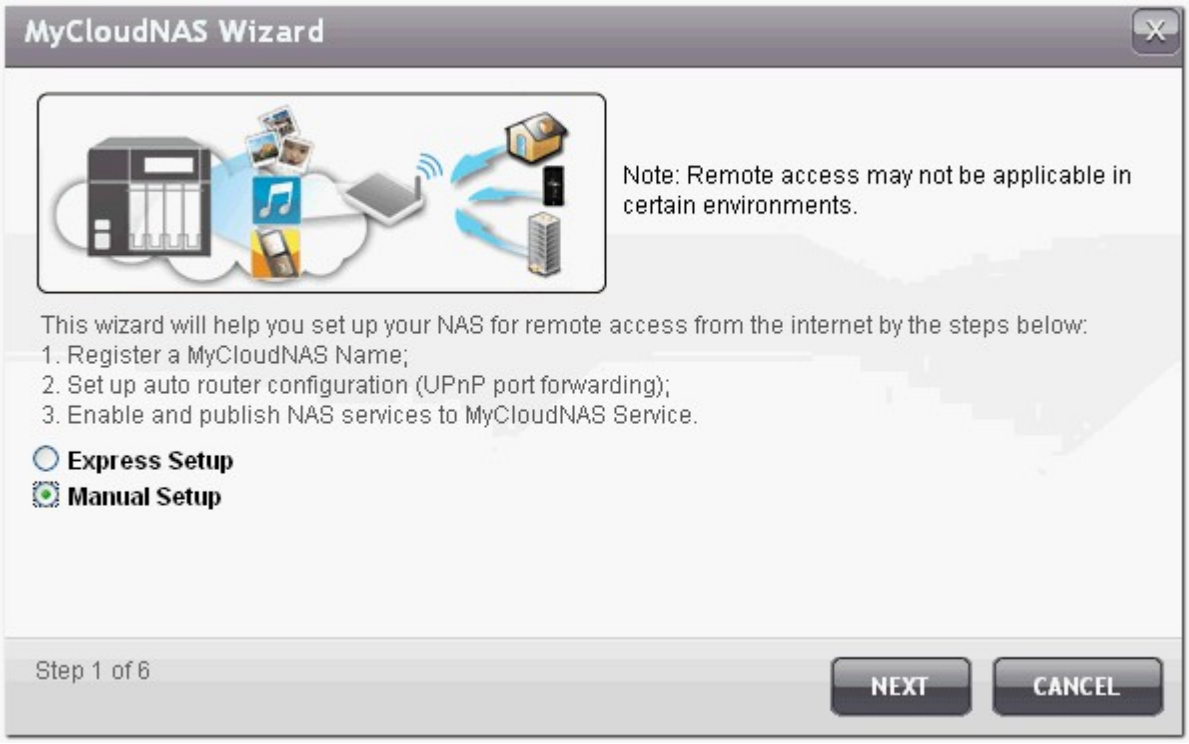
10.1 MyCloudNAS Wizard

The first time you use MyCloudNAS Service, you are recommended to use MyCloudNAS Wizard to complete the settings. The wizard shows up automatically if you have never configured the settings before. You can also click "Start" to use the wizard.

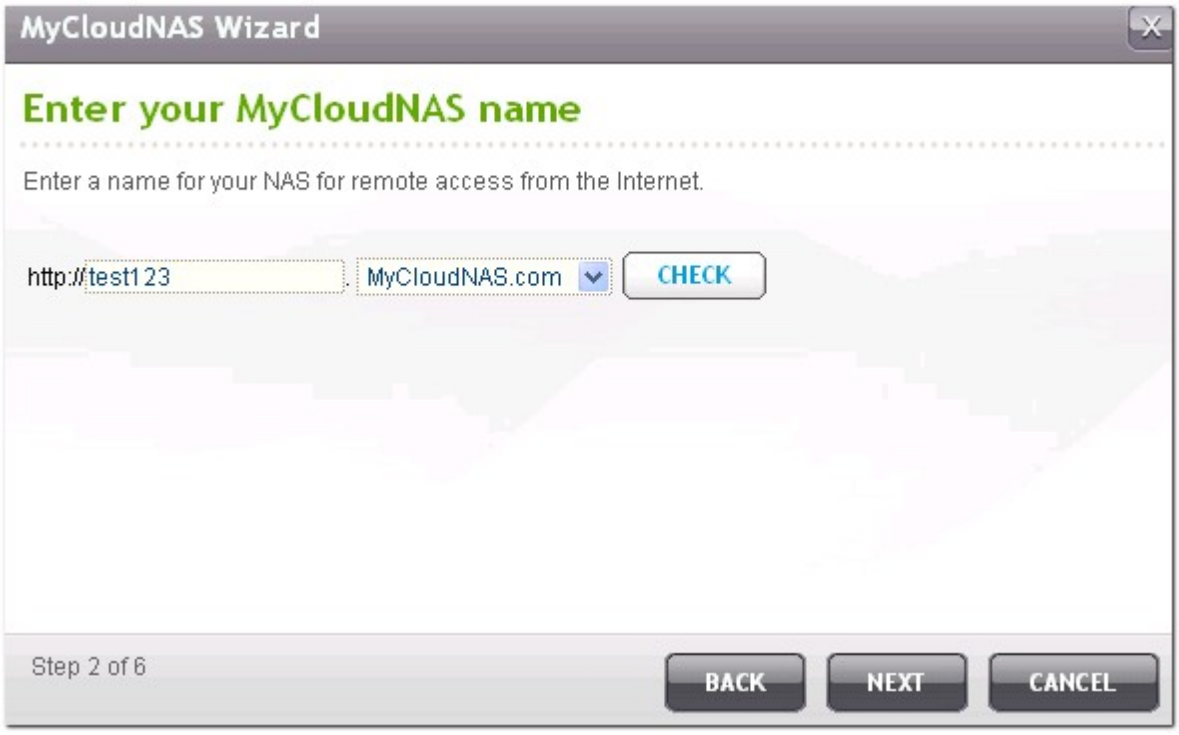


Follow the steps below to set up MyCloudNAS Service. To use MyCloudNAS Service, make sure you have connected the NAS to a UPnP router and the Internet.

1. Select to use Express Setup (default) or Manual Setup. Express Setup opens the ports for HTTP (8080), HTTP (80), FTP (21), FTPS (20) services automatically. To select the ports of the NAS services to open, select "Manual Setup". Click "Next".



2. Enter a host name (MyCloudNAS name) for your NAS and select a domain name. Click "Check" to check the availability of the host name. Then click "Next".



3. Select the ports to open on the UPnP router. The router will be configured to open and forward the ports to the NAS services automatically. Click "Next".

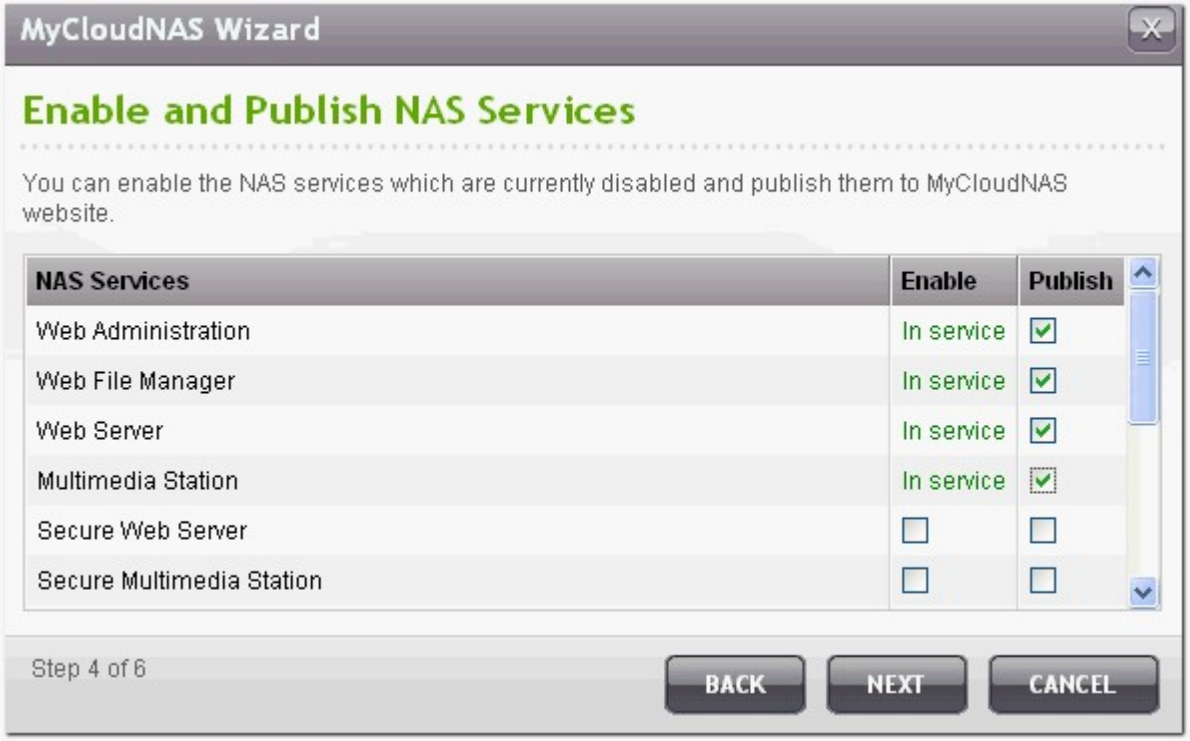
Port Number	NAS Services
HTTP (8080)	Web administration, Web File Manager
HTTP (80)	Web Server, Multimedia Station, QMobile
FTP, FTPS (21, 20)	FTP, FTPS
SSL (443)	Secure web administration
Telnet (13131)	Telnet server
SSH (22)	SSH, SFTP server
SSL (8081)	Secure web server
Rsync (873)	Remote replication

4. Publish NAS services.

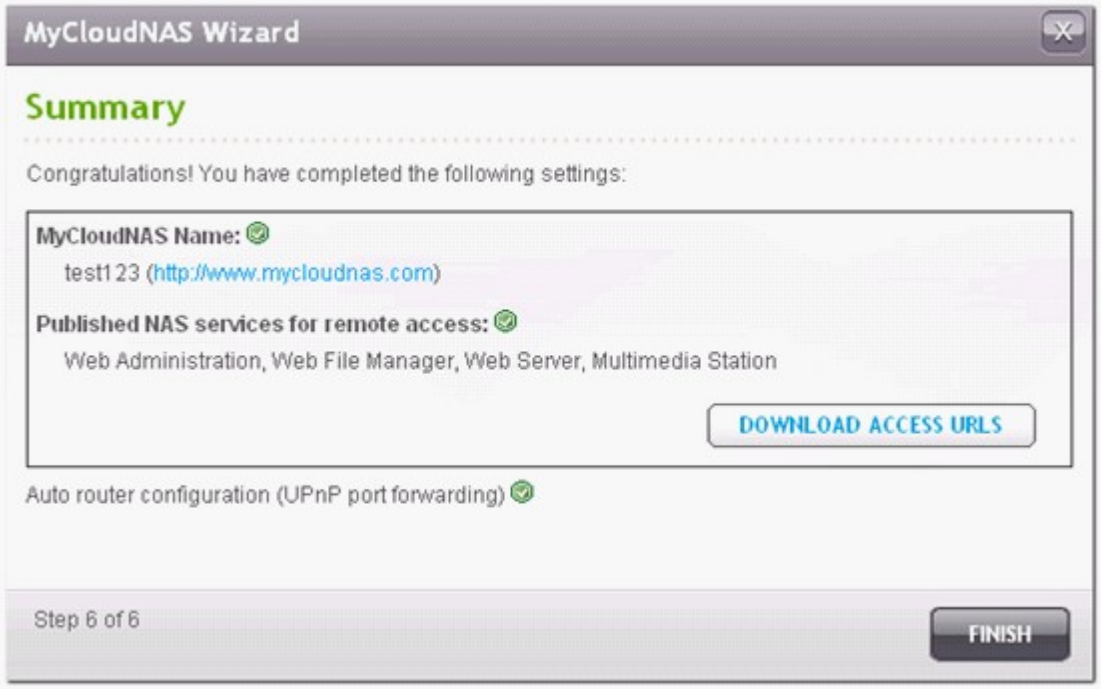
The NAS services which use the ports opened in the previous step will be shown. You can enable the services which are currently disabled and publish the web-based NAS services such as web administration, Web Server, Multimedia Server, and Web File Manager to http://www.mycloudnas.com. Click “Next”.

By enabling the NAS services in this step, they are opened for remote access even if they were not published.

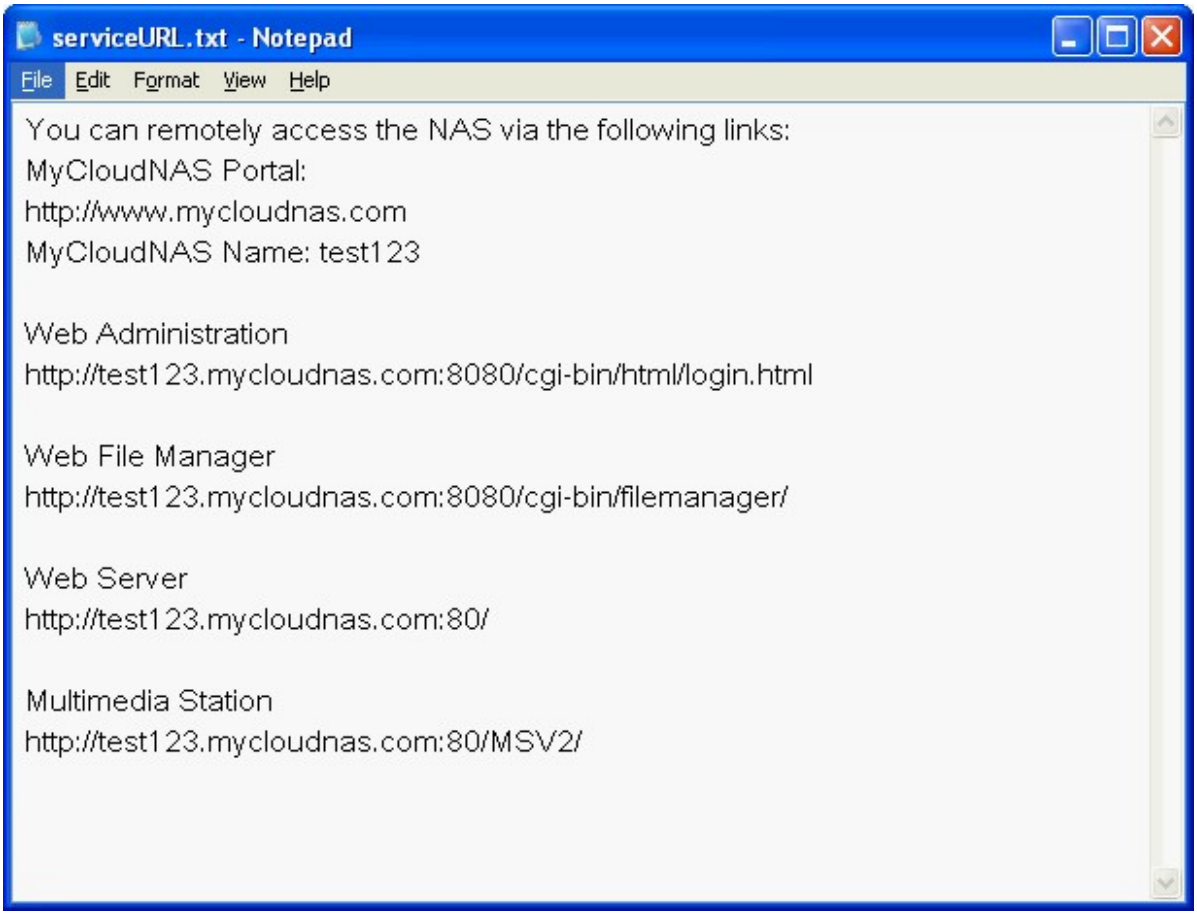
The NAS services can be published in private to allow only the users with the MyCloudNAS Access Code to view the private services on MyCloudNAS website. To use this feature, go to “MyCloudNAS Service” > “Configure MyCloudNAS” > “Publish Services”.



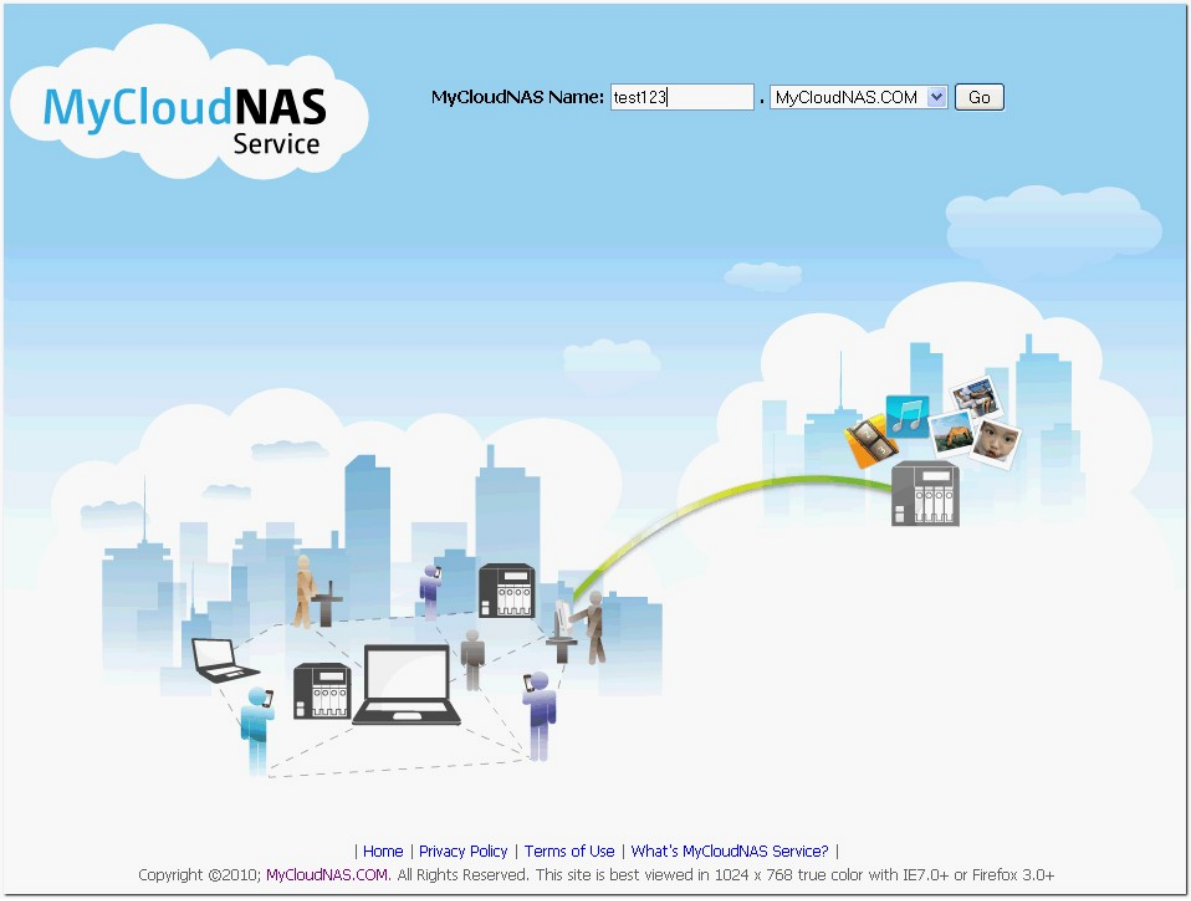
5. A summary will be shown. You can access the NAS by the MyCloudNAS name and download the URLs of the published services. Click "Finish" to exit.



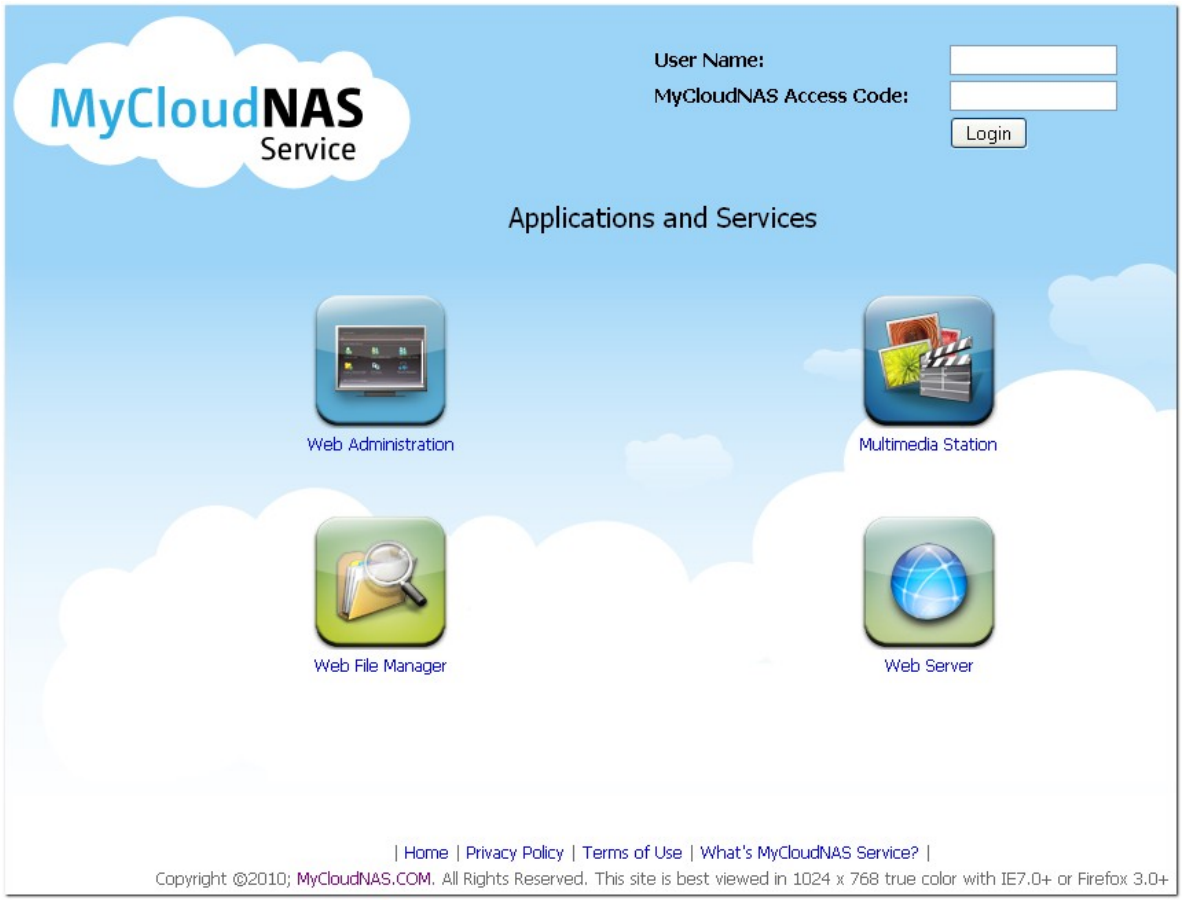
Copy the URLs and access the NAS services by the web browser.



6. To access the NAS services via MyCloudNAS website, go to http://www.mycloudnas.com, enter the MyCloudNAS name and select the correct domain name. Click "Go" to access the published NAS services.



7. Click the service icons and login the web-based NAS services.



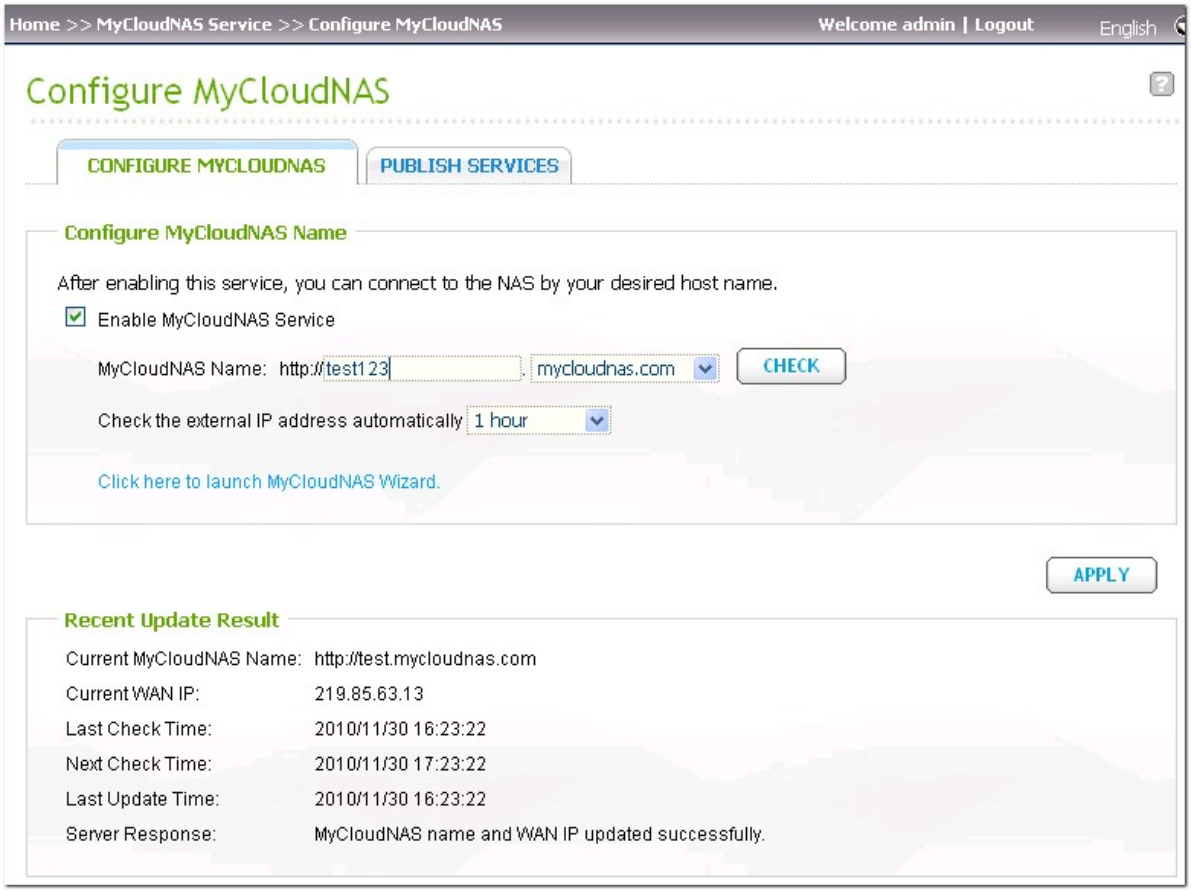
8. To view the private NAS services published on MyCloudNAS website, enter the user name and MyCloudNAS Access Code and click "Login".

To publish the NAS services in private and configure the MyCloudNAS Access Code, go to "MyCloudNAS Service" > "Configure MyCloudNAS" > "Publish Services".

9. Upon successful login, the public and private NAS services published on MyCloudNAS website will be shown. Click the service icons and login the web-based NAS services.

10.2 Configure MyCloudNAS

Enable MyCloudNAS Service in "MyCloudNAS Service" > "Configure MyCloudNAS". Register a host name for the NAS or change the host name anytime. Specify the time interval to check the external IP address of the NAS. The NAS will notify MyCloudNAS Service automatically if the WAN IP address of the NAS has changed. To use MyCloudNAS Service, make sure the NAS has been connected to a UPnP router and the Internet.

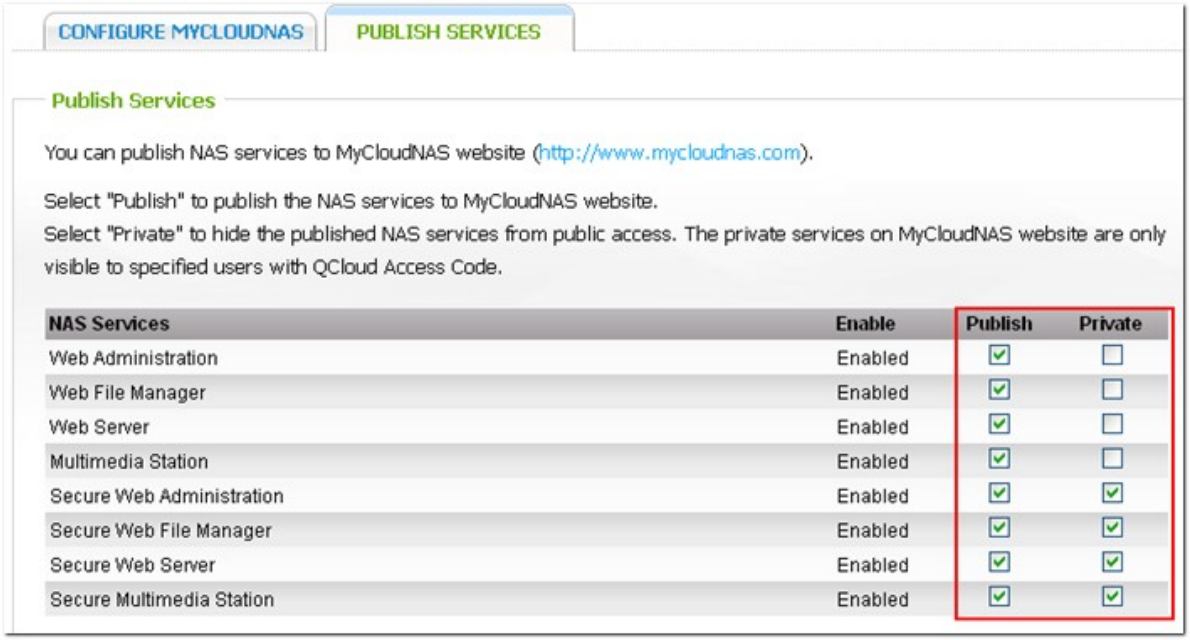


Note:

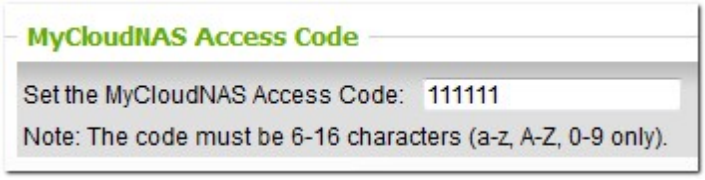
- The MyCloudNAS name of each QNAP NAS is unique. One MyCloudNAS name can only be used with one NAS.
- A registered MyCloudNAS name will expire in 120 days if your NAS have not been online within the period. Once the name is expired, it will be released for new registration by other users.

In “Configure MyCloudNAS” > “Publish Services”, the web-based NAS services are shown. Select “Publish” to publish the NAS services to MyCloudNAS website. Select “Private” to hide the published NAS services from public access. The private services on MyCloudNAS website are only visible to specified users with MyCloudNAS Access Code.

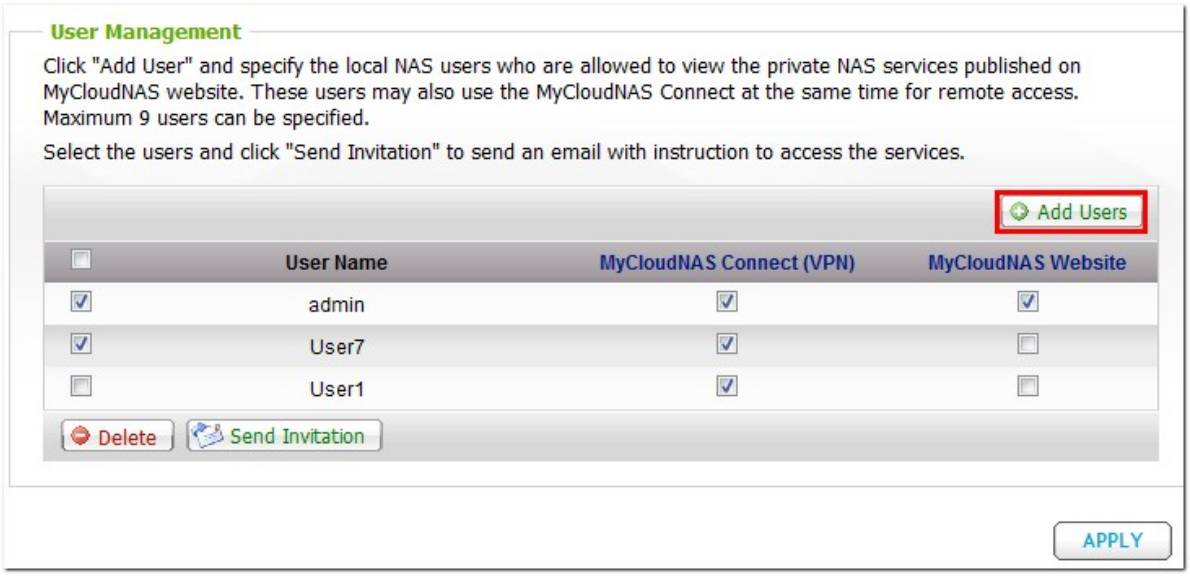
Note that if a disabled NAS service is published, the service will not be accessible even the corresponding icon is shown on MyCloudNAS website (http://www.mycloudnas.com).



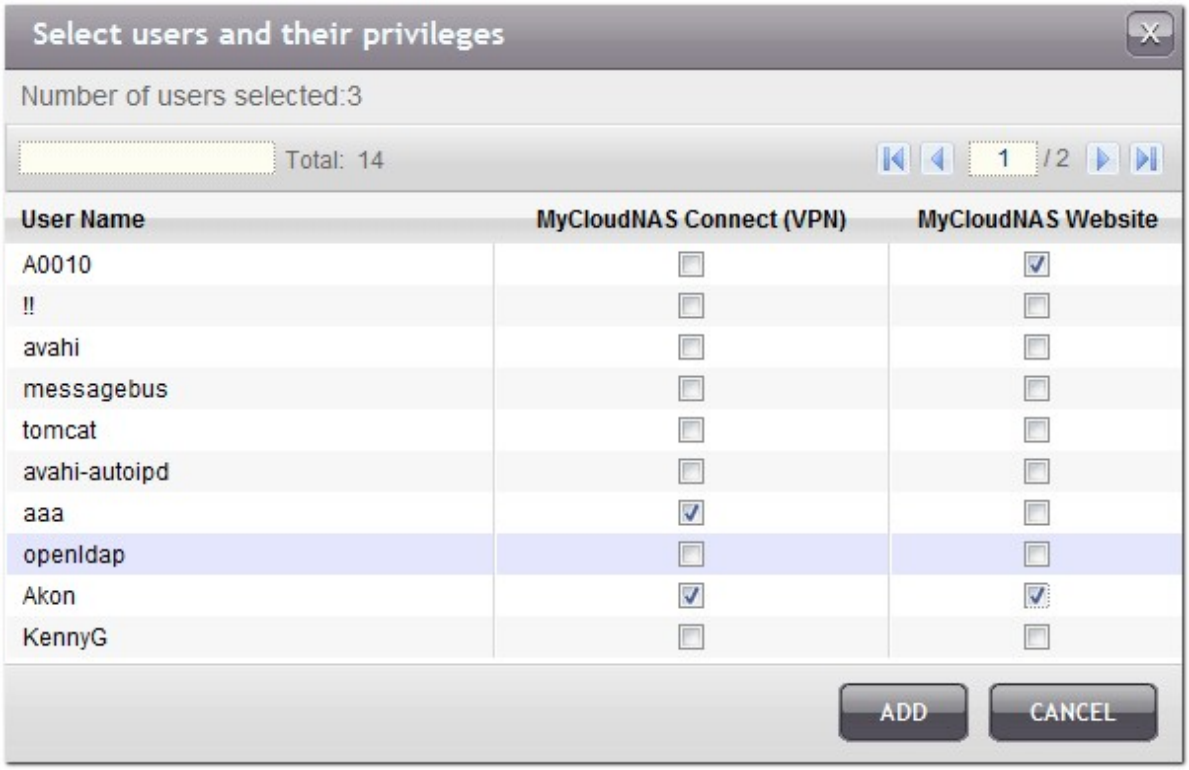
Set MyCloudNAS Access Code: Enter a code of 6-16 characters (a-z, A-Z, 0-9 only). The code is required when the NAS users attempt to view the private NAS services on MyCloudNAS website.



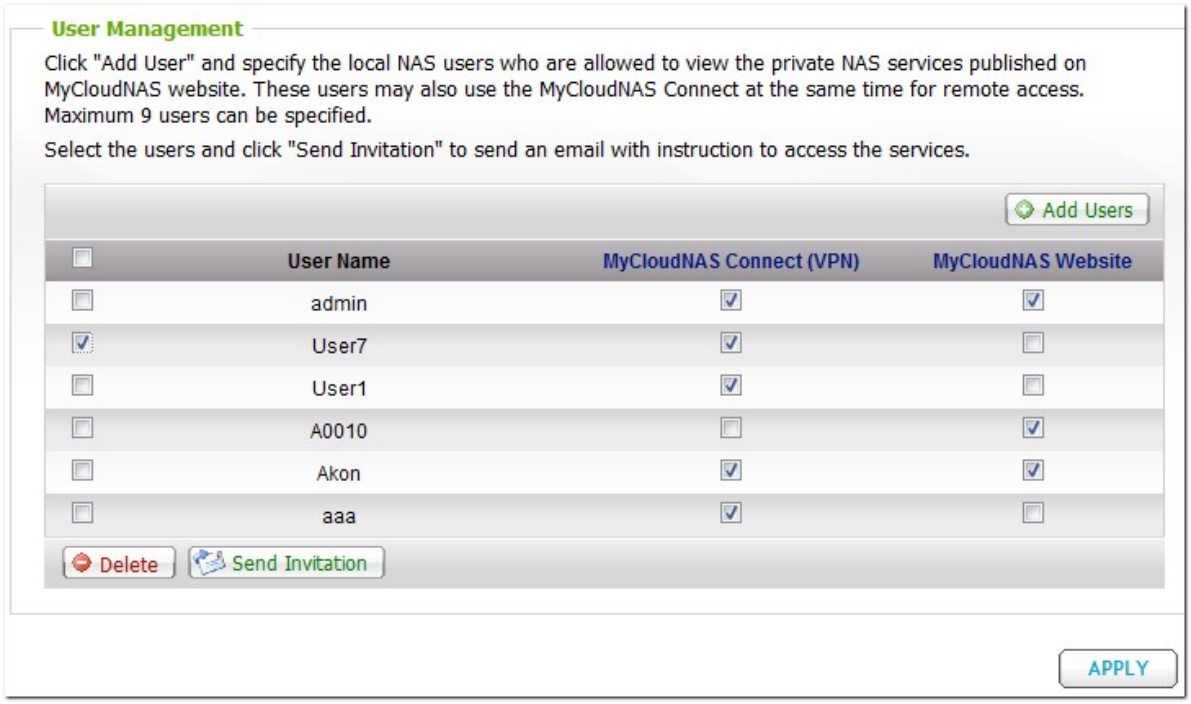
Click "Add Users" and specify maximum 9 local NAS users who are allowed to view the private NAS services published on MyCloudNAS website.



Select the connection method: MyCloudNAS Connect (VPN) utility and/or MyCloudNAS website. Click "Add".

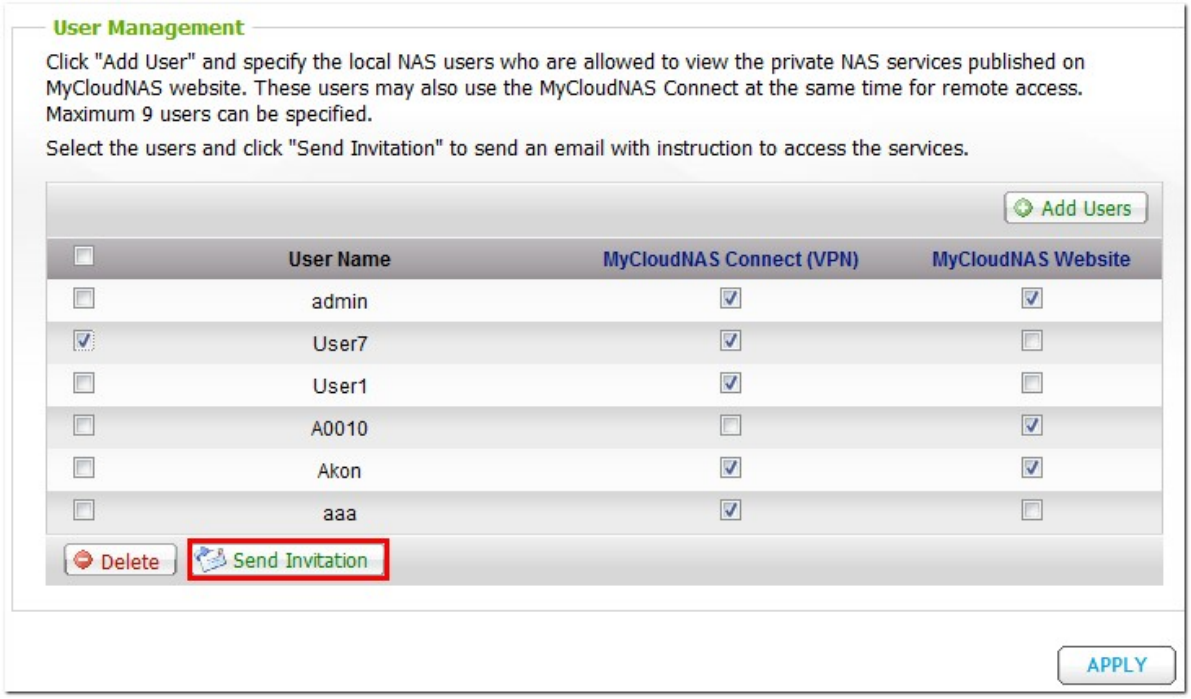

Select users and their privileges
Number of users selected:3
Total: 14
1
/ 2
User Name
MyCloudNAS Connect (VPN)
MyCloudNAS Website
A0010
!!
avahi
messagebus
tomcat
avahi-autoipd
aaa
openldap
Akon
KennyG
ADD
CANCEL

Click “Apply” to save the settings.



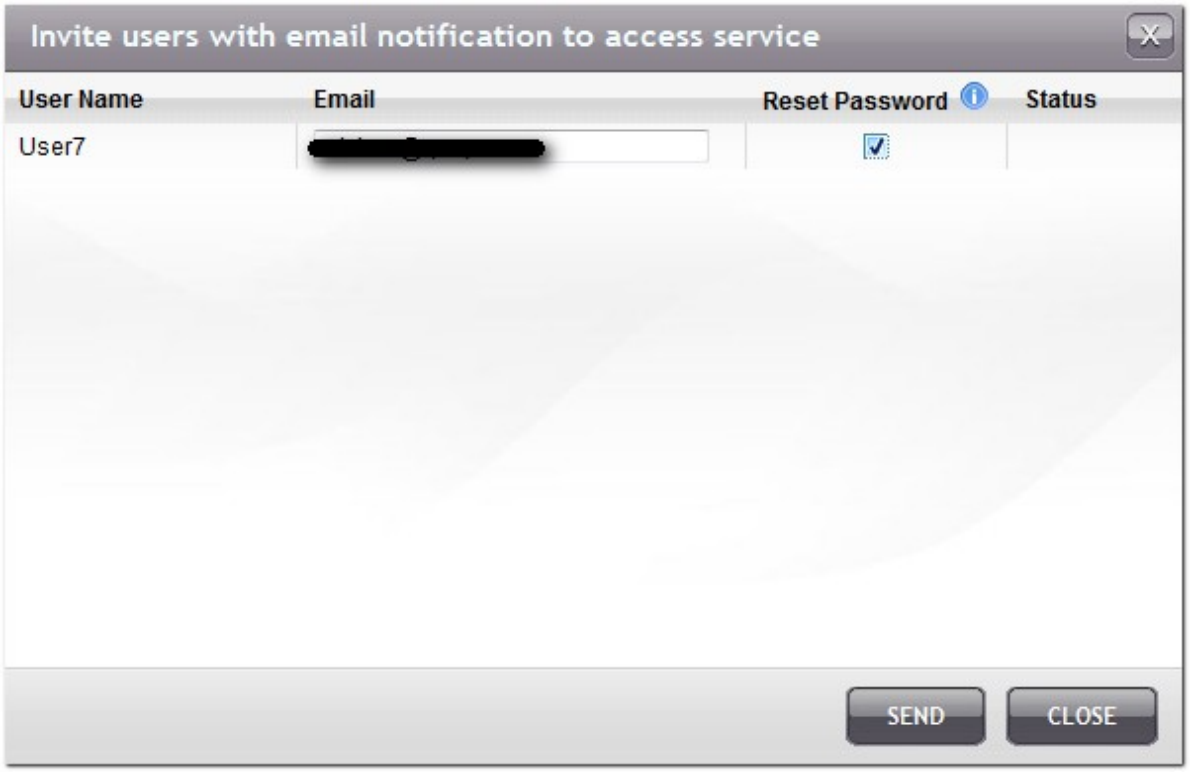
To send the instructions of using MyCloudNAS services to the users via email, select the user(s) and click “Send Invitation”.

Note: To use this function, the mail server settings must be properly configured in “System Administration” > “Notification” > “Configure SMTP Server”.



Enter the email address. To send the instructions with a link for users to reset their MyCloudNAS password, select "Reset Password". Click "Send".

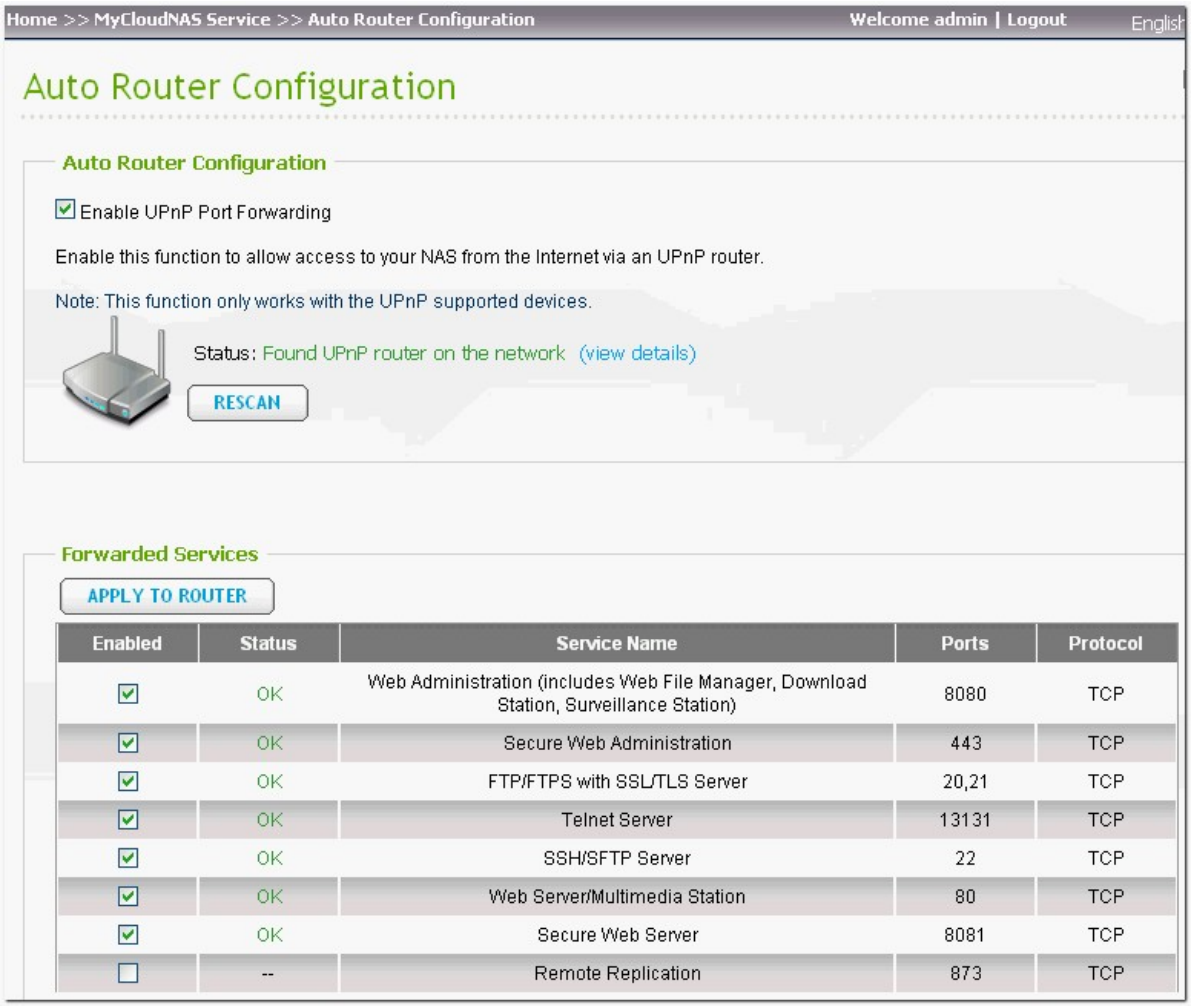
Note: The link for password reset will expire in 24 hours after the email is sent or after the user resets the password.



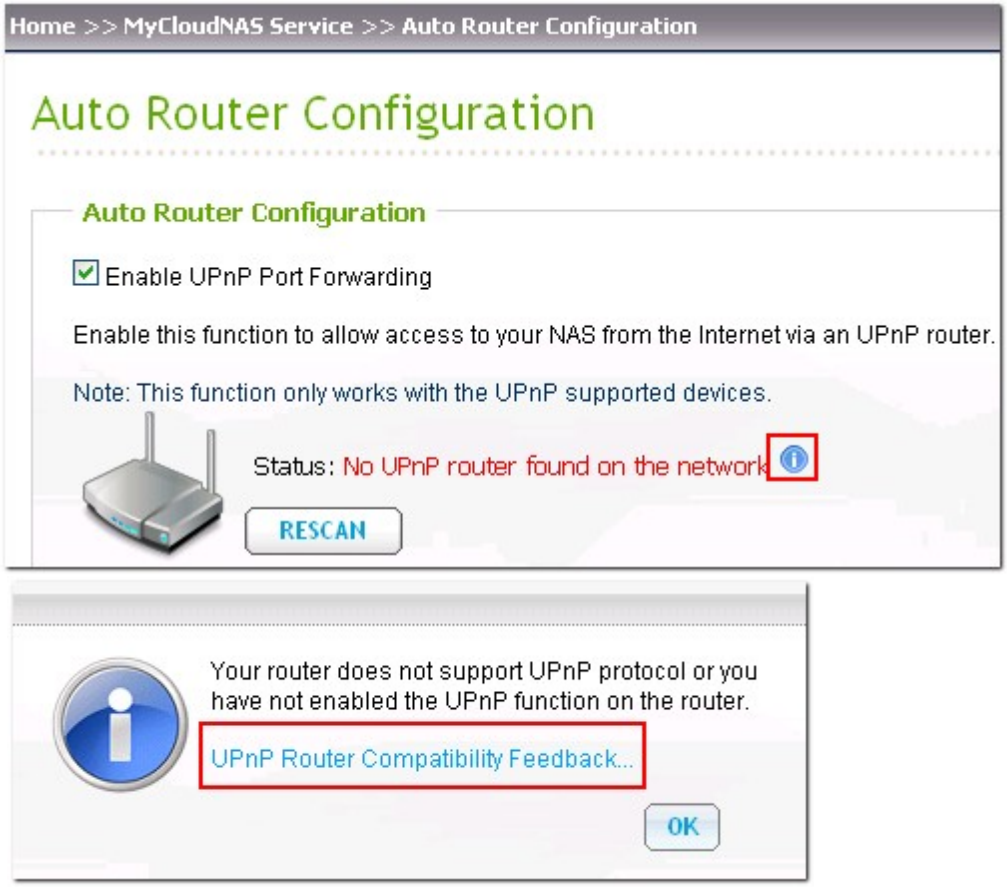
10.3 Auto Router Configuration

In "MyCloudNAS Service" > "Auto Router Configuration", you can enable or disable UPnP port forwarding. When this option is enabled, your NAS is accessible from the Internet via the UPnP router. Click "Rescan" to detect the router if no UPnP router is found on the local network. To view the router information, click "view details".

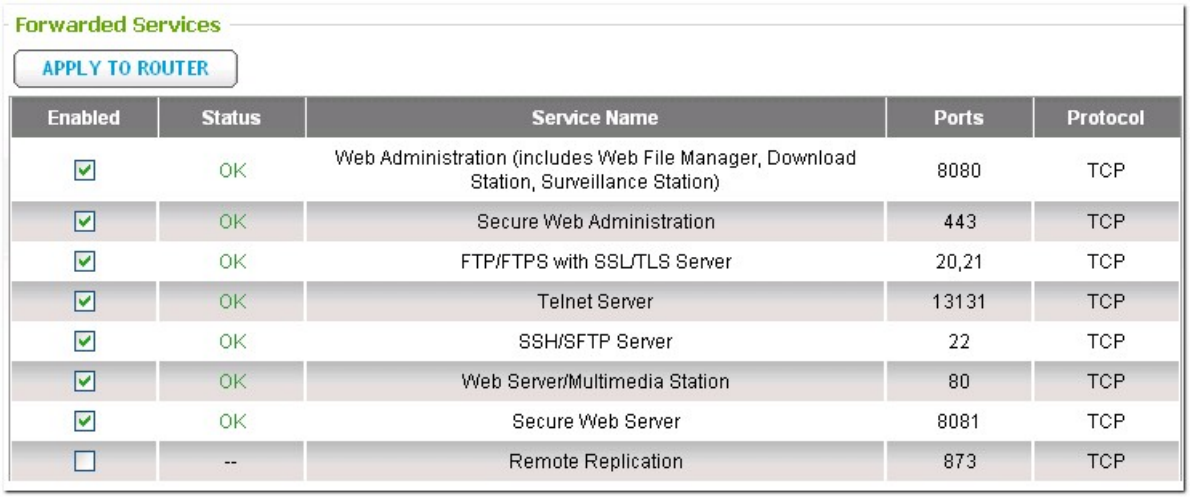
Note: If there is more than one router on the network, only the one which is set as the default gateway of the NAS will be detected.



If the UPnP router is incompatible with the NAS, click the icon and then click "UPnP Router Compatibility Feedback..." (http://www.qnap.com/onlinesupport.aspx) to contact the technical support.



Select the NAS services to be allowed for remote access. Click "Apply to router". The NAS will configure the port forwarding on the UPnP router automatically. You will then be able to access these NAS services from the Internet.



Enabled	Status	Service Name	Ports	Protocol
☑	OK	Web Administration (includes Web File Manager, Download Station, Surveillance Station)	8080	TCP
☑	OK	Secure Web Administration	443	TCP
☑	OK	FTP/FTPS with SSL/TLS Server	20,21	TCP
☑	OK	Telnet Server	13131	TCP
☑	OK	SSH/SFTP Server	22	TCP
☑	OK	Web Server/Multimedia Station	80	TCP
☑	OK	Secure Web Server	8081	TCP
☐	--	Remote Replication	873	TCP

Note: If the router does not support UPnP function, you need to configure port forwarding manually on the router. Please refer to the links below:

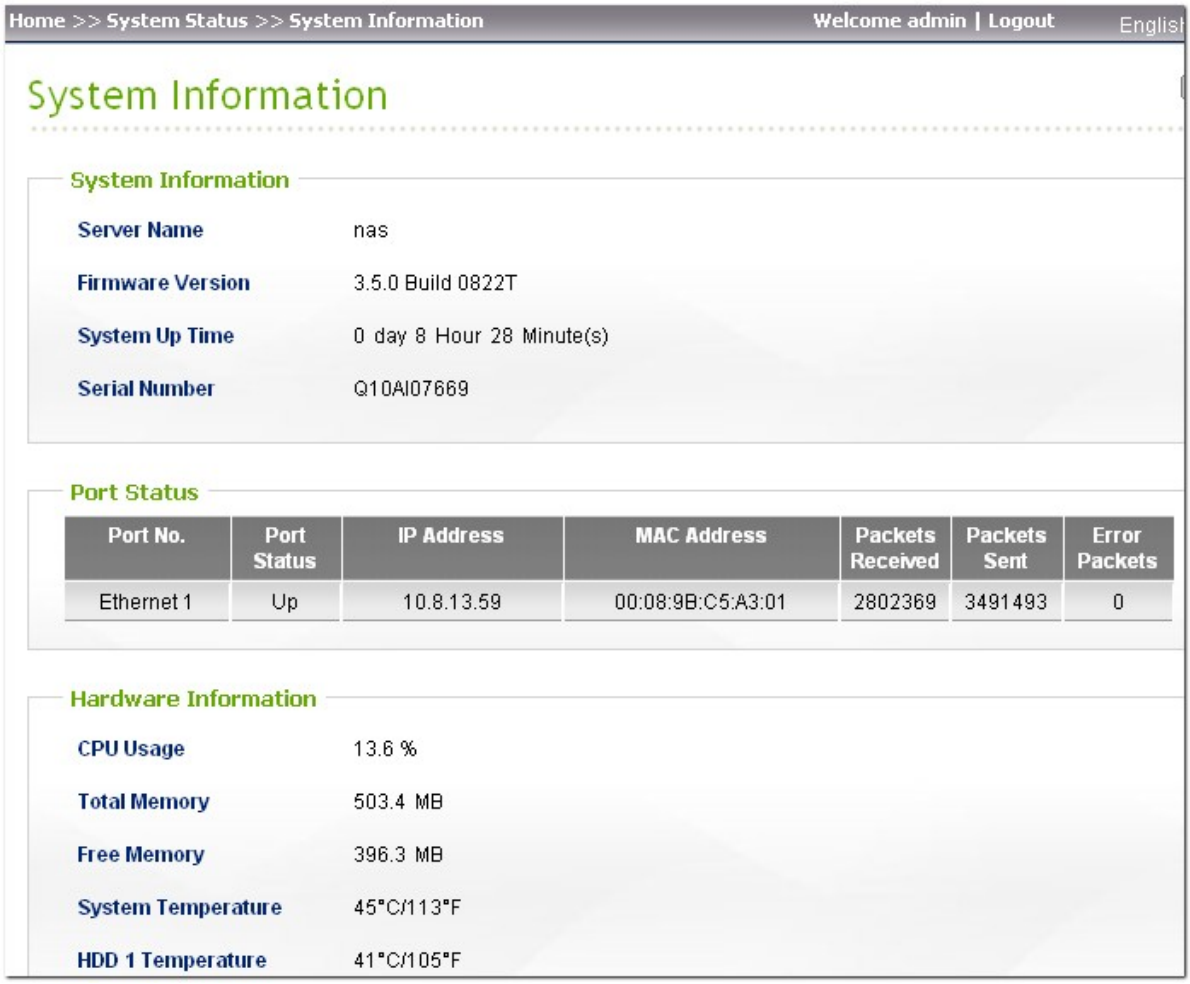
- Application note: http://www.qnap.com/pro_application.asp?ap_id=111
- FAQ: http://www.qnap.com/faq.asp
- UPnP router compatibility list: http://www.qnap.com/pro_compatibility.asp

11. System Status

System Information 636
System Service 637
Resource Monitor 638

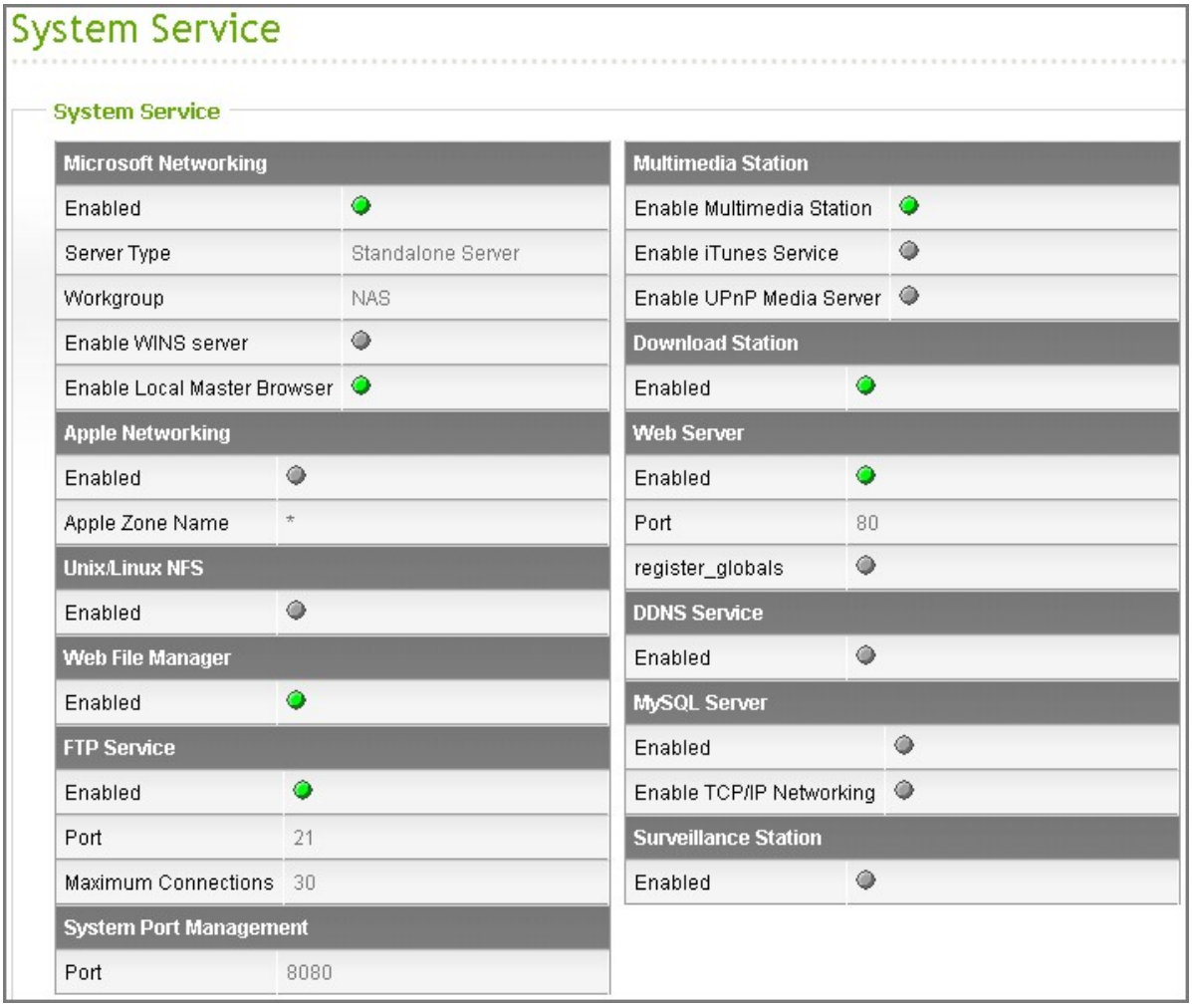
11.1 System Information

You can view the system information such as CPU usage and memory on this page.



11.2 System Service

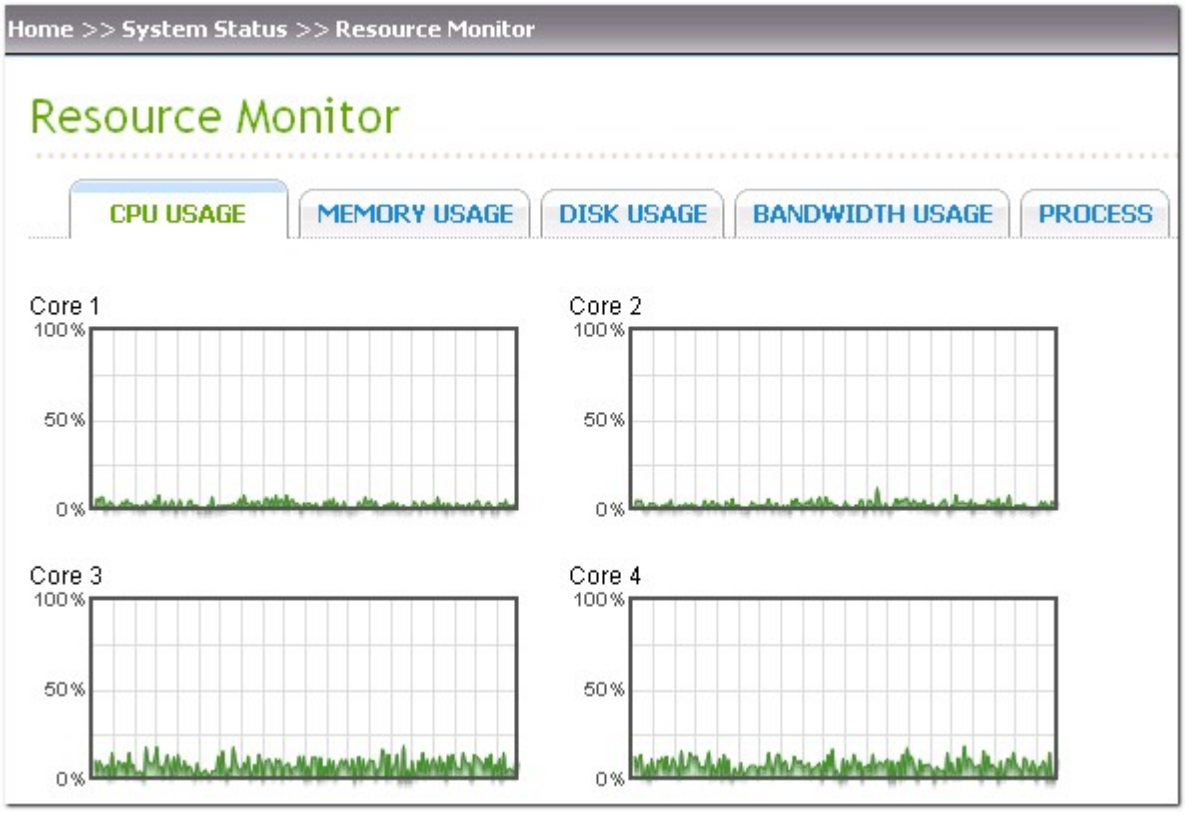
You can view the current network settings and status of the NAS in this section.



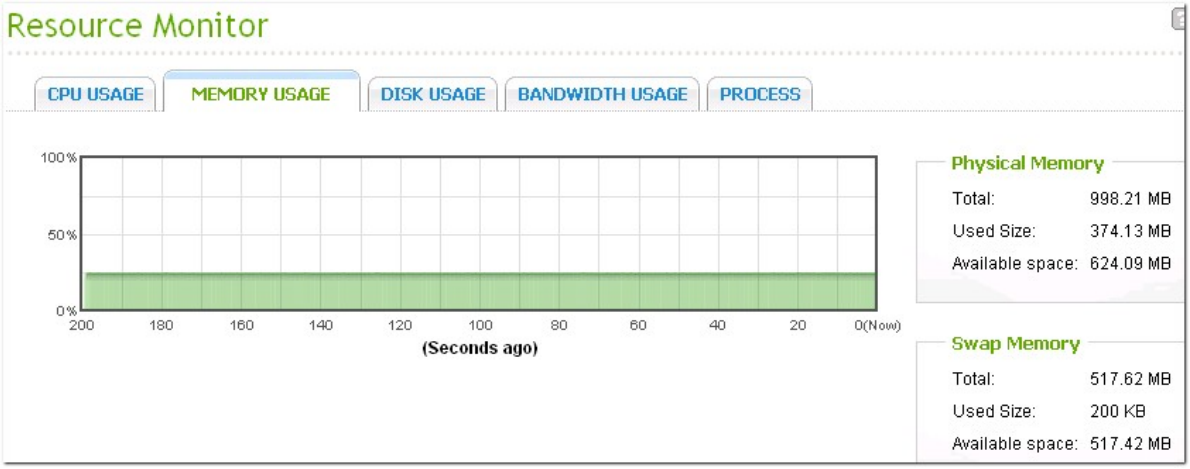
11.3 Resource Monitor

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

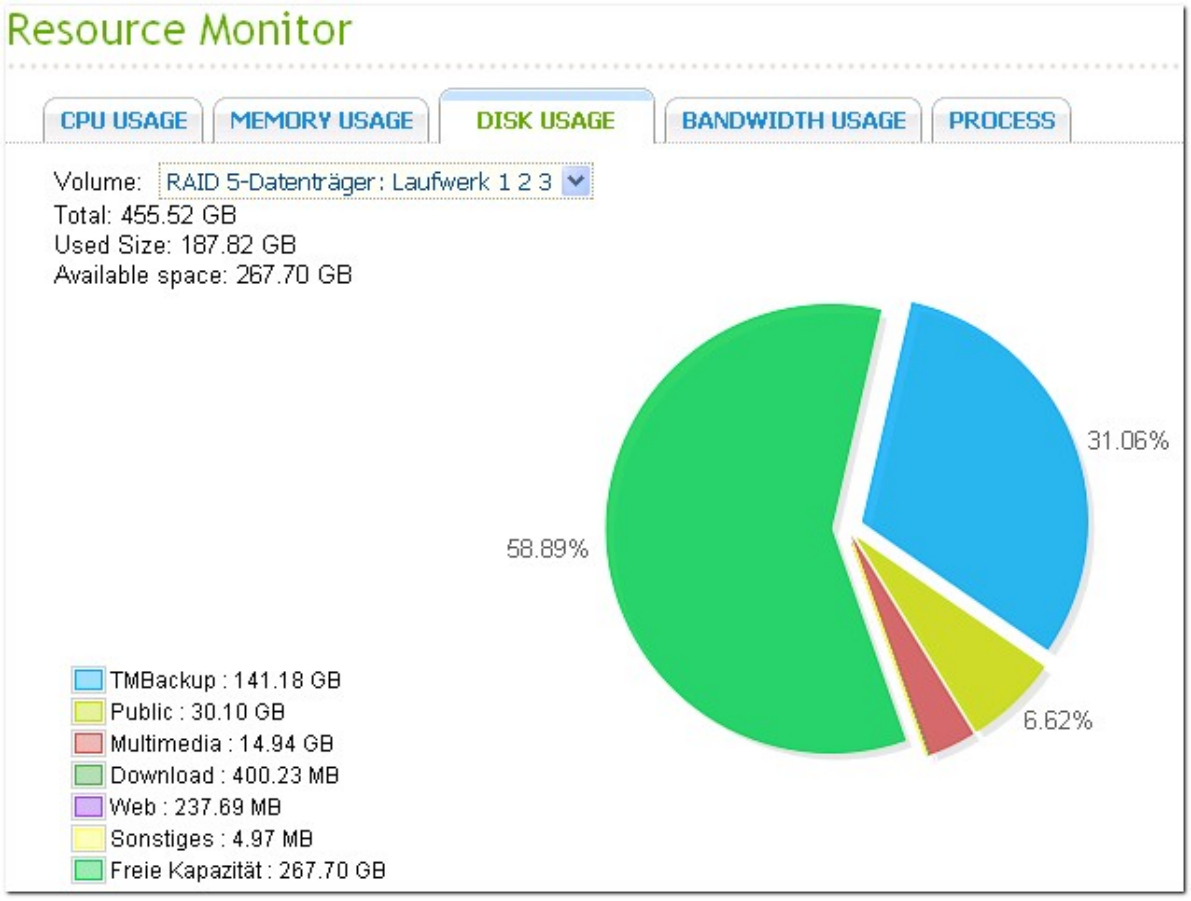
CPU Usage: This tab shows the CPU usage of the NAS.



Memory Usage: This tab shows the memory usage of the NAS by real-time dynamic graph.

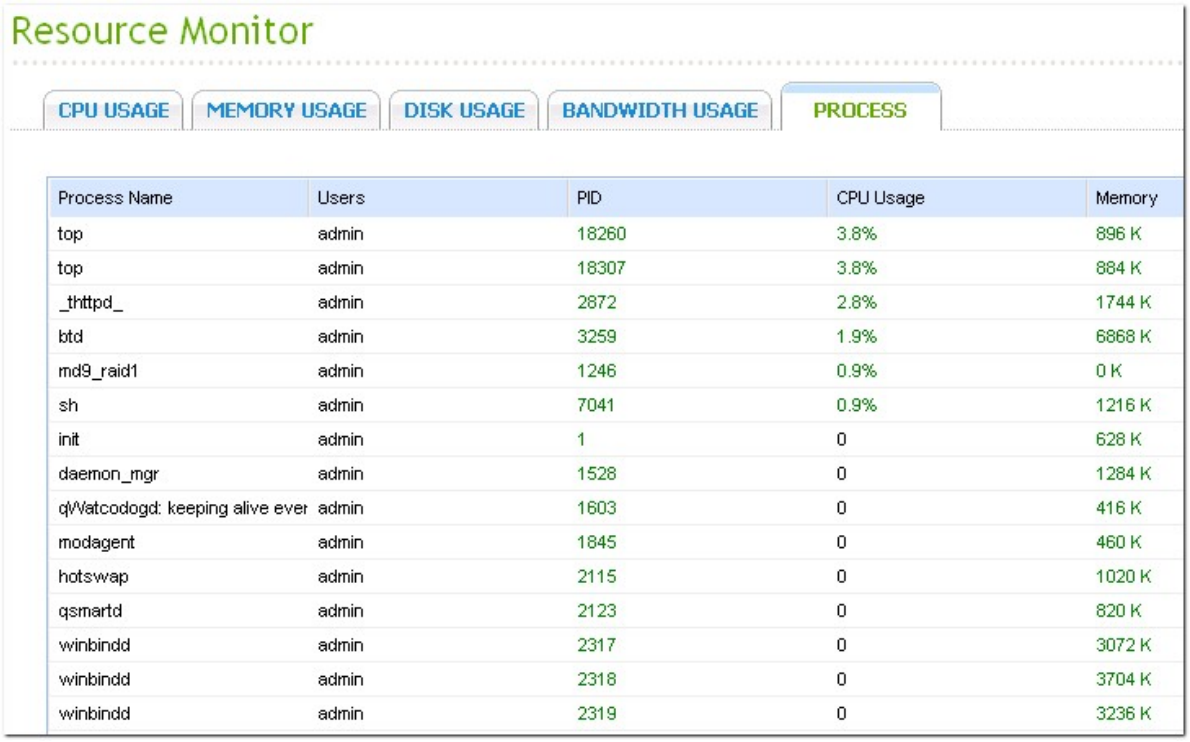


Disk Usage: This tab shows the disk space usage of each disk volume and its network shares.



Bandwidth Transfer: This tab provides information about bandwidth transfer of each available LAN port of the NAS.

Process: This tab shows information about the processes running on the NAS.



Process Name	Users	PID	CPU Usage	Memory
top	admin	18260	3.8%	896 K
top	admin	18307	3.8%	884 K
thttpd	admin	2872	2.8%	1744 K
btd	admin	3259	1.9%	6868 K
md9_raid1	admin	1246	0.9%	0 K
sh	admin	7041	0.9%	1216 K
init	admin	1	0	628 K
daemon_mgr	admin	1528	0	1284 K
qWatcodogd: keeping alive ever	admin	1603	0	416 K
modagent	admin	1845	0	460 K
hotswap	admin	2115	0	1020 K
qsmartd	admin	2123	0	820 K
winbindd	admin	2317	0	3072 K
winbindd	admin	2318	0	3704 K
winbindd	admin	2319	0	3236 K

12. Use the LCD Panel

This feature is only provided by the NAS models with LCD panels. Please visit http://www.qnap.com for details.

You can use the LCD panel to perform disk configuration and view the system information.

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

N	A	S	5	F	4	D	E	3						
1	6	9	.	2	5	4	.	1	0	0	.	1	0	0

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:

C	o	n	f	i	g	.		D	i	s	k	s	?		
→	R	A	I	D	5										

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

C	h	o	o	s	e		R	A	I	D	5	?		
→	Y	e	s			N	o							

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 connect to the RAID volume, for example, create 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 (varies depending on the 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 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, login the web-based administration interface of the NAS with an administrator account and change the settings in “Device Configuration” > “Disk volume Encryption Management”.

E	n	c	r	y	p	t		V	o	l	u	m	e	?
→	Y	e	s			N	o							

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

C	r	e	a	t	i	n	g	.	.	.				
R	A	I	D	5		F	a	i	l	e	d			

*This feature is not supported by TS-110, TS-119, TS-210, TS-219, TS-219P, TS-410, TS-419P, TS-410U, TS-419U, TS-119P+, TS-219P+, TS-419P+, TS-112, TS-212, TS-412, TS-419U+, TS-412U.

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

View system information by the LCD panel

When the LCD panel shows the NAS 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

TCP/IP

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

1. LAN IP Address
2. LAN Subnet Mask
3. LAN Gateway
4. LAN PRI. DNS
5. LAN SEC. DNS
6. Enter Network Settings
   - Network Settings – DHCP
   - Network Settings – Static IP*
   - Network Settings – BACK
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.**

Physical disk

In Physical disk, you can view the following options:

1. Disk Info
2. Back to Main Menu

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

D	i	s	k	:	1		T	e	m	p	:	5	0	°	C
S	i	z	e	:		2	3	2		G	B				

Volume

This section shows the hard drive 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.

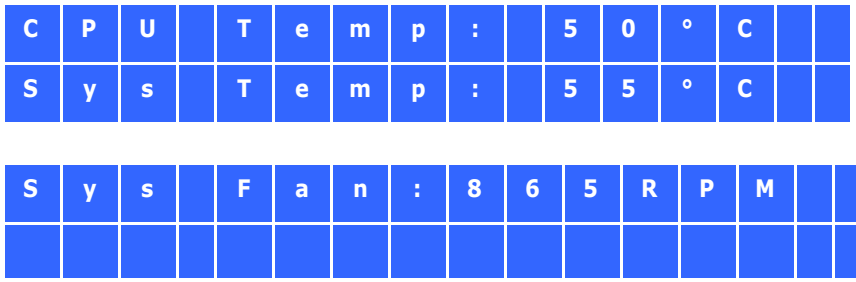
R	A	I	D	5							7	5	0	G	B
D	r	i	v	e		1	2	3	4						

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

System

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



Shut down

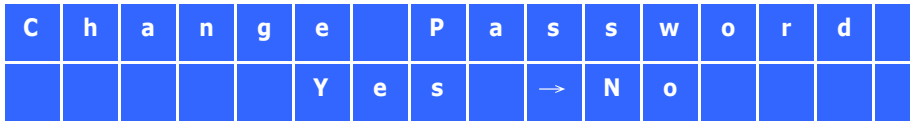
Use this option to turn off the NAS. Press the "Select" button to select "Yes". Then press the "Enter" button to confirm.

Reboot

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

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.



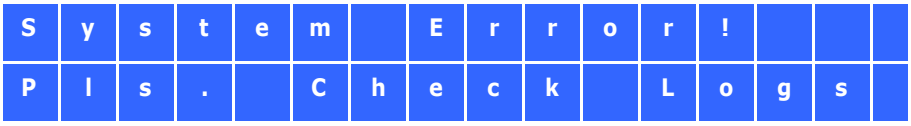
You may enter a password of maximum 8 numeric characters (0-9). When the cursor moves to "OK", press the "Enter" button. Verify the password to confirm the changes.

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.

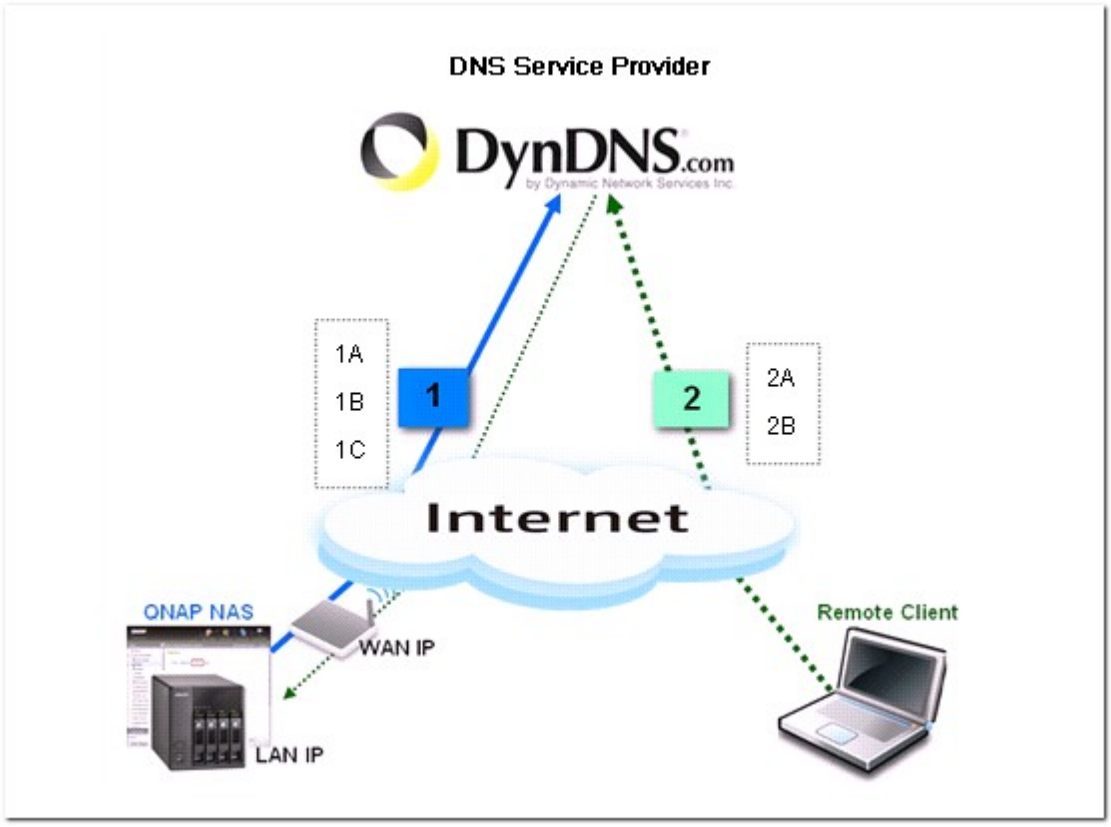


System Message	Description
Sys. Fan Failed	The system fan fails.
Sys. Overheat	The system overheats.
HDD Overheat	A hard drive overheats.
CPU Overheat	The CPU overheats.
Network Lost	Both LAN 1 and LAN 2 are disconnected in failover or load balancing mode.
LAN1 Lost	LAN 1 is disconnected.
LAN2 Lost	LAN 2 is disconnected.
HDD Failure	A hard drive fails.
Vol1 Full	The disk volume (1) is full.
HDD Ejected	A hard drive is ejected.
Vol1 Degraded	The disk volume (1) is in degraded mode.
Vol1 Unmounted	The disk volume (1) is unmounted.
Vol1 Nonactivate	The disk volume (1) is inactive.

13. Connect to QNAP NAS from the Internet (DDNS Service)

Set up DDNS Service for Remote Internet Access to QNAP NAS

Dynamic Domain Name Service (DDNS) is a service used to map a domain name to the dynamic IP address of a network device. QNAP NAS supports DDNS for quick system access on the Internet by an easy-to-remember domain name (URL) instead of a lengthy IP address. Once the IP is changed, the NAS will automatically update the information to the DDNS provide to ensure it is always available for remote access.



1A: Register a domain name, e.g. qnap.dyndns-office.com, from a DDNS provider.
1B: Enable DDNS service and fill in the DDNS account information on the NAS.
1C: QNAP NAS will update the WAN IP information to the DDNS provider automatically.

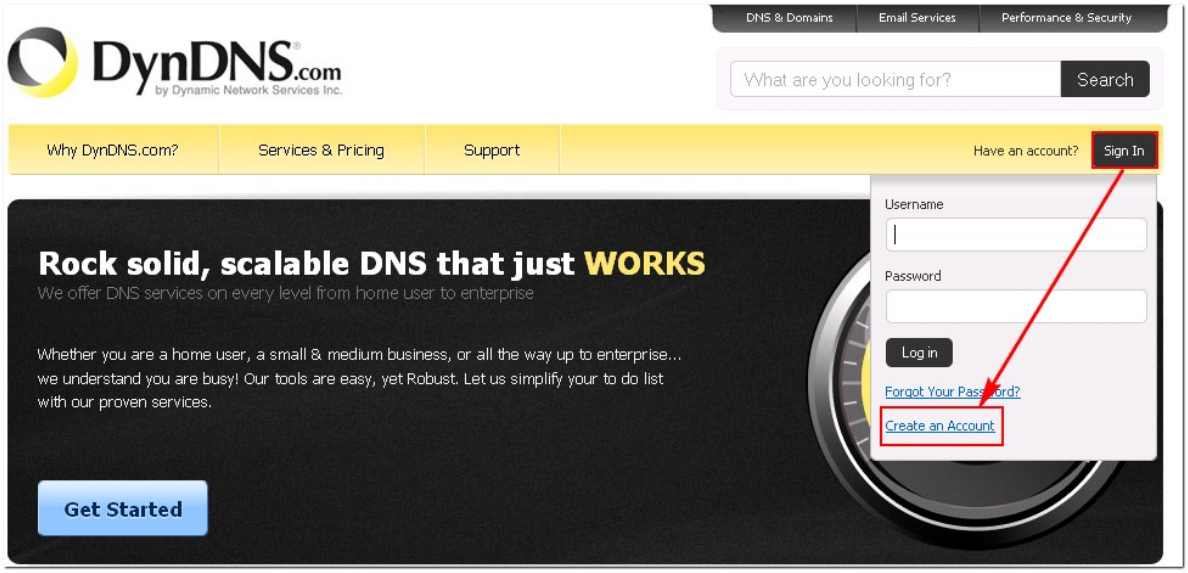
2A: Remotely connect to the NAS by the domain name you registered: http://qnap.dyndns-office.com:8080 from any PC.
2B: The DDNS provider will map the WAN IP updated by QNAP NAS to the domain name should the IP change.

Register DDNS service

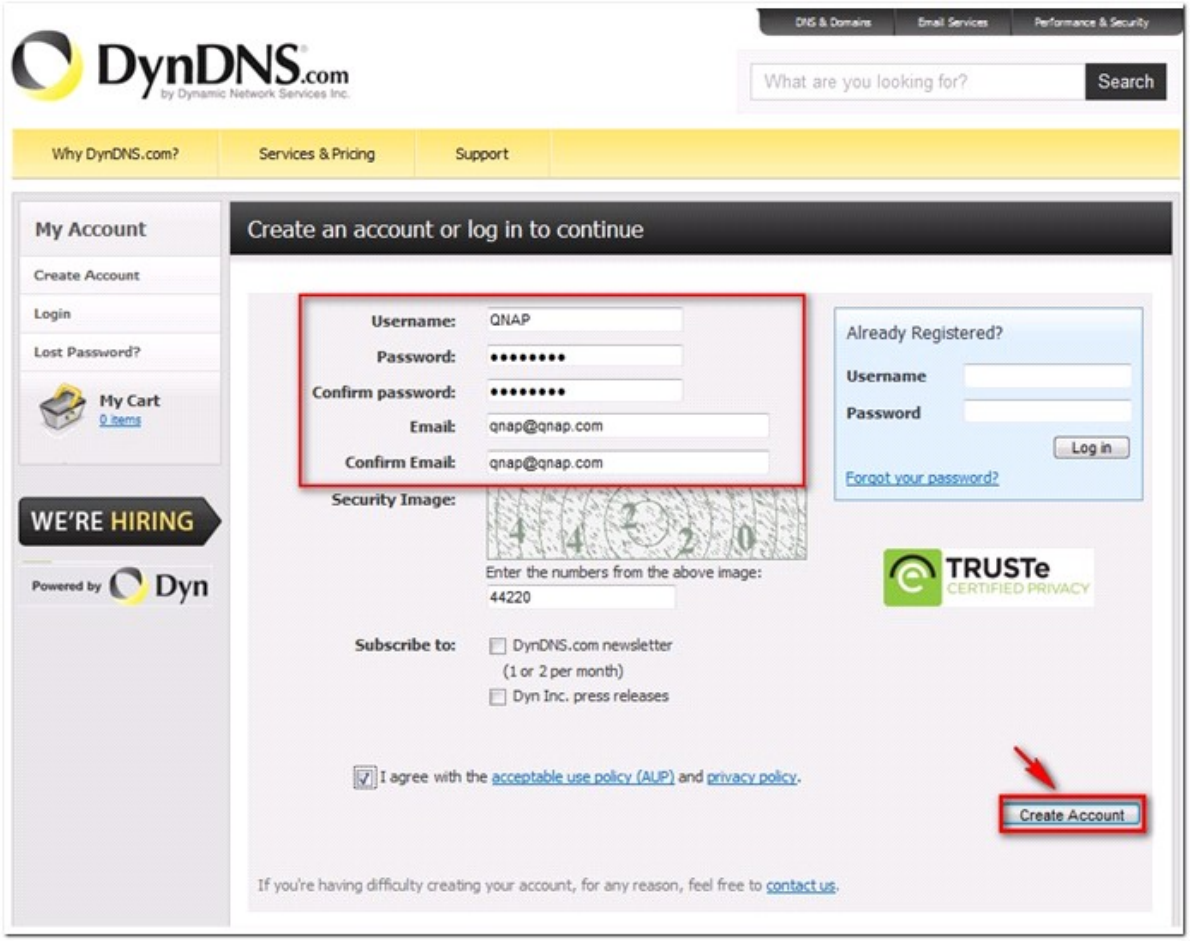
If the NAS is set up to use a dynamic IP address, you may register a free DDNS (dynamic DNS) account from a DNS service provider and assign a unique host name for easy access to the NAS on the Internet. To register a DDNS account, please refer to the steps below:

1. Choose a DNS service provider. QNAP NAS currently supports the following DDNS service providers:
   http://www.dyndns.com
   http://update.ods.org
   http://www.dhs.org
   http://www.dyns.cx
   http://www.3322.org
   http://www.no-ip.com

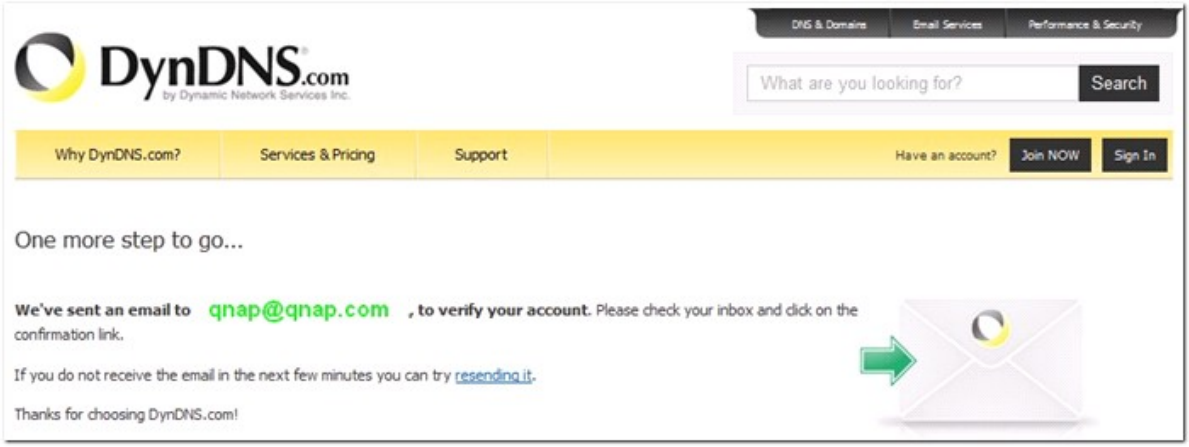
2. Create an account. Here we take http://www.dyndns.org as an example. Visit http://www.dyndns.org. Click "Sign In" and "Create an Account" to register a DynDNS account.



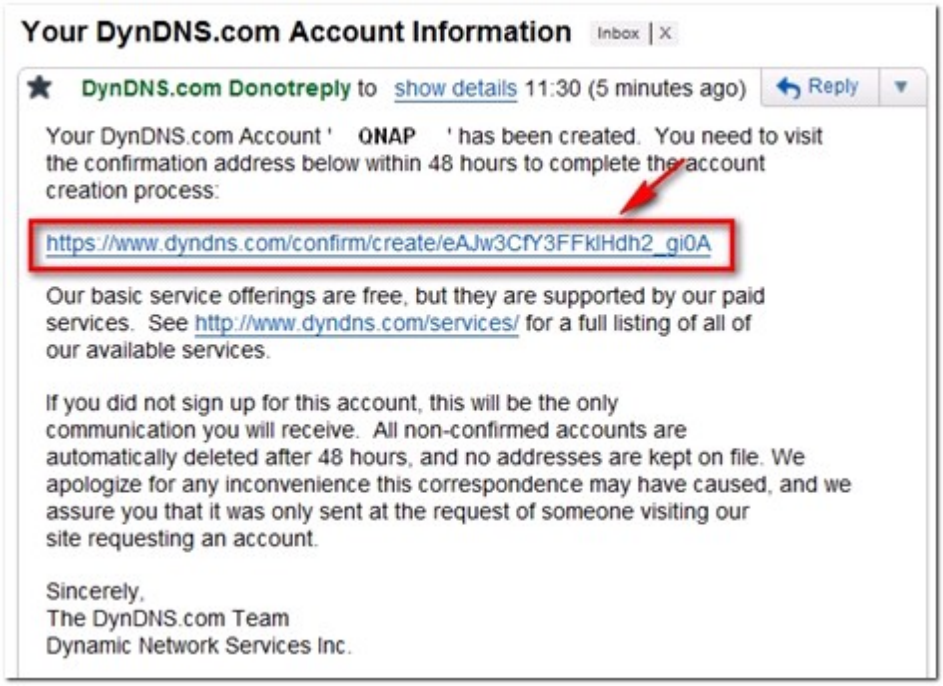
3. Complete the form to create a free account.



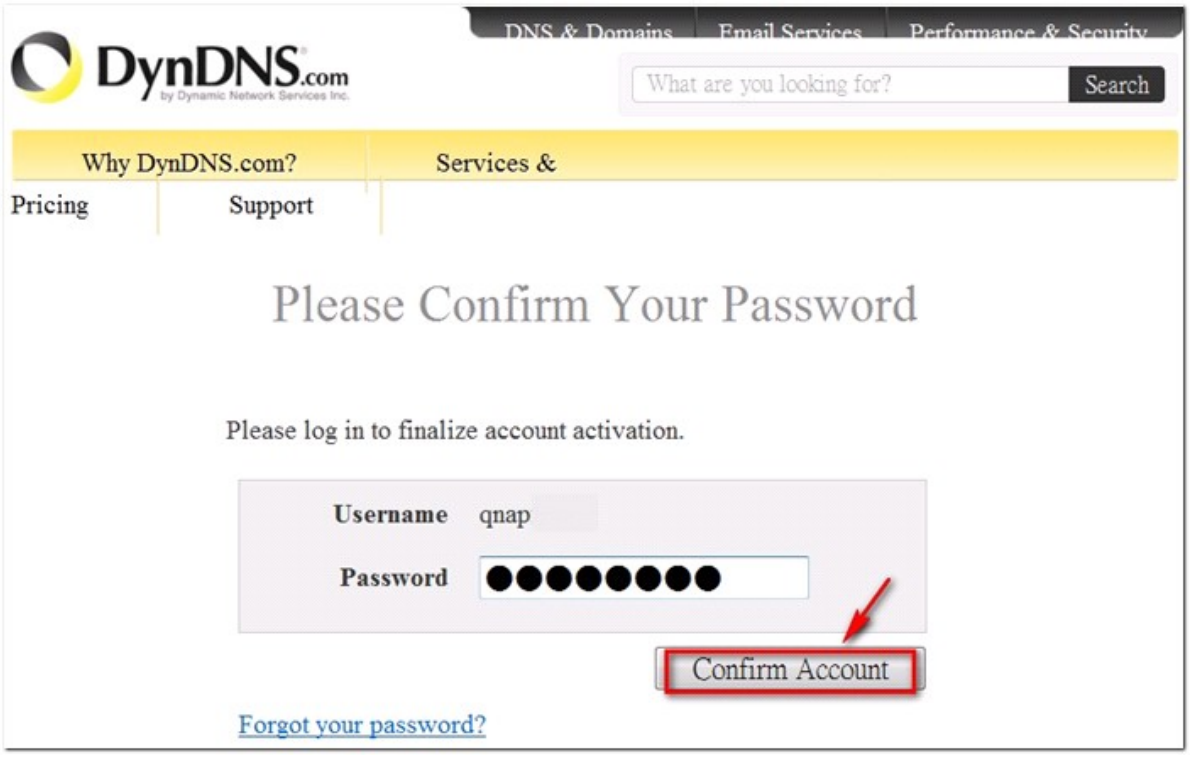
4. A confirmation email will be sent to the email address.



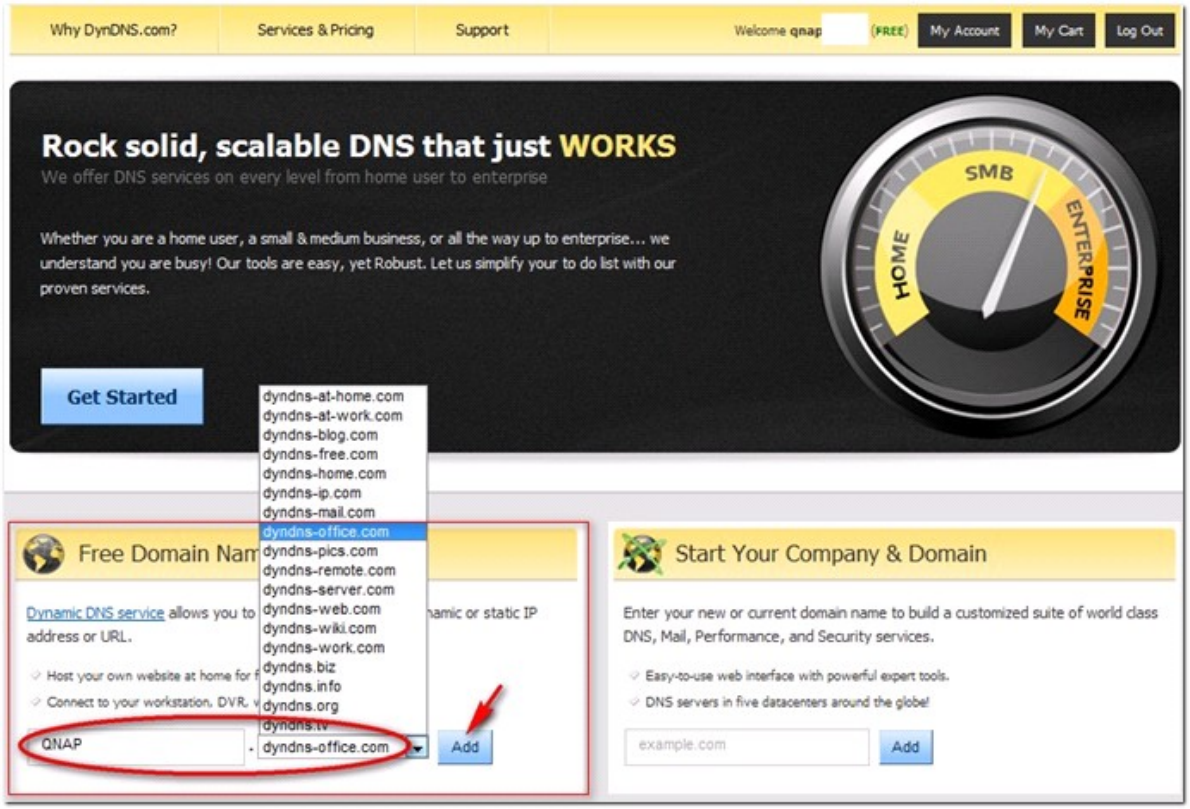
5. Click the link in the email for confirmation.



6. Click "Confirm Account" and login DynDNS.



7. Register a host name for the NAS. A host name is a unique name that identifies the NAS. Pick something you will remember. For example, fill in "QNAP" and select "dyndns-office.com". Then click "Add".

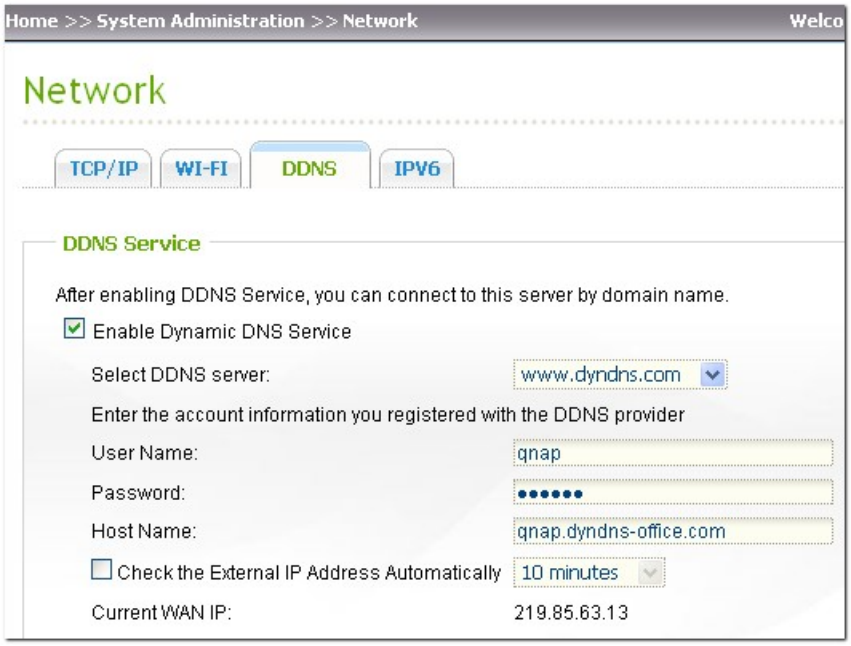


8. Activate the host name.

You can now login the NAS and set up the DDNS service.

Configure DDNS service on QNAP NAS

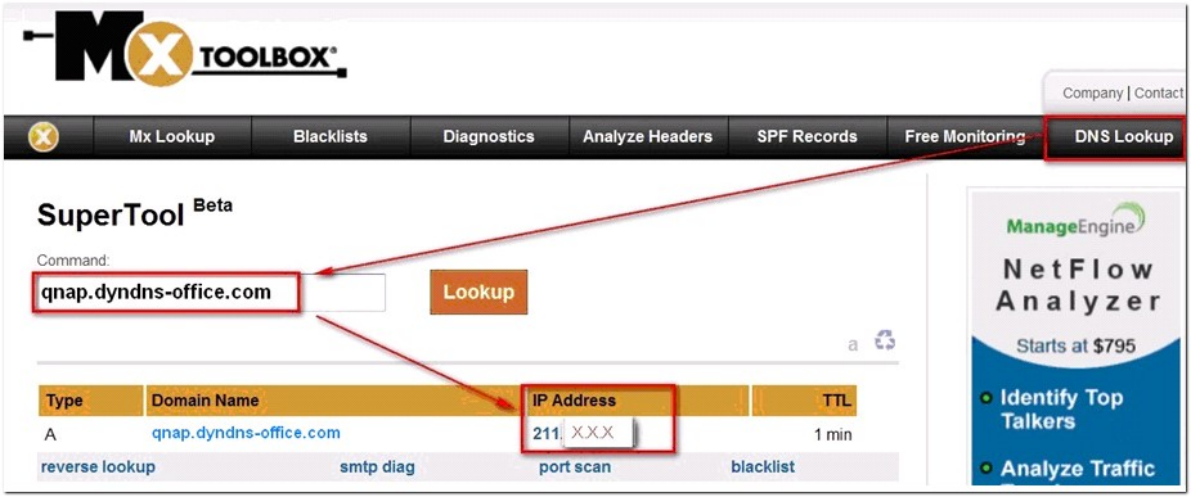
Login your NAS and go to "System Administration" > "Network" > "DDNS". Enter the DDNS information you registered from the DNS service provider. You may also schedule the NAS to update the DDNS record periodically by configuring the "Check the External IP Address Automatically" option.



After finishing the settings, the NAS will start to update the WAN IP to the DDNS provider for domain name mapping. You can now connect to the NAS by the domain name (qnap.dyndns-office.com) on the Internet.

Look up for your DNS if you need to verify:

To check that the domain name of the NAS is correctly mapped to its WAN IP, you may visit http://www.mxtoolbox.com/DNSLookup.aspx. Enter your domain name for DNS lookup and it will return your IP address.



Port Forwarding

If your NAS is located behind an NAT router, you need to open the ports of some services on the NAT router and forward these ports to the fixed LAN IP of the NAS so that you can connect to the services correctly from the Internet. This function is available on most routers in the market and is often known as "Port Forwarding", "NAT Server", or "Virtual Server". For example, to connect to the administration interface of NAS series, you need to open port 8080.

Current open service ports on QNAP NAS	
NAS Services	**Default Port**
Web-based system management	8080 (All models, TS-101/201 with firmware v2.3.0 or later)
Web-based system management	6000 (TS-100/101/201 firmware prior to v2.1.1)
FTP	21
Passive FTP	55536–56559
Web Server	80
Download Station (BT download)	6881–6999
Remote replication (Rsync)	873
Telnet	13131
SSH	22
SSL	443
SMTP	25
Samba	445
MySQL	3306
TwonkyMedia	9000

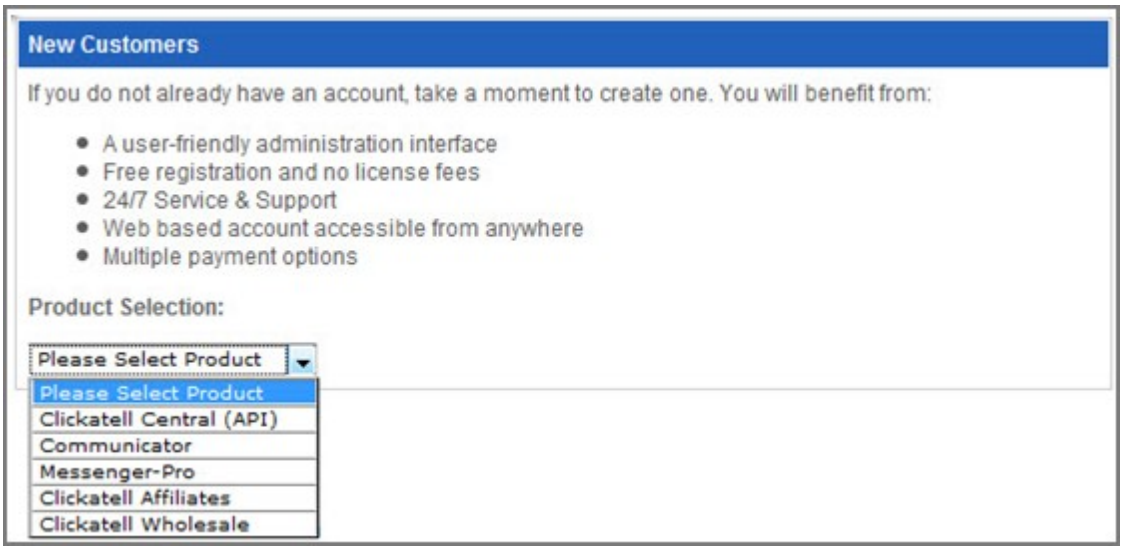
14. Set up SMS, Email, and IM Alert on QNAP NAS

The QNAP NAS supports SMS (Short Message Service), email, and Instant Messaging (IM) alert to inform users of system error or warning.
*TS-109/209/409/409U series only support email alert.

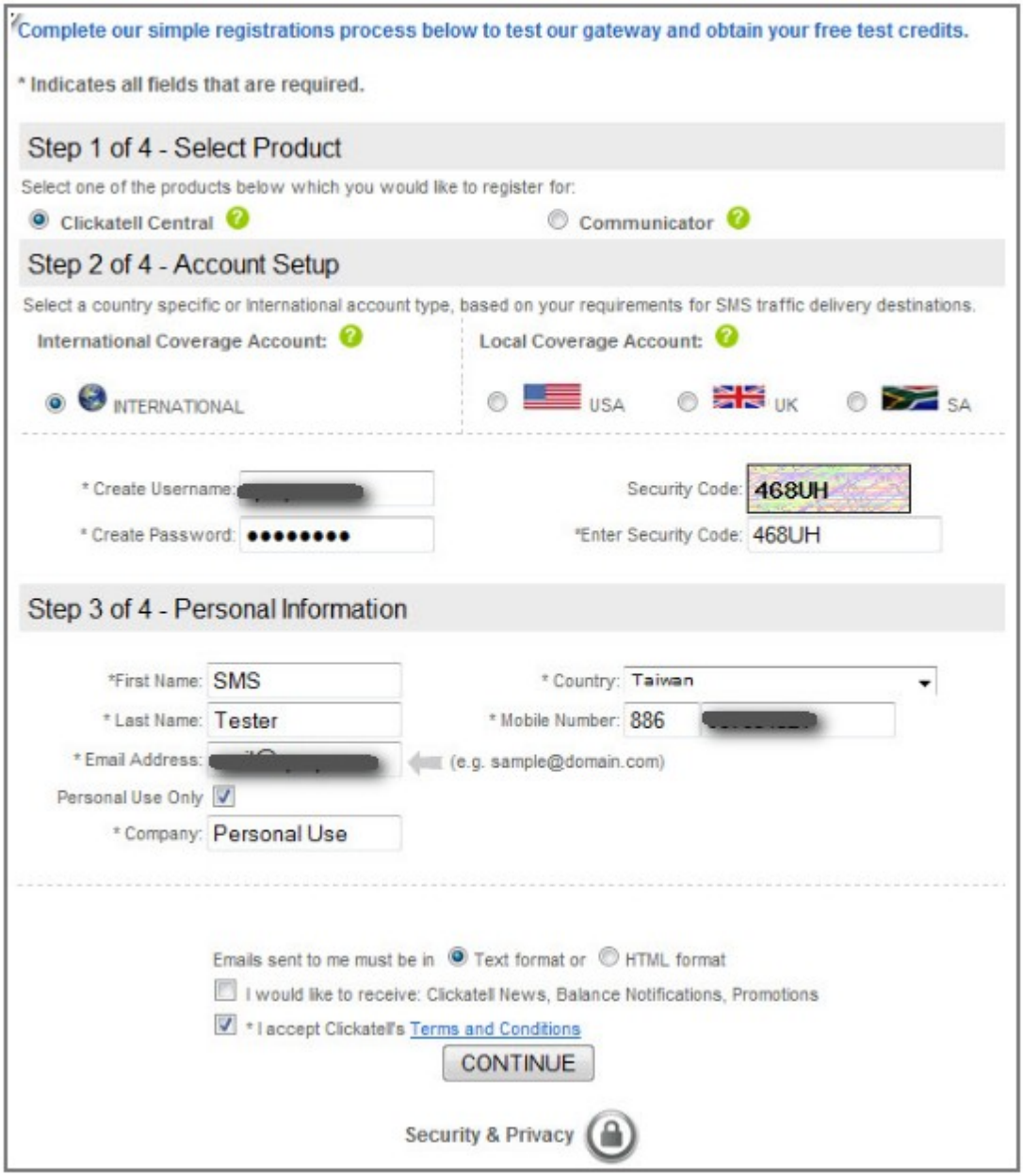
Set up SMS Alert

1. Sign up and set up an SMS service account

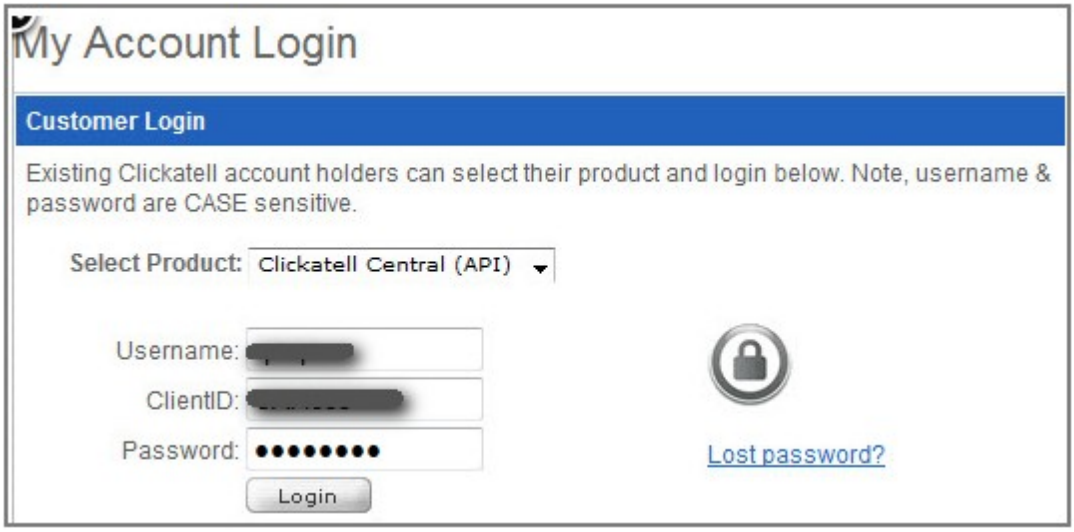
Clickatell will be used in this example. Go to Clickatell website http://www.clickatell.com/login.php. Under "New Customers" select "Clickatell Central (API)".



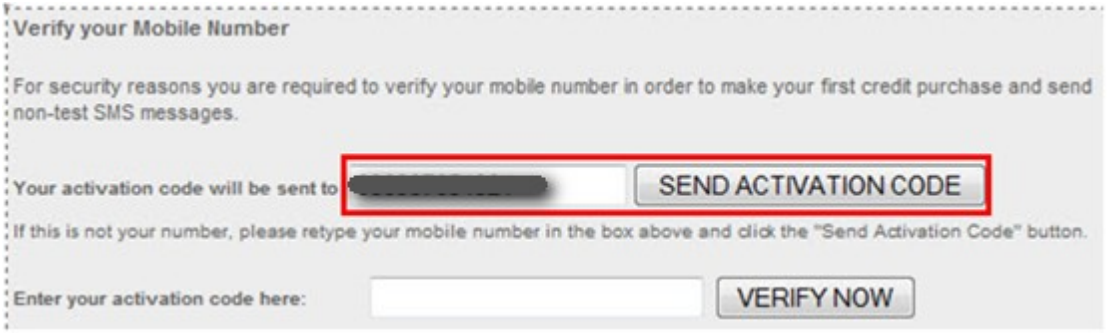
Fill out your personal information then click "Continue". Make sure you have carefully read the Terms and Conditions of the SMS service provider and that you agree to all the terms and regulations.



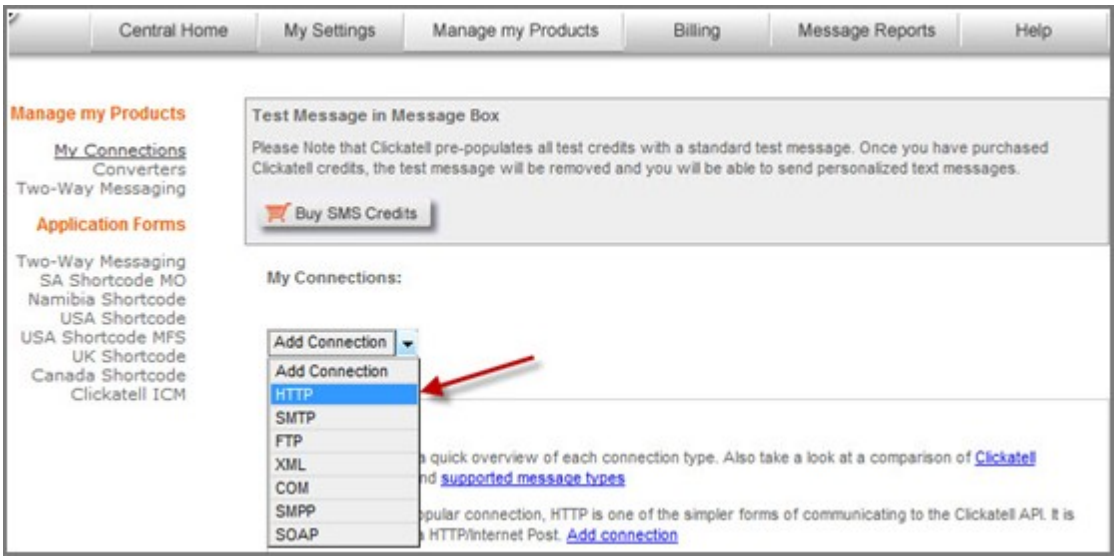
Upon successful registration you should receive an email containing the account activation link. You may now check your inbox to complete your account activation. By following the activation link you will be brought to the login screen as the image show below. Enter the password and click "Login".



Next verify your mobile number by entering an activation code sent by Clickatell after you enter your mobile phone number and click "SEND ACTIVATION CODE".



While still logged in with Clickatell, go to "Manage my Products" and select "HTTP" from "My Connections" dropdown menu.



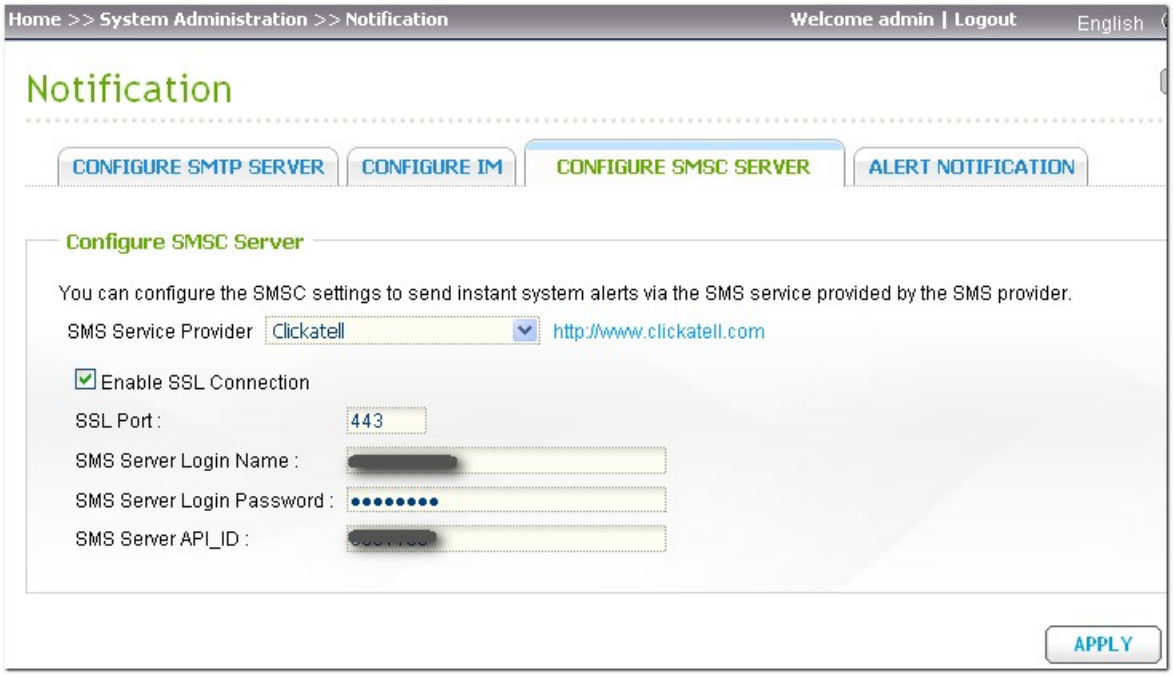
Set up the "HTTP API" by entering the minimum required information, the "Name", "Dial Prefix", and "Callback Type" as the image shown below. Click "Submit" once done.

You should now obtain an "API ID" that is required before using the SMS service. Write this down somewhere as we will need it for the setup in the NAS administration in the next step.

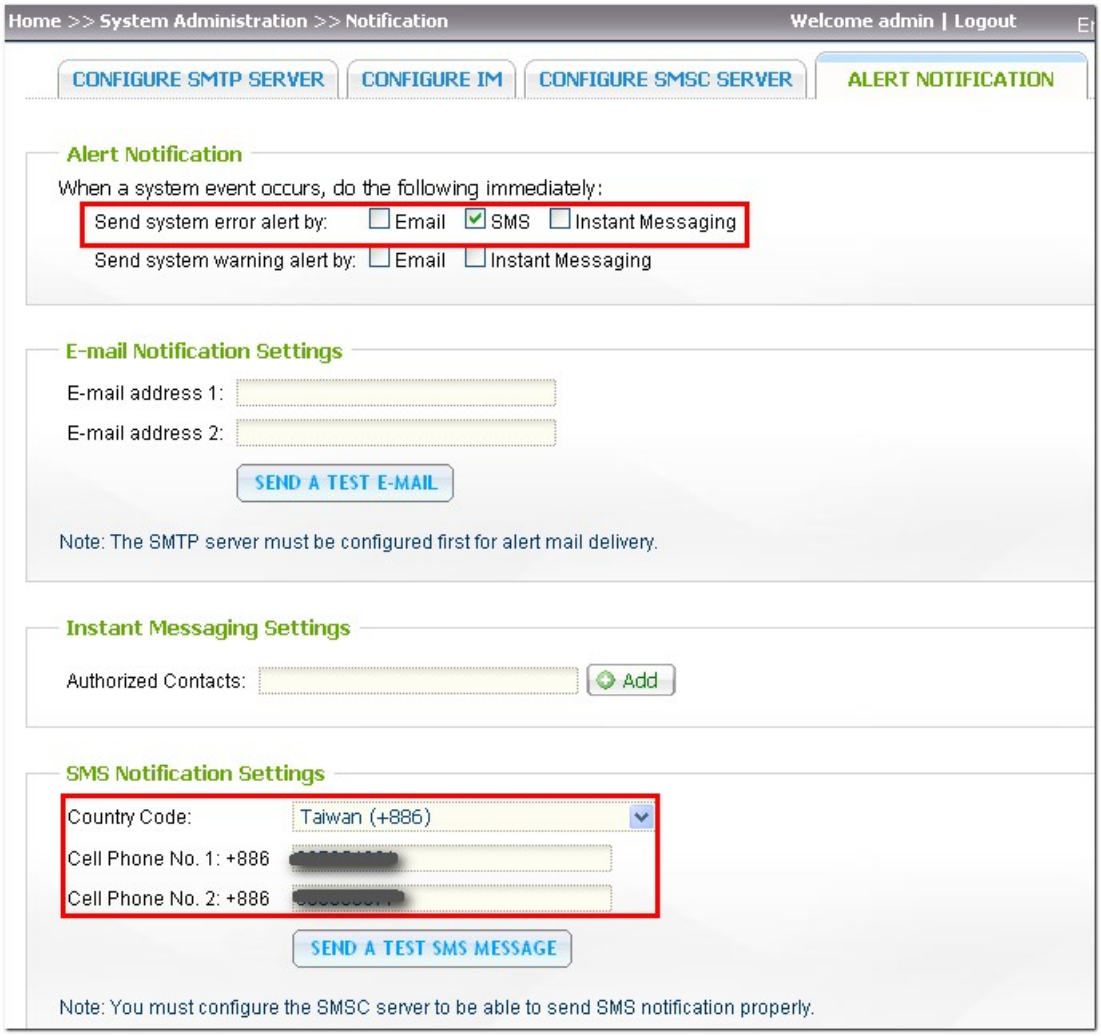
Up to this point you have completed the account registration and mobile number verifications with Clickatell and have successfully obtained an "API ID". You may now proceed to the next step.

2. Set the SMSC settings and SMS alert on the NAS

Go to "System Administration" > "Notification" > "Configure SMSC server" and enter the information we got from the previous step to configure the SMSC server.



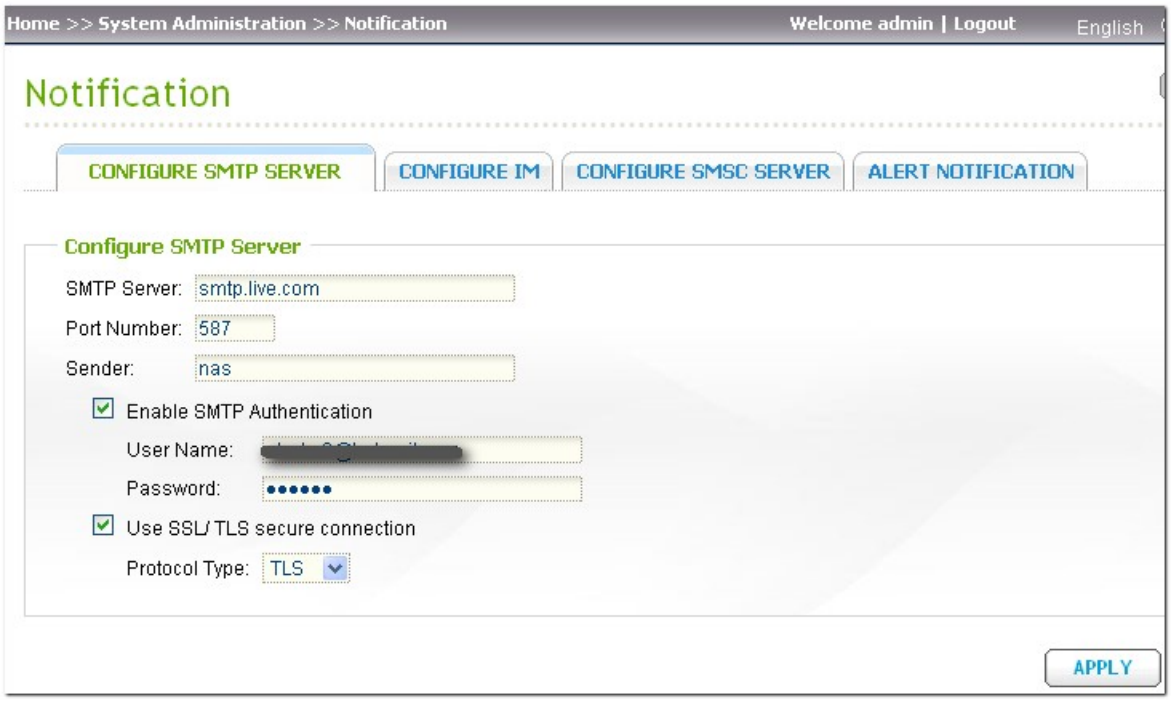
Next go to “System Administration” > “Notification” > “Alert Notification” and enter the mobile number (max 2) to receive the alert.



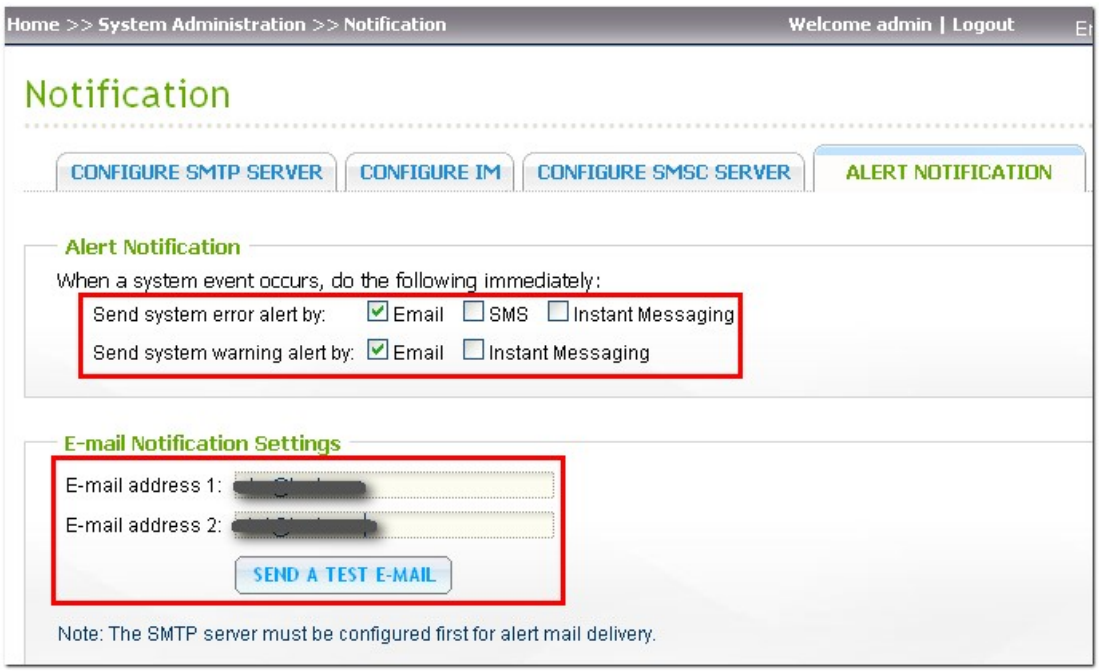
Congratulations! It is all set up and now you may want to test if your have configure the SMS notification properly by clicking “SEND A TEST SMS MESSAGE”. If nothing goes wrong you should be able to receive it in less than 10 seconds.

Set up Email Alert

Go to "System Administration" > "Notification" > "Configure SMTP server" and enter a valid SMTP information.



Next go to "System Administration" > "Notification" > "Alert Notification" and enter your email address and specify whether you want to receive system warning alerts too besides the system error alerts. Test if the email sending process works by clicking "Send a test e-mail".



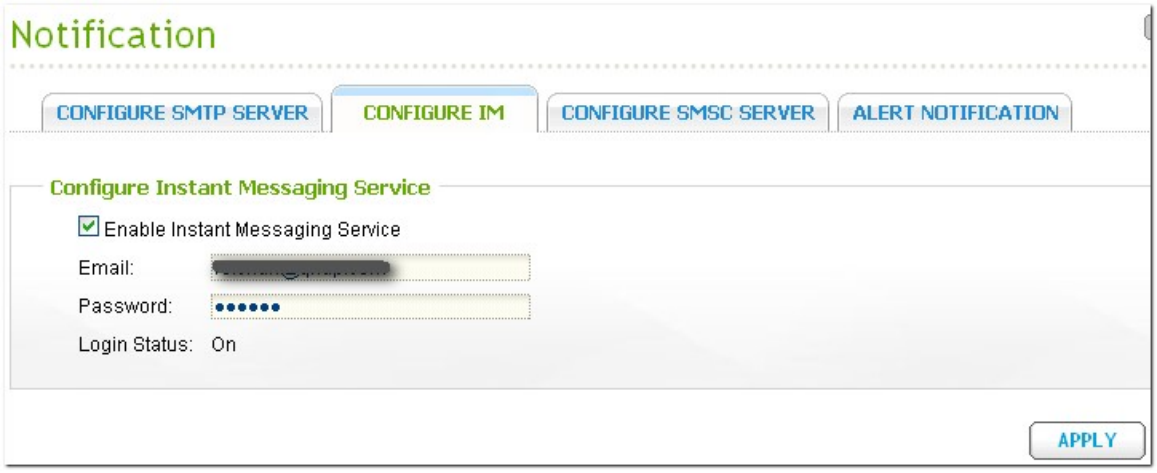
Set up Instant Messaging (IM) Alert

1. Sign up a Windows Live ID for the NAS from https://signup.live.com/.

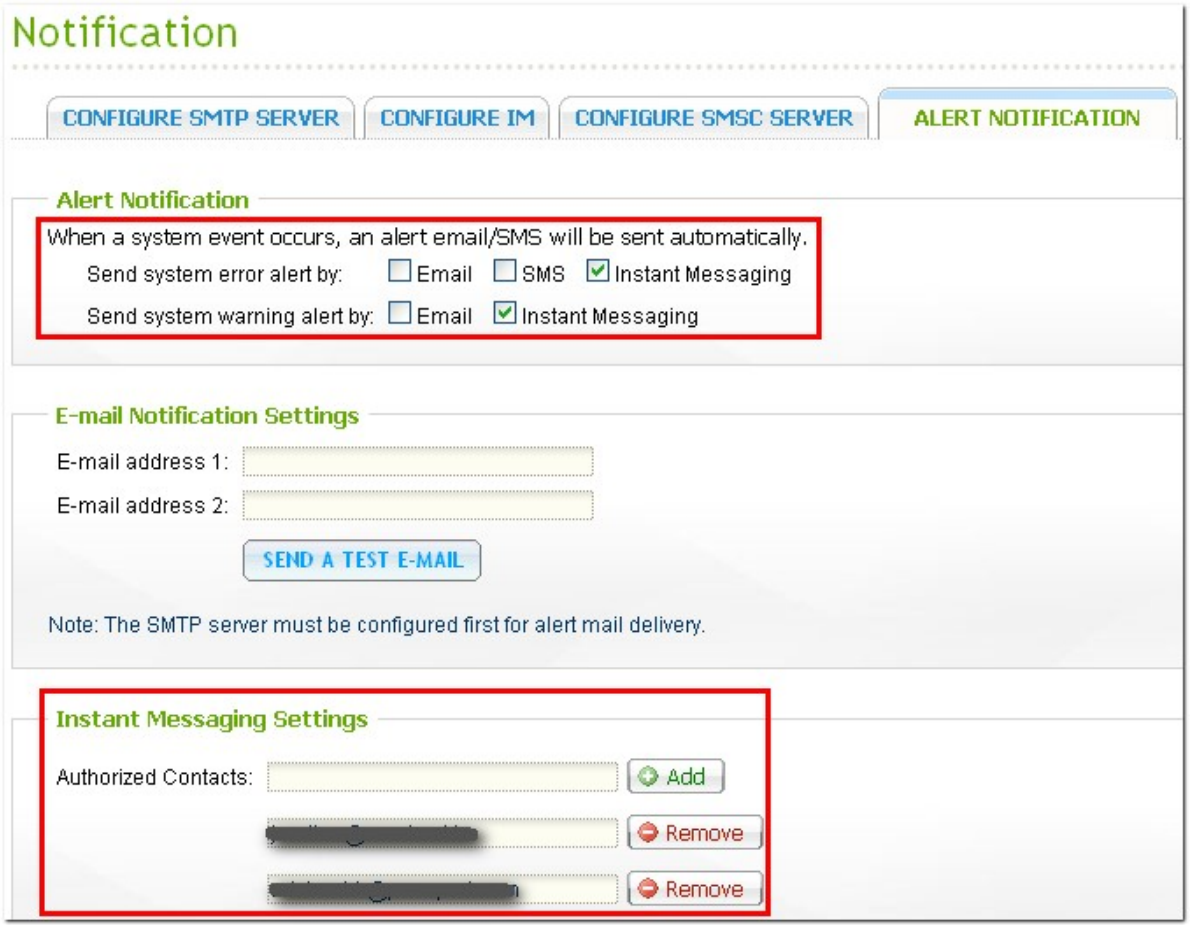
2. Download Windows Live Messenger for your Windows OS from http://explore.live.com/. The NAS supports Windows Live Messenger 2009 or above.

3. Login the Windows Live Messenger account registered in Step 1. Add the authorized contacts. Make sure these contacts have also added the Messenger account of the NAS.

4. Go to "Notification" > "Configure IM" and enter the login information registered in Step 1. Click "Apply". The login status will be shown as "On".



5. Go to "Notification" > "Alert Notification". Enable alert notification by Instant Messaging and enter the authorized contacts (up to 10) under "Instant Messaging Settings". Click "Apply".



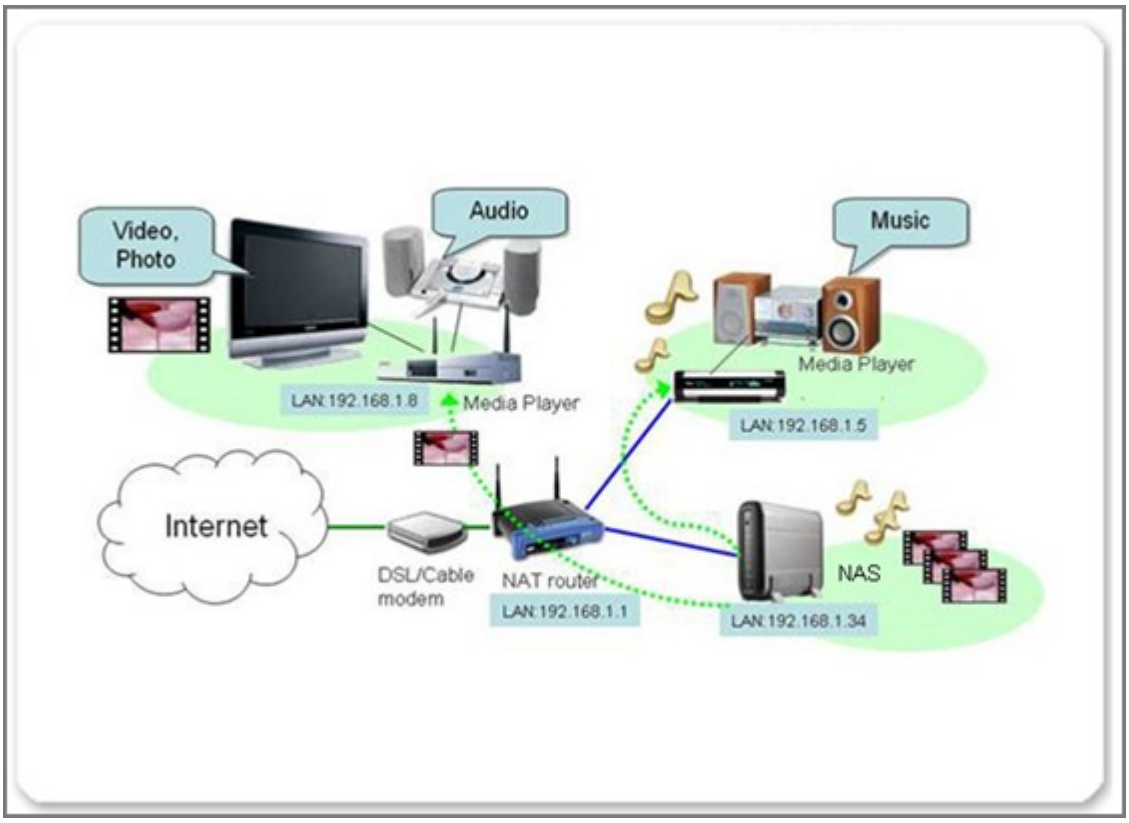
6. Login an authorized Windows Live Messenger account and interact with the NAS via Windows Live Messenger. The NAS will send instant error or warning alerts (English only) to the authorized contacts when events occur.

The authorized Windows Live Messenger contacts can enter the following command to inquire real-time system information from the NAS. The information is available in English only.

Command	Description
help	A list of command options will be shown.
info-cpu	Inquire the current CPU temperature.
info-sys	Inquire the current system temperature and fan speed.
info-model	Inquire the NAS model number.
info-hd	Inquire the number of hard disks on the NAS.
info-hd-[hd#]	Inquire the current temperature and S.M.A.R.T. status of a hard disk. For example, info-hd-1.
info-vol	Inquire the number of disks volumes on the NAS.
info-vol-[vol#]	Inquire the information of a disk volume. For example, info-vol-1.

15. Set up UPnP Media Server for Media Playing

This section shows you how to set up the UPnP media server on QNAP NAS to share the multimedia files to the media player on the local network and play them in the home entertainment system.

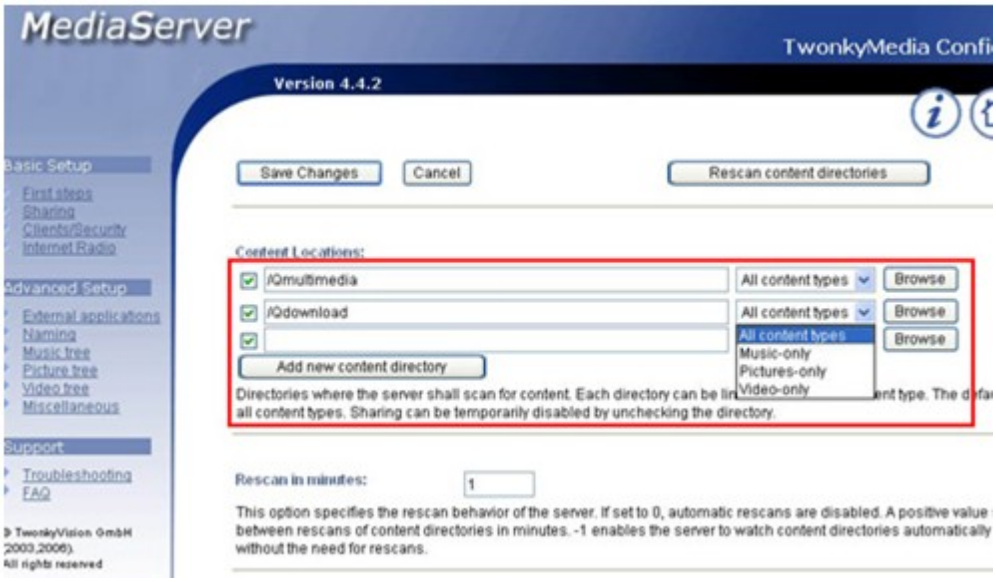


Enable UPnP Media Server

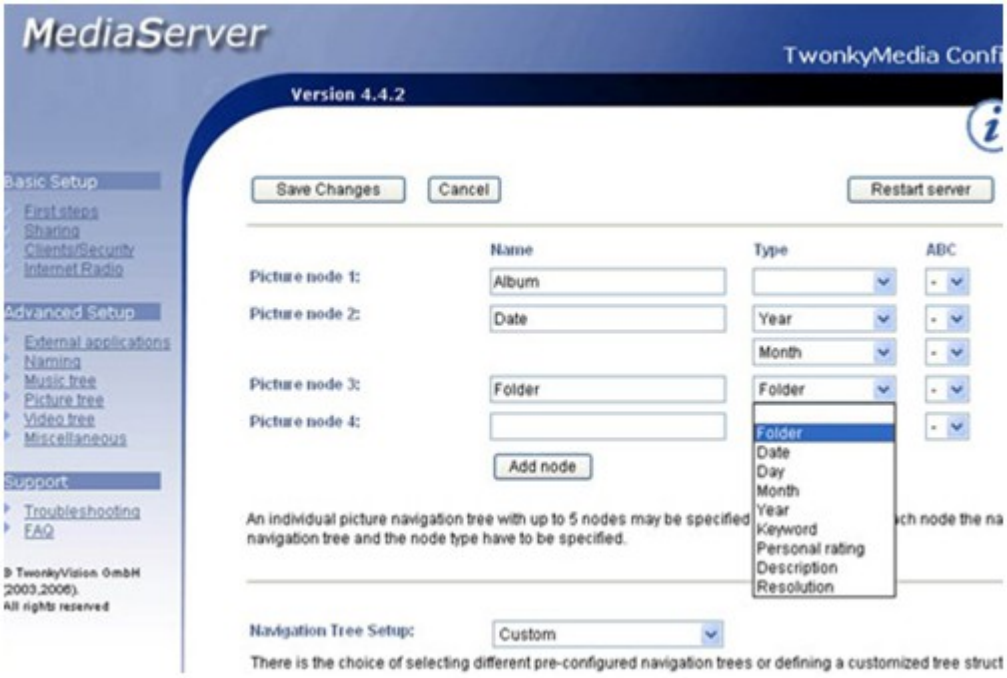
Go to “Application Servers” > “UPnP Media Server” and select the option “Enabled UPnP Media Server” and click “Apply”. The UPnP Media Server function is now ready.

Set up TwonkyMedia Server

The TwonkyMedia version shown in this example is 4.4.2. The actual version the NAS supports may vary from time to time without notice.
Point the web browser to http://NAS IP:9000, you will enter TwonkyMedia configuration page. You can specify the locations of the contents you would like to share in your home network under the "Content Locations". Simply type in the path to the contents on your QNAP NAS (default folder is Qmultimedia or Multimedia). In the example, we added an extra share /Qdownload.



For ease of browsing if you have a large amount of media contents, you can configure the navigation tree for your photos, videos, and music. You can sort your media contents on the TV easily.



When you have completed the configuration, make sure you have clicked the button “Save Changes” to save the settings.

You can now move the MP3, images, and videos to the Qmultimedia or Multimedia folder or any custom folders you added via Windows mapped drives or FTP to the NAS for your media player.

Set up the connection of media player

About physical wiring
We use a high definition (HD) media player with QNAP NAS is this example. The media player is used to receive the streamed multimedia file sent by your UPnP media server on the NAS, then transcode these files to your TV or Hi-Fi system. Because of the limited cable length of these interfaces, normally you have to place your media player near your TV and Hi-Fi system.

About TCP/IP settings
Connect your media player to the LAN at your home and set to acquire the IP address by DHCP. (Most of the media players are defined as DHCP client, which obtains an IP address automatically from the network.)

Connect the video and audio output of the media player to your TV

The media player may provide different video and audio interfaces, such as Composite video/audio output, S-Video for video output, S/PDIF digital audio, or HDMI interface which can carry both video and audio signals.

Example 1 (Buffalo LinkTheater)

In this example, the video out and audio out cables are connected to the TV. You can also connect audio out to your stereo acoustic system.

Turn on the TV that is connected to the media player, you can select the options available by the remote control of the media player. The media player will find the NAS on the network. The NAS name will be displayed on the screen.

You will find the photos, video, and music shared by the specified folder on the NAS. You can use the remote control of the media player to select and play the files.

Example 2 (ZyXEL's DMA-1000W)

ZyXEL DMA-1000W is one of the models which are based on SigmaDesigns' platform.

If your TV provides an HDMI interface, both audio and video signals can be carried by the single cable. Simply connect your media player to your TV by an HDMI cable.

If your TV does not provide an HDMI interface, you can connect an S-Video cable to your TV for video output, and connect Composite left/right audio interface for audio output. If you look for higher quality of music playing, you can use an S/PDIF cable to connect the media player to your Hi-Fi system.

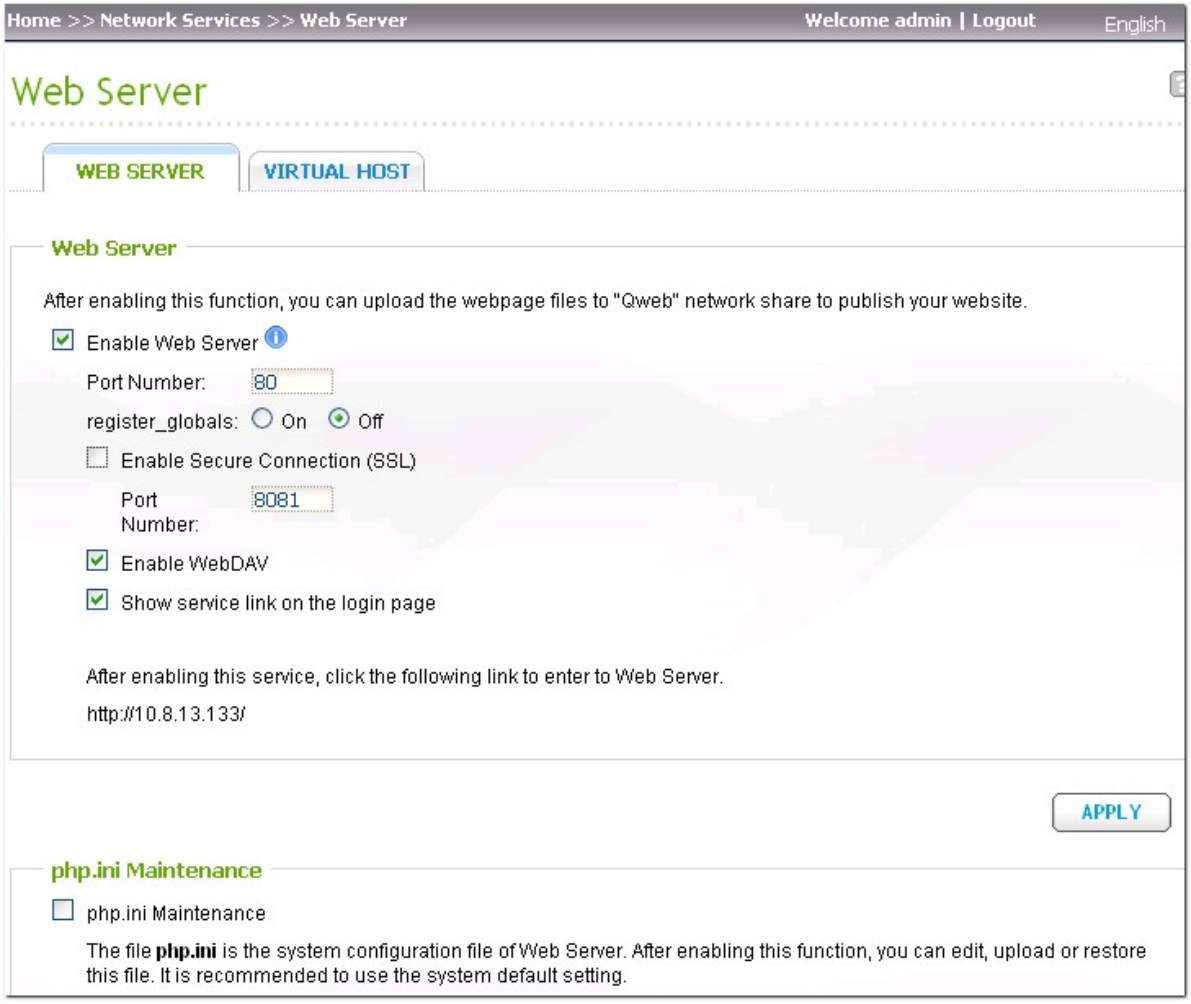
Turn on and switch your TV to the correct interface (HDMI or S-Video). Use the remote control of the media player to enter the “Server” page, the media player detects the NAS automatically. You can now play the multimedia files or listen to the Internet radio from the NAS.

16. Host a Forum with phpBB on QNAP NAS

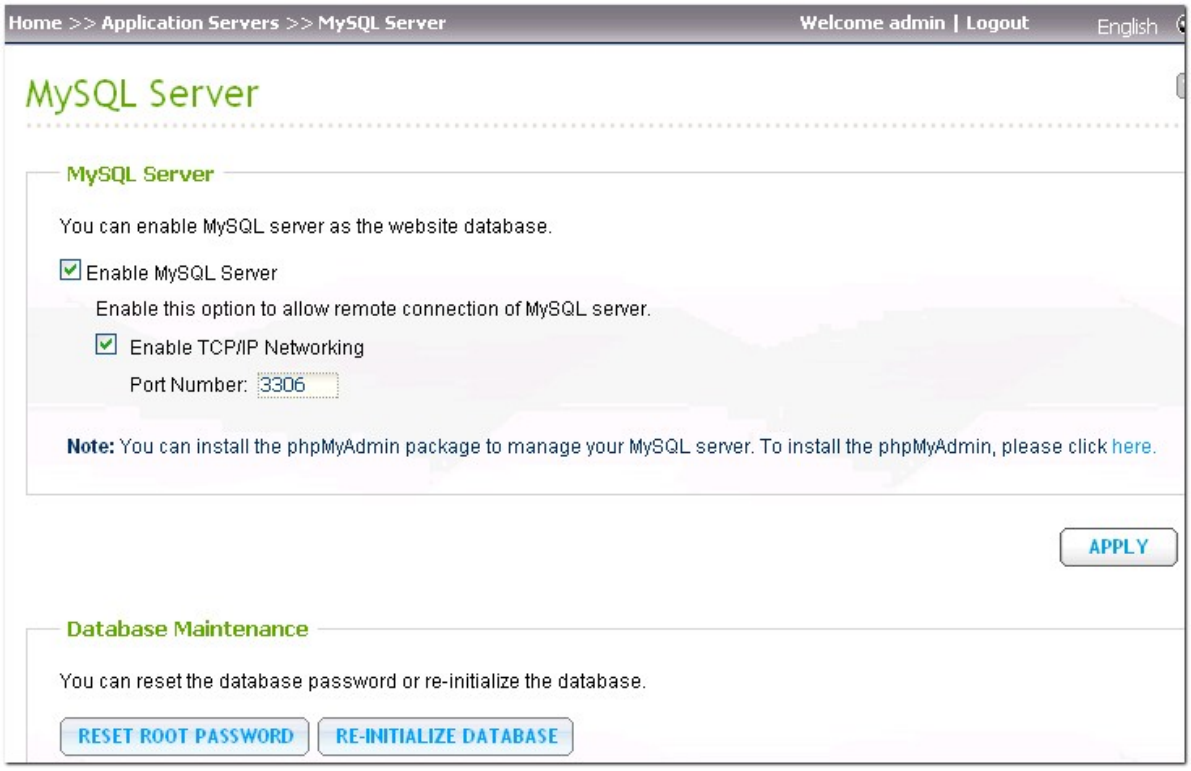
This section shows you how to host a forum with the popular open source forum software phpBB on QNAP NAS.

Activate the web server and MySQL database server

Login the administration page of the NAS and go to "Network Services" > "Web Server". Select the option "Enable Web server" and click "Apply".



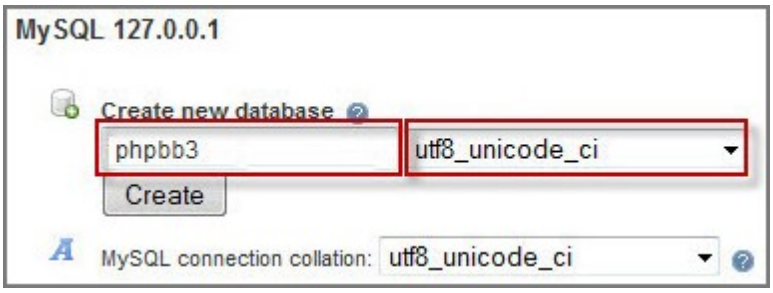
Next go to “Application Servers” > “MySQL Server” and select both “Enable MySQL Server” and “Enable TCP/IP Networking” then click “Apply”.



Create a database for phpBB3 in phpMyAdmin

Prior to installing phpBB3, create a new database for it and we will use phpMyAdmin to create the database so install phpMyAdmin QPKG if you do not have it running on the NAS yet. Once installed point the browser to http://NAS-IP/phpMyAdmin/ and enter the user name and password to login (default user name and password is root/admin). You can also select your preferred language.

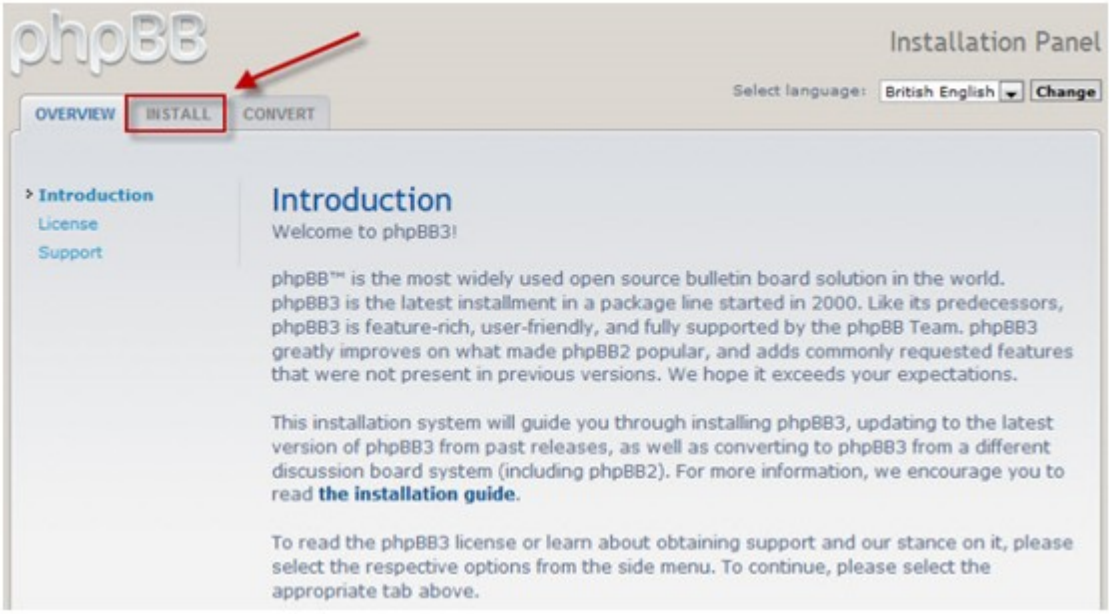
Once in, enter the database name "phpbb3" in the field says "Create new database" and choose a default encoding language you prefer (UTF-8 for best compatibility) then click "Create". Then, proceed to the next step.



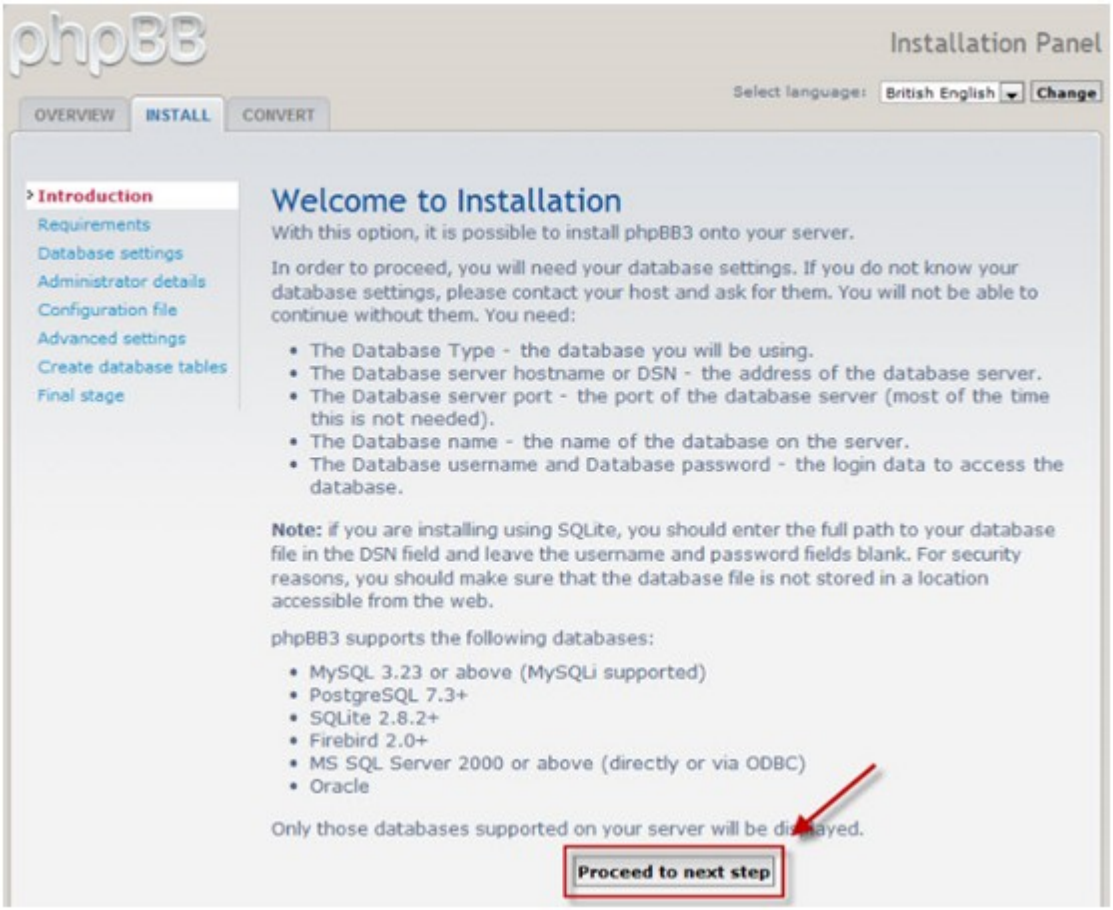
Start the phpBB3 web-based installation

Download the phpbb3 source archive from http://www.phpbb.com/downloads/olympus.php and download the [Full Package] one and unzip it to Qweb or Web network share.

Point your browser to "http://NAS-IP/phpBB3" and you should see the phpBB3 web-based installation page like below. Click "INSTALL" tab to start.

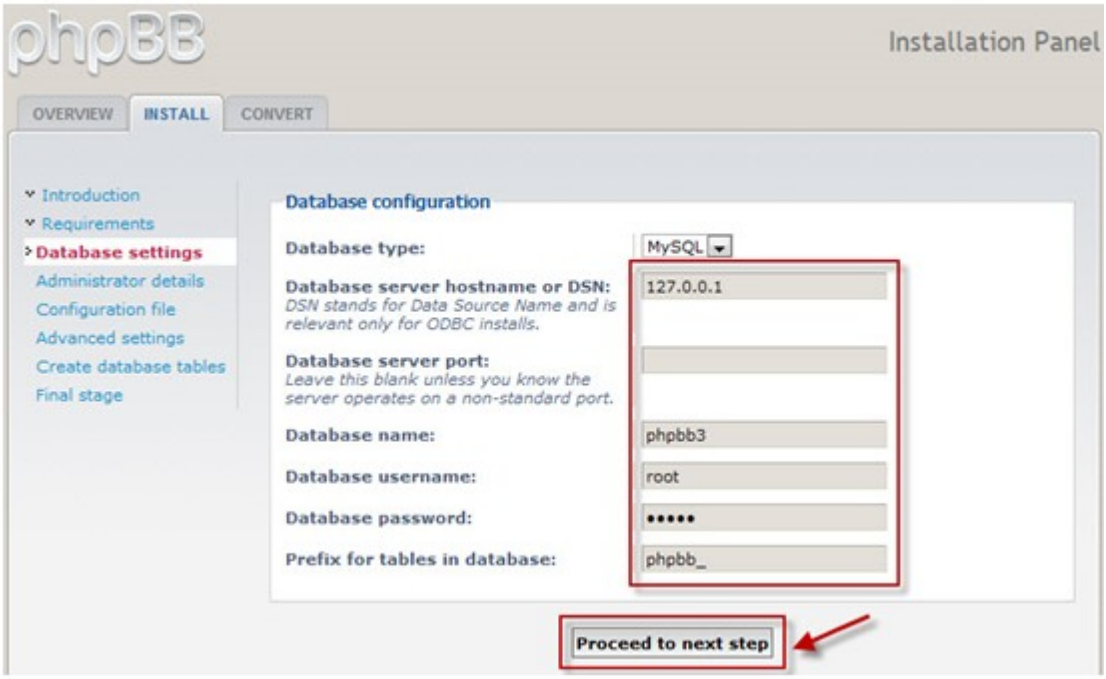


Click “Proceed to next step”.

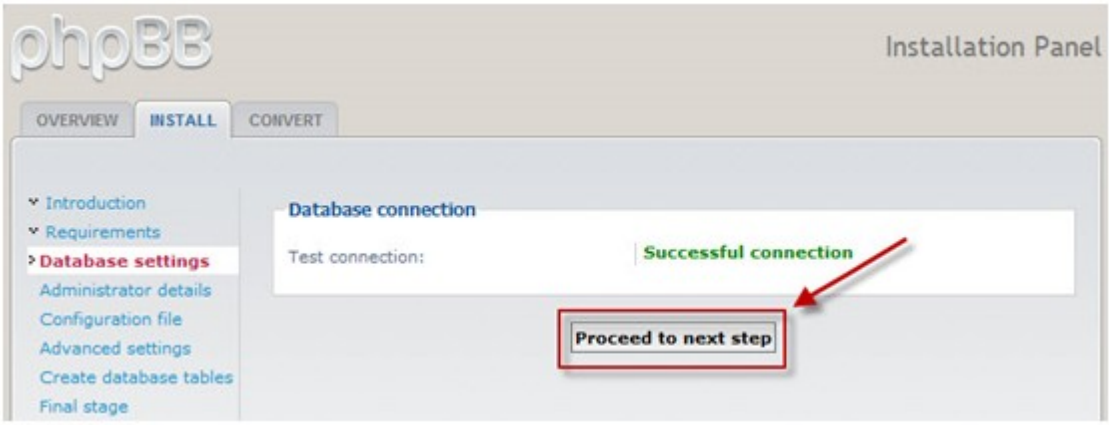


The installation compatibility page will be shown. In most of the cases your current web server should be compatible with the requirements so click “Start install” to go the next step.

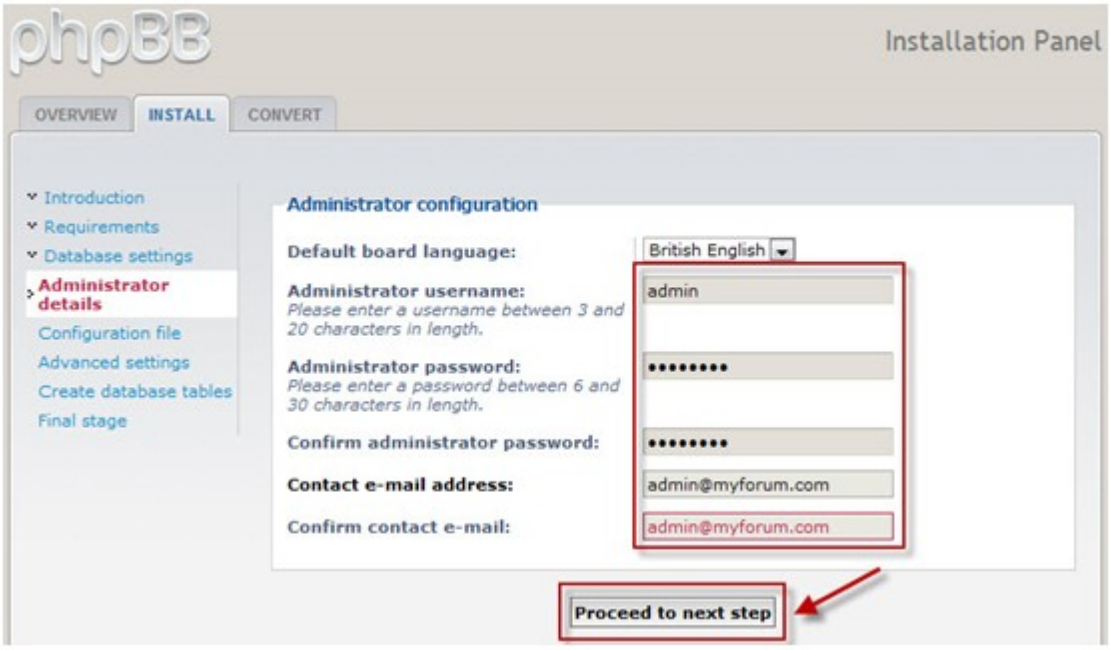
Fill up the fields with your MySQL information including the host name, database name, database username, and database password then click “Proceed to next step” to continue.



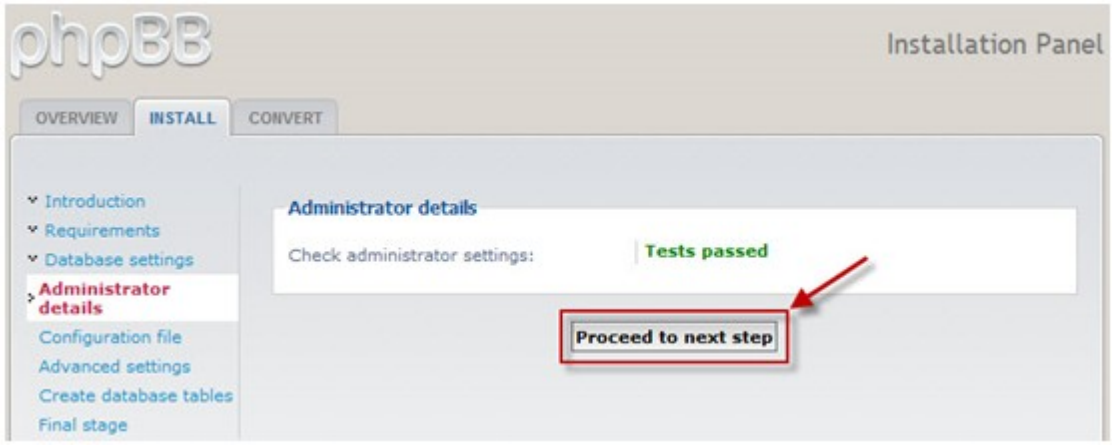
You should see “Successful connection” if your MySQL server is running and the database “phpbb3” we created earlier is present. Click “Proceed to next step”.



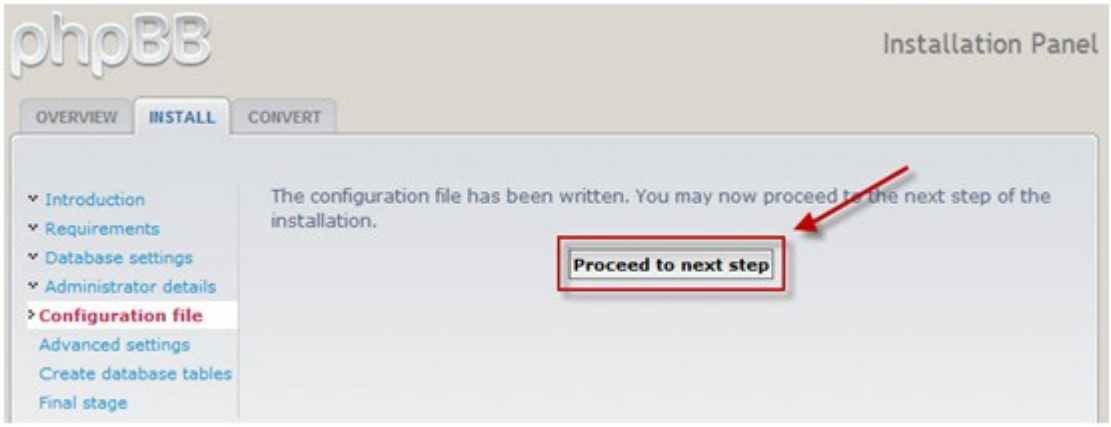
Specify the phpBB3 administrator username and password as well as a valid email address. Once done, click “Proceed to next step”.



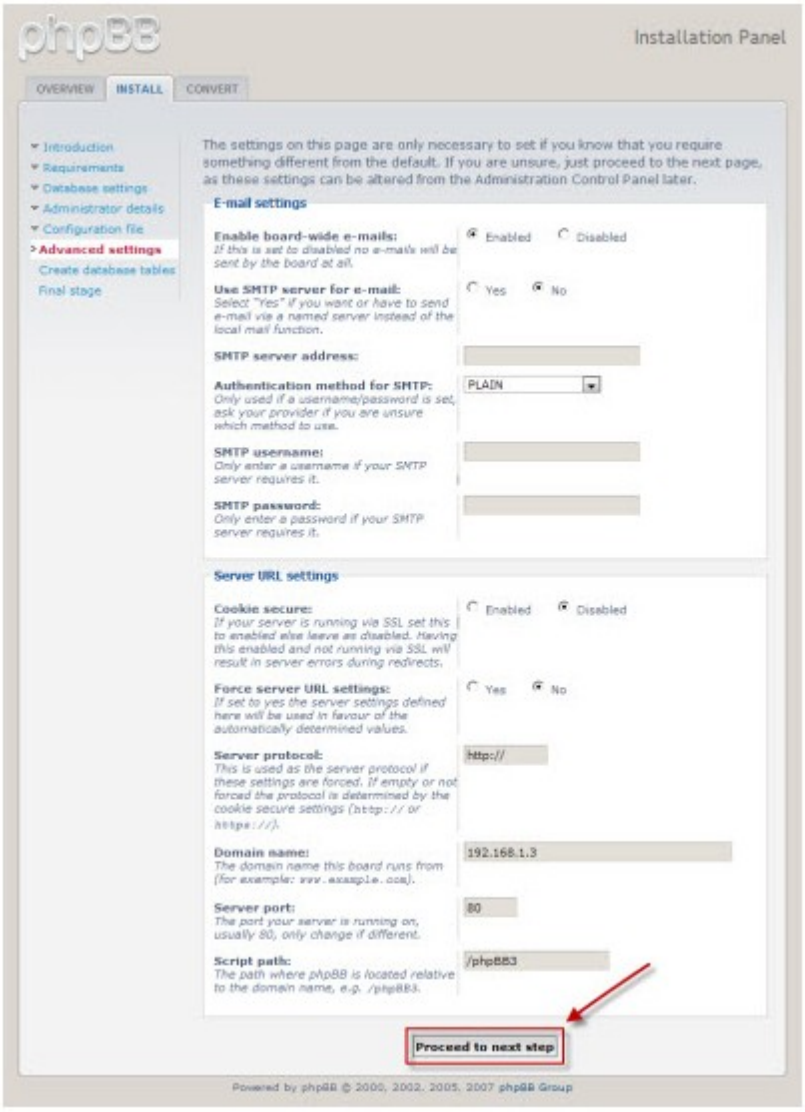
You should see “Tests passed” and click “Proceed to next step”.



phpBB3 writes all the settings information to a configuration file (config.php) at this stage. Click “Proceed to next step”.

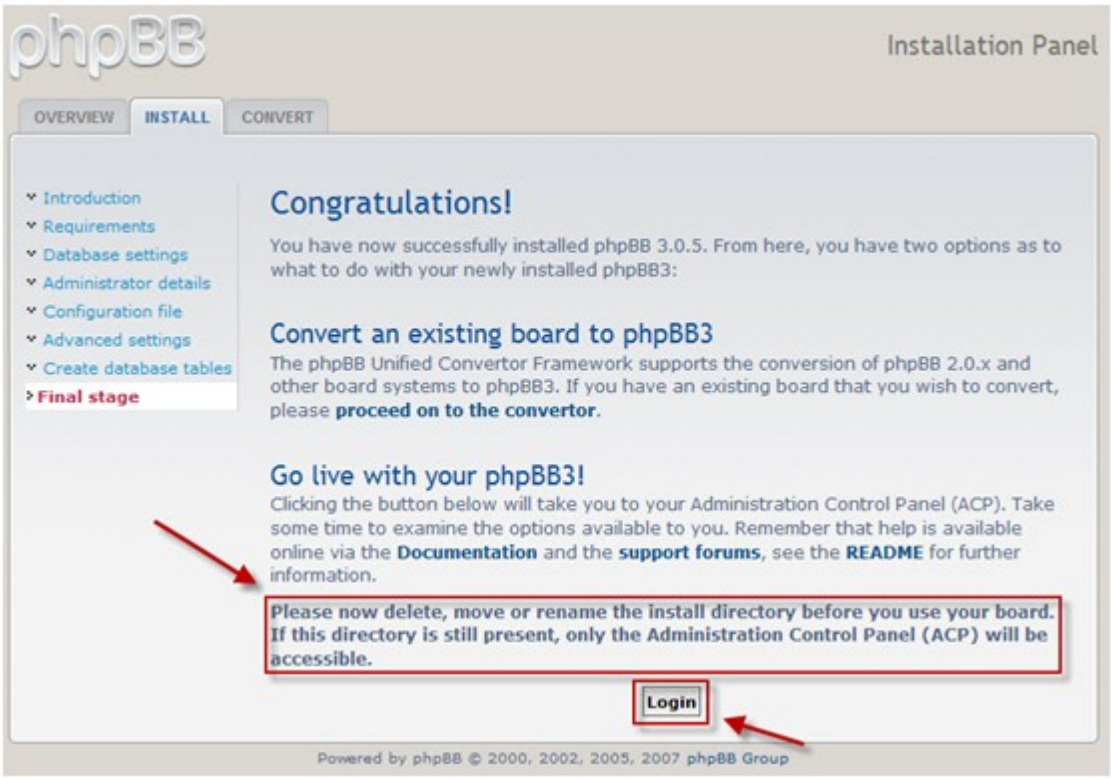


Specify advanced settings if you wish then click “Proceed to next step”.

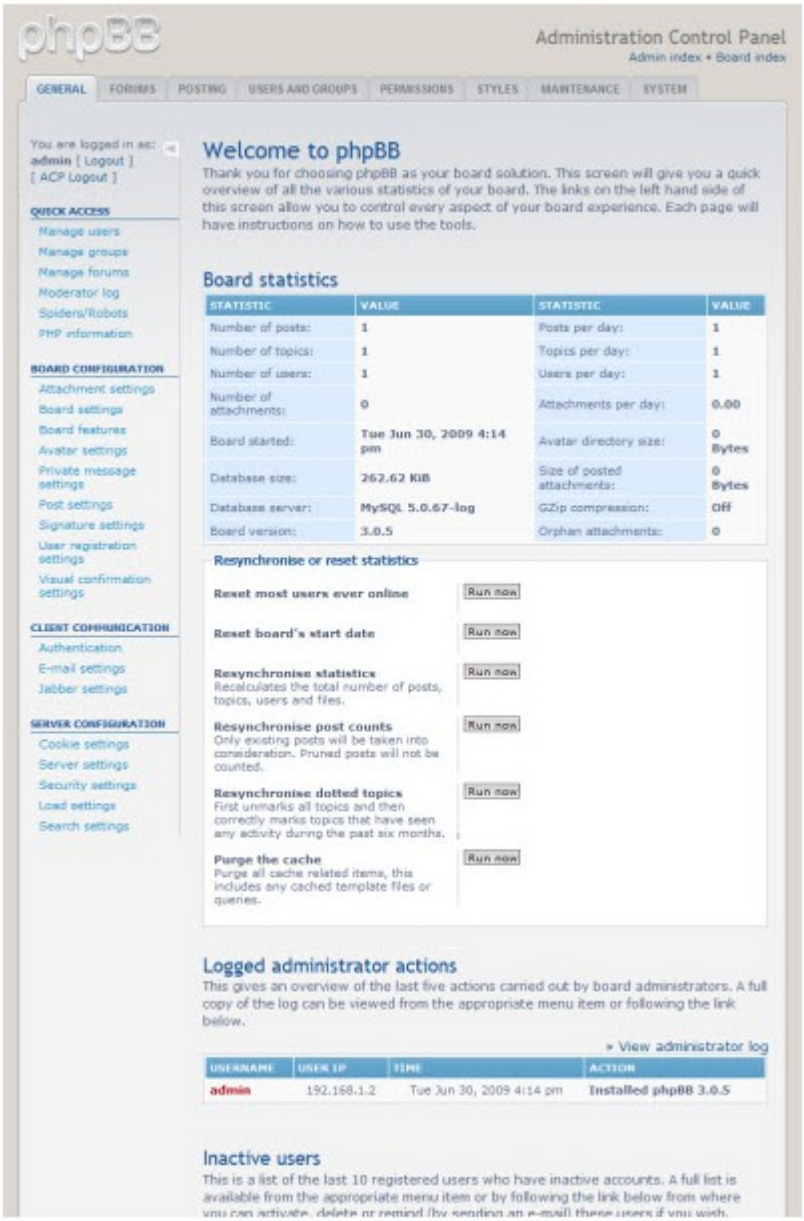


phpBB3 creates all the database tables and populates some initial data at this stage. Click “Proceed to next step”.

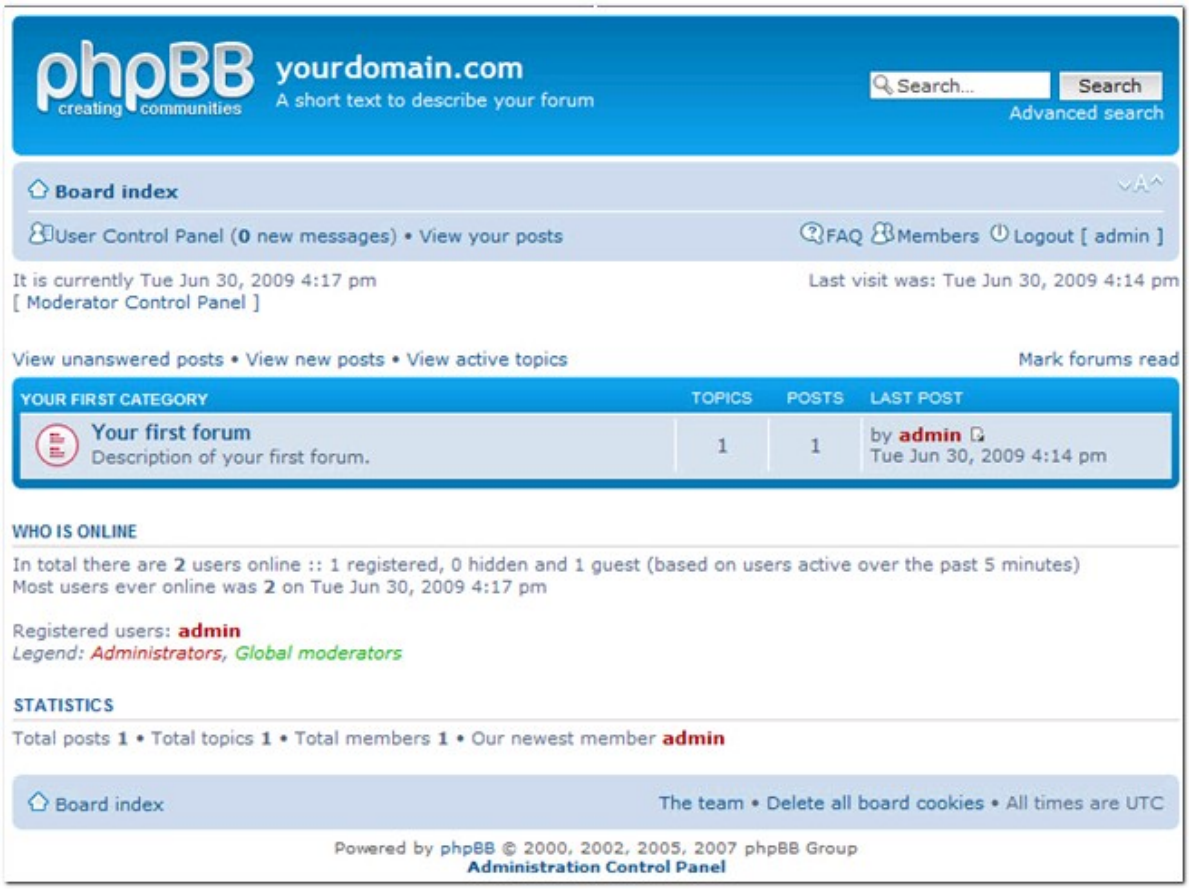
Now there is one more thing you need to do is that you have to delete the installation folder located under the phpBB3 folder. Once deleted you can click “Login” to enter the administration page of phpBB3.



This is the phpBB3 Administration Control Panel where you can perform all administrative tasks.



This is the front page of your freshly installed phpBB3 forum. Start sending out forum invitations to establish your online community.



17. NAS Maintenance Settings

System Restart/Shutdown 691
System Temperature Protection 693

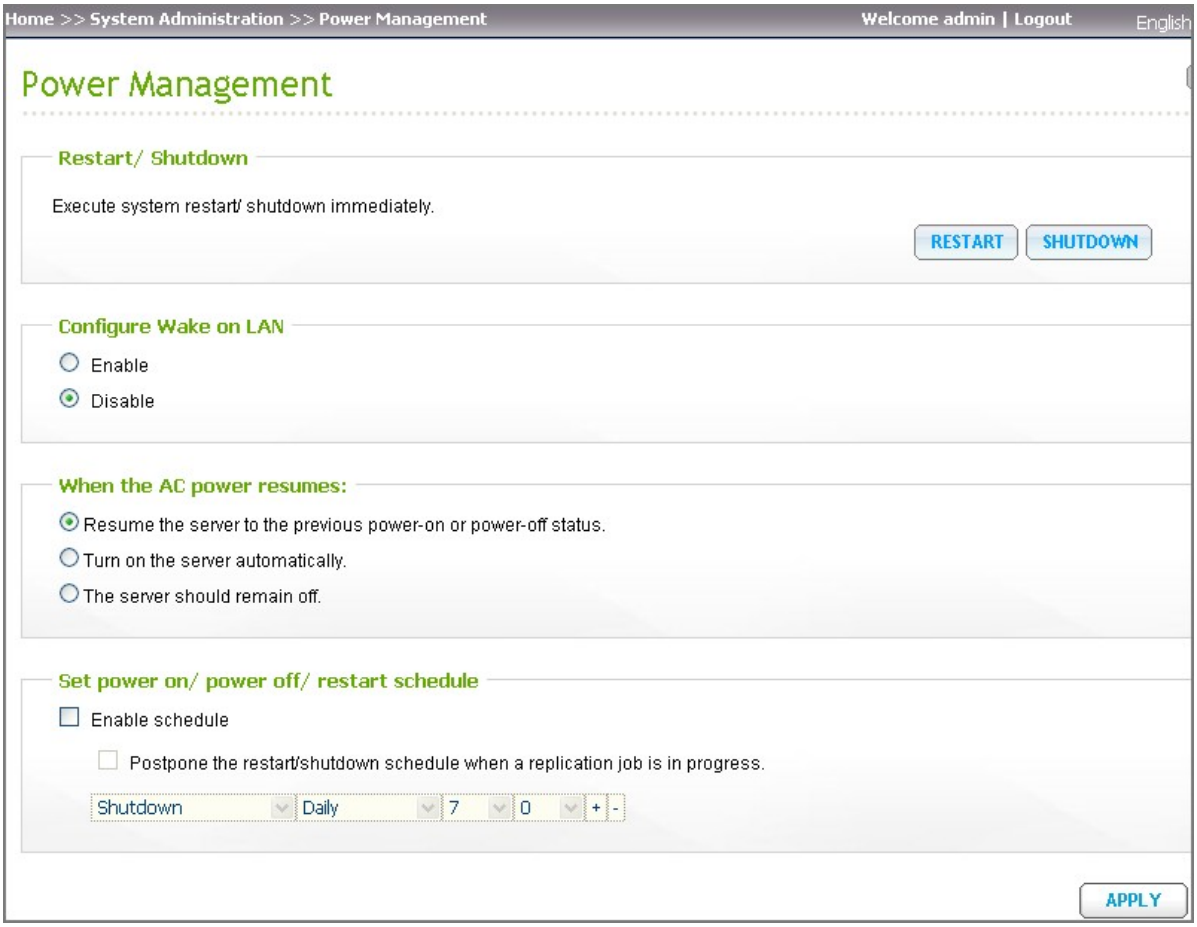
17.1 System Restart/Shutdown

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

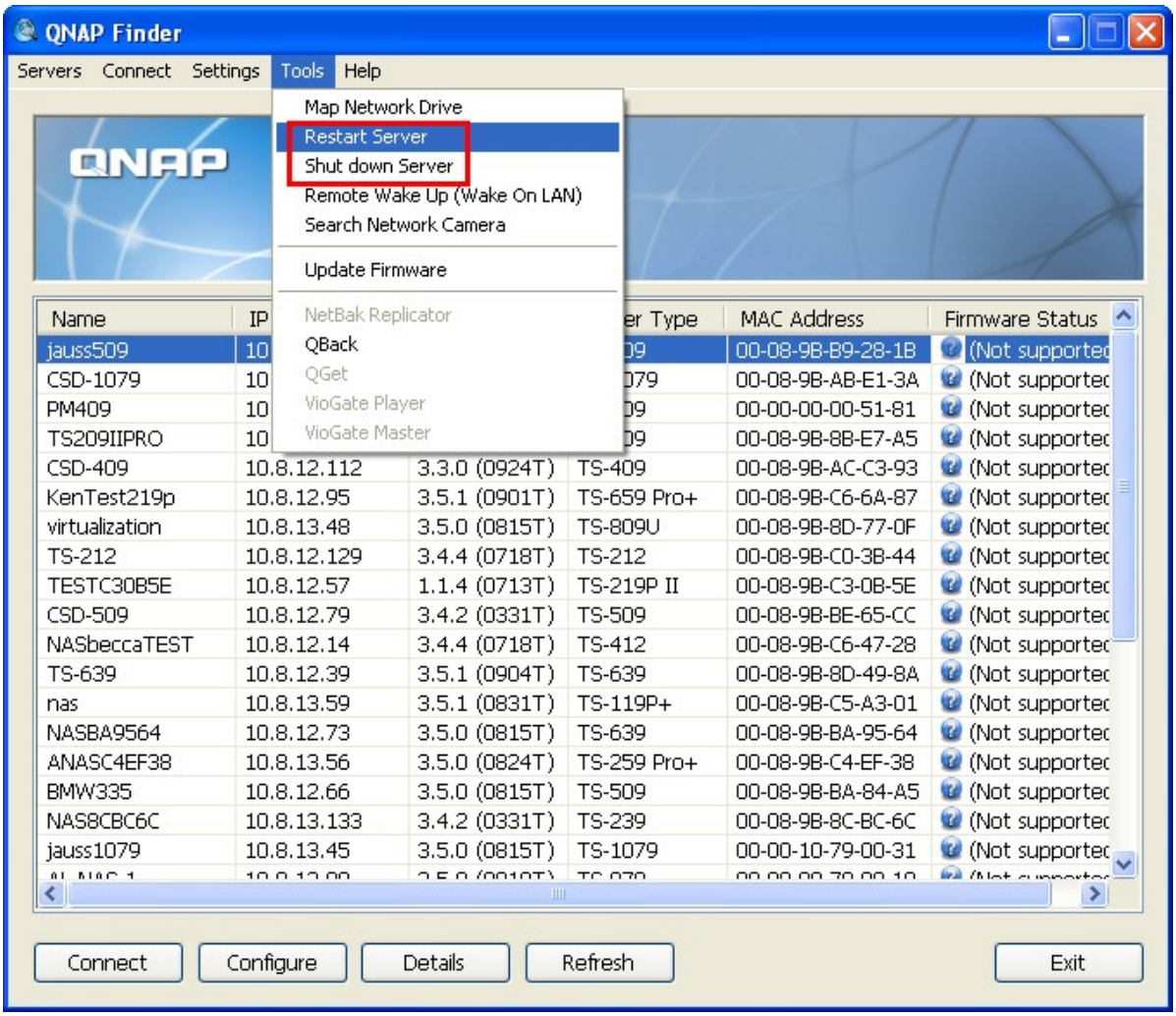
1. Login the NAS as an administrator. Go to "System Administration" > "Power Management".
2. Click "Restart" to reboot or "Shut Down" to turn off the NAS.

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 NAS 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.



Use the Finder to restart or shut down the NAS (administrator access required).



17.2 System Temperature Protection

The NAS 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 drives exceeds 65°C (149°F) continuously after 15 (5+10) minutes.

18. GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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